

Moxa VPort 56-2MP Rugged IP Camera User's Manual

Second Edition, September 2014

www.moxa.com/product

MOXA[®]

© 2014 Moxa Inc. All rights reserved.

Moxa VPort 56-2MP Rugged IP Camera User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

© 2014 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

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 Europe

Tel: +49-89-3 70 03 99-0

Fax: +49-89-3 70 03 99-99

Moxa China (Shanghai office)

Toll-free: 800-820-5036

Tel: +86-21-5258-9955

Fax: +86-21-5258-5505

Moxa Asia-Pacific

Tel: +886-2-8919-1230

Fax: +886-2-8919-1231

Before Getting Started

Before using your VPort 56-2MP, please pay close attention to the following instructions:

- ❑ After opening the VPort 56-2MP 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 a variety of 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 56-2MP Web-based Manager**.

Important Note

- ❑ Surveillance devices may be prohibited by law in your country. Since the 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	1-1
Overview	1-2
Package Checklist	1-2
Product Features	1-3
Typical Applications	1-4
Product Description	1-4
2. Getting Started	2-1
Before Getting Started	2-2
First-Time Installation and Configuration	2-2
Software Installation	2-2
Wiring Requirements	2-4
3. Accessing the VPort's Web-based Manager	3-1
Functions Featured on the VPort's Web Homepage	3-2
VPort's Information	3-2
IP Camera Name	3-2
Camera Image View	3-2
Client Settings	3-3
System Configuration	3-4
Video Information	3-4
4. System Configuration	4-1
System Configuration by Web Console	4-2
System	4-3
General Settings	4-3
Account Privileges	4-4
Local Storage	4-5
System Log History	4-6
System Parameters	4-7
Firmware Upgrade	4-7
Reset to Factory Default	4-8
Reboot	4-8
Network	4-9
General Network Settings	4-9
SMTP Server and Email Account Settings	4-14
FTP Server Settings	4-15
Dynamic DNS	4-15
Universal PnP	4-16
QoS (ToS)	4-16
Multicast	4-17
Configuring Multicast Settings	4-18
HTTP Event Server	4-19
Accessible IP List	4-20
SNMP	4-21
Configuring SNMP Settings	4-21
Modbus/TCP	4-23
IEEE 802.1X	4-23
Telnet	4-24
LLDP	4-24
Video	4-24
Image Settings	4-24
Camera Setting	4-26
ROI (Region of Interest)	4-28
Privacy Mask	4-29
Camera Modulation	4-29
Video Performance	4-30
Audio	4-32
PTZ	4-32
Digital Zoom	4-32
PT Scanner	4-33
Camera Control	4-33
Focus	4-34
DynaStream™	4-35
Basic	4-35
Conditions	4-36

Alarm	4-36
System Alarm.....	4-36
Basic.....	4-37
Schedule.....	4-39
Event Alarm	4-40
Video Motion Detection	4-40
CGI Event	4-42
Sequential Snapshot.....	4-43
Digital Input.....	4-43

A. Frequently Asked Questions.....	A-1
B. Modbus Address Table	B-1
C. Time Zone Table.....	C-1
D. Technical Specifications	D-1

1

Introduction

The VPort 56-2MP is a rugged Full HD resolution (1080P) box type IP zoom 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 56-2MP 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 Applications**
- ❑ **Product Description**

Overview

Rugged Design

The VPort 56-2MP series is the world's first rugged IP camera that can withstand environmental temperatures ranging from -40 to 75°C without cooling fan. It is an industrial-grade, H.264 box-type IP camera with Full HD resolution (1920 x 1080), to enhance surveillance system efficiency while delivering state-of-the-art video quality. Optional housing and PT scanner accessories are available for indoor and outdoor installation.

Superb Video Quality

The VPort 56-2MP is equipped with 10x optical zoom and a 16x digital zoom module, with a built-in removable IR-cut filter and automatic color mode switching, the VPort 56-2MP Series is suitable for day-and-night use. Highly-tuned ROI (Region of Interest), and 3DNR (3D Digital Noise Reduction) functions enable the VPort 56-2MP series to produce exceptionally clear images.

Convenient Installation

The VPort 56-2MP series is designed for indoor and outdoor applications that require operational reliability. It is a unique and competitive camera in the IP CCTV market, with features such as high EMI/surge protection, optional IP66 housing for rain/dust protection, and -40 to 75°C operation without requiring a heater or cooling fan. This camera is available with PoE+ (Power over Ethernet, 802.3at) or with wired power input supporting 12/24 VDC or 24 VAC.

High Video Performance and Network Security

The VPort 56-2MP series can encode analog video into both H.264 and MJPEG video streams and can transmit up to 3 independent video streams (2 in H.264, and 1 in MJPEG) simultaneously. Advanced video encoding technology enables the camera to support up to 30 FPS for each of the H.264 and MJPEG streams. Advanced network security functions, such as 802.1x and SSL/SSH, are also provided to prevent unauthorized access or data hijacking, a critical feature for many surveillance applications.



Package Checklist

Moxa's VPort 56-2MP Series is shipped with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

- 1 × VPort 56-2MP (one of following models)

Standard model	Description
VPort 56-2MP-CAM10X	Full HD zoom IP camera, RJ45 Ethernet port, 12/24 VDC or 24 VAC or PoE, 0 to 60°C
VPort 56-2MP-CAM10X-T	Full HD zoom IP camera, RJ45 Ethernet port, 12/24 VDC or 24 VAC or PoE, -40 to 75°C
VPort 56-2MP-CAM10X -S-SC	Full HD zoom IP camera, single-mode fiber Ethernet port, 12/24 VDC or 24 VAC, 0 to 60°C
VPort 56-2MP-CAM10X-S-SC-T	Full HD zoom IP camera, single-mode fiber Ethernet port, 12/24 VDC or 24 VAC, -40 to 75°C

- Terminal block accessory package

3-pin terminal block for power input	9-pin terminal block for RS-485 DX+ and DX-
	

- Quick installation guide

- Documentation and software CD (includes User's Manual, Quick Installation Guide, and VPort Utility)
- Warranty card

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

NOTE Check the model name on the VPort's side label to determine if the model name is correct for your order.

NOTE This product must be installed in compliance with your local laws and regulations.

Product Features

- **Sensor:** 1/2.5" Full HD progressive scan CMOS
- **Lens:** 6.3 to 63 mm auto focus zoom lens
- **Illumination (low light sensitivity):**
 - Color: 0.2 lux at F1.8
 - B/W: 0.05 lux at F1.8
- **White Balance:** ATW/AWB
- **Auto Electronic Shutter:** On/Off
- **S/N Ratio:** More than 50 dB (AGC OFF)
- **ICR Control:** Auto (light sensor control) or DI control
- **DNR:** Built-in 3DNR
- **AGC Control:** On/Off
- **Auto Exposure:** On/Off
- **Image Rotation:** Flip, Mirror, and 180° rotation
- **Image Setting:** Manual tuning and sharpness
- **Video Compression:** H.264 (ISO/IEC 14496-10) or MJPEG
- **Video Outputs:** Ethernet
- **Video Streams:** Up to 3 video streams (2 x H.264 and 1 x MJPEG)
 - Stream 1: H.264, 1920 x 1080 resolution (max.)
 - Stream 2: H.264, 1280 x 720 resolution (max.)
 - Stream 3: MJPEG, 720 x 480 resolution (max.)
- **Video Motion Detection:** 3 independently configurable motion areas
- **Scheduling:** Daily repeat timing schedule
- **Imaging:** JPEG snapshots for pre/trigger/post alarm images
- **Video Recording:** Event recording, stored on the SD card
- **Email/FTP Messaging:** Automatic transfer of stored images via email or FTP when alerted
- **Custom Alarms:** HTTP event servers for setting customized alarm actions
- **Pre-alarm Buffer:** 84 MB video buffer for JPEG snapshot images
- **Advanced Software Feature:**
 - DynaStream™ support for automatic adjustment of frame rate
 - 8 privacy mask areas provided
 - ROI (Region of Interest) configuration for up to 3 areas
- **Safety:** UL 60950-1, EN 50121-4, NEMA TS2
- **EMI:** FCC Part 15, CISPR (EN 55022) class A
- **EMS:** EN 61000-4-2 (ESD), Level 3 EN 61000-4-3 (RS), Level 3 EN 61000-4-4 (EFT), Level 3 EN 61000-4-5 (Surge), Level 3 EN 61000-4-6 (CS), Level 3 EN 61000-4-8, EN 61000-4-11
- **Shock:** IEC 60068-2-27
- **Freefall:** IEC 60068-2-32

- **Vibration:** IEC 60068-2-6
- **Warranty:** 3-year warranty (not including moving parts)

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 For moving parts, please check Moxa's warranty policy online at www.moxa.com/warranty

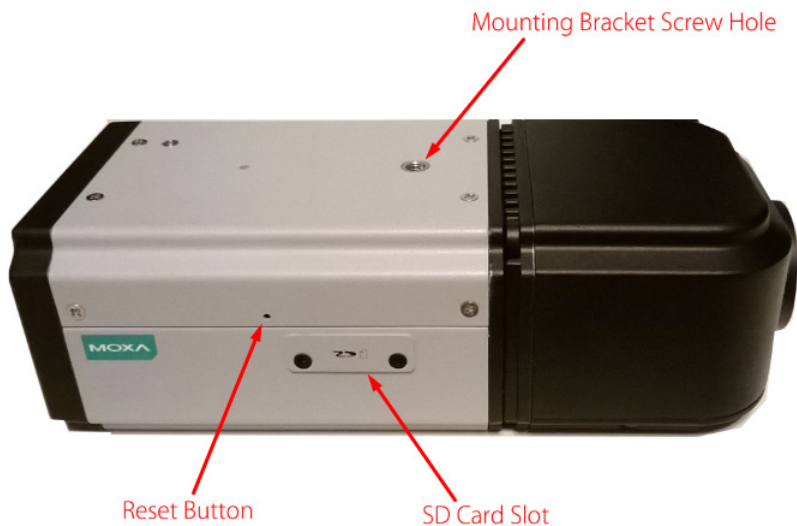
Typical Applications

With the industrial grade design and specifications, the VPort 56-2MP is suitable for both mission critical applications and general purpose surveillance systems, including the following:

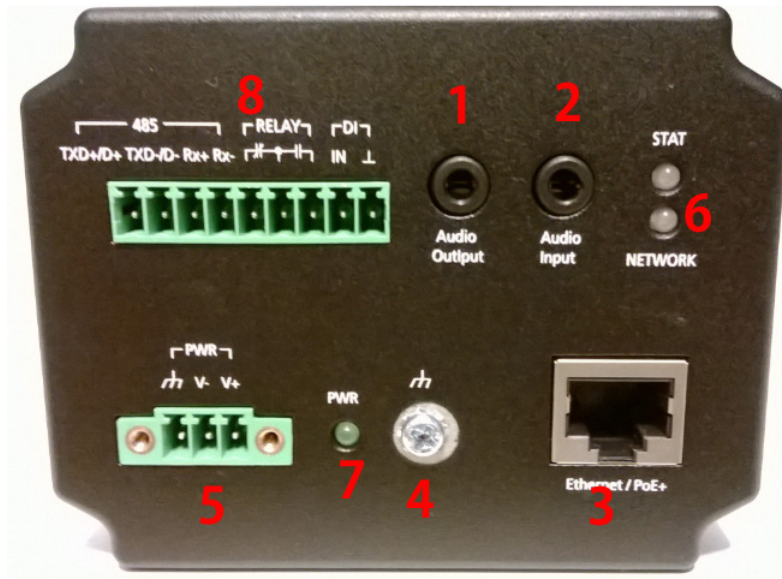
- **ITS (Intelligent Transportation System)**
- **City surveillance**
- **Railway wayside surveillance**
- **Railway station surveillance**
- **Industrial automation surveillance**
- **Oil & Gas facility surveillance**
- **Mining facility surveillance**

Product Description

Top View



- **SD Card Slot:** You can remove the SD card slot cover and insert an SD card for disconnection/event local storage.
- **Mounting Bracket Screw Hole:** Screw holes for fastening the camera to the protective housing.
- **Reset Button:** Use a pointed object to push in the reset button. Press and release to reboot, or press and hold until the system reboots to load factory defaults.

Back Panel View

1. Phone jack for audio output.
2. Phone jack for audio input.
3. RJ45 port for PoE/non-PoE connection
4. Ground screw for connecting the grounding wire
5. 3-pin terminal block for the power input
6. LED indicator to show network and system status. Green indicates normal operation.
7. LED indicator to show power status. Green indicates normal operation.
8. 9-pin terminal block for RS-485 and DI and relay

NOTE The VPort 56-2MP can be powered by a 12-32 VDC or 18-30 VAC power input, or Power over Ethernet (PoE+, 802.3at). For power redundancy, use DC or AC power together with PoE.

2

Getting Started

This chapter includes information about how to install a VPort 56-2MP IP camera.

The following topics are covered in this chapter:

- **Before Getting Started**
- **First-Time Installation and Configuration**
 - Software Installation
- **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, which allows making changes to the IP camera’s configuration and obtaining general access. Administrators should read this part of the manual carefully, especially during installation.

First-Time Installation and Configuration

Software Installation


Step 1: Configure the VPort 56-2MP’s IP address.

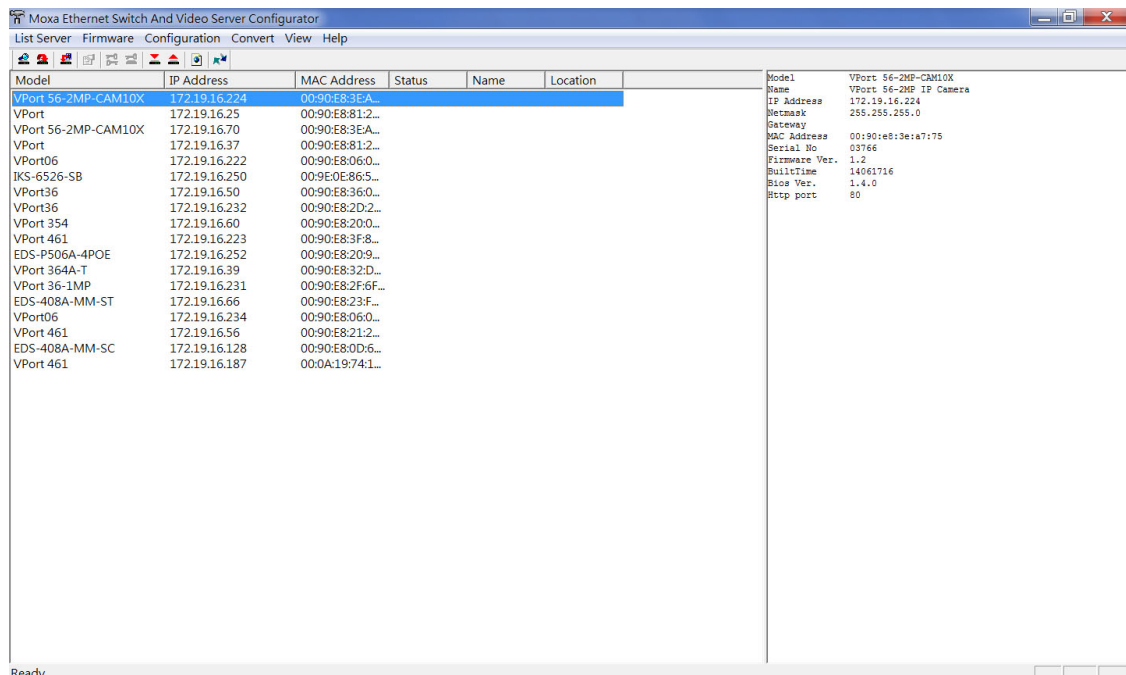
When the VPort 56-2MP is first powered on, the POST (Power On Self Test) will run for a few moments (about 30 seconds). The network environment determines how the IP address is assigned.

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 Configurator Utility (edscfgui.exe)

1. Run the **edscfgui.exe** program to search for the VPort. After the utility’s window opens, you may also click on the **Search** button  to initiate a search.
2. When the search has been completed, the Model Name, MAC address, IP address, serial port, and HTTP port of the VPort will be listed in the utility’s window.



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

Non DHCP Server Network Environment

If your VPort 56-2MP 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 56-2MP 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 then navigate to the **System Configuration** → **Network** → **General** page to configure the IP address and other network settings. Check the **Use fixed IP address** to ensure that the IP address you assign is not deleted each time the VPort is restarted.

Step 2: Access the VPort 56-2MP'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 ActiveX Control component on your PC or notebook. Click **Yes** to install this plug-in to enable the IE web browser for viewing video images.



NOTE For Windows XP SP2 or above operating systems, 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 unlock the ActiveX control blocked function or disable the security configuration to enable the installation of the VPort's ActiveX Control component.

Step 4: Access the homepage of VPort 56-2MP's web-based manager.

After installing the ActiveX Control component, the homepage of the VPort 56-2MP's web-based manager will appear. Check the following items to make sure the system was installed properly:

1. Video Images
2. Video Information



Step 5: Access the VPort's system configuration.

Click on **System Configuration** to access the overview of the system configuration to change the configuration. **Model Name**, **Server Name**, **IP Address**, **MAC Address**, and **Firmware Version** appear in the green bar near the top of the page. Use this information to check the system information and installation.

For details of each configuration, check the User's Manual on the software CD.

Category	Item	Description and Content
System	General	Setting Host Name and Date/Time
	Account	Administrator, User and Demo Account Privileges Management
	System Log	System Log and operation information
	System Parameter	System parameters information and Import/Export function
	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 DDNS
	Universal PnP	Enable UPnP function
	ToS	Configure ToS(Type of Service)
	Multicast	Set up Multicast (IGMP) Streaming
	HTTP Event Server	Set up the HTTP Event Server to send the event alarm action
	Accessible IP	Set up a list to control the access permission of clients by checking their IP address
	SNMP	Configure the SNMP settings
	Modbus/TCP	Enable Modbus/TCP function
	Dot1X	Configure 802.1X
	Telnet	Configure Telnet
Video	LLDP	Configure LLDP
	Image Settings	Configure the information of video image
	Camera Setting	Configure the attributes of video image
	ROI	Configure the ROI(region of interest) settings

Wiring Requirements



SAFETY FIRST

- Be sure to disconnect the power cord before installing and/or wiring your Moxa VPort 56-2MP.
- 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 separated.
- We strongly advise labeling the wiring to all devices in the system.

Accessing the VPort's Web-based Manager

This chapter includes information about how to access the VPort 56-2MP 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
- Client Settings
- System Configuration
- Video Information

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. We strongly recommend using IE 8.0 (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, firmware version, and the display status of the LEDs located on the VPort's front panel.

NOTE The VPort LEDs shown on the VPort's web homepage are updated every 10 seconds.

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.

Client Settings

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

1. **Encoder standard:** Shows the encoding algorithm currently being used. VPort 56-2MP features 2 built-in encode engine to generate a maximum of 3 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:** Enables the multicast video stream to be sent in RTSP control, which means the multicast video stream will be sent only if it receives the client's request.
 - **Push:** Enables 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 stream 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**.

