Moxa VPort 26 User's Manual

First Edition, March 2012

www.moxa.com/product

Moxa VPort 26 User's Manual

Copyright Notice

Trademarks

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Moxa Americas
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa China (Shanghai office)
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Europe
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa Asia-Pacific
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Before Getting Started

Before using your VPort 26, please pay close attention to the following instructions:

- ❒ After opening the VPort 26 box, compare the contents of the box with the **Package Checklist in Chapter 1**. Notify your sales representative if any of the items are missing or damaged.
- ❒ To prevent damage or problems caused by improper use, read the **Quick Installation Guide** (the printed handbook included in the package) before assembling and operating the device and peripherals. You may also refer to **Chapter 1**, under **Product Description**, and all of **Chapter 2**, of this manual.
- ❒ The VPort 26 IP Camera has been designed for various environments and can be used to build various applications for general security or demonstration purposes. For standard applications, refer **Chapter 2, Getting Started**, and **Chapter 3, Accessing the VPort 26 Web-based Manager**.

Important Note

- ❒ Surveillance devices may be prohibited by law in your country. Since VPort is both a high performance surveillance system and networked video server, verify that the operations of such devices are legal in your locality before installing this unit for surveillance purposes.

Table of Contents

1

Introduction

The VPort 26 is a rugged IP camera designed for use in harsh environments. In addition to being able to handle basic video feeds, many advanced features are also included to set up surveillance or web multimedia applications. The VPort 26 is designed to provide stability, robustness, ease-of-use, and flexibility.

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Product Features**
- **Typical Application**
- **Product Description**

Overview

The VPort 26 series is a vandal-proof, IP66-rated, fixed dome IP camera designed for outdoor use. With SVGA (max. 800 x 600) resolution, H.264/MJPEG 3 simultaneous video streams, and a day-and-night camera lens, the VPort 26 series is well-suited for outdoor video surveillance applications.

To enhance video image quality, the VPort 26 series is equipped with a 2.8 to 11 mm vari-focal lens that meets any viewing angle and distance requirements. With the built-in removable IR-cut filter, and automatic switching from color to B/W images, the VPort 26 series is suitable for day-and-night use. With the addition of a 3D-DNR (3D Digital Noise Reduction) function, which can greatly reduce noises of video frames, and WDR (Wide Dynamic Range), the VPort 26 series provides clear images under back lit conditions. The optional De-mist function also ensures a good image quality in rainy, snowy, or hazy environments.

The VPort 26 series is specially designed for outdoor applications with the following features: IP66 rain and dust protection, high EMI/surge protection, -40 to 50°C operating temperature without a fan or heater required, metal housing, and vandal-proof dome cover. In addition, the camera is built in a dehumidified membrane for spreading out the moisture inside the camera. Users can choose either the model with PoE (Power over Ethernet, 802.3af) function, or the wired power input model with 12/24 VDC or 24 VAC.

The VPort 26 series is designed to provide both H.264 and MJPEG video streams and transmit up to 3 independent video streams (2 in H.264, and 1 in MJPEG) simultaneously. The camera is able to encode and transmit up to 30 FPS for each of the H.264 and MJPEG streams. Advanced network security functions, such as 802.1x and SSH, are also provided to prevent unauthorized access or data snooping, which is critical for most surveillance applications.

High Quality 1/3" SVGA CMOS sensor with advanced 3D_DNR, WDR and BLC

The VPort 26 IP camera uses a 1/3" SVGA CMOS sensor with 3D-DNR (3D digital noise reduction), WDR (wide dynamic range) and BLC (backlight compensation), which can provide clearer video image in many environments, especially in a low illumination (lux) environment.

Comes with 2.8 to 11 mm vari-focal lens, to meet a variety of viewing requirements

The VPort 26 IP camera is designed with a 2.8 to 11 mm vari-focal lens for providing viewing angles from 125.2° to 31.6° diagonal. In addition, this lens supports auto-iris functionality, and possesses day & night capability with IR-cut removable (ICR), which is suitable for most outdoor applications.

-40 to 50°C operating temperature without fan and heater

The VPort 26 IP camera can work in -40 to 50°C operating temperature range without the need of fan and heater, which can reduces the maintenance workload substantially, especially in the outdoor or harsh environments.

IP66-rated form factor design for protection against dust and rain

The IP66-rated form factor design makes the VPort 26 suitable for use in outdoor environments, without the need for additional protective housing. In addition, cable glands are provided free of charge to ensure that attached cables also have IP66-rated protection.

Support for PoE (Power-over-Ethernet) or direct-wired power inputs

The VPort P26 supports standard 48 VDC power-over-Ethernet (IEEE 802.3af), and the VPort 26 supports a direct-wired 12/24 VDC or 24 VAC power input.

High Performance H.264/MJPEG Video Compression

Video input can be efficiently compressed into H.264/MJPEG video stream packets in real time. This is done without sacrificing remote monitoring capability or storage. Five levels of compression quality and four different image resolutions provide greater versatility.

2-way audio supported for a complete surveillance solution

The VPort 26 series support both audio input and audio output for voice over IP communication between a field site and central site. The 2-way audio function not only saves time, but also saves the cost of needing to add additional communication devices (such as a phone).

Three video streams for meeting versatile application requirements

VPort 26 is a powerful IP Camera. Aside from the high quality H.264 video compression, it can also generate a maximum of three video streams: two H.264 and one MJPEG simultaneously, to meet the needs of specific applications. For example, the user can view the h.264 video streams with full D1 resolution at 30FPS, do MJPEG image analysis with full D1 resolution at 10FPS, and record the H.264 video streams with CIF resolution at 30FPS.

Video latency under 200ms (milliseconds) for more real-time video

In some mission critical environments, low video latency is a key requirement. For example, a highway transportation system monitors vehicles that are moving very quickly. The video display in the traffic control center needs to reflect actual current traffic conditions. Therefore, the video latency must be under 200ms.

SD Card for recording video locally when the network is down

The VPort 26 is equipped with an SD card socket (SDHC, V2.0) for local storage and offline data logging, in the event of network interruptions. Currently, the VPort 26 supports SD cards up to 32 GB.

RTSP for easy integration with existing systems

RTSP (Real-time Streaming Protocol) is a client-server multimedia presentation control protocol, which ensures interoperability among video devices and software. Hardware or software that supports RTSP streaming can easily identify and decode the video stream without the hassle of codec installation. For example, users can view video images from the VPort 26 directly with Quick Time and VLC, both of which support RTSP streaming.

Multicast (IGMP) transmission for network efficiency

Transmitting digital video images via an IP network requires many times the bandwidth required for transmitting general data. For this reason, the efficiency of network bandwidth management is one of the most important factors that determine the performance of a video over IP surveillance system. The VPort 26 supports multicast transmission with the IGMP protocol, which can reduce the bandwidth requirements when multiple clients access the same video stream, and greatly increases the efficiency of network bandwidth management.

Easy web access using standard browsers

There is no need to install new software to access the IP camera, since the embedded web server allows users to use any popular web browser to access the IP camera from anywhere over the Internet. As long as you are connected to the network, you will be able to view the same images seen by your cameras.

Built-in 3 area-selectable Video Motion Detection (VMD)

External sensors are not required, since the video image can be configured to detect motion in 3 areas, making it easy to set up a security system either in your office or in the field. And the customizable settings allow you to tune the system for both object size and sensitivity, making the IP Camera adaptable to different environments.

Weekly schedule for automated surveillance

The user-defined time period will check security settings on a weekly basis, and send notifications or drive external devices, making the VPort 26 suitable for more versatile applications.

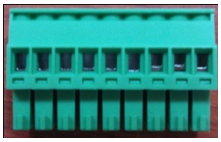
SDK support for developers

The high-performance IP camera can be integrated into many applications—without busting your budget—and the complete programming interface of the Moxa VPort SDK PLUS makes the developer's job easy and straightforward. To ask about SDK requirements, please contact a Moxa sales representative for details and an application form.

Package Checklist

The Moxa VPort 26 is shipped with the following items. If any of these items are missing or damaged, please contact your sales representative for assistance.

- 1 × VPort 26 or VPort P26 (Lens is included)
- Screw handle accessory package

Torx screw driver for attaching/detaching the upper case	4 sets of taping screws (6 cm length) and anchors	9-pin terminal block for DI/Relay/ Audio
		

- Cable glands accessories package

IP66 cable glands to ensure IP66 protection when the cables are connected


- Sticker for camera mounting positions

- Quick Installation Guide
- Document & Software CD (includes User's Manual, Quick Installation Guide, and VPort Utility)
- Warranty Statement

NOTE: *Notify your sales representative if any of the above items is missing or damaged.*

Product Features

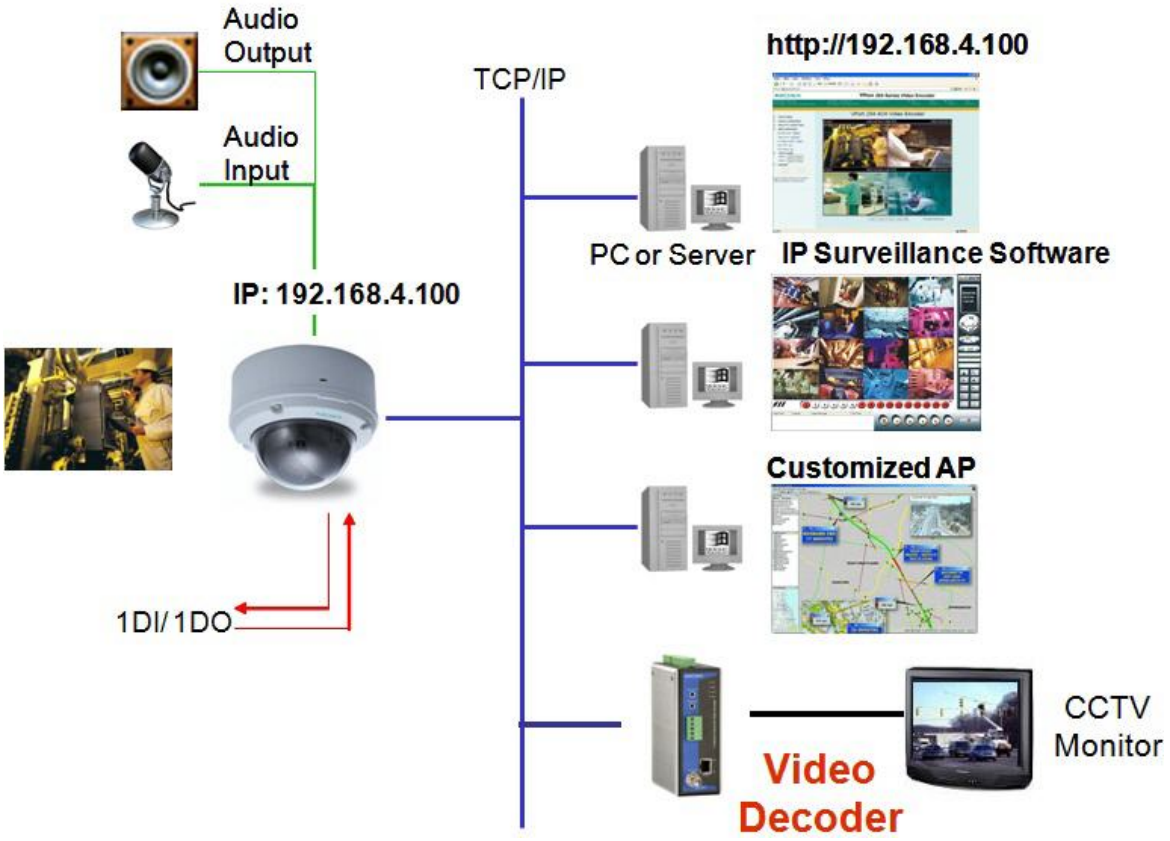
- 1/3" progressive CMOS sensor for SVGA (800x600) resolution
- Day and night viewing capability with ICR (IR cut filter) and color/black & white image switch
- Supports 3D_DNR (3D digital noise reduction), BLC (Backlight compensation) and WDR (wide dynamic range) for better image quality
- Built-in de-mist function for sharp images in rain, fog, and hazy environments
- Equipped with 2.8 mm to 11 mm vari-focal lens for wide-range fields of view

- Minimum illumination up to 0.01 lux at F=1.2 (AGC 30db and sense-up off)
- Image mirror and inverse
- 350° pan, 85° tilt and 360° rotate camera head angles for different installation positions.
- Support up to 8 privacy mask areas and 4X digital zoom
- Excellent Video/Audio streaming and network transmission performance
- Maximum 3 simultaneous video streams for H.264 and MJPEG codecs
- Video stream up to 30 frames/sec at SVGA (800 x 600) resolution (in single stream)
- DynaStream™ supported for optimal network efficiency
- Video latency under 200 ms
- 1 audio input and 1 audio output supported for video/audio complete surveillance solution
- SVGA/Full D1/ 4CIF/ VGA/ CIF/ QCIF resolution
- TCP, UDP and HTTP network transmission mode
- Supports RTSP Streaming
- Supports IGMP (ver.3) protocols for efficient network transmission
- Supports SNMP (V1/V2C/V3) for network system integration and management
- Supports QoS (ToS) for transmission priority
- Adjustable frame rate and bit rate control
- User-friendly IP filtering
- Supports IEEE802.1X for network access authentications
- Supports HTTPS and SSH for network transmission security
- UPnP Supported
- Maximum 8 unicast video streams, and 50 multicast clients
- Support multicast push for all multicast clients
- OnVIF standard support for compatibility with other IP video products
- Modbus/TCP supported for direct communication with SCADA system
- Rugged Design for Mission-critical Industrial Environments
- IP 66 form factor protection for rain and dust
- Model available with PoE (802.3af) or 12/24 VDC and 24 VAC power input, with LED indicators
- Panel mounting for ceiling, or outdoor installation kit for versatile installation method
- -40 to 50°C operating temperature for critical industrial environment
- No heater and fan for long MTBF
- Vandal-resistant with EN62262, IK10
- CE, FCC, UL60950-1
- 3-year product warranty
- Built-in Video Motion Detection (VMD)
- 1 DI and 1 Relay output (DO) for sensors and alarms
- Video loss and power failure alarm
- Pre, Trigger and post snapshot images supported
- Sequential pre-event snapshot images
- Sequential snapshot images supported
- Support SDHC slot for local storage with SD card in event recording
- Support SMTP and FTP for alarm message transmission
- Support HTTP Event Server
- Support for Moxa SoftNVR-IA IP surveillance software, a video recording and management solution
- Free MOXA VPort SDK Plus with CGI Commands, ActiveX Control and API support for third-party developers

NOTE If you are interested in Moxa's VPORT SDK PLUS, please go to Moxa's website www.moxa.com to download the package, or contact a Moxa sales representative for more information about this SDK

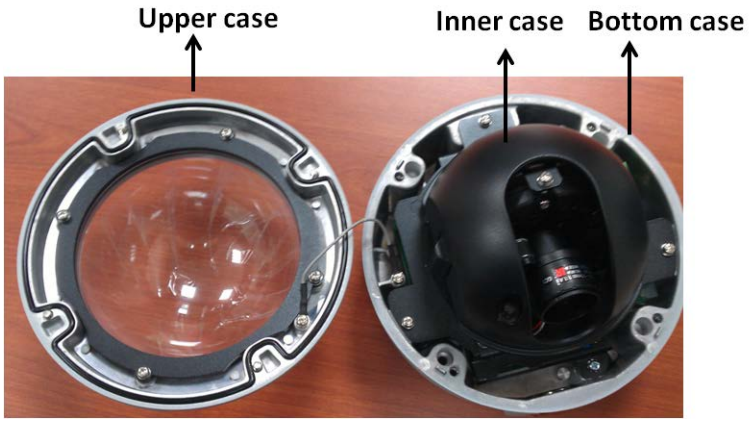
NOTE If you are interested in SoftNVR-IA IP surveillance software, please go to Moxa's website (www.moxa.com) to download the trial version.

Typical Application

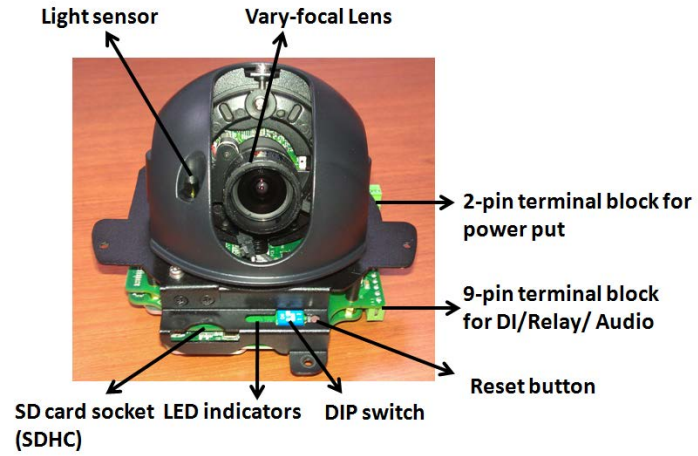


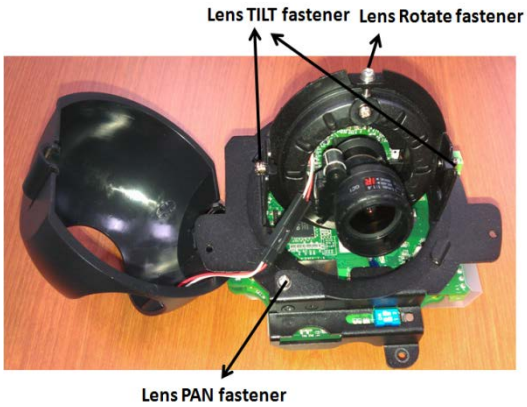
Product Description

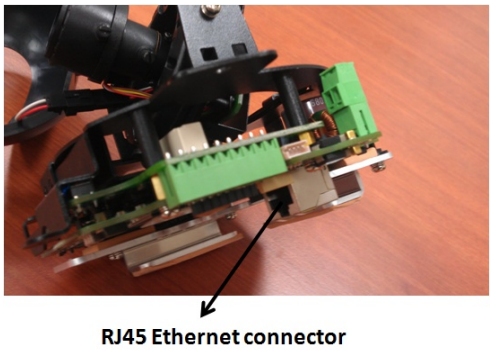
Form Factor



IP Camera Module

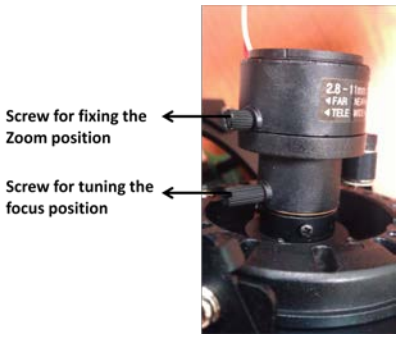






Vari-focal Lens

The VPort 26 series comes with a day and night 2.8 to 11 mm vari-focal lens for providing high quality video images. Users can adjust the Zoom and Focus manually to get clear images regardless of the site environment.



Pan, Rotation and Tilt Adjustment

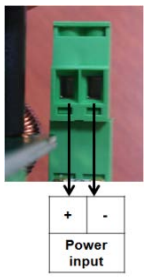
Use the pan, rotation and tilt fasteners for panning, rotating and tilting the lens angles. To do this, the screws must be loosened in advance. After the lens angles are correct, tighten the screws to fix the angles.

Light Sensor

The VPort 26 includes a light sensor for detecting illumination, which is for enabling the ICR (IR-cut filter removable) function. When the illumination is under 3 lux, the image will be switched to night mode in black and white, and when the illumination is greater than 5 lux, the image will be switched back to day mode in color.

2-pin Terminal Blocks for Power Input

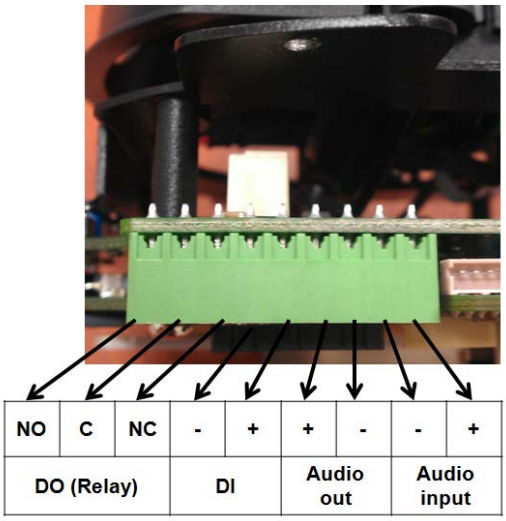
VPort 26 series has comes in two models: the VPort 26 is powered with 12/24VDC or 24VAC, and the VPort P26 is power with PoE (Power over Ethernet, 802.3af). This 2 pin terminal block is for the direct-wired power input of the VPort 26.



NOTE The specifications of the direct-wire power input are 12-32 VDC for 12/24 VDC power input, or 18-30 VAC for 24 VAC power input. The maximum power consumption is 11.7 Watt.

9-pin Terminal Block Connector for DI, DO, and Audio

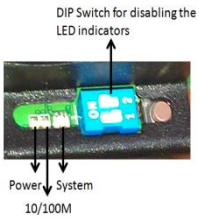
The VPort 26 supports 1 DI (digital input), 1 DO (relay output), 1 audio input (line-in or mic-in), and 1 audio output (line-out) through the 9-pin terminal block.



DO (Relay Output)	NO (Normal Open)	Max. 1A, 24 VDC Initial status is Normal Open
	C (Common)	
	NC (Normal Close)	
DI (Digital Input)	+	High: +13V to +30V Low: -30V to +3V
	-	

LED Indicators and DIP Switches

The VPort 26 has 3 LEDs for indicating the power status, 10/100 Mbps Ethernet link, and system status. In addition, one DIP switch (No.2) is provided for enabling or disabling the LED light for users who do not want the LED light to be visible at night.



LED	Description	
Power	On: power on Off: power off	
10/100 M	Amber: Ethernet link is 10 Mbps Green: Ethernet link is 100Mbps	
System	Red On	Hardware initialization
	Red blinking	Software initialization
	Green On	System boot-up successfully
	Green blinking	Firmware upgrade proceeding
DIP Switch 1	Reserved	
DIP Switch 2	On: LED light is on Off: LED light is off	

SD card Socket (SDHC)

The VPort 26 supports a standard SDHC interface for local storage with a current maximum size of 32 GB. The user can use an SD card which is fits this specification. Currently, the local storage supports triggered video recording when an event has occurred.

