Moxa VPort 07-3 Series Software User Manual

Version 1.0, October 2024

www.moxa.com/products

Moxa VPort 07-3 Series Software User 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

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

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 camera 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.

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 test tool: 23.06

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.

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 150 seconds. The network environment determines how the IP address is assigned.

NOTE

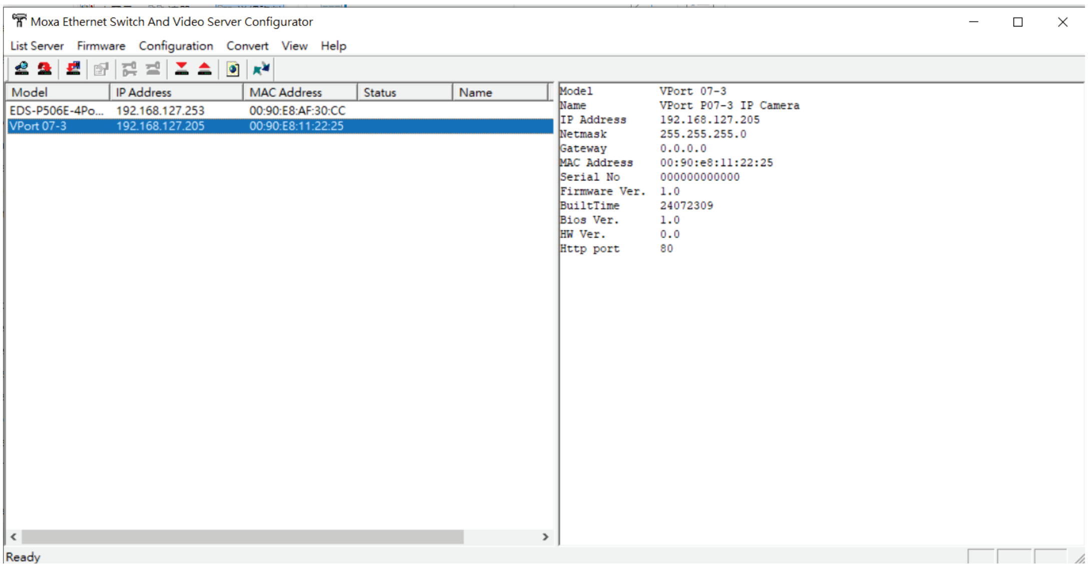
For security purpose, the VPort 07/P07-3 Series features a Secure Boot mechanism for validating the firmware, which results in an extended POST time of up to 150 seconds.

Network environments with a 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 MXconfig network configuration tool as described below:

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

1. Download the VPort and EtherDevice Configurator Utility from https://www.moxa.com
2. Run the utility (edscfgui.exe) and search for the VPort camera in the utility.



Model	IP Address	MAC Address	Status	Name
EDS-P506E-4Po...	192.168.127.253	00:90:E8:AF:30:CC		
VPort 07-3	192.168.127.205	00:90:E8:11:22:25		

```
Model          VPort 07-3
Name           VPort P07-3 IP Camera
IP Address     192.168.127.205
Netmask        255.255.255.0
Gateway        0.0.0.0
MAC Address    00:90:e8:11:22:25
Serial No      000000000000
Firmware Ver.  1.0
BuiltTime      24072309
Bios Ver.      1.0
HW Ver.        0.0
Http port      80
```

3. 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.
4. 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 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.

If your VPort 07-3 Series 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 07-3 Series 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.

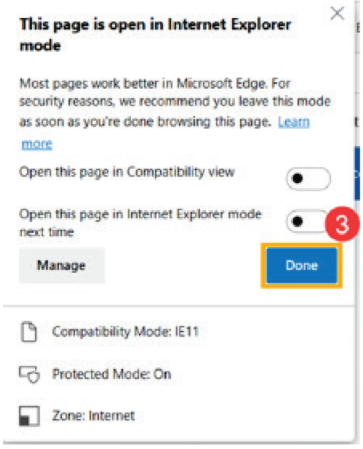
To change the IP address of the VPort manually, access the VPort's web interface and navigate to the **System Configuration > Network > General** page to configure the IP address and other network settings. Select the **Use fixed IP address** option to ensure that the IP address you assign is not deleted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

Step 2: Access the VPort 07-3 Series web-based manager

Type the VPort 07-3 IP address in the web browser’s address field and press Enter.

NOTE

If the ActiveX control component for Microsoft Internet Explorer is necessary, enable IE Mode in Microsoft Edge and reload the VPort’s web interface while in IE Mode. An IE Mode notification will appear. Make sure both toggles are disabled and the Compatibility Mode is showing IE11, then click Done. Refer to the Microsoft website for more information about IE Mode.



This page is open in Internet Explorer mode

Most pages work better in Microsoft Edge. For security reasons, we recommend you leave this mode as soon as you're done browsing this page. Learn more

Open this page in Compatibility view

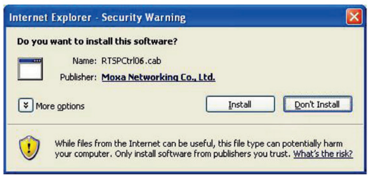
Open this page in Internet Explorer mode next time

Compatibility Mode: IE11

Protected Mode: On

Zone: Internet

A security warning message will appear when accessing the VPort’s web interface in Edge IE Mode for the first time. This message is related to installing the ActiveX Control component onto your PC or notebook. Click Install to install the plug-in to enable viewing video imagery in the IE web browser.



Internet Explorer - Security Warning

Do you want to install this software?

Name: RTSPCtrl06.cab

Publisher: Moxa Networking Co., Ltd.

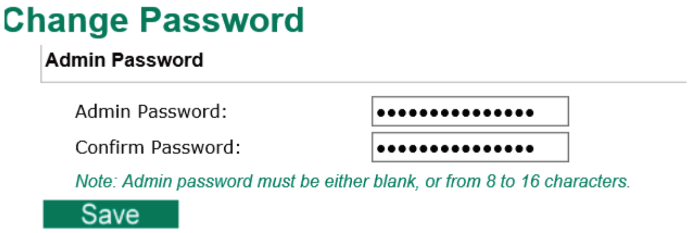
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Step 3: Log in and change the default password

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 back 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.

Save

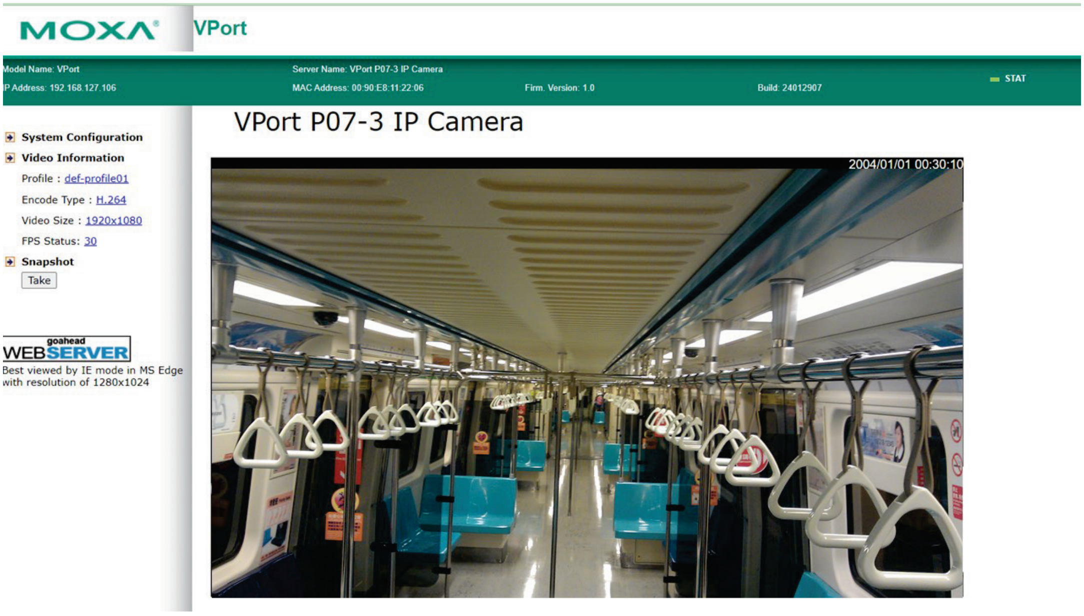
NOTE

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 4: 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



MOXA VPort

Model Name: VPort
IP Address: 192.168.127.106
Server Name: VPort P07-3 IP Camera
MAC Address: 00:90:E8:11:22:06
Firm. Version: 1.0
Build: 24012907
STAT

VPort P07-3 IP Camera

System Configuration

Video Information

Profile : def-profile01

Encode Type : H.264

Video Size : 1920x1080

FPS Status: 30

Snapshot

Take

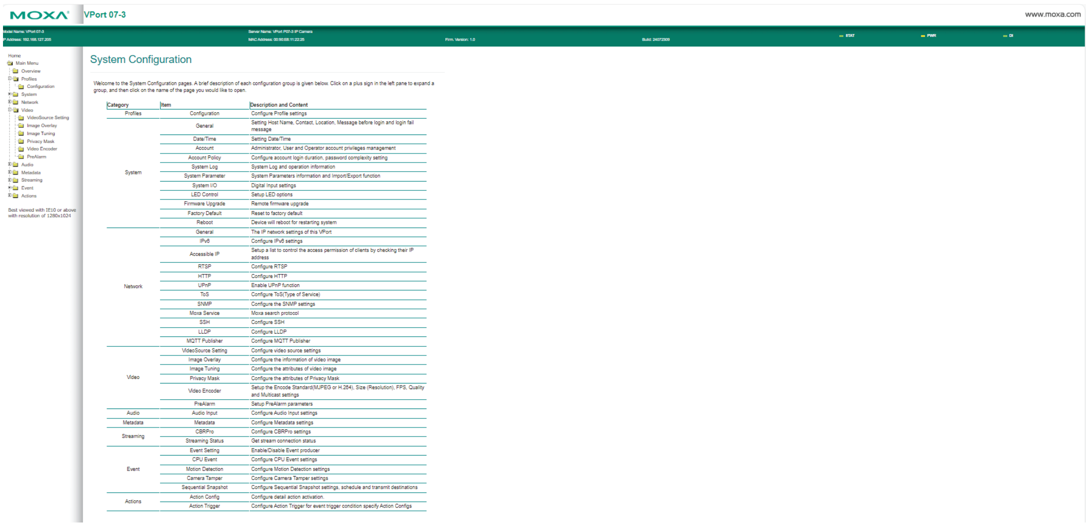
goahead WEBSERVER

Best viewed by IE mode in MS Edge with resolution of 1280x1024

2004/01/01 00:30:10

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



odel Name: VPort 07-3
P Address: 192.168.127.205
Server Name: VPort P07-3 IP Camera
MAC Address: 00:90:E8:11:22:25
Firm. Version: 1.0
Build: 24072309

Best viewed with IE10 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 Profile settings
System	General	Setting Host Name, Contact, Location, Message before login and login fail message
	Date/Time	Setting Date/Time
	Account	Administrator, User and Operator account privileges management
	Account Policy	Configure account login duration, password complexity setting
	System Log	System Log and operation information
	System Parameter	System Parameters information and Import/Export function
	System I/O	Digital Input settings
	LED Control	Setup LED options
	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
	IPv6	Configure IPv6 settings
	Accessible IP	Setup a list to control the access permission of clients by checking their IP address
	RTSP	Configure RTSP
	HTTP	Configure HTTP
	UPnP	Enable UPnP function
	ToS	Configure ToS(Type of Service)
	SNMP	Configure the SNMP settings
	Moxa Service	Moxa search protocol
	SSH	Configure SSH
	LLDP	Configure LLDP
	MQTT Publisher	Configure MQTT Publisher
Video	VideoSource Setting	Configure video source settings
	Image Overlay	Configure the information of video image
	Image Tuning	Configure the attributes of video image
	Privacy Mask	Configure the attributes of Privacy Mask
	Video Encoder	Setup the Encode Standard(MJPEG or H.264), Size (Resolution), FPS, Quality and Multicast settings
	PreAlarm	Setup PreAlarm parameters
Audio	Audio Input	Configure Audio Input settings
Metadata	Metadata	Configure Metadata settings
Streaming	CBRPro	Configure CBRPro settings
	Streaming Status	Get stream connection status
Event	Event Setting	Enable/Disable Event producer
	CPU Event	Configure CPU Event settings
	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

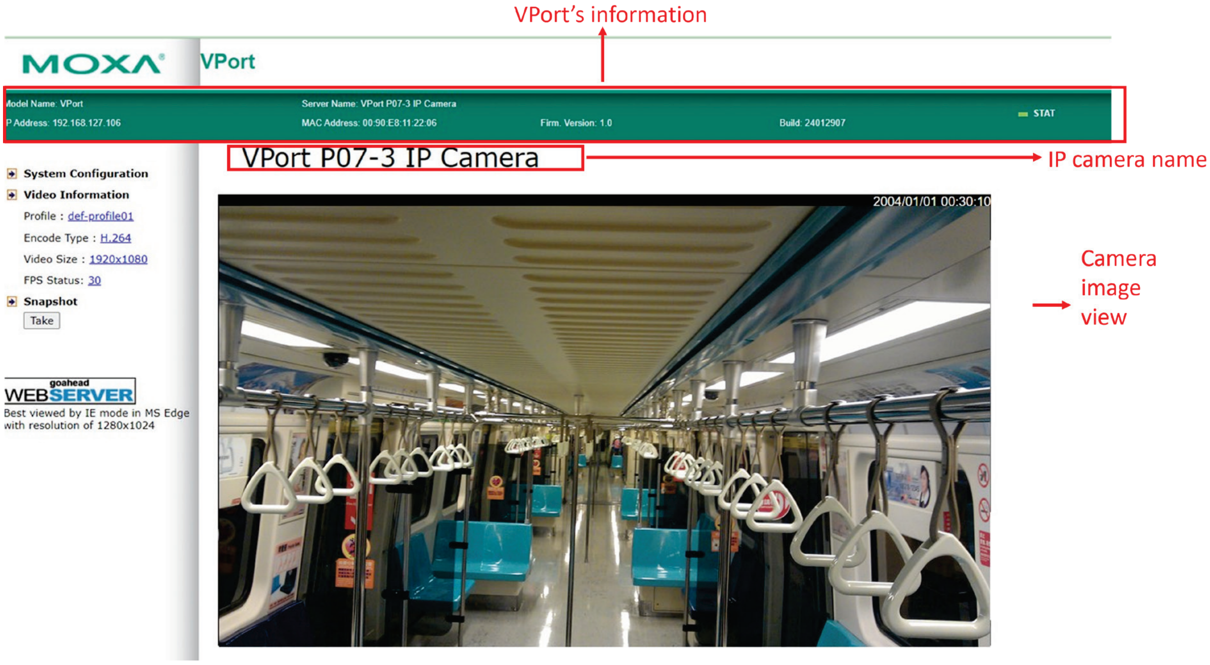
This chapter includes information about how to access the VPort IP camera for the first time.

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

Due to limitations in specific web browsers, the performance of H.264/H.265 video feeds may vary and some functions, such as client settings, privacy mask, and the preview video window, may be limited in Chrome, Microsoft Edge, or IE mode in Microsoft Edge.



VPort's information

IP camera name

Camera image view

odel Name: VPort

Server Name: VPort P07-3 IP Camera

P Address: 192.168.127.106

MAC Address: 00:90:E8:11:22:06

Firm. Version: 1.0

Build: 24012907

VPort P07-3 IP Camera

Profile : def-profile01

Encode Type : H.264

Video Size : 1920x1080

FPS Status: 30

Best viewed by IE mode in MS Edge 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.

NOTE

Due to limitations in the media player of certain web browsers, H.265 video feeds streamed in Chrome or Microsoft Edge may be choppy or may suffer from latency. To avoid these issues, use a web browser in IE mode or use RTSP multicast streaming for H.265 video feeds.

NOTE

Due to limitations in the media player of certain web browsers, audio is not supported when using the Chrome or Microsoft Edge web browsers.

Client Settings

NOTE

The Client Settings screen is only available when accessing the VPort interface via IE mode in Microsoft Edge.

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 codec, 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.

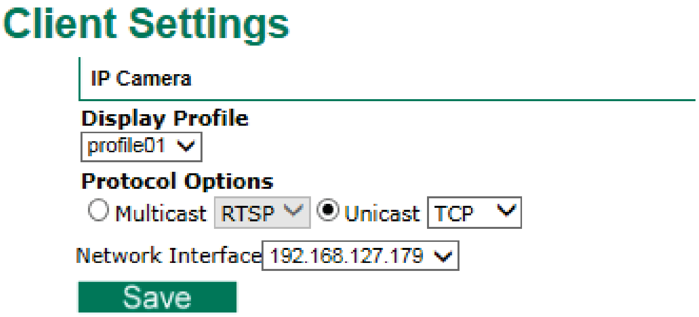
- ❐ **TCP** can be used to prevent packet loss, which results in a more accurate video display. The downside of using TCP is that the real-time delay is worse than with UDP protocol.
- ❐ **HTTP** can be used to prevent being blocked by a router's firewall. The downside of using HTTP is that the real-time 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

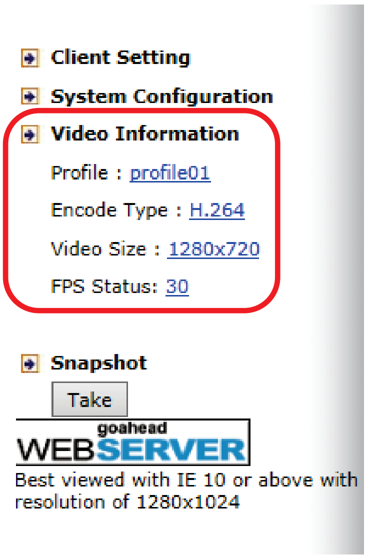
Network Interface 192.168.127.179

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.

System Configuration by Web Console

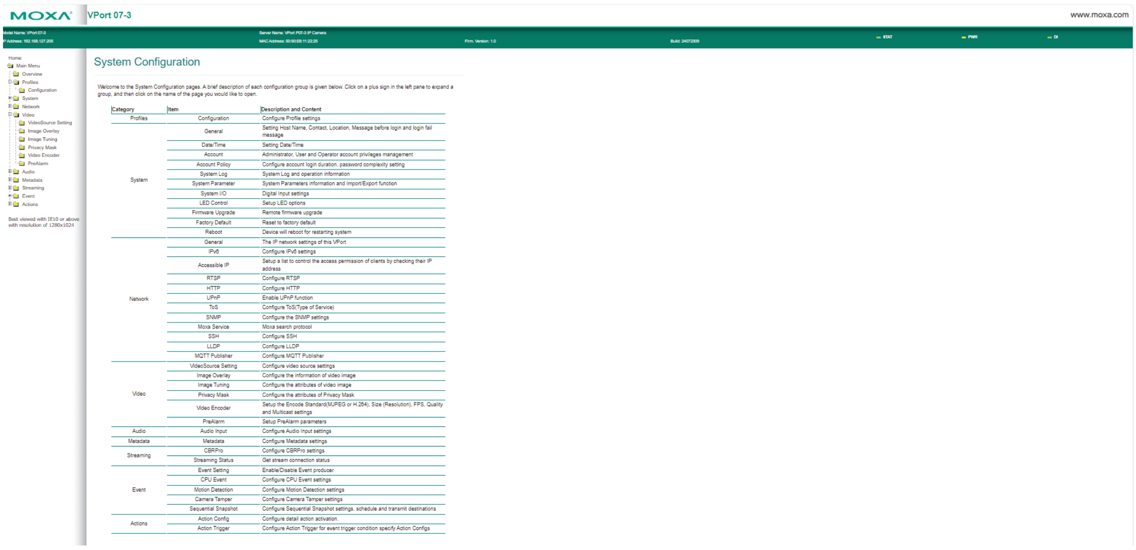
System configuration can be done remotely with Internet Explorer. To access the server, type the system configuration URL, **http://<IP address of Video Server>/overview.asp**, to open the configuration main page.

