Moxa VPort P06HC-1V Series
Software User's Manual

Version 1.0, September 2021

www.moxa.com/product

Moxa VPort P06HC-1V Series Software User's Manual

Copyright Notice

Trademarks

Disclaimer

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

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

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

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

Technical Support Contact Information

www.moxa.com/support

Moxa Americas

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

Moxa 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 IP camera, be sure to read the following instructions:

❒ 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.

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 operation of such devices is legal in your locality before installing this unit for surveillance purposes.

Table of Contents

1

Introduction

This software user's manual is designed for the VPort IP camera's ONVIF Profile S firmware.

The following topics are covered in this chapter:

- ❒ **Overview**
- ❒ **Version Information**

Overview

The ONVIF specification is an open standard protocol for communicating between IP-based security devices. An ONVIF profile is described by a fixed set of functionalities through a number of services that are provided by the ONVIF standard. ONVIF Profile S allows the ONVIF device and client to communicate information about the PTZ, audio and metadata streaming, and relay outputs.

VPort IP cameras with ONVIF Profile S compliance can work with most VMS software for building a complete IP surveillance system immediately, without needing to spend time integrating your hardware and software. ONVIF Profile S saves both time and resources when using VPort IP cameras with VMS software.

Version Information

The current version information is listed below:

- ONVIF Core specifications: V2.2
- ONVIF Test tool: 20.12

Patent: http://www.moxa.com/doc/operations/Moxa_Patent_Marking.pdf

2

Getting Started

This chapter includes information about how to get started with the VPort's software configuration.

The following topics are covered in this chapter:

❒ **Introduction**

❒ **Software Installation**

Introduction

In what follows, "user" refers to those who can access the IP camera, and "administrator" refers to the person who knows the root password that allows changes to the IP camera's configuration and has the right to assign general access to other users. Administrators should read this part of the manual carefully, especially during installation.

Software Installation

Step 1: Configure the VPort's IP address

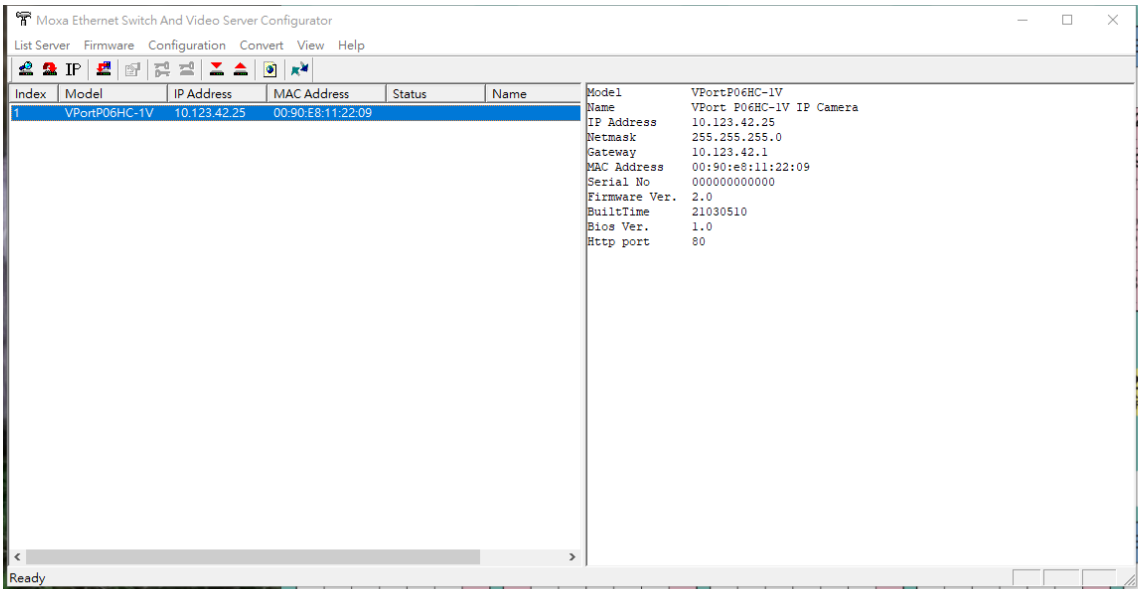
When the VPort is first powered on, the POST (Power On Self Test) will run for about 40 to 60 seconds. The network environment determines how the IP address is assigned.

Network environments with a DHCP server

In this case, 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 EtherDevice 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, Model Name, MAC address, IP address, serial number, firmware/BIOS version, and HTTP port of the VPort will be listed in the utility's window.



Index	Model	IP Address	MAC Address	Status	Name
1	VPortP06HC-1V	10.123.42.25	00:90:E8:11:22:09		

```
Model          VPortP06HC-1V
Name           VPort P06HC-1V IP Camera
IP Address     10.123.42.25
Netmask        255.255.255.0
Gateway        10.123.42.1
MAC Address    00:90:e8:11:22:09
Serial No      000000000000
Firmware Ver.  2.0
BuiltTime      21030510
Bios Ver.      1.0
Http port      80
```

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

Network environments that do NOT have a DHCP server

If your VPort 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 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.

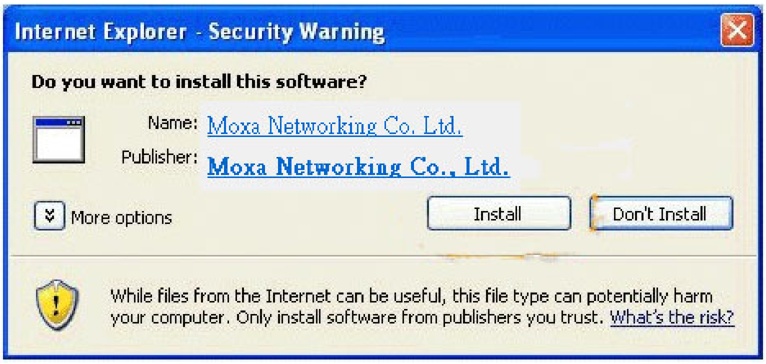
To change the IP address of the VPort manually, access the VPort's web server, and then navigate to the **System Configuration** → **Network** → **General** page to configure the IP address and other network settings. Checkmark **Use fixed IP address** to ensure that the IP address you assign is not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

Step 2: Access the VPort's web-based manager

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

Step 3: Install the ActiveX Control plug-in

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



Internet Explorer - Security Warning

Do you want to install this software?

Name: Moxa Networking Co. Ltd.

Publisher: Moxa Networking Co., Ltd.

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

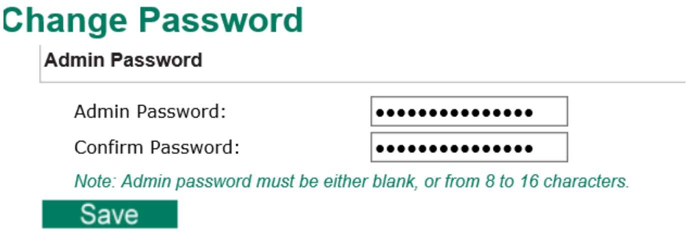
NOTE For Windows XP SP2 or above operating systems, the ActiveX Control component will be blocked for system security reasons. In this case, the VPort's security warning message window may not appear. Unlock the ActiveX control blocked function or disable the security configuration so that you can install the VPort's ActiveX Control component.

Step 4: Configure authentication for accessing the VPorts web -based manager.

When accessing the VPort's web-based manger, authentication is required. The default administrator account name is "admin" and the default password is "moxamoxa". After accessing the camera using the default admin password, you will need to change the password for security reasons. The default admin password (moxamoxa) can only be used once.

- For first-time web access, use the following login settings:
  > account name: admin
  > password: moxamoxa.
- You are required to change the password the first time you access the admin account.

If you log out and then log in without changing the password, the Change Password dialog will open, and you will not be able to get past this dialog without changing the password.



Change Password

Admin Password

Admin Password: ●●●●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●●●●

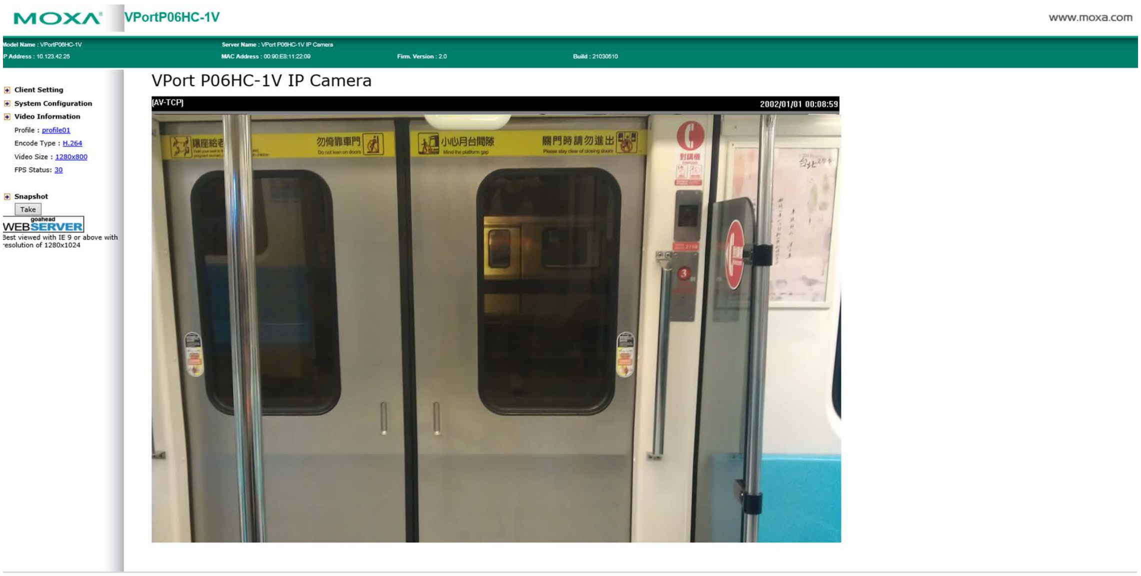
Note: Admin password must be either blank, or from 8 to 16 characters.

NOTE For network security reasons, do not lose the new admin password. If you lose the password, you will need to send the VPort back to Moxa for repair. ***Note that you will be assessed a repair charge for this service.***

Step 5: Access the homepage of the VPort camera's web-based manager

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

1. Video Images
2. Video Information



VPortP06HC-1V www.moxa.com

odel Name : VPortP06HC-1V Server Name : VPort P06HC-1V IP Camera
P Address : 10.123.42.25 MAC Address : 00:90:E8:11:22:09 Firm. Version : 2.0 Build : 21030510

VPort P06HC-1V IP Camera

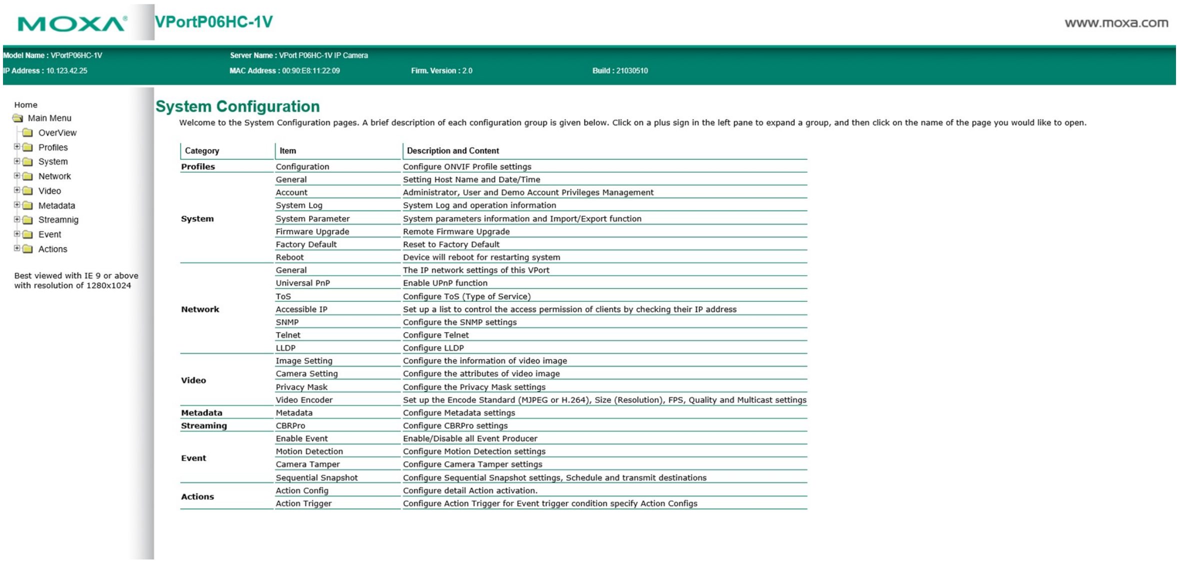
[AV-TCP] 2002/01/01 00:08:59

Profile : profile01
Encode Type : H.264
Video Size : 1280x800
FPS Status: 30

Best viewed with IE 9 or above with resolution of 1280x1024

Step 5: Access the VPort's system configuration

Click on **System Configuration** to access the system configuration overview 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.



