H.264 • Rack Mount Design VS8801/8401

VIDEO SERVER

User's Manual

VS8801

8-CH Audio and Video
Single Stream

VS8401

4-CH Audio and Video
Simultaneous Dual Streams

Rev. 1.3

VIVOTEK
www.vivotek.com

IP Surveillance

Table of Contents

Revision History

1. Rev. 1.0: Initial release.
2. Rev. 1.1: Most modifications are made to reflect functional changes on the user interface.
    * Modified the description for the expandable/Collapsible functional menus.
    * Added the Recording to SD/SDHC details. (SD local storage is now available on VS8401)
    * Added Local Storage options.
    * Added the Quad View setting options.
    * Added the joystick configuration options.
3. Rev. 1.2: Added description for VS8801 stating that it does not support the SD card local storage.
4. Rev. 1.3: Updated the URL commands.

Overview

VIVOTEK VS8801/8401, the new milestone in video server security performing 8-CH or 4-CH high resolution with high frame rate in H.264, are able to convert analog video into digital video with the highest quality. The H.264 compression format drastically reduces the file sizes and conserves valuable bandwidth and storage space. The VS8401 supports simultaneous dual streams, while the VS8801 supports single stream to be transmitted in H.264, MPEG-4 and MJPEG formats for versatile applications. The stream
can also be individually configured with frame rates, resolution, and image quality so as to meet different platforms or bandwidth constraints.

Featured with intelligent video functions, such as motion detection & tamper detection, the VS8801/8401 are capable of upgrading analog cameras into intelligent cameras. The tamper detection feature can detect events such as blockage, redirection, defocus, and spray-painting of camera lens, making it an intelligent solution to possible camera obstruction. Furthermore, the video server also upgrades the security level of the IP surveillance system with the network security protocols, HTTPS and 802.1x. It is also designed with Giga LAN for large transmission need and DC 12V / AC 24V compatible power input design. These features make VS8801/8401 easy to install and integrate with the existing analog system.

Monitoring with VIVOTEK's ST7501 as the video management software for better scalability and easy-to-use operation is another delightful benefit. Most importantly, it is designed for rack mount solution for easy installation. The solution for video server is a pioneering idea in the world. The innovative vision of video server, VS8801/8401, help you easily upgrade to a full-featured, high-end IP surveillance solution!

Read Before Use

The use of surveillance devices may be prohibited by law in your country. The video server is not only a high-performance web-ready camera but can also be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the Package Contents listed below. Take note of the warnings in the Quick Installation Guide before the video server is installed; then carefully read and follow the instructions in the Installation chapter to avoid damage due to faulty assembly and installation. This also ensures the product is used properly as intended.

The video server is a network device and its use should be straightforward for those who have basic networking knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the video server and ensure proper operations. For creative and professional developers, the URL Commands of the video server section serves as a helpful reference to customizing existing homepages or integrating with the current web server.

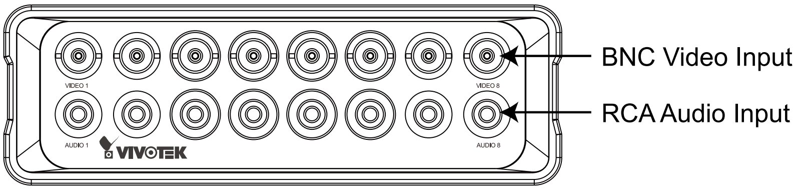
Package Contents

- VS8801/8401
- Power Adapter
- Software CD
- Warranty Card
- Quick Installation Guide
- Terminal blocks

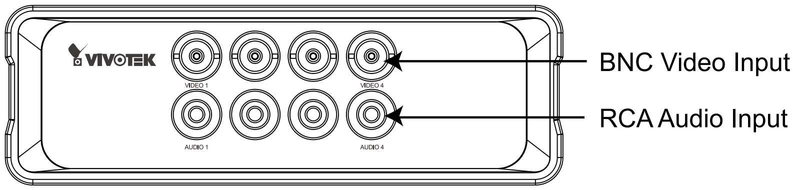
Physical Description

Front Panel

■ VS8801

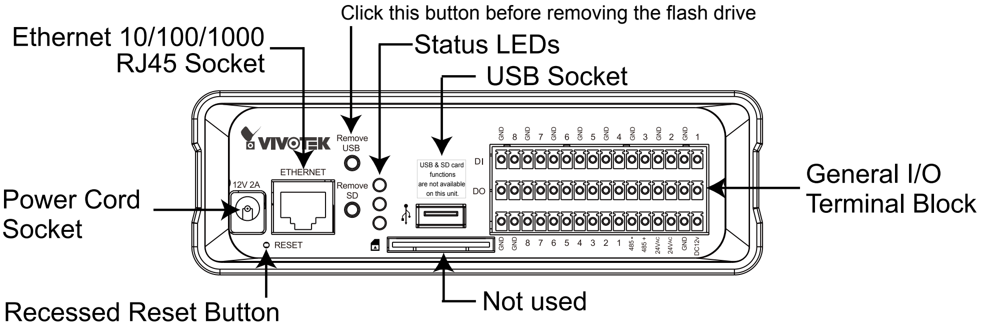


■ VS8401

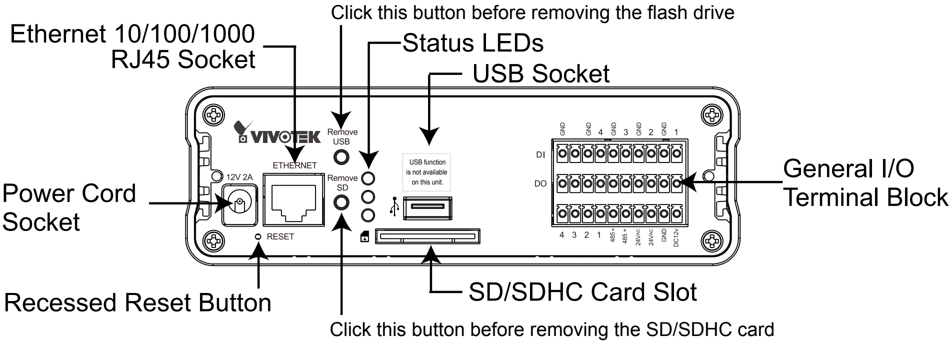


Back Panel

■ VS8801



■ VS8401

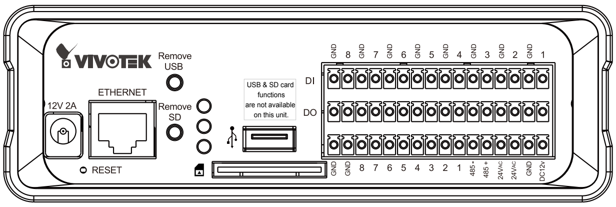


NOTE:
The USB socket is for maintenance purposes only.

General I/O Terminal Block

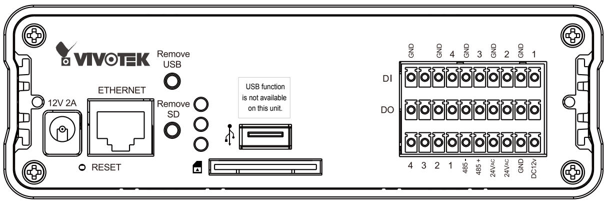
This video server provides a general I/O terminal block which is used to connect external input / output devices. The pin definitions are described below.

■ VS8801


VIVOTEK
Remove USB
ETHERNET
12V 2A
Remove SD
RESET
USB & SD card functions are not available on this unit.
DI
DO
GND 8 GND 7 GND 6 GND 5 GND 4 GND 3 GND 2 GND 1
GND GND 8 7 6 5 4 3 2 1 485- 485+ 24VAC 24VAC GND DC12V

CH 8 GND	CH 8 DI	CH 7 GND	CH 7 DI	CH 6 GND	CH 6 DI	CH 5 GND	CH 5 DI	CH 4 GND	CH 4 DI	CH 3 GND	CH 3 DI	CH 2 GND	CH 2 DI	CH 1 GND	CH 1 DI
CH 8 GND	CH 8 DO	CH 7 GND	CH 7 DO	CH 6 GND	CH 6 DO	CH 5 GND	CH 5 DO	CH 4 GND	CH 4 DO	CH 3 GND	CH 3 DO	CH 2 GND	CH 2 DO	CH 1 GND	CH 1 DO
GND	GND	CH 8 Audio out	CH 7 Audio out	CH 6 Audio out	CH 5 Audio out	CH 4 Audio out	CH 3 Audio out	CH 2 Audio out	CH 1 Audio out	RS 485-	RS 485+	24V AC	24V AC	GND	DC 12V

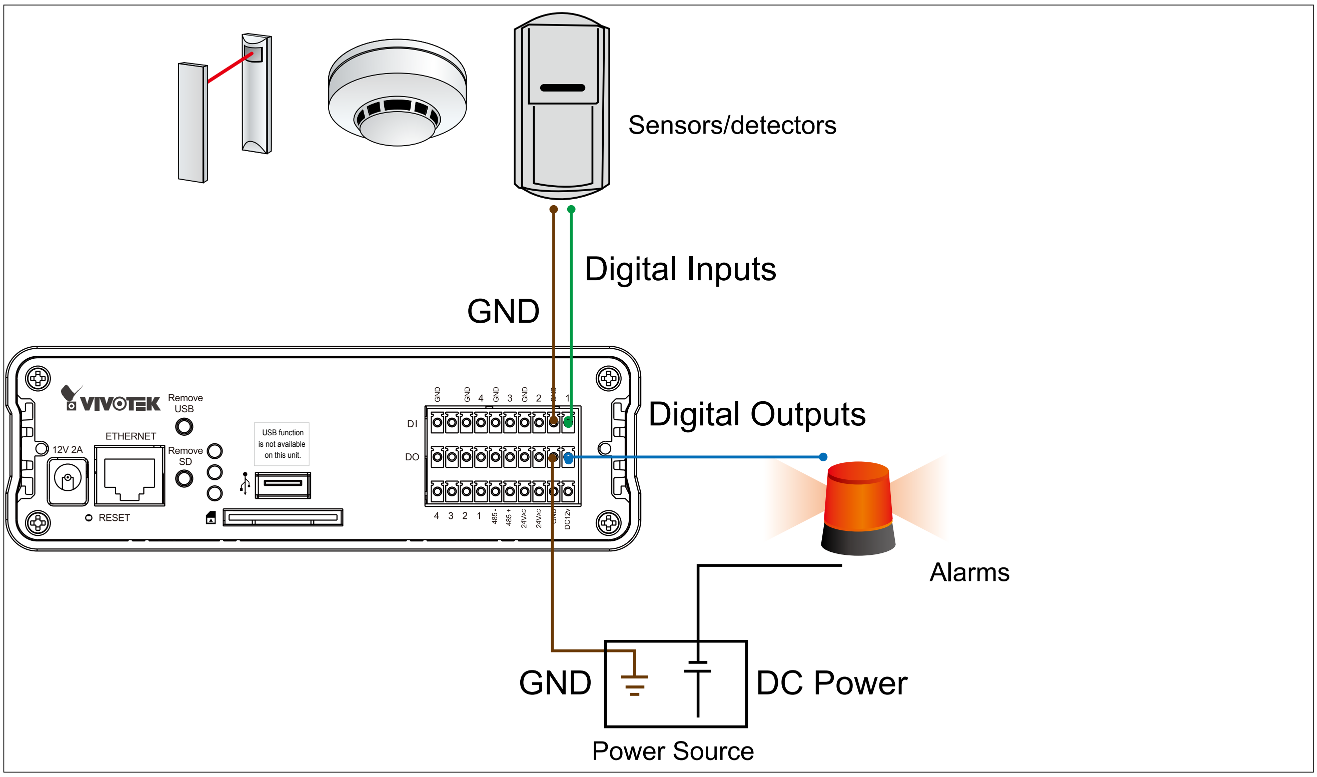
■ VS8401


VIVOTEK
Remove USB
ETHERNET
12V 2A
Remove SD
RESET
USB function is not available on this unit.
DI
DO
GND GND 4 GND 3 GND 2 GND 1
4 3 2 1 485- 485+ 24VAC 24VAC GND DC12V

GND	N/A	CH 4 GND	CH 4 DI	CH 3 GND	CH 3 DI	CH 2 GND	CH 2 DI	CH 1 GND	CH 1 DI
GND	N/A	CH 4 GND	CH 4 DO	CH 3 GND	CH 3 DO	CH 2 GND	CH 2 DO	CH 1 GND	CH 1 DO
CH 4 Audio out	CH 3 Audio out	CH 2 Audio out	CH 1 Audio out	RS 485-	RS 485+	24V AC	24V AC	GND	DC 12V

DI/DO Diagram

Please refer to the following illustration for the connection method.



NOTE:

- ► *External alarms or other devices that connect to the digital outputs require external power supply, e.g., DC power from a power adapter.*
- ► *12V Ground should connect to Video Server ground termail block. For detailed pin definition, please refer to page 7.*
- ► *It is recommended to keep the current running through each of the DO lines under 1A.*

Status LED

The LED indicates the status of the video server. The table below shows the statuses of the Yellow (SD), Green (Network), and Red (Power) LEDs.

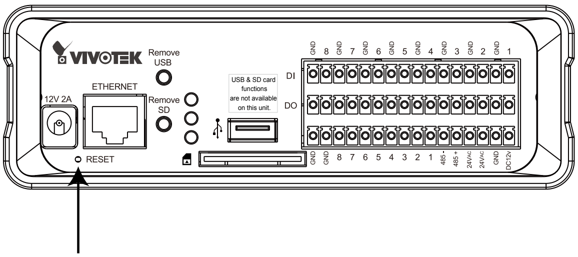
LED Name	Item	LED status	Description
SD	1	Steady Yellow	SD card is present and functioning normally
	2	Blinking Yellow	SD card is present yet problems occurred with data access
	3	LED Off	No SD card in the socket
Network	1	Blinking Green every 1 sec.	Network activity (heartbeat)
	2	Green LED Off	Network failed
Power	1	Steady Red	Power on and during system boot
	2	Red LED Off	Power off

Below are the definitions for other combinations of LEDs:

Item	LED status	Description
1	Blinking Green every 2 sec.	Audio mute (heartbeat)
2	Blinking Red every 0.15 sec. + Blinking Green every 1 sec.	Upgrading Firmware
3	Blinking Red every 0.15 sec. + Blinking Green every 0.15 sec.	Restoring default

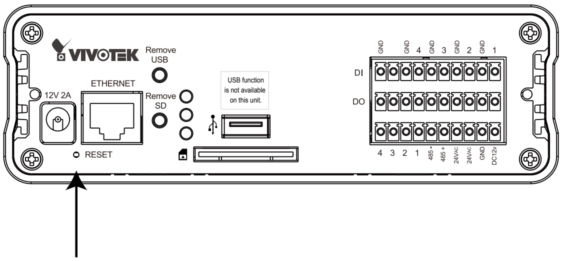
Hardware Reset

■ VS8801


VIVOTEK
Remove USB
ETHERNET
12V 2A
Remove SD
RESET
USB & SD card functions are not available on this unit.
DI
DO
GND 8 GND 7 GND 6 GND 5 GND 4 GND 3 GND 2 GND 1
GND GND 8 7 6 5 4 3 2 1 485 - 485 + 24VAC 24VAC GND DC12V

Recessed Reset Button

■ VS8401


VIVOTEK
Remove USB
ETHERNET
12V 2A
Remove SD
RESET
USB function is not available on this unit.
DI
DO
GND GND 4 GND 3 GND 2 GND 1
4 3 2 1 485 - 485 + 24VAC 24VAC GND DC12V

Recessed Reset Button

The reset button is used to reset the system or restore the factory default settings. Sometimes resetting the system can return the video server to normal operation. If the system problems remain after reset, restore the factory settings and install again.

Reset: Press and release the recessed reset button using a straightened paper clip. Wait for the video server to reboot.

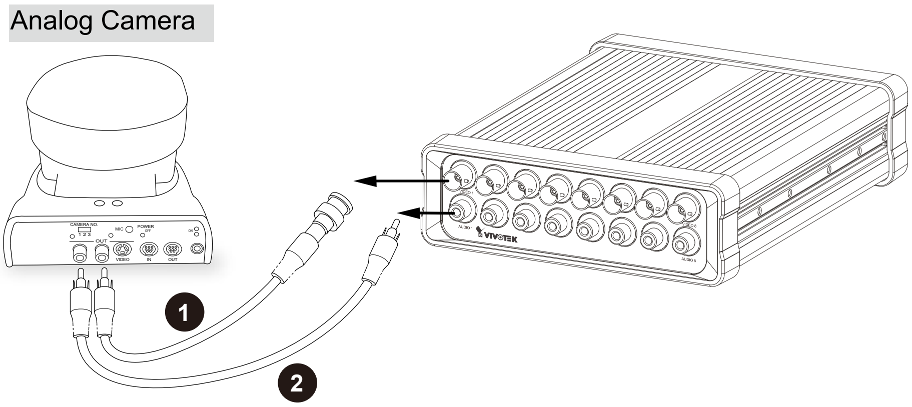
Restore: Press and hold the reset button down until the status LED rapidly blinks. It takes about 30 seconds. Note that all settings will be restored to factory default. Upon successful restore, the status LED will blink green and red during normal operation.

Network Deployment

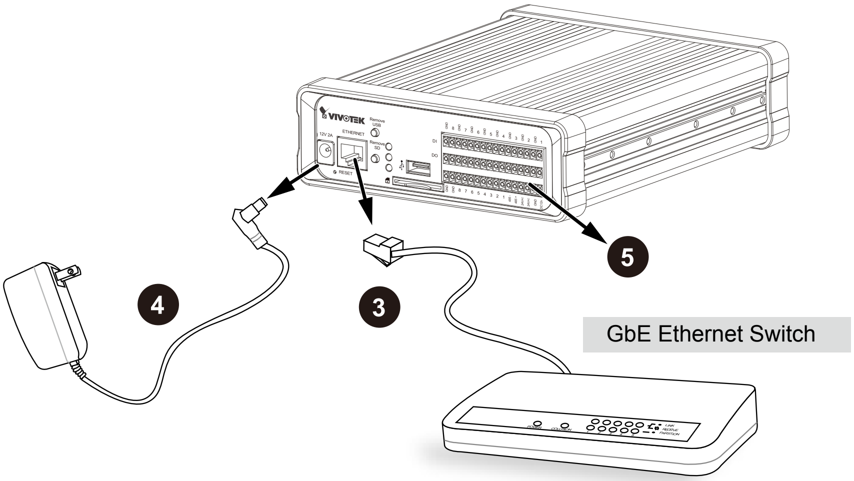
Setting up the Video Server over the Internet

This section explains how to configure the video server to an Internet connection.

1. Make video connection from the camera to the BNC video input.
2. Make audio connection from the Line-Out audio source to the RCA audio input.



3. Connect the Video Server to a switch via Ethernet cable.
4. Connect the power cable from the Video Server to a power outlet.
5. If you have external devices such as sensors and alarms, connect them to the general I/O terminal block. For detailed pin definition, please refer to the next page.

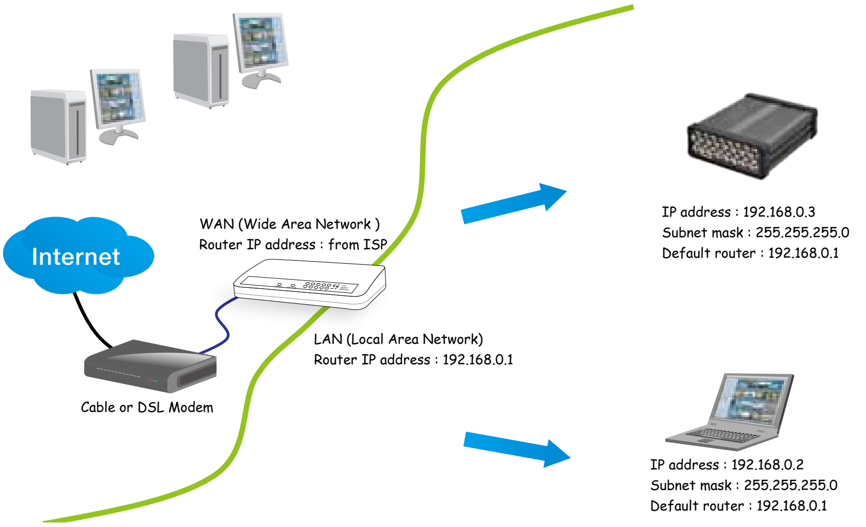


There are several ways to set up the video server over the Internet. The first way is to set up the video server behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet connection via a router

Before setting up the video server over the Internet, make sure you have a router and follow the steps below.

1. Connect your video server behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 12 for details.



WAN (Wide Area Network)
Router IP address : from ISP
Internet
IP address : 192.168.0.3
Subnet mask : 255.255.255.0
Default router : 192.168.0.1
LAN (Local Area Network)
Router IP address : 192.168.0.1
Cable or DSL Modem
IP address : 192.168.0.2
Subnet mask : 255.255.255.0
Default router : 192.168.0.1

2. In this case, if the Local Area Network (LAN) IP address of your Video server is 192.168.0.3, please forward the following ports for the Video server on the router.
   - HTTP port
   - RTSP port
   - RTP port for audio
   - RTCP port for audio
   - RTP port for video
   - RTCP port for video

If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to your router's user's manual.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Video server from the Internet. Please refer to Network Type on page 35 for details.

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Video server. Please refer to LAN on page 35 for details.

Internet connection via PPPoE (Point-to-Point over Ethernet)

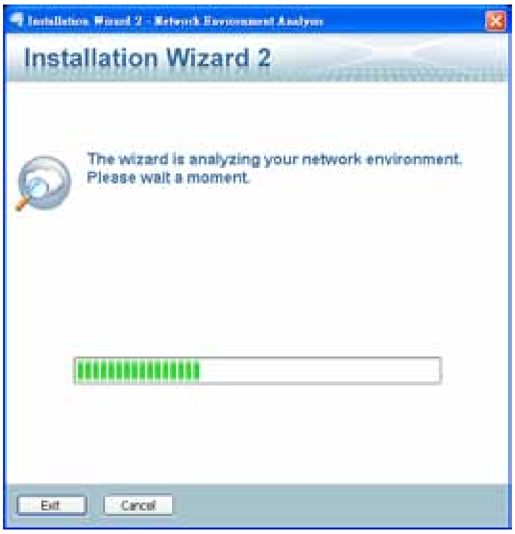
Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 36 for details.

Software Installation

Installation Wizard 2 (IW2), free-bundled software included on the product CD, helps you set up your video server on the LAN.

1. Install IW2 under the Software Utility directory from the software CD.
   Double click the IW2 shortcut on your desktop to launch the program.

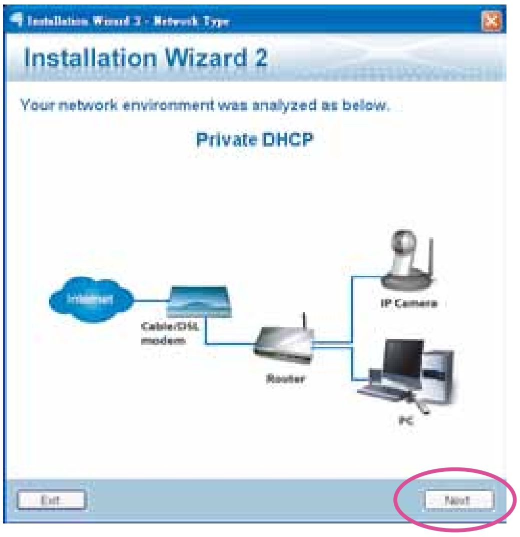
2. The program will conduct an analysis of your network environment.
   After your network environment is analyzed, please click **Next** to continue the program.



Installation Wizard 2 - Network Environment Analyzer

Installation Wizard 2

The wizard is analyzing your network environment.
Please wait a moment.



Installation Wizard 2 - Network Type

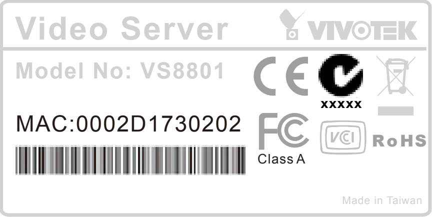
Installation Wizard 2

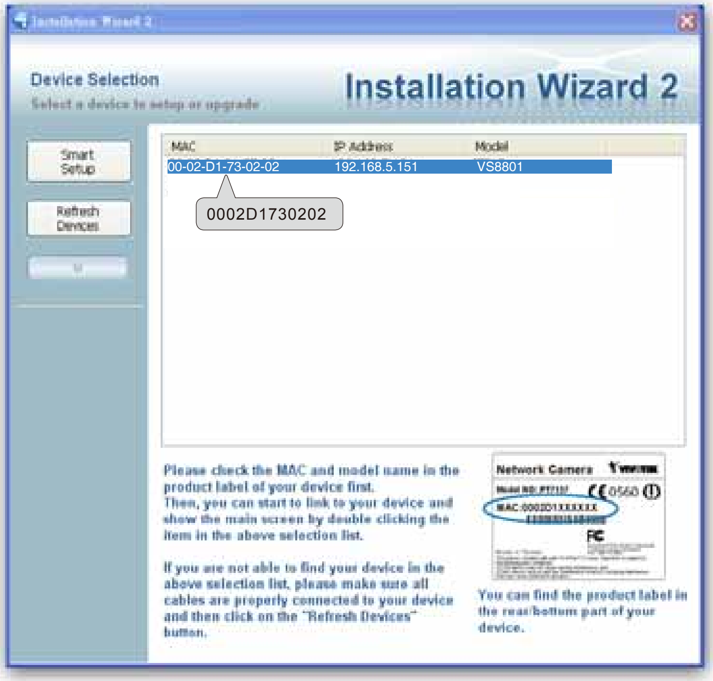
Your network environment was analyzed as below.

Private DHCP

3. The program will search for all VIVOTEK network devices on the same LAN.

4. After a brief search, the main installer window will prompt. Double-click on the MAC and model name which matches the product label on your device to connect to the Network Camera via a web browser.





Installation Wizard 2

Device Selection
Select a device to setup or upgrade

Installation Wizard 2

MAC	IP Address	Model
00-02-D1-73-02-02	192.168.5.151	VS8801

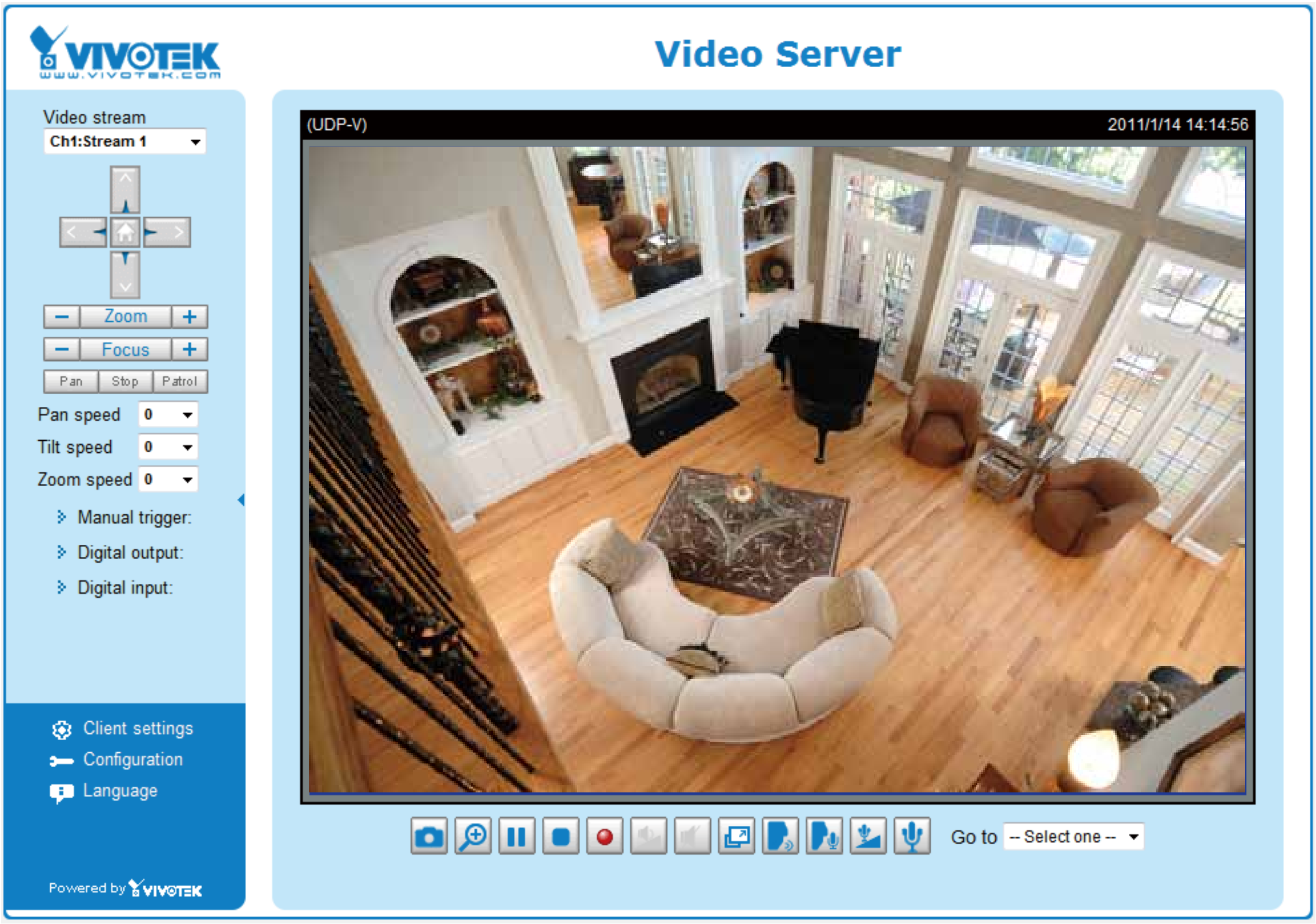
Please check the MAC and model name in the product label of your device first.
Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.