Client Setting

IP Camera

Receiving Stream

Stream 1: H.264 Stream 2: MJPEG ▼

Media Option

Video/Audio Video Only Audio Only

Protocol Option

Multicast RTSP ▼ Unicast TCP ▼

Network Interface 172.26.4.51 ▼

Save

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: 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.

You can open the PTZ control panel from the IP camera home page by clicking "Show PTZ Control Panel." The VPort 56-2MP series supports native optical zoom and digital zoom functions, which can be operated from this panel.

System Configuration

After installing the hardware, the next step is to configure the VPort 56-2MP's settings. The web console can be used for this configuration.

The following topics are covered in this chapter:

□ **System Configuration by Web Console**

- System
- Network
- Video
- Audio
- PTZ
- Focus
- DynaStream™
- 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, Video, PTZ, D**, 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 to restart the 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
	Universal PnP	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
DynaStream	Basic	Set up the video frame rate change once an alarm or event is triggered
	Conditions	Set up the event/alarm to trigger Dynastream, and the behavior after being triggered
Video	Image Settings	Configure the attributes of the video image
	Image Tuning	Configure the attributes of the camera
	ROI	Configure the ROI (region of interest) settings
	Privacy Mask	Configure the Privacy Mask settings
	Camera Modulation	Select the camera's modulation (NTSC or PAL)
	Video Performance	Set up the Encode Standard (MJPEG or MPEG4), Size (Resolution), FPS, and Video Quality
Event Alarm	Basic	General event alarm settings
	Schedule	Set up the Alarm schedule
	Motion Detection	Configure the motion detection alarm
	Digital Input	Configure the Digital Input Alarm
	CGI Event	Set up the CGI event alarm
Camera Tamper	Configure the Camera Tamper event Alarm	

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

System Configuration

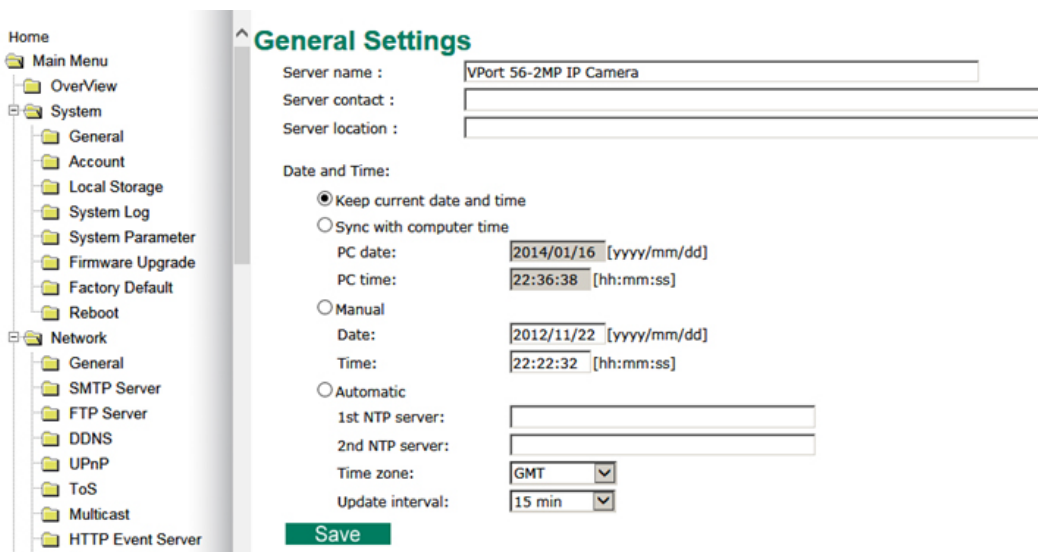
Welcome to the System Configuration pages. A brief description of each configuration group is given below. Click on a plus sign in the left pane to expand a group, and then click on the name of the page you would like to open.

Category	Item	Description and Content	
System	General	Setting Host Name and Date/Time	
	Account	Administrator, User and Demo Account Privileges Management	
	System Log	System Log and operation information	
	System Parameter	System parameters information and Import/Export function	
	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 DDNS	
	Universal PnP	Enable UPnP function	
	ToS	Configure ToS(Type of Service)	
	Multicast	Set up Multicast (IGMP) Streaming	
	HTTP Event Server	Set up the HTTP Event Server to send the event alarm action	
	Accessible IP	Set up a list to control the access permission of clients by checking their IP address	
	SNMP	Configure the SNMP settings	
	Modbus/TCP	Enable Modbus/TCP function	
	Dot1X	Configure 802.1X	
	Telnet	Configure Telnet	
LLDP	Configure LLDP		
Video	Image Settings	Configure the information of video image	
	Camera Setting	Configure the attributes of video image	
	ROI	Configure the ROI(region of interest) settings	
	Privacy Mask	Configure the Privacy Mask settings	
	Camera Modulation	Select the camera's modulation (NTSC or PAL)	
Video Performance	Set up the Encode Standard(MJPEG or H.264), Size (Resolution), FPS and Video Quality		
Audio	Audio Setting	Configure the Audio settings	
PTZ	Zoom Control	Configure the Zoom settings	
	PT Scanner	Configure the PT Scanner settings	
Focus	Focus Setting	Configure the Focus settings	
DynaStream	Basic	Configure the DynaStream settings	
	Conditions	Configure the DynaStream trigger conditions settings	
Alarm	System	Configure the System Alarm	
	Basic Setting	General settings of event alarm	
	Schedule	Set up the Alarm schedule	
	Event Alarm	Motion Detection	Configure the Motion Detection Alarm
		CGI Event	Configure the CGI event Alarm
		Sequential Snapshot	Configure the Sequential Snapshot
	Digital Input	Configure the Digital Input event Alarm	

System

General Settings

On the **General Settings** page, administrators can set up the IP camera **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 56-2MP IP camera

Server Contact

Setting	Description	Default
Max. 40 characters	Edit the responsible operator for this camera server	Blank

Server Location

Setting	Description	Default
Max. 40 characters	Edit the location of this camera server	Blank

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.

There are 2 NTP servers that can be set up as a backup, and the update interval can be configured from a minimum of 15 minutes to one month.

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

Account Privileges

Different account privileges are available for different purposes.

Account Privileges

Admin Password

Admin Password:

Confirm Password:

Note: Admin's password must be blank or 8 to 15 characters. If leave admin password blank will disable user authentication.

User's Privileges

No.	User Name	Password
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Admin password

Setting	Description	Default
Admin Password (max. 14 characters)	The administrator can type the new password in this box.	Default admin password is "admin"
Confirm Password (max. 14 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.	

NOTE The FPS of the video stream will be reduced as more and more users access the same VPort. Currently, the VPort 56-2MP is only allowed to send 10 unicast video streams. For this reason, you should limit the number of users simultaneously accessing a VPort 56-2MP to prevent performance problems.

Local Storage

The VPort 56-2MP supports an SD card slot (SDHC interface) for recording video when an event or alarm occurs. The administrator can download these recorded videos via FTP, or directly copy the files from the SD card with a card reader.

Local Storage Setting

This VPort supports local storage function for recording the video once there is an event/alarm. Users can download the recorded video files via FTP access.

Local Video Recording Setting

Enable video recording once there is an event/alarm.

Record Stream

Stream2: H.264 Stream2: MJPEG

FTP Server Daemon

Enable FTP Server Daemon

Server Port 21

SD Card

Reboot the system once the mounting of SD card is failed

Save

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

Record Stream

Setting	Description	Default
Stream 2: H.264 or Stream 2: MJPEG	Select the H.264 or MJPEG of stream 2 for the 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. Videos last 10 seconds, and are saved as AVI files, which can be played back on popular media players.

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

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.

System Log History

Index	Time	Type	Description
0001	Wed Nov 11 10:35:56 2009	FTP	Connect to Server 192.168.127.9:21 Failed
0002	Wed Nov 11 10:35:57 2009	FTP	Connect to Server 192.168.127.9:21 Failed
0003	Wed Nov 11 10:35:58 2009	FTP	Connect to Server 192.168.127.9:21 Failed
0004	Wed Nov 11 10:35:59 2009	FTP	Connect to Server 192.168.127.9:21 Failed
0005	Wed Nov 11 10:36:00 2009	FTP	Connect to Server 192.168.127.9:21 Failed
0006	Wed Nov 11 10:36:01 2009	FTP	Connect to Server 192.168.127.9:21 Failed
0007	Wed Nov 11 10:36:02 2009	FTP	Connect to Server 192.168.127.9:21 Failed
0008	Wed Nov 11 10:36:03 2009	FTP	Connect to Server 192.168.127.9:21 Failed
0009	Wed Nov 11 10:36:04 2009	FTP	Connect to Server 192.168.127.9:21 Failed
0010	Wed Nov 11 10:36:05 2009	FTP	Connect to Server 192.168.127.9:21 Failed
0011	Wed Nov 11 10:36:06 2009	FTP	Connect to Server 192.168.127.9:21 Failed
0012	Wed Nov 11 10:36:07 2009	FTP	Connect to Server 192.168.127.9:21 Failed

Send to system log Server

Syslog Server 1

Port Destination

Syslog Server 2

Port Destination

Send to system log server

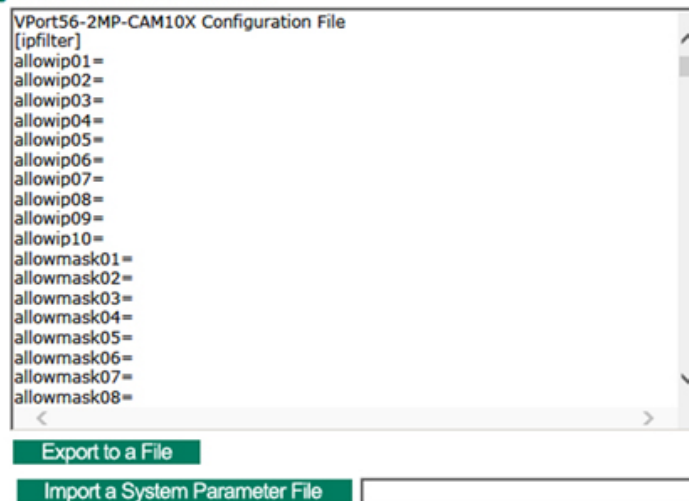
Setting	Description	Default
Send to system log server	Enables sending the system log to the log sever.	Disable
Syslog Sever 1	The address of the first system log server.	Blank
Port Destination	The port number of the first system log server.	514
Syslog Sever 2	The address of the second system log server.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

NOTE A maximum of 500 lines is displayed in the log. However, the log actually stores up to 1000 entries, which can be exported by the administrator 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.