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

Category	Item	Description and Contents
Profiles	Configuration	Configure ONVIF Profile settings
System	General	Specify the server name, contact, and location
	Date/Time	Configure the system date and time
	Accounts	Configure administrator, user, and operator account privileges management settings
	Account Policy	Configure account login duration and password complexity settings
	System Log	System log and operation information
	System Parameters	System parameter information and import/export functions
	System I/O	Configure digital input and relay settings
	LED Control	Turn on/off system LEDs
	Firmware Upgrade	Perform remote firmware upgrades
	Factory Default	Reset to factory default settings
	Reboot	Device will reboot to restart the system
Network	General	Configure the VPort's IP network settings
	IPv6	Configure IPv6 settings
	Accessible IP	Configure IP-based access control permissions for clients
	RTSP	Configure RTSP settings
	HTTP	Configure HTTP settings
	UPnP	Enable UPnP functionality
	ToS	Configure ToS (Type of Service) settings
	SNMP	Configure SNMP settings
	Moxa Service	Configure Moxa Service, which is used by Moxa software or tools to search for the VPort device
	SSH	Configure SSH
	LLDP	Configure LLDP
	MQTT Publisher	Configure MQTT Publisher settings
Video	Video Source	Configure video source settings
	Image Overlay	Configure the video image overlay information
	Image Tuning	Configure the video image attributes
	Privacy mask	Configure the privacy mask settings
	Video Encoder	Set up the encode standard (H.265, H.264, or MJPEG), size (resolution), FPS, quality, and multicast settings
	PreAlarm	Configure PreAlarm settings
Audio	Audio Input	Configure audio input settings
Metadata	Metadata	Configure the stream metadata
Streaming	CBRPro	Configure CBR Pro settings
	Streaming Status	Get the stream connection status
Event	Event Settings	Enable/disable events
	CPU Event	Configure CPU events
	Motion Detection	Configure motion detection settings

Category	Item	Description and Contents
	Camera Tamper	Configure camera tamper settings.
	Sequential Snapshot	Configure sequential snapshot settings, schedules, and transmission destinations.
Action	Action Config	Configure detailed action activation settings.
	Action Trigger	Configure the action trigger for the event trigger conditions based on the specific action configuration chosen for this trigger.

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



Model Name: VPort 07-3
IP Address: 192.168.127.205
Server Name: VPort P07-3 IP Camera
MAC Address: 00:90:E8:11:22:25
Firm. Version: 1.0
Build: 24072309

System Configuration

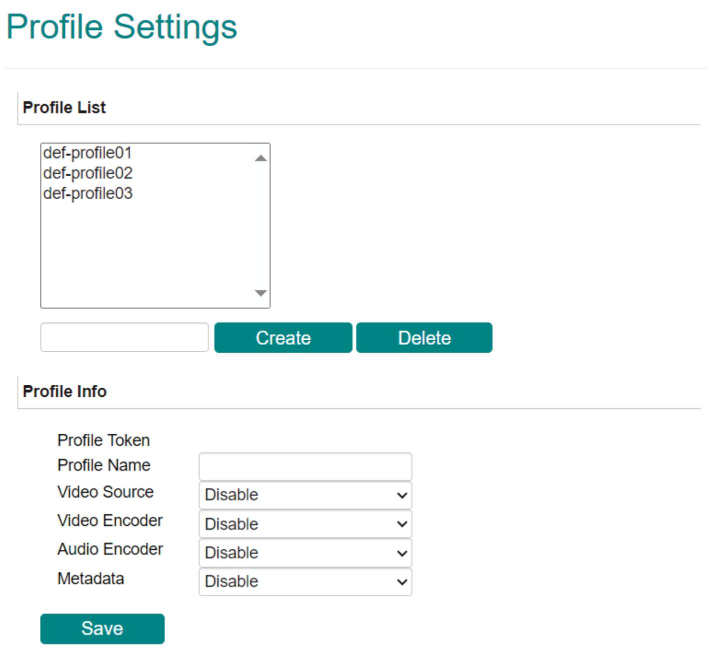
Welcome to the System Configuration pages. A brief description of each configuration group is given below. Click on a plus sign in the left pane to expand a group, and then click on the name of the page you would like to open.

Category	Item	Description and Content
Profiles	Configuration	Configure Profile settings
System	General	Setting Host Name, Contact, Location, Message before login and login fail message
	Date/Time	Setting Date/Time
	Account	Administrator, User and Operator account privileges management
	Account Policy	Configure account login duration, password complexity setting
	System Log	System Log and operation information
	System Parameter	System Parameters information and Import/Export function
	System I/O	Digital Input settings
	LED Control	Setup LED options
	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
	IPv6	Configure IPv6 settings
	Accessible IP	Setup a list to control the access permission of clients by checking their IP address
	RTSP	Configure RTSP
	HTTP	Configure HTTP
	UPnP	Enable UPnP function
	ToS	Configure ToS(Type of Service)
	SNMP	Configure the SNMP settings
	Moxa Service	Moxa search protocol
	SSH	Configure SSH
	LLDP	Configure LLDP
	MQTT Publisher	Configure MQTT Publisher
Video	VideoSource Setting	Configure video source settings
	Image Overlay	Configure the information of video image
	Image Tuning	Configure the attributes of video image
	Privacy Mask	Configure the attributes of Privacy Mask
	Video Encoder	Setup the Encode Standard(MJPEG or H.264), Size (Resolution), FPS, Quality and Multicast settings
	PreAlarm	Setup PreAlarm parameters
Audio	Audio Input	Configure Audio Input settings
Metadata	Metadata	Configure Metadata settings
Streaming	CBRPro	Configure CBRPro settings
	Streaming Status	Get stream connection status
Event	Event Setting	Enable/Disable Event producer
	CPU Event	Configure CPU Event settings
	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, each with its own configured codec (H.265, H.264, MJPEG), resolution, FPS (frame rate), and video quality.

Configuration



Profile Settings

Profile List

def-profile01
def-profile02
def-profile03

Profile Info

Profile Token	
Profile Name	
Video Source	Disable
Video Encoder	Disable
Audio Encoder	Disable
Metadata	Disable

Profile List

Setting	Description	Default

def-profile01
def-profile02
def-profile03
	Choose the video profile. Profile information shown on this page includes Profile Token, Profile Name, Channel number, Video encoder, Audio Encoder.	def-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
Video Source*	Current video source of this ONVIF device.	VideoSourceConfig01
Video Encoder	Select which video encoder this profile will use.	VideoEncoder01
Audio Encoder	Select which audio encoder this profile will use.	AudioEncoder01
Metadata	Enable or disable the metadata being used with the profiles.	metadataCfg01

***This item cannot be edited.**

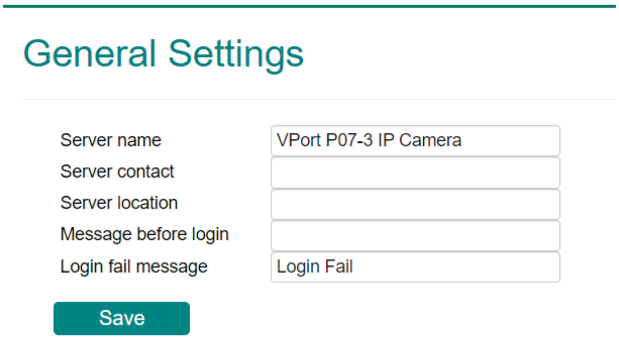
New Profile

You can create additional profiles if needed. Enter 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 P07-3 IP Camera
Server contact	
Server location	
Message before login	
Login fail message	Login Fail

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 07-3 IP camera

Server contact

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

Server location

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

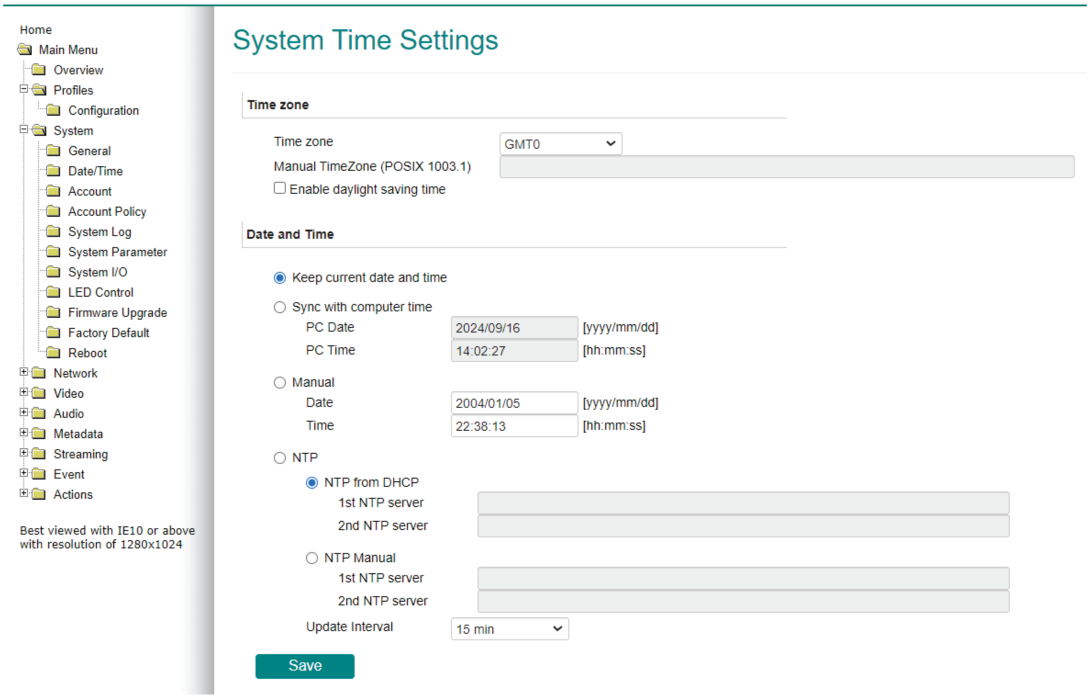
Message before login

Setting	Description	Default
Max. 40 characters	Enter the message that appears before logging in to the VPort's homepage.	Blank

Login fail message

Setting	Description	Default
Max. 40 characters	Enter the message that appears when a user fails to log in.	Blank

Date/Time



System Time Settings

Time zone

Time zone: GMT0

Manual TimeZone (POSIX 1003.1):

□ Enable daylight saving time

Date and Time

● Keep current date and time

○ Sync with computer time

PC Date: 2024/09/16 [yyyy/mm/dd]

PC Time: 14:02:27 [hh:mm:ss]

○ Manual

Date: 2004/01/05 [yyyy/mm/dd]

Time: 22:38:13 [hh:mm:ss]

○ NTP

● NTP from DHCP

1st NTP server

2nd NTP server

○ NTP Manual

1st NTP server

2nd NTP server

Update Interval: 15 min

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.	Keep current date and time
Sync with computer time	Synchronize the VPort’s data and time setting with the local computer time.	
Manual	Manually set the VPort’s date and time.	
NTP	Use an NTP server to set the VPort’s date and time.	

NOTE

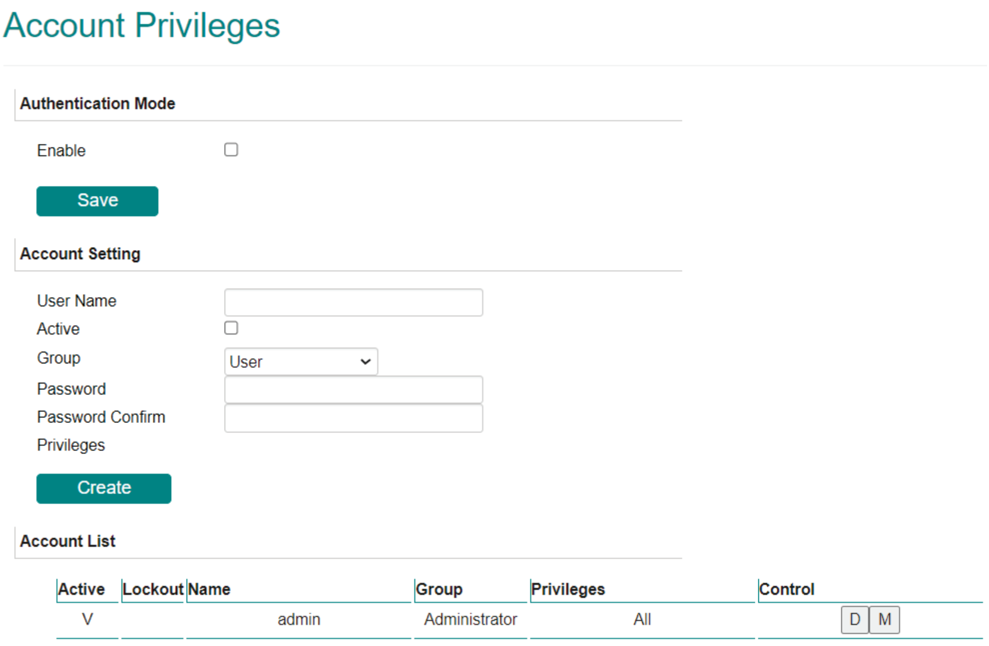
Select the **NTP** option to force the VPort to synchronize automatically with timeservers over the Internet. However, synchronization may fail if the assigned **NTP server** cannot be reached, or the VPort is connected to a local network. Enter either the Domain name or IP address format of the timeserver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

Authentication Mode

Enable □

Account Setting

User Name
Active □
Group: User
Password
Password Confirm
Privileges

Account List

Active	Lockout	Name	Group	Privileges	Control
V		admin	Administrator	All	D M

Authentication Enable

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

NOTE

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

Account Setting

Setting	Description	Default
User name	Enter the username for user authentication.	Blank
Active	Check the box to activate or uncheck it to deactivate the corresponding account.	Inactive
Group	Select the ONVIF group to assign the user to (User, Operator, or Administrator). Each group has different privileges. Refer to ONVIF specifications for the user access policy for each group.	User
Password	Enter the password for user authentication.	Blank
Password Confirmation	Enter the password again for confirmation.	Blank

Click **Create** to create the user account. The account will appear in the **Account List**.

Click **D** in the **Control** column to delete the corresponding user account.

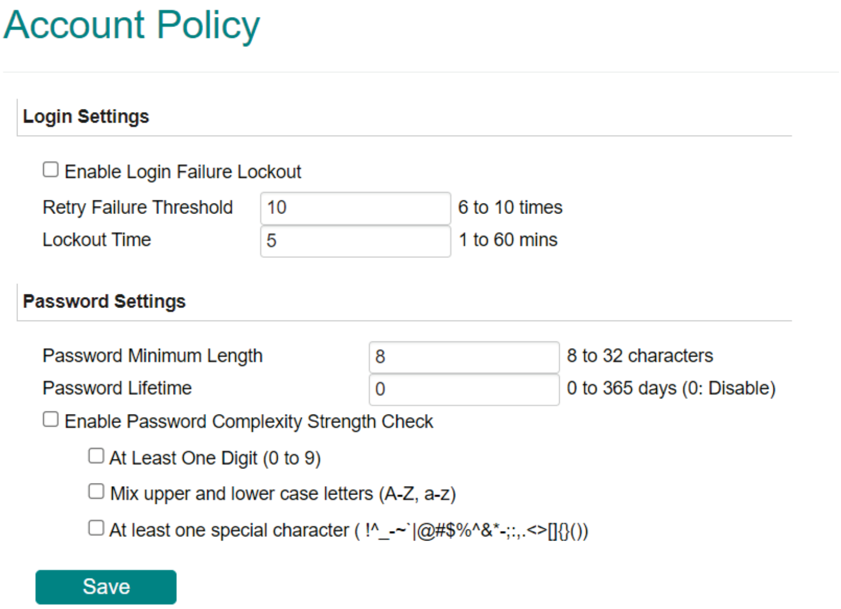
Click **M** in the **Control** column to modify the corresponding user account.

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.

Account Policy

The **Account Policy** page allows you to configure login and password policy settings.



Account Policy

Login Settings

☐ Enable Login Failure Lockout

Retry Failure Threshold: 10 (6 to 10 times)

Lockout Time: 5 (1 to 60 mins)

Password Settings

Password Minimum Length: 8 (8 to 32 characters)

Password Lifetime: 0 (0 to 365 days (0: Disable))

☐ Enable Password Complexity Strength Check

- ☐ At Least One Digit (0 to 9)
- ☐ Mix upper and lower case letters (A-Z, a-z)
- ☐ At least one special character (!^_-~`|@#$%^&*-;:,.<>[]{}())

Login Settings

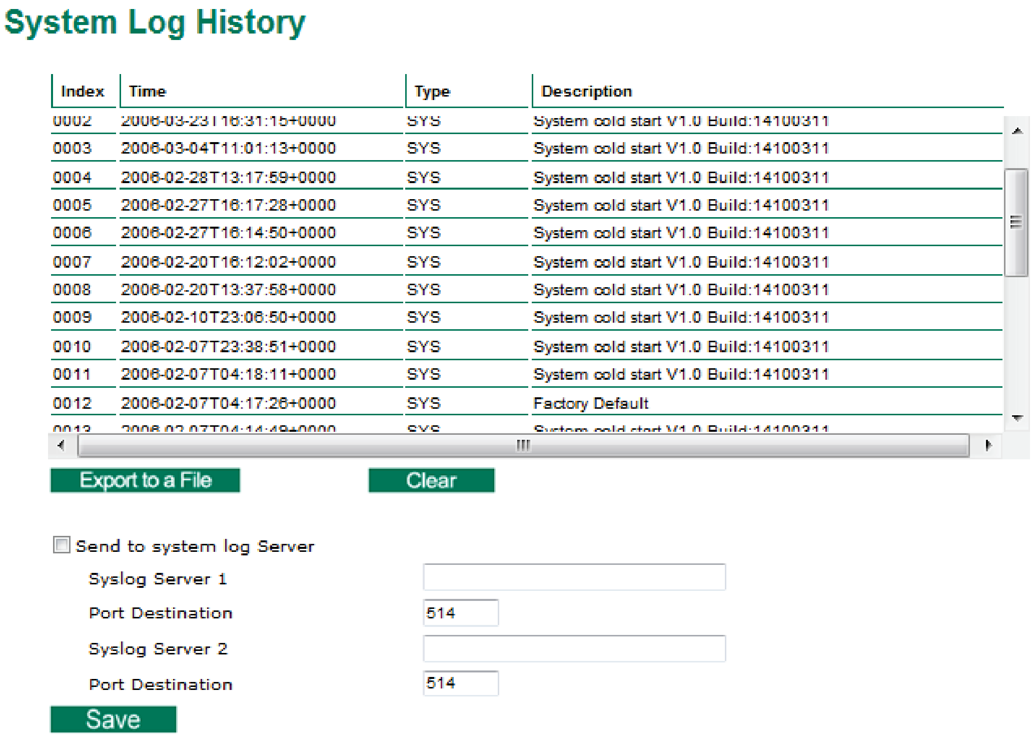
Setting	Description	Default
Enable Login Failure Lockout	Enable or disable login lockout. If a user fails to log in consecutively for the specified amount of retry attempts, the user will be locked out for the specified duration.	Disabled
Retry Failure Threshold	Specify the number of retry attempts allowed before the user is locked out.	10
Lockout time	Specify the duration (in minutes) the user will be locked out for after failing to log in too many times.	5

