DVIP ATM

Setup Guide

Contents

Software Issue No 04.4(019) M2IP-03.1 (09.2)

Introduction 3

Important Safeguards 7

Installing the Unit 9

Simple Installation...11

Network Configuration 20

Simple Configuration..22

Tools...90

Reviewing the Unit Logs 94

Appendix A...100

Appendix B – .ini Files 101

Appendix C – Port Assignment on the unit 112

Appendix D –Unit Serial and Network Cables 114

Appendix F – SMS Message Format......................................117

Additional Information 120

Whilst every attempt is made to ensure these manuals are accurate and current, Dedicated Micros reserve the right to alter or modify the specification of the machine described herein without prejudice.

Introduction

What is the…

DVIP ATM Interface?

ATM machines operate a service of convenience, which is taken for granted by most of the general public, however these cash points are open to abuse. Popular crimes include; card skimming, shoulder surfing, and plain straight forward theft.

To help the financial sector combat ATM crime, and the fraudulent use of debit/credit cards, Dedicated Micros designed the DV-IP ATM. The unit is specifically sized for installation within the confined conditions of an ATM machine. The DV-IP ATM processes transaction data which is then recorded with the video footage. Post event analysis via the built in text search engine provides video imagery of the ATM user plus transaction information. This will then allow the branch customer services team to quickly resolve any genuine withdrawal disputes. Coupled with a monitor the spot output provides a visual deterrent assuring customers that the facilities are secured by an active CCTV system.

DV-IP ATM is a professional network video server, and is designed to meet the demands of 24 hour video surveillance using new or existing IP enabled computer networks, for example, alarm reporting, FTP archiving, JPEG/MPEG-4 transcoded video transmission and MultiMode Recording can all be accessed and configured through the network.

The DM range of video servers provide a cost effective means to record and distribute video from your CCTV cameras to any computer on the network, anytime, anywhere.

As part of the ‘NetVu Connected’ family the new DV-IP ATM is built to adapt to future advances in security technology, protecting your investment for years to come.

- IP address notification through a connected spot monitor simplifies the installation process
- Simultaneous MPEG-4 & JPEG transmission and recording
- Designed for central monitoring applications (BS-8418 compliance)
- MultiMode Recording - Dynamically-switchable resolution, record-rate & compression (MPEG4/JPEG) per camera
- Simultaneous record, playback, live viewing, archiving and multiple user network viewing with no loss of recording performance
- Automatic connection to remote video receiving centre on alarm
- Pre-alarm recording to capture evidence before alarms are triggered
- Instant Remote Alarm monitoring using Ethernet, PPP modem link, Email and SMS
- False alarm suppression and alternative signalling path
- Immediate access to any time/date via instant GOTO capability
- Video motion search allows search back through recordings for movement in a specific area of the image
- Web based configuration allows remote system adjustments negating the need for site visits
- Free NetVu ObserVer remote viewing software
- SDK available for project customisation
- Multiway DuoVu for live and recorded viewing simultaneously
- All passwords and user accounts are configurable through the web interface

A Digital Video Recorder

MultiMode RECORDING

MultiMode recording gives you the ability to set different record rates, resolutions and compression algorithms across scheduled, normal and alarm modes. Up to 24 MultiMode Recording profiles can be set per unit, giving you the flexibility to adjust resolution (QCIF to 4CIF), record rates and compression settings (MPEG-4/JPEG) dynamically on individual cameras and across the whole unit.

RECORDING

Simultaneous recording and playback from any camera continues uninterrupted whilst other images are being viewed live. The DV-IP ATM also allows for the resolution of viewed images to be dynamically altered maximising live viewing performance over the available bandwidth.

NETWORK CONTROL

Control of DV-IP ATM is achieved over Ethernet either by NetVu ObserVer or via a standard web browser. Pre-loaded web pages allow for setup, configuration, image archiving, live viewing, telemetry and playback.

MULTIWAY DuoVu

DV-IP ATM has traditionally provided playback in full screen, picture in picture and quad display modes. Now you can choose to playback in any multiway display mode. For ultimate flexibility you can now have any combination of live and recorded segments on the multiway view, allowing you to review recorded material, while keeping an eye to ongoing surveillance.

TEXT INTEGRATION

Using the ATM Interface Module (available separately) transaction data can be captured. The ATM Interface Module interfaces with the ATM machine via serial async/bisync comms or Ethernet, the native protocol is then processed, reformatted and passed on to the DV-IP ATM for recording with the video. It is possible to perform retrospective searches on captured text via the pre loaded web pages and other text enabled DM applications. The NetVu Connected SDK offers developers text specific tools enabling integrators to create powerful custom applications.

TEXT SUPPORT

Through the inclusion of (RS) Text features, the DV-IP ATM can search captured transaction data e.g. for specific goods purchased, transaction numbers, credit card references, keywords and jump straight to the associated video sequence.Additional functionality allows alarms to be raised on the use of keywords from POS and other devices.

Search and playback is also supported through NetVu ObserVer.

INSTANT ALARM REPORTING

The system can dial-out on alarm to a remote site to provide instant alarm notification.

- Instant alarm reporting
- Dial-out on alarm
- Alternative signalling path

RECORD RATE

The DV-IP ATM can record real time on 2 cameras at 50PPS (PAL), 60PPS (NTSC).

MPEG-4 LIVE VIEWING AND PLAYBACK

This technology ensures that users of bandwidth limited networks have increased opportunity to view video in real-time. Features are provided to ensure the user can configure the DVIP ATM’s image resolution, bit rate, and also how many pictures per second to transmit. All images are recorded locally in JPEG format to ensure that recording continues in the event of a network failure.

NETVU CONNECTED

DV-IP ATM has NetVu technology built-in to ensure maximum compatibility with future developments in networked security. NetVu technology enables the DV-IP ATM to fully interoperate with other NetVu compatible products from DM including the DV-IP Decoder, NetVu Console, NetVu ObserVer and PDA Viewers.

VIDEO MOTION DETECTION

- 80x64 pixel VMD detection resolution
- Programmable VMD grid with 16 individually definable zones per camera
- User-definable sensitivity for each zone
- Pre and post activity recording, definable by user
- Change camera recording rates on activity
- Notify user of activity over Ethernet, ISDN and PSTN
- Stores all VMD instances in Events database
- Global VMD relay
- Linkable to alarm zone

SECURITY

DV-IP ATM features a built-in firewall for network intrusion detection and protection. Network PING responses can be disabled, meaning it is no longer possible to discover the DV-IP Servers IP address using automated subnet scanning software. This coupled with the Trusted IP addresses list and the ability to open/close specific TCP and UDP ports ensures the DV-IP ATM is configurable for use on any network large or small.

WEB BASED CONFIGURATION

Web based configuration enables system adjustments to be made remotely to a networked unit, such as change the record rate, setup the advanced VMD grids, program presets and more – without the need for a site visit.

ALARM SUPPORT (BS8418 Note1)

- Tamper (Resistance) ; 0 - 900Ω - Tamper (Short circuit) ; 900 - 1kΩ - Normal (Closed) ;
  1 - 12kΩ - Alarm (Open) ; 12kΩ - Infinity Tamper (Open circuit)
- Voltage Free
- Closed contact operation
- VMD Trigger
- Camera Fail Trigger

ADVANCED ALARM SUPPORT (BS-8418 Note1)

- Tamper proof alarm inputs
- Nuisance detector management
- Application watch dog
- Comprehensive system logs
- Secondary signalling support via relay contact
- Modem port for secondary signalling
- Relay system set/unset notification
- Entry/Exit routes for alarm inputs

Features

Design of the manual

The manual has three parts:

1. Installation

–Giving details of how to install the unit and connect external devices.

2. Setup

–Giving details of the configuration menus of the unit.

3. Operating

–Giving quick reference details on how to control the unit

Important Safeguards

Read Instructions

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

Power Sources

This unit should be operated only from the type of power source indicated on the manufacturer's label.

Servicing

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

Refer all servicing to qualified service personnel.

Ventilation

Ensure unit is properly ventilated to protect from overheating.

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

To prevent fire or shock hazard, do not expose this equipment to rain or moisture. The lightning flash with arrowhead symbol within an equilateral triangle is intended to alert the user of this equipment that there are dangerous voltages within the enclosure which may be of sufficient magnitude to constitute a risk of electric shock.

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Lightning Strike

The unit has some inbuilt protection for lightning strike, however it is recommended that isolation transformers be fitted to the system in areas where lightning is a common occurs.

Regulatory Notes and 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 will be required to correct the interference at their own expense.

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

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

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

CE Mark

If this product is marked with the CE symbol it indicates compliance with all applicable directives.

Directive 89/336/EEC.

A ‘Declaration of Conformity’ is held at Dedicated Micros Ltd.,

1200 Daresbury Park, Daresbury, Cheshire, WA4 4HS

Installing the Unit

Before you start

Check the contents of the box

The following items are included in the box:

- DV-IP ATM
- External Power Supply and Power Leads – one US and one Generic (without a plug)
- CD ROM
- DV-IP ATM Quick Start Guide - Printed version and also supplied on the CD ROM
- DV-IP ATM Simple Setup Guide - Supplied on the CD ROM
- DV-IP ATM Advanced Setup Guide - Supplied on the CD ROM
- RS232 Cross-over Communication cable
- RS485-bus cable with ferrite clamp filter
- Wall-mounting brackets

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

Choosing a location for installation

- Ensure the DV-IP ATM 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.

Typical Voltage Ratings

Typical Power Ratings

Voltage (VAC)	**Typical Current (amps)**	**Power (W)**
240	0.37	88.8
110	0.54	59.4

A quick overview of digital recording

Digital multiplex recorders work in exactly the same way as analogue multiplexers except that they use hard disks to store video, instead of VCR tapes. Analogue recording uses time-lapse recording to extend the length of time recorded onto 2 or 3-hour tape - recording fewer pictures every second.

Adjusting the number of pictures recorded every second also extends the length of time recorded onto the hard disk of a unit. However, other factors also determine the amount of time that can be stored on the disk of a digital multiplex recorder:

The image quality

The record rate

The hard disk capacity

Image quality

Digital multiplex recorders store images in a compressed format, allowing images to be recorded more efficiently. The higher the compression, the smaller the file size, but the image quality will suffer. The DVR offers a range of compression options and image storage formats to give the end user the flexibility to balance between image quality and storage capability.

Kilobytes and Gigabytes are units of storage, 1GB = 1000 Megabytes (MB) and 1MB = 1000 Kilobytes (KB), according to modern hard drive specifications. (Now specified under SI units as one kilobyte (1 kB) = 1000 bytes, whereas one kibibyte (1 KiB) = 1024 bytes to clear the confusion caused by the term kilobyte simultaneously being used to refer to both 1,000 and 1,024 bytes)

With analogue recording, the image quality is dependent on the type of VCR being used; VHS or S-VHS. The unit allows the image quality to be altered by adjusting the image size, for example, Low quality is 14KB, Medium is 18KB, and High is 25KB.

Note: *As for all digital recording, image quality can vary for different scene types, Medium quality may be 18KB in one scene, but it may be 30KB or more to get the same quality in a scene with more detail.*

Using a larger image size will fill the hard disk faster than a smaller image size, as more space is required to store it. To achieve the same amount of recording time when a larger image size is used requires the record rate (PPS) to be reduced.

Standard record rate

The record rate is the amount of pictures recorded to disk in a second, or pictures per second (PPS). This is a system wide figure and is not effected by how many cameras are connected. The update rate per camera can be worked out using the record rate:

Update rate = No. of cameras/Record rate

Hard disk capacity

Using a larger hard disk will allow image quality, recording rate, or recording time to be increased.

Calculating recording time

The unit calculates the recording time automatically when the record rate and image quality are entered. Using the Camera Setup wizard available through the web interface, will allo you to get the optimum settings for your requirements. These can still be edited later.

Alternatively, an interactive record calculator is available for download from our web site:

www.dedicatedmicros.com

Simple Installation

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

Installing the DV-IP ATM using wall-mounting brackets

Connecting Analogue video sources

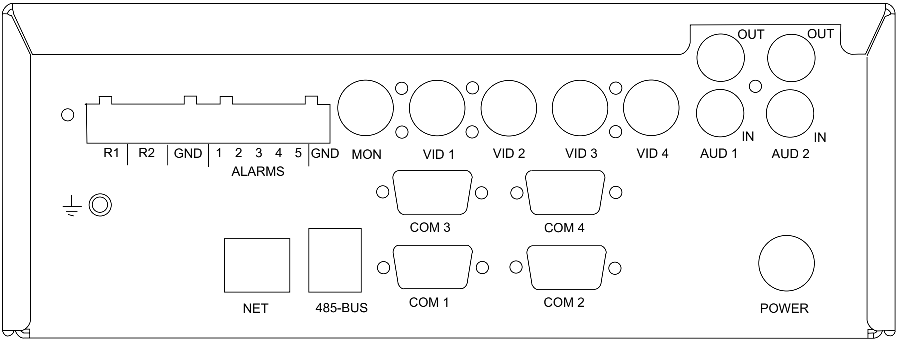
Connecting a Spot Monitor

Connecting the unit to the Network

Applying Power to the system

Rear Panel connections

The illustration shows the rear panel connections.



Video

VID1 to VID4	75Ω BNC composite camera connections, 1V pk-pk.
MON	Spot Moinitor - 75Ω BNC composite monitor output, 1V pk-pk.

Audio

Audio 1 IN	RCA (phono) socket, 8KHZ sampling 47KΩs input impedance
Audio 1 OUT	RCA (phono) socket
Audio 2 IN	RCA (phono) socket, 8KHZ sampling 47KΩs input impedance
Audio 2 OUT	RCA (phono) socket

Data

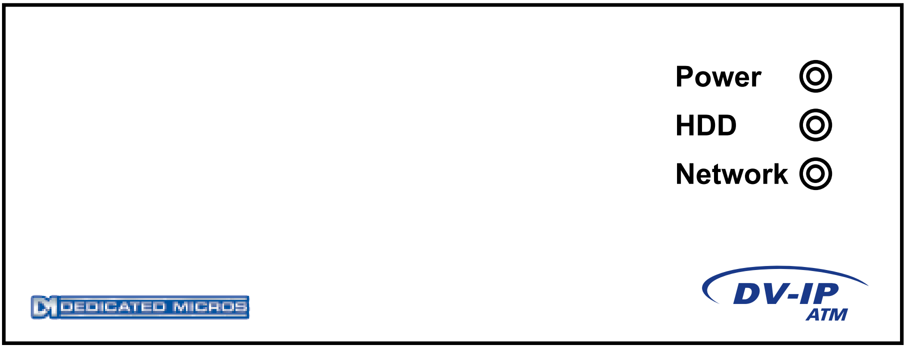
NET	RJ45 10/100BaseT Ethernet connection
485 BUS	1 x MMJ ports for DM 485-BUS accessories (additional alarm inputs/relays)
COM 1 - 2	9 way (male) D Type RS-232 serial port (PPP, general purpose, debug, text in image)
COM 3 - 4	9 way (male) D Type RS-232 (3 wire) serial port (Telemetry, debug, general

purpose, text in image)

Alarms and relays

ALARMS	Screw terminal, NO/NC, 1 - 4 for Aux, 5 for Direct
R1 + R2	Screw terminal, light duty relay output 500mA @ 12V-48V max, user definable

Front Panel



LED's

Power	The power LED will be green to indicate power is connected to the Decoder
HDD	Hard Disk Drive
Network	The Network LED will light when the unit is connected to the network

The Java Virtual Machine is one aspect of Java software used in web interaction. The Java Virtual Machine is built into the Java software download, and helps the Sun JRE run Java applications.

Administration rights will be required to install JRE onto a Windows 2000 or Windows XP machine. The JRE can be loaded using one of three methods, Automatic, Manual or Offline.

Automatic installation will require the machine stays connected to the internet whilst the software is loaded directly from the web. This method requires no user intervention.

Manual installation downloads a small program from the web, which will fetch the required files from the web when it is run. It offers more control over the installed options than the Automatic method.

Offline installation will download all the required files onto the computer before commencing installation. This file can then be run when the computer is not connected to the internet, and copied onto other machines without internet access, if necessary.

The software on the unit is written for the Sun Java Machine, and the Microsoft Java Machine should be disabled for optimum reliability.

You can switch between the Sun Java Virtual Machine and the Microsoft VM. The Sun JVM can be enabled and disabled without having to uninstall it. Switching back and forth between these Virtual Machines can be done through the Advanced tab in your Windows Internet Options Control Panel, OR by using the Java Control Panel.

Note: *It is good practice to check both locations.*

To switch between the Sun JVM and Microsoft VM using Internet Options:

1. Open Control Panel by clicking Start->Settings->Control Panel
2. Open the Internet Options window by double clicking Internet Options
3. Click the Advanced Tab
4. Find the “Java (Sun)” item and check or uncheck the checkbox which says “Use Java 2 v 1.4.x for applet (requires restart)”
5. Check or uncheck the box next to Microsoft VM
6. Save your changes by clicking the OK button
7. Restart the browse

Instructions for switching between the Sun JVM and Microsoft VM using the Java Control Panel:

1. Open the Windows Control Panel by clicking Start->Settings->Control Panel
2. Open the Java Control Panel by double clicking the icon labeled “Java Plug-in”
3. In the Java Control Panel, click the Browser Tab
4. Under the Browser Tab you will see checkboxes next to installed Web browsers.
5. Check or uncheck the checkbox next to the Web browser you want enable or disable from using the Sun JVM
6. Click the Apply button to save your settings
7. Restart Internet Explorer

Tools Required

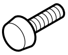
The tools required to install the unit:

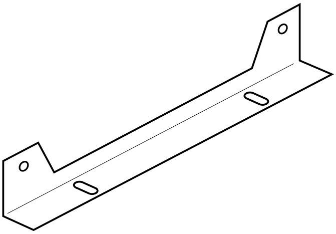
Item	Description
1	Suitable screw driver for mounting the unit in place
Note:	The rack screws are not supplied by Dedicated Micros.
2	Wall-mounting brackets (supplied)
3	Laptop connected to the same network as the unit
4	Power Supply (supplied)
5	Mains cable (supplied)
6	Ethernet cable

Connecting the Mounting Brackets

The unit can be rack or desk mounted the following details the wall mounting process. A mounting kit is supplied with this product, it is important to install this correctly. The kit comprises of:

4 x Rack mount screws

4 x 



2 x Mount ears

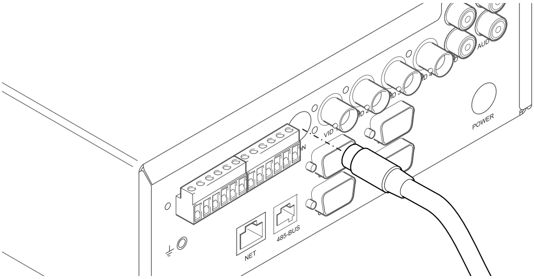
Before connecting any cables to the DV-IP ATM either place the unit on the shelf or connect the wall mounting kit:

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

Connect the DV-IP ATM mounting brackets to the wall.

Connect Monitor

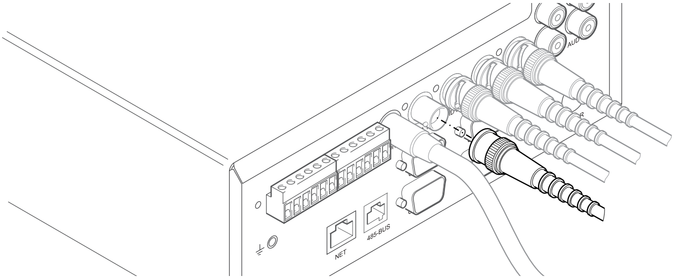
Connect monitor to enable the IP address to be displayed on boot.



Connecting Video Sources

The DV-IP ATM is available with four video inputs. The Video inputs are 75 Ω BNC Connectors and require a 1 Volt peak-to-peak video signal.

The video inputs are by default terminated at 75 Ωs; this is configurable within the DV-IP ATM web configuration pages



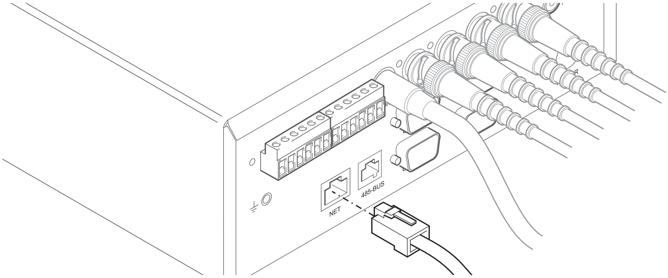
Note: *It is recommended that you connect the cameras from the lowest number first; however it is possible to disable inputs in the DV-IP ATM configuration pages.*

Connecting to the Network

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

Using a straight-through network cable (Appendix A) connect to the NET connector on the unit and a port on the network. The unit is shipped enabled for DHCP network. An IP Address will be automatically allocated when the unit is powered up, and will be displayed on the spot monitor for a user defined period (initially set as 10 minutes).

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

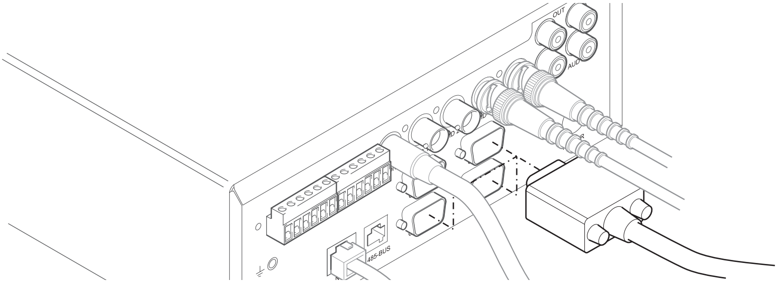


Connecting serial devices

The DV-IP ATM supports four RS232 serial (communication) ports.

Each port can be configured to support various peripheral devices.

By default COM 1 is the only port enabled and is set for Debug (Engineering mode) allowing you to connect and configure the unit on this serial port. All COM ports are 9 Way D-type connector’s with the following pin connections for RS232.

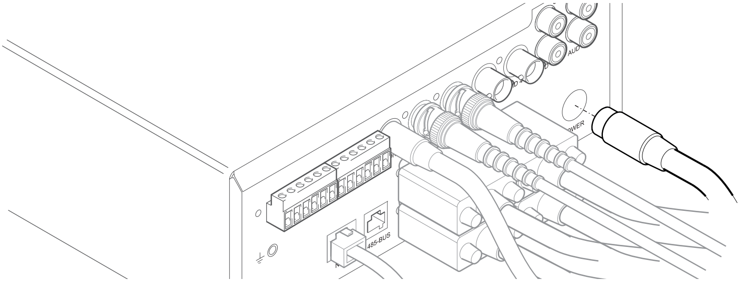


RS232

RS-232	Serial 1 & 2 Pin Allocation	Serial 3 & 4 Pin Allocation
Data Carrier Detect (DCD)	1	-
Receive Data (RX)	2	2
Transmit Data (TX)	3	3
Data Terminal Ready (DTR)	4	-
Ground (GND)	5	5
Data Set Ready (DSR)	6	-
Ready To Send (RTS)	7	7
Clear To Send (CTS)	8	8
Ring Indicate (RI)	9	-

Connecting Power

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



The unit is configured for DHCP and will be automatically allocated and IP Address if connected to a DHCP network.

If a static IP Address is required refer to the next step before applying power.

To connect power to the unit:

1. Ensure the mains if switched off at the socket.

2. Connect the power supply (supplied in the packing kit) to the POWER connector on the unit; this is the 4 pin Din connector.
3. Connect the mains lead (supplied in the packing kit) to the power supply, the European lead requires the relevant mains plug be attached to the lead, ensure you follow Health and Safety procedures.
4. Switch the mains on at the socket.
5. Check the green LED on the front panel of the DV-IP ATM lights to show the unit has powered up successfully.

Allocating an IP Address

The DVIP ATM will automatically retrieve an IP address from any available DHCP server. If no server is available, it will defaullt to a preprogrammed address. The address will be displayed on a connected Spot monitor during the boot sequence, and stay onscreen for a short time. The IP address can then be adjusted via the web interface, using a browser and the displayed IP address. If none of these facilities are available, the IP address can be retrieved and set using the following method. It is recommended that the installer ues the web pages to configure the IP address.

This section is separated into:

Setting a static IP address (Disabling DHCP)

Enabling DHCP

Note: *These changes can be applied using the web interface, once the unit is booted and connected to the network. This information can be found in the user section of this manual.*

Setting a static IP address

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

static IP address

subnet mask

and if required default gateway

1. Ask your Network Administrator to complete the following with the information that will be configured on the unit.

IP address _ _ _ . _ _ _ . _ _ _ . _ _ _ (for example 172.16.0.100)
Subnet mask _ _ _ . _ _ _ . _ _ _ . _ _ _ (for example 255.255.0.0)
Gateway(if required) _ _ _ . _ _ _ . _ _ _ . _ _ _ (for example 172.16.0.254)

2. If a video signal is not already connected to the unit, connect to VID 1 at the rear of the video server.
3. With the mains power OFF, connect the power cable to the unit.
4. If the RS232 communication cable is not connected to the unit, connect this between the COM port on your PC and COM1 on the rear of the unit.
5. On your Windows PC, from the Start menu, select Programs> Accessories> Communications> HyperTerminal and create a new connection using the COM port and the following settings:

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

6. Apply mains power to the unit. The green power LED should light on the front panel of the unit and some debug information should appear in HyperTerminal as the unit starts up, wait for this debug information to finish.
7. In HyperTerminal, log on to the unit by typing +++ and pressing enter.

8. At the command prompt, type the following commands, replacing <aaa.bbb.ccc.ddd>with the values issued by the Network Administrator. <ESC> denotes the Escape button on your keyboard, <ENTER> denotes the enter key on your keyboard.

This will allocate a permanent IP address to the unit and disable DHCP.

Note: *The IP address will be displayed on the spot monitor for a user defined period (nominally 10 minutes) after the machine starts up, providing there is a connected working camera*

Enabling DHCP

The unit is set for DHCP by default.

Allocating permanent IP address will disable DHCP. It can be re-enabled.

1. If a video signal is not already connected to the unit, connect to VID 1 on the top row of BNC connector’s.
2. With the mains power OFF, connect the power to the rear of the unit.
3. Connect RS232 communication cable between the COM port on your PC and COM1 on the rear of the unit.
4. On your PC, from the Start menu, select Programs> Accessories> Communications>HyperTerminal and create a new connection using the COM port and the following settings:

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

5. Apply mains power to the unit. The green power LED should light on the front panel of the unit and some debug information should appear in HyperTerminal as the unit starts up, wait for this debug information to finish.
6. In HyperTerminal, log on to the unit by typing +++ and pressing enter.

Note: *The IP address will be displayed on the spot monitor for a user defined period (nominally 10 minutes) after the machine starts up, providing there is a connected working camera*

7. At the command prompt, type the following commands.

```
<ESC>m\ether_ip\000.000.000.000 <ENTER>
<ESC>m\subnet\000.000.000.000 <ENTER>
<ESC>m\gateway\000.000.000.000<ENTER>
<ESC>m\save <ENTER>
```

reset (to restart the unit) - you must reset the unit for the settings to be applied.

The unit will automatically be allocated an IP address from the DHCP server.

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

```
<ESC>m\ether_ip\000.000.000.000 <ENTER>
<ESC>m\subnet\000.000.000.000 <ENTER>
<ESC>m\gateway\000.000.000.000<ENTER>
<ESC>m\save <ENTER>
reset (to restart the DV-IP ATM)
```

You must reset the DV-IP ATM for the settings to be applied.

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

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

Locating the DHCP Allocated IP Address

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

The unit must be connected to the DHCP network during this procedure.

1. Connect to unit using Hyper Terminal as described in Allocating and IP Address above.
2. At the prompt in HyperTerminal, run the IP configuration tool, type:

ipcfg<ENTER> - the DHCP IP address assigned is displayed.

Note: *The IP address will be displayed on the spot monitor for a user defined period (nominally 10 minutes) after the machine starts up, providing there is a connected working camera. This procedure is available in case there is no camera feed available.*

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

IP address

Subnet mask

Gateway (if required)

The unit now has been installed for simple operation.

Network Configuration

This manual is designed to help with the advanced configuration of the unit using the on-board web pages.

To assist with the configuration of the unit, sections are constructed as tutorials and will illustrate how to perform common requirements. Use the tutorials that will provide the required functionality and follow the step by step instructions.

This manual will be divided into:

Simple Configuration –required to get the unit up and running

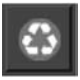
Advanced Configuration –project specific requirements

Software No 04.4(004) M2IP-03.1 (09.2)

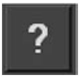
Note: *The unit should be configured in line with the main configuration steps detailed in the Setup Guide and therefore the cameras inputs have been enabled and the standard record rate has been set.*

Web Page Icons

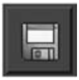
Each of the unit configuration web pages has the following buttons:



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



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



Save Settings –This will save a changes that has been made to the configuration page - remember to save the changes.

NOTE: *Selecting a new page before saving the changes will result in any changes being lost!*

Reset –This is displayed on configuration pages that require a unit reset to initiate a function.

Note: *Always save the settings before resetting the unit.*

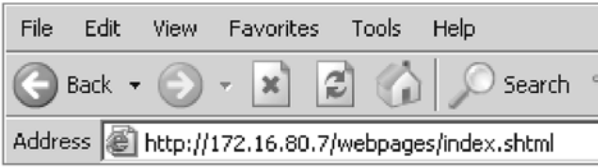
Each ‘How to.. Section’ will show the Tab and Function name to allow easy location of the correct configuration page.

Accessing the Configuration Web Pages

The unit is configured using on the on-board web pages. To access these:

Note: *The unit will display the IP Address on a connected Spot monitor during the boot up sequence. This can then be used to access the on board web pages.*

1. Launch Internet Explorer (or Netscape Navigator).



http://172.16.80.7/webpages/index.shtml

2. Type the IP address of the unit into the address bar.
3. The Main Menu page will be displayed.
4. Select Configuration Options. The unit will prompt for a username and password. The default settings are dm and web respectively.

Note: *The user name and password are case sensitive; they should be changed from the default username and password and kept safe. Mislaid usernames and passwords could result in the unit being returned to Dedicated Micros for reseting.*

Main Menu

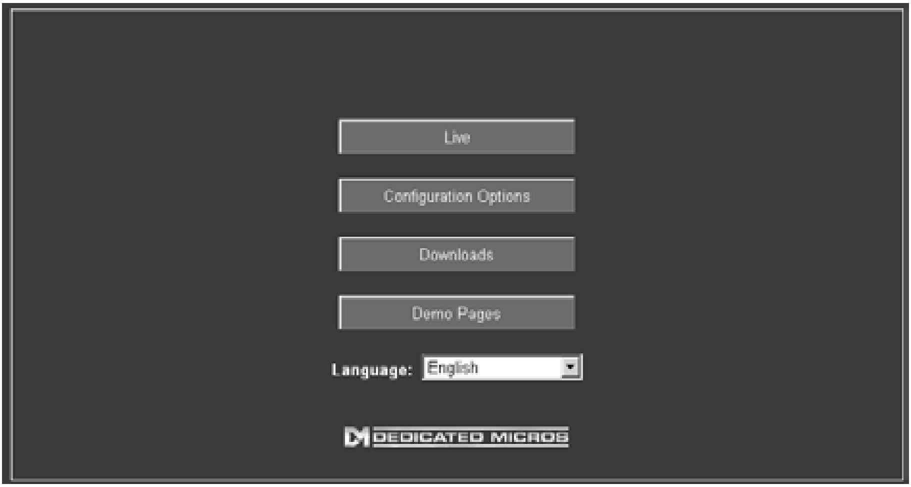
The unit Main Menu allows the Operator access to:

Live viewing of any of the connected cameras.

Configuration web pages for the unit.

Downloads which include the software applications and the product documentation.

Demo pages that demonstrate how viewing applications can be designed for varying system requirements.



