



DV-IP User Manual

Company and Product Information

Disclosure to Third Parties

This document may not be copied to, given to, copied by, or discussed with any third party other than Dedicated Micros without first obtaining the express permission in writing from Dedicated Micros.

All reasonable steps have been taken to ensure that this publication is correct and complete, but should any user be in doubt about any detail, clarification may be sought from Dedicated Micros, or their accredited representative. The information in this document is subject to change without notice and should not be construed as a commitment by Dedicated Micros. Dedicated Micros accepts no responsibility for any errors that may appear in this document

Regional Contacts

DEDICATED MICROS UK

Customer Services:

Tel: + 44 161 727 3244

Fax: + 44 161 727 3346

e-mail: customerservices@dmicros.com

Technical Support:

Tel: + 44 161 727 3243

Fax: + 44 161 727 3346

e-mail: uksupport@dmicros.com

DEDICATED MICROS USA

Customer Services:

Tel: + 1 800 864 7539 ext. 2000

Fax: + 1 703 904 7743

e-mail: customerservices@dmicros.com

Technical Support:

Tel: + 1 800 864 7539 ext. 2001

Fax: + 1 703 904 7743

e-mail: ussupport@dmicros.com

DEDICATED MICROS ASIA

Customer Services/Technical Support:

Tel: +65 6285 8982

Fax: +65 6285 8646

e-mail: asiastsupport@dmicros.com

DEDICATED MICROS AUSTRALIA

Customer Services:

Tel: +612 9634 4211

Fax: +612 9634 4811

e-mail: mrromer@dmicros.com

Technical Support:

e-mail: aussupport@dmicros.com

DEDICATED MICROS EUROPE

Customer Services:

Tel: + 49 243 352 580

Fax: + 49 243 352 5810

e-mail: infobox@dmicros.com

Technical Support:

Tel: + 49 243 3525 826

Fax: + 49 243 3525 820

e-mail: eusupport@dmicros.com

DEDICATED MICROS MALTA

Customer Services:

Tel: + 356 2148 3673/4

Fax: + 356 2144 9170

DEDICATED MICROS MIDDLE EAST & AFRICA

Customer Services:

Tel: + 971 (4) 390 1015

Fax: + 971 (4) 390 8655

Mobile: + 971 (50) 4500 149

e-mail: SI@dmicros.com

Technical Support:

e-mail: support@dmicros.com



Note: Feedback on this user documentation should be sent to the Marketing Department in the UK office of Dedicated Micros Ltd.

Contents

Introduction	1
1. Important Safety Information.....	2
1.1 Read these Instructions First	2
1.2 Power Sources.....	2
1.3 Servicing.....	2
1.4 Ventilation.....	2
1.5 Lifting and Handling.....	3
1.6 Storage.....	3
2. Introduction to the DV-IP	4
Installation	5
3 Installing the DV-IP Unit	6
3.1 Unpacking.....	6
3.2 The CD ROM	6
3.3 Web Browsing PC Requirements	6
3.4 DV-IP Viewer PC Requirements	7
3.5 Physical Set-up	7
3.5.1 Location Guidelines	7
3.5.2 Electrical Connections	7
3.6 Setting up the DV-IP Network Connection.....	8
3.6.1 Connecting to the DV-IP Using a Terminal Program.....	8
3.6.2 Permanent Network Settings	10
3.6.3 Dynamic Host Configuration Protocol (DHCP).....	12
3.6.4 Testing the Network Configuration of DV-IP	12
3.7 DVIP Communication Ports	14
3.7.1 RS232 Communication Ports (Com1, 2, 3, and 4 male D-Type)	14
3.7.2 RS485 Communication Ports (Com3 and 4 male D-Type)	14
3.7.3 DM-485 Bus.....	14
Configuration.....	15
4 Accessing the Configuration Screens	16
5 Configuring Cameras and Global Recording Parameters	18
5.1 Configuring Country Specific Information	18
5.2 Configuring the High, Medium, and Low View Levels.....	20
5.3 Configuring the Cameras	21
5.4 Configuring the Standard Recording Size, Resolution, and Expiry	21
5.5 Configuring the Standard Recording Rates	22
5.6 Configuring the Variable Record Set-up	23

6	Configuring the alarms.....	25
6.1.1	Configuring the Alarm Input.....	25
6.1.2	Configuring an Alarm Zone.....	26
6.1.3	Configuring the Events and Alarms Database.....	28
6.1.4	Configuring the DV-IP for the Alarm Receiving Centre	28
6.2	Configuring Image Protection	29
6.2.1	Configuring Alarm Zone Image protection	29
6.2.2	Removing Protection from Images.....	30
6.3	Configuring Automatic FTP Transfers.....	31
6.4	Configuring the Alarm Schedule	32
6.5	Configuring the Holiday Profiles and Timer Functions.....	33
7	Configuring VMD	35
7.1	Configuring Generic VMD Options.....	35
7.2	Configuring VMD Actions for a Camera	35
7.3	Configuring the VMD zones for a Camera.....	36
7.4	Configuring VMD Image Protection.....	38
8	Configuring the system settings.....	39
8.1	Configuring the Network Settings	41
8.2	Configuring the RS232 Ports	42
8.3	Setting up Coaxial Telemetry	43
8.4	Configuring Matrix Telemetry.....	43
8.5	Configuring RS232 DM* Commands Telemetry	44
8.6	Configuring Telemetry Image Compression	44
8.7	Audio Set-up	45
8.8	Adjusting the size of the RAMDisk	46
8.9	Configuring the Webcams.....	46
8.10	Configuring and Testing Relays.....	48
8.11	Enabling the System Features.....	49
8.12	Resetting the DV-IP Unit	49
8.13	Configuring the Logs.....	49
8.13.1	Viewing the Connection Log	50
8.13.2	Viewing the Anonymous FTP log.....	50
8.13.3	Viewing the Security Log.....	50
8.13.4	Accessing the Logfile	50
8.13.5	Accessing Logfile backup	51
9	Advanced Configuration	52
9.1	Configuring the Text in Images	52
9.2	Protecting the DV-IP Unit Using Passwords	53
9.2.1	Default Passwords.....	53
9.2.2	Configuring Password Protection on the DV-IP Unit	53
9.3	Default TCP/IP Port Mappings.....	57
	Operation.....	59
8	Operating DV-IP.....	60

8.1	Supported Systems	60
8.2	Using the Live Page	60
8.3	Using the DuoView™ Display	63
8.3.1	Using the DuoView™ to Compare Live and Replay Footage.....	64
8.3.2	Using the DuoView™ to View Eight Live Cameras in Two Quad Displays.....	64
8.4	Recording to a PC or to Network Storage	65
8.5	Installing the DV-IP Viewer Software	65
8.6	Setting Up Watermarking	68
Reference Information		69
10	Reference information	70
10.1	Service	70
10.2	Regulatory Notes FCC and DOC Information	70
10.3	CE Mark.....	70

Introduction

In this section

- **Safety information**
- **Introduction to the DV-IP**

1. Important Safety Information

1.1 Read these Instructions First

You should read all safety and operating instructions and labels before operating the DV-IP unit. This user manual helps you install, configure, and operate the DV-IP and the associated DV-IP Viewer software interface.

If you encounter any problems with the software then contact your supplier. Contact Dedicated Micros in the UK office if you have difficulties with this user manual.

The following conventions are used in this manual:



Help: Click the help icon on screen for details of the different fields.



Refer to: Gives a reference to a section where you can find further details.



The 1, 2, 3 icon indicates the start of a procedure.



Note: Notes indicate additional important information that you should be aware of.



Caution: Cautions are used when an incorrect action may damage the unit, the recording or other hardware attached to the unit.



WARNING: Warnings are used where there is a danger of injury or death.

The following key conventions are used throughout this document:

<SHIFT>	Indicates that you should hold down the shift key while pressing subsequent keys.
<ESC>M	Indicates the Escape key at the top left of your keyboard. You only need to press it once and release before pressing 'M'
<ENTER>	Press the Enter (also called Return) key once to enter data into the system.

1.2 Power Sources



WARNING: Only operate this unit from the type of power source indicated on the rear label. Failure to do so invalidates the warranty and may cause injury or death by electric shock.

1.3 Servicing

Do not attempt to service this unit yourself because opening or removing covers may expose you to dangerous voltage or other hazards. Refer all servicing to qualified service personnel.

1.4 Ventilation

Ensure the unit is properly ventilated to protect from overheating.

1.5 Lifting and Handling

The DV-IP is heavy. Always follow health and safety guidelines when lifting the unit from the box or installing the DV-IP unit.

1.6 Storage

The following guidelines apply to storage:

- Ensure the DV-IP unit is properly ventilated to protect from overheating.
- Ensure there is a 3cm gap on both sides of the unit.
- This unit must be stored in a low humidity and dust free area. Avoid places like damp basements or dusty hallways
- Ensure the unit is not located in an area where it is likely to be subject to mechanical shocks.

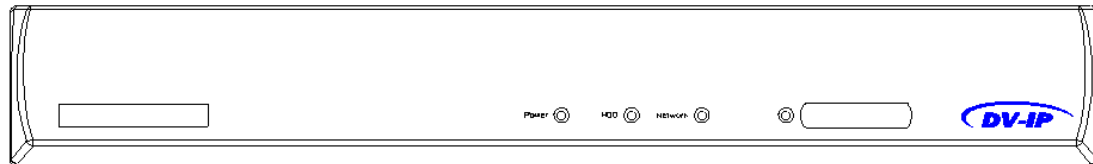


WARNING: To prevent fire or shock hazard, do not expose this unit to rain or moisture.

2. Introduction to the DV-IP

The DV-IP range comprises four, six, ten and sixteen-input high-performance networked video servers. These provide a simple and cost-effective way of recording and distributing high quality live and recorded video across a local area network, wide area network or over the Internet to viewer's PCs.

Figure 1 - The DV-IP Front Panel



DV-IP is designed to take in, record and distribute multiple camera signals around large sites, such as airports, universities, shopping centres, hotels and so on. DV-IP removes the necessity to cable all cameras back to a central location by bridging up to 16 analogue cameras per DV-IP onto the IP network at convenient network points. This offers significant cost savings over centralised coaxially cabled solutions, as most buildings already utilise IP-enabled networks for their data needs.

DV-IP simultaneously supports live, replay, alarm handling (including video motion detection), and archive via File Transfer Protocol (FTP), all without interrupting recording. All monitoring and control is achieved over Ethernet via the 10BaseT network port; supported protocols include, IP, TCP, UDP, DHCP, FTP Telnet, ICMP, HTTP. Video is transmitted over the network as TCP packets, whereas data for telemetry and audio use UDP packets. UDP provides minimal error checking, that is. if an error is detected the packet is not resent. However TCP packets if found to be corrupt are resent. This introduces marginal latency, which would not be acceptable when passing time critical data such as in the case of voice or telemetry.

External alarms may be integrated into DV-IP via the 16 alarm inputs on the reverse of the unit. These alarm inputs can be configured for normally open or normally closed operation, allowing for door contacts and PIRs etc to provide alarm notification. DV-IP can then be configured for an alarm response, which could include sending a PTZ camera to a predefined position, increasing the record rate, parsing an entry to the events database and closing an internal light duty relay contact. These relay contacts could be used to switch lights on remotely, open doors or lift car park barriers etc.

Communication with the outside world is achieved using Internet Protocol (IP). The IP stack provides the protocols that make up a suit of protocol commonly known as TCP/IP. These protocols include FTP, which provides the ability to copy data from the DV-IP to a remote server for backup and off line reviewing, Telnet, which is a terminal-based application, used for programming and debug, and Hyper Text Transfer Protocol (HTTP), which provides the transport for web pages to a web browser, allowing interaction using a common software application. DV-IP can also run the Point to Point Protocol (PPP) commonly known as Dial Up networking, over its serial ports. This allows modems and ISDN terminal adapters to talk to DV-IP to facilitate remote image transfer and alarm handling.

Installation



In this section

- Unpacking and installing the DV-IP unit
- Connecting to the network

3 Installing the DV-IP Unit

3.1 Unpacking

Before connecting your unit, you must remove all the items from the box and check you have each component listed below.

Your DV-IP package contains the following items:

- DV-IP unit
- External Power Supply
- Power Leads – one US and one Generic (without a plug)
- Installation CD ROM
- Quick Start guide
- RS232 Comms cable
- RS485-bus cable with ferrite clamp filter
- Front and rear rack mounting brackets

If any of these items are missing, please contact Customer Services at your distributor or Dedicated Micros.



WARNING: The DV-IP is heavy, be careful when lifting the DV-IP unit from the box or when installing. Improper handling may lead to physical injury.

3.2 The CD ROM

The CD ROM included with your DV-IP contains the following:

- DV-IP Quick Start Guide
- DV-IP User Manual – This document
- DV-IP Viewer – Viewing application
- VCR – Playback application
- Wmark – Watermarking application
- Dbwiz – Site database editor
- DM Config – Advanced configuration application

3.3 Web Browsing PC Requirements

The following systems support the DV-IP Viewer:

- Internet Explorer 5.5 or above
- Netscape Navigator 4.7x only
- Windows 98 Second Edition, NT4 Service Pack 6, Windows 2000 (Only with Internet Explorer 5.5 or above)
- Windows XP
- Recommended minimum spec PC
 - Pentium III, 1GHz processor
 - 256MB RAM
 - 1024 x 768 x 16bit colour monitor (min)
 - 10/100Mbit Ethernet network interface card



WARNING: For a web browser to correctly operate with DVIP, Java Virtual Machine (JVM) should be installed on each PC that will be used to access DVIP. The JVM enables Java components in webpages to operate as intended by Dedicated Micros.



Note: A version of Java Virtual Machine may be downloaded from www.java.com

3.4 DV-IP Viewer PC Requirements

The following operating systems support the DV-IP Viewer:

- Windows 98 Second Edition
- NT4 Service Pack 6
- Windows 2000
- Windows XP
- Recommended minimum spec PC
 - Pentium III, 1GHz processor
 - 256MB RAM
 - 20MB free HDD space (DVIP Viewer only)
 - 1024 x 768 x 16bit colour monitor (min)
 - 10/100Mbit Ethernet network interface card



Note: For best performance, set the colour quality on your PC to at least 16-bit. This can be done from the **Control Panel** by selecting **Display->Settings->Colour Quality**.

3.5 Physical Set-up

The physical set-up consists of the location or mounting of the unit and the electrical cabling needed to connect it.

3.5.1 Location Guidelines

The following guidelines apply to installing the DV-IP:

- Ensure the DV-IP unit is properly ventilated to protect from overheating.
- Ensure there is a 3cm gap on both sides of the unit.
- This unit must be stored in a low humidity and dust free area. Avoid places like damp basements or dusty hallways
- Ensure the unit is not located in an area where it is likely to be subject to mechanical shocks.

3.5.2 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 or Laptop PC with CD ROM drive and connection to the same network as the DV-IP



To physically set up the DV-IP:

1. Connect the video signals to the top row of the BNC connectors on the rear of the DV-IP.



Note: The first video channel is enabled by default, so it is advisable to connect a camera to this input.



Note: The second row of connectors allow loop-through to other pieces of equipment. Cameras routed to other equipment in this way must be set to 'un-terminated'. The default setting is terminated.

