Moxa VPort P06-1MP-M12 EN 50155 IP Camera User's Manual

Edition 2.1, April 2016

www.moxa.com/product

Moxa VPort P06-1MP-M12 EN 50155 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

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 India
Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

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 P06-1MP-M12, please pay close attention to the following instructions:

❒ After opening the VPort P06-1MP-M12 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 to **Chapter 2, Getting Started**, and **Chapter 3, Accessing the VPort P06-1MP-M12 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

The VPort P06-1MP-M12 is a rugged HD resolution (720P) box type IP camera designed for use in harsh environments. In addition to being able to handle basic video feeds, many advanced features are also included to set up surveillance or web multimedia applications. The VPort P06-1MP-M12 is designed to provide stability, robustness, ease-of-use, and flexibility.

The following topics are covered in this chapter:

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

Overview

The compact VPort P06-1MP-M12 cameras provide a HD (720P, 1280 x 720) video image, and feature an H.264/MJPEG IP dome, giving them the versatility and ruggedness to excel in many different installations and environments for mobile IP video surveillance applications. In addition, the cameras feature EN 50155 compliance, vandal-proofing (EN 62262 IK8), -25 to 55°C or -40 to 70°C (T models) operating temperature, a rugged M12 Ethernet port, 1 audio input, PoE power inputs, IP66 rain and dust protection, a dehumidifying membrane, and a selectable lens.

Excellent Image Quality

The VPort P06-1MP-M12 is equipped with a cutting-edge CMOS sensor, which provides excellent high resolution video images at 1280 x 800 pixels and covers larger areas than legacy analog cameras. With the addition of DNR (Digital Noise Reduction), BLC (Black Level Control), and WDR (Wide Dynamic Range) functions, the VPort P06-1MP-M12 provides an extremely clear picture of the surveillance region.

Rugged Hardware Design

The VPort P06-1MP-M12's 47 mm height makes it ideal for tough vehicle environments with limited installation space. It is compliant with EN 50121-3-2 (EMC), EN 61373 for shock and vibration, and essential sections of EN 5015, with standard models designed for T1 temperatures, and wide temp. models designed to withstand TX temperatures (-40 to 70°C; note that the T models are also tested for 10 min. at +15°C over the max. of 75°C), without a fan or other cooling equipment. Moreover, the VPort P06-1MP-M12 achieves the highest enclosure protection, IEC 62262 Class IK8, providing users with a true, vandal-proof IP camera.

High Video Performance

The VPort P06-1MP-M12 is designed to provide both H.264 and MJPEG video streams and transmit a maximum of 3 independent video streams (2 H.264, 1 MJPEG) simultaneously. In addition, Moxa's DynaStream™ function allows you to change the video frame rate automatically, which can help you control your network bandwidth budget and ease network system management. A DHCP Opt66/67 auto-configuration mechanism simplifies the workload of mass installation and maintenance by backing up the configuration on a TFTP server.

Package Checklist

Moxa's VPort P06-1MP-M12 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 P06-1MP-M12 series (lens included)

Standard Temp. Models	Wide Temp. Models	Lens
VPort P06-1MP-M12-CAM36	VPort P06-1MP-M12-CAM36-T	3.6 mm
VPort P06-1MP-M12-CAM42	VPort P06-1MP-M12-CAM42-T	4.2 mm
VPort P06-1MP-M12-CAM60	VPort P06-1MP-M12-CAM60-T	6.0 mm

- Screw handle accessory package

Torx screw driver for attaching/detaching the upper case	4 sets of nuts, gaskets and spring washers for mounting the camera	4 indented hexagon head tapping screws for mounting the camera on the ceiling

- Sticker for camera mounting positions
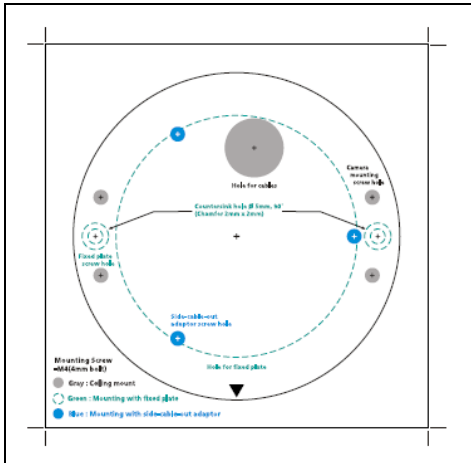
- Quick installation guide
- Documentation and software CD (includes User's Manual, Quick Installation Guide, and VPort Utility)
- Warranty card

    NOTE: *Notify your sales representative if any of the above items is 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

- 1/2.7"HD progressive CMOS image sensor
- High image quality with WDR (wide dynamic range) and DNR (Digital Noise Reduce) supported
- Minimum illumination is up to 0.2 lux (color)
- Supports MJPEG and H.264 Dual Codecs
- Provides 3 video streams for H.264 and MJPEG simultaneously
- Video streams at up to 30 frames/sec at WXGA (1280x800) resolution
- Supports video quality configuration with fixed bit rate (CBR) and fixed quality (VBR)
- Video latency under 200 ms
- DynaStream™ supported for network efficiency with dynamic frame rate change
- CBR Pro™ supported for high image quality in limited bandwidth transmissions
- WXGA/720P/SVGA/ Full D1/ 4CIF/ VGA/ CIF/ QCIF resolution
- TCP, UDP, and HTTP network transmission modes
- Supports DHCP OPT66/67 for automatic configuration from TFTP server, making mass installation easier
- Supports RTSP Streaming
- Supports Multicast (IGMP) video streaming
- Supports SNMP (V1/V2C/V3) for network system integration and management
- Supports QoS (ToS) for transmission priority
- Built-in web server for easy configuration
- Accessible IP filtering
- UPnP supported
- Compliant with EN 50121-3-2 and relevant sections of EN 50155 (compliant with IEC 60571)
- 1 10/100BaseT (X) with M12 D-code connector

- 1 audio input with RCA-type connector
- IP66 rain and dust protection with a dehumidifying membrane
- PoE (Power-over-Ethernet, 802.3af) supported
- EN 62262 IK9 level vandal resistant
- -25 to 55°C (EN 50155, class T1), or -40 to 70°C (EN 50155. Class TX) operating temperature for rolling stock environments
- CE, FCC, UL 60950-1
- Built-in tamper alarm and Video Motion Detection (VMD)
- Pre, Trigger, and post snapshot images supported
- Sequential snapshot images supported
- Supports SMTP and FTP for alarm message transmission
- Supports HTTP Event Server
- 5-year warranty
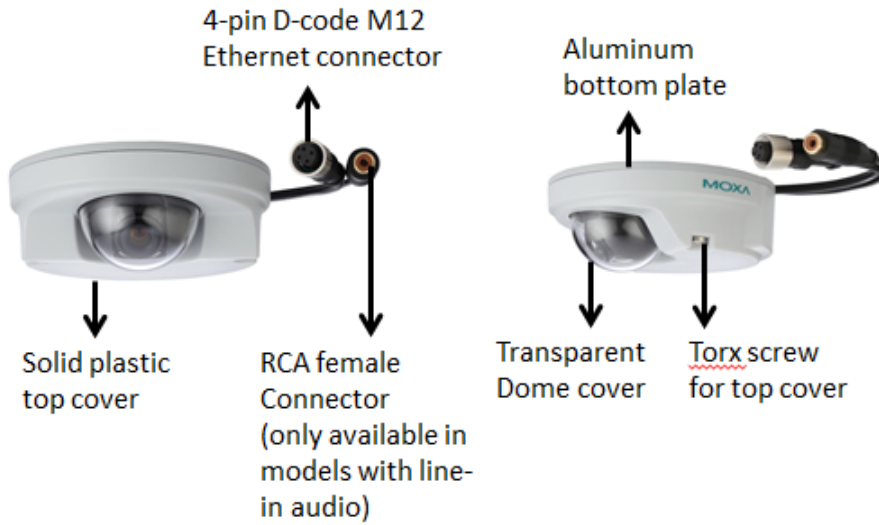