Simple Configuration

How to Configure Global Parameters

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

To configure these parameters:

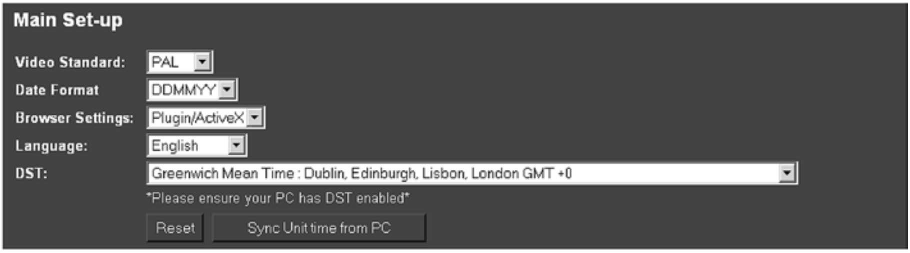
1. Select Home -> Main Set-up.
2. Select the video standard from the drop down list; this will be the standard for all the video inputs on the unit.

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

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

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

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


Main Set-up

Video Standard: PAL
Date Format DDMMYY
Browser Settings: Plugin/ActiveX
Language: English
DST: Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London GMT +0
Please ensure your PC has DST enabled

Function	Description
Video Standard	This displays the setting for all the video inputs on the unit.
Date Format	It is possible to identify the format in which the date will be displayed; the default setting is Day Day, Month Month, Year Year.
Browser Settings	The browser interface on the unit supports ActiveX or Java, select the most appropriate for the application from the drop down list. All users connecting to the system will be presented with the selected interface.

Language
The unit web configuration pages can be displayed in the language that is most suitable to the country of installation. The currently languages supported include; English, Spanish, French, Czech, Italian, Russian, Dutch, Portuguese, German, Turkish, Croatian, Danish, Finnish, Norwegian, Hungarian, Swedish, Polish, Arabic, Chinese

DST (Daylight Saving Time)
This reflects the local time zone for the area where the unit is installed.

Reset
This will reset the unit.

Sync Unit time from PC
The unit can be synchronised with the PC that is being used to configure the unit. If the PC is synchronised with the network clock then this time will be reflected in the unit.The synchronisation is not persistent and will only synchronise the unit and the PC at the time the button is pressed.

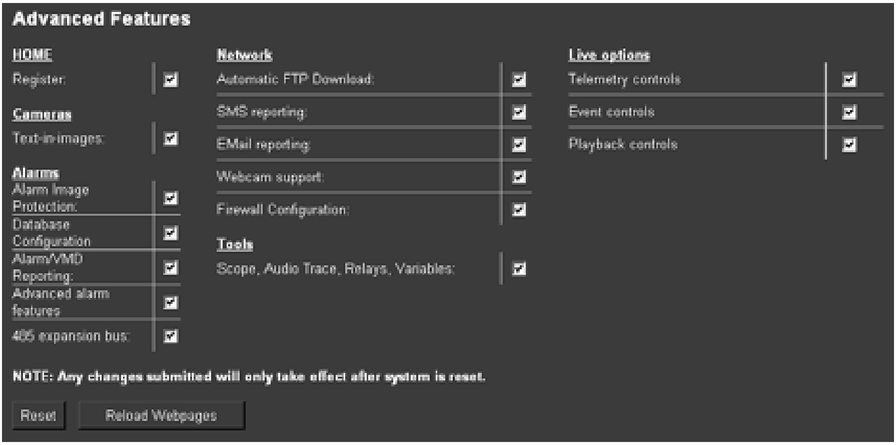
How to Enable System Features

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

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

To enable the features;

1. Select the System -> Advanced Features.
2. By default the Live options are enabled, to enable the other features tick the box next to the feature.
3. Remember to select Save Settings!
4. You will now need to select Reload Webpages for the relevant configuration pages for the enabled features to be displayed.
5. Some of the features require a system reset select the Reset button to reset the unit and re-load the web pages.



Advanced Features

HOME

Register: ☑

Cameras

Text-in-images: ☑

Alarms

Alarm Image Protection: ☑

Database Configuration ☑

Alarm/VMD Reporting: ☑

Advanced alarm features ☑

485 expansion bus: ☑

Network

Automatic FTP Download: ☑

SMS reporting: ☑

EMail reporting: ☑

Webcam support: ☑

Firewall Configuration: ☑

Tools

Scope, Audio Trace, Relays, Variables: ☑

Live options

Telemetry controls ☑

Event controls ☑

Playback controls ☑

NOTE: Any changes submitted will only take effect after system is reset.

Section	**Feature**	**Description**
Home	Register	Note: Configuration and registration of the unit is carried out at the factory, therefore this screen is for fault diagnostics only and it is recommended that the page is not enabled unless advised by Dedicated Micros Technical Support.
Cameras	Text in image	It is possible to integrate the unit into an application where receipt of specific text can be used to trigger an alarm. This will enable the configuration page to be included in the Cameras tab.
Alarms	Alarm image protection	It is possible to configure the unit to protect images within parameters set by the operator (time and date, etc). This will enable the configuration page to be included in the Alarms/VMD tab.
Alarms	Database configuration	The database can be set to have a maximum number of entries to ensure efficient management of the information. This will enable the configuration page to be included in the Alarms/VMD tab.
Alarms	Alarm/VMD reporting	It is possible for the unit to send information to a remote monitoring station under certain conditions (camera fail, alarm, etc). This will enable the configuration page to be included in the Alarms/VMD tab.
Alarms	Advanced Alarm Features	It is possible to enable advanced alarm features on the unit. When enabled the advanced features are added to the Alarm Setup pages with the Alarms/ VMD tab.
Network	Automatic FTP download	The unit can be configured to automatically download information using FTP, This will enable the configuration page to be included in the Network tab.
Network	SMS reporting	The unit can be configured to send data to an SMS server This will enable the configuration page to be included in the Network tab.
Network	E-mail reporting	The unit supports e-mail of data under certain conditions (alarm, start up, etc). This will enable the configuration page to be included in the Network tab.

Network	Webcam support	The unit can make any of the video inputs available to a web server for use within a web page. This function uses FTP to upload the images to the web server. This will enable the configuration page to be included in the Network tab.
Network	Firewall configuration	The unit supports an on board firewall to ensure no unauthorised users can access the unit. This will enable the configuration page to be included in the Network tab.
Tools	Scope, Audio Trace, Relays, Variables	There are a number of tools that can be used to obtain information on the system performance, enabling this options will display the relevant pages in the Tools tab.
Live options	Telemetry controls	This option allows the live pages to be tailored to the Operators requirements, disabling the option will remove all telemetry controls from the Live viewing pages.
Live options	Event controls	The unit supports an event database which can be accessed from the Live page, disabling this option will remove all event controls and will not allow the Operator to analyse the event database.
Live options	Playback controls	It is possible from the Live page to review any recorded images stored on the unit, disabling this option will remove all playback controls from the Live viewing page.

How to Configure Video Inputs and Standard Record Settings

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

This section is divided into:

Enabling and configure the camera inputs settings

Configuring the standard record settings

To enable/configure camera input settings:

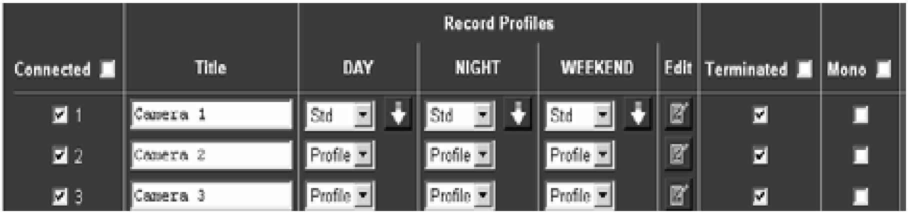
1. Select Cameras -> Camera and Record Set-up
2. It is possible to identify the global camera resolution (common to all video input); the current potion sets the resolution at 704x512.
3. Within the viewing application it is possible to select High, Medium or Low resolution images, enter the maximum file size for the High, Medium and low settings.

Note: *It is possible to select the viewing resolution of the images from the unit, however the unit always records at the high resolution settnigs for optimum quality on recorded images.*

4. All connected cameras will be automatically enabled, use this screen to check the enabled inputs are correct.
5. In the corresponding title box enter the camera name for the video source connected to that input.

6. If the final destination that the video source is to be connected is the unit then this input must be terminated, however if the loop through connections on the unit are to be used then the corresponding input must be un-terminated. To select termination place a tick in the box adjacent to the video input. To un-terminate remove the tick from the box.
7. By default the unit presumes all enabled inputs are colour video sources. If you are connecting a monochrome signal to the unit, it is recommended that the input be set for mono. Place a tick in the corresponding video input.
8. To enable the unit to send notification that the video input does not detect a 1V peak to peak signal place a tick in the box adjacent to the video input. This will give a camera fail alarm.
9. Save the configuration by select Save Settings!

Note: *The Day, Night and Weekend mode are displayed when the Schedule Record Rate is enabled in the Schedule menu (this is enabled by default).*



Connected □	Title	Record Profiles				Terminated □	Mono □
		DAY	NIGHT	WEEKEND	Edit		
☑ 1	Camera 1	Std ▾ ⬇	Std ▾ ⬇	Std ▾ ⬇	✎	☑	□
☑ 2	Camera 2	Profile ▾	Profile ▾	Profile ▾	✎	☑	□
☑ 3	Camera 3	Profile ▾	Profile ▾	Profile ▾	✎	☑	□

When setting the unit for Standard recording the unit will record JPEG images.

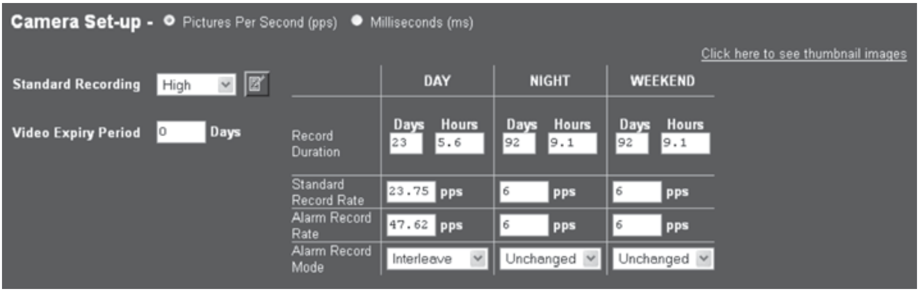
To configure the standard record settings:

10. Select the Edit Profiles button alongside the Standard Recording drop down box.
11. In the Profile Setup page select the JPEG resolution for High, Medium and Low.
12. Set the Image size for High, Medium and Low (these are set in KB).
13. Save Settings.
14. Return to the Camera and Record Setup page. From the drop down list select the Standard Recording resolution which corresponds to the settings configured in steps 9 to 12.
15. Enter the required settings in either the record duration or standard record rate (Global setting).
16. Enter the alarm record rate for when the unit is in an alarm situation (Global setting).
17. Select the alarm recording mode to reflect the recording requirements on receipt of an alarm
18. Enter the video expiry period in days. The unit supports day, night and weekend operation, if this has been enabled within the Cameras>Schedule function then it is possible to identify the alarm record rate for all operation modes. An example of dual mode operation is; a system can be in a ‘set’ or ‘unset’ mode or in an ‘Night’ or ‘Day’ mode. Cameras are individually selected in either or both modes to be available for alarm recording. The Night mode could be identified as out of hours and Day would be the time during normal working hours. This will ensure cameras (such as internal cameras) can be disabled when necessary so false triggers do not occur. Then these cameras would be re-enabled during non-working hours so the whole site is fully monitored.
19. Within the Record Profiles section select Std from the drop down list for cameras that are to be select for Standard Recording, do this for the Day, Night and Weekend modes,
20. Select the Edit button along side the cameras enabled for Standard recording to configure the Pre Alarm Pictures and Pre Alarm Rate settings for each camera.
21. Save the configuration by select Save Settings!

Note: *The record duration and standard record rate are inter-connected; changing one of these settings will automatically update the other. The alarm record rate is not taken into account.*

Note: *Running the unit at maximum Record Rate (50pps or 20ms in Standard Record Settings) will affect viewing and network transmission, as the video codecs will be operating close to capacity - the unit's priority is to record the footage to the internal HDD, so transmission performance will be reduced. This is exhibited by slow connection to the html pages and reduced viewing frame rates. Multi-user viewing will also be affected. It is recommended to not set the Standard Record rate to 20ms for everyday usage, and only use the high rate for specific situations where this it is necessary.*

Function	**Description**
Connected	The unit can automatically detect if a camera source is present, the corresponding input will be enabled in this menu for connected cameras.
Title	It is possible to allocate an ASCII camera title to each of the cameras, which will be displayed onscreen along with the camera number.
Terminated	As the unit supports loop through it is necessary to remove the termination of any inputs that are 'looped', by default all inputs are terminated at 75 Ωs.
Mono	If the video input on the unit has a black and white (monochrome) source connected then enable the corresponding camera. The unit will try and compress the colour contents of the image if this box is not enabled, ticking this box will remove unnecessary overhead on the compression process.
Camera Fail Reporting	If the video input on the unit does not identify a 1V peak-to-peak signal then the unit can transmit an alarm notification email for camera failure on the corresponding video input.
Click here to see thumbnail images	This will display a thumbnail view of video connected to the unit. Place the cursor in the camera title box to view the corresponding video input.



Camera Set-up - ◉ Pictures Per Second (pps) ○ Milliseconds (ms)

Click here to see thumbnail images

Standard Recording: High

Video Expiry Period: 0 Days

	DAY		NIGHT		WEEKEND	
	Days	Hours	Days	Hours	Days	Hours
Record Duration	23	5.6	92	9.1	92	9.1
Standard Record Rate	23.75 pps		6 pps		6 pps	
Alarm Record Rate	47.62 pps		6 pps		6 pps	
Alarm Record Mode	Interleave		Unchanged		Unchanged	

Function	**Description**
Pictures/Second / milliseconds	This allows the record settings to be configured as either Pictures Per Second or Milliseconds
Standard Recording	This is the resolution and image size of the images that will recorded to hard disk for the cameras that are selected for standard recording and are edited in the profile setup page. The options are High, Medium or Low.
Video Expiry Period	This indicates the maximum time any images can be stored on the hard disk, if the record duration is greater than the video expiry period the images will automatically be overwritten
Record Duration	The total record time available in (DD) Days and (HH) Hours. This indicates the storage capacity of the system without any alarm recording. It is estimated from size of video storage, the standard record rate and the requested target size of the recorded images.

Note: Changing the Record Duration will automatically update the Standard Record Rate. Changing the Standard Record Rate will likewise update the Record Rate. This should be configured for day, night and weekend operation modes.

Standard Record Rate: This is global setting and identifies the ‘common pictures per second’ for all enabled video inputs in non alarm mode. This can be set in milliseconds or the number of pictures per second.

The delay between consecutive images from any one camera is the Standard Record Rate multiplied by the number of cameras being recorded. Changing the Standard Record Rate will automatically update the Record Duration. Changing the Record Duration will likewise change the Standard Record Rate.

Example Record Rates:

40ms = 25 pictures per second

50ms = 20pps

100ms =10 pps

125ms = 8pps

200ms = 5 pps

500ms = 2pps

1000ms = 1pps

Alarm Record Rate: This identifies the alarm recording rate, for the mode of operation being configured (i.e. Day, Night and Weekend mode), which will be activated if an alarm is triggered on the unit. For example, the unit may be configured to increase the recording rate when a door contact is triggered.

Alarm Record Mode: This identifies what kind of alarm will trigger the alarm record rate to activate. It is selectable between None, Alarms, Activity, or Alarms and Activity (both).

Record Profiles: These drop down boxes allow the selection of either Standard or Profile recording. Selecting Standard recording will apply the settings selected for standard recording to the corresponding camera.

Edit: This will display the Profile Selector sub menu to allow the Pre alarm data to be set for each camera.

Note: *Reducing the file size will allow more data to be transmitted across the network, it is important to remember reducing the file size will require the compression applied to be increased and this will affect the quality of the image.*

Note: *Profile Recording is covered in the Advanced Configuration section of this manual.*

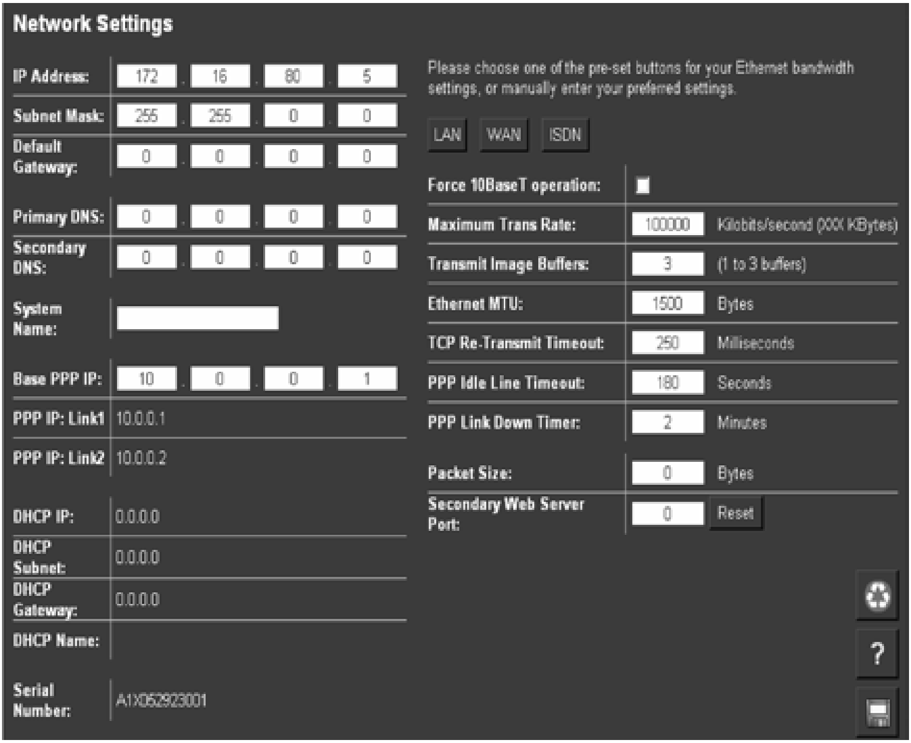
Configuring the Network Settings of the unit

The unit can be allocated an IP address, this web page allows these settings to be checked and changed if required.

To check / configure the network information:

1. Select Network -> Network Settings.
2. If the IP address, subnet mask and default gateway that has already been configured via the serial port or Web interface these will be displayed on this page, these can be changed by entering the new information in the relevant areas.

3. The unit supports Domain Name Server allowing the unit to reference other hosts by their name rather than their IP address, enter the IP address of the primary DNS and secondary DNS server.
4. The default system name for the unit is DVIP ATM, this can be changed to a more appropriate name by entering the information in this section.
5. As the unit can be connected to a LAN or WAN network it is possible to identify the maximum bit rate for the network connection. There are default settings for LAN, WAN and ISDN if these defaults are accept select the corresponding button for your network link, the Max trans rate, transmit image buffers and Ethernet MTU values will be automatically configured, if these default settings are not as require enter the new information in the sections.
6. Enter the TCP Re-transmit Time in milliseconds, this settings should be discussed with the Network Manager.
7. The secondary webserver port is system specific and allows a port to be allocated for webserving if the network is already utilising the default port.
8. Remember to save the configuration by selecting Save Settings!



Network Settings

IP Address: 172 . 16 . 80 . 5
Subnet Mask: 255 . 255 . 0 . 0
Default Gateway: 0 . 0 . 0 . 0
Primary DNS: 0 . 0 . 0 . 0
Secondary DNS: 0 . 0 . 0 . 0
System Name:
Base PPP IP: 10 . 0 . 0 . 1
PPP IP: Link1 10.0.0.1
PPP IP: Link2 10.0.0.2
DHCP IP: 0.0.0.0
DHCP Subnet: 0.0.0.0
DHCP Gateway: 0.0.0.0
DHCP Name:
Serial Number: A1X052923001

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

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

Function	**Description**
IP Address, Subnet Mask, etc	These are the settings that have already been configured. This is the static IP address and subnet mask, and if applicable default gateway.
Primary DNS	This is the primary DNS server IP address for applications that are utilising domain names.
Secondary DNS	This is the IP address of the secondary DNS server in case of failure of the primary server.

System Name

This is the name that is allocated to the unit, this will be used when transmitting alarm information to a Remote Monitoring Station.

Base PPP IP

This is the base IP address allocated to the unit. The PPP Link 1 and PPP Link 2 are automatically generated from the allocated Base IP. PPP Link 1 takes the Base IP and PPP Link 2 will take the next sequential IP address.

DHCP IP

If the unit is to be installed in a DHCP network, this option would display the IP address that was automatically allocated to the unit from the DHCP Server.

DHCP Subnet

If the unit is to be installed in a DHCP network, this option would display the subnet that was automatically allocated to the unit from the DHCP Server.

DHCP Gateway

If the unit is to be installed in a DHCP network, this option would display the gateway that was automatically allocated to the unit from the DHCP Server.

DHCP Name

This would be the name of the unit that is automatically allocated by the DHCP server.

Serial Number

This a read only section and is generated by the unit hardware identifying the serial number of the unit.

LAN, WAN, ISDN

This option ensures the speed of the data from the unit matches the speed of the network the data is being transmitted across. These are default settings and are configured as:

LAN – 10000 Kilobits/second

WAN – 256 Kilobits/second

ISDN – 64 Kilobits/second

Force 10BaseT operation

The unit supports 10 or 100BaseT half duplex transmission, this will force the unit to operate at a 10BaseT connection.

Transmit Image Buffers

This is used in order to improve the picture delivery over Ethernet when using a slow connection, i.e. 256Kbps. Options available are 1, 2 or 3 buffers.

Ethernet MTU

This is the maximum transmit unit for the Ethernet packet. The MTU is the largest physical packet size measured in bytes, that the network can transmit. By default this figure is set to 1500bytes.

TCP Re-Transmit Timeout

This is the time the unit will wait to re-send a packet if an acknowledgement is not received.

When making a connection across a WAN link this figure should be increased and should match the timeout figure for the router.

PPP Idle Line Timeout

This is the time the unit will wait before dropping the PPP link if data has not been transmitted or received.

PPP Link Down Timer

If for any reason the PPP connection is lost then this is the time period before the unit will be forced to drop the PPP connection.

Packet Size

This is the maximum packet size that will be transmitted from the unit. This figure is identified in Bytes.

Secondary Web Server Port

If the default port setting for web serving has already been allocated it is possible to configure a second port number.

eg. If the secondary web port is set for 8000 because the default (80) web port is blocked by the network or firewall. To obtain images from the unit enter the IP address plus the secondary web port in the address section of Internet Explorer or in the Viewer; http://172.16.1.2:8000 (<IP address><:><secondary port number.>

How to Select and Enable Coaxial Telemetry

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

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

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

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

1. Select Cameras -> Camera and Record Set-up to configure the individual cameras.

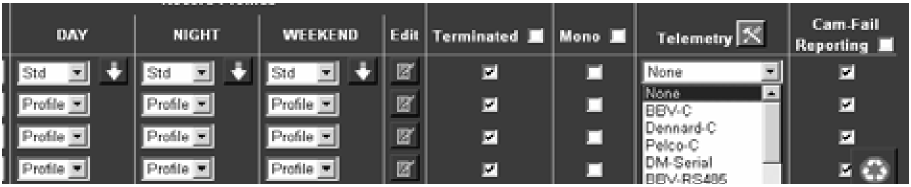
   The coaxial protocols currently supported on the unit are:

   BBV (BBV-C)

   Pelco (Pelco-C)

   Dennard (Dennard-C)

2. Ensure the corresponding camera has been enabled and select the telemetry protocol from the Telemetry list for the corresponding camera.
3. Remember to save the changes you have made by selecting Save Settings!



DAY	NIGHT	WEEKEND	Edit	Terminated □	Mono □	Telemetry	Cam-Fail Reporting □
Std ▾	Std ▾	Std ▾	✎	☑	□	None ▾	☑
Profile ▾	Profile ▾	Profile ▾	✎	☑	□	None BBV-C Dennard-C Pelco-C DM-Serial BBV-RS485	☑
Profile ▾	Profile ▾	Profile ▾	✎	☑	□		☑
Profile ▾	Profile ▾	Profile ▾	✎	☑	□		☑

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

Function	**Description**
Telemetry	The drop down list contains all the supported protocols for coaxial telemetry cameras, select the protocol for the corresponding camera.
Telemetry Setup	Once the protocol has been selected it is possible to access the camera menus. This allows any functions supported by the camera to be configured.

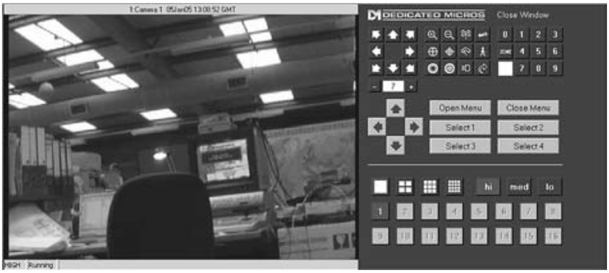
Telemetry Setup Page

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

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

The telemetry control buttons for configuration will be displayed along with camera selection, display options and resolution selection.

This web page allows the Operator to view any of the enabled inputs on the unit, control the telemetry connected to the system and set up any features that are required for their application (such as presets). It is also possible to access the dome/PTZ camera menus for configuration of the supported parameters that are only programmable from the camera menu.



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

How to Enable Serial Telemetry

The unit supports numerous serial telemetry protocols, any of the video inputs on the unit can be configured as a functional camera. Serial 3 (Bus A) and Serial 4 (Bus B) can be used for connecting serial telemetry.

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

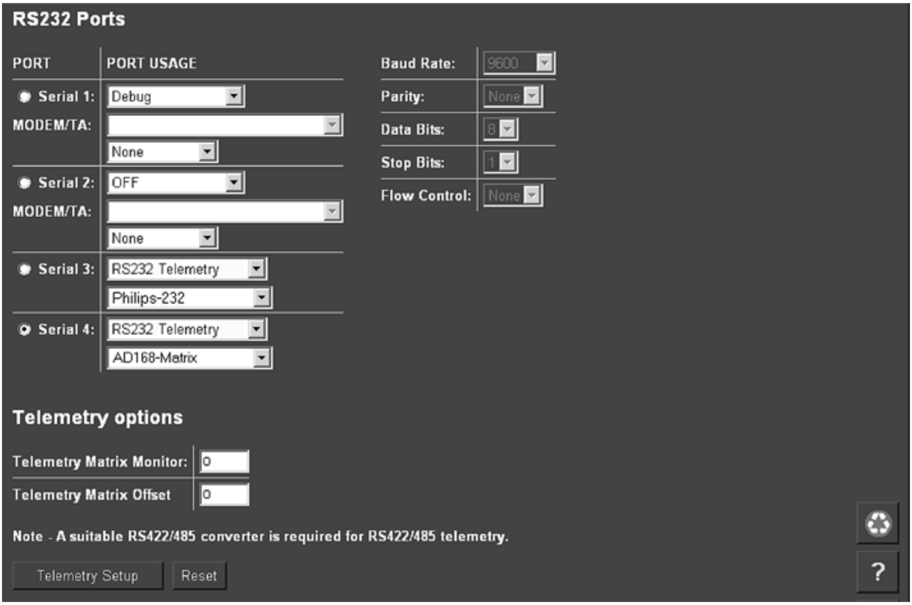
The current RS232 serial protocols supported on the unit are:

BBV-RS485
Philips
DM-Serial
VCL
AD Matrix
AD 168-Matrix

1. Connect the camera and cables to the unit before configuring the unit:
2. Select System -> Serial Ports & Telemetry.
3. Using the drop down list on the associated Communication port (Serial 3 (Bus A) or Serial 4 (Bus B)) select RS232 Telemetry.
4. Select the relevant telemetry type from the list of supported protocols.
5. Enter the dome/PTZ standard settings for:

   - Baud rate
   - Parity
   - Data bits
   - Stop bits
   - Flow control

6. Ensure the address of the dome/PTZ camera is the same as the video input number on the unit, e.g. Video input 3 would equate to the dome/PTZ camera being address 3.
7. Remember to save the changes you have made by selecting Save Settings!
8. Select Cameras -> Camera and Record Setup and select the telemetry protocol from the Telemetry list for the corresponding camera.



RS232 Ports

PORT	PORT USAGE
● Serial 1:	Debug
MODEM/TA:	 None
● Serial 2:	OFF
MODEM/TA:	 None
● Serial 3:	RS232 Telemetry Philips-232
◉ Serial 4:	RS232 Telemetry AD168-Matrix

Baud Rate:	9600
Parity:	None
Data Bits:	8
Stop Bits:	1
Flow Control:	None

Telemetry options

Telemetry Matrix Monitor: 0

Telemetry Matrix Offset 0

Note - A suitable RS422/485 converter is required for RS422/485 telemetry.

Function	Description
Serial 1 & Serial 2	Serial ports 1 & 2 are RS-232 ports and can have the following port usage assigned; Off, Debug, General purpose, PPP and Text in image.
Modem/TA	When the serial port has been configured for PPP it is necessary to select from one of the supported modems to identify the device connected to the unit, refer to table below for supported modems/ TA's.
Serial 3 & 4 (Bus A and Bus B)	Serial ports 3 & 4 are RS-232 ports and can have the following port usage assigned; Off, General purpose, Text in image, RS232 telemetry.
Telemetry type	This is the list of serial telemetry protocols that are supported on the unit.
Baud rate, parity, etc	This allows the communication settings to be configured, note when telemetry is selected these will not be active and will default to predetermined settings.

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

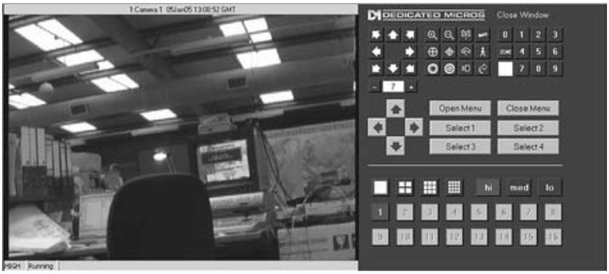
Telemetry Setup Page

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

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

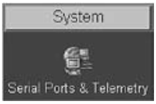
2. The telemetry control buttons for configuration will be displayed along with camera selection, display options and resolution selection.

This web page allows the Operator to view any of the enabled inputs on the unit, control the telemetry connected to the system and set up any features that are required for their application (such as presets). It is also possible to access the dome/PTZ camera menus for configuration of the supported parameters that are only programmable from the camera menu.



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

How to Configure Matrix Control



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

This ensures that any existing equipment does not need to be removed from the installation to allow control over a network, simply integrate the unit into the system a network output.

The unit supports connectivity to the matrix on any of the Serial Ports. The following matrix protocols are currently integrated into the unit's software:

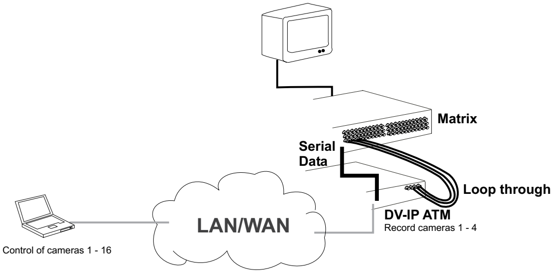
American Dynamics (AD) RS232 Matrix

AD168 RS232 Matrix

BBV TX1000, TX1500 and BBus-Interface Matrices

VCL/Ademco Maxcom Matrix

Connectivity

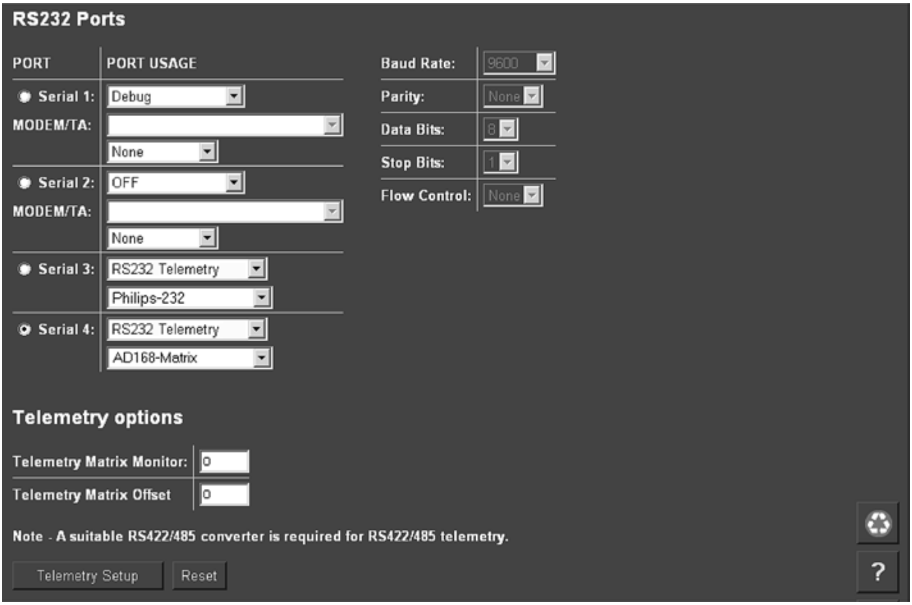


All video inputs from the matrix must be connected to the unit (loop through) as shown below, when installed carry out the following configuration process:

1. Select System -> Serial Ports & Telemetry.
2. Using the drop down list on the associated Communication port (Serial 3 (Bus A) or Serial 4 (Bus B)) select RS232 Telemetry.
3. Select the relevant matrix from the list of supported protocols.