NOTE The VPort 26 supports a standard SDHC interface. Users can use SD cards suitable for this specification. Transcend or Sandisk SD cards are recommended, particularly Sandisk Extreme III SD, because of their rapid read/write speed.

NOTE To check if the SD card has been successfully mounted, access the VPort's web-based manager and check under system configuration-> Local storage.

Reset Button

The reset button is used to reset the camera hardware.

1. Reboot:

To reboot the VPort 26, power it off and then power it back on again, or push the RESET button one time. The System LED will light in red as the POST (Power on Self Test) process runs. When the rebooting process is finished, the System LED will change to a green color.

2. Restore to Factory Settings:

To restore the VPort 26 to the factory default settings, press the reset button continuously until the System LED blinks in red. After the system LED stops blinking, release the reset button. The POST process will run, and the VPort will reboot. The System LED will light in green when the VPort has finished rebooting.

RJ45 Ethernet Port

The RJ45 Ethernet port is for 10/100Mbps network transmission, in addition to PoE (power over Ethernet, 802.3af) power supply for VPort P26.

NOTE The VPort P26 supports standard IEEE 802.3af Power-over-Ethernet (PoE). The power input rating is 48V/0.11A, and the maximum power consumption is about 4.8W.

NOTE The equipment is designed for in building installation only and is not intended to be connected to exposed (outside plant) networks.

2

Getting Started

This chapter includes information about how to install a VPort 26 IP camera.

The following topics are covered in this chapter:

- **Before Getting Started**
- **First-Time Installation and Configuration**
  - Hardware Installation
  - Software Installation
- **VPort 26 Dimension**
- **Wiring Requirements**

Before Getting Started

In what follows, “user” refers to those who can access the IP camera, and “administrator” refers to the person who knows the root password that allows changes to the IP camera’s configuration, in addition to providing general access. Administrators should read this part of the manual carefully, especially during installation.

First-Time Installation and Configuration

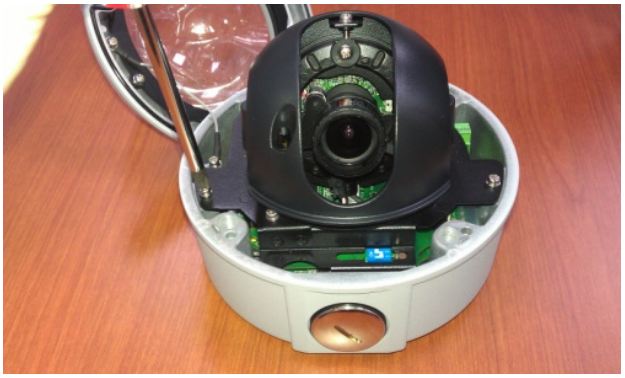
Hardware Installation

Step 1: Open and remove the upper case.

Use the security Torx to loosen the upper case screws.

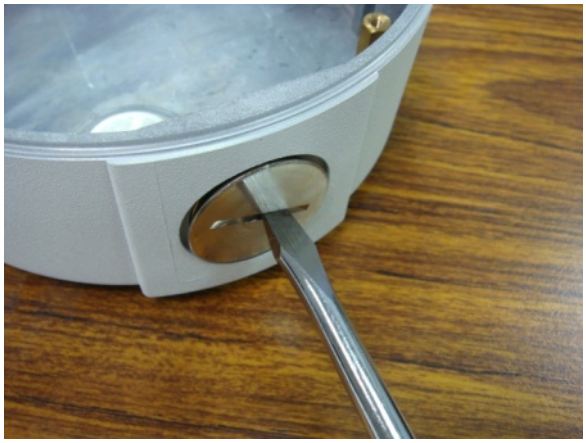
Step 2: Remove the IP camera module.

Loosen 4 screws, and take out the IP camera module.



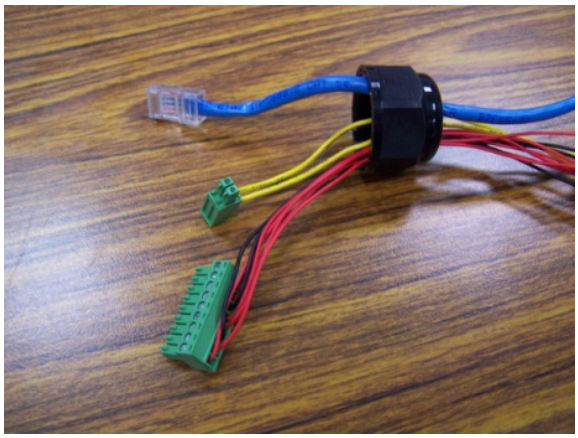
Step 4: Connect the cables.

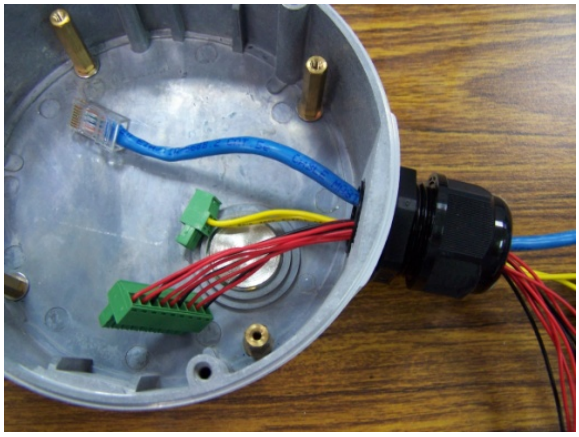
a) Open the conduit hole. (use the side conduit hole as example)



b) Prepare the cable gland (if required).

c) Use the cable gland to assemble the cables.

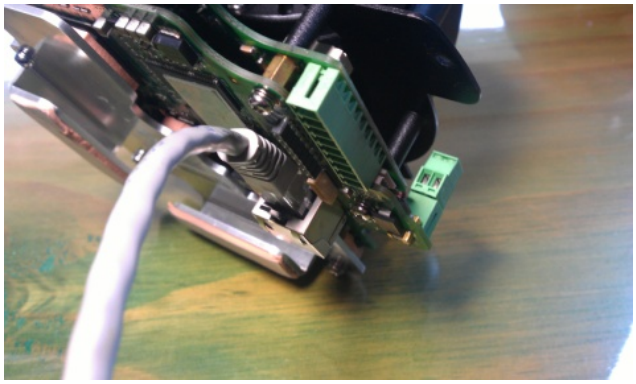


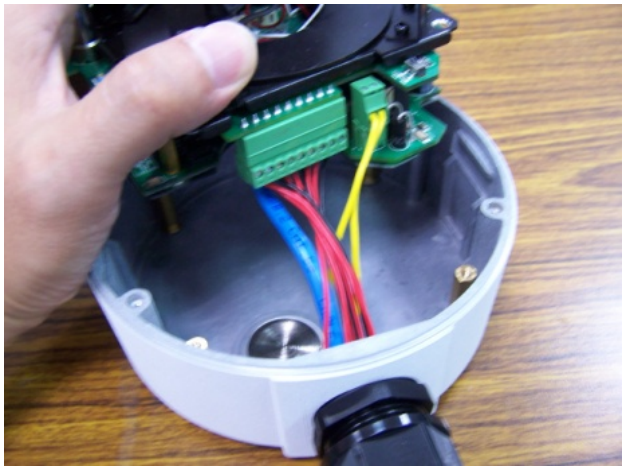


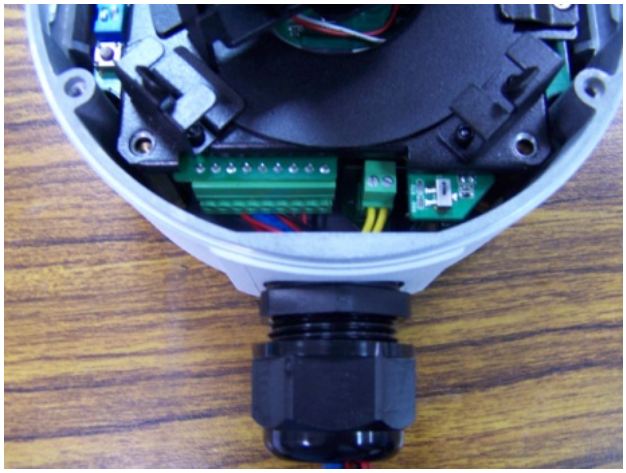
NOTE When installing the cable gland, make sure the 2 rubber rings are assembled properly for IP66 protection. If necessary, use silicon sealant.

d) Connect the cables to the IP camera module's connectors.

Remove the protective plastic film in the bottom of IP camera module. Then connect the Ethernet cable to RJ45 Ethernet port, as well as the terminal blocks with power line and DI /DO/ Audio lines (if used).







NOTE Be sure to arrange the cables carefully to make sure that all cables are connected properly. We recommend connecting the Ethernet cable first, and then the 9-pin terminal block. Connect the 2-pin terminal block last.

NOTE The conduit hole must face downward to provide the VPort 26 with IP66 protection against rain when installed in an outdoor environment.

Step 5: Mount the bottom case on the ceiling or accessory's mounting kit (VP-MK2)

a) Mounting on the ceiling

Step 1: Use the installation stick or attach the bottom case to the appropriate mounting location on the wall, and mark the positions of the four screw holes with a pen or a pencil.

Step 2: In the marked locations, drill a hole slightly smaller than the supplied screw anchors.

Step 3: Put anchors into these drilled holes.

Step 4: Fasten the bottom case with the four self-tap screws.

b) Mounting on the accessory's mounting kit (VP-MK2)

Step 1: Fasten the bottom case on the plate with the four machine screws, which are provided in VP-MK2's accessory package.

Step 2: Assemble the mounting kit with the selected accessory.

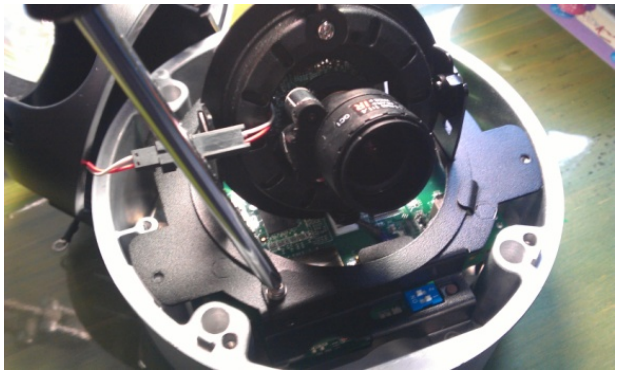
VPort 26 + VP-MK2 + VP-520L	VPort 26 + VP-MK2 + VP-520HB
	

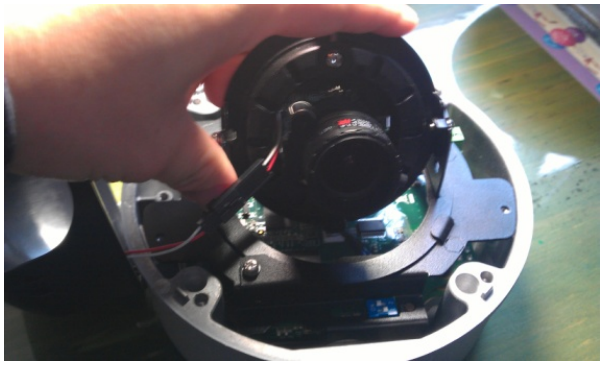
NOTE Choose the appropriate mounting accessories based on the installation requirements.

Step 6: Assemble the IP Camera Module with the bottom case.

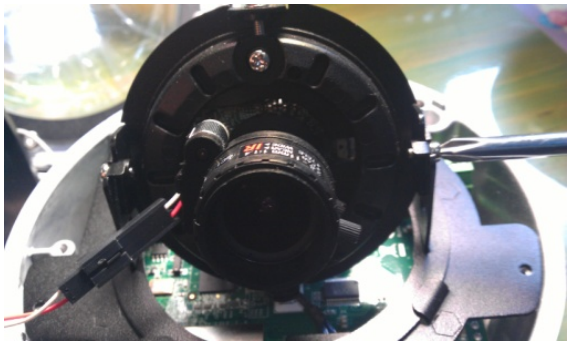
Step 7: To get the desired video image, adjust the angles and zoom strength.

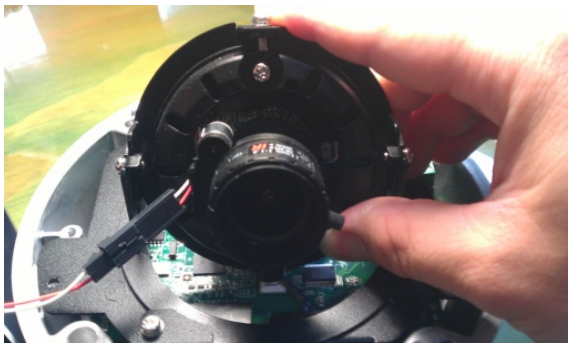
a) Pan adjustment



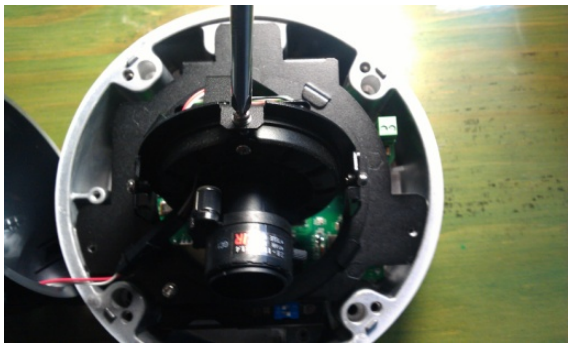


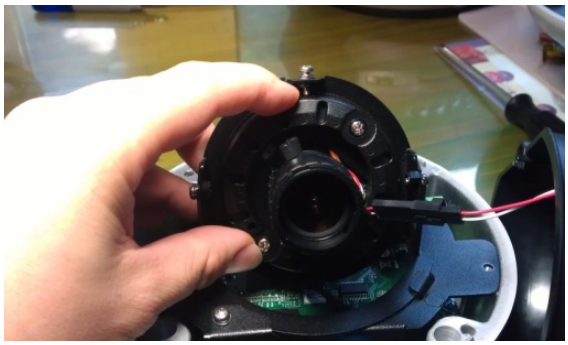
b) Tilt adjustment





c) Rotate adjustment





d) Zoom adjustment

Step 8: Fasten the upper case with bottom case to complete the hardware installation.

Software Installation

Step 1: Configure the VPort 26's IP address

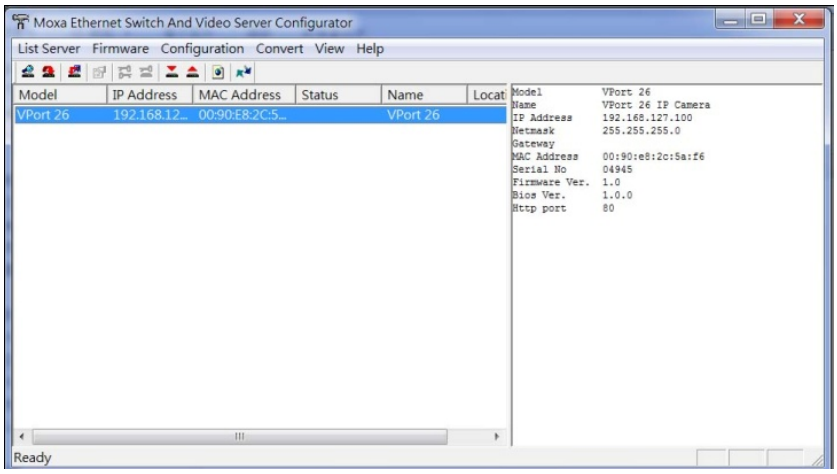
When the VPort 26 is first powered on, the POST (Power On Self Test) will run for a few moments. The System LED will turn green when the POST is complete. The 10 Mbps or 100 Mbps LED will then flash as the IP address is assigned. The network environment determines how the IP address is assigned.

Network Environment with DHCP Server

For this network environment, the unit's IP address will be assigned by the network's DHCP server. Refer to the DHCP server's IP address table to determine the unit's assigned IP address. You may also use the Moxa VPort and Ether Device Configurator Utility (edscfgui.exe), as described below:

Using the Moxa VPort and EtherDevice Configuration Utility (edscfgui.exe)

1. Run the **edscfgui.exe** program to search for the VPort device. After the application window opens, click on the **Search** button  to initiate a search.
2. When the search has concluded, the VPort's Model Name, MAC address, IP address, serial port, and HTTP port should be listed in the utility's window.



3. Users can double click the selected VPort, or use the IE web browser to access the VPort's web-based manager (web server).

Manual Address Assignment

If your VPort 26 is connected to a network that does not have a DHCP server, then you will need to configure the IP address manually. The default IP address of the VPort 26 is 192.168.127.100 and the default subnet mask is 255.255.255.0. Note that you may need to change your computer's IP address and subnet mask so that the computer is on the same subnet as the VPort.

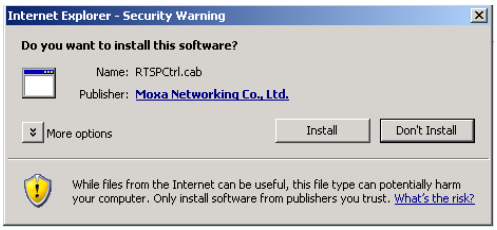
To change the IP address of the VPort manually, access the VPort's web server and navigate the **System Configuration → Network → General** page to configure the IP address and other network settings. Toggle the **Use fixed IP address** to ensure that the IP address you assign is not deleted each time the VPort is restarted.

Step 2: Accessing the VPort 26's web-based manager

Type the IP address in the web browser's address input box and then press enter.

Step 3: Install the ActiveX Control Plug-in

A security warning message will appear the first time you access the VPort's web-based manager. The message is related to installing the VPort AcitveX Control component on your PC or notebook. Click **Yes** to install this plug-in to enable viewing of video images over the IE web browser.



NOTE For Windows XP SP2 systems or later, the ActiveX Control component will be blocked for system security reasons. In this case, the VPort's security warning message window may not appear. Users should access the operating system control panel to unblock ActiveX controls or disable the security configuration to enable the installation of the VPort's ActiveX Control component.

Step 4: Access the VPort 26's web-based manager.

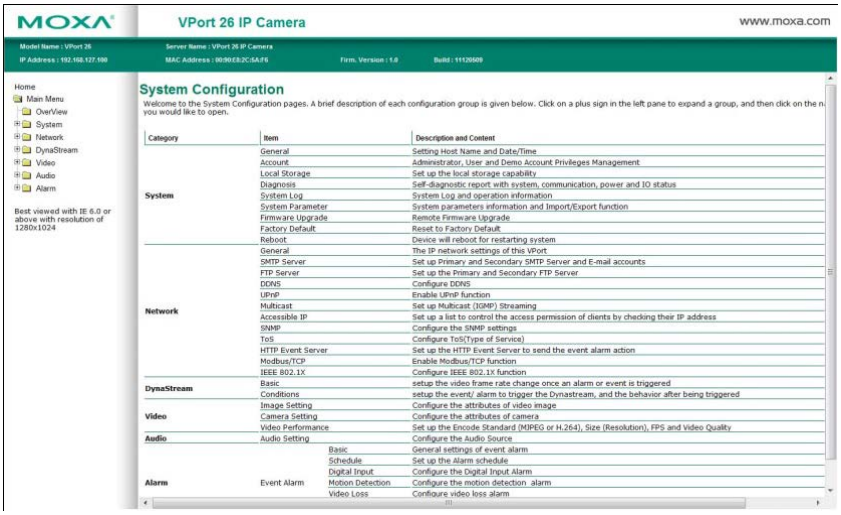
After installing the ActiveX Control component, enter the IP address of the VPort device to access its web-based controls; they should immediately appear. Check the following items to make sure the system was installed properly:

1. Video Images
2. Audio Sound (make sure your PC's or notebook's sound is turned on)
3. Video Information

Step 5: Access the VPort system configuration.

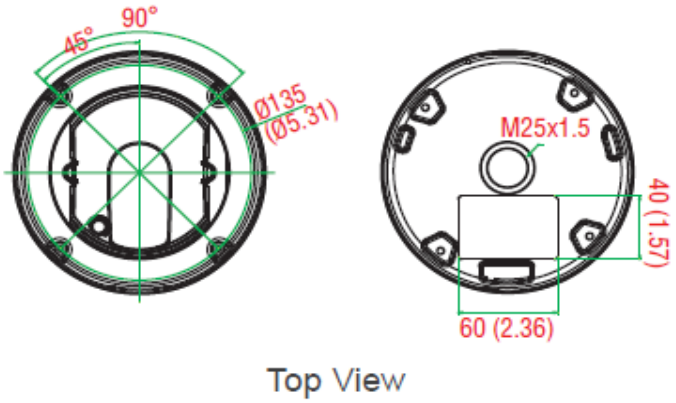
Click on **System Configuration** to display a system overview. The **Model Name**, **Server Name**, **IP Address**, **MAC Address** and **Firmware Version** will appear in the green bar at the top of the page. Use this information to review the installation details.

For details about configuration settings, check the User's Manual on the software CD.

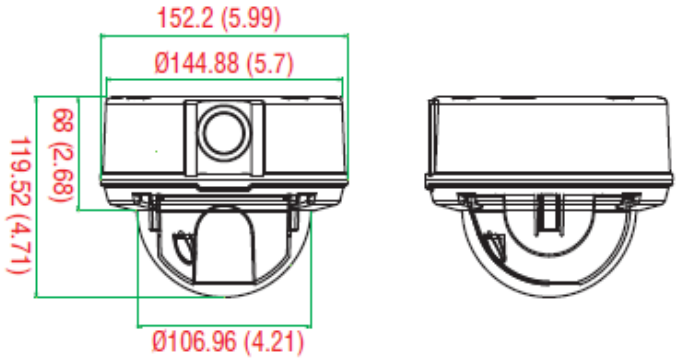


NOTE After accessing the VPort 26's web-based manager, administrators should access **System Configuration → System → Account** to set up the administrator's password and enable the authentication function. The administrator account name is admin.
An authentication window will pop up requesting the account name and password each time the VPort 26 is accessed.