NOTE   If you are interested in Moxa's VPORT SDK PLUS, please visit Moxa's website at www.moxa.com to download the package, or contact a Moxa sales representative for more information about this SDK

Typical Application
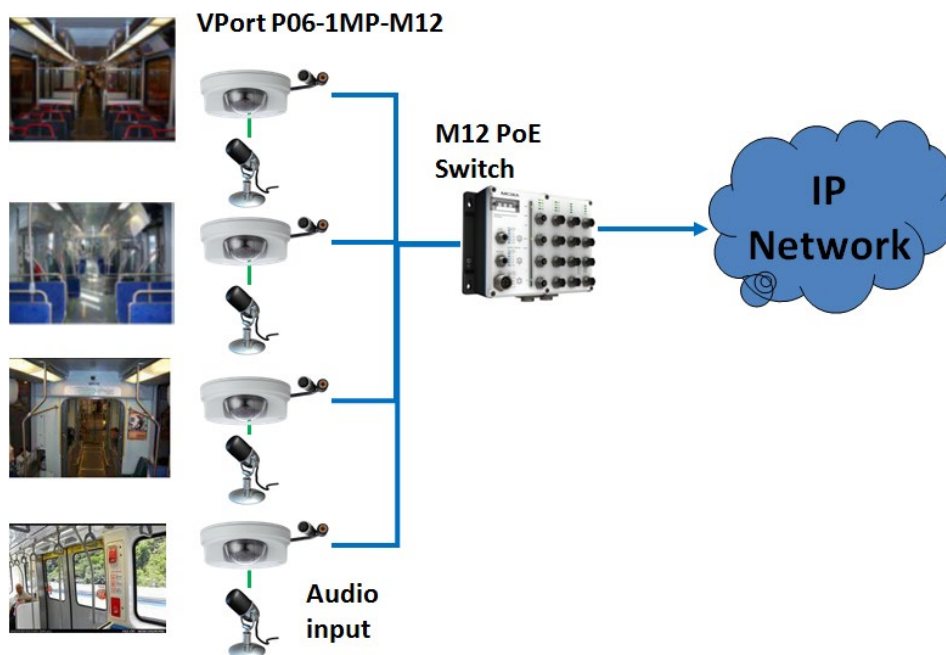
Product Description

Appearance

- **4-pin D-code M12 Ethernet connector:** A 4-pin M12 D-code connecter for both PoE power supply (Mode A) and Auto MDI/MDI-X Ethernet connection.

PIN	TX
1	TD+
2	RD+
3	TD−
4	RD−

NOTE	To connect the VPort P06-1MP-M12 to the network, use an Ethernet cable with a D-code M12 connector and an M12 PoE switch or RJ45 PoE switch

M12 D-code to M12 D-code cable	M12 PoE Switch (e.g., TN-5508-4PoE)
M12 D-code and RJ45 cable	RJ45 PoE switch (e.g., EDS-P510)

NOTE	The power input rating of the VPort P06-1MP-M12 is 48 VDC, 0.12 A, and the maximum power consumption is approximately 6 W.

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

- **RCA female connector:** The VPort P06-1MP-M12 supports one audio input with RCA female connector. The audio will be digitized and compressed as an audio stream for network tramission with the video stream.

NOTE	RCA audio connectors are popular and easy to find on the market. If a different audio connector is required, please contact your Moxa sales representative for customization service.

- **Solid plastic top cover:** This top cover can be removed when tuning the camera lens position.
- **Transparent dome cover:** The VPort P06-1MP-M12 is designed with a transparent PC dome cover, which is vandal-proof with EN 62262 (IEC62262) class IK9 level protection.
- **Torx screw for top cover:** There are 2 torx screws for the top cover. These 2 torx screws are designed with anti-shedding for convenient installation. The user can use the L-type torx screw driver for loosening or fixing the top cover.

NOTE	The color of the camera casing can be customized based on your installation environment. Please contact your Moxa sales representative for this customization service.

Inside the camera
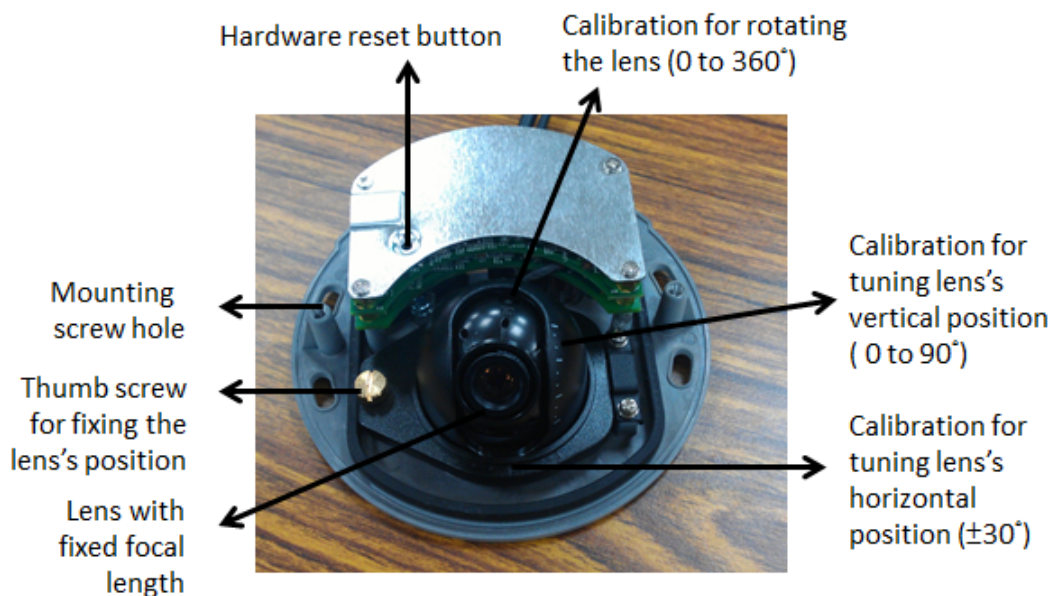
- **Mounting screw hole:** There are 4 mounting screw holes for mounting the VPort P06-1MP-M12.
- **Thumb screw for fixing the lens position:** To tune the lens's position, loosen this thumb screw. After the position tuning is done, secure this thumb screw.
- **Lens with fixed focal length:** The VPort P06-1MP-M12 is designed to use different fixed focal-length lenses. Choose the appropriate focal-length lens based on the viewing angle and object distance of your application.
- **Hardware reset button:** Use a pointed stick to push down the reset button to reboot or restore factory defaults.
    - ➢ Reboot: press the button one time.
    - ➢ Reset to factory default: press the button and hold for at least 5 seconds.
- **Calibration for rotating the lens (0 to 360°):** Rotate the lens to get the optimal image, and then mark the position with this calibration for future replacement or mass installation.
- **Calibration for tuning lens's vertical position (0 to 90°):** After tuning the lens's vertical position, mark the position with this calibration for future replacement or mass installation.
- **Calibration for tuning lens's horizontal position (±30°):** After tuning the lens's horizontal position, mark the position with this calibration for future replacement or mass installation.

2

Getting Started

This chapter includes information about how to install a VPort P06-1MP-M12 IP camera.

The following topics are covered in this chapter:

❒ **Before Getting Started**

❒ **First-Time Installation and Configuration**

   ➢ Hardware Installation

   ➢ Software Installation

❒ **VPort P06-1MP-M12 Dimensions**

❒ **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

Hardware Installation

Step 1: Open and remove the top cover.

