FireVu Detector Standalone Installation Manual

FV/MAN/003/4

Version History

Issue Number	Date	Comments
DRAFT Version 1.0	23rd March, 2018.	Author – R S Hawes
DRAFT Version 1.01	9th August, 2018.	Author – R S Hawes
DRAFT Version 2.0	5th March, 2020	Author – P Ridgeon
DRAFT Version 3.0	6th January, 2021	Author – P Ridgeon
DRAFT Version 4.0	15th July, 2021	Relay detail updated

Copyright Notice

Copyright © 2015 - 2021 NetVu Ltd. All rights reserved.

NetVu Ltd. copyrights this manual and the products it describes. Express permission from NetVu Ltd. is required before any part of this manual is reproduced, transcribed or stored in any electronic device.

This manual is intended for use by authorised representatives of NetVu Ltd. and it must not be distributed to any unauthorised person.

This manual covers the FireVu product ranges and is effective as of 5th March 2020.

It supersedes all previous manuals and instructions.

IMPORTANT
READ CAREFULLY BEFORE USE
KEEP FOR FUTURE REFERENCE

Preamble

For the avoidance of doubt and for the purposes of this manual, “camera” and “detector” are defined as meaning the same thing.

Feature	FireVu Multidetector	FireVu Detector
Flame Detection	✔	✔
Smoke Detection	✔	✔
Detects both indoor and outdoor	✔	✔
Dynamic Masking	✔	✔
Exclusion Masking	✔	✔
Video Management Software Included	✔	✔
Secure Alarm Transmission	✔	✔
Watchdog Function	✔	✔
Event logging	✔	✔
Internal Recording	✔	✔
Heat Detection	✔	☐
Two built-in dry-contact outputs (allowing stand-alone use as inputs to a fire alarm system).	✔	✔

Contents

Version History 1
Copyright Notice 2
Preamble 2
Contents 3
Important Safeguards 6
Read Instructions 6
Power Sources 6
Servicing 6
Ventilation 6
FCC Information 6
FCC Conditions 7
CE Mark 7
Introduction 7
Background and Overview 8
FireVu Detector Features 8
Additional FireVu Multi-Detector Features 9
Quality 9
Warranty 9
Restrictions on Use (Intended User) 9
Input Voltage 10
Energy Consumption 10
Noise 10
Limitations of Liability 10
Intended Use 10
Hazards 10
Safety Notes 11
Transport and Storage 11
Installation 12
FireVu System Installation Flow Diagram 12
Before you start check the contents of the box 13
First Fix – Physical Installation of FireVu Detectors 14
Principle of Operation 14
Appropriate Applications for FireVu 14
Situations to avoid when using FireVu 15

Environmental Considerations 16
Detector Lens Selection 16
Detector Positioning 16
Covering the “Risk Area” 16
Height 18
Angle of Detector 18
Ensuring maximum useable view 18
Avoiding problematic areas wherever possible 19
Lighting 19
Artificial lighting, including IR. 19
Other lighting 20
Background of Image when using detectors externally 20
Second Fix – Cabling and Connection of Standalone FireVu Detectors 20
Cabling Requirements 20
Wiring Block Diagram – Single Standalone FireVu Detector 21
Wiring Block Diagram – Up to Four Standalone FireVu Detectors 22
Remote access 23
Individual FireVu Detector Connections and Wiring 24
Relay Outputs and Alarm Inputs 25
Configuring Relay Outputs #2 and #3 25
Relay #1 – Alarm/Fault Relay 26
Post-Wiring and connection tasks 28
Configuration 29
Basic Configuration / Pre-Commissioning 29
Initial Settings 29
Viewing Detector Video Images 34
Pre-Commissioning Checklist 36
Remote Commissioning and System Sign-Off 37
On-Site Smoke Testing 37
Equipment Needed 37
Process 38
On-Site Flame/Thermal Testing 43
Using Telnet to Simulate Smoke/Flame/Thermal Detection 43
Observing Smoke/Flame/Thermal detections using Enterprise Observer 46
Advanced Configuration 47
System Web-pages 48
System – Attributes Page 49
Attributes 50

Status Page 51
Upload Page 53
Time and Date 54
User Accounts 55
Maintain 56
Features 57
Camera Web-pages 58
Camera Setup Web-page 59
Record Settings Web-pages 59
Video Storage Web-page 60
Alarm Web-pages 60
Alarm – Expression Wizard Page 61
Alarm – Expressions Editor page 63
Alarm – Activity page 64
Alarm – VMD Setup page 66
Alarm – Schedule page 67
FireVu Dashboard Web-pages 68
Parameters Web-page 68
VSD Setup and Pre-Processor Web-pages 68
Flame Web-page 68
Thermopile Web-page 70
Thermal Setup Web-page 71
Fault Warning Web-page 72
Regions Web-page 75
Regions Web-page 77
Exclusions Web-page 78
Frame Analysis Web-page 79
Frame Analysis Web-page 81
Network Web-pages 82
Setup Web-page 83
Email Web-page 84
Multicast Web-page 86
Firewall Web-page 87
ARC Configuration Web-page 87
Profile Setup Web-page 89
Live Viewer Page 90
Fault Finding, Maintenance and Support 90
Fault Finding 90

Detector cannot be found or viewed 90
Maintenance 91
Accessories, Consumables and Spare Parts 92
Safe disposal When Expired 93
Other Related Documents 94
Glossary 95

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.

FCC Information

(USA and Canadian Models Only)

This equipment has been tested and found to comply with the limits for a Class B 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.

FCC Conditions

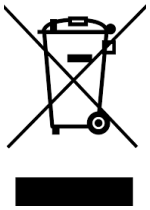
(USA and Canadian Models Only)

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference
2. This device must accept any interference received, including interference that may cause undesired operation.

CE Mark

This product and – if applicable – the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC directive 2014/30/EU.



This 2012/19/EU (WEEE Directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of new equipment, or dispose of it at designated collection points.

Introduction

FireVu from NetVu Ltd, innovators in Video Smoke Detection (VSD), is an advanced embedded VSD server.

FireVu overcomes detection challenges such as smoke stratification, varying air flow and contaminated environments. FireVu "sees" the source of smoke or flames or both, identifying them anywhere within its field of view at any height or direction of flow.

"At source detection" is faster than other forms of detection as there is no need to wait for the smoke to reach the detector. It works by analysing the video information it generates within the FireVu processing system where extensive algorithms are used to analyse movement. The system will alarm should the motion patterns be recognised as smoke or flames, or both. Each FireVu detector can simultaneously identify smoke using up to 16 separate detection zones per detector.

The FireVu Multi-Detector provides all the same capabilities as the other FireVu detectors with regards to visual fire detection and also has the ability to detect the presence of heat within the detector's field of view by means of its in-built thermopile sensor.

In addition to the normal visual images the FireVu Multi-Detector produces a thermal image which over-laid onto the visual image, the system's sophisticated software then determines where in the visual image any heat signatures exist. An absolute threshold for temperature detection can be set for various areas within the detector's field of view, which is able to detect temperatures from -30°C to +300°C.

The thermal detection capabilities can be configured to be used in one of two ways:

- As a Double-Knock solution whereby the detector needs to see both a visual indication of fire and a heat signature in the same area of the detectors field of view.
- As a stand-alone method of generating an alarm based on an item within the detectors field of view reaching or exceeding a predetermined absolute temperature threshold. This can be implemented to detect fire or as a means of process monitoring.

Background and Overview

The processing is completely self-contained within the detector and drives the sensor directly by a sophisticated sequence of controlled exposures. This allows a direct correlation of Black Body colours and intensities to reliably determine the presence of a flame.

The Multi-Detector adds a thermal sensing array, providing for sensor determination of absolute temperature in 0.1 degree Celsius increments for identifying hot areas within an image, for either an independent thermal threshold, or as further validation of a Flame or Smoke source to qualify against a maximum threshold.

FireVu Detector Features

FireVu is equipped with an array of valuable features designed to provide the End User with a secure system of unrivalled performance.

- Custom embedded Smoke and Flame detection algorithms.
- Visual confirmation of any alarm.
- Integrated Camera Recording and full enterprise video server within the detector.
- Camera recording up to 4CIF resolution, 540TVL, 25pps.
- Multi-Mode Recording - Dynamically-switchable resolution, record-rate and compression, (MPEG4/JPEG).
- Transmission of multiple, simultaneous video streams in MPEG-4 and JPEG format enables multiple users to view video streams at the settings they require.
- Easy remote configuration Web-pages.
- Internal video storage in each detector.
- Up to 16 configurable detection zones.

- Evidential quality event recording.
- Live and playback viewing locally and over Ethernet.
- Easy to use on-screen, colour coded "soft-key" menu options.
- Meets BS 5839 part 1 requirements.
- Colour IP Camera with excellent low light sensitivity.
- 0.3 lux F1.2 40 IRE.
- Power over Ethernet (PoE), or PoE/12VDC/24VAC.
- Local analogue test monitor output for use when positioning and adjusting the camera's field of view and focus.
- Alarm reporting using four on-board solid-state relays and/or monitored loop operation.

Additional FireVu Multi-Detector Features

- Built in Thermopile sensor providing absolute temperature measurements.

Quality

NetVu Limited's manufacturing arm (Dedicated Micros, Malta) has ISO 9001 certification and all products are manufactured and tested in accordance with a comprehensive quality system.

Warranty

FireVu product comes with a one-year warranty. FireVu is sold under a return-to-base upon any failure agreement. Any returned product must be returned in the original packaging in accordance with NetVu Limited's return process, under which all returns are first approved, a materials returns reference number issued, and then the equipment can be returned to NetVu Limited's service facility with the returns number clearly displayed.

Restrictions on Use (Intended User)

The equipment is intended for use in non-domestic premises by suitably trained and qualified persons of at least 16 years of age. It should be protected from extremes of heat, cold, humidity, ultraviolet, infrared and all forms of ionising radiation. It should be used in a well-ventilated area and if used in a hostile environment, protected from the ingress of dust and liquids by a suitable ventilated enclosure. With the exception of FireVu detectors, all FireVu equipment is for indoor use only.

Minimum Operating Temperature:	-10°C (14°F)
Maximum Operating Temperature:	50°C (122°F) FireVu Detectors
Operating Humidity:	20% to 90% Relative Humidity (Non condensing)
Minimum Lighting:	20lux
Maximum Lighting:	150,000lux

Input Voltage

FireVu Detector and Multi-Detector: 12-15VDC or PoE Class 3.

Energy Consumption

Multi-Detector: 8W

Noise

FireVu equipment are solid state devices and should not emit any audible noise under normal operating conditions.

Limitations of Liability

FireVu must be installed and configured in accordance with NetVu Limited's instructions. NetVu Ltd. cannot be held liable for any incidental or consequential damages resulting from loss of property or damages due to misuse of NetVu Ltd. products.

Errors and omissions excepted (E&OE). NetVu Limited assumes no responsibility for errors or omissions within this document.

NetVu Ltd. reserve the right to make product improvements at any time.

If in any doubt whatsoever, please contact NetVu Limited to confirm that your understanding is correct.

Intended Use

The FireVu detectors can be deployed as a stand-alone visual detector or as part of a FireVu Internet Protocol (IP) system.

It is NOT intended that the FireVu detector itself be utilised to handle the alarm outputs and perform the final annunciation within a Fire Detection System. This function should be performed by the Fire Alarm Control Panel (FACP).

NOTE: It is extremely important that the F-stop Iris adjustment is not altered from the "as supplied" setting, as this is part of the calibration for Flame Detection.

NOTE: It is also important that the correct lens is selected on each detector, under " FireVu Dashboard", "Flame".

The requirements for smoke, flame or thermal event detection often conflict with security requirements for a CCTV camera. Consequently, NetVu Ltd. advise against detectors being used for a dual security and Visual Smoke Detection (VSD) purpose.

This equipment MUST NOT be modified in any way, shape or form except by a trained NetVu Ltd. Engineer or agent with express permission from NetVu Ltd.

Hazards

Electric Shock. FireVu units are low voltage equipment. However, they may be supplied with

power supplies which if misused or incorrectly installed could present an electric shock hazard. FireVu equipment must only be used with the power supply provided and the power supply must be installed in accordance with local regulations by suitably qualified persons.

Manual handling. FireVu equipment is robustly constructed and can be heavier than it looks. Suitable precautions MUST be taken when handling them to prevent personal injury. They must only be installed in accordance with local regulations by suitably trained and qualified persons.

Safety Notes

With the exception of FireVu detectors, all FireVu equipment is for indoor use only. FireVu equipment is robustly constructed and can be heavier than it looks. Suitable precautions MUST be taken when handling them to prevent personal injury. They must only be installed in accordance with local regulations by suitably trained and qualified persons.

Note: Before deciding upon a position for Video Smoke Detection detectors the potential fire hazards must first be identified. The client or consultant will need to perform the risk assessment and identify the nature and area of risk within the detector field of view.

A FireVu installation is intended for use as an automated early warning system and not as a primary protection method, except where no other detection method is practicable. An in-depth knowledge of the monitored area and fire risk is required to use FireVu effectively.

FireVu should not be used as a direct means of activating any fire suppression equipment. NetVu Limited require that there must be human visual verification before any suppression equipment is activated. The operator must have the ability to quickly raise the alarm, initiate the fire evacuation procedure and activate fire suppression equipment as appropriate. Consequently, it is strongly recommended that a break-glass call point be sited within easy reach of the VSD monitor operator.

Transport and Storage

NetVu products are securely packed, using appropriate materials which are recyclable where reasonably practicable. However, the products contain delicate electronic equipment and should be handled with due care and attention.

Ensure that all cartons or boxes are the right way up before opening them at the indicated point.

Keep the original packaging for the duration of the warranty period, in case any item should need to be returned.

When no longer required the packaging should be reused, recycled, or disposed of in accordance with local waste disposal arrangements and regulations.

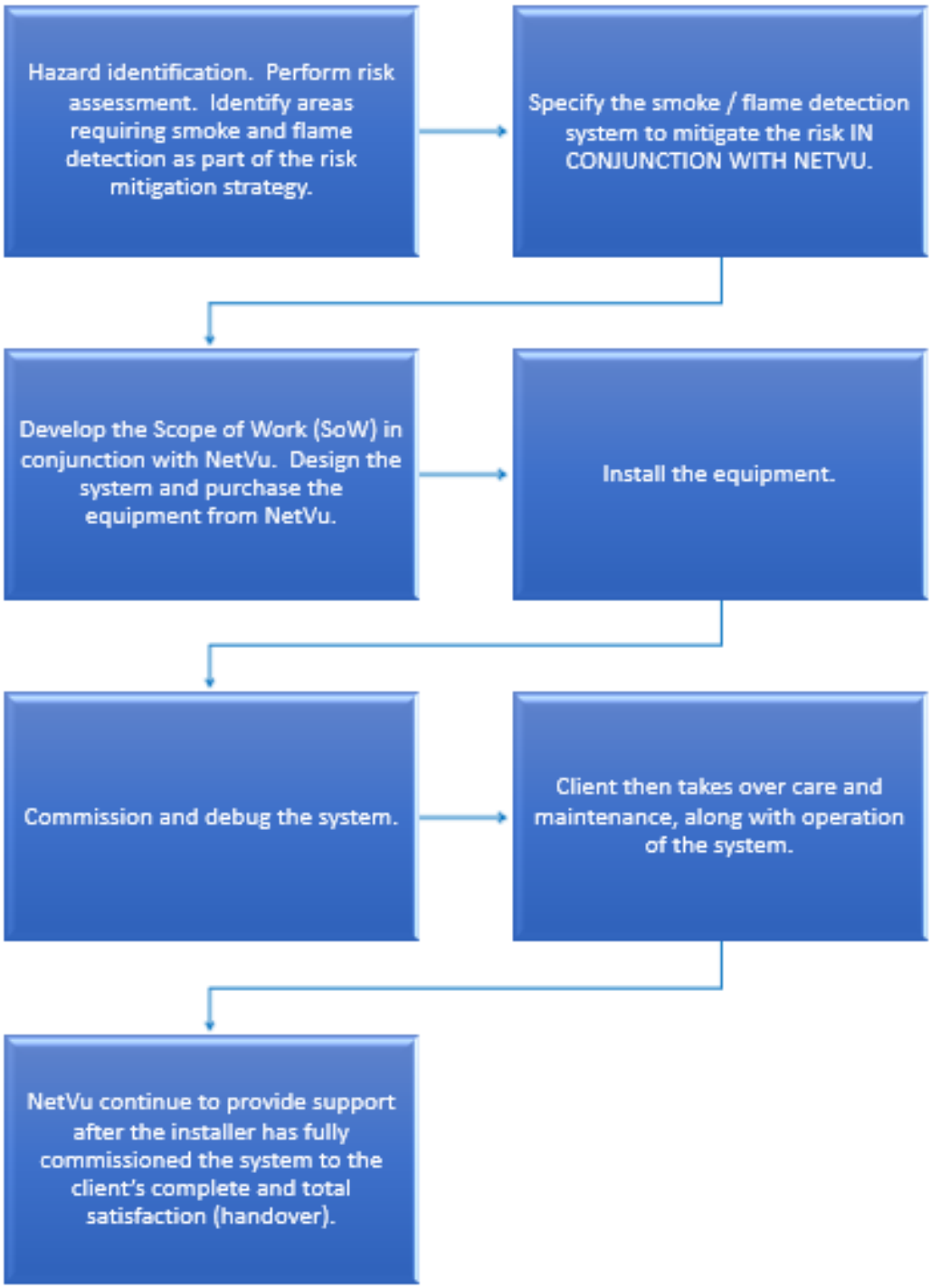
These products must only be stored indoors, with their environment being maintained within the limits outlined below.

Minimum Storage Temperature	-10°C (14°F)
Maximum Storage Temperature	70°C (158°F)
Storage Humidity	20% to 90% Relative Humidity (Non condensing)

Installation

Each Installer will have a specific "Scope of Work" (SoW) document issued to them by NetVu Limited. The SoW should be consulted for the specific details pertinent to each individual installation.

FireVu System Installation Flow Diagram



Before you start check the contents of the box

The box should contain the following items:

- FireVu Detector
- Swivel
- Wall Mount Bracket
- Sunshield

Installation Accessories:

- Wall Mount Bracket Gland
- Wal Mount Bracket Drilling Template
- Rawl Plugs and Screws
- Sunshield fixing screws
- Allen Key
- Silica Bag
- Free Extended Warranty Registration Reminder Card

First Fix – Physical Installation of FireVu Detectors

Principle of Operation

The FireVu detectors are autonomous devices capable of recognising smoke, a flame or a thermal event in a video image and alerting the system user on a connected PC VDU, or Annunciator connected monitor, or by a variety of remote outputs.

Alarm conditions are stored within the FireVu detector's log.

The FireVu detectors use patented Black Body Emissivity analysis technology, alongside flicker detection, to quickly detect the presence of a flame.

The system also rapidly detects smoke by looking for small areas of change within the image at the digitisation stage and only passing these pixel changes to the main processor for further filtering. The video information is passed through a series of filters which seek particular characteristics which can be associated with smoke. Further analysis is then carried out on the relationships between the filtered characteristics to determine whether all the conditions have been met for the system to confidently predict the presence of smoke.

To provide compensation for areas of the image which would otherwise prove troublesome, such as windows or smoke or steam producing processes, part of the image can be eliminated from detection by use of masks. The masks are user defined and can be fixed on a per pixel basis (Exclusion Masking) or on a colour detection basis (Dynamic Masking), or both.

The FireVu detector has four solid-state relays that can be configured to operate in the event of an alarm. These can be hard-wired to the Client's Fire Alarm Control Panel (FACP), or Building Management System (BMS), or both.

Appropriate Applications for FireVu

FireVu can be deployed as an effective detection system in almost all environments. Consequently, any decision not to utilise FireVu is usually as a result of the lower cost of conventional technology being able to provide an appropriate solution and not because of any technical shortfall with

FireVu.

Conversely, there are applications where cheaper more conventional solutions simply cannot offer an effective detection solution and here FireVu is often the best or even the only viable solution.

Such environments and applications include, but are not restricted to:

- Any area with very large air spaces where smoke will stratify before reaching ceiling mounted detectors or high-up beam detectors.
- Any area with large amounts of complex machinery.
- Any area of machinery that produces an oil haze or that is too hot for point detection.
- Outdoor applications.
- Any area which cannot support other forms of early detection for aesthetic reasons.
- Any area where an intrusive form of detection cannot be used and detectors can only be installed where they would need to look through viewing glass, for example in hazardous or radioactive areas. It should be noted that a distorted image will not affect flame detection by FireVu detectors, so long as any glass is sufficiently transparent. However, the thermopile sensor in the FireVu Multi-Detector will NOT work through glass.
- Areas where chemical fires produce smoke which damages obscuration type detectors, (yellow phosphorous for instance produces an acid when mixed with moist air).
- Areas where health and safety requirements make the installation of conventional forms of fire detection difficult or expensive.

Situations to avoid when using FireVu

FireVu is a visual based Fire detection system and as a consequence any phenomena which share the visual properties of smoke, or results in pixel by pixel changes within an image similarly to smoke, will be identified as smoke by FireVu.

This does not mean there are environments where FireVu should not be used, but certain considerations must be taken as to whether a FireVu detector should be configured to monitor its entire view or whether a form of masking should be employed to “ignore” certain areas.

Below is a list of the types of areas where care needs to be exercised in deciding where to monitor:

- Where background smoke levels are very high such as welding processes or excessive diesel smoke from forklift trucks etc. (reasonable levels of background smoke can be tolerated).
- Lighting conditions likely to cause camera flare or saturation of the camera sensor.
- Where the detector is required to view through things such as mesh fences, blinds, railings, frosted glass and other items likely to obscure or cause deterioration of the image. It should be noted that a distorted image will not affect flame detection by the FireVu detectors, so long as any glass is sufficiently transparent. However, the thermopile sensor in the FireVu Multi-Detector will NOT work through glass.
- Lighting levels which are lower than the detector is capable of dealing with.

- Highly polished shiny floors, especially if combined with large openings where shadows and bright sunlight will cause reflections and large contrast changes.
- If using flame detection, the presence of flashing beacons or lights on fast moving vehicles will require a higher threshold setting to avoid false alarms. Consequently, there will be an increase in the minimum flame size that will be detected.

Environmental Considerations

Adequate lighting is required for the presence of smoke to be defined sufficiently for accurate VSD operation. Typically, a minimum of 20 lux of visible light is required. This is only required for the visual smoke detection. Both the visual flame detection and heat detection will work at any illumination.

Detector Lens Selection

The detection footprints defined further on within this section are based upon the assumption that for effective smoke detection 10% of the screen height would be occupied by the minimum amount of smoke that is required to be detected. This applies to the furthest point in the field of view where the user is intending that the detector in question will monitor and respond as required.

For practical purposes, a human target occupying 10% screen height at the furthest point is assumed to be a suitable size to produce good results, meaning that a smoke cloud will need to be approximately 2m (6 feet) high and 600mm (2 feet) wide at the furthest point within the monitored area before effective detection will take place. Consequently, a smaller smoke cloud will result in an alarm if closer to the detector.

Response distance for flame is based upon a need to respond in less than 30 seconds to a 330mm x 330mm x 50mm (13" x13" x 2") pan fire with 500ml (1.06 US pints) of N Heptane.

Detector Positioning

Detectors should be mounted on as firm a structure as possible. If large amounts of detector vibration are present, then the video image will have continuing large differences within it and the detection algorithms will be less effective. FireVu analyses changes within the video images it receives on a pixel by pixel basis. Consequently, if all pixels and constantly changing as a result of "camera shake" its sensitivity to changes as a result of smoke presence will be reduced.

Covering the "Risk Area"

Note: Before deciding upon a position for Video Smoke Detection detectors the potential fire hazards must first be identified. The client or consultant will need to perform the risk assessment and identify the nature and area of risk within the detector field of view.

If the risk is an identified item or area within the total area being monitored then the detector view should be set to maximise the size of that defined area whilst ensuring that all the required monitored items fit within the field of view. This requirement often conflicts with any CCTV requirements for a camera and as a result NetVu Ltd. advise against detectors being used for a dual security and Visual Smoke Detection (VSD) purpose.

Consideration must be given to any potential obstructions to the "risk area" being monitored. These may be either permanent, (pipe-work for example), or temporary, (vehicles or plant parked in times of non-operation). Although smoke will rise above and around such obstacles, it will reduce the FireVu's ability to identify it and increase the detection time, and may remove all chances of seeing any flame. Consequently, wherever possible, the detector should be given a clear direct line of sight to the "risk area".

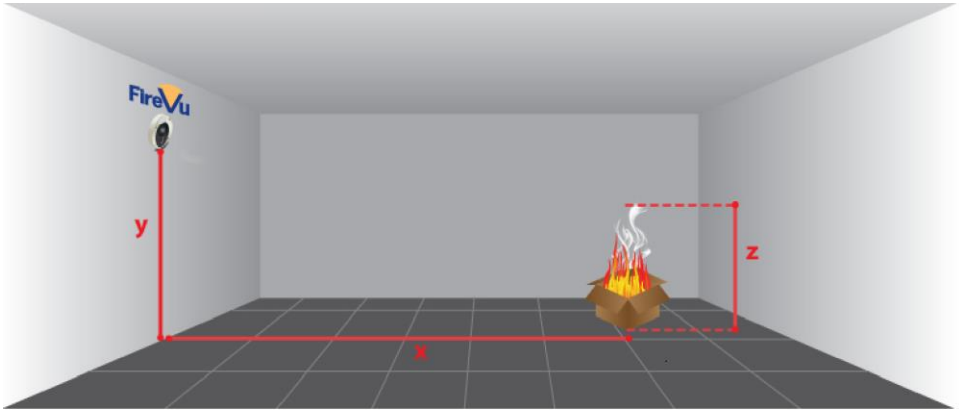
If the risk is identified as anywhere within the area then a sufficient number of detectors need to be used so that the entire area falls within the "useable" field of view of at least one detector and at least two if a "double knock" requirement is specified. As a minimum, neighbouring detector views MUST overlap to ensure the entire area is monitored.

It is advisable to have each monitored area covered from more than one aspect, and ideally from opposite sides, so that the area underneath a detector is covered by an opposing detector view.

Note: NetVu Ltd. recommend that wherever possible all parts of a risk area be covered by two detectors so "double knock" alarming can be utilised reducing the chances of a false alarm. This also ensures areas behind or below detectors are covered and that if a detector is obscured the area it is covering is still being monitored by another detector.

The "useable" field of view of the detector is that area within which a fire, or cloud of smoke, is considered large enough to result in an alarm. For flame detection, the flame needs to occupy only 1% of the height of the detector's view. In instances where flashing beacon are in use, or other fluctuating light sources oblige a reduction in the flame detection threshold to prevent false alarms, a flame will need to occupy 2% to 3% of the height of the detector's view.

For smoke detection, the smoke cloud needs to occupy at least 10% of the height of the detector's view. A cloud of smoke smaller than 10% of the height of the field of view of the detector may not be detected by the system. As the further away an incident is the smaller it appears, even a large plume of smoke may not be detected if it is so far away from the detector that it occupies less than 10% of the detector's view height.



Therefore, in the diagram above, if we assumed a 3.5mm lens, a fire could be 20 metres away (x) and still result in an alarm as long as "z" were 1% or greater of the detectors vertical field of view for flame, or 10% or greater of the detectors vertical field of view for smoke.

Height

The ideal scenario with VSD is to have the detector positioned such that if the view were split horizontally into two equal parts, all "traffic" would pass through only the lower half and the upper half would be sterile. Traffic refers to anything which may move through the field of view and is not always present, e.g. people, vehicles or machinery.

In an office space where the only traffic will be people the detector should be positioned between 2 and 3 metres from floor level, although this may be affected by the ceiling height. In larger, taller spaces the detectors can be positioned higher. The actual mounting height will depend on the expected traffic height and that of the building itself.

Care must be taken not to mount the detector too high, resulting in a need to point it downwards. "Not angling the detector down" is more important than "avoiding all movement". The FireVu algorithms "see" smoke rising and moving through the image. Consequently, the system will be less effective if looking down upon smoke rising towards the detector, as the movement appears differently.

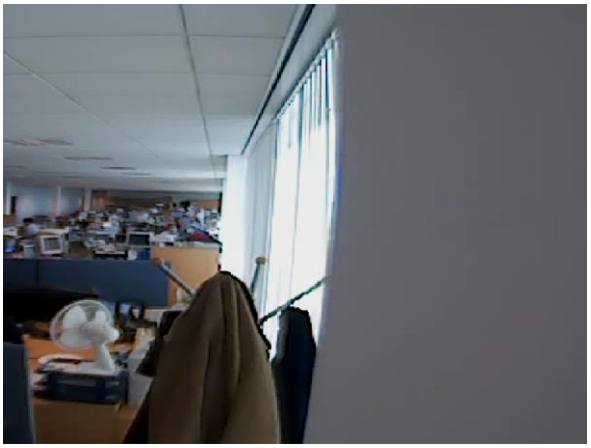
Angle of Detector

In order to achieve the criteria required to effectively split the detector view into a lower and upper half horizontally and any traffic moving through the scene be confined to the lower half, the detector must be looking out horizontally, otherwise traffic at a distance from the detector will cross the split and enter the upper half of the view.