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

   - Baud rate, Parity, Data bits, Stop bits, Flow control.
4. Enter the Matrix Monitor number of the matrix that the unit is connected to and that you will be controlling.
5. Enter the Matrix Offset address.
6. Save the configuration by selecting the Save Settings!
7. Select Cameras -> Camera Inputs and select the matrix protocol from the telemetry list for the corresponding camera.



RS232 Ports

PORT	PORT USAGE
Serial 1:	Debug
MODEM/TA:	 None
Serial 2:	OFF
MODEM/TA:	 None
Serial 3:	RS232 Telemetry Philips-232
Serial 4:	RS232 Telemetry AD168-Matrix

Baud Rate:	9600
Parity:	None
Data Bits:	8
Stop Bits:	1
Flow Control:	None

Telemetry options

Telemetry Matrix Monitor: 0

Telemetry Matrix Offset 0

Note - A suitable RS422/485 converter is required for RS422/485 telemetry.

Function	Description
Serial1 & Serial2	Serial ports 1 & 2 are RS-232 ports and can have the following port usage assigned; off, debug, general purpose, PPP and text in image, RS232 telemetry.
Serial 3 & 4 (Bus A and Bus B)	Serial ports 3 & 4 are RS-232 ports and can have the following port usage assigned; off, debug, general purpose, text in image, RS232 telemetry.
Telemetry type	This is the list of serial telemetry protocols that are supported on the unit.
Telemetry Matrix Monitor	Matrices support many monitor outputs, this is the monitor output that has been allocated for connection to the unit.
Telemetry Matrix Offset	This is the matrix offset to allow any camera input on the matrix to be set as input 1 for the unit. An example of this is in large systems where multiple operators are allocated groups of cameras, for ease of use each camera can be configured to start at camera 1. However they could actually be connected to any input on the matrix but we would select camera 1 which could be controlling input 32 on the matrix.
Baud rate, parity, etc	This allows the communication settings to be configured, note when telemetry is selected these will not be active and will default to predetermined settings.

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

The following parameters have been configured:

Global settings

Video inputs

Cameras parameters

Record rates

Remote connectivity

Advanced Configuration

How to Configure Profile Recording

The unit supports MultiMode recording. This offers the ability to set different recording rates, resolutions and compression formats across scheduled, normal and alarm modes for each individual camera.

By varying the quality, bit rate and file size of the recorded images using the MultiMode function can increase recording capabilities of the unit.

MultiMode offers:

Ability to set different recording resolutions including 720x512, 704x256, 352x256 and 176x128.

Ability to set MPEG or JPEG compression recording.

Ability to set PPS or millisecond recording rate per camera.

Dynamically switchable resolution when switching from Normal to Event recording.

Dynamically switchable compression between MPEG4 and JPEG from Normal to Event recording.

Note: *It is recommended when configuring the record settings to use the Standard Record Schedule option or the MultiMode option but not a combination or the two. Standard Recording will divide the record settings across all inputs selected for recording; MultiMode allows the record settings for each camera to be individually configured.*

Note: *It is recommended that the Profile Wizard be used when configuring Profile recording.*

Notes on MultiMode Recording

Pre-Alarm Recording

If a unit is set up to record MPEG4 for normal recording and JPEG for Events, the pre-alarm image stored in RAM will be saved as JPEG at the same resolution as the Event images. If no changes are made to the standard configuration, the unit will still 'Plug and Play' at 2CIF resolution, JPEG Normal and Event recording at 6pps across all cameras, using Std rate recording.

MPEG recording

MPEG compression records the changes between the two sequential images (known as temporal redundancy) and then calculates the difference between two frames and supplies the information required to complete an image (called motion estimation). MPEG uses I-frames (complete new image frames) at a user defined rate to allow easy verification. These two technologies combine to achieve a greater level of data compression than can be normally achieved with JPEG compression.

The user must appreciate the difference between the quality definitions used within this section.

Each camera must use either Std Recording or Profile recording for each part of the schedule, Day, Night and Weekend. Cameras using the Std recording setting will use the same, common setting which is defined at the top of the first page.

Profile definitions are editable by the user, up to 12 JPEG and 12 MPEG user defined specifications can be saved and used within the Camera Setup.

To configure profile recording:

1. Select the Camera and Record Setup menu.
2. From the drop down list within the Record Profiles section select Profile for the cameras to be included in profile recording.

Note: *If the schedule option has been enabled select Profile for all three operating modes (Day, Night, Weekend).*

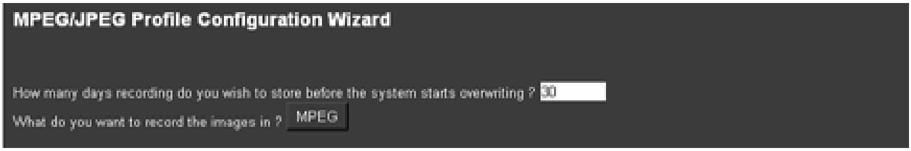
Using the Profile Wizard

It is possible to set the unit recording configuration based on the users priorities. Using the Configuration wizard, the Administrator can set the unit configuration according to the users priorities.

To use the Camera Profile Wizard:

1. Select Cameras -> Profile Wizard.
2. Input the number of days that images should be stored by the system before being overwritten. This will influence the quality and rate of images being stored.
3. Use the selector button to determine if the images are to be stored as MPEG or JPEG.

Note: *Ensure cameras have been selected for profile recording as detailed above.*



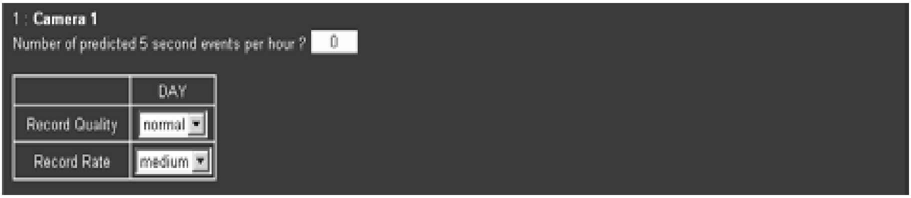
MPEG/JPEG Profile Configuration Wizard

How many days recording do you wish to store before the system starts overwriting ? 30

What do you want to record the images in ? MPEG

4. Input an estimate of the number of events that will be recorded during an hour in standard recording mode.
5. Use the drop down boxes under the individual camera entry to input the quality of image and the recording rate required.

Note: *Any of the settings that are outside the parameters of the unit will be highlighted in red. Change to a lower setting until the highlighted field returns to white.*

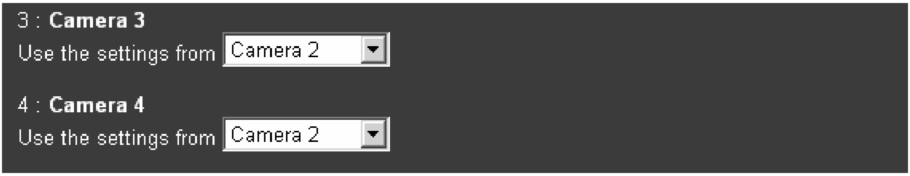


1 : **Camera 1**

Number of predicted 5 second events per hour ? 0

	DAY
Record Quality	normal
Record Rate	medium

6. For ease of installation, settings can be copied from other configured cameras, using the drop down menu. Alternatively, individual settings can be added for each camera by selecting User Defined from the drop down list and using the process described above.



3 : **Camera 3**

Use the settings from Camera 2

4 : **Camera 4**

Use the settings from Camera 2

7. Save options by selecting Save Settings button.

The unit is now ready for Profile Recording.

Editing Camera Profiles

The Camera Profile menu is an alternative to using the Profile Wizard for configuring Profile recording. This allows each camera to be individually configured for normal and alarm recording and pre alarm data.

First it is necessary to configure the MPEG4 and JPEG profiles on the unit.

All camera recording parameters for the unit are defined on this page. The user should have an understanding of what settings are required to suit the application.

To edit the profile settings:

1. Select Cameras -> Camera Profiles. Note that cameras enabled for Standard recording will be read only in this menu.
2. Select the Profile Setup button at the top of this menu. This will display the Profile Setup Menu.

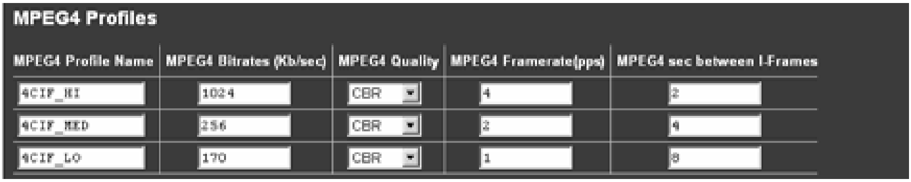
Note: *The Profile Setup menu can also be accessed by pressing the edit button adjacent to the Standard Recording drop down menu in the Camera and Recording Setup menu.*

MPEG4 Profiles

There are twelve MPEG profiles that can have individual settings allocated to each profile. These include bit rate, quality, framerate and I-frame rate.

1. Enter the MPEG profile name. Each profile can be allocated a title to identify the settings use significant titles to make configuration easier.
2. Enter the maximum bitrate for the profile, this is defined in Kb/second.
3. The quality settings should be left at CBR (Constant Bit Rate).
4. Enter the number of pictures per second (frame rate) required for the profile.
5. Identify how often the I-Frame will be included.

Note: *Increasing the I-Frames will improve the video image but will also incease the amount of data being produced.*



MPEG4 Profiles

MPEG4 Profile Name	MPEG4 Bitrates (Kb/sec)	MPEG4 Quality	MPEG4 Framerate(pps)	MPEG4 sec between I-Frames
4CIF_HI	1024	CBR	4	2
4CIF_MED	256	CBR	2	4
4CIF_LO	170	CBR	1	8

Function	**Description**
MPEG4 Profile Name	This is a user defined description that identifies a particular set of parameters.
MPEG4 Bitrates (Kb/sec)	This parameter designates the rate at which data will be transferred or recorded.

MPEG Quality	This parameter defines whether the bandwidth allocation will be a set figure (Constant Bit Rate) or will fluctuate depending on the quality of the image being recorded. Select a suitable level of detail from the drop down list. If a setting other than CBR is used, the bit rate column is not available. Use a constant bit rate to accurately predict hard drive capacity.
MPEG4 Framerate (pps)	This sets the number of frames captured per second under this setting.
MPEG4 sec between I-Frames	MPEG technology uses Index frames (I-Frames) as reference images, and then records the differences between the subsequent images. This cuts down on the amount of data stored. This setting determines the frequency of individual I-Frames.

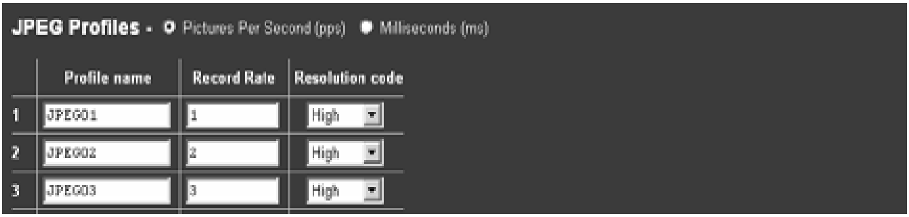
JPEG Profiles

The are twelve JPEG profiles that can be individually configured. The configuration options include record rate (in pps or miliseconds) and resolution.

***Note:** The resolution settings are those configured in the Standard Recording section.*

1. Each profile can be allocated a name, use a suitable name that identifies the settings configured for the profile to make configuration simpler.
2. Select the record rate (this is pps or milliseconds) required for the profile being configured.
3. Select the resolution of the image from High, Medium, Low as configured in the JPEG settings for Standard Recording.
4. Save Settings.

These profiles can now be allocated to cameras that have been enabled for profile recording.



JPEG Profiles - ○ Pictures Per Second (pps) ● Milliseconds (ms)

	Profile name	Record Rate	Resolution code
1	JPEG01	1	High
2	JPEG02	2	High
3	JPEG03	3	High

Function	**Description**
Profile Name	This field can be edited to something significant for the Administrator.
Record Rate	This field either displays the pictures per second recorded under this setting, or the milliseconds between each picture, depending on the selection at the top of the table.
Resolution code	The drop down menu allows selection of a suitable resolution for this profile, from the settings at the top of the page (See JPEG Resolution Alias).

View Profiles

This identifies the viewing profile when viewing MPEG4 video across the network using a NetVu application such as NetVu ObserVer.

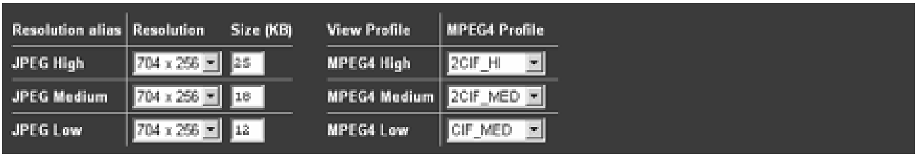
The MPEG options are associated with the Resolution alias for High, Medium and Low options.

1. From the drop down list select one of the twelve MPEG4 options for High, Medium and Low.

The twelve settings correspond to the settings configured in the MPEG4 Profiles section.

2. Save settings.

Return to the Camera Profile menu.



Resolution alias	Resolution	Size (KB)	View Profile	MPEG4 Profile
JPEG High	704 x 256	25	MPEG4 High	2CIF_HI
JPEG Medium	704 x 256	18	MPEG4 Medium	2CIF_MED
JPEG Low	704 x 256	12	MPEG4 Low	CIF_MED

Function **Description**

View Profile
Remote viewing is possible by using a NeVu Connected application such as NetVu ObserVer. Select the MPEG profile that will be associated when the High, Medium or Low options are selected in the viewing application. This determines the size of the network linl established between the PC running the application and the DVR. This option is useful in systems where bandwidth is an issue allowing low bit rate MPEG images to be transmitted across the network while still recording high quality JPEG images.

MPEG4 Profile
Select the MPEG4 profile to be associated with the high, medium and low options. The options in the list correpsond with the settings configured previously.

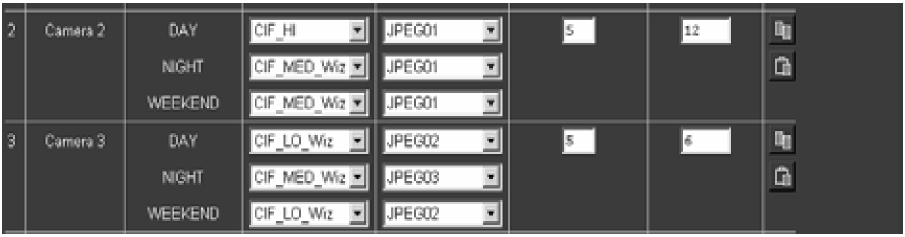
Selecting the Profile for Each Camera

All Cameras that have been enabled for Profile Recording can now be allocated the required Profile.

1. Enter the number of predicited 5 second events per hour for the system.
2. From the drop down list select the Profile for each of the cameras. The options are as configured previously and are twelve JPEG and twelve MPEG4.
3. If schedule is enabled select the profile for Day, Night and Weekend mode.
4. Select the number of pre alarm pictures that will be stored along with the event images.
5. Enter the pre alarm record rate.
6. Save settings.

Note: *Profiles can be copied and pasted to ease configuration. Use the copy button on the required camera settings and paste these to the other cameras.*

Note: *The Record Duration at the top of the menu gives an indication of the number of days and hours storage that can be achieved and includes Standard and Profile record settings.*



2	Camera 2	DAY	CIF_HI	JPEG01	5	12
		NIGHT	CIF_MED_Wiz	JPEG01		
		WEEKEND	CIF_MED_Wiz	JPEG01		
3	Camera 3	DAY	CIF_LO_Wiz	JPEG02	5	6
		NIGHT	CIF_MED_Wiz	JPEG03		
		WEEKEND	CIF_LO_Wiz	JPEG02		

Function Description

Camera Title
This idenitifes the camera title as allocated in the Camera and Record Setup menu.

Schedule Mode
This displays the operating mode. If weekend has been enabled in the Schedule menu the will be three operating modes (Day, Night, Weekend -default). Each of these must have a profile selected.

Normal Profile

This allows the recording profile to be allocated for each camera when the unit is in normal operation (i.e. non-alarm mode). A profile for each operating modes must be selected from the drop down list. The profiles correspond to the JPEG and MPEG profiles configured in the Profile Setup menu.

Alarm Profile

This idenitifes the recording profile for the camera being configured when the unit is in alarm mode (an event has been triggered). A profile for each of the operating modes must be selected from the drop down list. The profiles correspond to the JPEG and MPEG profiles configured in the Profile Setup menu.

Pre Alarm Pictures

This determines the number of images that will be continuously recorded into the pre-alarm memory and available for enhanced pre-alarm recording. Select a record rate in PPS (or ms) to be recorded on the camera being configured.

Pre Alarm Rate

This identifies the period prior to the trigger that images will be stored providing pre-alarm recording to allow an Operator to view the lead up to the incident.

How to Enable Audio Recording

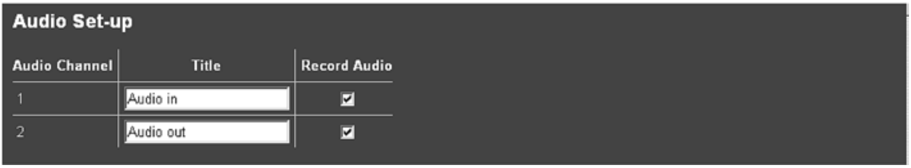
The unit supports two audio inputs which can allow for external audio equipment to be connected to the unit. This allows the Operator to communicate via the Viewer software across the network to the camera location.

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

To configure and enable the audio to be recorded:

1. Select System -> Audio Recording.
2. Enter the title for the Audio Channel 1.
3. Tick the box adjacent to the Channel 1 option to enable audio recording. This is the audio coming in to the server.
4. Enter the title of the Audio Channel 2.
5. Tick the box adjacent to the Channel 2 option to enable audio recording of the output audio, i.e. the audio being transmitted from the Operator application.
6. Make sure you save the information by selecting Save Settings!
7. Reset the unit for the settings to be actioned.

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



Audio Set-up

Audio Channel	Title	Record Audio
1	Audio in	☑
2	Audio out	☑

Function	Description
Audio Channel 1	This is the local audio in on the unit; peripheral audio equipment can be connected to the unit (such as intercom systems, microphones and help points) for complete integration. Allocate a title to the channel which will be saved with the recording.
Audio Channel 2	This is the audio from the network, i.e. from an Operator viewing application, peripheral audio equipment can be connected to the unit (such as speakers), for audio integration. Allocate a title to the channel which will be saved with the recording.
Record Audio	Both the Line in and Line out channels can be enabled for recording this means that any communication across the audio link can be recorded alongside the associated video.

How to Configure the Video Inputs for VMD and Activity

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

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

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

Configuration of VMD will be separated into three sections:

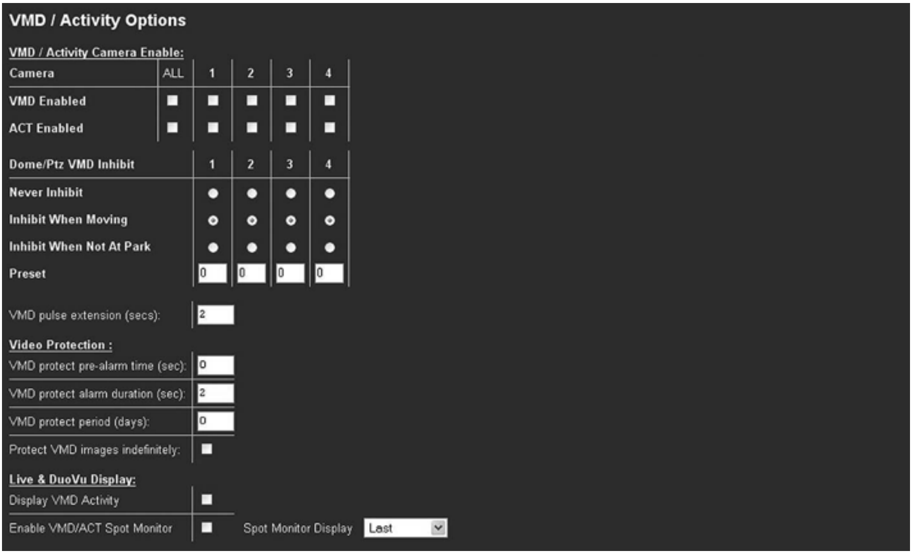
Enabling video inputs and display options

Configuring action on notification of VMD or activity

Setting up the VMD / Activity area

To enable individual video inputs on the unit:

1. Select Alarms/VMD -> VMD.
2. Enable the video inputs that will identify movement by placing a tick next to the corresponding input for either VMD, Activity or both.
3. The pulse extension ensures that the unit does not have double triggers by extending the alarm time. If a second alarm is received after the first alarm is complete but still within this time period the unit will not enter a new event in the database, this setting is set in seconds.
4. Enter the pre-alarm time settings in seconds, this is the time prior to the VMD trigger that is to be saved and protected from being overwritten along with the actual incident.



VMD / Activity Options

VMD / Activity Camera Enable:

Camera	ALL	1	2	3	4
VMD Enabled	□	□	□	□	□
ACT Enabled	□	□	□	□	□

Dome/Ptz VMD Inhibit	1	2	3	4
Never Inhibit	○	○	○	○
Inhibit When Moving	●	●	●	●
Inhibit When Not At Park	○	○	○	○
Preset	0	0	0	0

VMD pulse extension (secs): 2

Video Protection :

VMD protect pre-alarm time (sec): 0

VMD protect alarm duration (sec): 2

VMD protect period (days): 0

Protect VMD images indefinitely: □

Live & DuoVu Display:

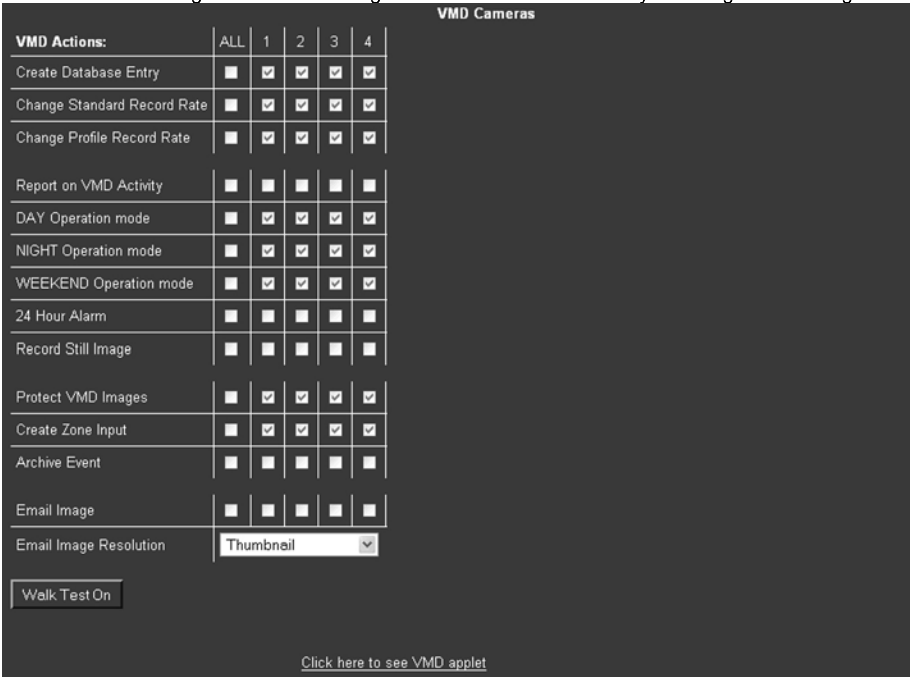
Display VMD Activity □

Enable VMD/ACT Spot Monitor □ Spot Monitor Display Last

Function	Description
VMD/Activity Camera Enable	This option allows for both VMD and Activity display to be enabled on individual or all video inputs on the unit. Tick the VMD, Activity of both boxes that correspond to the input that is to display VMD and/or Activity.
VMD pulse extension	The pulse extension extends the trigger to avoid double triggers of VMD from occurring, i.e. if a second incident of VMD is received on the same input, after the first alarm is finished, but still within the pulse extension period the unit will treat this as a single trigger and not create a new event.
VMD protect pre-alarm time	This is the time period prior to the VMD trigger where the images will be saved along with the VMD recording, these images will be available for archive and will be protected from being overwritten.
VMD protect alarm duration	This is the minimum time period in seconds from the start of the VMD trigger that will be protected from being overwritten. This time will include the VMD recording, the pulse extension and any post alarm recording but will not include the pre-alarm images.
VMD protect period	Any VMD entry in the database can be protected from being overwritten, this is the period of time the files will be saved and protected. After this time the files will be automatically overwritten unless specified.
Protect VMD images indefinitely	It is possible to protect VMD images indefinitely to ensure any incidents are saved and protected for review at a later date. These files will remain protected until specified differently.
Live & DuoVu Display	It is possible to utilise the web interface to monitor live and recorded video, if the Live or DuoVu are to be used it is possible to identify when VMD and/or Activity has been triggered, squares will appear over the area where there is movement.

To configure the alarm action on identification of VMD:

5. In the Alarms/VMD -> VMD web page there are a number of system actions that can be automatically initiated when VMD has been triggered, each camera can be individually configured. Place a tick in the boxes of the VMD action under the corresponding camera input.
6. If an e-mail is to be sent on identification of an alarm it is possible to configure what information will be contained in the e-mail, using the drop down box select the resolution of the image to be sent.
7. Don't forget to save the configuration of the alarm actions by selecting Save Settings!



VMD Cameras

VMD Actions:	ALL	1	2	3	4
Create Database Entry	□	☑	☑	☑	☑
Change Standard Record Rate	□	☑	☑	☑	☑
Change Profile Record Rate	□	☑	☑	☑	☑
Report on VMD Activity	□	□	□	□	□
DAY Operation mode	□	☑	☑	☑	☑
NIGHT Operation mode	□	☑	☑	☑	☑
WEEKEND Operation mode	□	☑	☑	☑	☑
24 Hour Alarm	□	□	□	□	□
Record Still Image	□	□	□	□	□
Protect VMD Images	□	☑	☑	☑	☑
Create Zone Input	□	☑	☑	☑	☑
Archive Event	□	□	□	□	□
Email Image	□	□	□	□	□
Email Image Resolution	Thumbnail				

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

24 Hour Alarm
This will ensure that VMD is permanently enabled on the corresponding input (24/7).

Record Still Image
This will record (and mark the image by stating the word ‘ALARM’ in the title) a still of the corresponding video input alongside the recording of the event, access to the still is via the Live Page.

Protect VMD Images
This will protect the whole recorded 50 Mbyte block of video regardless of which camera(s) are recorded.

Create Zone Input
This turns the VMD camera into an alarm input when used with the Alarm Zones page, Select VMD1 instead of an alarm input to trigger the event.

Archive Event
This will mark the VMD event for automatic download to the FTP Server identified or to the Archive list.

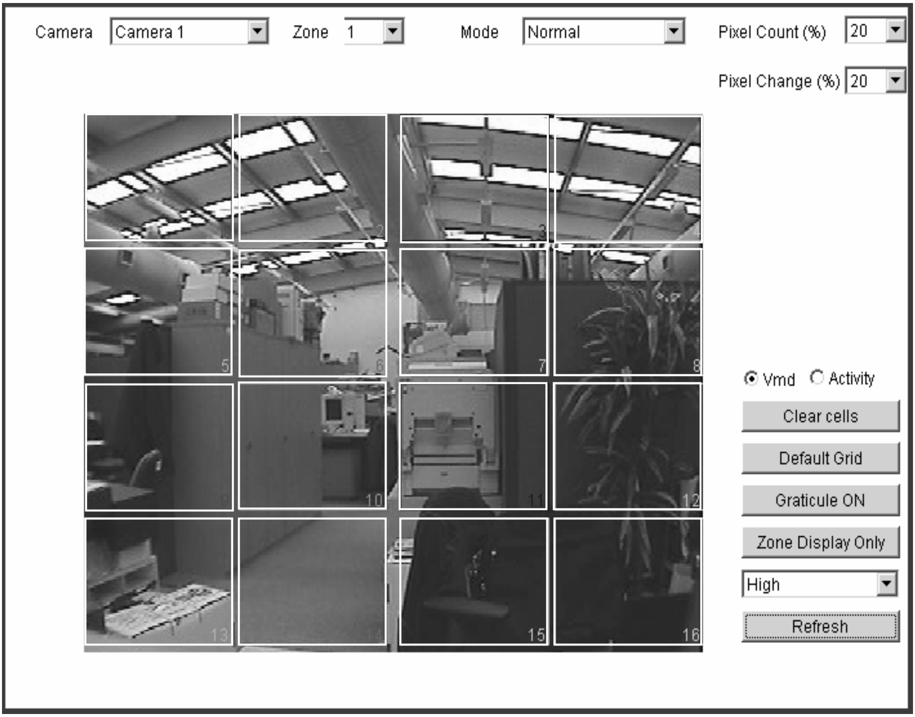
Email Image
This will automatically e-mail a snapshot of the VMD incident to the SMTP server identified. refer to Email configuration page for more information.

Email Image Resolution
This is a system setting, the selected resolution will affect any option where snapshot images are possible, i.e. alarms, VMD, etc.

The setting identifies the resolution of the image that will be attached to the e-mail as a result of an event.

To set up each camera with a VMD grid:

8. In the Alarms/VMD -> VMD web page click on Click here to VMD applet option to display the video image and VMD grid, by default video input 1 will be displayed and the grid is divided into 16 zones.



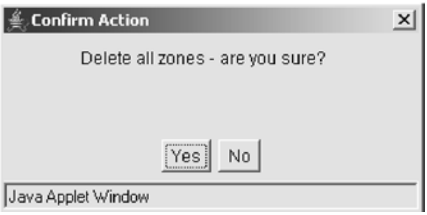
Camera: Camera 1
Zone: 1
Mode: Normal
Pixel Count (%): 20
Pixel Change (%): 20
● Vmd ○ Activity
High

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

10. Select zone you are configuring from the drop down box.

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

11. Alternatively if the default zones are not positioned over the areas you intend assign for detecting motion detection there is an option to clear all cells, you will be presented with a prompt to check you want them cells deleting, select Yes.

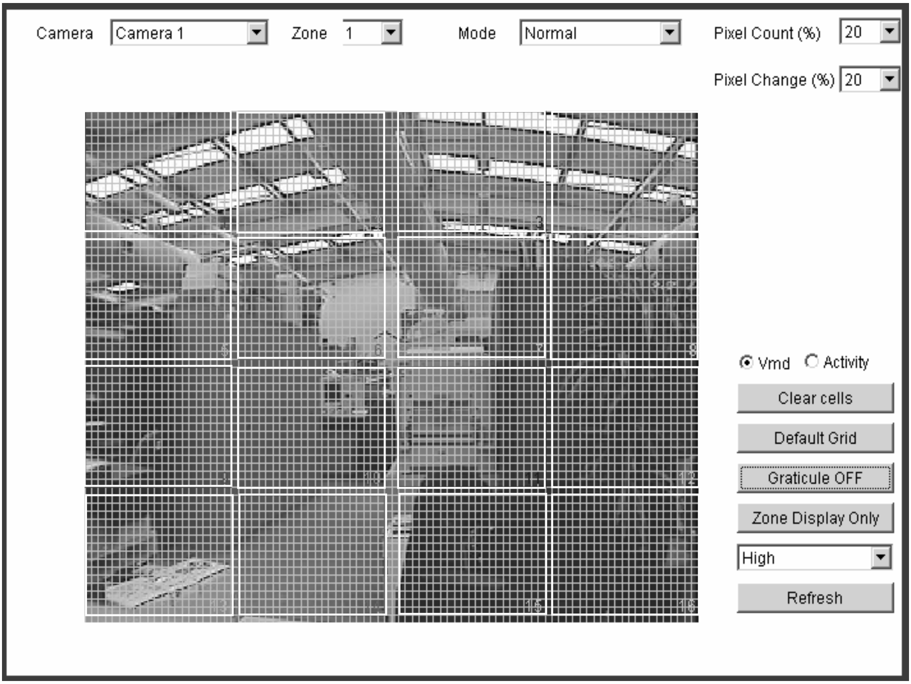


Confirm Action

Delete all zones - are you sure?