If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.

You can find the product label in the rear/bottom part of your device.

Ready to Use

1. A browser session with the Video Server should prompt as shown below.
2. You should be able to see live video from your camera. You may also install the 32-channel recording software from the software CD in a deployment consisting of multiple cameras. For its installation details, please refer to its related documents.

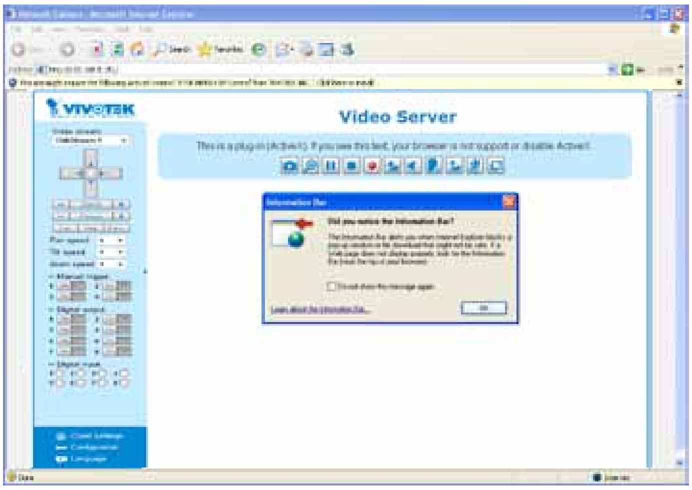


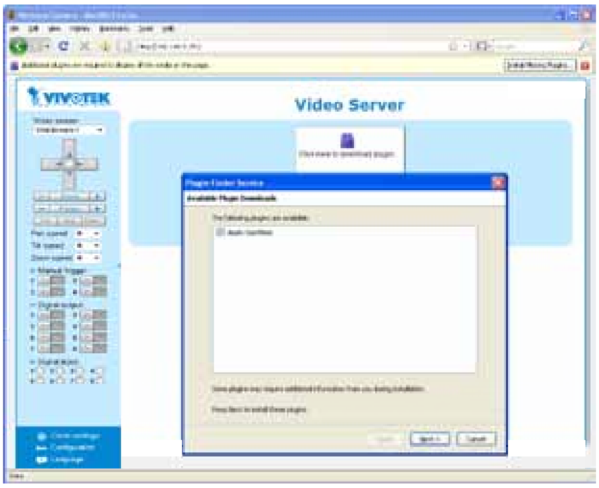
Accessing the Video Server

This chapter explains how to access the video server through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

Use Installation Wizard 2 (IW2) to access to the video servers on the LAN.
If your network environment is not a LAN, follow these steps to access the Netwotk Camera:
1. Launch your web browser (ex. Microsoft® Internet Explorer, Mozilla Firefox, or Netscape).
2. Enter the IP address of the video server in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If it is the first time installing the VIVOTEK video server, an information bar will pop up as shown below. Follow the instructions to install the required plug-ins on your computer.



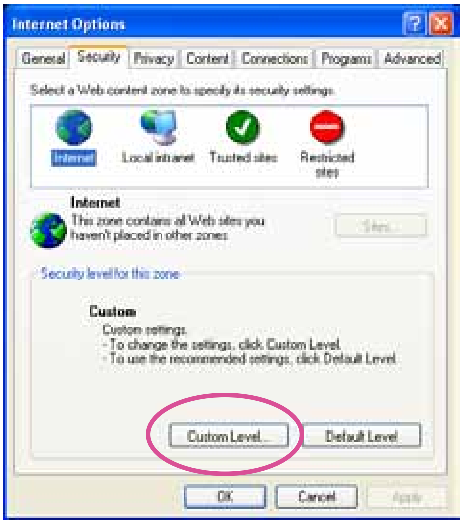


NOTE:

► *By default, the video server is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the video server. For more information about how to enable password protection, please refer to Security on page 28.*

► *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable the ActiveX® Controls for your browser.*

1. Choose Tools > Internet Options > Security > Custom Level.

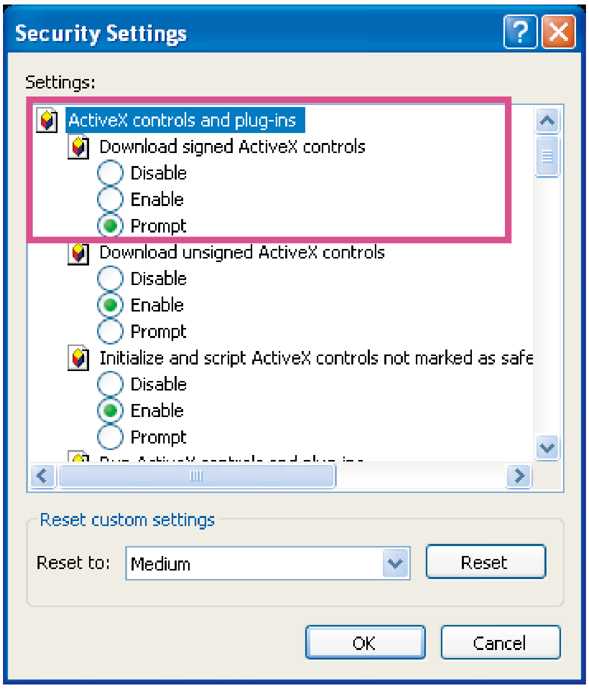


Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

2. *Look for Download signed ActiveX® controls; select Enable or Prompt. Click **OK**.*



Security Settings

Settings:

ActiveX controls and plug-ins

Download signed ActiveX controls
- ○ Disable
- ○ Enable
- ● Prompt

Download unsigned ActiveX controls
- ○ Disable
- ● Enable
- ○ Prompt

Initialize and script ActiveX controls not marked as safe
- ○ Disable
- ● Enable
- ○ Prompt

Run ActiveX controls and plug-ins

Reset custom settings

Reset to: Medium

3. *Refresh your web browser, then install the Active X® control. Follow the instructions to complete installation.*

Using RTSP Players

To view the MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.

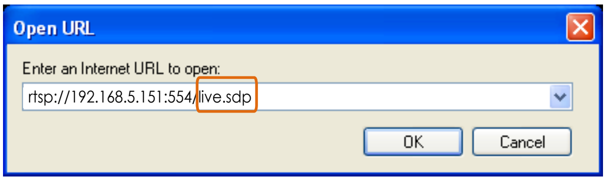
Quick Time Player

Real Player

1. Launch the RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. The address format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 48.

For example:



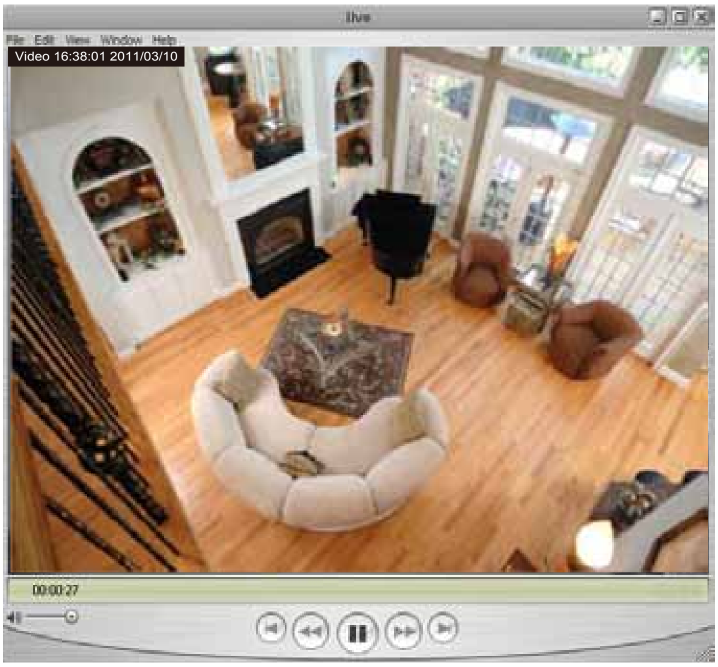
Open URL

Enter an Internet URL to open:

rtsp://192.168.5.151:554/live.sdp

4. The live video will be displayed in your player.

   For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 48 for details.



Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the video server can be accessed over the Internet. For more information on how to set up the video server over the Internet, please refer to Setup the video server over the Internet on page 10.

To utilize this feature, please check the following settings on your video server:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
   For more information, please refer to RTSP Streaming on page 48.

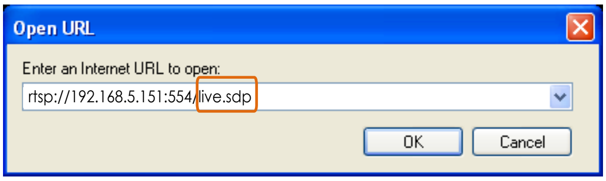
2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video and audio streaming parameters as listed below.

Video Mode	MPEG-4
Frame size	QCIF
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (G.711)	64kbps

3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 48.

4. Launch the player on the 3GPP-compatible mobile devices (ex. Real Player).

5. Type the following URL commands into the player.
   The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream 3>.
   For example:



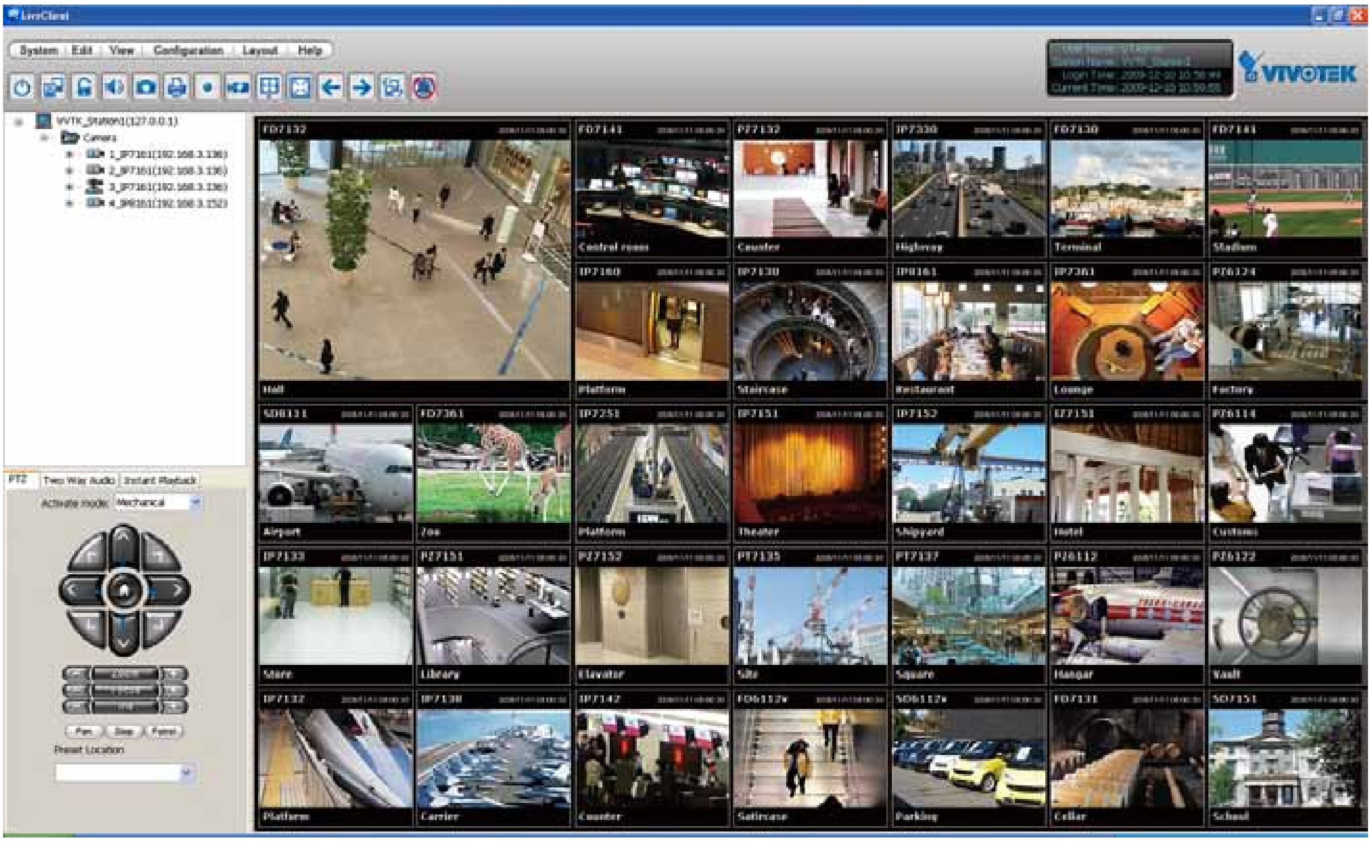
Open URL

Enter an Internet URL to open:

rtsp://192.168.5.151:554/live.sdp

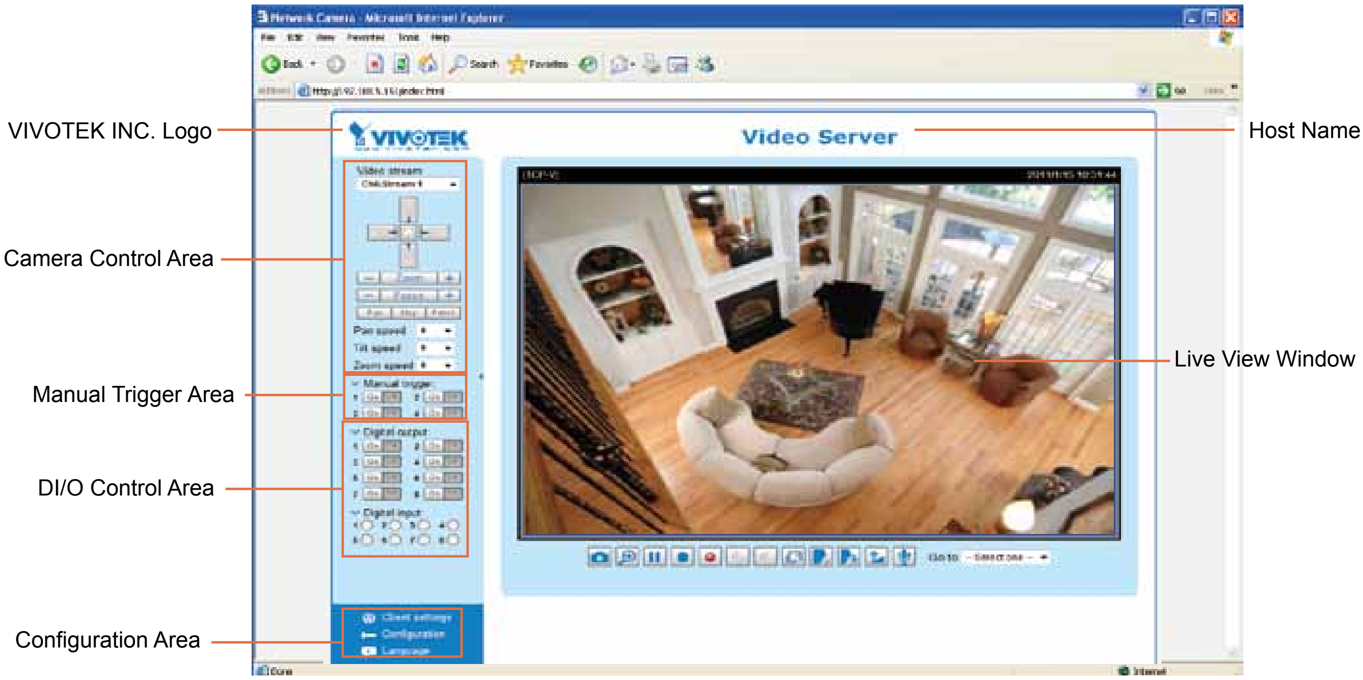
Using VIVOTEK Recording Software

The product software CD also contains recording software, allowing simultaneous monitoring and video recording for multiple video servers. Please install the recording software; then launch the program to add the video server to the Channel list. For detailed information about how to use the recording software, please refer to the user’s manual of the software or download it from http://www.vivotek.com.



Main Page

This chapter explains the layout of the main page. It is composed of the following sections: VIVOTEK INC. Logo, Host Name, Camera Control Area, Configuration Area, Menu, and Live Video Window. The Manual Trigger and Digital Input/Digital Output control menus are expandable and collapsible, while the PTZ navigation panel is available only when a PTZ camera is attached.



VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

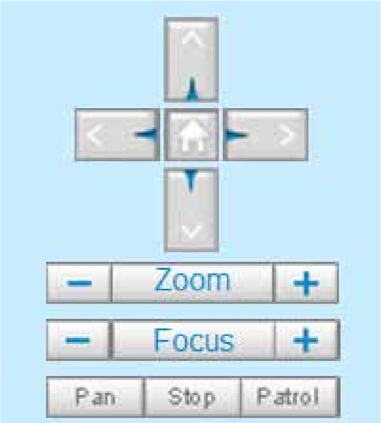
Host Name

The host name can be customized to fit your needs. For more information, please refer to System settings on page 26.

Camera Control Area

Video Stream: VS8401 supports 4 channels for video live viewing, as VS8801 supports 8 channels. Each channel allows you to view only one stream. There are channel1,2,3,4,(5,6,7,8),and Quad View for you to choose. For more information about video settings, please refer to page 56 for detailed information.

PTZ Control Area: The up/down/left/right/zoom/focus/pan buttons allow you to adjust the video in the viewing window to the spot you wish to watch. **Home** button allows you to resume the center of the screen. Click **Patrol** to move from one point to another; click it again to stop patroling. Click **Stop** to stop the pan movement. Please refer to **Configuration > Camera Control** on page 68 for more information.



Pan/Tilt/Zoom Speed: In the drop-down list, the speed ranges from -5~5 (slow/fast).

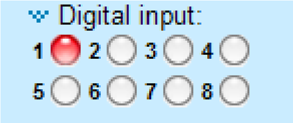
Manual Trigger Area

Click to enable/disable an event trigger manually. Please configure an event setting on Application page before enable this function. A total of 4 event settings can be configured. For more information about event settings, please refer to page 79.
If you want to hide this item on the homepage, please go to the Homepage layout page to uncheck "show manual trigger button". Please refer to page 75 for detail.

DI/O Control Area

Digital output: There are 4 (VS8401) or 8 (VS8801) digital output switches; click to turn the digital output device on or off. Switch 1 is for channel 1 digital output control, switch 2 is for channel 2 digital output control, and so on.

Digital input: There are 4 (VS8401) or 8 (VS8801) digital input status indicators. A Red indicator shows the digital input status is active, while the white indicator shows inactive.



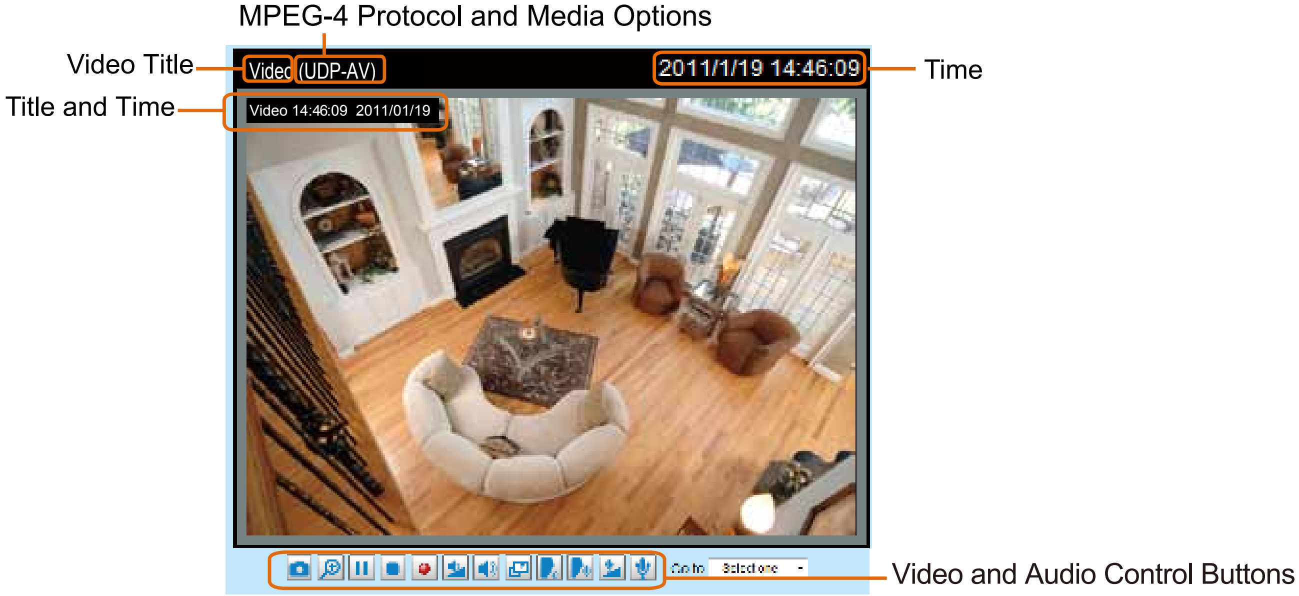
Configuration Area

Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 22.

Configuration: Click this button to access the configuration page of the video server. It is suggested that a password be applied to the video server so that only the administrator can configure the video server. For more information, please refer to Configuration on page 25.

Language: Click this button to choose a language for the user interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Live Video Window


MPEG-4 Protocol and Media Options
Video Title
Title and Time
Video (UDP-AV)
2011/1/19 14:46:09
Time
Video 14:46:09 2011/01/19
Go to
Select one
Video and Audio Control Buttons

Video Title: The video title can be configured. For more information, please refer to Video settings on page 56.

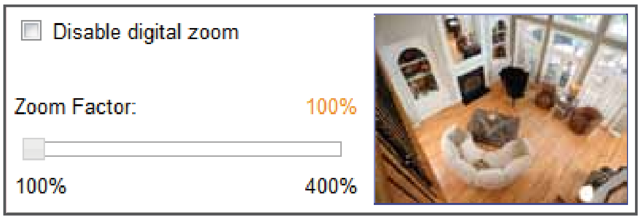
MPEG-4 Protocol and Media Options: The transmission protocol and media options for MPEG-4 video streaming. For further configuration, please refer to Client settings on page 22.

Time: Display the current time. For further configuration, please refer to Video settings on page 56.

Title and Time: The video title and time can be stamped on the streaming video. For further configuration, please refer to Video settings on page 56.
Video and Audio Control Buttons: Depending on the video server model and video server configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.



☐ Disable digital zoom

Zoom Factor: 100%

100% 400%

⏸ Pause: Pause the transmission of the streaming media. The button becomes the ▶ Resume button after clicking the Pause button.

■ Stop: Stop the transmission of the streaming media. Click the ▶ Resume button to continue transmission.

● Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the ■ Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 saving options on page 23 for details.

Volume: When the Mute function is not activated, move the slider bar to adjust the volume on the local computer.

Mute: Turn off the volume on the local computer. The button becomes the Audio On button after clicking the Mute button.

Talk: Click this button to talk to people around the video server. Audio will project from the external speaker connected to the video server. Click this button again to end talking transmission.

Broadcast: Click this button to broadcast to all channels.

Mic Volume: When the Mute function is not activated, move the slider bar to adjust the microphone volume on the local computer.

Mute: Turn off the Mic volume on the local computer. The button becomes the Mic On button after clicking the Mute button.

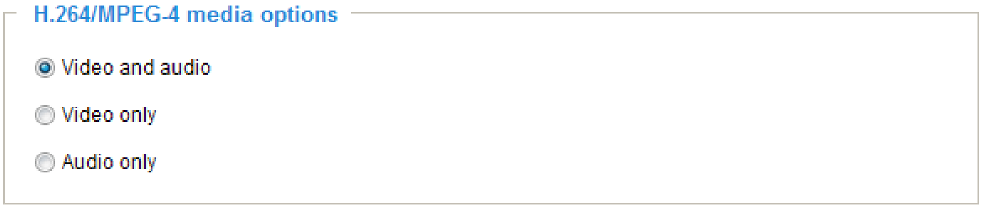
Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

Go to: The drop-down menu enables you to locate and move to a preset location instantly on the viewing window.

Client settings

This chapter explains how to select the stream transmission mode and saving options on the local computer. When completed with the settings on this page, click **Save** on the page bottom to enable the settings.

H.264 / MPEG-4 media options



H.264/MPEG-4 media options

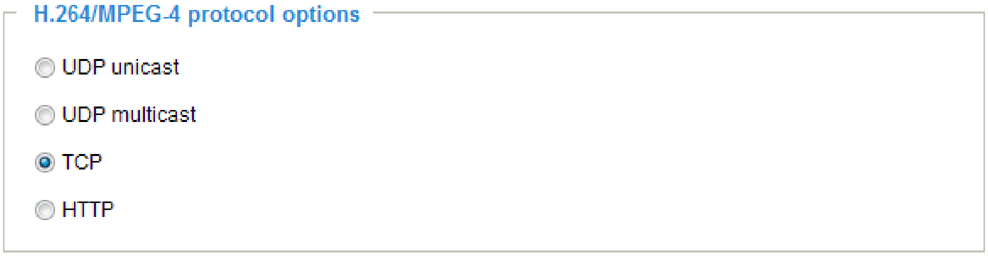
● Video and audio

○ Video only

○ Audio only

Select to stream video or audio data or both. This is enabled only when the video mode is set to H.264 or MPEG-4.

H.264 / MPEG-4 protocol options



H.264/MPEG-4 protocol options

○ UDP unicast

○ UDP multicast

● TCP

○ HTTP

Depending on your network environment, there are four transmission modes of H.264 or MPEG-4 streaming:

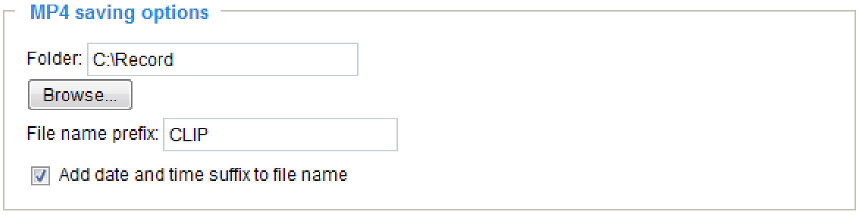
UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the video server allows up to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the video server while serving multiple clients at the same time. Note that to utilize this feature, the video server must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 48.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. The downside of this protocol is that its real-time effect is not as good as that of the UDP protocol.

HTTP: This protocol allows the same quality as TCP protocol without needing to open specific ports for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data through.

MP4 saving options



MP4 saving options

Folder: C:\Record

Browse...