VPortP06HC-1V www.moxa.com

Model Name : VPortP06HC-1V Server Name : VPort P06HC-1V IP Camera
IP Address : 10.123.42.25 MAC Address : 00:90:E8:11:22:09 Firm. Version : 2.0 Build : 21030510

Best viewed with IE 9 or above with resolution of 1280x1024

System Configuration

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

Category	Item	Description and Content
Profiles	Configuration	Configure ONVIF Profile settings
System	General	Setting Host Name and Date/Time
	Account	Administrator, User and Demo Account Privileges Management
	System Log	System Log and operation information
	System Parameter	System parameters information and Import/Export function
	Firmware Upgrade	Remote Firmware Upgrade
	Factory Default	Reset to Factory Default
	Reboot	Device will reboot for restarting system
Network	General	The IP network settings of this VPort
	Universal PnP	Enable UPnP function
	ToS	Configure ToS (Type of Service)
	Accessible IP	Set up a list to control the access permission of clients by checking their IP address
	SNMP	Configure the SNMP settings
	Telnet	Configure Telnet
	LLDP	Configure LLDP
Video	Image Setting	Configure the information of video image
	Camera Setting	Configure the attributes of video image
	Privacy Mask	Configure the Privacy Mask settings
	Video Encoder	Set up the Encode Standard (MJPEG or H.264), Size (Resolution), FPS, Quality and Multicast settings
Metadata	Metadata	Configure Metadata settings
Streaming	CBRPro	Configure CBRPro settings
Event	Enable Event	Enable/Disable all Event Producer
	Motion Detection	Configure Motion Detection settings
	Camera Tamper	Configure Camera Tamper settings
	Sequential Snapshot	Configure Sequential Snapshot settings, Schedule and transmit destinations
Actions	Action Config	Configure detail Action activation.
	Action Trigger	Configure Action Trigger for Event trigger condition specify Action Configs

3

Accessing the VPort's Web-based Manager

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

The following topics are covered in this chapter:

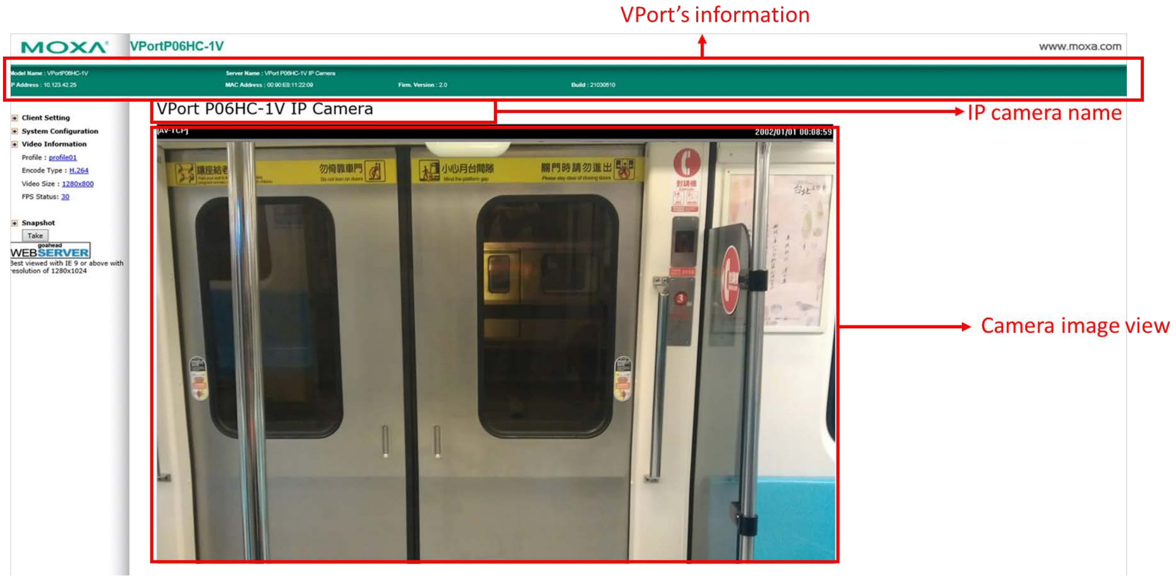
❒ **Functions Featured on the VPort's Web Homepage**

- ➢ VPort's Information
- ➢ IP Camera Name
- ➢ Camera Image View
- ➢ Client Settings
- ➢ System Configuration
- ➢ Video Information
- ➢ 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 best screen resolution for viewing VPort's web homepage depends on the resolution of the camera image. For example, if the camera image can be viewed at resolutions up to HD (1280 x 720), the screen resolution should be 1280 x 1024. We strongly recommend using IE 9.0 (Microsoft Internet Explorer) or above to avoid incompatibility with the ActiveX Plug-in.


VPortP06HC-1V

Model Name : VPortP06HC-1V
Server Name : VPort P06HC-1V IP Camera
IP Address : 10.123.42.25
MAC Address : 00:90:E8:11:22:09
Firm. Version : 2.0
Build : 21030510

VPort P06HC-1V IP Camera

Client Setting
System Configuration
Video Information
Profile : profile01
Encode Type : H.264
Video Size : 1280x800
FPS Status: 30

Snapshot
Take

Best viewed with IE 9 or above with resolution of 1280x1024

VPort's Information

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

IP Camera Name

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

Camera Image View

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

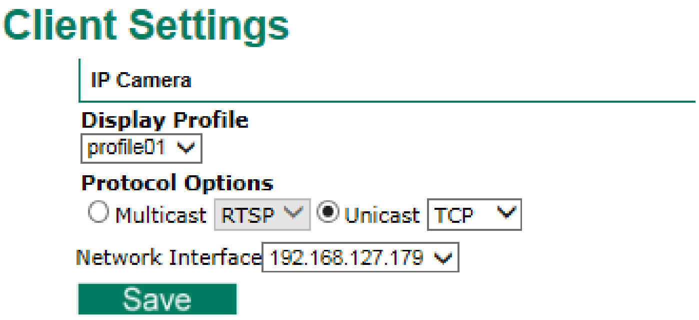
Client Settings

The following functions can be configured in **Client Settings**.

1. **Display profile:** Shows the profile currently being used. There are 3 default profiles: profile01, profile02, profile03. Each profile refers to one independent video stream with a unique codecs, resolution, frame rate (FPS), and video quality. If you need to, you can create additional profiles, but keep in mind that more profiles mean more video streams. Enabling too many video streams could reduce the frame rate and overall video performance of each stream. For configuring the profile, go to **System Configuration/profile**.
2. **Protocol Options:** Choose one of four protocols to optimize your usage—Multicast (RTSP or Push) or Unicast (UDP, TCP, HTTP).
   - **Multicast Protocol** can be used to send a single video stream to multiple clients. In this case, a lot of bandwidth can be saved since only one video stream is transmitted over the network. However, the network gateway (e.g., a switch) must support the multicast protocol (e.g., IGMP snooping). Otherwise, the multicast video transmission will not be successful.
     - **RTSP:** Enable the multicast video stream to be sent using RTSP control, which means the multicast video stream will be sent only if it receives the client's request.
     - **Push:** Enable the multicast video stream to be sent using Push control, which means that after this setting is selected, the multicast video stream will be sent continuously even without any client requests.
   - **Unicast Protocol** is used to send a single video stream to one client.
     - **UDP** can be used to produce audio and video streams that are more real-time. However, some packets may be lost due to network burst traffic, and images may become blurred.
     - **TCP** can be used to prevent packet loss, which results in a more accurate video display. The downside of using TCP is that the real-time delay is worse than with UDP protocol.
     - **HTTP** can be used to prevent being blocked by a router's firewall. The downside of using HTTP is that the real-time delay is worse than with UDP protocol.
   - **Network Interface** designates the connection interface for multicast video streams selection. The box lists the current NIC interfaces. Select which NIC interface will receive multicast streams.

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

NOTE For multicast video stream settings, see **System Configuration → Network → Multicast**.



Client Settings

IP Camera

Display Profile
profile01

Protocol Options
○ Multicast RTSP ● Unicast TCP

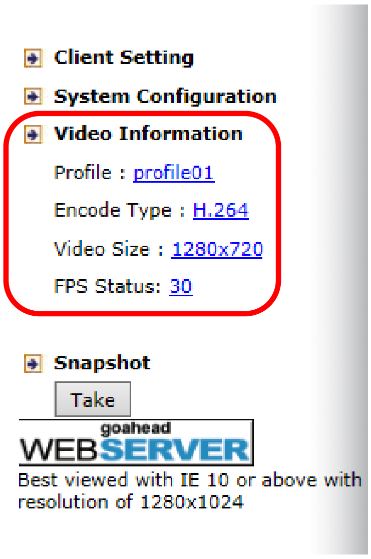
Network Interface 192.168.127.179

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

You can easily monitor the current video performance by looking at the **Video Information** section on the left side of the homepage. The following properties are shown: Profile, Encoder type, Video Size, and FPS status. (Some models also include Display FPS and Process FPS. Display FPS means the FPS of live video displayed by computer, and Process FPS means the FPS provided by the camera). For multichannel encoders, you can select the target camera image to view the camera's video performance.



Profile : profile01

Encode Type : H.264

Video Size : 1280x720

FPS Status: 30

Best viewed with IE 10 or above with resolution of 1280x1024

Snapshot

You can take snapshot images for storing, printing, and 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's settings. You can do this with the web console.

The following topics are covered in this chapter:

❐ **System Configuration by Web Console**

- Profiles
- System
- Network
- Video
- Metadata
- Streaming
- Event
- Actions

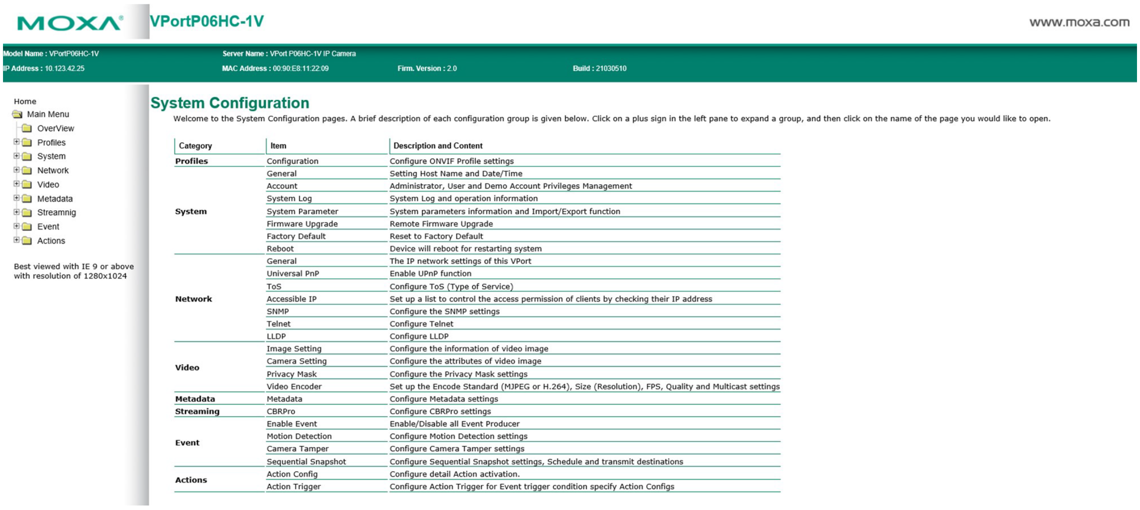
System Configuration by Web Console

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.

Each of the configuration categories—**Profiles, System, Network, Video, Metadata, Event, Action**—are described below:

Category	Item	Description and Contents
Profiles	Configuration	Configure ONVIF Profile settings
System	General	Set Server Name, Contact, and Location
	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	IP network settings of this VPort
	Universal PnP	Enable UPnP function
	ToS	Configure ToS (Type of Service)
	Accessible IP	Set up a list to control access permission of clients by IP address
	SNMP	Configure SNMP settings
	Telnet	Configure Telnet
	LLDP	Configure LLDP
Video	Image Settings	Configure video image information
	Camera Settings	Configure the camera's attributes
	Primacy mask	Configure the privacy mask settings
	Video Encoder	Set up the Encode Standard (MJPEG or H.264), Size (Resolution), FPS, Quality, and Multicast settings
Metadata	Metadata	Configure the stream metadata
Streaming	CBRPro	Configure CBR Pro settings
Event	Enable Event	Enable/Disable all Event Producer
	Motion Detection	Configure Motion Detection settings
	Camera Tamper	Configure Camera Tamper settings
	Sequential snapshot	Configure Sequential Snapshot settings, Schedule and transmit destinations
Action	Action Config	Configure detailed Action activation settings
	Action Trigger	Configure the Action Trigger for the Event trigger condition based on the specific Action Config chosen for this trigger.

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



Model Name : VPortP06HC-1V
Server Name : VPort P06HC-1V IP Camera
IP Address : 10.123.42.25
MAC Address : 00:90:E8:11:22:09
Firm. Version : 2.0
Build : 21030510

Best viewed with IE 9 or above with resolution of 1280x1024

System Configuration

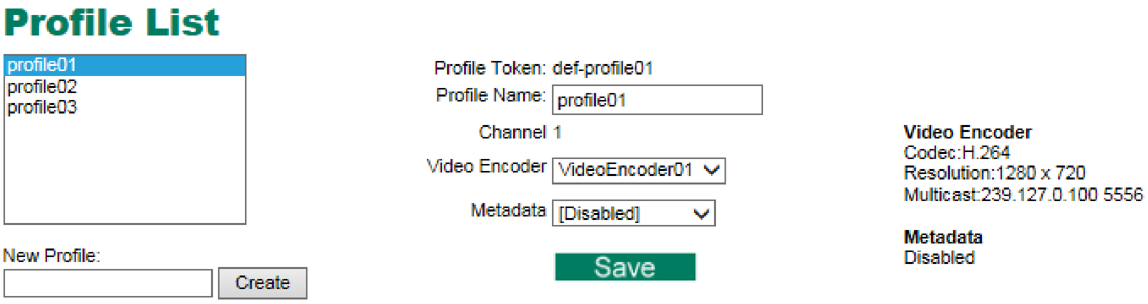
Welcome to the System Configuration pages. A brief description of each configuration group is given below. Click on a plus sign in the left pane to expand a group, and then click on the name of the page you would like to open.

Category	Item	Description and Content
Profiles	Configuration	Configure ONVIF Profile settings
System	General	Setting Host Name and Date/Time
	Account	Administrator, User and Demo Account Privileges Management
	System Log	System Log and operation information
	System Parameter	System parameters information and Import/Export function
	Firmware Upgrade	Remote Firmware Upgrade
	Factory Default	Reset to Factory Default
	Reboot	Device will reboot for restarting system
Network	General	The IP network settings of this VPort
	Universal PnP	Enable UPnP function
	ToS	Configure ToS (Type of Service)
	Accessible IP	Set up a list to control the access permission of clients by checking their IP address
	SNMP	Configure the SNMP settings
	Telnet	Configure Telnet
	LLDP	Configure LLDP
Video	Image Setting	Configure the information of video image
	Camera Setting	Configure the attributes of video image
	Privacy Mask	Configure the Privacy Mask settings
	Video Encoder	Set up the Encode Standard (MJPEG or H.264), Size (Resolution), FPS, Quality and Multicast settings
Metadata	Metadata	Configure Metadata settings
Streaming	CBRPro	Configure CBRPro settings
Event	Enable Event	Enable/Disable all Event Producer
	Motion Detection	Configure Motion Detection settings
	Camera Tamper	Configure Camera Tamper settings
	Sequential Snapshot	Configure Sequential Snapshot settings, Schedule and transmit destinations
Actions	Action Config	Configure detail Action activation.
	Action Trigger	Configure Action Trigger for Event trigger condition specify Action Configs

Profiles

In the ONVIF Profiles specifications, one video profile represents one video stream, which can have a unique codecs (H.264), resolution, FPS (frame rate), and video quality.