Use the Security Torx to loosen the top cover screws.

Step 2: Use the installation sticker to drill the holes. There are 3 types of installation.

a.   Mounting with 4 mounting screws

Drill the gray hole in the sticker, and then mount the camera with 4 sets of nuts, gaskets, and spring washers and 4 indented hexagon head tapping screws for mounting the camera on the ceiling.
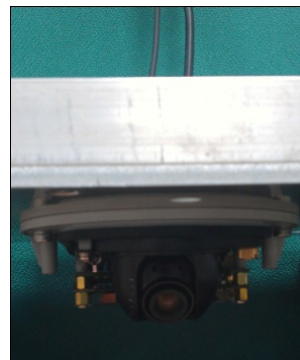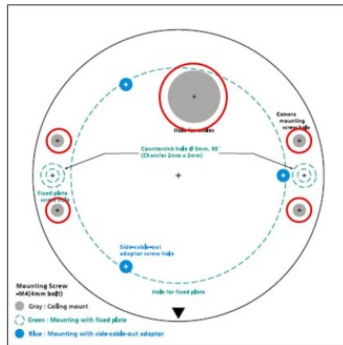
b.   Mounting with the side-cable-out adaptor

VP-SCO1

If the installation requires a cable –out on the side, then the side-cable-out adaptor (VP-SCO1) is required. Drill the blue hole in the sticker for mounting the adaptor on the surface with 3 sets of nuts, gaskets, spring washers, and indented hexagon head tapping screws. Then, mount the VPort P06-1MP-M12 on the adaptor with 4 sets of M4 screws, which are provided in the VP-SCO1's package.

4 M4 screws for mounting the camera on VP-SCO1 adaptor
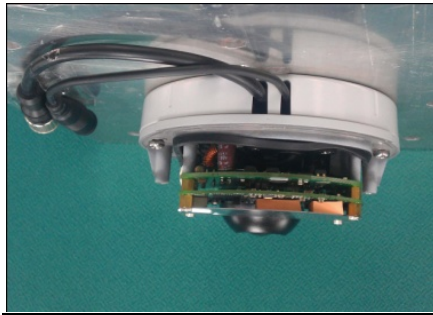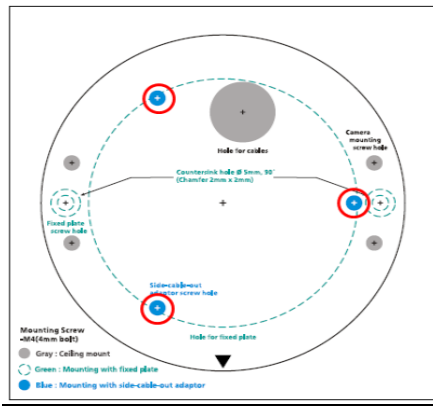
c. Mounting with the fixed plate

VP-FP1

If nuts, gaskets, and spring washers cannot be used when mounting on the ceiling, use the VP-FP1 fixed plate. Drill the green dotted-line holes and the 4 camera mounting screw holes in the sticker, and then put the VP-FP1 inside the hole. Use the 2 countersink screws to mount the VP-SP1. Finally, mount the VPort P06-1MP-M12 on the fixed plate with 4 indented hexagon head tapping screws.
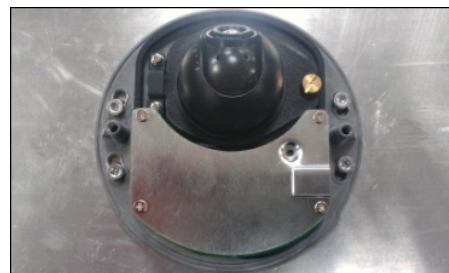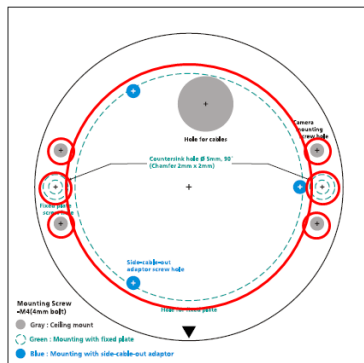
NOTE	The screw hole for mounting the VP-FP1 fixed plate is a countersink hole with 5 mm diameter, 90° to the surface, with 2 x 2 mm chamfer. Be sure to take this into account when drilling these 2 screw holes.

Step 3: Connect the camera with 4-pin M12 D-code Ethernet connector and RCA male connector.

Step 4: Loosen the thumb screw for tuning the horizontal, vertical, and rotating lens position. Once the lens position is correct, fix this thumb screw.

Step 5: Fix the top cover. The installation is now complete.

Software Installation

Step 1: Configure the VPort P06-1MP-M12's IP address

When the VPort P06-1MP-M12 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 concluded, the Model Name, MAC address, IP address, serial port, and HTTP port of the VPort will be listed in the utility's window.
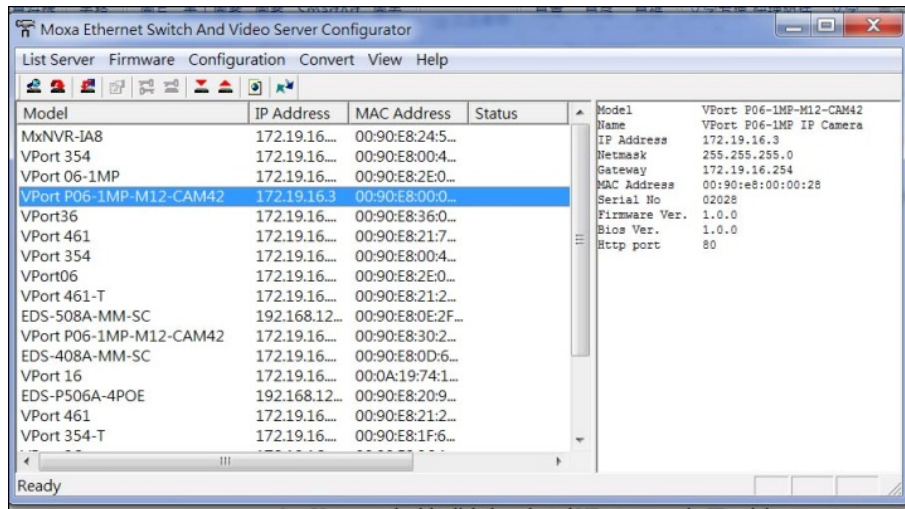
Users can double click the selected VPort, or use the IE web browser to access the VPort's web-based manager (web server).

Non DHCP Server Network Environment

If your VPort 16-M12 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 16-M12 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 **Use fixed IP address** to ensure that the IP address you assign is not deleted each time the VPort is restarted.

Step 2: Accessing the VPort P06-1MP-M12's web-based manager

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

Step 3: Install the ActiveX Control Plug-in

A security warning message will appear the first time you access the VPort's web-based manager. The message is related to installing the VPort AcitveX Control component on your PC or notebook. Click Yes to install this plug-in to enable 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 VPort P06-1MP-M12's web-based manager homepage.