2. BEFORE applying mains power, connect the PSU to the power input on the rear of the unit.
3. Apply mains power.
The green power LED should light. You are now ready to set up the network connection.

3.6 Setting up the DV-IP Network Connection

There are two methods to set-up the DV-IP network connection, configuring a permanent IP address or connecting the unit for automatic network configuration using the Dynamic Host Configuration Protocol (DHCP).

DHCP automatically assigns the DV-IP unit with a temporary IP address, subnet mask, and default gateway. However, it is recommended that you manually set up a unique IP address for the unit when you first configure the unit.



Note: We recommend that you assign a permanent IP-address, subnet mask, and default gateway. Using DHCP applies a temporary IP address that changes when the unit is next powered up. You should discuss the situation with your network administrator.



Refer to: *Section 3.6.3, Dynamic Host Configuration Protocol (DHCP)* for more information on DHCP.

For a permanent IP address your network administrator needs to provide the following information:

Category	Complete with your network information
IP address	___ . ___ . ___ . ___ for example 169.254.123.1
Subnet mask	___ . ___ . ___ . ___ for example 255.255.0.0
Gateway	___ . ___ . ___ . ___ for example 169.254.123.10



Note: If the DV-IP is only used on the local subnet then a default gateway is not required.

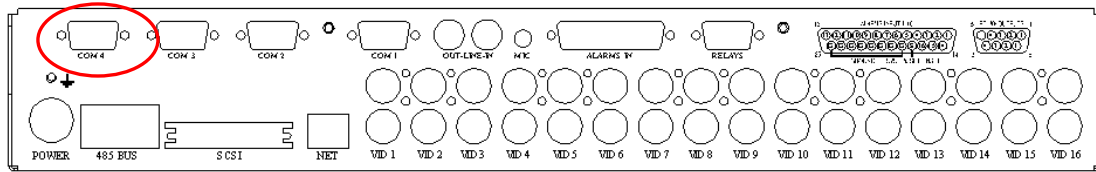
Both DHCP and permanent IP require that you first connect directly to the DV-IP through its RS232 port using a terminal program on a PC.

3.6.1 Connecting to the DV-IP Using a Terminal Program



To connect to the network via a terminal program:

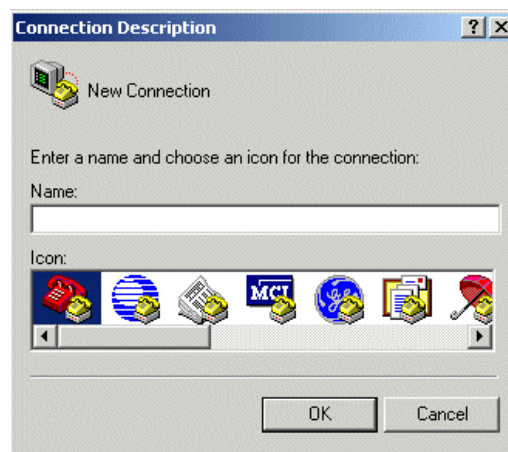
1. Power down the DV-IP and your PC. Remove the mains input from the PSU but leave the PSU connected to the DV-IP
2. Connect the supplied RS232 cable from a PC serial port to the port labelled 'COM 4' port at the back of the DV-IP.



3. For DHCP configurations **ONLY**, connect an Ethernet cable from the RJ45 socket marked 'NET' on the DV-IP to a live empty network socket.
4. For permanent IP-address, subnet mask and default gateway leave the RJ45 disconnected.
5. Restart your PC.
6. Open your terminal program, for example, **HyperTerminal**. This can be found usually in your **Windows Start** menu under:

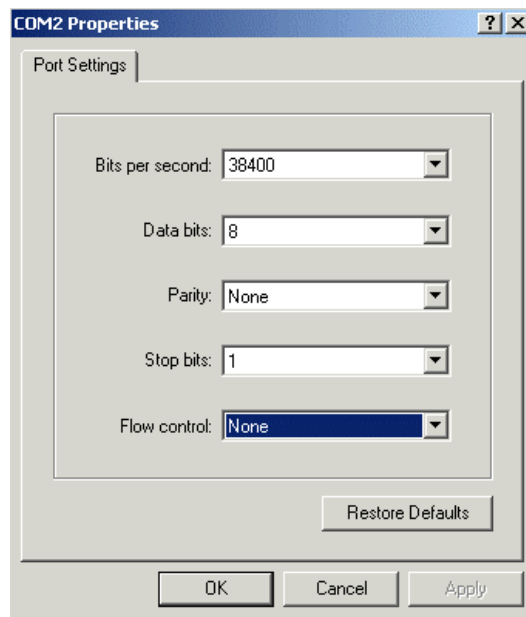
Programs> Accessories> Communications> HyperTerminal

7. The following dialog appears.



8. Type a name in the **New Connection** field, for example, DVIP and click **OK**.
9. Select the COM port that the serial lead is attached to on your PC from the **Connect Using** drop-down menu.
10. Click **OK**.

11. Configure the serial port settings on the PC to the following:



12. Click **OK**.

13. Power up the DV-IP unit. You should see some debugging information on the HyperTerminal screen. Ignore it.

14. To log on, type:

+++<ENTER>



Note: You may need to hold down the **<SHIFT>** key to access the + symbol on your keyboard.

The system responds back with the **DVIP>** command line prompt.

3.6.2 Permanent Network Settings

As described earlier, setting a permanent IP-address, subnet mask and default gateway is the recommended method. If you are using DHCP, go to the next section.



To make permanent network settings:



Note: The RJ45 network connection should be disconnected during this procedure.



Note: "<ESC>m" Indicates the Escape key at the top left of your keyboard followed by "m". You only need to press the Escape key once and release before pressing the 'm' key.

1. Connect to DV-IP using Hyper Terminal as described in section 3.4.1
2. Type the following command in the terminal session:

<ESC>m\ether_ip\aaa.bbb.ccc.ddd<ENTER>

Where **aaa.bbb.ccc.ddd** is the network's IP address.

The response should be similar to that shown in the screenshot below.



Note: It is possible to use either the '.' Or '\' as the delimiter between entries

- Set the subnet mask by typing:

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

Where **aaa.bbb.ccc.ddd** is the network's subnet mask.

The response should be similar to that shown in the screenshot below.

- Where necessary, set the default gateway by typing:

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

Where **aaa.bbb.ccc.ddd** is the network's default gateway.

The response should be similar to that shown in the screenshot below.



Note: A default gateway may not be required on networks that do not contain intermediate routers.

```
ALARMS: contact changed on 14
ALARMS: contact changed on 15
ALARMS: contact changed on 16
FSIMAGE: fs_rebuild_index found 2109 good images in realm 0, file 0, offset=4428
2972, time=11410
PICBUFF: Assigning camera 1 to codec 0
PICBUFF: sequence order -
1 (0)
PICBUFF: added buffer, total 2
RECORD: start main loop seq_mask = 0x0000000000000001
PORTS: attempt DHCP request again
PORTS: requested DHCP hostname AIX032809007
PORTS: quoted DHCP hostname AIX032809007, 13
RECORD: 373 pix written at 6 pix per sec, reqs = 0
Welcome to the DV-IP command line processor
DV-IP> m\ether_ip\172\16\100\10
\OK
DV-IP> m\subnet\255\255\0\0
\OK
DV-IP> m\gateway\172\16\100\1
\OK
DV-IP> m\save
\OK
DV-IP> reset
```

- Save the entered values to memory by typing the following commands at the terminal session:

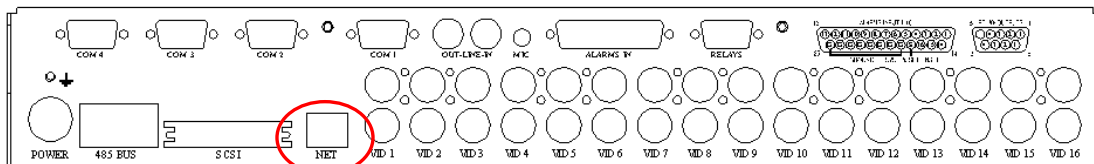
<ESC>m\save<ENTER>

- To restart the DV-IP unit and make your changes effective, type:

reset<ENTER>

Once the DVIP> prompt reappears, the DV-IP is ready.

- Power down the DV-IP.
- Connect an Ethernet cable from the RJ45 socket marked 'NET' on the DV-IP to a live empty network socket.



- Power up the DV-IP.

The green network LED should start to flash. If it doesn't flash, ask your network administrator to check the network socket.

The DV-IP is now fully installed.

10. Proceed to Section 3.6.4, *Testing the Network Configuration of DV-IP*.

3.6.3 Dynamic Host Configuration Protocol (DHCP)

If your network administrator has advised you that the network you wish to configure is served by DHCP server, there may be no need to set the IP address, subnet mask, or default gateway. The DHCP protocol can automatically configure the DV-IP network interface.

By default, the DHCP name on the network is the machine serial number. The IT or network manager can predefine the IP address by configuring the DHCP server to use the DV-IP unit's serial number, found on the packaging or on the underneath of the unit itself, to look up the IP address that's to be assigned to the unit.



Note: Although this configuration provides an IP address for the DV-IP 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.



Refer to: *Section 3.6.2, Permanent Network Settings* for instructions on how to permanently configure the DV-IP network settings.



To determine the IP address automatically assigned via DHCP.



Note: The network should be connected via the RJ45 "NET" socket during this procedure.

1. Connect to DV-IP using Hyper Terminal as described in section 3.4.1
2. At the DV-IP> prompt in HyperTerminal, run the IP configuration tool, type:

ipcfg<ENTER>

The IP address that has been assigned automatically using DHCP is displayed.

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

3.6.4 Testing the Network Configuration of DV-IP

This section tells you how to test that the DV-IP network configuration was successful.

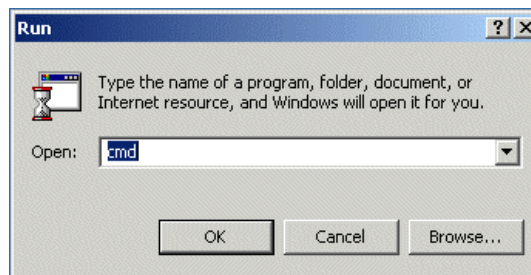
The PC must be connected to the network with a valid IP address, but does not have to be in the same location as the DV-IP unit.



To test the set-up:

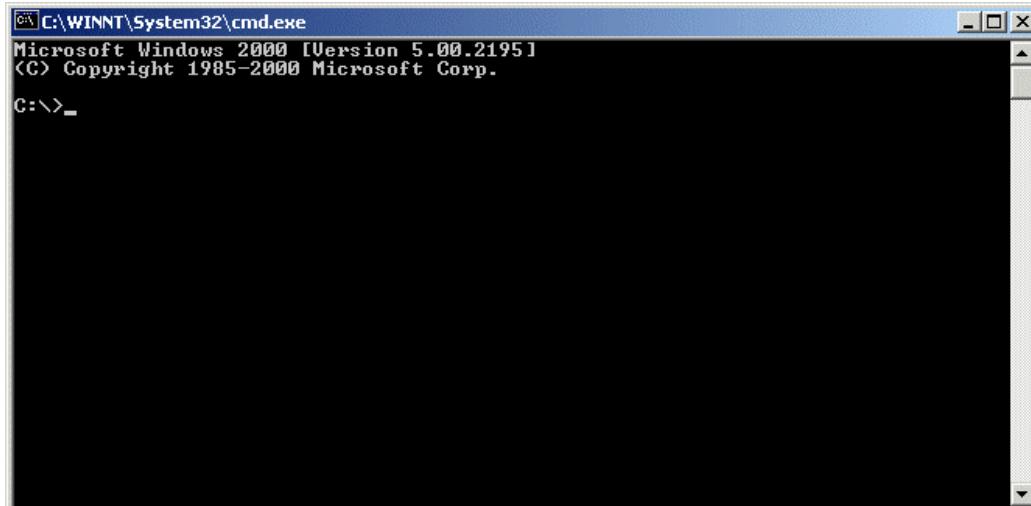
1. On the PC, from the Start menu select **Run**.

The Run dialog appears:



2. Type **cmd** (in Windows 95/98 type **Command** instead).
3. Click **OK**.

An MS-DOS prompt appears:



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

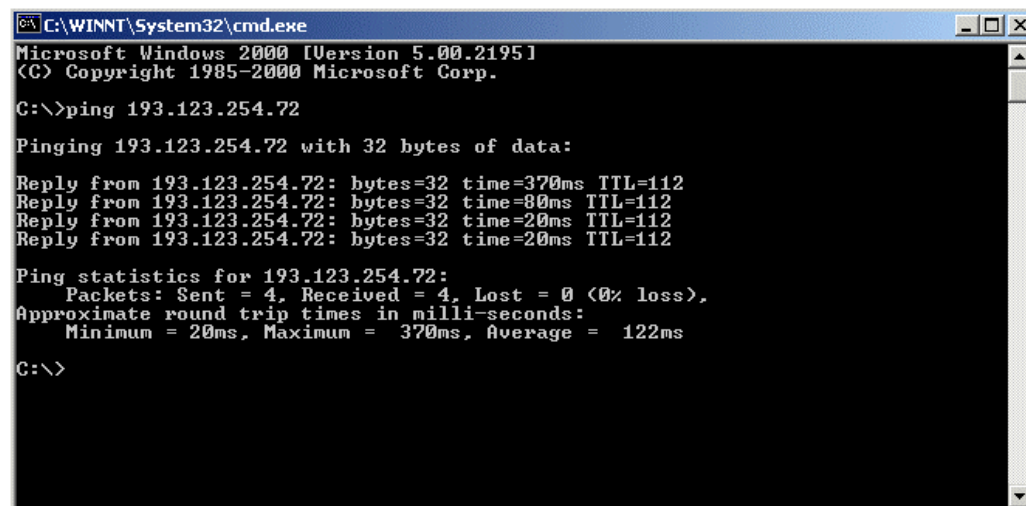
C:\>_
```

4. Launch the ping command. Type:

ping aaa.bbb.ccc.ddd<ENTER>

Where **aaa.bbb.ccc.ddd** is the IP address of the DV-IP.

If the test was a success then you should see replies similar to the following:



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping 193.123.254.72

Pinging 193.123.254.72 with 32 bytes of data:

Reply from 193.123.254.72: bytes=32 time=370ms TTL=112
Reply from 193.123.254.72: bytes=32 time=80ms TTL=112
Reply from 193.123.254.72: bytes=32 time=20ms TTL=112
Reply from 193.123.254.72: bytes=32 time=20ms TTL=112

Ping statistics for 193.123.254.72:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 370ms, Average = 122ms

C:\>
```

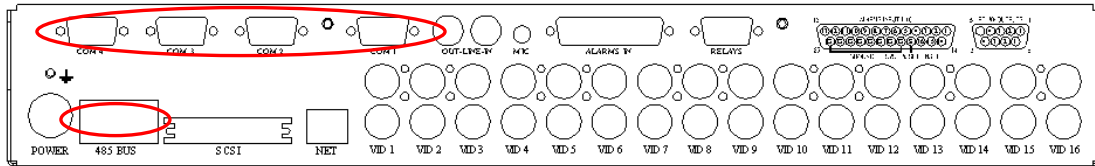
If the test fails, ping returns a message of unreachable.