Password Settings

Setting	Description	Default
Password Minimum Length	Specify the minimum required character length for passwords.	8
Password Lifetime	Specify the duration a password is valid before users are required to update their password.	0 (Disabled)
Enable Password Complexity Strength Check	Enable or disable enforcing password complexity checks. Check the boxes to enable the corresponding complexity requirement(s).	Disabled

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

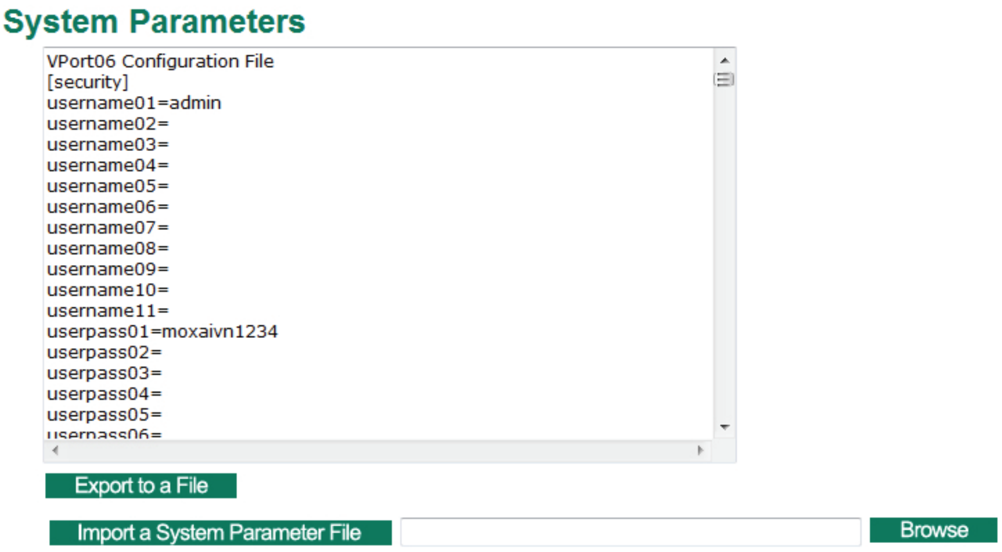
Setting	Description	Default
Send to system log server	Enables sending the system log to the log sever	Disable
Syslog Sever 1	The address of the first system log server	Blank
Port Destination	The port number of the first system log server	514
Syslog Sever 2	The address of the second system log server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



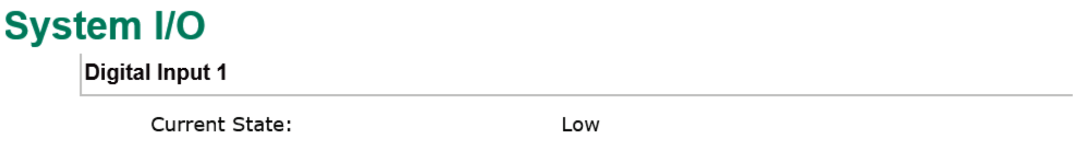
```
VPort06 Configuration File
[security]
username01=admin
username02=
username03=
username04=
username05=
username06=
username07=
username08=
username09=
username10=
username11=
userpass01=moxaivn1234
userpass02=
userpass03=
userpass04=
userpass05=
userpass06=
```

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.

System I/O

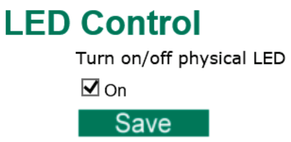
This page shows the current status of the camera's digital input.



Current State: Low

LED Control

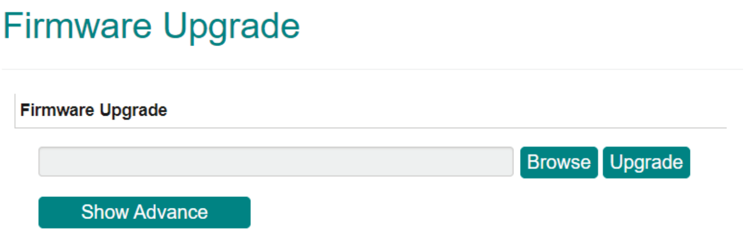
From this page, users can enable or disable the physical LED on the device.



Turn on/off physical LED

☑ On

Firmware Upgrade



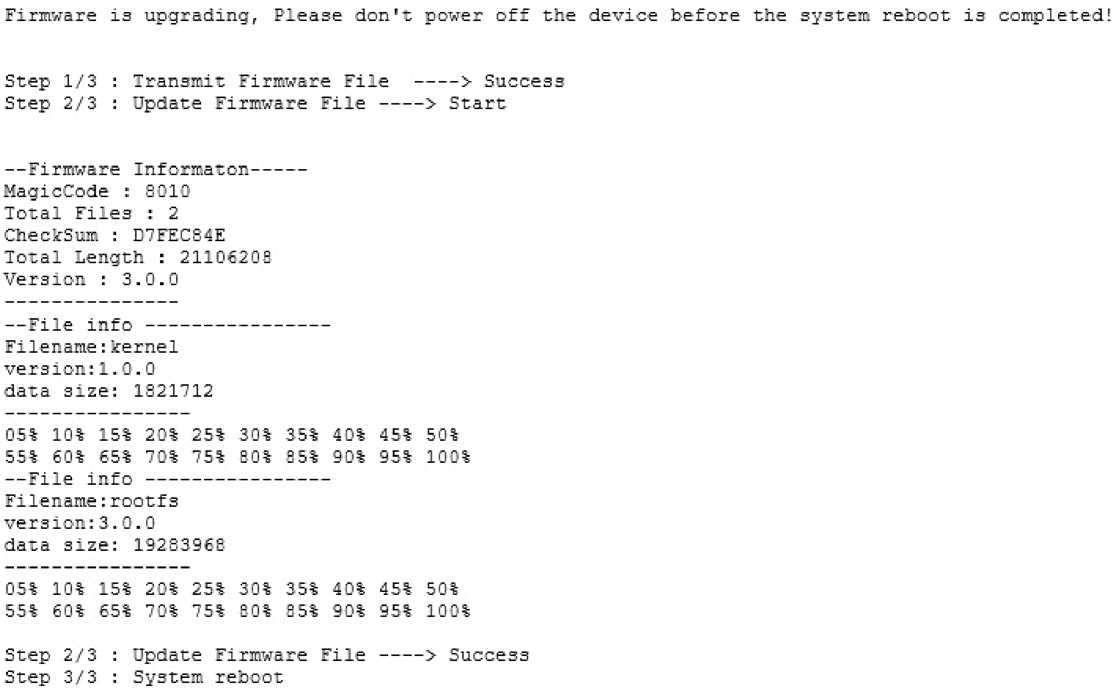
Take the following steps to upgrade the firmware:

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.



```
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 : 8010
Total Files : 2
CheckSum : D7FEC84E
Total Length : 21106208
Version : 3.0.0
---------------
--File info ----------------
Filename:kernel
version:1.0.0
data size: 1821712
----------------
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:3.0.0
data size: 19283968
----------------
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

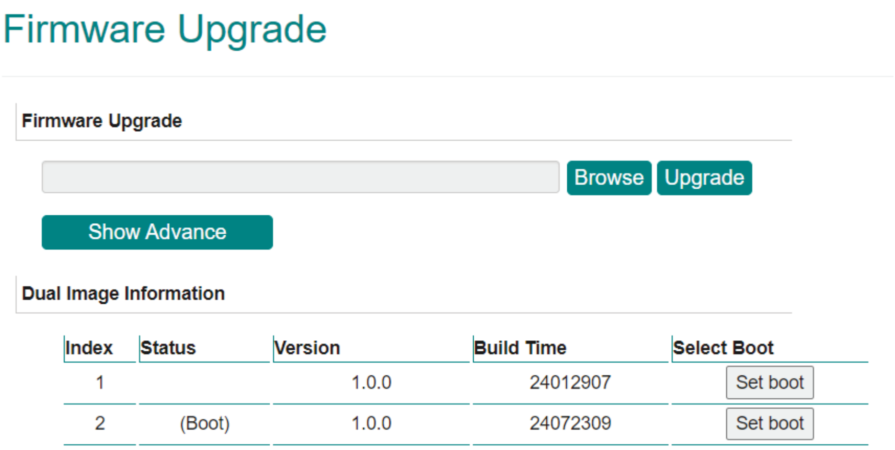
For the VPort, the firmware file extension should be **.rom**.

NOTE

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

Show Advance

The VPort camera supports dual firmware functionality for redundancy in the event of issues.



Index	Status	Version	Build Time	Select Boot
1		1.0.0	24012907	Set boot
2	(Boot)	1.0.0	24072309	Set boot

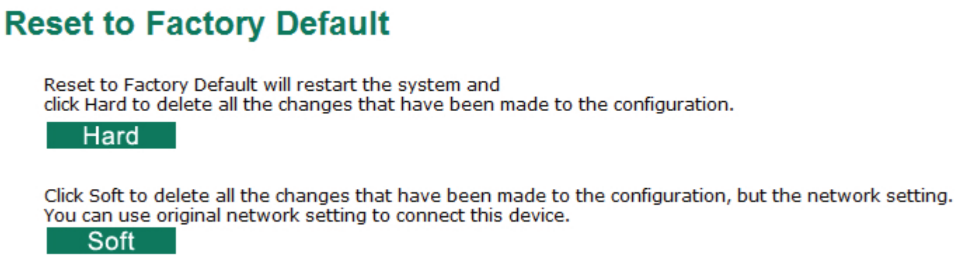
Step 1: Click the **Show Advance** button to access dual firmware settings.

Step 2: Select the firmware versions and set the primary boot firmware by clicking **Set boot**. If the system fails to load the primary software, it will load the secondary firmware instead.

Step 3: Click **Save** to save your 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

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

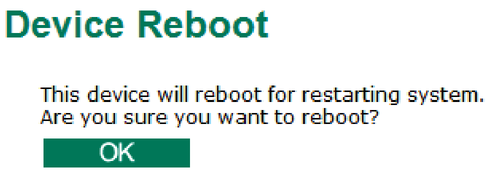
Click Soft to delete all the changes that have been made to the configuration, but the network setting.
You can use original network setting to connect this device.

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.



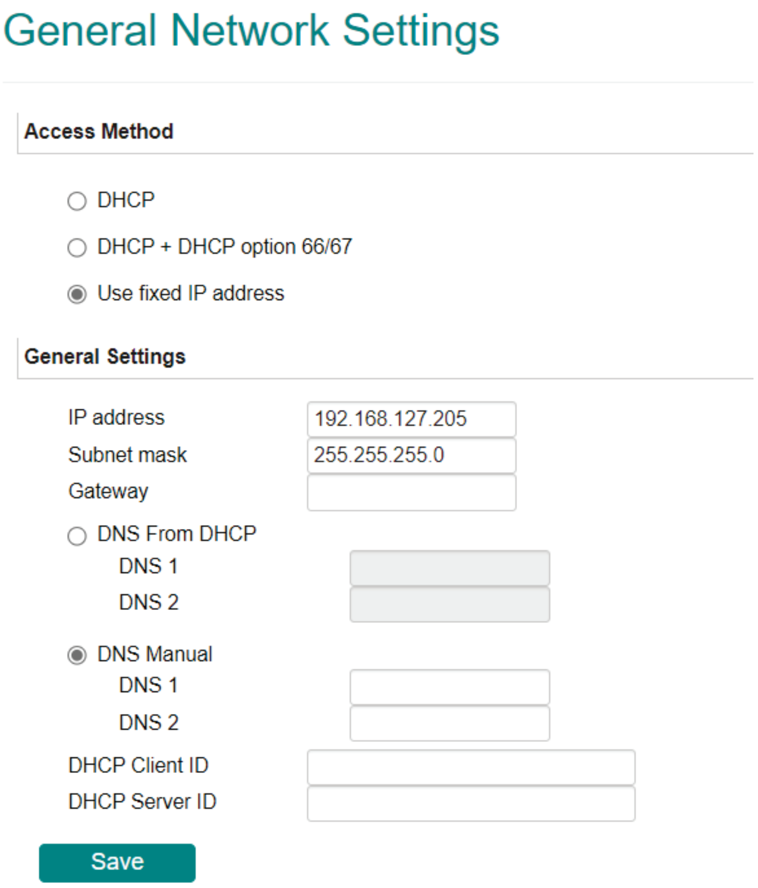
Device Reboot

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: 192.168.127.205

Subnet mask: 255.255.255.0

Gateway:

○ DNS From DHCP

DNS 1:

DNS 2:

● DNS Manual

DNS 1:

DNS 2:

DHCP Client ID:

DHCP Server ID:

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.	

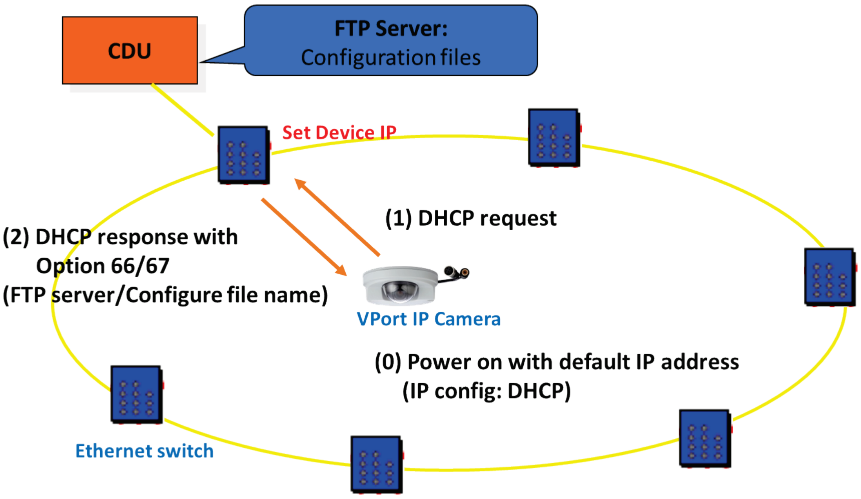
NOTE

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.

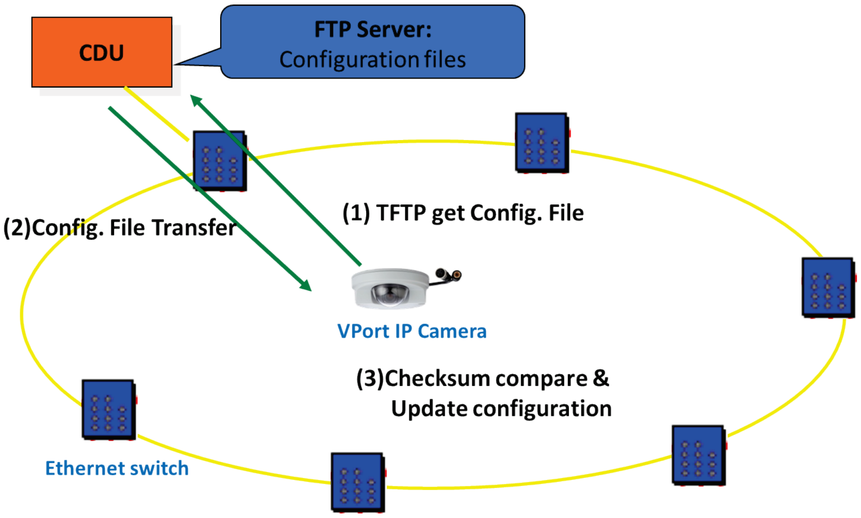
DHCP Option 66/67 for auto configuration

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

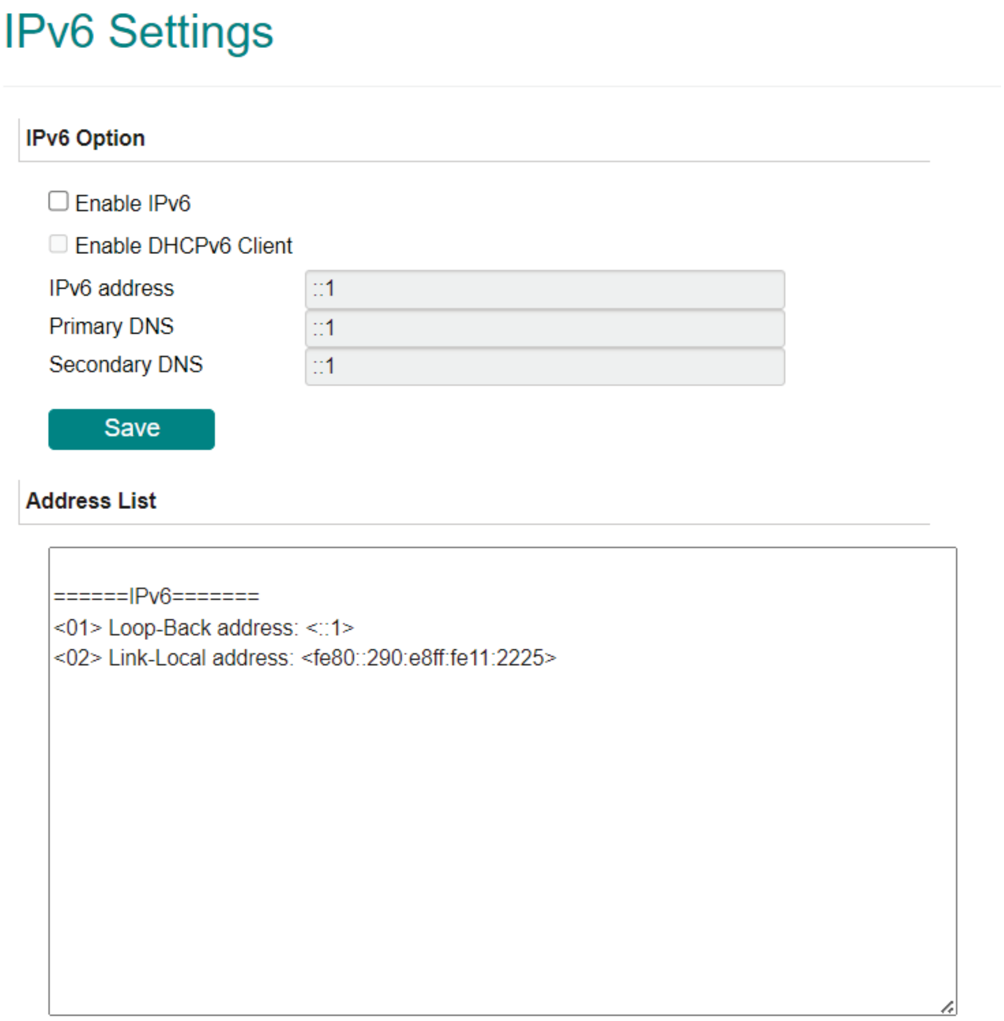
For the auto-configuration function to work, the system should

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
DNS Manual	Manually specify the DNS server address.	Disable
DNS 1	Enter the IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can Enter 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.
DNS 2	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

IPv6



IPv6 Settings

IPv6 Option

□ Enable IPv6

□ Enable DHCPv6 Client

IPv6 address: ::1

Primary DNS: ::1

Secondary DNS: ::1

Address List