VPort 26 Dimension



Top View



Side View

(Unit=mm)

Wiring Requirements

ATTENTION

Be sure to disconnect the power cord before installing and/or wiring your Moxa VPort 26.
Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.
If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

You should also pay attention to the following:

- Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross make sure the wires are perpendicular at the intersection point.
  NOTE: Do not run signal or communications wiring and power wiring in the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
- You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- Keep input wiring and output wiring separate.
- It is strongly advised that you label wiring to all devices in the system when necessary.

3

Accessing the VPort 26's Web-based Manager

This chapter includes information about how to access the VPort 26 IP camera for the first time.

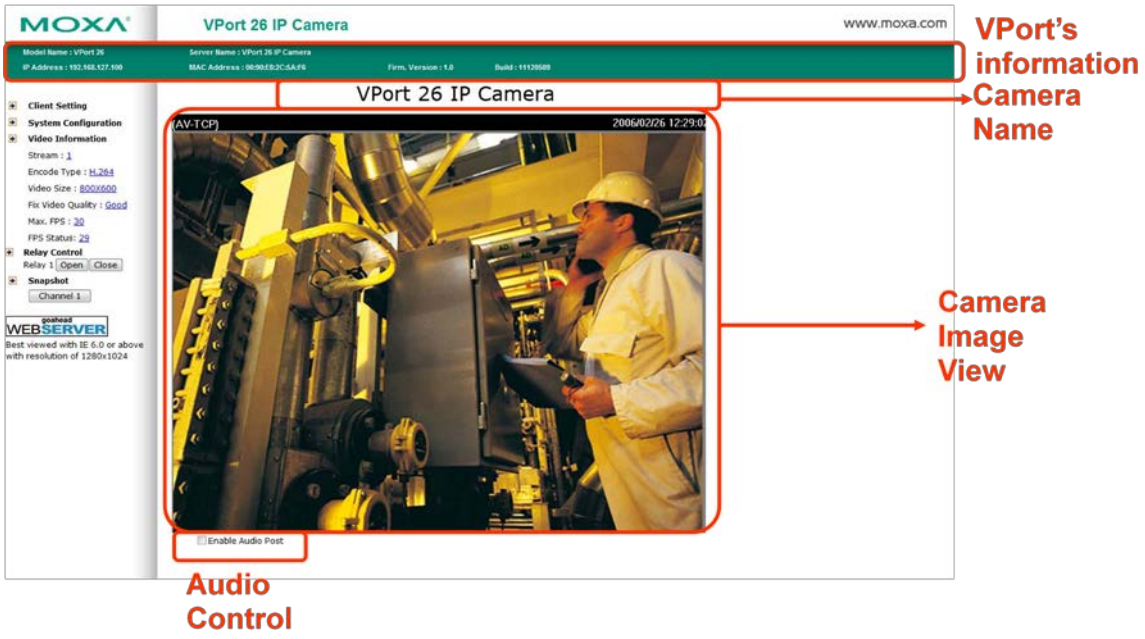
The following topics are covered in this chapter:

- **Functions Featured on the VPort's Web Homepage**
  - VPort's Information
  - IP Camera Name
  - Camera Image View
  - Audio Control
  - Client Settings
  - System Configuration
  - Video Information
  - Relay Control
  - Snapshot

Functions Featured on the VPort's Web Homepage

The homepage of the VPort's web console shows information specific to that VPort, the camera image, and configurations for the client and server.

NOTE The VPort's web homepage is best viewed in 1280 x 1024 screen resolution. This is because the camera image can be viewed at a resolution up to Full D1 (NTSC: 720 x 480; 720 x 576). We strongly recommend using IE 6.0 (Microsoft Internet Explorer) or above to avoid incompatibility with the ActiveX Plug-in.



VPort's Information

This section shows the VPort's model name, server name, IP address, MAC address and firmware version.

IP Camera Name

A server name can be assigned to each server. Administrators can change the name in **System Configuration / System / General**. The maximum length of the sever name is 40 bytes.

Camera Image View

The assigned image description and system date/time will be displayed in the caption above the image window. You may disable the caption or change the location of the image information in **System Configuration / Video / Image Setting**. Note that if the VPort's motion detection function is active, some windows in the video picture might be framed in red.

Audio Control

The VPort 26 provides both audio input and audio output for voice over IP communication. Client users can directly enable and disable the audio input (a microphone, for example) by checking the box of **Enable Audio Post** on the VPort's web homepage. You may also use the Client Setting to disable the audio transmission.

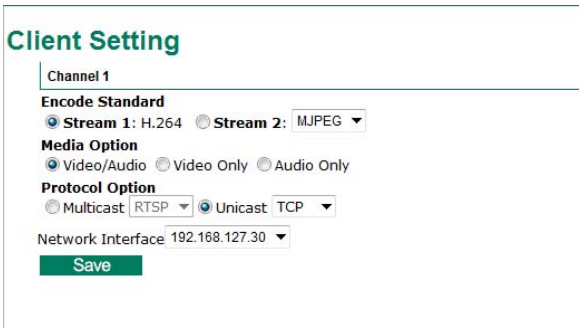
Client Settings

Users can configure the following functions in **Client Settings**.

1. **Encode standard:** Shows the encoding algorithm currently being used. VPort 26 features built-in 2 encode engine to generate a maximum of three simultaneous video streams. Each client can select the H.264 video streams from Stream 1, or the MJPEG/ H,264 video stream from Stream 2. To configure these video streams, please go to:
   System Configuration / Video / Video Performance.
2. **Protocol Options:** Choose one of four protocols to optimize your usage—Multicast (RTSP or Push) or Unicast (UDP, TCP, HTTP).
   - **Multicast** protocol can be used to send a single video stream to multiple clients. In this case, a lot of bandwidth can be saved since only one video stream is transmitted over the network. However, the network gateway (e.g., a switch) must support the multicast protocol (e.g., IGMP snooping). Otherwise, the multicast video transmission will not be successful.
     - **RTSP:** Enable the multicast video stream to be sent in RTSP control, which means the multicast video stream will be sent only it receives the client's request.
     - **Push:** Enable the multicast video stream to be sent in Push control, which means that after this setting is selected the multicast video stream will be sent continuously even without any client request.
   - Unicast protocol is used to send a single video stream to one client.
     - **UDP** can be used to produce audio and video streams that are more real-time. However, some packets may be lost due to network burst traffic, and images may become blurred.
     - **TCP** can be used to prevent packet loss, which results in a more accurate video display. The downside of using TCP is that the real-time delay is worse than with UDP protocol.
     - **HTTP** can be used to prevent being blocked by a router's firewall. The downside of using HTTP is that the real-time delay is worse than with UDP protocol.
   - **Network Interface** designates the connection interface for multicast video streams selection. The box lists the current NIC interfaces. Select which NIC interface will receive multicast streams.

Once the IP camera is connected successfully, Protocol Options will indicate the selected protocol. The selected protocol will be stored on the user's PC, and will be used for the next connection.

NOTE For multicast video stream settings, please refer to **System Configuration → Network → Multicast**.



System Configuration

A button or text link on the left side of the system configuration window only appears on the administrator's main page. For detailed system configuration instructions, refer to Chapter 4, **System Configuration**.

Video Information

Users can easily monitor the current video performance by looking at the **Video Information** shown on the left side of the homepage. The following properties are shown: Stream, Video Size, Video Quality (Fixed bit rate or Fixed video quality), Max. FPS (frames per second), and (current) FPS Status. Users can select the target camera image to view each camera's video performance.

Relay Control

The VPort 461 has 2 relay outputs for external devices, such as alarms. Administrators and permitted users can click on **Open** to short the Common and Normal Open digital output pins, or click on **Close** to short the Common and Normal Close digital output pins.

Snapshot

Users can take snapshot images for storing, printing, or editing by clicking the **Channel 1** button. Save the image by rick-clicking and selecting **Save**.

4

System Configuration

After installing the hardware, the next step is to configure the VPort 26's settings. Users can configure by web console.

The following topics are covered in this chapter:

- **System Configuration by Web Console**
  - System
  - Network
  - DynaStream™
  - Video
  - Audio
  - Alarm

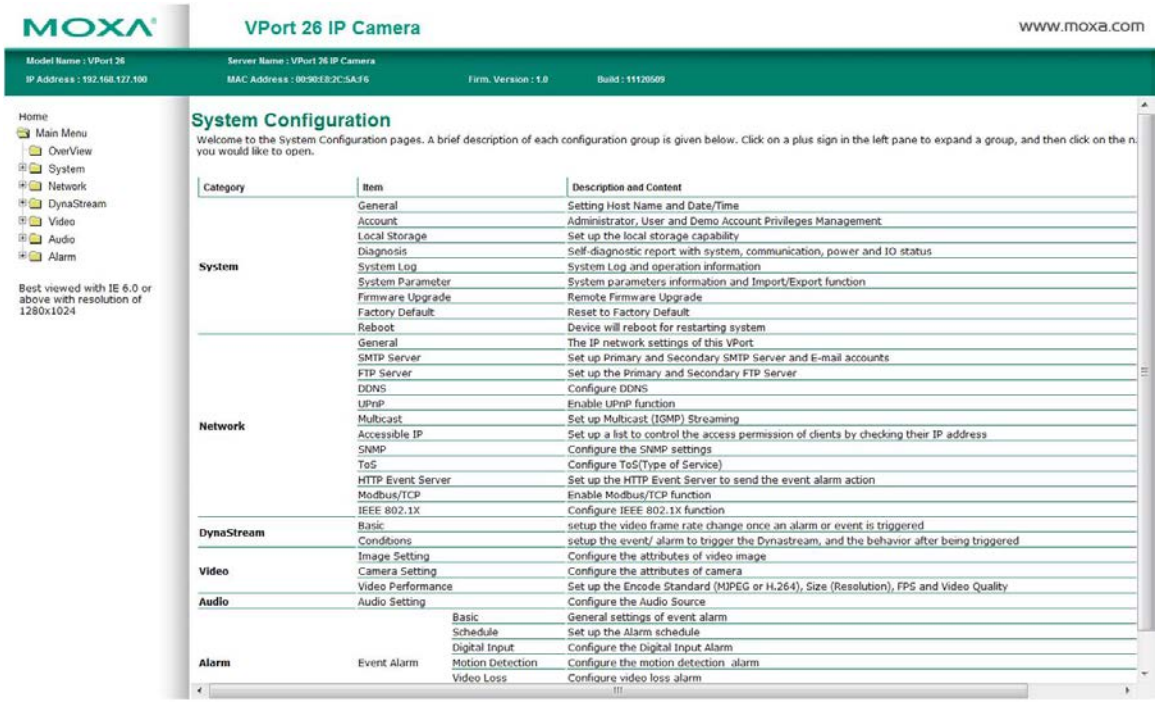
System Configuration by Web Console

System configuration can be done remotely with Internet Explorer. To access the server, type the system configuration URL, **http://<IP address of Video Server>/overview.asp**, to open the configuration main page.

There are six configuration categories: **System, Network, DynaStream, Video, Audio**, and **Alarm**. A description of each configuration item is shown in the table below:

Category	Item		Description and Contents
System	General		Set Host Name and Date/Time
	Accounts		Administrator, User, and Demo Account Privileges Management
	Local Storage		Configure the local storage settings
	Diagnosis		Self-diagnostic report with system, communication, power, and LED status
	System Log		System Log and operation information
	System Parameter		System parameter information and Import/Export functions
	Firmware Upgrade		Remote Firmware Upgrade
	Factory Default		Reset to Factory Default
	Reboot		Device will reboot for restarting system
Network	General		The IP network settings of this VPort
	SMTP Server		Set up Primary and Secondary SMTP Server and e-mail accounts
	FTP Server		Set up the Primary and Secondary FTP Server
	DDNS		Configure Dynamic DNS service
	UPnP		Enable UPnP function
	Multicast Setting		Set up Multicast (IGMP) Streaming
	Accessible IP		Set up a list to control the access permission of clients by IP address
	SNMP		Configure the SNMP settings
	ToS		Configure ToS (Type of Service)
	HTTP Event Server		Set up the HTTP Event Server to send the event alarm action
	Modbus/ TCP		Enable Modbus/TCP function
	IEEE 802.1X		Configure IEEE 802.1X function
DynaStream	Basic		setup the video frame rate change once an alarm or event is triggered
	Conditions		setup the event/ alarm to trigger the Dynastream, and the behavior after being triggered
Video	Image Setting		Configure the attributes of the video image
	Camera Setting		Configure the attributes of camera
	Video Performance		Set up the Encode Standard (MJPEG or MPEG4), Size (Resolution), FPS and Video Quality
Audio	Audio Setting		Configure the Audio Source
Alarm	Event Alarm	Basic	General event alarm settings
		Schedule	Set up the Alarm schedule
		Digital input	Configure the Digital Input Alarm
		Motion Detection	Configure the motion detection alarm
		Video Loss	Configure the video loss alarm
		CGI Event	Set up the CGI event alarm
		Sequential Snapshot	Set up the operation of Sequential Snapshot

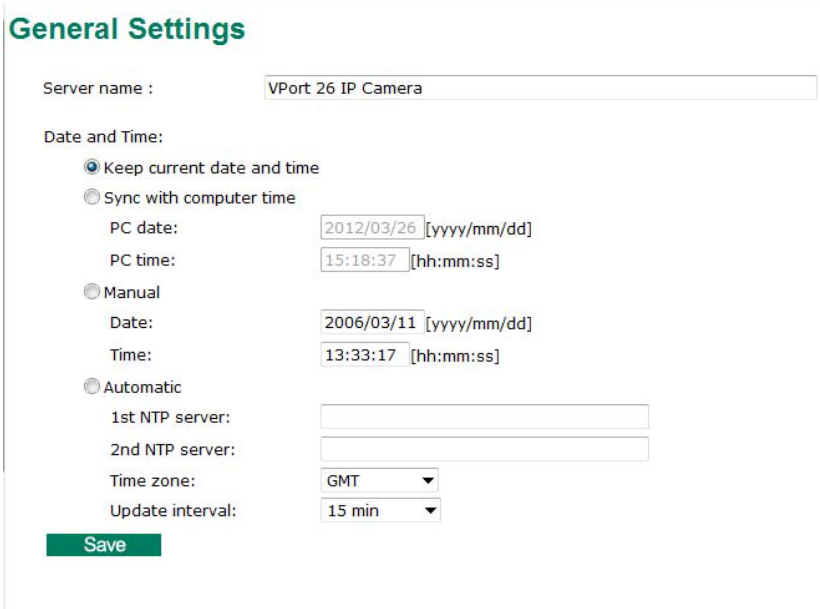
This table can also be found on the **System Configuration → Overview webpage**.



System

General Settings

On the **General Settings** page, administrators can set up the video **Server name** and the **Date and Time**, which is displayed in the image's caption.



Server name

Setting	Description	Default
Max. 40 characters	Use a different server name for each server to help identify the different servers. The name appears on the web homepage.	VPort 26 IP camera

Date and Time

Setting	Description	Default
Keep current date and time	Use the current date and time as the VPort's time setting.	Keep current date and time
Sync with computer time	Synchronize VPort's data and time setting with the local computer time.	
Manual	Manually change VPort's date and time setting.	
Automatic	Use the NTP server for changing VPort's date and time setting in a given period.	

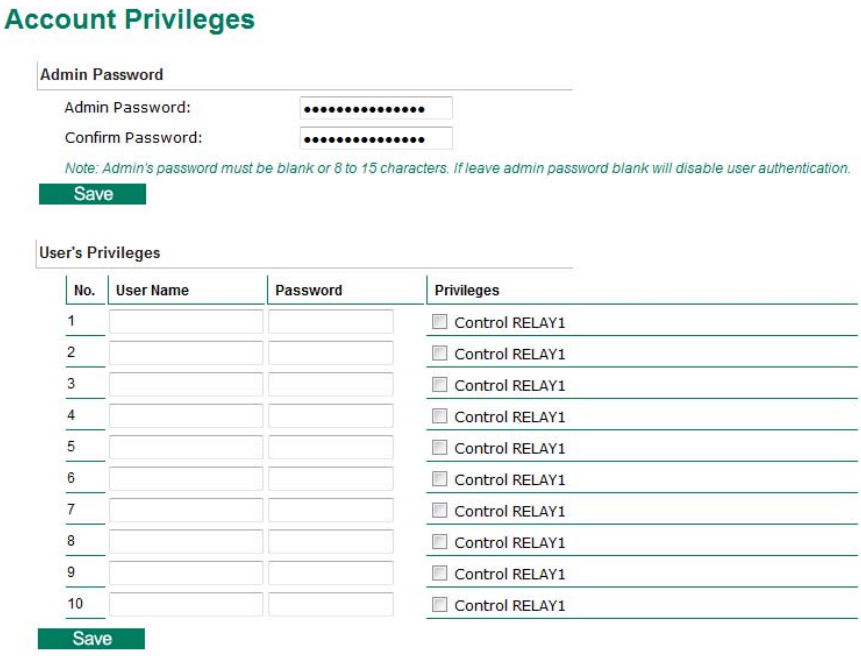
NOTE Select the **Automatic** option to force the VPort to synchronize automatically with timeservers over the Internet. However, synchronization may fail if the assigned **NTP server** cannot be reached, or the VPort is connected to a local network. Leaving the **NTP server** blank will force the VPort to connect to default timeservers. Enter either the Domain name or IP address format of the timeserver if the DNS server is available.

2 NTP servers may be set as backups, and update intervals can be configured from a minimum of 15 minutes to a maximum of one month.

Don't forget to set the **time zone** in local settings. Refer to Appendix G for your region's time zone.

Account Privileges

Different account privileges are available for different purposes.



Admin password

Setting	Description	Default
Admin Password (8 to 15 characters)	The administrator can type the new password in this box.	Default admin password is "admin"
Confirm Password (8 to 15 characters)	If a new password is typed in the **Admin Password** box, you will need to retype the password in the **Confirm Password** box before updating the new password.	

NOTE The default account name for administrator is **admin**; the administrator account name cannot be changed.

User's Privileges

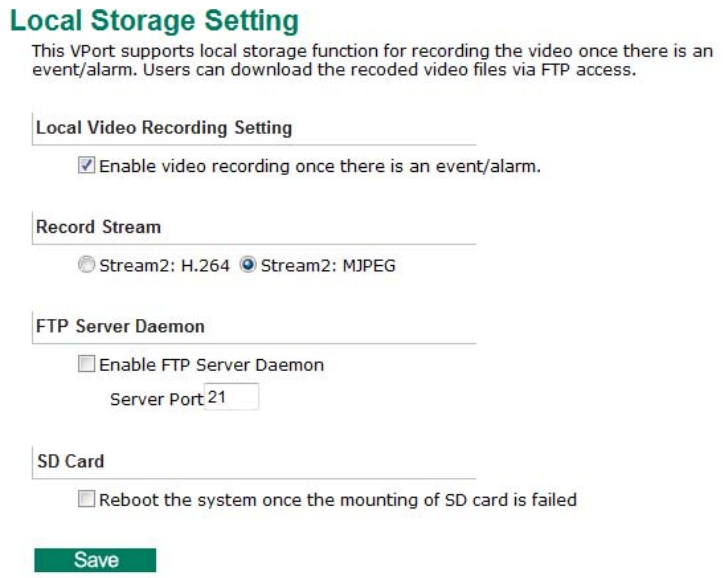
VPort products provide 10 user accounts for accessing the VPort.

Setting	Description	Default
User Name	Type a specific user name for user authentication.	None
Password	Type a specific password for user authentication.	
Privilege	Check the function boxes to assign privileges for users in Control Relay1	

NOTE The FPS of the video stream will be reduced as more and more users access the same VPort. Currently, the VPort 26 is only allowed to send 10 unicast video streams. Therefore, limit the number of users simultaneously accessing a VPort 26 to prevent performance problems.

Local Storage

The VPort 26 supports an SD card slot (SDHC interface) for recording video when preconfigured events (alarms) occur. Administrators can download these recorded videos via FTP, or remove the SD card and directly copy the files via a card reader.



Local Video Recording Setting

Setting	Description	Default
Enable video recording once there is an event/alarm	Enable the video recording action once there is an event/alarm	Enable

Recording Stream

Setting	Description	Default
Stream 2: H.264 or Stream 2: MJPEG	Select the H.264 or MJPEG of stream 2 for video recording	Stream 2: MJPEG

FTP Daemon

Setting	Description	Default
Enable FTP daemon	Enable the FTP service for downloading the recorded video files by the administrator	Enable
Server Port	The FTP server port number	21

SD card

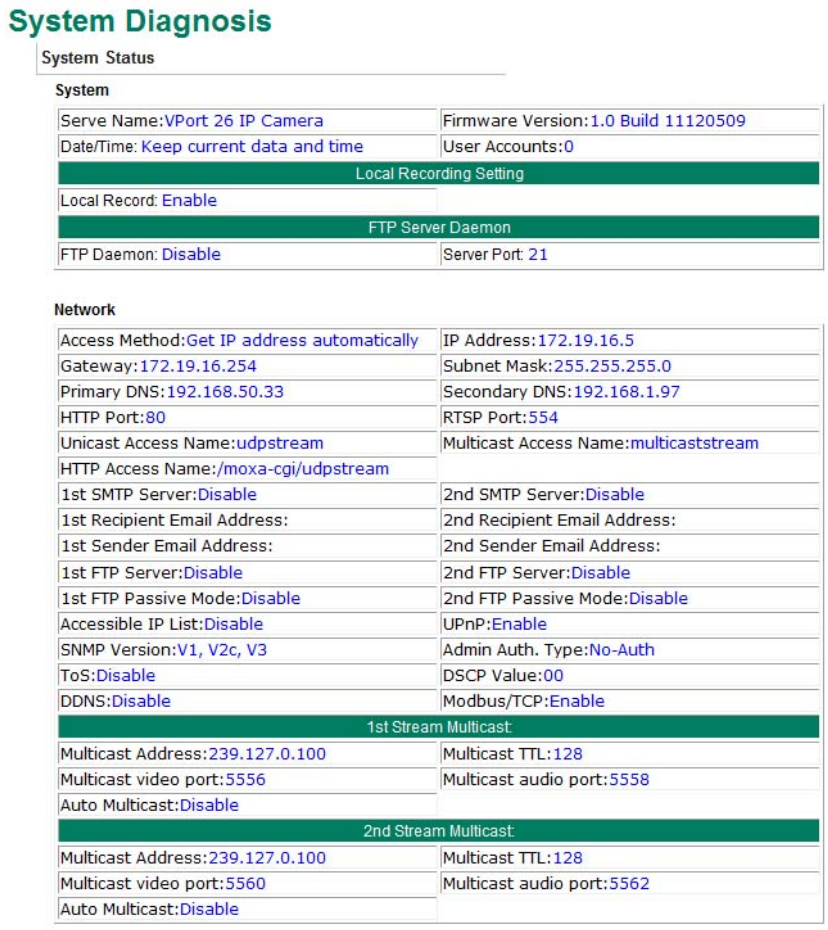
Setting	Description	Default
Reboot the system when the SD card fails to mount	This function can reboot the system when the SD card mount fails to re-detect the SD mount.	Enable

NOTE The recorded videos will be stored in the "/VPortfolder" folder. Each recorded file is 10 seconds of video. These are AVI files for playback in a popular media player.