After installing the ActiveX Control component, the homepage of the VPort P06-1MP-M12'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 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.
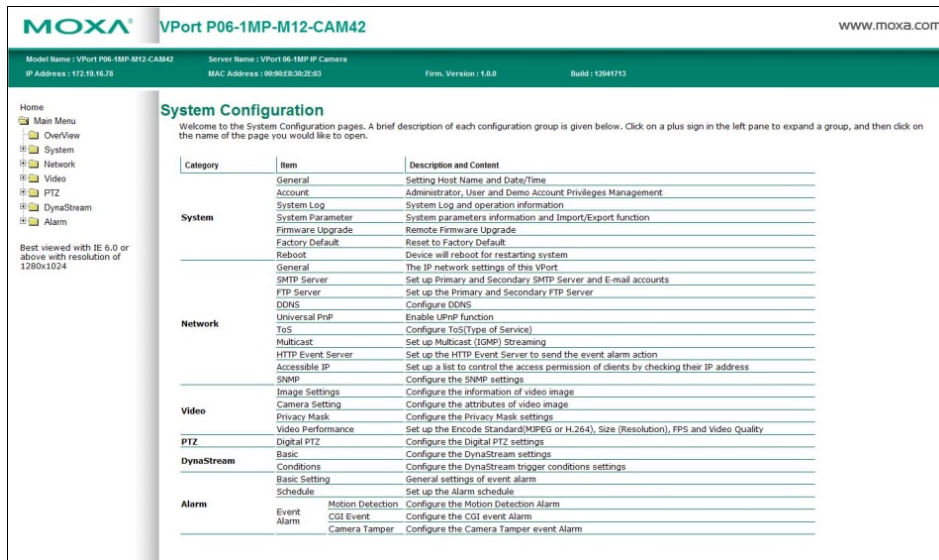
VPort P06-1MP-M12 Dimensions
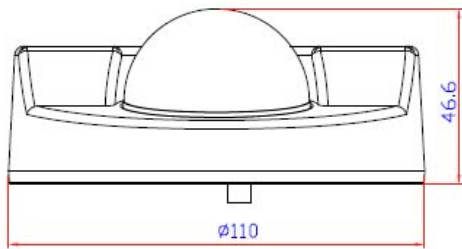
Front View
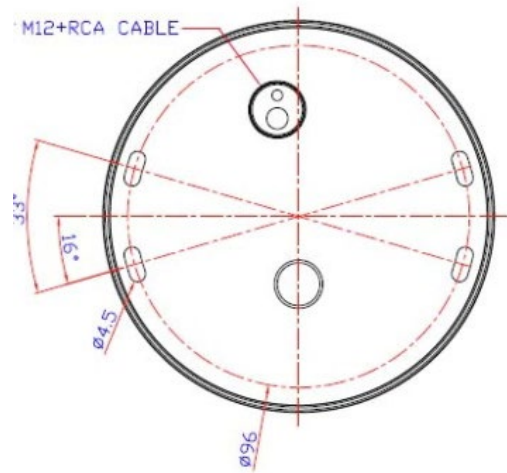
Bottom View
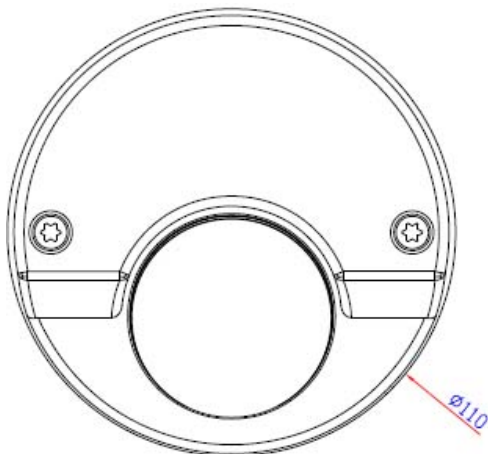
Top View
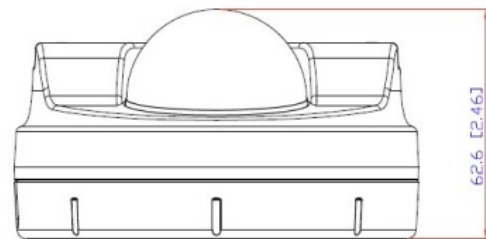
Camera with SC01 adaptor

(Unit = mm)

Wiring Requirements

ATTENTION

- Be sure to disconnect the power cord before installing and/or wiring your Moxa VPort P06-1MP-M12.
- 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.

3

Accessing the VPort's Web-based Manager

This chapter includes information about how to access the VPort P06-1MP-M12 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

  ➢ Show PTZ Control Panel

  ➢ Snapshot

Functions Featured on the VPort's Web Homepage

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

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

VPort's Information

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

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. **Receiving Stream:** Shows the encoding algorithm currently being used. The VPort P06-1MP-M12 features 2 built-in encode engines 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. **Media Options:** Enable or disable the video or audio transmission.

3. **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 172.19.10.21 ▼

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.

Show PTZ Control Panel

The VPort P06-1MP-M12 supports a maximum 4X digital zoom. The user can control the PAN, TILT, ZOOM on this PTZ control panel.

Snapshot

Users can take snapshot images for storing, printing, or editing by clicking the **Snapshot** button. To save the image, right-click and select the **Save** option.

4

System Configuration

After installing the hardware, the next step is to configure the VPort P06-1MP-M12's settings. Users can configure by web console.

The following topics are covered in this chapter:

❒ **System Configuration by Web Console**

- ➢ System
- ➢ Network
- ➢ Video
- ➢ Audio
- ➢ PTZ
- ➢ DynaStream^{TM}
- ➢ 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
	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 email accounts
	FTP Server	Set up the Primary and Secondary FTP Server
	DDNS	Configure Dynamic DNS service
	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 IP address
	SNMP	Configure the SNMP settings
Video	Image Settings	Configure the attributes of the video image
	Image Tuning	Configure the attributes of camera
	Privacy Mask	Configure the Privacy Mask settings
	Video Performance	Set up Encode Standard (MJPEG or MPEG4), Size (Resolution), FPS, and Video Quality
Audio	Audio Settings	Configure the Audio settings
PTZ	Digital PTZ	Configure the Digital PTZ settings
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
Event Alarm	Basic	General event alarm settings
	Schedule	Set up the Alarm schedule
	Motion Detection	Configure the motion detection 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**, as shown below:

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 P06-1MP-M12 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 the VPort's data and time setting with the local computer time.	
Manual	Manually change the VPort's date and time setting.	
Automatic	Use the NTP server for changing the 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 B for your region's time zone.

Account Privileges

Different account privileges are available for different purposes.

Admin password

Setting	Description	Default
Admin Password (max. 14 characters)	The administrator can type the new password in this box.	Default admin has no password
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 P06-1MP-M12 is only allowed to send 10 unicast video streams. For this reason, you should limit the number of users simultaneously accessing a VPort P06-1MP-M12 to prevent performance problems.

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

Export to a File   Send a Report via E-mail   Clear

☐ Send to system log Server

Syslog Server 1   [   ]
Port Destination   [514]
Syslog Server 2   [   ]
Port Destination   [514]

Save

Send to system log server

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

NOTE	A maximum of 500 lines is displayed in the log. 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

```
VPort06 Configuration File
[security]
username01=admin
username02=
username03=
username04=
username05=
username06=
username07=
username08=
username09=
username10=
username11=
userpass01=
userpass02=
userpass03=
userpass04=
userpass05=
userpass06=
```

Export to a File

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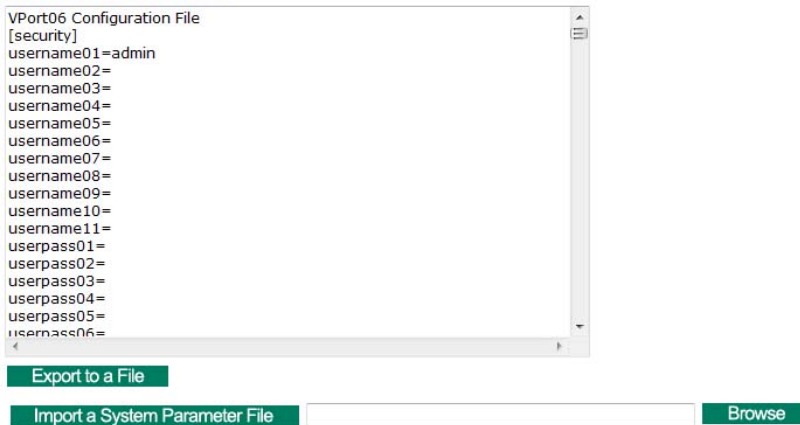
NOTE	The system parameter import/export functions allow the administrator to backup and restore system configurations. The Administrator can export this sys_config.ini file (in a special binary format) for backup, and import the sys_config.ini file to restore the system configurations of VPort IP cameras.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