System Parameters



NOTE The system parameter import/export functions allow the administrator to back up 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

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 56-2MP, 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 a 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.

Reset to Factory Default

Reset to Factory Default will restart the system and delete all the changes that have been made to the configuration. Are you sure you want to reset to factory default?

OK

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.

Device Reboot

This device will reboot for restarting system. Are you sure you want to reboot?

OK

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.

General Network Settings

Access Method

DHCP
 DHCP + Auto configure
 Use fixed IP address

General Settings

IP address	<input type="text" value="192.168.127.75"/>
Subnet mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.127.254"/>
Primary DNS	<input type="text" value="192.168.127.254"/>
Secondary DNS	<input type="text" value="192.168.127.254"/>
DHCP Client ID	<input type="text"/>
DHCP Server ID	<input type="text"/>

HTTP

HTTP port	<input type="text" value="80"/>
HTTPS port	<input type="text" value="443"/>
HTTP mode	<input type="text" value="HTTP Only"/>

RTSP Streaming

RTSP port	<input type="text" value="554"/>
-----------	----------------------------------

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 a fixed IP address	Use the IP address assigned by the administrator.	

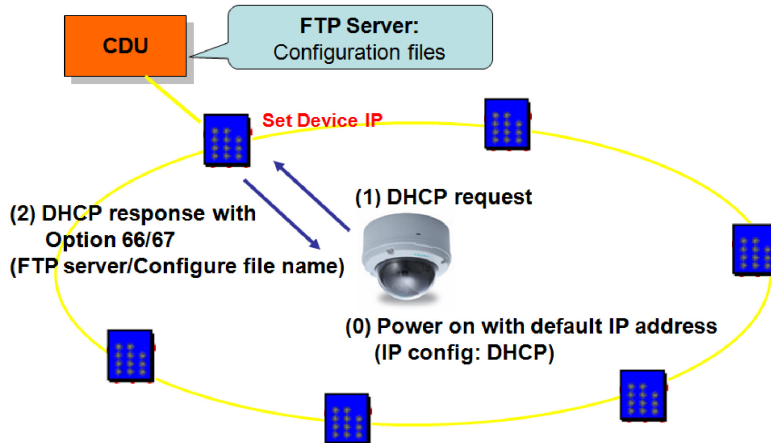
NOTE We strongly recommend that the administrator assign a fixed IP address to the VPort, since all of the functions and applications provided by the VPort are active when the VPort is connected to the network. Use DHCP to determine if the VPort's IP address may change when then network environment changes,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

Auto Configuration

Since configuring a large number of devices one by one can be extremely time-consuming, 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 effort in mass device installation. Follow the steps below to use the auto-configuration function via Opt 66/67.

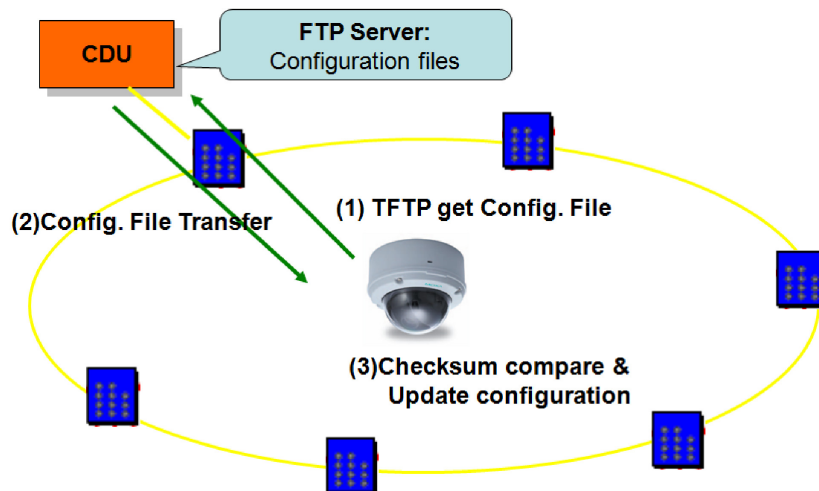
Step 1:

When the VPort 56-2MP's auto-configuration function is enabled, it will ask for the IP address from DHCP server, and the path of the TFTP server and configuration file.



Step 2:

Once the VPort 56-2MP completes the IP settings, it will acquire the configuration file from the TFTP server, and check if this configuration file is correct or not.



NOTE

- For the auto-configuration function to work, 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	HTTP mode Select the HTTP transmission mode: HTTP Only or HTTP + HTTPS	HTTP Only

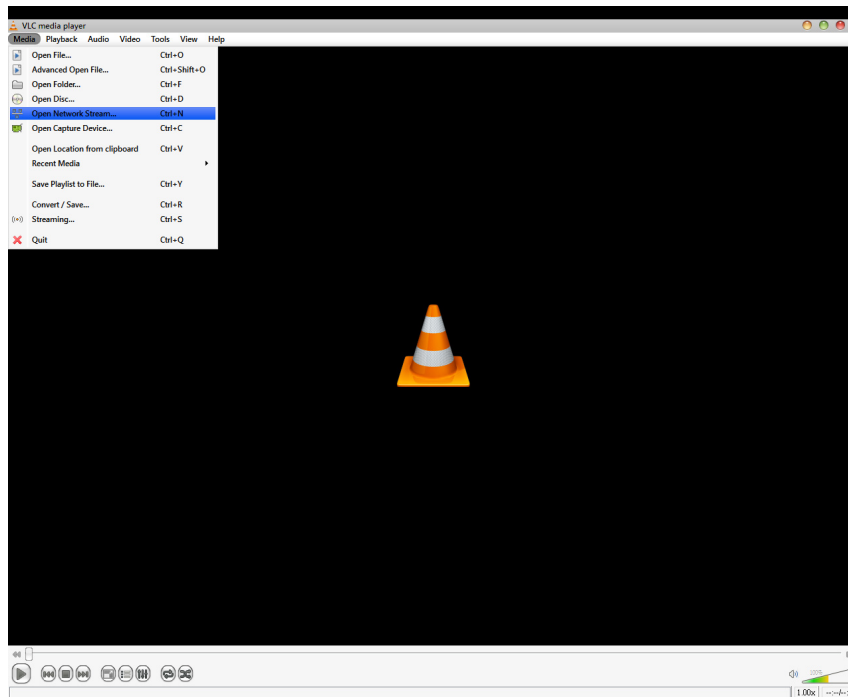
RTSP Streaming

The VPort 56-2MP 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 56-2MP 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.

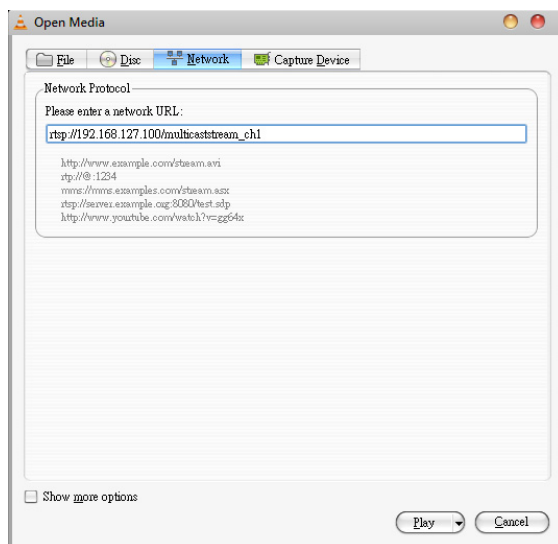
Setting	Description	Default
RTSP Port	An RTSP port is similar to an HTTP port, which can enable the connection of video/audio streams by RTSP.	554

The VLC media player is used here to illustrate an RTSP streaming application:

Step 1: Start VLC Player and select **Media - Open network streaming**



- Step 2:** When the following pop-up window appears, type the URL in the input box. E.g., type **rtsp://<VPort 56-2MP's IP address>[:<RTSP Port>]/udpstream_ch1_stream< 1 or 2>** or **rtsp://<VPort 56-2MP's IP address>[:<RTSP Port>]/multicaststream_ch1_stream<1 or 2>**
RTSP Port: 554 is the default; click **OK** to connect to the VPort 56-2MP.



- Step 3:** Wait a few seconds for VLC Player to establish the connection.

Step 4: After the connection has been established, the VPort 56-2MP's video will appear in the VLC Player display window.



NOTE The video performance of the VPort 56-2MP may vary when using other media players. For example, you will notice a greater delay when viewing the VPort 56-2MP's video from the VLC player compared to viewing it directly from the VPort 56-2MP's built-in web server. In addition, viewing the VPort 56-2MP's video from the VLC player through a router or Internet gateway could result in a broken connection.

NOTE For the time being, the VPort 56-2MP'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 56-2MP'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.