If the test fails, try the following:

- Check all the cables are fitted securely on the rear of the DV-IP
- Try reapplying the network settings
- Ask your network administrator for advice

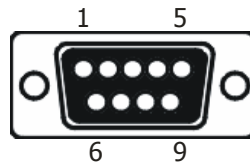
3.7 DVIP Communication Ports

This section describes the pins assignments on the communication ports (circled) found on the reverse of the DV-IP.



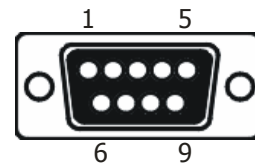
3.7.1 RS232 Communication Ports (Com1, 2, 3, and 4 male D-Type)

PIN No	Description	COM4	COM3	COM2	COM1
1	Data Carrier Detect	DCD	DCD	DCD	DCD
2	Receive Data	RxD	RxD	RxD	RxD
3	Transmit Data	TxD	TxD	TxD	TxD
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



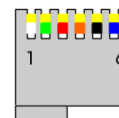
3.7.2 RS485 Communication Ports (Com3 and 4 male D-Type)

PIN N°	COM4	COM3
1	RS485A (+)	RS485A (+)
9	RS485B (-)	RS485B (-)



3.7.3 DM-485 Bus

PIN N°	Description	485 BUS
1	Ground	GND
2	Ground	GND
3	RS485A (+)	485 A
4	RS485B (-)	485 B
5	Ground	GND
6	+ 8 Volts	Power



Configuration

In this section

- **Accessing the configuration screens**
- **Configuring the cameras**
- **Configuring the alarms**
- **Configuring VMD**
- **Configuring the system settings**
- **Advanced configuration**

4 Accessing the Configuration Screens

Once you have successfully set up the hardware and configured network, you can configure DV-IP for use.



WARNING: Please see section 3.3 for the minimum PC requirements required for web browser control.

1
2
3

To access the DV-IP configuration web pages:

1. Open a Web browser and type the IP address of DV-IP in the Address Bar.
For example, "http://172.16.87.234/".

The following screen appears:



2. Click the **Configuration Options** button (circled).
A username and password prompt box appears.
3. Type the default username, which is **dm**.
4. Type the default password, which is **web**.
5. Click **OK**.

The **Main Set-up** page appears:

Video Standard: PAL	
Language: English	
DST: Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London GMT +0	
<input type="button" value="Reset"/> <input type="button" value="Sync DVIP time from PC"/>	
DVIP time:	26 August 2003 14:13:40
DVIP GMT offset (mm):	60
DVIP timezone:	BST
PC time:	26 August 2003 14:22:02
PC GMT offset (mm):	60
Product:	DV-IP
Machine Serial Number:	A1X031022008
PCB Serial Number:	MP024934N
MAC Address:	00-D0-D9-02-D9-7D
Software Version:	03.1 (04.9)
Web Page Version:	01.0 (03.6) - 07/08/2003
Video Inputs:	16
HDD Size:	75.878 Gbytes
Video Standard:	PAL
PPP IP:	10.1.1.1
COM1:	Text in Image
COM2:	Disabled
COM3:	Disabled
COM4:	Debug
IP Address:	172.16.89.50
Subnet:	255.255.0.0
Gateway:	172.16.50.60
DHCP name:	
DHCP IP:	0.0.0.0
DHCP Subnet:	0.0.0.0
DHCP Gateway:	0.0.0.0

The buttons and icons in the left-hand frame allow you to access the configuration screens of the DV-IP.



Help: Click the help icon on screen for details of the different fields.



Help: Click the Save icon to implement any changes you make.

5 Configuring Cameras and Global Recording Parameters

5.1 Configuring Country Specific Information

The Main Set-up screen allows the DV-IP to be configured with country specific information depending where the unit is being set up and used.

1
2
3

To configure the country specific information:

1. From the **Home** tool bar in the left frame, click **Main Set-up**.

The Main Set-up screen appears as follows:

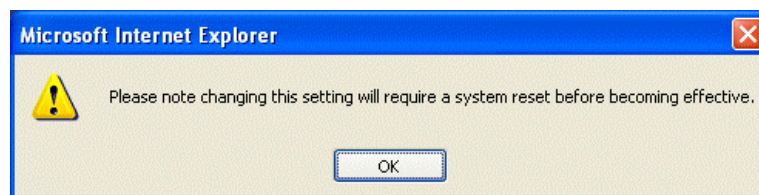
Video Standard:	PAL	HDD Size:	75.878 Gbytes
Language:	English	Video Standard:	PAL
DST:	Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London GMT +0	PPP IP:	10.1.1.1
<input type="button" value="Reset"/> <input type="button" value="Sync DVIP time from PC"/>		COM1:	Text in Image
DVIP time:	17 July 2003 12:11:55	COM2:	Disabled
DVIP GMT offset (mm):	60	COM3:	Disabled
DVIP timezone:	BST	COM4:	Debug
PC time:	17 July 2003 12:13:29	IP Address:	172.16.89.50
PC GMT offset (mm):	60	Subnet:	255.255.0.0
Product:	DV-IP	Gateway:	172.16.50.60
Machine Serial Number:	A1X031022008	DHCP name:	
PCB Serial Number:	MP024934N	DHCP IP:	0.0.0.0
MAC Address:	00-D0-D9-02-D9-7D	DHCP Subnet:	0.0.0.0
Software Version:	03.1 (04.8)	DHCP Gateway:	0.0.0.0
Web Page Version:	01.0 (03.0) - 23/05/2003		
Video Inputs:	16		

2. From the **Video Standard** drop-down box, choose either PAL or NTSC.



Caution: To ensure high picture quality select the correct setting for your cameras.

The following warning message appears:



3. Click **OK**.

4. For this setting to take effect, you must restart the DV-IP. Click the **Reset** button.



Caution: For the Video Standard setting DO NOT save before clicking Reset. If you do, the setting will be ignored.

The following screen appears:



5. Click **Yes**.

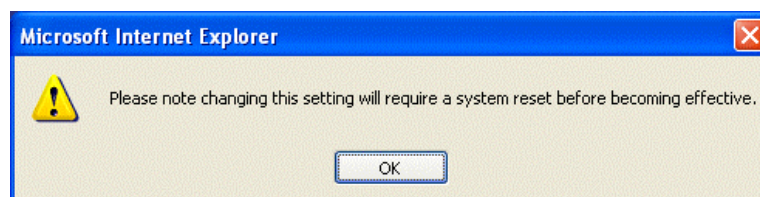
This screen appears once you have clicked the **Yes** button:



Note: For all other options, you must click the **Save** icon before clicking **Reset**.

6. Choose the required language for the **Language** drop-down menu, once the DV-IP returns.
7. Choose the daylight saving option from the **Daylight Saving Time (DST)** drop-down menu.

The following prompt message appears:



8. Click the **Save** icon.



Note: DV-IP will the current time and date as shown on the personal computer, when the Sync DV-IP time button is pressed



Note: Recorded images are referenced from GMT. An offset is applied during playback to the relevant time zone. Make sure that the PC is setup to automatically adjust its self to daylight savings other wise a discrepancy in time will occur during playback. This feature can be found by double clicking on the time bottom right of the task bar and selecting "Time Zone" check the daylight savings box. Time will now be referenced correctly.

5.2 Configuring the High, Medium, and Low View Levels

The high, medium, and low settings are used during viewing on the live page. They decide the network bandwidth and image quality used by the DV-IP to display images on the PC screen.

To configure the high, medium, and low views:

1. From the tool bar in the left frame, click the **Camera** button to expand the camera icons.
2. Click the **Camera Set-up** icon in the expanded toolbar.

The Camera Set-up screen appears:

Connected	Title	Terminated	Mono	Cam-Fail Reporting
<input checked="" type="checkbox"/>	Camera 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Camera 2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	VCL Dome & RX100	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Camera 4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Pelco Dome	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Camera 6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Camera 7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Camera 8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Camera 9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Camera 10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Camera 11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Camera 12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Camera 13	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Camera 14	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Camera 15	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Camera 16	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The Camera Set-up screen is used to set-up the connected cameras and define the viewing resolutions and compression of the live images.

3. Select the **Live Resolution** for each level by choosing one option in each of the drop-down boxes.



Note: Live resolution settings differ between PAL and NTSC regional modes.

- For each live resolution option, insert an image size in kilobytes (KB) in the **Image Size** field.



Note: Smaller image sizes require lower network bandwidth but provide a higher live frame rate. However, smaller image sizes require greater compression, and so the images are lower quality.

- Click **Save**.

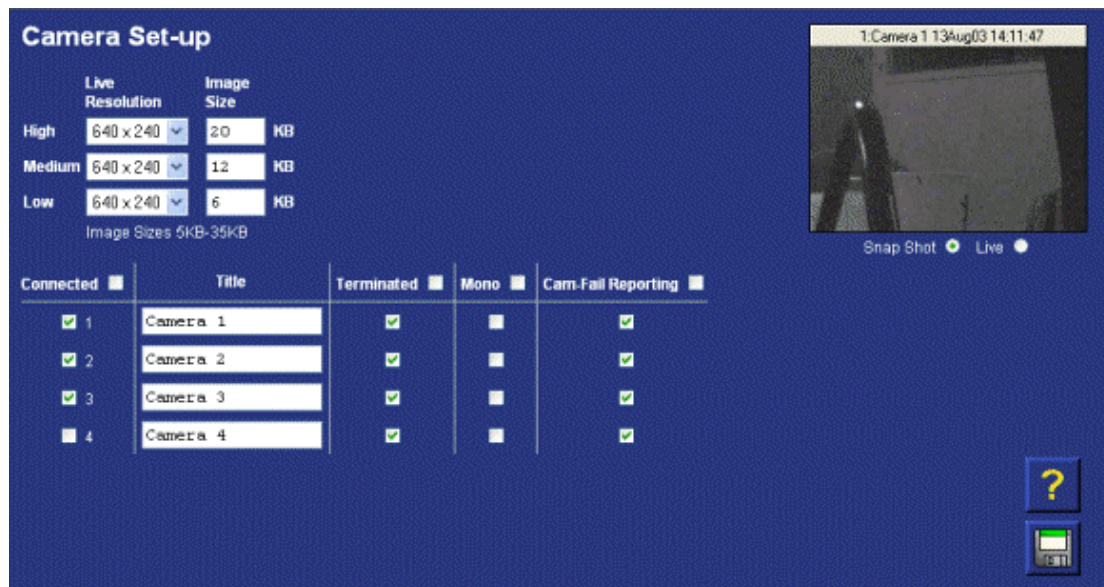
5.3 Configuring the Cameras



To configure the cameras:

- From the tool bar in the left frame, click the **Camera** button to expand the camera icons.
- Click the **Camera Set-up** icon in the expanded toolbar.
- Tick the **Connected** box for each camera you are using.
- Type a descriptive names in the **Title** boxes.
- Click the **Save** icon.

The images from each camera can be previewed in the top right hand corner of the screen when each camera name is clicked.



Note: By default the image appears as a **Snap Shot**. To view live motion, click the **Live** button under the image window in the top right-hand corner.

- Unless the video input is looped through on the DV-IP rear panel, tick the **Terminated** box for each selected camera.
- Tick the **Cam-Fail Reporting** box for each camera that requires an alarm if the camera fails.
- Click **Save**.

5.4 Configuring the Standard Recording Size, Resolution, and Expiry

The DV-IP has a predefined maximum bandwidth for recording images to disk. This bandwidth can be shared evenly between the cameras using the Standard Recording settings,

or can be allocated on a camera-by-camera basis using the Variable recording. Cameras can belong to either group.



Refer to: *Section 5.6, Configuring the Variable Record Set-up* for more information on variable recording.

1
2
3

To configure standard recording:

1. On the left-hand toolbar in the **Cameras** area, click the **Standard Recording** icon.

The following screen appears:

2. Select the **Record Resolution** from the drop-down menu.



Note: The greater the resolution, the more detailed the images.

3. Type an image size between 5KB and 35KB.



Note: The greater the image file size, the better the quality of the image. Very low image sizes are blocky resulting in smaller details being difficult to view. However, larger image file sizes reduce the amount of time images are stored on the unit before being overwritten.

4. Type an expiry time in the **Video Expiry Period** field if you want the video to be discarded automatically after a set number of days.



Note: By entering 0 days, the video will only be discarded when the disk becomes full over writing the oldest video first.

5. Click **Save**.

5.5 Configuring the Standard Recording Rates

This screen is also used to configure the cameras for standard recording, that is, where all cameras share the available record rate. The maximum record rate is dependant on

your DV-IP model. This rate needs to be shared between all the cameras configured on the unit.

1
2
3

To configure the standard record rate:

1. If you are not already on the **Standard Record Setup** screen, click the **Cameras** button on the left-hand toolbar followed by the **Standard Recording** icon.



Note: The Record Resolution, Image Size, and Video Expiry Period have already been configured in *Section 5.4, Configuring the Standard Recording Size, Resolution, and Expiry*.

2. Type the number of milliseconds (Msecs) or pictures per second that all the cameras share, in the **Standard Record Rate** fields. Alternatively you can enter the desired Record Duration in days and hours.

Record Duration	DD	HH
	3	18.5
Standard Record Rate	160	Msec
	6	pps
Alarm Record Rate	160	Msec
	6	pps



Note: Changing the **Standard Record Rate** automatically updates the **Record Duration** and vice-versa.

3. Type the number of milliseconds (Msecs) or pictures per second required in the **Alarm Record Rate** fields. When one or more alarms are triggered, all the cameras associated with the alarms share this alarm record rate between them.
4. Tick the **Recording** box beside each camera that you want to share standard record rates.
5. Click **Save**.

5.6 Configuring the Variable Record Set-up

This is an advanced screen that configures each camera for its own individual record rate. To enable variable recording on a camera, standard recording must be disabled for that camera.

Note that although variable record rates allow for individual record rates, the system's maximum record rate is shared between all the selected cameras. For example, three cameras running at 40ms (25 pictures per second (pps)) each is not a valid setting for a system with a maximum record rate of 50pps, but three cameras running at 16pps (62ms) is a valid setting for such a system.

1
2
3

To configure the variable record rate:

1. Click the **Variable Rate Recording** icon on the left hand-side toolbar.

The Variable Record Setup screen appears:

Camera	Title	Variable record	Variable record rate (ms)	Alarm record rate (ms)	Pre-alarm record rate (ms)	Number of pre-alarm pictures
1	Camera 1	<input type="checkbox"/>	0	0	0	0
2	Camera 2	<input type="checkbox"/>	0	0	0	0
3	Camera 3	<input type="checkbox"/>	0	0	0	0
4	Camera 4	<input type="checkbox"/>	0	0	0	0
5	Camera 5	<input type="checkbox"/>	0	0	0	0
6	Camera 6	<input type="checkbox"/>	0	0	0	0
7	Camera 7	<input type="checkbox"/>	0	0	0	0
8	Camera 8	<input type="checkbox"/>	0	0	0	0
9	Camera 9	<input type="checkbox"/>	0	0	0	0
10	Camera 10	<input type="checkbox"/>	0	0	0	0
11	Camera 11	<input type="checkbox"/>	0	0	0	0
12	Camera 12	<input type="checkbox"/>	0	0	0	0
13	Camera 13	<input type="checkbox"/>	0	0	0	0
14	Camera 14	<input type="checkbox"/>	0	0	0	0
15	Camera 15	<input type="checkbox"/>	0	0	0	0
16	Camera 16	<input type="checkbox"/>	0	0	0	0

RAM disk requirement: 0 KBytes

RAM disk available: 2048 KBytes

2. Tick the **Variable record** box beside each camera to enable it to record at a variable rate.



Note: If this box is un-ticked, you can configure the camera to share the standard record rate instead.