```
======IPv6=======
<01> Loop-Back address: <::1>
<02> Link-Local address: <fe80::290:e8ff:fe11:2225>
```

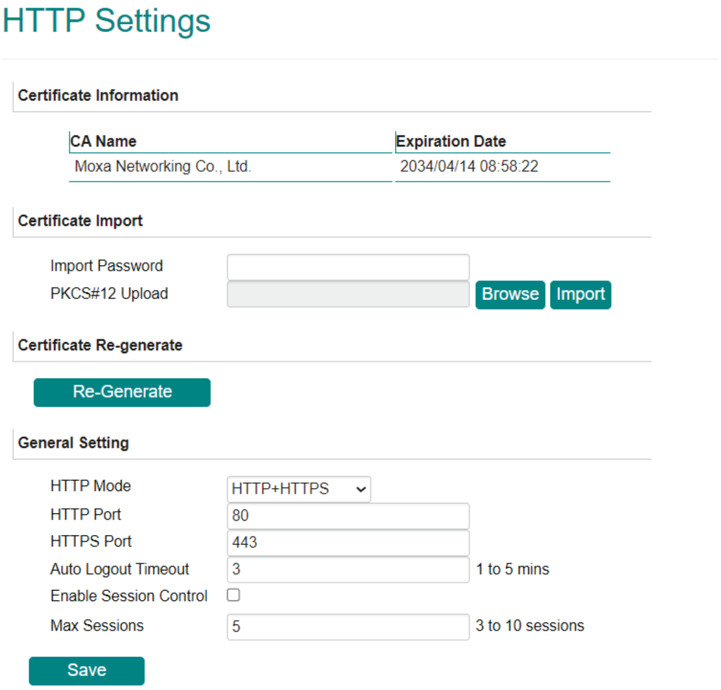
IPv6 Option

Setting	Description	Factory Default
Enable IPv6	Enable or disable IPv6.	Disable
Enable DHCPv6 Client	Enable or disable the DHCPv6 Client. If enabled, the system will automatically get an IPv6 address from the DHCP server.	Disable
IPv6 Address	Show the IPv6 address assigned by the DHCP server.	Blank
Primary DNS	Show the primary DNS IPv6 address assigned by the DHCP server.	Blank
Secondary DNS	Show the secondary DNS IPv6 address assigned by the DHCP server.	Blank

Address List

The IPv6 address list shows all IPv6 addresses relevant to the camera.

HTTP



HTTP Settings

Certificate Information

CA Name	Expiration Date
Moxa Networking Co., Ltd.	2034/04/14 08:58:22

Certificate Import

Import Password

PKCS#12 Upload

Certificate Re-generate

General Setting

HTTP Mode: HTTP+HTTPS

HTTP Port: 80

HTTPS Port: 443

Auto Logout Timeout: 3 1 to 5 mins

Enable Session Control: □

Max Sessions: 5 3 to 10 sessions

Certificate Information

This section shows information about the digital SSL certificate information provided by Moxa. This certificate allows users to access the VPort's web-based interface via a trusted HTTPS connection.

Certificate Import

From this section, you can import a third-party certificate.

Setting	Description	Factory Default
Import password	Enter the password of the third-party certificate.	Blank
PKCS#12 Upload	Click **Browse** to navigate to the certificate file on your local drive. With the certificate file selected, click **Import** to upload the certificate.	Blank

Certificate Re-generate

Click the **Re-Generate** button to regenerate VPort's SSL certificate.

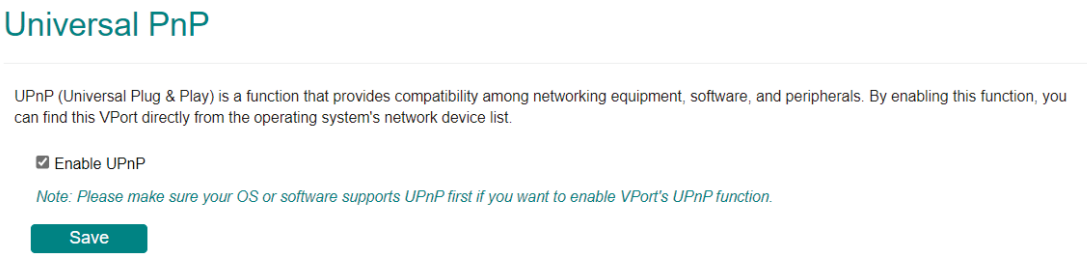
General Settings

Setting	Description	Factory Default
HTTP Mode	Select the HTTP mode: HTTP only, HTTP+HTTPS, or Disable.	HTTP+HTTPS
HTTP Port	Specify the HTTP port. The valid range is 80, or 1024 to 65535.	80

Setting	Description	Factory Default
HTTPS Port	Specify the HTTPS port. The valid range is 1 to 65535.	443
Auto Logout Timeout	Configure the idle duration (in minutes) before the user is automatically logged out of the web interface.	3
Enable Session Control	Enable or disable session control when accessing the VPort's web interface. This determines the number of concurrent sessions allowed.	Disabled
Max Sessions	If Session Control is enabled, specify the maximum number of concurrent sessions allowed to access the VPort's web interface at any given time.	5

UPnP

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



Universal PnP

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

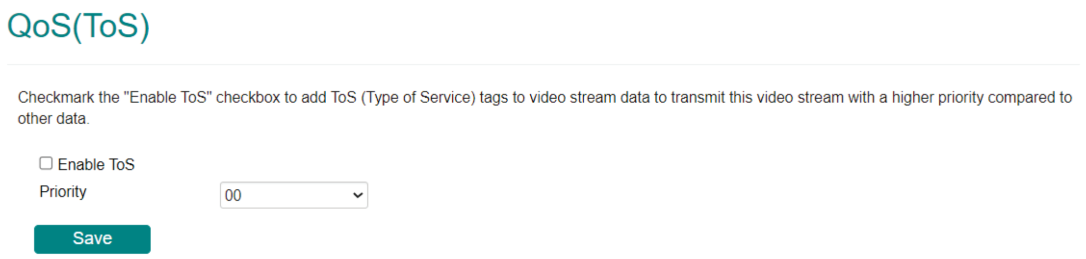
☑ Enable UPnP

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

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

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)

Checkmark the "Enable ToS" checkbox to add ToS (Type of Service) tags to video stream data to transmit this video stream with a higher priority compared to other data.

☐ Enable ToS

Priority 00

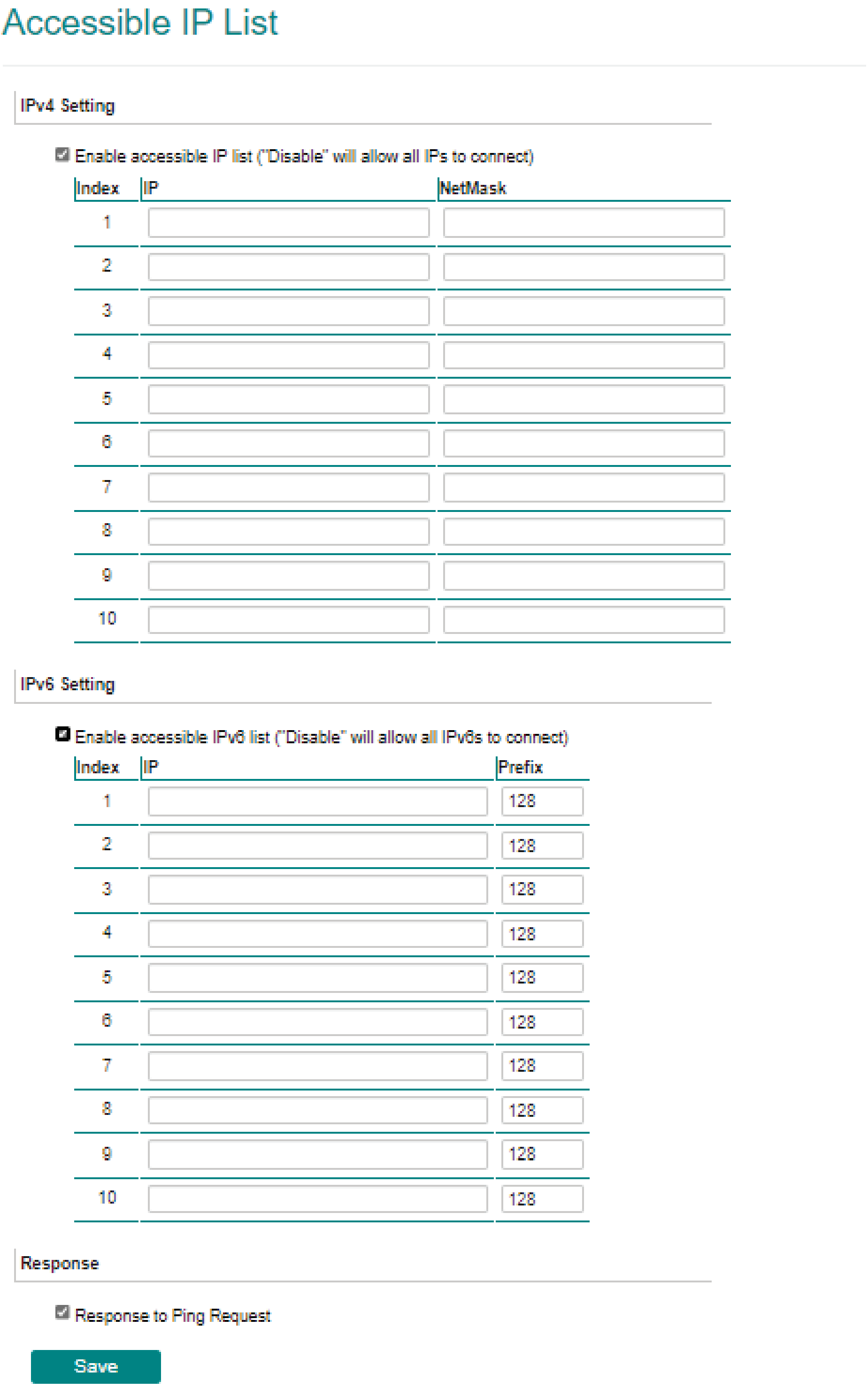
Setting	Description	Factory Default
Enable ToS	Enable ToS to transmit the video stream with the given priority.	Disable
Priority	Configure the mapping table with different ToS values.	00

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

IPv4 Setting

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

Index	IP	NetMask
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

IPv6 Setting

☑ Enable accessible IPv6 list ("Disable" will allow all IPv6s to connect)

Index	IP	Prefix
1		128
2		128
3		128
4		128
5		128
6		128
7		128
8		128
9		128
10		128

Response

☑ Response to Ping Request

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:

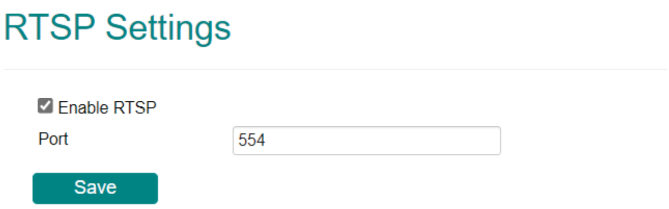
- Allow only one host with a specific "IP address" to access the VPort. For example,
  IP = 192.168.1.16 NetMask = 255.255.255.255
  will only allow the host with IP = 192.168.1.16 to access the VPort.

- 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

RTSP



RTSP Settings

☑ Enable RTSP

Port: 554

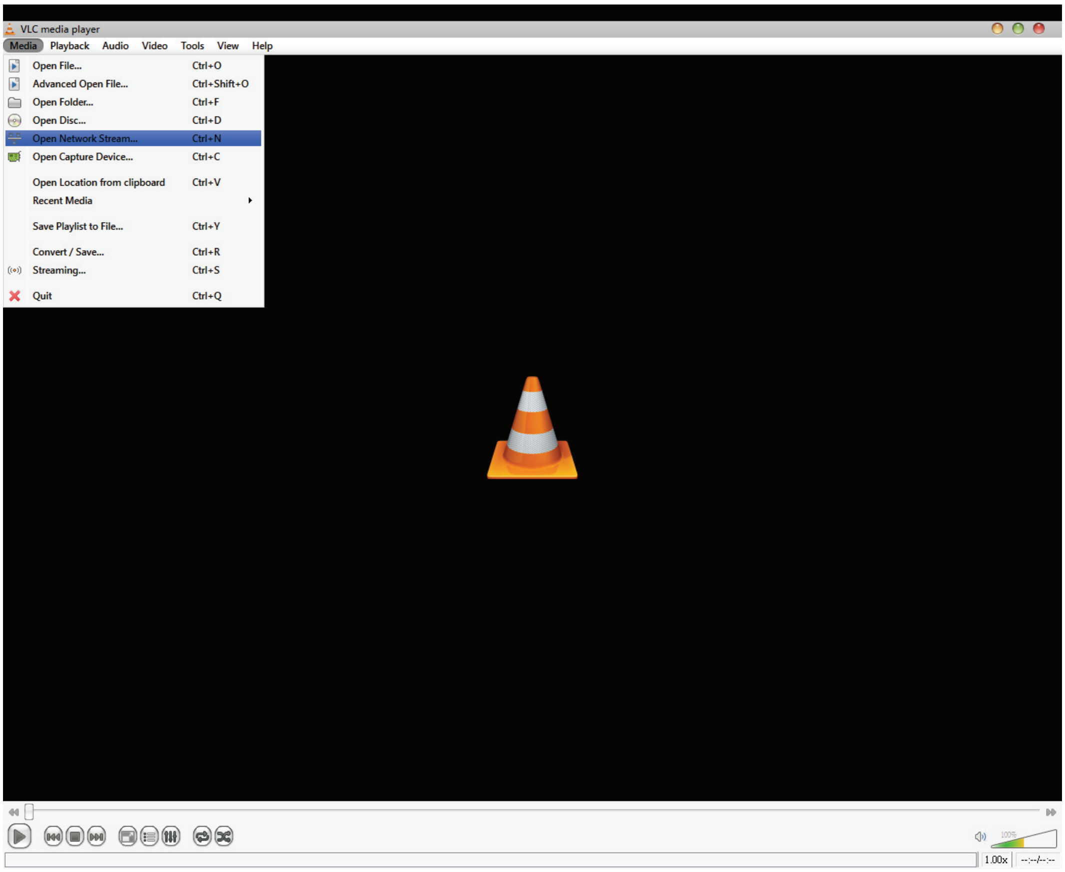
RTSP Streaming

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

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



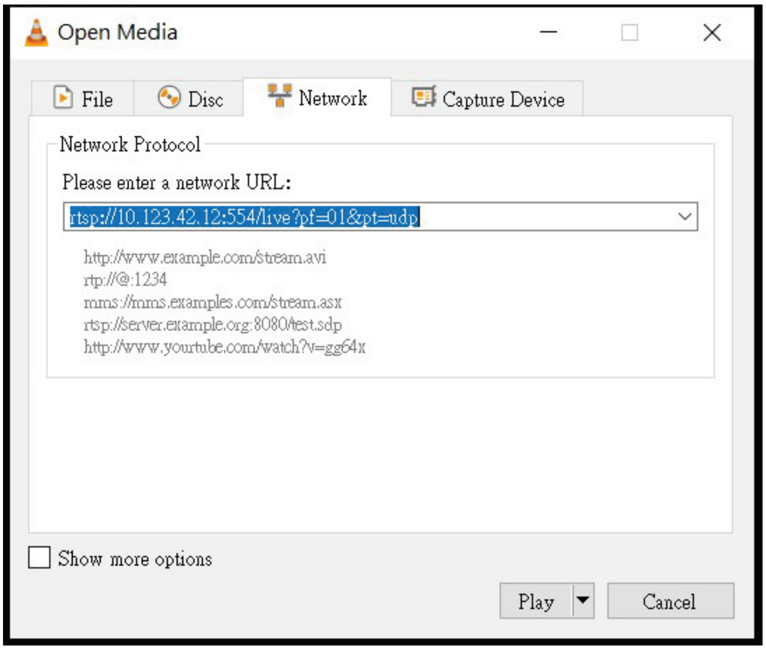
Step 2: When the following pop-up window appears, type the URL in the input box. E.g., type

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.

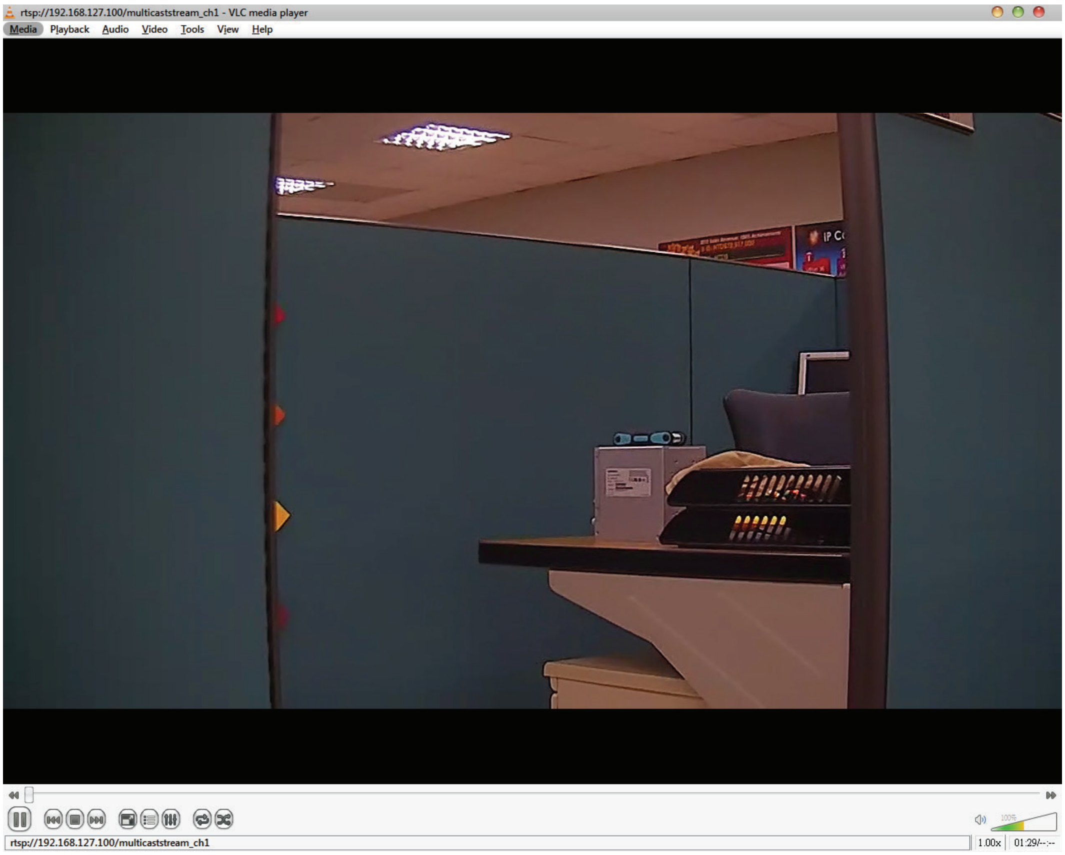

Open Media
File
Disc
Network
Capture Device
Network Protocol

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

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

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.

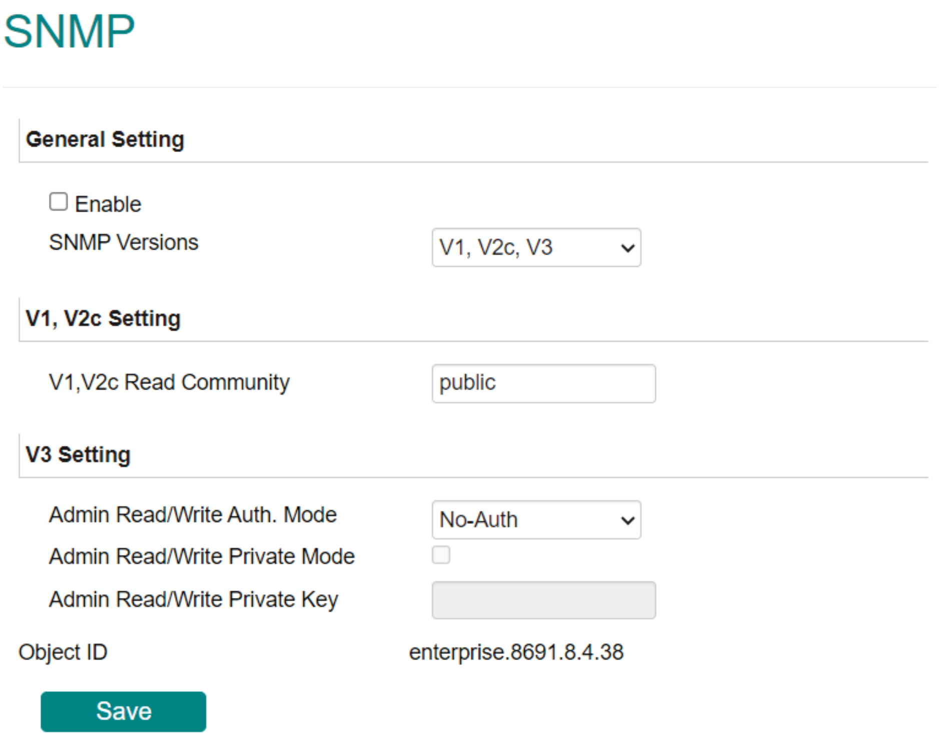
SNMP

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
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

General Setting

□ Enable

SNMP Versions: V1, V2c, V3

V1, V2c Setting

V1,V2c Read Community: public

V3 Setting

Admin Read/Write Auth. Mode: No-Auth

Admin Read/Write Private Mode: □

Admin Read/Write Private Key:

Object ID: enterprise.8691.8.4.38

General Settings

Enable

Setting	Description	Default
Checkbox	Check to enable SNMP functionality. If enabled, selected the SNMP versions to use from the drop-down box.	Disable
SNMP Versions	Select SNMP protocol versions to manage the VPort.	V1, V2c, V3

V1, V2c Setting

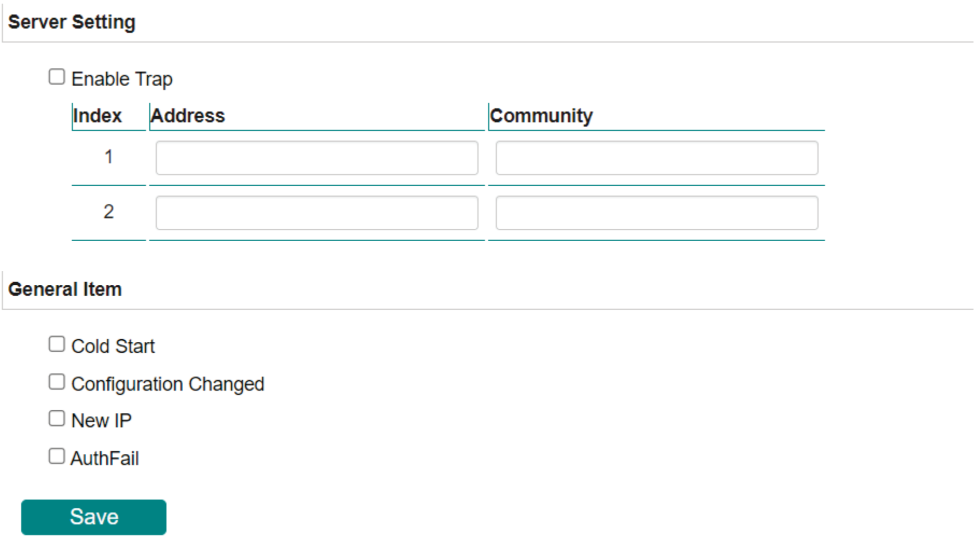
Setting	**Description**	**Default**
V1, V2c Read Community	Use a community string match for authentication. This means that the SNMP agent accesses all objects with read-only permissions using the community string public.	public (max. 30 characters)

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 allow writing to the file.

V3 Setting

Setting	**Description**	**Default**
Admin Read/Write Auth. Mode	Select the admin authentication model: **No-Auth**: Do not use authentication. **MD5**: Use authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication. **SHA**: Use authentication based on the MAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No-Auth
Admin Read/Write Private Mode	Enable or disable Admin Read/Write private mode.	Disabled
Admin Read/Write Private Key	If Admin Read/Write Private Mode is enabled, specify the data encryption key (8 to 30 characters).	Blank

SNMP Trap


Server Setting

□ Enable Trap

Index	Address	Community
1		
2		

General Item

□ Cold Start

□ Configuration Changed

□ New IP

□ AuthFail

Server Setting

Setting	**Description**	**Default**
Enable Trap	Enable or disable SNMP Trap functionality.	Disabled
1st and 2nd Trap Server IP/Name	Enter the IP address or name of the Trap Server used by your network.	Blank
1st and 2nd Trap Community	Use a community string match for authentication; Maximum of 30 characters.	Blank

General Item

Setting	**Description**	**Default**
Checkbox	Check the box to enable triggering an SNMP Trap for the corresponding event.	None

Setting	Description	Default
1st and 2nd Trap Server IP/Name	Enter the IP address or name of the Trap Server used by your network.	Blank

Private MIB information

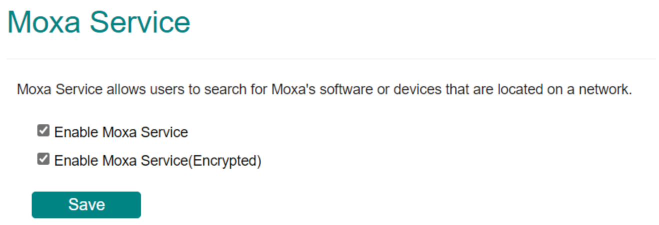
Different VPorts have different object IDs.

NOTE

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

Moxa Service

Moxa Service is a Moxa proprietary discovery protocol. If necessary, you can disable this function to prevent the camera from being discovered by the Moxa's VPort and EtherDevice Configurator Utility.



Moxa Service

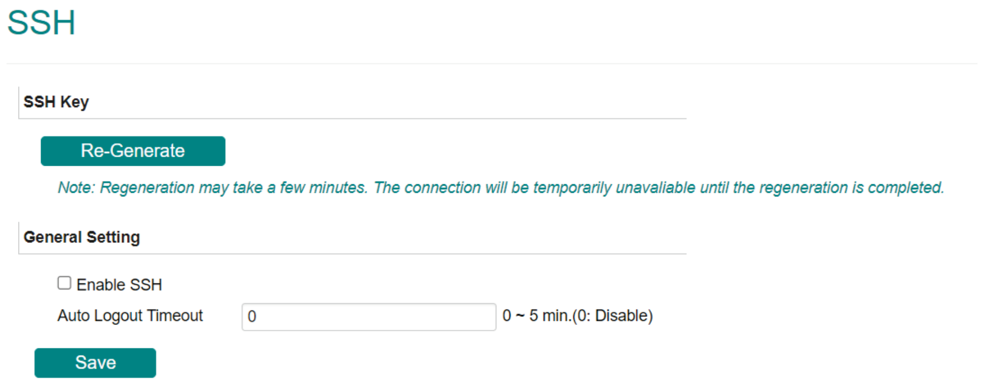
Moxa Service allows users to search for Moxa's software or devices that are located on a network.

☑ Enable Moxa Service