Configuration



Profile List

profile01
profile02
profile03

New Profile:

Profile Token: def-profile01
Profile Name: profile01
Channel 1
Video Encoder VideoEncoder01
Metadata [Disabled]

Video Encoder
Codec:H.264
Resolution:1280 x 720
Multicast:239.127.0.100 5556

Metadata
Disabled

Profile List

Setting	Description	Default
profile01 profile02 profile03	Chose the video profile. Profile information shown on this page includes Profile Token, Profile Name, Channel number, Video encoder, Audio Encoder	profile01

Profile Information

Setting	Description	Default
Profile Token*	Reply when queried by another device asks	<variable>
Profile Name	Configure the profile name, max. 40 bytes	profile01
Channel*	Current video channel of this ONVIF device	<variable>
Video Encoder	Select which video encoder this profile will use	VideoEncoder01
Metadata	Enable or disable the metadata being used with the profiles	metadataCfg01

***This item cannot be edited.**

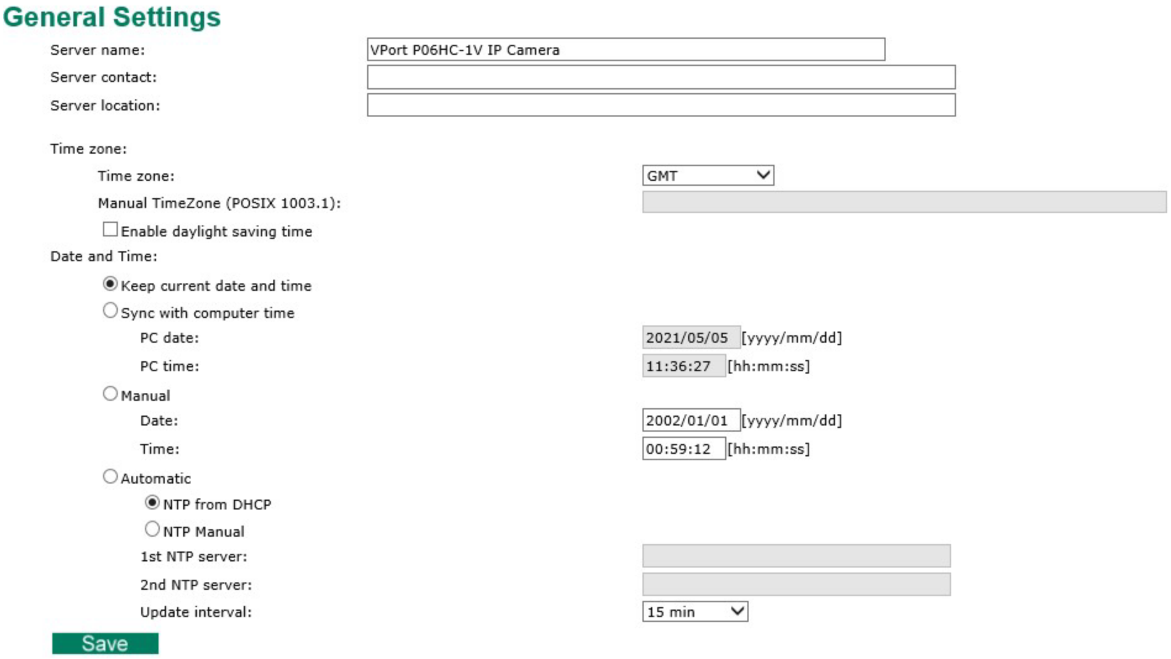
New Profile

You can create additional profiles if needed. Input the name of the new profile and then click **Create**. A maximum of 8 profiles can be created. When the new profile appears in the Profile List, select the new profile and then configure its video encoder and audio encoder to generate the video streams. Click **Save** to save the new profile. To remove a profile, select the profile you wish to remove, and then click **Remove**.

System

General Settings

On the **General Settings** page, administrators can set up the IP camera **Server name** and the **Date and Time**, which is included in the caption of all images.



General Settings

Server name: VPort P06HC-1V IP Camera

Server contact:

Server location:

Time zone:

Time zone: GMT

Manual TimeZone (POSIX 1003.1):

□ Enable daylight saving time

Date and Time:

● Keep current date and time

○ Sync with computer time

PC date: 2021/05/05 [yyyy/mm/dd]

PC time: 11:36:27 [hh:mm:ss]

○ Manual

Date: 2002/01/01 [yyyy/mm/dd]

Time: 00:59:12 [hh:mm:ss]

○ Automatic

● NTP from DHCP

○ NTP Manual

1st NTP server:

2nd NTP server:

Update interval: 15 min

Server name

Setting	Description	Default
Max. 40 characters	Use a different server name for each server to help identify your servers. The name appears on the web homepage.	VPort P06HC-1V IP camera

Server contact

Setting	Description	Default
Max. 40 characters	Input the name of the operator who is responsible for this camera server	Blank

Server location

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

Time zone

Setting	Description	Default
Time Zone	Configure the time zone	GMT
Manual Time Zone (POSIX 1003.1):	Manually configure the specified time zone. To enable this configuration, select **manual setting** from the Time Zone drop-down box	Blank
Enable daylight saving time	Enable/disable daylight saving time (Only for Manual Time Zone settings)	Disable

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 to set the VPort's date and time setting	

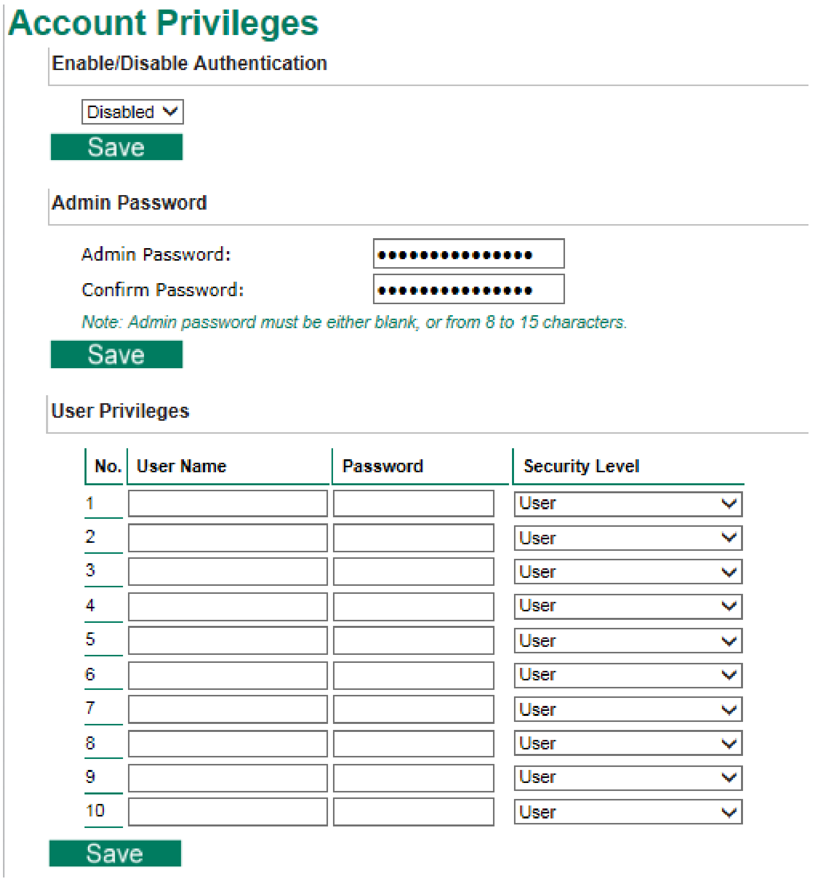
NOTE Select the **Automatic** option to force the VPort to synchronize automatically with timeservers over the Internet. However, synchronization may fail if the assigned **NTP server** cannot be reached, or the VPort is connected to a local network. Enter either the Domain name or IP address format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

You can configure two NTP servers as backups; the update interval can be configured from a minimum of 5 seconds up 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

Different account privileges are available for different purposes.



Account Privileges

Enable/Disable Authentication

Disabled

Save

Admin Password

Admin Password: •••••••••••••••

Confirm Password: •••••••••••••••

Note: Admin password must be either blank, or from 8 to 15 characters.

Save

User Privileges

No.	User Name	Password	Security Level
1			User
2			User
3			User
4			User
5			User
6			User
7			User
8			User
9			User
10			User

Save

Authentication Enable

Setting	Description	Default
Authentication Enable	Enable/disable the account protection of web-based manager access	disabled

Admin password

Setting	Description	Default
Admin Password (8 to 16 characters)	Input the administrator password	moxamoxa
Confirm Password (8 to 16 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.

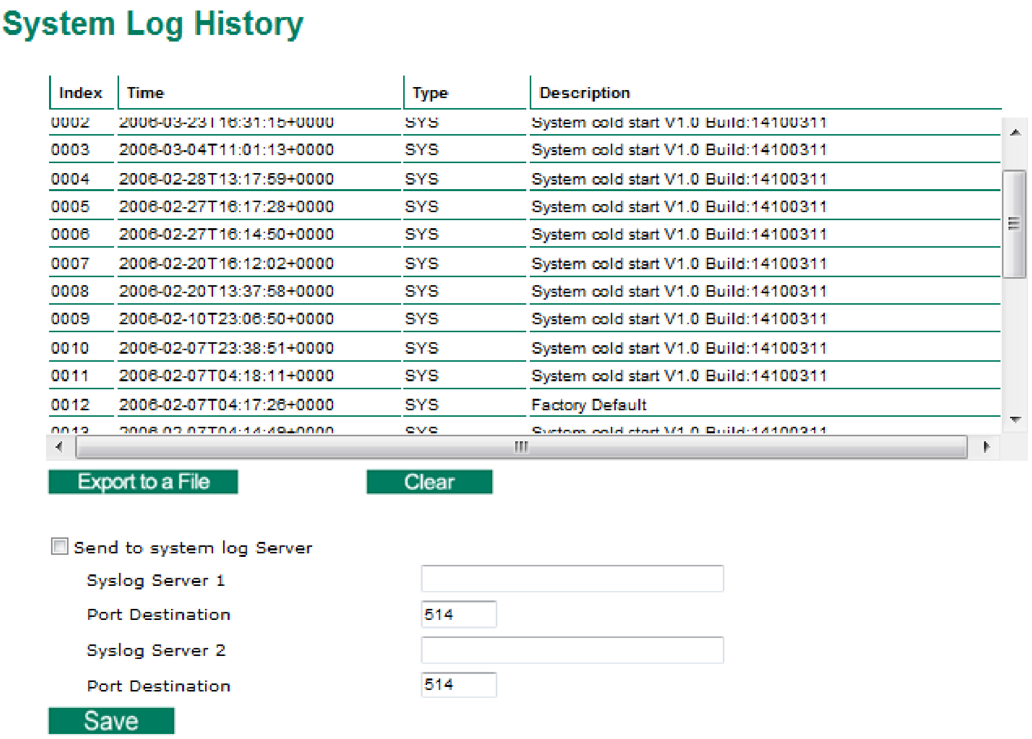
User's Privileges

Setting	Description	Default
User name	Type a specific user name for user authentication.	None
Password	Type a specific password for user authentication.	
Security Level	You may select from 4 ONVIF roles: Administrator, Operator, User, and Anonymous. **We do not recommend using the Anonymous role due to security issues.** Different roles have different privileges. Refer to ONVIF Specifications for the user's access policy.	User

NOTE The FPS of the video stream will be reduced as more and more users access the same VPort. Currently, the VPort camera is only allowed to send 10 unicast video streams. To avoid performance problems, limit the number of users who can simultaneously access a VPort camera.

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. In addition, the log can also be sent to a **Log Server** for backup. The administrator can configure "Syslog Server 1" and "Syslog Server 2" below the system log list.



System Log History

Index	Time	Type	Description
0002	2006-03-23T16:31:15+0000	SYS	System cold start V1.0 Build:14100311
0003	2006-03-04T11:01:13+0000	SYS	System cold start V1.0 Build:14100311
0004	2006-02-28T13:17:59+0000	SYS	System cold start V1.0 Build:14100311
0005	2006-02-27T16:17:28+0000	SYS	System cold start V1.0 Build:14100311
0006	2006-02-27T16:14:50+0000	SYS	System cold start V1.0 Build:14100311
0007	2006-02-20T16:12:02+0000	SYS	System cold start V1.0 Build:14100311
0008	2006-02-20T13:37:58+0000	SYS	System cold start V1.0 Build:14100311
0009	2006-02-10T23:06:50+0000	SYS	System cold start V1.0 Build:14100311
0010	2006-02-07T23:38:51+0000	SYS	System cold start V1.0 Build:14100311
0011	2006-02-07T04:18:11+0000	SYS	System cold start V1.0 Build:14100311
0012	2006-02-07T04:17:26+0000	SYS	Factory Default
0013	2006-02-07T04:14:49+0000	SYS	System cold start V1.0 Build:14100311

☐ Send to system log Server

Syslog Server 1	
Port Destination	514
Syslog Server 2	
Port Destination	514

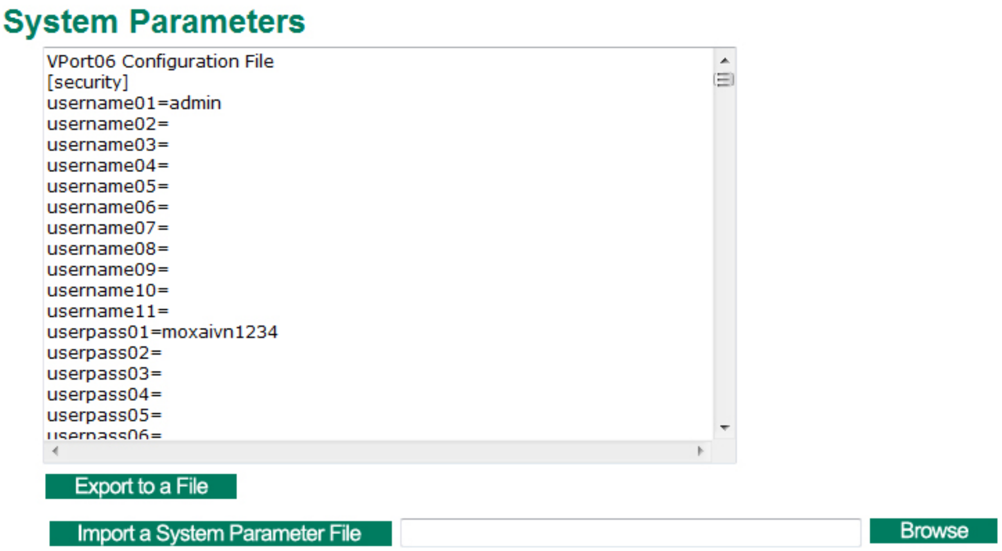
Send to system log Server

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

NOTE A maximum of 500 lines is displayed in the log. Earlier log entries are stored in the VPort's database, which the administrator can export 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.