3. Type a figure (in milliseconds) in the **Variable record rate (ms)** box beside each camera. This is the delay between recorded images for each camera.
4. Type a figure (in milliseconds) in the **Alarm record rate (ms)** box beside each camera. This is the delay between recorded images for each camera when an alarm input assigned to that camera is triggered.
5. Type a figure (in milliseconds) in the **Pre-alarm record rate (ms)** box beside each camera. This creates a record rate used to store pre-alarmed images from the RAMDisk to the hard disk.



Note: The number of pre-alarm pictures is limited to the available RAMDisk.

6. Type the number of buffered pre-alarm images stored that should be kept on the RAMDisk for each camera in the **Number of pre-alarm pictures** box.
7. Repeat steps 2 through 6 for each camera.
8. Click **Save**.

6 Configuring the alarms

DV-IP can have events and alarms triggered from a number of sources, built in alarm contacts, camera signal failure, Video Motion Detection (VMD), and combinations of events called Alarm Zones. If additional alarm contacts are required you can connect an external alarm contact module. Each alarm contact is configurable as normally open (triggered on contact closure) or normally closed (triggered when contact opens).

Alarm Zones also allow you to define a variety of actions in response to alarms including, increased recording rates, a Pan-Tilt-Zoom (PTZ) preset and notifying an Alarm Receiver Centre.

6.1.1 Configuring the Alarm Input

This screen is used to configure the alarm contacts to be used as inputs to the alarm zones.

On-Board Alarms 1-16				Module-1 (Address 96) Alarms 17-32			
Contact	Enabled	Normally Closed Contact	Pulse extension	Contact	Enabled	Normally Closed Contact	Pulse extension
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	17	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	18	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	19	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	21	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	22	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	23	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	24	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	25	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	26	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
11	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	27	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	28	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
13	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	29	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
14	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	30	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
15	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	31	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10
16	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10	32	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10

1
2
3

To configure alarm inputs:

1. In the configuration area, from the **Alarms** tool bar in the left frame, click **Alarm Inputs**.
2. To use a contact, check the **Enable** box.
3. If the contact is normally closed, check the **Normally Closed Contact** box.
4. Provide a minimum period (in seconds) that the contact should be active for any alarm in the **pulse extension** field.

As an example, if a door with a pulse extension of 10 is opened triggering an alarm event, but closed immediately, the alarm event still lasts 10 seconds. If the door is opened twice within the pulse extension period, this will only count as one alarm, rather than two.

5. Click **Save**.

6.1.2 Configuring an Alarm Zone

Alarm Zones enable single or combinations of alarm inputs to record multiple cameras in their alarm state. An alarm zone can also cause multiple actions, for instance, selecting cameras, closing an output relay, and selecting a pan-tilt-zoom (PTZ) preset for a camera.

The screenshot shows the 'Alarm Zone Configuration' web page. At the top, there are fields for 'Alarm image protect period (days):' set to 1 and a checkbox for 'Protect alarm images indefinitely:'. Below this is a 'Select Alarm Zone:' dropdown menu showing '01 - (Zone 1)'. The 'Zone Title:' field contains 'Zone 1', with a 'Use Camera Title' button to its right. Further down are input fields for 'Pre-Alarm Time(sec):' (2), 'Alarm Duration:' (10), 'Zone Alarm Input:' (1), 'Zone AND Input:' (No Contact), and 'Zone NOT Input:' (No Contact). A section titled 'Select Zone Cameras:' contains a list of 16 cameras, with '01 - EPOS CAMERA' selected. To the right of this list is a 'Select All' checkbox. Another section titled 'Alarm Zone Actions: (select all)' contains several checkboxes: 'Text Only Alarm', 'System Set (Keyswitch)', 'Create Database Entry' (checked), 'Change Standard Record Rate', 'Change Variable Record Rate', 'Connect on Alarm' (checked), '24 Hour Alarm', 'Record Still Image', 'Protect Alarm Images', and 'Archive Alarms - Enables scheduled FTP download of the alarm - used with FTP Download Page'. Below these are 'Goto Preset' (1) and 'Camera' (1) dropdowns, and a 'Close Relay' dropdown set to 'None'. An 'Apply To All' button is at the bottom right.

1
2
3

To configure the alarm zone:

1. From the **Alarms** tool bar in the left frame, click **Alarm Zone**.
2. Select an alarm zone from the **Select Alarm Zone** drop-down menu.
3. Type a descriptive name (maximum of 30 characters) in the **Zone Title** box.



Note: Alternately, after you have selected a camera, you can click the **Use Camera Title** button.

4. Type a figure (in seconds) in the **Pre-Alarm Time (sec)** field. This provides a period before the alarm is activated, when the DV-IP marks the start of recorded footage viewed with the Alarm Event.



Note: If the **Protect Alarm Images** box is checked, the **Pre-Alarm Time (sec)** field is also used to start the optional write protection of alarmed images.

5. Type a time in seconds in the **Alarm Duration** field.



Note: If the **Protect Alarm Images** box is checked then the pre-alarm time is included in the Alarm Duration. That is, where the pre-alarm time is 2 seconds and the Alarm Duration is 10 seconds, the Alarm Zone will only be active for 8 seconds after the event.

6. Choose an alarm input number from the **Zone Alarm Input** drop-down menu.

7. If you only want to trigger the zone when two alarm inputs are active then, select an additional input from the **Zone AND Input** drop-down list.
8. If you want to prevent the zone from triggering when a particular alarm input is active then, select an additional input from the **Zone NOT Input** drop-down list.



Note: VMD can also be designated as a Zone Alarm Input, Zone AND Input, or Zone NOT Input. This is achieved by selecting one of VMD1 to VMD16 (maximum dependant on the available number of cameras) from the drop-down menu. This allows VMD activity to cause the same results as the triggering of a contact alarm.

9. Select cameras from the **Select Zone Cameras** window. When the zone goes into alarm, all grouped cameras become part of the alarm sequence.



Note: You can check the **Select All** box to select all the cameras.

10. Check the **Text Only Alarm** box if the alarm is required to be text only (not accompanied by video images).



Note: When the **Text Only Alarm** box is checked, any associated cameras are removed from the **Select Zone Cameras** window.

11. To enable the alarm zone, check the **System Set (Keyswitch)** box.



Note: Ensure that the system keyswitch is enabled and the schedule has not had a system keyswitch override enabled in the schedule configuration.

12. To add the alarm to the events database using the zone title, check the **Create Database Entry** box.
13. To change the cameras defined in the Standard Recording screen to the alarm record rate specified when the zone is triggered, check the **Change Standard Record Rate** box.
14. To change the cameras grouped in the zone and defined in the Variable Rate Recording screen to the individual alarm record rates defined when the zone is triggered, check the **Change Variable Record Rate** box.
15. To connect to an Alarm Receiving Centre on alarm, check the **Connect on Alarm** box.
This feature requires a specially registered version of DV-IP Viewer application to be enabled at the Alarm Receiving Centre and the Alarm Connection Settings to be correctly configured.



Refer to: *Section 6.1.4, Configuring the DV-IP for the Alarm Receiving Centre.*

16. Check the **24 hour Alarm** box to set the zone alarm to be active 24 hours a day, even if all schedules are disabled.
17. Check the **Record Still** box to record a single image at the time of the alarm, in addition to the standard video recording sequence.
18. Check the **Protect Alarm Images** box to write-protect the alarm images on disk associated with this zone.



Refer to: *Section 6.2, Configuring Image Protection.*

19. Check the **Archive Alarms** box to select the zone alarm for Automatic FTP Download.



Refer to: *Section 6.3, Configuring Automatic FTP Transfers* for information about configuring the FTP download settings.

20. Check the **Close Relay** box and select an option from the drop-down menu to close either on-board relay 4 or optional relays 1 to 16 on ROM Module-1, if required.
21. Do not click **Apply To All** unless you want the same actions to be applied to all previously defined zones.



Note: You can abandon changes by pressing the refresh button on your Web browser, if you have not already clicked the **Save** icon.

22. Click **Save**.

6.1.3 Configuring the Events and Alarms Database

The event database records alarms and events on the system. It can either be reset (deleted) regularly or transferred automatically by FTP to another location.

Database Configuration	
Last database reset time:	21 February 2003 08:59:55
Current number of entries:	1000
Maximum number of entries:	<input type="text" value="1000"/>
<input type="button" value="Reset database"/>	

This screen shows the last time the events database was reset, and the current number of events held. It also allows you to set the maximum number of events held in the database, and reset the database, clearing all unprotected events.



To configure the database:

1. From the **Alarms** tool bar in the left frame, click **Database Configuration**.
2. Type the number of event entries in the **Maximum number of entries** field.
3. Click the **Reset database** button.
4. Click **Save**.



Note: Any events, which are currently protected, remain in the database and are not reset. Protected events can only be cleared if they are first unprotected using the **Alarm Image Un-protection** menu.



Refer to: *Section 6.2, Configuring Image Protection.*

6.1.4 Configuring the DV-IP for the Alarm Receiving Centre

Two alternative profiles connect to an Alarm Receiving Centre (a PC on a network using a specially unlocked version of the DV-IP Viewer). The IP address of the Alarm Receiving Centre is needed to provide a destination for DV-IP to correctly send alarms.

The **Connect On Alarm** option must be enabled in the **Configuring the Alarm Zone** screen, or the **Report on VMD Activity** option.



Refer to: *Section 6.1.2, Configuring an Alarm Zone* to check that the **Connect On Alarm** option is enabled.

Hosts and Profiles

	HOST	PROFILE
Primary:	<input type="text"/>	<input type="text"/>
Secondary:	<input type="text"/>	<input type="text"/>

DVIP Alarm Name:

Dial on Alarm: ☐

Dial on Camera Fail: ☐

Dial Retry Time: (minutes)

Dial Limit:



Note: The DV-IP unit ensures that a connection with an Alarm Receiving Centre or a PC on a network is achieved, by using the configured **Hosts** and **Profiles**.



To configure the Alarm Receiving Centre connection settings:

1. From the **Alarms** tool bar in the left frame, click **Alarm Connection Setting**.
2. Type the IP address of the Alarm Receiving Centre in both the **Primary** and **Secondary** host fields in the **HOST** windows.



Note: If the Alarm Receiving Centre has a backup IP address, this can be used for the secondary host instead of repeating the primary host address. Alternatively, if a DNS server is configured in the network settings, you can use host names.

3. Type the word 'Ethernet' in the **Primary** and **Secondary Profile** fields.



Note: The Ethernet profile causes DV-IP to 'dial out' over the Ethernet, via an optional router to the Alarm Receiving Centre. For advice on other possible profiles, contact your supplier or Dedicated Micros.

4. Type the name of this DV-IP in the **DVIP Alarm Name** window, to be included in alarms.
5. Check the **Dial on Alarm** box to enable DV-IP dial out for alarms.
6. Check the **Dial on Camera Fail** box to enable automatic dial-out if a camera fails.
7. Type in a retry time (minutes) in the **Dial Retry Time** field, for the system to try to connect to the Alarm Receiving Centre if an initial attempt is unsuccessful.
8. Type in the maximum number of times in the **Dial Limit** window that the unit is allowed to attempt to connect to the Alarm Receiving Centre.
9. Click **Save**.

6.2 Configuring Image Protection

Image protection sets a protect flag on all images recorded by an alarm zone. These images cannot then be overwritten or removed without being unprotected first.

6.2.1 Configuring Alarm Zone Image protection

Configuring the alarm zone image protection protects all the images that are recorded when an alarm zone is activated.



Refer to: *Section 6.1.2, Configuring an Alarm Zone.*

1
2
3

To configure alarm zone image protection:

1. From the **Alarms** tool bar in the left frame, click **Alarm Zone**.
2. Type the number of days that the alarm image(s) are protected from being overwritten in the **Alarm image protect period (days)** field.
3. Check the **Protect alarm images indefinitely** box to protect images from being overwritten unless manually overridden using Alarm Image Un-protection.

Alarm Zone Configuration

Alarm image protect period (days):

Protect alarm images indefinitely: ☐

6.2.2 Removing Protection from Images

This screen is used to select alarm image periods which are to be unprotected.

Alarm Image Un-protection

	Hours	Mins	Secs	Date	Mon	Year
Start Date and time:	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="19"/>	<input type="text" value="27"/>	<input type="text" value="8"/>	<input type="text" value="2003"/>
End Date and time:	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="19"/>	<input type="text" value="27"/>	<input type="text" value="8"/>	<input type="text" value="2003"/>

Protect Image Partition Summary

1
2
3

To remove protection from images:

1. From the **Alarms** tool bar in the left frame, click **Alarm Image Un-protection**.
2. Type in the time and date in the **Start Date and time** fields that starts the period that the selected images are to be discarded.
3. Type in the time and date in the **End Date and time** fields that ends the period that the selected images are to be discarded.



Caution: If the time and date is typed directly into the **Start Date and time** and **End Date and time** fields, all events within this period are unprotected when the **Un-Protect image button** is clicked.

- Click the **Un-protect Images** button.



Note: If you want to unprotect the images, they *must* be removed from the database on this screen.

6.3 Configuring Automatic FTP Transfers

This screen is used to set configuration options for automatic download of events to a specified FTP server. This allows for remote storage of alarm events. For example, in a multi DV-IP installation, this allows all events from all units to be stored on a central FTP server.

FTP Events Download Settings

FTP Server (IP, URL or name):

FTP Control Port (Default 21):

FTP Root Drive/Directory:

Username:

Password:

Download options

On Connection: ☒

Scheduled: ☐

Schedule time:

Server Directory:



To configure the FTP events download settings:

- From the **Alarms** tool bar in the left frame, click **FTP Events Download**.
- Type in the IP address, URL, or name of the **FTP Server** that DV-IP is to connect.



Note: A DNS must be configured in the network settings if you want to use a URL or host name.

- Type in the directory on the FTP server, where DVIP should transfer events, in the **FTP Root Drive/Directory** field.
- Type in a **Username** for the FTP login onto the server.
- Type in a **Password** for the FTP login onto the server.



Note: The password must be typed in every time the screen is submitted.

- Choose either **On Connection** or **Scheduled** under the **Download Option** by clicking the appropriate radio button.
If you choose **On Connection**, the DVIP tries to transfer the events as soon as it detects a working network connection to the server.
- If you selected a scheduled connection then, type the time of day in 24 hour format in the **Schedule Time** field that you want the scheduled upload to start each day.
- Click the **Save** icon.

6.4 Configuring the Alarm Schedule

The Schedule screen provides a 7-day system control timer. This allows for timed schedules, for example, the unit could be switched to Alarms Set mode at 17:30 on weekdays when work finishes and changed back to normal, or Alarms Unset, mode at 08:30 each morning. For special profiles for, for example holidays, you can use the Timer Functions screen described in the next section.

Day	Alarms-Set	Alarms-Unset
Sunday	24:00	24:00
Monday	24:00	24:00
Tuesday	24:00	24:00
Wednesday	24:00	24:00
Thursday	24:00	24:00
Friday	24:00	24:00
Saturday	24:00	24:00

Alarms State: "Enabled (Set)"

If both alarm times are 00:00, the alarm will be disabled.
If both alarm times are 24:00, and the Schedule Enable is ticked, the alarms will permanently be enabled.