☑ Enable Moxa Service(Encrypted)

SSH

Use this function to enable/disable the SSH function.



SSH

SSH Key

Note: Regeneration may take a few minutes. The connection will be temporarily unavaliable until the regeneration is completed.

General Setting

☐ Enable SSH

Auto Logout Timeout 0 0 ~ 5 min.(0: Disable)

Server Setting

Click **Re-Generate** to regenerate the SSH key.

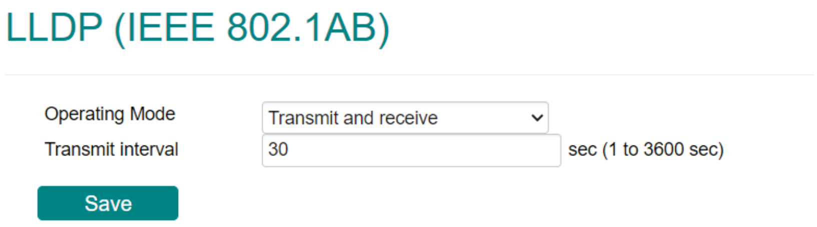
General Setting

Setting	Description	Default
Enable SSH	Enable or disable SSH functionality.	Disabled
Auto Logout Timeout	Configure the idle time (in min) before being automatically logged out of the SSH connection.	0 (disabled)

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.



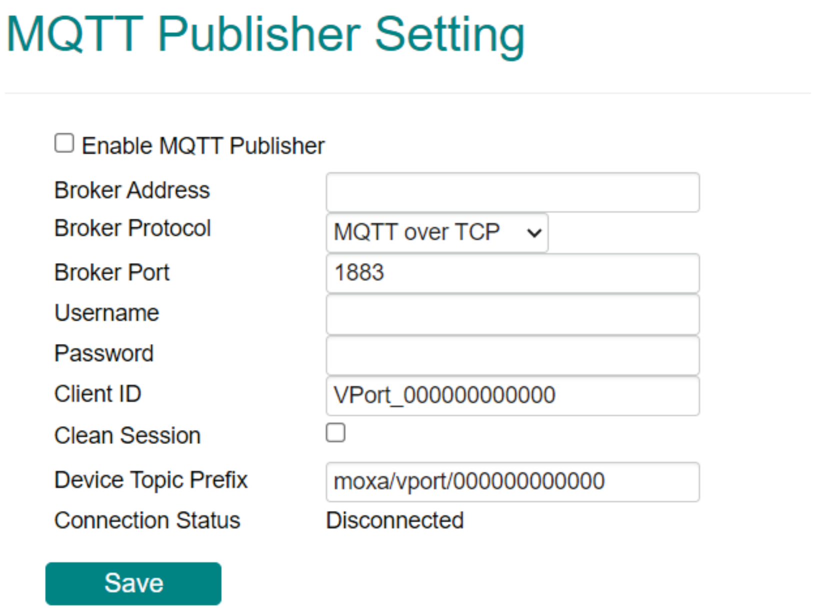
LLDP (IEEE 802.1AB)

Operating Mode: Transmit and receive

Transmit interval: 30 sec (1 to 3600 sec)

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

MQTT Publisher



MQTT Publisher Setting

☐ Enable MQTT Publisher

Broker Address:

Broker Protocol: MQTT over TCP

Broker Port: 1883

Username:

Password:

Client ID: VPort_000000000000

Clean Session: ☐

Device Topic Prefix: moxa/vport/000000000000

Connection Status: Disconnected

Setting	Description	Default
Enable MQTT Publisher	Enable or disable the MQTT Publisher function.	Disable
Broker Address	Specify the MQTT broker address.	Blank
Broker Protocol	Select the protocol used to communicate with the broker.	MQTT over TCP
Broker port	Specify the broker port.	1883
Username	Enter the authentication username to access MQTT information.	Blank
Password	Enter the authentication password to access MQTT information.	Blank
Client ID	Specify the VPort's client ID.	VPort_ 000000000000

Setting	Description	Default
Clean Session	Enable or disable clean MQTT sessions. If enabled, the MQTT connection will be terminated after sending or receiving MQTT information to free up system resources.	Disable
Device Topic Prefix	Specify the VPort device's MQTT information prefix.	Blank
Connection Status	Shows the current MQTT connection status.	Disconnected

Video

Video Source

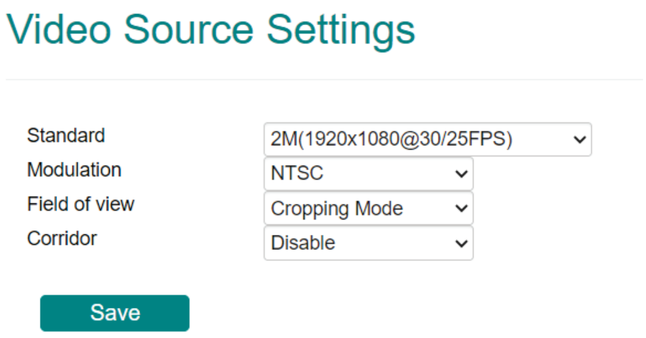
The **Video Source** page lets you configure the video stream resolution, field of view, and image rotation settings.

NOTE

If the source video image is 3 megapixels (2048 x 1536), the maximum frame rate is limited to 20 FPS no matter what image resolution is configured.

NOTE

Changing the video source settings requires a system reboot to take effect.



Video Source Settings

Standard	2M(1920x1080@30/25FPS)
Modulation	NTSC
Field of view	Cropping Mode
Corridor	Disable

Setting	Description	Default
Standard	Select the source video image resolution.	2M (1920x1080@30/35FPS)
Modulation	Select the video encoding standard.	NTSC
Field of view	Select a field of view mode which determines how resolution changes are processed. **Cropping Mode**: This mode will alter the size of the video capture region. **Scaling Mode**: This mode will alter the object ratio to fit all content into the frame.	Cropping Mode
Corridor	Select the image rotation degree to improve coverage of corridors. The image can be rotated 90, 180, or 270 degrees.	Disable

Image Overlay

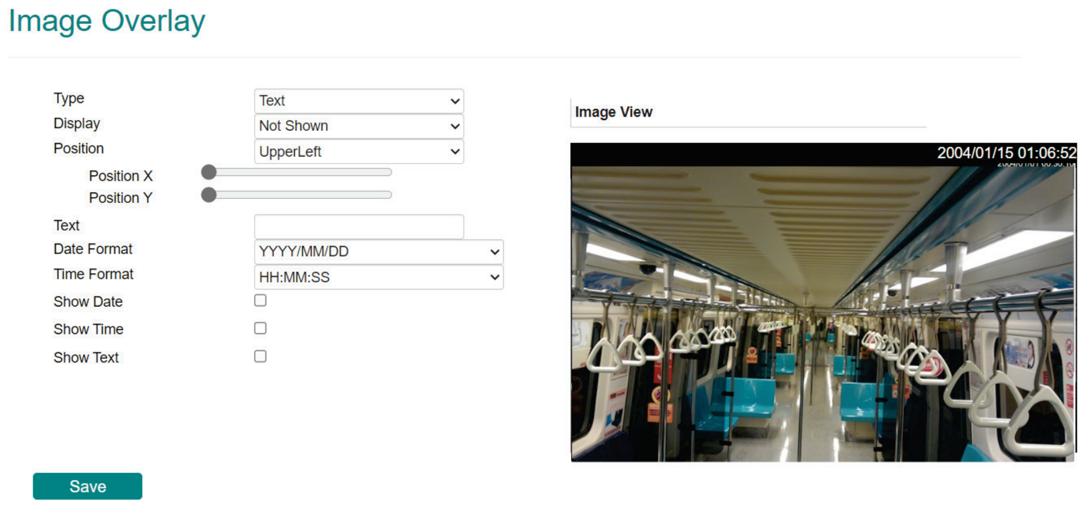


Image Overlay

Type: Text

Display: Not Shown

Position: UpperLeft

Position X

Position Y

Text:

Date Format: YYYY/MM/DD

Time Format: HH:MM:SS

Show Date □

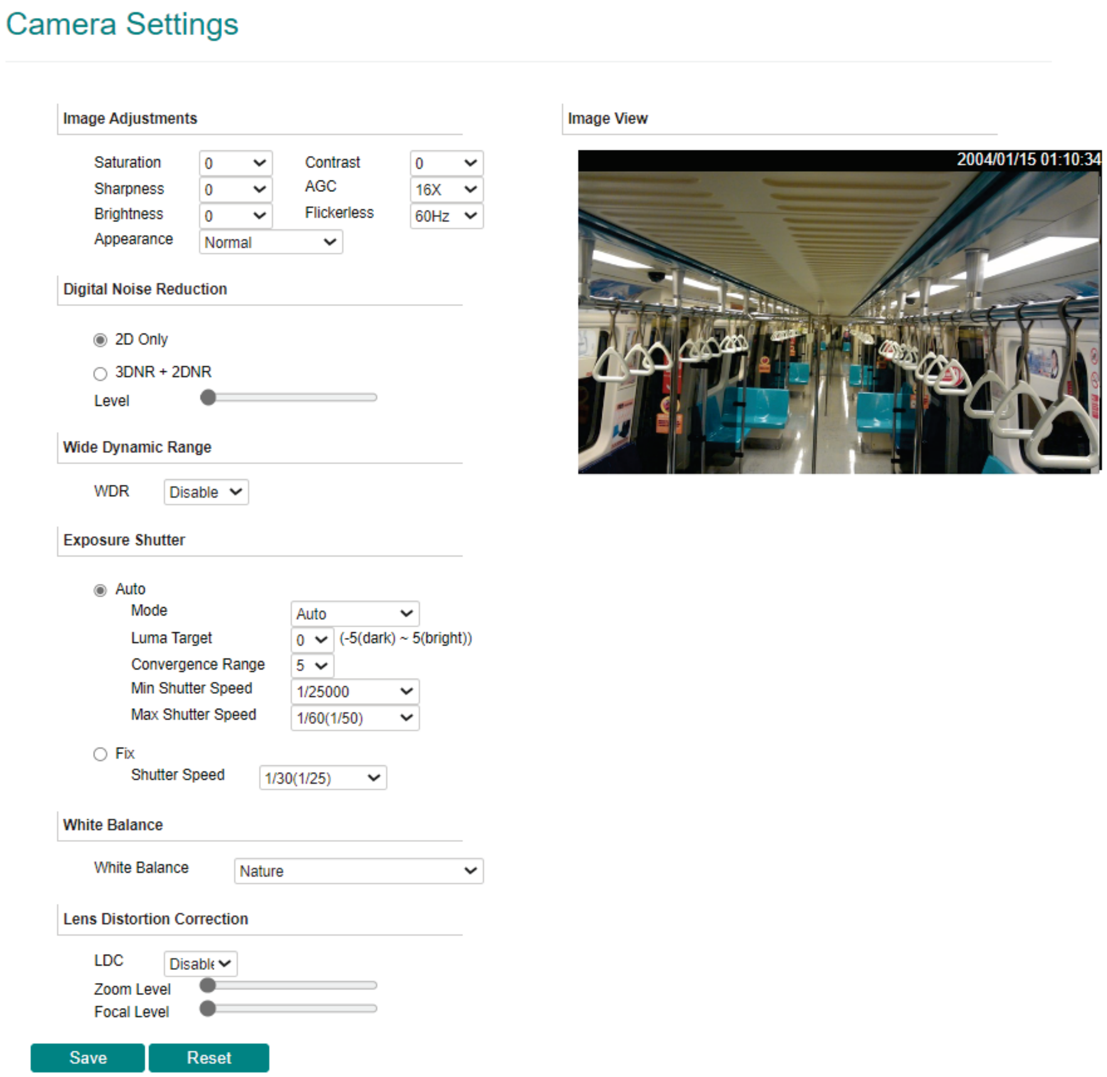
Show Time □

Show Text □

Setting	Description	Default
Type	Select the Text or Image shown on the video image	Text
Display	Select a display mode for the overlay text: Not Shown, Show on the Caption, Show on image.	Not shown
Position	Choose the default position of the overlay text on the image. Alternatively, use the Position X and Position Y sliders to manually adjust the text position. The actual position is based on the configured resolution.	Upper Left
Text	Enter the text that will be overlayed on the image.	Blank
Date Format	Select the date format shown on the video image.	YYYY/MM/DD
Time Format	Select the time format shown on the video image.	HH:MM:SS
Show Date	Enable or disable showing date information in the overlay text.	Disable
Show Time	Enable or disable showing time information in the overlay text.	Disable
Show Text	Enable or disable showing custom text in the overlay text.	Disable

Image Tuning

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



Camera Settings

Image Adjustments

Saturation: 0
Sharpness: 0
Brightness: 0
Appearance: Normal
Contrast: 0
AGC: 16X
Flickerless: 60Hz

Digital Noise Reduction

● 2D Only
○ 3DNR + 2DNR
Level

Wide Dynamic Range

WDR: Disable

Exposure Shutter

● Auto
Mode: Auto
Luma Target: 0 (-5(dark) ~ 5(bright))
Convergence Range: 5
Min Shutter Speed: 1/25000
Max Shutter Speed: 1/60(1/50)

○ Fix
Shutter Speed: 1/30(1/25)

White Balance

White Balance: Nature

Lens Distortion Correction

LDC: Disable
Zoom Level
Focal Level

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
Brightness	Select a value from -4 to +4.	0
Flickerless	Adjust the sensor scan frequency to synchronize with the environmental lighting frequency.	60 Hz
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
Disable, 2D only, 3DR+2DR	Enable or disable the digital noise reduction function. If enabled, select the 2D only or 3DR+2DR noise filter mode.	Disable
Level	Use the tuner bar to adjust the DNR level.	Low

WDR

Setting	Description	Default
WDR	Configure the WDR mode from Level 1 to Level 8, or enable/ disable, depending on the 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.	Disable

Exposure Shutter

Setting	Description	Default
Auto	Configure the exposure shutter in Auto, Backlight, or Manual mode with a luma target ranging from -5 (dark) to +5 (bright). Select the convergence range from 0 (more sensitive) to 255 (less sensitive) to determine the sensitivity of the exposure shutter. The maximum and minimum shutter speed can be also configured as required.	Luma target: 0 Convergence range: 5 Min. shutter speed: 1/25000 Max shutter speed: 1/60 (1/50)
Fix	Set the shutter to a fixed speed of 1 to 1/25000 seconds.	1/30 (1/25)

White Balance

Setting	Description	Default
White balance	Choose a white balance mode. For most conditions, we suggest using Nature to allow the camera to automatically adjust the white balance. Other available white balance modes include Tungsten light (3100K), White Fluorescent light (4100K), Day Light (5300K), Cloudy (6500K, ATW), and Shade (7500K).	Nature

Line Distortion Correction

The line distortion correction function helps straighten the edges of bent images made with low focal-length lenses.

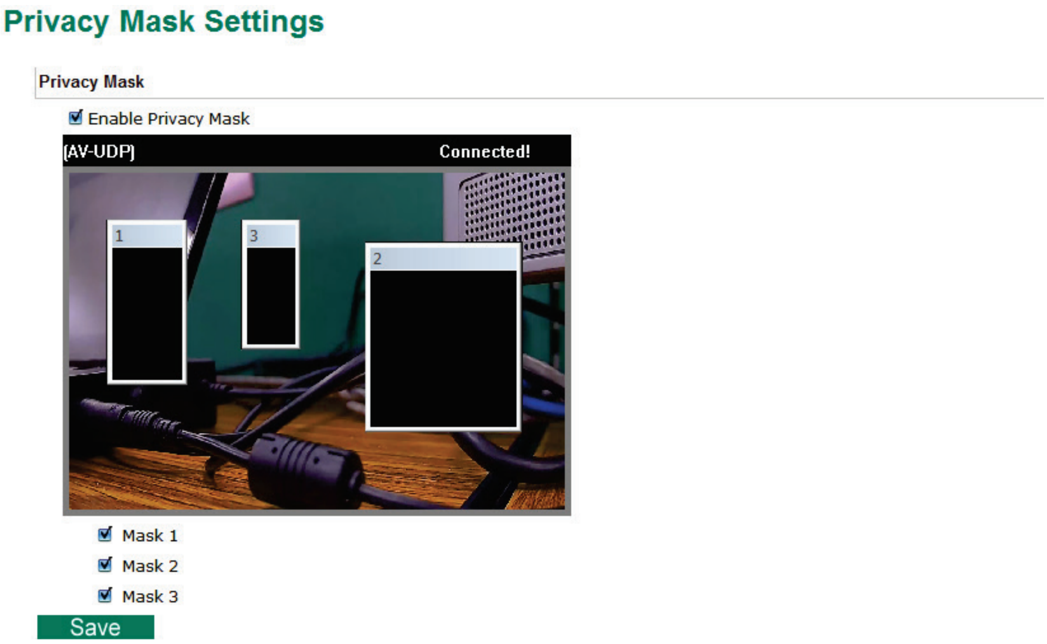
Setting	Description	Default
LDC	Enable or disable the line distortion correction function based on the lens's focal length (2.4 mm, 3.6 mm, 4.2 mm, 6.0 mm, 8.0 mm).	Disable
Zoom Level	Use the tuning bar to adjust the zoom level of line distortion correction. The preview image in the Image View section shows the image with the selected level of line distortion correction applied. Use the **Save** and **Reset** buttons to save or reset the line distortion settings accordingly.	None
Focal Level	Use the tuning bar to adjust the focal level of line distortion correction. The preview image in the Image View section shows the image with the selected level of line distortion correction applied. Use the **Save** and **Reset** buttons to save or reset the line distortion settings accordingly.	None

Privacy Mask

NOTE

The Privacy Mask screen is only available when accessing the VPort interface via the Chrome or Microsoft Edge web browser.

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

(AV-UDP) Connected!

☑ Mask 1

☑ Mask 2

☑ Mask 3

Privacy Mask

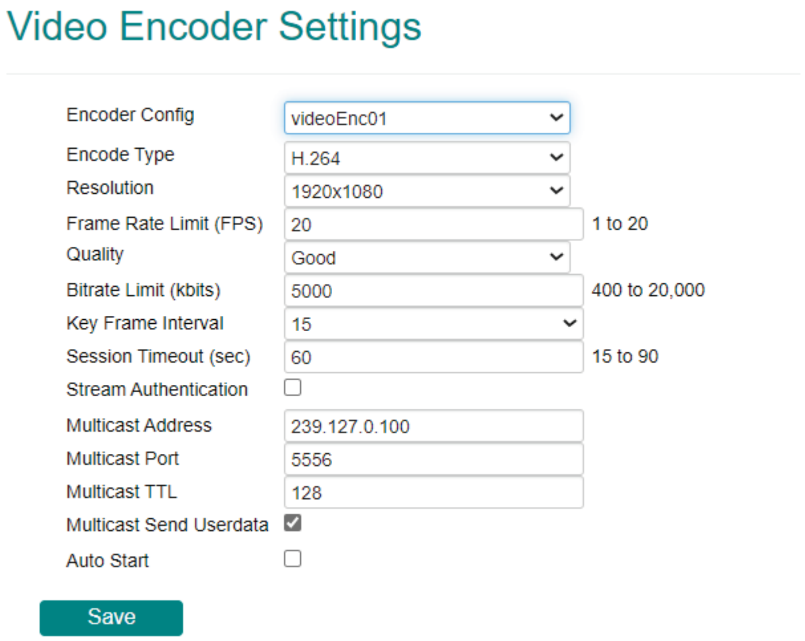