SMTP Server and Email Account Settings

1st SMTP Server and Sender Email

1st SMTP (mail) server	<input type="text"/>
1st SMTP account name	<input type="text"/>
1st SMTP password	<input type="text"/>
1st Sender's email address	<input type="text"/>

2nd SMTP Server and Sender Email

2nd SMTP (mail) server	<input type="text"/>
2nd SMTP account name	<input type="text"/>
2nd SMTP password	<input type="text"/>
2nd Sender's email address	<input type="text"/>

Note: There are 2 SMTP servers and sender Email accounts for sending system information and alarms. enable the email transmitting system.

Recipient's Email

1st Recipient's Email Address:	<input type="text"/>
2nd Recipient's Email Address:	<input type="text"/>

Note: There are 2 recipient email accounts for receiving system information and alarms.

Save

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.

FTP Server Settings

1st FTP server

1st FTP server

1st FTP server port

1st FTP user name

1st FTP password

1st FTP remote folder

1st FTP passive mode

2nd FTP server

2nd FTP server

2nd FTP server port

2nd FTP user name

2nd FTP password

2nd FTP remote folder

2nd FTP passive mode

Note: There are 2 FTP servers for sending alarms. At least one of them should be set up correctly to enable the FTP s

Save

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.

Dynamic DNS

The Dynamic DNS function allows your VPort to get a domain name linked to a changeable IP address w IP address if you want to remote access this VPort from Internet.

Enable DDNS

Provider

Host name

Username/E-mail

Password/Key

Note: If you don't have a DDNS account, please follow the application procedure on the website listed above.

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.

Universal PnP

UPnP (Universal Plug & Play) is a function that provides compatibility among networking equipment, software and peripherals. By enabling this function, you can find this VPort directly from the operating system's network device list.

Enable UPnP

Note: Please make sure your OS or software supports UPnP first if you want to enable VPort's UPnP function.

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

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.

QoS(ToS)

Configure the QoS (ToS) to add the ToS (Type of Service) tag onto the video streaming data for transmitting this video stream with higher priority compared to other data.

Enable ToS

DSCP Value

Save

Setting	Description	Factory Default
Enable ToS	Enable 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.

Multicast

The VPort 56-2MP 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.

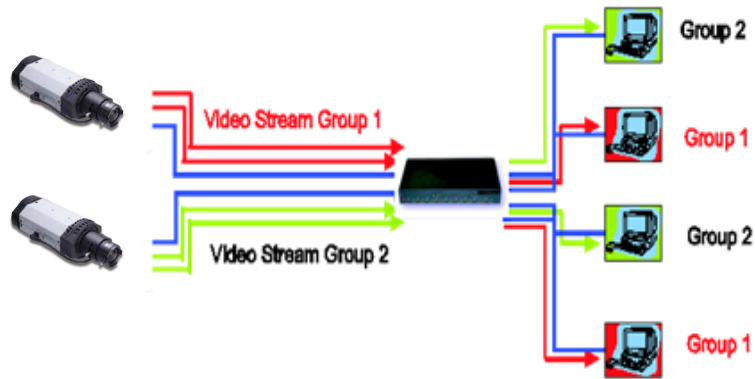
Benefits of Multicast

The benefits of using IP multicast are that it:

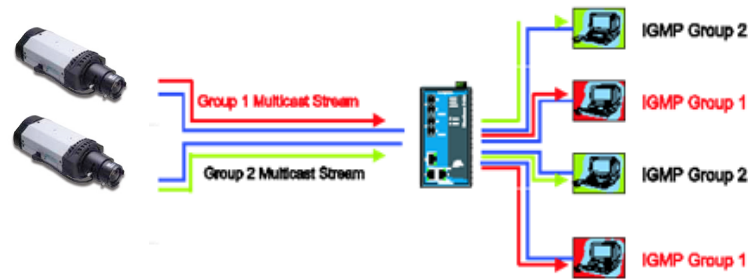
- Enables the simultaneous delivery of information to many receivers in the most efficient, logical way.
- Reduces the load on the source (for example, a server) because it does not need to produce multiple copies of the same data.
- Makes efficient use of network bandwidth and scales well as the number 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 56-2MP 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 EtherDevice™ series Industrial Ethernet Switch user’s manual.

Configuring Multicast Settings

Multicast Settings

Stream 1		Stream 2	
Multicast group address	<input type="text" value="239.127.0.100"/>	Multicast group address	<input type="text" value="239.127.0.100"/>
Multicast video port	<input type="text" value="5556"/>	Multicast video port	<input type="text" value="5560"/>
Multicast TTL	<input type="text" value="128"/>	Multicast TTL	<input type="text" value="128"/>
Continuous Multicast Push	<input type="checkbox"/> Enable	Continuous Multicast Push	<input type="checkbox"/> Enable
<input type="button" value="Save"/>			

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 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

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.

HTTP Event Servers

VPort can send the customized alarm actions and messages to the HTTP Event Servers capability for the users designing the customized alarm system.

Hostname
Server 1
 User name:
 Password:
Server 2
 User name:
 Password:
Server 3
 User name:
 Password:
Server 4
 User name:
 Password:

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 <Base64(username:password)>\r\n]
Host: <HTTP Server IP Address>\r\n
Connection: Keep-Alive\r\n
\r\n
    