File name prefix: CLIP

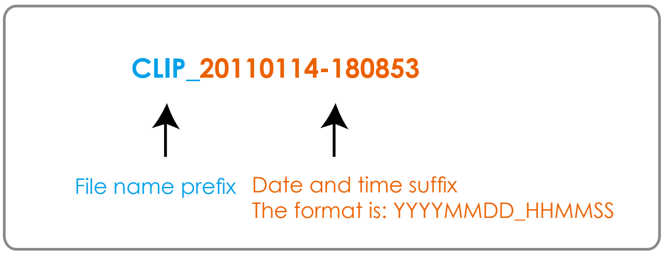
☑ Add date and time suffix to file name

Users can record live video as they are watching it by clicking ● Start MP4 Recording on the main page. Here, you can specify the storage destination and file name.

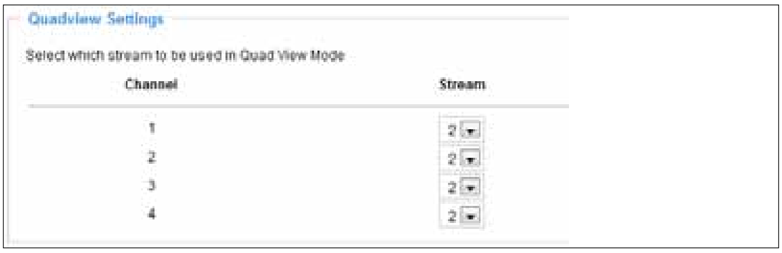
Folder: Specify a storage destination for the recorded video files.

File name prefix: Enter the text that will be appended to the front of the video file name.

Add date and time suffix to the file name: Select this option to append the date and time to the end of the file name.



Quadview settings



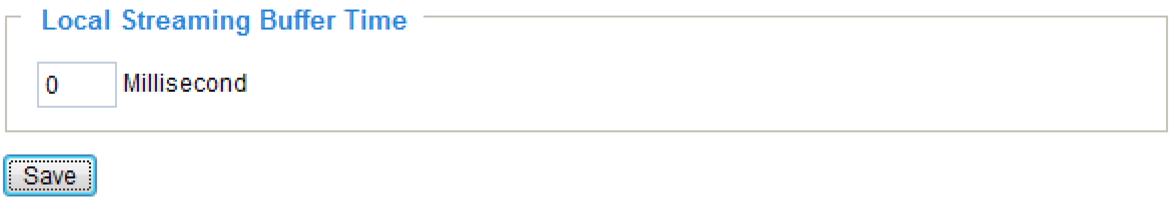
Quadview Settings

Select which stream to be used in Quad View Mode

Channel	Stream
1	2
2	2
3	2
4	2

Here is where you configure which video streams will be displayed in the Quad View window. The default is the stream 2 with a lower resolution.

Local Streaming Buffer Time



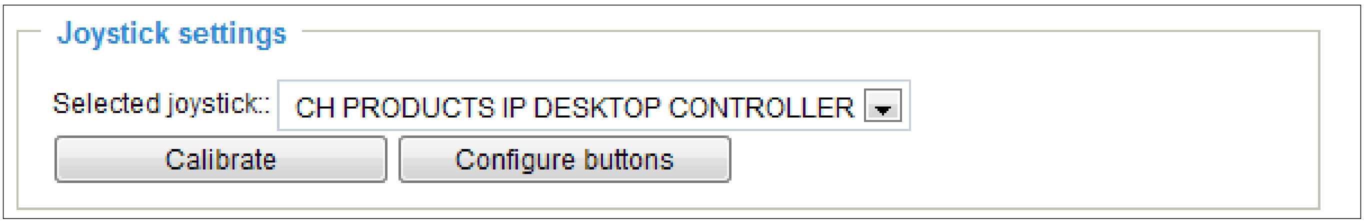
Local Streaming Buffer Time

0 Millisecond

Save

Due to the unsteady bandwidth flow, the live streaming may lag and not be very smoothly. If you enable this option, the live streaming will be stored on the camera's buffer area for a few seconds before playing on the live viewing window. This will help you see the streaming more smoothly. If you enter 3000 Millisecond, the streaming will delay 3 seconds.

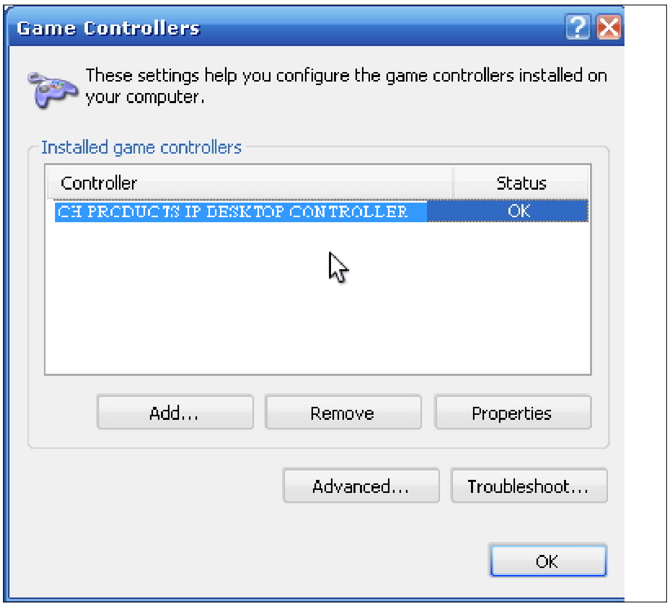
Joystick settings



Joystick settings

Selected joystick:: CH PRODUCTS IP DESKTOP CONTROLLER

Calibrate: Make sure a joystick is already attached to your COM port or USB port on your client computer. Click on the Calibrate button and the Windows Game Controller function will be started. If properly connected, your operating system should have already detected the joystick. Follow the onscreen instructions to calibrate your joystick.

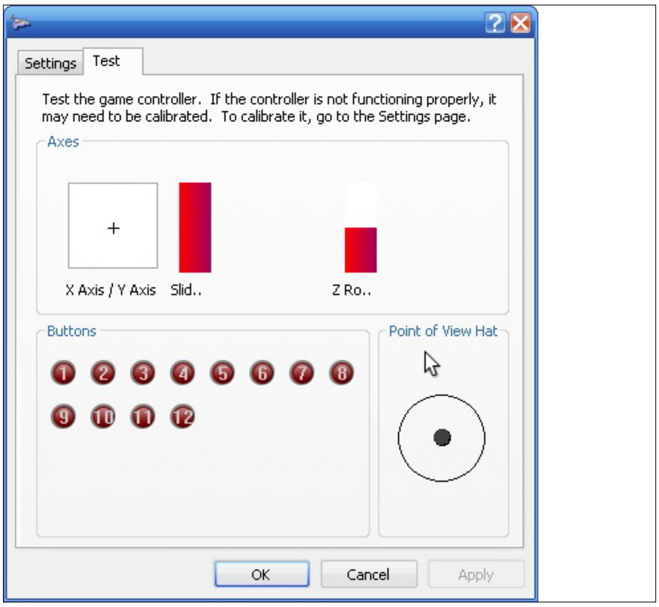


Game Controllers

These settings help you configure the game controllers installed on your computer.

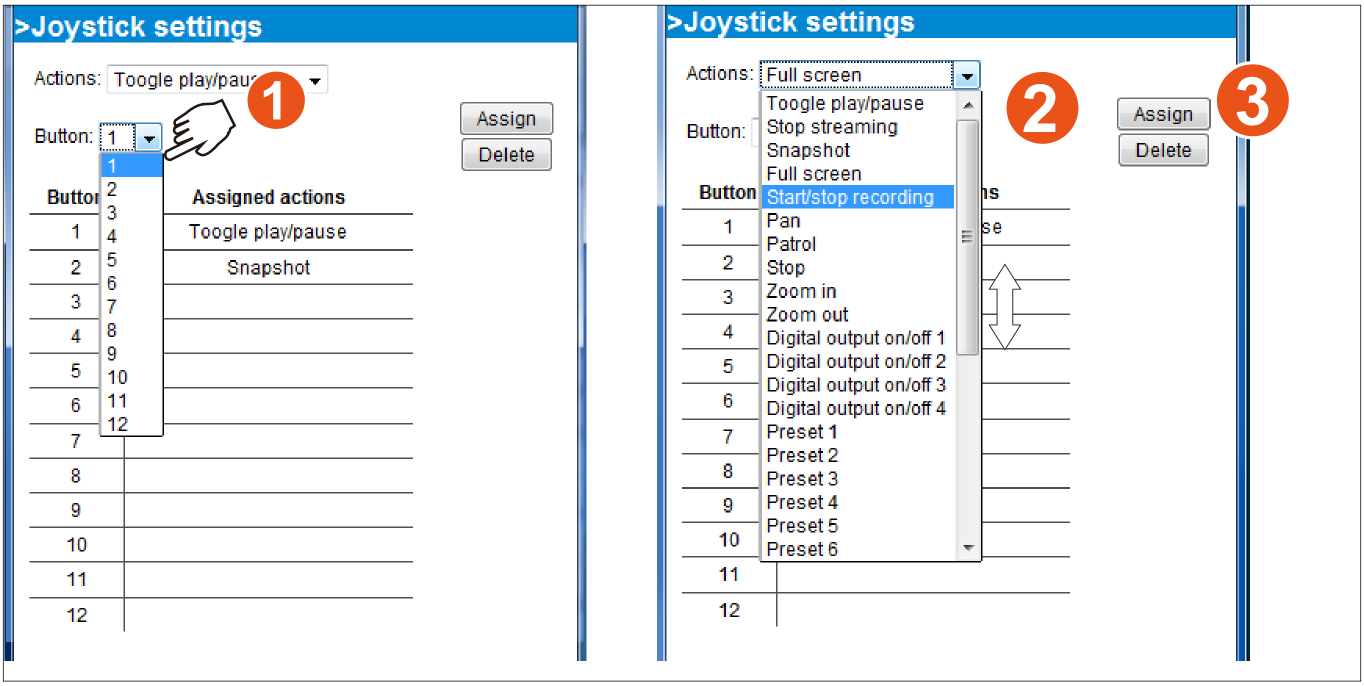
Installed game controllers

Controller	Status
CH PRODUCTS IP DESKTOP CONTROLLER	OK



Test the game controller. If the controller is not functioning properly, it may need to be calibrated. To calibrate it, go to the Settings page.

Configure buttons: You can define individual joystick buttons using this function. Click to open a configuration window and assign functions to joystick buttons using the following steps: 1. Select a button uing the pull-down menu. 2. Select an Action to be toggled by the button. 3. Click on the Assign button, and then repeat the process to define other buttons.



>Joystick settings

Actions: Toogle play/pau

Button: 1

Button	Assigned actions
1	Toogle play/pause
2	Snapshot
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

>Joystick settings

Actions: Full screen

Configuration

Click **Configuration** on the main page to enter the camera setting pages. Note that only Administrators can access the configuration page.

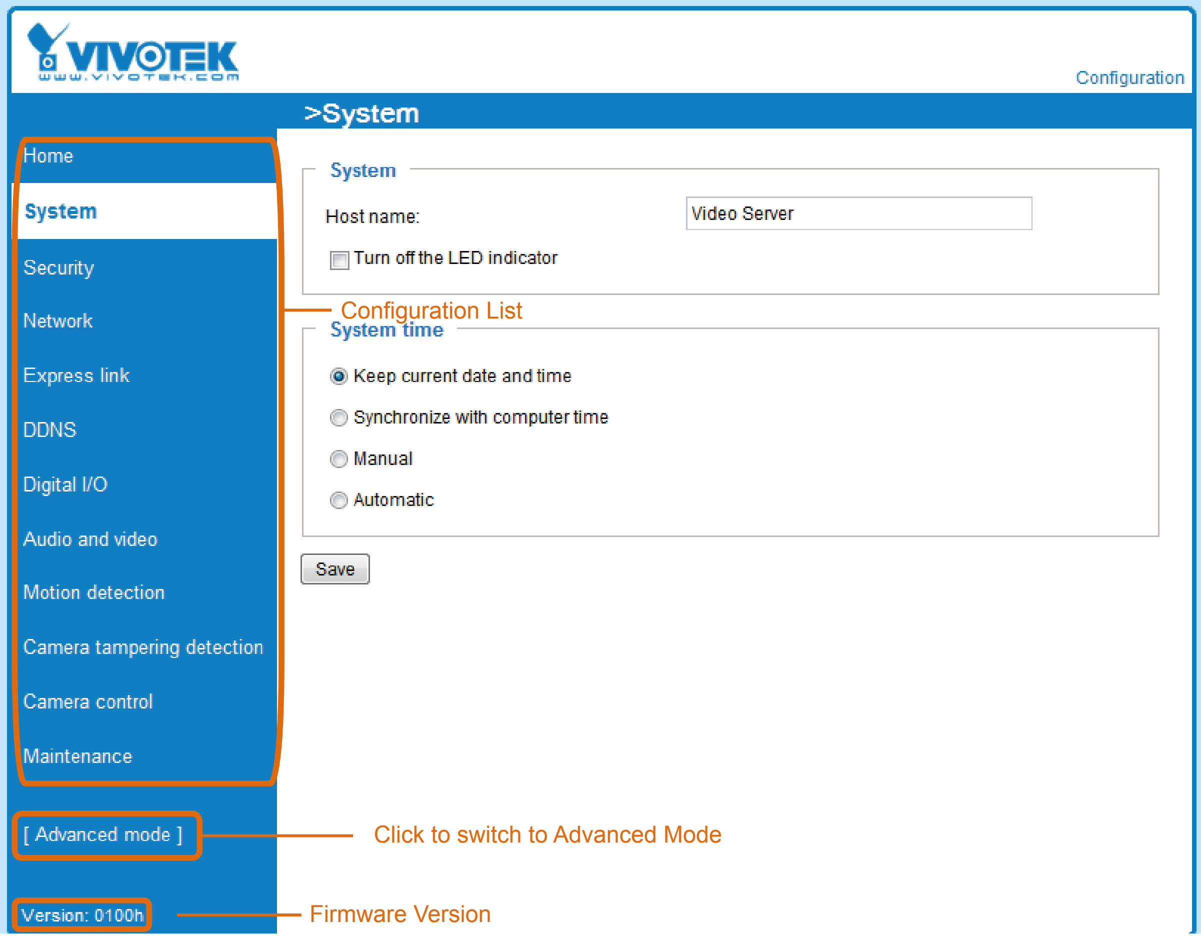
VIVOTEK offers an easy-to-use user interface that helps you set up your video server with minimal effort. To simplify the setting procedure, two types of user interfaces are available: Advanced Mode for professional users and Basic Mode for entry-level users. Some advanced functions (HTTPS/ SNMP/ Access list/ Homepage layout/ Application/ System log/ View parameters) are not displayed in Basic Mode.

If you want to set up advanced functions, please click **[Advanced mode]** on the bottom of the configuration list to quickly switch to Advanced Mode.

In order to simplify the user interface, the detailed information will be hidden unless you click on the function item. When you click on the first sub-item, the detailed information for the first sub-item will be displayed; when you click on the second sub-item, the detailed information for the second sub-item will be displayed and that of the first sub-item will be hidden.

The following is the interface of the Basic mode and the Advanced mode:

Basic mode



System

Host name: Video Server

□ Turn off the LED indicator

System time

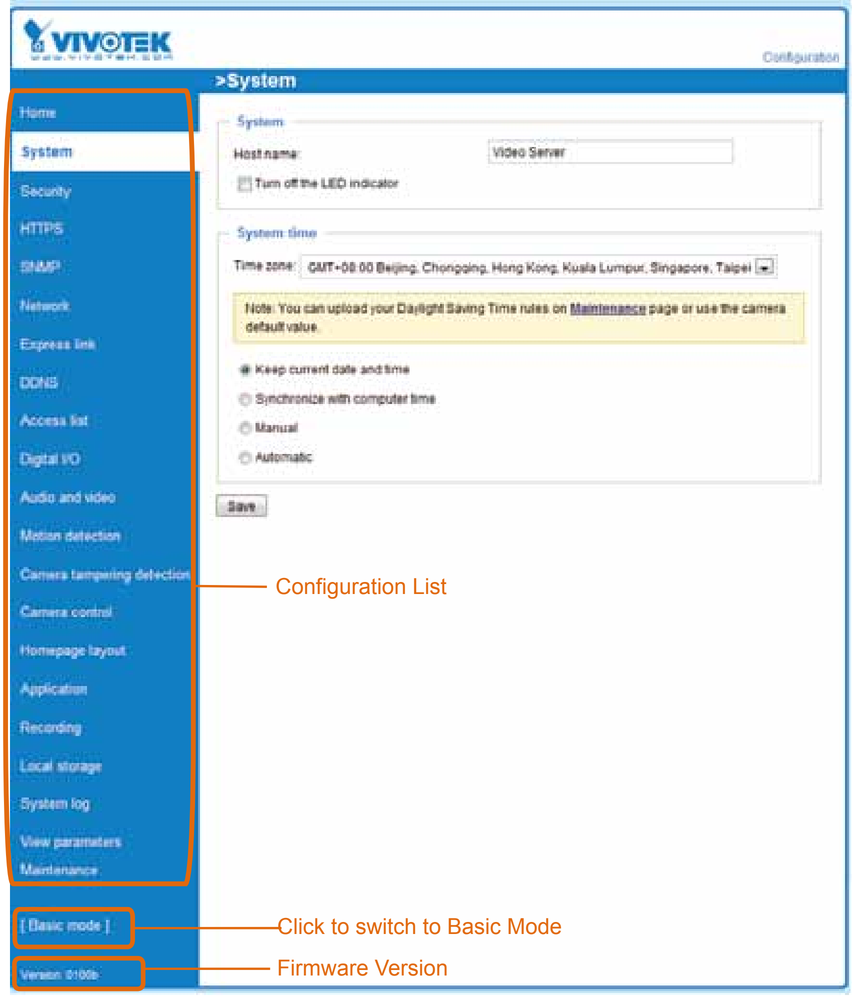
● Keep current date and time

○ Synchronize with computer time

○ Manual

○ Automatic

Advanced mode



>System

System

Host name: Video Server

□ Turn off the LED indicator

System time

Time zone: GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei

Note: You can upload your Daylight Saving Time rules on Maintenance page or use the camera default value.

● Keep current date and time

○ Synchronize with computer time

○ Manual

○ Automatic

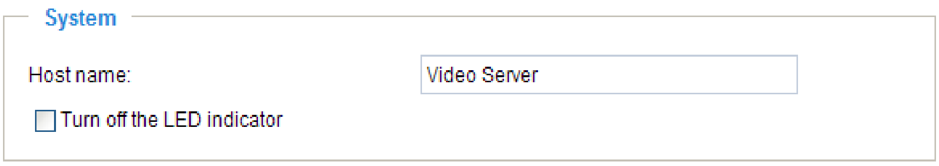
Version: 0100b

Each function on the configuration list will be explained in the following sections. Those functions that are displayed only in Advanced Mode are marked with Advanced mode. If you want to set up advanced functions, please click **[Advanced Mode]** at the bottom of the configuration list to quickly switch over.

System

This section explains how to configure the basic settings for the video server, such as the host name and system time. It is composed of the following three columns: System, System Time and DI and DO. When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

System



System

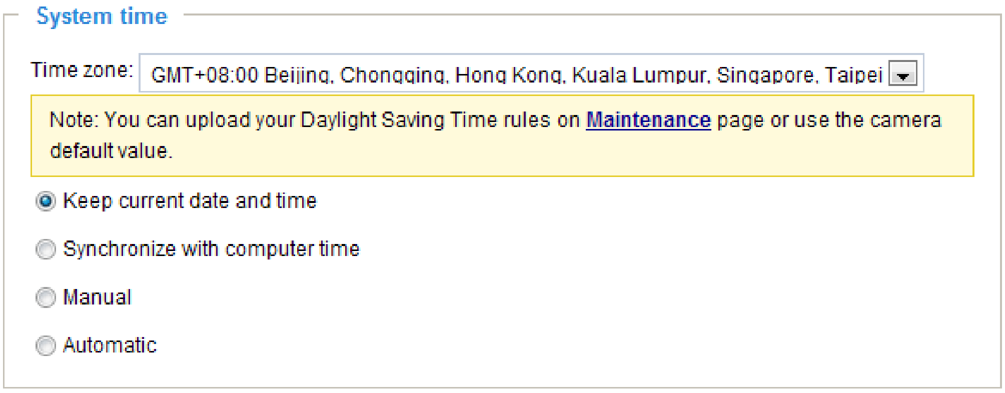
Host name: Video Server

□ Turn off the LED indicator

Host name: Enter a desired name for the video server. The text will be displayed at the top of the main page.

Turn off the LED indicators: If you do not want to let others know that the video server is in operation, you can select this option to turn off the LED indicators.

System time



System time

Time zone: GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei

Note: You can upload your Daylight Saving Time rules on Maintenance page or use the camera default value.

● Keep current date and time

○ Synchronize with computer time

○ Manual

○ Automatic

Keep current date and time: Select this option to preserve the current date and time of the Video server. The video server's internal real-time clock maintains the date and time even when the power of the system is turned off.

Sync with computer time: Select this option to synchronize the date and time of the video server with the local computer. The read-only date and time of the PC is displayed as updated.

Manual: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the video server to the default time servers.

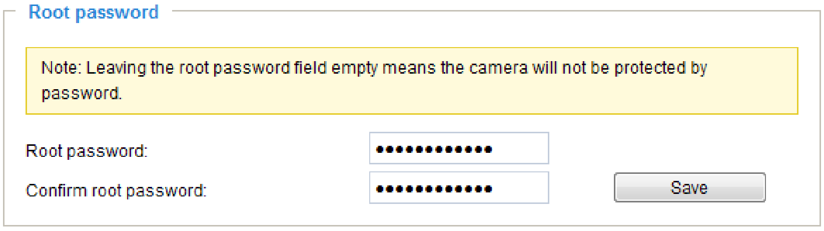
Update interval: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

Time zone Advanced Mode: Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules on the Maintenance page, please refer to Upload / Export daylight saving time configuration file on page 102 for details.

Security

This section explains how to enable password protection and create multiple accounts.

Root password



Root password

Note: Leaving the root password field empty means the camera will not be protected by password.

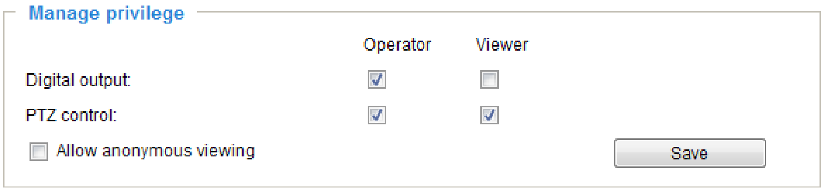
Root password: ••••••••••••

Confirm root password: ••••••••••••

The administrator account name is “root”, which is permanent and can not be deleted. If you want to add more accounts in the Manage User column, please apply the password for the “root” account first.

1. Type the password identically in both text boxes, then click **Save** to enable password protection.
2. A window will be prompted for authentication; type the correct user’s name and password in their respective fields to access the video server.

Manage privilege Advanced Mode



Manage privilege

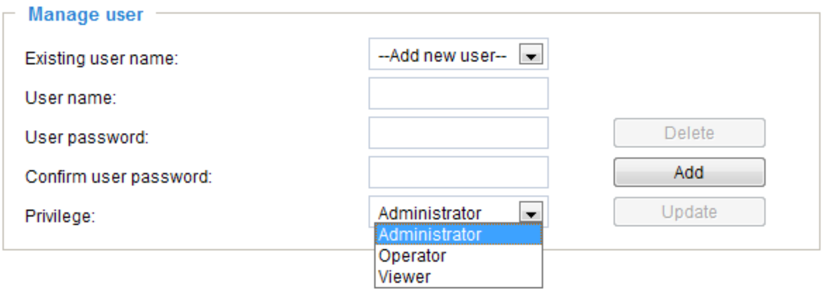
	Operator	Viewer
Digital output:	☑	□
PTZ control:	☑	☑

□ Allow anonymous viewing

Digital Output & PTZ control: You can modify the manage privilege of operators or viewers. Check or uncheck the item, then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the video server through the main page. (Please refer to Main Page on page 19.)

Allow anonymous viewing: If you check this item, any client can access the live stream without entering a User ID and Password.

Manage user



Manage user

Existing user name: --Add new user--

User name:

User password:

Confirm user password:

Privilege: Administrator

Administrators can add up to 20 user accounts.

1. Input the new user’s name and password.
2. Select the privilege level for the new user account. Click **Add** to enable the setting.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Though operators cannot access the Configuration page, they can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands of the video server on page 105. Viewers access only the main page for live viewing.

Here you also can change a user’s access rights or delete user accounts.

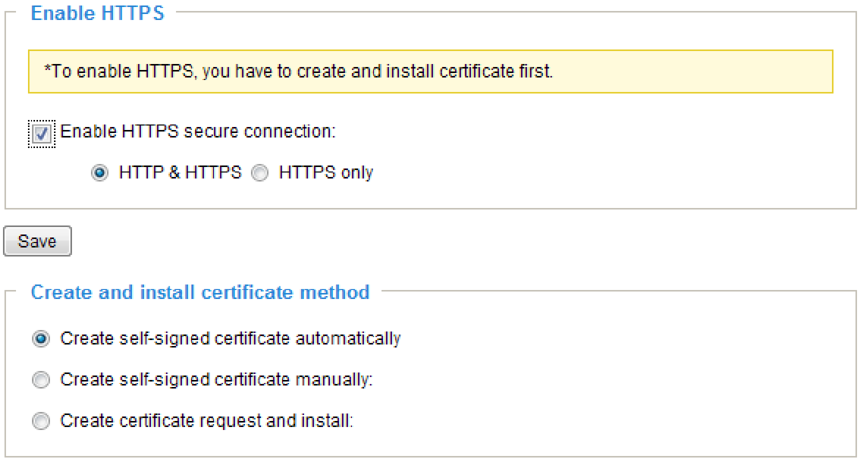
1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

HTTPS (Hypertext Transfer Protocol over SSL) Advanced Mode

This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

Enable HTTPS

Check this item to enable HTTPS communication, then select a connection option: "HTTP & HTTPS" or "HTTPS only". Note that you have to create and install a certificate first in the second column before clicking the **Save** button.



Enable HTTPS

*To enable HTTPS, you have to create and install certificate first.

☑ Enable HTTPS secure connection:

● HTTP & HTTPS ○ HTTPS only

Save

Create and install certificate method

● Create self-signed certificate automatically

○ Create self-signed certificate manually:

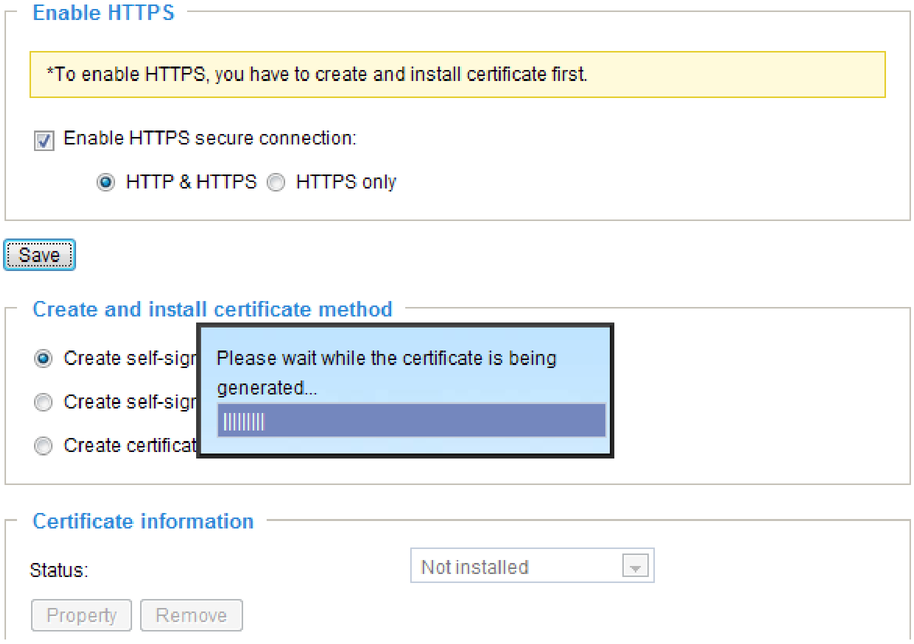
○ Create certificate request and install:

Create and install certificate method

Before using HTTPS for communication with the video server, a **Certificate** must be created first. There are three ways to create and install a certificate:

Create self-signed certificate automatically

1. Select this option.
2. In the first column, check **Enable HTTPS secure connection**, then select a connection option: “HTTP & HTTPS” or “HTTPS only”.
3. Click **Save** to generate a certificate.