NOTE Due to file system limitations, the maximum number of files is 16584. When the number of files in the SD card is up to 16584, or the free space is under 100MB, the system will start to delete the oldest files.

System Diagnosis

VPort products have a self-diagnosis function to let the administrator get a quick view of the system and connection status. Administrators can save this diagnosis information in a file (diagnosis.log) by clicking the **Export to a File** button, or send the file via email by clicking the **Send a Report via Email** button.



System Diagnosis

System Status

System

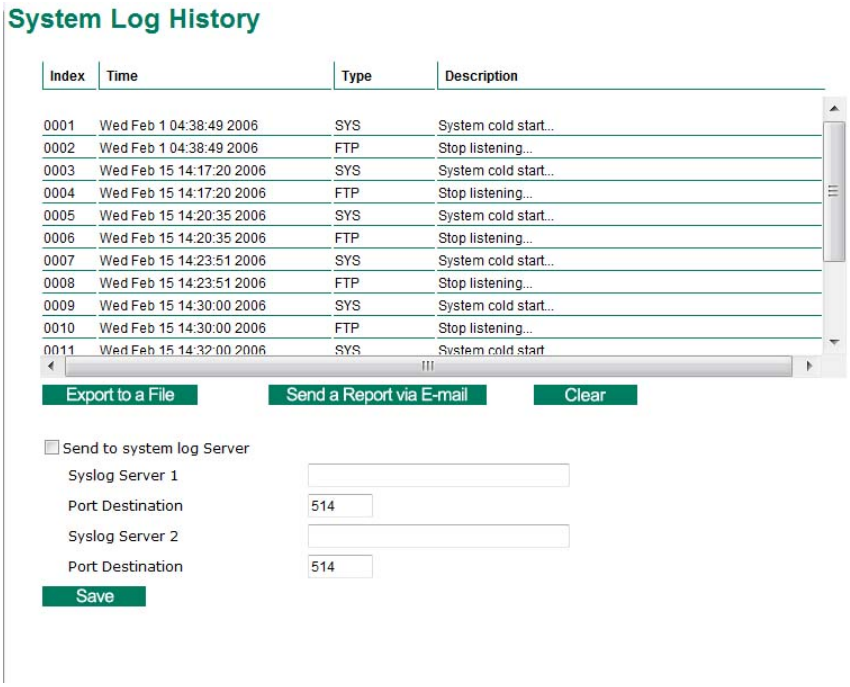
Serve Name:VPort 26 IP Camera	Firmware Version:1.0 Build 11120509
Date/Time: Keep current data and time	User Accounts:0
Local Recording Setting	
Local Record: Enable	
FTP Server Daemon	
FTP Daemon: Disable	Server Port: 21

Network

Access Method:Get IP address automatically	IP Address:172.19.16.5
Gateway:172.19.16.254	Subnet Mask:255.255.255.0
Primary DNS:192.168.50.33	Secondary DNS:192.168.1.97
HTTP Port:80	RTSP Port:554
Unicast Access Name:udpstream	Multicast Access Name:multicaststream
HTTP Access Name:/moxa-cgi/udpstream	
1st SMTP Server:Disable	2nd SMTP Server:Disable
1st Recipient Email Address:	2nd Recipient Email Address:
1st Sender Email Address:	2nd Sender Email Address:
1st FTP Server:Disable	2nd FTP Server:Disable
1st FTP Passive Mode:Disable	2nd FTP Passive Mode:Disable
Accessible IP List:Disable	UPnP:Enable
SNMP Version:V1, V2c, V3	Admin Auth. Type:No-Auth
ToS:Disable	DSCP Value:00
DDNS:Disable	Modbus/TCP:Enable
1st Stream Multicast:	
Multicast Address:239.127.0.100	Multicast TTL:128
Multicast video port:5556	Multicast audio port:5558
Auto Multicast:Disable	
2nd Stream Multicast:	
Multicast Address:239.127.0.100	Multicast TTL:128
Multicast video port:5560	Multicast audio port:5562
Auto Multicast:Disable	

System Log History

The system log contains useful information, including current system configuration and activity history with timestamps for tracking. Administrators can save this information in a file (system.log) by clicking the **Export to a File** button, or send the file by email by clicking the **Send a Report via Email** button. In addition, the log can also be sent to a **Log Server** for backup. The administrator can set up the Syslog Server 1 and Syslog server 2 below the system log list.



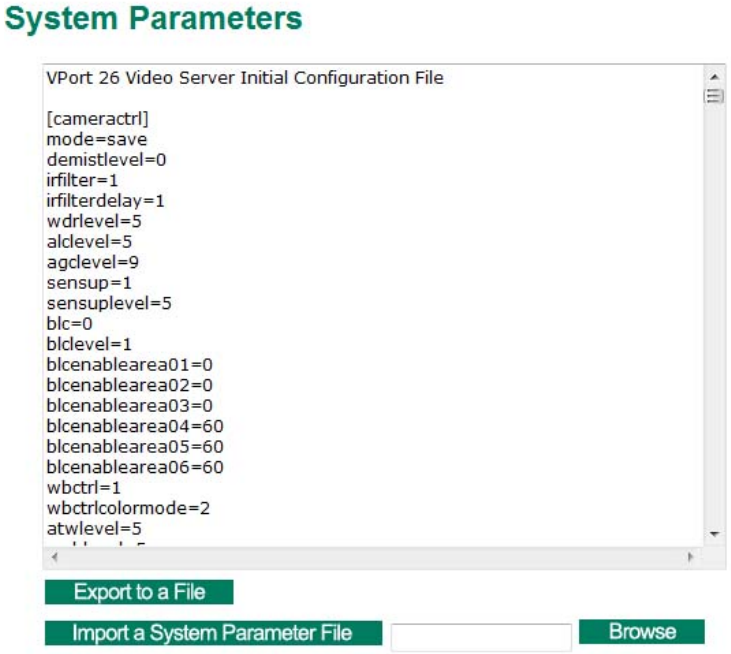
Send to system log server

Setting	Description	Default
Send to system log server	Enables sending the system log to the log sever.	Disable
Syslog Sever 1	The address of the first system log server.	Blank
Port Destination	The port number of first system log server.	514
Syslog Sever 2	The address of the second system log server.	Blank
Port Destination	The port number of second system log server.	514

NOTE A maximum of 500 lines is displayed in the log. Earlier data beyond the first 500 entries are still in the VPort's database; the administrator can export them at any time.

System Parameters

The **System Parameters** page allows you to view all system parameters, which are listed by category. The content is the same as the VPort's sys_config.ini file. Administrators can also save this information in a file (sys_config.ini) by clicking the **Export to a File** button, or import a file by clicking the **Browse** button to search for a sys_config.ini file and then clicking the **Import a System Parameter File** button to update the system configuration quickly.



NOTE The system parameter import/export functions allow the administrator to backup and restore system configurations. The Administrator can export this sys_config.ini file (in a special binary format) for backup, and import the sys_config.ini file to restore the system configurations of VPort IP cameras. System configuration changes will take effect after the VPort is rebooted.

Firmware Upgrade

Take the following steps to upgrade the firmware:

Step 1: Press the **Browse** button to select the firmware file.

NOTE For the VPort 26, the firmware file extension should be **.rom**.

Step 2: Click on the **Upgrade** button to upload the firmware to the VPort.

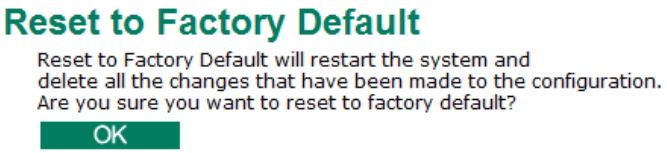
Step 3: The system will start to run the firmware upgrade process.

Step 4: Once **Firmware Update Success.....Reboot....** is displayed, please wait for few seconds for the VPort to reboot. The reboot process is finished once the **STAT** LED is lit continuously in green.

NOTE Upgrading the firmware will not change the original settings.

Reset to Factory Default

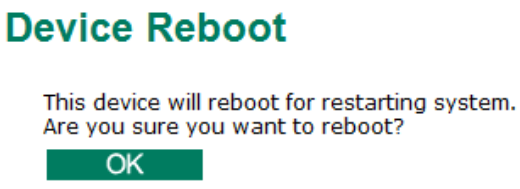
From the "Reset to Factory Default" page, click on **OK** (as shown in the following figure) to reset the VPort to its factory default settings.



NOTE All parameters will be reset to factory defaults when you use the Factory Default function. For this reason, if you want to keep a digital copy of the current configuration, remember to export the sys_config.ini file before using the Factory Default function.

Reboot

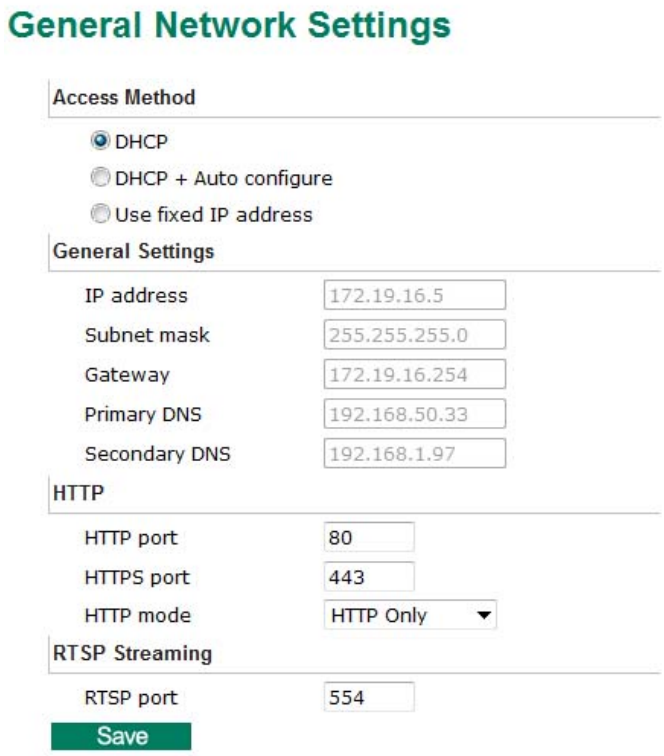
From the "Device Reboot" page, click **OK** (as shown in the following figure) to restart the VPort's system.



Network

General Network Settings

The **General Network Settings** page includes some basic but important network configurations that enable the VPort to be connected to a TCP/IP network.



Access Method

VPort products support the DHCP protocol, which means that the VPort can get its IP address from a DHCP server automatically when it is connected to a TCP/IP network. The Administrator should determine if it is more appropriate to use DHCP, or assign a fixed IP.

Setting	Description	Default
DHCP	Get the IP address automatically from the DHCP server.	DHCP
DHCP + Auto configure	Get the IP address automatically from the DHCP server, and download the configurations from the TFTP server with Opt 66/67 mechanism.	
Use fixed IP address	Use the IP address assigned by the administrator.	

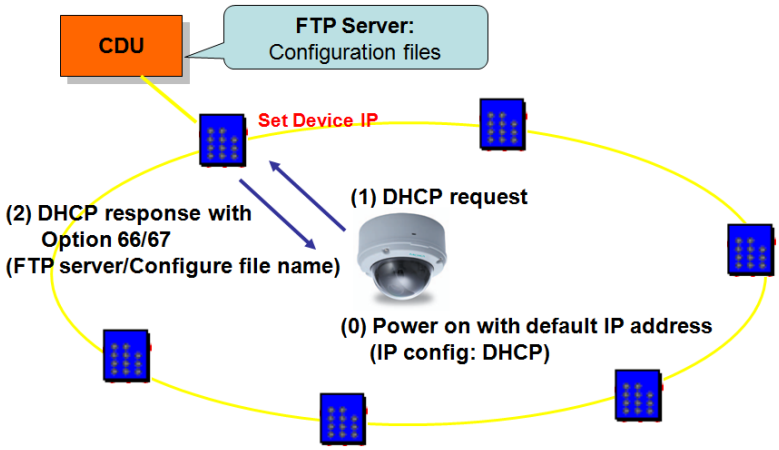
NOTE We strongly recommend that the administrator assign a fixed IP address to the VPort, since all of the functions and applications provided by the VPort are active when the VPort is connected to the network. Use DHCP to determine if the VPort's IP address may change when then network environment changes, or the IP address is occupied by other clients.

Auto Configuration

In a mass installation, it is time consuming to configure each of the many devices one by one. Therefore, DHCP Opt 66/67 provides a mechanism whereby configurations can be saved on a TFTP server. Once a new device is installed, the configurations can be downloaded to this new device automatically. By doing this, the installer can save a lot of time and efforts in mass device installation. Follow the steps below to use the auto-configuration function via Opt 66/67.

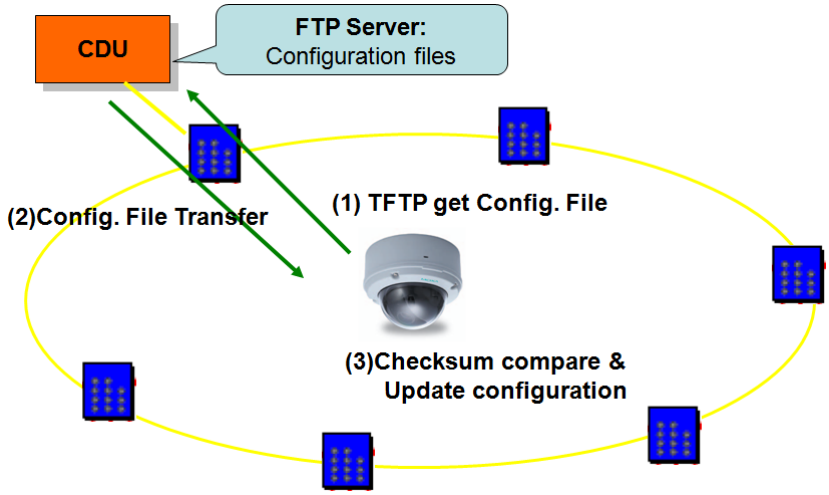
Step 1:

When VPort 26 enables the auto-configuration function, it will ask for the IP address from DHCP server, and the path of the TFTP server and configuration file.



Step 2:

Once VPort 26 completes the IP settings, it will acquire the configuration file from the TFTP server, and check if this configuration file is right or not.



NOTE For auto-configuration to work properly, the system should:

1. Have a DHCP Server that supports DHCP Opt 66/67 in the network switches and routers.
2. Have a TFTP server that supports the TFTP protocol

General Settings

Setting	Description	Default
IP address	Variable IP assigned automatically by the DHCP server, or fixed IP assigned by the Administrator.	192.168.127.100
Subnet mask	Variable subnet mask assigned automatically by the DHCP server, or a fixed subnet mask assigned by the Administrator.	255.255.255.0
Gateway	Assigned automatically by the DHCP server, or assigned by the Administrator.	Blank
Primary DNS	Enter the IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input the VPort's url (e.g., www.VPort.company.com) in your browser's address field, instead of entering the IP address.	Obtained automatically from the DHCP server, or left blank in non-DHCP environments.
Secondary DNS	Enter the IP address of the DNS Server used by your network. The VPort will try to locate the secondary DNS Server if the primary DNS Server fails to connect.	Obtained automatically from the DHCP server, or left blank in non-DHCP environments.

HTTP

Setting	Description	Default
HTTP Port (80, or 1024 to 65535)	HTTP port enables connecting the VPort to the web.	80
HTTPS port (80, or 1024 to 65535)	HTTPS port number for communication encryption (do not set the same port number as the HTTP port)	443
HTTP mode	Select the HTTP transmission mode: HTTP Only or HTTP + HTTPS	HTTP Only

RTSP Streaming

The VPort 26 supports standard RTSP (Real Time Streaming Protocol) streaming, which means that all devices and software that support RTSP can directly acquire and view the video images sent from the VPort 26 without any proprietary codec or SDK installations. This makes network system integration much more convenient. For different connection types, the **access name** is different. For UDP and TCP streams, the access name is **udpStream**. For HTTP streams, the access name is **moxa-cgi/udpstream_ch<channel number>**. For multicast streams, the access name is **multicastStream_ch<channel number>**. You can access the media through the following **URL: rtsp://<IP address>:<RTSP port>/<Access name> for software that supports RTSP**.

Setting	Description	Default
RTSP Port	An RTSP port is similar to an HTTP port, which can enable the connection of video/audio streams by RTSP.	554

The Apple QuickTime media player is used here as an example of a RTSP streaming application:

Step 1: Open Apple QuickTime Player and select **File - Open URL in New Player**.

Step 2: When the following pop-up window appears, type the URL in the input box. E.g., type **rtsp://<VPort 26's IP address>[:<RTSP Port]/udpstream_ch1_stream< 1 or 2>**
rtsp://<VPort 26's IP address>[:<RTSP Port]/multicaststream_ ch1_stream<1 or 2>
RTSP Port: 554 is default, and then click on **OK** to connect to the VPort 26.

Step 3: Wait a few seconds for QuickTime Player to establish the connection.

Step 4: After the connection has been established, the VPort 26's video will appear in the QuickTime Player display window.

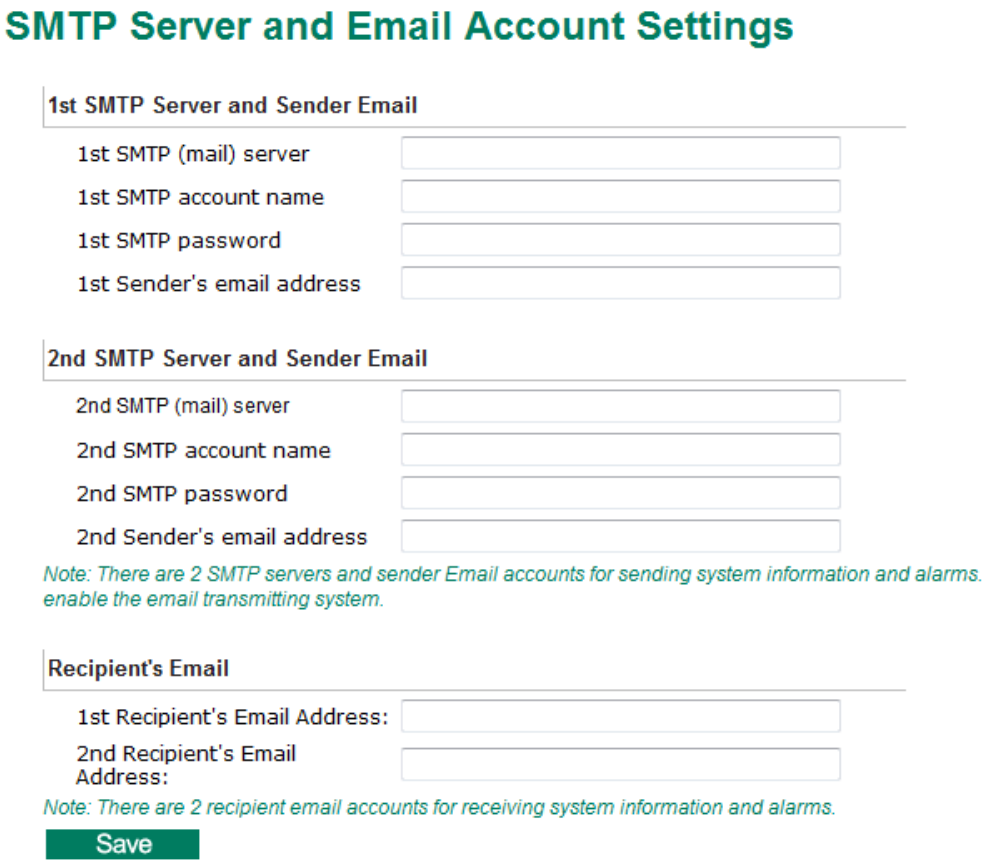
NOTE The video performance of the VPort 26 may vary when using other media players. For example, you will notice a greater delay when viewing the VPort 26's video from the QuickTime player compared to viewing it directly from the VPort 26's built-in web server. In addition, viewing the VPort 26's video from the Quicktime player through a router or Internet gateway could result in a broken connection.

NOTE For the time being, the VPort 26's RTSP video/audio stream can be identified and viewed by Apple QuickTime Ver. 6.5 and above, and the VLC media player. System integrators can use these 2 media players to view the VPort 26's video directly, without needing to use the VPort's SDK to create customized software.

NOTE When using RTSP, the video stream format should be H.264 or MPEG4. MJPEG does not support RTSP.

SMTP Server and Email Account Settings

The VPort not only plays the role of a server, but can also connect to outside servers to send alarm messages and snapshots. If the administrator has set up some applications in either system information or alarm, the VPort will send out messages or snapshots once these conditions occur.



1st SMTP Server and Sender Email

Setting	Description	Default
1st SMTP (mail) server	SMTP Server's IP address or URL address.	None
1st SMTP account name	For security reasons, most SMTP servers require the account name and password to be authenticated.	None
1st SMTP password		None
1st Sender's email address	For security reasons, SMTP servers must see the exact sender email address.	None

NOTE Note that if the **Sender's email address** is not set, a warning message will pop up and the e-mail system will not be allowed to operate.