```

Accessible IP List

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

Accessible IP List

Enable accessible IP list ("Disable" will allow all IPs to connect)

Index	IP	NetMask
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Save

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 56-2MP 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

SNMP Read/Write Settings

SNMP Versions	V1, V2c, V3
V1,V2c Read Community	public
V1,V2c Write/Read Community	public
V3 Admin Read/Write Auth. Mode	No-Auth
V3 Admin Read/Write Private Mode	<input type="checkbox"/> Key

Trap Settings

1st Trap Server IP/Name	
1st Trap Community	
2nd Trap Server IP/Name	
2nd Trap Community	

Private MIB information

Object ID enterprise.8691.8.4.15

Save

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: 8691.8.4.2. This number cannot be changed.

NOTE The MIB file is MOXA-VPORT16-MIB.mib (or.my). You can find it on the software CD or the download center of the Moxa website.

Modbus/TCP

Modbus is a serial communications protocol that 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.

ModBus/TCP

Modbus is a serial communications protocol for the industrial devices' communications with the SCADA/HMI system. With the Modbus/TCP protocol, the SCADA/ HMI system can directly communicate with VPort for acquiring the working status.

Enable ModBus/TCP

Save

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

IEEE 802.1X

IEEE 802.1X is a network security protocol for authenticating devices wishing to connect to a LAN or WLAN.

IEEE 802.1X

Enable 802.1X

EAP Method

Username

Password

EAP-MD5 ▼

- EAP-MD5
- EAP-PEAP/MSCHAPv2
- EAP-TLS

Save

Setting	Description	Default
Enable 802.1X	Enable/Disable 802.1X function	No
EAP Method	Choose Authentication method	EAP-MD5
Username	Set username	Blank
Password	Ser password	Blank

Telnet

Use this option to Enable/Disable the Telnet function.

Telnet

Enable Telnet

Save

LLDP

LLDP is a link layer protocol **used by network devices for advertising their identity.**

LLDP (IEEE 802.1AB)

Operating Mode
 Transmit interval second(s) (1 ~ 3600 secs)

Save

Setting	Description	Default
Operating Mode	Choose Disabled / Transmit only / Receive only / Transmit and Receive operating mode	Transmit and Receive
Transmit Interval	Set the interval between transmit	30

NOTE For Modbus address table, please refer to Modbus_Address_Define.pdf, which is located on the software CD. It can also be downloaded from Moxa’s website.

Video

Image Settings

Image Settings

Image Information

Description:

Image Appearance

Image Information:

Not Shown

Shown on the caption

Shown on the image

Save



Image Information Setting

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

Image Appearance Setting

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

Image Settings

Image Information

Description:

Image Appearance

Image Information:

Not Shown

Shown on the caption

Shown on the image

Position X: (0~400)

Position Y: (0~300)

Save



Position X and Position Y to designate image information display position in the video.

Camera Setting

There are detailed camera parameters that can be configured to create a better image quality, with settings dependent on the environment.

Camera Setting

Image Adjustments

Sharpness AWB

AGC Stabilizer

Flickerless Appearance

Digital Noise Reduction

2D Spatial noise filter
 3D noise filter

Mode Level

BLC

Enable Level : (Larger value increases brightness)

Day / Night

Day
 Night
 Light Sensor Switch lux level : Detect duration sec (1 ~ 60sec)
 DI Control

Trigger relay output when day/night mode switch
Relay status is : when day mode
Relay status is : when night mode

IRIS

Auto Level (0 (Dark) - 100 (Bright))
 Manual Stop (1 - 17)

Exposure Shutter

Shutter Speed :
Manual Sense Sensitivity :

Image View

Image Adjustment

Setting	Description	Default
Flickerless	Adjust sensor scan frequency to synchronize with environmental lighting frequency	Disable
Sharpness	Tune the image attribute to a value between -4 and + 4	0
Auto Gain Control (AGC)	The AGC function provides a clear image in low light conditions by controlling an amplifier that is used to boost the video signal when the light dims so as to increase the camera’s sensitivity. In some bright environments, the amplifier may be overloaded, which could distort the video signal. In this case, it is necessary to monitor the signal level with the AGC control circuit and AGC may need to be switched off.	Normal
Stabilizer	This function helps to stabilize a shaky video view	Disable
AWB (Auto White Balance)	In most conditions you should choose ATW, which allows the camera to automatically adjust the white balance. AWB is recommended when your camera is focused on a scene in which one color occupies most of the view. Take these steps to use AWB: <ol style="list-style-type: none"> 1. Focus the camera on a white color in an actual environment with normal lighting. 2. Select AWB and then press Save. 3. Move the camera back to the scene that will be monitored. 	ATW

Setting	Description	Default
Appearance	Normal: Normal view Mirror: Image will be displayed as in a mirror Flip: 180 degree rotation followed by a mirrored display 180 degree rotation: Image is rotated 180 degrees	Normal

Digital Noise Reduction

Setting	Description	Default
2D or 3D	Choose 2D or 3D noise filter	2D

BLC

Setting	Description	Default
Enable	Enable BLC function	Unchecked
Level	Select BLC level	L7

Day / Night

Setting	Description	Default
Day	Manually set the camera to day mode (color mode)	Checked
Night	Manually set the camera to night mode (monochrome mode)	Unchecked
Light Sensor	The camera light sensor will switch between day and night modes based on the ambient illumination level. Set duration (in sec.) to define how long the illumination level should persist before switching modes.	Unchecked
DI Control	Switch day/night when by DI <ul style="list-style-type: none"> High Low Switch: The camera will force a day/night switch whenever the DI status changes. Pull High: The camera will force a day/night switch whenever the DI status is high. Pull Low: The camera will force a day/night switch whenever the DI status is low. 	Unchecked
Trigger relay output when day/night mode switches	Triggers relay output when day/night mode switches; the relay status for day/night mode can be configured separately.	Unchecked

Exposure Shutter

Setting	Description	Default
Manual Sense Sensitivity	Select from the drop-down menu to enable the sense up function. Shutter speed can be selected once this function is on.	Off
Shutter Speed	Manually adjust shutter speed	Disable

Auto Iris

Setting	Description	Default
Enable	Enables the auto-iris function (Not for Hazardous Location)	Checked

ROI (Region of Interest)

When network bandwidth is limited, real-time HD video streams may be too large for the network to handle, and in that case the VPort 56-2MP will automatically allocate available bandwidth to those parts of the video that are of greater interest. For example, when focused on a factory entrance, the camera can allocate more bandwidth for the entryway, and allocate minimum bandwidth for a wall in the same scene.

ROI Settings

ROI (Region of Interest)

Enable ROI

(AV-UDP) 2000/01/01 05:48:55

Region 1 Priority Low

Region 2 Priority Low

Region 3 Priority Low

Save

ROI

Setting	Description	Default
Enable	Enable the ROI function	Off
Region 1/2/3	Assign priority to up to 3 different regions in the camera view.	unchecked
High/Medium/Low	High: The camera will reserve a majority of bandwidth for this part of the video. Medium: The camera will reserve moderate bandwidth for this part of the video. Low: The camera will reserve only minimum bandwidth for this part of the video.	Low

Privacy Mask

In some conditions, you may want to block part of the view so that your surveillance system won't include some private video information when displaying live video or video playback.

Privacy Mask Settings

Enable Privacy Mask

Privacy Mask

Mask 1

Enable

Set Show



Save

Privacy Mask

Setting	Description	Default
Enable	Enable the privacy mask function	Off
Mask 1/2/3	Enable up to 3 different privacy mask areas. Once enabled, you can drag the masked area directly into the camera scene.	1

NOTE Only use this function when you want to mask parts of the scene. You cannot recover masked video either when viewed live or during playback.

Camera Modulation

Choose camera modulation for your system for different resolutions and FPS parameters.

Camera Modulation

NTSC

PAL

Save

Camera Modulation

Setting	Description	Default
NTSC or PAL	Choose NTSC or PAL for your system	NTSC

Video Performance

The VPort 56-2MP can send a maximum of three simultaneous video streams: two H.264 and one MJPEG. In fact, the VPort 56-2MP has two encoder engines. The first encoder engine can generate one completely independent H.264 video stream, which means that 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 resolutions 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.

Encode Standard, Resolution (Size), Frame Rate and Quality

Streams	Codec Type	Resolution	Max FPS	Quality
<input checked="" type="checkbox"/> 1	H264	1920x1080	30	<input checked="" type="radio"/> Fixed quality (VBR) Good <input type="radio"/> Fixed bit rate(CBR) 4000 (400~12000)Kbps
<input checked="" type="checkbox"/> 2	H264	1280x720	30	<input checked="" type="radio"/> Fixed quality (VBR) Good <input type="radio"/> Fixed bit rate(CBR) 4000 (400~8000)Kbps
<input checked="" type="checkbox"/> 2	MJPEG	720x480	30	Fixed quality Good

Limit the maximum throughput of each connection in 20 (4~5000)kbits within 5 (1~1000)milliseconds

Save

Streams

Setting	Description	Default
Enable the video streams	Enables the VPort to send this video stream.	Enable stream 1/2: H.264 and stream 3: MJPEG

Codec Type

This codec type shows the codec of each video stream.

Resolution

The VPort 56-2MP supports 8 different resolutions: Full HD, 1MP, HD, SVGA, Full D1, 4CIF, VGA, CIF

Setting	Description	Default
Select the image size	7 image resolutions (size) are provided. The administrator can choose each option with NTSC or PAL modulation.	1920 x 1080 for stream1; 1280 x 720 for stream 2; 720 x 480 for stream 3

Resolution	NTSC	PAL
Full HD 1080P	1920 x 1080	1920 x 1080
HD 720P	1280 x 720	1280 x 720
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

NOTE 1920 x 1080 is only available in stream 1. The maximum resolution for stream 2 is HD resolution.

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 56-2MP 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.	4000Kbps
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

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.

NOTE Visit http://www.moxa.com/event/Net/2012/IP_CCTV_Calculator/index.htm to get a help for network bandwidth estimation of different resolution, FPS, video content

Audio

The VPort 56-2MP supports 1 audio input and 1 audio output, and 2-way audio. To use this function, connect an external audio device to the VPort 56-2MP.

Setting	Description	Default