Schedule Enable	<input checked="" type="checkbox"/>	System Set/Unset (Keyswitch, On-board Alarm Input 17)	<input type="checkbox"/>
Scheduled Recording	<input checked="" type="checkbox"/>	Normally closed	<input type="checkbox"/>

Holiday Profiles

1
2
3

To configure the alarm schedule:

1. From the **Cameras** tool bar in the left frame, select **Schedule**.
2. Choose the days and times to activate the alarms by typing the time in 24-hour format in the **Alarm-Set** and **Alarm-Unset** fields.



Note: If both fields are set to 00:00 then the alarms and the Video Motion Detection (VMD) are permanently disabled. If both fields are set to 24:00, then the alarms are permanently enabled.

3. Check the **Schedule Enable** box to enable the schedule.
4. Check the **Scheduled Recording** box if you want the cameras to change record rate during the **Alarm-Set** period.



Note: If the **Scheduled Recording** box is checked, then a **Set** and **Unset** column are added to the **Standard Recording** and **Variable Rate Recording** screens as shown below. You may want to return to these screens to configure the values.

Standard Record Set-up

Record Resolution
640 x 256

Image Size
20 KB

Image Sizes 5KB-35KB

Video Expiry Period
0 Days

	Set		Unset	
	DD	HH	DD	HH
Record Duration	7	21	7	21
Standard Record Rate	1.67	Msec	1.67	Msec
	6	pps	6	pps
Alarm Record Rate	1.67	Msec	1.67	Msec
	6	pps	6	pps

Camera	Title	Recording (Set)	(Unset)	Camera	Title	Recording (Set)	(Unset)
1	EPOS CAMERA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9	Camera 9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Sens Dome	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10	Camera 10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	VCL Dome	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	11	Camera 11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	The God Father	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	12	Camera 12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Camera 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	13	Camera 13	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Camera 6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	14	Camera 14	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Camera 7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	15	Camera 15	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Camera 8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	16	Camera 16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



Refer to: The *Section 5.3, Configuring the Cameras* for more information.

5. Tick the **System Set/Unset (Keyswitch)** box if you would like the schedule to be overridden by alarm input contact 17.
Tick the **Normally Closed** box if you want the contact to operate in normally closed operation, leave it empty for Normally Open.
6. Click **Save**.

6.5 Configuring the Holiday Profiles and Timer Functions

The holiday profiles (Timer Functions screen) allows you to allocate any one of the ten extra alarm profiles to dates that you declare as holidays. The screen is shown below:

Timer Functions

Holiday Dates

Current Holiday List		Add new holiday date			
Date	Month	Year	Profile		
	00	January	00		

Add Holiday

Holiday Profiles

If both 00:00:00 then defaults to UNSET, if 24:00:00 then SET.

Profile	Set Time	Unset Time	Profile	Set Time	Unset Time
1	24:00	24:00	6	24:00	24:00
2	24:00	24:00	7	24:00	24:00
3	24:00	24:00	8	24:00	24:00
4	24:00	24:00	9	24:00	24:00
5	24:00	24:00	10	24:00	24:00

1
2
3

To configure the holiday profiles:

1. Click the **Holiday Profiles** button on the **Schedule** screen.



Note: Changing a profile after it has been assigned to a holiday also automatically changes the times used for the holiday.

2. Create profiles by typing times in 24-hour format in the **Set** and **Unset** boxes.



Note: If both the **Set Time** field and the **Unset Time** field are set to 00:00 then the alarms are disabled (Unset) throughout the holiday. If both fields are set to 24:00 then the alarms are enabled (Set) throughout the holiday.

3. Click **Save**.

You have now set up the profiles. Next add some holidays.

4. Enter the Day Month and Year that you want to make a holiday.
5. Enter a holiday profile number from 1 to 10.
6. Click **Add Holiday**.

The new holiday profile is added to the **Current Holiday List** drop-down list.

1
2
3

To delete a holiday:

1. Select the unwanted holiday from the **Current Holiday List**.
2. Type '0' in the **Profile** field.
3. Click **Save**.

1
2
3

To edit a holiday:

1. Select the holiday from the **Current Holiday List** that you would like to edit.
2. Alter the **Profile** field for that selected holiday.
3. Click **Save**.

7 Configuring VMD

Video Motion Detection (VMD) allows cameras to automatically detect changes in the scene that they are monitoring, and perform a number of basic actions such as notify an operator, create an event database entry, or increase record rate of the camera detecting motion, if required.

For maximum flexibility, VMD can be used as an input to Alarm Zones; this can create more complex alarm actions affecting multiple cameras.

7.1 Configuring Generic VMD Options


To configure the generic VMD options:

1. Click the **VMD** button on the left-hand side toolbar.
2. Select the cameras that require VMD settings by checking the **Enable** box under each camera number.

VMD Options																
VMD Camera Enable:																
Camera	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Enabled	<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"/>

VMD pulse extension (secs):	<input type="text" value="1"/>
VMD pre-alarm time (secs):	<input type="text" value="2"/>
VMD alarm duration (secs):	<input type="text" value="1"/>
VMD protect period (days):	<input type="text" value="1"/>
Protect VMD images indefinitely:	<input checked="" type="checkbox"/>

3. Type the number of seconds required in the **VMD pulse extension** box to extend the time an alarm is valid for, before another alarm event can be activated by motion detected on the same camera.
4. Type a figure (in seconds) in the **VMD pre-alarm time** field. This provides a period before the alarm is activated, when the DV-IP marks the start of recorded footage viewed with the Alarm Event.
5. Type the alarm duration (in seconds) in the **VMD alarm duration**.
6. Type a **VMD protect period** in days or check the **Protect VMD images indefinitely**.

 **Note:** If the **Protect VMD images indefinitely** box is checked, the **Pre-Alarm Time (sec)** field is used to start the optional write protection of alarmed images.

7.2 Configuring VMD Actions for a Camera

The actions for VMD on a camera can be configured separately to the actual VMD zones for the camera. See the next section for details of setting up the VMD zones.

To configure the VMD camera actions:

1. Select the camera you wish to configure for VMD from the **Select VMD Camera** drop-down menu.



Note: Many actions may be repeated if the VMD is used as an input to an Alarm Zone. It is recommended that you choose to only enable an action in the VMD or in the Alarm Zone to reduce the number of actions that occur and events that have to be reviewed.

2. To record an events in the event database using the VMD zone number, check the **Create Database Entry** box.
3. To set the alarm record rate across ALL cameras enabled in the record sequence and configured for standard recording, check the **Change Standard Record Rate** box.
4. To change the alarm record rate for the selected VMD camera *only*, enable the camera in the **Camera Set-up** screen, configure an alarmed variable record rate, and place a check in the **Change Variable Record Rate** box.
5. To connect to the DV-IP Viewer, check the **Report on VMD Activity** box (when the alarm handling functionality is enabled).
6. Check the **24 Hour Alarm** box to enable the VMD for 24 hours on the selected camera even if a schedule has not been defined.
7. Check the **Record Still Image** box to record a high quality single image at the time of the VMD activation, in addition to the ongoing recording.
8. Check the **Protect VMD Images** box to protect the images associated with this VMD activation from being overwritten using the **Pre-Alarm**, **Alarm Duration**, and **Protect Period** parameters.



Refer to: *Section 6.2.2, Removing Protection from Images in Section 6, Configuring the alarms.*

9. Check the **Create Zone Input** box to create a zone event by activating a VMD from this channel.



Note: The **Create Zone Input** *must* be enabled if you want to use a VMD channel as an alarm base contact input into the Alarm Zone settings.

10. Check the **Archive Event** box to mark a VMD event for automatic FTP download.
11. Mark the associated VMD images to be scheduled for Automatic FTP Events Download.



Caution: Clicking **Apply to all** any previously defined actions in other zones. If you accidentally press **Apply to All**, you can abandon changes by pressing the refresh button on your Web browser, if you have not already pressed the **Save** button.

12. Click **Apply to All** if you want to ensure that all cameras use the same selected VMD actions.



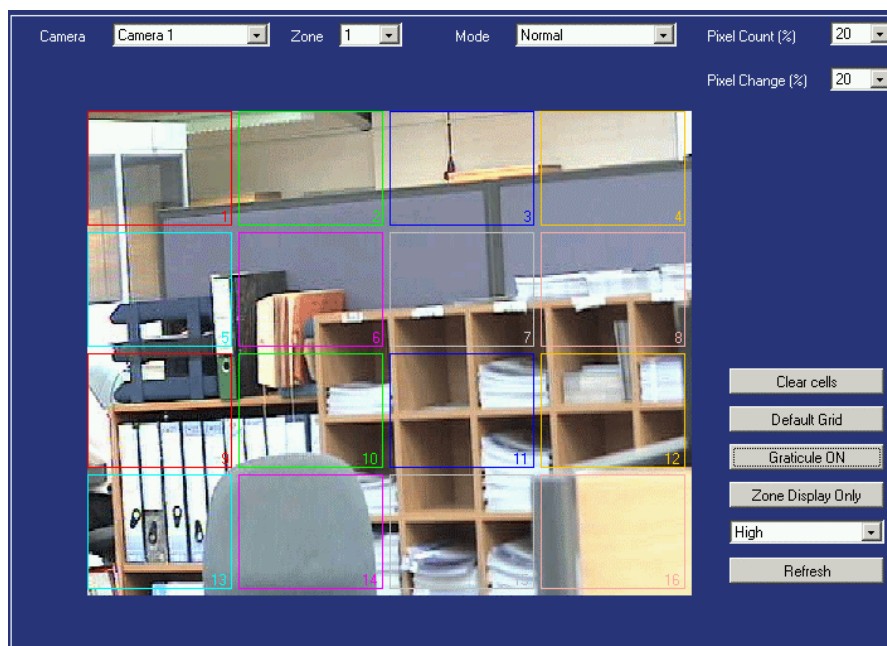
Note: VMD triggers are shown in the thumbnail, allowing you to increase or decrease sensitivity as required.

13. Click **Save**.

7.3 Configuring the VMD zones for a Camera

To establish the best settings for VMD, it is recommended that you undertake testing based on different **Pixel Count** and **Pixel Change** settings. A setting that is too high will miss the activity, and one that is too low will cause false triggers. The Walk Test helps set the optimum levels by providing a thumbnail image where triggers are seen on screen. VMD triggers can also be seen in the **Live View** as boxes that appear when that particular area is triggered.

The VMD Configuration box allows you to set 16 individually defined areas for each camera, allowing for very complex motion detection. The **configuration** box (below) shows the 16 fields:




To configure the VMD zones for a camera:

1. Choose a camera from the **Camera** drop-down menu in the VMD zone configuration box.

 **Note:** By default, the 16 motion detection zones of each camera are arranged in a 4x4 grid of squares. Press the **Clear cells** button to delete these default squares.

2. Select a **Zone** between 1 and 16 from the drop-down menu, to enable the zone shape and parameters to be redefined.


To define additional zones, choose different zones from the **Zone** drop-down menu.

 **Note:** To draw a zone, left click on the screen to define the top-left corner of the VMD zone. Click again on the screen to define the bottom-right corner.

3. Select **Normal**, **Last Trigger**, or **Static** from the **Mode** drop-down menu.

 **Note:** Last trigger and Static modes are for indoor use *only*.

4. From the **Pixel Count (%)** drop-down menu, select the percentage of pixels that must change to invoke an alarm.
5. From the **Pixel Change (%)** drop-down menu, select the percentage change in grey scale of the each pixel before it is considered to have changed.
6. Click the **Walk Test On** button to provide a simple test to ensure that the settings work correctly.
7. Click **Save**.

 **Refer to:** 'How to set up and use VMD guide', which is available from Dedicated Micros for further information about using VMD.

7.4 Configuring VMD Image Protection

VMD image protection protects all the images that are recorded when a VMD camera is activated.



To configure VMD image protection:

1. Click the **VMD** button on the left-hand side toolbar.
2. Type the time period the images are protected from being overwritten in the **VMD protect period (days)** box, or, check the **Protect VMD images indefinitely**.



Note: If the **Protect VMD images indefinitely** box is checked then the events remain in the database even if the database is reset.



Refer to: *Section 6.2.2, Removing Protection from Images* in *Section 6, Configuring the alarms* to remove protection from images.

8 Configuring the system settings

The Main Set-up screen allows the DV-IP to be configured with country specific information depending where the unit is being set up and used.

1
2
3

To configure the country specific information:

1. From the **Home** tool bar in the left frame, click **Main Set-up**.

The Main Set-up screen appears as follows:

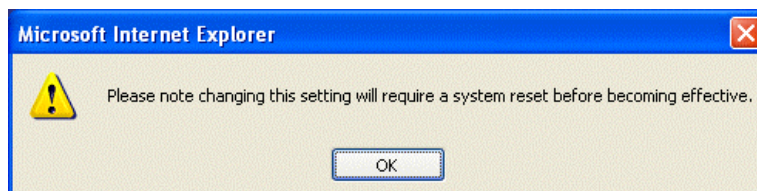
Video Standard:	PAL		
Language:	English		
DST:	Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London GMT +0		
<input type="button" value="Reset"/> <input type="button" value="Sync DVIP time from PC"/>			
DVIP time:	17 July 2003 12:11:55	HDD Size:	75.878 Gbytes
DVIP GMT offset (mm):	60	Video Standard:	PAL
DVIP timezone:	BST	PPP IP:	10.1.1.1
PC time:	17 July 2003 12:13:29	COM1:	Text in Image
PC GMT offset (mm):	60	COM2:	Disabled
Product:	DV-IP	COM3:	Disabled
Machine Serial Number:	A1X031022008	COM4:	Debug
PCB Serial Number:	MP024934N	IP Address:	172.16.89.50
MAC Address:	00-D0-D9-02-D9-7D	Subnet:	255.255.0.0
		Gateway:	172.16.50.60
Software Version:	03.1 (04.8)		
Web Page Version:	01.0 (03.0) - 23/05/2003	DHCP name:	
Video Inputs:	16	DHCP IP:	0.0.0.0
		DHCP Subnet:	0.0.0.0
		DHCP Gateway:	0.0.0.0

2. From the **Video Standard** drop-down box, choose either PAL or NTSC.



Caution: To ensure high picture quality select the correct setting for your cameras.

The following warning message appears:



3. Click **OK**.
4. For this setting to take effect, you must restart the DV-IP. Click the **Reset** button.



Caution: For the Video Standard setting DO NOT save before clicking Reset. If you do, the setting will be ignored.

The following screen appears:



5. Click **Yes**.

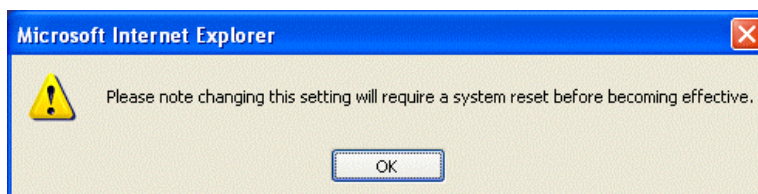
This screen appears once you have clicked the **Yes** button:



Note: For all other options, you must click the **Save** icon before clicking **Reset**.