Enable HTTPS

*To enable HTTPS, you have to create and install certificate first.

☑ Enable HTTPS secure connection:

● HTTP & HTTPS ○ HTTPS only

Save

Create and install certificate method

● Create self-sign

○ Create self-sign

○ Create certificat

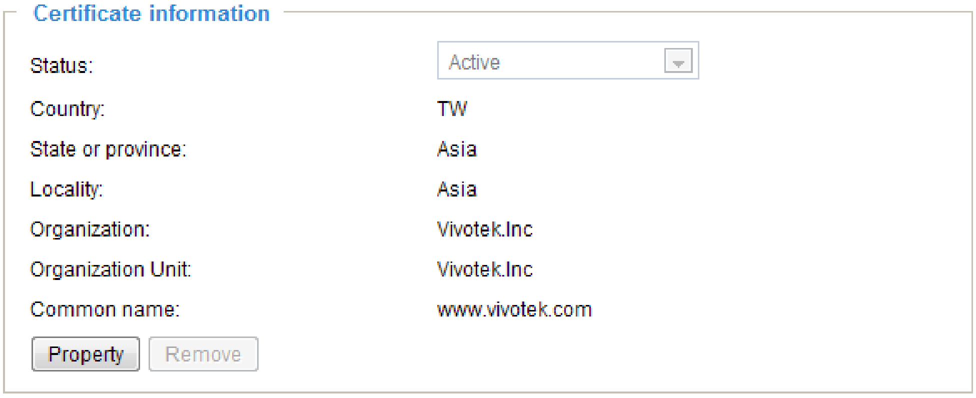
Please wait while the certificate is being generated...

Certificate information

Status: Not installed

Property Remove

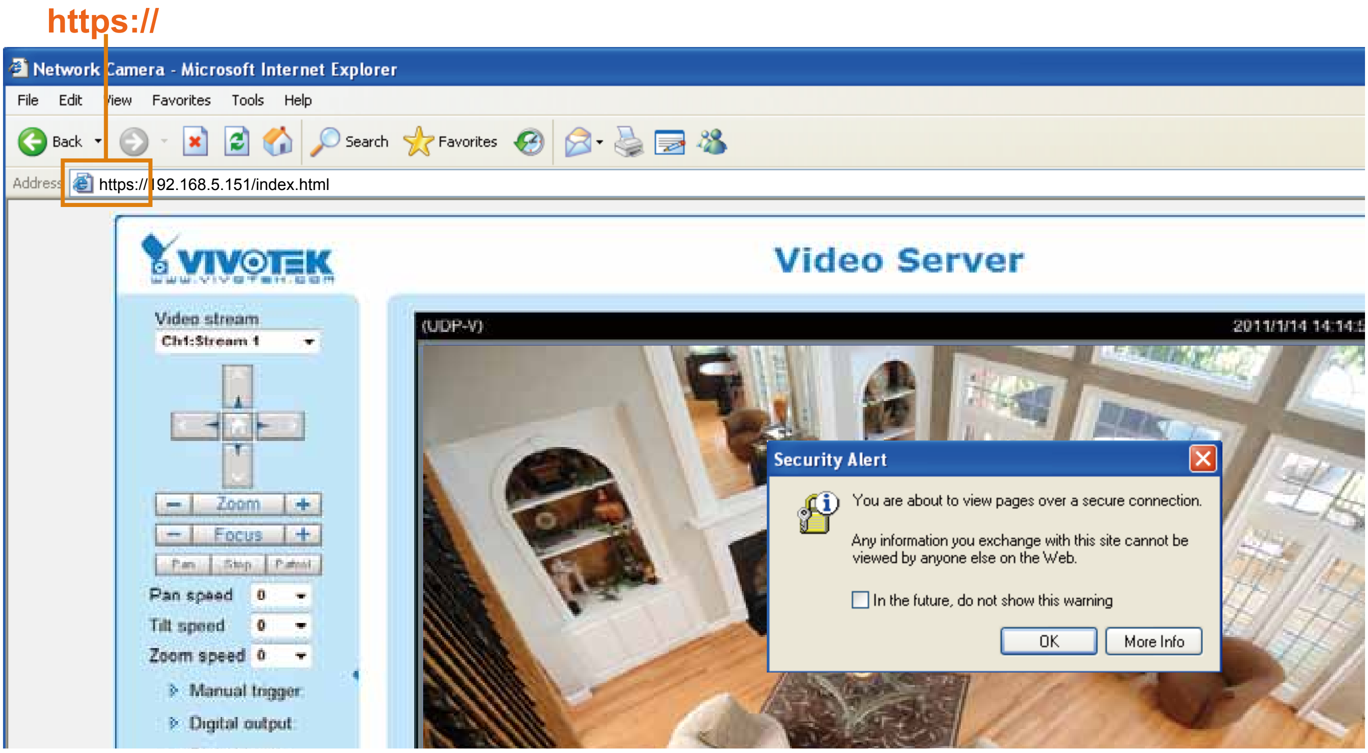
4. The Certificate Information will automatically de displayed in the third column as shown below. You can click **Property** to view detailed information about the certificate.



Certificate information

Status:	Active
Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	Vivotek.Inc
Organization Unit:	Vivotek.Inc
Common name:	www.vivotek.com

5. Click **Home** to return to the main page. Change the address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.



https://

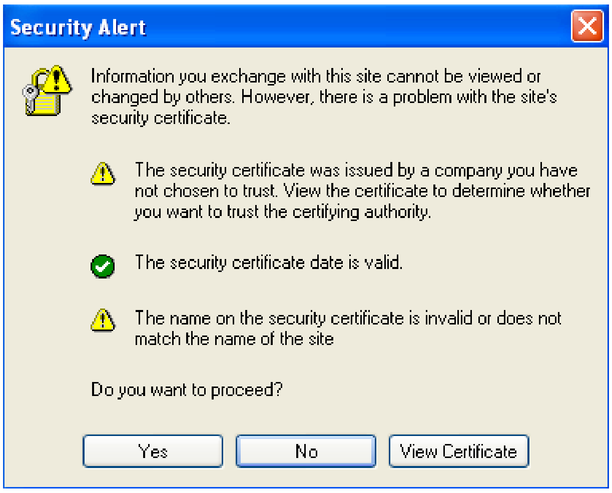
Address https://192.168.5.151/index.html

Security Alert

You are about to view pages over a secure connection.

Any information you exchange with this site cannot be viewed by anyone else on the Web.

□ In the future, do not show this warning



Security Alert

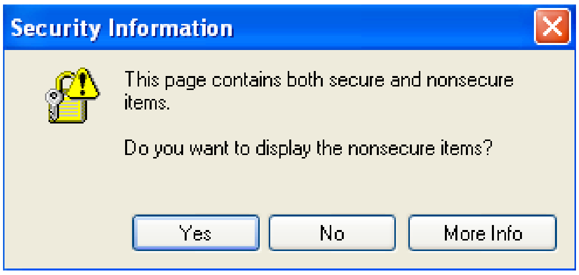
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?



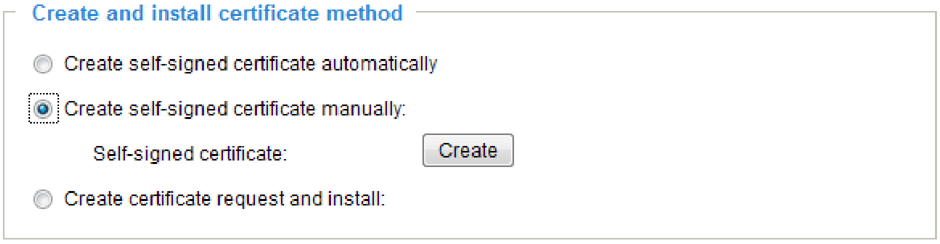
Security Information

This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

Create self-signed certificate manually

1. Select this option.
2. Click **Create** to open the Create Certificate page, then click **Save** to generate the certificate.



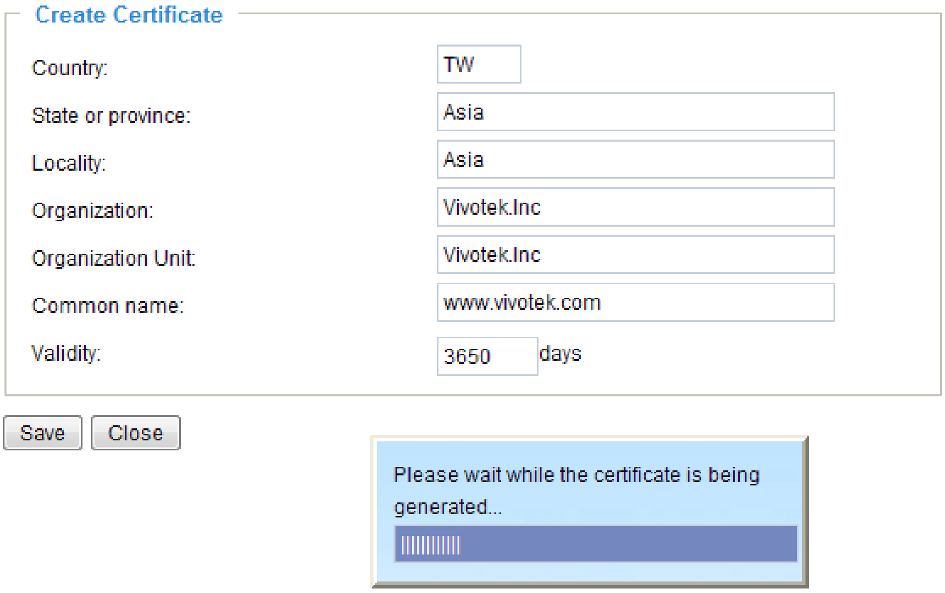
Create and install certificate method

○ Create self-signed certificate automatically

● Create self-signed certificate manually:

Self-signed certificate: Create

○ Create certificate request and install:



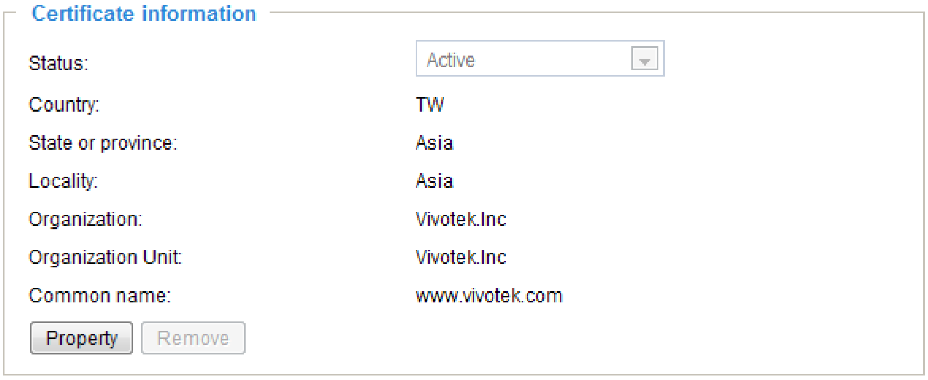
Create Certificate

Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	Vivotek.Inc
Organization Unit:	Vivotek.Inc
Common name:	www.vivotek.com
Validity:	3650 days

Save Close

Please wait while the certificate is being generated...

3. The Certificate Information will automatically be displayed in the third column as shown below. You can click **Property** to see detailed information about the certificate.



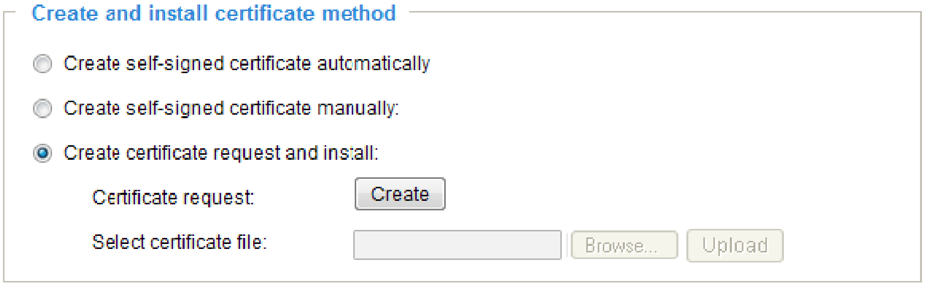
Certificate information

Status:	Active
Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	Vivotek.Inc
Organization Unit:	Vivotek.Inc
Common name:	www.vivotek.com

Property Remove

Create certificate and install : Select this option if you want to create a certificate from a certificate authority.

1. Select this option.
2. Click **Create** to open the Create Certificate page, then click **Save** to generate the certificate.



Create and install certificate method

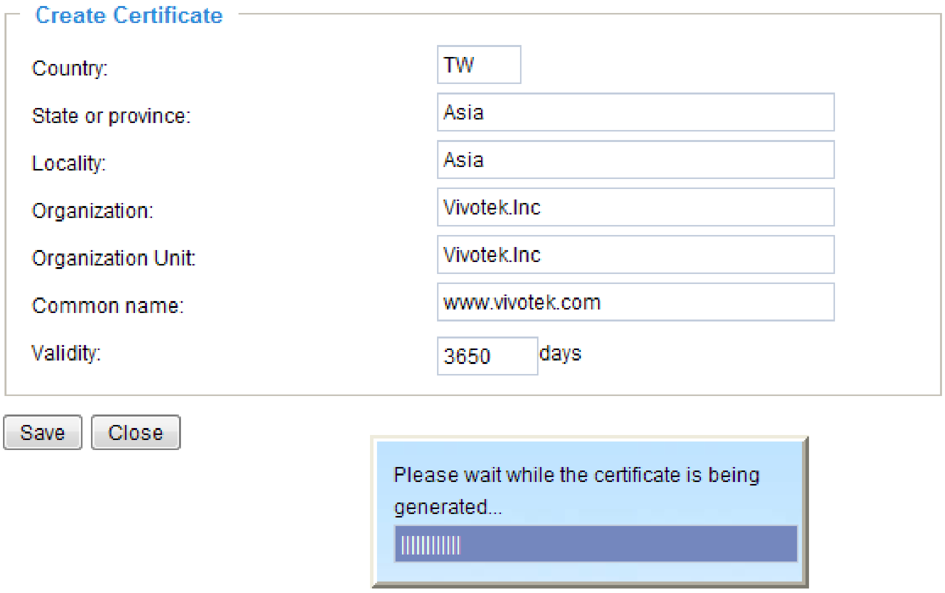
○ Create self-signed certificate automatically

○ Create self-signed certificate manually:

● Create certificate request and install:

Certificate request: Create

Select certificate file: Browse... Upload

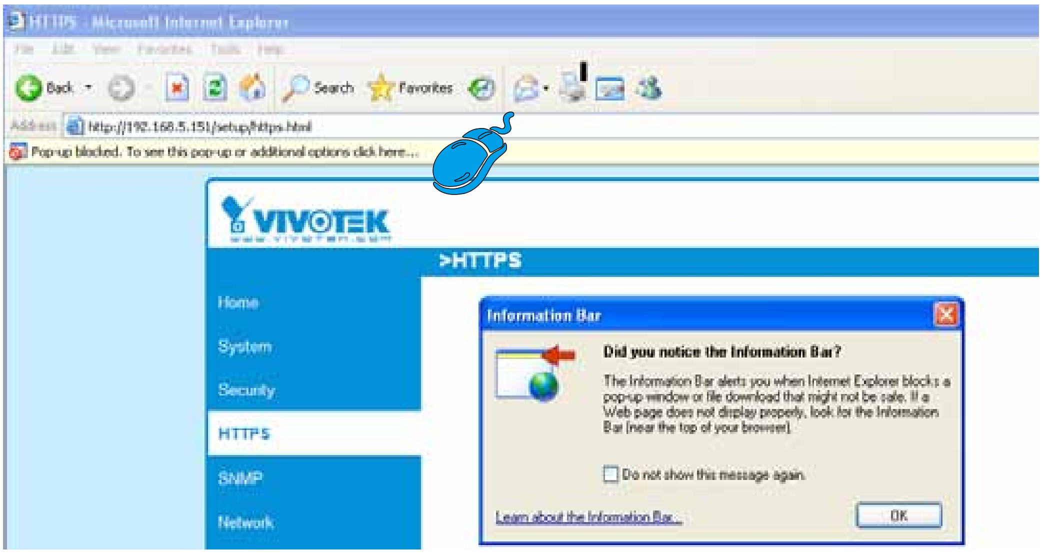


Create Certificate

Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	Vivotek.Inc
Organization Unit:	Vivotek.Inc
Common name:	www.vivotek.com
Validity:	3650 days

Please wait while the certificate is being generated...

3. If you see the following Information bar, click **OK** and click on the Information bar at the top of the page to allow pop-ups.



Address: http://192.168.5.151/setup/https.html

Pop-up blocked. To see this pop-up or additional options click here...

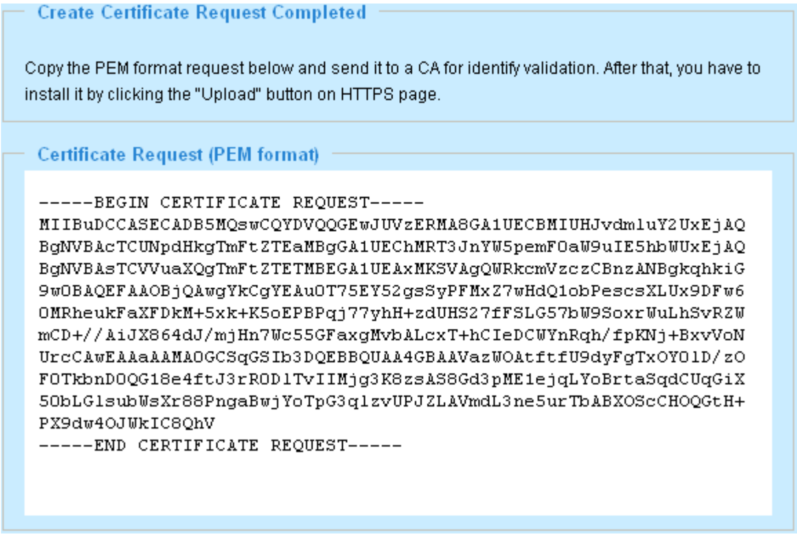
Did you notice the Information Bar?

The Information Bar alerts you when Internet Explorer blocks a pop-up window or file download that might not be safe. If a Web page does not display properly, look for the Information Bar (near the top of your browser).

□ Do not show this message again.

Learn about the Information Bar...

4. The pop-up window shows an example of a certificate request.



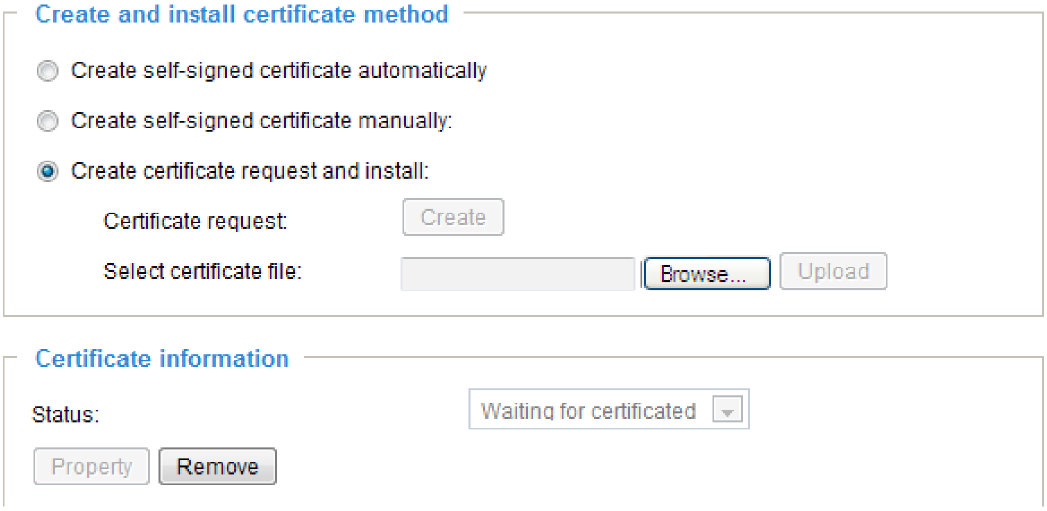
Create Certificate Request Completed

Copy the PEM format request below and send it to a CA for identify validation. After that, you have to install it by clicking the "Upload" button on HTTPS page.

Certificate Request (PEM format)