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

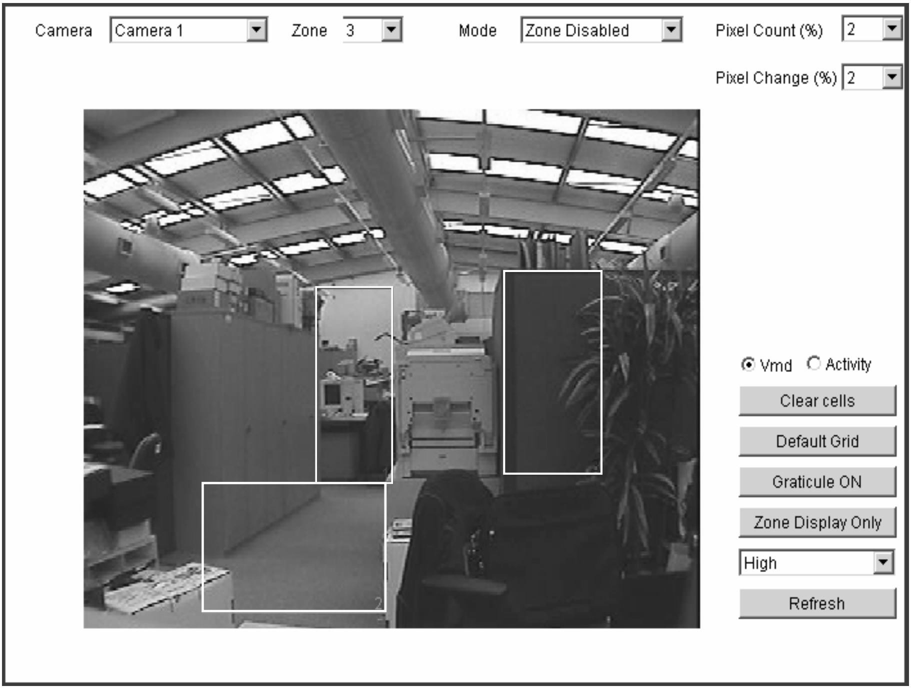
13. It is possible to have a grid overlay displayed on the image to assist in placing the zone areas, select graticule on to display the grid.



Camera: Camera 1
Zone: 1
Mode: Normal
Pixel Count (%): 20
Pixel Change (%): 20

● Vmd ○ Activity

14. Select the next zone from the drop down box to create another zone area and follow Step 16.

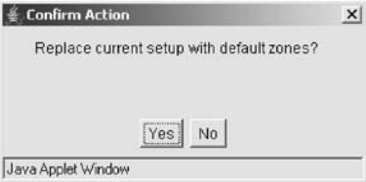


Camera: Camera 1 | Zone: 3 | Mode: Zone Disabled | Pixel Count (%): 2 | Pixel Change (%): 2

● Vmd ○ Activity

High

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



Confirm Action

Replace current setup with default zones?

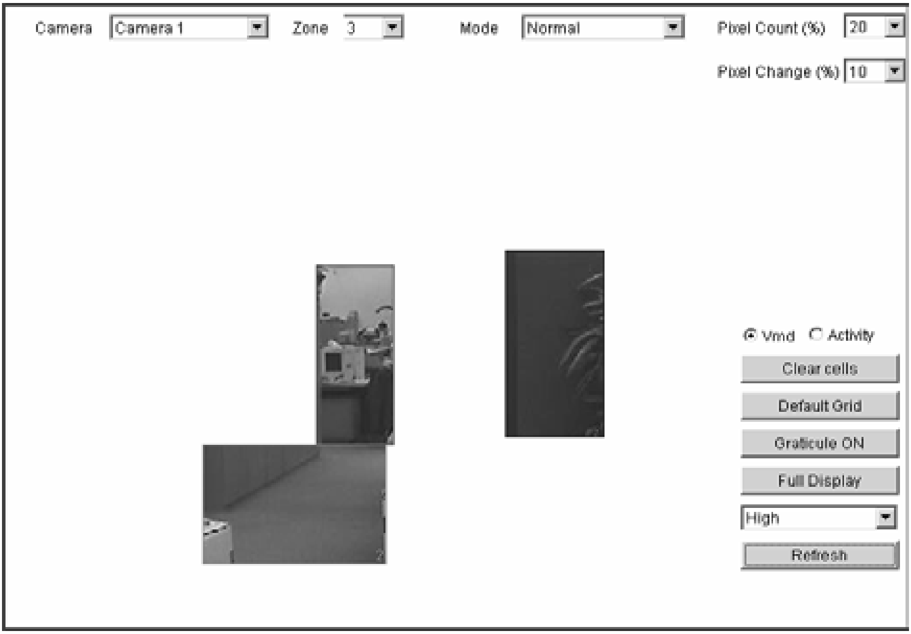
Java Applet Window

15. If you want to use the default zone settings you can select the default grid option, this will place 16 zones over the image. You will be presented with a prompt, select Yes.
16. Select the zone mode from the drop down box that will apply to the zone you have selected see below for description of zone modes.
17. Set the pixel count (%) by selecting from the drop down box the range is between 2 and 100%.
18. Set the pixel change (%) by selecting a value from the drop down box the range is between 2 and 100%,

An example of VMD operation:

Select the ‘zone area’ that will be configured and set the ‘pixel count’ to 20%, this determines the percentage of pixels, in the selected zone, that must change for VMD to be triggered. Set the ‘pixel change’ to 10%, this is the percentage value of the overall change required in the greyscale.

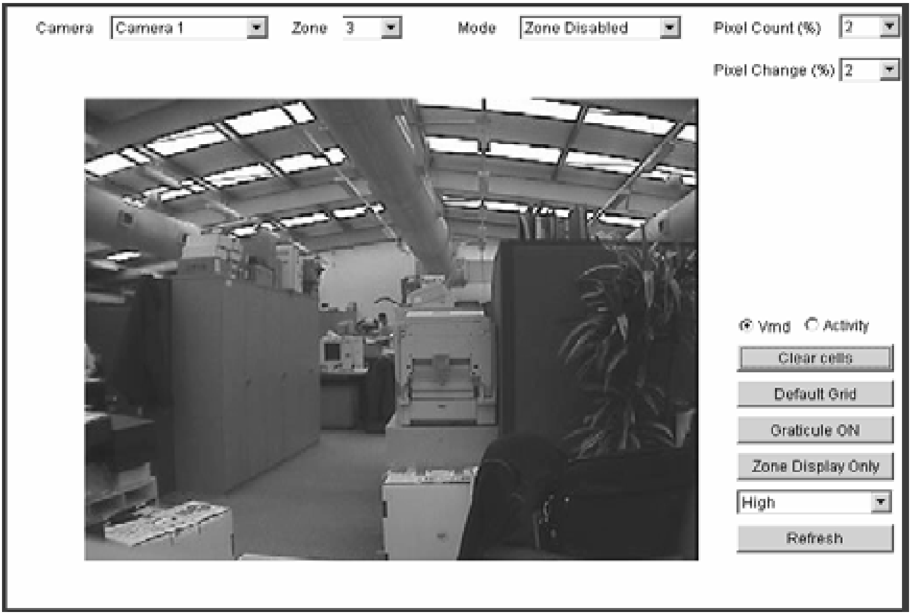
19. To check you have covered the areas that you want to monitor for motion you can select to view the zone areas only, select zone display only and you will be presented with the areas you have highlighted.



Camera: Camera 1
Zone: 3
Mode: Normal
Pixel Count (%): 20
Pixel Change (%): 10
● Vmd ○ Activity
High

20. Selecting full display will show the whole image.

21. Remember to save the configuration by select Save Settings!



Camera: Camera 1

Zone: 3

Mode: Zone Disabled

Pixel Count (%): 2

Pixel Change (%): 2

● Vmd ○ Activity

High

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

Sensitivity

This option is displayed when Activity is selected and allows the sensitivity of the activity grid being configured to be selected. There are five sensitiviy settings to select from: Indoor high, Indoor low, Outdoor high, Outdoor low, Very low.

VMD / Activity

Select whether the grid display will be for VMD (4 x 4 grid) or Activity (16 x 16 grid)

Clear Cells

Removes all defined zones from the image.

Default Grid

Displays the default grid of VMD or activity zones over the whole image.

Graticule On

Displays a grid to assist in identifying and creating zone areas.

Note this is disabled when the Activity option is selected. This is active when VMD is selected.

Zone Display Only

This will display the areas of the image that are covered by a zone only and will assist you in ensuring the necessary areas are covered.

Resolution

This is the resolution of the reference VMD image being displayed.

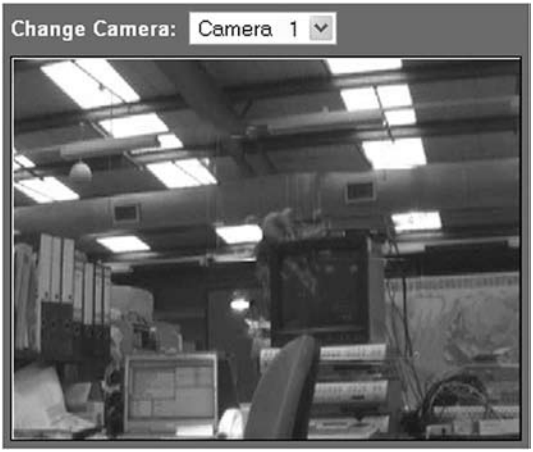
Refresh

This will update the reference image to the latest view during set up.

Note: *Ensure that the display VMD in image option is checked before continuing.*

Note: *VMD 0 refers to Activity Detect.*

Walk Test



Change Camera: Camera 1

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

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

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

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

How to Enable and Configure Alarms

The unit supports 4 alarm inputs which can be individually configured.

This section will be divided into:

Enabling and configuring the alarm inputs

Enabling and configuring the alarm actions

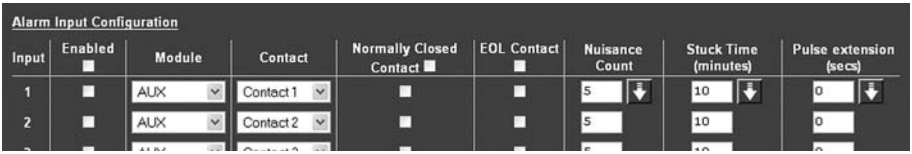
By default the alarm inputs are disabled, these need to be enabled so that external alarm devices can be connected to the unit.

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

Note: *There are 4 alarm inputs on board the unit and the option for an additional 16 alarm inputs (5 to 20) by connecting a DM alarm module to the unit. Ensure the additional alarm module is connected to the unit before powering up the unit.*

3. Select the input that the alarm will be triggered on from the drop down menu, select the contact number.
4. Select whether the input is Normally Open or Normally Closed by default.
5. Enable the alarm input if the End Of Line (EOL) option is to be active on that input.
6. Set the Nuisance Count for the input.
7. Set the Stuck Time in minutes
8. Set the pulse extension for the relevant alarm input (if applicable).
9. Remember to save the configuration by selecting Save Settings!

Once the alarm inputs have been enabled it is necessary to configure what actions will be taken when an alarm is triggered.



Alarm Input Configuration

Input	Enabled □	Module	Contact	Normally Closed Contact □	EOL Contact □	Nuisance Count	Stuck Time (minutes)	Pulse extension (secs)
1	□	AUX	Contact 1	□	□	5	10	0
2	□	AUX	Contact 2	□	□	5	10	0
3	□	AUX	Contact 3	□	□	5	10	0

Function	Description
Input	This identifies which input is being configured. The unit supports 4 on-board alarms and 16 virtual alarms plus the unit can also have an additional alarm modules connected each supporting 16 alarm inputs.
Enabled	Each input must be enabled for it to be functional; if the input is not enabled and an alarm is received the unit will not acknowledge the alarm. By default none of the alarm inputs are enabled.
Module	This identifies whether the alarm is from the onboard alarms or one of the additional alarm modules. The options are Aux, Direct, Module 1 to 16.

Contact
Identify the contact that is associated with the selected module. This option allows you to select from contact 1 to 4 for Aux, Contact 1 for Direct and Contact 1 to 16 for additional modules.

Normally Closed Contact
This applies to both the on-board alarms and the additional alarm module, that can be connected to the unit via the 485-bus. When an input is enabled then by default it will be normally closed, removing the tick in the normally closed box makes the corresponding input normally open going closed for alarm.

EOL Contact
The End Of Line (EOL) option enables the inputs to detect any changes in the input electronic resistance. A change outside the expected values will result in a Tamper Alarm (short circuit or open circuit) being detected as well as the system switching to alarm mode. By default the EOL contacts are disabled for each input.

Nuisance Count
This is a repetitive detector value. When an alarm is received on the unit it will store the alarm time and will monitor the number of times the same detector is triggered within an hour period. If the detector is triggered the number of times that has been set for the nuisance count then the unit will de-activate this detector from triggering an alarm on the system for an hour. The unit will continue to monitor the detector and check how many times it is triggered during this hour, if it is triggered the same number at the nuisance counter it will remain de-activated for another hour, this will continue until the trigger value goes below the nuisance count setting.

Stuck Time
If any of the alarms/detectors are active for a period longer than specified then these will automatically be omitted. This time period is set in minutes

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

Actions can be allocated to each alarm zone; This menu allows a single alarm trigger to carry out any action such as increase record cameras 1-4, send notification via FTP, etc.

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

Note: *There are some pre-defined alarm zones; Zone 30 Disk Low, Zone 31 Disk Full, Zone 32 Panic Alarm.*

This section is separated into:

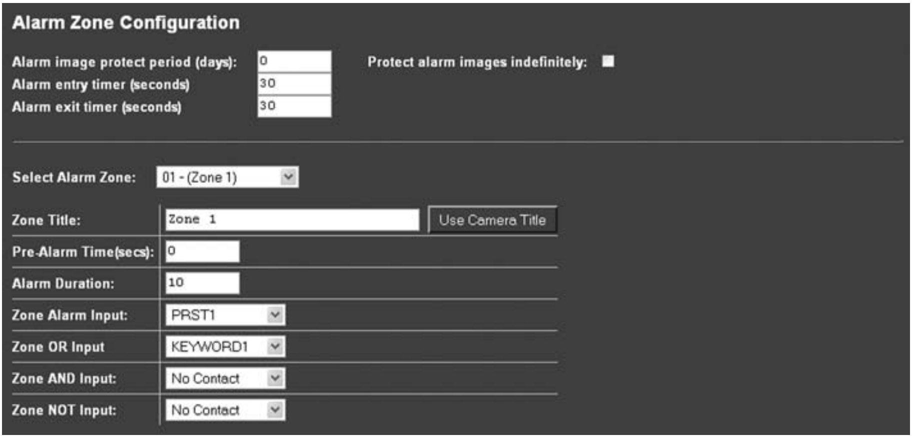
Enabling and configuring the alarm zone

Allocating alarm actions

To enable and configure the alarm zone:

1. Select Alarms/VMD -> Alarm Zone.
2. Alarm recordings can be protected from being overwritten for a set period of time or indefinitely. Enter the time period in days that the alarms are to be protected or place a tick in the box alongside indefinitely.
3. Set the alarm entry timer in seconds, this is part of the advanced alarm feature and are displayed when this feature is enabled.

4. Set the alarm exit timer in seconds, this is part of the advanced alarm feature and are displayed when this feature is enabled.
5. Select the alarm zone to be configured from the drop down option (Zone 1 to Zone 32).
6. Enter an appropriate title to the alarm zone, this will be stored in the database (if enabled), it is also possible to use the camera title for identification.
7. Enter the time period prior to the alarm that you wish to save along with the incident for review with the incident, this time is in seconds.
8. Enter alarm duration in seconds; this is the time period where associated video will be protected from being overwritten.
9. The zone alarm input can be an of the external alarms (direct or 485), any of the configured VMD zones or any of the preset settings, select the appropriate alarm input from the drop down list.
10. The Zone OR input allows you to configure a situation where an alarm received on either of the zone alarm input or the zone OR input will force the unit go into alarm mode and initiate pre-defined alarm actions, select the appropriate option from the drop down list.
11. The zone AND input allows you to configure a situation where an alarm must be received on both the zone alarm input and the zone AND input to force the unit to go into alarm mode, select the appropriate option from the drop down list.
12. The zone NOT input allows you to configure a situation where if an alarm is received on the zone alarm input then an alarm must not be received on the zone NOT input to force the unit into alarm mode which will initiate the alarm actions configured, select the appropriate option from the drop down list.
13. Remember to save the configuration by selecting Save Settings!



Alarm Zone Configuration

Alarm image protect period (days): 0

Protect alarm images indefinitely: □

Alarm entry timer (seconds) 30

Alarm exit timer (seconds) 30

Select Alarm Zone: 01 - (Zone 1)

Zone Title: Zone 1

Pre-Alarm Time(secs): 0

Alarm Duration: 10

Zone Alarm Input: PRST1

Zone OR Input KEYWORD1

Zone AND Input: No Contact

Zone NOT Input: No Contact

Function **Description**

Alarm image protect period
This is the time period in days that the alarm images will be protected from being overwritten, when this time period elapses the images will be automatically overwritten.

Note: *When protecting an image it is important to remember that the unit saves files in 50 Megabyte blocks, the whole block that contains the image will be protected. If the image overlaps into another block the all associated blocks will be protected this can start to reduce the hard disk capacity available for storing images. To unprotect images refer to System -> Protect/Unprotect Images.*

Protect alarm images indefinitely
Protecting the alarm images indefinitely will ensure the alarm images are never overwritten .

Note: *This section must be used in conjunction with System -> Protect/Unprotect Images.*

Alarm entry timer
This is the number of seconds set for the user to disable the alarms. If the alarm is not disabled within this period then the alarm will be triggered

Alarm exit timer
This is the number of seconds from the alarm being set to allow the user to exit the set zones. If the user is still within the set zones after this time period the alarm will be triggered

Select Alarm Zone
An alarm zone logically groups alarms and initiates actions when an alarm is activated, there are 32 zones that can be configured.

Note: *There are a number of zones which have been pre-configured; Zone 27 Archive Slow, Zone 28 Archive Fault, Zone 29 Disk Low, Zone 30 Disk Full, Zone 31 Disk Fault, Zone 32 Panic alarm.*

Zone Title
This information is stored along with the images in the database, ensure this has relevance to the alarm trigger. There is an option to use the camera title.

Pre-Alarm Time
This is the period of time prior to the alarm start that will be included along with the alarm recording for archive and these images will also be protected from being overwritten.

Alarm Duration
This is the minimum time period in seconds from the start of the alarm that will be protected from being overwritten. This time will include the alarm trigger, the pulse extension and any post alarm recording, it will not include the pre-alarm images.

Zone Alarm Input
This determines which input or system function will trigger the zone alarm, the options are; Contacts 1 to 32, VMD 1 to 16, Presets 1 to 16, Disk Low, Keywords, Disk full, Panic, Archiving slow, Archiving fault, Disk fault and no contact.

Zone OR Input
The Zone OR Input identifies an alternative input that can also be used to trigger the zone alarm. This means an alarm trigger can be received on the Zone Alarm Input or the Zone OR Input for the trigger to be activated, the options available are the same as the Zone Alarm Input.

Zone AND Input
The Zone AND Input identifies that an alarm trigger needs to be received on both the Zone Alarm Input and the Zone AND Input for the trigger to be activated and the alarm action to the automatically initiated. The options available are the same as the Zone Alarm Input.

Zone NOT Input
The unit will only issue the alarm actions if the trigger is received on the zone alarm input and not on the Zone NOT input. The allocated alarm triggers available are the same as the Zone Alarm Input.

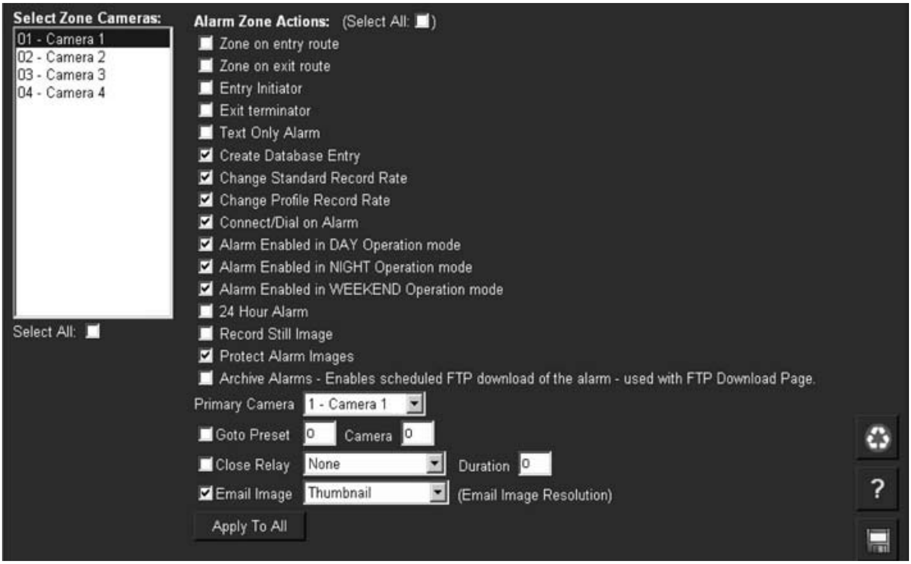
To allocate the cameras and actions that will be carried out when an alarm is received:

13. Select the cameras from the select zone camera list which are to be included in the zone being configured. To select a camera click the mouse over the cameras these will then be highlighted. At least one camera must be highlighted at all times.
14. All of the alarm zone actions can be allocated to each of the zones, to select all actions, place a tick in the select all box.
15. To select individual actions place a tick alongside the relevant action, see the table below for more information on the actions listed.
16. If multiple cameras have been selected a primary camera must be allocated to the zone, select the corresponding camera from the drop down list. The primary camera is the camera that a still image will be taken from for e-mailing on alarm and will be the first camera displayed on the Operator monitor.
17. It is possible to send a camera to a preset position on receipt of an alarm, identify the preset number and the corresponding camera that is to be switched.

18. It is possible to automatically close a relay output when an alarm zone is triggered, the relay can be connected to an external device; door entry system, loudspeaker announcement system which means the system can function automatically without user intervention. Select the relay that is to be actioned on receipt of an alarm.

19. An e-mail can be sent to an e-mail server on alarm, enable this option and identify the resolution of the image that will be attached to the e-mail.

20. Save the information configured by selecting Save Settings!



Select Zone Cameras:
01 - Camera 1
02 - Camera 2
03 - Camera 3
04 - Camera 4
Select All: □

Alarm Zone Actions: (Select All: □)
□ Zone on entry route
□ Zone on exit route
□ Entry Initiator
□ Exit terminator
□ Text Only Alarm
☑ Create Database Entry
☑ Change Standard Record Rate
☑ Change Profile Record Rate
☑ Connect/Dial on Alarm
☑ Alarm Enabled in DAY Operation mode
☑ Alarm Enabled in NIGHT Operation mode
☑ Alarm Enabled in WEEKEND Operation mode
□ 24 Hour Alarm
□ Record Still Image
☑ Protect Alarm Images
□ Archive Alarms - Enables scheduled FTP download of the alarm - used with FTP Download Page.
Primary Camera: 1 - Camera 1
□ Goto Preset 0 Camera 0
□ Close Relay None Duration 0
☑ Email Image Thumbnail (Email Image Resolution)

Function	Description
Select Zone Cameras	This allows you to select one or more cameras that will be associated with the Alarm Zone being configured. Each camera will become part of the 'alarm sequence' when this alarm zone is triggered.
Alarm Zone Actions (select all)	There are numerous actions that can be included in any of the zones being configured, this option will enable all actions.
Zone on entry route	This is part of the Advanced Alarm Features and will create deferred alarms while the entry time is active. The primary alarm input will initiate the 'entry counter' to count down; this has specific alarm areas associated with it. If someone enters the specified alarm areas during the count down process the alarm will not be triggered allowing them to reach the alarm panel to switch the alarm off.
Zone on exit route	This is part of the Advanced Alarm Features and will create deferred alarms while the exit timer is active. This is the similar to the zone on entry option, but works in the reverse, this allows an Operator to switch on a building alarm and will give them a set time period to exit the building and allow them to pass through specified alarm areas without triggering the alarm.
Entry Initiator	This is part of the Advanced Alarm Features and will trigger the entry timer if the system is set. This is a count down timer that will automatically start when the 'primary' alarm trigger (e.g. front door) is actioned and this ensures the alarm system is not activated by other specified alarm triggers for the set time

Exit terminator

This is part of the Advanced Alarm Features and will trigger the exit timer if the system is set. This is a count down timer that will automatically start when the alarm is activated and ensures the alarm system is not activated by other specified alarm triggers for the set time, i.e. allowing the Guard to leave the building.

Text Only Alarm

This is not currently supported.

Create Database Entry

An alarm entry will be added to the database, the zone title will be used as part of the entry information.

Change Standard Record Rate

This will change the record rate of the cameras that have been identified in the Standard Record Rate page (refer to Camera Set-up for information on how to configure standard record rate). The cameras will switch to the alarm record rate specified.

Note: *Changing the zone cameras has no effect on which cameras have their standard record rate changed.*

Change Profile Record Rate

This changes the record rate of the cameras that are selected in the alarm zone to the profile record rate previously specified (refer to How to Configure Profile Recording in this section of the manual). Each of the cameras must have an alarm record rate specified.

Connect/Dial on Alarm

The unit will automatically connect to the remote alarm monitoring station defined.

Note: *You need to enable the dial on alarm system feature for this function to work.*

Alarm Enabled in Day operation mode

Each alarm can be configured to be active when the unit is in a specific operation mode, enable this for the alarm to be active in Day operation mode.

Alarm Enabled in Night operation mode

Each alarm can be configured to be active when the unit is in a specific operation mode, enable this for the alarm to be active in Night operation mode.

Alarm Enabled in Weekend operation mode

Each alarm can be configured to be active when the unit is in a specific operation mode, enable this for the alarm to be active in Weekend operation mode.

24 Hour Alarm

This option would be enabled for alarms that do not want to change at any time and will remain as programmed, i.e. Panic Alarm. When this is selected the day, night and weekend options are not available.

Record still image

This will record a still image of the trigger along with the standard recording. Still images are accessible through the Live page of the web interface. This will also add the word ‘alarm’ to the title header.

Protect alarm Images

Alarm images can be automatically protected from being overwritten.

Archive Alarms

This will force the unit to automatically download alarm images via FTP to an FTP server.

Primary Camera

The primary camera is the camera that the unit will take a still image from for e-mailing on alarm, added to the event database, and this will be the camera that will be the first to be displayed on the Operator monitor.

Goto Preset

It is possible to action a camera to be automatically sent to a preset position when an alarm is triggered, identify the camera and the preset number.

Close Relay

Any of the onboard or external relays can be configured to automatically close on receipt of an alarm, the options are onboard relays 1 or 2 and Module 1 Relays 1 to 16.

Email Image

When e-mail on alarm is enabled it is possible to attach an image to the e-mail, the resolution of the image must be defined. It is important to consider the speed of the link between the unit and the SMTP Server that the e-mail will be sent to. The resolution options available are: thumbnail, high resolution, mediume resolution and low resolution. The resolution setting is a system setting and will have an affect on all options that include e-mail attachments.

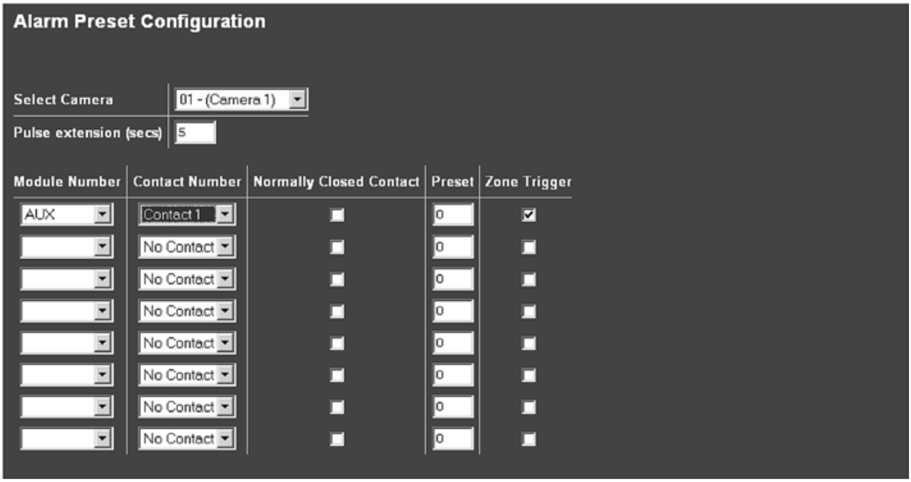
How to Configure Alarm Presets

The unit supports the ability to automatically send a camera to a preset position on the receipt of an alarm.

Within this web page it also possible to identify if the alarm is to be available as a trigger for an alarm zone.

To enable and configure alarm presets:

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



Alarm Preset Configuration

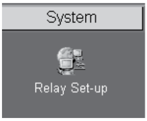
Select Camera: 01 - (Camera 1)

Pulse extension (secs): 5

Module Number	Contact Number	Normally Closed Contact	Preset	Zone Trigger
AUX	Contact 1	□	0	☑
	No Contact	□	0	□
	No Contact	□	0	□
	No Contact	□	0	□
	No Contact	□	0	□
	No Contact	□	0	□
	No Contact	□	0	□
	No Contact	□	0	□

Function	Description
Select Camera	Select the camera that is to be configured.
Pulse extension	The pulse extension extends the trigger to avoid double triggers of alarms from occurring, i.e. if a second incident is received, after the first alarm has finished but within this time period, the unit will not create a new event.
Module Number	This identifies the alarm input that will be the trigger for the camera being configured, the options available are the Direct input, Auxiliary input and Module 1 to 16 for the additional alarm modules that can be connected to the unit.
Contact Number	The Auxiliary input and the additional alarm modules support sixteen input contacts any of these can be allocated as the alarm input trigger.
Normally Closed Contact	The alarm trigger can be configured as normally open (default) or normally closed.
Preset	The preset position is the position the camera will move to when the alarm is triggered.
Zone Trigger	It is possible for a camera specific alarm to also trigger an alarm zone. If the input is to trigger a zone as well as send a camera to a preset position this option must be enabled.

How to Configure the Relay Connections



The unit supports a number of onboard relay connections and can also integrate additional relay modules via the 485 bus connection.

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

This section details how to configure the default actions supported on the unit.

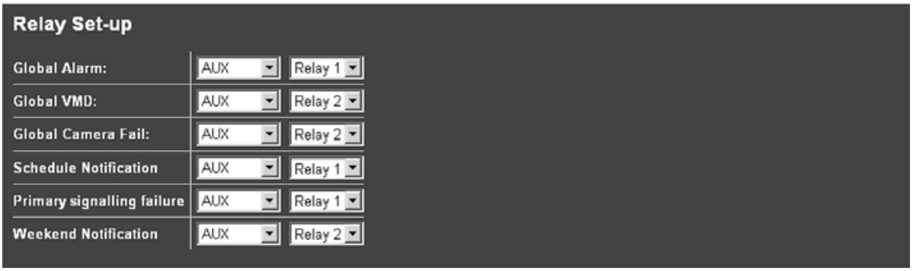
Note: *If the defaults are not set this allows the onboard relays to be available to be automatically triggered on alarm, this is configured within the Alarm/VMD -> Alarm Zone option.*

To configure the relay output settings.