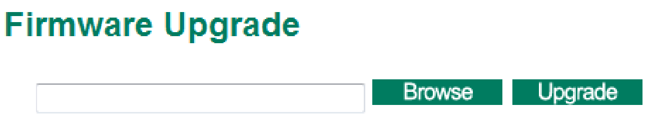


System Parameters

```
VPort06 Configuration File
[security]
username01=admin
username02=
username03=
username04=
username05=
username06=
username07=
username08=
username09=
username10=
username11=
userpass01=moxaivn1234
userpass02=
userpass03=
userpass04=
userpass05=
userpass06=
```

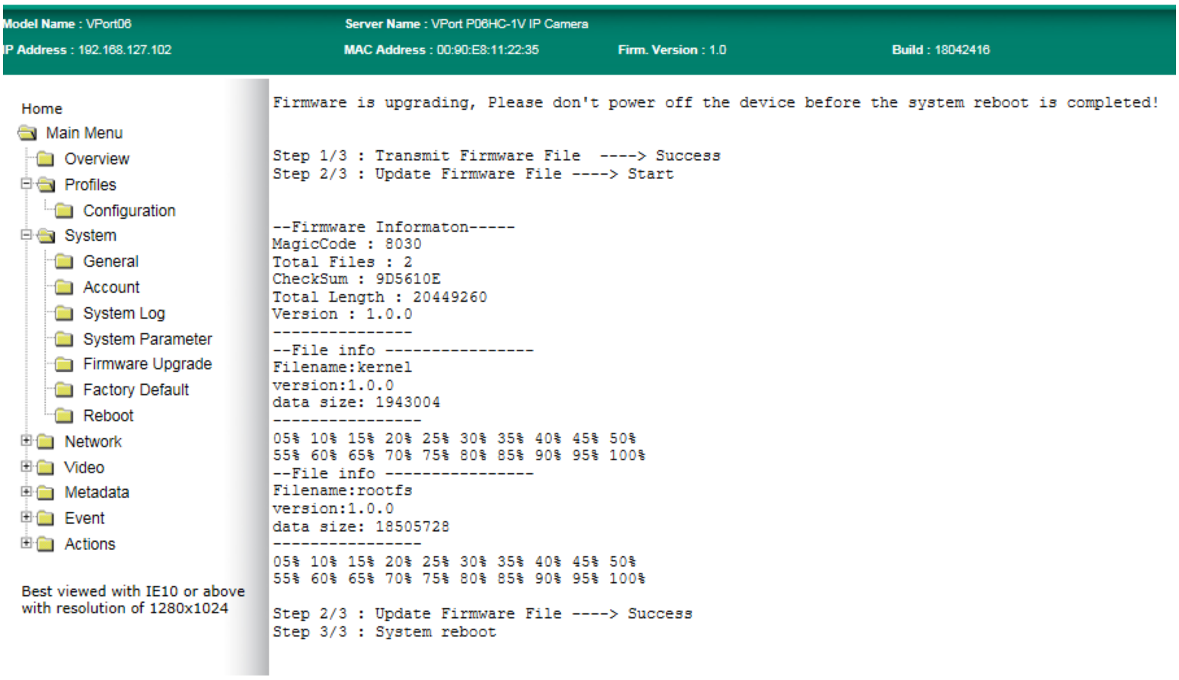
NOTE The system parameter import/export functions allow the administrator to back up and restore system configurations. The Administrator can export this sys_config.ini file (in a special binary format) for backup, and import the sys_config.ini file to restore the system configurations of VPort IP cameras.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

Firmware Upgrade



Take the following steps to upgrade the firmware:

Step 1: Press the **Browse** button to select the firmware file.
Step 2: Click on the **Upgrade** button to upload the firmware to the VPort.
Step 3: The system will start the firmware upgrade process.
Step 4: Once **Success .....Step 3/3 : System reboot** is displayed, wait 30 seconds for the VPort to reboot.



odel Name : VPort06 Server Name : VPort P06HC-1V IP Camera
P Address : 192.168.127.102 MAC Address : 00:90:E8:11:22:35 Firm. Version : 1.0 Build : 18042416

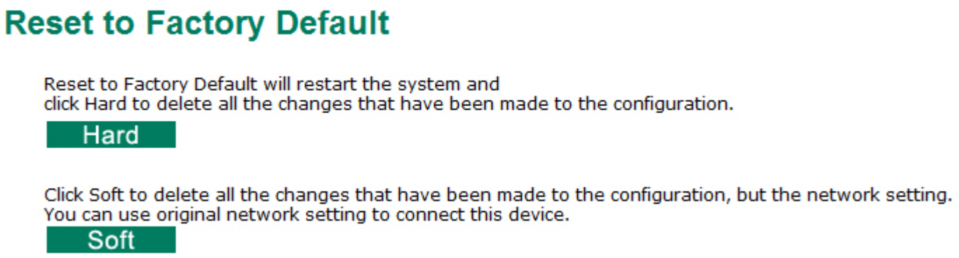
```
Firmware is upgrading, Please don't power off the device before the system reboot is completed!


Step 1/3 : Transmit Firmware File  ----> Success
Step 2/3 : Update Firmware File ----> Start


--Firmware Informaton-----
MagicCode : 8030
Total Files : 2
CheckSum : 9D5610E
Total Length : 20449260
Version : 1.0.0
---------------
--File info ---------------
Filename:kernel
version:1.0.0
data size: 1943004
---------------
05% 10% 15% 20% 25% 30% 35% 40% 45% 50%
55% 60% 65% 70% 75% 80% 85% 90% 95% 100%
--File info ---------------
Filename:rootfs
version:1.0.0
data size: 18505728
---------------
05% 10% 15% 20% 25% 30% 35% 40% 45% 50%
55% 60% 65% 70% 75% 80% 85% 90% 95% 100%

Step 2/3 : Update Firmware File ----> Success
Step 3/3 : System reboot
```

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

NOTE Upgrading the firmware will not change most of the original settings.

Reset to Factory Default

From the “Reset to Factory Default” page, choose **Hard** or **Soft** factory default to reset the VPort to its factory default settings.



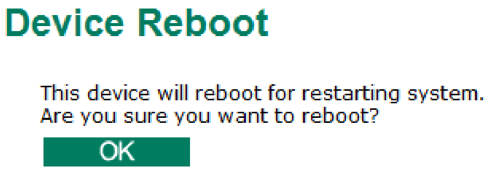
Reset to Factory Default will restart the system and
click Hard to delete all the changes that have been made to the configuration.

Click Soft to delete all the changes that have been made to the configuration, but the network setting.
You can use original network setting to connect this device.

NOTE Only some VPorts support the hardware reset button. Refer to your product’s QIG for operation instructions.

Reboot

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



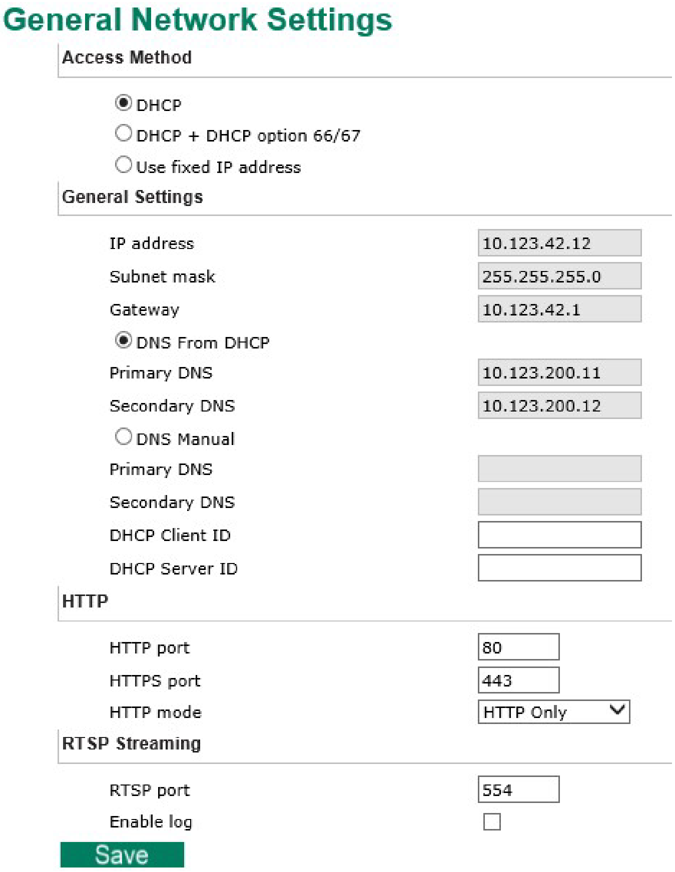
Device Reboot

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

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 + DHCP option 66/67
○ Use fixed IP address

General Settings

IP address	10.123.42.12
Subnet mask	255.255.255.0
Gateway	10.123.42.1
● DNS From DHCP	
Primary DNS	10.123.200.11
Secondary DNS	10.123.200.12
○ DNS Manual	
Primary DNS	
Secondary DNS	
DHCP Client ID	
DHCP Server ID	

HTTP

HTTP port	80
HTTPS port	443
HTTP mode	HTTP Only

RTSP Streaming

RTSP port	554
Enable log	□

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 + DHCP Option 66/67	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.	

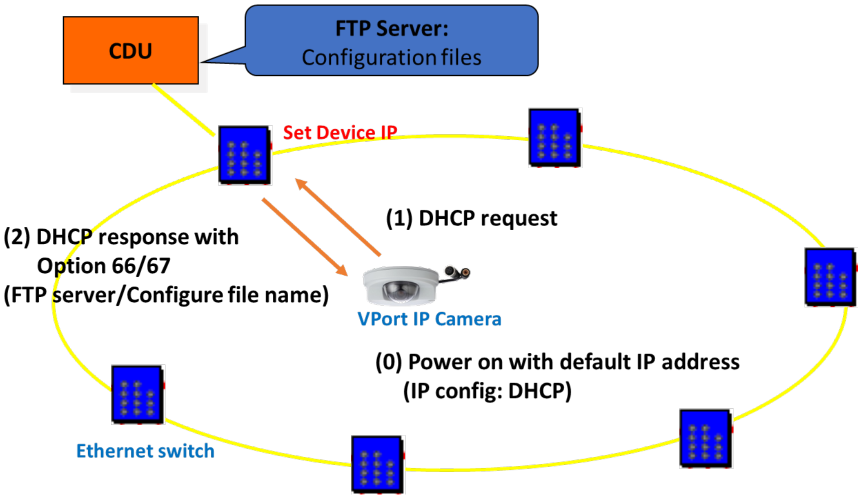
NOTE We strongly recommend that the administrator assign a fixed IP address to the VPort, since all of the functions and applications provided by the VPort are active when the VPort is connected to the network. Use DHCP to determine if the VPort's IP address may change when then network environment changes,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

DHCP Option 66/67 for auto configuration

If you need to install a large number of devices, it can be extremely time consuming to configure each of the many devices one by one. DHCP Opt 66/67 provides a mechanism whereby configurations can be saved on a TFTP server, and then once a new device is installed, the configurations can be downloaded to this new device automatically. Follow the steps below to use the Opt 66/67 auto-configuration function. We use VPort 16-M12 to illustrate.

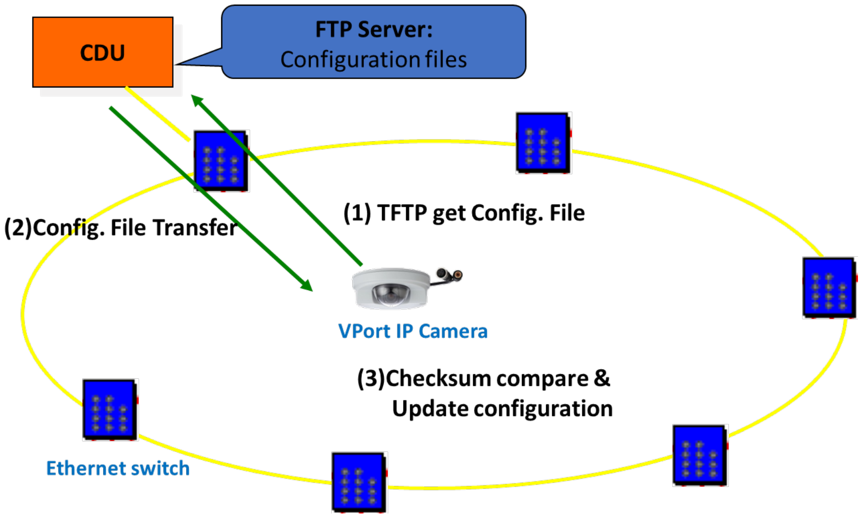
Step 1:

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



Step 2:

Once the VPort camera completes the IP settings, it will acquire the configuration file from the TFTP server, and then check if this configuration file is the right one 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
DNS from DHCP	The DNS server is assigned by DHCP server	Enable
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.
DHCP Client ID	Configure the DHCP Client ID if it is required	Blank
DHCP Server ID	Configure the DHCP Server ID if it is required	Blank

HTTP

Setting	Description	Default
HTTP port (80, or 1024 to 65535)	HTTP port enables connecting the VPort to the web.	80
HTTPS port	HTTPS port enables HTTPS encryption	443
HTTP mode	Configure HTTP mode to HTTP only, or HTTP+HTTPS	HTTP only

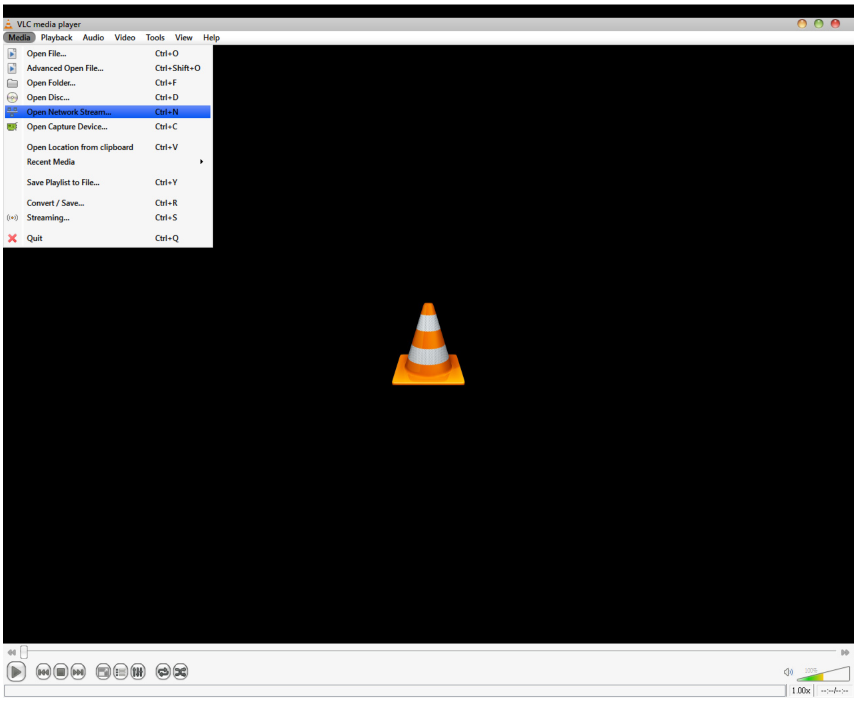
RTSP Streaming

The VPort 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 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
Enable log	Enable allowing the RTSP streaming status to be recorded to the system log.	Disable

The VLC media player is used here as an example of an RTSP streaming application:

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


VLC media player
Media Playback Audio Video Tools View Help
Open File... Ctrl+O
Advanced Open File... Ctrl+Shift+O
Open Folder... Ctrl+F
Open Disc... Ctrl+D
Open Network Stream... Ctrl+N
Open Capture Device... Ctrl+C
Open Location from clipboard Ctrl+V
Recent Media
Save Playlist to File... Ctrl+Y
Convert / Save... Ctrl+R
Streaming... Ctrl+S
Quit Ctrl+Q
1.00x