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBuDCCASECADB5MQswCQYDVQQGEwJUVzERMA8GA1UECBMIUHJvdmluY2UxEjAQ
BgNVBAcTCUNpdHkgTmFtZTEaMBgGA1UEChMRT3JnYW5pemF0aW9uIE5hbWUxEjAQ
BgNVBAsTCVVuaXQgTmFtZTETMBEGA1UEAxMKSVAgQWRkcmVzczCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwgYkCgYEAu0T75EY52gsSyPFMxZ7wHdQ1obPescsXLUx9DFw6
OMRheukFaXFDkM+5xk+K5oEPBPqj77yhH+zdUHS27fFSLG57bW9SoxrWuLhSvRZW
mCD+//AiJX864dJ/mjHn7Wc55GFaxgMvbALcxT+hCIeDCWYnRqh/fpKNj+BxvVoN
UrcCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBAAVazWOAtftfU9dyFgTxOYOlD/zO
FOTkbnDOQG18e4ftJ3rRODlTvIIMjg3K8zsAS8Gd3pME1ejqLYoBrtaSqdCUqGiX
5ObLGlsubWsXr88PngaBwjYoTpG3qlzvUPJZLAVmdL3ne5urTbABXOScCHOQGtH+
PX9dw4OJWkIC8QhV
-----END CERTIFICATE REQUEST-----
```

5. Look for a trusted certificate authority that issues digital certificates. Enroll the video server. Wait for the certificate authority to issue a SSL certificate; click **Browse...** to search for the issued certificate, then click Upload in the second column.



Create and install certificate method

○ Create self-signed certificate automatically

○ Create self-signed certificate manually:

● Create certificate request and install:

Certificate request: Create

Select certificate file: Browse... Upload

Certificate information

Status: Waiting for certificated

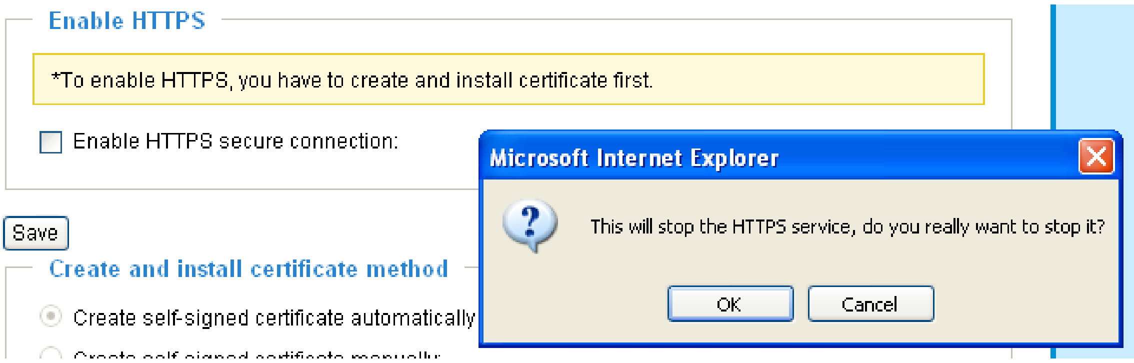
Property Remove

NOTE:

▶ *How do I cancel the HTTPS settings?*

*1. Uncheck **Enable HTTPS secure connection** in the first column and click **Save**; a warning dialog will pop up.*

*2. Click **OK** to disable HTTPS.*



Enable HTTPS

*To enable HTTPS, you have to create and install certificate first.

□ Enable HTTPS secure connection:

Save

Create and install certificate method

○ Create self-signed certificate automatically

○ Create self-signed certificate manually:

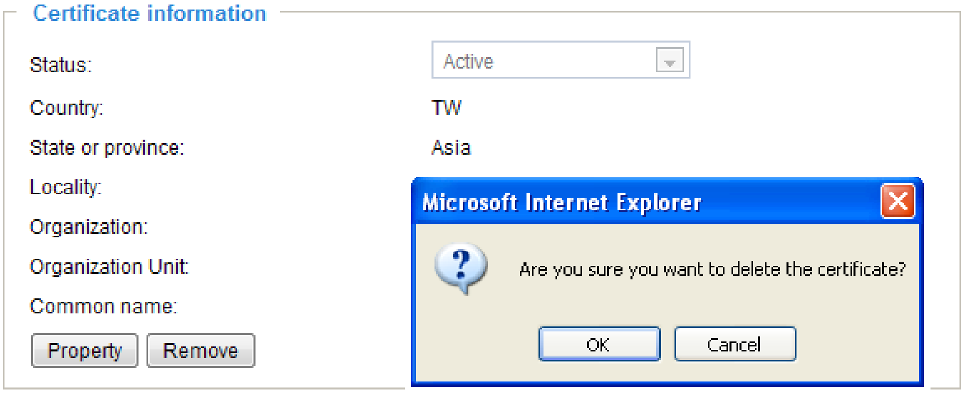
Microsoft Internet Explorer

This will stop the HTTPS service, do you really want to stop it?

OK Cancel

3. The webpage will redirect to a non-HTTPS page automatically.

▶ *If you want to create and install other certificates, please remove the existing one. To remove the signed certificate, uncheck **Enable HTTPS secure connection** in the first column and click **Save**. Then click **Remove** to erase the certificate.*



Certificate information

Status: Active

Country: TW

State or province: Asia

Locality:

Organization:

Organization Unit:

Common name:

Property Remove

Microsoft Internet Explorer

Are you sure you want to delete the certificate?

OK Cancel

SNMP (Simple Network Management Protocol) Advanced Mode

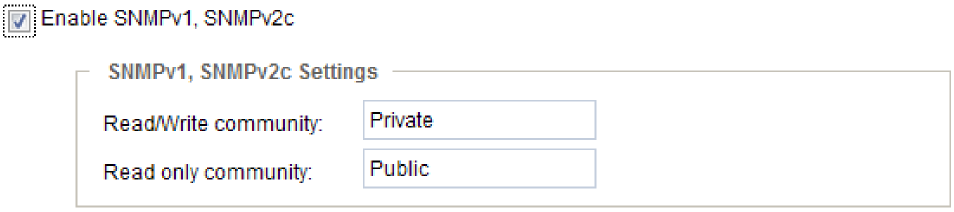
This section explains how to use the SNMP on the video server. The Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices. It helps network administrators to remotely manage network devices and find, solve network problems with ease.

■ The SNMP consists of the following three key components:
1. Manager: Network-management station (NMS), a server which executes applications that monitor and control managed devices.
2. Agent: A network-management software module on a managed device which transfers the status of managed devices to the NMS.
3. Managed device: A network node on a managed network. For example: routers, switches, bridges, hubs, computer hosts, printers, IP telephones, video servers, web server, and database.

Before configuring SNMP settings on the this page, please enable your NMS first.

SNMP Configuration

Enable SNMPv1, SNMPv2c
Select this option and enter the names of Read/Write community and Read Only community according to your NMS settings.



☑ Enable SNMPv1, SNMPv2c

SNMPv1, SNMPv2c Settings

Read/Write community:	Private
Read only community:	Public

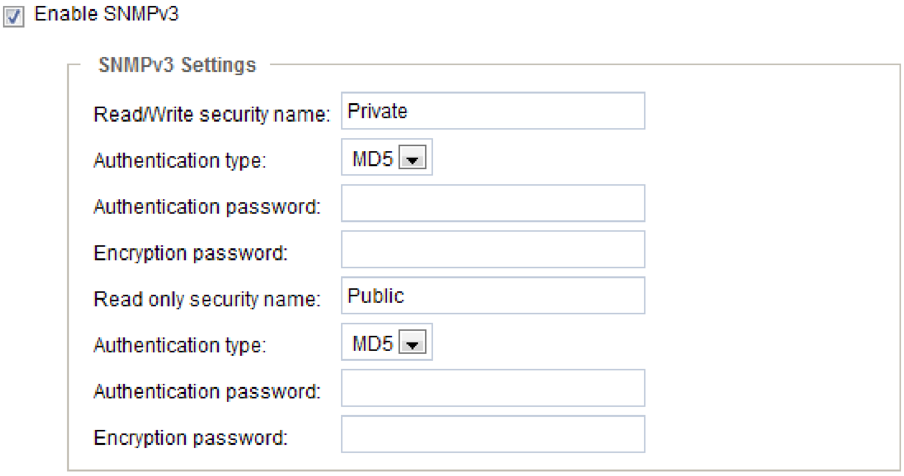
Enable SNMPv3
This option contains cryptographic security, a higher security level, which allows you to set the Authentication password and the Encryption password.

■ Security name: According to your NMS settings, choose Read/Write or Read Only and enter the community name.

■ Authentication type: Select MD5 or SHA as the authentication method.

■ Authentication password: Enter the password for authenrication (at least 8 characters).

■ Encryption password: Enter a password for ecryption (at least 8 characters).



☑ Enable SNMPv3

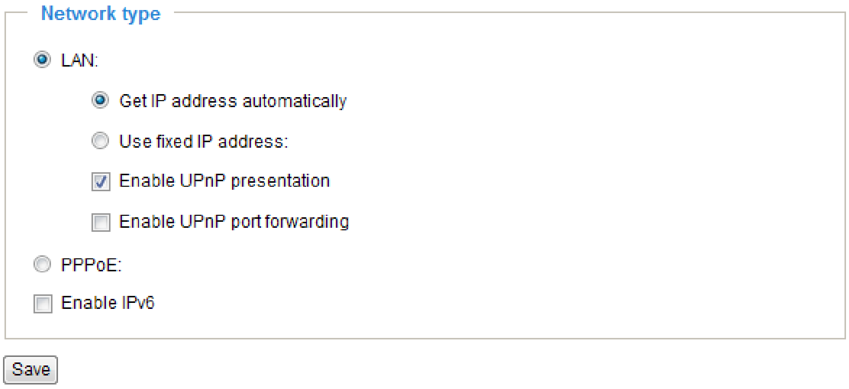
SNMPv3 Settings

Read/Write security name:	Private
Authentication type:	MD5
Authentication password:	
Encryption password:	
Read only security name:	Public
Authentication type:	MD5
Authentication password:	
Encryption password:	

Network

This section explains how to configure a wired network connection for the video server.

Network type



Network type

● LAN:

● Get IP address automatically

○ Use fixed IP address:

☑ Enable UPnP presentation

□ Enable UPnP port forwarding

○ PPPoE:

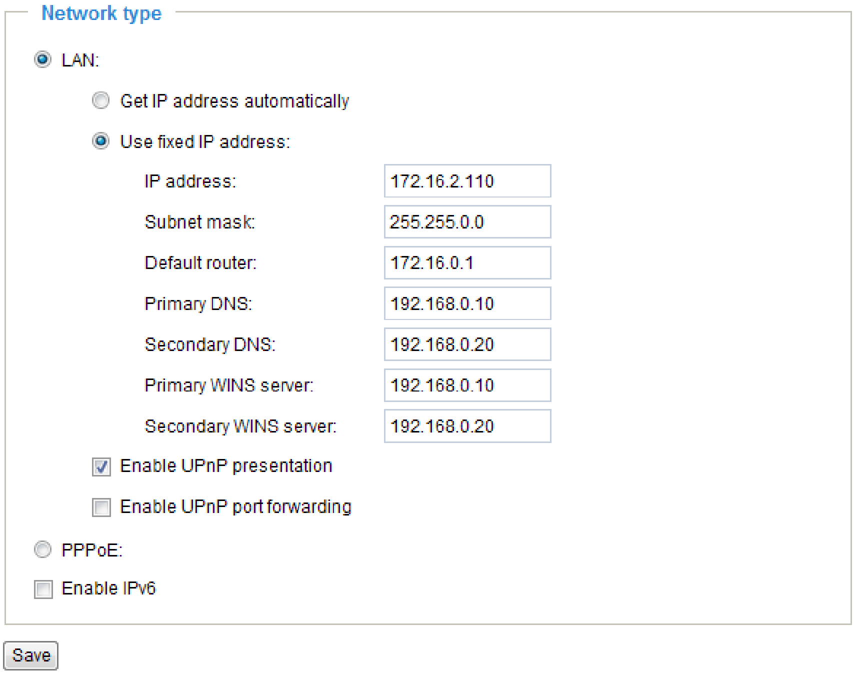
□ Enable IPv6

LAN

Select this option when the video server is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. Rememer to click **Save** when you complete the Network setting.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the video server.



Network type

● LAN:

○ Get IP address automatically

● Use fixed IP address:

IP address:	172.16.2.110
Subnet mask:	255.255.0.0
Default router:	172.16.0.1
Primary DNS:	192.168.0.10
Secondary DNS:	192.168.0.20
Primary WINS server:	192.168.0.10
Secondary WINS server:	192.168.0.20

☑ Enable UPnP presentation

□ Enable UPnP port forwarding

○ PPPoE:

□ Enable IPv6

1. You can make use of VIVOTEK Installation Wizard 2 on the software CD to easily set up the Network Camera on LAN. Please refer to Software Installation on page 12 for details.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP.

Subnet mask: This is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.

Default router: This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will fail the transmission to destinations in different subnet.

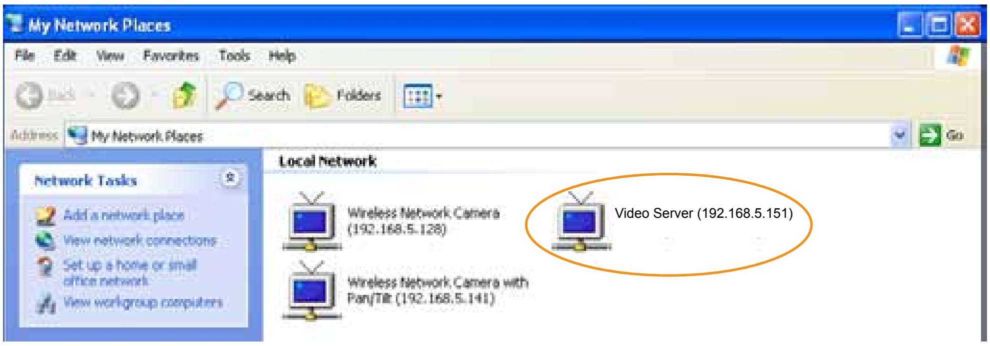
Primary DNS: The primary domain name server that translates hostnames into IP addresses.

Secondary DNS: Secondary domain name server that backups the Primary DNS.

Primary WINS server: The primary WINS server that maintains the database of computer name and IP address.

Secondary WINS server: The secondary WINS server that maintains the database of computer name and IP address.

Enable UPnP presentation: Select this option to enable UPnP^{TM} presentation for your video server so that whenever a video server is presented to the LAN, shortcuts of connected video servers will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnP^{TM} is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP^{TM} component is installed on your computer.


My Network Places
File Edit View Favorites Tools Help
Back
Search
Folders
Address
My Network Places
Go
Network Tasks
Add a network place
View network connections
Set up a home or small office network
View workgroup computers
Local Network
Wireless Network Camera (192.168.5.128)
Video Server (192.168.5.151)
Wireless Network Camera with Pan/Tilt (192.168.5.141)

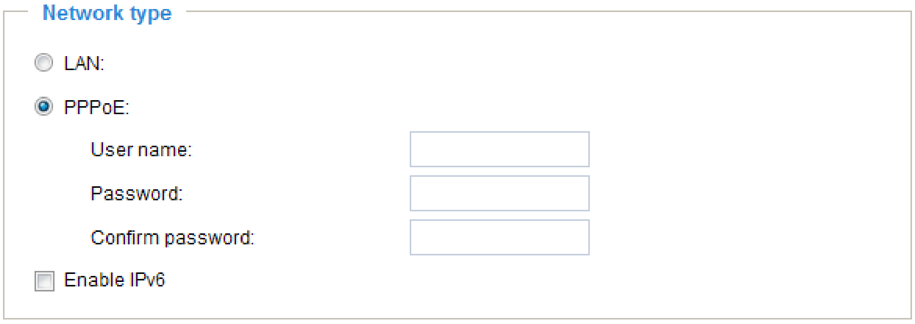
Enable UPnP port forwarding: To access the video server from the Internet, select this option to allow the video server to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP^{TM} and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your video server to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your video server's public IP address.

1. Set up the video server on the LAN.
2. Go to Home > Configuration > Application > Server Settings (please refer to Server settings on page 85) to add a new email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 88). Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > Network Type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.



Network type

○ LAN:

● PPPoE:

User name:

Password:

Confirm password:

□ Enable IPv6

5. The video server will reboot.
6. Disconnect the power to the video server; remove it from the LAN environment.

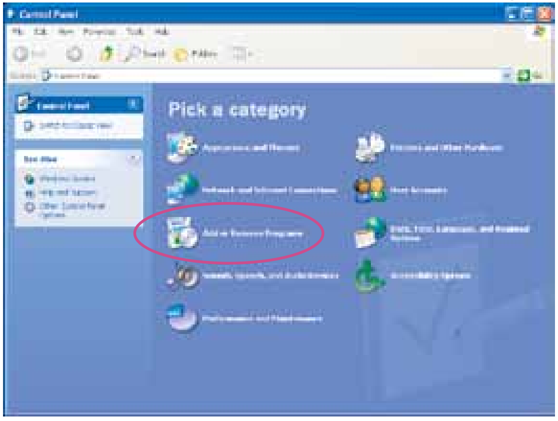
NOTE:

▶ *If the default ports are already used by other devices connected to the same router, the video server will select other ports for the video server.*

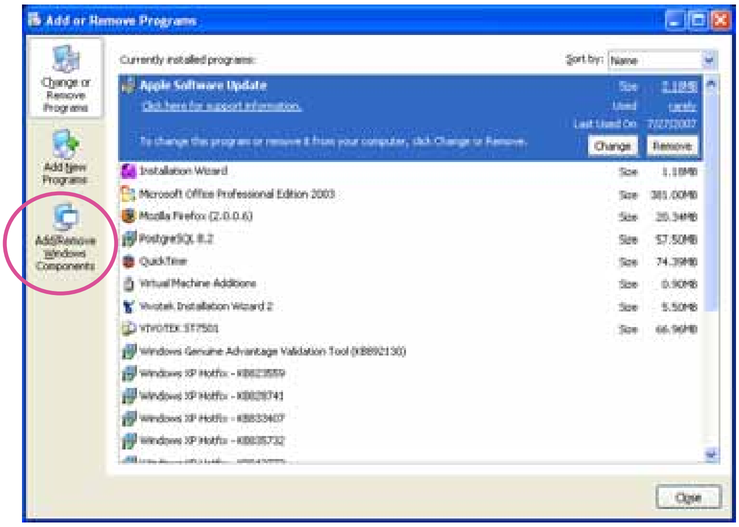
▶ *If UPnP^{TM} is not supported by your router, you will see the following message:*
Error: Router does not support UPnP port forwarding.

▶ *Steps to enable the UPnP^{TM} user interface on your computer:*
Note that you must log on to the computer as a system administrator to install the UPnP^{TM} components.

*1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.*



*2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.*

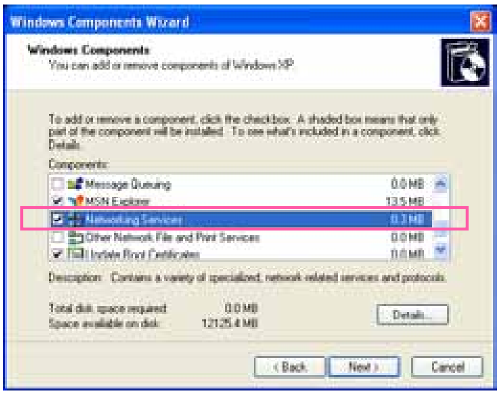


Currently installed programs:

Apple Software Update — Size 1.18MB, Used rarely, Last Used On 7/27/2007
Click here for support information.
To change this program or remove it from your computer, click Change or Remove.

Installation Wizard	Size 1.18MB
Microsoft Office Professional Edition 2003	Size 381.00MB
Mozilla Firefox (2.0.0.6)	Size 25.34MB
PostgreSQL 8.2	Size 57.50MB
QuickTime	Size 74.39MB
Virtual Machine Additions	Size 0.90MB
Vivotek Installation Wizard 2	Size 5.50MB
VIVOTEK ST7501	Size 66.96MB
Windows Genuine Advantage Validation Tool (KB892130)	
Windows XP Hotfix - KB823559	
Windows XP Hotfix - KB828741	
Windows XP Hotfix - KB833407	
Windows XP Hotfix - KB835732	

*3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.*



Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

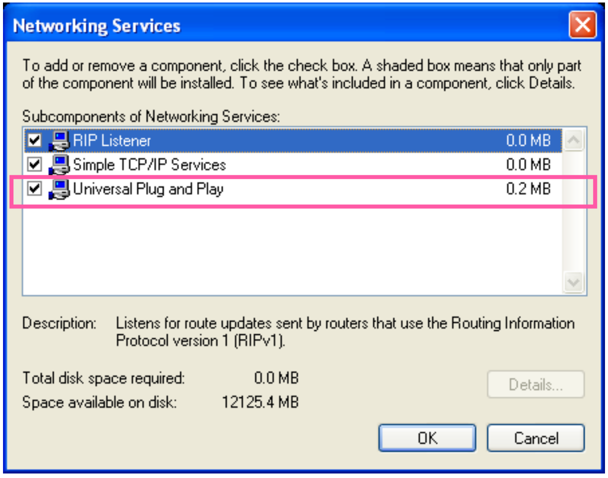
Components:

□ Message Queuing	0.0 MB
☑ MSN Explorer	13.5 MB
☑ Networking Services	0.3 MB
□ Other Network File and Print Services	0.0 MB
☑ Update Root Certificates	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB
Space available on disk: 12125.4 MB

4. In the Networking Services dialog box, select ***Universal Plug and Play*** *and click* ***OK****.*



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

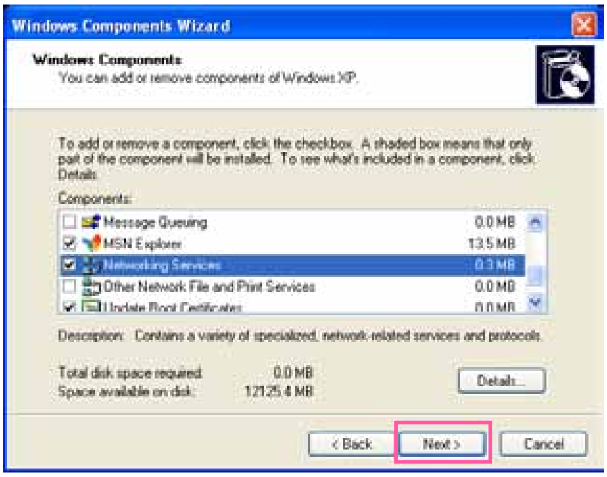
☑	RIP Listener	0.0 MB
☑	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Listens for route updates sent by routers that use the Routing Information Protocol version 1 (RIPv1).

Total disk space required: 0.0 MB

Space available on disk: 12125.4 MB

5. Click ***Next*** *in the following window.*



Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

□	Message Queuing	0.0 MB
☑	MSN Explorer	13.5 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB
☑	Update Root Certificates	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 12125.4 MB

6. Click ***Finish****. UPnP^{TM} is enabled.*

▶ *How does UPnP^{TM} work?*
UPnP^{TM} networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of video servers, you will see video server shortcuts under My Network Places.

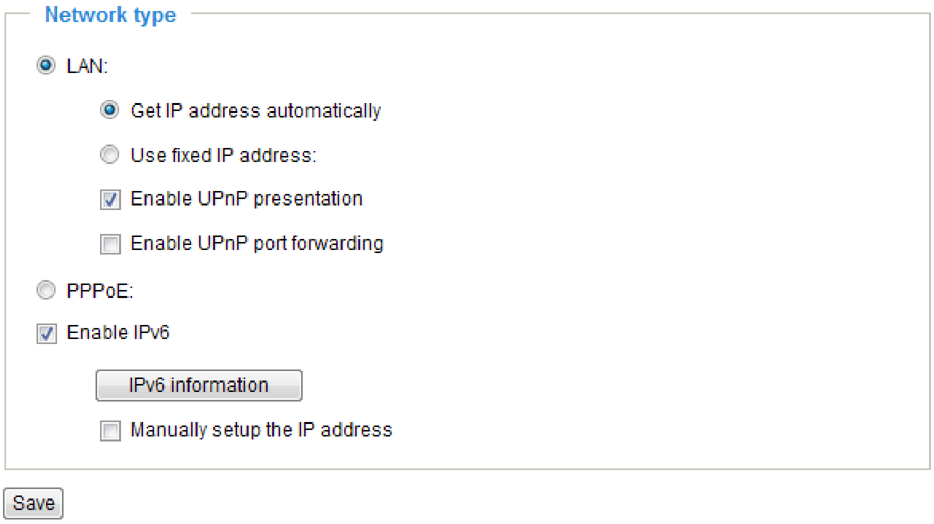
▶ *Enabling UPnP port forwarding allows the video server to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the video server's public address in order to access the video server from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the video server's IP address.*

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

▶ *If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the video server to factory default; please refer to Restore on page 101 for details. After the video server is reset to factory default, it will be accessible on the LAN.*

Enable IPv6

Select this option and click **Save** to enable IPv6 settings.
Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.



Network type

● LAN:

● Get IP address automatically

○ Use fixed IP address:

☑ Enable UPnP presentation

□ Enable UPnP port forwarding

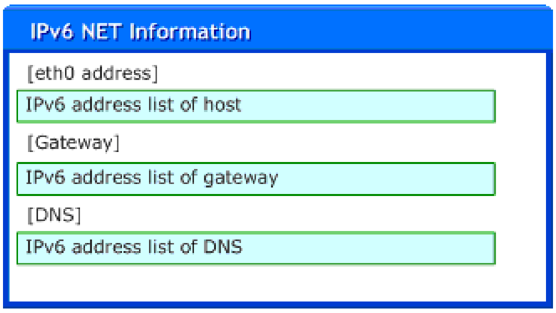
○ PPPoE:

☑ Enable IPv6

□ Manually setup the IP address

When IPv6 is enabled, by default, the video server will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