1. Select System -> Relay Setup. There are six default settings that can have any of the onboard or additional relay modules selected as the output for the default function.
2. Global Alarm when a global alarm is received select the relay that will be automatically triggered from the drop down lists, select from the onbaord relays (AUX) or the additional 485-bus modules (Module 1 or Module 2) then select the relay number (1 or 2 for onboard or 1 to 16 for the additional modules).
3. The same process can be carried out for Global VMD, Global Camera Fail, Schedule Notification, Primary Signalling Failure and Weekend Notification.
4. Save the configuration by selecting Save Settings!

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

Note: *The relays that are allocated for the deafult function in this page will not be available for testing in the Relay Test Page (within the Tools menus).*



Relay Set-up

Global Alarm:	AUX	Relay 1
Global VMD:	AUX	Relay 2
Global Camera Fail:	AUX	Relay 2
Schedule Notification	AUX	Relay 1
Primary signalling failure	AUX	Relay 1
Weekend Notification	AUX	Relay 2

Function	**Description**
Global Alarm	It is possible to configure any of the onboard or additional module relays to be the default global alarm relay, this means that the relay will close when an alarm is received on any of the alarm inputs.
Global VMD	It is possible to configure any of the onboard or additional module relays to be the default global VMD relay, this means that the relay will close when VMD is identified on any of the camera inputs.
Global Camera Fail	It is possible to configure any of the onboard or additional module relays to be the default global camera fail relay, this means that the relay will close when there is notification on the system that any of the enabled video inputs has camera failure (no 1V pk-to-ok signal).
Schedule Notification	The schedule notification relay will identify when the unit has switched out of Day mode operation (i.e. when switching to Night or Weekend mode). It is possible to configure any of the onboard or additional module relays as the Schedule Notification relay.
Primary Signalling Failure	The unit can transmit an alarm to a central station via a primary route, if for any reason the alarm is unable to send this message via this route the corresponding relay will close. It is possible to select any of the onboard or additional module relays.
Weekend Notification	The unit will close the corresponding relay when the unit switches to weekend mode operation.

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

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

For these actions to operate correctly there are additional configuration requirements; FTP server address, SMS / GSM settings and SMTP Server address. Without this information the unit would not have a route to transmit images on receipt of an alarm or notification of VMD. This section will be separated into the configuration processes required to enable these functions to operate.

How to Configure Connect/Dial on Alarm

It is possible to force the unit to transmit a message to an allocated Viewer on receipt of an alarm. This connection can be via the Ethernet port of the unit or via a dial up connection on the serial port of the unit.

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

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

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

This section will be separated into:

Enabling PPP for dialling into the unit

Enabling PPP and identifying specific modems for dial up

Configuring Alarm/VMD Reporting via the web and editing the profile.ini file

How to Enable and Configure PPP via Serial Port

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

To enable PPP and allocate a modem:

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

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

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

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

Supported Modems

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

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

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

5. Remember to save the configuration by selecting Save Settings!
6. Reset the unit for the unit to initialise the modem.

How to Configure the Remote Alarm Host Information

When an alarm is triggered the unit will send a message via the serial port or over the network using PPP.

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

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

To configure the 'profiles' file:

1. Using an FTP client application connect to the unit.
2. Locate the \etc directory and expand.
3. Locate the profiles file.
4. Select open/view/edit (depending on the application) to open the file for editing.
5. The profile information will be displayed, enter the information regarding the modem link; Username (& Profile Label), Password, Port, Phone No, IP Address Range, Subnet Mask.

The port options available are:

PPP_Link2 = Serial 2

PPP_Link2 = Serial 1

Ether = Ethernet

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

An example of the profiles file is shown below:

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



<Username>    <Password><Port>     <Phone No>          <IP Address Range>   <Subnet Mask>
dm  password  PPP_Link2 1234567890           10.0.0.1  255.255.255.0
username      password  PPP_Link2  123456789010.0.0.1  255.255.255.0
test          password  PPP_Link2  1234      10.0.0.1  255.255.255.0
```

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

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

6. Save the file and upload back onto the unit. You will now need to add this information to the Alarm/VMD Reporting page via the web interface.
7. Reset the unit.

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

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

1. Select Alarms/VMD -> Alarm/VMD Reporting.
2. Enter the IP address of the primary remote host, this is required for connections via the network and via the serial ports.

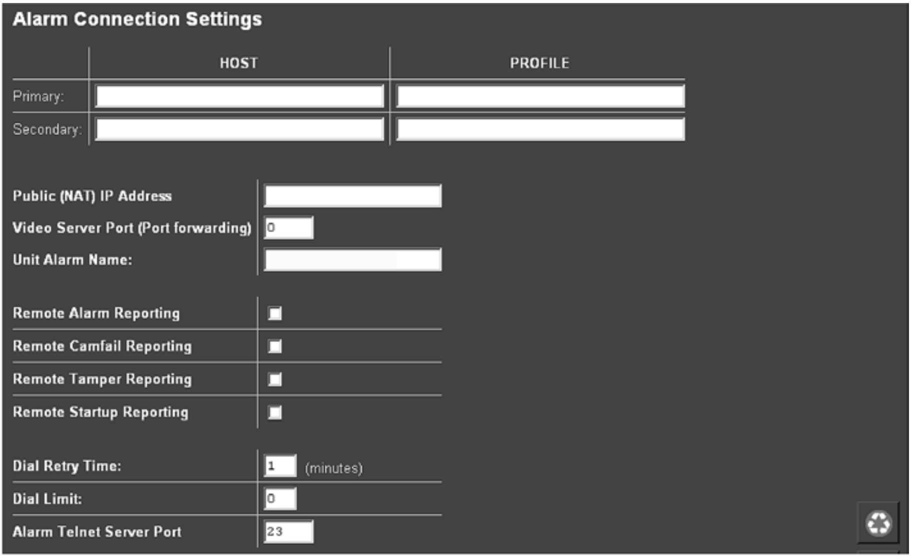
3. When making a connection via the Ethernet network enter Ethernet to identify the medium by which the connection will be made. Alternatively for dial up connections via the modem enter the username previously configured in the 'profiles' file, the example above would result in the profile entry being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

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

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

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

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



Alarm Connection Settings

	HOST	PROFILE
Primary:		
Secondary:		

Public (NAT) IP Address	
Video Server Port (Port forwarding)	0
Unit Alarm Name:	
Remote Alarm Reporting	□
Remote Camfail Reporting	□
Remote Tamper Reporting	□
Remote Startup Reporting	□
Dial Retry Time:	1 (minutes)
Dial Limit:	0
Alarm Telnet Server Port	23

Function	Description
Primary Host	This is the IP address or name of the initial host that the unit will transmit an alarm message to.
Secondary Host	If the unit is unable to contact the primary host then it is possible to identify an alternative route and a secondary host. If there is only one alarm receiving IP address, you must enter the details in both the primary and secondary connection settings.
Profile	This is the medium that the unit will use to make the connection to the primary or secondary host.

Note: *If the connection is via the serial port the profile will be the username configured in the 'profiles' file in the \etc directory on the unit.*

Public (NAT) IP Address	This is public IP (or domain name) for a unit connected to the Internet via a NAT Router or Firewall. This field should be left blank if NAT is not used e.g. on a private network.
Video Server Port (port forwarding)	This field allows the ARC to connect to the unit through a router that is using port forwarding e.g. if the video server does not appear on port 80 (HTTP) to the external network.
Unit Alarm Name	This is the name that will be presented to the remote alarm viewing application and therefore should have some significance to the Operator. This name must match the defined folder name in the Viewer PC folder tree.
Remote Alarm Reporting	This must be enabled for the unit to automatically connect on alarm, it must also be enabled in the Alarm Zone option.
Remote Camfail Reporting	If the unit identifies camera failure on any of the inputs, enabling this option will force the unit to connect to the remote alarm station.

Remote Tamper Reporting
The unit supports End Of Line for the onboard alarm inputs, if these have been enabled it is possible to identify that the alarms have been tampered with, when this occurs enabling this option will force the Unit to send a message to a remote station to identify alarm tamper.

Report Startup Reporting
This will send an alarm report when the unit starts up, this will identify any system resets.

Dial Retry Time
If the initial connection attempt fails then the unit will wait for the specified time period before attempting to re-connect.

Dial Limit
This identifies the number of times the unit will attempt to connect to the remote alarm monitoring station after a failed attempt. A setting of 0 identifies no limit and the unit will continue to try and connect until it is successful.

Alarm Telnet Server Port
This specifies the network port number to use for reporting to the alarm server. This is normally left at the default value.

How to Configure FTP Settings for Archiving Images

The unit can archive images to a central FTP server; this can be on receipt of an alarm or VMD using a scheduled time to backup the video.

When using FTP in a multi-unit application this ensures that all files are stored in one central location for each of the units, offering efficient file management and easier review capabilities.

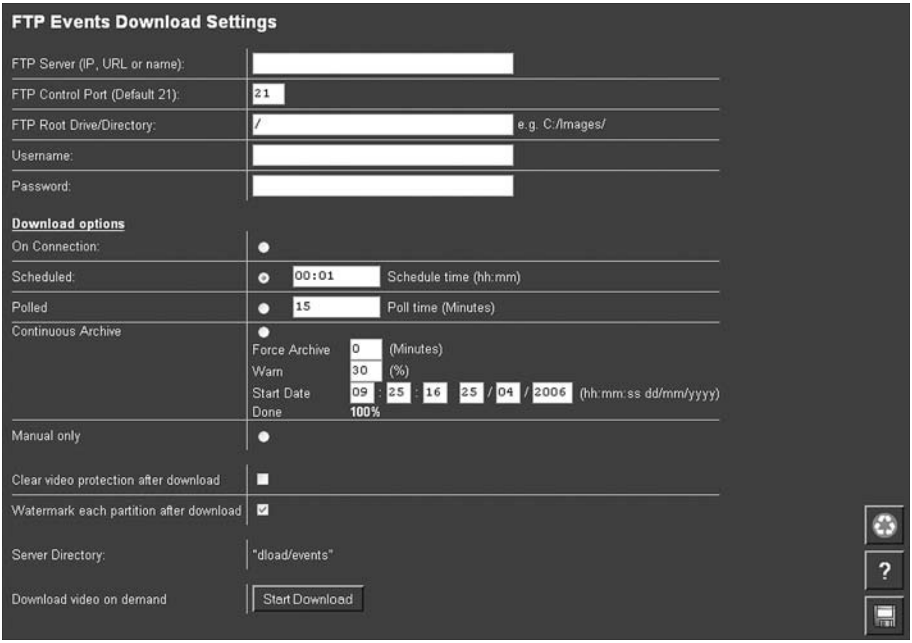
To configure the FTP information:

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

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

7. If the FTP download is to happen automatically at a set time each day, enter the required time in the scheduled time option.
8. It is possible to enable an FTP download and more regular intervals by enabling the polled option, once enabled identify the time period between the end of one FTP download to the start of the next.

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



FTP Events Download Settings

FTP Server (IP, URL or name):	
FTP Control Port (Default 21):	21
FTP Root Drive/Directory:	/ e.g. C:/Images/
Username:	
Password:	

Download options

On Connection:	○
Scheduled:	◉ 00:01 Schedule time (hh:mm)
Polled	○ 15 Poll time (Minutes)
Continuous Archive	○ Force Archive 0 (Minutes) Warn 30 (%) Start Date 09 : 25 : 16 25 / 04 / 2006 (hh:mm:ss dd/mm/yyyy) Done 100%
Manual only	○
Clear video protection after download	□
Watermark each partition after download	☑
Server Directory:	"dload/events"
Download video on demand	Start Download

Function	**Description**
FTP Server	This is the IP address, URL or name of the FTP server the unit will connect to for FTP download of images.
FTP Control Port	The default port for FTP is port 21, if this port has already been allocated on the network it is possible to identify and alternative port number.
FTP Root Drive/Directory	This is the directory where the images are to be stored, it is recommended that a name associated with the unit name be used for ease of retrieval.
Username	To access an FTP Server it is necessary to go through an authentication process, this is the username for you to gain access to the FTP Server.

Password
To access an FTP Server it is necessary to go through an authentication process, this is the password for you to gain access to the FTP Server.

On Connection
This will automatically start the Archive download when the unit detects the archive destination is present.

Scheduled and Schedule time
It is possible to force the unit to archive images at a scheduled time, the time entered will be the time each day that this function will be activated.

Polled and Poll time
This will set the unit to activate archive download at regular intervals, the time period is in minutes and is the time between the end of one archive download to the start of the next.

Continuous Archive
The archive process can be automated to continuously record automatically. The force archive option will allow any recorded images to be archived within a set time. However, if the forced archive time occurs before the recorded files complete a video partition (50MB file) this partition will be closed and archived. The Warn option allows the unit to identify when there is a danger of unarchived, recorded images being overwritten. When a set percentage (example is set to 30%) of recorded but unarchived images remain the unit will issue a warning before the un-archived images will be overwritten. This will allow the Operator to either slow the record rate down or review the speed of the archive process. The Start Date option allows the archive process to be started in the future stating all recordings after this date will be archived, or in the past to ensure previous recorded images plus all new recordings are archived.

Manual only
The archive process will commence when the User initiates the action by pressing the ‘Start Download’ button.

Clear video protection after download
This automatically clears the image protect from the images that are successfully downloaded.

Watermark each partition after download
This enables a watermark to be generated and stored in a text file downloaded with the video to the FTP server for each image partition, this watermark is logged in the log file.

Server Directory
This is the main directory on the FTP server where the images will be stored. The Root Drive/Directory will be created under this main directory. This is read only.

Start Download
This allows the user to manually start the download process.

How to Configure SMS Text messaging

The unit supports the function to send an SMS text message to a mobile phone.

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

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

The typical process for SMS messaging is:

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

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

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

The remote station can then access the unit to acknowledge and action the alarm.

To enable the serial port for the SMS feature:

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

   Baud rate, Parity, Data bits, Stop bits, Flow control.
5. Remember to save the configuration by selecting Save Settings!

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

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

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

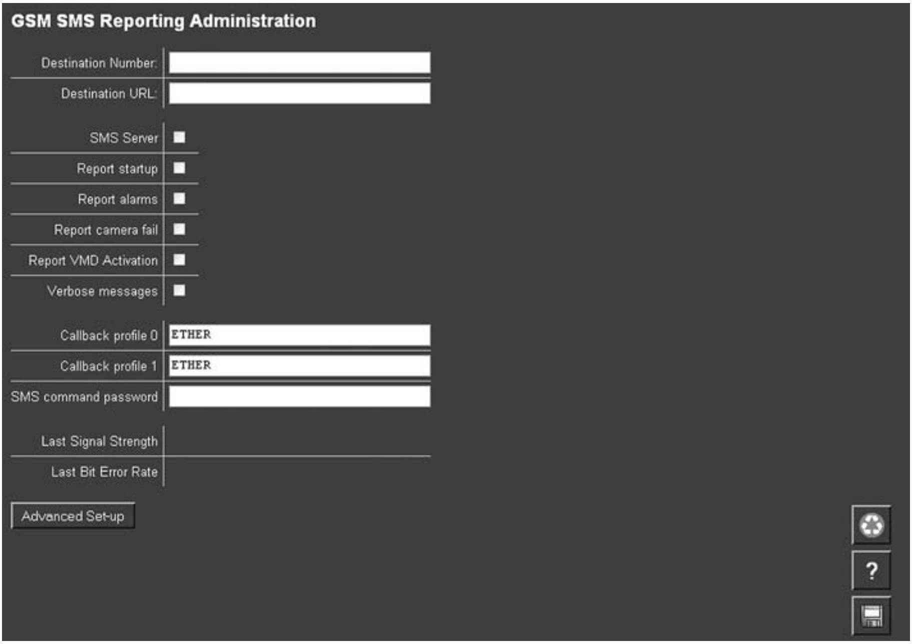
To configure the SMS information to allow a text message to be transmitted on receipt of an alarm:

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

7. Enter the password to enable SMS commands to be initiated. This password will be included in the text message from the Operator.
8. Select the advanced setup button to enter details on the GSM module that will be used in the system.
9. Enter the service centre number, this is the network service centre number of the mobile phone, this information can usually be found on the phone in Messages -> Message Settings -> Profile -> Message Centre Number based on a Nokia phone menu.
10. Enter the pin number for the SIM card (if applicable)

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

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



GSM SMS Reporting Administration

Destination Number:

Destination URL:

SMS Server □

Report startup □

Report alarms □

Report camera fail □

Report VMD Activation □

Verbose messages □

Callback profile 0 ETHER

Callback profile 1 ETHER

SMS command password

Last Signal Strength

Last Bit Error Rate

Function — **Description**

Destination Number — This is the GSM number for the mobile to receive the message. The format should be entered in international format including the country code and local area code.

Destination URL — This can be the URL or the IP address of the SMS Server when utilising SMS over TCP/IP. The messages will be sent over an Ethernet link if present, alternatively it will be sent over the GSM network.

SMS Server — This will enable the unit to accept and log SMS messages.

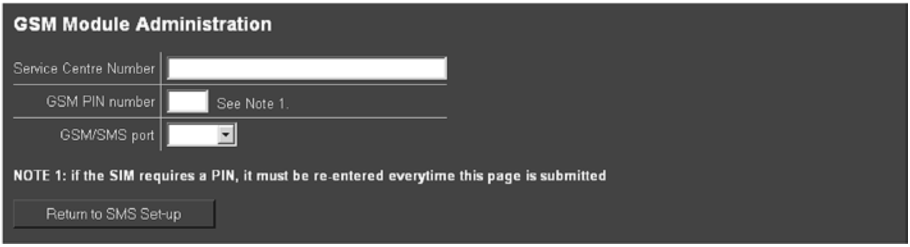
Note: *The Verbose option must not be enabled when this option is selected.*

Report startup — This will enable the unit to transmit a message on power up of the unit.

Report alarms	Sends a text message on receipt of an alarm via the onboard or additional alarm inputs.
Report camera fail	If any of the enabled video inputs on the unit does not detect a 1 volt peak-to-peak signal then the unit will send a SMS message.
Report VMD activation	If VMD is identified on any of the enabled video inputs the unit will send a SMS message.
Verbose messages	This will send a SMS message in a readable format to a mobile devices (e.g. mobile phone).

Note: *This format is not supported in standard SMS Servers.*

Callback profile	This identifies the route the return message, from the Operator mobile device, will take. The return message must contain the SMS command password, callback IP address (IP address of the remote PC with the Viewer application) and the command to action the unit to call the remote station.
SMS command password	This is the password to enable the SMS commands to be initiated and will be included in the return text from the Operator.
Last signal strength	This is a read only section and identifies the signal strength of the GSM module.
Last bit error rate	This is a read only section and will detail the error rate of the GSM module.



GSM Module Administration

Service Centre Number

GSM PIN number See Note 1.

GSM/SMS port

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

Function	**Description**
Service Centre Number	This page is specific to the GSM module connected to the unit, this is the number for the service centre that will be responsible for the SMS message.
GSM PIN Number	This is the pin code for the SIM card in the mobile device that will receive the SMS message. If any changes are made to this page the Pin number must be re-entered each time.
GSM/SMS Port	This is the port address that will be used for the SMS message to be transmitted/received, the options are Serial 1 or Serial 2.

SMS Message Format

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

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

password	This is the SMS password that has been identified in the SMS Set-up page and enables the command to be executed.

destination This is the IP address or DNS name of the Viewing application that has telserver/Viewer (Telnet listener) enabled to receive the message.

profile This can be a number or name that has been configured on the SMS Set-up page, this will be via the serial port or Ethernet connection.

text This is the text message that will be sent to the remote viewer informing the Operator of an incident and therefore should be meaningful.

How to Configure Email Settings

The unit can automatically transmit and e-mail to an SMTP Server under numerous conditions, including on start up of the unit, on receipt of an alarm, or camera failure.

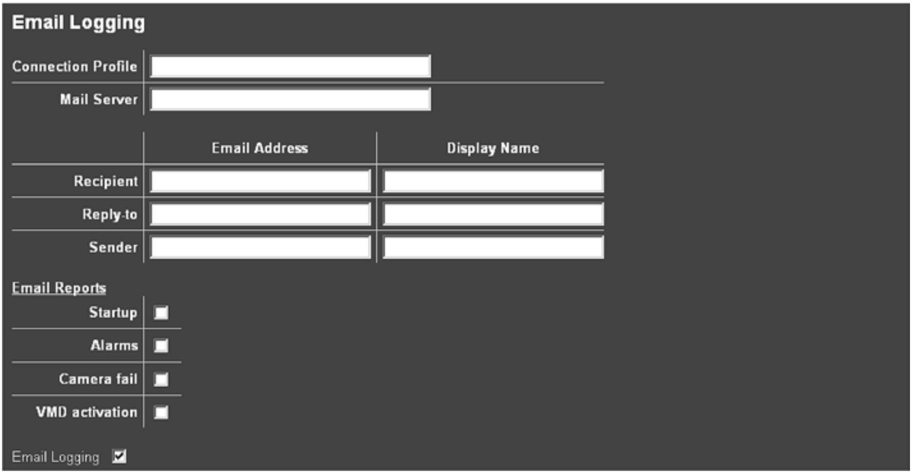
This allows the unit to be installed in unmanned applications where a Remote Monitoring Station (or Manager, etc) would be notified, by e-mail, if any of these conditions occur.

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

1. Select Network -> Email.
2. The feature must be enabled to work. Click the ‘Enable Email’ checkbox to enable or disable the feature.
3. Enter the connection profile; this can be Ethernet if the e-mail is to be transmitted over the LAN or WAN or named profile if using a dial up connection.
4. Enter the IP address or the DNS name of the SMTP Server the e-mail will be sent to.
5. Enter the e-mail address that the SMTP server should forward the e-mail to.
6. If applicable enter the display name for the e-mail address.
7. Enter the e-mail address that the recipient is to reply to. This is only applicable if a reply is required and MUST be filled in for this to happen.
8. If applicable enter the display name of the reply e-mail address.
9. It is possible to identify where the e-mail has be sent from. This is optional and if this is left empty, the video server will use the system name & DNS name to create a sender name.

Note: *The unit can not receive e-mail replies but this must be a valid e-mail address for an SMTP Server.*

10. The unit can be forced to send an e-mail under numerous conditions including start up of the unit, on alarm (this must also be enabled in Alarm Zone page), camera failure and VMD/ACT activation. Place a tick against the actions that are applicable to your systems functional requirements.
11. Place a tick in the e-mail log box to ensure ever e-mail transaction is added to the system logs.
12. Save your configuration by selecting Save Settings!



Email Logging

Connection Profile

Mail Server

	Email Address	Display Name
Recipient		
Reply-to		
Sender		

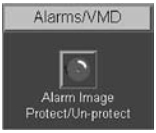
Email Reports

- Startup □
- Alarms □
- Camera fail □
- VMD activation □

Email Logging ☑

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

How to Protect or Un-protect Images



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

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

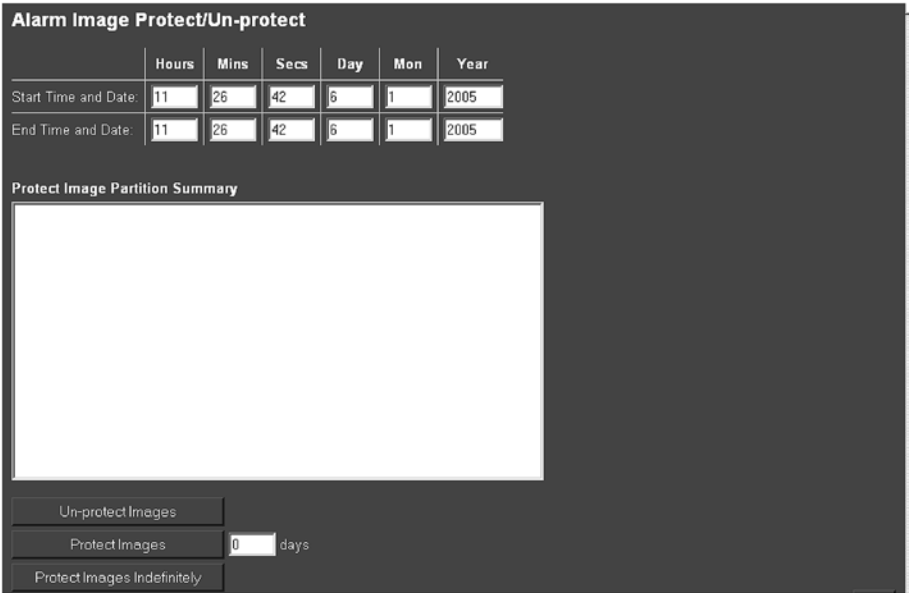
Alternatively it is also possible to highlighted protected recordings and un-protect these so they can be overwritten.

To protect existing recorded images:

1. Select Alarms/VMD – Alarm Image Protect/Unprotect, If there are any existing protected images these will be displayed within the protect image partition summary.
2. Enter the start and end time and date and select Protect Images to display the corresponding recordings.
3. Highlight the recorded file in the protect image partition summary.
4. Enter the time period that images are to be protected in the protect image option or select protect images indefinitely for these never to be overwritten.

To unprotect existing protected images:

1. Select Alarms/VMD -> Alarm Zone.
2. Alarm recordings can be protected from being overwritten for a set period of time or indefinitely. Enter the time period in days that the alarms are to be protected or place a tick in the box alongside indefinitely.
3. Set the alarm entry timer in seconds, this is part of the advanced alarm feature and are displayed when this feature is enabled.
4. Set the alarm exit timer in seconds, this is part of the advanced alarm feature and are displayed when this feature is enabled.
5. Select the alarm zone to be configured from the drop down option (Zone 1 to Zone 32).
6. Enter an appropriate title to the alarm zone, this will be stored in the database (if enabled), it is also possible to use the camera title for identification.
7. Enter the time period prior to the alarm that you wish to save along with the incident for review with the incident, this time is in seconds.
8. Enter alarm duration in seconds; this is the time period where associated video will be protected from being overwritten.
9. The zone alarm input can be an of the external alarms (direct or 485), any of the configured VMD zones or any of the preset settings, select the appropriate alarm input from the drop down list.
10. The Zone OR input allows you to configure a situation where an alarm received on either of the zone alarm input or the zone OR input will force the unit go into alarm mode and initiate pre-defined alarm actions, select the appropriate option from the drop down list.
11. The zone AND input allows you to configure a situation where an alarm must be received on both the zone alarm input and the zone AND input to force the unit to go into alarm mode, select the appropriate option from the drop down list.
12. The zone NOT input allows you to configure a situation where if an alarm is received on the zone alarm input then an alarm must not be received on the zone NOT input to force the unit into alarm mode which will initiate the alarm actions configured, select the appropriate option from the drop down list.
13. Remember to save the configuration by selecting Save Settings!



Alarm Image Protect/Un-protect

	Hours	Mins	Secs	Day	Mon	Year
Start Time and Date:	11	26	42	6	1	2005
End Time and Date:	11	26	42	6	1	2005

Protect Image Partition Summary

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

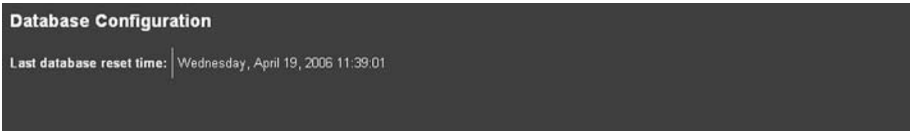
How to Configure the Alarm Database

The unit supports numerous logs which will store information on the actions and processes the unit carries out.

To review the database information:

1. Select Alarms/VMD -> Database Configuration.

2. The last database reset time will be displayed; this is a read only section.



Database Configuration

Last database reset time: Wednesday, April 19, 2006 11:39:01

Function	**Description**
Last database reset time	This is a read only section and is generated by the unit, it identifies the last time that the database was reset.

How to Configure an Alarm Schedule

It's possible to utilise the onboard schedule function of the unit to enable and disable alarm triggers and VMD activation and to determine when specific record rates will be enabled. This can reduce unnecessary alarm triggers, e.g. during office hours it would be unnecessary to have VMD active and ensure the correct record rates are set during night, day and weekend time periods.

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

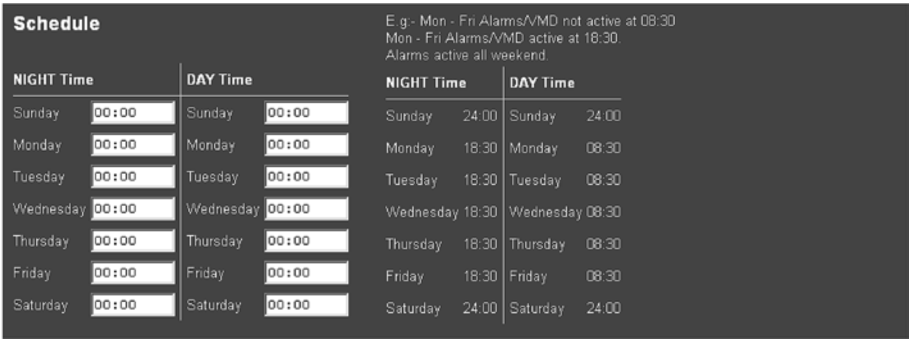
Monday to Friday – Alarms/VMD are not active from 08:30

Monday to Friday – Alarms/VMD become active from 18:30

Weekend – Alarms/VMD are active all weekend

1. Enter 24:00 in the Day box adjacent to Sunday and Saturday.
2. Enter 24:00 in the Night box adjacent to Sunday and Saturday.
3. Enter 18:30 in the Night box adjacent to Monday, Tuesday, Wednesday, Thursday and Friday.
4. Enter 08:30 in the Day box adjacent to Monday, Tuesday, Wednesday, Thursday and Friday.
5. Save the information configured by selecting Save Settings!

Note: *24:00 -24:00 = Schedule 24 hour enabled, 00:00 – 00:00 = Schedule disabled.*



Schedule

NIGHT Time		**DAY Time**	
Sunday	00:00	Sunday	00:00
Monday	00:00	Monday	00:00
Tuesday	00:00	Tuesday	00:00
Wednesday	00:00	Wednesday	00:00
Thursday	00:00	Thursday	00:00
Friday	00:00	Friday	00:00
Saturday	00:00	Saturday	00:00

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

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

Function **Description**

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

DAYTime This identifies the time when the unit will switch to Day operation mode.

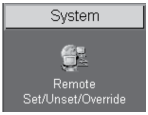
NIGHTTime This identifies the time when the unit will switch to Night operation mode.

6. If Weekend operation is to be active, enable the option and configure the start and end times, weekend settings will be applied to the recorded video during this time period.
7. Select the schedule type from the drop down list.
8. When Zone Control is enabled the Night and Weekend (Zone Control) options are active. Select the Zone from the drop down list which will trigger the unit into Night or Weekend mode.
9. Configure the Operation mode titles, defaults are Day, Night and Weekend.
10. If the keyswitch is to be functional, select the input and contact that will be used to trigger the keyswitch.
11. Select whether the keyswitch is normally open (default) or normally closed.
12. Save the configuration by selecting Save Settings!

Note: *Disabling the record schedule rates would result in the day, night and weekend record settings being replaced by a single 'Rate' record setting.*

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

How to force the unit into another operating mode (Day/Night/Weekend)



It is possible from the unit web pages to manually force the unit to switch from the current operating mode to any of the other enabled modes.

For this feature to operate correctly the following checks must be made.

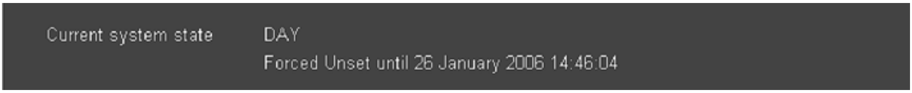
Schedule Settings - Ensure the schedule recording settings have been configured for the relevant operational modes (Day, Night, Weekend). Forcing the unit into a mode that has not been pre-configured with record settings could result in the unit not recording as required.

Advanced Alarms - Within the Advanced Alarm menu there is an option to enable the Force Day, Night and Weekend options, these must be enabled to make the buttons active of the web pages. Make sure only the buttons that have the relevant recording settings configured are enabled.

To force the unit into one of the operation mode:

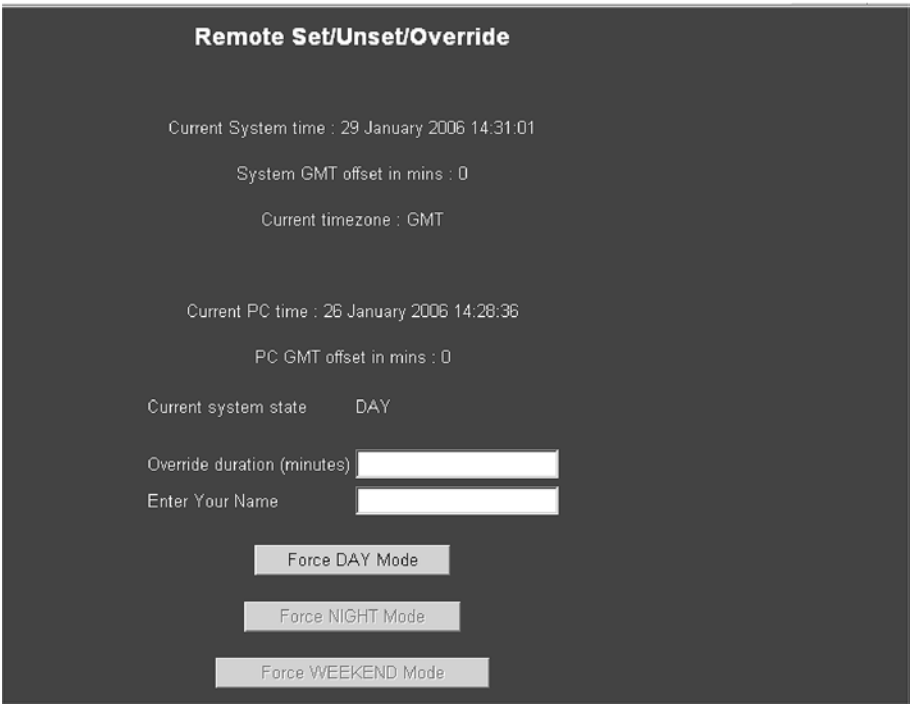
1. Select System -> Remote Set/Unset/Overide menu.
2. Enter the override duration in minutes.
3. Enter the Operator name.
4. Select the Force Day, Night or Weekend mode button.

When the system has been forced into one of the other operating modes the screen will change to show the Mode and the time the unit will remain in this mode for.



Current system state DAY
Forced Unset until 26 January 2006 14:46:04

When the override time entered elapses the unit will go back to the normal operating mode and the screen will reflect this.



Remote Set/Unset/Override

Current System time : 29 January 2006 14:31:01

System GMT offset in mins : 0

Current timezone : GMT

Current PC time : 26 January 2006 14:28:36

PC GMT offset in mins : 0

Current system state DAY

Override duration (minutes)

Enter Your Name

Function	Description
Current Systsem information	This information details the date, time, GMT offset and current time zone.
Current PC information	This details the information on the PC that is being used to force the unit into one of the operation modes, this includes date, time and PC GMT offset.
Current system state	This identifes the current mode the unit is operating in (if the default titles remain this will be Day, Night or Weekend mode).
Force mode buttons	There are three mode buttons the example shows these as being labelled for DAY, NIGHT and WEEKEND mode. These buttons will only be active if the corresponding option has been enabled.

How to Configure Text in Image Functionality

Text-In-Images

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

The unit can be configured to search for specific text information, allowing for fast retrieval and review of images. This section is divided into:

Enable text in image on the serial port.

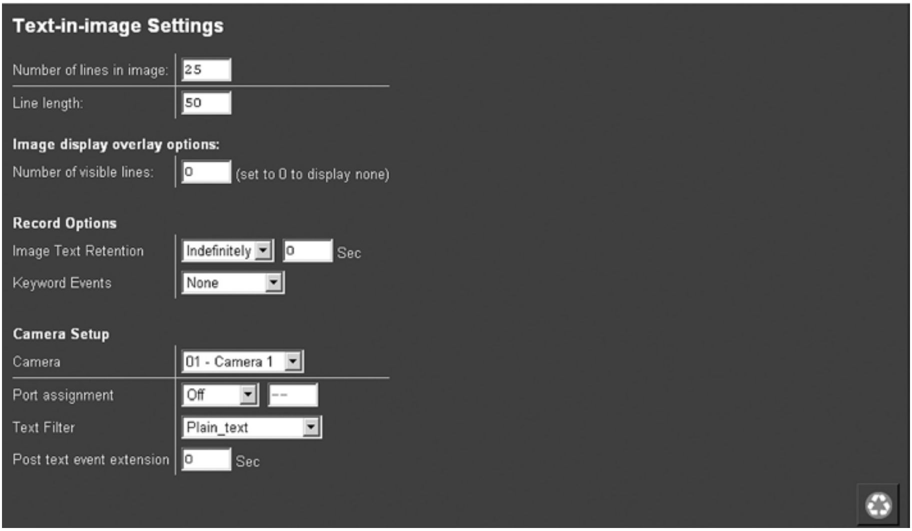
Configuring the paths.ini file to specify the communication port and text information.

Enabling and configuring the function using the web pages.

To enable the serial port for text in image.

1. Select System -> Serial Ports & Telemetry.
2. Using the drop down list associated with the serial port that will be connected to the peripheral equipment select TEXT in Image.
3. The serial parameters will switch to defaults for text in image, however these (Baud rate, Parity, Data bits, Stop bits, Flow control) can be changed as required.
4. Save configuration by selecting Save Settings!
5. Reset the unit for the settings to be applied.

Default Settings



Text-in-image Settings

Number of lines in image:	25
Line length:	50

Image display overlay options:

Number of visible lines:	0 (set to 0 to display none)

Record Options

Image Text Retention	Indefinitely ▾ 0 Sec
Keyword Events	None ▾

Camera Setup

Camera	01 - Camera 1 ▾
Port assignment	Off ▾ --
Text Filter	Plain_text ▾
Post text event extension	0 Sec

Camera 1 – COM1 (Serial 1)
Camera 2 – COM2 (Serial 2)

Camera 3 – COM3 (Serial 3 (Bus A))
Camera 4 – COM4 (Serial 4 (Bus B))

To configure the communication port.

1. Using an FTP client application connect to the unit.
2. Locate the \etc directory and expand.
3. Locate the paths.ini file.
4. Highlight and press the right mouse button, select edit/open.
5. Enter the text information in the .ini file, the example details how the file is configured and shows an typical configuration for COM1:

```
# COM1 = tty
# COM2 = term
# COM3 = aux1 or if input_path set to pic0 GPS stored on Port 3
# COM4 = aux2
# TEXT00 = camera 1
# TEXT01 = camera 2
# TEXT02 = camera 3
# input_path  - the ports COM1 to COM4 that will receive text
# output_path - the command that will associate text to a camera
# buffer_size - the total number of character stored per line
# prefix      - this strips off leading characters received from EPOS
# ============================================
# COM1 will store text with Camera-1
# ============================================
[PATH0]
input_path=\tty
output_path=\pipe\TEXT00
buffer_size=80
# prefix=J
```

This shows that the ‘text in image’ function is enabled and configured for COM1 which means text will be associated with Camera 1 using 80 characters per line with no text filtering.

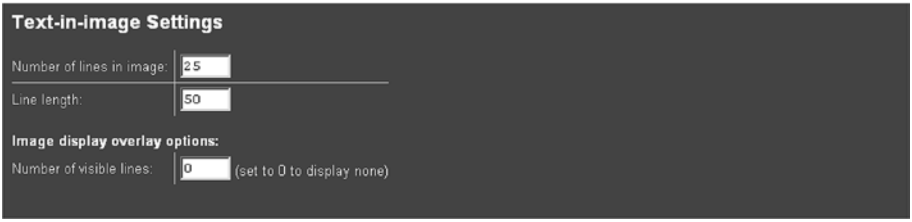
6. Save the configuration and upload to the unit.
7. Reset the unit for the settings to be applied.

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

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

Note: *Reference to COM1 - 4 is Serial 1, Serial 2, Serial 2(Bus A) and Serial 4 (Bus B) respectively.*

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



Text-in-image Settings

Number of lines in image: 25

Line length: 50

Image display overlay options:

Number of visible lines: 0 (set to 0 to display none)

Function	**Description**
Number of lines in Image	This is the number of lines that will be displayed in live and replay (via the web pages) along with the relevant images. The default setting is 10 lines.
Line length	This identifies the length of the lines that will be stored with the image. The default setting is 80 characters which is generally the full screen.
Number of visible lines	To enable the text information to be viewed in the Live page it is necessary to identify the number of visible lines.Record Options Image Text Retention - This identifies the time period the text will remain displayed on the screen and stored within the image data. The timeout refers to period between consecutive lines of data, if text is continuously received then the text will remain on the screen and with the image data. If no data is received within the set time then the text will be cleared for the selected camera, for example in between transactions. Alternatively all text can be displayed and stored within the image data for an idenfinite period. Keyword Events - The unit can be configured to react to defined keywords appearing in text data, and treat them as alarm zone inputs, which in turn generates events in the event database. The keyword event options allows you to record keyword events in the event database as well as (or instead of) alarm zone events. The advantage of this feature is that it will allow the user to see exactly which keyword triggered an alarm in the event database.

Note: *This will increasing the number of events stored. Typically the system would be configured to react to keyword events within the zone page, however this option has been included to provide the option to switch keyword specific events on for systems that require this functionality.*

Camera Setup Camera - Select the camera input that you would like to configure from the drop down list.

Port assignment - All four serial ports on the unit support the option for Text In Image, it is also possible to use the Network port on the unit. For serial transmission ensure one of the serial ports is configured appropriately (System -> Serial Ports and Telemetry), then select the port from the drop down list.

Text filter - Select the text filter option from the drop down list the options are: Plain text (default), RAW, EPSON, Laserjet, DM POS Receipt, DM POS Journal, TVC-1066

Post text event extension - When the system has been configured for event trigger on receipt of text or a keyword it is possible to define an extended time frame. This means that the event and any additional activity after the trigger will be captured and stored.

Note: *Any other text events that are received in this time on this camera will be treated as a single event.*

How to Configure the Onboard Firewall

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

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

Note: *The Firewall function is always enabled on the unit.*

To configure the firewall functionality:

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

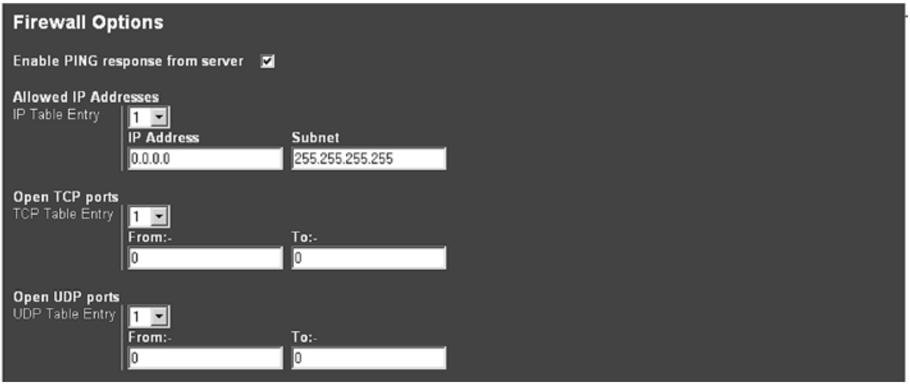
   If there is a range of address then enter the first IP address in the sequence followed by /nn where nn is the last IP address in the range. Refer to IP Address and Subnet Calculation below.
5. Enter the subnet of the network, if a subnet has been specified in the IP address then that will take precedence over this subnet.
6. Identify the TCP ports that are enabled and available on the unit, enter the same number in the To and From values if a single port is required.

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

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

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

8. Save the configuration by selecting Save Settings!



Firewall Options

Enable PING response from server ☑

Allowed IP Addresses

IP Table Entry: 1

IP Address: 0.0.0.0

Subnet: 255.255.255.255

Open TCP ports

TCP Table Entry: 1

From:- 0

To:- 0

Open UDP ports

UDP Table Entry: 1

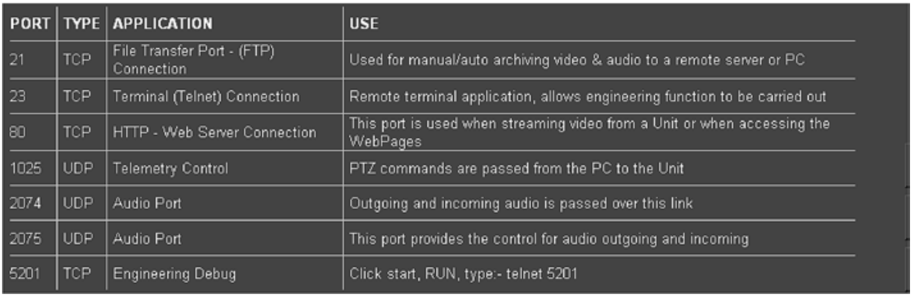
From:- 0

To:- 0

Note: *If you enable this function ensure the IP address of the PC you are using to configure the system is also in the list. If the address is not added then you will be unable to communicate with the unit via the network, it is important to take this feature into account when the unit is on a DHCP network, where IP addresses are allocated automatically. If no IP addresses are specified than any IP address can connect to the unit.*

Function	**Description**
Enable PING response from server	By default this option is enabled and allows the unit to be pinged. Disabling this option will make the unit less visible on the network.
Allowed IP address	These are the IP addresses and subnets that the server will allow connections from, i.e. the IP address of the host PC's that will connect to the unit to; review video, download information.
Open TCP ports	This list identifies the TCP ports that are on the system and available. If a host tries to communicate with the unit using a TCP port that is not in the list, even with a valid IP address, the host will not gain access to the unit. The enabled ports can be a range or single port address, if a single port is needed then enter the same port number in the to and from section.
Open UDP ports	This is the list of UDP ports that are available on the unit. If a host tries to communicate with the unit using a UDP port that is not specified in the list, even with a valid IP address, the host will not gain access.The enabled ports can be a range or single port address, if a single port is needed then enter the same port number in the to and from section.
Port, Type, Application, Use	This identifies the default ports and their functionality that is supported on the unit.

The following are the default port settings supported on the unit; this is shown on the Firewall page menu.



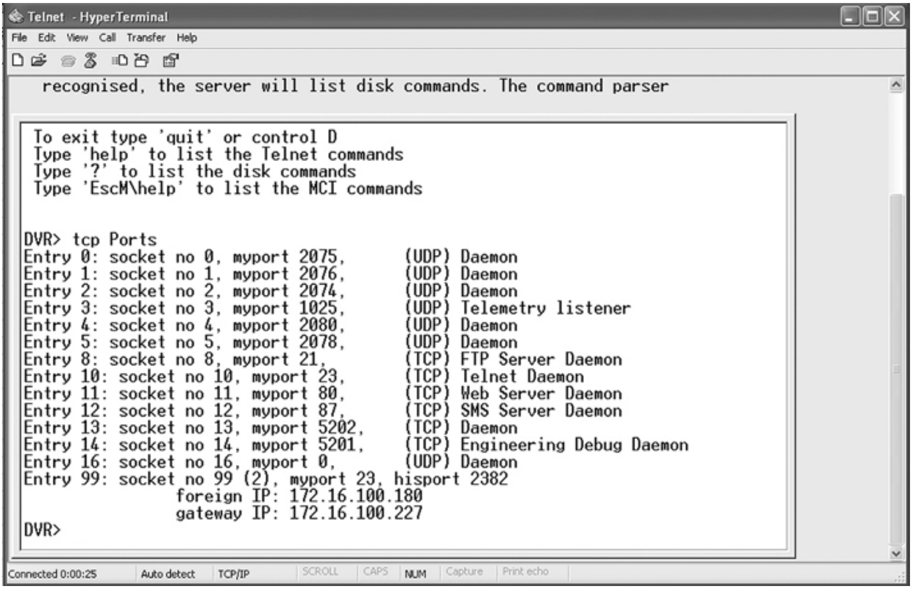
PORT	TYPE	APPLICATION	USE
21	TCP	File Transfer Port - (FTP) Connection	Used for manual/auto archiving video & audio to a remote server or PC
23	TCP	Terminal (Telnet) Connection	Remote terminal application, allows engineering function to be carried out
80	TCP	HTTP - Web Server Connection	This port is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

Alternatively it is possible to identify the supported ports and also determine who is connected to the unit via a telnet session.

At the prompt enter:

TCP Ports

The information displayed should look like this.



```
   recognised, the server will list disk commands. The command parser

 To exit type 'quit' or control D
 Type 'help' to list the Telnet commands
 Type '?' to list the disk commands
 Type 'EscM\help' to list the MCI commands


DVR> tcp Ports
Entry 0: socket no 0, myport 2075,      (UDP) Daemon
Entry 1: socket no 1, myport 2076,      (UDP) Daemon
Entry 2: socket no 2, myport 2074,      (UDP) Daemon
Entry 3: socket no 3, myport 1025,      (UDP) Telemetry listener
Entry 4: socket no 4, myport 2080,      (UDP) Daemon
Entry 5: socket no 5, myport 2078,      (UDP) Daemon
Entry 8: socket no 8, myport 21,        (TCP) FTP Server Daemon
Entry 10: socket no 10, myport 23,      (TCP) Telnet Daemon
Entry 11: socket no 11, myport 80,      (TCP) Web Server Daemon
Entry 12: socket no 12, myport 87,      (TCP) SMS Server Daemon
Entry 13: socket no 13, myport 5202,    (TCP) Daemon
Entry 14: socket no 14, myport 5201,    (TCP) Engineering Debug Daemon
Entry 16: socket no 16, myport 0,       (UDP) Daemon
Entry 99: socket no 99 (2), myport 23, hisport 2382
                foreign IP: 172.16.100.180
                gateway IP: 172.16.100.227
DVR>
```

IP Address Range and Subnet

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

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

The address can be written in two ways:

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

IP address and subnet mask – 192.168.3.1 255.255.255.0

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

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

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

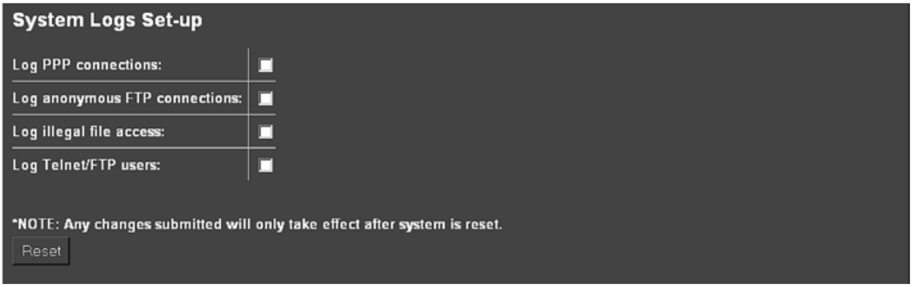
IP address	Network address	Included IP Address Range
192.168.3.1/24	255.255.255.0 0 - 255	
192.168.3.1/25	255.255.255.128	0 - 127
192.168.3.1/26	255.255.255.192	0 - 63
192.168.3.1/27	255.255.255.224	0 – 31
192.168.3.1/28	255.255.255.240	0 – 15
192.168.3.1/29	255.255.255.248	0 – 7
192.168.3.1/30	255.255.255.252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

How to Enable System Logs

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

By default the unit will log illegal file access and telnet/FTP users, to enable the other functions:

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



System Logs Set-up

Log PPP connections:	□
Log anonymous FTP connections:	□
Log illegal file access:	□
Log Telnet/FTP users:	□

*NOTE: Any changes submitted will only take effect after system is reset.

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

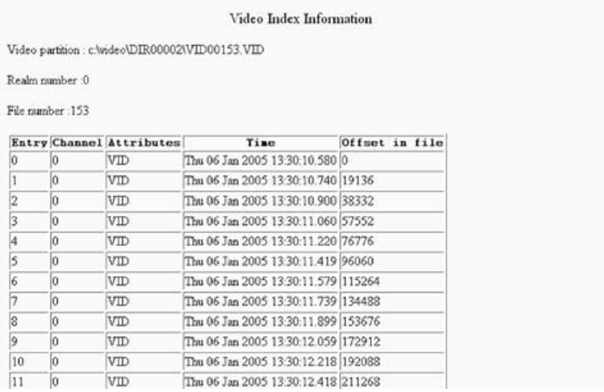
How to Configure Watermarking

The unit supports the facility to watermark recorded images. It is also possible to produce a watermark certificate which proves that an image has not been altered or tampered with, using a unique MD5 signature which will change if the image files are changed.

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

To configure and produce a watermark certificate it is presumed that the Tools option has been enabled in the Advanced Features menu:

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



Video Index Information

Video partition : c:\video\DIR00002\VID00153.VID

Realm number :0

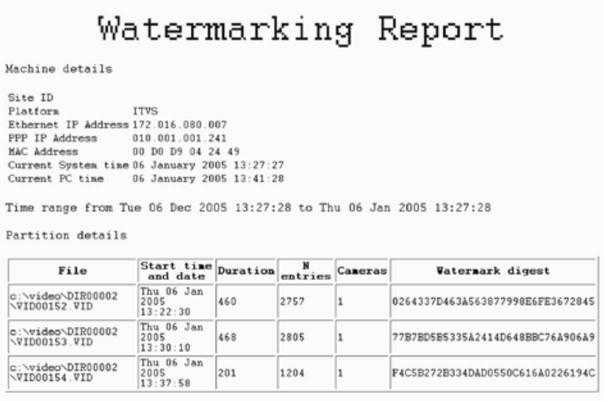
File number :153

Entry	Channel	Attributes	Time	Offset in file
0	0	VID	Thu 06 Jan 2005 13:30:10.580	0
1	0	VID	Thu 06 Jan 2005 13:30:10.740	19136
2	0	VID	Thu 06 Jan 2005 13:30:10.900	38332
3	0	VID	Thu 06 Jan 2005 13:30:11.060	57552
4	0	VID	Thu 06 Jan 2005 13:30:11.220	76776
5	0	VID	Thu 06 Jan 2005 13:30:11.419	96060
6	0	VID	Thu 06 Jan 2005 13:30:11.579	115264
7	0	VID	Thu 06 Jan 2005 13:30:11.739	134488
8	0	VID	Thu 06 Jan 2005 13:30:11.899	153676
9	0	VID	Thu 06 Jan 2005 13:30:12.059	172912
10	0	VID	Thu 06 Jan 2005 13:30:12.218	192088
11	0	VID	Thu 06 Jan 2005 13:30:12.418	211268

7. If the Operator that is generating the watermark certificates is to be logged, enter the report author information, this will be added to the certificate.
8. Enter the step size information; this identifies the 'skip' distance between bytes used in the watermark calculations, default 256 bytes.
9. To generate the watermark codes that will be linked to the partition selected press the watermark button.

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

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



Watermarking Report

Machine details

Site ID	
Platform	ITVS
Ethernet IP Address	172.016.080.007
PPP IP Address	010.001.001.241
MAC Address	00 D0 D9 04 24 49
Current System time	06 January 2005 13:27:27
Current PC time	06 January 2005 13:41:28

Time range from Tue 06 Dec 2005 13:27:28 to Thu 06 Jan 2005 13:27:28

Partition details

File	Start time and date	Duration	N entries	Cameras	Watermark digest
c:\video\DIR00002 \VID00152.VID	Thu 06 Jan 2005 13:22:30	460	2757	1	0264337D463A563877998E6FE3672845
c:\video\DIR00002 \VID00153.VID	Thu 06 Jan 2005 13:30:10	468	2805	1	77B7BD5B5335A2414D648BBC76A906A9
c:\video\DIR00002 \VID00154.VID	Thu 06 Jan 2005 13:37:58	201	1204	1	F4C5B272B334DAD0550C616A0226194C

How to Configure the Webcam functionality

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

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

Examples of where this can be incorporated are:

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

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

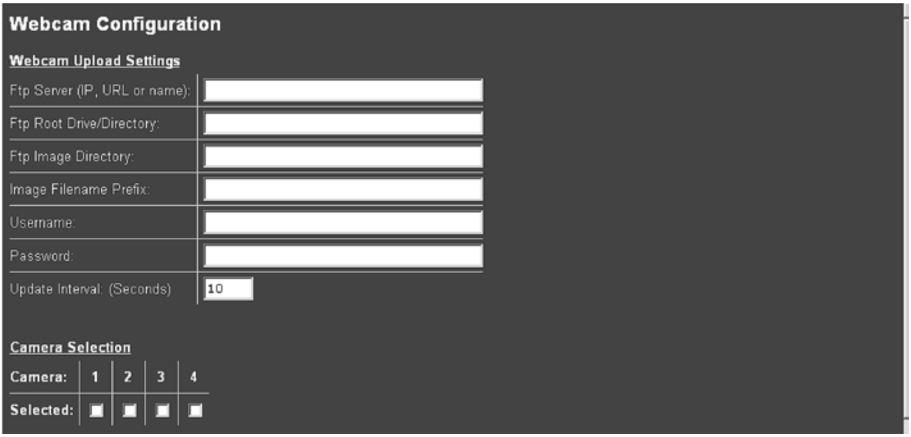
This section has been divided into:

Enabling the feature, identifying server information and enabling the cameras

Configuring the FTP session details.

To enable and configure the webcam feature:

1. Select Network -> Webcam Set-up.
2. Enter the FTP Server details; this can be the IP address, URL or domain name of the Server that will forward the images to the web pages. This link is usually provided by the Internet Service Provider (ISP).
3. Enter the root directory on the FTP server where the files will be saved.
4. Enter the image directory information; this is the path within the root drive that will store the images that are being FTP’d to the Server.
5. Enter the prefix information that will precede the image file when uploaded to the FTP Server, an example is ‘cam_’ which would create a file name of cam_01.jpg.
6. Enter the username and password to allow the files to be uploaded to the FTP Server, this will be given to you by the Network Administrator.
7. Enter the update interval in seconds, this identifies the time between updated files being transmitted from the unit to the FTP Server. The speed and cost of the network connection being used should be taken into account when setting this time period.
8. Enable the video input(s) that are to be made available for webcam functionality. Images from these inputs will be transmitted to the FTP Server for integration into web pages.
9. Save the configuration information by selecting Save Settings!



Webcam Configuration

Webcam Upload Settings

Ftp Server (IP, URL or name):	
Ftp Root Drive/Directory:	
Ftp Image Directory:	
Image Filename Prefix:	
Username:	
Password:	
Update Interval: (Seconds)	10

Camera Selection

Camera:	1	2	3	4
Selected:	☐	☐	☐	☐

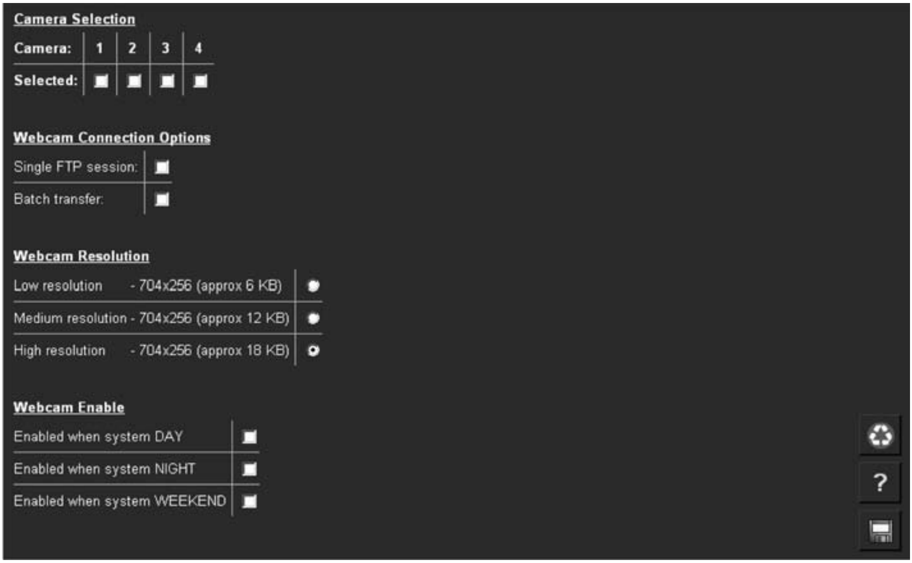
Function	Description
FTP Server	This is the IP address, URL or Domain Name of the FTP Server. Images will be uploaded from the unit to this FTP server as time intervals specified.
FTP Root Drive/Directory	This is the main/root directory on the FTP server where the image directory will be located.
FTP Image Directory	This directory will be created when the initial image is uploaded to the FTP Server, it is the directory where all images will be saved on the server.
Image Filename Prefix	This is an identifier for images sent from this unit and will be stored as a prefix to the file name.
Username	To gain access to the FTP server it is necessary to go through an authentication process this is the username that will allow the images from the unit to be uploaded to the FTP Server.
Password	To gain access to the FTP server it is necessary to go through an authentication process this is the password that will allow the images from the unit to be uploaded to the FTP Server.
Update interval	This is the minimum update interval between each image that is transmitted from the unit.
Camera selection	This allows you to enable the video inputs that will be accessible for upload to the FTP Server.

To enable the webcam connection information:

1. Enable the single FTP session so the FTP link from the unit to the FTP server is permanently up. If this is not enabled then an FTP session will need to be established every time the unit needs to transmit images.
2. Enable batch transfer and images will be transmitted to the FTP Server in a ‘batch’, e.g. the unit will take ‘snap shots’ from video inputs 1, 2, 4 and send these in a single batch to the FTP Server. If this is disabled then the unit will transmit files individually. The delay between batch files being transmitted is the update interval, e.g. every 10 seconds the unit will send images from video inputs 1, 2, 3. If batch is disabled then the update interval is the time between the unit sampling an image from one input to the next, e.g. the unit will transmit an image from input 1, 10 seconds later it will transmit and image from input 2, etc.

3. Select the resolution of the image that will be transmitted to the FTP Server, the files sizes that are applicable to this resolution are displayed. The file size should be taken into account with reference to the speed and type of network link.
4. Enable the Webcam functionality for this feature to operate, tick the box which is appropriate to your application; Enabled when system DAY, Enabled when system NIGHT, Enabled when system WEEKEND. Selecting all options will always enable the webcamera function.
5. Remember to save the configuration by selecting Save Settings!

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



Camera Selection

Camera:	1	2	3	4
Selected:	□	□	□	□

Webcam Connection Options

Single FTP session:	□
Batch transfer:	□

Webcam Resolution

Low resolution - 704x256 (approx 6 KB)	○
Medium resolution - 704x256 (approx 12 KB)	○
High resolution - 704x256 (approx 18 KB)	●

Webcam Enable

Enabled when system DAY	□
Enabled when system NIGHT	□
Enabled when system WEEKEND	□

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

Tools

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

To access the Tools option:

1. Select the Tools tab, the tools available are:

   Camera Adjustment

   Video Scope

   Audio Trace

   Relay Test Page

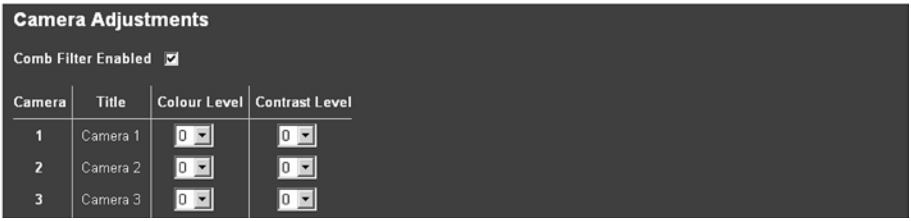
   Watermarking

   System Variables

   Reset

Camera Adjustment

This provides the Administrator the opportunity to adjust the colour and contrast settings for each camera connected to the unit. The Comb Filter improves image clarity and is turned on by default. Some NTSC line locked cameras may give better image quality results with the Comb Filter disabled.



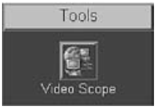
Camera Adjustments

Comb Filter Enabled ☑

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

Function	Description
Comb Filter Enabled	The Comb Filter improves clarity and is turned on by default. Some NTSC line locked cameras may give better image quality results with the Comb Filter disabled.
Camera	This identifes the video input number on the unit.
Title	This identifies the corresponding camera title allocated to the video input.
Colour	Select a value from the drop down list to select the colour level for the video input.
Contrast	Select a value from the drop down list to select the contrast level for the video input.

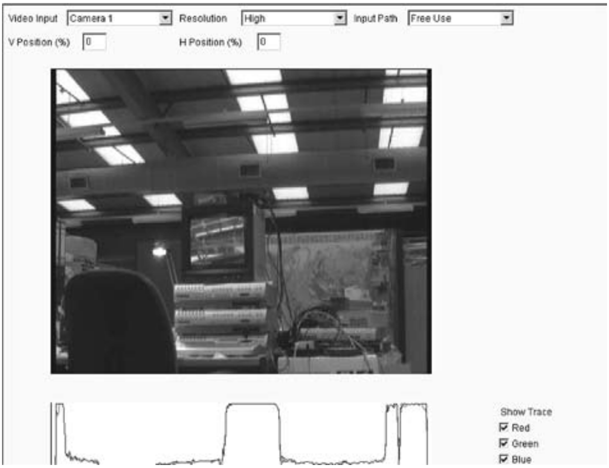
Video Scope



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

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

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



Video Input: Camera 1 · Resolution: High · Input Path: Free Use

V Position (%): 0 · H Position (%): 0

Show Trace
☑ Red
☑ Green
☑ Blue

Function	Description
Comb Filter	This feature improves image clarity and is turned on by default. Some NTSC line locked cameras may give better image quality results with the Comb Filter disabled.
Video Input	This is a drop down list of the available video inputs on the unit.
Resolution	This is a drop down list allowing selection of the resolution being viewed/traced (high, medium and low).
Input Path	This is a drop down list allowing selection between free use or preselector 1 – 4.
V and H Position	When a line of video is selected this identifies the vertical and horizontal position. For the overall image these values will be 0.
Show Trace	This allows the R, G, B trace to be enabled or disabled.
RGB	These are the calculated values for the RGB contents within the whole image or the selected line.

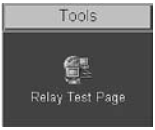
Audio Trace

It is possible to use the audio trace option to identify if audio is being transmitted or received by the unit.

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

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

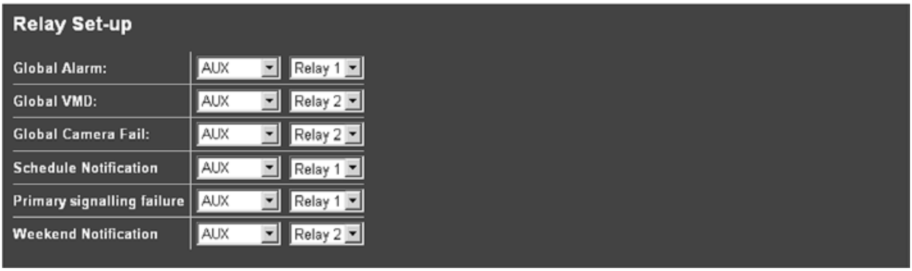
Relay Test Page



The relay test page allows you to test the onboard relays and the additional relay modules. The unit supports two onboard relays and up to two additional relay modules, these modules have sixteen relay connections each.

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

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



Relay Set-up

Global Alarm:	AUX	Relay 1
Global VMD:	AUX	Relay 2
Global Camera Fail:	AUX	Relay 2
Schedule Notification	AUX	Relay 1
Primary signalling failure	AUX	Relay 1
Weekend Notification	AUX	Relay 2

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

Primary Signalling Failure
This identifies which of the relays has been enabled for primary signalling failure. Note this relay will be disabled for test.

Weekend Notification
This identifies which of the relays has been enabled for weekend notification. Note this relay will be disabled for test.

On-board Relays
There are two on-board relays, enabling the corresponding relay will close the output .

Module 1
If an additional relay module has been connected to the 485 bus, this allows the relevant relays to be tested

Note: *The relay will only be initiated when the Save option has been selected.*

Module 2
If a second additional relay module has been connected to the 485 bus, this allows the relevant relays to be tested.

Note: *The relay will only be initiated when the Save option has been selected.*

Watermarking

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

System Variable

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

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

Reset

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

Reviewing the Unit Logs

The unit can be configured to produce a number of log files, these are for:

PPP connections

Anonymous FTP connections

Illegal file access attempts

FTP and telnet users

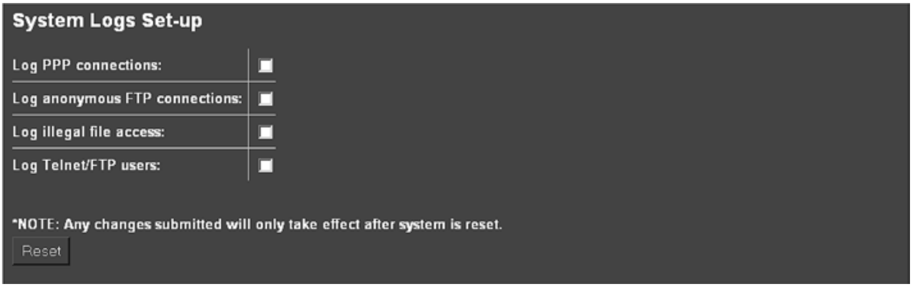
System Logs Setup

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

To access the logs:

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

   Connection Log
   Anonymous FTP Log
   Security Log
   e-mail Log
   Sent Message Log
   FTP Download Log
   Logfile
   Logfile Backup
   Archive
3. To review the files select the corresponding option, the information will be displayed on screen.



System Logs Set-up

Log PPP connections: ☐

Log anonymous FTP connections: ☐

Log illegal file access: ☐

Log Telnet/FTP users: ☐

*NOTE: Any changes submitted will only take effect after system is reset.

Function	Description
Log anonymous	This identifies when an unauthorised user tries to

FTP connections — access the unit by entering anonymous in the username or password.

Log illegal file access — Any web access to a CGI protected directory or non-existent file will be logged with an IP address, time and type of action

Log Telnet/FTP users — This will log users that are trying to gain access to the unit using an FTP or telnet session

Connection Log

This log details all FTP and telnet connections made to the unit.

Telnet and FTP can be allocated a username and password by enabling and configuring the option within the USER.ini file, this file registers all the information on the User name, IP address of the remote PC, time of transaction.Having this log containing the above information ensures ease of identification of Operators/Administrators that have logged into the system, the following shows typical log information;

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

Anonymous FTP Log

The FTP function on the unit is password protected, however it is possible to disable the password allowing any user access to the unit via

FTP.

If the password is disabled then any user accessing the unit will be logged in the Anonymous FTP log.

A typical example of the log is shown:

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

Security Log

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

The information logged is:

The action requested and status

Time and date

IP address

Port information

This information can be used to monitor the connections to the unit and identify unauthorised actions.

The following shows typical log information;