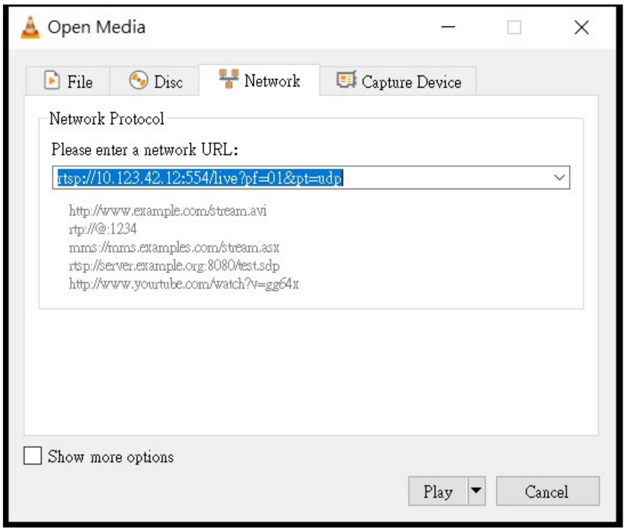
Step 2: When the following pop-up window appears, type the URL in the input box. E.g., type

rtsp://<VPort's IP address>[:<RTSP Port]/live?pf=<profile ID>&pt=udp

rtsp://<VPort's IP address>[:<RTSP Port]/live?pf=<profile ID>&pt=multicast

RTSP Port: 554 (the default),

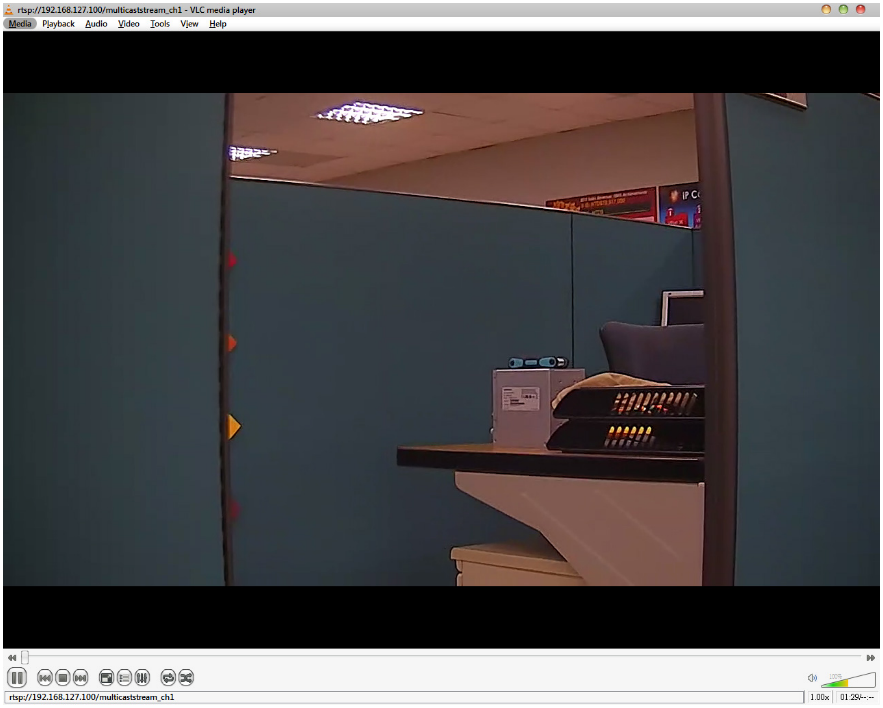
and then click **OK** to connect to the VPort.


Open Media
File
Disc
Network
Capture Device
Network Protocol
http://www.example.com/stream.avi
rtp://@:1234
mms://mms.examples.com/stream.asx
rtsp://server.example.org:8080/test.sdp
http://www.yourtube.com/watch?v=gg64x
□ Show more options
Play
Cancel

Please enter a network URL: rtsp://10.123.42.12:554/live?pf=01&pt=udp

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

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


rtsp://192.168.127.100/multicaststream_ch1 - VLC media player
Media
Playback
Audio
Video
Tools
View
Help
100%
rtsp://192.168.127.100/multicaststream_ch1
1.00x
01:29/--:--

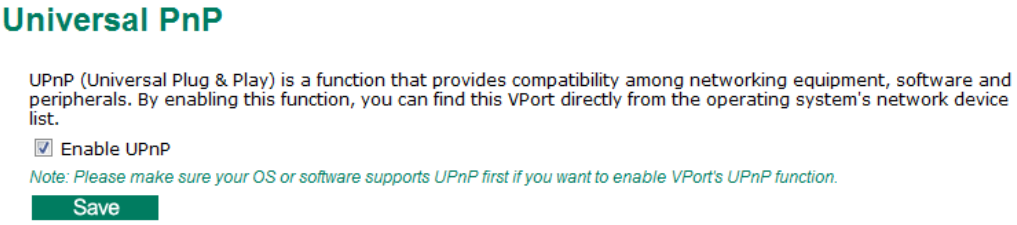
NOTE The video performance of the VPort may vary depending on the media players or on network performance. For example, you will notice a greater delay when viewing the VPort's live stream from the VLC player compared to viewing it directly from the VPort's home webpage. Also, additional delays could happen if viewing the VPort's live stream from the VLC player over a router or Internet gateway.

NOTE VPort's RTSP video/audio stream can be identified and viewed by both Apple QuickTime V. 6.5 or above and VLC media player. System integrators can use these two media players to view the 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. MJPEG does not support RTSP.

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

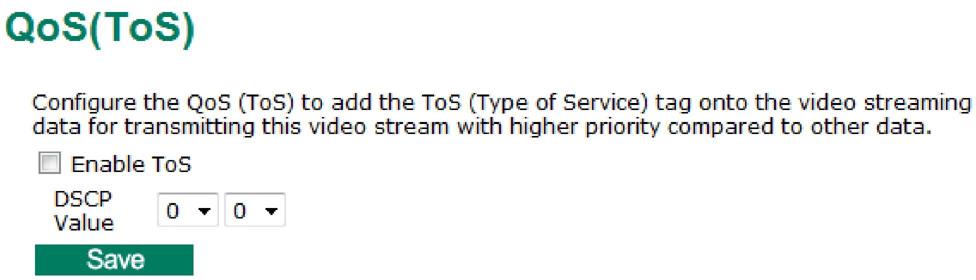
Note: Please make sure your OS or software supports UPnP first if you want to enable VPort's UPnP function.

Save

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

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

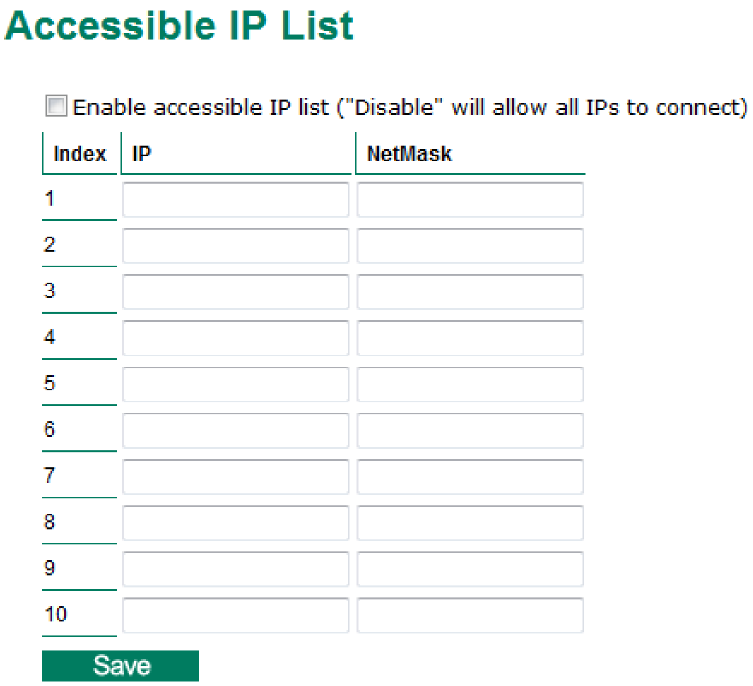
DSCP Value 0 0

Setting	Description	Factory Default
Enable ToS	Enable ToS to transmit the video stream with the given priority.	Disable
DSCP Value	Configure 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.

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		

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. In particular, an **IP** together with a **NetMask** is used to specify a range of IP addresses. Here are some examples:

- Allow only one host with a specific "IP address" to access the VPort. For example,
  IP = 192.168.1.16 NetMask = 255.255.255.255
  will only allow the host with IP = 192.168.1.16 to access the VPort.
- Allow all hosts on a specific subnet to access the VPort. For example:
  IP = 192.168.1.0 NetMask = 255.255.255.0
  will allow all hosts with IP addresses of the form 192.168.1.xxx to access the VPort.
- Allow any host to access the VPort.
  Do not checkmark the "Enable accessible IP list" checkbox.

The following table gives additional IP/NetMask 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

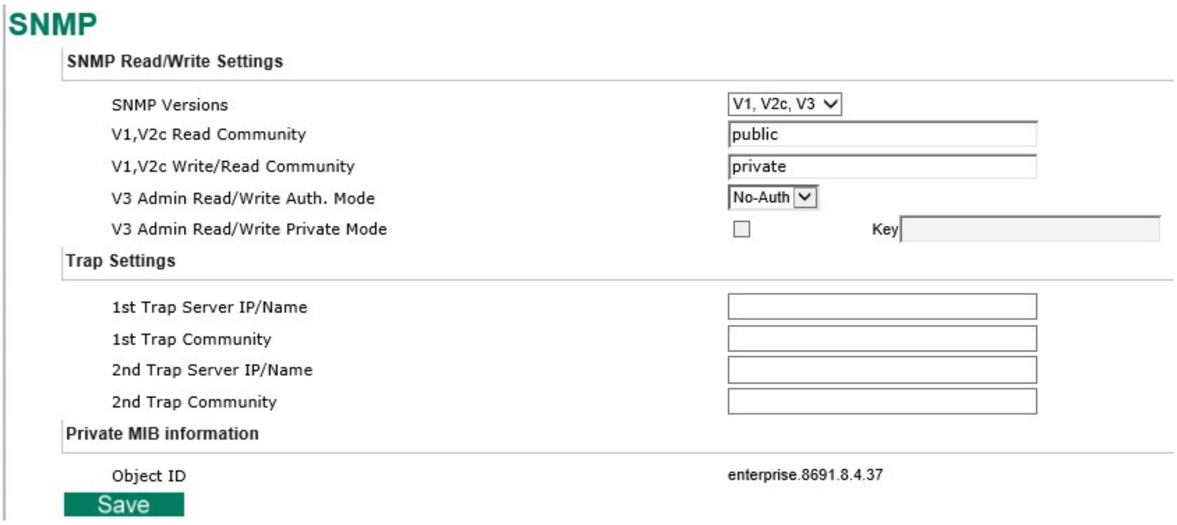
SNMP

The VPort 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: private

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.8691.8.4.37

Save

SNMP Read/Write Settings

SNMP Versions

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

V1, V2c Read Community

Setting	Description	Default
V1, V2c Read Community	Use a community string match for authentication. This 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. This 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.

V3 Admin Read/Write Auth. mode

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

V3 Admin Read/Write private mode

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
1st and 2nd Trap Server IP/Name	Enter the IP address or name of the Trap Server used by your network.	No
1st and 2nd Trap Community	Use a community string match for authentication; Maximum of 30 characters.	No

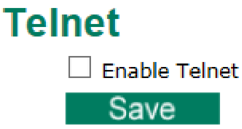
Private MIB information

Different VPorts have different object IDs.

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

Telnet

Use this function to enable/disable the Telnet function.



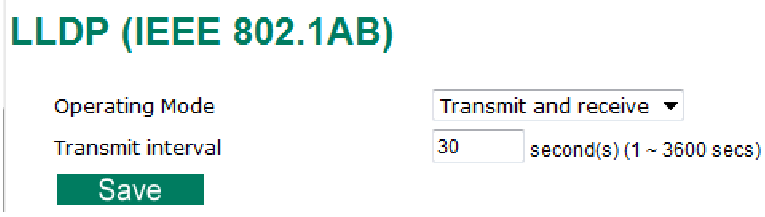
Telnet

□ Enable Telnet

LLDP

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configuration, and with SNMP, this information can be transferred to Moxa's MXview for auto-topology and network visualization.

From the VPort's web interface, you can enable or disable LLDP, and set the LLDP transmit interval. In addition, you can view each VPort's neighbor-list, which is reported by its network neighbors.



LLDP (IEEE 802.1AB)

Operating Mode: Transmit and receive

Transmit interval: 30 second(s) (1 ~ 3600 secs)

Setting	Description	Default
Operation Mode	Choose the LLDP operation mode: Disabled, Transmit only, Receive only, or Transmit and receive.	Transmit and receive
Transmit interval	Sets the transmit interval of LLDP messages, in seconds.	30 seconds

Video

Image Settings

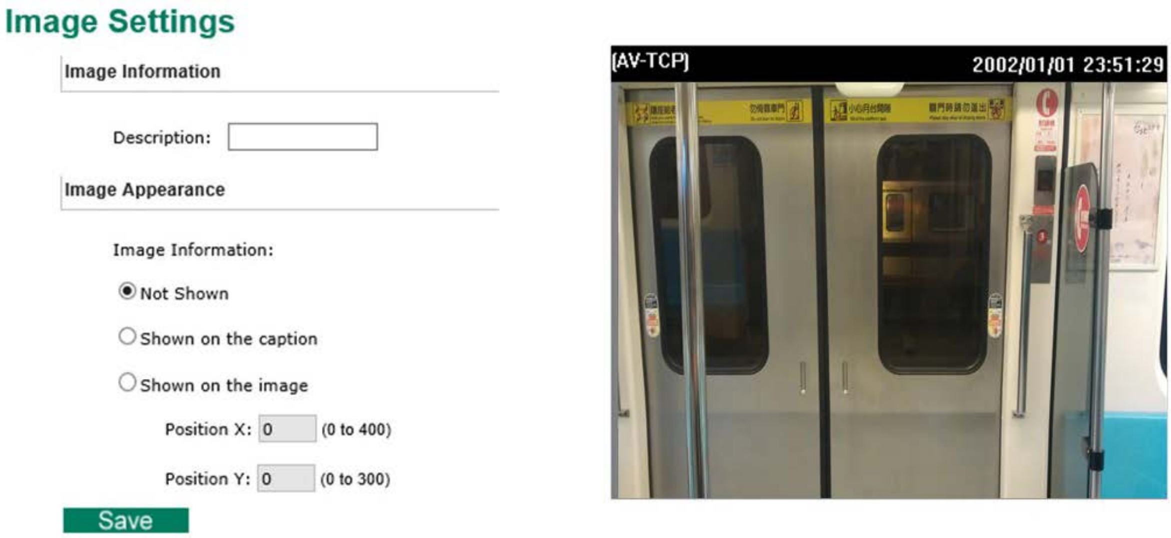


Image Settings

Image Information

Description:

Image Appearance

Image Information:

● Not Shown

○ Shown on the caption

○ Shown on the image

Position X: 0 (0 to 400)

Position Y: 0 (0 to 300)

Image Information Setting

Setting	Description	Default
Description (max. of 15 characters)	The customized description shown on the caption to identify this video camera.	None

Image Appearance Setting

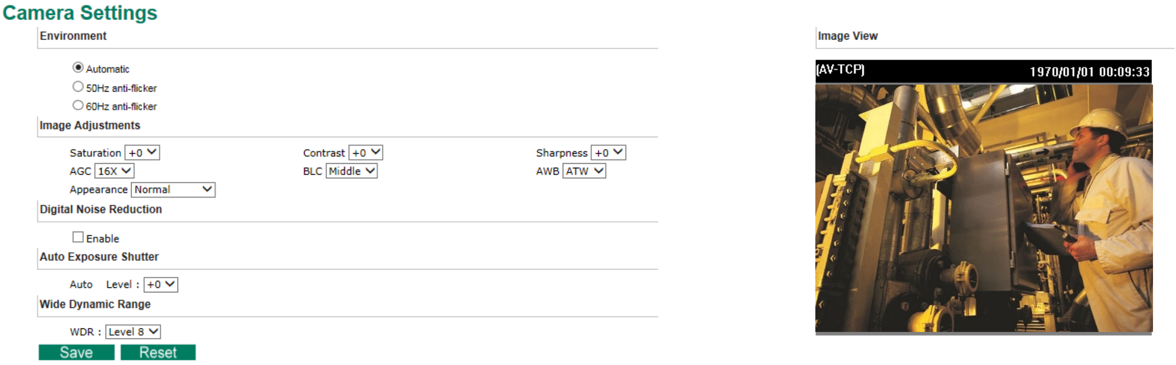
Setting	Description	Default
Image Information	Determines how image information is shown. Options are: Not Shown, Show on the Caption, and Show on image	Not Shown

Image Appearance Position

The position of the Image Appearance window can be changed by configuring Position X and Position Y. The arrangement of the position is based on the resolution of each model.