The VSD system works by "seeing" smoke rise through the view, it does not detect smoke if it is rising up towards the detector or if the detector is looking down on the smoke. Consequently, if the detector is positioned at an angle of greater than 20 degrees it cannot be guaranteed to "see" smoke.

Ensuring maximum useable view

Example: In the view to the left, the detector has been positioned beside a pillar which effectively makes that area of the view useless.



When positioning detectors ensure that items or fixings mounted or positioned nearby do not unnecessarily come into the detectors view. For example, if mounted beside an air conditioning unit the detector may need to be bought forward so as to not see the side of that unit "up close".

Avoiding problematic areas wherever possible

This can be done with careful placement of the "detection regions" as well as using the "Exclusion masking" feature in the FireVu dashboard configuration tool. However, it is worth considering these issues at least in part when positioning the detectors.

In cases where these aspects cannot be avoided from being within the detector's field of view, but do not need to be monitored, then we can ignore them by arranging the analysed regions so as not to cover those parts. In cases where the problem area is small or irregularly shaped we can exclude it using the manual fixed "exclusion mask" feature within the FireVu dashboard configuration tool.

Lighting

Areas of the view where there will be significant changes in light during the course of the day or year can be difficult to configure to see smoke in the differing conditions and not false alarm with the changes in those conditions, if those changes result in such a variety of lighting within a single detector view that in order to accommodate the darker areas the brightest areas saturate the detector's sensor.

The easiest way to ensure a stable and reliable configuration which will work well all day long and year-round is to avoid having certain areas within the "detection regions".

Examples of these are:

- External detectors which point due east or west as the sun will come into view at either dusk or dawn.
- External doors and windows which may be left open allowing light to stream in, both the opening itself and the area onto which light will shine should be considered.
- Roller shutter or hanger doors; where possible detectors should be positioned to be looking into the building rather than internally looking towards the doors which would result in looking out of the building in periods when those doors are opened.

Artificial lighting, including IR.

If 24-hour operation of the VSD system is required, the detectors will need to be able to "see" at all times. Consequently, the monitored areas must be lit either by leaving sufficient lights on or fitting IR lighting specifically for the purpose. When fitting either the lighting or the detectors, (subject to which came first or other restrictions), care should be taken so as to avoid any detector looking directly into any of the lighting.

Note: NetVu Ltd. recommend the use of 850nm IR flood lighting with 60 degree spread of light to

a length sufficient to cover the room being lit.

Other lighting

If using flame detection, the presence of flashing beacons and other fluctuating sources of bright light, will require a higher threshold setting to avoid false alarms. Consequently, there will be an increase in the minimum flame size that will be detected.

Background of Image when using detectors externally

The detector should be positioned to give as sterile a view as possible behind the "risk area", particularly when looking for smoke rather than flame. Continual movement in the background will require setting a greatly reduced sensitivity of the smoke detection parameters, in order to avoid false alarms.

Examples of phenomena to avoid are:

- Large areas of sky (distant clouds can be easily mistaken as smoke by the system and so areas of sky should not be monitored).
- Machinery and natural phenomena which may emit visible steam.
- Plant that emits smoke.
- Visible air-borne particles.

Second Fix – Cabling and Connection of Standalone FireVu Detectors

By definition, a standalone FireVu detector is one where less than four detectors are used on an individual site and where FireVu Annunciators and FireVu Network Extenders are not used. This section of this manual describes the cabling and connections in this circumstance. For FireVu systems large than four detectors different methods apply and these are described in the FireVu Systems Installation Manual FV/MAN/002

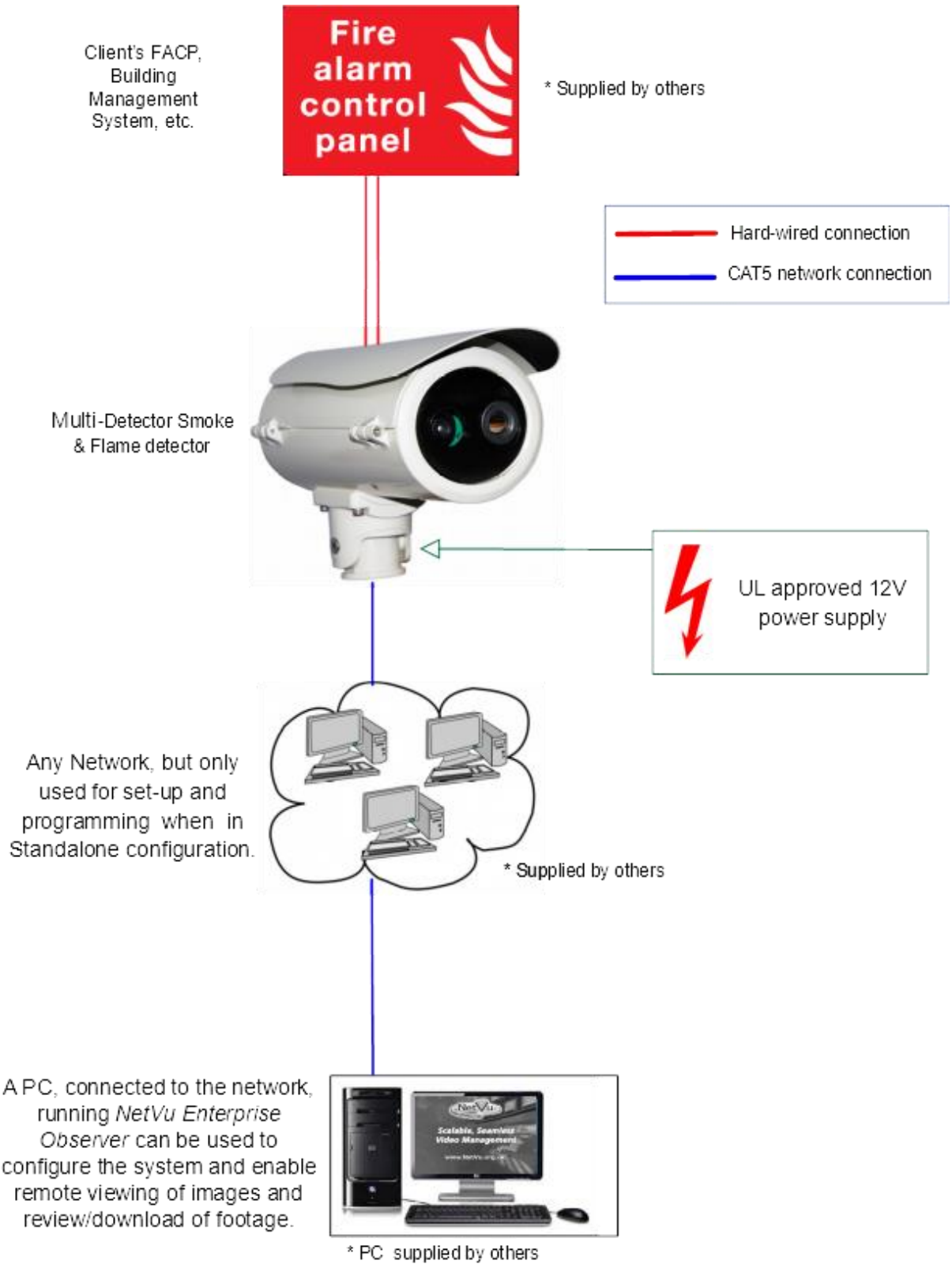
Cabling Requirements

Detectors should be cabled in the normal way using fireproof CAT5 suitable for the lengths of run involved.

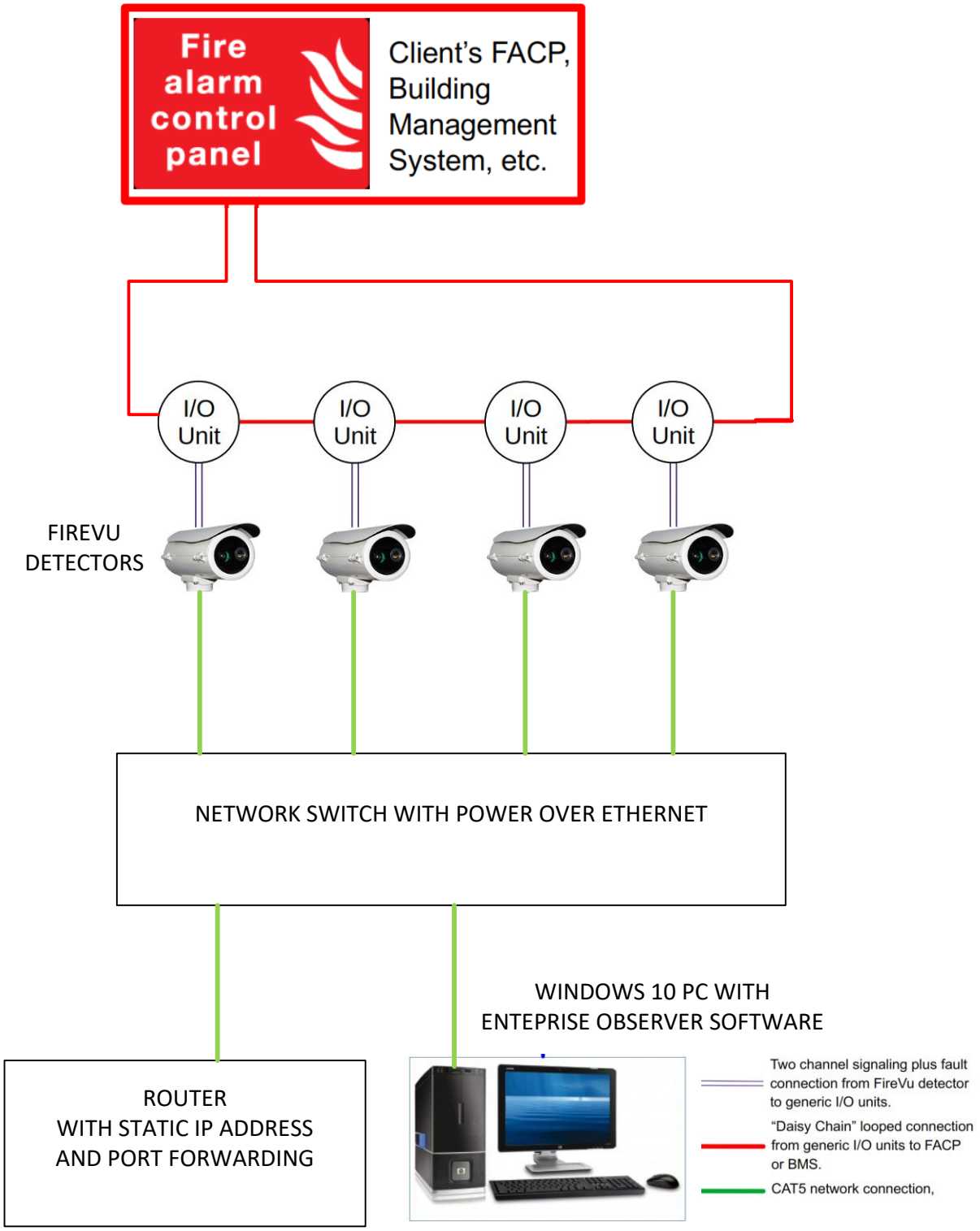
It is recommended that any other connection between the FireVu and the items to which it is networked, (or if appropriate, the FACP) should also be run in appropriate fireproof cabling.

Typical block diagrams for FireVu detectors being used in standalone applications are shown on the next two pages.

Wiring Block Diagram – Single Standalone FireVu Detector



Wiring Block Diagram – Up to Four Standalone FireVu Detectors



Note: Local power supplies may be used for the FireVu detectors as an alternative to Power-over-Ethernet (PoE) if preferred, or if required by local regulation.

NetVu Ltd. do not supply UPS or battery backup equipment. However, it is strongly recommended that provision for such be made and a suitable means of ensuring continued operation of the FireVu system in event of a power failure. This must cover all required aspects of the system and not just the FireVu detectors, lighting and storage devices must also be supported. NetVu Ltd. will provide data on power consumption requirements on request.

Remote access

For any other installation other than where FireVu detectors are required to provide flame detection qualified thermally ONLY i.e. For all cases where FireVu smoke and flame detectors are to be used and for all cases where video smoke detection is required, provision of remote direct IP access to the FireVu system to allow for commissioning configuration and technical support is mandatory. Such support may come direct from NetVu or their nominated Agent.

As a minimum, NetVu require an ADSL link with 2Mb/s download and 0.5Mb/s upload speeds, but a higher upload speed is recommended. Fixed IP address SIM cards may be a viable option if a 4G network is available in the area.

In the case of standalone installations remote access for the following services must be provided:

- HTTP
- FTP
- TELNET

Remote access to these services must be provided for each detector in the standalone system.

Consequently, port-forwarding must be configured in any router providing remote access to the standalone FireVu system. For example, port-forwarding configured for four FireVu detectors employed standalone on a site might take the following form:

Detector Number	Local IP Address	Service	Local Port	Port Forwarding
1	192.168.1.1	HTTP	80	8090
1	192.168.1.1	FTP	21	8091
1	192.168.1.1	TELNET	23	8092
2	192.168.1.2	HTTP	80	8093
2	192.168.1.2	FTP	21	8094
2	192.168.1.2	TELNET	23	8095
3	192.168.1.3	HTTP	80	8096
3	192.168.1.3	FTP	21	8097
3	192.168.1.3	TELNET	23	8098
4	192.168.1.4	HTTP	80	8099
4	192.168.1.4	FTP	21	8100
4	192.168.1.4	TELNET	23	8101

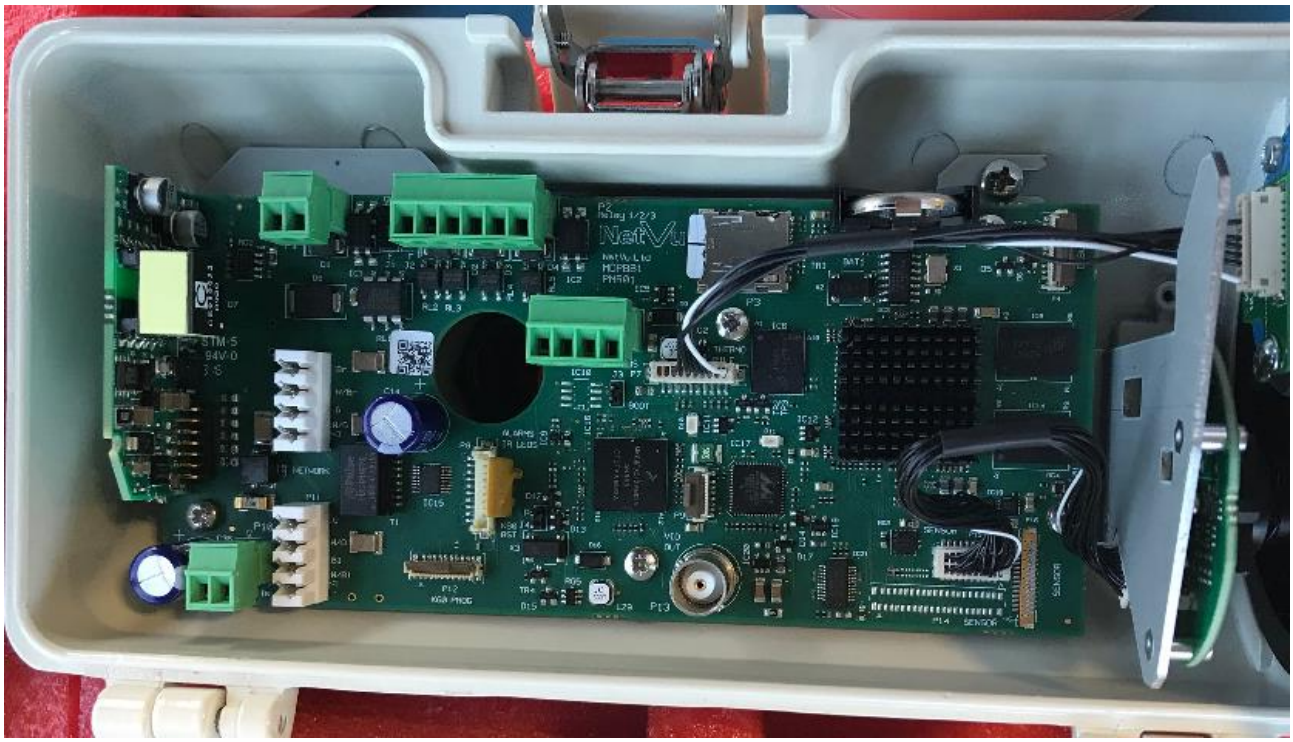
In the case where the static IP address of the router might be, for example, 172.17.250.4

Then to access the web pages of detector 3 remotely the URL would be 172.17.250.4:8096

Note: All port forwarding schemes must be put in place, tested and advised to NetVu Ltd in advance of remote commissioning of the system by NetVu.

Individual FireVu Detector Connections and Wiring

All connections to the FireVu detector are made on the main printed circuit board (PCB).



The available connections include:

- Ethernet cable connection ("push-down")
- Low voltage power supply input (terminal block)
- Four Solid state relay outputs (terminal block)
- Composite video signal output (BNC)
- Two Alarm Inputs (terminal block)

The location and wiring of these connections is shown on the following page.

Relay Outputs and Alarm Inputs

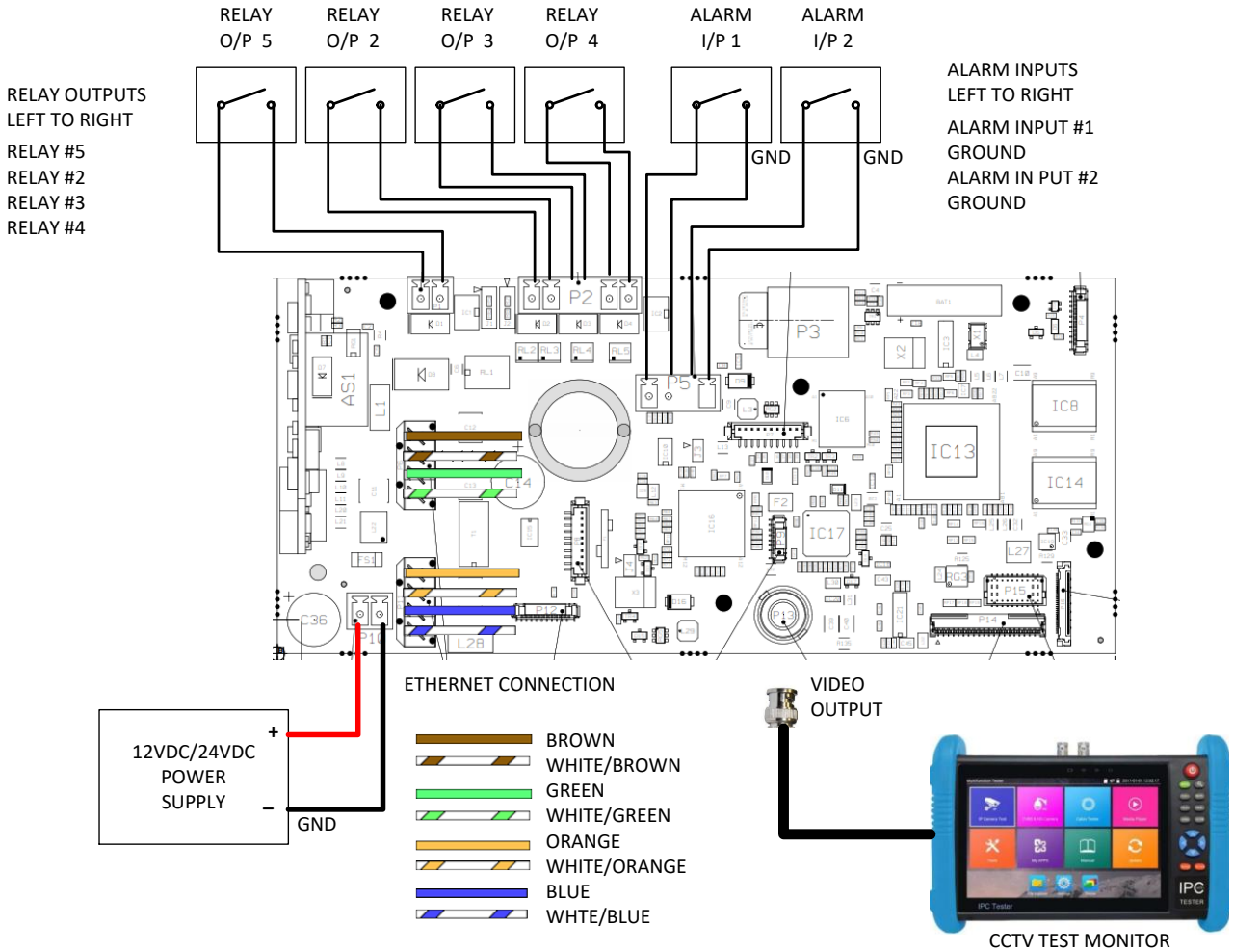
Four non-polarised solid-state relay outputs are provided.

Relay Outputs 2 – 4 are capable of switching 600mA at 60VDC.

Relay Output is 5 capable of switching 2.2A @60Vdc.

Relay Outputs 2 and 3 are also configurable for Loop Monitored fire loop alarms (see following section for configuration)

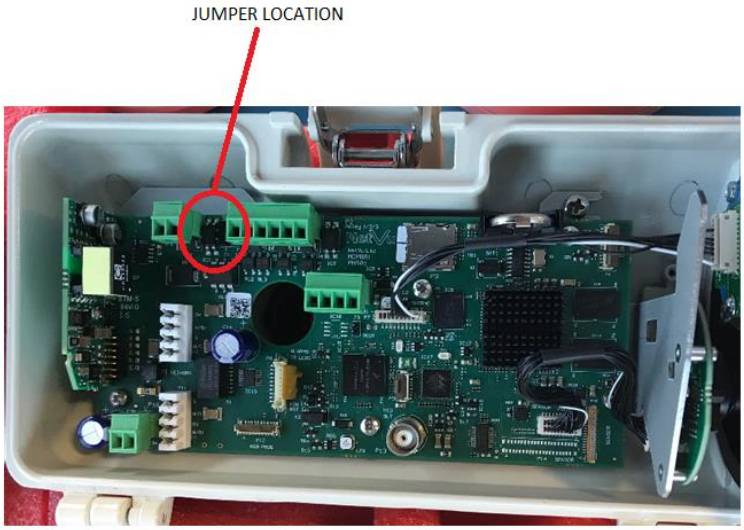
Two Alarm Inputs are provided. These are logic level inputs, single ended.



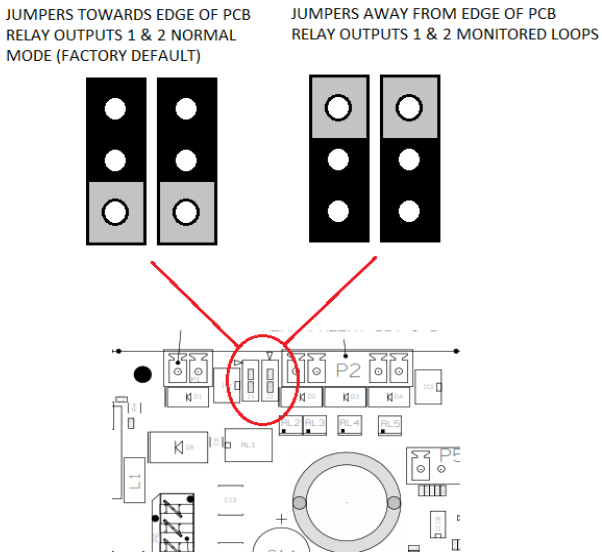
Configuring Relay Outputs #2 and #3

If desired relay outputs #2 and #3 can be configured as monitored loop outputs. In this mode, should the connection to the Fire Alarm Control Panel (FACP) or other system become short circuit or open circuit then both the FACP and the FireVu detector will be able to detect this fault and report it.

The operating mode of relay outputs #2 and #3 is controlled by two sets of jumpers, which are located in between the connection blocks for relay output #5 and relay output #2



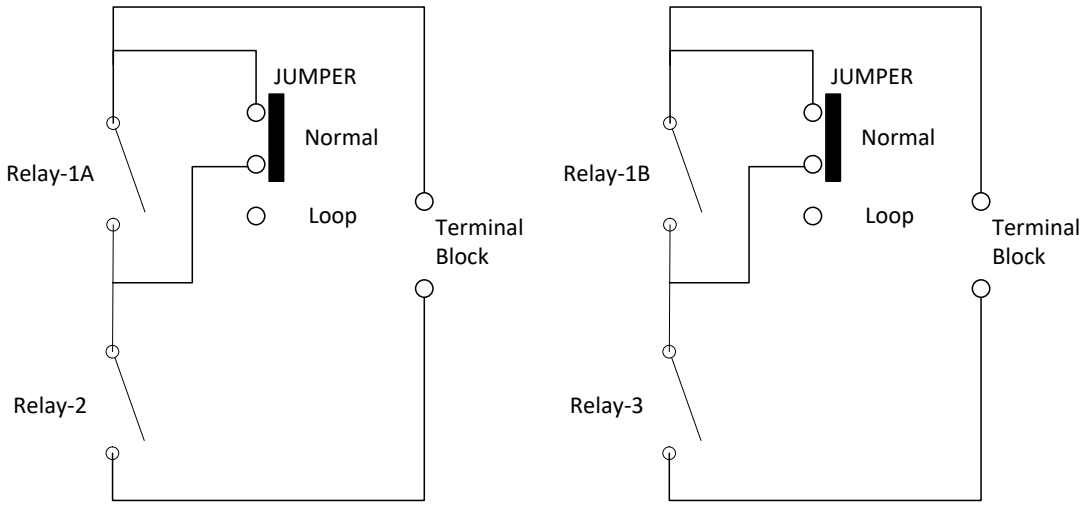
The following diagram, shows jumper position for normal and monitored loop configuration.



Relay #1 – Alarm/Fault Relay

Relay 1 is a combine alarm and fault relay.

The equivalent circuit diagram of relays 1, 2 and 3 is as follows:



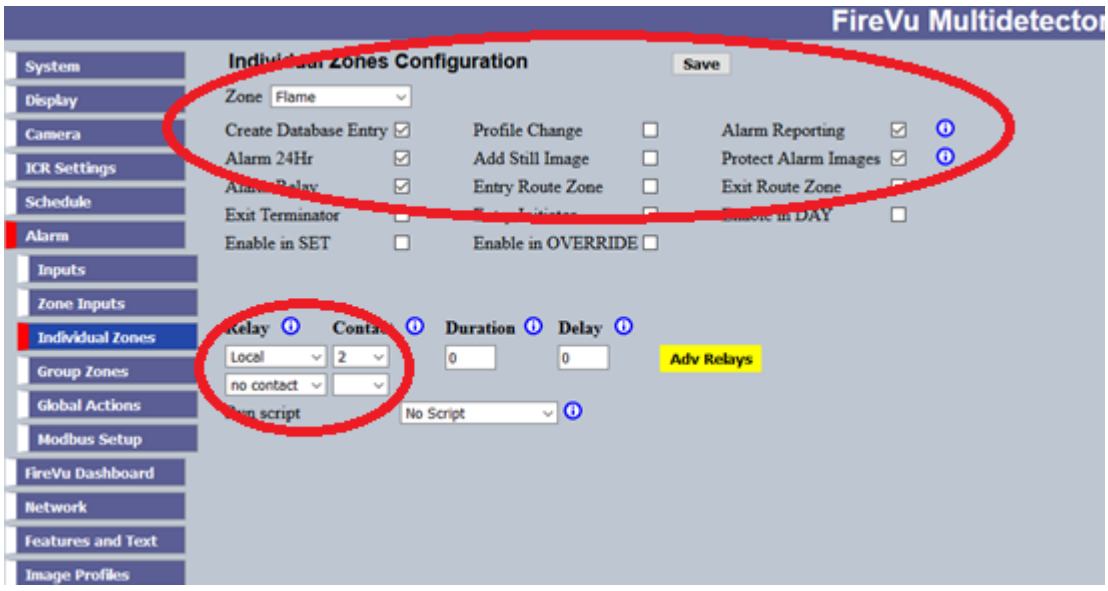
With the jumper in the "Normal" position the position of relay 1 (open or closed) is irrelevant as it's contacts are shorted out by the jumper. This means that relays 2 and 3 will work normally and their position (open or closed) will be repeated on the terminal block for those relays.