```
Attempt to access to frmpages\index.html at Tue Jun 08 12:43:04 2004 +0100, action GET
Authentication fail
Foreign IP 172.16.50.60
Socket no 22, myport 80, hisport 12226
Attempt to access to scripts\root.exe at Tue Jun 08 13:50:35 2004 +0100, action GET file
does not exist
Foreign IP 172.16.50.60
Socket no 23, myport 80, hisport 1049
```

E-mail Log

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

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

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

```
Sending message to jsmith@dmicros.com at Wed Jun 30 14:21:26 2004 +0200
220 heron.jbloggs ESMTP Server (Microsoft Exchange Internet Mail Service 5.7.2653.13) ready
HELO unit
250 OK
MAIL FROM:<unit@unit>
250 OK - mail from <unit@unit>
RCPT TO: <jsmith@jbloggs.com>
250 OK - Recipient <jsmith@jbloggs.com>
```

```
DATA
354 Send data.  End with CRLF.CRLF
Date: Wed, 30 Jun 2004 14:21:32 +0200
X-Mailer: ADH SendMail V1.0
MIME-Version: 1.0
To: jsmith@jbloggs.com (John Smith)
From: unit@unit
Subject: System Exception
Content-Type: text/html; charset=us-ascii;
Content-Transfer-Encoding: 7bit
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html>
Site-Id: unit<br>
System-Exception: Camera fail 3 at Wed Jun 30 14:21:26 2004 +0200<br>
</html>
250 OK
QUIT 221 closing connection
```

Sent Message Log

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

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

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

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

FTP Download Log

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

Logfile

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

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

This ensures current and recent information is always available.

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

The typical log information should look like this:

```
#
System-Start :  at 15:11:39 on 24-06-2004 UTC
System-Halt :  at 15:11:28 on 24-06-2004 UTC
Restart code : 100
Restart reason : Controlled user RESET from Telnet or the webpages
Alarm-Log : Alarm initiated : Zone 1 at 15:11:59 on 24-06-2004 +0100
Connection-Status: request connection for Alarm Reporting at 15:11:59 on 24-06-2004 +0100
Connection-Status : Connection to 172.16.100.12\Ethernet at 15:11:59 on 24-06-2004 +0100
Site-Id: unit50
Arc-ID: unit-50
System-Status:
Local-IP: 172.16.89.50
Activating-Channel: 3
Response-Images: 1
Response-Area: Zone 1
Response-Level: GREEN
Alarm-Time: 15:11:59 on 24-06-2004
Rec-Index: 14:11:59 on 24-06-2004
Connection-Status : Connection closed at 15:11:59 on 24-06-2004 +0100
#
```

Logfile Backup

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

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

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

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

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

```
Sat Apr 24 05:53:50 2004 (+0100): FTP FAILED LOGIN User: [test] Password: [test]
Sat Apr 24 05:53:50 2004 (+0100): Foreign IP 62.214.19.65
Sat Apr 24 05:53:50 2004 (+0100): Socket no 82, myport 21, hisport 4953
Sat Apr 24 05:53:50 2004 (+0100): FTP FAILED LOGIN User: [test] Password: [test12]
Sat Apr 24 05:53:50 2004 (+0100): Foreign IP 62.214.19.65
Sat Apr 24 05:53:50 2004 (+0100): Socket no 83, myport 21, hisport 4999
Sat Apr 24 05:53:50 2004 (+0100): FTP FAILED LOGIN User: [test] Password: [test123]
Sat Apr 24 05:53:50 2004 (+0100): Foreign IP 62.214.19.65
Sat Apr 24 05:53:50 2004 (+0100): Socket no 84, myport 21, hisport 1049
Sat Apr 24 05:53:50 2004 (+0100): FTP FAILED LOGIN User: [test] Password: [123]
Sat Apr 24 05:53:50 2004 (+0100): Foreign IP 62.214.19.65
Sat Apr 24 05:53:50 2004 (+0100): Socket no 85, myport 21, hisport 1071
```

Archive

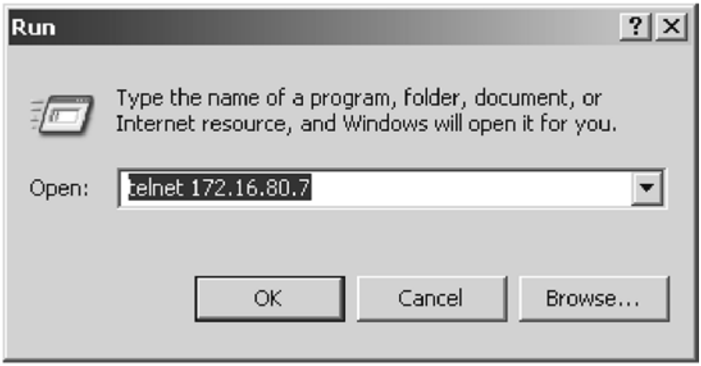
The archive log shows information on the last archive session including date of archive, file archived and the watermark assigned to that session.

Appendix A

Reset using Telnet

An alternative option for resetting the unit is to connect to the unit using telnet.

1. Go to Start -> Run.
2. Enter <telnet <IP address of Server>>



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet 172.16.80.7

3. You will be prompted for a username and password (default dm and telnet) and press return.

Note: *Echo is enabled on the unit for telnet.*

4. Type <reset>, the unit will reset itself and will not be available for a few minutes.

Appendix B – .ini Files

Editing the ini Files using FTP Client Application

There are a number of parameters that can be configured within the ini files on the unit. This section details the files, their function and how these are configured.

To edit and configure these files on the unit you will require:

FTP communication to be enabled on the unit

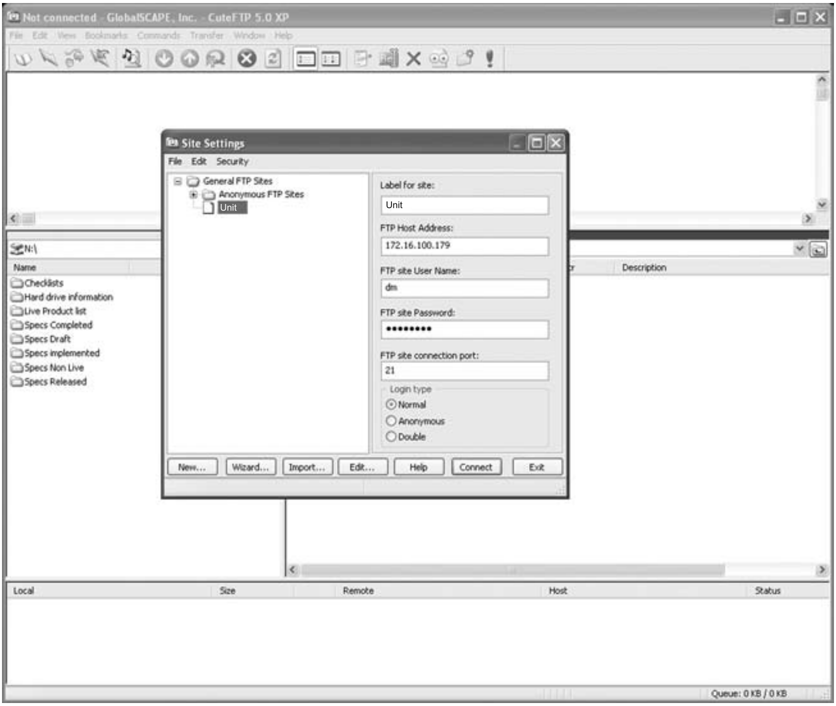
Valid FTP username and password

FTP Client software application

Connection via the Ethernet network to the unit

The following steps give an example of how to create an FTP session with the unit to configure these files, take note this may differ from the process of the FTP software you are utilising.

1. Launch the FTP client software.
2. You will need to create a site for the FTP link, enter the IP address of the unit, enter the FTP username and password.



Not connected - GlobalSCAPE, Inc. - CuteFTP 5.0 XP

Site Settings

Label for site: Unit

FTP Host Address: 172.16.100.179

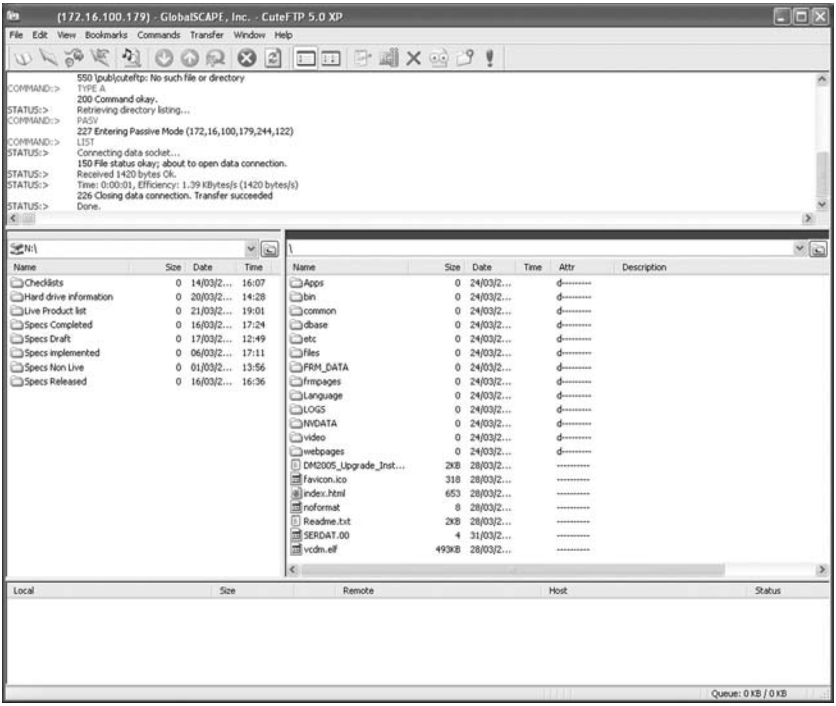
FTP site User Name: dm

FTP site Password: •••••••••

FTP site connection port: 21

Login type: ● Normal ○ Anonymous ○ Double

3. Select the Connect button to make the connection.
4. If the connection is successful you will be issued a connection prompt.



(172.16.100.179) - GlobalSCAPE, Inc. - CuteFTP 5.0 XP
File Edit View Bookmarks Commands Transfer Window Help

```
              550 \pub\cuteftp: No such file or directory
COMMAND:>     TYPE A
              200 Command okay.
STATUS:>      Retrieving directory listing...
COMMAND:>     PASV
              227 Entering Passive Mode (172,16,100,179,244,122)
COMMAND:>     LIST
STATUS:>      Connecting data socket...
              150 File status okay; about to open data connection.
STATUS:>      Received 1420 bytes Ok.
STATUS:>      Time: 0:00:01, Efficiency: 1.39 KBytes/s (1420 bytes/s)
              226 Closing data connection. Transfer succeeded
STATUS:>      Done.
```

N:\

Name	Size	Date	Time
Checklists	0	14/03/2...	16:07
Hard drive information	0	20/03/2...	14:28
Live Product list	0	21/03/2...	19:01
Specs Completed	0	16/03/2...	17:24
Specs Draft	0	17/03/2...	12:49
Specs implemented	0	06/03/2...	17:11
Specs Non Live	0	01/03/2...	13:56
Specs Released	0	16/03/2...	16:36

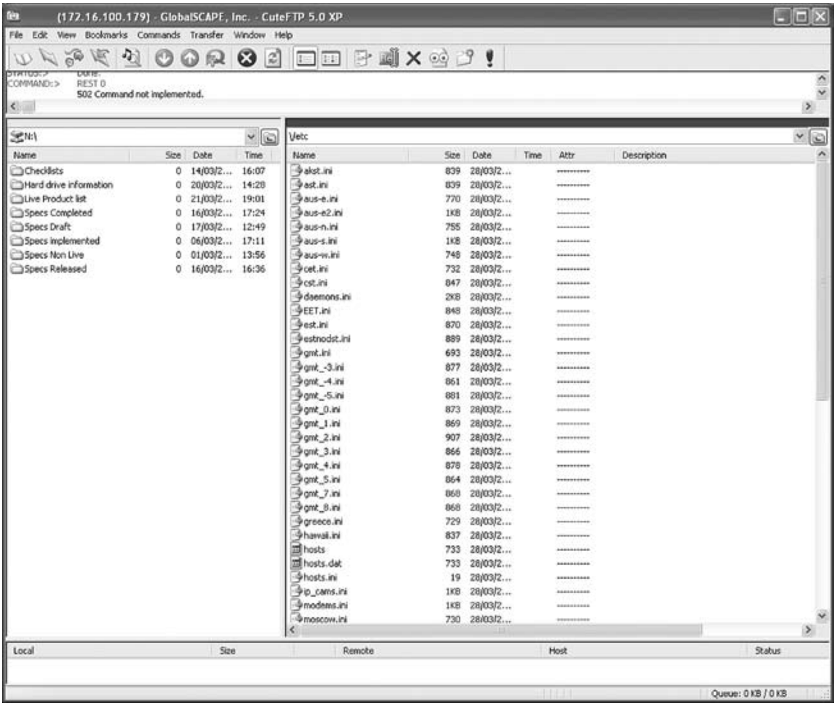
\

Name	Size	Date	Time	Attr	Description
Apps	0	24/03/2...		d---------	
bin	0	24/03/2...		d---------	
common	0	24/03/2...		d---------	
dbase	0	24/03/2...		d---------	
etc	0	24/03/2...		d---------	
files	0	24/03/2...		d---------	
FRM_DATA	0	24/03/2...		d---------	
frmpages	0	24/03/2...		d---------	
Language	0	24/03/2...		d---------	
LOGS	0	24/03/2...		d---------	
NVDATA	0	24/03/2...		d---------	
video	0	24/03/2...		d---------	
webpages	0	24/03/2...		d---------	
DM2005_Upgrade_Inst...	2KB	28/03/2...		----------	
favicon.ico	318	28/03/2...		----------	
index.html	653	28/03/2...		----------	
noformat	8	28/03/2...		----------	
Readme.txt	2KB	28/03/2...		----------	
SERDAT.00	4	31/03/2...		----------	
vcdm.elf	493KB	28/03/2...		----------	

Local	Size	Remote	Host	Status

5. Click OK.

6. You will be presented with the directory structure on the unit, locate and select the etc directory in the root drive.


(172.16.100.179) - GlobalSCAPE, Inc. - CuteFTP 5.0 XP
File Edit View Bookmarks Commands Transfer Window Help
Local Size Remote Host Status
Queue: 0 KB / 0 KB

```
STATUS:>     Done.
COMMAND:>    REST 0
             502 Command not implemented.
```

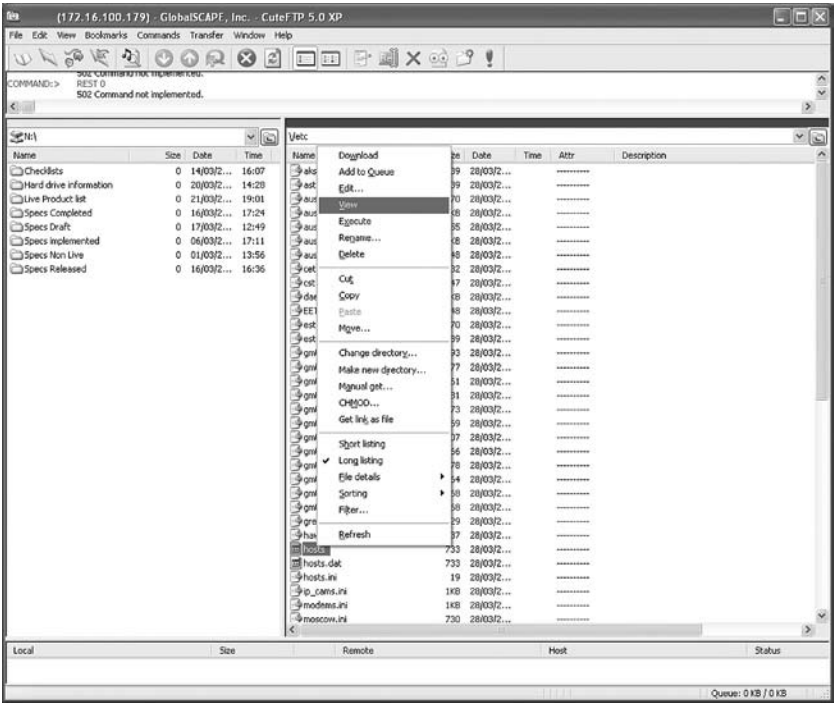
N:\

Name	Size	Date	Time
Checklists	0	14/03/2...	16:07
Hard drive information	0	20/03/2...	14:28
Live Product list	0	21/03/2...	19:01
Specs Completed	0	16/03/2...	17:24
Specs Draft	0	17/03/2...	12:49
Specs implemented	0	06/03/2...	17:11
Specs Non Live	0	01/03/2...	13:56
Specs Released	0	16/03/2...	16:36

\etc

Name	Size	Date	Time	Attr	Description
akst.ini	839	28/03/2...		----------	
ast.ini	839	28/03/2...		----------	
aus-e.ini	770	28/03/2...		----------	
aus-e2.ini	1KB	28/03/2...		----------	
aus-n.ini	755	28/03/2...		----------	
aus-s.ini	1KB	28/03/2...		----------	
aus-w.ini	748	28/03/2...		----------	
cet.ini	732	28/03/2...		----------	
cst.ini	847	28/03/2...		----------	
daemons.ini	2KB	28/03/2...		----------	
EET.ini	848	28/03/2...		----------	
est.ini	870	28/03/2...		----------	
estnodst.ini	889	28/03/2...		----------	
gmt.ini	693	28/03/2...		----------	
gmt_-3.ini	877	28/03/2...		----------	
gmt_-4.ini	861	28/03/2...		----------	
gmt_-5.ini	881	28/03/2...		----------	
gmt_0.ini	873	28/03/2...		----------	
gmt_1.ini	869	28/03/2...		----------	
gmt_2.ini	907	28/03/2...		----------	
gmt_3.ini	866	28/03/2...		----------	
gmt_4.ini	878	28/03/2...		----------	
gmt_5.ini	864	28/03/2...		----------	
gmt_7.ini	868	28/03/2...		----------	
gmt_8.ini	868	28/03/2...		----------	
greece.ini	729	28/03/2...		----------	
hawaii.ini	837	28/03/2...		----------	
hosts	733	28/03/2...		----------	
hosts.dat	733	28/03/2...		----------	
hosts.ini	19	28/03/2...		----------	
ip_cams.ini	1KB	28/03/2...		----------	
modems.ini	1KB	28/03/2...		----------	
moscow.ini	730	28/03/2...		----------	

7. The following files are all stored in the etc directory.



```
         502 Command not implemented.
COMMAND:> REST 0
         502 Command not implemented.
```

N:\

Name	Size	Date	Time
Checklists	0	14/03/2...	16:07
Hard drive information	0	20/03/2...	14:28
Live Product list	0	21/03/2...	19:01
Specs Completed	0	16/03/2...	17:24
Specs Draft	0	17/03/2...	12:49
Specs implemented	0	06/03/2...	17:11
Specs Non Live	0	01/03/2...	13:56
Specs Released	0	16/03/2...	16:36

\etc

Name	ze	Date	Time	Attr	Description
aks	39	28/03/2...		----------	
ast	39	28/03/2...		----------	
aus	70	28/03/2...		----------	
aus	B	28/03/2...		----------	
aus	35	28/03/2...		----------	
aus	B	28/03/2...		----------	
aus	48	28/03/2...		----------	
cet	32	28/03/2...		----------	
cst	47	28/03/2...		----------	
dae	B	28/03/2...		----------	
EET	48	28/03/2...		----------	
est	70	28/03/2...		----------	
est	39	28/03/2...		----------	
gml	93	28/03/2...		----------	
gml	77	28/03/2...		----------	
gml	51	28/03/2...		----------	
gml	31	28/03/2...		----------	
gml	73	28/03/2...		----------	
gml	59	28/03/2...		----------	
gml	07	28/03/2...		----------	
gml	56	28/03/2...		----------	
gml	78	28/03/2...		----------	
gml	54	28/03/2...		----------	
gml	58	28/03/2...		----------	
gml	58	28/03/2...		----------	
gre	29	28/03/2...		----------	
hav	37	28/03/2...		----------	
hosts	733	28/03/2...		----------	
hosts.dat	733	28/03/2...		----------	
hosts.ini	19	28/03/2...		----------	
ip_cams.ini	1KB	28/03/2...		----------	
modems.ini	1KB	28/03/2...		----------	
moscow.ini	730	28/03/2...		----------	

Local	Size	Remote	Host	Status

8. There are two ways of opening and editing these files, depending on the file that is selected.

hosts and profiles

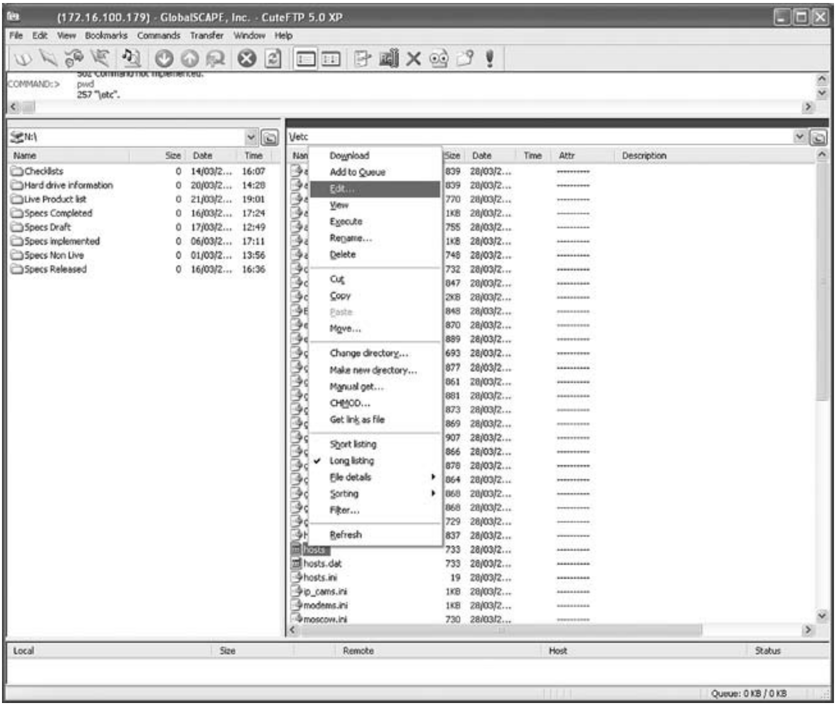
Highlight the file, click the right mouse key and select View.

The file will be opened and you can edit the information.

modems.ini, USER.ini, Vidcfg.ini, WEBUSER.ini

Highlight the file, click the right mouse key and select Edit.

The file will be opened and you can edit the information.



```
         502 Command not implemented.
COMMAND:> pwd
         257 "\etc".
```

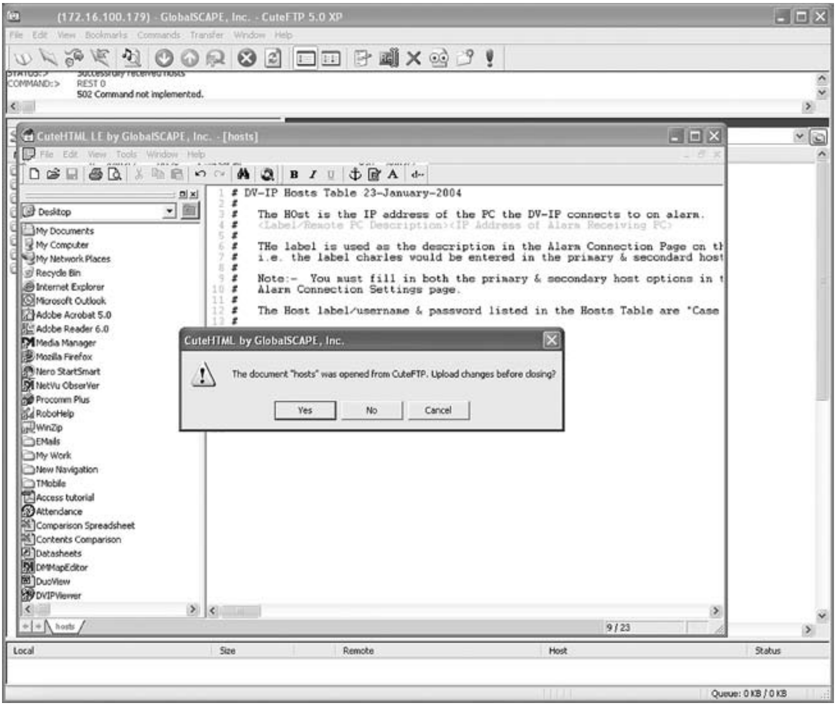
N:\

Name	Size	Date	Time
Checklists	0	14/03/2...	16:07
Hard drive information	0	20/03/2...	14:28
Live Product list	0	21/03/2...	19:01
Specs Completed	0	16/03/2...	17:24
Specs Draft	0	17/03/2...	12:49
Specs implemented	0	06/03/2...	17:11
Specs Non Live	0	01/03/2...	13:56
Specs Released	0	16/03/2...	16:36

\etc

Nan	Size	Date	Time	Attr	Description
a	839	28/03/2...		----------	
a	839	28/03/2...		----------	
a	770	28/03/2...		----------	
a	1KB	28/03/2...		----------	
a	755	28/03/2...		----------	
a	1KB	28/03/2...		----------	
a	748	28/03/2...		----------	
c	732	28/03/2...		----------	
c	847	28/03/2...		----------	
c	2KB	28/03/2...		----------	
E	848	28/03/2...		----------	
e	870	28/03/2...		----------	
e	889	28/03/2...		----------	
g	693	28/03/2...		----------	
g	877	28/03/2...		----------	
g	861	28/03/2...		----------	
g	881	28/03/2...		----------	
g	873	28/03/2...		----------	
g	869	28/03/2...		----------	
g	907	28/03/2...		----------	
g	866	28/03/2...		----------	
g	878	28/03/2...		----------	
g	864	28/03/2...		----------	
g	868	28/03/2...		----------	
g	868	28/03/2...		----------	
g	729	28/03/2...		----------	
H	837	28/03/2...		----------	
hosts	733	28/03/2...		----------	
hosts.dat	733	28/03/2...		----------	
hosts.ini	19	28/03/2...		----------	
ip_cams.ini	1KB	28/03/2...		----------	
modems.ini	1KB	28/03/2...		----------	
moscow.ini	730	28/03/2...		----------	

9. Once you have completed the configuration Save the file.
10. When you close the file you will be prompted to upload the file to the unit, select Upload.