6. Choose the required language for the **Language** drop-down menu, once the DV-IP returns.
7. Choose the daylight saving option from the **Daylight Saving Time (DST)** drop-down menu.

The following prompt message appears:



8. Click the **Save** icon.



Note: DV-IP will use the current time and date as shown on the personal computer, when the Sync DV-IP time button is pressed



Note: Recorded images are referenced from GMT. An offset is applied during playback to the relevant time zone. Make sure that the PC is setup to adjust to daylight savings automatically other wise a discrepancy in time will occur during playback. This feature can be found by double clicking on the time bottom right of the task bar and selecting "Time Zone" check the daylight savings box. Time will now be referenced correctly.

8.1 Configuring the Network Settings

The Network Settings screen displays and enables you to make changes to the existing network settings. It also allows for limitation of bandwidth, to ensure the DV-IP only uses as much bandwidth as you can spare. Normally the main network settings of the IP address, subnet mask, and default gateway are only configured at installation.

1
2
3

To configuring the network settings:

1. From the **System** tool bar in the left frame, click **Network Settings**.



Caution: Changing the IP address, subnet mask, or gateway will disable access to the DV-IP unit over the network on the old values.

2. Type in the IP Address of the DV-IP system.



Note: If the IP Address is set to 0.0.0.0, the DV-IP attempts to obtain an IP Address, a Subnet Mask, and a Gateway from a Dynamic Host Configuration Protocol (DHCP) server.

3. Type a Subnet number to specify a Subnet Mask in the **Subnet Mark** field.
4. Type an IP address in the **Default Gateway** field. This is usually the IP address of the router that provides connectivity outside of the immediate LAN.



Note: Setting the Gateway to 0.0.0.0 provides connectivity only within a LAN, which disables access over a router.

5. If your network administrator can provide a DNS server address, type the IP address of the **Primary** and **Secondary** DNS servers. Using a DNS allows the use of text based host names instead of IP addresses.

6. Give the DV-IP unit a name in the **DVIP Name** field. The DHCP server that dynamically assigns an IP address to DV-IP uses the DV-IP name as a reference. If you change the name here, you must ask your network administrator to add it to the DHCP server.
If the **DVIP Name** field is empty, DV-IP uses the unit's serial number as its reference when contacting the DHCP server.
7. Type a Point-to-Point Protocol (PPP) IP address in the **PPP IP** field, if serial ports are to be used to connect over IP.



Note: The PPP IP address is used when the DV-IP dials on alarm or receives a dial in connection (on the PPP_Link2 profile). The PPP IP address is independent of the main DV-IP IP address.

8. Click either the **LAN**, **WAN**, or **ISDN** button to set the defaults for the maximum transmission rate and other network parameters, regardless of the number of connections expected over the links.



Caution: The LAN, WAN, and ISDN bandwidth limitation controls can seriously affect the transmission operation of the DV-IP. Refer to the help system for more information.



Help: Click the help icon on screen for details of the different fields.

9. Click **Save**.

8.2 Configuring the RS232 Ports

This screen is used to configure the four communication ports on the DV-IP web server.



To configure the RS232 ports:

1. From the **System** tool bar in the left frame, click **Serial Ports & Telemetry**.
2. Choose either COM 1, 2, 3, and 4 by either selecting the radio button beside the **Port** or selecting an option from the **Port Usage** drop-down menu.



Note: If you choose PPP (PPP_Link1) or PPP (PPP_Link2) from the Port Usage drop-down menu for COM 1 or 2, then optional modems and terminal adapters are available from the second drop-down menu.

3. Select appropriate settings for **Baud Rate, Parity, Data Bits, Stop Bits** and **Flow Control** according to the requirements of the connected equipment.
4. Click **Save**.
5. Restart the DV-IP by clicking **Reset**.



Note: Changes will only take effect when saved and the DV-IP unit is reset.



Help: Click the help icon on screen for details of the different fields.

8.3 Setting up Coaxial Telemetry

The DV-IP supports coaxial telemetry for PTZ cameras and domes using Pelco or BBV compatible coax protocols.



To set-up coaxial telemetry:

1. From the **System** tool bar in the left frame, click **Serial Ports & Telemetry**.
2. Select **Coax(BBV/Pelco)** from the **Telemetry Type** drop-down menu in the **Telemetry Option** section of the screen,.
3. Click **Save**.
4. Restart the DV-IP by clicking **Reset**.
5. Once the DV-IP returns, from the **Cameras** tool bar in the left frame, click **Camera Set-up**.
6. On the **Camera Set-up** screen, select the type of telemetry desired from the **Coax Telemetry** column.
7. Click **Save**.
8. From the **System** tool bar in the left frame, click **Serial Ports & Telemetry**.
9. Restart the DV-IP a second time by clicking **Reset**.



Note: Your changes have now been applied.

10. From the **Home** tool bar in the left frame, click **Live Page**.
11. Use the telemetry controls in DV-IP Viewer to test the operation of the PTZ motion.



Refer to: *Section 8.6, Configuring Telemetry Image Compression.*

8.4 Configuring Matrix Telemetry

RS232 Telemetry can be used with the following Matrices:

- Ademco(VCL)
- American Dynamics
- BBV

The DV-IP connects to these matrices as a keyboard emulator via their RS232 ports.



To configure the matrix telemetry:

1. In the Config screen, from the **System** tool bar in the left frame, click **Serial Ports and Telemetry**.

2. Choose the matrix type from the **Telemetry Type** drop-down menu.
3. Enter the keyboard number that has been allocated to DV-IP from the Matrix, in the **Telemetry Matrix Monitor** field.
4. Click **Save**.
5. Test the motion of the activated cameras.



Refer to: Section 8.6, *Configuring Telemetry Image Compression*.

8.5 Configuring RS232 DM* Commands Telemetry

The DM* Commands protocol is also available as follows.



To configure the RS232 telemetry:

1. From the **Camera** tool bar in the left frame, click **Camera Set-up**.
2. Ensure all cameras are set to OFF in the Coax telemetry option.
3. From the **System** tool bar in the left frame, click **Serial Ports and Telemetry**.
4. Select the relevant telemetry type from the **Telemetry Type** drop-down menu.
5. Select a serial port using the radio button next to the relevant COM number and change the drop-down option to **Telemetry**.
6. Configure the serial port settings as follows:

Baud rate	9600
Parity	None
Data bits	8
Stop bit (unless VCL Ademco, when it must be set to two stop bits)	1
Flow control	None

7. Click **Save**.
6. Restart the DV-IP by clicking **Reset**.



Note: Your changes may not appear to have been registered. You must reset the unit by clicking the **Reset** button on the left-hand toolbar and then clicking **Yes** to ensure the options become active.

12. From the **Home** tool bar in the left frame, click **Live Page**.
13. Test the functionality by examining the camera motion.

8.6 Configuring Telemetry Image Compression

During motion you may want to change the level of image compression to produce clearer images. Telemetry image compression is determined by inserting a compression limit in the screen below:



Note: Telemetry image compression compares the IP ranges of the DV-IP and the viewing application. If the PC controlling the DV-IP is on a different subnet, the telemetry compress will increase the image compression to provide a quicker update during telemetry control. This is for use over reduced bandwidth connections.

RS232 Ports

PORT	PORT USAGE
COM1:	TEXT in IMAGE
MODEM/TA:	
COM2:	OFF
MODEM/TA:	
COM3:	OFF
COM4:	Debug

Baud Rate: 38400
Parity: None
Data Bits: 8
Stop Bits: 1
Flow Control: None

Telemetry options

Telemetry Type: Coaxial - BBV/Pelco
Telemetry Matrix Monitor: #
Telemetry Image Compression: 0 (0=off or 8 to 255)

Reset

1
2
3

To configure telemetry image compression:

1. Choose a **Telemetry Image Compression** rate.



Note: Values of 1 to 7 are not accepted or used as a **Telemetry Image Compression** rate.

2. Click **Save**.
7. Restart the DV-IP by clicking **Reset**.



Note: Changes will only take effect when saved and the DV-IP unit is reset.

8.7 Audio Set-up

This screen is used to initiate audio recording. You can listen to audio and activate the microphone by using the DV-IP Viewer software.

Audio Set-up

Audio Channel	Title	Enabled
Line-in/Mic	Audio in	<input checked="" type="checkbox"/>
Line-out	Audio out	<input checked="" type="checkbox"/>

1
2
3

To set up audio recording on the DV-IP unit:

1. From the **System** tool bar in the left frame, click **Audio Set-up**.
2. To record audio attached to the Line-Input of the unit, check the **Enable** box for **Line-In/Mic**.
3. To record audio transmitted from a PC with DV-IP Viewer software, check the **Enable** box for **Line-out**.
4. Click **Save**.



Note: An operator can listen and send audio regardless of whether the DV-IP is recording the audio streams. Audio is passed using UDP on PORTS 2074 & 2074.

8.8 Adjusting the size of the RAMDisk

The RAMDisk is an area of memory where images are stored before being written to the hard disk. This means, for instance, that images from before an alarm event can be stored at a lower compression ratio (higher quality) from the period immediately preceding an alarm than they would otherwise have been.

1
2
3

To set-up the RAMDisk:

1. From the **System** tool bar in the left frame, click **RamDisk**.

The following screen is displayed:



Ramdisk Administration	
RAMDISK (A:)	16 Kbytes
NV-RAMDISK (B:)	29 Kbytes
RAMDISK (A:) 16 Kb - 2048 KB NV-RAMDISK (B:) This value can not be changed.	
Note:- The system must be reset after changing the value to RAMDisk (A:)	
<button>Reset</button>	

2. Define the pre-alarm image buffer between 16K and 2048K in the **RAMDISK (A)** field.



Note: The RAMDISK needs to be of a sufficient size to store all the pre-alarmed images that have been configured in the system. For example, if 100 pictures of pre-alarm have been assigned over all the recorded video inputs and the recorded image size is 18K then the buffer needs to be at least 1800K in size.

3. Click **Save**.
4. Restart the DV-IP by clicking **Reset**.

8.9 Configuring the Webcams

The Webcam Configuration screen is used to configure one or more cameras as 'webcams'. For example, the images may be made available to a public web server for use on web pages that large numbers of people can access. The selected cameras are uploaded by FTP to a web server for viewing by anyone who has access to the server on the intranet or Internet.

Webcam Configuration

Webcam Upload Settings

Webcam Server (IP, URL or name):

Webcam Root Drive/Directory:

Webcam 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"/>

Webcam Connection Options

Single FTP session: ☐

Batch transfer: ☐

Webcam Resolution

Low resolution	- 640x256 (approx 6 KB)	<input type="radio"/>
Medium resolution	- 640x256 (approx 12 bytes)	<input type="radio"/>
High resolution	- 768x280 (approx 35 bytes)	<input type="radio"/>

1, 2, 3

To configure webcams on the DV-IP unit:

1. From the **System** tool bar in the left frame, click **Webcam Set-up**.
2. Type in either an IP address, URL, or name for the **Webcam Server** that the DV-IP is connected to.



Note: You can only use a server name if the DNS addresses have been correctly configured in the network settings.

3. Select a home drive and/or directory for the webcam root by typing an address in the **Webcam Root Drive/Directory** field.
4. Insert the address for where the images are stored for upload.
5. Provide the file with an **Image Filename Prefix**.



Note: If this prefix is 'cam_', for example, the uploaded files are cam_01.jpg, cam_02.jpg.

6. Type in a **Username** for FTP login.
7. Type in a **Password** for the FTP login.



Note: A password must be typed in every time the screen is submitted for security reasons.

8. Select a minimum time frame in the **Update Interval (Seconds)** field to wait before updating each image on the Web server.



Note: The **Update Interval (Seconds)** is used to limit the bandwidth used for the upload process.

9. Select cameras by ticking the **Selected** boxes.

10. Select **Single FTP Session** to avoid the login/logout procedure for each image. The video server stays connected to the ISP until it is disabled or there is a connection error.
11. Select **Batch transfer** to transfer all camera images in one batch.



Note: With the **Batch transfer** option, the **Update Interval** is the delay between all images being updated. Without this option the **Update Interval** is the delay between each camera update.

12. Choose the **Webcam Resolution** by selecting low, medium, or high.
13. Choose when the webcam updates are enabled to the host system by selecting Disabled, Enable with system SET, Enable when system UNSET, Always Enable.
14. Click **Save**.

8.10 Configuring and Testing Relays

This screen is used to test the four on-board relays or the optional 485 BUS expansion ROM.

Relay Outputs

Global Alarm:	<input checked="" type="checkbox"/>	(On-Board Relay 1)
Global VMD:	<input checked="" type="checkbox"/>	(On-Board Relay 2)
Global Camera Fail:	<input checked="" type="checkbox"/>	(On-Board Relay 3)

On-Board Relays

Relay:	1	2	3	4
Closed:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Module 1 (Address 160) - Default, used with alarms

Relay:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Closed:	<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"/>

Module 2 (Address 161) - Default, controlled by DV-IPviewer

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

1
2
3

To configure the four internal relays:

1. From the **System** tool bar in the left frame, click **Relay Test Page**.
2. If you want the DV-IP to control **Relay 1** automatically when an alarm occurs, check the **Global Alarm** box.
3. If you want the DV-IP to control **Relay 2** automatically when a Video Motion Detection (VMD) event occurs, check the **Global VMD** box.
4. If you want the DV-IP to control **Relay 3** automatically if a camera fails, check the **Global Camera Fail** box.
5. Tick the appropriate **Closed** box for relays that are not configured to be automatically controlled by DV-IP to manually close the contacts on the relay.
6. Click **Save** to save the configuration and activate the **Closed** boxes.

8.11 Enabling the System Features

The System features screen is a master control menu for enabling the following five features on the DV-IP unit:

- Text-in-images
- 485 expansion bus
- Remote reporting
- Automatic FTP download
- Webcam support

1
2
3

To set the DV-IP system features:

1. From the **System** tool bar in the left frame, click **System Features**.
2. Select the features that are required for the DV-IP unit by placing a check by the option.
3. Click **Save**.
4. Restart the DV-IP by clicking **Reset**.

Any changes made to this screen only takes effect after the system is reset.



Note: If these features are not enabled on this screen, they are inactive, no matter how the other screens are set up.

8.12 Resetting the DV-IP Unit

Some features require that the DV-IP be reset for changes to take effect, for example, those held in non-volatile memory.

1
2
3

To reset the DV-IP unit:

1. From the **System** tool bar in the left frame, click **Reset**.

The following screen appears:



2. Click **Yes**.

The reset happens immediately on confirmation of reset, and the countdown represents the period until the html pages can be accessed again.

8.13 Configuring the Logs

The DV-IP produces log files for PPP connections, anonymous FTP connections, illegal file access attempts, and FTP and telnet users.

System Logs Set-up	
Log PPP connections:	<input checked="" type="checkbox"/>
Log anonymous FTP connections:	<input checked="" type="checkbox"/>
Log illegal file access:	<input checked="" type="checkbox"/>
Log Telnet/FTP users:	<input checked="" type="checkbox"/>
Reset	

1
2
3

To set-up the system logs:

1. From the **System** tool bar in the left frame, click **System Logs Set-up**.
2. Select the settings that are required by checking the appropriate boxes.
3. Click **Save**.
4. Restart the DV-IP by clicking **Reset**.



Note: Any changes made to this screen only takes effect after the system is reset.