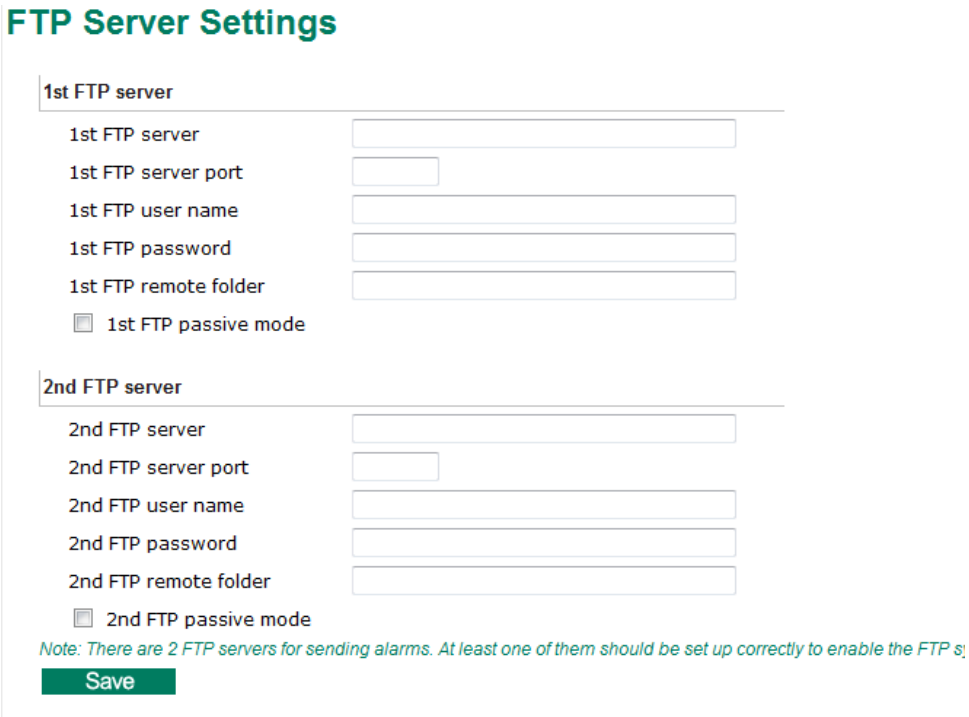
NOTE The **2nd SMTP Server** and Sender Email are backups that are used if the 1st SMTP Server and Sender Email fail when connecting or sending email.

Two recipient email accounts are available for receiving emails sent by the VPort. For redundancy, both addresses receive the sent messages and alarm snapshots simultaneously.

Setting	Description	Default
1st Recipient's Email Address	Email address of the 1st recipient.	None
2nd Recipient's Email Address	Email address of the 2nd recipient.	None

FTP Server Settings

FTP is the other method available for the VPort to send alarm messages and snapshots.



1st FTP Server

Setting	Description	Default
1st FTP server	FTP server's IP address or URL address.	None
1st FTP server port	FTP server's authentication.	None
1st FTP user name		None
1st FTP remote folder	FTP file storage folder on the remote FTP server.	None
1st FTP passive mode	Passive transfer solution for FTP transmission through a firewall.	Disabled

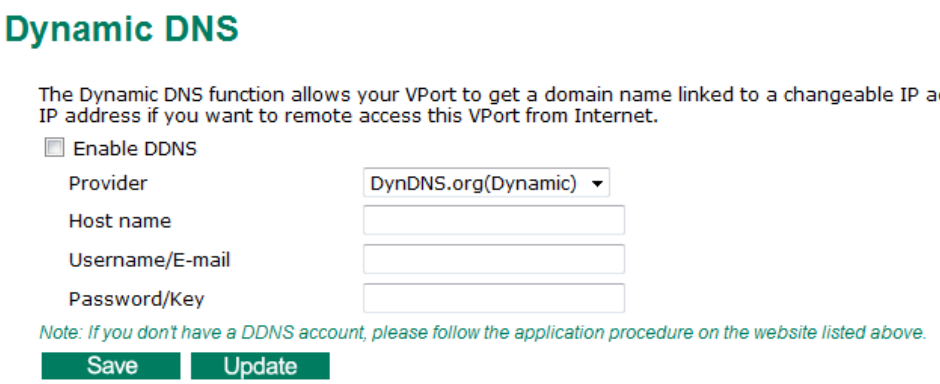
NOTE The **2nd FTP Server** is a backup in case the 1st FTP Server fails to connect or has trouble sending files.

NOTE Whenever the system reboots, a system log will be sent by email or FTP to show the login status of the VPort. The system log will be sent to the Sender email address if the SMTP server settings are correct. To send the system log via FTP, the SMTP server should be erased since the E-mail system is used by default to transmit the system log.

NOTE For either e-mail or FTP, the information of the 1st server should be entered first. If the 1st server is not set, the related FTP or email will be cancelled. Note that it may take time to connect to the 2nd server after the first server fails, and this may affect some applications when adverse conditions occur too often.

Dynamic DNS

DDNS (Dynamic Domain Name System) is a combination of DHCP, DNS, and client registration. DDNS allows administrators to alias the VPort's dynamic IP address to a static hostname in any of the domains provided by the DDNS service providers listed on the VPort's Network/DDNS configuration page. DDNS makes it easier to access the VPort from various locations on the Internet.



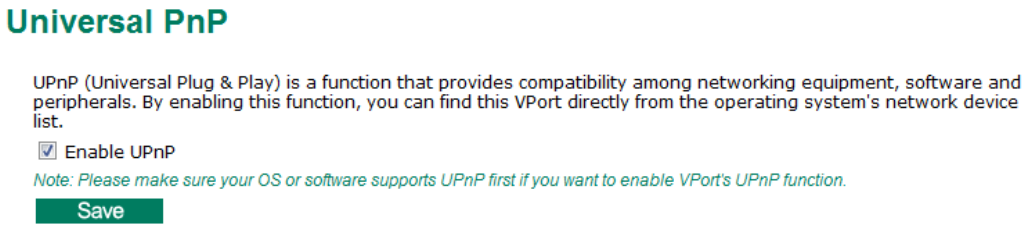
Setting	Description	Default
Enable DDNS	Enable or disable DDNS function	Disable
Provider	Select the DDNS service providers, including DynDNS.org (Dynamic), DynDNS.org (Custom), TZO.com, and dhs.org.	None
Host Name	The Host Name you use to link to the VPort.	None
Username/ E-mail	The Username/E-mail and Password/Key are used to enable the service from the DDNS service provider (based on the rules of DDNS websites).	None
Password/ Key		None

NOTE Dynamic DNS is a very useful tool for accessing a VPort over the Internet, especially for xDSL connections with a non-fixed IP address (DHCP). The administrator and users can simplify connecting to a VPort with a non-fixed IP address, by using the unique host name in the URL to establish a connection with the VPort.

NOTE Different DDNS service providers have different application rules. Some applications are free of charge, but most require an application fee.

Universal PnP

UPnP (Universal Plug & Play) is a networking architecture that provides compatibility among the networking equipment, software, and peripherals of the 400+ vendors that are part of the Universal Plug and Play Forum. This means that they are listed in the network devices table for the operating system (such as Windows XP) supported by this function. Users can link to the VPort directly by clicking on the VPort listed in the network devices table.



Setting	Description	Default
Enable UPnP	Enable or disable the UPnP function.	Enable

Multicast

The VPort 26 supports the advanced Multicast network protocol IGMP, which can greatly improve the efficiency of network traffic. In this section, we explain multicasts, multicast filtering, and how multicast can be implemented on your VPort.

What is Multicast?

A multicast is a packet that is intended for “one-to-many” and “many-to-many” communication. Users explicitly request to participate in the communication by joining an end-station to a specific multicast group. If the network is set up correctly, a multicast can only be sent to an end-station or a subset of end-stations on a LAN or VLAN that belongs to the relevant multicast group. Multicast group members can be distributed across multiple subnetworks. Therefore, multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only one copy of the desired information across the network. The packets are only replicated if they reach a network node that links to two or more members of the multicast network. Transmitting packets in this way makes more efficient use of network bandwidth. A multicast packet is identified by the presence of a multicast group address in the destination address field of the packet’s IP header.

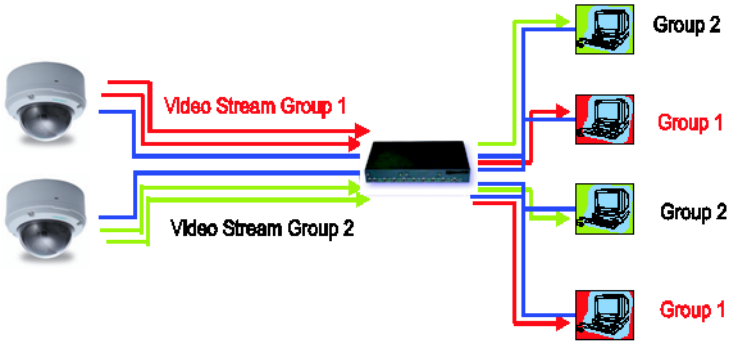
Benefits of Multicast

The benefits of using IP multicast are that it:

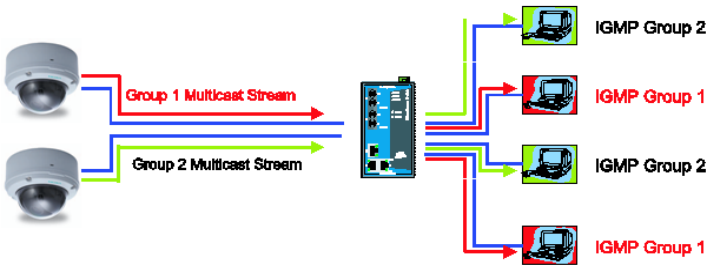
- Enables the simultaneous delivery of information to many receivers in the most efficient, logical way.
- Reduces the load on the source (for example, a server) because it does not need to produce multiple copies of the same data.
- Makes efficient use of network bandwidth and scales well as the number of participants or collaborators expands.
- Works with other IP protocols and services, such as Quality of Service (QoS).

There are situations where a multicast approach is more logical and efficient than a unicast approach. A typical use of multicasts is in video-conferencing, in which high volumes of traffic need to be sent to several end-stations simultaneously, but for which broadcasting that traffic to all end-stations would seriously reduce network performance. Several industrial automation protocols, such as Allen-Bradley, EtherNet/IP, Siemens Profibus, and Foundation Fieldbus HSE (High Speed Ethernet), use the multicast approach. These industrial Ethernet protocols use publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic. IGMP provides the ability to prune multicast traffic so that it travels only to those end destinations that require the traffic, thus reducing the amount of traffic on the Ethernet LAN.

The network WITHOUT Multicast

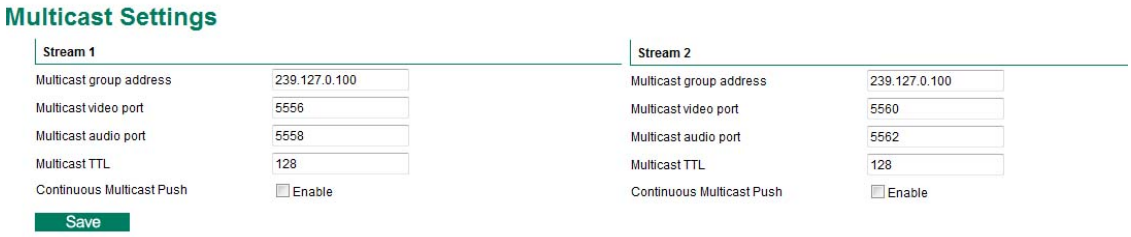


The network WITH Multicast



NOTE The VPort 26 is the source that delivers the multicast video stream. To benefit from the Multicast protocol, the gateway or network switch should support the multicast filtering function (such as IGMP Snooping) so that the multicast stream is delivered correctly and precisely. To learn more about IGMP Snooping, refer to the Moxa EtherDeviceTM series Industrial Ethernet Switch user's manual.

Configuring Multicast Settings



Setting	Description	Default
Multicast group address	Multicast Group address for sending video stream.	239.127.0.100
Multicast video port	Video port number.	Stream 1: 5556 Stream 2: 5560
Multicast audio port	Audio port number.	Stream 1: 5558 Stream 2: 5562
Multicast TTL	Multicast-TTL (Time-to-live) threshold. There is a certain TTL threshold defined for each network interface or tunnel. A multicast packet's TTL must be larger than the defined TTL for that packet to be forwarded across that link.	128
Continuous Multicast Push	Enable PUSH control of the multicast video stream	Disable

Accessible IP List

The VPort uses an IP address-based filtering method to control access to the VPort.

Accessible IP Settings allow you to add or remove "Legal" remote host IP addresses to prevent unauthorized access. Access to the VPort is controlled by IP address. That is, if a host's IP address is in the accessible IP table, then the host will be allowed access to the VPort. Administrators can allow one of the following cases by setting this parameter:

- Only one host with a specific IP address can access the VPort. Enter "IP address/255.255.255.255" (e.g., 192.168.1.1/255.255.255.255)
- Hosts on a specific subnet can access the VPort. Enter "IP address/255.255.255.0" (e.g., "192.168.1.0/255.255.255.0")
- Any host can access the VPort. Disable this function.

Refer to the following table for more configuration examples.

Allowable Hosts	Input Formats
Any host	Disable
192.168.1.120	192.168.1.120/255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0/255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0/255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0/255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128/255.255.255.128

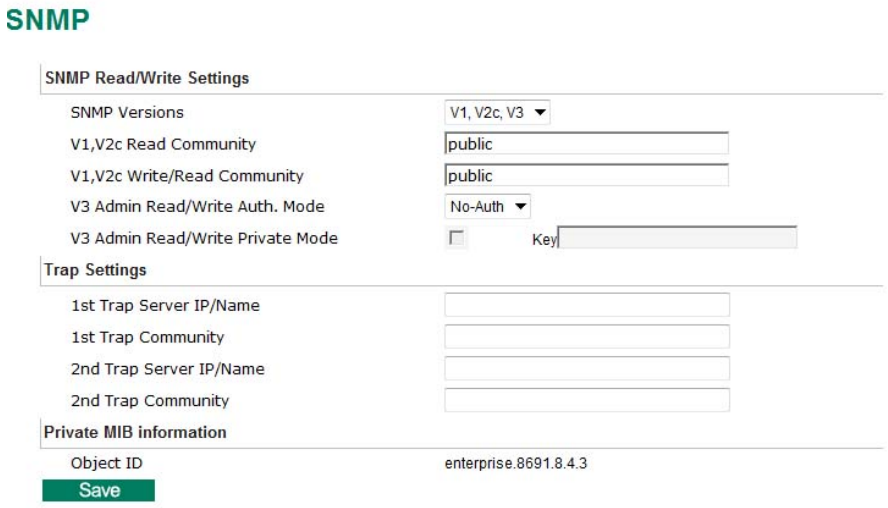
SNMP

The VPort 26 supports three SNMP protocols. The available protocols are SNMP V1, SNMP V2c, and SNMP V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community string public/private (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security. SNMP security modes and security levels supported by the VPort are shown in the following table. Select one of these options to communicate between the SNMP agent and manager.

Protocol Version	Security Mode	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Use a community string match for authentication
	V1, V2c Write/Read Community	Community string	No	Use a community string match for authentication
SNMP V3	No-Auth	No	No	Use account with admin or user to access objects
	MD5 or SHA	MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

Configuring SNMP Settings

The following figures indicate which SNMP parameters can be configured. A more detailed explanation of each parameter is given below the figure.



SNMP Read/ Write Settings

SNMP Versions

Setting	Description	Default
V1, V2c, V3	Select SNMP protocol versions V1, V2c, V3 to manage the switch	V1, V2c, V3
V1, V2c	Select SNMP protocol versions V1, V2c to manage the switch	
V3 only	Select SNMP protocol versions V3 only to manage the switch	

V1, V2c Read Community

Setting	Description	Default
V1, V2c Read Community	Use a community string match for authentication, which means that the SNMP agent accesses all objects with read-only permissions using the community string **public**.	public (max. 30 characters)

V1, V2c Read/Write Community

Setting	Description	Default
V1, V2c Read/Write Community	Use a community string match for authentication, which means that the SNMP agent accesses all objects with read-only permissions using the community string **public**.	public (max. 30 characters)

For SNMP V3, there are two levels of privilege for different accounts to access the VPort. Admin privilege allows access and authorization to read and write MIB files. User privilege only allows reading the MIB file, but does not authorize writing to the file.

Root Auth. Type (For SNMP V1, V2c, V3 and V3 only)

Setting	Description	Default
No-Auth	Use admin. account to access objects. No authentication.	No
MD5-Auth	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA- Auth	Provide authentication based on the MAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

Root Data Encryption Key (For SNMP V1, V2c, V3 and V3 only)

Setting	Description	Default
Enable	8-character data encryption key is the minimum requirement for data encryption. Maximum 30-character encryption key.	No
Disable	No data encryption.	No

User Auth. Type (For SNMP V1, V2c, V3 and V3 only)

Setting	Description	Default
No-Auth	Use account of admin or user to access objects. No authentication.	No
MD5-Auth	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA- Auth	Provide authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

User Data Encryption Key (For SNMP V1, V2c, V3 and V3 only)

Setting	Description	Default
Enable	8-character data encryption key is the minimum requirement for data encryption. Maximum 30-character encryption key.	No
Disable	No data encryption.	No

Trap Settings

Setting	Description	Default
Trap Server IP/Name	Enter the IP address or name of the Trap Server used by your network.	No
Trap Community	Use a community string match for authentication; Maximum of 30 characters.	No

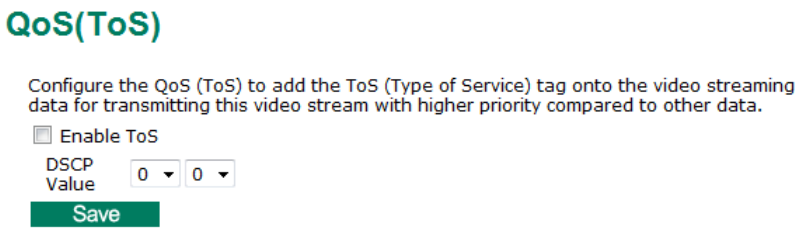
Private MIB information

The private SNMP Object ID of the VPort is the enterprise value: 8691.8.4.3. This number cannot be changed.

NOTE The MIB file is MOXA-VPORT26-MIB.mib (or.my). You can find it on the software CD or the download center of the Moxa website.

QoS (ToS)

Quality of Service (QoS) provides traffic prioritization capabilities to ensure that important data is delivered consistently and predictably. The VPort can inspect layer 3 ToS (Type of Service) information to provide a consistent classification of the entire network. The VPort's ToS capability improves your industrial network's performance and determinism for mission critical applications.

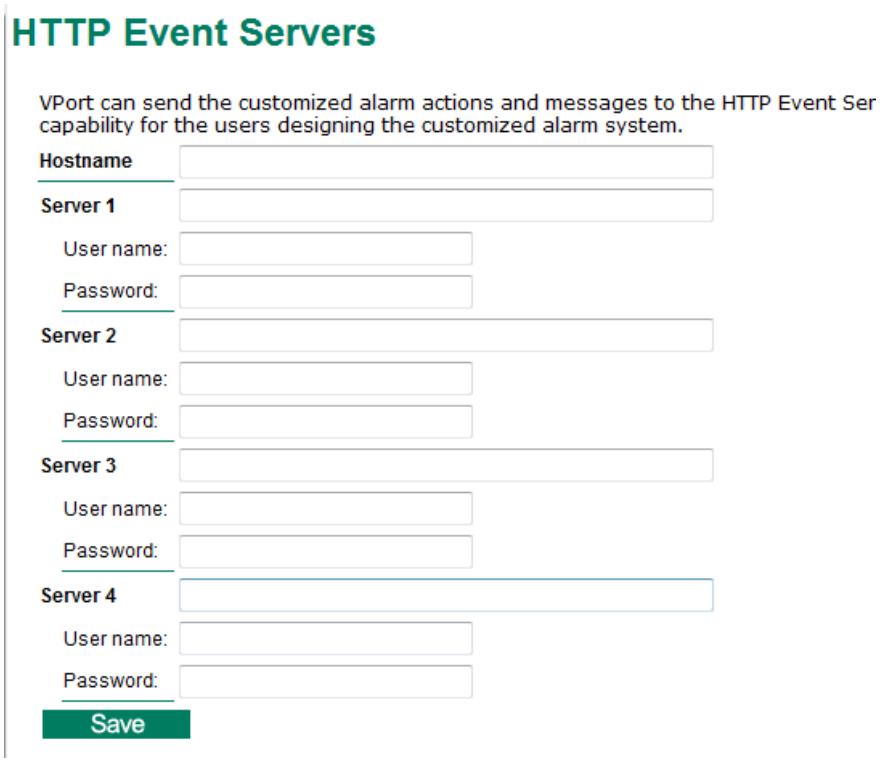


Setting	Description	Factory Default
Enable ToS	Enable the ToS for transmitting the video stream with the given priority	Disable
DSCP Value	Set the mapping table with different ToS values	0, 0

NOTE To configure the ToS values, map to the network environment settings for QoS priority service.

HTTP Event Server

The VPort can send the customized alarm actions and messages to the HTTP Event Servers, which allows users to design a customized alarm system.