audio	Enable audio function	unchecked

PTZ

The VPort 56-2MP comes with a zoom lens that enables users to zoom in on an image to observe finer details.

Digital Zoom

Press save when you are finished configuring the digital PTZ settings.

PT Scanner

The VPort 56-2MP series can be used with Videotec Ulisse Netcam PT scanner to form an industrial-grade PTZ solution. You can also configure the VPort 56-2MP's RS-485 interface to work with other PT scanners if needed. Use the following configuration for the Videotec Ulisse Netcam PT scanner:

- **RS485 Mode:** 2-wire
- **Control Mode:** Specific PTZ driver
- **Port Settings:** Baudrate 9600; data bits 8; stop bits 1; parity bit none
- **PTZ Camera Driver:** Pelco D

PT Scanner

RS485 Mode

2-wire 4-wire

Control Mode

Transparent PTZ Control
 Specific PTZ Driver

Port Settings

Baud rate (bps)

Data bits

Stop bits

Parity bit

PTZ Camera Driver

Select the camera driver:

[Remove Camera Driver](#)

[Set up Custom Commands](#)

[Set up Custom Camera](#)

[Upload a PTZ Camera Driver](#) [Browse](#)

Note: There are 24 custom commands for users to define PTZ camera actions (except for PAN, TILT, ZOOM, FOCUS and preset positions). To do this, users need to refer to the control protocols provided by the supplier of PTZ camera.

[Save](#)

Camera Control

The VPort supports PTZ (PAN/TILT/ZOOM) motorized camera control via an RS-232, RS-422, or RS-485 PTZ/COM port. Before setting up camera control, the administrator should first connect the PTZ camera to the VPort. (Refer to Chapter 2 for the PTZ port's wiring specifications.)

PTZ (Motorized) Camera Control

Camera Selection

Camera ID

Position Alias **Edit/Save**

Preset Position **Delete**

Go To Last Position **Set Home**

Save

Tilt Speed

Pan Speed

Zoom Speed

Camera ID

Camera ID Setting	Description	Default
Camera ID	Each PTZ camera has an ID to identify which PTZ camera is in the multi-drop connection. To connect to the PTZ camera, the VPort should first identify its ID.	1

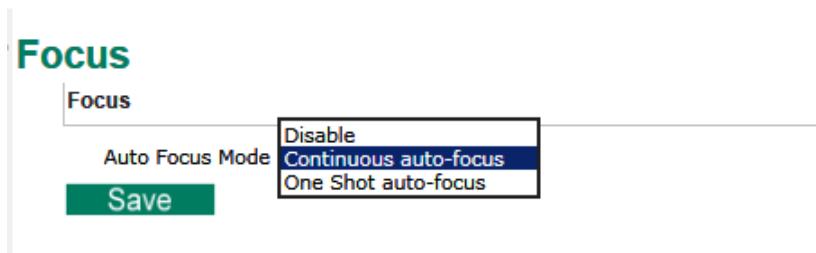
Setting Up a Preset Position

Administrators can use the **Preset Position** function to set up the behavior of the PTZ camera in advance, and then users with camera control privilege can move the camera’s lens to a preset position without the need to control the pan, tilt, and zoom buttons on the PTZ control panel.

Setting	Description	Default
Position Alias	Customized name of the preset position	blank
Preset Position	25 preset positions are available for the VPort.	01
Go to	The administrator can use “Go to” to select or test the preset position before the save.	Select
Last Position	This column shows the current preset position of this PTZ camera.	blank
Set Home	This button can decide the Home position of PTZ control (not all PTZ protocol support this function)	
TILT SPEED PAN SPEED ZOOM SPEED	These items are used to change the TILT, PAN, and ZOOM speeds.	8

Focus

The VPort 56-2MP’s zoom lens supports multiple focus modes, allowing users to choose the focus mode that best fits their application. The VPort 56-2MP will constantly perform auto-focus based on the latest scene if continuous auto-focus is selected. If one shot auto-focus is selected, then the VPort 56-2MP will only perform auto-focus when the focus button on the PTZ control panel is clicked.



Setting	Description	Default
Focus Mode	Select auto-focus mode	continuous auto-focus

DynaStream™

DynaStream™ 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 systems (as well as the MxNVR-MO4'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 switched 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 To enable the DynaStream function from CGI commands and Modbus TCP, refer to the CGI Commands User's Manual for VPort SDK PLUS.

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 frame 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.

DynaStream Basic Setting

This innovative Dynastream function is to change the video streams' frame rate automatically once an event/ alarm is happened (VPort's alarms or external events). This change can be from low to high frame rate to increase the smooth of the video streams, or from high to low frame rate to lower down the bandwidth consumption. The Live is to setup the current frame rate, and the Alarm is to setup the frame rate after being changed by an alarm/ event.

Stream	CodecType	Status	Max FPS	Resolution	Quality	Preview
Stream 1	H.264	Live	25	800x600	Fixed quality	<input type="button" value="Test"/>
		Alarm	25			



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 can 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 to facilitate automatic frame rate adjustment (e.g., from Live to Alarm status).

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

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

Alarm

System Alarm

In addition to the LED indicators, a network disconnect alarm is provided by the VPort 56-2MP for notifying system operators and the administrator. The video is stored on the SD card so that you can retrieve recorded images after the network connection is restored.

NOTE Refer to page 4-5 of this manual for detailed configuration instructions on recording when the network is disconnected.

Basic

On this page you can configure some general parameters of the VPort 56-2MP's alarm function, including alarm time interval, alarm snapshot, relay behavior, and more.

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 this number of 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 this number of 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 56-2MP supports a 84 MB memory buffer to record the pre-alarm MJPEG image up to 15 FPS. This function is to configure the frame rate per second of the MJPEG images being recorded.

Setting	Description	Default
Max. Frame Rate	Configure the maximum frames per second to be record before the alarm in 1, 3, 5, 10, 12, 15	10

NOTE The 84 MB pre-alarm buffer is for storing MJPEG image frames before the alarm. So, if the max. frame rate is set to 10, and the video size of each image is 30 KB, then 280 seconds of pre-alarm MJPEG images can be recorded . $((84000 \text{ KB} / 30 \text{ KB}) / 10 = 280)$

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 and **Override Relay 2 warning** setting boxes, and then click **Save**.

NOTE The relays will not be triggered when the **Override Relay 1 warning setting** and **Override Relay 2 warning setting** boxes are checked. Un-check these 2 boxes to ensure that the relays will trigger.

Relay Active Behavior

Three types of relay behavior can be configured when an event is triggered.

Relay Active Behavior

- Relay is in active continuously once an alarm is happened.
- Relay is in active for the period of alarm interval time once an alarm is happened.
- Relay is in active for the period of the alarm being triggered(DI trigger and lan port link-down).

Schedule

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

Event Type

Setting	Description	Default
Video Motion Detection, CGI Event, Sequential Snapshot, DI Event	Configure the schedule of each event type.	Video Motion Detection

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
<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> 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

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)	<ol style="list-style-type: none"> 1. VMD 1 2. VMD 2 3. VMD 3 	<ol style="list-style-type: none"> 1. Trigger Relay 2. Email 3. FTP 4. HTTP Event Server 5. Record on SD card
CGI Event	The CGI trigger message	<ol style="list-style-type: none"> 1. Trigger Relay 2. Email 3. FTP 4. HTTP Event Server 5. Record on SD card
Sequential Snapshot	Always triggered when this function is enabled	<ol style="list-style-type: none"> 1. Send snapshot via Email 2. Send snapshot via FTP
Digital Input	<ol style="list-style-type: none"> 1. High 2. Low 3. Rising 4. Falling 	<ol style="list-style-type: none"> 1. Trigger Relay 2. Email 3. FTP 4. HTTP Event Server 5. Record on SD card

Video 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.

VMD (Video Motion Detection)

- Enable VMD alarm
- Show alert on the image when VMD is triggered

Set up VMD Alarm

2006/05/31 17:15:50

Stream1 Stream2

Enabled	Window Name	Percent %
<input checked="" type="checkbox"/>	VMD1	80
<input checked="" type="checkbox"/>	VMD2	80
<input checked="" type="checkbox"/>	VMD3	80

Sensitive: 1

Save

Trigger Conditions and Actions

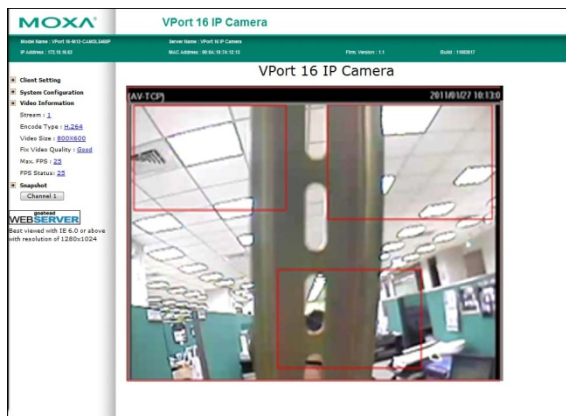
Trigger Condition	Trigger Action	HTTP Action Setting
VMD1	<input type="checkbox"/> Trigger Relay1 alarm <input type="checkbox"/> Send snapshot image via E-mail <input type="checkbox"/> Send snapshot image via FTP <input type="checkbox"/> Send message via HTTP Event Servers <input type="checkbox"/> Record video on SD card 5 Sec	<input type="checkbox"/> Server1 <input type="checkbox"/> Server2 <input type="checkbox"/> Server3 <input type="checkbox"/> Server4 <input type="text"/>
VMD2	<input type="checkbox"/> Trigger Relay1 alarm <input type="checkbox"/> Send snapshot image via E-mail <input type="checkbox"/> Send snapshot image via FTP <input type="checkbox"/> Send message via HTTP Event Servers <input type="checkbox"/> Record video on SD card 5 Sec	<input type="checkbox"/> Server1 <input type="checkbox"/> Server2 <input type="checkbox"/> Server3 <input type="checkbox"/> Server4 <input type="text"/>
VMD3	<input type="checkbox"/> Trigger Relay1 alarm <input type="checkbox"/> Send snapshot image via E-mail <input type="checkbox"/> Send snapshot image via FTP <input type="checkbox"/> Send message via HTTP Event Servers <input type="checkbox"/> Record video on SD card 5 Sec	<input type="checkbox"/> Server1 <input type="checkbox"/> Server2 <input type="checkbox"/> Server3 <input type="checkbox"/> Server4 <input type="text"/>

Note: HTTP Action Setting allows the VPort sending the customized alarm messages to the HTTP Event Server when the event is triggered. Please refer to URL syntax being defined in RFC 1738 and the customer-defined commands for writing this setting with 100 characters.

Save

Setting	Description	Default
Enable VMD alarm	Enable or disable the Video Motion Detection alarm	Disabled
Show alerts 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 indicates 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

Administrators can set triggers, such as Send snapshot image via E-mail, Send snapshot image via FTP, Send Message via HTTP Event servers, Save Sanpshot on Storage and Record video on SD card, for each VMD.

Setting	Description	Default
Trigger Relay 1 alarm	Once this VMD is triggered, the VPort will trigger relay 1. Note that relay behavior will follow the configuration in alarm basic setting page.	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 <input type="text"/> Sec	Once this VMD is triggered, the VPort will record the video on the SD card for a configured time period.	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

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

Enable CGI Event alarm

CGI Event Trigger Actions

Event Index	Trigger Action	HTTP Action Setting