With the jumper in the "loop" position the position of relay 1 also has an effect on the state of the output at the terminal block. If relay 1 is closed then the position of relays 2 and 3 (open or closed) will be repeated on their terminal blocks. If relay 1 is open the terminal block status will be open, regardless of the position of relays 2 and 3.

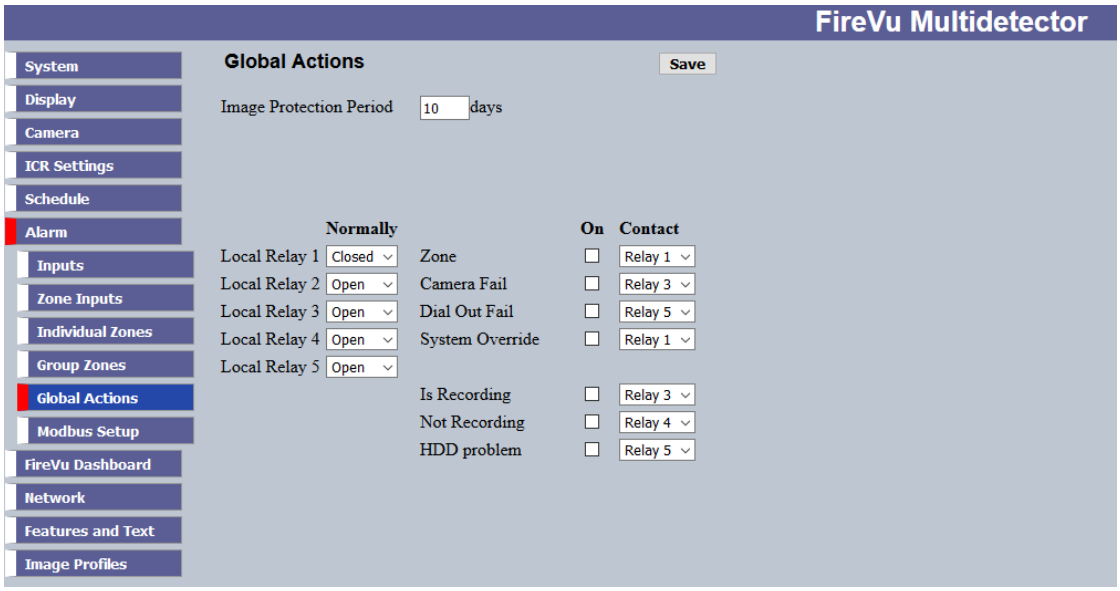
Relay one can be programmed or controlled by the fault status of the detector (including cable faults measured on the terminal blocks of relays 2 and 3 if the jumpers are in the "Loop" position).

If normal relay operation is desired and somehow the jumpers have become lost then relays 2 and 3 can be made to work normally by setting relay 1 to permanent normally closed.

The practical effect of the above is that relays 2,3,4 & 5 should be used to signal smoke/flame high temperature using the **Individual Zones Configuration** page of the detector.



Similarly, the Normally Open or Normally Closed State of these relays is set in the **Global Actions** page of the detector.



Post-Wiring and connection tasks

When all wiring, connections and physical configuration have been completed do not forget to take out the Silica Bag from the plastic bag supplied, place it in the FireVu Detector housing and then immediately close and seal the housing.

This will help to prevent the build-up of moisture inside the detector housing which might otherwise form as condensation on the inside of the camera window, spoiling the performance of the system.

Configuration

Basic Configuration / Pre-Commissioning

Once the detectors have been physically installed, positioned and wired some basic configuration work can be done as preparation for remote commissioning of the system.

Considering the implications of triggering a fire alarm control panel it is recommended that the final connections to any FACP are not made at this stage, but are connected later in commissioning when the operation of any relays in response to smoke/flame/thermal detection has been tested and proved.

Initial Settings

In a large FireVu system, where FV2 Annunciators and FireVu Network Extenders are used, secure IP addresses are automatically assigned to each detector. In a standalone FireVu installation this is not the case and so, when the detectors are powered, the first job will be to set an IP address in each detector.

As a factory default FireVu detectors are set for DHCP IP addressing.

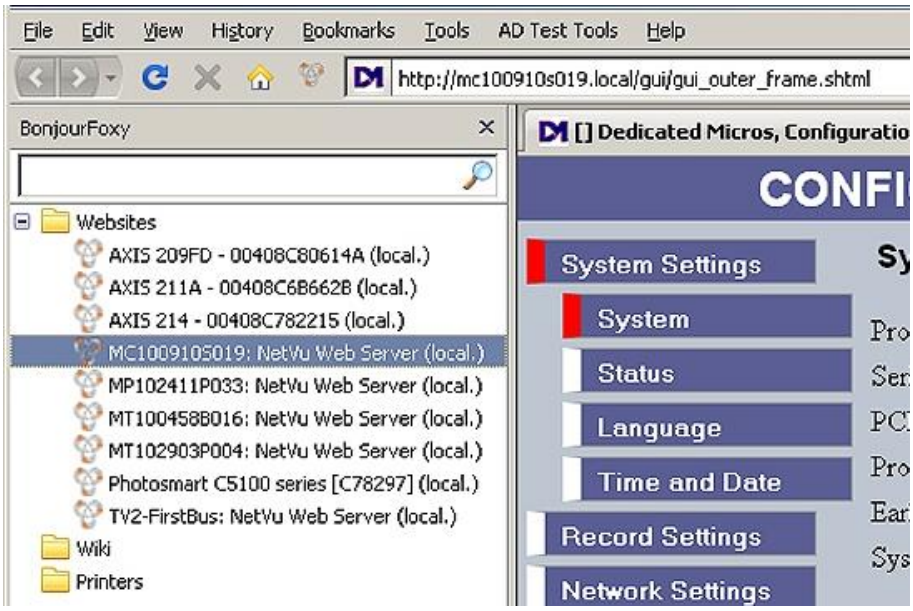
Consequently, if FireVu detectors are connected to a network or router which supports DHCP then IP addresses will automatically be assigned. The IP addresses set can then be discovered by connecting to the same network/router and using an ARP command or other network discovery tool.

Each FireVu detector is configured using on-board webpages. This can be done remotely once the unit has been installed in its chosen location, using the web browser on a PC in the same subnet as the unit.

The configuration pages can be accessed using the detector IP address or DNS name.

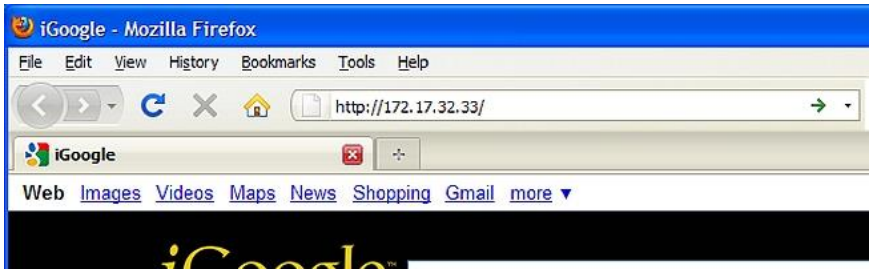
The default DNS address for each unit is factory set as the serial number. This address can be found on the serial label on the unit or on the packaging the unit came in.

The DNS or IP address can be typed directly into the address bar of a web browser:



The figure above shows access to detector web pages using DNS; the detector serial number.

Note: The unit's DNS address can be changed subsequently to something more memorable or meaningful than its serial number by editing the System name option in the System configuration page.

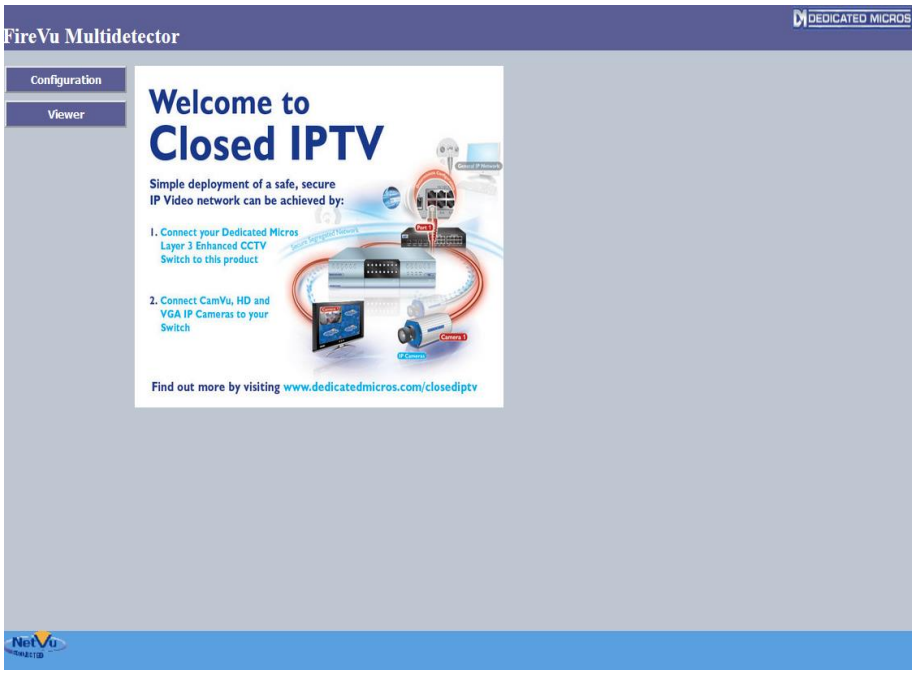


The figure above shows access to detector web pages using IP address.

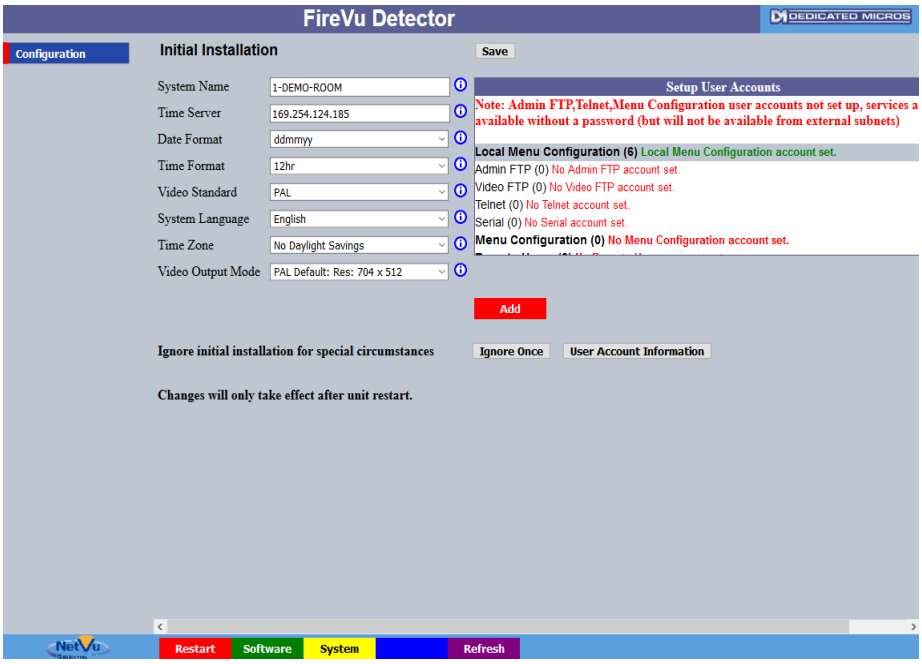
As a minimum, the following configuration should be done once the detector is running:

1. Set User Names and Passwords,
2. Set Time and Date,
3. Configure the Network Settings of the NVR (IP address, Subnet, Gateway).

On connecting to a detector the following web page will be displayed:



Click on "Configuration" to start setting up the detector. The first time that you do this an initial installation web page will be displayed:



This is an initial installation screen which allows you to:

- Set passwords
- Set time and date format
- Set a time server (if available)
- Set language
- Set a name for the detector

The detector can protect configuration procedures and access to video images by limiting access using usernames and passwords. By default, no usernames and passwords are configured for any account type.

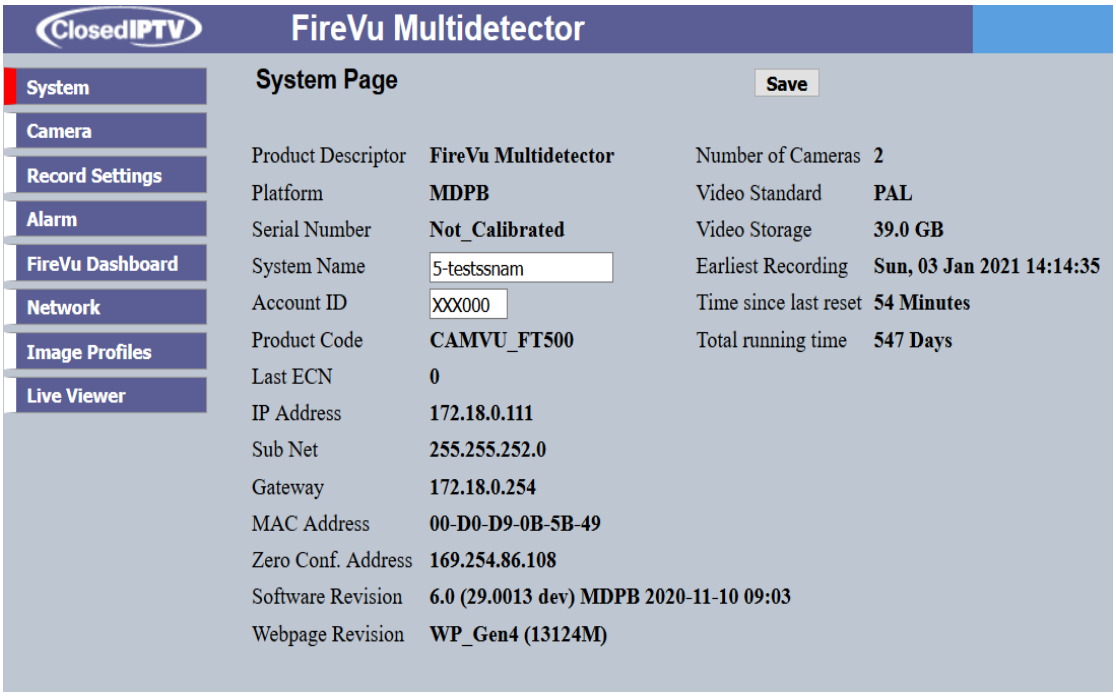
The following account types are available.

User Account Information
Unit can protect configuration, control FTP and viewing rights by limiting access via user names and passwords. Setting different user accounts will allow varying levels of access. Adding a username and password to:
Admin FTP will limit access to the unit via an FTP connection.
Video FTP will limit access to the Video FTP archiving feature (used with NetVu ObserVer).
Telnet will limit Telnet access to the unit (Telnet can be used to upgrade the unit).
Serial will limit access via a Serial link.
Menu Configuration will limit access to the Configuration menus. The user will be prompted for a username and password before access to the Configuration menus is allowed.
Local Users will limit access to the Viewer pages for local users. The local user will be prompted for a username and password before access to the Viewer pages will be granted.
Remote Users will limit access to the Viewer pages for remote users. The remote user will be prompted for a username and password before access to the Viewer pages will be granted.
It is possible to limit access to specific cameras for Local and Remote Users. Use the Camera Selection segment of the Add New Account menu to enter the cameras they can access. Select the cameras according to the input channel on the rear of the unit.

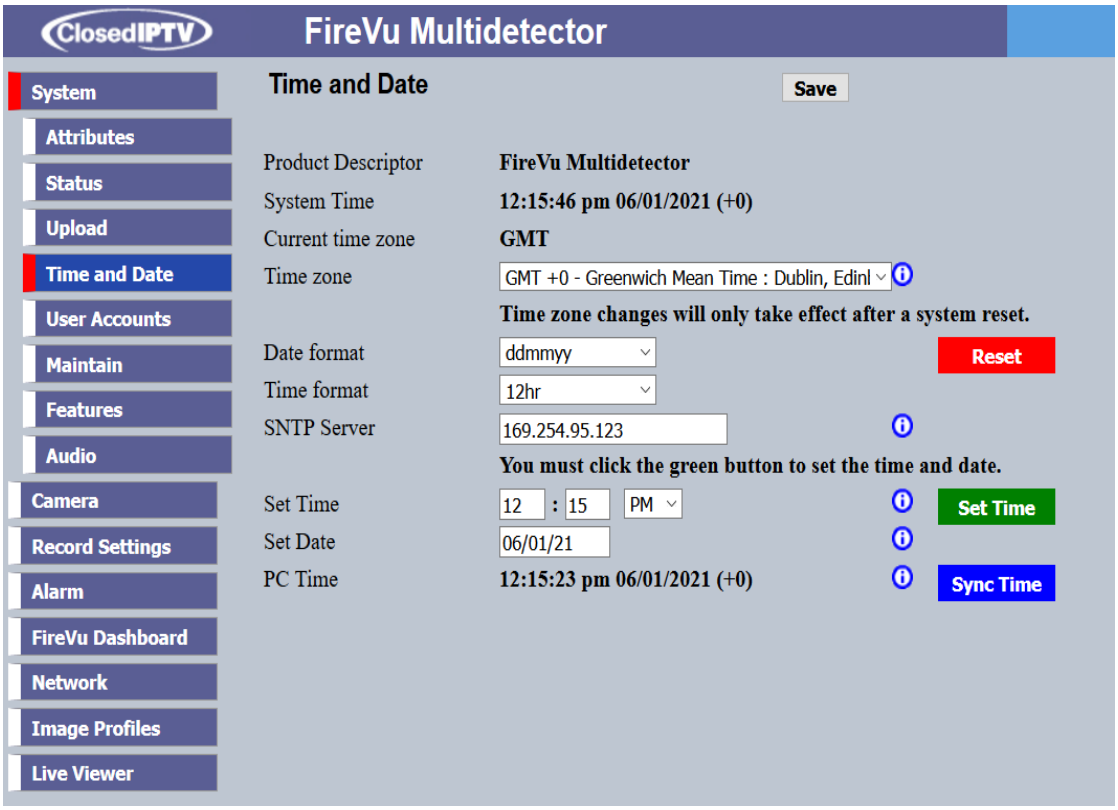
To add a set of user credentials click on the account type and then click on “Add”. Enter the User name and password and then click on “Save”.

When you have made all the required changes to the initial installation web page then click on “Save”.

The System page of the detector will then be displayed.



To set the time/date in the detector click on the green "Time/Date" button at the bottom of the screen. The time and date web page should then appear.

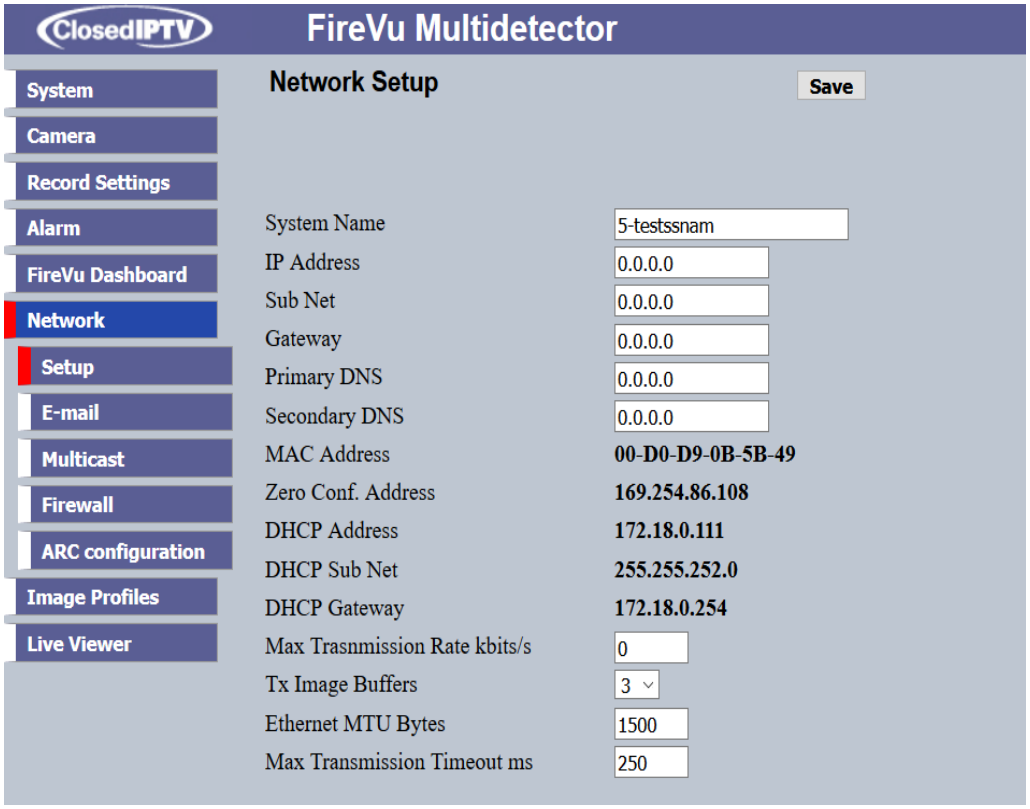


You can then set the date/time as required. When you are finished click on "Save".

If a permanent IP address is not assigned to the unit, it will attempt to contact the DHCP server every time it starts up, and periodically thereafter. This might cause the IP address of a detector to change which would cause port-forwarding (and therefore remote access) to stop working.

Consequently, a static IP address should be set for each detector.

To set a static IP address in the detector click on the blue "Network" button and then click on "setup". The Network Setup web page will then appear.



Enter a static IP address, Subnet mask and gateway and then click on "Save".

The detector may request a reset, on setting the IP address. Allow the detector to reset. When the detector comes back online it will be possible to access it using the static IP address.

Viewing Detector Video Images

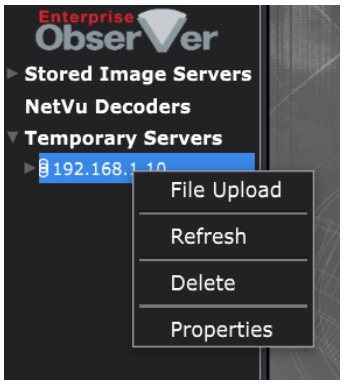
With the FireVu detectors, installed, wired, powered, and with their static IP addresses set you should now be able to view video images from the detectors, so that their fields of view can be checked and adjusted in advance of the start of remote commissioning.

Video images from FireVu detectors can be viewed using the Enterprise Observer Software, Premium Level License (ENVO/PRE/S) supplied with the FireVu detectors.

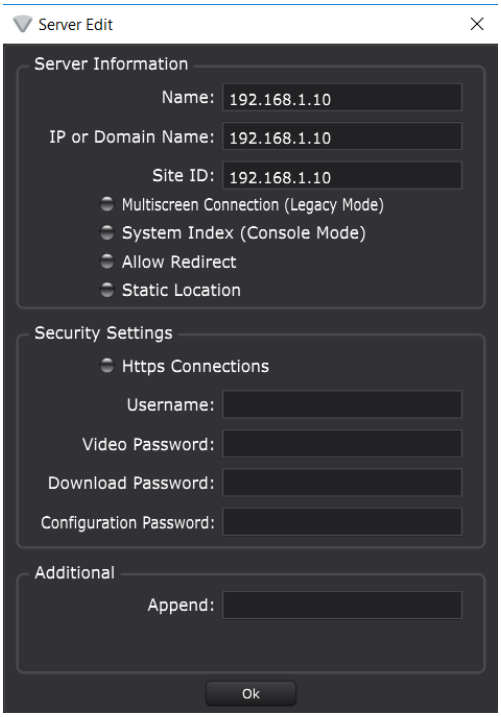
To view the video images from a FireVu detector, enter it's static IP address in to the field in the bottom left-hand corner of the Enterprise Observer software and then click on "Add".

The IP address of the detector will then appear under the list of Temporary Servers in the Site Tree.

Next, right-click on the IP address in the Temporary Servers list. And then left-click on "Properties".



The properties window for this IP address will then appear.



If you set usernames and passwords for the detector, enter those on this screen and then click on "OK"

The "Video Password" and the "Download Password" must correspond to the "Remote User" password for the Username configured in the detector.

The "Configuration Password" must correspond to the "Menu Configuration" password for the Username configured in the detector.

Having set the credentials you should be able to see images from the detector.

Double clicking on the IP address of the detector in the temporary servers list should cause two camera icons to appear underneath the IP address. The first icon will show live colour images from the video smoke detector and the second icon will show flame detection images from the video flame detector.

Click on a camera icon to view the video images, or drag an icon on to the video window of the Enterprise Observer software.

With the ability to see live video images from the detectors their position and view can then be checked before the start of remote commissioning.

Pre-Commissioning Checklist

A pre-commissioning check list will be included with Scope of Works that accompanies all FireVu Installations. In advance of arranging the start of remote commissioning with NetVu you should run through this checklist to make sure that all works are in place and that the FireVu system is ready.

Item	Description	Details/Variance	Complete and operational Y / N	Signed	Name, Position and Company	Date
1	Location of detectors, fields of view and focus correct as per plan.					
2	Installation complete, products powered up, images visible on Enterprise Observer.					
3	Detectors named and IP address and location as per plan.					
4	Direct Remote access set up and operational. Details provided to NetVu.					

Remote Commissioning and System Sign-Off

Remote commissioning of a FireVu system consists of a period of time where the installed FireVu system is remotely monitored by FireVu engineers. Any false positive detections, particularly those for video smoke detection are monitored, analysed and solutions implemented in revised settings of the detectors so as to reduce the level of false positive detections produced by the FireVu system to an acceptably low level, where possible.

During this period, any interfaces and interactions with Fire Alarm Control Panels (FACP), building management or other third-party systems laid out in the Scope-of-Works will be reviewed and implemented, with the limit of responsibility for such interfaces end at each FireVu detector.

Also during the remote commission period you may choose to do smoke testing and other testing to prove the operation of the FireVu system, in advance of system sign-off.

On-Site Smoke Testing

In order to confirm the operation of a FireVu system it is necessary to perform a smoke test of some description in front of each detector. This section details how this should be done and describes how the resultant footage of the test should be kept so as to avoid future potentially disruptive tests.

Equipment Needed

- Laptop loaded with current release of Enterprise Observer viewing software, (or access to PC on same network as the FireVu equipment with Enterprise Observer viewing software loaded) Enterprise Observer to be of version 1.18.27 or newer.
- USB storage, DVD or other device upon which downloaded files can be saved. This is essential if using site PC.

- Means of generating smoke for test, plumber's pellets or a smoke machine, or both. The choice of which will depend on the size, airflow within and availability of an electric mains power supply, at the area viewed by the detector.
- Accurate portable time-piece, (e.g. a wristwatch).
- Portable chart or form and pen for noting test start and end times whilst on site performing the tests.

Process

i. FireVu Equipment Preparation

1. Ensure the FireVu equipment is powered up, running the appropriate validated release of software, and that the detector(s) are also powered, properly and appropriately positioned in accordance with any existing screen shots and site assessment information. This must have been completed, assessed and approved prior to any commissioning visit.
2. Ensure that the time and date information as displayed in the web-pages are correct.
3. Ensure your portable time piece and the FireVu equipment are synchronised.

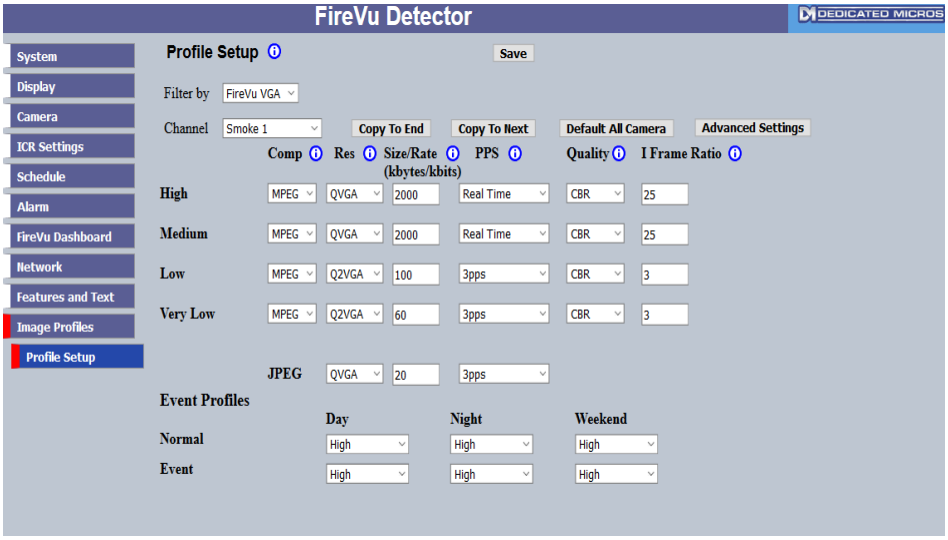
ii. Configuring FireVu Equipment for Test

Overview: The smoke tests MUST be kept so that they are performed only once and can then be reused for future evaluation and configuring of the FireVu detector's settings. This is essential, due to the disruption caused by, and resource required in, performing the tests.