Setting	Description	Default
Enable Privacy Mask	Enable the privacy mask function	Off
Mask 1/2/3	Enable up to 3 different privacy mask areas. Once enabled, you can drag the masked areas to different parts of the camera scene.	Disable

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 4 video encoders for generating video stream profiles. The video encoders can each be configured with different codecs (H.265, H.264, or MJPEG), resolution, FPS (frame rate), and video quality.



Video Encoder Settings

Encoder Config	videoEnc01
Encode Type	H.264
Resolution	1920x1080
Frame Rate Limit (FPS)	20 (1 to 20)
Quality	Good
Bitrate Limit (kbits)	5000 (400 to 20,000)
Key Frame Interval	15
Session Timeout (sec)	60 (15 to 90)
Stream Authentication	□
Multicast Address	239.127.0.100
Multicast Port	5556
Multicast TTL	128
Multicast Send Userdata	☑
Auto Start	□

Setting	Description	Default
Encoder Config	Select a video encoder. This will use the ONVIF profile associated with the selected encoder. To configure profiles, refer to the Profiles section.	VideoEnc01
Encoder Type	Select the codec type of the video encoder: H.265, H.264, MJPEG	H.264
Resolution	Select a video resolution based on the used modulation method (NTSC or PAL).	1920 x 1080

Refer to the table below for a comparison of resolutions for NTSC and PAL modulation.

Resolution	NTSC	PAL
QXGA	2048 x 1536	2048 x 1536
Full HD	1920 x 1080	1920 x 1080
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
4CIF	704 x 480	704 x 576
VGA	640 x 480	640 x 480
CIF	352 x 240	352 x 288

Setting	Description	Default
Frame Rate Limit (FPS)	Specify the maximum FPS (frames per second). The maximum supported frame rate for all resolutions depends on the source video image resolution. 1920 x 1080: 30 (NTSC), 25 (PAL) 2048 x 1536: 20 (NTSC, PAL)	30/ 20

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.

Setting	Description	Default
Quality	Select 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
Bitrate Limit (kBits)	Specify the bandwidth to tune the video quality and FPS (frames per second) to the optimal 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.	5000

NOTE

Due to inherent characteristics of the MJPEG encoder, the bit rate of MJPEG video streams may exceed the maximum bit rate if this value is set too low. It is recommended to create an MJPEG snapshot image at a field site and calculate the required bit rate based on the desired quality and frame rate.

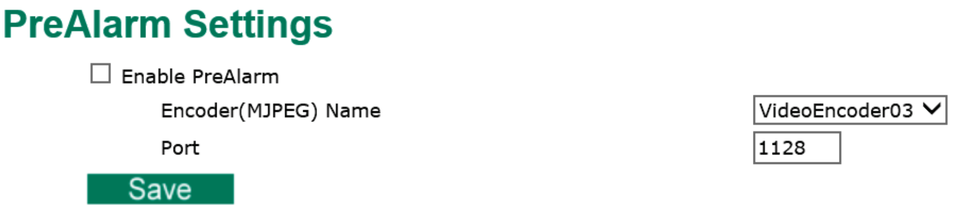
Setting	Description	Default
Key Frame Interval	Configure the key frame interval of the H.265/H.264 stream. A low number means higher video quality (due to more key frames), but more bandwidth will be consumed. If you have concerns about bandwidth, then select a higher number for key frame interval.	15
Session Timeout (sec)	Configure the idle time (in seconds) before the video stream client connection times out.	60
Stream Authentication	Enable or disable video stream authentication.	Disabled
Multicast Address	Specify the Multicast Group address for sending a video stream.	239.127.0.100
Multicast Port	Specify the video multicast port number.	Videoencoder01: 5556 Videoencoder02: 5558 Videoencoder03: 5560 Videoencoder04: 5562
Multicast TTL	Specify the 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
Multicast Send Userdata	Enable or disable video streams including user data.	Enable
Auto Start	Enable or 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.

PreAlarm

The PreAlarm function is used to configure the snapshot images of before an alarm or event is triggered.


PreAlarm Settings

☐ Enable PreAlarm

Encoder(MJPEG) Name: VideoEncoder03

Port: 1128

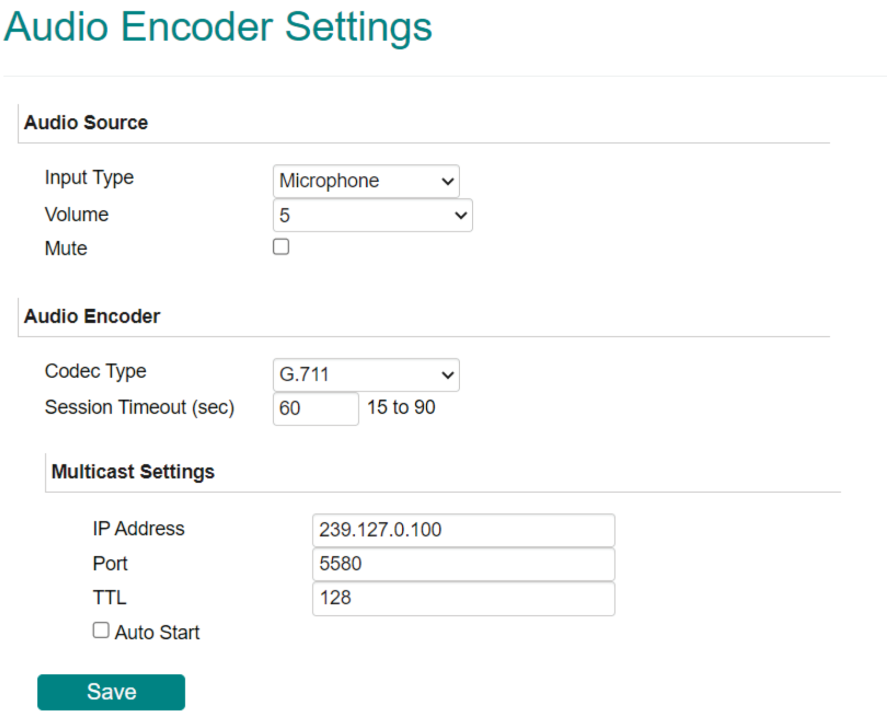
PreAlarm Settings

Setting	Description	Default
Enable PreAlarm	Enable or disable the Prealarm function.	Disable
Encoder (MJPEG) Name	Select which encoder will be used for prealarm.	VideoEncoder03
Port	Specify the network port for the prealarm encoder.	1128

Audio

The VPort 07-3 Series supports an audio input (line-in or microphone in). The audio streaming settings need to be configured for video or audio streams.

Audio Encoder Settings


Audio Encoder Settings

Audio Source

Input Type: Microphone

Volume: 5

Mute ☐

Audio Encoder

Codec Type: G.711

Session Timeout (sec): 60 15 to 90

Multicast Settings

IP Address: 239.127.0.100

Port: 5580

TTL: 128

☐ Auto Start

Audio Source

Setting	Description	Default
Input type	Choose the input type: Line-in or Microphone.	Microphone
Volume	Select the audio volume (0 to 10).	5
Mute	Check to mute all audio input.	Disable

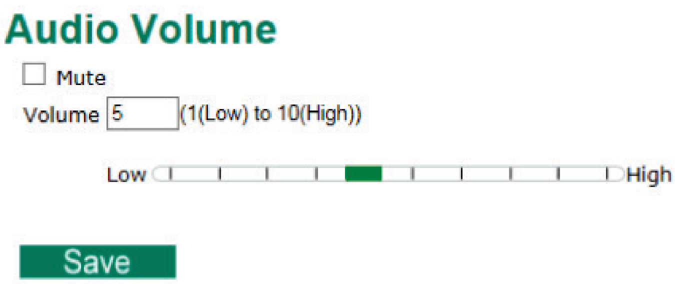
Audio Source

Setting	Description	Default
Codec Type	Select the audio encoder type: G.711 or AAC.	G.711
Session Timeout (sec)	Specify the idle time (in seconds) for disconnecting the client's audio connection.	60

Multicast Settings

Setting	Description	Default
IP Address	Specify the Multicast Group address for sending audio streams.	239.127.0.100
Port	Specify the audio Multicast port number.	5580
TTL	Specify the 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
Auto Start	Enable or disable the Multicast stream push mode.	Disable

Audio Volume



Audio Volume

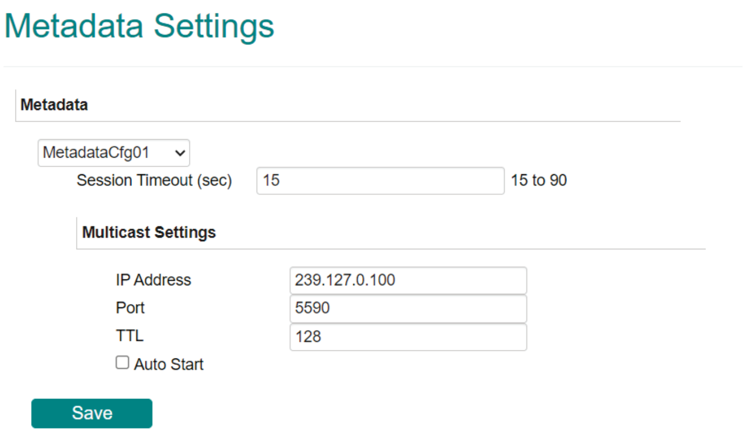
☐ Mute

Volume 5 (1(Low) to 10(High))

Setting	Description	Default
Mute	Check to mute all audio.	Blank
Volume	Specify the audio volume (1 to 10).	5

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

Session Timeout (sec) 15 15 to 90

Multicast Settings

IP Address 239.127.0.100

Port 5590

TTL 128

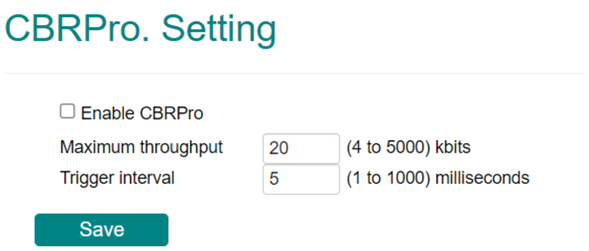
☐ Auto Start

Multicast setting

Setting	Description	Default
Session Timeout (sec)	Configure the idle time (in seconds) before the metadata stream times out.	60
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
Auto Start	Enable/disable the Multicast stream push mode	Disable

Streaming

CBR Pro



CBRPro. Setting

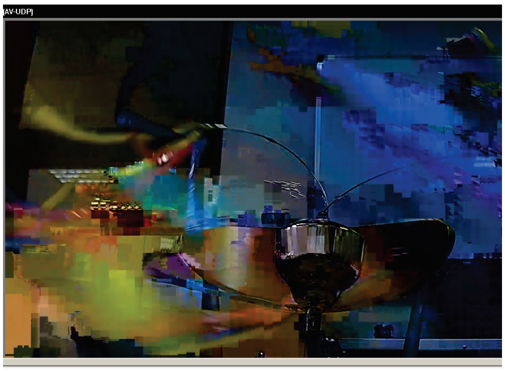
□ Enable CBRPro

Maximum throughput	20	(4 to 5000) kbits
Trigger interval	5	(1 to 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

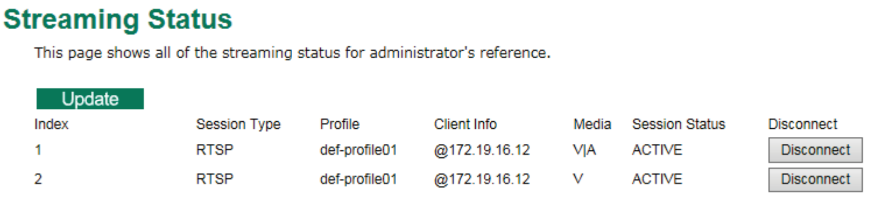
Image with packet loss



Setting	Description	Default
Enable CBRPro	Enable or disable CBRPro functionality.	Disabled
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

Streaming Status

This page shows the status of all connected media streams.



Streaming Status

This page shows all of the streaming status for administrator's reference.

Index	Session Type	Profile	Client Info	Media	Session Status	Disconnect
1	RTSP	def-profile01	@172.19.16.12	V|A	ACTIVE	Disconnect
2	RTSP	def-profile01	@172.19.16.12	V	ACTIVE	Disconnect

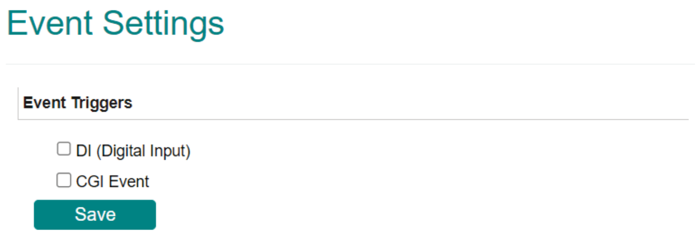
Setting	Description
Index	The index of the media stream.
Session Type	The video stream transmission method.
Profile	The profile being used.
Client Info	The address of the client.
Media	The type of media stream. V: video, A: Audio, V/A: Video and audio.
Session status	The current status of the media stream session.
Disconnect	Click to manually disconnect the stream.

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

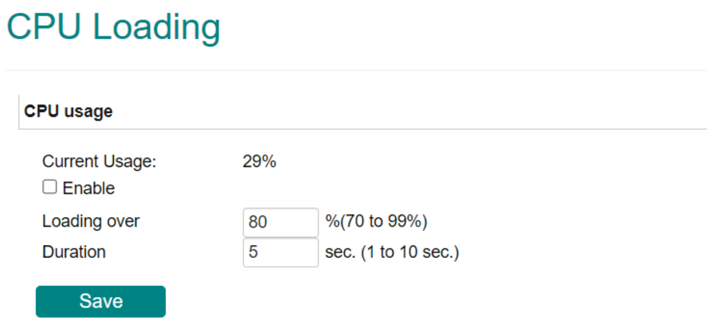
Event Triggers

□ DI (Digital Input)

□ CGI Event

CPU Event

CPU events inform the user whenever a CPU-related event occurs.



CPU Loading

CPU usage

Current Usage: 29%

□ Enable

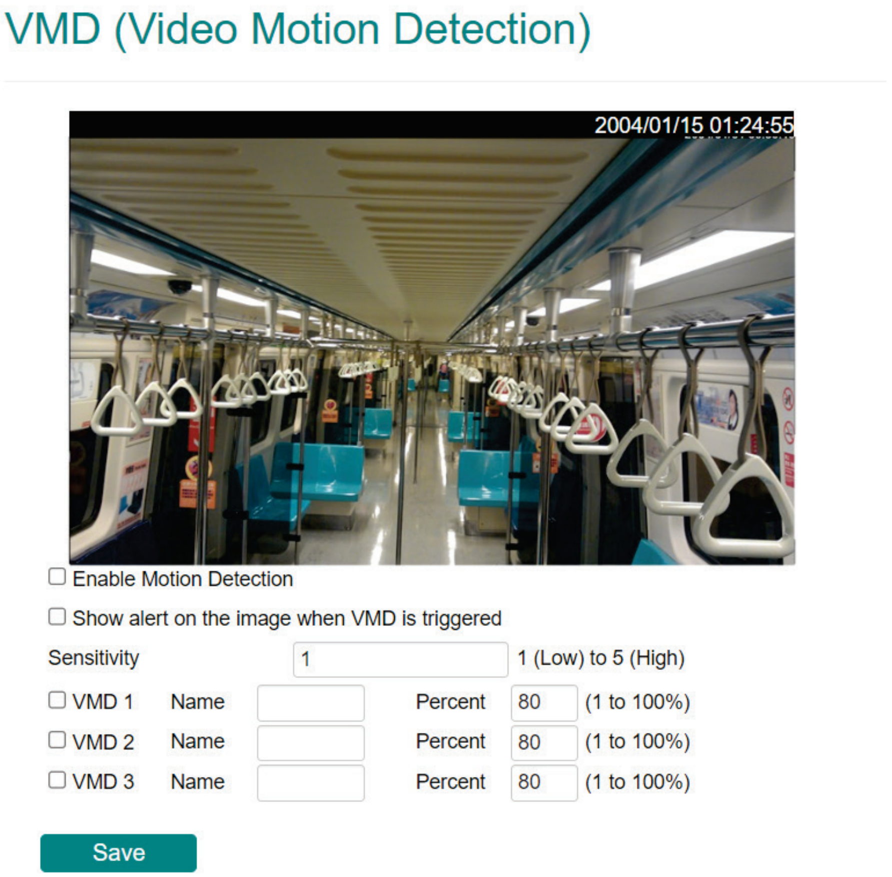
Loading over 80 %(70 to 99%)

Duration 5 sec. (1 to 10 sec.)

Setting	Description	Default
Enable	Enable or disable system events.	Disabled
Loading Over	Specify the threshold value for CPU usage events.	80
Duration	Specify how long (in seconds) CPU usage needs to exceed the set threshold before an event is triggered.	5

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 Motion Detection