8.13.1 Viewing the Connection Log

This log details connections to the unit, with a username for easy identification.



Help: Click the help icon on screen for details of the different fields.

8.13.2 Viewing the Anonymous FTP log

This details anonymous FTP connections to the unit. Setting up a password can prevent anonymous connections to the unit.

By editing the *USERS.ini* file found in the *ETC* directory of the DV-IP you can set up a password to prevent an anonymous connection to the unit.



Help: Click the help icon on screen for details of the different fields.

8.13.3 Viewing the Security Log

This log details illegal file access attempts.



Help: Click the help icon on screen for details of the different fields.

8.13.4 Accessing the Logfile

The logfile screen shows a log of system information such as start ups, resets, and timed set/unsets.



Help: Click the help icon on screen for details of the different fields.

8.13.5 Accessing Logfile backup



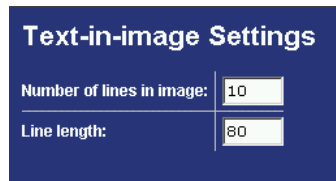
Help: Click the help icon on screen for details of the different fields.

9 Advanced Configuration

9.1 Configuring the Text in Images

You can configure **Text in Images** to display incoming data via an RS232 port from, for example, a POS till or an ATM machine.

This screen specifies the maximum line length of the data and the number of lines of data stored with each image. A full screen width would normally be 80 characters.

A screenshot of a configuration screen titled "Text-in-image Settings". It has a dark blue background with white text. There are two input fields: "Number of lines in image:" with a value of "10" and "Line length:" with a value of "80".

Text-in-image Settings	
Number of lines in image:	10
Line length:	80

To configure the text in images:

1. In the Config area, click **Cameras** from the left-hand toolbar followed by **Text in Images**.
2. Assign communication ports to the required cameras.
3. Use FTP software to access the PATHS.ini file in the DV-IP /etc directory.
4. Edit the file using a text editor to specify which communication port(s) receive the data. An example file is included below.
5. Once it has been edited, upload the file back to the unit.



Note: When files are edited in this way, a system reset is recommended to activate the changes.

PATHS.ini file

```
# DV-IP 04-12-02
# -----
# Example ini file to add text for Serial Port-1 to Serial Port-4
#
# Serial Ports 1 = tty
# Serial Ports 2 = term
# Serial Ports 3 = aux1
# Serial Ports 4 = aux2
#
# TEXT00 camera 1....TEXT16 camera16
# The Serial Ports in the to be set as "TEXT" input.
# -----

# =====
# Serial Port 1 will store text with Camera-1
# =====
[PATH0]
input_path=\tty
output_path=\pipe\TEXT00    {Text requires changing only}
buffer_size=80
```

```
# =====
# Serial Port 2 will store text with Camera-2
# =====
[PATH1]
input_path=\termv output_path=\pipe\TEXT01 {Text requires changing only}
buffer_size=80

# =====
# Serial Port 3 will store text with Camera-3
# =====
[PATH2]
input_path=\aux1
output_path=\pipe\TEXT02 {Text requires changing only}
buffer_size=80

# =====
# Serial Port 4 will store text with Camera-4
# =====
[PATH3]
input_path=\aux2
output_path=\pipe\TEXT03 {Text requires changing only}
buffer_size=80
```

9.2 Protecting the DV-IP Unit Using Passwords

The DV-IP has password protection for viewing live and recorded footage, configuration, telnet, and FTP. This helps prevent unauthorised access to areas restricted by the administrator.

9.2.1 Default Passwords

The DV-IP unit comes with the following default username and passwords.

Screens	Username	Password
Configuration	dm	web
FTP	dm	ftp
Telnet	dm	telnet
Serial	dm	serial



Note: As every DV-IP has these passwords by default, you are advised to change them.

9.2.2 Configuring Password Protection on the DV-IP Unit

Passwords are held in two files on the DV-IP; the *USERS.ini* and the *WEBUSER.ini* file. These can be found in the */etc* directory on the unit. You can accessed the files by FTP, edit them, then upload them back onto the unit.

Before you make changes to either password file, it is recommended you make a copy of the default file, in case you wish to restore it later.

USERS.ini

The *USERS.ini* file holds the usernames and passwords for FTP, telnet and serial access. To alter the usernames and passwords, change the relevant text in the file, then upload the changed file to the unit.

For example, original settings for FTP are dm=ftp (dm = username, FTP = password), shown as below:

```
[FTP]
dm = ftp
```

To change the password, edit the file in text editor and change dm = ftp to:

```
user = password
```

So the new username is **user** and the new password is **password**

Save the file and upload it to the unit, reset the unit for the changes to become active.

If you wish to define multiple usernames and passwords for a unit, add each new username and password below the existing one:

For example, existing information:

```
[FTP]
dm=web
```

To add usernames and passwords, just add the following:

```
[FTP]
dm=web
user=password
third=here
another=user
```



Note: A “#” symbols indicate comments. In the example below, the serial username and password is commented out, so no username or password is required for serial access.

```
# DV-IP v1.0 12-12-02
[FTP]
dm=ftp
[Telnet]
dm=telnet
[Serial]
# serial=password
```

WEBUSER.ini

The *WEBUSER.ini* file holds usernames and passwords for accessing Live View, playback and configuration. It also holds username and password details for accessing the unit via the DV-IP Viewer.

To change the username and password, locate the existing username and password for each section. The file below is set up for password-protected configuration. To enable password protection for each other section, remove the # sign in front of each ‘object =’ line up to the username and password lines.

To remove password protection, add a # to the start of each ‘object =’ line for the relevant section. If two or more usernames are desired, add each new username and password below to the existing information.

#	#####
#	# DV-IP Webuser.ini Version (25-08-2003) #
#	#####

```
[UNlock]
object=frmpages/dvip_register.shtml
# -- Users Passwords --
dm=unlock
```

```
[Watermarking]
#      object=frmpages/dvip_watermarking.shtml
#
# -- Users Passwords --
#      dm=watermark
```

```
[WebPage Configuration]
# ..HOME MENU
#
#      object=webpages/index.html
#      object=webpages/blank.html
#      object=webpages/live.shtml
#      object=webpages/twinview.shtml
object=frmpages/index.html
object=frmpages/dvip_main.shtml
object=frmpages/dvip_about.shtml
# ..CAMERAS MENU
#
object=frmpages/dvip_camera_setup.shtml
object=frmpages/dvip_camera_setup_adv.shtml
object=frmpages/dvip_std_rec.shtml
object=frmpages/dvip_var_rec.shtml
object=frmpages/dvip_Schedule.shtml
object=frmpages/dvip_holidays.shtml
object=frmpages/dvip_text_in_images.shtml
```

```
# ..ALARMS MENU
#
object=frmpages/dvip_alarm_inputs.shtml
object=frmpages/dvip_alarm_zones.shtml
object=frmpages\vmsetup.jar
object=frmpages/dvip_vmd.shtml
object=frmpages/dvip_database.shtml
object=frmpages/dvip_hosts_profiles.shtml
```

```
# ..SYSTEM MENU
#
object=frmpages/dvip_network_settings.shtml
object=frmpages/dvip_serial_ports.shtml
object=frmpages/dvip_audio.shtml
object=frmpages/audioscope.shtml
object=frmpages\audioscope.class
object=frmpages/dvip_ramdisk.shtml
object=frmpages/dvip_ftp.shtml
object=frmpages/dvip_webcam.shtml
object=frmpages/dvip_relays.shtml
object=frmpages/dvip_confirm_shutdown.shtml
```

```
object=frmpages/dvip_shutdown.shtml
```

```
# ..LOGS MENU
#
object=frmpages/dvip_system_logs.shtml
object=logs/connect.txt
object=logs/access.txt
object=logs/security.txt
object=logs/log.txt
object=logs/bak.txt
```

```
# -- Users Passwords --
dm=web
```

```
[Admin]
#####
# Provides full access live & playback #
#####
#      object=cgi
# -- Username(s) Password(s) --
#      admin=admin
```

```
[User1]
#####
# Provides access only to camera-1 in live & playback #
#####
#      object=cgi
#      live_cams=1
#      replay_cams=1
# -- Username(s) Password(s) --
#      1=1
```

```
[User2]
#####
# Provides access only to camera-2 in live & playback #
#####
#      object=cgi
#      live_cams=2
#      replay_cams=2
# -- Username(s) Password(s) --
#      2=2
```

```
[User3]
#####
# Provides access only to camera-1,2,3,4 & 6 in live & playback #
#####
#      object=cgi
#      live_cams=1-4,6
#      replay_cams=1-4,6
# -- Username(s) Password(s) --
#      3=3
```

9.3 Default TCP/IP Port Mappings

DV-IP uses ports within the TCP/IP stack to pass information from the physical layer to the application layer. Applications which are supported by DV-IP include Telnet, FTP, HTTP etc. Depending on the data being passed TCP or UDP packet formatting will be used. Below is a table detailing port assignments and their use.



Note: This information will be valuable to the IT Administrator if problems are encountered receiving video and audio etc. This information will also be required by the IT Administrator when applying security to firewalls etc.

PORT	TYPE	APPLICATION	USE
21	TCP	File Transfer Port – (FTP) Connection	This is used for archiving alarmed images to a remote server
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 DVIP or when accessing the WebPages.
1025	UDP	Telemetry Control	PTZ commands are passed from the PC to the DV-IP
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 <ip address> 5201

Operation

In this section

- **Using the DV-IP viewer**
- **Using the Live Page**
- **Using the DuoView™**
- **Recording to a PC**
- **Installing the viewer software**
- **Watermarking images**

8 Operating DV-IP

The onboard viewer is a set of onboard HTML pages that can be accessed through a standard web browser. These screens allow you to configure the DV-IP and view the screens locally.

For multi-user viewing and alarm receiving, you must install the DV-IP Viewer application from the CD ROM.

8.1 Supported Systems

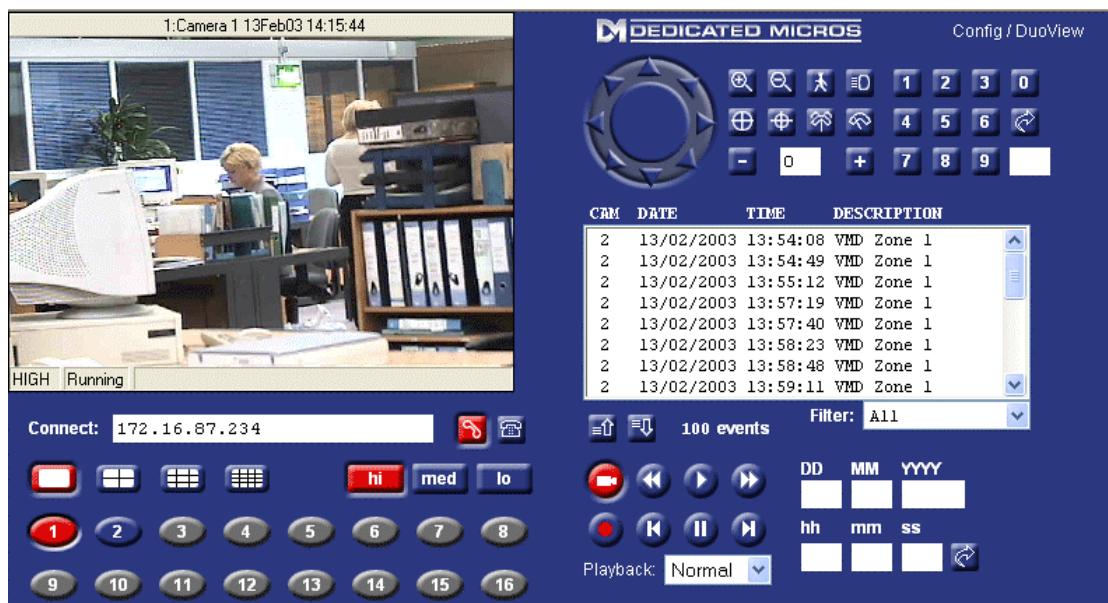
Dedicated Micros only supports DV-IP using the following operating systems or web browsers:

- Operating System: Windows 98SE, NT4 SP6, 2000 and XP
- Internet Browser: IE 5.5 onwards, Netscape 4.7



WARNING: Please see section 3.3 for the minimum PC requirements required for web browser control.

8.2 Using the Live Page



The **Live Page** is accessible from the home page of the DVIP by selecting the **Live Page** button. This screen allows you to view live or recorded images from any camera active on the system.



Note: You can only view recorded images from those cameras set to record in the configuration. The optimum screen resolution on your PC is 1024x768

1
2
3

To use the Live Page:

- Choose the image display view by selecting either **single camera**, **quad display**, **9-way**, or **16-way**.





Note: Quad views and above take their cameras in sequential order from the first selected camera, so in a quad view, selecting camera one gives cameras 1 to 4, selecting camera 5 gives cameras 5 to 8 and so on.

2. To copy images to the clipboard for use by other applications, right click on the display.



Note: Right clicking and pasting to an external application can be achieved for all views; a 16-way view is copied in the same way as a single camera.

3. Select the image resolution by clicking either the **hi**, **med**, or **lo** button from the toolbar.



Note: The actual image resolution and file size settings for each button are set in the **Camera Set-up** screen.

4. To view the live or recorded image, select the available camera(s) from the **Camera Selection** toolbar.



Note: For cameras that are available the buttons are shown in blue (or red if active). Buttons are greyed for cameras that are unavailable.



5. Pan, Tilt and Zoom (PTZ) cameras using the joystick.
6. Control the speed of the joystick movement using the plus and minus signs to the right of the joystick.



Note: The current movement speed setting is displayed in the number box.

7. The **Telemetry Controls** buttons are as follows:



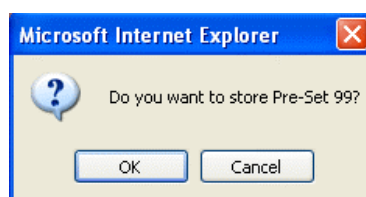
Top row	Zoom In, Zoom Out, Patrol, Lights On/Off
Middle row	Iris Open, Iris Close, Washer, Wiper
Bottom row	Reduce Movement Speed, Current Speed, Increase Speed

8. Click the number button between 0 to 99 in the **Preset Control** panel to select the require PTZ preset.



9. Right click on the last number depressed to store the preset.

The following confirmation box appears:



10. Click **OK**.

11. Double click on the required event in the **Events Database** that you want to view.



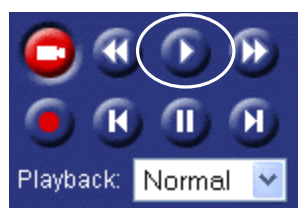
Note: The events database is a listing of all power ups, VMD alarm events, and contact alarm events. This database is automatically updated every time a new event occurs.