1. The FireVu equipment's record settings must be set to a suitable level for the smoke test footage to be of optimum use. These settings may differ from those required on a continuing basis by the client and so MUST be set as detailed below before performing the smoke test. Subsequently, once the test is complete and the footage is protected, these can be set as needed.

   This is performed by following these steps:

- Open a suitable web-browser, (e.g. Mozilla Firefox®).
- Enter the IP address of each FireVu detector, or the Annunciator if this is also recording.
- From the menu structure select " Configuration " then " Image Profiles " then " Profile Setup ".
- For SMOKE testing Set up as follows, (also shown in the below screen-shot):
  - MPEG
  - VGA
  - 2000 kbps
  - 25pps



2. Select the "Copy to end" key shown in the above screen-shot to ensure all detectors are set as required.
3. Select the "Save" button.

iii. Preparation for The Smoke Test

1. Before going out to perform the actual smoke tests review each detector view area and decide what method of smoke testing best fits, based on how much smoke is required and whether power is available for the smoke machine. A large area with no access to power will require several smoke pellets, so care should be taken on deciding where to place them to give a plume of smoke over all the detector view where regions will need to be set and smoke parameters configured. Whatever method used the "risk areas" which have already been defined must be smoke tested in such a manner that a plume of smoke is achieved in front of all of them.
2. Identify the best route around the detectors to be smoke tested. FireVu Ltd. recommend doing no more than 8 channels in one go. Ideally, you should be able to travel from one channel to the next with the minimum amount of time between tests.
3. Ensure you have the necessary number of smoke pellets along with at least a 10% overhead for repeat tests and a sufficient amount of the appropriate smoke fluid if using a smoke machine.

iv. Performing the Smoke Test

1. Proceed to the first detector's viewable area and set up the smoke test as required. Before lighting pellets or starting smoke machine discharge note the time from your time-piece, (which has been synchronised to that of the FireVu equipment), on your chart or form.
2. Wait for 30 seconds to allow all pixel changes resulting from your presence to "settle". Start the smoke test. If using a machine discharge for at least 30 seconds, or as long as needed

to achieve a persistent plume which remains present for a minimum of 5 seconds across a good portion of the field of view of the detector being tested.

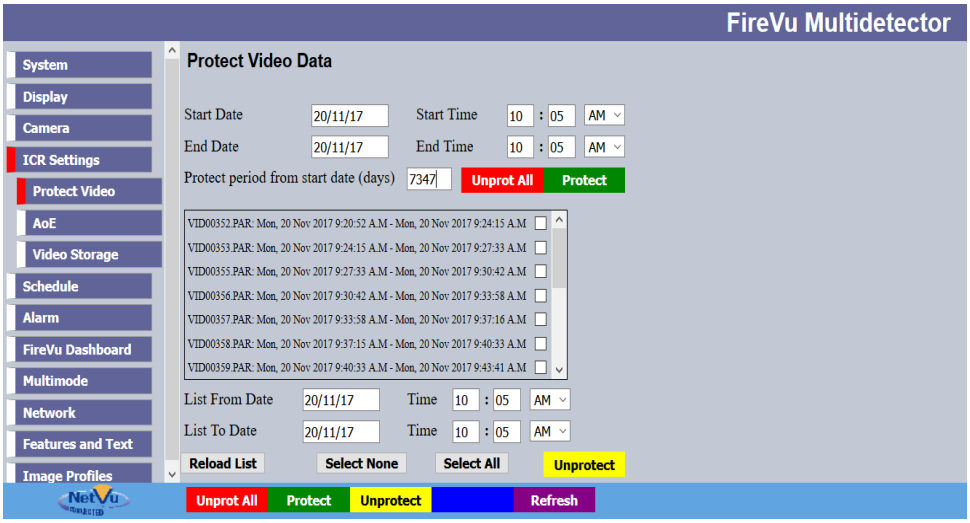
3. On completion of the smoke discharge allow sufficient time for the smoke to rise and disperse, which will vary depending on the environment.
4. Once sufficient smoke has been deployed to constitute pluming smoke over the whole risk area and has cleared at least in part, note the time on your chart or form as smoke test end time for the relevant detector.
5. Proceed to the next detector view. If near to any others already smoke tested ensure there is no lingering smoke from previous tests. At the start of the test there should be no smoke present. Perform the test as with the previous detector view noting start and end times.
6. Follow the below steps to protect the footage on each FireVu detector or the Annunciator if that is doing the recording and then repeat the process above for the set of detectors and so on.

v. Protecting the Smoke Test Footage

This is an essential stage and MUST be performed as soon as the smoke tests are complete.

This is done from the FireVu Equipment's web-pages as follows:

- Open a suitable web-browser, (e.g. Mozilla Firefox®).
- Enter the IP address of FireVu detector.
- From the menu structure select "Configuration", "ICR Settings" and "Protect Video".



- For each smoke tested detector in turn, enter the time periods as noted on your chart or form giving the date, start and end time. Always add 60 seconds to the start and end time to get a "run-in" and "run-out" of footage before the smoke test begins and at its end. If working on an Annunciator and the smoke tests are consecutive with no gaps you can protect the entire time as one block.
- In the entry box labelled "Protect period from start date (days)" enter 999999.

- Select the " Protect " button.
- Check the boxes to ensure the required times are listed as protected, and that the lower box shows them as being protected until "2038".
- Example below shows a single entry for a smoke test for one channel performed between 09.00 and 09.05 on 20th November, 2017.

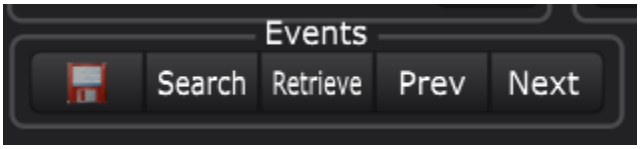
vi. Downloading the Smoke Test Footage

Although the smoke test footage is now safe from being over written, it should also be downloaded and archived in case of hard drive failure or accidental deletion from the FireVu equipment. This MUST include the 60 second "run-in" time in the same manner as the footage was protected.

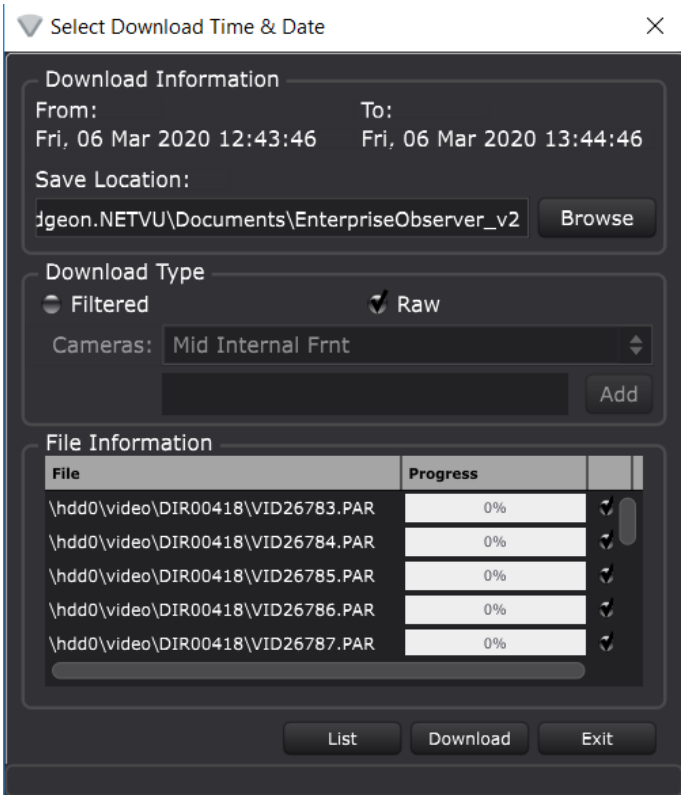
This is done by extracting the relevant PAR files from the FireVu detector or Annunciator record media. There are several methods of extracting these files not all of which are appropriate, (or possible), for ALL variants of the FireVu product range. Consequently, the method covered here is chosen because it applies equally to the entire FireVu product range, both current and legacy products.

To download the required footage, follow the below process:

1. Using either a PC on site or your laptop with Enterprise Observer viewing software loaded open that software.
2. Ensure that you can connect to the detectors from which you want to download footage, using the Enterprise observer software. The process of connecting is described on pages 33 – 35 of this manual.
3. Select live images from the first detector to be downloaded
4. Ensure there is a blank DVD in the local PC drive and that it is writeable, or some other media for the download, such as a USB stick.
5. Click on the red disk symbol in the Events window of the Enterprise Observer Software.



6. A download time and date window will open



7. Enter starting and ending times for the footage to be downloaded, using your chart and the guidance mentioned above
8. Select the location on the PC (USB stick, or DVD) where the downloaded footage is to be stored.
9. Select Raw download. This will download all the data from all detectors between the selected times (next step).

Note: Do NOT select "Filtered" download as this may not include some of the embedded FireVu parameter information.

10. Click on "List". This will display the names of all the associated video PAR files that will be downloaded
11. Click on "Download". The PAR files will now start to download and status bars will update as each file is downloaded. Downloading the images may take some time depending on the size of the video segment selected and the network connection to the unit.
12. When all files have downloaded. Click on "Exit"
13. Repeat stages 1 – 12 for each of the other detectors.

Your smoke tests are now complete, protected and you have a copy of them which should be safely archived for all future use. If a suitable PC is located with the FireVu system then a copy of the smoke tests should also be saved on the desktop there to enable future maintenance and service validation of settings and configuration.

On-Site Flame/Thermal Testing

The standard method of testing flame detection is to use a (EN54-TF5), (330mm x 330mm x 50mm (13" x 13" x 2") test pan with 500ml (1.06 US Pints) of fuel) as a target flame source.

When ignited, flames from such a target placed within the working range of a detector should be detected within 30 seconds of the establishment of the flame.

Due to the high temperatures involved such a test is also suitable for testing high temperature detection offered by the FireVu Multidetector.

However, such tests carry a high level of risks, and in some sites may not be possible at all.

Consequently, careful thought and planning must be undertaken before considering carrying out on-site flame testing.

Using Telnet to Simulate Smoke/Flame/Thermal Detection

A useful means exists for testing FireVu detectors which can be carried out either locally or remotely, without having to perform on-site smoke/flame or thermal tests.

Using Telnet client software connect to the FireVu detector using the command :

OPEN (IP ADDRESS OF FIREVU DETECTOR)

If a Telnet password has been set (recommended the detector will prompt for the Telnet username and password

Once the valid credentials have been entered the Detector will respond with :

This engineering server will execute engineering and configuration commands

There are limited line editing capabilities. If the command is not recognised, the server will echo what you type. The command parser will also respond to MCI commands.

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

The following prompt will also be displayed :

Multidetector> (for a FireVu Multidetector)

Detector> (for a FireVu smoke and flame detector

The FireVu Simulation command is then available:

FVSIM

The usage of this command is as follows:

FVSIM <camera> <type> <regions>

Where:

camera - specify camera no. if within [1 .. 2]. If omitted defaults to 1 for smoke, 2 for flame/thermal

type -type of alarm to generate -

flame | f - Flame alarm

smoke | s - Smoke alarm

thermal | t - Thermal alarm (level 1)

thermal1 | t1 - Thermal alarm level 1

thermal2 | t2 - Thermal alarm level 2

low-l | ll - Low Light warning condition

high-1 | hl - High Light warning condition

high-m | hm - High Movement warning condition

low-c | lc - Low Contrast warning condition

env | e - Environmental lockout condition

regions – The 16 detection zones of the detector, numbered 1 to 16

Every FireVu detector has the field of view divided in to 16 detection zones in a four by four grid, numbered top left to bottom right, i.e.:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Note: The smoke/flame detection parameters can be adjusted individually in each zone and the individual zones can be temporarily or permanently deactivated. These techniques for useful tools during remote commissioning to assist FireVu engineers to suppress false triggers, which would otherwise be a nuisance.

For example, the following commands will have the following effects:

FVSIM S 1-16 <ENTER> will cause the detector to trigger for smoke in zones 1 – 16

FVSIM F 4-6 <ENTER> will cause the detector to trigger for flame in zones 4-6

FVSIM T 3 <ENTER> will cause the detector to trigger for high temperature in zone 3

When observing FireVu detectors with Enterprise Observer software using these commands will cause the corresponding colour of zone to be briefly displayed on the video image of the detector (providing that "display analytics" is enabled in the Enterprise Observer software video window).

The corresponding smoke/flame/thermal event will also appear in the event log of the detector and will appear in the Events Window of the Enterprise Observer Software after an Events Search.

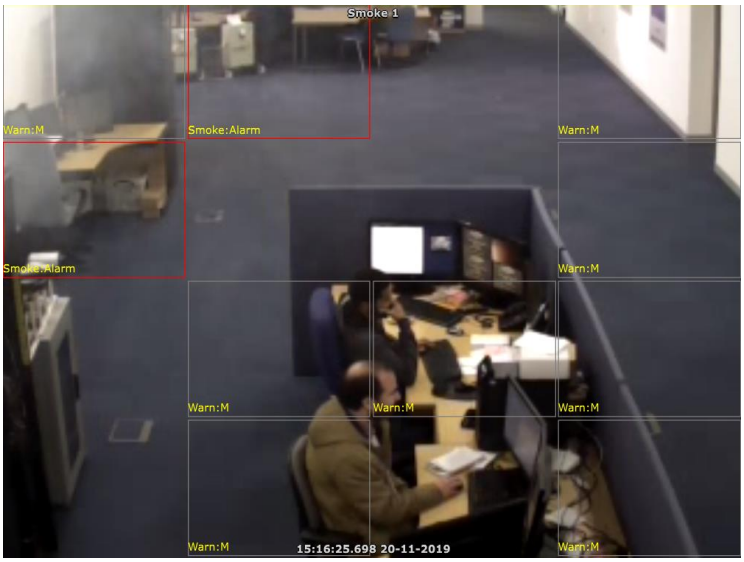
Events

Date	Camera	Alarm Text	Video
15:14:48 20-11-2019	1 - Smoke 1	Smoke:	no
15:14:48 20-11-2019	1 - Smoke 1	Smoke:	no
15:16:09 20-11-2019	1 - Smoke 1	Smoke:	no
15:16:09 20-11-2019	1 - Smoke 1	Smoke:	no
15:48:25 20-11-2019	1 - Smoke 4	Flame:	no
15:48:25 20-11-2019	1 - Smoke 4	Flame:	no
15:48:57 20-11-2019	1 - Smoke 4	Flame:	no
15:48:57 20-11-2019	1 - Smoke 4	Flame:	no
15:49:18 20-11-2019	1 - Smoke 4	Flame:	no
15:49:18 20-11-2019	1 - Smoke 4	Flame:	no
15:50:11 20-11-2019	1 - Smoke 4	Flame:	no
15:50:11 20-11-2019	1 - Smoke 4	Thermal2:	no
15:50:11 20-11-2019	1 - Smoke 4	Thermal2:	no
15:51:12 20-11-2019	1 - Smoke 4	Thermal2:	no
15:51:12 20-11-2019	1 - Smoke 4	Thermal2:	no
15:50:11 20-11-2019	1 - Smoke 4	Flame:	no
15:52:48 20-11-2019	1 - Smoke 4	Flame:	no
15:52:48 20-11-2019	1 - Smoke 4	Flame:	no
15:53:09 20-11-2019	1 - Smoke 4	Flame:	no
15:53:09 20-11-2019	1 - Smoke 4	Flame:	no
15:53:26 20-11-2019	1 - Smoke 4	Flame:	no
15:53:26 20-11-2019	1 - Smoke 4	Flame:	no

This technique is also useful in testing the interaction of relays with Fire Alarm Control Panels, and other systems, without having to do on-site smoke/flame/thermal testing.

Observing Smoke/Flame/Thermal detections using Enterprise Observer

As well as viewing normal live video from FireVu detectors Enterprise Observer can also display the smoke, flame and high temperature events themselves as coloured rectangles overlaid on to the video images of the detectors. These coloured rectangles represent the 16 detection zones of the detector.



The colour key for these rectangles is as follows:

Smoke Detection:

Yellow: Smoke detection in region.

Orange: Smoke detection in region and Zone Wait time exceeded but Zone Vote not reached.

Red: Smoke detection in region and Zone Wait time exceeded and Zone Vote reached. A smoke alarm is generated when this condition occurs.

Flame Detection:

Cyan: Black body colour match and awareness count > 0 (movement detected) but awareness threshold not yet met.

Magenta: Flame detected. A flame alarm is generated if this condition occurs.

High Temperature Detection:

Green: Thermal threshold exceeded. A thermal alarm is generated if this condition occurs.

Segmentation boxes

Grey: Low/High light or High motion warning condition. Smoke detection temporarily suppressed.

Consequently, at the start of a smoke detection event you may see yellow rectangles appear and these may change colour to orange and then red, as the smoke detection event actually takes place.

Similarly, at the start of a flame detection even you may see cyan rectangle appear, followed by magenta rectangle for the actual flame detection event.

A green rectangle means that a high temperature has been detected (above the trigger value set in the FireVu Multidetector).

Grey rectangles will appear when either the light level is too high or too low for smoke detection to take place. They will also appear if people or machinery is moving in the field of view of the detector. In these cases, smoke detection will be temporarily suppressed in the zones highlighted (smoke detection will work in all other zones without grey rectangles), while the grey rectangles are displayed. In the case of movement of people or machinery the grey rectangles will disappear about 30 seconds after movement stops, indicating that smoke detection has been enabled once more.

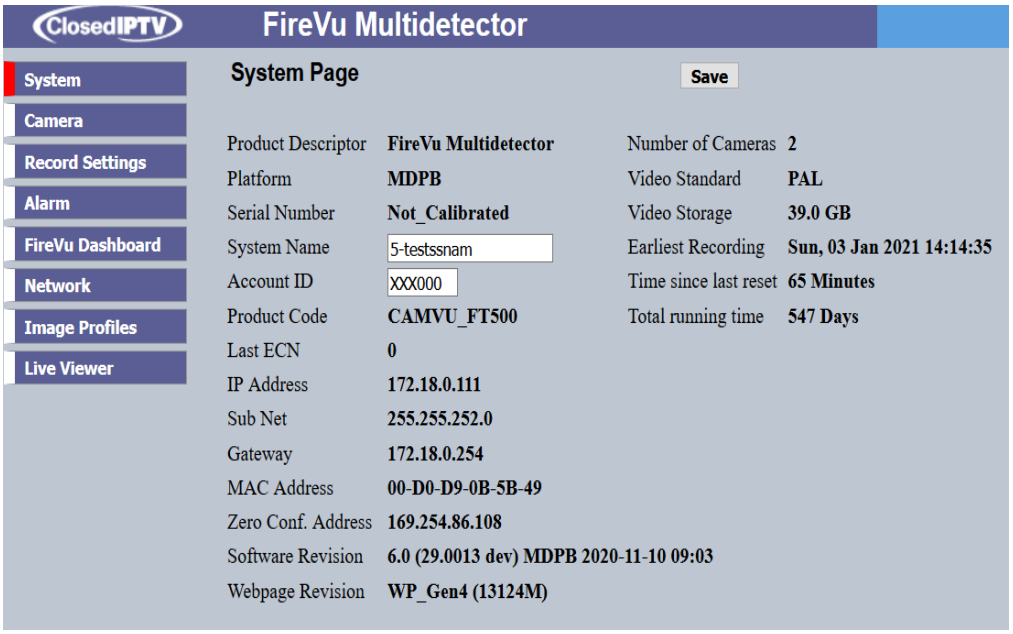
Advanced Configuration

The contents of this section of this manual will not be needed normally during most FireVu standalone installations as any adjustments made to the FireVu detectors using the web pages mentioned in this section will be carried out by FireVu engineers, during remote commissioning.

However, they are included in this manual to assist more experienced installers of FireVu systems and to aid in the understanding of the capabilities of the product and how it actually works.

Note: Adjustments should not be made to any of the settings described in this section, unless training from NetVu Ltd has been previously received, particularly in the FireVu Dashboard as incorrect settings may seriously affect the ability of the product to function properly.

Access to the setting of FireVu detectors is achieved through web pages which can be accessed using browser software, as mentioned in earlier sections of this manual. Having connected to a detector, selected “Configuration” and having supplied the correct credentials the main configuration page of the detector will be displayed:



From this main menu the various sub-menus which control the detector and it's operation can be selected by clicking on the labels on the left hand side of the screen.

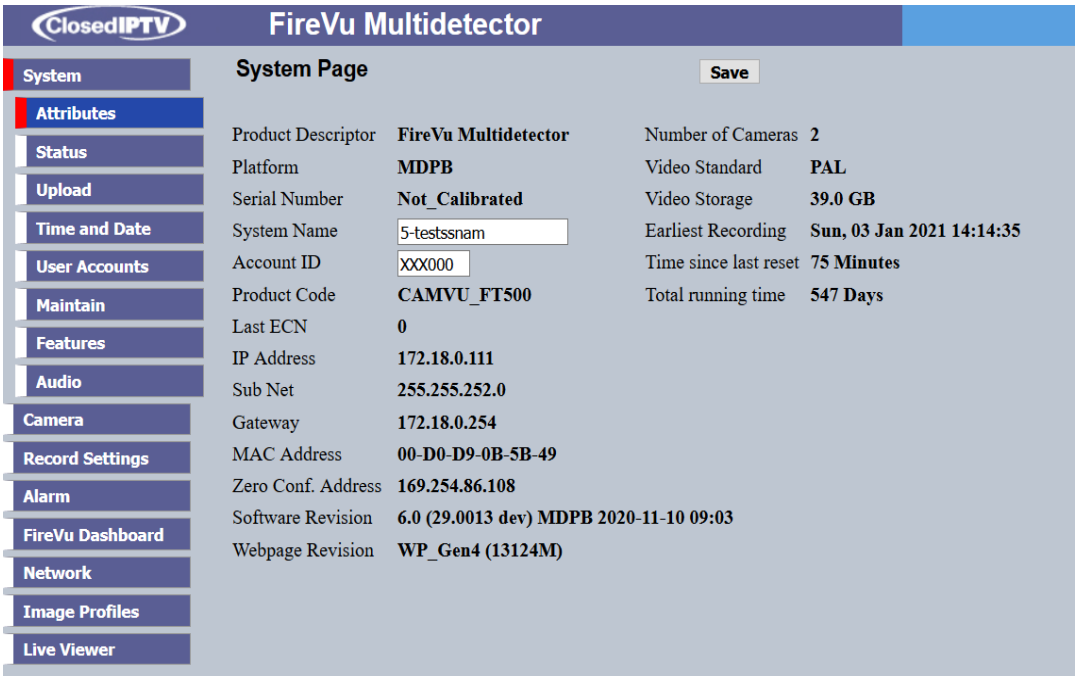
System Web-pages

Listed below are descriptions of the Web-pages to be found by navigating to the "System" Web-page.

System – Attributes Page

From the main menu of the camera, click on Configuration.
If prompted, enter a username and password.

The System - Attributes page will be displayed;



The menus under the System Settings heading allow the unit's core settings to be viewed, changed and the system software upgraded.

The Attributes option displays details about the unit including the IP address, unit serial number, MAC address and software version.

The Status page displays information about the unit's operating condition, shows how long the unit has been operating and the reason for the last reset. It also shows the camera status.

The Upload page facilitates uploading files to the detector for software upgrade or to add features or functionality.

The Time and Date page allows the unit time and date settings to be adjusted, including setting the time zone.

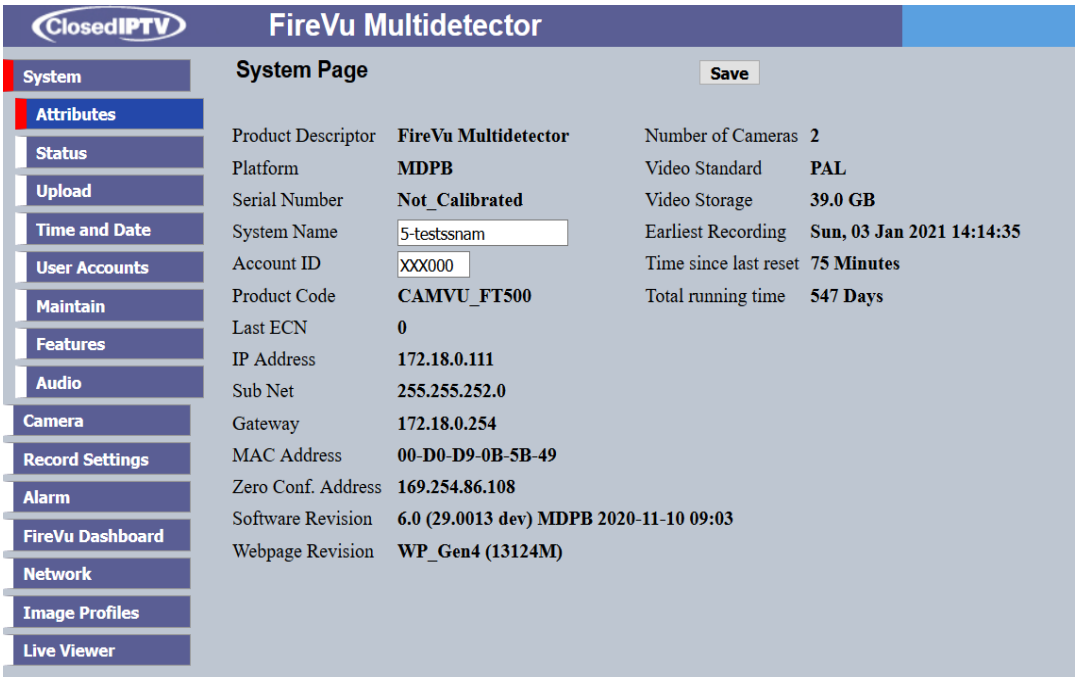
The User Accounts page allows user names and password credentials to be set for the detector.

The Maintain page allows the current configuration to be saved, and for previously saved settings to be loaded.

The Features page shows the video standard being used in the detector.

Attributes

This menu shows the general information about the unit including the version of software installed, the unit's serial number and the allocated DHCP IP address.



Product Descriptor: Details the product model.

Platform: The type of hardware being used for the detector.

Serial Number: Identifies the serial number of the specific unit.

System Name: This field can be edited to allocate a name to the unit, which can be typed directly into a browser to access the configuration pages. This is displayed when the unit is accessed using NetVu Enterprise Observer Software and is sent when transmitting information to a Remote Video Response Centres (RVRC).

Account ID: Used to provide an additional method of remotely connecting to the detector. Identifies this individual detector when reporting to an RVRC using Enterprise Observer or Pick-a-Point software.

IP Address: This is the IP address allocated to the unit.

Sub Net: This is the subnet mask for the unit.

MAC Address: This is the MAC address assigned to the unit.

Zero conf address: The starting IP address of the closed IP network for this detector.

Software Revision: The Software version of the detector.

Switch Version: The software version of the onboard network switch.

Webpage revision: The Webpage version installed on this detector.

Number of Cameras: The maximum number of cameras licensed for recording on this detector.

Video Standard: Displays the video standard adopted by the unit (i.e. PAL or NTSC).

Video Storage: The amount of available hard disk storage installed.

Earliest Recording: Displays the date and time of the earliest recording held on the unit.

Time Since Last Reset: the amount of time that has passed since the last reset of the detector.

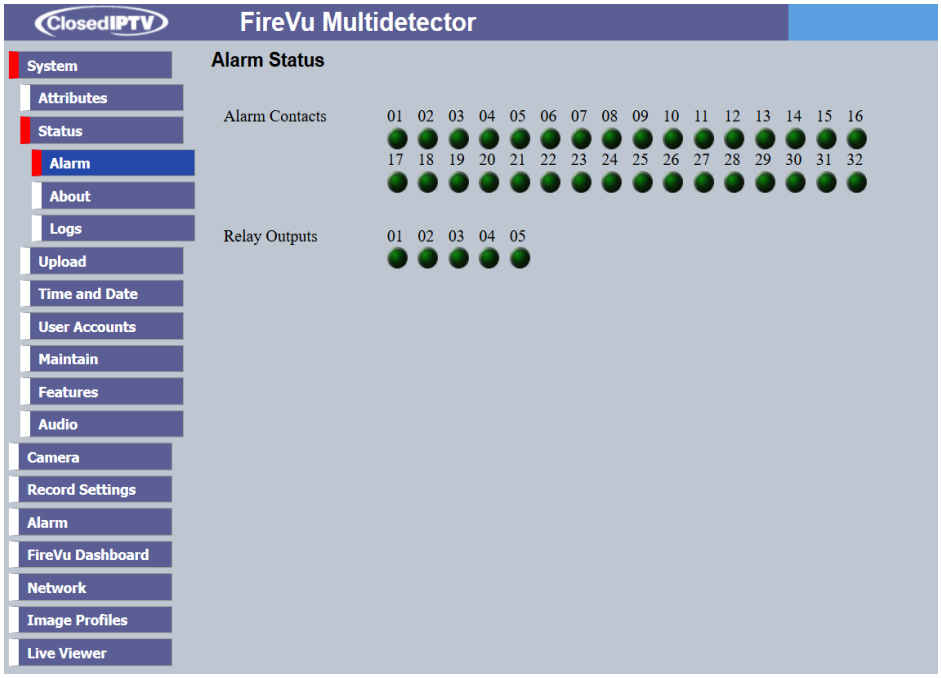
Time/Date (Green): Links to the System->Time and Date page.