```
STATUS:>     Successfully received hosts
COMMAND:>    REST 0
             502 Command not implemented.
```

```
# DV-IP Hosts Table 23-January-2004
#
#   The HOst is the IP address of the PC the DV-IP connects to on alarm.
#   <Label/Remote PC Description><IP Address of Alarm Receiving PC>
#
#   THe label is used as the description in the Alarm Connection Page on tl
#   i.e. the label charles would be entered in the primary & secondard host
#
#   Note:-  You must fill in both the primary & secondary host options in t
#   Alarm Connection Settings page.
#
#   The Host label/username & password listed in the Hosts Table are "Case
#
```

The document "hosts" was opened from CuteFTP. Upload changes before closing?

Note: *If you are not prompted ensure you upload the file to the unit for the configuration to take affect.*

Structure of the Files

Each of the following files usually has an explanation at the beginning of the file describing what the feature command set is and how they can be edit.

If any of the configuration commands have a comment (#) at the beginning of the line then this has been disabled, remove the comment (#) enables the feature and allows you to configure the settings.

Headings will be included when more that one feature can be configured within the file to identify the command string within that section, e.g. [unlock], [watermarking].

hosts

This file contains the IP address of the remote monitoring PC that is the point of contact when an alarm is received on the unit.

The file allows you to identify the name and IP address of the PC.

Note: *There is a corresponding web page that is the usual interface for configuring this information; however this file has also be supplied.*

An example of the information contained in this file is shown.

```
# unit Hosts Table 23-January-2004
# The Host is the IP address of the PC the unit connects to on alarm.
# <Label/Remote PC Description><IP Address of Alarm Receiving PC>
# The label is used as the description in the Alarm Connection Page on the unit.
# i.e. the label location1 would be entered in the primary & secondary host name.
# Note:- You must fill in both the primary & secondary host options in the
# Alarm Connection Settings page.
# The Host label/username & password listed in the Hosts Table are “Case Sensitive”.
# Hosts Table List
# ————————
# <Label/PC Description><IP Address of remote PC>
  JohnSmith  10.0.0.50
  ARC1         10.0.0.51
  Location1   192.168.2.3
  NULL         0.0.0.0
```

modems.ini

The unit supports a number of modems that can be configured in the Serial Port & Telemetry web page, however if a modem is not supported then the configuration and operational information for the modem can be added to the modems.ini file.

An example of the information stored in this .ini file is shown:

```
# modem description file
# These modem strings will be installed prior to the fixed strings and can therefore be
# used to update the initialisation strings
# format:
# [code]
# name=descriptive text name
# reset=string to reset device to factory defaults
# init=initialisation string
# save=string to save current settings
# negate_dtr=0 assert DTR line during modem initialisation
# negate_dtr=1 negate DTR line during modem initialisation
# type=0,1,2 type of PPP device
# 0 - modem / terminal adaptor (default)
# 1 - router
# 2 - always on eg GPRS, CDPD
# code is the product code as returned by ATI (if appropriate)
# name is the descriptive text name (including spaces if required)
# initialisation string is the complete AT string sent to the TA/modem on detection of DTR
# The negate_dtr line allows control over DTR during initialisation. Some modems will
# not respond if DTR is negated whilst others will answer calls unless DTR is negated
# Initialisation requirements - brackets indicate usual settings
# echo off (E0), DCD follows carrier (&C1), DTR causes hangup (&D2)
# useful settings - hardware handshaking, autobaud
[FALCOM_A2]
 name=Falcom GSM Phone/Modem
 reset=AT&F
 init=ATE0&C1&D2&S0S0=1
 save=AT&W
 negate_dtr=0
[ENFORA]
 name=Spider 4 CDPD Modem
 reset=AT&F
 init=ATE0&C1&D2+WS45=4
 save=AT&W
 negate_dtr=0
 type=2
```

paths.ini

This file is part of the Text in Image configuration and identifies the communication port on the unit that will be connected to the peripheral equipment and also the text information.

Once the associated serial port has been enabled for text in image (refer to the Configuration Section of this manual) it is necessary to enter the relevant information in the paths.ini file so the unit is aware or the route (path) of the text information that will be stored with the associated image.

This is an example of the information that is stored within the paths.ini file.

```
# unit 17-07-03
# ————————————————————————————————————-
# Example ini file to add text for COM1 to COM4
# COM1 = tty
# COM2 = term
# COM3 = aux1 or if input_path set to pic0 GPS stored on Port 3
# COM4 = aux2
# TEXT00 = camera 1
# TEXT01 = camera 2
# TEXT02 = camera 3
# input_path  - the ports COM1 to COM4 that will receive text
# output_path - the command that will associate text to a camera
# buffer_size - the total number of character stored per line
# prefix      - this strips off leading characters received from EPOS
# ===========================================
# COM1 will store text with Camera-1
# ===========================================
[PATH0]
input_path=\tty
output_path=\pipe\TEXT00
buffer_size=80
# prefix=J
# ===========================================
# COM2 will store text with Camera-2
# ===========================================
[PATH1]
input_path=\term
output_path=\pipe\TEXT01
buffer_size=80
# prefix=J
profiles
```

When utilising the Connect/Dial on alarm function of the unit, it is necessary to identify the receiving station information – profile – so the unit is aware of the route the alarm is to take. For Ethernet connectivity this can be carried out using the web interface, for connection via a serial port it is necessary to enter the information in the 'profiles' file.

Note: *Ethernet profiles can also be entered in the profiles file instead of using the web interface page.*

```
# unit Profiles Table 23-January-2004
# Profile list
# PPP_Link1 = COM2 - Default alarm dial communication port.
# PPP_Link2 = COM1 - Default dial in communication port.
# Ether1 = Alarm connection across an Ethernet Port (Entering Ethernet as the Profile
# will connect over Ethernet)
# Rules
# 1) The IP address range is that of the remote network the unit is connecting to.
# 2) IF you set the IP range to 10.0.0.50 with a subnet of 255.255.255.0, the HOST PC
#     IP address range will be 10.0.0.51 to 10.0.0.254
# 3) If you only wish to dialling into the unit, the Phone No.
# 4) The first field <Username & Profile Label> is the description you will use in the
#     Alarm Connection Page as the Profile description for the primary & secondary call.
#    The Profile label/username & password listed in the Profiles Table are "Case
   Sensitive".
# ————————-
# Profiles Table List
# ————————-
#<Username>  <Password>  <Port>     <Phone No>   <Address Range>   <Subnet Mask>
Dm           password    PPP_Link2  1234567890   10.0.0.1          255.255.255.0
username     password    PPP_Link1  1234567890   10.0.0.1          255.255.255.0
Test         password    PPP_Link1  1234         10.0.0.1          255.255.255.0
```

USER.ini

A number of features on the unit are password protected; these have default usernames and passwords. The features that can be enabled for authentication are FTP, telnet and serial communication.

The user.ini file contains the username and password information for these features and is also the interface to enable or disable password protection.

The example shows the default usernames and passwords and which of these features are enabled on the unit when shipped from the factory.

```
[FTP]
dm=ftp
[Telnet]
dm=telnet
[Serial]
# dm=serial
# serial=password
```

vidcfg.ini

The unit can support up to 600Gb of internal storage, however in applications that require large storage capacities it is possible to integrate the Dedicated Micros RAID storage units into the application.

As the unit automatically detects external storage, this file is dynamically updated by the system, the example below shows a typical file configuration.

```
# ================
# unit 03-03-2004
# ================
# Entries are as follows
# [Partition name]
# path = <pathname>
# file_size = <file_size>
# max_blocks = <max_blocks>
# disk_offset = <day_mask>
# write_type =
# The meanings of the parameters are as follows
# Partition Name: Any ascii name for this partition. Does not perform any other function
# path :The effective MSDOS style root path of the partition directory structure
#         default 3.5” = c:\video
# file_size :The size in bytes of each partition file - default = 50Mbyte (52428800)
# max_blocks : The number of files in this partition. A value of -1 makes the system use
the maximum available
# space on the disk specified in path
# default = -1



# disk_offset : The offset into the disk for the WebPages, Application, Form Files etc;
start making video partitions
# specified in 64 KiloBytes blocks default=3200 (Equal to 200 MegaBytes)
# write_type : unbuffered - writes data straight to the hard disk drive. Useful to speed up
height images sizes
# written at fast to the HDD.
#     NOTE:- This can be wasteful when writing images to HDD i.e. 256 bytes per image on
average. buffered -
#     Default setting - Buffers data to a fixed 20 KiloByte
#    buffer prior to a HDD write. More efficient when writing
#    images to the HDD.
# ———————————-
# Drive Definitions A – Z
# ———————————-
# Drive a = 4096 KB Ram
# Drive b = 16 KB RAM
# Drive c = MASTER 3.5”
# Drive d = SLAVE 3.5”
# Drive e = Master 3.5”
# Drive f = Slave  3.5”
# Drive g = Flash Drive
# Drive h to K not used
# unit will support up to Drive letter Z
# ———————————-
# Drive Partition Options
# ———————————-
# 10  MegaByte Partition - 10485760  - For hard disk sizes 160 GB or less
# 50  MegaByte Partition - 52428800  - Default in Bootloader & upto 600 GB
# 100 MegaByte Partition - 104857600 - For hard disk blocks larger that 600 GB
# 200 MegaByte Partition - 209715200 - For hard disk blocks larger than 2000 GB
# ———————————————————————————————————————————————-
```

WEBUSER.ini

The WEBUSER.ini file contains the username and passwords for accessing the web configuration pages on the unit.

It also contains the username and password for the Viewer software and the ability to identify which mode of operation can be accessed by a user (live or replay) and which cameras the user can access.

The first example shows the default username and password for accessing the web configuration pages on the unit.

```
###################################################################
#
                           #
# unit Webuser.ini Version  18th May 2004
       #
#
                           #
###################################################################
# ——————————————————————————————————
# Note: This file requires a blank line at the end of this file.
# Note: Line with #— are comments. i.e. #—  Username(s) Password(s)
# ——————————————————————————————————
   [WebPage Configuration]
# —  Username(s) Password(s)  —
            dm=web
```

This example shows the command string for enabling John Smith to have access to cameras 1 to 4 in live mode, cameras 1 to 4 in replay and the username and password for this Operator when logging in using the Viewer software.

```
####################################################################
#
                            #
# Provides access for cameras 1 to 4 in live and cameras 1 to 4 in playback       #
# for John Smith
                     #
#
                           #
###################################################################
# object=cgi
 live_cams=1-4
 replay_cams=1-4
 #—  Username(s) Password(s)  —
 john=smith
```

Appendix C – Port Assignment on the unit

Port Allocation

It is possible to identify specific ports that will be used for functionality supported on the unit.

These functions are:

FTP

Telnet

HTTP

Telemetry Control

Audio

Debug

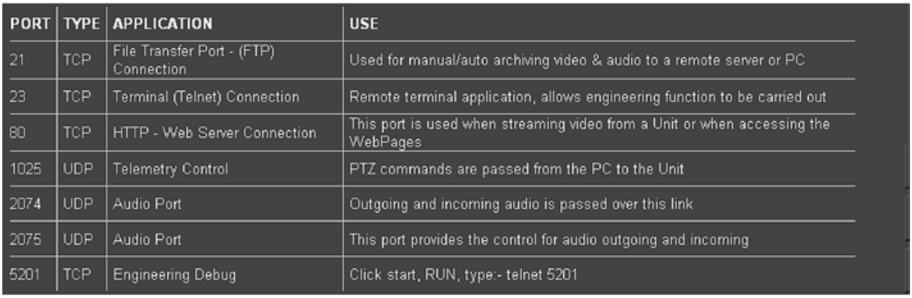
Some of these ports have default settings that will link to the default settings of a standard network infrastructure, e.g. port 21 default port for FTP, port 80 default port for HTTP.

However if these default port numbers have already been allocated to other devices on the network then it is possible to identify alternative port numbers.

NOTE: *It's important to ensure all devices that are part of the system configuration are all allocated the same port number otherwise communication between the devices will not be successful.*

To view the ports that have been enabled and configured on the unit, select Network -> Firewall Options. This details the port numbers, type of connection, application and use.

The screen shot shows the default settings for each of the features that utilises a port number as part of its communication path.



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

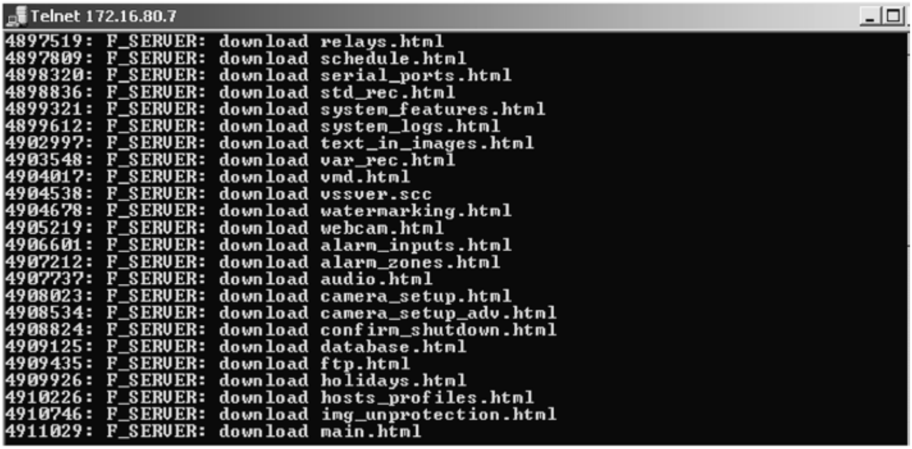
It is possible to redefine the port allocation for FTP, telnet and HTTP, how this is achieved is detailed in the Configuration section of this manual.

The telemetry control, audio port and engineering debug are default settings and are not configurable; these port numbers must be given to the Network Manager to ensure there are no other devices on the network using these ports.

Using a telnet session it is possible to telnet to a specific port to obtain debug information, for example at the prompt enter:

Telnet <IP address or unit> 5201

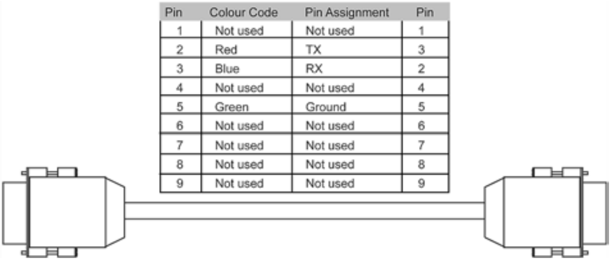
This will download debug information on the Engineering port, the following is an example of the information obtained:



```
4897519: F_SERVER: download relays.html
4897809: F_SERVER: download schedule.html
4898320: F_SERVER: download serial_ports.html
4898836: F_SERVER: download std_rec.html
4899321: F_SERVER: download system_features.html
4899612: F_SERVER: download system_logs.html
4902997: F_SERVER: download text_in_images.html
4903548: F_SERVER: download var_rec.html
4904017: F_SERVER: download vmd.html
4904538: F_SERVER: download vssver.scc
4904678: F_SERVER: download watermarking.html
4905219: F_SERVER: download webcam.html
4906601: F_SERVER: download alarm_inputs.html
4907212: F_SERVER: download alarm_zones.html
4907737: F_SERVER: download audio.html
4908023: F_SERVER: download camera_setup.html
4908534: F_SERVER: download camera_setup_adv.html
4908824: F_SERVER: download confirm_shutdown.html
4909125: F_SERVER: download database.html
4909435: F_SERVER: download ftp.html
4909926: F_SERVER: download holidays.html
4910226: F_SERVER: download hosts_profiles.html
4910746: F_SERVER: download img_unprotection.html
4911029: F_SERVER: download main.html
```

Appendix D –Unit Serial and Network Cables

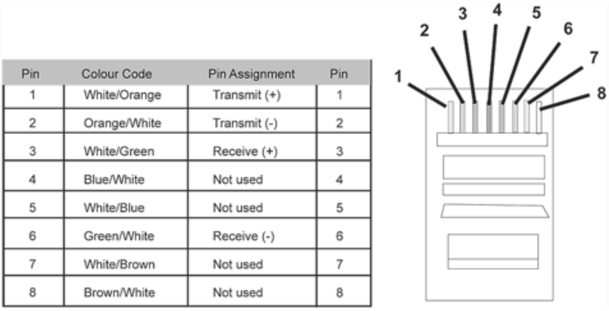
DM RS232 Debug Cable (supplied)



Pin	Colour Code	Pin Assignment	Pin
1	Not used	Not used	1
2	Red	TX	3
3	Blue	RX	2
4	Not used	Not used	4
5	Green	Ground	5
6	Not used	Not used	6
7	Not used	Not used	7
8	Not used	Not used	8
9	Not used	Not used	9

The RS232 Debug cable can be used to connect the PC serially to the unit for configuration using a terminal application (such as HyperTerminalTM).

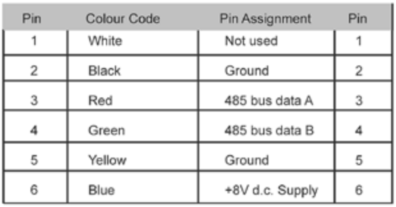
Straight-through Network Cable



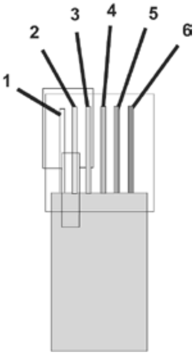
Pin	Colour Code	Pin Assignment	Pin
1	White/Orange	Transmit (+)	1
2	Orange/White	Transmit (-)	2
3	White/Green	Receive (+)	3
4	Blue/White	Not used	4
5	White/Blue	Not used	5
6	Green/White	Receive (-)	6
7	White/Brown	Not used	7
8	Brown/White	Not used	8

A straight through network cable connects hosts to network devices; PC to switch, unit to Switch.

DM 485 Bus Cable (supplied)

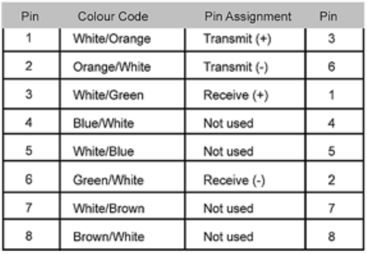


Pin	Colour Code	Pin Assignment	Pin
1	White	Not used	1
2	Black	Ground	2
3	Red	485 bus data A	3
4	Green	485 bus data B	4
5	Yellow	Ground	5
6	Blue	+8V d.c. Supply	6

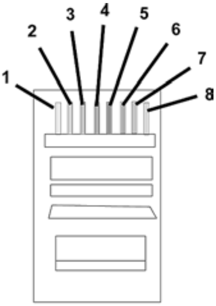


The DM 485 Bus cable is supplied for connectivity to peripheral DM devices such as Alarm Modules and Relay Modules.

Cross Over Network Cable

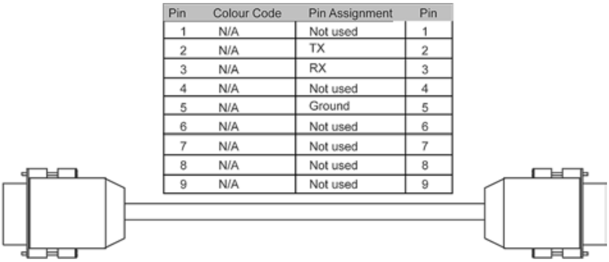


Pin	Colour Code	Pin Assignment	Pin
1	White/Orange	Transmit (+)	3
2	Orange/White	Transmit (-)	6
3	White/Green	Receive (+)	1
4	Blue/White	Not used	4
5	White/Blue	Not used	5
6	Green/White	Receive (-)	2
7	White/Brown	Not used	7
8	Brown/White	Not used	8



A cross over network cable is used to connect hosts to hosts or network equipment to network equipment, switch to router, PC to unit.

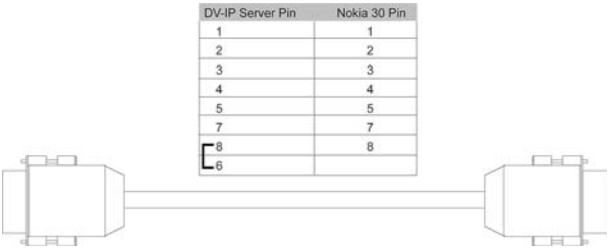
DM RS232 Null Modem Cable



Pin	Colour Code	Pin Assignment	Pin
1	N/A	Not used	1
2	N/A	TX	2
3	N/A	RX	3
4	N/A	Not used	4
5	N/A	Ground	5
6	N/A	Not used	6
7	N/A	Not used	7
8	N/A	Not used	8
9	N/A	Not used	9

The null modem cable can be used to connect ancillary devices that require 'handshaking' such as modems, GSM, etc.

Nokia 30 Cable



DV-IP Server Pin	Nokia 30 Pin
1	1
2	2
3	3
4	4
5	5
7	7
8	8
6	

This cable is for use from the unit to the modem only.

Appendix F – SMS Message Format

The unit supports GSM communications and SMS messaging. This allows the unit to report events via SMS and to receive SMS messages in order to create events on the system.

Command Format

The commands consist of a descriptor followed by a variable parameter list. The order in which the parameters appear must follow the format detailed below.

SMS Commands

These are messages that are sent to the unit to force an event to be triggered on the unit. These messages can be sent from a mobile phone or an Internet Service Provider (ISP) supporting SMS messaging.

Callback

This command is used to force the unit to make a connection to an Alarm Receiving Centre where the telnet listener (telserve) application is running.

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

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

SMS Reports

These are messages sent from the unit to a pre-defined SMS Server when an event occurs. The ‘events’ that will initiate this function are configured within the unit configuration web pages.

Startup

An SMS message will be sent from the unit to the receiving station when the unit ‘starts up’.

```
STARTUP?<name>&<time>&<IP address>&<latitude>&<longitude>&<zone>
```

name	This is the system name configured on the unit.
time	This is the local julian time of the message. The julian time is the number of seconds since 00:00:01 hour on January 1st 1970. If the Verbose message option has been enabled on the unit this message will be in a human readable format.
IP address	This is the Ethernet IP address of the unit.
latitude	This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.
longitude	This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.
zone	This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

Alarm

This report is generated when an alarm is received on the unit.

```
ALARM?<name>&<time>&<lat>&<long>&<speed>&<course>&<zone>&<camera>&<title>
```

name This is the system name configured on the unit.

time This is the local julian time of the message. The julian time is the number of seconds since 00:00:01 hour on January 1st 1970. If the Verbose message option has been enabled on the unit this message will be in a human readable format.

lat This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

long This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

Speed This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

course This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

zone This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

camera This is the video input number that is directly associated with the alarm on the unit.

title This is the alarm title allocated to the alarm that forced the SMS message.

VMD

This report is generated when activity has been identified on the unit.

```
VMD?<name>&<time>&<lat>&<long>&<speed>&<course>&<zone>&<camera>&<vmd zone>
```

name This is the system name configured on the unit.

time This is the local julian time of the message. The julian time is the number of seconds since 00:00:01 hour on January 1st 1970. If the Verbose message option has been enabled on the unit this message will be in a human readable format.

lat This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

long This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

speed This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

course This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

zone This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

camera This is the video input number that is directly associated with the alarm on the unit.

vmd zone VMD zones are configured on the unit, this identifies the zone that has been activated to initiate the SMS message.

Camfail

This report will be generated if the unit identifies that any of the video inputs does not have a 1V peak-to-peak signal.

```
CAMFAIL?<name>&<time>&<lat>&<long>&<speed>&<course>&<zone>&<upper>&
<lower>
```

name
This is the system name configured on the unit.

time
This is the local julian time of the message. The julian time is the number of seconds since 00:00:01 hour on January 1st 1970. If the Verbose message option has been enabled on the unit this message will be in a human readable format.

lat
This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

long
This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

speed
This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

course
This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

zone
This parameter is not relevant to the unit and included to support other Dedicated Micros platforms.

upper
This identifies the bitmask of failed cameras 33 – 64.

lower
This identifies the bitmask of failed cameras 1 - 32.

Additional Information

Command Reference List

For use over an RS232 comms connection between the PC and the unit, using HyperTerminal.

1. Power down the unit and connect the RS232 communication cable between the COM port on your PC and COM1 on the rear of the unit.
2. On your Windows PC, from the Start menu, select Programs> Accessories> Communications> HyperTerminal and create a new connection using the COM port and the following settings:

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

3. Apply mains power to the unit. The green power LED will light on the front panel and debug information should appear in HyperTerminal as the unit starts up.
4. When the debug finishes, log on to the unit by typing +++ in HyperTerminal and press enter.
5. The following commands can now be typed in Hyperterminal, replacing <aaa.bbb.ccc.ddd>with the values assigned to the DVIP ATM. <ESC> denotes the Escape button on your keyboard, <ENTER> denotes the enter key on your keyboard.

Command line

Command	Description
<ESC> m\Ether_IP\xxx.xxx.xxx.xxx	Set IP address of the unit.
<ESC> m\subnet\xxx.xxx.xxx.xxx	Set subnet of the unit.
<ESC> m\gateway\xxx.xxx.xxx.xxx	Set gateway of the unit.
<ESC> m\status	Displays the status information or the unit; drive information, comm. Ports information, enabled telemetry, etc.
<ESC> m\serial_mode\comx\disabled	
Debug	
PPP	
Text	
Telem	This command will allow the serial ports to be set for a specific function.
	Replace the x with the port number and select from the list the option available (refer to the serial port section of this manual for allocated functionality for each port).
<ESC> m\security\Eng\Open	
Off	
Pass	Allows the security password for debug mode to be enabled (pass)or disable (off) on the unit.
<ESC> m\security\debug\Open	
Off	
Pass	Allows the security password for debug mode to be enabled (pass)or disable (off) on the unit.
ipcfg	Shows the IP address, subnet mask and gateway set on the unit.
TCP Ports	Displays the active TCP ports supported on the unit.

Contents

Accessing the Configuration Web Pages 21
Additional Information 120
A Digital Video Recorder 4
Alarm 118
Alarms and relays 12
Allocating an IP Address 17
Anonymous FTP Log 95
Appendix A 100
Appendix B – .ini Files 101
Appendix C – Port Assignment on the unit 112
Appendix D –Unit Serial and Network Cables 114
Appendix F – SMS Message Format 117
A quick overview of digital recording 9
Archive 99
Audio 11
Audio Trace 92
Before you start 9
Calculating recording time 10
Callback 117
Camera Adjustment 90
Camfail 118
CE Mark 8
Check the contents of the box 9
Choosing a location for installation 9
Command Format 117
Command Reference List 120
Configuring the Network Settings of the unit 28
Connecting Power 16
Connecting serial devices 15
Connecting the Mounting Brackets 14
Connecting to the Network 15
Connecting Video Sources 15
Connection Log 95
Connectivity 35
Connect Monitor 14
Cross Over Network Cable 115
Data 11
Default Settings 78
Design of the manual 6
DM 485 Bus Cable (supplied) 115
DM RS232 Debug Cable (supplied) 114
DM RS232 Null Modem Cable 116
E-mail Log 96
Editing Camera Profiles 39
Editing the ini Files using FTP Client Application 101
Enabling DHCP 17
Front Panel 12
FTP Download Log 97
Hard disk capacity 10
hosts 106
hosts and profiles 104
How to Configure Alarm Presets 58
How to Configure an Alarm Schedule 75
How to Configure Connect/ Dial, FTP, SMS and Email on Alarm 60
How to Configure Connect/Dial on Alarm 60
How to Configure Email Settings 71
How to Configure FTP Settings for Archiving Images 65
How to Configure Global Parameters 22
How to Configure Matrix Control 34
How to Configure Profile Recording 37
How to Configure SMS Text messaging 67
How to Configure Text in Image Functionality 78
How to Configure the Alarm Database 74
How to Configure the Onboard Firewall 81

How to Configure the Relay Connections ... 59
How to Configure the Remote Alarm Host Information ... 62
How to Configure the Video Inputs for VMD and Activity ... 43
How to Configure the Webcam functionality ... 87
How to Configure Video Inputs and Standard Record Settings ... 25
How to Configure Watermarking ... 85
How to Enable and Configure Alarms ... 52
How to Enable and Configure PPP via Serial Port ... 61
How to Enable Audio Recording ... 42
How to Enable Serial Telemetry ... 32
How to Enable System Features ... 23
How to Enable System Logs ... 84
How to force the unit into another operating mode (Day/Night/Weekend) ... 76
How to Protect or Un-protect Images ... 72
How to Select and Enable Coaxial Telemetry ... 31
Image quality ... 10
Important Safeguards ... 7
Installing the Unit ... 9
Instructions for switching between the Sun JVM and Microsoft VM using the Java Control Panel: ... 13
Introduction ... 3
IP Address Range and Subnet ... 83
JPEG Profiles ... 40
LED’s ... 12
LED’s ... 12
Lightning Strike ... 7
Locating the DHCP Allocated IP Address ... 18
Logfile ... 98
Logfile Backup ... 98
Main Menu ... 21
modems.ini ... 107
modems.ini, USER.ini, Vidcfg.ini, WEBUSER.ini ... 104
MPEG4 Profiles ... 39
Network Configuration ... 20
Nokia 30 Cable ... 116
Notes on MultiMode Recording ... 37
paths.ini ... 108
Port Allocation ... 112
Power Sources ... 7
Read Instructions ... 7
Rear Panel connections ... 11
Refer all servicing to qualified service personnel. ... 7
Regulatory Notes and FCC and DOC Information ... 7
Relay Test Page ... 92
Reset ... 93
reset (to restart the DV-IP ATM) ... 18
Reset using Telnet ... 100
Reviewing the Unit Logs ... 94
RS422 Connectivity ... 16
Security Log ... 96
Selecting the Profile for Each Camera ... 41
Sent Message Log ... 97
Servicing ... 7
Setting a static IP address ... 17
Simple Configuration ... 22
Simple Installation ... 11
SMS Commands ... 117
SMS Message Format ... 70
SMS Reports ... 117
Standard record rate ... 10
Startup ... 117
Straight-through Network Cable ... 114
Structure of the Files ... 106
Supported Modems ... 61
System Logs Setup ... 94
System Variable ... 93
Telemetry Setup Page ... 31
Telemetry Setup Page ... 34

Tools 90
Tools Required.......... 14
To switch between the Sun JVM and Microsoft VM using Internet Options: 13
Typical Voltage Ratings 9
USER.ini 109
Using the Profile Wizard 38
Ventilation 7
vidcfg.ini.......... 109
Video 11
Video Scope 91
View Profiles.......... 40
VMD..........118
Walk Test 51
Watermarking 93
Web Page Icons 20
WEBUSER.ini..........111

DEDICATED MICROS

Dedicated Micros Ltd.
1200 Daresbury Park, Daresbury,
Cheshire, WA4 4HS, UK
Tel: +44 (0) 845 600 9500
Fax: +44 (0) 845 600 9504

Dedicated Micros Europe
Neckarstrafle 15,
41836 Hückelhoven, Germany
Tel: +49 2433 5258-0
Fax: +49 2433 5258-10

Dedicated Micros France
9-13 rue du Moulinet
75013 Paris, France
Tel : +33 (0) 1 45 81 99 99
Fax : +33 (0) 1 45 81 99 89

Dedicated Micros Slovenia
Delavska cesta 26,
4208 Sencure, Slovenia
Tel: +386 4279 1890
Fax: +386 4279 1891

Dedicated Micros Benelux
Joseph Chantraineplantsoen 1,
3070 Kortenberg, Belgium
Tel: +32 2751 3480
Fax: +32 2751 3481

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

Dedicated Micros USA.
23456 Hawthorne Blvd.
Suite 100, Torrance,
CA 90505, USA
Tel: +1 310 791-8666
Fax: +1 310 791-9877

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

Dedicated Micros, Asia PTY
16 New Industrial Road,
#03-03 Hudson Techno Centre,
Singapore 536204
Tel: +65 62858982
Fax: +65 62858646

Dedicated Micros Middle East
Building 12, Suite 302, P.O. Box 500291, Dubai Internet
City, Dubai, United Arab Emirates
Tel: +971 (4) 390 1015
Fax: +971 (4) 390 8655

Dedicated Micros (Malta) Ltd.
BLB017, Bulebel Industrial Estate,
Zejtun, ZTN08, Malta
Tel: +356 21483 673
Fax: +356 21449 170   Fax: +356 21449 170

NetVu CONNECTED