Firmware Upgrade

Firmware Upgrade

[   ] Browse   Upgrade

Take the following steps to upgrade the firmware:

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

NOTE	For the VPort P06-1MP-M12, 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	172.19.16.62
Subnet mask	255.255.255.0
Gateway	172.19.16.254
Primary DNS	192.168.50.33
Secondary DNS	192.168.1.97

HTTP

HTTP port	80

RTSP Streaming

RTSP port	554

Save

Access Method

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

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

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

Auto Configuration

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 VPort P06-1MP-M12 enables the auto-configuration function, it will ask for the IP address from the DHCP server, and the path of the TFTP server and configuration file.
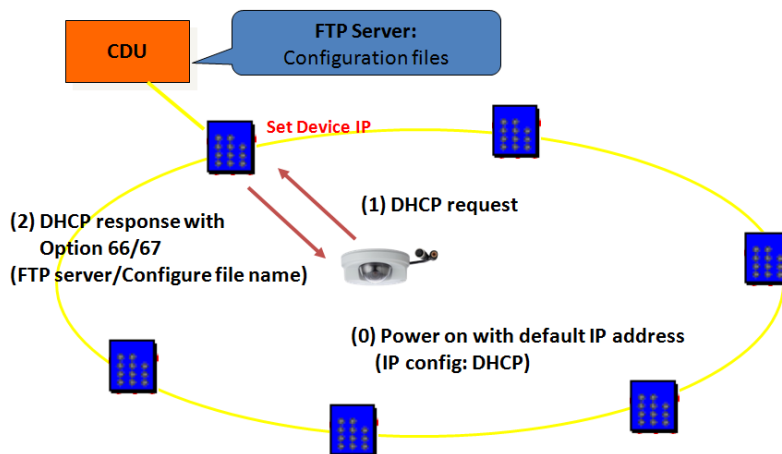
Step 2:

Once the VPort P06-1MP-M12 completes the IP settings, it will acquire the configuration file from the TFTP server, and check if this configuration file is correct or not.
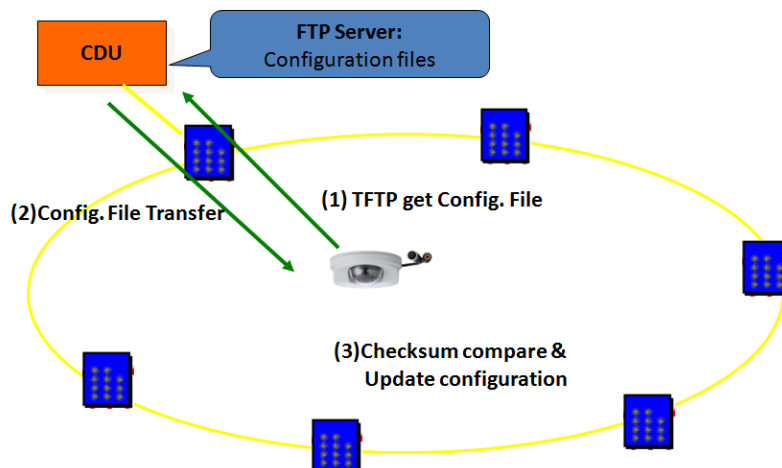
NOTE	For the auto-configuration function to work, the system should:
	1. Have a DHCP Server that supports DHCP Opt 66/67 in the network switches and routers.
	2. Have a TFTP server that supports the TFTP protocol

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	Select the HTTP transmission mode: HTTP Only or HTTP + HTTPS	HTTP Only

RTSP Streaming

The VPort P06-1MP-M12 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 P06-1MP-M12 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: Open VLC Player and select **Media - Open network streaming**
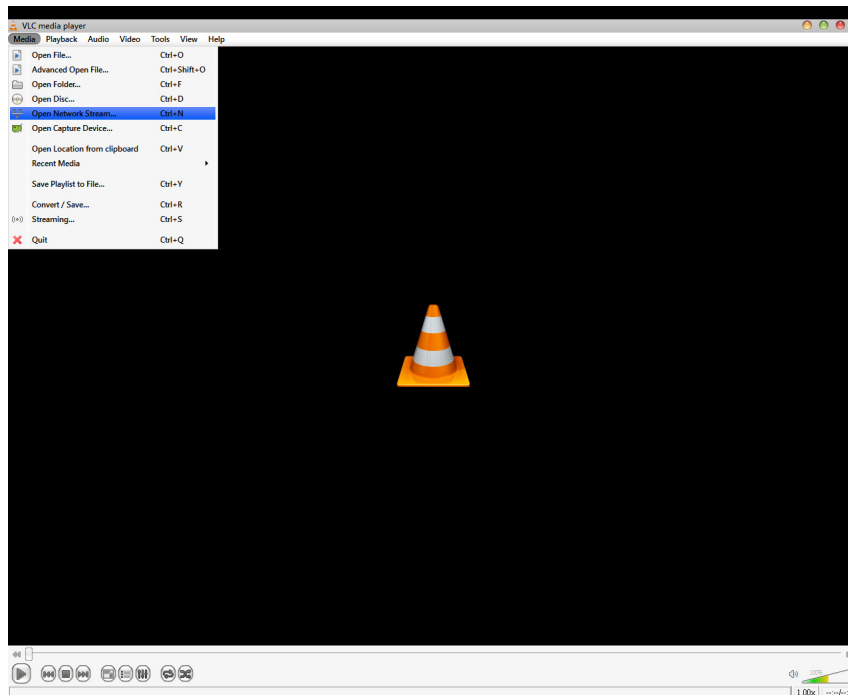
Step 2: When the following pop-up window appears, type the URL in the input box. E.g., type
rtsp://<VPort P06-1MP-M12's IP address>[:<RTSP Port]/udpstream_ch1_stream< 1 or 2>
rtsp://<VPort P06-1MP-M12's IP address>[:<RTSP Port]/multicaststream_ ch1_stream<1 or 2>
RTSP Port: 554 is the default, and then click on **OK** to connect to the VPort P06-1MP-M12.
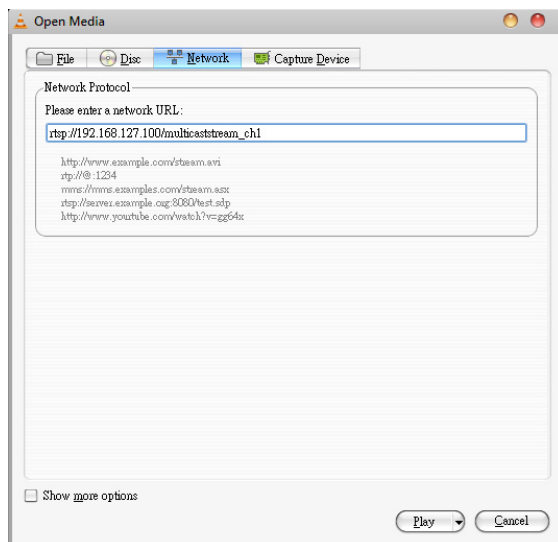
Step 3: Wait a few seconds for VLC Player to establish the connection.

Step 4: After the connection has been established, the VPort P06-1MP-M12's video will appear in the VLC Player display window.