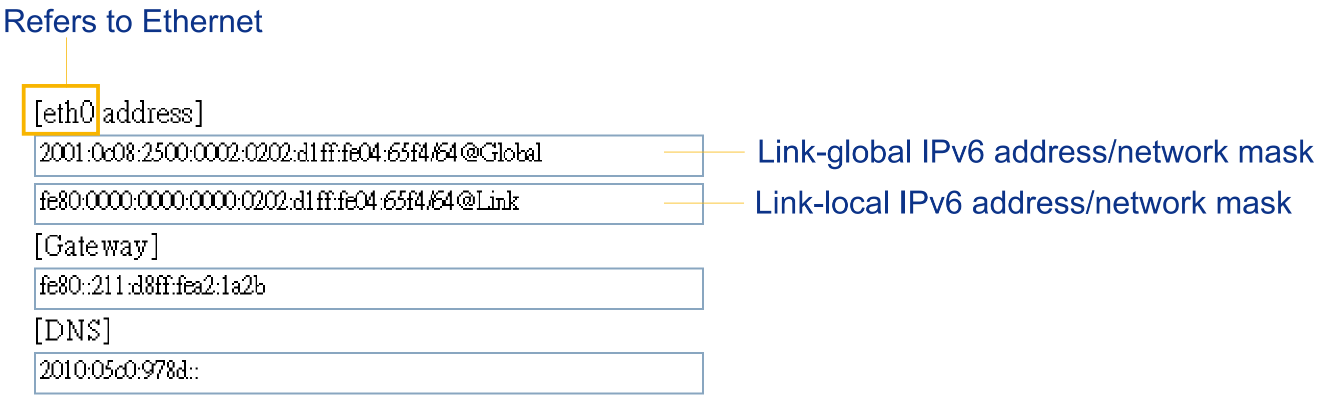
IPv6 Information: Click this button to obtain the IPv6 information as shown below.



IPv6 NET Information

[eth0 address]
IPv6 address list of host
[Gateway]
IPv6 address list of gateway
[DNS]
IPv6 address list of DNS

If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window. The IPv6 address will be displayed as follows:



Refers to Ethernet

[eth0 address]
2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global
fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link
[Gateway]
fe80::211:d8ff:fea2:1a2b
[DNS]
2010:05c0:978d::

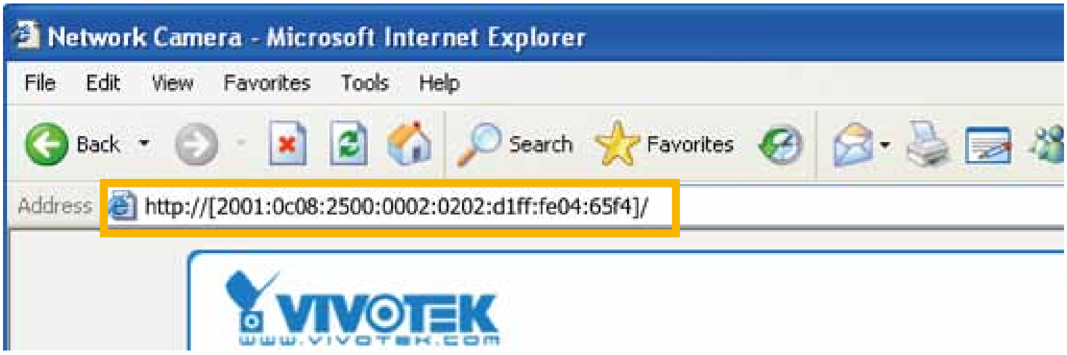
Link-global IPv6 address/network mask

Link-local IPv6 address/network mask

Please follow the steps below to link to an IPv6 address:
1. Open your web browser.
2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
3. The format should be:

http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/
↑
IPv6 address

4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.
For example:



Network Camera - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address

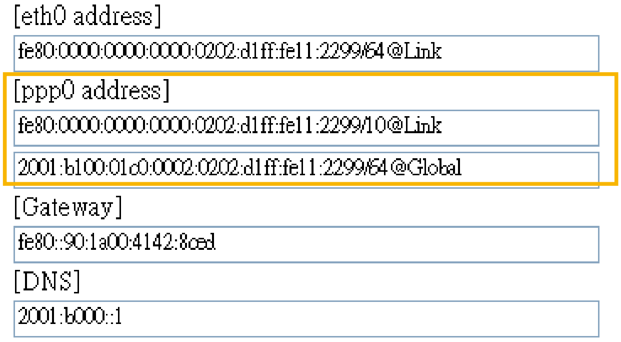
http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/

NOTE:

► *If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to* ***HTTP*** *on page 46 for detailed information.)*

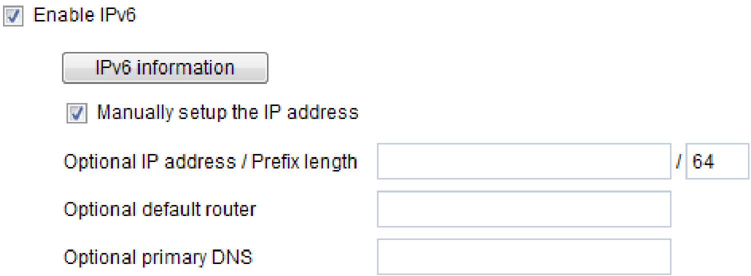
http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/:8080
↑ IPv6 address ↑ Secondary HTTP port

► *If you choose PPPoE as the Network Type, the [PPP0 address] will be displayed in the IPv6 information column as shown below.*



[eth0 address]
fe80:0000:0000:0000:0202:d1ff:fe11:2299/64@Link
[ppp0 address]
fe80:0000:0000:0000:0202:d1ff:fe11:2299/10@Link
2001:b100:01c0:0002:0202:d1ff:fe11:2299/64@Global
[Gateway]
fe80::90:1a00:4142:8ced
[DNS]
2001:b000::1

Manually setup the IP address: Select this option to manually set up IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers.
If you check this item, the following blanks will be displayed for you to enter the corresponding information:



☑ Enable IPv6

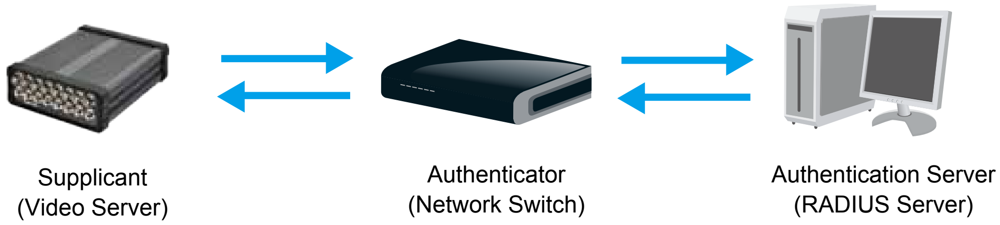
☑ Manually setup the IP address
Optional IP address / Prefix length ___ / 64
Optional default router ___
Optional primary DNS ___

IEEE 802.1x Advanced Mode

Enable this function if your network environment uses IEEE 802.1x, which is a port-based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x settings.

The 802.1x standard is designed to enhance the security of local area networks, which provides authentication to network devices (clients) attached to a network port (wired or wireless). If all certificates between client and server are verified, a point-to-point connection will be enabled; if authentication fails, access on that port will be prohibited. 802.1x utilizes an existing protocol, the Extensible Authentication Protocol (EAP), to facilitate communication.

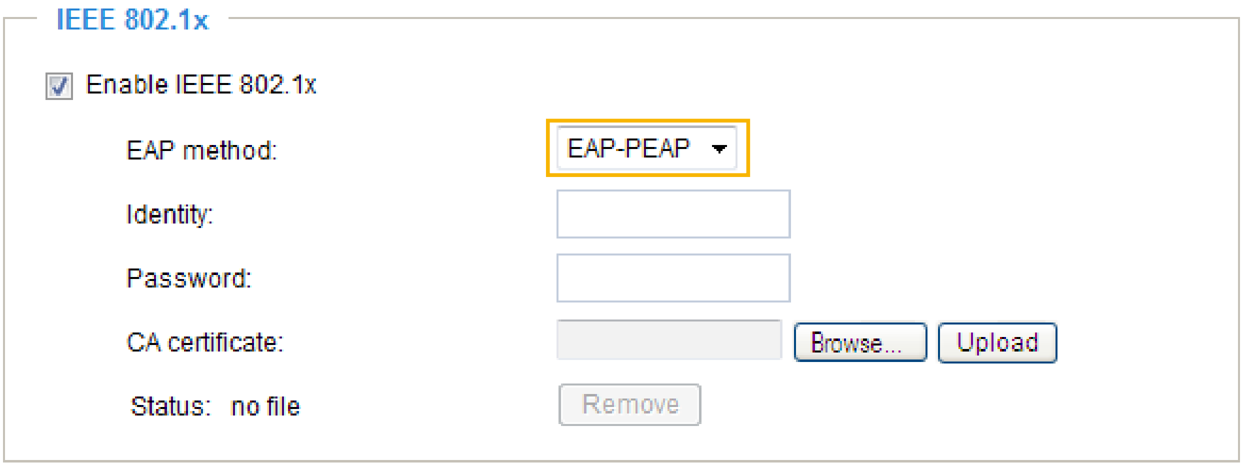
■ The components of a protected network with 802.1x authentication:



1. Supplicant: A client end user (video server), which requests authentication.
2. Authenticator (an access point or a switch): A "go between" which restricts unauthorized end users from communicating with the authentication server.
3. Authentication server (usually a RADIUS server): Checks the client certificate and decides whether to accept the end user's access request.

■ VIVOTEK video servers support two types of EAP methods to perform authentication: **EAP-PEAP** and **EAP-TLS**.

Please follow the steps below to enable 802.1x settings:
1. Before connecting the video server to the protected network with 802.1x, please apply a digital certificate from a Certificate Authority (ie. MIS of your company) which can be validated by a RADIUS server.
2. Connect the video server to a PC or notebook outside of the protected LAN. Open the configuration page of the video server as shown below. Select **EAP-PEAP** or **EAP-TLS** as the EAP method. In the following blanks, enter your ID and password issued by the CA, then upload related certificate(s).



IEEE 802.1x

☑ Enable IEEE 802.1x

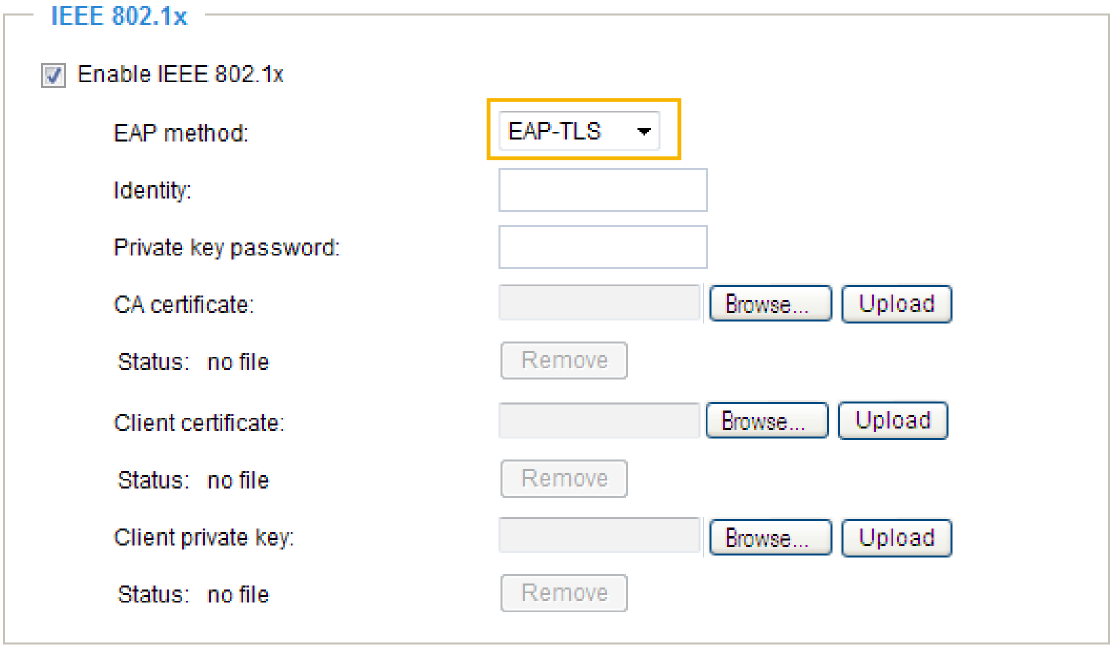
EAP method: EAP-PEAP

Identity:

Password:

CA certificate:

Status: no file



IEEE 802.1x

☑ Enable IEEE 802.1x

EAP method: EAP-TLS

Identity:

Private key password:

CA certificate:

Status: no file

Client certificate:

Status: no file

Client private key:

Status: no file

3. When all settings are complete, move the video server to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

NOTE:

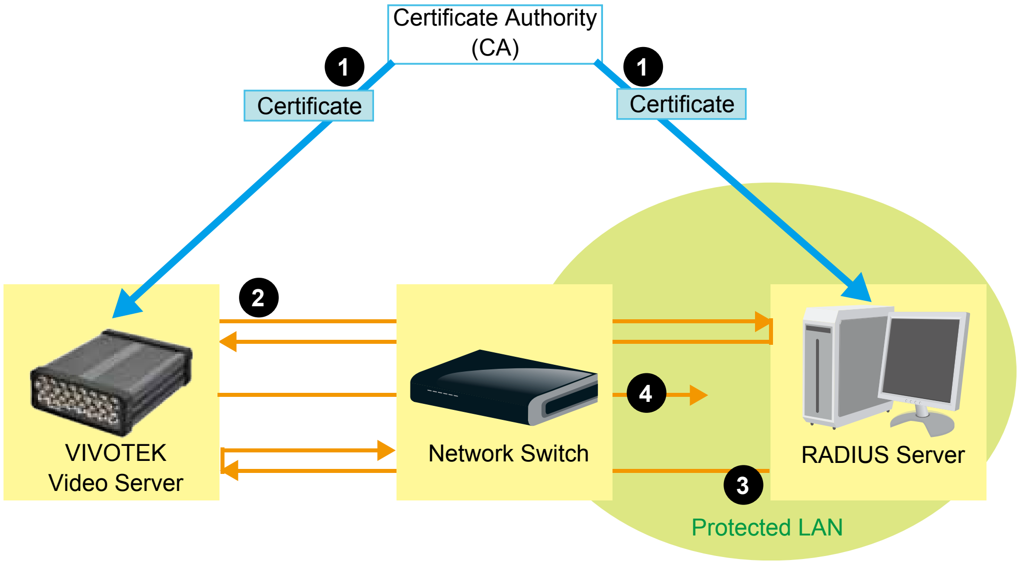
► *The authentication process for 802.1x:*

1. The Certificate Authority (CA) provides the required signed certificates to the video server (the supplicant) and the RADIUS Server (the authentication server).

2. A video server requests access to the protected LAN using 802.1X via a switch (the authenticator). The client offers its identity and client certificate, which is then forwarded by the switch to the RADIUS Server, which uses an algorithm to authenticate the video server and returns an acceptance or rejection back to the switch.

3. The switch also forwards the RADIUS Server's certificate to the video server.

4. Assuming all certificates are validated, the switch then changes the video server's state to authorized and is allowed access to the protected network via a pre-configured port.



QoS (Quality of Service) Advanced Mode

Quality of Service refers to a resource reservation control mechanism, which guarantees a certain quality to different services on the network. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. Quality can be defined as, for instance, a maintained level of bit rate, low latency, no packet dropping, etc.

The following are the main benefits of a QoS-aware network:

- The ability to prioritize traffic and guarantee a certain level of performance to the data flow.
- The ability to control the amount of bandwidth each application may use, and thus provide higher reliability and stability on the network.

Requirements for QoS

To utilize QoS in a network environment, the following requirements must be met:

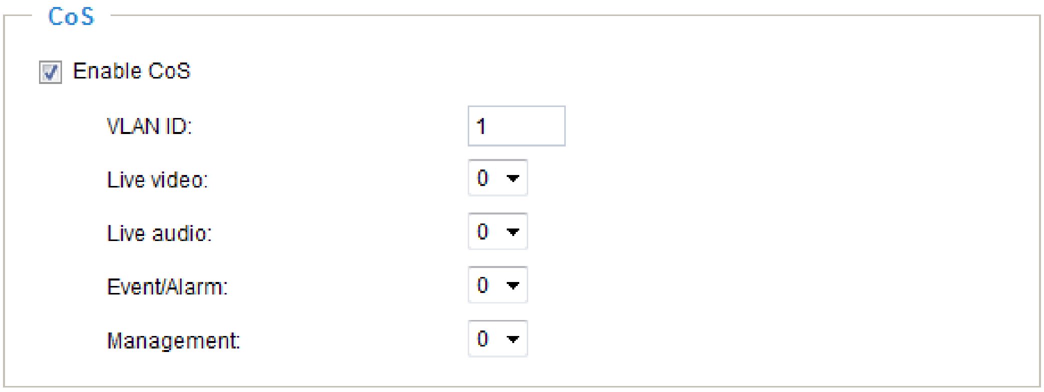
- All network switches and routers in the network must include support for QoS.
- The network video devices used in the network must be QoS-enabled.

QoS models

CoS (the VLAN 802.1p model)

IEEE802.1p defines a QoS model at OSI Layer 2 (Data Link Layer), which is called CoS, Class of Service. It adds a 3-bit value to the VLAN MAC header, which indicates prioritization from 0~7 (Eight different classes of service are available). The priority is set up on the network switches, which then use different queuing disciplines to forward the packets.

Below is the setting column for CoS. Enter the **VLAN ID** of your switch (0~4095) and choose the priority for each application (0~7).



CoS

☑ Enable CoS

VLAN ID: 1

Live video: 0

Live audio: 0

Event/Alarm: 0

Management: 0

If you assign Video the highest level, the switch will handle video packets first.

NOTE:

► *The web browsing may fail if the CoS setting is incorrect.*

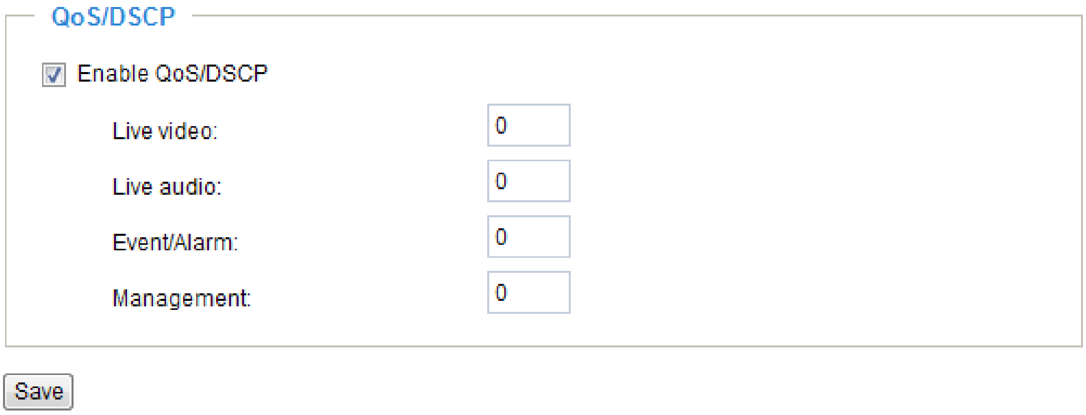
► *Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.*

► *Although CoS is simple to manage, it lacks scalability and does not offer end-to-end quarantees since it is based on L2 protocol.*

QoS/DSCP (the DiffServ model)

DSCP-ECN defines QoS at Layer 3 (Network Layer). The Differentiated Services (DiffServ) model is based on packet marking and router queuing disciplines. The marking is done by adding a field to the IP header, called the DSCP (Differentiated Services Codepoint). This is a 6-bit field that provides 64 different class IDs. It gives an indication of how a given packet is to be forwarded, known as the Per Hop Behavior (PHB). The PHB describes a particular service level in terms of bandwidth, queueing theory, and dropping (discarding the packet) decisions. Routers at each network node classify packets according to their DSCP value and give them a particular forwarding treatment; for example, how much bandwidth to reserve for it.

Below are the setting options of DSCP (DiffServ Codepoint). Specify the DSCP value for each application (0~63).



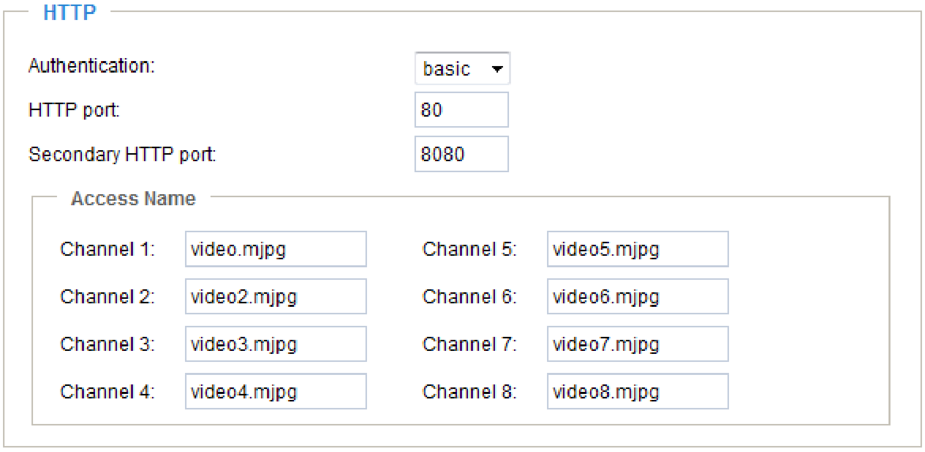
QoS/DSCP

☑ Enable QoS/DSCP

Live video:	0
Live audio:	0
Event/Alarm:	0
Management:	0

HTTP Advanced Mode

To utilize HTTP authentication, make sure that your have set a password for the video server first; please refer to Security on page 28 for details.



HTTP

Authentication: basic

HTTP port: 80

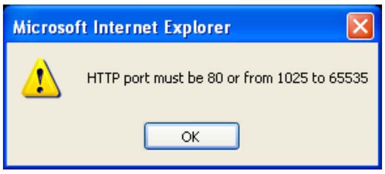
Secondary HTTP port: 8080

Access Name

Channel 1:	video.mjpg	Channel 5:	video5.mjpg
Channel 2:	video2.mjpg	Channel 6:	video6.mjpg
Channel 3:	video3.mjpg	Channel 7:	video7.mjpg
Channel 4:	video4.mjpg	Channel 8:	video8.mjpg

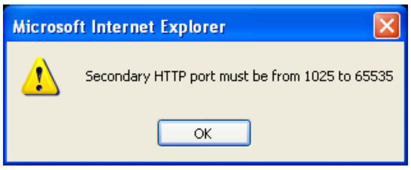
Authentication: Depending on your network security requirements, the video server provides two types of security settings for an HTTP transaction: basic and digest.
If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. They can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages will be displayed:



Microsoft Internet Explorer

HTTP port must be 80 or from 1025 to 65535



Microsoft Internet Explorer

Secondary HTTP port must be from 1025 to 65535

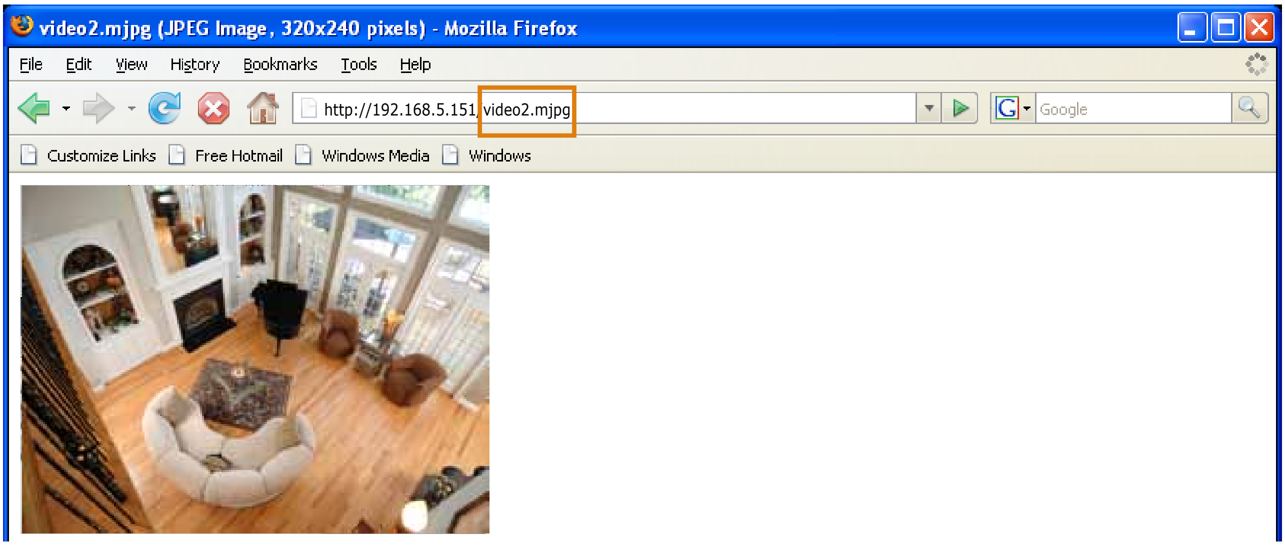
To access the video server on the LAN, both the HTTP port and secondary HTTP port can be used to access the video server. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the video server's IP address.

on a LAN
http://192.168.4.160 or http://192.168.4.160:8080

Access name for channel 1~4/8: VS8401 supports 4 channels for video live viewing, as VS8801 supports 8 channels. Each channel allows you to view only one stream. The access name is used to differentiate the streaming source. Users can go to **Configuration > Audio and video > Video settings** to set up the video quality of linked streams.

When using Mozilla Firefox or Netscape to access the video server and the video mode is set to JPEG, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the video server to feed live pictures to Mozilla Firefox and Netscape.

URL command -- http://<ip address>:<http port>/<access name for channel 1 ~ 4/8>
For example, when the Access name for stream 2 is set to video2.mjpg:
1. Launch Mozilla Firefox or Netscape.
2. Type the above URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.



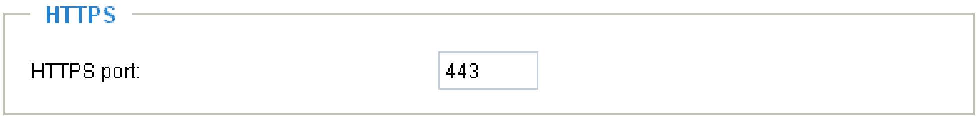
video2.mjpg (JPEG Image, 320x240 pixels) - Mozilla Firefox

http://192.168.5.151/video2.mjpg

NOTE:

▶ *Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for channel 1 ~ 4/8> will fail to access the video server.*

HTTPS

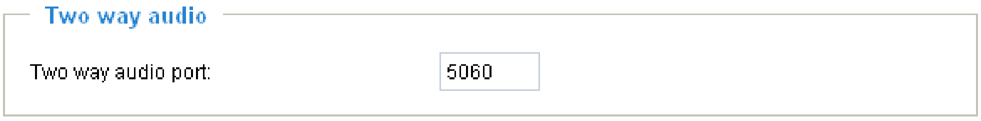


HTTPS

HTTPS port: 443

By default, the HTTPS port is set to 443. It can also be assigned to another port number between 1025 and 65535.

Two way audio



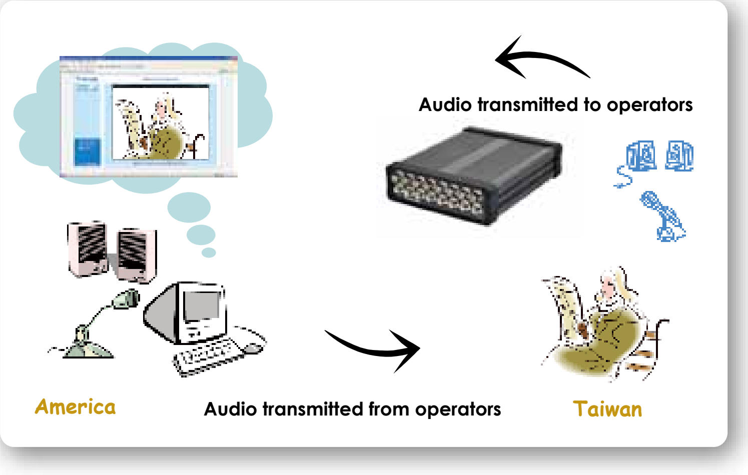
Two way audio

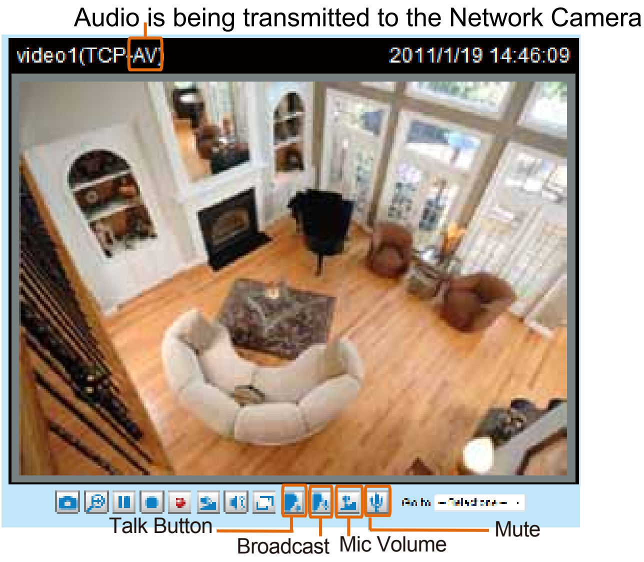
Two way audio port: 5060

By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number between 1025 and 65535.

The video server supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the video server's built-in or external microphone and an external speaker, you can communicate with people around the video server.

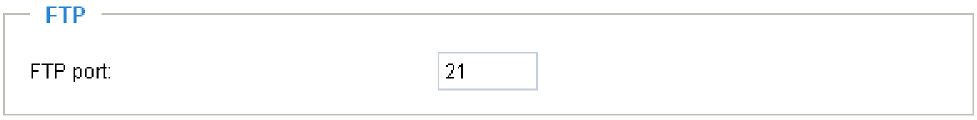
Note that as JPEG only transmits a series of JPEG images to the client, to enable the two-way audio function, make sure the video mode is set to “MPEG-4” on the Audio and Video Settings page and the media option is set to “Video and Audio” on the Client Settings page. Please refer to Client settings on page 22 and Audio and video settings on page 56.


Audio transmitted to operators
America
Audio transmitted from operators
Taiwan



Click to enable audio transmission to the video server; click to broadcast; click to adjust the volume of microphone; click to turn off the audio. To stop talking, click again.