Accounts (Yellow): Links to the Viewer Settings->User Accounts details page.

Network (Blue): Links to the Network Settings page.

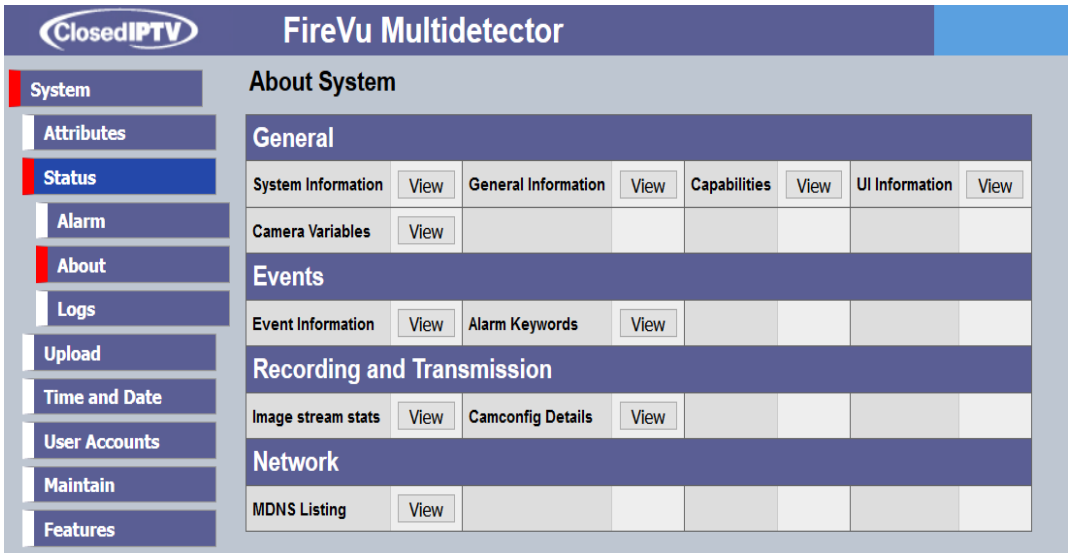
Status Page

Alarm Status



This page shows the current status of the alarm inputs and the relay outputs of the detector. A dark green colour indicates an inactive state whilst a light green colour indicates an active state. The page refreshes every few seconds.

About Page



System Information: Opens the System Settings->System page.

General Information: Opens the System Settings->Software page.

Capabilities: Opens the Capabilities Details page.

UI Information: Opens the UI Information page.

Camera Variables : Opens the Sysvar Editor page.

Event Information: Opens the Event Information page.

Alarm Keyword: opens the Alarm Keywords page.

Image Stream Stats: Opens the Image Stream Stats page.

Camconfig Detail: opens the Camconfig page.

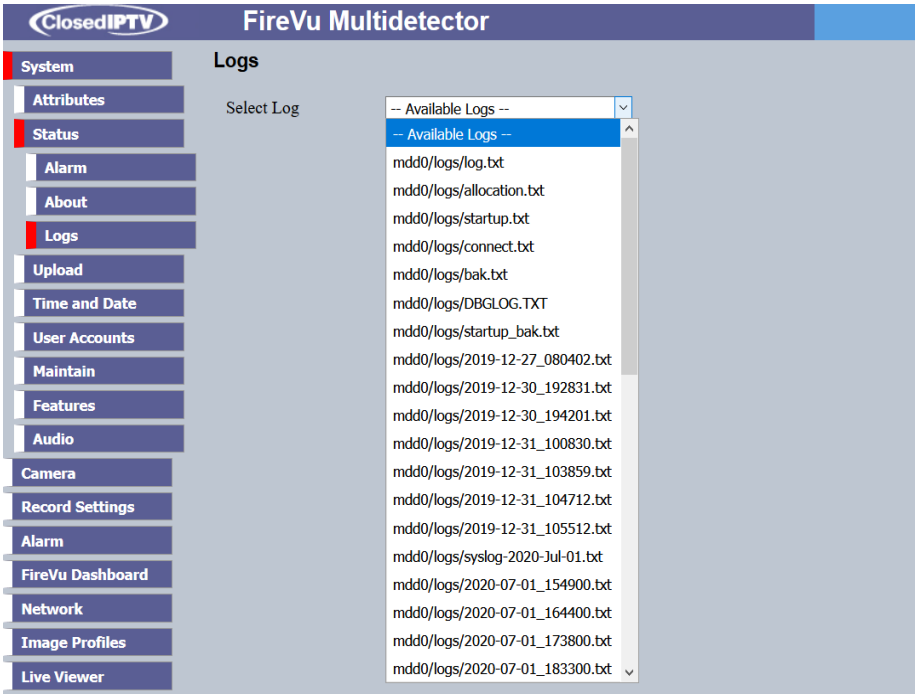
MDNS Listings: Opens the MDNS listings page.

Auto Configuration: opens the Auto Configuration page.

Most of these pages have no installer application, unless guided by NetVu technical support.

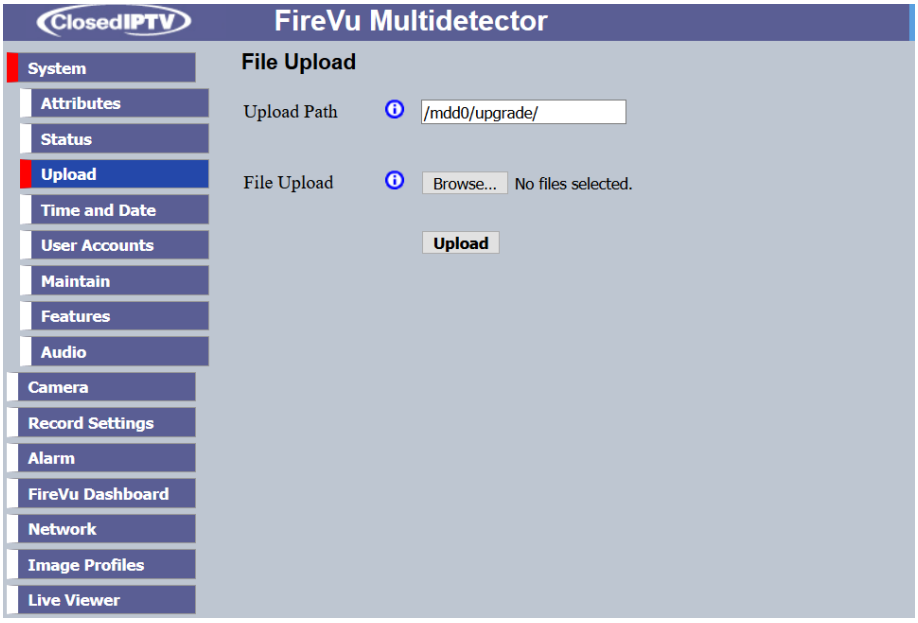
The exception is Alarm Keywords, which provides a list of the words which may be used when programming alarm events.

Logs Page



The logs page allows various diagnostics reports to be run, under the guidance of NetVu Support. There are no Installer settings on this page.

Upload Page



This page provides a means of transferring new files to the detector, without having to use FTP.

This can be used to update the software of the detector, install PowerScript files etc.

Click on Browse to select the files to be uploaded from your computer.

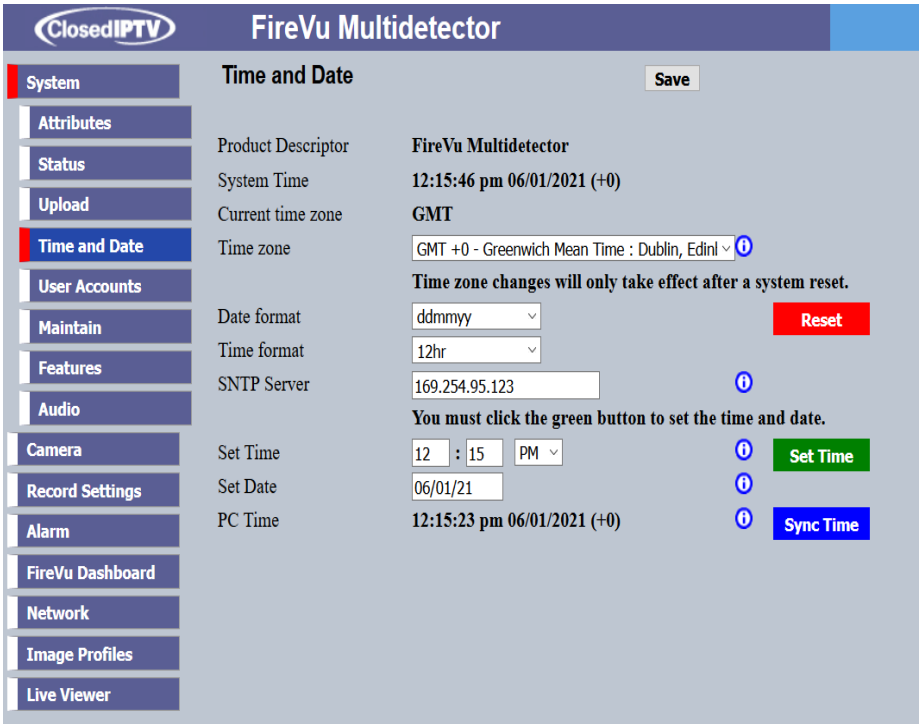
Upload Path: Used to select directory the files will be uploaded.

Some Examples below.

1. /mdd0/upgrade for upgrade products.
2. /mdd0/gui/frmpages for frm pages.
3. /mdd0/gui/json for json file update.
4. /mdd0/qnc for PowerScript files.

When you are ready click on "Upload" to upload files.

Time and Date



System Time: The current system time and date is displayed.

Current Time Zone: Displays the currently selected time zone settings.

Time Zone: Select the relevant time zone offset from the accompanying drop-down menu.

Date Format: As default, the date is entered dd/mm/yy. It can also be displayed as mm/dd/yy or yy/mm/dd.

Reset (Red): Resets the unit.

Time Format: As default, the time displayed is in 12-hour format. This can be changed to 24-hour if required.

SNTP Server: A Simple Network Time Protocol (SNTP) server allows external devices to connect and set their current date and time settings to that of the SNTP. If required, enter the SNTP server IP address here.

Set Time: Allows current unit time to be updated.

Set Time (Green): Applies the new time.

Set Date: Allows current unit date to be updated.

PC Time: Displays the system time of the PC currently being used to view the webpages.

Sync Time (Blue): Use this button to synchronise the time of the unit to that of the PC being used to view the webpages.

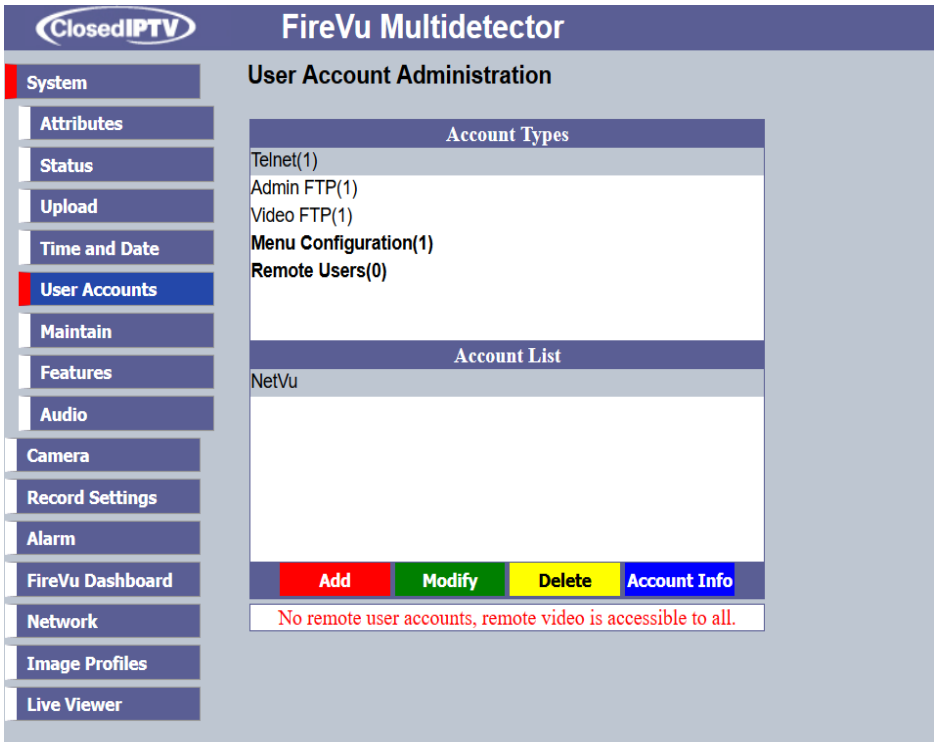
Note: The PC Time and Sync Time options will only be available if viewing the menu using the webpages.

System (Yellow): Opens the System Settings->System page.

Refresh (Purple): Refreshes the current page.

User Accounts

The unit can protect configuration procedures by limiting access using usernames and passwords. By default, no usernames and passwords are configured for any account type.



Add (Red): Add a new account of the type selected.

Modify (Green): Modify an existing account.

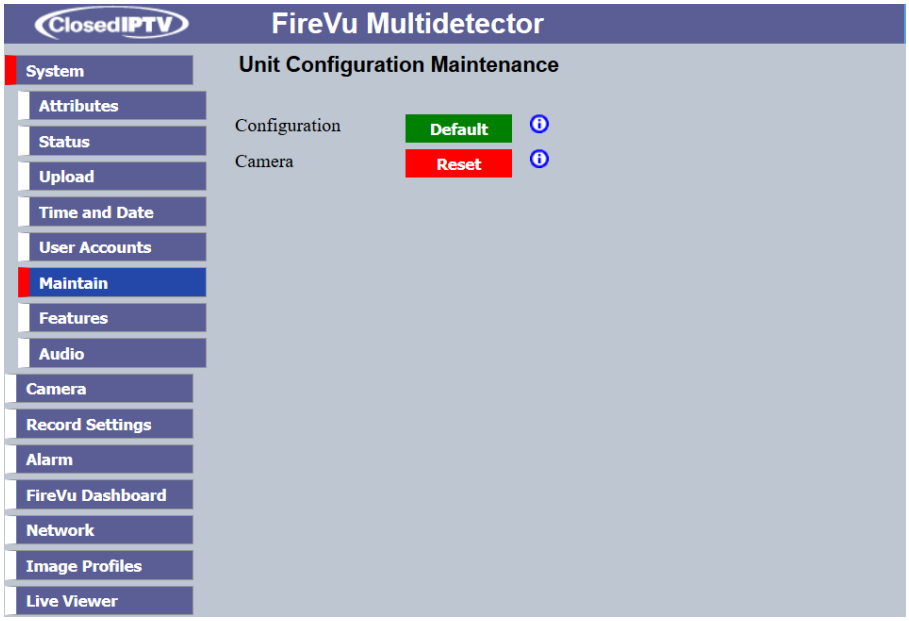
Delete (Yellow): Delete an existing account.

Account Info (Blue): Displays a window describing the types of account.

User Account Information
Unit can protect configuration, control FTP and viewing rights by limiting access via user names and passwords. Setting different user accounts will allow varying levels of access. Adding a username and password to:
Admin FTP will limit access to the unit via an FTP connection.
Video FTP will limit access to the Video FTP archiving feature (used with NetVu ObserVer).
Telnet will limit Telnet access to the unit (Telnet can be used to upgrade the unit).
Serial will limit access via a Serial link.
Menu Configuration will limit access to the Configuration menus. The user will be prompted for a username and password before access to the Configuration menus is allowed.
Local Users will limit access to the Viewer pages for local users. The local user will be prompted for a username and password before access to the Viewer pages will be granted.
Remote Users will limit access to the Viewer pages for remote users. The remote user will be prompted for a username and password before access to the Viewer pages will be granted.
It is possible to limit access to specific cameras for Local and Remote Users. Use the Camera Selection segment of the Add New Account menu to enter the cameras they can access. Select the cameras according to the input channel on the rear of the unit.

Maintain

The page allows for the unit to be reset or changed back to the default settings as supplied from the factory.

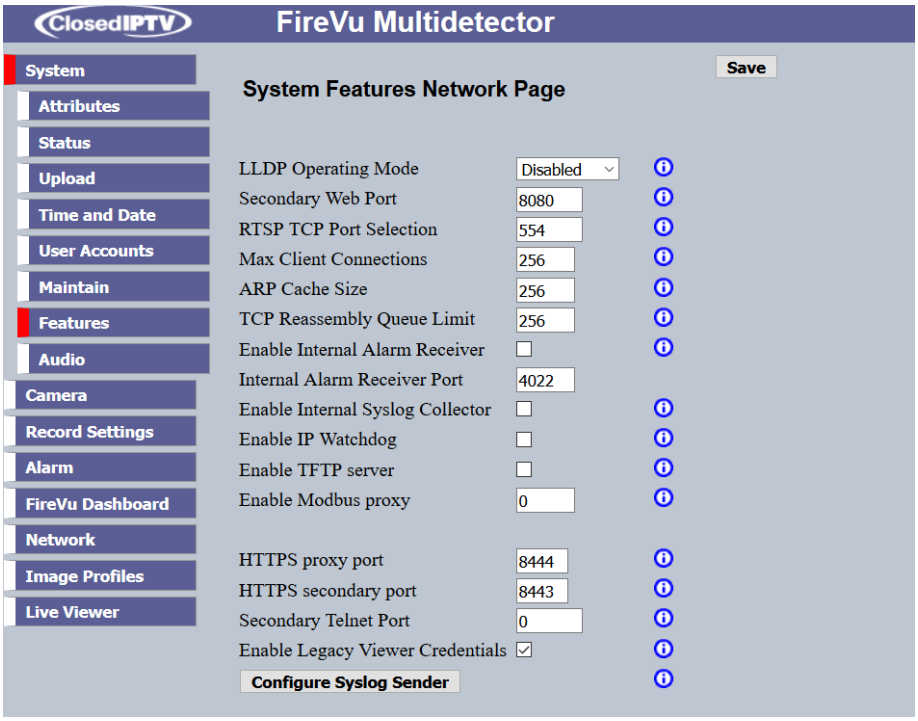


Click on Default (Green) to return the detector to factory default settings. Network Settings such as IP address will not be affected.

Click on Reset (Red) to re-start the detector.

Features

The page is used to enable additional network ports on the detector



LLDP Operating Mode: Sets the current LLDP Operating Mode. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a local area network based on IEEE 802 technology, principally wired Ethernet.

Secondary Web Port : If the primary web port is blocked by the firewall, it is possible to configure a second port number here. The unit is then accessed using the IP address of the unit, followed by a colon (:) and this port number.

RTSP TCP Port Selection: Use this option to change the TCP port number used by the RTSP server.

Max Client Connections: This limits the number of client connections to the server. It defaults to 256 but in heavy network traffic it is recommended that this value be increased. Please consult your network administrator for appropriate settings if needed.

ARP Cache Size: This limits the number of cache entries available in the ARP table. It defaults to 256 which is adequate for most instances. Consult your network administrator for advice about whether this should be increased.

TCP Reassembly Queue Limit: This limits the maximum number of TCP segments that can be in the reassembly queue, to prevent a common DoS attack.

Enable Internal Alarm Receiver: When selected, the internal alarm receiver will be selected instead of handling the alarms via powerscript. Changes to this value will need a reset.

Internal Alarm Receiver Port: Sets the port to be used by the internal alarm receiver of the detector.

Enable Internal Syslog Collector: When selected, the internal syslog collector will be selected instead of handling the syslog via powerscript. Changes to this value will need a reset.

Enable IP Watchdog: When selected, the IP Watchdog configuration page will be made available under the Network menu.

Enable TFTP Server: Enables a TFTP server for read-only access to ELF files stored in /slave-bin on the application drive.

Enable modbus proxy: Enables the Modbus proxy daemon on the default Modbus TCP port and specifies the number of proxy relays supported. Setting "0" will disable the proxy daemon. This value can be changed without having to reset the system

HTTPS: proxy port: Sets the port number for the HTTPS proxy daemon

HTTPS: secondary port: Sets the port number for the secondary HTTPS proxy daemon

Secondary Telnet Port: If the primary telnet port is blocked by the firewall, it is possible to configure a second port number here. The unit is then accessed using the IP address of the unit, followed by a colon (:) and this port number.

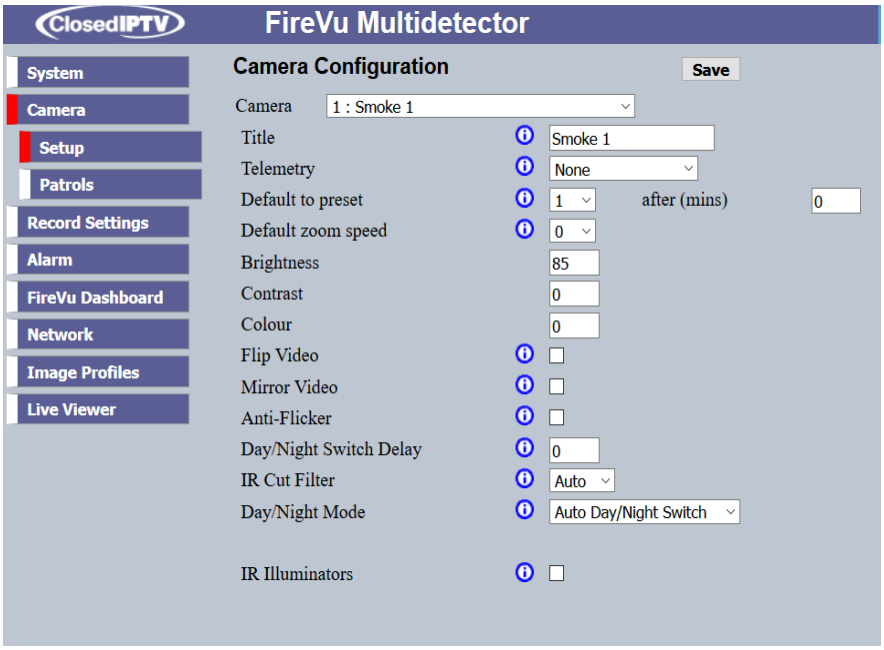
Enable Legacy Viewer Credentials: When selected, system variables required for legacy viewers can be read without credentials.

Configure Syslog Sender: Provides configuration options to enable sending of syslog messages from this unit to a specified IP address and setting which messages should be sent.

Camera Web-pages

Listed below are descriptions of the Web-pages to be found by navigating to the "Camera" Web-page.

Camera Setup Web-page



Camera: Selects which of the two video streams available from the detector is to be configured.

Title – Used to set a custom name for the selected. Default is "Smoke 1" for the first video stream and "Flame 1" for the second Video Stream.

Brightness: Adjusts the brightness of the video stream

Contrast: Adjusts the contrast of the video stream

Colour: Adjusts the colour of the video stream

Flip Video – This setting will vertically flip the video when ticked.

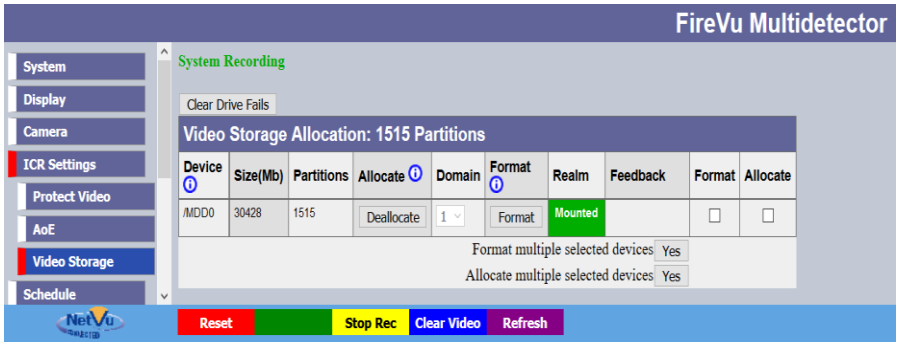
Mirror Video – This setting will horizontally mirror the video when ticked.

Anti-Flicker: This setting will enable anti-flicker mode when ticked.

Record Settings Web-pages

Listed below are descriptions of the Web-pages to be found by navigating to the "Record Settings" Web-page.

Video Storage Web-page



This Web-page enables configuration of the unit's on-board (µSD card) video storage.

Device – The device corresponds to one of the following types:
mddX - (e.g. mdd0) Internal storage, µSD card
mdd1X - (e.g. mdd10) External µSD card
uddX - (e.g. udd0) External USB device, from udd0 to udd3.

Allocate – This will allocate this drive to have a video storage capability. When a device is allocated the system will begin building video partitions. Progress is shown on screen.

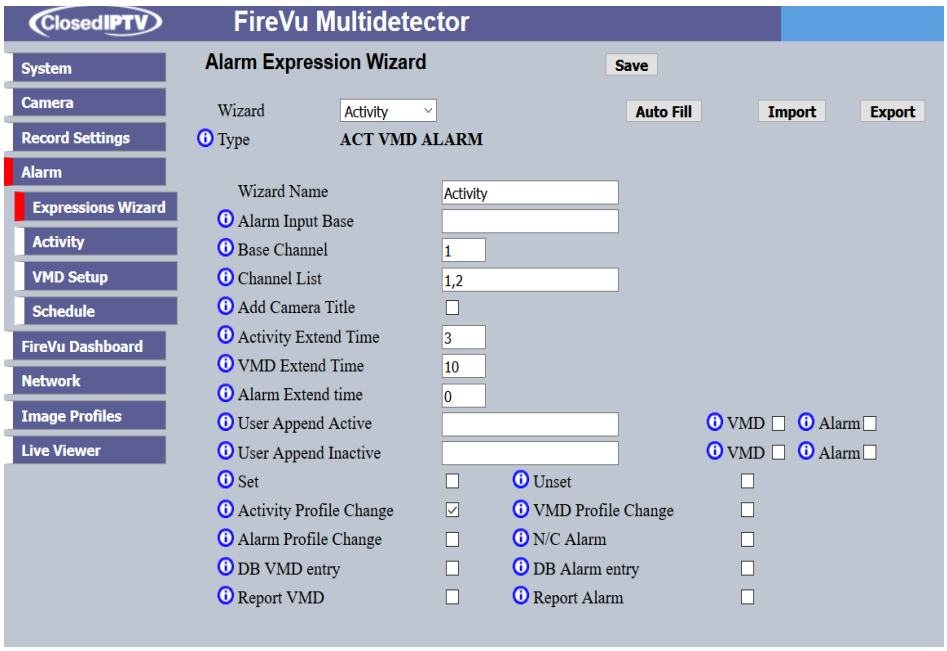
Format – When formatting the unit's application drive only, the video folder will be removed.

Formatting any other device will remove all the data. In both cases, recording on the system is halted when formatting and, if already allocated, the formatted device will be deallocated as a video storage device.

Alarm Web-pages

Listed below are descriptions of the Web-pages to be found by navigating to the "Alarm" Web-page.

Alarm – Expression Wizard Page



This page is used to configure the way that the detector will respond to triggers from a variety of sources.

With the exception of camera failure, if these triggers are momentary they can be extended in their active period by a number of seconds so that any response by the detector can immediately take action to capture the event in detail.

The Alarm Expression Wizard page also determines what actions are taken by the detector in response to the activation of the triggers.