NOTE	The video performance of the VPort P06-1MP-M12 may vary when using other media players. For example, you will notice a greater delay when viewing the VPort P06-1MP-M12's video from the VLC player compared to viewing it directly from the VPort P06-1MP-M12's built-in web server. In addition, viewing the VPort P06-1MP-M12'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 P06-1MP-M12'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 P06-1MP-M12'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	
1st SMTP account name	
1st SMTP password	
1st Sender's email address	

2nd SMTP Server and Sender Email

2nd SMTP (mail) server	
2nd SMTP account name	
2nd SMTP password	
2nd Sender's email address	

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:	
2nd Recipient's Email Address:	

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	None
1st SMTP password	name and password to be authenticated.	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	DynDNS.org(Dynamic) ▾
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.

[Save]   [Update]

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	None
Password/ Key	the service from the DDNS service provider (based on the rules of DDNS websites).	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.

Save

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　0 ▾　0 ▾

Save

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

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

Multicast

The VPort P06-1MP-M12 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.

Network WITHOUT Multicast
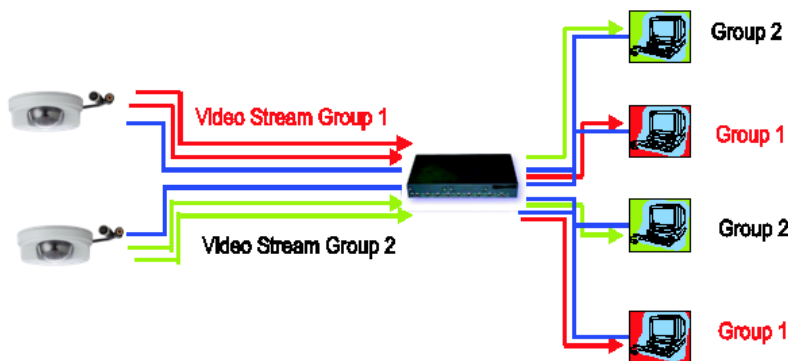
Network WITH Multicast
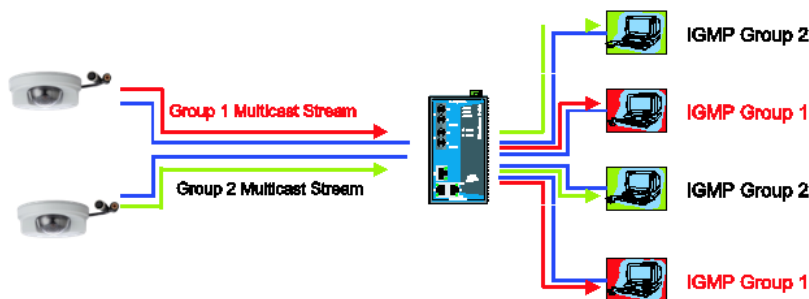
NOTE	The VPort P06-1MP-M12 is the source that delivers the multicast video stream. To benefit from the Multicast protocol, the gateway or network switch should support the multicast filtering function (such as IGMP Snooping) so that the multicast stream is delivered correctly and precisely. To learn more about IGMP Snooping, refer to the Moxa EtherDevice™ series Industrial Ethernet Switch user's manual.

Configuring Multicast Settings

Multicast Settings

Stream 1

Multicast group address	239.127.0.100
Multicast video port	5556
Multicast audio port	5558
Multicast TTL	128
Continuous Multicast Push	☐ Enable

Stream 2

Multicast group address	239.127.0.100
Multicast video port	5560
Multicast audio port	5562
Multicast TTL	128
Continuous Multicast Push	☐ Enable

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 Ser 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:	

Save

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

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

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

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		
2		
3		
4		
5		
6		
7		
8		
9		
10		

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 P06-1MP-M12 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	☐ 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.8691.8.4.5

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 (only for SNMP V1, V2c, V3, or SNMP V3)

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: 8691.8.4.5. This number cannot be changed.

NOTE	The MIB file is MOXA-VPORT06-MIB.mib (or.my). You can find it on the software CD or the download center of the Moxa website.

Telnet

Use this option to Enable/Disable the telnet function.

Telnet

☐ Enable Telnet

Save

Video

Image Settings

Image Settings

Image Information

Description: [   ]

Image Appearance

Image Information:

◯ Not Shown

◯ Shown on the caption

◉ Shown on the image

Position X: 0   (0~400)

Position Y: 0   (0~300)

Save

(AV-TCP)   2000/01/05 05:08:38

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 Appearance Position

The position of the Image Appearance window can be changed by configuring Position X (0 to 400) and Position Y (0 to 300).

Image Tuning

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

Environment

Setting	Description	Default
Environment	Choose the kind of environment the VPort camera be installed in; parameters will be optimized depending on which environment is specified. **Automatic:** The system will detect the environment automatically; use this setting when the camera is installed outdoors. **50 Hz and anti-flicker:** This setting should be enabled when the camera is installed in a 50 Hz power frequency environment, for anti-image flicker. **60 Hz and anti-flicker:** This setting should be enabled when the camera is installed in a 60 Hz power frequency environment , for anti-image flicker	Automatic
Auto exposure level	A higher level will reduce the shutter speed, resulting in a brighter image; a lower level will have the opposite effect.	+0

Image Adjustment

Setting	Description	Default
Saturation	Tune the image attribute to a value between -4 and +6	0
Contrast & Sharpness	Tune the image attribute to a value between -4 and + 4	0
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
Auto Gain Control (AGC)	The AGC function provides a clear image in low light conditions. An amplifier is used to boost the video signal when the light dims to increase the camera's sensitivity. In some bright environments, the amplifier may be overloaded, resulting in a distorted video signal. For this reason, it may be necessary to monitor the signal level with the AGC control circuit, and in some cases AGC will need to be switched off.	16x
Black level control (BLC)	This function changes the black level of the image. Higher settings will make the image brighter, and lower settings will make the image darker.	Middle
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: 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

Digital Noise Reduction

Setting	Description	Default
Enable	Enable the digital noise reduction function	Off

WDR

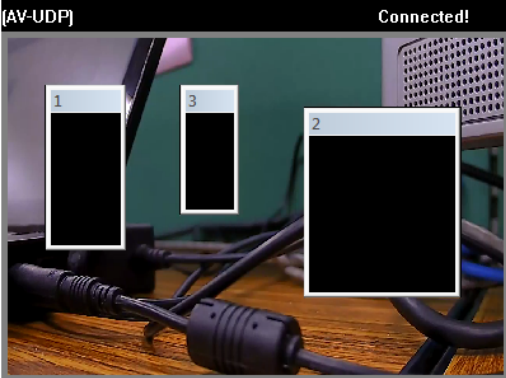| Setting	Description	Default
WDR (Wide Dynamic Range)	A higher level results in a stronger WDR effect. Choose a higher WDR the camera is focused on a scene with both highly lit regions and dark regions.	Level 8

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

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.	unchecked

---

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.

Video Performance

The VPort P06-1MP-M12 can send a maximum of three simultaneous video streams: two H.264 and one MJEPG. In fact, the VPort P06-1MP-M12 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

Resolution Type

Setting	Description	Default
NTSC or PAL	Choose NTSC or PAL resolution typefor your system	NTSC

Streams

Setting	Description	Default
Enable the video streams	Enables the VPort to send this video stream.	Enable stream 1 for H.264; Enable stream 2 for MJPEG

Codec Type

This codec type shows the codec of each video stream.