☐ Show alert on the image when VMD is triggered

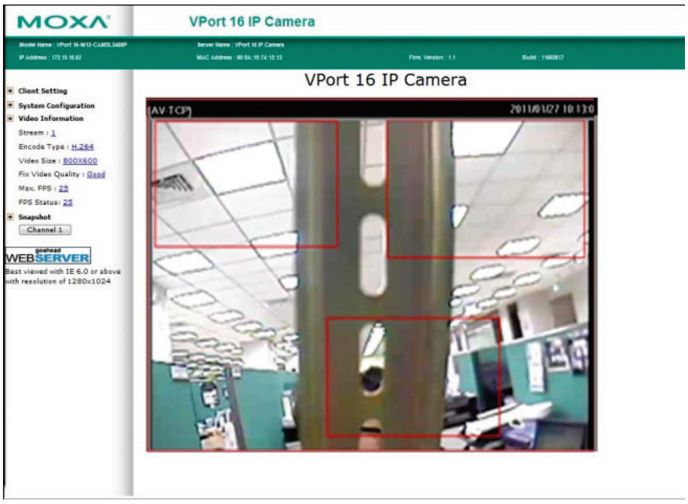
Sensitivity 1 1 (Low) to 5 (High)

☐ VMD 1	Name		Percent	80	(1 to 100%)
☐ VMD 2	Name		Percent	80	(1 to 100%)
☐ VMD 3	Name		Percent	80	(1 to 100%)

Setting	Description	Default
Enable Motion Detection	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.



MOXA VPort 16 IP Camera

Model Name : VPort 16-M12-CAMSL5400P

Server Name : VPort 16 IP Camera

IP Address : 172.19.16.62

MAC Address : 00:0A:19:74:12:13

Firm. Version : 1.1

Build : 11082617

VPort 16 IP Camera

Stream : 1

Encode Type : H.264

Video Size : 800X600

Fix Video Quality : Good

Max. FPS : 25

FPS Status: 25

Setup a VMD Alarm

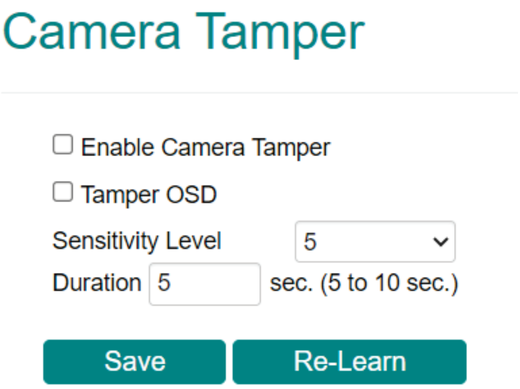
Setting	Description	Default
Enable	Enable or disable the VMD1, VMD2, or VMD3	Disable
Window	The name of each VMD window	Blank
Percent	The minimum percentage of change to an image that will trigger VMD. Decrease the percentage to make it easier to trigger VMD.	80
Sensitivity	The measurable difference between two sequential images for triggering VMD. Increase the sensitivity to make it easier for VMD to be triggered.	1

NOTE

After setting the Motion Detection settings, 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

□ Tamper OSD

Sensitivity Level: 5

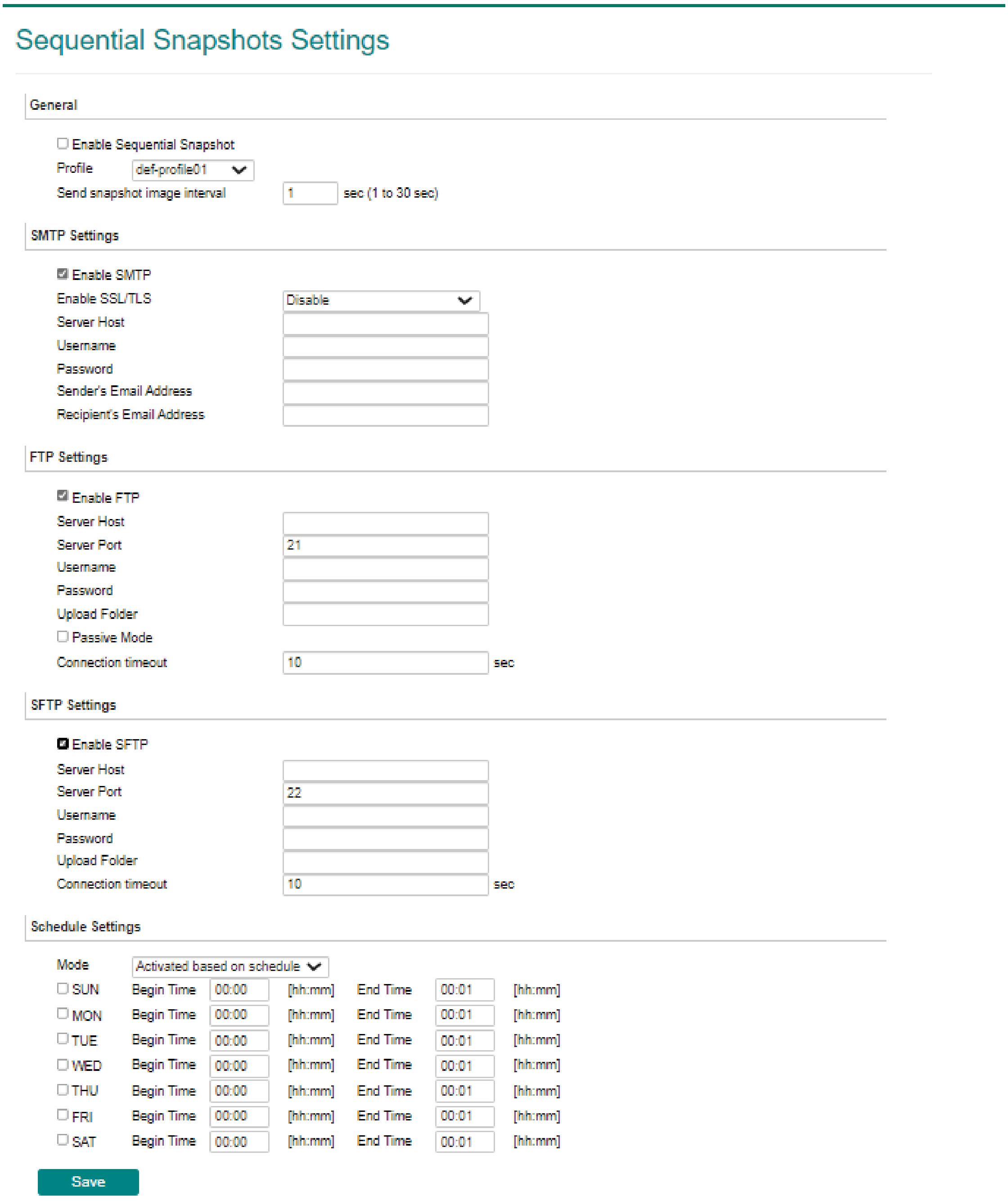
Duration: 5 sec. (5 to 10 sec.)

Setting	Description	Default
Enable camera tamper	Enable or disable the digital input alarm.	Disable
Tamper OSD	Determines whether or not the camera will display an on-screen 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 Settings

General

□ Enable Sequential Snapshot

Profile: def-profile01

Send snapshot image interval: 1 sec (1 to 30 sec)

SMTP Settings

☑ Enable SMTP

Enable SSL/TLS: Disable

Server Host:

Username:

Password:

Sender's Email Address:

Recipient's Email Address:

FTP Settings

☑ Enable FTP

Server Host:

Server Port: 21

Username:

Password:

Upload Folder:

□ Passive Mode

Connection timeout: 10 sec

SFTP Settings

☑ Enable SFTP

Server Host:

Server Port: 22

Username:

Password:

Upload Folder:

Connection timeout: 10 sec

Schedule Settings

Mode: Activated based on schedule

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

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

General Settings

Setting	Description	Default
Enable Sequential Snapshots	Enable or disable Sequential Snapshot.	Disable
Profile	Select which video profile will take snapshot images.	def-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)

SMTP Settings

Setting	Description	Default
Enable SMTP	Enable or disable SMTP for sending sequential snapshot images via email.	Disable
Enable SSL/ TLS	Enable or disable the SSL/TLS or STARTTLS encryption for SMPT connections.	Disable
Server Host	Specify the SMTP server's IP address or URL address.	Blank
Username	Specify the username for SMTP server authentication.	Blank
Password	Specify the password for SMTP server authentication.	None
Sender's Email Address	Specify the email address for sending the snapshot images.	Blank
Recipient's Email Address	Specify the email address for receiving the snapshot images,	Blank

FTP Settings

Setting	Description	Default
Enable FTP	Enable FTP to save snapshot images on a remote SFTP server.	Disable
Server Host	Specify the FTP server's IP address or URL address.	None
Server Port	Specify the FTP server port.	21
Username	Specify the username for FTP server authentication.	None
Password	Specify the password for FTP server authentication.	None
Upload Folder	Specify the storage folder on the remote FTP server.	None
Passive Mode	Enable or disable passive transfers for FTP transmissions passing a firewall.	Disable
Connection Timeout	Specify the idle time for disconnecting the FTP server.	10 (seconds)

SFTP Settings

Setting	Description	Default
Enable SFTP	Enable SFTP to save snapshot images on a remote SFTP server.	Disable
Server Host	Specify the SFTP server's IP address or URL address.	None
Server Port	Specify the SFTP server port.	22
Username	Specify the username for SFTP server authentication.	None
Password	Specify the password for SFTP server authentication.	None
Upload Folder	Specify the storage folder on the remote SFTP server.	None
Connection timeout	Specify the idle time for disconnecting the SFTP server.	10 (seconds)

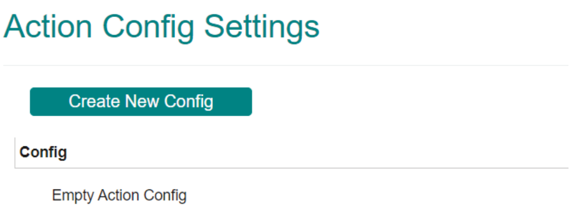
Schedule Settings

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 Config Settings

Create New Config

Config

Empty Action Config

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

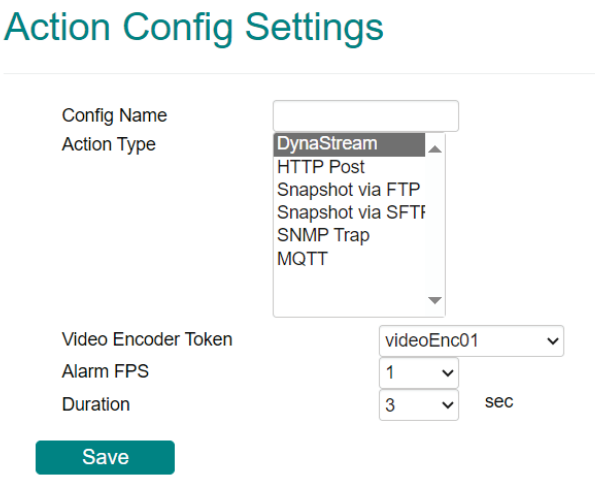
Step 2: Create the new action.

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

Different actions have different configuration items.

DynaStream

DynaStream™ is a unique and innovative function that allows for adaptive frame rates in response to events on the network, such as event triggers and system commands. When network traffic becomes congested, DynaStream™ allows VPort products to respond to CGI, SNMP, and 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

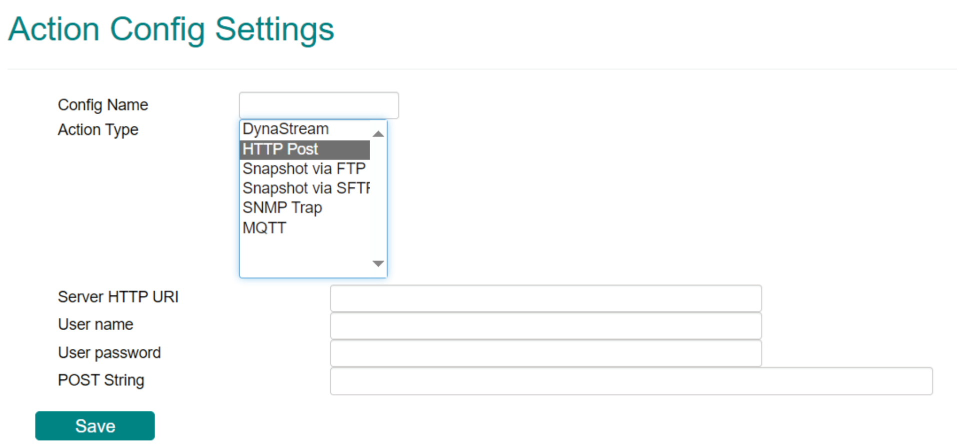
Video Encoder Token: videoEnc01

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: DynaStream / HTTP Post / Snapshot via FTP / Snapshot via SFTI / SNMP Trap / MQTT (HTTP Post selected)

Server HTTP URI

User name

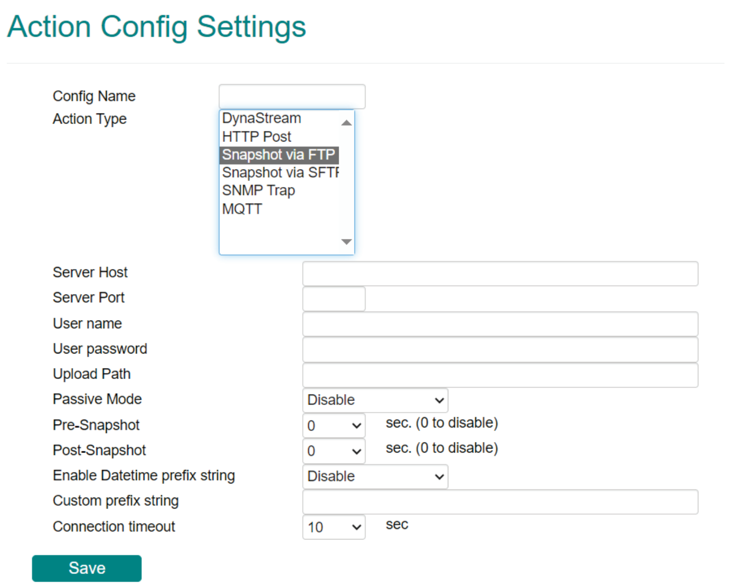
User password

POST String

Save

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 / Snapshot via SFTI / SNMP Trap / MQTT (Snapshot via FTP selected)

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

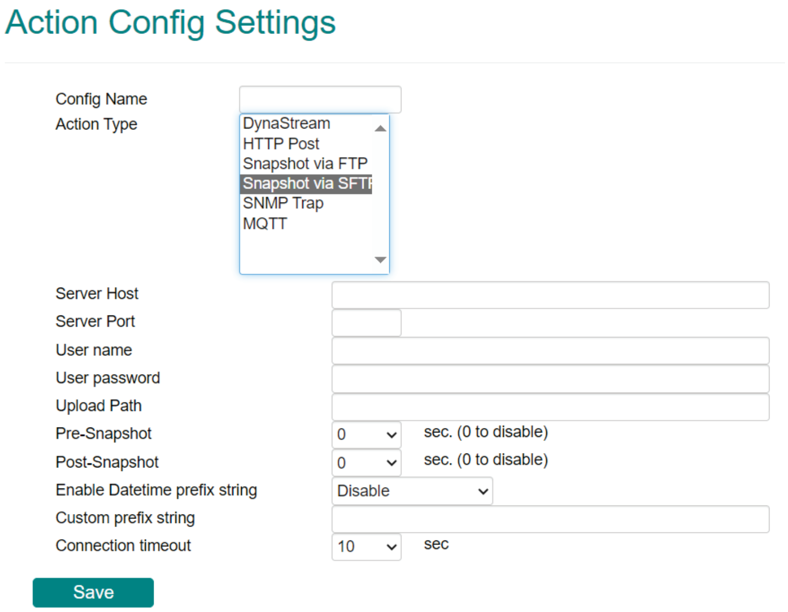
Connection timeout: 10 sec

Save

Setting	Description	Default
Server Host	Enter the FTP server's IP address or URL address.	Blank
Server Port	Enter the FTP server's port.	Blank
User name	Enter the FTP server username.	Blank
User password	Enter the FTP server password.	Blank
Upload Path	Specify the FTP file storage folder on the remote FTP server.	Blank
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

Setting	Description	Default
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.	Blank
Connection timeout	Configure the idle time (in seconds) for the system to stop uploading snapshot images to the FTP server.	10

Snapshot via SFTP

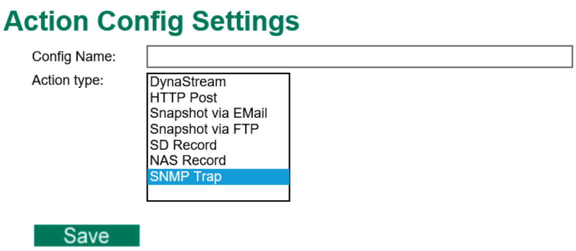


Action Config Settings

Config Name		
Action Type	DynaStream HTTP Post Snapshot via FTP Snapshot via SFTP SNMP Trap MQTT	
Server Host		
Server Port		
User name		
User password		
Upload Path		
Pre-Snapshot	0	sec. (0 to disable)
Post-Snapshot	0	sec. (0 to disable)
Enable Datetime prefix string	Disable	
Custom prefix string		
Connection timeout	10	sec

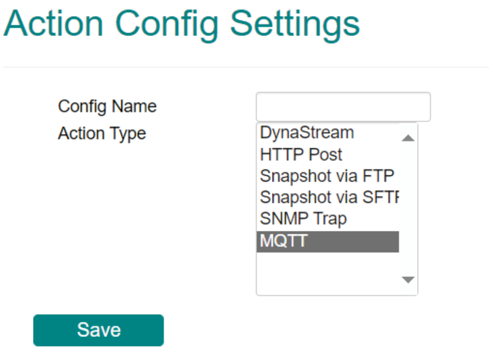
Setting	Description	Default
Server host	Enter the SFTP server’s IP address or URL address.	Blank
Server port	Enter the SFTP server’s port.	Blank
User name	Enter the SFTP server username.	Blank
User password	Enter the SFTP server password.	Blank
Upload Path	Specify the FTP file storage folder on the remote SFTP server.	Blank
Recipient’s address	For security reasons, SMTP servers must see the exact recipient’s email address.	None
Pre-Snapshot sec (0: disabled)	= 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 sec (0: disabled)	= 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 Date and time prefix string	Add the date & time to the filename of snapshot images.	Disable
Customer prefix string	The file names of snapshot images will be prefixed with this string.	blank
Connection timeout	Configure the idle time (in seconds) for the system to stop uploading snapshot images to the SFTP server.	10

SNMP Trap



Setting	Description	Default
Config Name	Enter a name for this SNMP trap action.	Blank