The actions which can be taken by the detector include:

- Changing the recording profile used while the trigger is active so that, for example, the detector records in high quality while the trigger is active
- Creating a database entry such that the event appears in the history logs of the detector, allowing the logs to be searched by event so that video recordings associated with the event can be found quickly.
- Reporting the event to a remote video receiving centre RVRC*
- Sending a PTZ camera to a specific preset position*
- Operating a relay output (local to the detector or remotely, on a modbus module)*
- Playing an audio file through the audio output of the detector*
- Protecting a period of recording of a specific camera for a number of days*
- Running a PowerScript program located on the detector

* Depending on software version of the detector

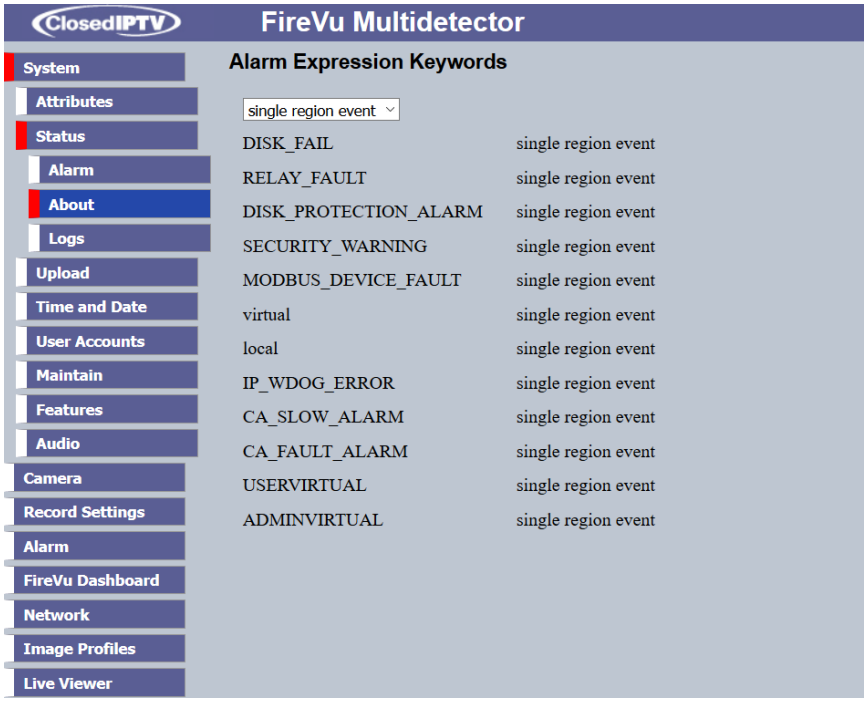
The controls available on this page are as follows :

Wizard: Selects an existing Alarm Wizard so that it can be edited. Choose the alarm wizard from the drop-down list

Type: Selects the type of Alarm Wizard. Choose "ACT VMD ALARM" for an activity detection, video motion detection (VMD) or alarm input wizard. Choose "Camera Fail" for the camera failure wizard

Wizard Name: Enter or edit a descriptive name for the alarm wizard.

Alarm Input Base: Enter or edit the type of trigger to be used by the alarm wizard. The list of usable triggers (keywords) is available on the Alarm Expression Keyword page. To view this page click on System – Status – About – Alarm Keywords – View



Base Channel: Where the trigger type is an alarm input this field sets the starting number from which the wizard will begin

Channel List: for activity detection and video motion detection (VMD) triggers this field contains the channel numbers which will be processed by the wizard. This field can be automatically populated with channel numbers *where no wizard is currently set* by clicking on the Auto Fill button. In this way activity detection for multiple cameras/alarm inputs can be set up simultaneously using the wizard.

Add Camera Title: If ticked, will add the camera name to any database entry action configured by the wizard.

Activity Extend Time: Used with the Activity Detection Trigger. Extends any momentary activity detected to the time in seconds entered in to this box.

VMD Extend Time: Used with the VMD Trigger. Extends any momentary VMD event to the time in seconds entered in to this box.

Alarm Extend Time: Used with the Alarm Input Trigger. Extends any momentary alarm event detected to the time in seconds entered in to this box.

User Append Active: A freeform list for appending actions on expression active. Tick on the box VMD to add Active Append Strings to VMD Expressions. Tick on the box Alarm to add Active Append Strings to Alarm Expressions.

User Append Inactive: A freeform list for appending actions on expression inactive. Tick on the box VMD to add Inactive Append Strings to VMD Expressions. Tick on the box Alarm to add Inactive Append Strings to Alarm Expressions.

Set: If ticked, actions will be taken if the detector is in SET mode (can be controlled using Alarm input 19, an SIA Alarm Panel or some other input).

Unset: If ticked, actions will be taken if the detector is in UNSET mode (can be controlled using Alarm input 19, an SIA Alarm Panel or some other input).

Activity Profile Change: If ticked, activity detection will change the recording profile from NORMAL to EVENT while activity detection event is active and then back to NORMAL when the event ends.

VMD Profile Change: If ticked, VMD will change the recording profile from NORMAL to EVENT while the VMD event is active and then back to NORMAL when the event ends.

Alarm Profile Change: If ticked, an alarm event will change the recording profile from NORMAL to EVENT while the alarm event is active and then back to NORMAL when the event ends.

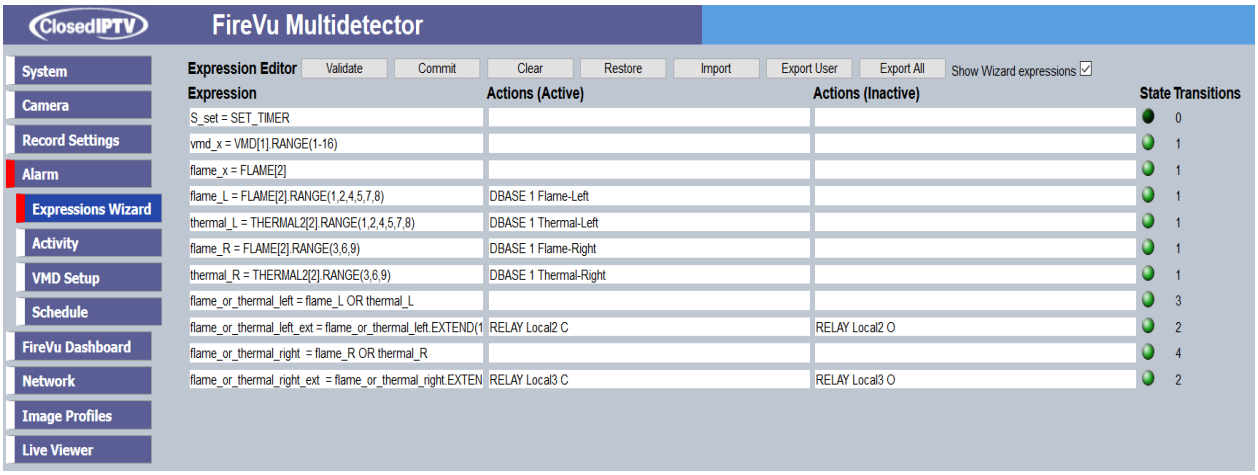
DB VMD Entry: If ticked a VMD event will create a database entry, allowing the event to be found by event searches of Enterprise Observer and Pick-a-Point Software.

DB Alarm Entry: If ticked an Alarm Input event will create a database entry, allowing the event to be found by event searches of Enterprise Observer and Pick-a-Point Software.

Report VMD: If ticked a VMD event will be reported to an RVRC.

Report Alarm: If ticked a Alarm event will be reported to an RVRC.

Alarm – Expressions Editor page



Expression: The first column in the page is used to enter the details of the alarm input or trigger which will cause the associated actions in the same row to take place.

All devices (physical or virtual) which can trigger events are named. One example is LOCAL_INPUT_1, which is physical alarm input number 1, connected to the main board of the detector.

Actions (active): The second column in the page is used to enter the required action desired when the expression in the left-hand column is true (active).

Actions (inactive): The third column in the page is used to enter the required action desired when the expression in the left-hand column is not true (inactive).

You can have more than one action, by separating the actions with a semi-colon.

The 'left-hand side' of the expression can be any unique label. In the above example “A”, “B”, “C” etc are used but the label can be anything as long as it is unique and does not clash with other labels.

Clear: Clears all currently programmed alarm expressions.

Restore: Restores all previously cleared alarm expressions.

Validate: Checks for any illegal values / none existent variables / names.

Commit: Saves the listed expressions.

Import: Allows expressions to be imported from a JSON file. This facilitates copying expressions made on another unit.

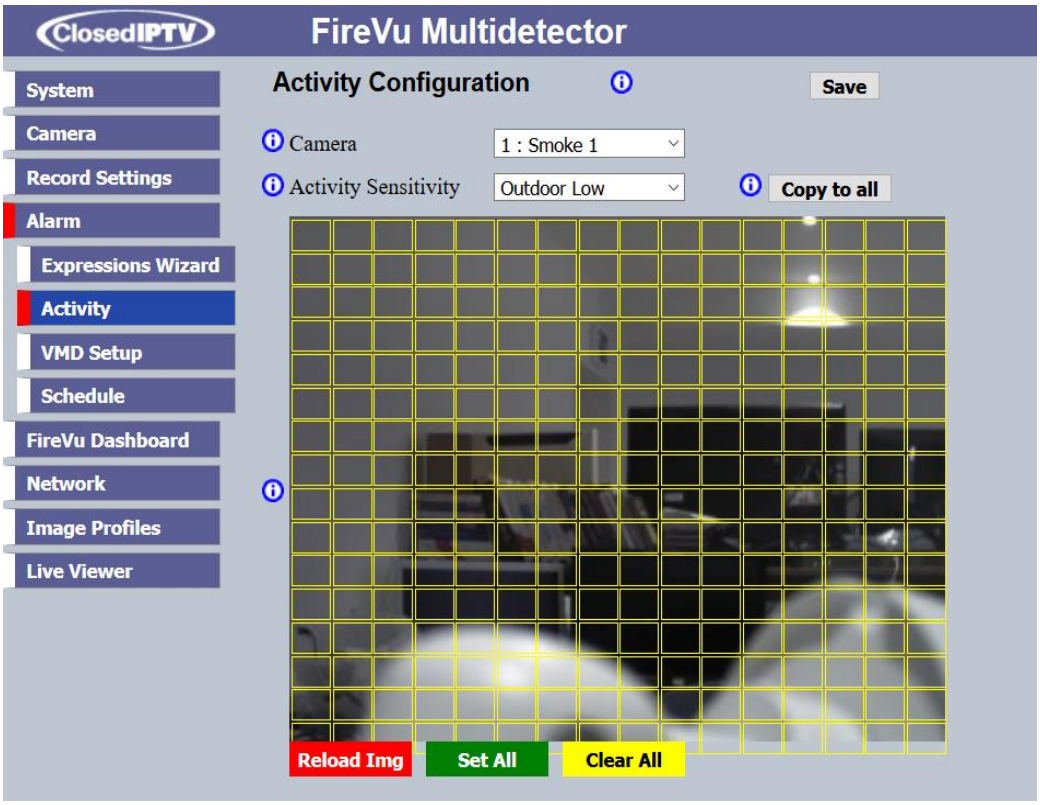
Export User : Exports user-created expressions to a JSON file.

Export All : Exports all expressions to a JSON file.

Show Wizard expressions: displays expressions which have been created by a wizard.

Alarm – Activity page

This Web-page enables cameras to be configured to automatically detect any movement or changes within the video scene and trigger a number of operations such as an increase in recording rate.



The video stream to be configured can be selected by clicking on the down arrow on the right-hand side of the Camera field and then clicking on the camera name from the drop-down list.

Activity Sensitivity: Used to set the level of sensitivity to activity in the scene. Click on the down arrow on the right-hand side of the field and then select the required sensitivity from choices in the drop-down list:

- Indoor high
- Indoor low
- Outdoor high
- Outdoor low
- Very low

Grid Editor: Use the Grid Editor by placing cells in areas of the camera view where movement will trigger an alarm. Use the mouse to navigate across the image, use the left mouse button to place a cell. Click on an active cell to deactivate it.

Clicking Reload Img (Red) will reload the image behind the grid editor.

Clicking Set All (Green) will set all the cells in the grid editor to active.

Clicking Clear All (Yellow) will clear (i.e. de-select) all the cells in the grid editor.

Click the Save button when you have finished, in order to save the changes that you have made.

Alarm – VMD Setup page

Video Motion Detection enables a greater degree of control over detection settings and configuration than the Activity Setup function. Each of the 16 VMD Zones can be directly sized and configured to suit specific requirements.

The camera to be configured can be selected by clicking on the down arrow on the right-hand side of the Camera field and then clicking on the camera name from the drop-down list.

There are 16 VMD zones within the image that can be individually configured.

VMD Zone: Select the desired zone from the drop-down list.

Mode: The zone mode controls when the reference image is taken for triggering. This can be one of the following choices, selected from the drop-down list:

- Normal: The reference image is updated approximately every second. 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 is best used under controlled lighting to avoid false triggers due to ambient light changes.
- Static: The reference image is collected on start-up and is never updated. This would be used in "sterile" areas where there are no changes expected.
- Pixel Count (%): Percentage of pixels in the selected zone that must change for the VMD event to be triggered. Default is 20%.
- Pixel Change (%): Percentage value of the overall change required, over the complete range of black to white, to be included in the pixel count. A 100% pixel change would be from black to peak white. Default is 20%.

To create a VMD zone:

1. Select the desired zone.
2. Position the mouse pointer at the top left-hand corner of the zone and then left click.
3. Move the mouse to the bottom right-hand corner of the zone and then right click.

A rectangle will then be displayed based on these two selected points.

Clicking Reload Img (Red) will reload the image behind the grid editor.

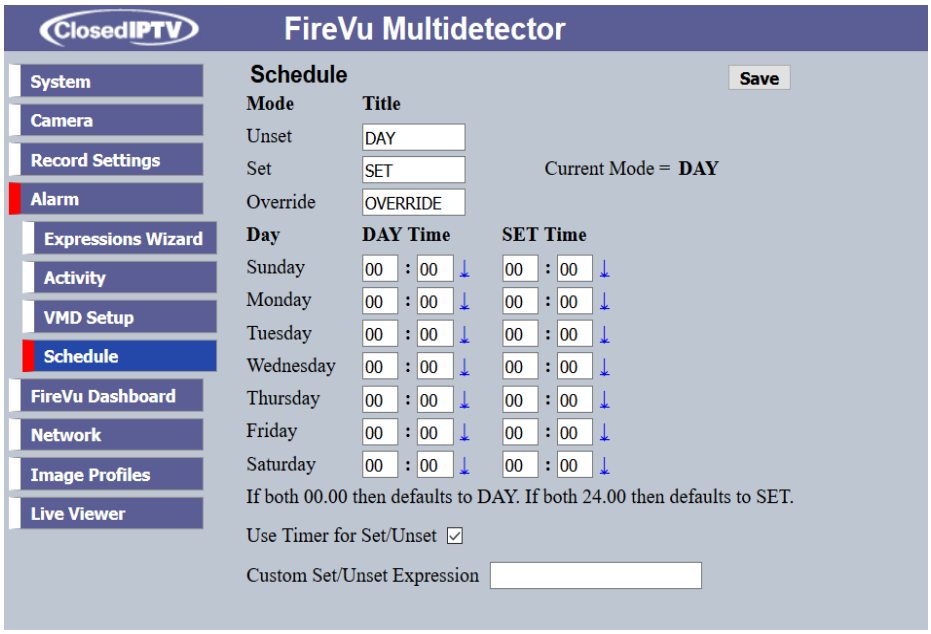
Clicking Clear All (Green) will clear (i.e. de-select) all the zones in the grid editor.

Clicking Default Grid (Yellow) will create 16 equally sized zones in a 4 x 4 grid with zone 1 in the top left-hand corner and zone 16 in the bottom right-hand corner.

Click the Save button when you have finished, in order to save the changes that you have made.

Alarm – Schedule page

The page configures how the NVR will move between two modes, SET and UNSET.



Using these two modes the detector can respond to the same stimuli (alarms, VMD etc.) in different ways, depending on whether the detector is SET or UNSET.

Use Timer for Set/Unset: When ticked, the times configured above will be used to change the detector from the Set to the Unset condition and vice versa.

FireVu Dashboard Web-pages

Listed below are descriptions of the Web-pages to be found by navigating to the "FireVu Dashboard" Web-page.

Parameters Web-page

There are two sets of parameters which can be configured for FireVu detection. The first set "SET 1" is always used, as shipped both SET 1 & SET 2 are configured with the same default settings.

By having a second SET of parameters a different level of detection can be employed as appropriate (for example a more sensitive set in unoccupied times) the switch between SET 1 and SET 2 can be initiated based on time or an external input.

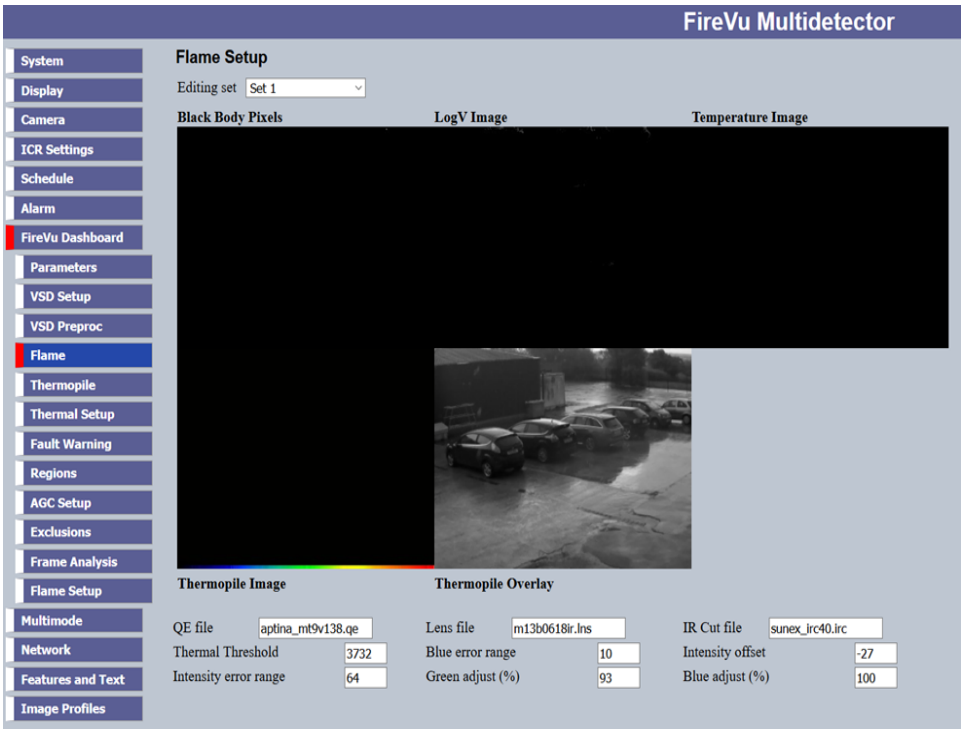
Within the "Parameters" web-page the user can define whether Low, Medium or High sensitivity levels are applied to each channel or detector input of the FireVu system using the "Camera" drop-down menu to select the detector channel to be configured.

Click the "Save" button when you have finished.

VSD Setup and Pre-Processor Web-pages

The "VSD Setup" and Pre-processor web-pages are engineering evaluation tools and changes to these pages can only be made by trained FireVu engineers.

Flame Web-page



The patented Flame algorithm utilises the detection and measurement of pixels conforming with the physical laws of a Black Body emitter. The 'colours' in a flame are the Black Body emissions from soot particles. While there are a number of parameters available, they rarely require adjustment, other than to ensure a match with the appropriate hardware / lens setup.

It is important that the correct calibrations are applied for a given lens, sensor, IR bandpass filter etc, which are configured below the algorithm indication images.

QE File – The Quantum Energy transform file for the CMOS sensor – currently only this device supported.

Lens File – Specific to the lens fitted.

IR Cut File – Specifies the transfer characteristics of the bandpass IR cut filter used. Currently, only this IR filter is in use.

Thermal Threshold – Specified temperature above which, or below which, an alarm will be tripped.

Blue Error Range – a threshold for determining colour against intensity. It may be appropriate to consider an increased value if flames with a chemical content resulting in a colour change are anticipated.

Intensity Offset – This is the intensity transform value, in this case for a lens at F4.0. (Note that Multi-Detectors an intensity offset of -27 is more typical as these operate at F1.4).

Intensity Error Range – Variation in intensity from the Planckian Locus value for that colour or temperature. A higher value gives greater tolerance due to dirt or contamination on the Detector lens, at the expense of a greater risk of false positives.

Green Adjust / Blue Adjust – Rarely requires adjustment – part of the overall colour and intensity

transform calculation.

The diagnostic screens show the black body pixels detected, and the apparent temperature according to the Planckian locus law calculation.

Black Body Pixels – Relative colours result in pixels potentially on the Planckian Locus.

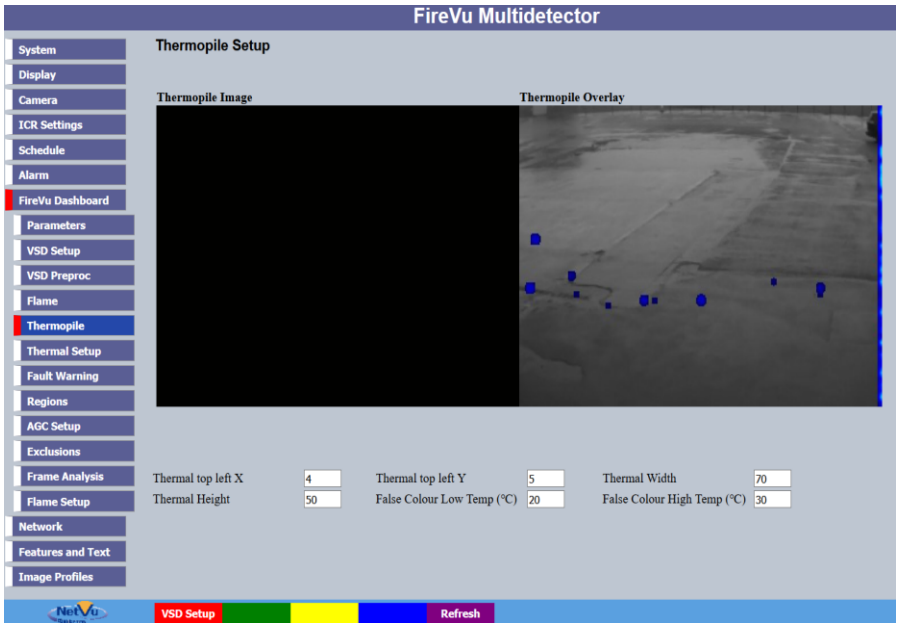
LogV Image – Log of the absolute value of the flame intensity. This indicates pixels sufficiently bright to be considered for a match to the Planckian Locus test.

Temperature Image – Colour and intensity within the intensity error range, and then subject to 'movement' threshold, tests to determine if it fully meets the flame detection requirements.

Thermopile Image – Displays the image as seen by the thermopile sensor.

Thermopile Overlay – Displays the thermopile sensor image superimposed upon the camera image. This highlights the location of any hot sports or flame detections

Thermopile Web-page

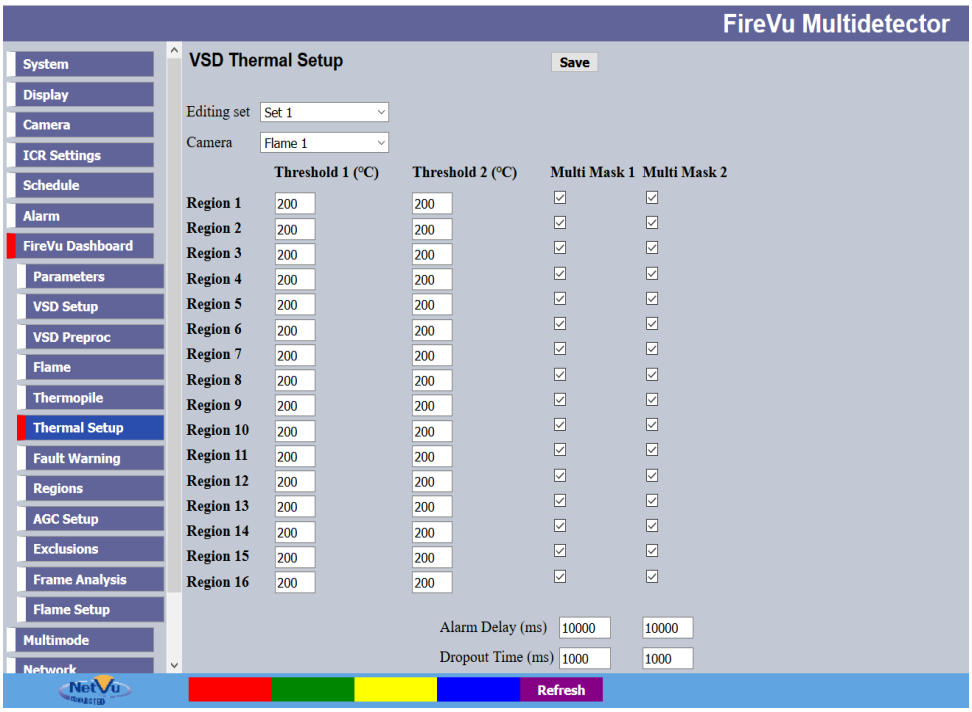


This Web-page is only available on the FireVu Multi-Detector. It allows the area to be monitored by the thermopile sensor to specified, as a rectangular region within the overall image, if required.

The region to be monitored is set by selecting the X and Y co-ordinates of the top left-hand corner of the image, by pixel. The width and height of the rectangle can then be selected.

The false colour scale (in Celsius) for the thermopile sensor image can also be set using this web-page. The "False Colour Low Temp" sets the blue end of the spectrum of false colours. The "False Colour High Temp" sets the red end of the spectrum of false colours

Thermal Setup Web-page



This Web-page is only available on the FireVu Multi-Detector. It enables the user to select the upper and lower temperature limits (in Celsius) at which the thermopile sensor will alarm for each region. See the section below on setting and adjusting regions for an explanation of "Regions" in FireVu.

Click the "Save" button when you have finished.

Fault Warning Web-page

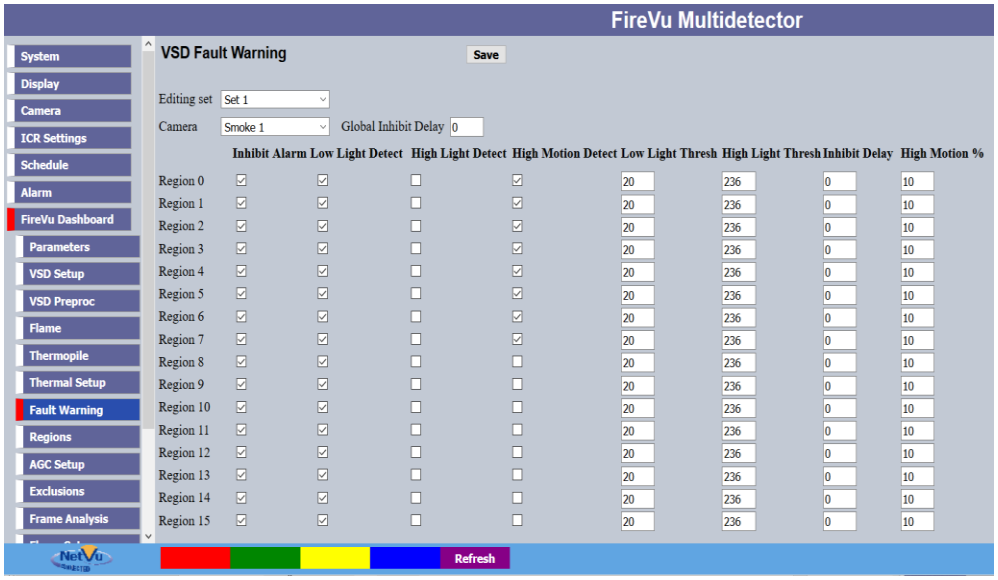
Bright light which is intense enough to saturate a detector sensor can result in a false alarm as the pixel changes within the image will appear similar to those of smoke to the smoke detection algorithm.

Consequently, the FireVu detector has a feature whereby any region where the user feels bright light may be present at certain times can be set to detect this bright light, this feature is called "high light detection". This feature can be enabled on a region by region basis on each detector using the "Fault warning" web-page.

At the top of the page is a "Set" drop-down menu which allows you to select the parameter to configure.

Having selected the relevant parameter set you can then turn on the "High Light Detect" on a region by region basis.

Having enabled the FireVu to detect a "High light" condition you then have the option of setting that region to be "inhibited" if the "High light" detection results in a false alarm. This means that a region identified as suffering from high light detection can be selected to not count towards an alarm vote until it is no longer suffering from the high light situation. A screen shot of the "Fault Warning" page described here is shown below:



Click the "Save" button when you have finished.

Low Contrast Trouble/Fault Indication

One of the methods by which FireVu's intelligent algorithms determine the presence of smoke is through a reduction in contrast within the monitored view.

As a result, for this method to be effective there needs to be a detectable amount of contrast within the detector view that can be measured. To assist in ensuring this is the case the FireVu detector is capable of providing a trouble or fault indication when there is insufficient contrast.

This warning is turned on by default, but by default will only provide a visual indication of areas of insufficient contrast when the detector's signal is viewed in NetVu Limited's Enterprise Observer viewing software.

Any region (monitored area of the detectors view) which contains insufficient contrast will become highlighted grey as a trouble/fault indication.

This can be used in one of two ways:

- A visual indication that areas within the field of view have very little or no detectable contrast.
- By enabling the "Inhibit alarm" option for the required regions within the "Fault Warnin " Web-page under the "FireVu Dashboard" section of Web-pages (see previous section in this manual), you can generate an output from the FireVu detector if or when any region loses its contrast.