Resolution

The VPort P06-1MP-M12 supports 7 different resolutions: 1MP, HD, SVGA, Full D1, 4CIF, VGA, CIF

Setting	Description	Default
Select the image size	6 image resolutions (sizes) are provided. The administrator can choose each option with NTSC or PAL modulation.	1280 x 720 for stream1; 720 x 480 for stream 2

Resolution	NTSC	PAL
1MP	1280 x 800	1280 x 800
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
QCIF	176 x 112	176 x 144

NOTE   1280 x 800, 1280 x 720, and 800 x 600 are only available in stream 1. QCIF (176 x 112 or 176 x 144) is only available in stream 2. The maximum resolution for stream 2 is full D1 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.

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.	Stream 1: 5400 Kbps Stream 2: 4000 Kbps
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 help with network bandwidth estimation of different resolutions, FPS, and video content.

Audio

Users can enable or disable the Audio input function on the webpage. The setting is disabled by default.

PTZ

The VPort P06-1MP-M12's HD 720P (1280 x 720) image resolution provides crystal clear video images with fine detail even after the image is zoomed in on. The VPort P06-1MP-M12 comes with a digital PTZ function that enables users to zoom in on an image to observe finer details.

Digital PTZ

Before using digital PTZ, first enable it on the Digital PTZ page:

Digital PTZ

Digital PTZ Control
☑ Enable digital PAN/ TILT/ ZOOM
Save

Once Digital PTZ is enabled, click **Show PTZ Control Panel** from the IP camera home page. Click the "+" button in the bottom right of the page to use the digital zoom function. After zooming in, you can then use the wheel shown below to navigate the camera image.

NOTE	The direction button in the wheel will not be displayed until a digital zoom is performed. Once the camera image is zoomed out to its original size, the direction button will disappear.

NOTE	The VPort P06-1MP-M12 supports up to 4x digital zoom. Press the "+" button to view a 2x zoomed image, and twice to view a 4x zoomed image.

DynaStream^{TM}

DynaSteam^{TM} 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 to low during regular streaming to reduce bandwidth usage and automatically switch to a high frame rate during triggered events to ensure quick transmission of critical video data or video streams, or to provide detailed visual images for problem analysis.

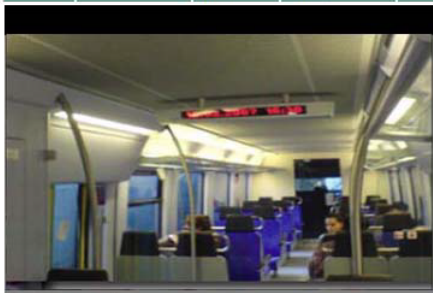| NOTE	To enable the DynaStream function from CGI commands and Modbus TCP, refer to the CGI Commands User's Manual for VPort SDK PLUS.

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 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.

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

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

Conditions

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

Currently, there are two types of trigger conditions: CGI Event and Motion Detection.

Setting	Description	Factory Default
Enable	To enable or disable the DynaStream function.	Disable
Duration	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 Live to the Alarm status, and remain in Alarm status for a 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

Basic

On this page you can configure some general parameters of the VPort P06-1MP-M12's alarm function, including alarm time interval, alarm snapshot, and suffix of image file name.

Event Alarm Basic Settings

Alarm Time Interval

Delay [32] second(s) before detecting the next alarm (10~999 secs)

Send Alarm with Snapshot images

☐ Take snapshot in [2] seconds(s) before event (1~6 secs)
☐ Take snapshot in [11] seconds(s) after event

Suffix of Image File Name in FTP and Mail attachment

☐ With Data and Time
☐ With Customized words [_____]

[Save]

Alarm Time Interval

Setting	Description	Default
Number of 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 a 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 a 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 the 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

Schedule

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

Event Type

Setting	Description	Default
Video Motion Detection, CGI Event, and Camera tamper	Set up 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
☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat	Select the weekday for scheduling event alarms.	None
Begin 00:00	Set the start time of the event alarm.	00:00
Duration 00:00	Set the duration for the event alarm to be active.	00:00

NOTE	Administrators can use the following steps to set up an event schedule:
	1. Select Event Type
	2. Enable "Event Alarms are active based on weekly schedule"
	3. Select the weekday
	4. Set the start time
	5. Set the duration this event will be active.
	6. Save

Event Alarm

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

Alarm Type	Triggered Condition	Triggered Action
Video Motion Detection (VMD)	VMD 1 VMD 2 VMD 3	Email FTP HTTP Event Server
CGI Event	The CGI trigger message	Email FTP HTTP Event Server
Camera Tamper Event	Camera Tamper	Email FTP HTTP Event Server

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

Trigger Conditions and Actions

Trigger Condition	Trigger Action	HTTP Action Setting
VMD1	☐ Send snapshot image via E-mail ☐ Send snapshot image via FTP ☐ Send message via HTTP Event Servers	☐ Server1 ☐ Server2 ☐ Server3 ☐ Server4
VMD2	☐ Send snapshot image via E-mail ☐ Send snapshot image via FTP ☐ Send message via HTTP Event Servers	☐ Server1 ☐ Server2 ☐ Server3 ☐ Server4
VMD3	☐ Send snapshot image via E-mail ☐ Send snapshot image via FTP ☐ Send message via HTTP Event Servers	☐ Server1 ☐ Server2 ☐ Server3 ☐ Server4

Note: HTTP Action Setting allows the VPort sending the customized alarm messages to the HTTP Event Server when the event is triggered. Please 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 alert on the image when VMD is triggered	Enable or disable the "show the alert," which when enabled displays a red square frame on the video image of the VMD alarm notification	Disabled

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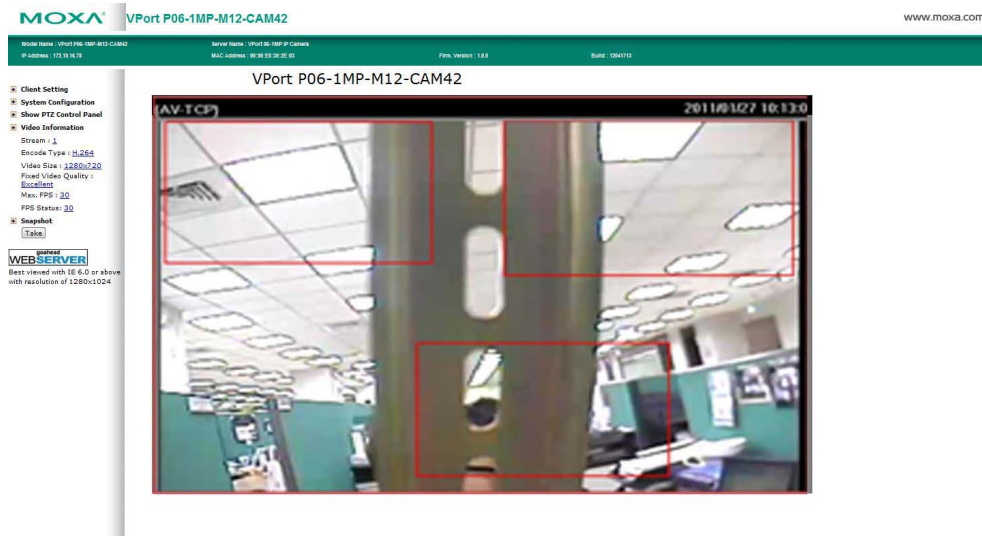
Setup a VMD Alarm

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

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

Trigger Conditions and Actions

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
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 on 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 on 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 on the Network/ HTTP Event Server page.	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 devices, to be the event alarms.