Action Enabled	Enable or disable the SNMP trap action.	Enabled

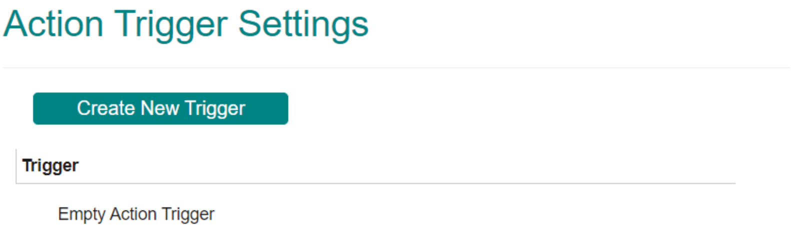
MQTT



Setting	Description	Default
Config Name	Enter a name for this MQTT action.	Blank
Action Enabled	Enable or disable the MQTT action.	Enabled

Action Trigger

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



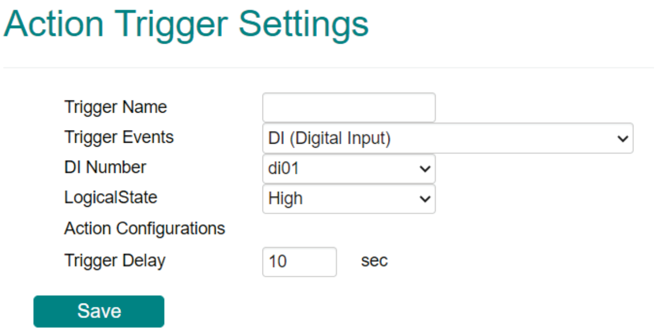
Step 1: Click the "Create New Trigger" button.

Step 2: Create the new trigger.

Setting	Description	Default
Trigger Name	Enter a new for the trigger.	None
Trigger Events	Select the event type: Digital input, VMD, Camera Tamper, CPU, CGI Event	DI (Digital Input)

Different triggers have different configuration items.

(DI) Digital Input

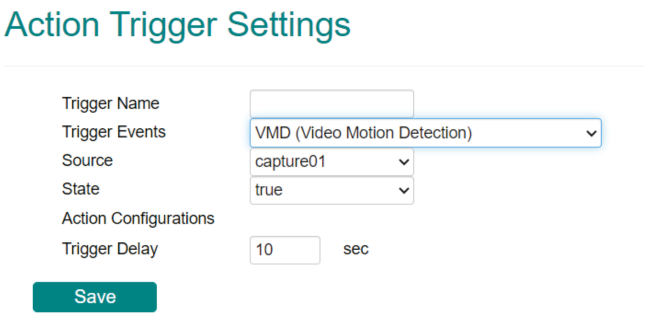


Action Trigger Settings

Trigger Name	
Trigger Events	DI (Digital Input)
DI Number	di01
LogicalState	High
Action Configurations	
Trigger Delay	10 sec

Settings	Description	Default
DI Number	Select the digital input.	DI01
Logical State	Select the DI status: High or Low.	High
Action Configurations	Select a previously configured action. Refer to the Action Config section to configure an action.	Blank
Trigger Delay	Specify the delay time (in seconds) before the action is triggered when the specified event occurs.	10

VMD

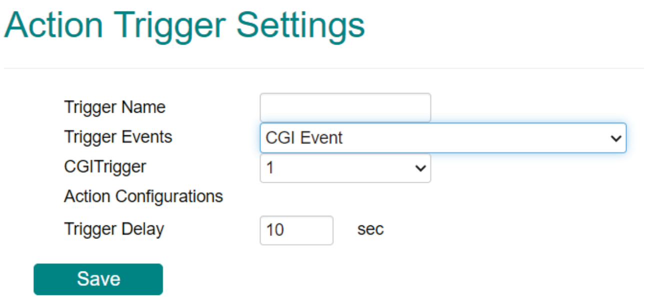


Action Trigger Settings

Trigger Name	
Trigger Events	VMD (Video Motion Detection)
Source	capture01
State	true
Action Configurations	
Trigger Delay	10 sec

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
Action Configurations	Select a previously configured action. Refer to the Action Config section to configure an action.	Blank
Trigger Delay	Specify the delay time (in seconds) before the action is triggered when the specified event occurs.	10

CGI Event



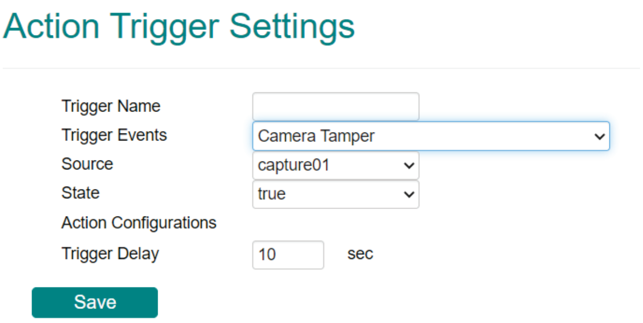
Action Trigger Settings

Trigger Name	
Trigger Events	CGI Event
CGITrigger	1
Action Configurations	
Trigger Delay	10 sec

Settings	Description	Default
CGITrigger	Select from 5 CGI triggers.	1
Action Configurations	Select a previously configured action. Refer to the Action Config section to configure an action.	Blank

Settings	Description	Default
Trigger Delay	Specify the delay time (in seconds) before the action is triggered when the specified event occurs.	10

Tamper

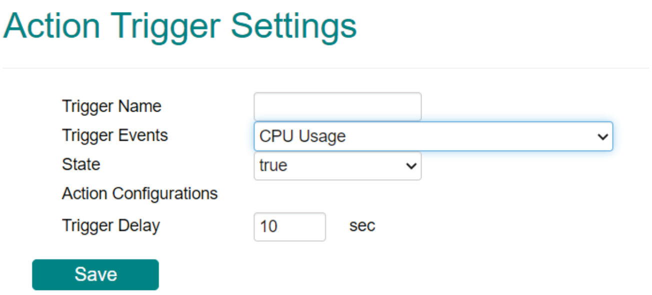


Action Trigger Settings

Trigger Name:
Trigger Events: Camera Tamper
Source: capture01
State: true
Action Configurations
Trigger Delay: 10 sec

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
Action Configurations	Select a previously configured action. Refer to the Action Config section to configure an action.	Blank
Trigger Delay	Specify the delay time (in seconds) before the action is triggered when the specified event occurs.	10

CPU Usage



Action Trigger Settings

Trigger Name:
Trigger Events: CPU Usage
State: true
Action Configurations
Trigger Delay: 10 sec

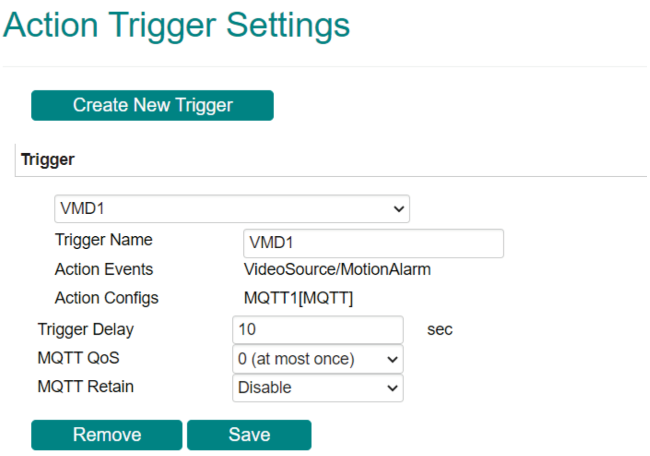
Settings	Description	Default
Token	Select the CPU.	CPU
State	Select the CPU state: true or false.	True
Action Configurations	Select a previously configured action. Refer to the Action Config section to configure an action.	Blank
Trigger Delay	Specify the delay time (in seconds) before the action is triggered when the specified event occurs.	10

Step 3 (Optional): Configure the MQTT connection for MQTT.

After creating a trigger for an MQTT action, an additional 2 MQTT connection parameters must be configured.

NOTE

While these additional MQTT options will show for all action types, these settings only affect triggers for "MQTT" actions.



Action Trigger Settings

Trigger

VMD1

Trigger Name	VMD1
Action Events	VideoSource/MotionAlarm
Action Configs	MQTT1[MQTT]
Trigger Delay	10 sec
MQTT QoS	0 (at most once)
MQTT Retain	Disable

Setting	Description	Default
MQTT QoS	Configure the MQTT event delivery behavior in 0 (at most once), 1 (at least once), or 2 (exactly once)	0 (at most once)
MQTT Retain	Enable or disable MQTT event retention by the MQTT broker.	Disable

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 07-3 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>

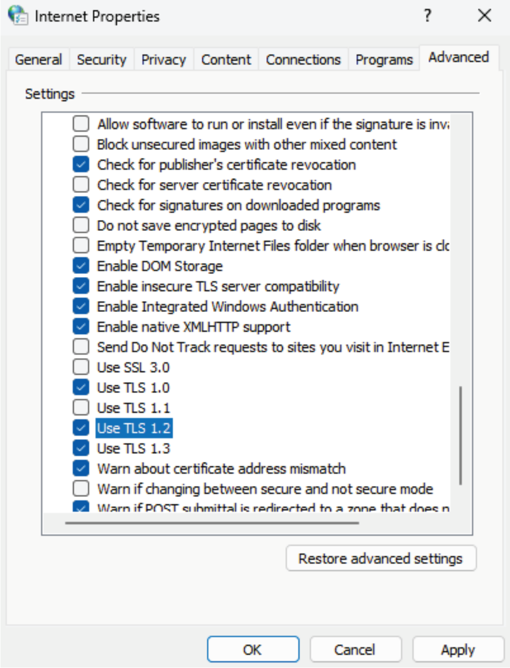
NOTE

Action type: Dynastream, HTTP Post and snapshotFTP.

D. Security Hardening Guide

HTTPS and SSL Certificates

HTTPS is an encrypted communication channel. As TLS v1.1 and earlier versions have severe vulnerabilities that can be easily compromised, the VPort Series uses TLS v1.2 for HTTPS connections to ensure data transmissions are secured, as long as TLS v1.2 is enabled for your browser.

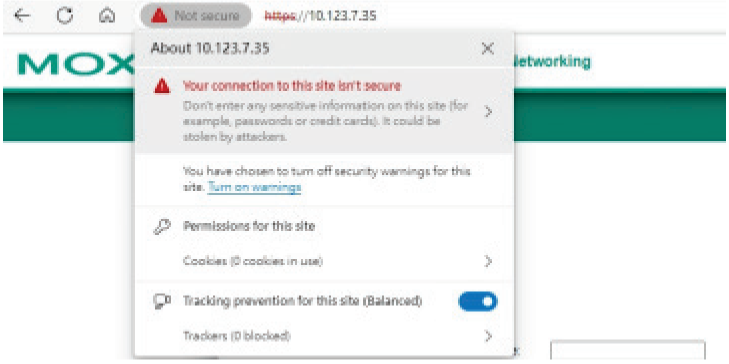


- □ Allow software to run or install even if the signature is inv
- □ Block unsecured images with other mixed content
- ☑ Check for publisher's certificate revocation
- □ Check for server certificate revocation
- ☑ Check for signatures on downloaded programs
- □ Do not save encrypted pages to disk
- □ Empty Temporary Internet Files folder when browser is cl
- ☑ Enable DOM Storage
- ☑ Enable insecure TLS server compatibility
- ☑ Enable Integrated Windows Authentication
- ☑ Enable native XMLHTTP support
- □ Send Do Not Track requests to sites you visit in Internet E
- □ Use SSL 3.0
- ☑ Use TLS 1.0
- □ Use TLS 1.1
- ☑ Use TLS 1.2
- ☑ Use TLS 1.3
- ☑ Warn about certificate address mismatch
- □ Warn if changing between secure and not secure mode
- ☑ Warn if POST submittal is redirected to a zone that does n

Using HTTPS without the proper certificates will prompt a security warning. To prevent these warnings, you will need to import the self-signed certificate from the VPort IP camera Series. Follow the steps below to export the VPort's certificate and import it to the host's web browser:

Step 1: Open a supported browser and enter *https://[VPort’s IP address]* in the address field to access the web console of the VPort IP camera.

Step 2: You may notice a **Not secure** icon in front of the IP address. Click this icon to open a prompt with several options. Click the **Your connection to this site isn't secure** option.


Not secure
~~https~~://10.123.7.35
About 10.123.7.35
MOX
letworking

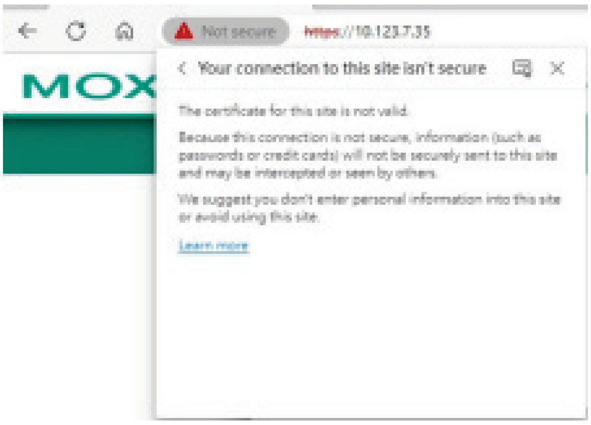
Your connection to this site isn't secure

Don't enter any sensitive information on this site (for example, passwords or credit cards). It could be stolen by attackers.

You have chosen to turn off security warnings for this site. Turn on warnings

Permissions for this site
Cookies (0 cookies in use)
Tracking prevention for this site (Balanced)
Trackers (0 blocked)

Step 3: Click **Learn more** to show more information about the self-signed certificate of the VPort IP camera.



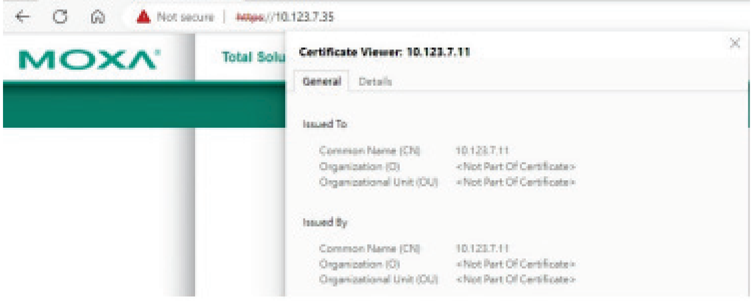
Your connection to this site isn't secure

The certificate for this site is not valid.

Because this connection is not secure, information (such as passwords or credit cards) will not be securely sent to this site and may be intercepted or seen by others.

We suggest you don't enter personal information into this site or avoid using this site.

Learn more



Certificate Viewer: 10.123.7.11

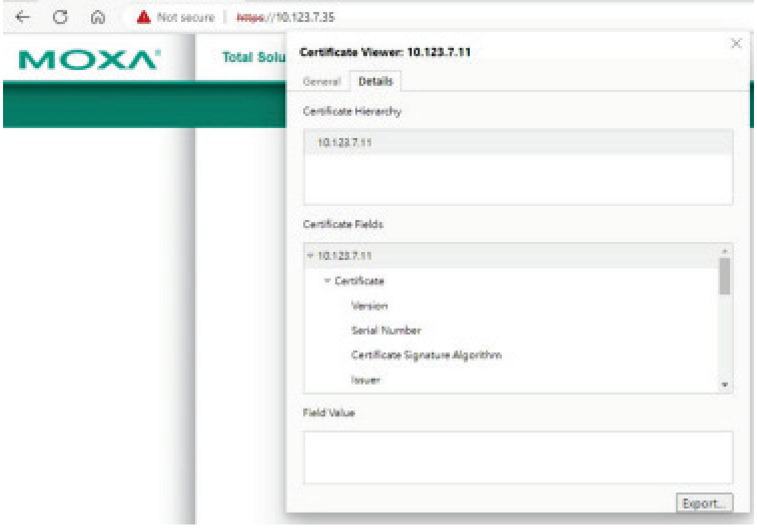
Issued To

Common Name (CN) 10.123.7.11
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>

Issued By

Common Name (CN) 10.123.7.11
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>

Step 4: In this window, go to the **Details** tab and click **Export** to export the VPort's self-signed certificate.



Certificate Viewer: 10.123.7.11

Certificate Hierarchy

10.123.7.11

Certificate Fields

- 10.123.7.11
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer

Field Value

Step 4: Import the VPort's self-signed certificate into your browser. Next time you access the VPort's web interface, the security warning will no longer appear.