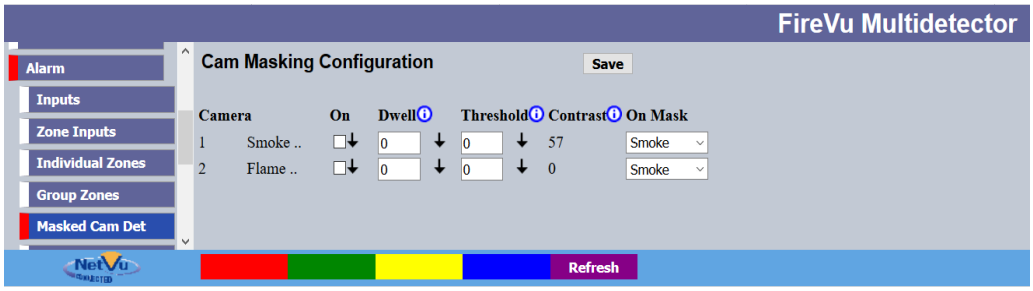
The second option listed above will create a system alarm when an area of the monitored view which usually has sufficient contrast for effective detection reduces in contrast. This will draw the user's attention to excessively dirty detectors or detectors that have gone out of focus, as either of these situations will erode the measurable contrast.

Focus Trouble and Detector Masking Indication

In addition to fault indications, the FireVu detector can be configured to provide an output if its image becomes unusable as a result of being masked (obscured). This could be as a result of the detector's view going out of focus, an excessive dirt build-up on the detector housing, or if a detector is deliberately covered over or closely blocked following some form of site activity.

By default, the detector masking detection is turned on and the instructions below can be followed. However, if the feature is ever turned off, then to turn it on again there is a tick box labelled "Camera Masking" in the web-page menu structure ("Configuration" then "System" then "Features"). Once turned on, the unit will ask to be reset. This reset has to be performed to enable the detector masking feature and make visible its configuration menu.

Following a reset, a "Masked Cam Detect" page will become visible within the unit's web-pages. This will appear under: "Configuration", "Alarm" then "Masked Cam Det", see image below:



From this menu the "Dwell" defines a period of time for which the system needs to have detected a "masking" of the detector before it will alarm. It is strongly recommended that this is not left set to zero as this may result in detector masked alarms every time a large object passes within the detector vicinity. A level of 5 (being 5 seconds) is advised as a minimum.

The "Contrast" column indicates a numeric representation of the current contrast within the detector image. If the detector is masked either fully or partially, this level will drop. This remains at the level detected when the page is first loaded, and so any changes in the contrast measurement whilst the page is displayed will not be seen. However, selecting the " Refresh " button at the bottom of the page will show if, or how, the contrast level is changing.

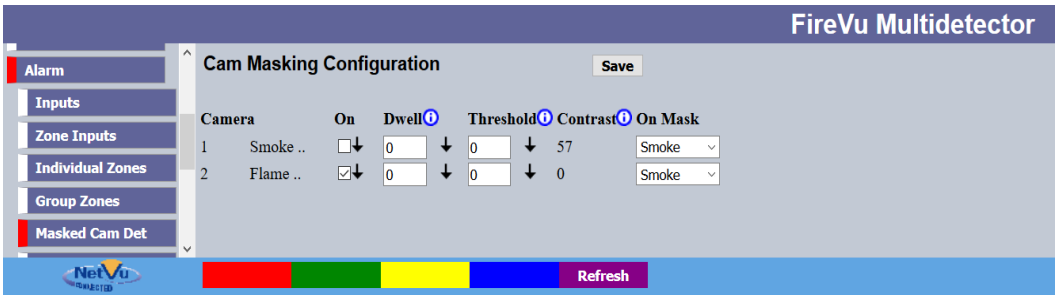
The "Threshold" is a user defined level at which, if the detected contrast drops below it, will result in a fault alarm.

When setting the threshold level consideration must be taken for how much the contrast level will vary for each scene throughout the day, as contrast may be affected by lighting levels and may differ between a colour image under natural light and the same scene but as a mono image under IR lighting. As a start point, it is recommended that the Threshold be set 3 or 4 points below the current measured level.

What happens when a masked detector is discovered is defined by a zone, the "On Mask" column allows the user to define which zone is activated and the results of that zones activation are then determined by what it is configured to do.

The "On Mask" column provides a drop-down menu option enabling you to select a zone to be activated following masking of the FireVu detector enabling the user to have an output which will determine which camera has gone into "mask" alarm. By default, this should be set to Zone 20 which is titled "Detector Masking" as detailed earlier in this manual.

In the example below, (from selecting "Alarm"> "Masked Cam Det" in the web-page menu), only camera 2 has been fully set up for "mask" detection, Zone 20 was selected as a Global Zone for a masked detection being named "Detector Masking".



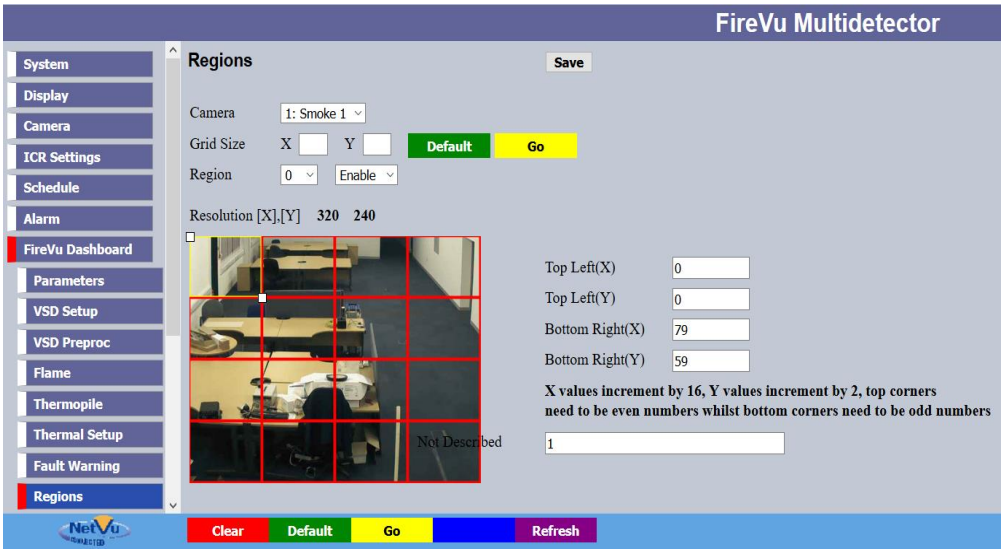
Click the "Save" button when you have finished.

Connecting to a FACP or BMS Requiring one single Trouble or Fault indication

It is recognised that in some applications the user may not wish to, or may not be able to, accept numerous inputs due to the number of inputs available to them on their Fire Alarm Control Panel (FACP), or building management system (BMS).

In such cases, outputs from the FireVu system are completely flexible and can be altered so that a trouble or fault state from any of the detectors will trigger the same relay contact.

Regions Web-page



The FireVu detector is capable of providing up to 16 detection regions, and as shipped each view is split into the maximum 16 as a 4 x 4 grid.

However, should the specific detector view to be monitored require it, these regions can be altered. They are in fact, fully configurable as to the number used, (1 to 16), their placement, their size, and how much of the detector's view they actually cover.

The act of breaking the detector's view down into multiple regions provides a high degree of flexibility and the ability to customise each and every detector's view to provide a highly robust detection with minimal false alarm risk.

There are three main benefits achieved with this method:

1. Areas within the detector's view which may cause false alarms, have visible steam or smoke present as part of a manufacturing or other process, or are simply not of interest can be excluded from the active analysis of FireVu's algorithms simply by not covering those areas with a region.
2. Regions can be sized and positioned so as to cover similar areas within each field of view, this may prove useful if needing to filter out non-smoke phenomena using the colour filtering tool.

3. Providing detectors are installed in accordance with NetVu Ltd.'s recommended best practice the upper half of the view will be capable of being more sensitive than the lower half of the view. This is achieved by using different parameters in the regions located above the half way mark and those regions located below the half way mark.

Note: Any area of the detector's view which does not fall within a region is NOT being monitored and smoke or flame present in such areas will not be detected until it spreads to areas that are within the detection zones.

The only rules relating to detection regions are:

- There must be at least one region
- They must not overlap
- They must be of a pixel size that is divisible by 8. If not, the configuration tool will highlight the region in red in the "region list" so that attention is drawn to it.
- They must be of a pixel size that is divisible by 8. If not, the configuration tool will highlight the region in red in the "region list" so that attention is drawn to it.

At the top of the regions page is a camera drop-down box, here you select the detector you wish to configure. On selecting a detector, the image from that channel will appear in the page and be overlaid with any existing regions. No overlay means no regions are set.

If no regions are present they can be added or created in a number of ways:

1. A grid or regions of equal size can be created by putting the number of horizontal and vertical regions required into the "X" and "Y" boxes beside the "Grid" text. (Note: maximum region count is 16 so the grid numbers must not result in a grid which would exceed 16 regions). The "Default" button will populate a 4 x 4 grid. Once the "X" and "Y" grid numbers are populated, select the "Go" button to create the grid overlay in the web-page, then select "Save" to save it to the FireVu detector.
2. Individual regions can be created by selecting the region in the "Regions" drop-down box and then selecting "Enable" in the other drop-down box, the region will then appear in a default grid position and can be amended from there if required.
3. Once created regions can be altered manually using the mouse by positioning the cursor over either the top left or bottom right corner of the region and then clicking the left-hand mouse button and dragging the cursor in the direction required to alter the region as wanted.

Note: If you attempt to set a configuration which would exceed 16 regions then only the first 16 will be created, starting from the top left and working across to the right and then down, if left this will result in an area starting from the bottom right of the view not being covered.

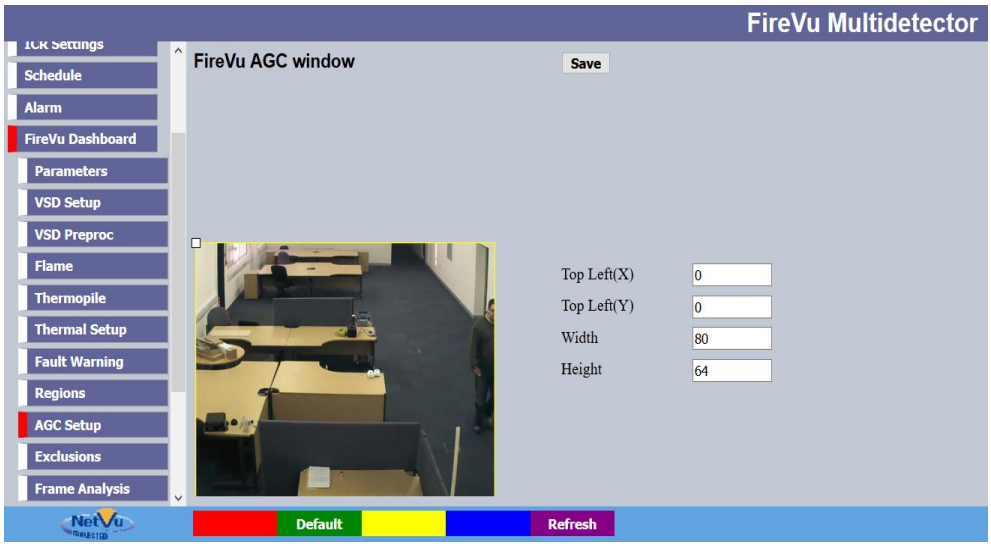
Once created regions can be moved and re-sized in two ways:

1. Select the region with the mouse from the drop-down “Region” menu and then adjust it as required by dragging the mouse cursor.
2. Select the region with the mouse from the drop-down “Region” menu and then adjust it as required by typing the new upper and lower X and Y co-ordinates for each corner of the region in the boxes labelled “Top Left X”, “Top Left Y”, “Bottom Right X” & “Bottom Right Y”. The X axis runs from 0 to 351 and the Y axis from 0 to 255.

Unwanted regions can be deleted by selecting the region from the drop-down “Region” list and then setting it as “Disabled” in the other region drop-down box.

Click the “Save” button when you have finished.

Regions Web-page

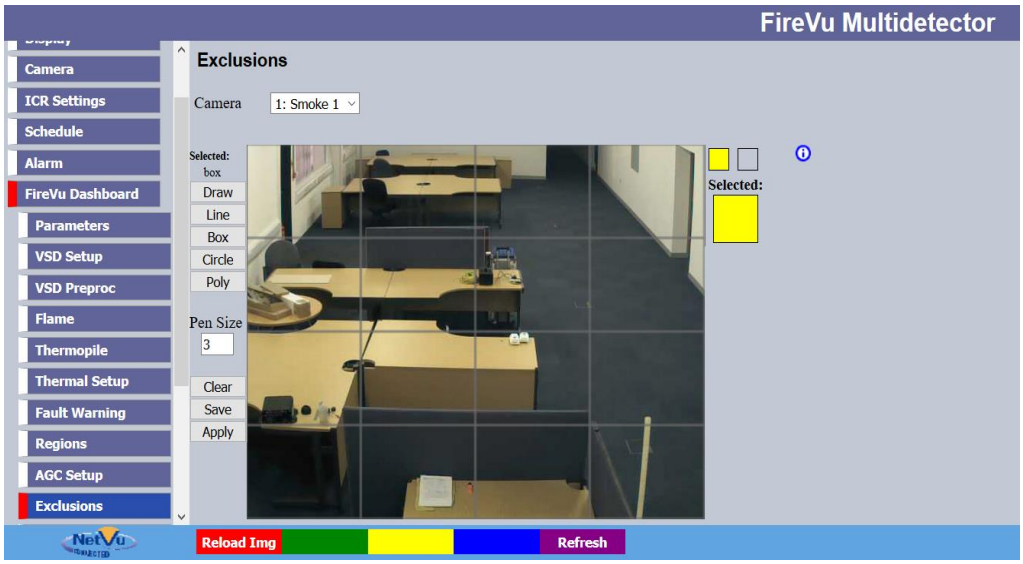


This allows definition of the rectangular area of the scene that controls the Video Automatic Gain Control (AGC). In the event that a detector has a field of view that is partially internal and partially external, it may be appropriate to determine the AGC operation based on just the internal element, and ignore the external lighting.

Setting the rectangular area is performed in the same was as setting the thermopile sensor monitored area, as illustrated above.

Click the “Save” button when you have finished.

Exclusions Web-page



As detailed earlier in this manual there are some scenarios which should be avoided within the analysed field of view of FireVu detector. In some cases, avoiding these using region placement can be difficult to achieve and as a result of the rectangular nature of the regions to remove areas from the analysed view in this manner can result in larger than required or "at risk" areas also not being analysed.

In such cases the regions should be positioned to cover the entire area and the section of the view not to be monitored should be "masked" using the manual masking feature. This feature is enabled and configured using the "Exclusions" Web-page.

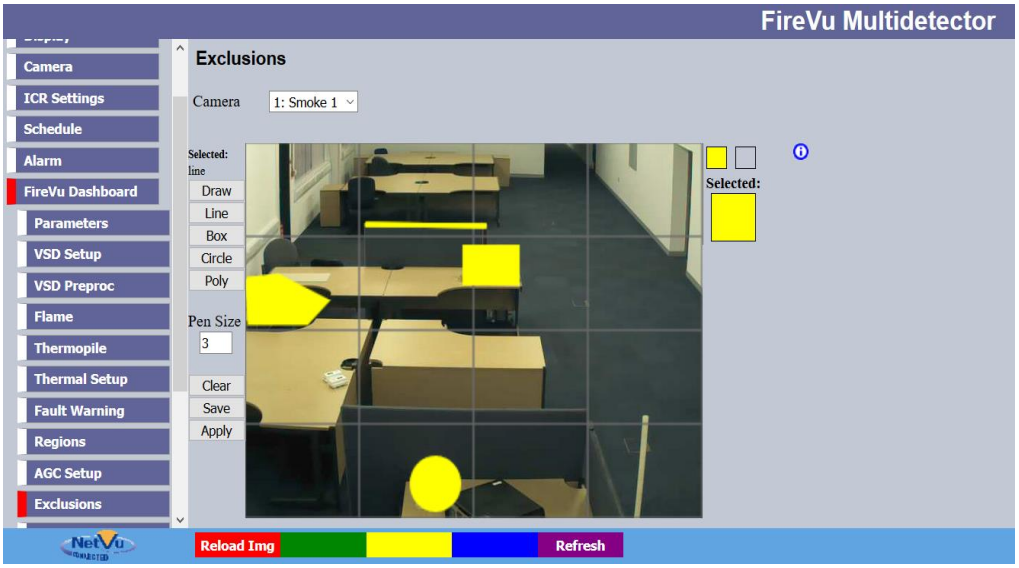
By factory default, (as supplied) there will be no area of the view excluded and the exclusion tab will appear as displayed above.

In order to set up a manual exclusion mask the steps to configure masking are as follows:

1. At the top of the page is a "Camera" drop-down menu, this selects the detector to be modified/have a mask implemented.
2. Areas to be excluded are yellow, whilst clear areas/areas displayed as the detector view are included.
3. You can now exclude any part of the detector view down to a pixel by pixel basis if required.
4. Using the upper five buttons in the web-page you can exclude areas as filled in shapes, rectangles, circles or polygons, alternatively you can exclude areas with lines of whatever length required or have full control using the "Free Draw" option.
5. The "Pen Size" button enables you to set a variety of sizes of cursor for exclusion using the "Line" or "Free Draw" options.
6. The "Clear" button clears an existing exclusion mask allowing you to start again, the "Save" button save the mask in the web-pages but does not apply it to the server, this allows

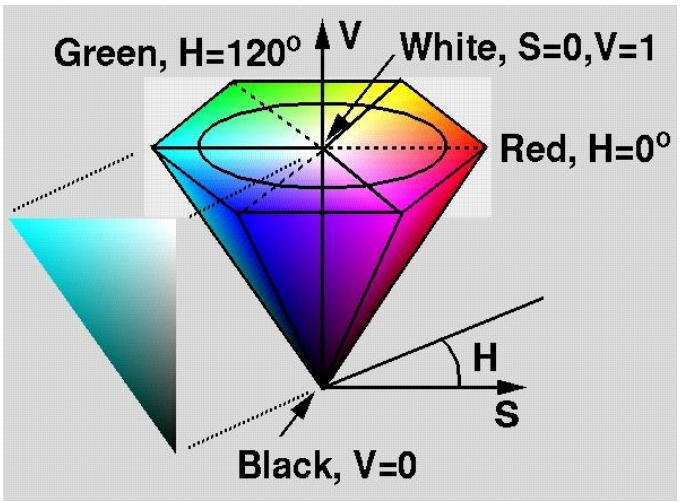
further configuration before applying it, then when finished the "Apply" button will save it to the FireVu server and apply it to the detector required.

Below is a screen shot of the "Exclusions" web-page, showing several different exclusion types:



Frame Analysis Web-page

In addition to being able to set a fixed mask up as detailed above the FireVu detector also has the feature of allowing you to dynamically exclude pixels within the field of view of the detector based on the Hue, Saturation and Value of a pixel, (HSV).
This allows for the exclusion of phenomena which may present similar movement patterns to smoke but which are brightly coloured and so can be distinguished from smoke on that basis. It also allows the exclusion of areas where bright lighting can periodically saturate the detector sensor.



Hue – angle around cone (by example, red is 0 degress).

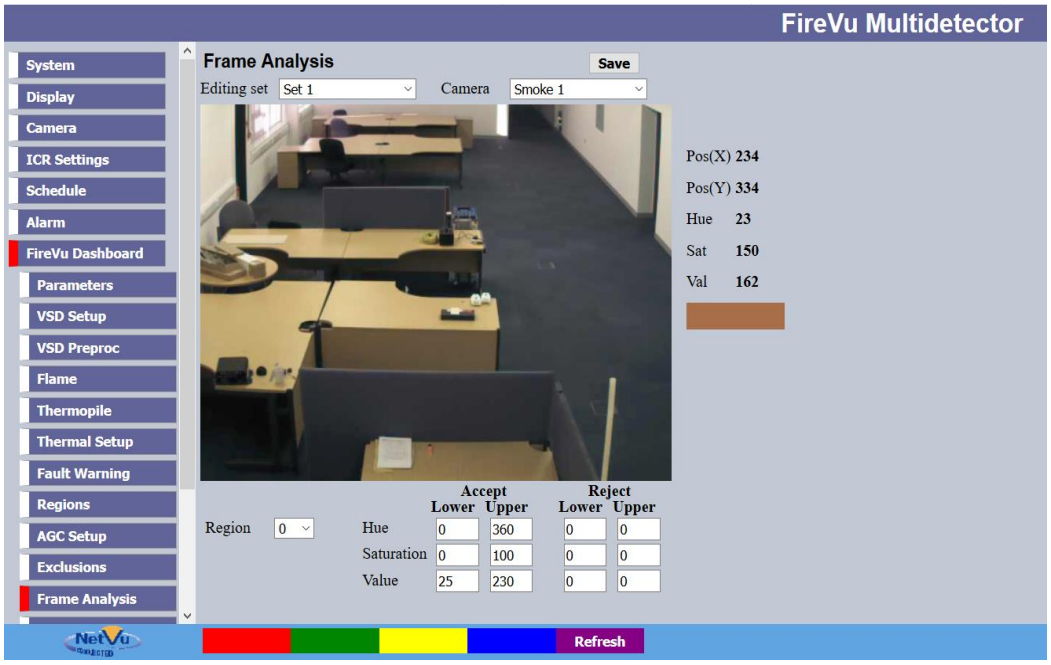
Saturation – how far from centre of circle. What position along radius you are at (0 at centre 255 on circumference of circle).

Value – How far up the "cone" (i.e. how bright the colour is 0 to 255).

This allows you to either reject pixels based on a range of H, S, or V or a combination of any of the three, or to only allow pixels based on a range of H, S or V or a combination of any of the three. From within this web-page you can limit the number of pixels analysed by either rejecting a range of pixels based on their Hue, Saturation or Value by setting a lower limit to reject from and an upper limit to reject to. This will exclude pixels within that H, S or V range leaving all pixels outside that range being analysed by the FireVu detector's algorithm.

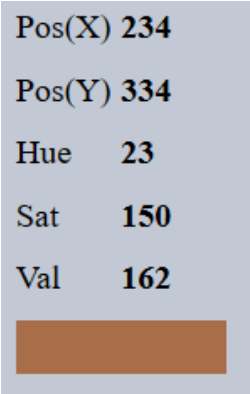
Alternatively, you can only accept a range of pixels based on their Hue, Saturation or Value by setting a lower range to accept from and an upper range to select to. Pixels with an H, S of V outside that range will be excluded from the FireVu detector's algorithms analysis.

A screen shot of the "Frame Analysis" web-page is shown below.



Establishing the relevant Hue Saturation or Value levels to either accept or reject can be achieved using the "Frame Analysis" part of this web-page.

At the top of the "Frame Analysis" web-page is a "Camera" selection drop-down box. This allows you to select the detector you wish to configure, and once selected a still image from the video connected to that detector input will be shown within this web-page.



If you hover the mouse cursor over the detector image the data shown to the right of the image will show the X and Y co-ordinates of the pixel the mouse cursor is pointing to and the Hue, Saturation & Value for the pixel at which the cursor is pointing.

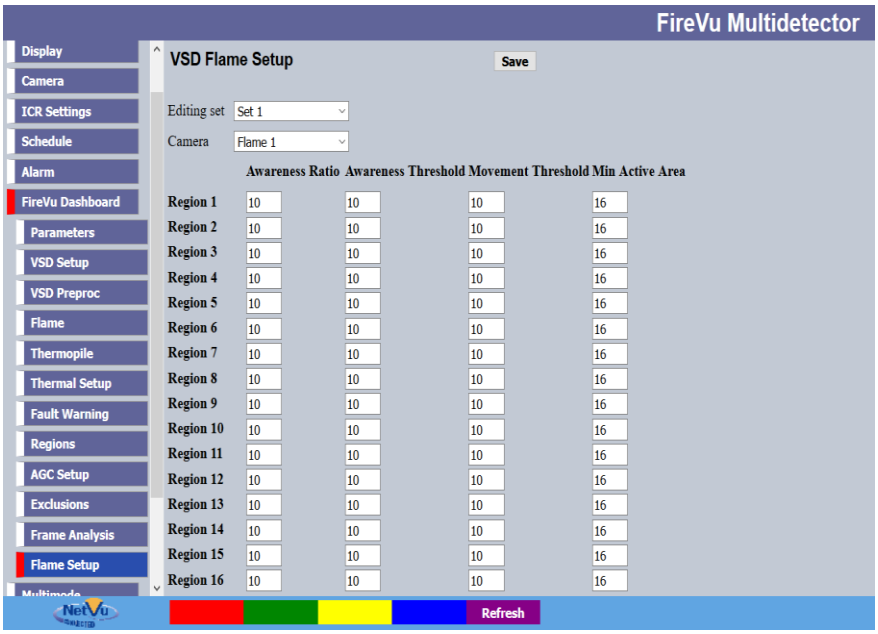
Using the "Frame Analysis" web-page you can run the cursor over similarly coloured areas and then either accept only those areas, or reject those areas, using the range of Hue, Saturation or Value seen in the data beside the image.

Whether you pick H, S or V will depend on the pixels of interest as you need to pick the characteristic which gives a close continuous range of values to either accept or reject.

Note: Colour Filtering is per region and so you will need to apply it to each region required, selecting the region(s) to which you wish to apply the colour filtering is performed using the "Region" drop-down menu below the detector screen shot and to the left of the H, S, V acceptance or rejection settings.

Click the "Save" button when you have finished.

Frame Analysis Web-page



Once the Black Body pixels representing the glowing soot particles in flame source have been identified, then further tests are made to determine if there are sufficient of them, and that they vary sufficiently.

The rate at which 'awareness' increases is set by the Awareness Ratio for each region, and then there is a threshold at which there has been sufficient changing activity of Black Body pixels to be determined as a Flame source.

If these thresholds are set too low, then a brief Black Body pixel match would result in a trigger. This may be a high intensity light, or even High-Visibility jackets reflecting sunlight. However, as a result of this processing, a continuing changing flame pattern has to be detected for a minimum number of pixels, represented by the Minimum (Min) Active Area.

The default Min Active area is 16 pixels, and is suitable for many circumstances, including the presence of high intensity yellow / orange beacons. This level would typically detect a standard (EN54-TF5) test pan fire (330mm x 330mm x 50mm (13" x 13" x 2") pan with 500ml (1.06 US Pints) of fuel) at twice the target distance.

The threshold can be reduced to as little as 8 pixels, giving greater sensitivity, resulting in detection of a standard test pan fire at three or more times the target range. However, in the event of fork lifts or similar with rotating beacons in the foreground there may be a small risk of false positives.

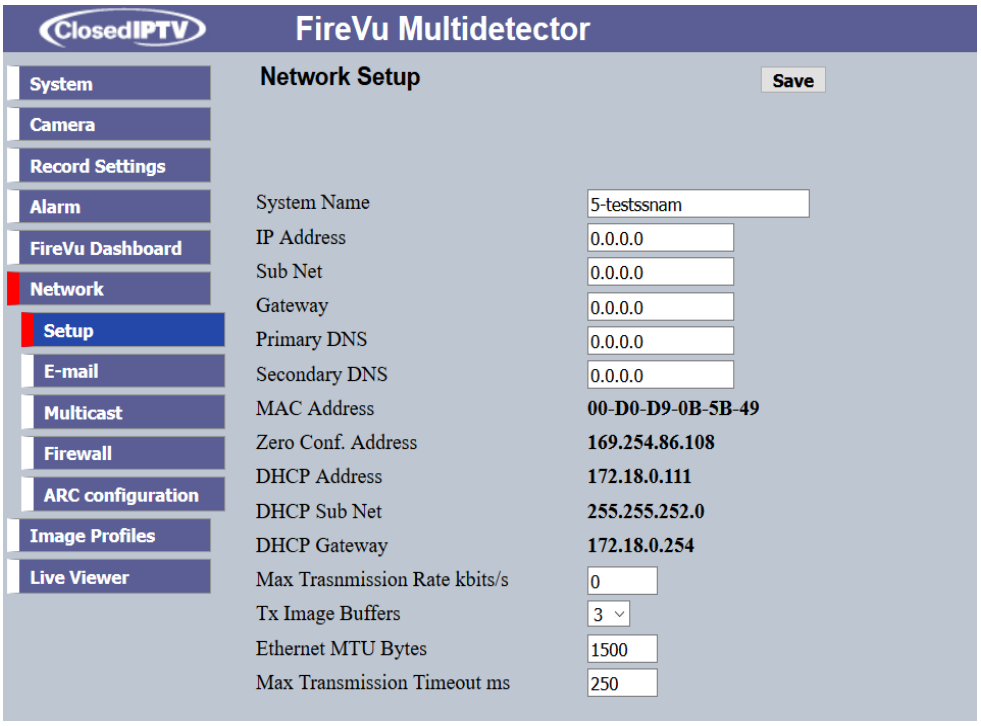
The preferred solution is to increase the lower row or two to 24 and 32 respectively which will still provide excellent protection to any flame sources in the foreground, while maintaining immunity from such sources, even if close to, and in the direct line of view.