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

CGI Event

Enable CGI Event alarm
CGI Event Trigger Actions

Event Index	Trigger Action	HTTP Action Setting
Event 1	☐ Send snapshot image via E-mail ☐ Send snapshot image via FTP ☐ Send message via HTTP Event Servers	☐ Server1 ☐ Server2 ☐ Server3 ☐ Server4
Event 2	☐ Send snapshot image via E-mail ☐ Send snapshot image via FTP ☐ Send message via HTTP Event Servers	☐ Server1 ☐ Server2 ☐ Server3 ☐ Server4
Event 3	☐ Send snapshot image via E-mail ☐ Send snapshot image via FTP ☐ Send message via HTTP Event Servers	☐ Server1 ☐ Server2 ☐ Server3 ☐ Server4
Event 4	☐ Send snapshot image via E-mail ☐ Send snapshot image via FTP ☐ Send message via HTTP Event Servers	☐ Server1 ☐ Server2 ☐ Server3 ☐ Server4
Event 5	☐ Send snapshot image via E-mail ☐ Send snapshot image via FTP ☐ Send message via HTTP Event Servers	☐ Server1 ☐ Server2 ☐ Server3 ☐ Server4

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

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
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 entered on 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 is configured on 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 configured on the Network/ HTTP Event Server page.	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

Camera Tamper

The VPort P06-1MP-M12 supports a camera tamper function to detect malicious behavior, such as spray painting, view blocking, angle adjustment, etc. This page allows you to configure the parameters and alarm conditions/actions of the camera tamper alarm.

Camera Tamper

☐ Enable camera tamper alarm
☐ Show alert on the image when camper tamper is triggered
Trigger Conditions and Actions

Trigger Condition	Trigger Action	HTTP Action Setting
		☐ Server1 ☐ Server2 ☐ Server3 ☐ Server4
Camera Tamper Cover Area 30 Duration 5 Sec.	☐ Send snapshot image via E-mail ☐ Send snapshot image via FTP ☐ Send message via HTTP Event Servers	

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   Reset

Setting	Description	Default
Enable camera tamper alarm	Enable or disable the digital input alarm	Disabled
Show alert on the image when camper tamper is triggered	Determine whether or not the camera will display an onscreen warning square when the camera tamper alarm is triggered.	Not Displayed

Trigger Conditions

Setting	Description	Default
Cover Area	What percentage of the camera view should be affected before the camera tamper alarm is triggered.	30%
Duration	How long the camera tamper behavior should persist before the alarm is triggered.	5 sec

Trigger Actions

Setting	Description	Default
Send snapshot image via E-mail	Once this VMD is triggered, the VPort will send the snapshot images set on the Event Alarm/Basic page to the E-mail addresses, which are entered on the Network/ SMTP Server page.	Disabled
Send snapshot image via FTP	Once this VMD is triggered, the VPort will send the snapshot images set on the Event Alarm/Basic page to the FTP server, which is configured on 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 configured on the Network/ HTTP Event Server page.	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

A

Frequently Asked Questions

Q: **What if I forget my password?**

A: Every access to the IP camera needs authentication, unless the admin password is set 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 the IP camera is to utilize the **RESET** button to restore the factory settings (see Chapter 1 for details).

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

A: There are several possible reasons:
(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 working 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. Consult with 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 P06-1MP-M12 IP camera will allow 5 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 actual performance depends on several factors:
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 occurs
frequently. 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

Time Zone Table

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

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

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

C

Technical Specifications

Camera

Sensor: 1/2.7" HD progressive scan CMOS

Lens: 3.6, 4.2, 6 mm fixed focal length

Angle of View:

• 3.6 mm, F1.6: Diagonal 160°, Horizontal 100°, Vertical 71°

• 4.2 mm, F1.8: Diagonal 97°, Horizontal 80°, Vertical 58°

• 6.0 mm, F1.8: Diagonal 83°, Horizontal 65°, Vertical 51°

Camera Angle: Pan: ±30°; Tilt: 0-90°, Rotate: ±180°

Illumination (low light sensitvity): 0.2 Lux at F=1.2

Synchronization: Internal

White Balance: ATW/AWB (range: 3200 to 10000°K)

Auto Electronic Shutter: 1/30 to 1/25000 sec

Electronic Shutter: Auto

S/N Ratio: 50 dB (Gamma, Aperture, AGC, OFF; DNR ON)

DNR: Built-in DNR

WDR: Level 1-8

AGC control: 2X, 4X, 8X, 16X, 32X, 64X

Flickerless Control: Automatic/50 Hz/60 Hz mode

Black Level Control: High/Medium/Low

Auto Exposure: Level ±5

Image Rotation: Flip, Mirror, and 180° rotation

Image Setting: Manual tuning with saturation, sharpness, and contrast

Video

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

Video Outputs: Via Ethernet

Video Streams: Maximum of 3 video streams

• Stream 1: H.264, 1280 x 800 resolution (max.)

• Stream 2: H.264, 720 x 576 resolution (max.)

• Stream 3: MJPEG, 720 x 576 resolution (max.)

Note: Streams 2 and 3 must be set to the same resolution

Video Resolution and FPS (frames per second):

	NTSC		PAL	
	Size	Max. FPS	Size	Max. FPS
QCIF	176 x 112	30	176 x 144	25
CIF	352 x 240	30	352 x 288	25
VGA	640 x 480	30	640 x 480	25
4CIF	704 x 480	30	704 x 576	25
Full D1	720 x 480	30	720 x 576	25
SVGA	800 x 600	30	800 x 600	25
HD	1280x720	30	1280x720	25
WXGA	1280x800	30	1280x800	25

Video Viewing:

• DynaStream™ supported for automatic frame rate adjustment

• 3 privacy mask areas configurable

• Adjustable image size and quality

• Timestamp and text overlay

• OSD (On screen Display) position adjustable

• Maximum of 5 simultaneous unicast connections

• Digital PTZ with 4x zoom

Audio

Audio Inputs: 1, Line-in, rugged RCA connector

Audio Format: Mono, PCM (G.711)

Network

Protocols: TCP/IP, UDP, HTTP, SMTP, NTP, DNS, DHCP, UPnP, RTP, RTSP, ICMP, QoS,IGMPv3, SNMPv1/v2c/v3, DDNS, TFTP, ARP, DHCP, OPT66/67

Ethernet: 1 10/100BaseT(X) Ethernet port, 4-pin M12 A-code connector

Power Requirements

Input: Power-over-Ethernet (IEEE 802.3af)

Physical Characteristics

Housing: IP66 rain and dust protection, EN 62262 IK8 vandal-proof protection

Dimensions: 110 mm (diameter) x 47 mm (height)

Installation: Surface mounting

Security

Password: User level password protection

Filtering: By IP address

Encryption: HTTPS, SSH

Alarms

Intelligent Video: Camera tamper

Video Motion Detection: 3 independently configurable motion areas

Scheduling: Daily repeat timing schedule

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

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

Custom Alarms: HTTP event servers for setting customized alarm actions

Pre-alarm Buffer: 12 MB video buffer for JPEG snapshot images

Environmental Limits

Operating Temperature:

Standard model: -25 to 55°C (-13 to 131°F)

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

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

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

Conformal Coating: Available on request

Standards and Certifications

Safety: UL 60950-1

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

Rolling Stock: EN 50155:2007 compliance (shock, vibration, temperature, EMC)

Shock: IEC 61373

Freefall: IEC 60068-2-32

Vibration: IEC 61373

Vandal Resistance: EN 62262, IK8 level

Note: Please check Moxa's website for the most up-to-date certification status.

Warranty

Warranty Period: 5 years

Details: See www.moxa.com/warranty

Minimum Viewing System Requirements

CPU: Pentium 4, 2.4 GHz

Memory: 512 MB of memory

OS: Windows XP with SP3 or above, Windows 7

Browser: Internet Explorer 6.x or above

Multimedia: DirectX 9.0c or above

Software Development Kit

VPort SDK PLUS: Includes CGI commands, ActiveX Control, and API library for customized applications or system integration for third-party developers (the latest version of SDK is vailable for download from Moxa's website).

Standard: ONVIF