Camera Setting

Different environments require different camera settings to ensure acceptable image quality.



Camera Settings

Environment

● Automatic

○ 50Hz anti-flicker

○ 60Hz anti-flicker

Image Adjustments

Saturation +0 Contrast +0 Sharpness +0

AGC 16X BLC Middle AWB ATW

Appearance Normal

Digital Noise Reduction

□ Enable

Auto Exposure Shutter

Auto Level : +0

Wide Dynamic Range

WDR : Level 8

Environment

Setting	Description	Default
Environment	Choose the kind of environment the VPort camera will be installed in; parameters will be optimized depending on which environment is specified. **Automatic:** This setting is usually for cameras used in an outdoor environment. **50 Hz anti-flicker:** This setting should be enabled when the camera is installed in a 50 Hz power frequency environment. **60 Hz anti-flicker:** This setting should be enabled when the camera is installed in a 60 Hz power frequency environment.	Automatic

Image Adjustments

Setting	Description	Default
Saturation	Select a value from -4 to +6.	0
Contrast & Sharpness	Select a value from -4 to +4	0
Auto Gain Control (AGC)	The AGC function produces clear images in low light conditions. The setting controls an amplifier that is used to boost the video signal when the light dims so to increase the camera’s sensitivity. In some bright environments, the amplifier may be overloaded, which may distort the video signal.	16x
Back light control (BLC)	This function corrects the exposure of objects that are in front of a bright light source.	Middle
AWB (Auto White Balance)	For most conditions, we suggest using ATW to allow the camera to automatically adjust the white balance. We suggest using AWB when your camera is monitoring a scene in which one color occupies most of the view. If you like to use AWB, follow these steps: Step 1: Move the camera to a white color, real-world environment with normal lighting. Step 2: Select AWB and then click “Save”. Step 3: Move the camera back to the location that is to be monitored.	ATW
Appearance	Normal: Normal view Mirror: Image will be displayed as in a mirror Flip: 180 degree rotation followed by mirrored display 180 Rotation: Display image after a 180 degree rotation	Normal

Digital Noise Reduction

Setting	Description	Default
Enable/Disable	Enable/Disable digital noise reduction function	Disable

Auto Exposure Shutter

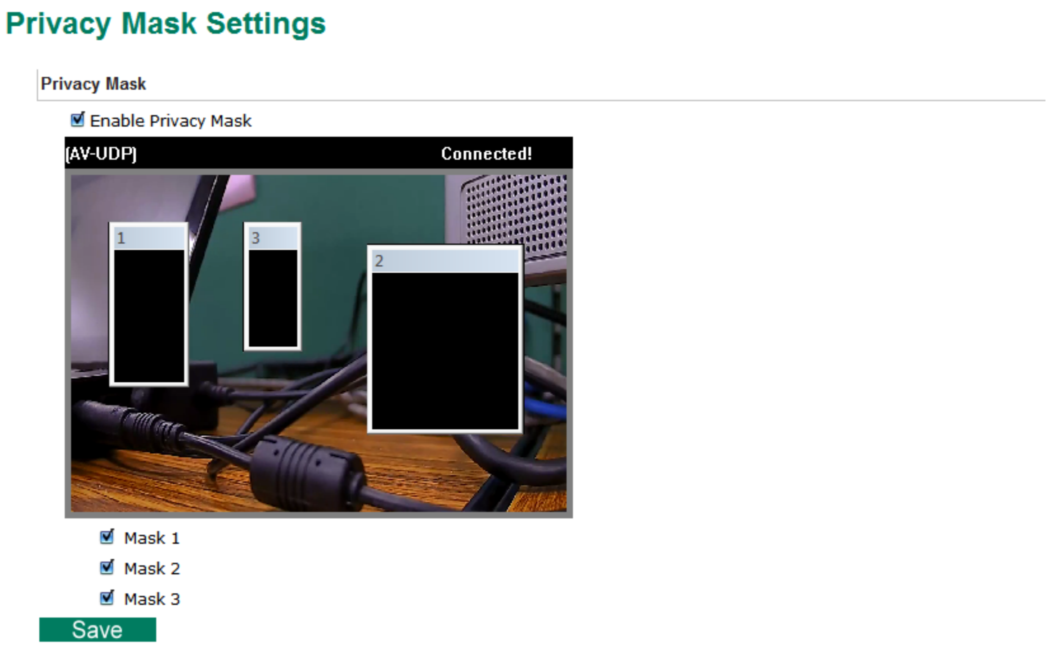
Setting	Description	Default
Auto Level	Configure the exposure mode from -5 to +5. Higher levels cause a slower shutter speed (hence brighter images); lower levels do the opposite.	0

Wide Dynamic Range

Setting	Description	Default
WDR	Configure the WDR mode from Level 1 to Level 8, or enable/ disable, based on different VPort models. A higher level causes a stronger WDR effect. Choose a higher WDR level when your camera is monitoring a scene with both bright and dark areas.	Level 8, or disable

Privacy Mask

In some conditions, you may want to block part of the view so that your surveillance system won't display private information that would otherwise be visible; the information will be blocked when displaying live video and during video playback.


Privacy Mask Settings

Privacy Mask

☑ Enable Privacy Mask

☑ Mask 1
☑ Mask 2
☑ Mask 3

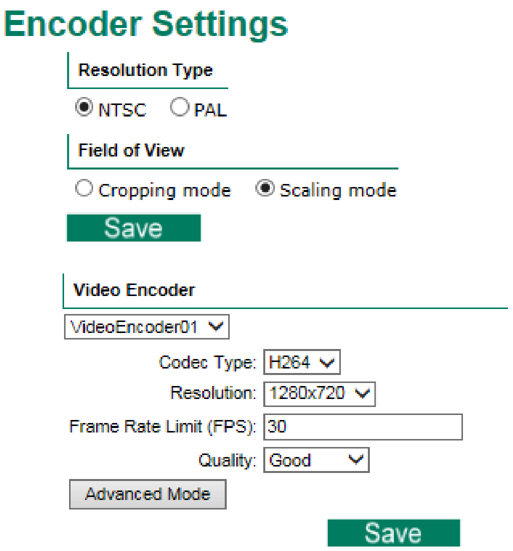
Privacy Mask

Setting	Description	Default
Enable Privacy Mask	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 areas to different parts of the camera scene.	Disable

NOTE There is no way to recover masked video. The masked areas are not displayed when viewing the video live, or during playback, so be sure to use this function carefully.

Video Encoder

The VPort supports up to three video encoders for generating video stream profiles. The video encoders can each be configured with different codecs (H.264 or MJPEG), resolution, FPS (frame rate), and video quality.



Encoder Settings

Resolution Type

● NTSC ○ PAL

Field of View

○ Cropping mode ● Scaling mode

Video Encoder

VideoEncoder01

Codec Type: H264

Resolution: 1280x720

Frame Rate Limit (FPS): 30

Quality: Good

Resolution Type

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

Field of view

Setting	Description	Default
Cropping mode or Scaling mode	Choose the cropping or scaling mode when modifying resolution. (Cropping mode will alter viewing angle and scaling mode will alter object ratio)	Cropping mode

Video Encoder

Setting	Description	Default
Videoencoder01 Videoencoder02 Videoencoder03	To configure the attributes of the video encoder	Videoencoder01

Codec Type

This codec type shows the codec of each video stream.

Setting	Description	Default
Codec type	Configure the codec type of the video encoder: H.264, MJPEG	H.264

Resolution

Different VPort models support different resolutions. See each model's specifications for details.

Setting	Description	Default
Select the image size	Different image resolutions (size) are provided based on different VPort models. The administrator can choose each option with NTSC or PAL modulation.	1280 x 800

Resolution	NTSC	PAL
WXGA	1280 x 800	1280 x 800
HD 720P	1280 x 720	1280 x 720
SVGA	800 x 600	800 x 600
Full D1	720 x 480	720 x 576

Resolution	NTSC	PAL
4CIF	704 x 480	704 x 576
VGA	640 x 480	640 x 480
CIF	352 x 240	352 x 288
QVGA	320 x 240	320 x 240
QCIF	176 x 112	176 x 144

Max. FPS (Frame per second)

Setting	Description	Default
Frame Rate Limit (FPS)	Configure the maximum FPS (frames per second); up to 30	30

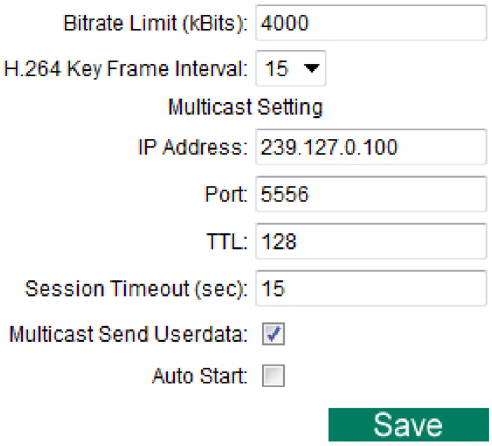
NOTE Frame rate (frames per second) is determined by the resolution, image data size (bit rate), and transmission traffic status. The Administrator and users can check the frame rate status in the FPS Status on the VPort's web homepage.

NOTE Enabling more video streams can lower the frame rate of each video stream.

Quality

Setting	Description	Default
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

The video encoder setting supports an **Advanced Mode**. Click on the Advance Mode button to view the following configuration options.



Bitrate Limit (kBits): 4000

H.264 Key Frame Interval: 15

Multicast Setting

IP Address: 239.127.0.100

Port: 5556

TTL: 128

Session Timeout (sec): 15

Multicast Send Userdata: ☑

Auto Start: □

Setting	Description	Default
Bitrate Limit (kBits) (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.	8000
H.264 Key Frame Interval	Configure the key frame interval of the H.264 stream. A low number means higher video quality (due to more key frames), but more bandwidth will be consumed. If you have concerns about bandwidth, then select a higher number for *key frame interval*.	15

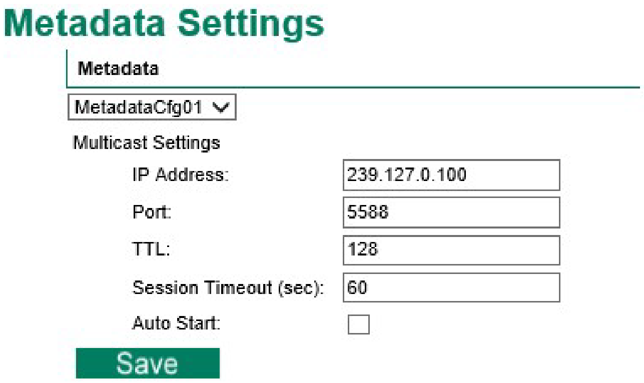
Multicast Setting

Setting	Description	Default
IP Address	Multicast Group address for sending a video stream.	239.127.0.100
Port	Video port number.	Videoecnoder01: 5556 Videoencoder02: 5558 Videoencoder03: 5560
TTL	Multicast-TTL (Time-to-live) threshold. A certain TTL threshold is 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
Session Timeout (sec)	Timeout between the client and the stream	60 (seconds)
Multicast Send Userdata	Configure the video stream with or without userdata	Enable
Auto Start	Enable/disable the Multicast stream push mode	Disable

NOTE 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.

Metadata

The metadata includes date, time, event, alarm, etc., and even some private information. The metadata can be sent with the video stream to provide the information to the system. If the video stream is in unicast mode, the metadata will be sent with the video stream. If the video stream is in multicast mode, then the following multicast settings are required.



Metadata Settings

Metadata

MetadataCfg01

Multicast Settings

IP Address: 239.127.0.100

Port: 5588

TTL: 128

Session Timeout (sec): 60

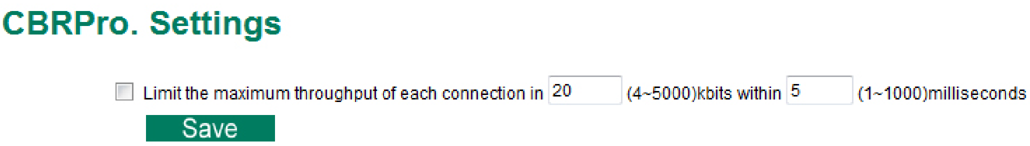
Auto Start: □

Multicast setting

Setting	Description	Default
IP Address	Multicast Group address for sending the metadata.	239.127.0.100
Port	Metadata port number.	5588
TTL	Multicast-TTL (Time-to-live) threshold. A certain TTL threshold is 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
Session Timeout (sec)	Timeout between the client and the stream	60 (seconds)
Auto Start	Enable/disable the Multicast stream push mode	Disable

Streaming

CBR Pro



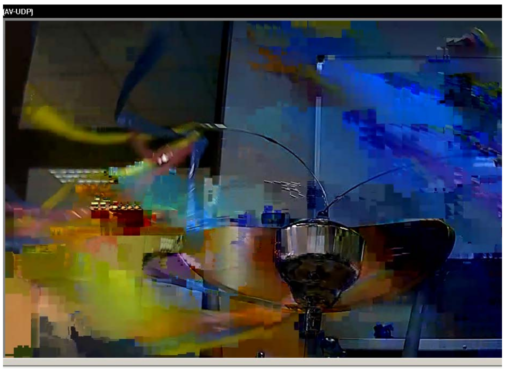
CBRPro. Settings

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

General CBR (constant bit rate) configuration limits throughput to 1 second, but since video streaming is designed to transmit immediately to shorten latency, network throughput may experience a burst in action during short time periods, in which case packet loss will occur if the network bandwidth buffer is not large enough. When packet loss occurs, images will show a mosaic effect. For this reason, the VPort supports an advanced CBR Pro™ function, which can enable the flow control of image packets to ensure no packet loss for limited bandwidth transmissions, such as on xDSL or wireless networks.