FTP



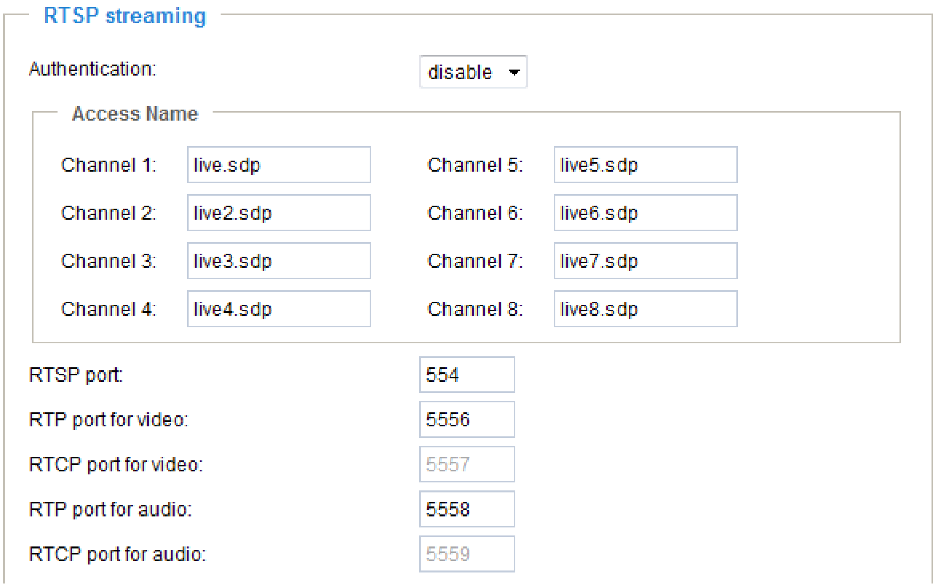
FTP

FTP port: 21

The FTP server allows the user to save recorded video clips. You can utilize VIVOTEK's Installation Wizard 2 to upgrade the firmware via FTP server. By default, the FTP port is set to 21. It also can be assigned to another port number between 1025 and 65535.

RTSP streaming

To utilize RTSP streaming authentication, make sure that you have set a password for the video server first; please refer to Security on page 28 for details.



RTSP streaming

Authentication: disable

Access Name

Channel 1:	live.sdp	Channel 5:	live5.sdp
Channel 2:	live2.sdp	Channel 6:	live6.sdp
Channel 3:	live3.sdp	Channel 7:	live7.sdp
Channel 4:	live4.sdp	Channel 8:	live8.sdp

RTSP port: 554

RTP port for video: 5556

RTCP port for video: 5557

RTP port for audio: 5558

RTCP port for audio: 5559

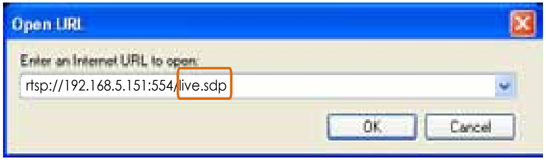
Authentication: Depending on your network security requirements, the video server provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest.
If **basic** authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.
The availability of the RTSP streaming for the three authentication modes is listed in the following table:

	Quick Time player	Real Player
Disable	O	O
Basic	O	O
Digest	O	X

Access name for channel 1 ~4/8: VS8401 supports 4 channels for video live viewing, as VS8801 supports 8 channels. Each channel allows you to view only one stream. The access name is used to differentiate the streaming source.

If you want to use an RTSP player to access the video server, you have to set the video mode to MPEG-4 and use the following RTSP URL command to request transmission of the streaming data.
rtsp://<ip address>:<rtsp port>/<access name for stream1 ~ channel 1 ~4/8>
For example, when the access name for stream 1 is set to live.sdp:

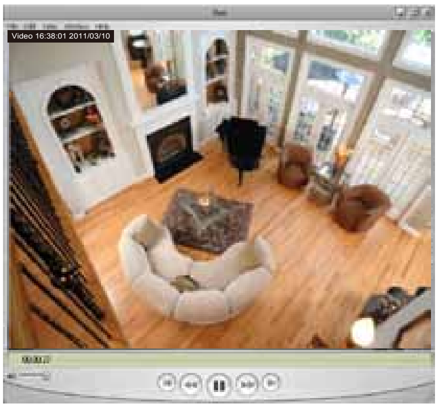
1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the above URL command in the text box.
4. The live video will be displayed in your player as shown below.



Open URL

Enter an Internet URL to open:

rtsp://192.168.5.151:554/live.sdp



RTSP port /RTP port for video, audio/ RTCP port for video, audio

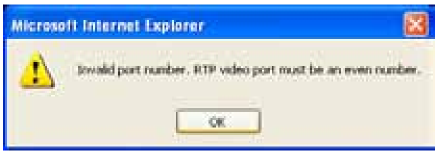
- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

- The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.

- The RTCP (Real-time Transport Control Protocol) allows the video server to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

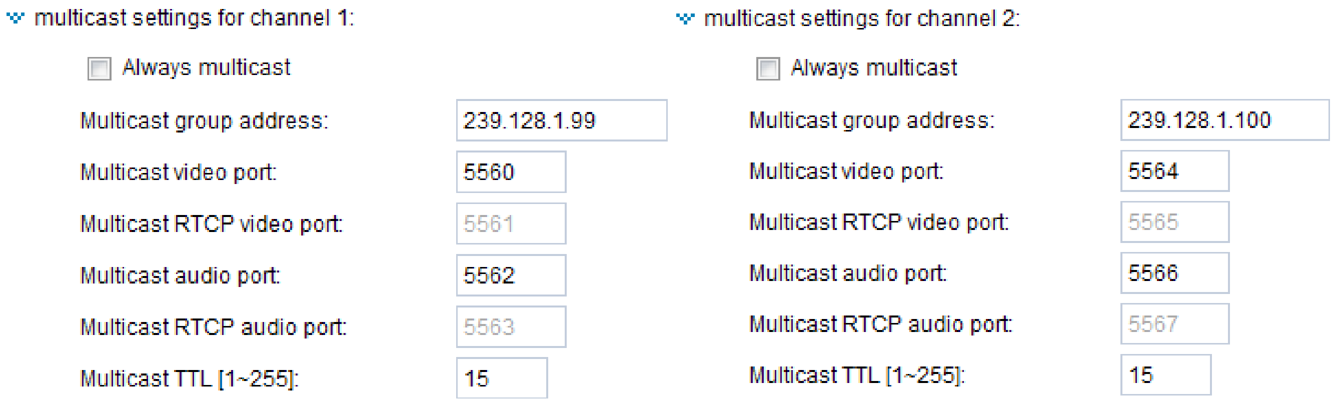
The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always an odd number. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message will be displayed:



Invalid port number. RTP video port must be an even number.

Multicast settings channel 1 ~4/8: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for channel 1~4/8.



multicast settings for channel 1:

□ Always multicast

Multicast group address:	239.128.1.99
Multicast video port:	5560
Multicast RTCP video port:	5561
Multicast audio port:	5562
Multicast RTCP audio port:	5563
Multicast TTL [1~255]:	15

multicast settings for channel 2:

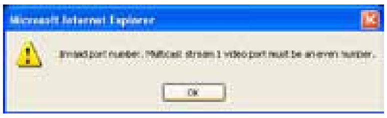
□ Always multicast

Multicast group address:	239.128.1.100
Multicast video port:	5564
Multicast RTCP video port:	5565
Multicast audio port:	5566
Multicast RTCP audio port:	5567
Multicast TTL [1~255]:	15

Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save Internet bandwith.

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus is always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:



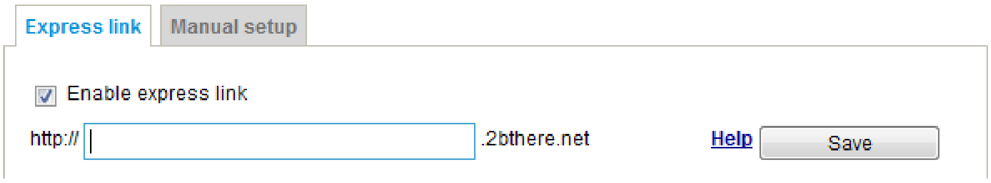
Invalid port number. Multicast stream 1 video port must be an even number.

Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

Express link

Express link is a free service provided by VIVOTEK server, which allows users to register an domain name for a network device. One URL can only be mapped to one Mac address. This service will check out if the host name is valid and automatically open a port on your router. Unlike DDNS, the user has to manually check out UPnP port forwarding, Express link is more convenient and easy to set up.

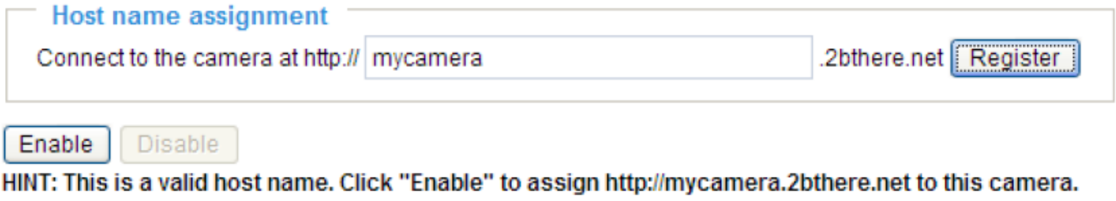
Host name assignment



☑ Enable express link

http:// .2bthere.net

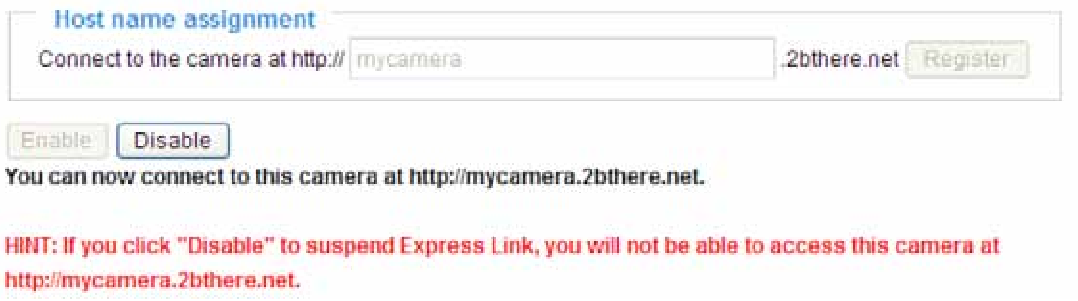
Please follow the steps below to enable Express link:
1. Make sure that your router supports UPnP port forwarding and it is activated.
2. Enter a host name for the network device and click **Register**. If the host name has been used by another device, a warning message will show up. If the host name is valid, it will show an error message.



Connect to the camera at http:// mycamera .2bthere.net

HINT: This is a valid host name. Click "Enable" to assign http://mycamera.2bthere.net to this camera.

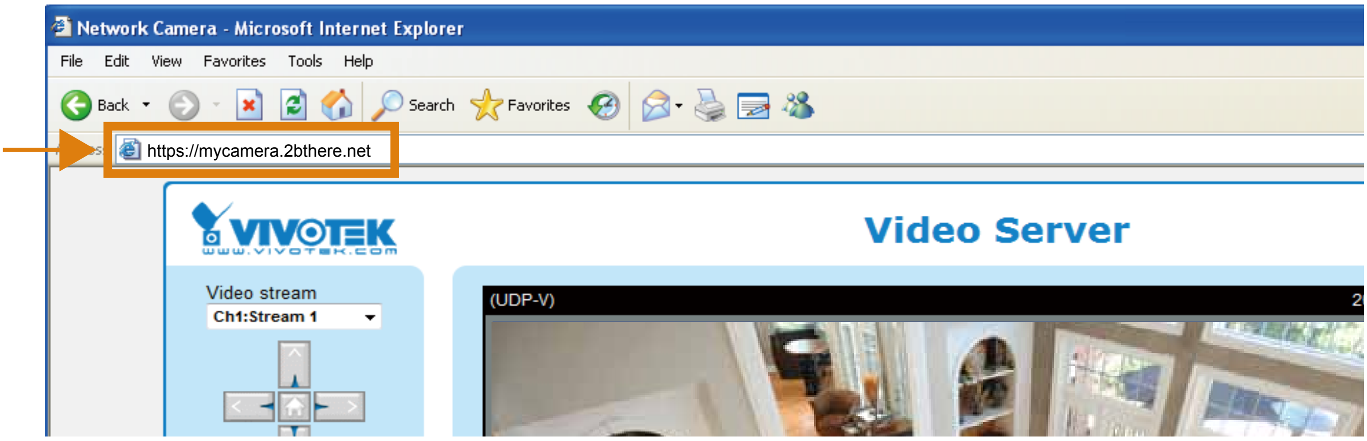
3. Click **Enable** to validate your setting. To access the camera, enter its express link address in a browser's URL field.



Connect to the camera at http:// mycamera .2bthere.net

You can now connect to this camera at http://mycamera.2bthere.net.

HINT: If you click "Disable" to suspend Express Link, you will not be able to access this camera at http://mycamera.2bthere.net.

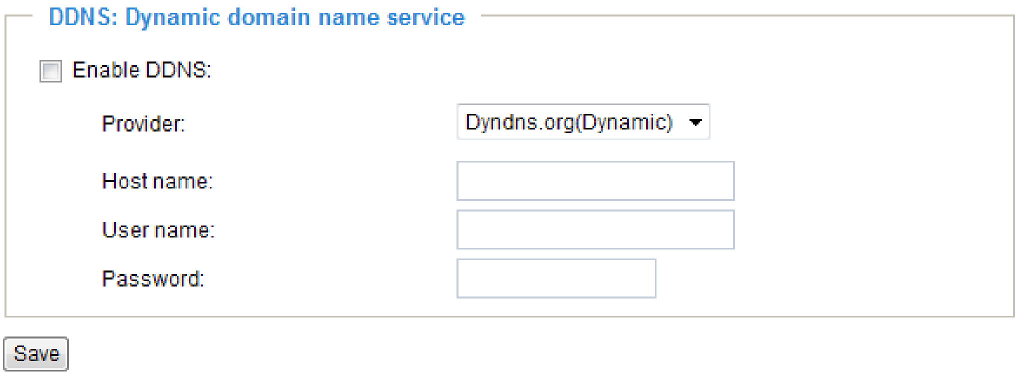


https://mycamera.2bthere.net

DDNS

This section explains how to configure the dynamic domain name service for the video server. DDNS is a service that allows your video server, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

DDNS: Dynamic domain name service



DDNS: Dynamic domain name service

□ Enable DDNS:

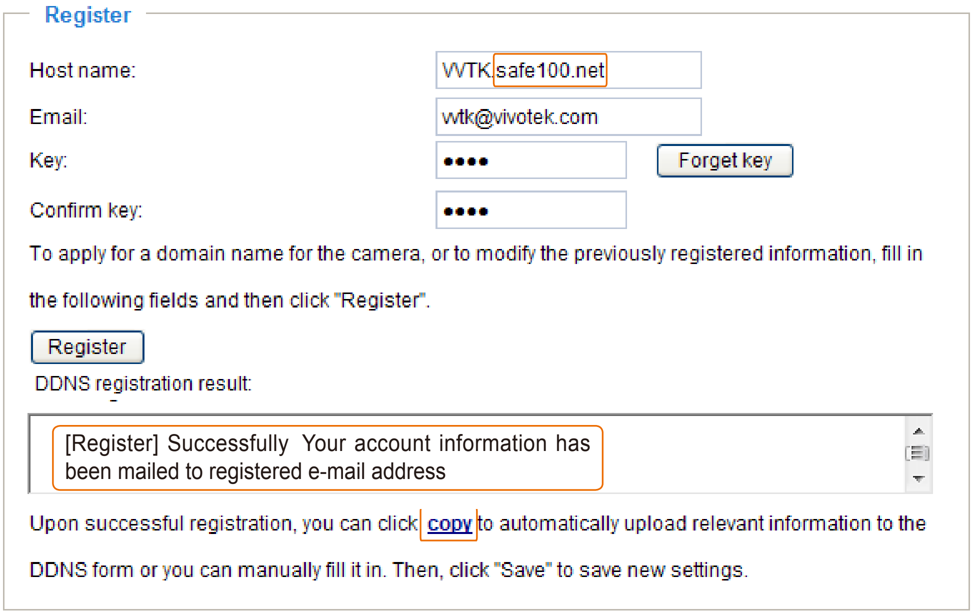
Provider:	Dyndns.org(Dynamic) ▾
Host name:	
User name:	
Password:	

Enable DDNS: Select this option to enable the DDNS setting.

Provider: Select a DDNS provider from the provider drop-down list.
VIVOTEK offers **Safe100.net**, a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's video servers from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it.
Note that before utilizing this function, please apply for a dynamic domain account first.

■ Safe100.net

1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the terms of the Service Agreement.
2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key, and Confirm Key, and click **Register**. After a host name has been successfully created, a success message will be displayed in the DDNS Registration Result column.



Register

Host name:	VVTK.safe100.net
Email:	vvtk@vivotek.com
Key:	●●●● Forget key
Confirm key:	●●●●

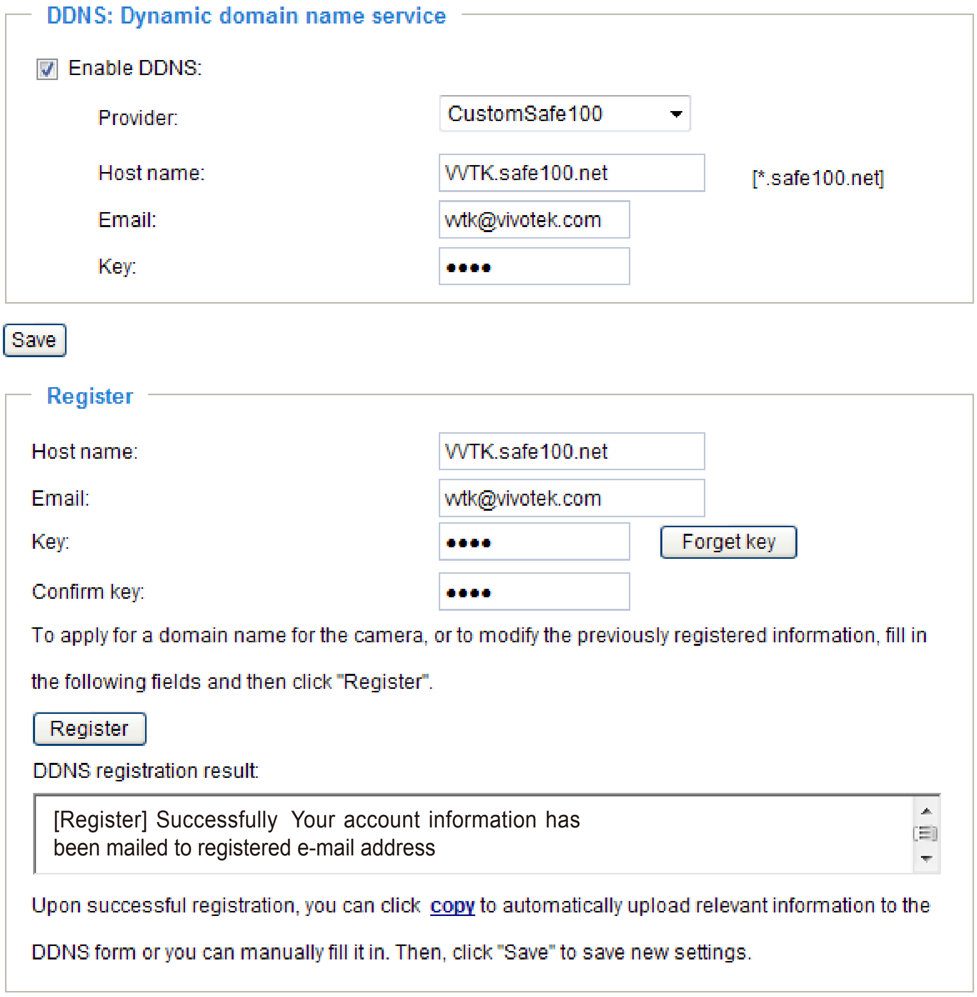
To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".

DDNS registration result:

[Register] Successfully Your account information has been mailed to registered e-mail address

Upon successful registration, you can click copy to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click "Save" to save new settings.

3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields in the DDNS column at the top of the page as seen in the picture.



DDNS: Dynamic domain name service

☑ Enable DDNS:

Provider: CustomSafe100

Host name: VVTK.safe100.net [*.safe100.net]

Email: vvtk@vivotek.com

Key: ●●●●

Save

Register

Host name: VVTK.safe100.net

Email: vvtk@vivotek.com

Key: ●●●● Forget key

Confirm key: ●●●●

To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".

Register

DDNS registration result:

[Register] Successfully Your account information has been mailed to registered e-mail address

Upon successful registration, you can click copy to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click "Save" to save new settings.

4. Select Enable DDNS and click **Save** to enable the setting.

■ CustomSafe100

VIVOTEK offers documents to establish a CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the drop-down list.
2. In the Register column, fill in the Host name, Email, Key, and Confirm Key; then click **Register**. After a host name has been successfully created, you will see a success message in the DDNS Registration Result column.
3. Click **Copy** and all for the registered information will be uploaded to the corresponding fields in the DDNS column.
4. Select Enable DDNS and click **Save** to enable the setting.

Forget key: Click this button if you have forgotten the key to Safe100.net or CustomSafe100. Your account information will be sent to your email address.

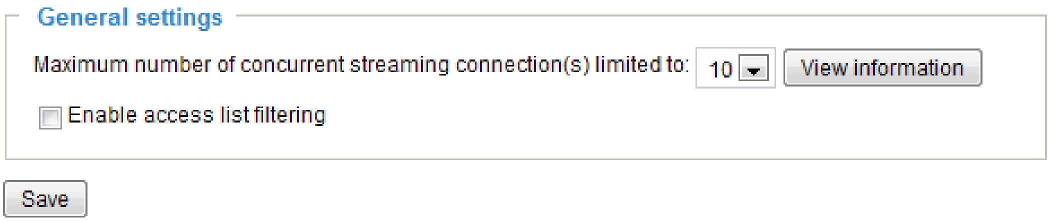
Refer to the following links to apply for a dynamic domain account when selecting other DDNS providers:

■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/
■ TZO.com: visit http://www.tzo.com/
■ DHS.org: visit http://www.dhs.org/
■ dyn-interfree.it: visit http://dyn-interfree.it/

Access list Advanced Mode

This section explains how to control access permission by verifying the client PC's IP address.

General settings



General settings

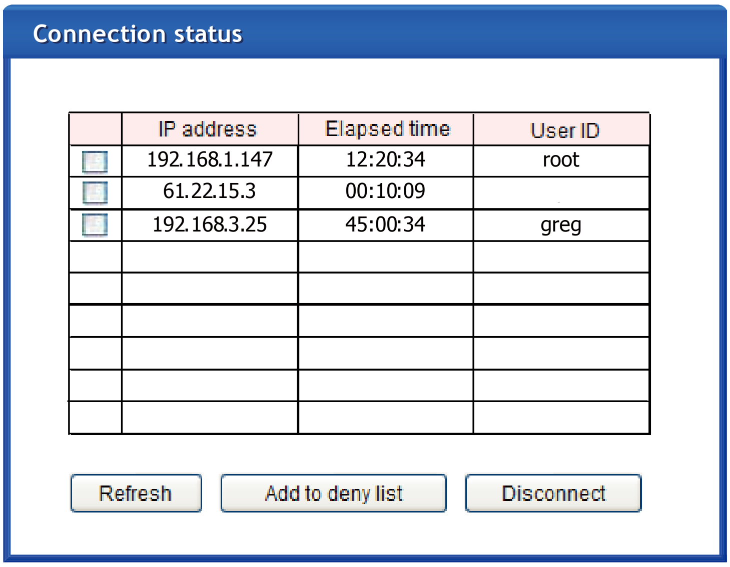
Maximum number of concurrent streaming connection(s) limited to: 10 ▾ View information

□ Enable access list filtering

Save

Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 and stream 2). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (IE Explore or Quick Time Player).

View Information: Click this button to display the connection status window showing a list of the current connections.
For example:



Connection status

	IP address	Elapsed time	User ID
□	192.168.1.147	12:20:34	root
□	61.22.15.3	00:10:09	
□	192.168.3.25	45:00:34	greg

■ IP address: Current connections to the Video server.

■ Elapsed time: How much time the client has been at the webpage.

■ User ID: If the administrator has set a password for the webpage, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to link to the webpage without a user name and password, the User ID column will be empty.

There are some situations which allow clients access to the live video without a user name and password:

1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security on page 28.
2. The administrator has set up a root password, but set **RTSP authentication** to "disable". For more information about **RTSP authentication**, please refer to RTSP Streaming on page 48.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing,** please refer to Security on page 28.

■ Refresh: Click this button to refresh all current connections.

■ Add to deny list: You can select entries from the Connection Status list and add them to the Deny List to deny access. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player). If you want to enable the denied list, please check **Enable access list filtering** and click **Save** in the first column.

■ Disconnect: If you want to break off the current connections, please select them and click this button. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player).

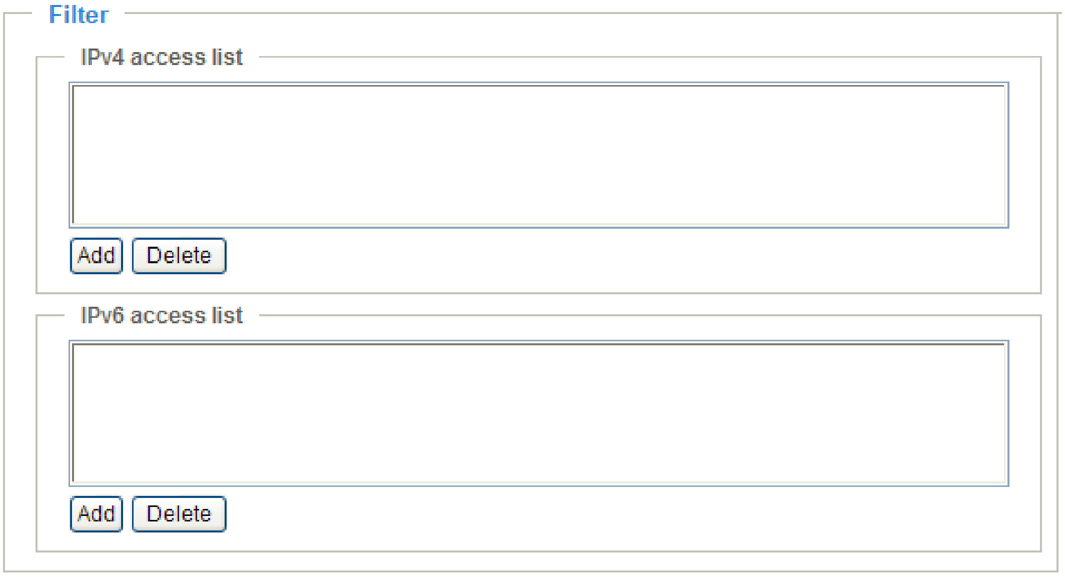
Enable access list filtering: Check this item and click **Save** if you want to enable the access list filtering function.

Filter type

Select **Allow** or **Deny** as the filter type. If you choose **Allow Type**, only those clients whose IP addresses are on the Access List below can access the Network Camera, and the others cannot access. On the contrary, if you choose **Deny Type**, those clients whose IP addresses are on the Access List below will not be allowed to access the Network Camera, and the others can access.

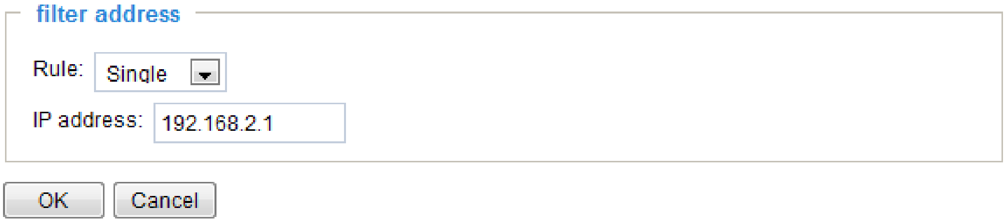
Filter

Then you can add a rule to the following Access List. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to page 39 for detailed information.



■ Add a rule to Allowed/Denied list: Click **Add** to add a rule to Allowed/Denied list.

There are three types of rules:
Single: This rule allows the user to add an IP address to the Allowed/Denied list.
For example:


filter address

Rule: Single

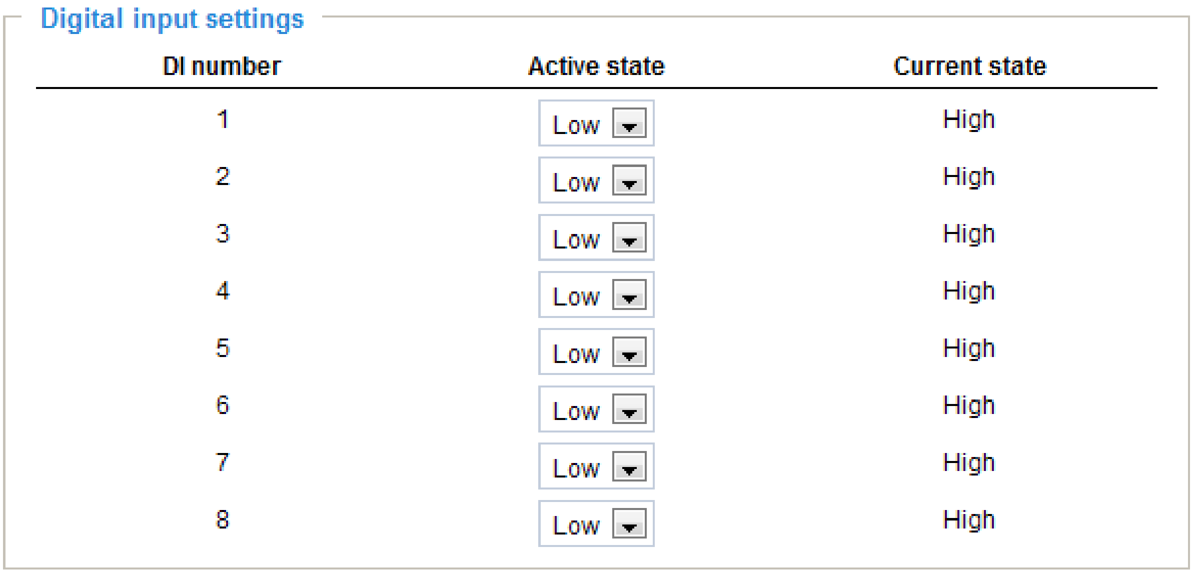