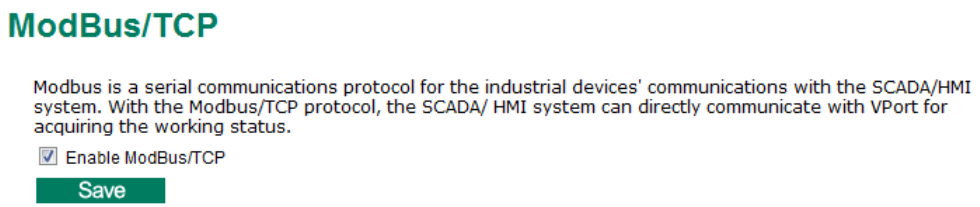
Setting	Description	Factory Default
Host Name	User-defined name for identification	Blank
Server 1, 2, 3, 4	The server's URL address with complete CGI commands Ex. http:// http event server:Port/CGI_Name	Blank
User name	The account name for accessing the HTTP server	Blank
Password	The password for accessing the HTTP server	Blank

Once the Http Alarm is triggered, the VPort will send the following HTTP commands to the HTTP event servers.

```
GET CGI_Name?address=<Hostname or IP Address>&[Custom CGI] HTTP/1.0\r\n
User-Agent: IP camera V1.1\r\n
[Authorization: Basic <Buse64(username:password)>\r\n]
Host: <HTTP Server IP Address>\r\n
Connection: Keep-Alive\r\n
\r\n
```

ModBus/TCP

Modbus is a serial communications protocol which is often used to connect a supervisory computer with a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems. To transmit Modbus over a TCP/IP network, a standard Modbus/TCP protocol is provided. With the support of the Modbus/TCP protocol, the SCADA/HMI system can directly communicate with the VPort to acquire its operational status.

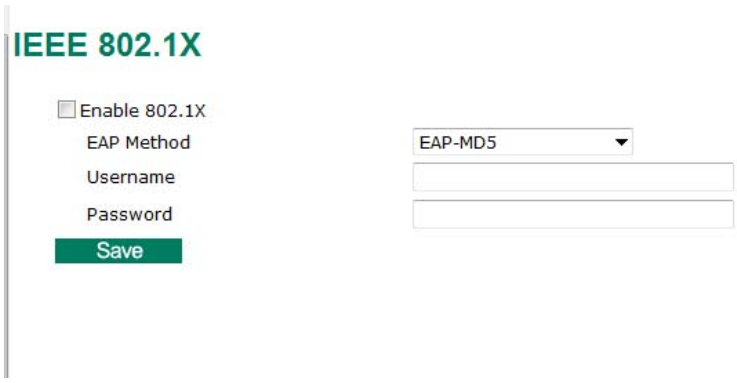


Setting	Description	Factory Default
Enable Modbus/TCP	Enable the Modbus/TCP protocol	Enable

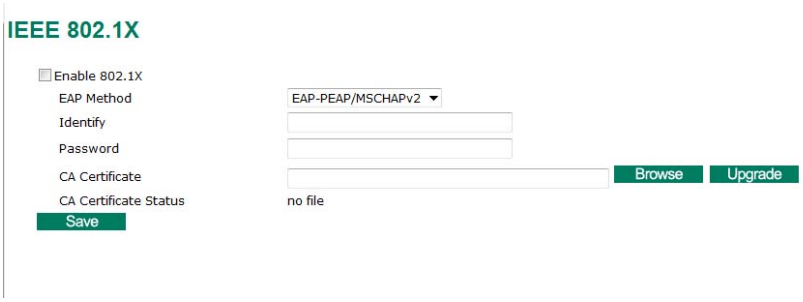
NOTE For Modbus address table, please refer to the Modbus_Address_Define.pdf. You can find it on the software CD or the download center of the Moxa website.

The VPort 26 supports advanced IEEE 802.1X network authentication function. There are three types of 802.1X supported: EAP-MD5, EAP-PEAP/MSCHAPv2 and EAP-TLS. The Administrator should choose the appropriate type base on the network system situation.

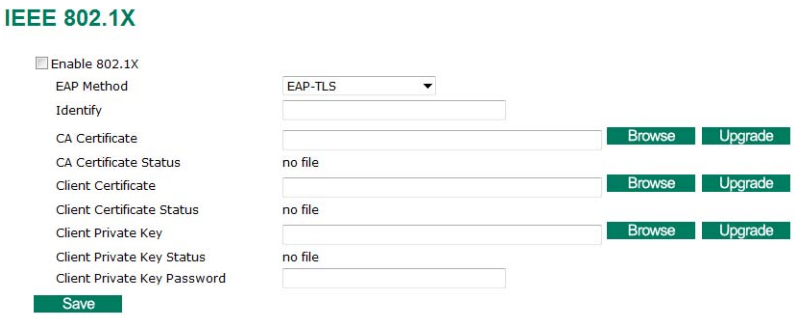
EAP-MD5



EAP-PEAP / MSCHAPv2



EAP-TLS



NOTE Please consult an expert or your network administrator for the configurations of 802.1X if you have trouble in it.

DynaStream™

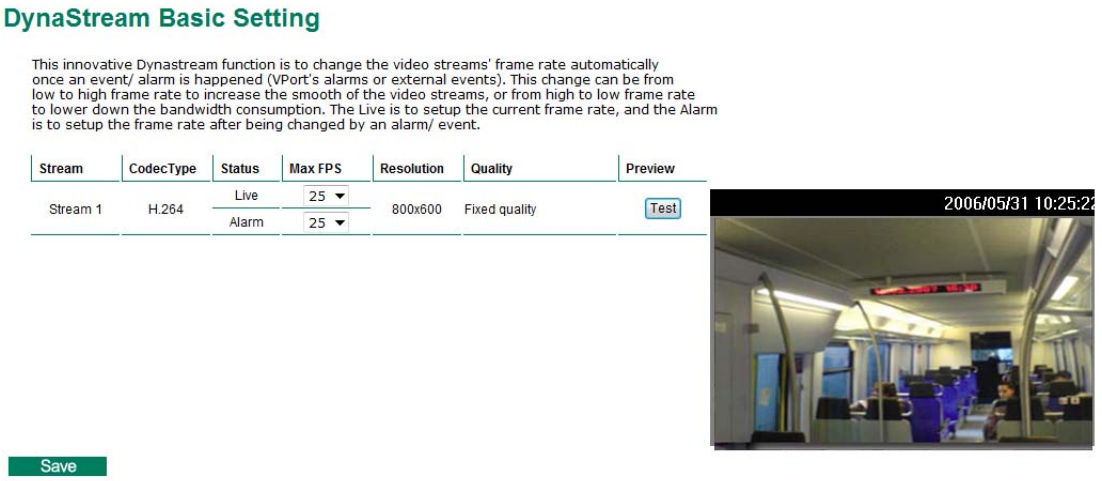
DynaSteam™ is a unique and innovative function that allows for adaptive frame rates in response to events on the network, such as event triggers and system commands. When network traffic becomes congested, DynaStream™ allows VPort products to respond to CGI, SNMP, and Modbus commands from SCADA (as well as the VPort 26's VMD, DI, CGI events, and video loss triggers) and automatically decrease the frame rates to reduce bandwidth consumption. This reserves bandwidth for the SCADA system to maintain Quality of Service (QoS) and guarantees that the SCADA performance will not be impacted by video traffic. For example, the frame rate can be set low during regular streaming to reduce bandwidth usage and automatically switch to a high frame rate during triggered events to ensure quick transmission of critical video data or video streams, or to provide detailed visual images for problem analysis.

NOTE For enabling the DynaStream function from CGI commands and Modbus TCP, please refer to the CGI Commands User's Manual of VPort SDK PLUS and Modbus Address Table

Basic

The administrator can adjust the number of frames per second for each channel. There are two types of frame rate status: Live and Alarm. Live status refers to the normal frames rates for live video displays. Alarm status refers to what the frame rate will be adjusted to when the DynaStream function is activated.

Currently, the video stream for DynaStream is only set up for H.264 video streams, and the resolution and quality are the same as for the settings in the Video Performance configuration.



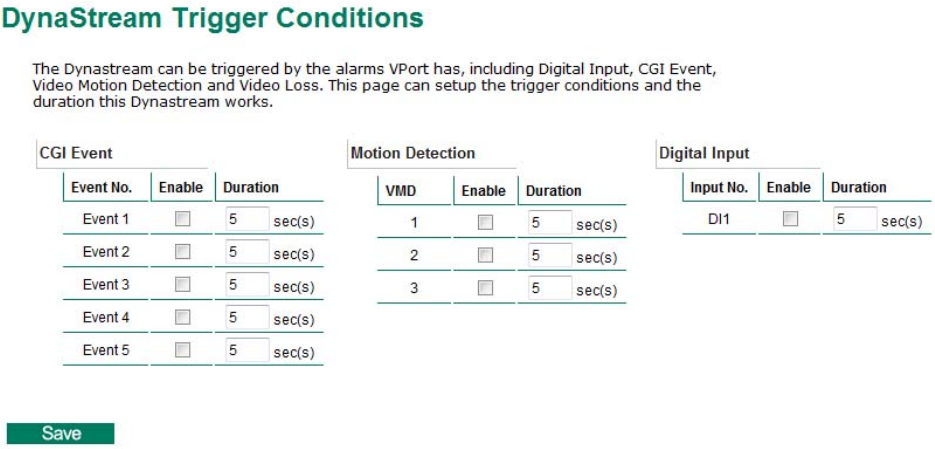
Setting	Description	Factory Default
Max. FPS	For setting the maximum frame rate per second.	PAL: 25 NTSC: 30

After setting the Alarm frame rate, you may preview the video performance by clicking the Test button to ensure it meets your requirements

Conditions

The administrator can set up DynaStream's trigger conditions for facilitating automatic frame rate adjustment, e.g., from Live to Alarm status.

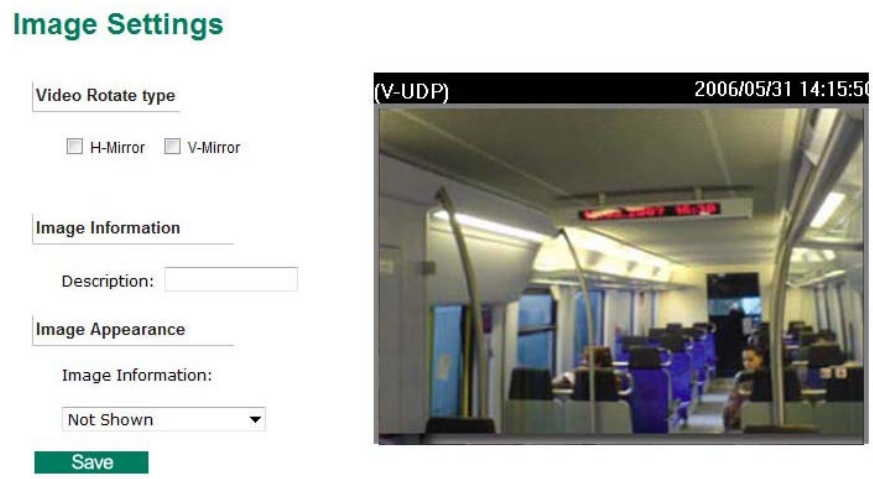
Currently, there are four types of trigger conditions: CGI Event, Motion Detection, and Digital input.



Setting	Description	Factory Default
Enable	To enable or disable the DynaStream function.	Disable
Duration	This refers to the time period that DynaStream is in operation. For example, if the duration is set to 5 seconds, then the frame rate will change from the Live to the Alarm status for the duration of 5 seconds. After 5 seconds, the frame rate will return to the Live status setting.	5 seconds
Trigger Channel	To enable or disable the video channels.	Disabled

Video

Image Settings



Video Rotation

Setting	Description	Default
H-mirror	Rotate the image direction horizontally	None
V-mirror	Rotate the image direction vertically	None

Image Information Setting

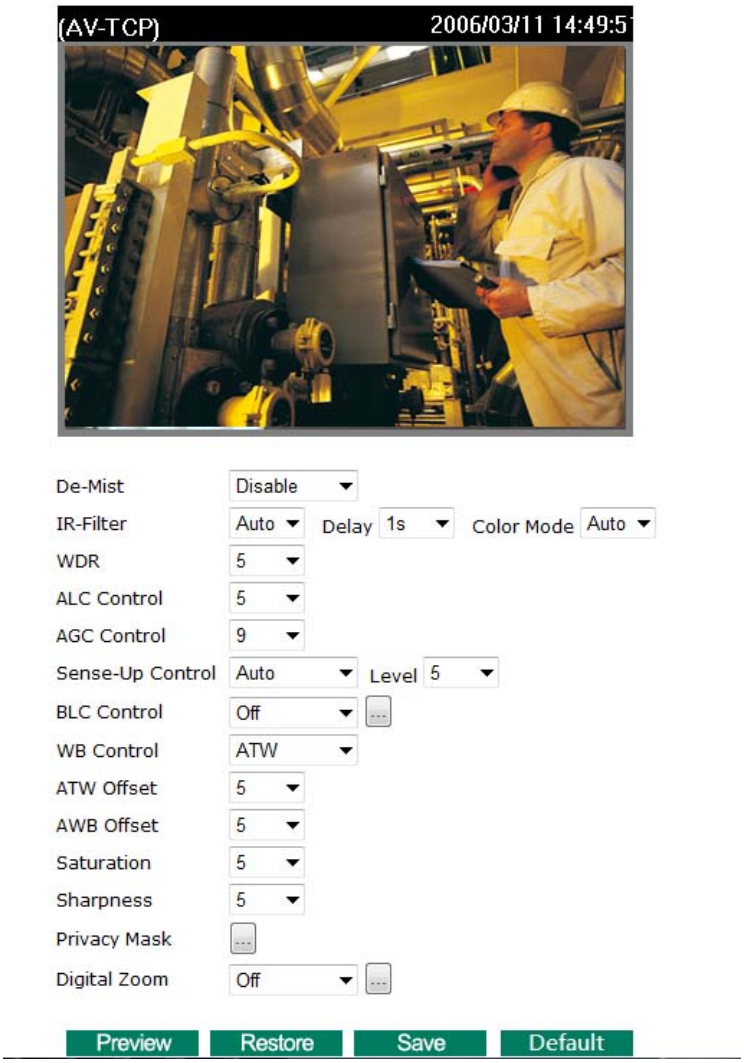
	Description	Default
Description (max. of 14 characters)	The customized description shown on the caption to identify this video camera.	None

Image Appearance Setting

	Description	Default
Image Information	To determine what style of image information is being shown. Includes **Not Shown, Show on the Caption and Show on image**	Not Shown

Camera Setting

A few camera parameters can be configured for improving image quality according to the environment.



De-mist

Setting	Description	Default
De-mist	Activate this De-mist function to sharpen images in rainy, foggy, and hazy environments.	Disable

NOTE Enabling the De-mist function will increase the bit rate of the image a lot, which may affect the network performance.

IR Filter

The VPort 26 supports ICR (IR-cut filter removable) functionality for day & night image switching.

Setting	Description	Default
IR filter	Auto: remove the IR filter automatically Off: disable the IR-cut filter removable function	Auto
Delay	To delay the remove of IR filter for the given time: 1s, 5s, 10s, 20s, 30s, 40s, 50s and 60s.	1s
Color mode	Auto: Change the image to color or black & white automatically On: Change the image to color Off: Change the image to black & white	Auto

WDR

The VPort 26 supports WDR (wide dynamic range) up to 94 db.

Setting	Description	Default
WDR	Configure the WDR function from level 1 (low effect) to level 9 (high effect)	Level 5

ALC control

The VPort 26 supports ALC (auto light control) to adjust the brightness of the image.

Setting	Description	Default
ALC control	Configure the ALC function from level 1 (less brightness) to level 8 (high brightness)	Level 5

AGC control

The VPort 26 supports AGC (auto gain control) for higher image quality in low light environments.

Setting	Description	Default
ALC control	Configure the AGC function from level 1 (low effect) to level 9 (high effect)	Level 5

Sense-up Control

The VPort 26 supports Sense-up control for slow shutter in low light environment.

Setting	Description	Default
Sense-up control	Configure the Sense-up function. Auto: control the sense-up function automatically Off: disable the sense-up function Level: configure the effect of sense-up from 1 (low effect) to 9 (high effect)	Auto, Level 5

BLC control

The VPort 26 supports area-selectable BLC (backlight compensation) for clearer objects in backlit environments.

Setting	Description	Default
BLC control	Configure the BLC function. On: enable the BLC function Off: disable the BLC function	Off
...	Open the area-selectable configuration webpage   The image is separated into 48 blocks. To select which areas to enabling the BLC function in, select the corresponding block in the table.	

WB control

The VPort 26 supports WB (White balance) control for tuning the image color based on the field-site environment. To use this function, follow the steps below.

Step 1:

Point the camera at a white, lit object

Step 2:

Select ATW (Auto-tracking white balancing) to let the camera to adjust to the correct right white color. If the color is not correct, please configure the ATW offset number from 1 to 9 to find the correct color.

Step 3:

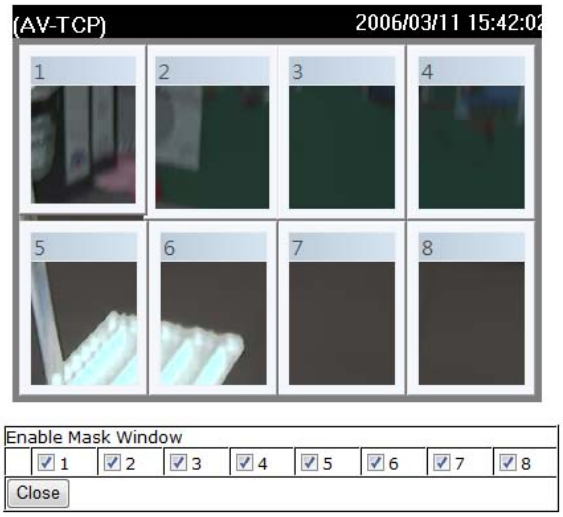
Select AWB (Auto white balance) to adjust the color in the environment. If the color is not correct, please configure the AWB offset number from 1 to 9 to find the correct color.

Saturation and Sharpness

Setting	Description	Default
Saturation	Configure the saturation of image from 1 (low) to 9 (high)	5
Sharpness	Configure the sharpness of image from 1 (low) to 9 (high)	5

Privacy mask

VPort 26 supports up to 8 privacy mask areas on image for privacy protection.

Setting	Description	Default
...	Open the privacy mask configuration webpage. There are total 8 privacy mask areas. Select which mask areas to cover with a privacy mask. 	

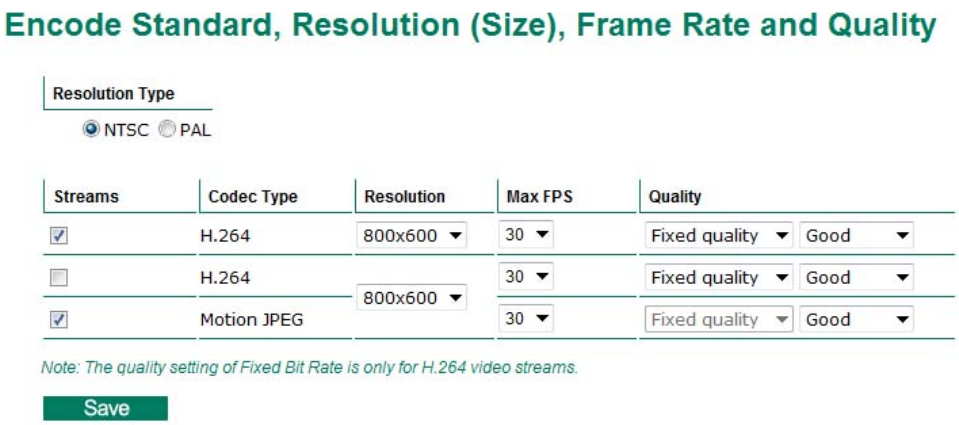
Digital Zoom

VPort 26 supports 4X digital zoom on the image.

Setting	Description	Default
Digital zoom	On: Enable the digital zoom function Off: Disable the digital zoom function	Off
...	Open the digital zoom webpage. The window on the image is the 4X image view. Use the left button of the mouse to adjust the region of the 4x image view. Then click the close button. The image showed on the homepage will be the 4X image view. 	

Video Performance

The VPort 26 can send a maximum of three simultaneous video streams: two H.264 and one MJEPG. In fact, the VPort 26 has two encoder engines. The first encoder engine can generate one H.264 video stream, and this H.264 video stream is a completely independent video stream, which means its resolution, FPS and video quality can be configured independently. The second encoder engine can generate one H.264 video stream and one MJPEG video stream. Because both the H.264 and MJPEG video streams come from the same encoder engine, their resolution must be the same, but the FPS and the Video Quality can be configured separately. The administrator can set the Resolution, Max. Frame Rate and Video Quality on this web page.



Resolution Type

For meeting different CCTV resolution requirement, there are **NTSC** or **PAL** mode can be selected.

NOTE Due to there is only one video source, different resolution will have different viewing angle.

Streams

Setting	Description	Default
Enable the video streams	To enable the VPort to send this video streams or not.	Enable stream 1: H.264 and stream 2: MJPEG

Codec Type

This codec type shows the codec of each video stream.

Resolution

The VPort 26 supports 5 different resolutions: SVGA, Full D1, 4CIF, VGA, CIF, and QCIF.

Setting	Description	Default
Select the image size	6 image resolutions (size) are provided. The administrator can choose each option with NTSC or PAL modulation.	800 x 600

Resolution	NTSC	PAL
SVGA	800 x 600	800x 600
Full D1	720 x 480	720 x 576
4CIF	704 x 480	704 x 576
VGA	640 x 480	640 x 480
CIF	352 x 240	352 x 288
QCIF	176 x 112	176 x 144

Max. FPS (Frame per second)

Setting	Description	Default
Maximum frame rate	The maximum frame rate is different to accommodate different modulations of video input. Administrators can also set up the maximum frame rate to optimize bandwidth use. NTSC: 1, 3, 5, 10, 15, 20, 25, 30 PAL: 1, 3, 5, 8, 12,16, 20, 25	30 for NTSC, 25 for PAL

NOTE Frame rate (frames per second) is determined by the resolution, image data size (bit rate), and transmission traffic status. The Administrator and users can check the frame rate status in the **FPS Status** on the VPort's web homepage.

NOTE The VPort 26 supports a maximum of three simultaneous video streams, and the FPS will be affected when all three video streams are enabled. If the video quality is set very high for all three video streams, the total FPS for the three streams combined is about 75. We strongly recommended that you configure these three video streams based on specific requirements to optimize video performance.

Video Quality Control

Video Quality Control is used to optimize the bandwidth of the MPEG4 video stream. There are 2 modes for video quality control.