Image without packet loss

Image with packet loss



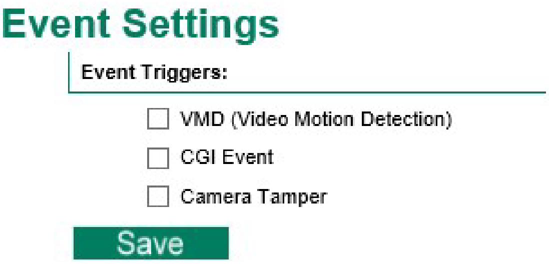
Setting	Description	Default
Limit the maximum throughput of each connection in [xxx] (4 to 5000) kbits within [xxx] (1 to 1000) milliseconds	Configure how much throughput is allowed on the network within the given number of milliseconds. For example, if the configuration is 20 kbits within 5 milliseconds, the video packet throughput will be limited to 20 kbits within 5 milliseconds.	20 kbits within 5 milliseconds

Event

You can set up all of the events that you want to be detected by the camera; in fact, you may set an action once an event occurs.

Enable Event

Checkmark those events you would like to enable. Events without a checkmark are disabled.



Event Settings

Event Triggers:

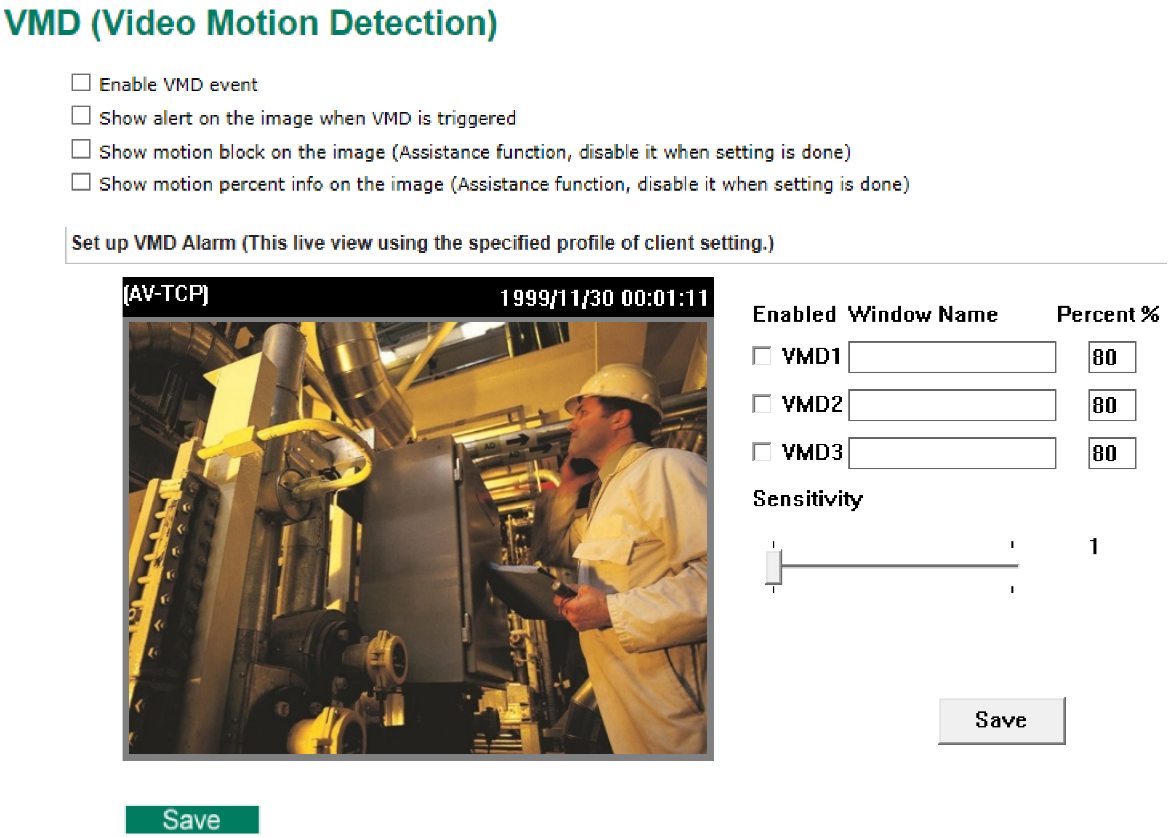
☐ VMD (Video Motion Detection)

☐ CGI Event

☐ Camera Tamper

Video Motion Detection

Video Motion Detection (VMD) is an intelligent event alarm for video surveillance network systems. With three 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 event
□ Show alert on the image when VMD is triggered
□ Show motion block on the image (Assistance function, disable it when setting is done)
□ Show motion percent info on the image (Assistance function, disable it when setting is done)

Set up VMD Alarm (This live view using the specified profile of client setting.)

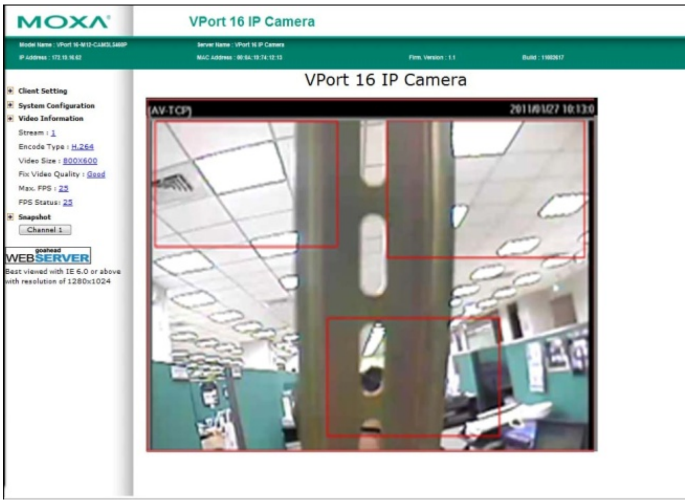
(AV-TCP) 1999/11/30 00:01:11

Enabled	Window Name	Percent %
□ VMD1		80
□ VMD2		80
□ VMD3		80

Sensitivity 1

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 “show alert on the image…” When enabled, when a VMD alarm notification is received, a red square frame will be displayed on the video image.	Disabled
Show the motion block on the image (Assistance function, disable it when setting is done)	Enable this item for real-time motion detection, which is related to VMD sensitivity configuration.	Disabled
Show the motion percentage information on the image (Assistance function, disable it when setting is done.)	Enable this item to show the change in percentage of motion detection, which is related to the VMD’s percentage configuration.	Disabled

NOTE Once "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.



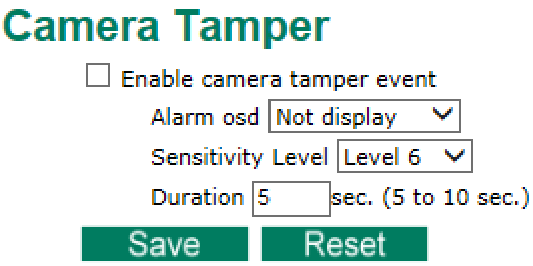
Setup a VMD Alarm

Setting	Description	Default
Enable	Enable or disable the VMD1, VMD2, or VMD3	Disable
Window	The name of each VMD window	Blank
Percent	The minimum percentage of change to an image that will trigger VMD. Decrease the percentage to make it easier to trigger VMD.	80
Sensitivity	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.

Camera Tamper

Use the VPort's camera tamper function to detect malicious behavior done to the camera, such as spray painting, view blocking, angle adjustment, etc. This page allows you to configure the parameters and alarm condition/action of the camera tamper alarm.



Camera Tamper

☐ Enable camera tamper event

Alarm osd Not display

Sensitivity Level Level 6

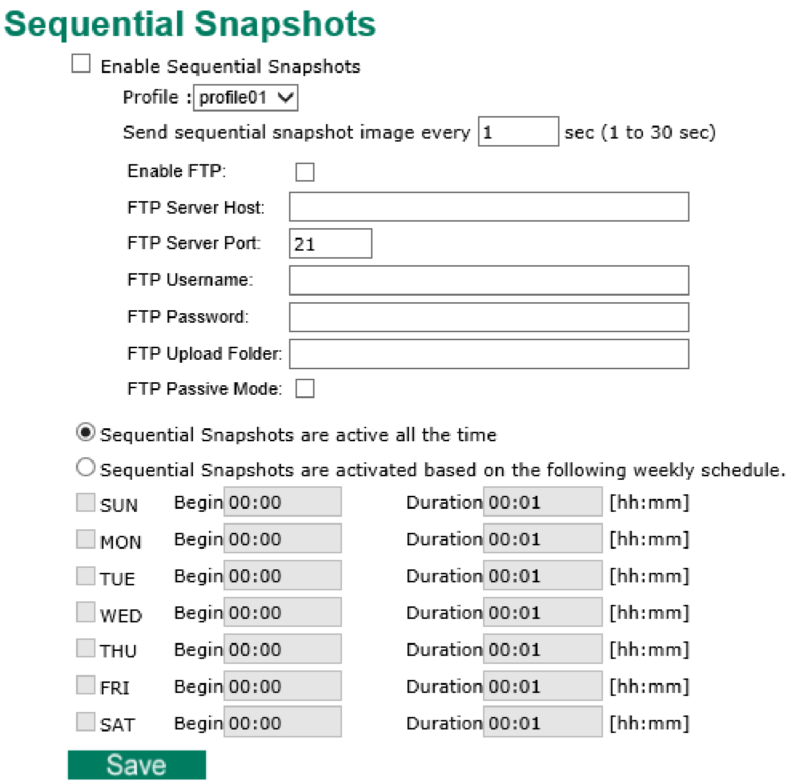
Duration 5 sec. (5 to 10 sec.)

Setting	Description	Default
Enable camera tamper event	Enable or disable the digital input alarm	Disable
Alarm osd	Determines whether or not the camera will display an onscreen warning square when the camera tamper alarm is triggered	Not display

Trigger Conditions

Setting	Description	Default
Sensitivity Level	Adjust the sensitivity level of tamper detection (level 10 is the most sensitive level)	Level 5
Duration	How long should the camera tamper behavior persist before the alarm is triggered.	5 sec.

Sequential Snapshot



Sequential Snapshots

□ Enable Sequential Snapshots

Profile : profile01

Send sequential snapshot image every 1 sec (1 to 30 sec)

Enable FTP: □

FTP Server Host:

FTP Server Port: 21

FTP Username:

FTP Password:

FTP Upload Folder:

FTP Passive Mode: □

● Sequential Snapshots are active all the time

○ Sequential Snapshots are activated based on the following weekly schedule.

□ SUN Begin 00:00 Duration 00:01 [hh:mm]

□ MON Begin 00:00 Duration 00:01 [hh:mm]

□ TUE Begin 00:00 Duration 00:01 [hh:mm]

□ WED Begin 00:00 Duration 00:01 [hh:mm]

□ THU Begin 00:00 Duration 00:01 [hh:mm]

□ FRI Begin 00:00 Duration 00:01 [hh:mm]

□ SAT Begin 00:00 Duration 00:01 [hh:mm]

With this feature, the VPort can upload snapshots periodically to an external E-mail or FTP server as a live video source.

Setting	Description	Default
Enable Sequential Snapshots	Enable or disable Sequential Snapshot.	Disable
Profile	Select which video profile will take snapshot images.	Profile01
Send sequential snapshot image every [xxx] sec (1 to 30 sec)	The time interval between successive snapshot images.	1 second (from 1 second to 30 seconds)

FTP

Setting	Description	Default
Enable FTP	Enable the FTP system to save snapshot images remotely.	Disable
FTP Server Host	FTP server's IP address or URL address.	None
FTP Server Port	FTP server's authentication.	21
FTP Username		None
FTP Password		None
FTP Upload Folder	FTP file storage folder on the remote FTP server.	None
FTP Passive Mode	Passive transfer solution for FTP transmission through a firewall.	Disable

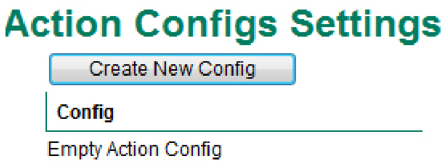
Weekly Schedule

Setting	Description	Default
Sequential Snapshot is active all the time	The Sequential Snapshot function is always active.	Sequential Snapshot are active all the time
Sequential Snapshot are activated based on the following weekly schedule	The Sequential Snapshot is activated based on the configured weekly schedule.	
SUN, MON, TUE, WED, THU, FRI, SAT	Select which days of the week to schedule event alarms.	None
Begin 00:00	Set the start time of the event alarm.	00:00
Duration 00:00	Set how long the event alarm will be active.	00:01

Actions

Action Config

To set up an event alarm, the corresponding action needs to be configured first.


Action Configs Settings

Config

Empty Action Config

Step 1: Click the "Create New Config" button.

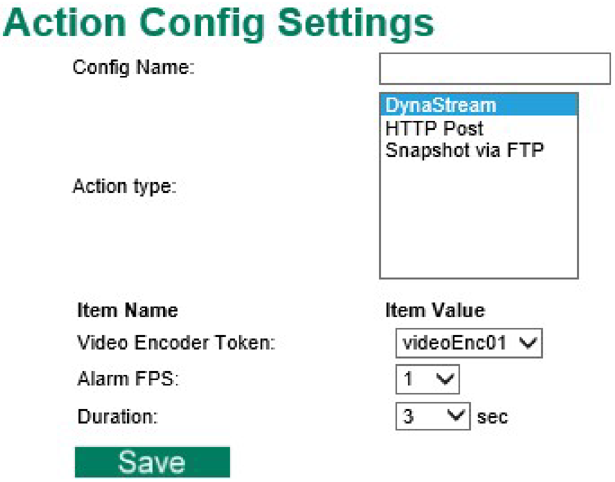
Step 2: Create the new action.

Setting	Description	Default
Config Name	Configure the name of the new action	None
Action type	Select the Action type: DynaStream, HTTP Post, Snapshot via FTP	DynaStream

Different actions have different configuration items.

DynaStream

DynaSteam™ is a unique and innovative function that allows for adaptive frame rates in response to events on the network, such as event triggers and system commands. When network traffic becomes congested, DynaStream™ allows VPort products to respond to CGI, SNMP, and video loss triggers, and automatically decreases the frame rates to reduce bandwidth consumption. This reserves bandwidth for the system to maintain Quality of Service (QoS) and guarantees that the system 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.