Event 1	<input type="checkbox"/> Send snapshot image via E-mail <input type="checkbox"/> Send snapshot image via FTP <input type="checkbox"/> Send message via HTTP Event Servers <input type="checkbox"/> Save snapshot on Storage <input type="checkbox"/> Record video on SD card <input type="text"/> Sec.	<input type="checkbox"/> Server1 <input type="checkbox"/> Server2 <input type="checkbox"/> Server3 <input type="checkbox"/> Server4 <input type="text"/>
Event 2	<input type="checkbox"/> Send snapshot image via E-mail <input type="checkbox"/> Send snapshot image via FTP <input type="checkbox"/> Send message via HTTP Event Servers <input type="checkbox"/> Save snapshot on Storage <input type="checkbox"/> Record video on SD card <input type="text"/> Sec.	<input type="checkbox"/> Server1 <input type="checkbox"/> Server2 <input type="checkbox"/> Server3 <input type="checkbox"/> Server4 <input type="text"/>
Event 3	<input type="checkbox"/> Send snapshot image via E-mail <input type="checkbox"/> Send snapshot image via FTP <input type="checkbox"/> Send message via HTTP Event Servers <input type="checkbox"/> Save snapshot on Storage <input type="checkbox"/> Record video on SD card <input type="text"/> Sec.	<input type="checkbox"/> Server1 <input type="checkbox"/> Server2 <input type="checkbox"/> Server3 <input type="checkbox"/> Server4 <input type="text"/>
Event 4	<input type="checkbox"/> Send snapshot image via E-mail <input type="checkbox"/> Send snapshot image via FTP <input type="checkbox"/> Send message via HTTP Event Servers <input type="checkbox"/> Save snapshot on Storage <input type="checkbox"/> Record video on SD card <input type="text"/> Sec.	<input type="checkbox"/> Server1 <input type="checkbox"/> Server2 <input type="checkbox"/> Server3 <input type="checkbox"/> Server4 <input type="text"/>
Event 5	<input type="checkbox"/> Send snapshot image via E-mail <input type="checkbox"/> Send snapshot image via FTP <input type="checkbox"/> Send message via HTTP Event Servers <input type="checkbox"/> Save snapshot on Storage <input type="checkbox"/> Record video on SD card <input type="text"/> Sec.	<input type="checkbox"/> Server1 <input type="checkbox"/> Server2 <input type="checkbox"/> Server3 <input type="checkbox"/> Server4 <input type="text"/>

Note: HTTP Action Setting allows the VPort sending the customized alarm messages to the HTTP Event Server when the event is triggered. Please refer to URL syntax being defined in RFC 1738 and the customer-defined commands for writing this setting with 100 characters.

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 Relay 1 alarm	Once this VMD is triggered, the VPort will trigger relay 1. Note that relay behavior will follow the configuration in alarm basic setting page.	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 <input type="checkbox"/> Sec	Once this VMD is triggered, the VPort will record the video on the SD card for a configured time period.	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

The VPort can actively take snapshot sequentially and transmit snapshot photos to designated FTP or mail box. You can configure the sequence interval between 1-30 seconds.

Sequential Snapshots

Enable sequential snapshots
 Send sequential snapshot image every [1~30] second(s)
 Send snapshot image via E-mail
 Send snapshot image via FTP

Digital Input

One digital input is provided by the VPort 56-2MP for linking with alarm detection devices, such as sensors.

Digital Inputs

Enable digital input alarm

Trigger Conditions and Actions

Trigger Condition	Trigger Action	HTTP Action Setting
<input type="radio"/> High <input checked="" type="radio"/> Low <input type="radio"/> Rising <input type="radio"/> Falling	<input type="checkbox"/> Trigger Relay1 alarm <input type="checkbox"/> Send snapshot image via E-mail <input type="checkbox"/> Send snapshot image via FTP <input type="checkbox"/> Send message via HTTP Event Servers <input type="checkbox"/> Record video on SD card <input type="text" value="5"/> Sec.	<input type="checkbox"/> Server1 <input type="checkbox"/> Server2 <input type="checkbox"/> Server3 <input type="checkbox"/> Server4 <div style="border: 1px solid gray; height: 40px; width: 100%;"></div>

Note: HTTP Action Setting allows the VPort sending the customized alarm messages to the HTTP Event Server when the event is triggered. Please refer to URL syntax being defined in RFC 1738 and the customer-defined commands for writing this setting with 100 characters.

Setting	Description	Default
Enable the digital input alarm	Enable or disable the digital input alarm	Disabled

Trigger Conditions

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

Trigger Actions

Setting	Description	Default
Trigger Relay 1 alarm	Once this VMD is triggered, the VPort will trigger relay 1. Note that relay behavior will follow the configuration in alarm basic setting page.	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, the VPort will record the video on the SD card for a configured time period.	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

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 the 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	Word (2 bytes)	Item name	R/W	Description
0x0000	1	Vender ID	R	0x1393
0x0001	1	Unit ID	R	0x01
0x0002	1	Product Code	R	0x880E
0x0010	20	Vender Name	R	moxa
0x0030	20	Product Name	R	VPort 56-2MP
0x0050	1	Serial Number	R	
0x0051	2	Firmware Version	R	
0x0053	2	Release Date	R	
0x0055	2	MAC Address	R	
0x0080	1	DI Status	R	1: High 0: Low
0x0084	1	Relay Status	R/W	0: Open 1: Close
0x0701	1	Record Status	R/W	R: 0: No record 1: recording W: 0: stop record 1: start record
0x0801	1	Dynastream Status	R/W	R 0: No run dynastream 1: run dynastream W 0: stop dynastream 1: start dynastream
0x0802	1	IVA Tamper Status	R/W	0x0000: No alert 0x0001: Alert
0x0803	1	IVA Learning Status	R	0x0000: No learning 0x0001: Is learning
0x0804	1	IVA Item 01 Status	R/W	0x0000: No alert 0x0001: Alert
0x0805	4	IVA Item 01 Object detected coordination	R	Word 0: Left Top X Word 1: Left Top Y Word 2: Right Down X Word 3: Right Down Y
0x0809	1	IVA Item 02 Status	R/W	0x0000: No alert 0x0001: Alert
0x080A	4	IVA Item 02 Object detected coordination	R	Word 0: Left Top X Word 1: Left Top Y Word 2: Right Down X Word 3: Right Down Y

0x080E	1	IVA Item 03 Status	R/W	0x0000: No alert 0x0001: Alert
0x080F	4	IVA Item 03 Object detected coordination	R	Word 0: Left Top X Word 1: Left Top Y Word 2: Right Down X Word 3: Right Down Y
0x0813	1	IVA Item 04 Status	R/W	0x0000: No alert 0x0001: Alert
0x0814	4	IVA Item 04 Object detected coordination	R	Word 0: Left Top X Word 1: Left Top Y Word 2: Right Down X Word 3: Right Down Y

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 Verde 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

Technical Specifications

Camera

Sensor: 1/2.5" HD progressive scan CMOS

Lens: 6.3 to 63 mm auto focus zoom lens

Angle of view (tele-wide):

- **Horizontal:** 5.5° to 50.6°
- **Vertical:** 3.1° to 29.3°
- **Diagonal:** 6.2° to 57°

Illumination:

- Color: 0.2 lux at F1.8
- B/W: 0.05 lux at F1.8

Synchronization: Internal

White Balance: ATW, AWB

Electronic Shutter:

AES: On/Off

Fix: 1/50, 1/100, 1/250, 1/500, 1/1000, 1/2000, 1/4000, 1/10000 sec

S/N Ratio: More than 50 dB (AGC off)

ICR Control: Auto (light sensor control) or DI control

DNR: Built-in 3D DNR

AGC Control: On/Off

Backlight Compensation: On/Off

Auto Exposure: On/Off

Image Rotation: Flip, Mirror, and 180° rotation

Auto Sense Up: On/Off, Max. 64x

Image Setting: Manually tune sharpness

Video

Video Compression: H.264 (ISO/IEC 14496-10) or MJPEG

Video Output: via Ethernet

Video Streams: Up to 3 video streams (2 x H.264 and 1 x MJPEG)

Video Resolution and FPS (frames per second):

	NTSC		PAL	
	Size	Max. FPS	Size	Max. FPS
Full HD 1080P	1920 x 1080	30	1920 x 1080	25
HD 720P	1280 x 720	30	1280 x 720	25
SVGA	800 x 600	30	800x 600	25
Full D1	720 x 480	30	720 x 576	25
4CIF	704 x 480	30	704 x 576	25
VGA	640 x 480	30	640 x 480	25
CIF	352 x 240	30	352 x 288	25

Note: Up to 30/25 FPS for each of 3 independent streams at max resolution.

Video Viewing:

- DynaStream™ supported for automatic adjustment of frame rate
- Image stabilizer to reduce video shaking
- CBR Pro™ for optimized image quality within limited bandwidth
- 8 privacy mask areas provided
- Adjustable image size and quality
- Timestamp and text overlay
- Maximum of 5 simultaneous unicast connections
- ROI (Region of Interest) configuration for up to 3 area

Audio

Audio Inputs: 1 Line-in with 3.5 mm phone jack

Audio Outputs: 1 Line-out with 3.5 mm phone jack

Two-Way Audio: Full duplex two-way audio

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, SSL

Ethernet: 1 10/100BaseT(X) Ethernet port, RJ45 connector, or 1 100BaseFX, single mode

Serial Interface

RS-485: 1 full-duplex RS-485

GPIO

Digital Inputs: 1, max. 8 mA

- High: +13 to +30 V

- Low: -30 to +3 V

Relay Output: 1, max. 24 VDC @ 1 A

LED Indicators

STAT: Indicates if the system is booted properly or not

Network: 10 Mbps or 100 Mbps

Power: Power on/off

Local Storage

SD Socket: Standard SD socket (SDHC, SDXC)

Power Requirements

Input:

12/24 VDC, 24 VAC or Power-over-Ethernet (PoE+, 802.3at), redundant power design

Power Consumption: 23 W

Physical Characteristics

Camera Body Housing: Metal, IP30 protection

Weight: 1415 g

Installation: Wall mounting, ceiling mounting, pole mounting, corner mounting (optional external housing and mounting accessory may be required)

Alarms

Video Motion Detection: 3 independently configurable motion areas

Camera Tamper: Sensitivity adjustable camera tamper detection (Pending)

Scheduling: Daily repeat timing schedule

Imaging: JPEG snapshots for pre/trigger/post alarm images

Custom Alarms: HTTP event and CGI events for setting customized alarm actions

Email/FTP Messaging: Automatic transfer of stored images via email or FTP as event-triggered actions

Pre-alarm Buffer: 84 MB video buffer for JPEG snapshot images

Environmental Limits

Operating Temperature:

Standard Models: 0 to 60°C (32 to 140°F)

Wide Temp. Models: -40 to 75°C (-40 to 167°F)

Storage Temperature: -40 to 85°C (-40 to 185°F)

Ambient Relative Humidity: 5 to 95% (non-condensing)

Standards and Certifications

Safety: UL60950-1, EN 50121-4, NEMA TS2

EMI: FCC Part 15, CISPR (EN 55022) class A

EMS:

EN 61000-4-2 (ESD), Level 3,

EN 61000-4-3 (RS), Level 3,

EN 61000-4-4 (EFT), Level 3,

EN 61000-4-5 (Surge), Level 3,

EN 61000-4-6 (CS), Level 3,

EN 61000-4-8,

EN 61000-4-11

Shock: IEC 60068-2-27

Freefall: IEC 60068-2-32

Vibration: IEC 60068-2-6

MTBF (mean time between failures)

Time: 169,886 hours

Database: Telcordia (Bellcore), GB 25°C

Warranty

Warranty Period: 3 years (not including moving parts; see Moxa's warranty policy online for details)

Details: See www.moxa.com/warranty

Software Development Kit

VPort SDK PLUS: Includes CGI commands, ActiveX Control, and API library for customized applications or system integration for third-party developers (latest version available on Moxa website).

Standard: ONVIF ProfileS