Setting	Description	Default
Fixed bit rate (Only for H.264)	The administrator can fix the bandwidth to tune the video quality and FPS (frames per second) to the optimum combination. Different resolutions have different bandwidth parameters. The VPort will tune the video performance according to the bandwidth. A higher bandwidth means better quality and higher FPS.	600Kbps in 800x600 resolution
Fixed Quality	The administrator can set the image quality to one of 5 standards: **Medium, Standard, Good, Detailed**, or **Excellent**. The VPort will tune the bandwidth and FPS automatically to the optimum combination.	Good

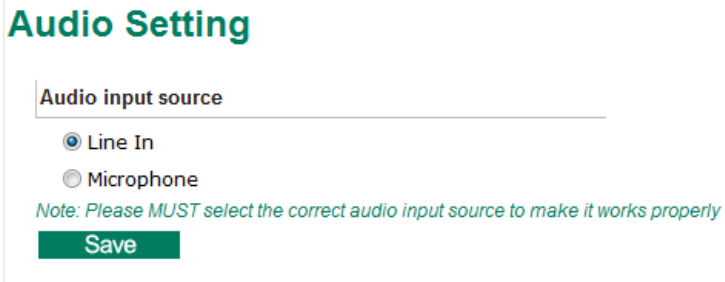
Video Size Bit rate	800x600	720x480(NTSC) 720x576(PAL)	704x480(NTSC) 704x576(PAL)	640x480(NTSC) 640x480(PAL)	352x240(NTSC) 352x288(PAL)	176x112(NTSC) 176x144(PAL)
B0	267 kbps	230 Kbps	225 Kbps	170 Kbps	56 Kbps	14 Kbps
B1	600 kbps	518 Kbps	507 Kbps	384 Kbps	126 Kbps	31 Kbps
B2	1200 kbps	1036 Kbps	1014 Kbps	768 Kbps	253 Kbps	63 Kbps
B3	1800 kbps	1555 Kbps	1521 Kbps	1152 Kbps	379 Kbps	95 Kbps
B4	2400 kbps	2073 Kbps	2028 Kbps	1536 Kbps	506 Kbps	126 Kbps
B5	3000 kbps	2592 Kbps	2535 Kbps	1920 Kbps	633 Kbps	158 Kbps
B6	3600 kbps	3110 Kbps	3042 Kbps	2304 Kbps	759 Kbps	290 Kbps
B7	4200 kbps	3628 Kbps	4549 Kbps	2688 Kbps	886 Kbps	221 Kbps

NOTE The image quality, FPS, and bandwidth are influenced significantly by network throughput, system network bandwidth management, applications the VPort runs (such as VMD), how complicated the image is, and the performance of your PC or notebook when displaying images. The administrator should take into consideration all of these variables when designing the video over IP system, and when specifying the requirements for the video system.

Audio

Audio Source

The VPort supports real-time and synchronous video/audio transmission. Administrators need to select the correct audio input type to avoid audio input distortion.



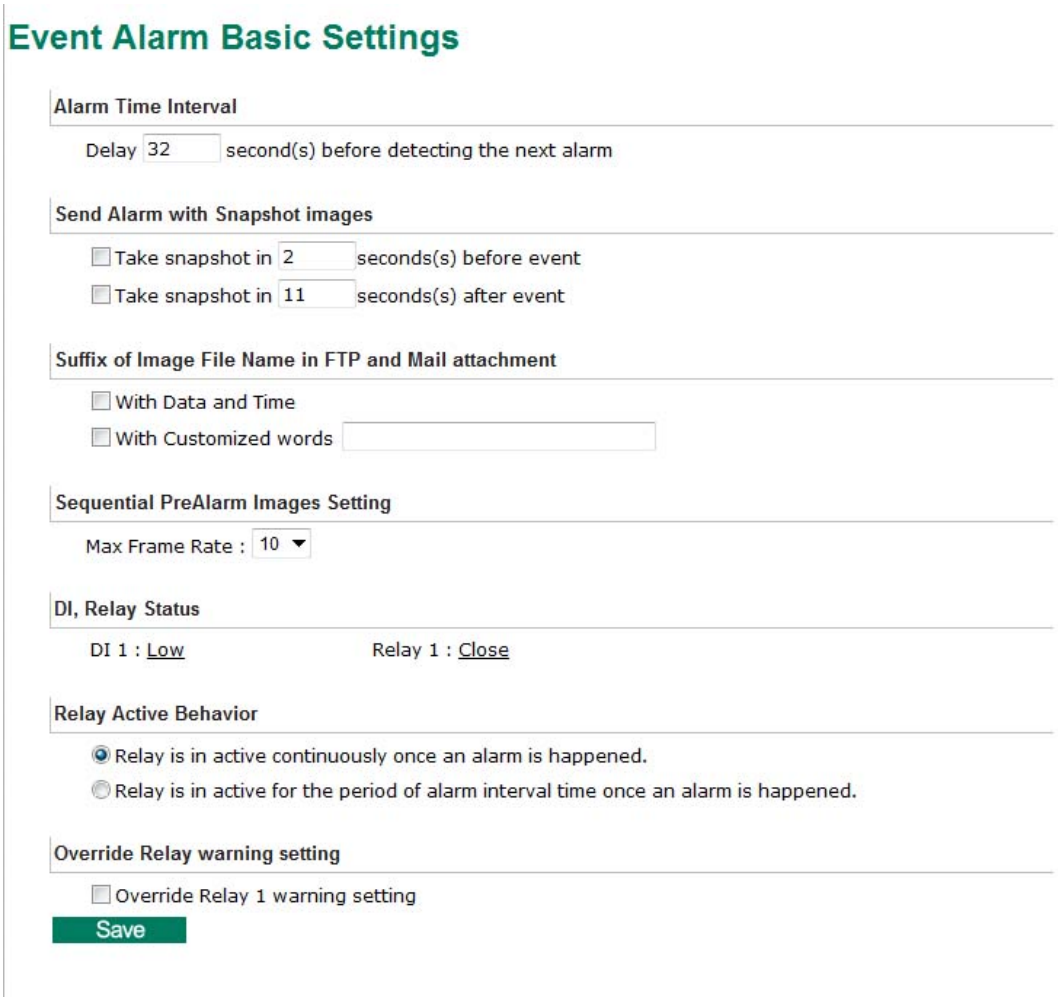
Alarm

Event Alarm

Four kinds of event alarm are provided by the VPort for building an intelligent video surveillance system.

Alarm Type	Triggered Condition	Triggered Action
Video Motion Detection (VMD)	VMD 1 VMD 2 VMD 3	Relay Email FTP HTTP Event Server Record on SD card
Video Loss	Video signal is lost	Relay HTTP Event Server
Digital Input	High, Low, Rising and Falling	Relay Email FTP HTTP Event Server Record on SD card
CGI Event	The CGI trigger message	Relay Email FTP HTTP Event Server Record on SD card
Sequential Snapshot	Enable sequential snapshot	Email FTP

Basic



Alarm Time Interval

Setting	Description	Default
Delay second(s) before detecting the next alarm	Set the minimum time interval before another event alarm is triggered.	32 seconds (10 to 999 seconds)

NOTE The delay before triggering the next alarm cannot be less than the time needed to take a snapshot after an event (post-event image).

Send Alarm with Snapshot images

Setting	Description	Default
Take snapshot seconds(s) before the event	A snapshot image is taken this number of seconds before the event alarm is triggered.	2 seconds (from 1 to 6 seconds)
Take snapshot seconds(s) after the event	A snapshot image is taken this number of seconds after the event alarm is triggered.	11 seconds (from 1 to 999 seconds)

NOTE VPort products will take 3 JPEG snapshot images: VPRE.JPG (pre-event), VTRG.JPG (the moment of event) and VPOS.JPG (post-event) for the video channel when the trigger condition is met. The three snapshots can also be downloaded by Email and FTP.

Suffix of Image File Name in FTP and Mail attachment

The snapshot images can be sent either by email or FTP. Administrators can add a suffix to the filename of each JPEG snapshot image to make it easier to identify the files when using FTP to download the snapshots.

Setting	Description	Default
With Date and Time	Enable or disable adding the date and time to the filename.	Disable
With Customized words	Enable or disable adding some additional custom text to the filename to identify the snapshot image.	Disable

Sequential PreAlarm Image Setting

The VPort 26 supports a 24MB memory buffer to record pre-alarm MJPEG images up to 15FPS. This function configures the frame rate of the MJPEG images being recorded.

Setting	Description	Default
Max. Frame Rate	Configures the maximum pre-alarm frames-per-second to be logged, either 1, 3, 5, 10, 12, or 15.	10

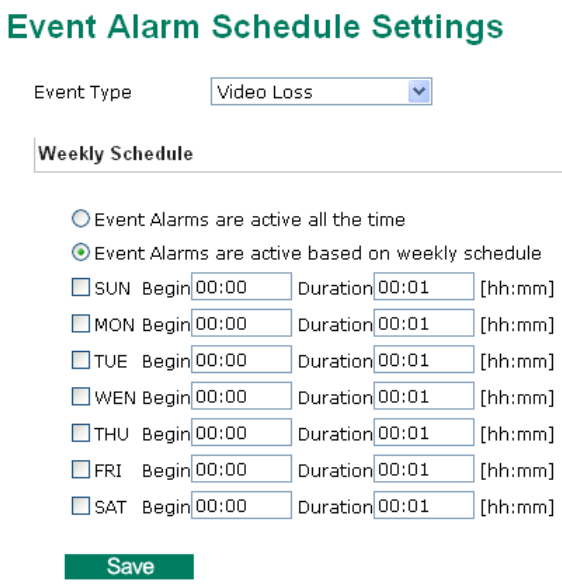
NOTE Pre-alarm buffers are 9MB in size. So if the maximum frame rate is set to 10, and the video size of each image is 30KB, then there will be 30 seconds of pre-alarm MJPEG images recorded: 9000KB/30KB/10=30. If the maximum frame rate is set to fifteen, then there will be 20 seconds of pre-alarm images recorded: 9000KB/30KB/15=20.

DI, Relay Status

Administrators can check the current DI and Relay status of the VPort in the **"DI, Relay Status"** section on the "Event Alarm Basic Settings" page. Two options are available to return the relay's status back to the system defaults. To enable the function, check the **Override Relay 1 warning setting** box, and then click on **Save**. In addition, in the "**Relay Active behavior**" section, you can configure the duration of the relay action, with options of activating the relays continuously, for the specified **Alarm Interval Time**, or for the period of time when the alarm is triggered.

Schedule

A schedule is provided to set event alarms for daily security applications.



Event Type

Setting	Description	Default
Video Loss, Digital Input, CGI Event, and Sequential Snapshot	Set up the schedule of each kind of event type.	Video Loss

Weekly Schedule

Setting	Description	Default
Event Alarms are active all the time	Select the option “Event Alarms are active all the time”	Event Alarms are active based on a weekly schedule
Event Alarms are active based on a weekly schedule	Select to operate event alarms on a weekly schedule.	

NOTE The applications described in the following sections will only work properly if either **Event Alarms are active all the time** or **Event Alarms are active based on weekly schedule** is Selected.

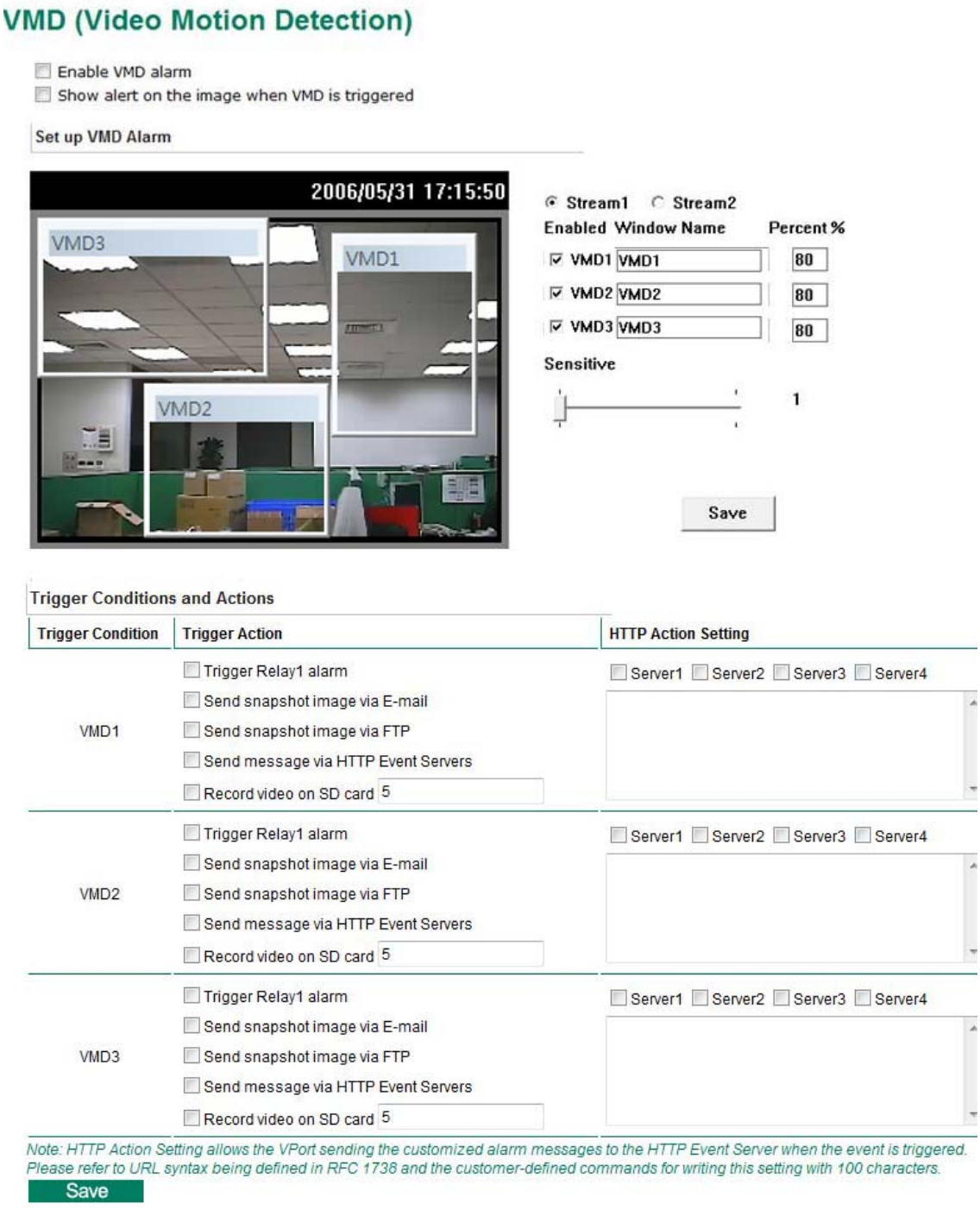
Setting	Description	Default
□Sun □Mon □Tue □Wed □Thu □Fri □Sat	Select the weekday for scheduling event alarms.	None
Begin 00:00	Set the start time of the event alarm.	00:00
Duration 00:00	Set the duration for the event alarm to be active.	00:00

NOTE Administrators can use the following steps to set up an event schedule:

1. Select Event Type
2. Enable “Event Alarms are active based on weekly schedule”
3. Select the weekday
4. Set the start time
5. Set the duration this event will be active.
6. Save

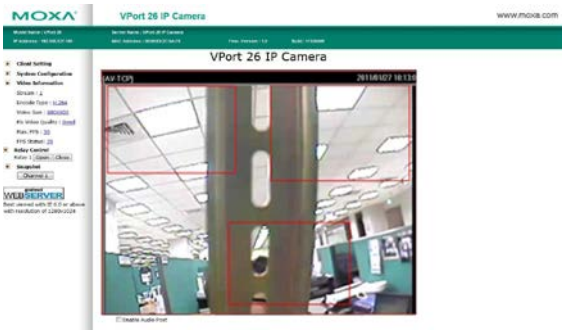
Motion Detection

Video Motion Detection (VMD) is an intelligent event alarm for video surveillance network systems. With the 3 area-selectable VMDs and sensitivity/percentage tuning, administrators can easily set up the VMD alarm to be active 24 hours a day, 7 days a week.



Setting	Description	Default
Enable VMD alarm	Enable or disable the Video Motion Detection alarm	Disabled
Show alert on the image when VMD is triggered	Enable or disable the “show the alert,” which when enabled displays a red square frame on the video image of the VMD alarm notification	Disabled

NOTE Once the Show alert on the image when VMD is triggered is enabled, the red frames that appear on the homepage image indicate the size of the VMD window set up by the administrator.



Setup a VMD Alarm

Setting	Description	Default
Enable	Enable or disable the VMD1, 2, and 3	Disabled
Window	The name of each VMD window	Blank
Percent	The minimum percentage of an image change for triggering VMD. Decrease the percentage to make it easier to trigger VMD.	80
Sensitive	The measurable difference between two sequential images for triggering VMD. Increase the sensitivity to make it easier for VMD to be triggered.	1

NOTE After setting the VMD Alarm, click the **Save** button to save the changes

Trigger Conditions and Actions

For each VMD administrators can set triggers, such as “send snapshot image via E-mail”, “send snapshot image via FTP”, “send Message via HTTP event servers”, “save snapshot on storage” and “record video on SD card”.

Setting	Description	Default
Trigger Relay1 alarm	Once the VMD is triggered, the Relay alarm will be activated	Disabled
Send snapshot image via E-mail	Once this VMD is triggered, the VPort will send the snapshot images set in the **Event Alarm / Basic** page to the E-mail addresses, which are set in the **Network / SMTP Server** page.	Disabled
Send snapshot image via FTP	Once this VMD is triggered, the VPort will send the snapshot images set in the **Event Alarm / Basic** page to the FTP server, which are set in the **Network / FTP Server** page.	Disabled
Send message via HTTP Event Servers	Once this VMD is triggered, the VPort will send the message set in **HTTP Action Setting** to the HTTP event servers, which are set in the **Network / HTTP Event Server** page.	Disabled
Record video on SD card for ☐ Sec	Once this VMD is triggered, then for a configured time period VPort will record video to an (optional) SD card.	Disabled

HTTP Action Setting

Setting	Description	Default
Server 1, 2, 3, or 4	Select the HTTP event server for sending the HTTP action	Disabled
Blank text box	For customizing the message to the HTTP event server.	Blank

How to Configure a VMD alarm

Step 1:
Check the **Enable VMD alarm** box. If the Administrator wants to show the red frame alert on the image on the VPort 26's web homepage, check the **Show alert on the image when VMD is triggered** box. Click on the **Save** button to save these two configurations.

Step 2:
Select **Stream 1** or **Stream 2** for video motion detection. Check VMD1 through 3 to enable the respective VMD windows. Left click the title bar of this window to move the location of the VMD window, or drag the border to change the window size so that it fits the desired VMD area.

Step 3:
Assign a name to the VMD window in the **Window Name** column.

Step 4:
Set up the **Percent%** parameters for individual VMD windows and the **Sensitivity** for all VMD windows.

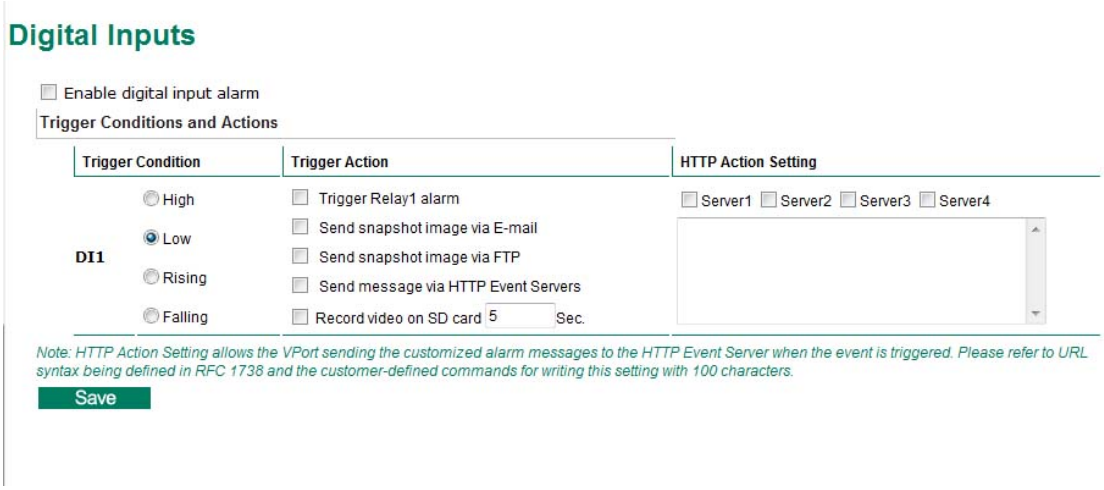
Step 5:
Click on the **Save** button to save the settings.

Step 6:
To test the VMD condition, check the action of the graphics bar on the left side of the save button. Wave your hand in front of the camera, in the VMD area, and then note which color shows up in the graphics bar. Green means VMD is not triggered. Red means VMD is triggered.

Step 7:
Set up the Trigger Conditions and Actions of each VMD, and then click on the **Save** button to save these configurations.

NOTE Video Motion Detection is provided as a reference because it is environment-dependent. When the settings are configured to be very sensitive to motion, some triggered events might actually be false alarms that were triggered by only a small difference between sequential images. These false alarms might be triggered by the flicker of fluorescent lights, the movement of shadows, or similar everyday events.

Digital Input



Setting	Description	Default
Enable digital input alarm	Enable or disable the digital input alarm.	Disable

Trigger Conditions

Setting	Description	Default
High	The DI is always in the “High” state after an alarm is detected.	Disable
Low	The DI is always in the “Low” state after an alarm is detected.	Enable
Rising	The DI works from state “Low” to state “High” and then back to state “Low” when an alarm is detected.	Disable
Falling	The DI works from state “High” to state “Low” and then back to state “High” when an alarm is detected.	Disable

NOTE Please refer to Chapter 1 to see the DI specifications.