Action Config Settings

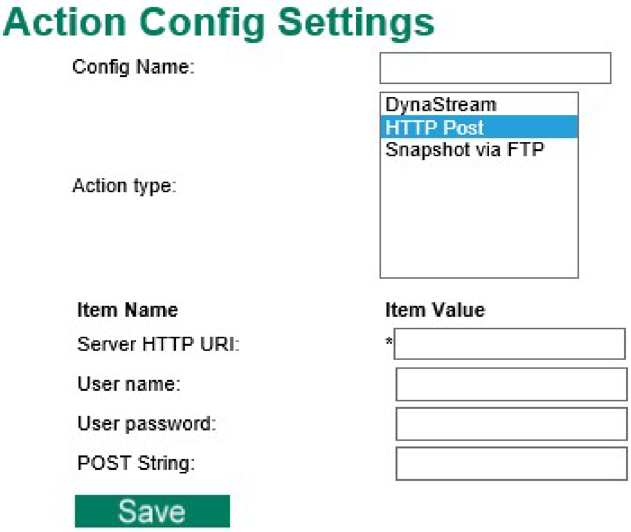
Config Name:

Action type: DynaStream

Item Name	Item Value
Video Encoder Token:	videoEnc01
Alarm FPS:	1
Duration:	3 sec

Settings	Description	Default
Video Encoder Token	Select the video encoder.	videoEnc01
Alarm FPS	Configure what the frame rate will be set to when the event is triggered.	1
Duration	Configure how long Dynastream will be active.	3 seconds

HTTP Post



Action Config Settings

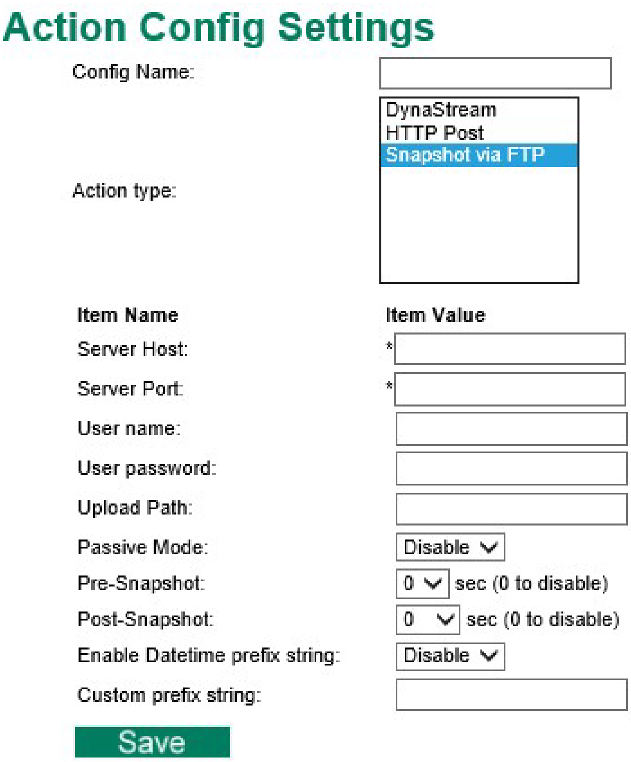
Config Name:

Action type: HTTP Post

Item Name	Item Value
Server HTTP URI:	*
User name:	
User password:	
POST String:	

Settings	Description	Default
Server HTTP URL	URL of the HTTP server.	None
User name	Authentication information for the HTTP server.	None
User password		
POST String	Configure the string that will be posted.	None

Snapshot via FTP



Action Config Settings

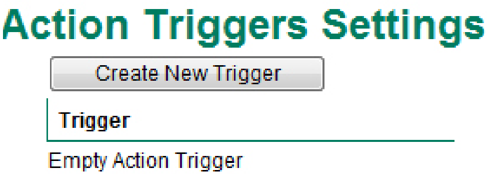
Config Name:	
Action type:	DynaStream HTTP Post Snapshot via FTP

Item Name	Item Value
Server Host:	*
Server Port:	*
User name:	
User password:	
Upload Path:	
Passive Mode:	Disable
Pre-Snapshot:	0 sec (0 to disable)
Post-Snapshot:	0 sec (0 to disable)
Enable Datetime prefix string:	Disable
Custom prefix string:	

Setting	Description	Default
Server Host	FTP server's IP address or URL address.	None
Server Port	FTP server's authentication information.	21
User name		None
User password		None
Upload Path	FTP file storage folder on the remote FTP server.	None
Passive Mode	Passive transfer solution for FTP transmission through a firewall.	Disable
Pre-Snapshot [xxx] sec (0 to disable)	= 0: A pre-snapshot image will not be generated. > 0: The image this many seconds before the event will be used as the pre-snapshot image.	0
Post-Snapshot [xxx] sec (0 to disable)	= 0: A post-snapshot image will not be generated. > 0: The image this many seconds after the event will be used as the post-snapshot image.	0
Enable Datetime prefix string	Add the date & time to the file name of snapshot image.	Disable
Customer prefix string	The file names of snapshot images will be prefixed with this string.	None

Action Trigger

After the action type is configured, users can configure how to trigger the action.



Action Triggers Settings

Trigger

Empty Action Trigger

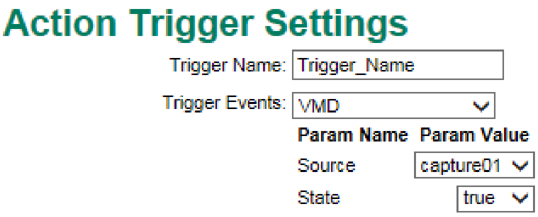
Step 1: Click the "Create New Trigger" button.

Step 2: Create the new trigger.

Setting	Description	Default
Trigger Name	Configure the name of the new trigger	None
Trigger Events	Select the event type: Digital input, VMD, Tamper, CGI trigger, Link status	Active Relay

Different triggers have different configuration items.

VMD



Action Trigger Settings

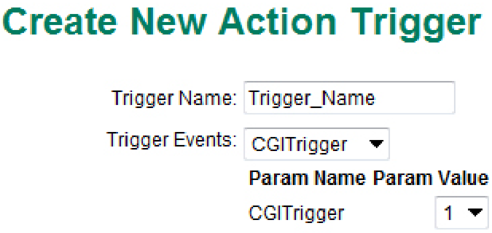
Trigger Name: Trigger_Name

Trigger Events: VMD

Param Name	Param Value
Source	capture01
State	true

Settings	Description	Default
Source	Select the video source. Currently, VPort IP cameras only have one video source.	capture01
State	Enable (true) or disable (false) the VMD trigger	true

CGI trigger



Create New Action Trigger

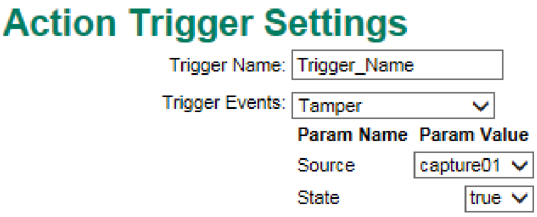
Trigger Name: Trigger_Name

Trigger Events: CGITrigger

Param Name	Param Value
CGITrigger	1

Settings	Description	Default
CGITrigger	Select from 5 CGI triggers.	1

Tamper



Action Trigger Settings

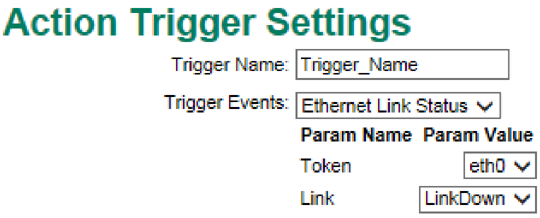
Trigger Name: Trigger_Name

Trigger Events: Tamper

Param Name	Param Value
Source	capture01
State	true

Settings	Description	Default
Source	Select the video source. Currently, VPort IP cameras only have one video source.	capture01
State	Enable (true) or disable (false) the Tamper trigger	true

Link Status



Action Trigger Settings

Trigger Name: Trigger_Name

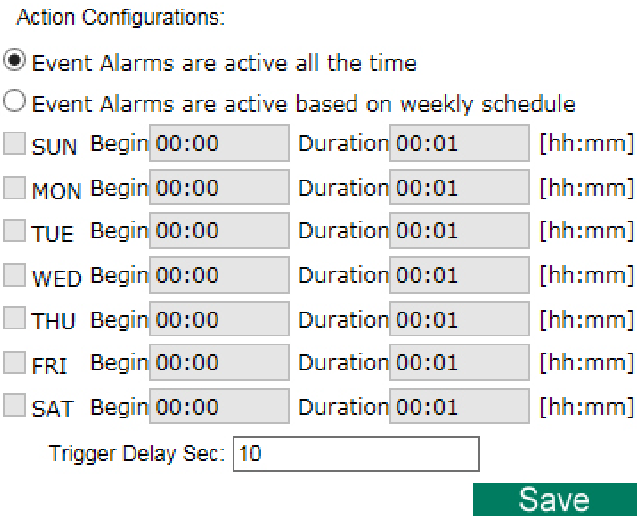
Trigger Events: Ethernet Link Status

Param Name	Param Value
Token	eth0
Link	LinkDown

Settings	Description	Default
Token	Select the Ethernet port number. Some VPort models have 2 Ethernet ports.	eth0
Link	Configure the trigger to LinkDown or LinkUp	LinkDown

NOTE When the Ethernet link is down, you will not be able to access the VPort via the IP network. In this case, the local relay output will be active, and video can be recorded on the VPort's SD card.

Step 3: Configure the schedule of the trigger actions.



Action Configurations:

● Event Alarms are active all the time

○ Event Alarms are active based on weekly schedule

□ SUN	Begin 00:00	Duration 00:01	[hh:mm]
□ MON	Begin 00:00	Duration 00:01	[hh:mm]
□ TUE	Begin 00:00	Duration 00:01	[hh:mm]
□ WED	Begin 00:00	Duration 00:01	[hh:mm]
□ THU	Begin 00:00	Duration 00:01	[hh:mm]
□ FRI	Begin 00:00	Duration 00:01	[hh:mm]
□ SAT	Begin 00:00	Duration 00:01	[hh:mm]

Trigger Delay Sec: 10

Setting	Description	Default
Event Alarms are active all the time	The trigger action configurations are always active.	Event Alarms are active all the time
Event Alarms are active based on weekly schedule	The trigger action configurations are activated based on the configured weekly schedule	
□SUN □MON □TUE □WED □THU □FRI □SAT	Select which days of the week to schedule event alarms.	None
Begin 00:00	Set the start time of the event alarm.	00:00
Duration 00:00	Set how long the event alarm will be active.	00:01
Trigger Delay Sec	The amount of time the system will wait before acting on the next trigger.	10 seconds

A

Frequently Asked Questions

Q: What if I forget my password?

A: Unless the authentication is disabled, you will need to log in every time you access the VPort IP camera. If you are *not* the administrator, you will need to ask the administrator to create a new account for you. 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 use the **RESET** button to restore the camera to its factory default settings. The reset button is located on the electronic board. Contact a Moxa technical service engineer if you need help using the reset button.

Q: Why can't I see video from the IP camera after logging in?

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, try resetting the camera to its factory default settings to see if that solves the problem.

Q: What is the plug-in for?

A: The plug-in provided by the IP camera is used to display videos. 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. We recommend consulting the network supervisor in your office before adjusting the security level of your browser.

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 VPort is connected to the Internet and the function is enabled. If the time zone is changed, subsequent timestamps could be several hours earlier or later than timestamps that were already generated.

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 IP camera will allow 10 video streams for udp/tcp/http connections. We recommend using an additional web server that retrieves images from the IP camera periodically if you need to host a large number of users.

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

A: The codec can process 30 frames per second internally. However, the actual performance is affected by many factors, as listed below:

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

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

A: The IP camera is designed for surveillance purposes and has many flexible interfaces. Enabling user authentication during installation can prevent the VPort from being accessed by people without authorization. You may also change the HTTP port to a non-public number. Check the system log to analyze any abnormal activities and trace the origin of the activity.

Q: Why can't I access the IP camera after activating certain configuration options?

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 video if the event you're monitoring occurs frequently. If you prefer to retrieve images by FTP, the time could be smaller since an FTP server responds more quickly than a web server. When the system is "too busy to configure" (i.e., it hangs), use the restore factory default and reset button to restart 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 Verde Is.
(GMT)	Casablanca, Monrovia
(GMT)	Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
(GMT+01:00)	Amsterdam, Berlin, Bern, Stockholm, Vienna
(GMT+01:00)	Belgrade, Bratislava, Budapest, Ljubljana, Prague (GMT+01 :00) Brussels, Copenhagen, Madrid, Paris
(GMT+01:00)	Sarajevo, Skopje, Warsaw, Zagreb
(GMT+01:00)	West Central Africa
(GMT+02:00)	Athens, Istanbul, Minsk
(GMT+02:00)	Bucharest
(GMT+02:00)	Cairo
(GMT+02:00)	Harare, Pretoria
(GMT+02:00)	Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
(GMT+02:00)	Jerusalem
(GMT+03:00)	Baghdad

(GMT+03:00)	Kuwait, Riyadh
(GMT+03:00)	Moscow, St. Petersburg, Volgograd
(GMT+03:00)	Nairobi
(GMT+03:30)	Tehran
(GMT+04:00)	Abu Dhabi, Muscat (GMT+04:00) Baku, Tbilisi, Yerevan (GMT+04:30) Kabul
(GMT+05:00)	Ekaterinburg
(GMT+05:00)	Islamabad, Karachi, Tashkent (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
(GMT+05:45)	Kathmandu
(GMT+06:00)	Almaty, Novosibirsk (GMT+06:00) Astana, Dhaka
(GMT+06:00)	Sri Jayawardenepura (GMT+06:30) Rangoon
(GMT+07:00)	Bangkok, Hanoi, Jakarta (GMT+07:00) Krasnoyarsk
(GMT+08:00)	Beijing, Chongqing, Hong Kong, 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

System Log

VPort P06HC-1V System Log List

Category	
Log Type	Log description

Cold Start	
SYS	System cold start <VPort’s firmware version>

Reboot	
SYS	Reboot

RTSP	
RTSP	Connecting from remote Address <Client’s IP address>
RTSP over HTTP	
RTSPGet	Connecting from remote Address <Client’s IP address>
RTSPSet	Connecting from remote Address <Client’s IP address>

FTP	
FTP	Connect to Server <FTP IP address: FTP port> Failed
FTP	Send Alarm Snapshot to <FTP IP address: FTP port> timeout
FTP	Login <FTP IP address: FTP port> with <account name> Failed
FTP	Set Binary Mode Failed
FTP	Change Folder Failed
FTP	Send Alarm Snapshot Image [snapshot_xxxxxxxx_xxxxxx_seq_chx.jpg] Failed
FTP	Send Alarm Snapshot Image [snapshot_xxxxxxxx_xxxxxx_seq_chx.jpg] Success

Snapshot	
FAILED	Sequential Snapshot Frame Size Overflow <snapshot image size>
FAILED	Snapshot Frame Size Overflow <snapshot image size>

Note: The maximum size of the snapshot image is 150 KB.

FACTORY Button	
SYS	Factory default through factory default button
FAILED	Factory default through factory default button Failed

Auto Config	
AutoCfg	DHCP Request Failed
AutoCfg	DHCP Server no support Auto Config
AutoCfg	TFTP Server connect Failed
AutoCfg	Config. File no exist
AutoCfg	Config. File mismatch
AutoCfg	Auto Config. Ok

Event	
EVENT	Tamper[1] Deactived (YYYY-MM-DDTHH:MM:SS+0000) Tamper[1] Actived (YYYY-MM-DDTHH:MM:SS+0000)
EVENT	VMD[1] Deactived (YYYY-MM-DDTHH:MM:SS+0000) VMD[1] Actived (YYYY-MM-DDTHH:MM:SS+0000)
EVENT	CGIEvent[1] Deactived (YYYY-MM-DDTHH:MM:SS+0000) CGIEvent[1] Actived (YYYY-MM-DDTHH:MM:SS+0000)
EVENT	Action execute [vport:<Action type>] <Action config name>

Note: Action type: Dynastream, HTTP Post and snapshotFTP