Note: Events are listed with the following information (from left to right); **camera number, date, time, description of alarm.**

CAM	DATE	TIME	DESCRIPTION
2	13/02/2003	13:57:40	VMD Zone 1
2	13/02/2003	13:58:23	VMD Zone 1
2	13/02/2003	13:58:48	VMD Zone 1
2	13/02/2003	13:59:11	VMD Zone 1
2	13/02/2003	13:59:39	VMD Zone 1
2	13/02/2003	13:59:54	VMD Zone 1
2	13/02/2003	14:00:18	VMD Zone 1
2	13/02/2003	14:00:47	VMD Zone 1
2	13/02/2003	14:01:08	VMD Zone 1
2	13/02/2003	14:01:23	VMD Zone 1
2	13/02/2003	14:03:19	VMD Zone 1
2	13/02/2003	14:03:36	VMD Zone 1
2	13/02/2003	14:04:15	VMD Zone 1
2	13/02/2003	14:04:42	VMD Zone 1
2	13/02/2003	14:05:00	VMD Zone 1

12. Click the **Play** button (indicated by the white circle below) to view the event.



13. Select next/previous event block icons to view the next 20 events listed in the database.



14. The **Player Control** buttons are as follows:

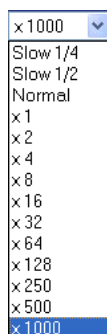


Top row	Live View, Rewind, Playback, Fast Forward
Middle row	Record to Local Storage, Frame Rewind, Still, Frame Advance
Bottom row	Rewind/Fast Forward speed



Note: The **Record** button is for saving live or recorded footage to the PC desktop. It does not affect recording to the DV-IP hard disks.

15. Select a **Playback** speed from the drop-down menu.



Note: The **Playback** speed button only affects the rewind and fast forward speed. The speed of these functionalities can be set from 1/4 normal speed to 1000 times normal speed.

16. To access a piece of footage recorded on the DV-IP hard drive, type the date and time into the **Instant Go-To** fields and click the arrow button

DD	MM	YYYY
<input type="text"/>	<input type="text"/>	<input type="text"/>
hh	mm	ss
<input type="text"/>	<input type="text"/>	<input type="text"/>



Whichever cameras are being viewed will then immediately be seen with footage from the time and date selected. If a time and date selected are before footage has been recorded, then 'Image not Available' appears.

8.3 Using the DuoView™ Display

DuoView™ is a new concept seen on the DV-IP. The DuoView™ screen allows you to view both live and recorded footage from any cameras, on the same PC screen simultaneously.

The DuoView™ screens are controlled using the same controls as seen on the Live View screen. The only difference is the check boxes used to indicate control of the left or right screen (known as the Live Images Screen or Replay Images Screen). Both screens can, in fact, be used as live or replayed views.

A check in the box next to the screen title indicates control of a screen; the screen under control is the Replay Images screen (see the screen-shot above).



Note: If both screens are checked, then both are controlled simultaneously, and any button pressed will affect both screens.



8.3.1 Using the DuoView™ to Compare Live and Replay Footage

To compare live and replay footage:

1. Check both the **Live Images** and **Replay Images** boxes to control both screens.
2. Select the cameras and view you require (**single camera, quad view, 9-way, or 16-way**).
3. Uncheck the **Live Images** box, leaving the **Replay Images** box checked.
4. Select the date and time you wish to compare the **Live Image** screen with, and enter these in the **Date (DD/MM/YY)** and/or **Time (hh/mm/ss)** fields.
5. Press the arrow button to **Instant Go-to** that point in time.
6. Press **Play**, and the replay footage is displayed in the **Replay Images** screen.



Note: The footage can now be controlled using the playback controls, and compared to the Live Images screen.

8.3.2 Using the DuoView™ to View Eight Live Cameras in Two Quad Displays

To view eight live cameras simultaneously:

1. Place a check in the **Live Images** box only.
2. Select the first camera in the quad sequence. This displays the selected camera, and the next three in sequence.
3. Uncheck the **Live Images** box.
4. Check the **Replay Images** box.
5. Select the first camera in the quad sequence.

6. Press the **Live** button in the playback controls.



Note: You will now see up to eight different cameras on the two screens, four in each quad view. This will also work in the other following views; **single camera**, **9-way**, and **16-way**.

8.4 Recording to a PC or to Network Storage

To record the footage being viewed, be it live or recorded, follow the steps below:



Note: Recording on PC or network storage is visible on the **Live Page** and the **DuoView™** screen.

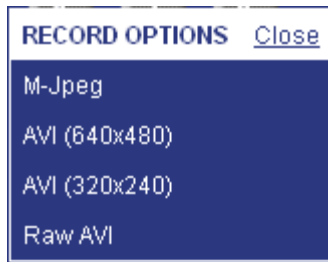


To record to a PC or network storage:

1. Rewind the video to the desired time, or use the **Instant Go-To** fields.
2. Click the **Record** button in the controls, once you have reached the desired time.



This brings up the **Record Options**.



You can select the type of video you wish to record as M-JPEG, Raw AVI, or two resolutions of AVI. Once a type of video is selected, recording will start if you are viewing live footage. If you are viewing replay footage, you need to press the **Play** button to start the recording.

3. Press the **Record** button again to stop recording.



Note: You can now find a recorded file on your PC desktop. To play back the footage, use the DV-IP VCR programme included with the DV-IP Viewer.

8.5 Installing the DV-IP Viewer Software

You interact with the DV-IP unit by using the functionality of the DV-IP viewer application. This allows you to complete the following tasks:

- Camera set-up and configuration
- Event management

You can install the DV-IP Viewer software in two ways:

- Install the software from the DV-IP unit itself
- Install the files from the CD ROM supplied with the unit



WARNING: Please see section 3.4 for the minimum PC requirements required for DVIP Viewer.



Note: It is recommended that the DV-IP Viewer software be downloaded from the **Home Page** screen.

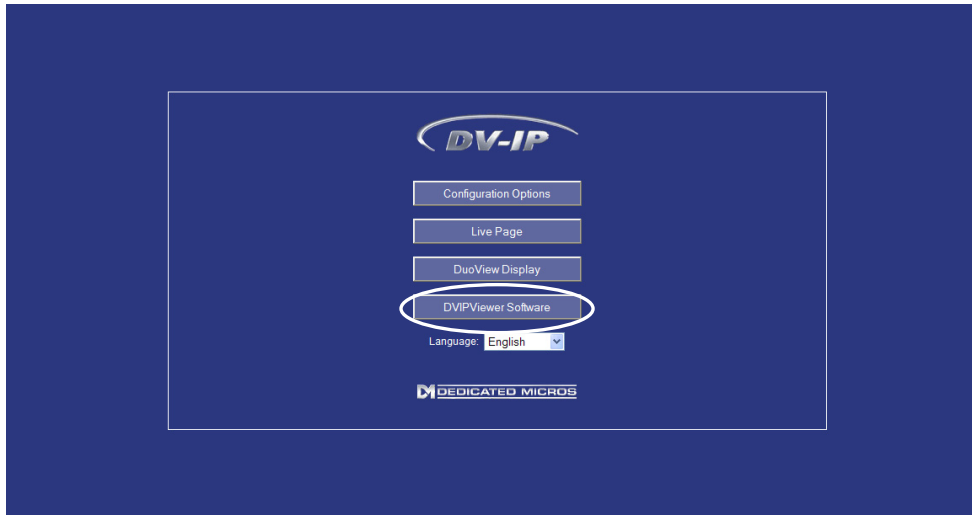


Note: Both options are outlined below, but it is recommended that you install the software from the unit itself, only using the CD ROM option as a backup.

1
2
3

To install the DV-IP Viewer software from the unit:

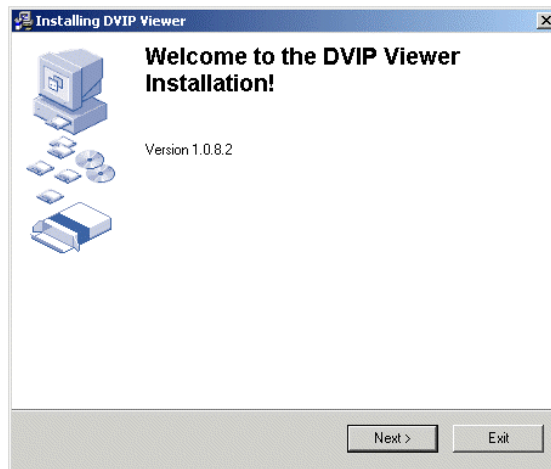
1. Insert the DV-IP unit's IP address in to the address bar of the web browser.
2. The following home page will appear.



3. Click the **DVIP Viewer Software** button, (circled).

5. Accept any warnings concerning installing software and continue.

The following DV-IP Viewer welcome screen is displayed:



4. Click **Next** and follow the on screen prompts to install the software.
5. Click **Browse** and select the directory where the program is to be installed.
6. Click **Next**.
7. Click **Finish**.



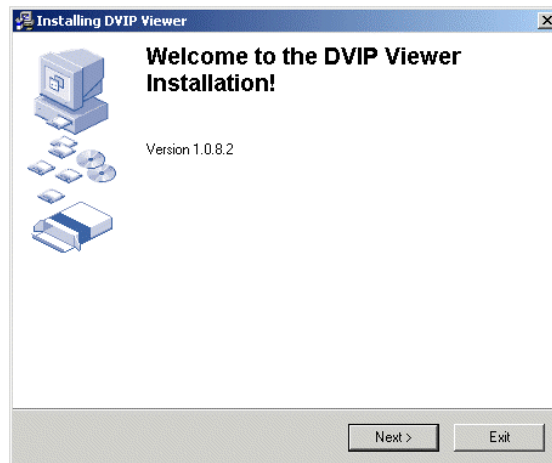
Note: The software is also available on the CD ROM supplied with the DV-IP unit.



To install the DV-IP Viewer software from the CD ROM:

1. Insert the Installation CD ROM.
2. The CDROM will autorun.
3. Click on the **DVIP Viewer Software** button.
4. Accept any warnings concerning installing software and continue.

The following DV-IP Viewer welcome screen is displayed:



5. Follow the on screen prompts to install the software.

8.6 Setting Up Watermarking

Using the Watermarking screen, you can examine the video partition index information and generate watermark certificates. These watermarks prove that an image has not been altered or tampered with by producing MD5 signatures that change if any alterations are made to the image files.

	Hours	Mins	Secs	Date	Mon	Year
Start Date and time:	14	55	34	22	2	2003
End Date and time:	14	55	34	24	2	2003

Report Author: Rob Bell

Watermark step size: 256

Partition Information Summary

- C:\VIDEO\DIR00000\VID00000.VID Mon 24 Feb 2003 01:23:10 245 1530 0xb
- C:\VIDEO\DIR00000\VID00001.VID Mon 24 Feb 2003 01:27:15 245 1530 0xb
- C:\VIDEO\DIR00000\VID00002.VID Mon 24 Feb 2003 01:31:20 244 1529 0xb
- C:\VIDEO\DIR00000\VID00003.VID Mon 24 Feb 2003 01:35:25 244 1528 0xb
- C:\VIDEO\DIR00000\VID00004.VID Mon 24 Feb 2003 01:39:29 245 1530 0xb
- C:\VIDEO\DIR00000\VID00005.VID Mon 24 Feb 2003 01:43:34 244 1529 0xb
- C:\VIDEO\DIR00000\VID00006.VID Mon 24 Feb 2003 01:47:39 244 1528 0xb
- C:\VIDEO\DIR00000\VID00007.VID Mon 24 Feb 2003 01:51:43 245 1530 0xb
- C:\VIDEO\DIR00000\VID00008.VID Mon 24 Feb 2003 01:55:48 244 1528 0xb
- C:\VIDEO\DIR00000\VID00009.VID Mon 24 Feb 2003 01:59:52 245 1529 0xb
- C:\VIDEO\DIR00000\VID00010.VID Mon 24 Feb 2003 02:03:57 245 1530 0xb
- C:\VIDEO\DIR00000\VID00011.VID Mon 24 Feb 2003 02:08:02 244 1530 0xb
- C:\VIDEO\DIR00000\VID00012.VID Mon 24 Feb 2003 02:12:07 244 1529 0xb
- C:\VIDEO\DIR00000\VID00013.VID Mon 24 Feb 2003 02:16:11 245 1529 0xb
- C:\VIDEO\DIR00000\VID00014.VID Mon 24 Feb 2003 02:20:16 244 1528 0xb
- C:\VIDEO\DIR00000\VID00015.VID Mon 24 Feb 2003 02:24:20 245 1528 0xb

Partition info Get index info Watermark Create Certificate

1,2,3

To configure the watermarking:

1. In the System area, click the **Watermaking** button on the left-hand side toolbar.
2. Select **Start Date and Time** and **End Date and Time** to set the time range.
3. Click the **Partition Info** button to set the partition information.



Note: The selection window displays the partition information covering the specified time period.



Note: Click the **Get Index Info** button to view the index information, if an individual partition is selected.

4. Click the **Watermark** button to generate the watermark codes.



Note: The **Watermark step size** specifies the skip distance between the bytes used in the watermark calculation. For example, a step of one uses every byte in the video partition in the watermark calculation. A smaller step size results in a longer calculation time.



Note: Progress and/or completion is indicated by messages in the status bar.

5. Type the report author's name in the **Report Author** text box, if required.
6. Click the **Create Certificate** button to create a watermark certificate.

The watermark certificate can be printed if required.



Note: Watermarked video data can be downloaded using the DV-IP Viewer application. Downloaded watermarked video data may be authenticated using the watermark utility installed with the DV-IP Viewer.

Reference Information



In this section

- **Service**
- **Regulatory Notes**
- **CE Mark**

10 Reference information

10.1 Service



WARNING: Do not attempt to service the DV-IP unit yourself as opening or removing covers may expose you to dangerous voltage or other hazards. Refer all servicing to qualified service personnel.

10.2 Regulatory Notes FCC and DOC Information

(USA 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 is required to correct the interference at their own expense.

If necessary the user must consult the dealer or an experienced radio and/or television technician for corrective action.

This reminder is provided to call the CCTV system installer's attention to article 820-40 of the NEC that provides guidelines for proper grounding and, in particular, specifies that the cable ground must be connected to the grounding system of the building, as close to the point of cable entry as practical.



Refer to: The following booklet prepared by the Federal Communications Commission: "How to Identify and Resolve Radio and/or TV Interference Problems". This booklet is available from the US Government Printing Office, Washington, DC20402, and Stock No 004-000-00345-4.

10.3 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 Limited, Swinton



www.dedicatedmicros.com

DEDICATED MICROS UK

11 Oak Street,
Swinton,
Manchester
M27 4FL
UK
Tel: + 44 (0) 161 727 3200
Fax: + 44 (0) 161 727 3300

DEDICATED MICROS USA

14434 Albemarle Point Place
Suite 100
Chantilly
Virginia 20151
USA
Freephone: + 1 800 864 7539
Tel: + 1 703 904 7738
Fax: + 1 703 904 7743

DEDICATED MICROS ASIA

16 New Industrial Road
#03-03 Hudson Technocentre
Singapore 536204
Singapore
Tel +65 6285 8982
Fax +65 6285 8646

DEDICATED MICROS AUSTRALIA

5/3 Packard Avenue,
Castle Hill,
NSW 2154,
Australia
Tel: +612 9634 4211
Fax: +612 9634 4811

DEDICATED MICROS EUROPE

Neckarstraße 15a,
41836 Hückelhoven,
Germany
Customer Services:
Tel: + 49 243 352 580
Fax: + 49 243 352 5810

DEDICATED MICROS MALTA

UB2,
San Gwann Industrial Estate.,
San Gwann,
SGN09
Malta
Tel: + 356 2148 3673
Fax: + 356 2144 9170

DEDICATED MICROS MIDDLE EAST & AFRICA

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
Mobile: + 971 (5) 0450 0149