Trigger Actions

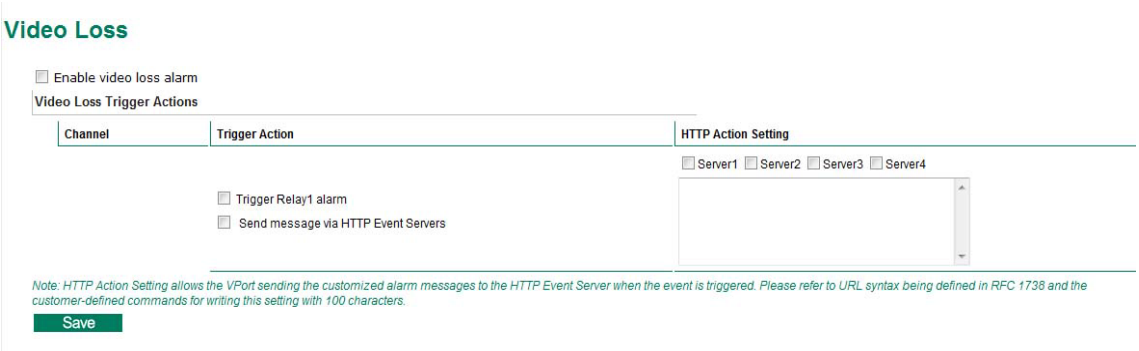
Setting	Description	Default
Trigger Relay1 alarm	Once this DI is triggered, the Relay1 alarm will be activated	Disable
Send snapshot image via E-mail	Once this DI is triggered, the VPort will send the snapshot images set in the **Event Alarm / Basic** page to the E-mail addresses, which are set in the **Network / SMTP Server** page.	Disable
Send snapshot image via FTP	Once this DI is triggered, the VPort will send the snapshot images set in the **Event Alarm / Basic** page to the FTP server, which are set in the **Network / FTP Server** page.	Disable
Send message via HTTP Event Servers	Once this DI is triggered, the VPort will send the message set in **HTTP Action Setting** to the HTTP event servers, which are set in the **Network / HTTP Event Server** page.	Disable
Record video on SD card for Sec	Once this DI is triggered, then for a configured time period VPort will record video to an (optional) SD card.	Disabled

HTTP Action Setting

Setting	Description	Default
Server 1, 2, 3, 4	Select the HTTP event server for sending the HTTP action	Disable
Blank column	Administrators can customize the message sent to the HTTP event sever in this column	Blank

Video Loss

The Video Loss event means that the VPort cannot detect the camera module.



Video Loss Trigger Actions

Setting	Description	Default
Enable video loss alarm	Enable or disable video loss alarm.	Disable
Trigger Relay1 alarm	Once the video is lost, the Relay alarm will be activated	Disabled
Record video on SD card for ☐ sec	Once the video is lost, then for a configured time period the VPort will record video to an (optional) SD card.	Disabled

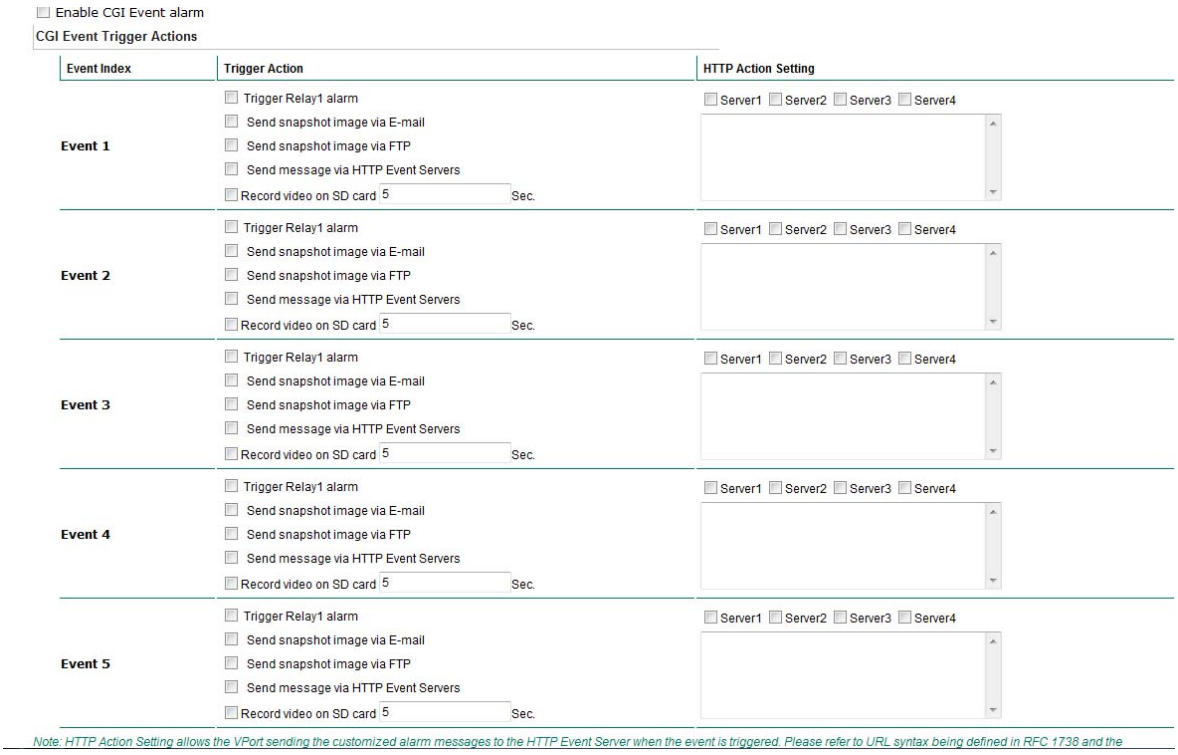
HTTP Action Setting

Setting	Description	Default
Server 1, 2, 3, 4	Select the HTTP event server for sending the HTTP action.	Disable
Blank column	Administrators can customize the message sent to the HTTP event sever in this column.	Blank

CGI Event

The VPort can accept 5 CGI commands, which are sent from external devices, such as ioLogik series Ethernet I/O, to be the event alarms.

NOTE The VPort only can accept the CGI commands that follow the VPort's CGI commands format.



CGI Event Trigger Actions

Setting	Description	Default
Enable CGI Event alarm	Enable or disable CGI Event alarm.	Disable
Event	Select the Event 1, 2, 3, 4, 5	Disable
Trigger Relay1 alarm	Once this CGI Event is triggered, the Relay alarm will be activated	Disabled
Send snapshot image via FTP	Once this CGI Event is triggered, the VPort will send the snapshot images set in the **Event Alarm / Basic** page to the FTP server, which are set in the **Network / FTP Server** page.	Disable
Send message via HTTP Event Servers	Once this CGI Event is triggered, the VPort will send the message set in the **HTTP Action Setting** to the HTTP event servers, which are set in the **Network / HTTP Event Server** page.	Disable
Save snapshot to storage	The pre-alarm, trigger, and post-alarm snapshot images can be saved on an (optional) SD card.	Disabled
Record video on SD card for ☐ Sec	Once this VMD is triggered, then for a configured time period the VPort will record video to an (optional) SD card.	Disabled

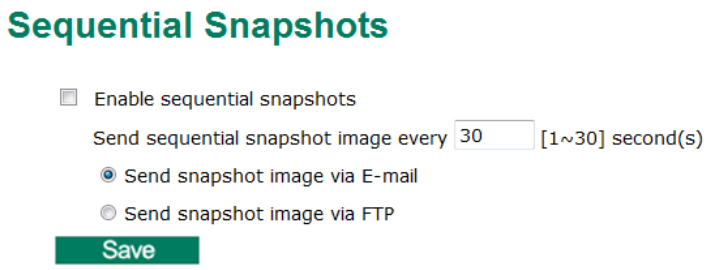
HTTP Action Setting

Setting	Description	Default
Server 1, 2, 3, 4	Select the HTTP event server for sending the HTTP action	Disable
Blank column	Administrators can customize the message sent to the HTTP event sever in this column	Blank

Sequential Snapshot

With this feature, the VPort can upload snapshots periodically to an external E-mail or FTP server as a live video source. Use the **Send sequential snapshot image every seconds** option to set the time interval. The interval can be set to any number between 1 and 9999 seconds.

Setting	Description	Default
Enable Sequential Snapshots	Enable or disable the Sequential Snapshots.	Disable
Send sequential snapshot image every seconds	Set the time interval of each snapshot image.	30 seconds (from 1 second to 30 seconds)
Send Snapshot image via E-mail	Choose how to send the snapshot images.	Send Snapshot image via Email
Send Snapshot image via FTP		



A

Frequently Asked Questions

Q: What if I forget my password?

A: Every access to the IP camera needs authentication, unless the admin password is set up as blank. If you are one of the managed users, you will need to ask the administrator for the password. If you are the administrator, there is no way to recover the admin password. The only way to regain access to IP camera is to utilize the **RESET** button to restore the factory settings (see Chapter 1 for details).

Q: Why can't I see video from the IP camera after it has been authenticated?

A: There are many possible scenarios:
(a) If the IP camera is installed correctly and you are accessing the IP camera for the first time using Internet Explorer, adjust the security level of Internet Explorer to allow installation of plug-ins.
(b) If the problem still exists, the number of users accessing the IP camera at the same time may exceed the maximum that the system allows.
(c) If the video is still not displayed, please try to run the Factory default to see if it is in work properly.

Q: What is the plug-in for?

A: The plug-in provided by IP camera is used to display motion pictures. The plug-in is needed because Internet Explorer does not support streaming technology. If your system does not allow installation of plug-in software, the security level of the web browser may need to be lowered. It is recommended that you consult the network supervisor in your office before adjusting the security level.

Q: Why is the timestamp different from the system time of my PC or notebook?

A: The timestamp is based on the system time of the IP camera. It is maintained by an internal real-time clock, and automatically synchronizes with the time server if the video encoder is connected to the Internet and the function is enabled. Differences of several hours may result from the time zone setting.

Q: How many users are allowed to access the IP camera at the same time?

A: Basically, there is no limitation. However the video quality also depends on the network. To achieve the best effect, the VPort 26 IP camera will allow 10 video streams for udp/tcp/http connections. We recommend using an additional web server that retrieves images from the IP camera periodically if you need to host a large number of users.

Q: What is the IP camera's video rate?

A: The codec can process 30 frames per second internally. However the total performance is subject to many variables, as listed below:

1. Network throughput.
2. Bandwidth share.
3. Number of users.
4. More complicated objects result in larger image files.
5. The speed of the PC or notebook that is responsible for displaying images.

Q: How can I keep the IP camera as private as possible?

A: The IP camera is designed for surveillance purposes and has many flexible interfaces. The user authentication and special confirmation when installing can keep the video encoder from unauthorized access. You may also change the HTTP port to a non-public number. Check the system log to examine any abnormal activities and trace the origins.

Q: Why can't I access the IP camera when I set up some options in the application?

A: When the IP camera is triggered by events, video and snapshots will take more time to write to memory. If the events occur too often, the system will always be busy storing video and images. We recommend using sequential mode or an external recorder program to record motion pictures if the event is frequent. If you prefer to retrieve images by FTP, the value could be smaller since an FTP server responds more quickly than a web server. Once the system is too busy to configure, use the restore factory default and reset button to save the system.

B

Modbus Address Table

Read/Write Registers (Support Function Code 4 & Function Code 3)

Address	Access	Data Type	Description
System Information			
0x0000	R	1 word	Vendor ID = **0x1393**
0x0001	R	1 word	Unit ID (Ethernet = 1)
0x0002	R	1 word	Product Code = Magic Code(2 byte)
0x0010	R	20 word	Vendor Name = "Moxa" Word 0 Hi byte = 'M' Word 0 Lo byte = 'o' Word 1 Hi byte = 'x' Word 1 Lo byte = 'a' Word 2 Hi byte = '\0' Word 2 Lo byte = '\0'
0x0030	R	20 word	Product Name = "VPort 26" Word 0 Hi byte = 'V' Word 0 Lo byte = 'P' Word 1 Hi byte = '0' Word 1 Lo byte = 'r' Word 2 Hi byte = 't' Word 2 Lo byte = ' ' Word 3 Hi byte = '2' Word 3 Lo byte = '6' Word 4 Hi byte = '\0'
0x0050	R	1 word	Product Serial Number
0x0051	R	2 word	Firmware Version Word 0 Hi byte = major (A) Word 0 Lo byte = minor (B) Word 1 Hi byte = release (C) Word 1 Lo byte = build (D)
0x0053	R	2 word	Firmware Release Date Firmware was released on 2007-05-06 at 09 o'clock Word 0 = 0x0609 Word 1 = 0x0705
0x0055	R	3 word	Ethernet MAC Address Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0x00 Word 0 Lo byte = 0x01 Word 1 Hi byte = 0x02 Word 1 Lo byte = 0x03 Word 2 Hi byte = 0x04 Word 2 Lo byte = 0x05

0x005B	R	1 word	Channel 1 Video Signal 0x0000:Off 0x0001:On
0x0080	R	1 word	DI1 0x0000:Off 0x0001:On
0x0084	R/W	1 word	DO1 0x0000:Off 0x0001:On
0x0700	RW	1 word	Record Duration
0x0701	RW	1 word	Record Always Enable 0x0000:Disable 0x0001:Enable
0x0800	RW	1 word	DynaStream Duration
0x0801	RW	1 word	DynaStream Always Enable 0x0000:Disable 0x0001:Enable

C

Time Zone Table

The hour offsets for different time zones are shown below. You will need this information when setting the time zone in automatic date/time synchronization. GMT stands for Greenwich Mean Time, which is the global time that all time zones are measured from.

(GMT-12:00)	International Date Line West
(GMT-11:00)	Midway Island, Samoa
(GMT-10:00)	Hawaii
(GMT-09:00)	Alaska
(GMT-08:00)	Pacific Time (US & Canada), Tijuana
(GMT-07:00)	Arizona
(GMT-07:00)	Chihuahua, La Paz, Mazatlan
(GMT-07:00)	Mountain Time (US & Canada)
(GMT-06:00)	Central America
(GMT-06:00)	Central Time (US & Canada)
(GMT-06:00)	Guadalajara, Mexico City, Monterrey
(GMT-06:00)	Saskatchewan
(GMT-05:00)	Bogota, Lima, Quito
(GMT-05:00)	Eastern Time (US & Canada)
(GMT-05:00)	Indiana (East)
(GMT-04:00)	Atlantic Time (Canada)
(GMT-04:00)	Caracas, La Paz
(GMT-04:00)	Santiago
(GMT-03:30)	Newfoundland
(GMT-03:00)	Brasilia
(GMT-03:00)	Buenos Aires, Georgetown
(GMT-03:00)	Greenland
(GMT-02:00)	Mid-Atlantic
(GMT-01:00)	Azores
(GMT-01:00)	Cape V erde Is.
(GMT)	Casablanca, Monrovia
(GMT)	Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
(GMT+01:00)	Amsterdam, Berlin, Bern, Stockholm, Vienna

(GMT+01:00)	Belgrade, Bratislava, Budapest, Ljubljana, Prague (GMT+01 :00) Brussels, Copenhagen, Madrid, Paris
(GMT+01:00)	Sarajevo, Skopje, Warsaw, Zagreb
(GMT+01:00)	West Central Africa
(GMT+02:00)	Athens, Istanbul, Minsk
(GMT+02:00)	Bucharest
(GMT+02:00)	Cairo
(GMT+02:00)	Harare, Pretoria
(GMT+02:00)	Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
(GMT+02:00)	Jerusalem
(GMT+03:00)	Baghdad
(GMT+03:00)	Kuwait, Riyadh
(GMT+03:00)	Moscow, St. Petersburg, Volgograd
(GMT+03:00)	Nairobi
(GMT+03:30)	Tehran
(GMT+04:00)	Abu Dhabi, Muscat (GMT+04:00) Baku, Tbilisi, Yerevan (GMT+04:30) Kabul
(GMT+05:00)	Ekaterinburg
(GMT+05:00)	Islamabad, Karachi, Tashkent (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
(GMT+05:45)	Kathmandu
(GMT+06:00)	Almaty, Novosibirsk (GMT+06:00) Astana, Dhaka
(GMT+06:00)	Sri Jayawardenepura (GMT+06:30) Rangoon
(GMT+07:00)	Bangkok, Hanoi, Jakarta (GMT+07:00) Krasnoyarsk
(GMT+08:00)	Beijing, Chongqing, Hongkong, Urumqi
(GMT+08:00)	Taipei
(GMT+08:00)	Irkutsk, Ulaan Bataar (GMT+08:00) Kuala Lumpur, Singapore (GMT+08:00) Perth
(GMT+09:00)	Osaka, Sapporo, Tokyo (GMT+09:00) Seoul
(GMT+09:00)	Yakutsk
(GMT+09:30)	Adelaide
(GMT+09:30)	Darwin
(GMT+10:00)	Brisbane
(GMT+10:00)	Canberra, Melbourne, Sydney
(GMT+10:00)	Guam, Port Moresby (GMT+10:00) Hobart
(GMT+10:00)	Vladivostok
(GMT+11:00)	Magadan, Solomon Is., New Caledonia
(GMT+12:00)	Auckland, Wellington (GMT+ 12:00) Fiji, Kamchatka, Marshall Is.
(GMT+13:00)	Nuku'alofa

D

Technical Specifications

Camera	
Sensor	1/3” SVGA progressive scan CMOS
Lens	Wide end: F=1.4, Diagonal 125.2°, horizontal 97.1°, vertical 71.1° Tele End: F=2.8, diagonal 31.6°, horizontal 25.3°, vertical 19.0° Focal length= 2.8 to 11 mm
Auto Iris type	DC drive
Camera Angle	Pan: ±175°; Tilt: 0 to 85°; Rotation: ±180°
Minimum illumination (low light sensitivity)	0.01 lux, F=1.2
Synchronization	Internal
Gamma Correction	0.45
White Balance	ATW/AWB (range: 3200 to 10000°K)
ICR Control	Auto
S/N Ratio	52dB (TYP) (Gamma, Aperture, AGC Off; 3D-DNR On)
DNR	Built-in 3D-DNR (3D digital noise reduction)
WDR	94 dB, Level 1 to Level 9
De-mist	Off, low, medium, high
AGC Control	Level 1 to Level 9
Backlight Compensation	On/off with selectable areas
Digital Zoom	4X
Auto Light Control	Level 1 to Level 8
Image Rotation:	Flip, Mirror, and 180° rotation
Image Setting	Manual tuning with saturation and sharpness
Video	
Video Compression	H.264 (ISO/IEC 14496-10) or MJPEG
Video Output	Via Ethernet port
Video Streams	Maximum of 3 video streams (2 x H.264, 1 x MJPEG)

Video Resolution and FPS (Frame per second):

	NTSC		PAL	
	Size	Max. FPS	Size	Max. FPS
QCIF	176 x 112	30	176 x 144	25
CIF	352 x 240	30	352 x 288	25
VGA	640 x 480	30	640 x 480	25
4CIF	704 x 480	30	704 x 576	25
Full D1	720 x 480	30	720 x 576	25
SVGA	800 x 600	30	800 x 600	25

Video Viewing	DynaStream™ supported for changing the video frame rate automatically 8 privacy mask areas provided Adjustable image size and quality Timestamp and text overlay Maximum of 10 simultaneous unicast connections
PTZ	Digital PTZ with 4X zoom

Audio	
Audio Input	1 line-in or mic-in with 2-pin terminal block connector
Audio Output	1 line-out with 2-pin terminal block connector
Network	
Protocols	TCP, UDP, HTTP, SMTP, FTP, Telnet, NTP, DNS, DHCP, UPnP, RTP, RTSP, ICMP, IGMPv3, QoS, SNMPv1/v2c/v3, DDNS, Modbus/TCP, 802.1X, SSH, HTTPS
Ethernet	1 10/100BaseT(X) Ethernet port, RJ45 connector
GPIO	
Digital Input	1, max. 8 mA “Low”: +13V to +30V “High”: -30V to +3V
Relay Output	1 (max. 24 VDC @ 1A)
LED Indicators	
Network	10 Mbps or 100 Mbps
Power	Power On/ Off
System	Indicates if the system booted properly or not
DIP Switch	For turning the LED light ON or Off
Local Storage	
SD Socket:	Standard SD socket (SDHC)
Power Requirement	
Input	VPort 26: 1, 12/24 VDC or 24 VAC with 2-pin terminal block connector VPort P26: 1, Power-over-Ethernet (IEEE802.3af)
Consumption	Max. 11.7 W
Physical Properties	
Housing	Metal, IP66 rated for rain and dust protection, vandal-resistant
Dimensions	Diameter: 149 mm (5.7 in) Height: 1w0 mm (4.7 in)
Weight	1.4 kg
Installation	Surface mounting, or outdoor mounting with accessories
Environmental Limits	
Operating Temperature	-40 to 50°C (-40 to 122°F)
Storage Temperature	-40 to 85°C (-40 to 185°F)
Ambient Relative Humidity	5 to 95% (non-condensing)
Standards and Certifications	
UL	UL 60950-1
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), Level 3 EN61000-4-3 (RS), Level 3 EN61000-4-4 (EFT), Level 3 EN61000-4-5 (Surge), Level 3 EN61000-4-6 (CS), Level 3 EN61000-4-8 EN61000-4-11
Shock	IEC60068-2-27
Freefall	IEC60068-2-32
Vibration	IEC60068-2-6
Vandal-resistant	EN 62262, IK10 level
Warranty	3 years

Alarm Features	
Intelligent Video: Camera tamper (Pending)	
Video motion detection with sensitivity tuning	
Video loss alarm	
Daily repeat timing schedule	
JPEG snapshots for pre/trigger/post alarm images	
Automatic transfer of stored images via email or FTP as event-triggered actions	
HTTP event servers and CGI events for setting customized alarm actions	
24 MB pre-alarm video buffer for JPEG snapshot images	
Security	
User level password protection	
IP address filtering	
802.1X authentication	
HTTPS, SSH encryption	
Minimum Viewing System Requirements	
Pentium 4, 2.4 GHz	
512 MB of memory	
Windows XP/2000 with SP4 or above	
Internet Explorer 6.x or above	
DirectX 9.0c or above	
Software Development Kit	
VPort SDK PLUS	Includes CGI commands, ActiveX Control, and API library for customized applications or system integration for third-party developers (the latest version of SDK is vailable for download from Moxa's website).
Standard	ONVIF