Click the "Save" button when you have finished.

Network Web-pages

Listed below are descriptions of the Web-pages to be found by navigating to the "Network" Web-page.

Setup Web-page



This page is use to configure the network settings of the detector.

System Name – This field can be edited to allocate a name to the unit. This would be used if accessing the unit using a Domain Name Server (DNS). The setting is the same as the system name displayed in the System Attributes Web-page and defaults to the unit serial number.

IP Address – IP Address is a 32-bit number that uniquely identifies a unit on a TCP/IP network. To set DHCP usage and obtain an IP address from the general / corporate network set address to 0.0.0.0

Sub Net – Subnet mask is used by the TCP/IP protocol to determine whether the host communicating with the Annunciator is on the local subnet or on a remote network. Subnets are determined by the class (A, B, or C) of TCP/IP network and by how much the network has been further divided (subnetted), by a system administrator.

Gateway – If the unit communicates with a host on another subnet, it will talk through a device called a router which links the detector subnet to other networks, the IP address of this router is called a default gateway.

Primary DNS – This is the primary DNS server IP address for applications that are using domain names. If you want to use other DNS addresses from other units sitting on another domain on the internet you need to add the IP address of your domains DNS server. This is done in this Primary DNS setting. Adding the primary DNS server just means that the unit can use DNS names that that the primary DNS server can see. It should be noted that DNS works hierarchically such that firstly

any DNS enabled product will look at it local hosts.ini entries first. If it cannot find any reference there it looks in the DNS mapping in its primary DNS server and if it is not there this will be referred out further.

DHCP – If no IP address is set, the unit interrogates the network for a DHCP server, which assigns an available IP address. This IP address can change every time the unit is powered up. Therefore, it is recommended that DHCP be disabled by entering a suitable static IP address. You could use DHCP to locate a free IP address, then fix the unit IP address to the free one by entering the details into the IP address, subnet and gateway fields.

Max Transmission Rate (kbits/s) – Allows you to set the maximum transmission speed for the network type, consult the network administrator if necessary.

Tx Image Buffers – This is used in order to improve the picture delivery over Ethernet, use 1 for a low bandwidth connection, and 3 for a higher bandwidth. This limits the amount of frame buffering in transmission between Annunciator and client. This is used in order to improve the picture delivery over Ethernet when using a slow connection, e.g. 256Kbps. Options available are 1, 2 or 3 buffers.

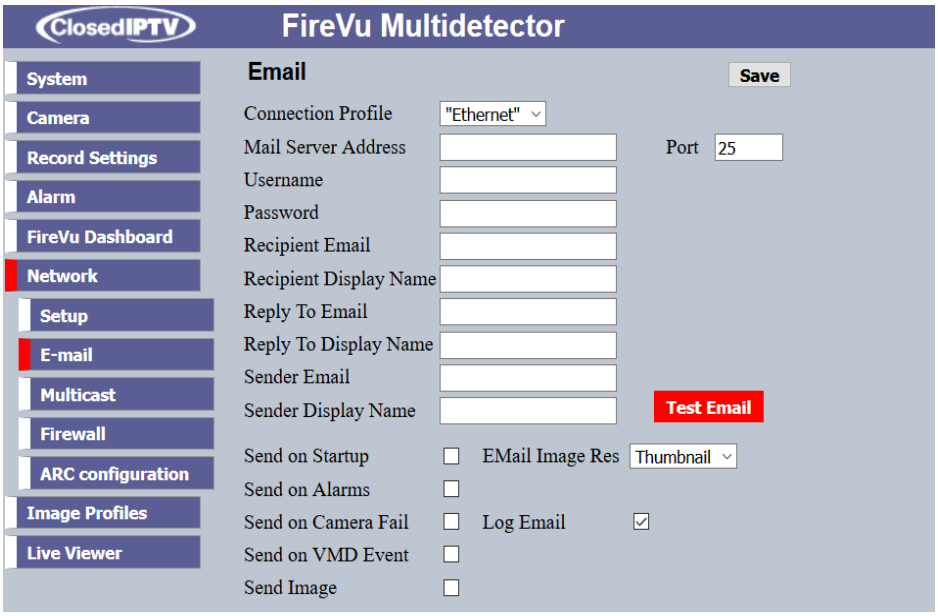
Ethernet MTU Bytes – The MTU is the largest physical packet size measured in bytes that the network can transmit, default is set at 1500bytes. This is the maximum transmission unit (MTU) in bytes of the largest packet that can be passed through the network interface. Typically, 1500 is a good default for most networks, speak to your network administrator if this needs to be matched to suit your network topology.

Max Transmission Timeout (ms) – This is the time (in milliseconds) the unit will wait to re send a packet if an acknowledgement is not received.

Click the “Save” button when you have finished.

Email Web-page

The detector has the ability to send emails in the case of a video smoke/flame detection or other event. This page is used to configure the settings to enable the detector to send emails.



Connection Profile: The name of the profile selected. Different profiles can be created so that different events send emails to different users.

Mail Server Address: The IP address or domain name of the mail server to be used.

Port: The port used on the mail server

Username: The User name of the email account to be used.

Password: The Password of the email account to be used.

Recipient Email: The email address to which the email will be sent

Recipient Display Name: The display name of the email recipient

Reply to Email: The email address which will be marked on the outgoing email

Reply to Display Name: The display name to be associated with the reply-to email address

Sender Email: The email address of the sender (will appear as “from”).

Sender Display Name: The display name of the sender (will appear as “from”).

Test Email: Click on this button to manually send an email and test the settings above.

Send on Startup: Tick to send an email on start up of the TransVu.

Send on Alarms: Tick to send an email when an alarm becomes active.

Send on Camera Fail: Tick to send an email if a camera failure is detected

Send on VMD Event: Tick to send an email when a VMD event becomes active.

Send Image: Tick to attach an still image of the primary alarm camera to the email.

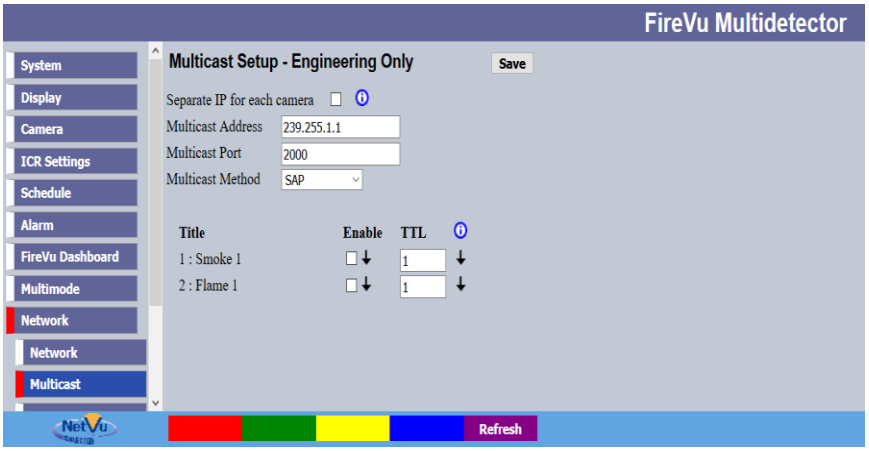
Email Image Res: Sets the resolution of an attached image, using image profile settings (choices are LO/MED/HI).

Log Email : Tick to include the sending of an email in system logs.

Multicast Web-page

In computer networking, multicast is group communication where data transmission is addressed to a group of destination computers simultaneously. Multicast can be one-to-many distribution, or many-to-many distribution.

Multicast should not be confused with physical layer point to multipoint communication.



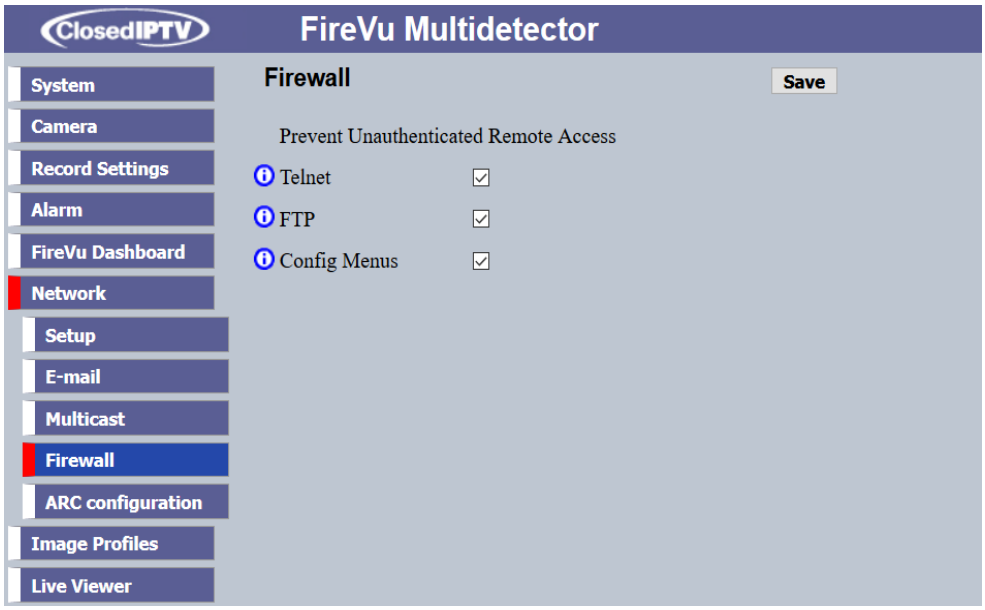
If the “Separate IP for each camera” box is checked then each detector will be transmitted with a different multicast address and the default port number.

TTL – The IP multicast routing protocol uses the Time-To-Live (TTL) field to decide how "far" from a sending host a given multicast packet should be forwarded. The default TTL for multicast datagrams is 1, which will result in multicast packets going only to other hosts on the local network.

Multicast datagrams with initial TTL 0 are restricted to the same host.
Multicast datagrams with initial TTL 1 are restricted to the same subnet.
Multicast datagrams with initial TTL 32 are restricted to the same site.
Multicast datagrams with initial TTL 64 are restricted to the same region.
Multicast datagrams with initial TTL 128 are restricted to the same continent.
Multicast datagrams with initial TTL 255 are unrestricted in scope.

Click the “Save” button when you have finished.

Firewall Web-page



This page prevents unauthorised remote access to the detector.

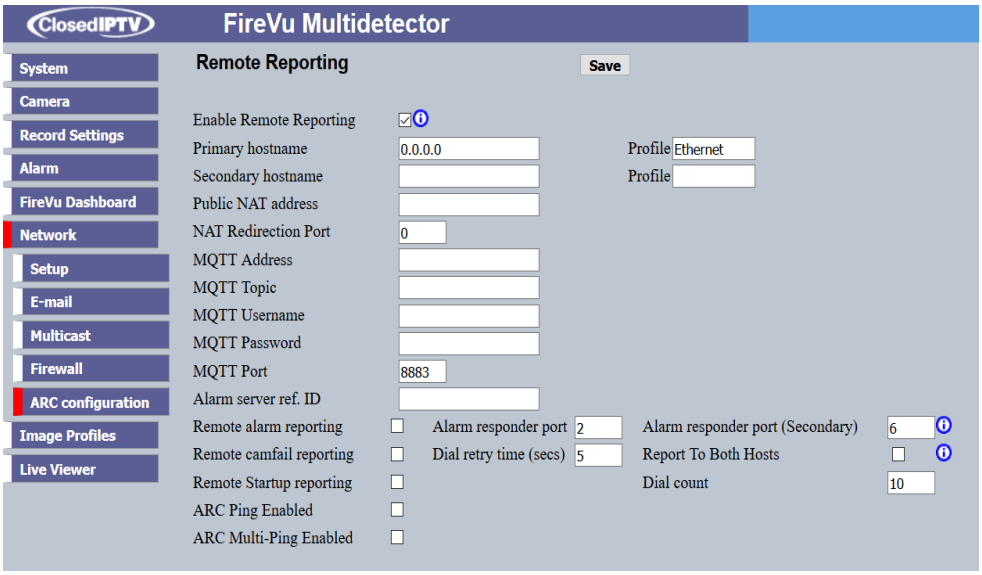
Telnet: If ticked, prevents remote users from logging in to Telnet if no username/password is set up.
FTP: If ticked, prevents remote users from logging in to FTP if no username/password is set up.
Config Menus: If ticked, prevents remote users from logging in to Configuration Menus if no username/password is set up.

ARC Configuration Web-page

The remote reporting function is used to send messages to an external device (e.g. an Alarm Receiving Centre (ARC), or building management / VMS server). The messages are sent as plain text in a Multipurpose Internet Mail Extensions (MIME) like format over the network using TCP.

The ARC Configuration Web-page is used to set-up the remote reporting function.

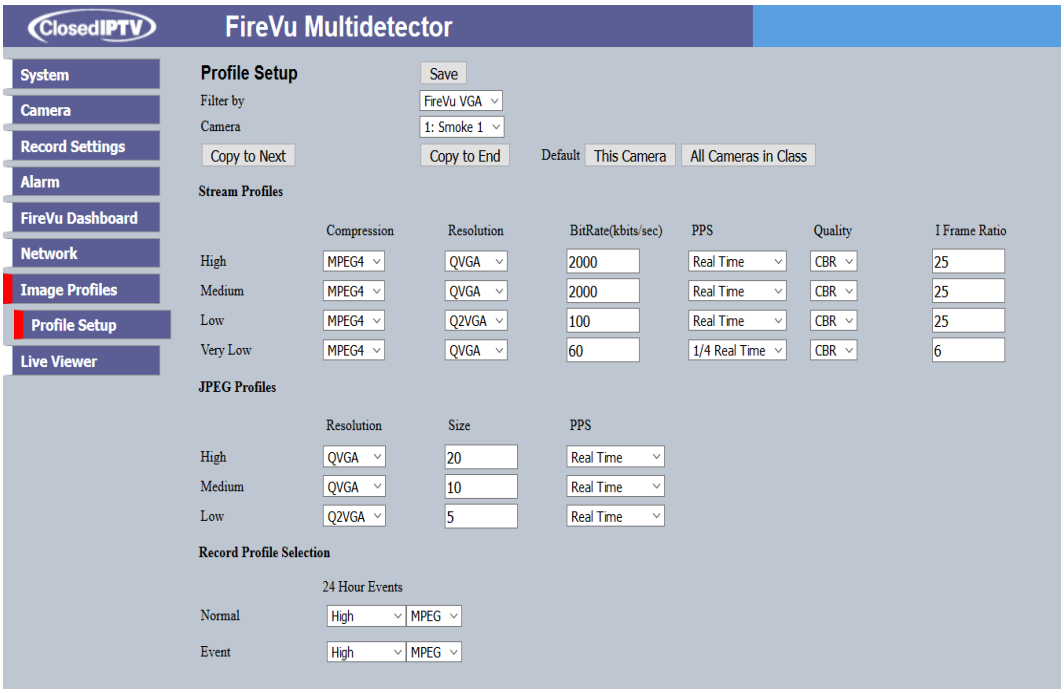
It is strongly recommended that all the remote reporting options are enabled (i.e. check; Remote alarm, Remote camfail, Remote Startup and ARC Ping Enabled tick boxes).



Enable Remote Reporting – When enabled the system will connect to the primary hostname (or secondary if the primary is not available) and send reports via the configured port. Changing this option requires a reboot.
Primary Hostname: The IP address or domain of the primary ARC host.
Secondary Hostname: The IP address or domain of the secondary ARC host.
Remote Alarm Reporting: When ticked, alarms will be reported to the ARC
Remote camfail reporting: When ticked, camera failure will be reported to the ARC
Remote Startup reporting: When ticked, a restart of the detector will be reported to the ARC
ARC Ping Enabled: Enables ping of the ARC by the detector.
Alarm responder port: Sets the alarm responder port of the detector.
Alarm Responder Port (Secondary) – If the secondary alarm responder port is 0 the server will use the primary alarm responder port number.
Dial retry time: Sets the time in seconds which will elapse between each attempt to contact an ARC.
Report to both hosts: When ticked, the detector will report to both ARC.
Dial Count: Sets the maximum number of times that the detector will attempt to contact an ARC.

Click the "Save" button when you have finished.

Profile Setup Web-page



This page configures the way in which the smoke detector video images and the flame detector video images are recorded. It gives four configurable options of recording performance: High, Medium Low and Very Low.

In each option the compressions format, resolution, file size, pictures per second, quality and I-Frame ration are adjustable.

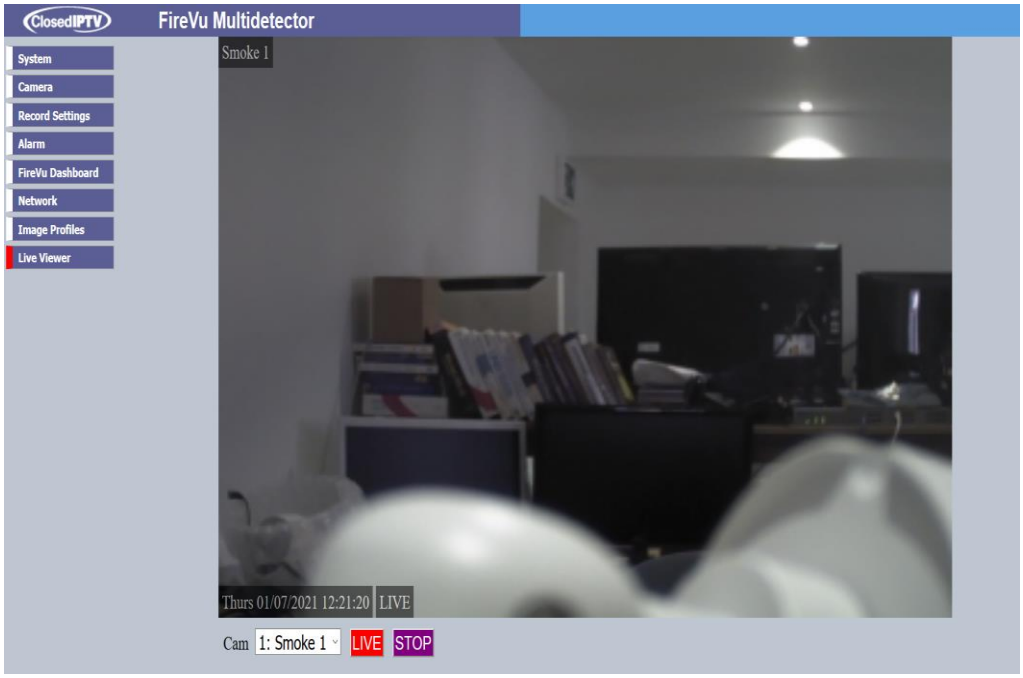
The profile to be used can be selected to change if the detector is activated (smoke detection, flame detection) – the "Event" setting, with a different recording profile for the rest of the time – The "Normal" Setting. These profiles can also be configured differently for day, night and weekend operation.

Different profiles can be selected for the smoke detector or flame detector. This is achieved using the "Channel" selector.

Click the "Save" button when you have finished.

Live Viewer Page

Live images from the detector may be viewed using this page.



Select the video stream to be viewed using the cam drop-down box at the bottom of the page. The resolution of the image may be selected using the res control.

Fault Finding, Maintenance and Support

Fault Finding

This section describes some tools and techniques which are helpful in fault finding a FireVu Stand Alone System.

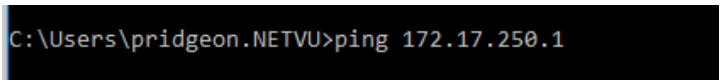
Detector cannot be found or viewed

If a detector cannot be found or it's images viewed then the best first step is to check whether the detector is actually active on the network. The simplest way to do this is to ping the detector. To do this connect a PC to the same network as the detector. Then, click on the windows start button and type **command prompt**. The following app should be displayed:

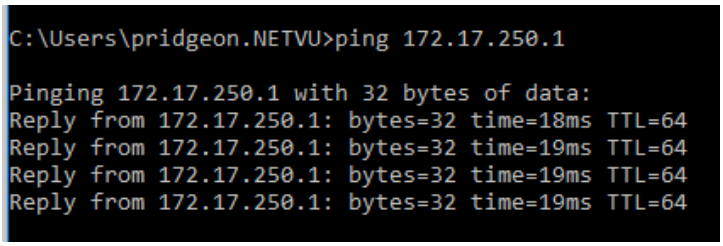
The command prompt window will open.

Type ping <the IP address of the detector> and then press **Enter.**

For example. If the detector had been set to an IP address of 172.17.250.1 you would type



After pressing ENTER the detector should respond



This means that the detector is active on the network and you should be able to type the IP address in to your browser and see the web pages of the detector.

If you get the following response:

Then the detector is not on the network and you should check the following things:

- Wiring of the detector
- Power supply to the detector
- Network connections to the detector

As these are the most common causes of this type of problem.

Maintenance

NetVu Ltd. recommend that any FireVu based system be regularly maintained.

The number of maintenance visits will vary from annual to quarterly subject to the nature of the site.

Details of the recommended actions to be carried out during a maintenance visit can be obtained on request.

Note: In addition to maintenance on the FireVu software and configuration the FireVu detectors MUST be kept clean and screen shots regularly checked to ensure the detector has not been moved or its image altered in any way.

After FireVu system commissioning and sign-off NetVu offers a full support package to ensure the correct ongoing operation of FireVu systems.

This includes the following:

- Telephone, email and remote support.
- Review of any operational anomalies and application of software upgrades and patches as required to maintain continued system integrity and security.
- Subject to review and agreement with the client settings will be updated with regard to ongoing features and best practice.
- Maintenance of backups and records of all system settings including the status of any specific settings varying from the standard default values and the basis for the change.
- At the request of the client (and subject to additional charge) monitor and support any regular system testing typically at six-month intervals.
- Download and have available for review, video from activations during times that minimal or zero false activations are otherwise anticipated, such as smoke detection out of hours.

To provide this support NetVu require remote network access to the system Gateway (FV2), or directly to the detectors which can be achieved through completely secure links, locked solely to the IP address of the NetVu headquarters network, so completely inaccessible from elsewhere.

While not mandatory, the placement of a remote support contract after system sign-off is strongly recommended as it will keep the FireVu system working at peak efficiency. Remote support contracts may be placed at a later time, but the process will be more expensive as a previously un-supported system will need to be onboarded and may also need re-commissioning, For full details and pricing of remote support please contact your local NetVu sales representative.

Accessories, Consumables and Spare Parts

Accessories and replacement parts are available from:

NetVu Limited,

№1 Thellow Heath Park,

Northwich Road, Northwich,

Cheshire.

WA9 6JB.

See https://netvu.org.uk /, e-mail support@netv.org.uk or telephone +44 (0) 1928 706400.

The components which make up a full FireVu IP system are listed below. However, not all elements may be deployed in all installations and those selected will be dependent upon the application and specific system design.

- Unlimited number of FireVu Detectors.
- Unlimited number of FireVu Multi-Detectors, with Built-in Thermopile sensor providing absolute temperature measurements.
- Unlimited number of Closed IPTV® Secure Network Extenders (8 way or 16 way).

- FireVu Annunciator module (FV2).
- Enterprise Observer video management software.
- Modbus Watchdog module.
- Optional – Modbus relay output module(s).
- Optional – Uninterruptible power Supply (UPS) / battery backup.

Several components listed above are referred to in this manual. However, the primary aim of this document is the use and configuration of the FireVu product itself, for the overall FireVu IP system please refer to "FireVu IP System Manual"

Trouble Shooting and Repairs

There are no user serviceable parts inside FireVu equipment.

On-site repairs can only be undertaken by a trained NetVu Ltd. Engineer or agent with express permission from NetVu Ltd. In all other instances,

FireVu equipment should be returned to NetVu Ltd in the original packaging for repairs.

Please contact https://netvu.org.uk , e-mail support@netv.org.uk or telephone +44 (0) 1928 706400 to arrange repairs of your FireVu equipment.

Safe disposal When Expired

Compliance with the UK Waste Electric and Electronic Equipment (WEEE) Regulations

NetVu Ltd is classed as a producer with respect to WEEE for 'users other than private households' under the Waste Electrical Equipment Regulations 2013. Regulation 12 places an obligation on NetVu Ltd to finance the costs of treatment, recovery and environmentally sound disposal of waste electric and electronic equipment (WEEE) from customers where that WEEE:

I. Is composed of equipment sold to our customers before 13th August 2005 and that is being replaced by products from NetVu Ltd of the same type or that perform the same function.

II. Is composed of NetVu Ltd equipment purchased by our customers after 13th August 2005.

Where NetVu Ltd is responsible for WEEE under scenarios (I) or (II) above, it is the responsibility of the customer to deliver the WEEE in question to NetVu Limited's chosen recycling facility, after which point we will accept any further treatment or recycling costs.

To arrange a collection of WEEE, please contact NetVu Ltd to allow us to ensure that the correct procedure can be applied.

Include contact information and any other details you consider relevant.

For the avoidance of doubt:

When customers wish to dispose of WEEE that is of equipment purchased before 13th August 2005, but is not being replaced by equipment of the same type or that performs the same function, then the customer retains responsibility for disposal under The Environmental Protection (Duty of Care) Regulations 1991.

When customers wish to dispose of WEEE that is of equipment purchased after 13th August 2005, then the original producer of the equipment retains responsibility for financing the costs of the collection, treatment, recovery and environmentally sound disposal, subject to the proviso that the responsibility has not been passed on to the customer through any contractual terms of the original purchase contract.

See https://netvu.org.uk/downloads/WEEE-B2B-Take-Back.pdf

Other Related Documents

This Manual is intended to support the initial installation and configuration of a FireVu being used in a default configuration.

FireVu is fully configurable when being set-up by a trained NetVu Ltd. FireVu agent and for such personnel further instructive documents are available.

See https://netvu.org.uk/ for any further information, or e-mail support@netv.org.uk or telephone +44 (0) 1928 706400

Glossary

AGC	Automatic Gain Control
ALPR	Automatic License Plate Recognition (US)
AMS	Archive and Management System
ANPR	Automatic Number Plate Recognition (UK and Europe)
AoE	ATA over Ethernet
ARC	Alarm Receiving Centre
ATA	Advanced Technology Attachment
BMS	Building Management System
BNC	Bayonet Neill–Concelman (connector used for coaxial cable).
CCTV	Closed-Circuit Television
CIF	Common Intermediate Format
CIP	Closed Internet Protocol
CIPTNET	Closed Internet Protocol Telnet
CMOS	Complementary Metal-Oxide-Semiconductor
CRT	Cathode Ray Tube
CSV	Comma Separated Values
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DoS	Denial of Service
DVR	Digital Video Recorder
EDP	Electronic Data Processing
EOL	End of Line
FACP	Fire Alarm Control Panel
FoV	Field of View
FQDN	Fully Qualified Domain Name
FSV	Fail-Safe Video
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
GUI	Graphical User Interface
ICR	In-Camera Recording (Edge Recording)
ID	Identity
IDE	Integrated Development Environment
IP	Internet Protocol

IR	Infrared
IRE	A unit used in the measurement of composite video signals
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MDNS	Multicast Domain Name System
MIME	Multipurpose Internet Mail Extensions
MTU	Maximum Transmission Unit
N/C	Normally Closed
N/O	Normally Open
NTSC	National Television System Committee (a colour encoding system for analogue television used in North America and Japan).
NVR	Network Video Recorder
ONVIF	Open Network Video Interface Forum
OSD	On Screen Display
PAL	Phase Alternation Line (a colour encoding system for analogue television).
PAR files	Video Partition files
PIR	Passive Infrared
PLC	Programmable Logic Controller
PoE	Power over Ethernet
PPP	Point to Point Protocol
PPS	Pictures Per Second
PSIM	Physical Security Information Management
PTZ	Pan-Tilt-Zoom
RTOS	Real-Time Operating System
RTU	Remote Terminal Unit
RVRC	Remote Video Response Centre
SAP	Service Access Point
SCADA	Supervisory, Control and Data Acquisition System
SIA	Security Industry Authority
SMB	Server Message Block
SNTP	Single Network Time Protocol
SoW	Scope of Work
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol / Internet Protocol

TTL	Time To Live
TVL	Television Lines
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
VSaaS	Video Surveillance as a Service
VESA mount	A family of standards defined by the Video Electronics Standards Association for mounting flat panel monitors, TVs, and other displays to stands or wall mounts.
ViSP	Visual Signal Processor
VLAN	Virtual Local Area Network
VMD	Video Motion Detector
VPN	Virtual Private Network
VSD	Visual Smoke Detection
UDP	User Datagram Protocol
UI	User Interface
WEEE	Waste Electrical and Electronic Equipment
WDT	Watchdog Timer
Zeroconf	Zero Conflict