IP address: 192.168.2.1

Digital I/O

This section explains how to change digital input and digital output settings.

Digital input settings

You can select **High** or **Low** to define normal status for the digital input. The video server will report the current status.

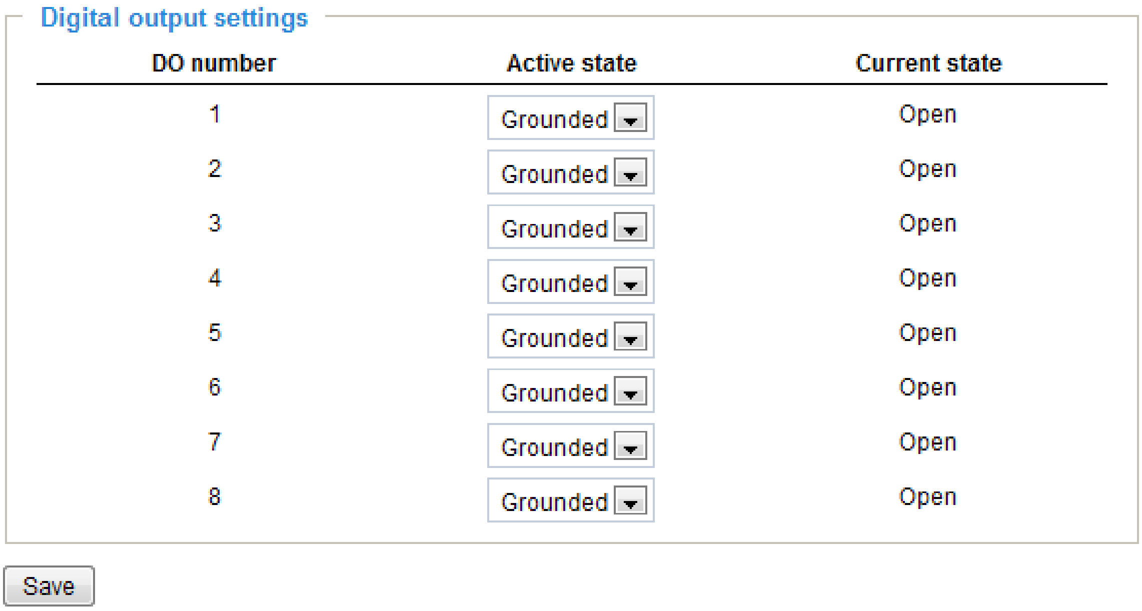


Digital input settings

DI number	Active state	Current state
1	Low	High
2	Low	High
3	Low	High
4	Low	High
5	Low	High
6	Low	High
7	Low	High
8	Low	High

Digital output settings

You can select **Grounded** or **Open** to define normal status for the digital output. The video server will show the trigger is activated or not.



Digital output settings

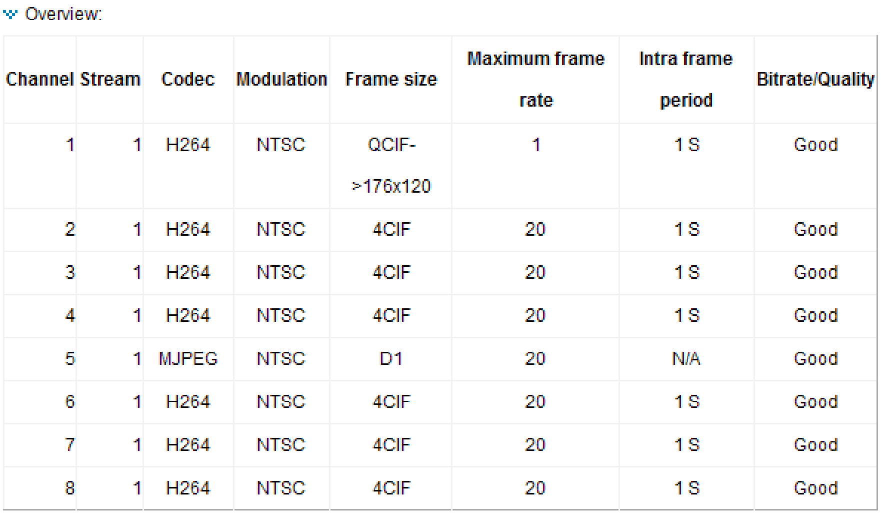
DO number	Active state	Current state
1	Grounded	Open
2	Grounded	Open
3	Grounded	Open
4	Grounded	Open
5	Grounded	Open
6	Grounded	Open
7	Grounded	Open
8	Grounded	Open

Audio and video

This section explains how to cofigure the audio and video settings of the video server.

Overview

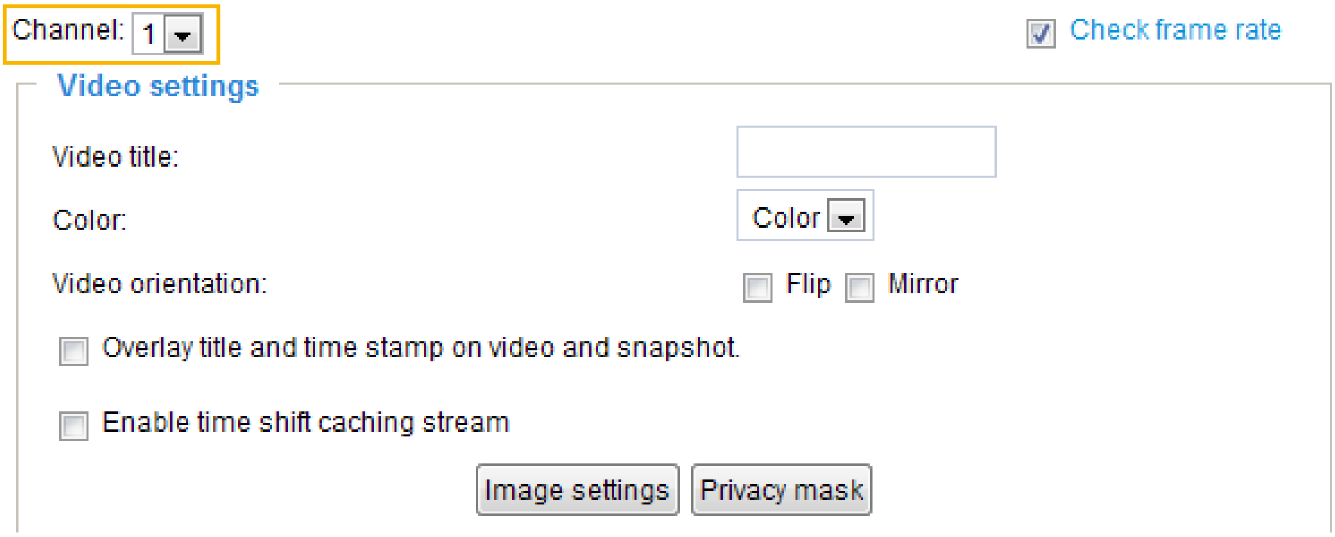
This table shows all stream settings of each channel.



Overview:

Channel	Stream	Codec	Modulation	Frame size	Maximum frame rate	Intra frame period	Bitrate/Quality
1	1	H264	NTSC	QCIF->176x120	1	1 S	Good
2	1	H264	NTSC	4CIF	20	1 S	Good
3	1	H264	NTSC	4CIF	20	1 S	Good
4	1	H264	NTSC	4CIF	20	1 S	Good
5	1	MJPEG	NTSC	D1	20	N/A	Good
6	1	H264	NTSC	4CIF	20	1 S	Good
7	1	H264	NTSC	4CIF	20	1 S	Good
8	1	H264	NTSC	4CIF	20	1 S	Good

Video settings



Channel: 1 ▾

☑ Check frame rate

Video settings

Video title:

Color: Color ▾

Video orientation: □ Flip □ Mirror

□ Overlay title and time stamp on video and snapshot.

□ Enable time shift caching stream

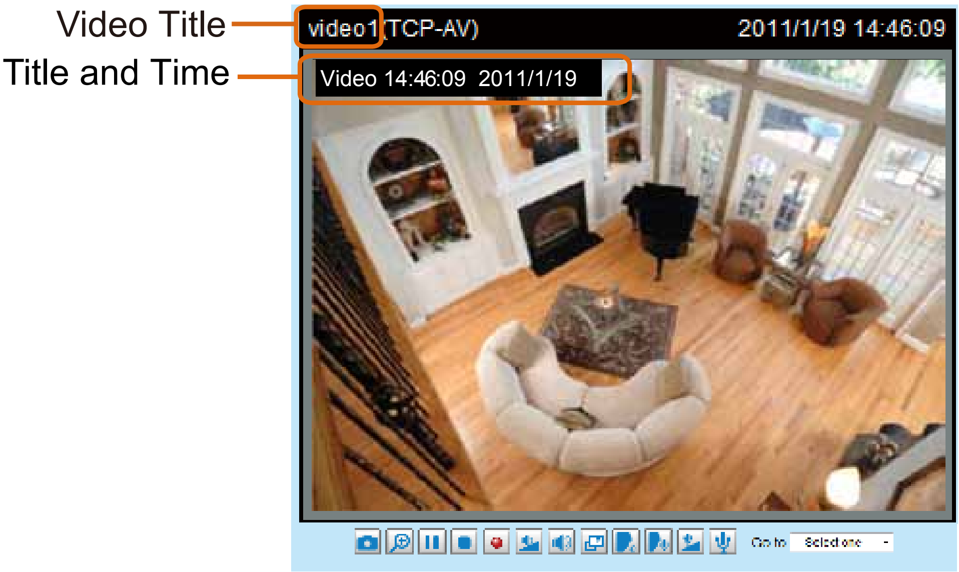
Channel: In the drop-down list, there are channel 1~4/8, select one to set video settings on it in the column below.

Check frame rate: Check **Check frame rate** to display the current available frame rate status for all frame sizes**.** Please refer to page 63 for details.

Video title: Enter a name that will be displayed on the title bar of the live video.

Color: Select to display color or black/white video streams.

Video orientation: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display of the live video. Select both options if the linked device is installed upside-down (e.g., on the ceiling) to correct the image orientation.



Overlay title and time stamp on video and snapshot: Select this option to place the video title and time on the video streams.

Enable time shift caching stream Advanced Mode: Check this item to enable the time shift cache stream on the video server, which will stores video in the video server's embedded memory for a period of time depending on the cache memory size of each video server. This function can work seamlessly with VIVOTEK's ST7501 recording software. When an event occurs, the recording software can request time shift cache stream from the camera, which allows the user to retrieve pre-event video data.

Image settings Advanced Mode

Click **Image Settings** to open the Image Settings page. On this page, you can tune the White balance, Brightness, Saturation, Contrast, and Sharpness settings for the video. Please choose the **Channel** first.

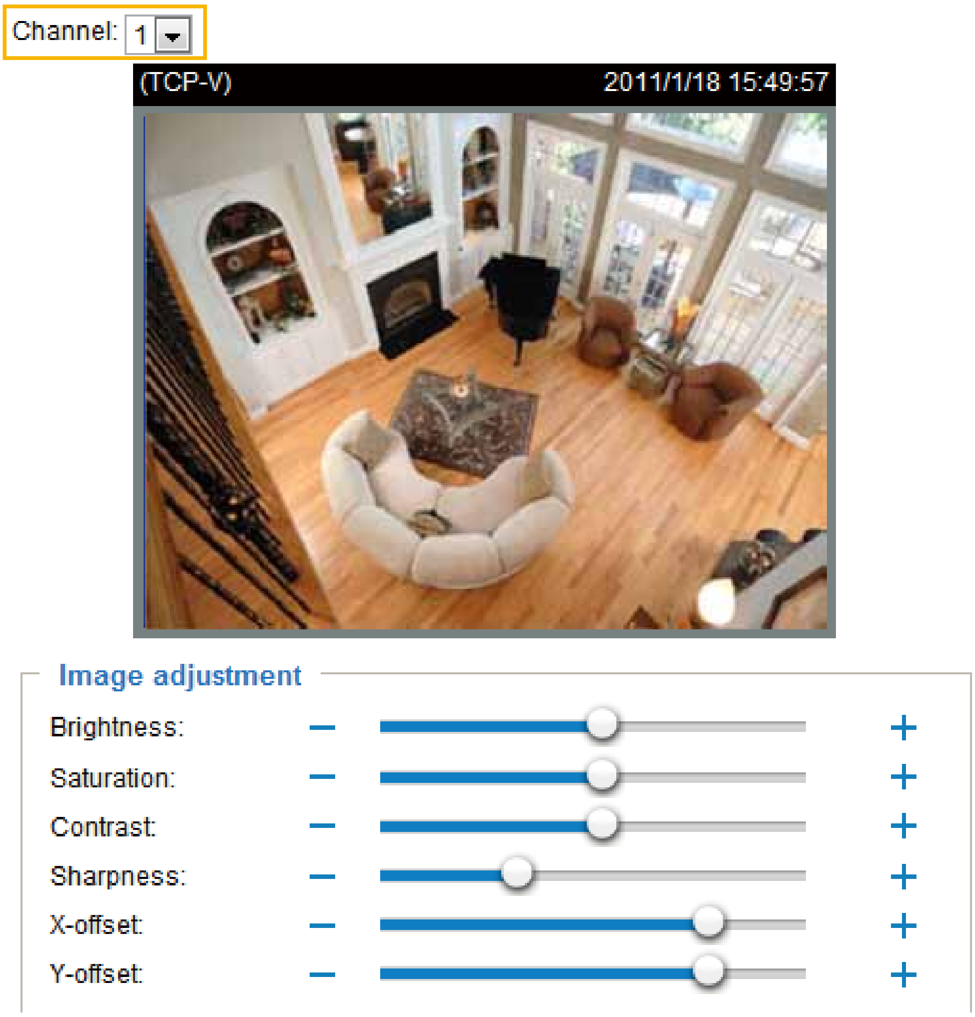


Image adjustment

■ Brightness: To adjust the image brightness level, please drag the slider bar to the right (+) to increase the effect, or to the left (-) to reduce the effect.

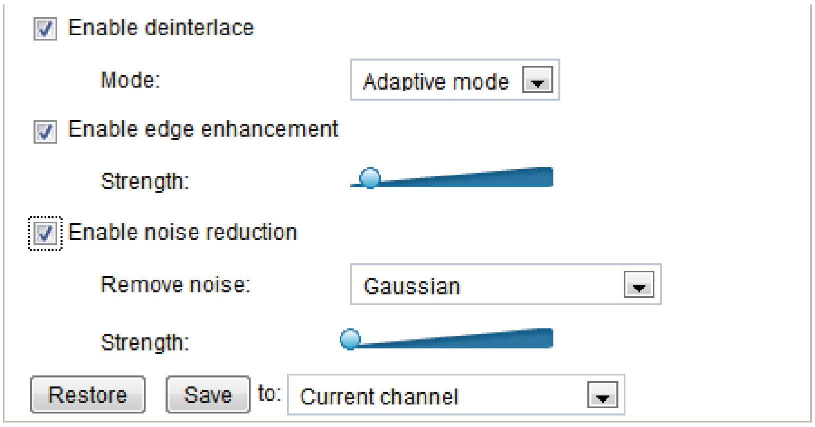
■ Saturation: To adjust the image saturation level, please drag the slider bar to the right (+) to increase the effect, or to the left(-) to reduce the effect.

■ Contrast: To adjust the image contrast level, please drag the slider bar to the right (+) to increase the effect, or to the left(-) to reduce the effect.

■ Sharpness: To adjust the image sharpness level, please drag the slider bar to the right (+) to increase the effect, or to the left(-) to reduce the effect.

■ X-offset: Adjust the image to the proper position horizontally.

■ Y-offset: Adjust the image to the proper position vertically.



☑ Enable deinterlace

Mode: Adaptive mode

☑ Enable edge enhancement

Strength:

☑ Enable noise reduction

Remove noise: Gaussian

Strength:

- ■ Enable deinterlace: Check to enable deinterlace, and choose **Adaptive mode** or **Blend mode** in the drop-down list. Adaptive mode provides the best image quality, while Blend mode provides better image quality (than not using the deinterlace function at all). Note that applying this function to all channels at the same time will consume quite a lot computing power.

- ■ Enable edge enhancement: Check to enable edge enhancement, and drag the slider bar to adjust the strength. Note that applying this function to all channels at the same time will consume quite a lot of computing power.

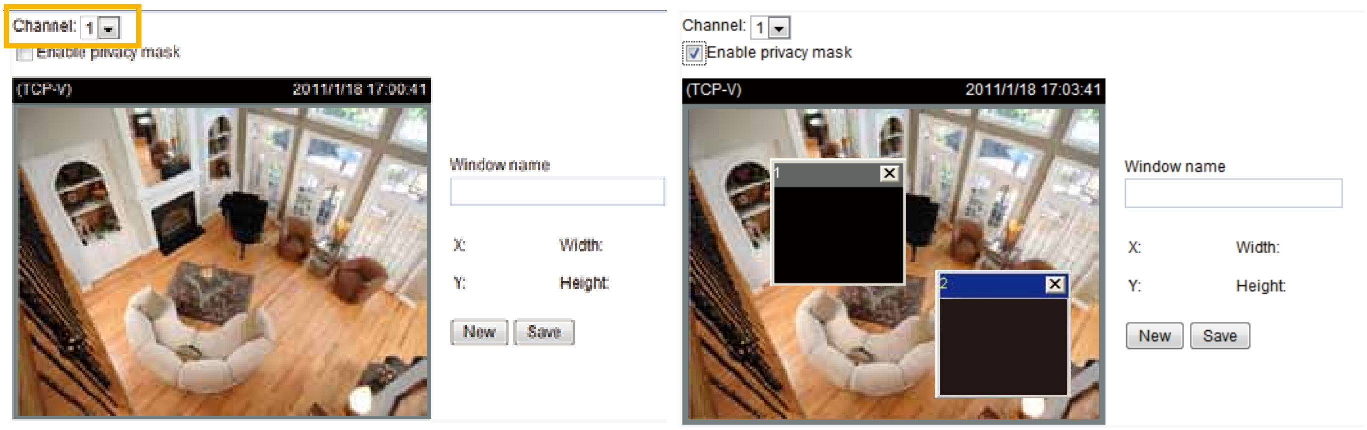
- ■ Enable noise reduction: Check to enable noise reduction, and you can also choose to reduce **Gaussian** noise, **impulse** noise, or **Gaussian** and **impulse** noise in the drop-down list. Drag the slide bar to adjust the strength. Noted that applying this function to all channels at the same time will consume quite a lot of computing power.

- ■ Restore: Click to restore the default setting.

- ■ Save: When finished with the setting, you can choose to apply the settings to **Current channel, All channels, Current channel and channel 2**, etc. in the drop-down list. Then click **Save** to enable the settings.

Privacy Mask Advanced Mode

Click **Privacy Mask** to open the settings page. On this page, you can block out sensitive zones to address privacy concerns. Please choose the **Channel** first.



Channel: 1
□ Enable privacy mask
(TCP-V) 2011/1/18 17:00:41

Channel: 1
☑ Enable privacy mask
(TCP-V) 2011/1/18 17:03:41

■ To set the privacy mask windows, follow the steps below:

1. Click **New** to add a new window.
2. Use the mouse to size and drag-drop the window, which is recommended to be at least twice the size of the object (height and width) you want to cover.
3. Enter a Window Name and click **Save** to enable the setting.
4. Select **Enable privacy mask** to enable this function.

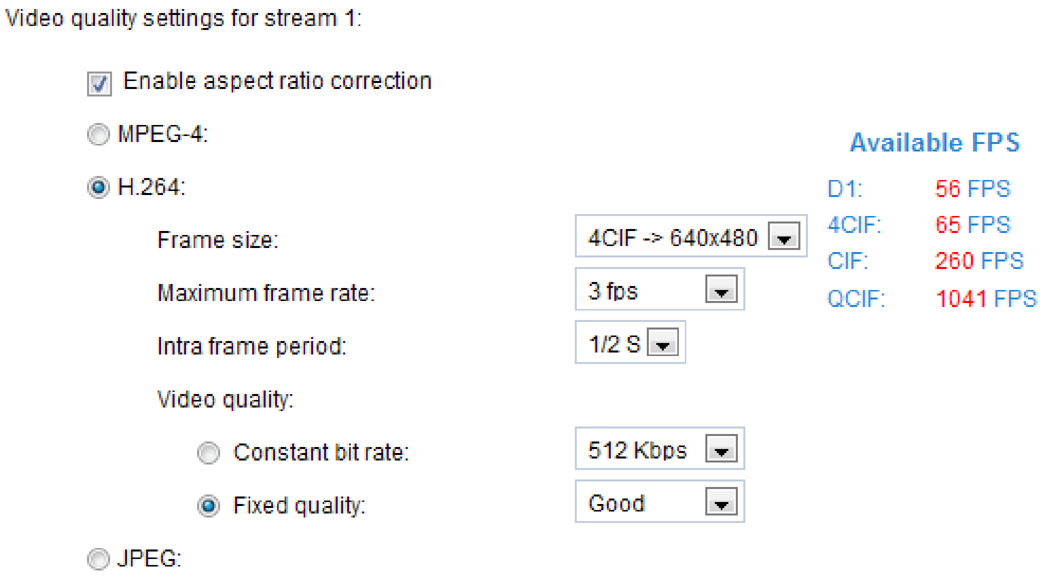
NOTE:

▶ *Up to 5 privacy mask windows can be set up on the same screen.*

▶ *If you want to delete a privacy mask window, please click on the 'x' mark at the upper right corner of the window.*

Video quality settings for stream 1 Advanced Mode

Click the items to display the detailed video quality settings.



Video quality settings for stream 1:

☑ Enable aspect ratio correction

○ MPEG-4:

● H.264:

Frame size:	4CIF -> 640x480
Maximum frame rate:	3 fps
Intra frame period:	1/2 S
Video quality:	
○ Constant bit rate:	512 Kbps
● Fixed quality:	Good

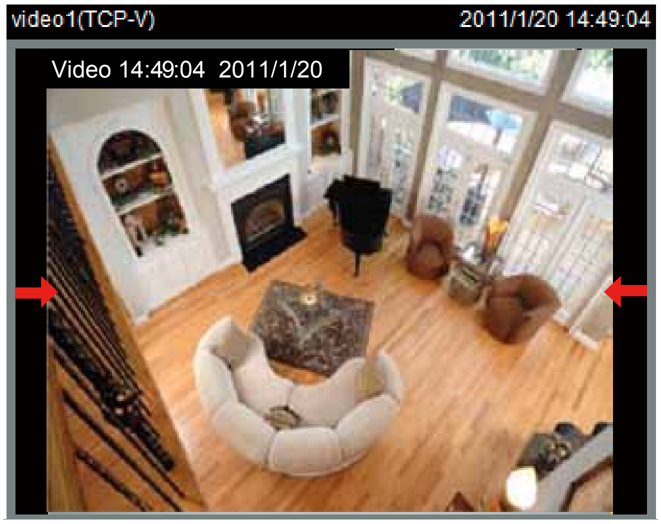
○ JPEG:

Available FPS

D1:	56 FPS
4CIF:	65 FPS
CIF:	260 FPS
QCIF:	1041 FPS

■ Enable aspect ratio correction:

In the default settings, the size of the video window will change according to the layout of the live viewing window you choose. However, the frame size may be distorted. If you check **Enable aspect ratio correction**, the video window will be adjusted to the same frame size as the preview window. This function is disabled as default.



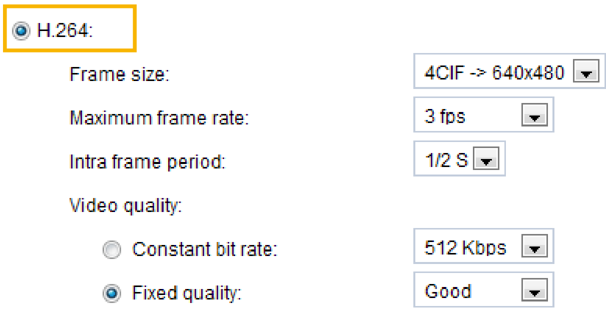
NOTE:

▶ *Aspect ratio correction doesn't support QCIF.*

▶ *When aspect ratio correction takes effect, the frame size for D1 will be adjusted to 640x480.*

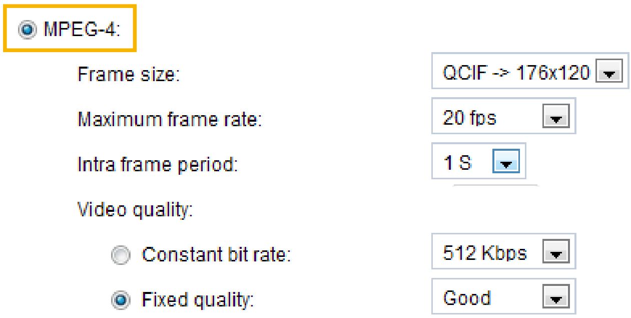
This video server offers real-time H.264, MPEG-4, and MJPEG compression standards (Triple Codec) for real-time viewing.

If **H.264 / MPEG-4** mode is selected, the video is streamed via RTSP protocol. There are four parameters for you to adjust the video performance:



● H.264:

Frame size:	4CIF -> 640x480
Maximum frame rate:	3 fps
Intra frame period:	1/2 S
Video quality:	
○ Constant bit rate:	512 Kbps
● Fixed quality:	Good



● MPEG-4:

Frame size:	QCIF -> 176x120
Maximum frame rate:	20 fps
Intra frame period:	1 S
Video quality:	
○ Constant bit rate:	512 Kbps
● Fixed quality:	Good

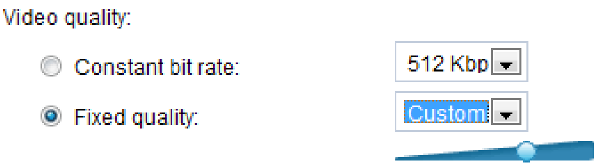
■ Frame size
You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions: QCIF, CIF, 4CIF, and D1.

■ Maximum frame rate
This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality. You can also select **Customize** and manually enter a value. The frame rate will decrease if you select a higher resolution.

■ Intra frame period
Determine how often to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

■ Video quality
A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. Therefore, if **Constant bit rate** is selected, the bandwidth utilization is fixed at a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, and 4Mbps. You can also select **Customize** and manually enter a value.

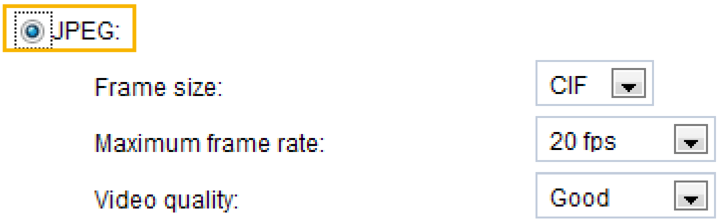
On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually adjust the slider bar. You may adjust the slider bar to the right to have better video quality.



Video quality:

○ Constant bit rate:	512 Kbp
● Fixed quality:	Custom

If **JPEG** mode is selected, the video server continuously sends JPEG images to the client, producing a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents are a combination of JPEG images, no audio data is transmitted to the client. There are three parameters provided in MJPEG mode to control the video performance:



● JPEG:

Frame size: CIF

Maximum frame rate: 20 fps

Video quality: Good

■ Frame size

You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions: QCIF, CIF, 4CIF, and D1.

■ Maximum frame rate

This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.

You can also select **Customize** and manually enter a value. The frame rate will decrease if you select a higher resolution.

■ Video quality

The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

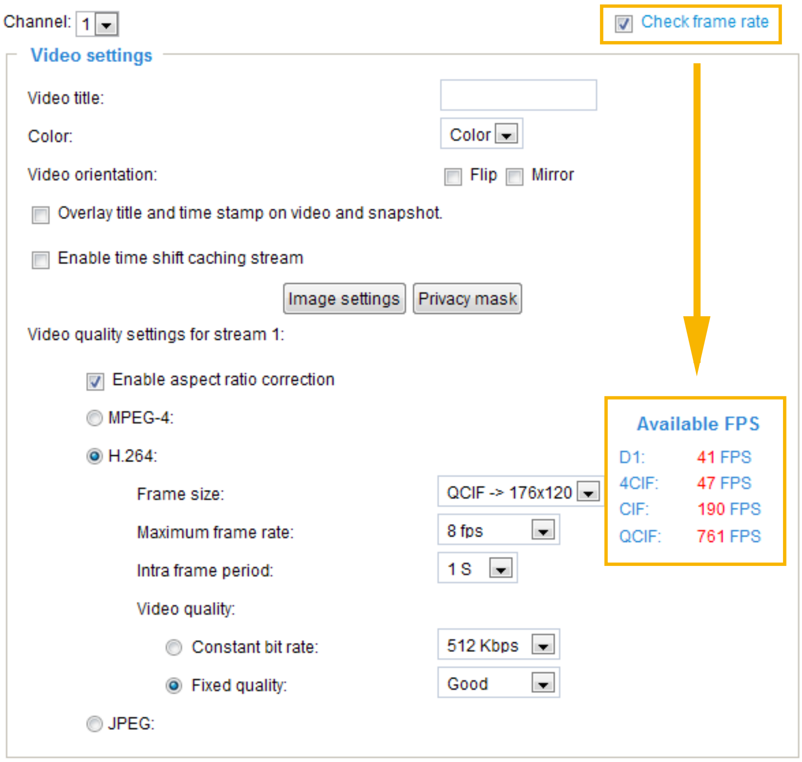
NOTE:

▶ *Video quality and fixed quality refers to the **compression rate**, so a lower value will produce higher quality.*

▶ *Converting high-quality video may significantly increase the CPU loading, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the event of occurance, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

■ Available FPS

Check **Check frame rate** to display the current available frame rate status **(Available FPS).** Available FPS provides the information of the unused encoding capability with available frame rate in different frame size.



Channel: 1 ▾

☑ Check frame rate

Video settings

Video title:

Color: Color ▾

Video orientation: □ Flip □ Mirror

□ Overlay title and time stamp on video and snapshot.

□ Enable time shift caching stream

Image settings | Privacy mask

Video quality settings for stream 1:

☑ Enable aspect ratio correction

○ MPEG-4:

● H.264:

Frame size: QCIF -> 176x120 ▾

Maximum frame rate: 8 fps ▾

Intra frame period: 1 S ▾

Video quality:

○ Constant bit rate: 512 Kbps ▾

● Fixed quality: Good ▾

○ JPEG:

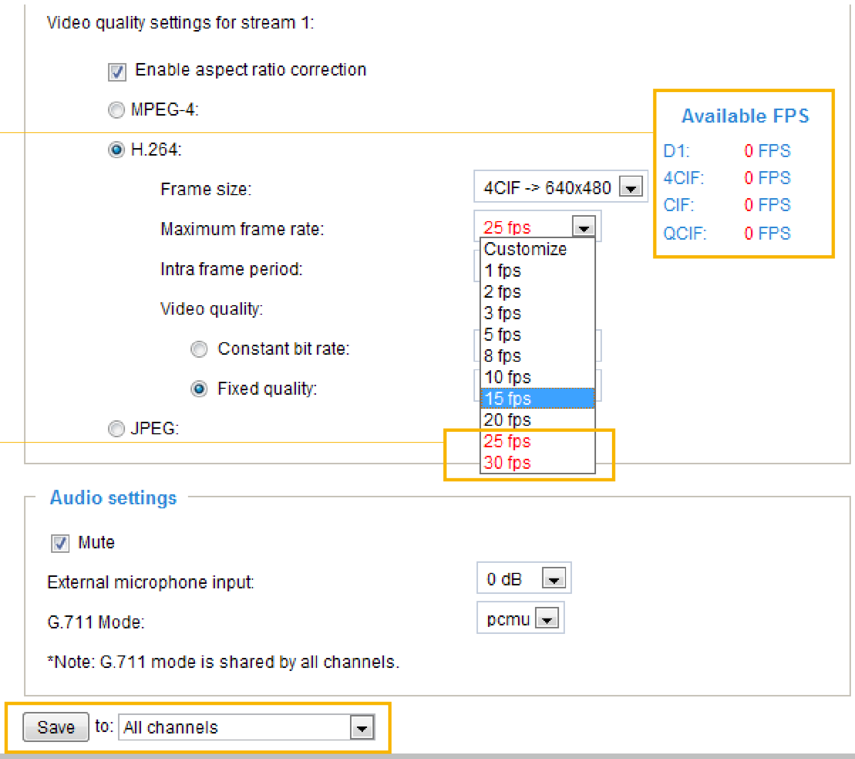
Available FPS

D1:	41 FPS
4CIF:	47 FPS
CIF:	190 FPS
QCIF:	761 FPS

The embedded Soc (System-on-Chip) has limited encoding capability, so you may set the video quality according to the available FPS. Due to the limited encoding capability, the maximum frame rate for 4CIF in H.264 or MPEG-4 codec can only support up to 23 FPS when all channels are applied to this setting and being used. If the total amount of frame rate exceeds encoding capability, a warning message "Frame rate is not guaranteed" will show up in a pop-up window. Also the frame rate that cannot be reached for each stream will be marked in red color in the "Overview" column.

No available FPS due to the total amount of frame rate exceeds the encoding capability.

the frame rate that cannot be reached is marked in red color.



Video quality settings for stream 1:

☑ Enable aspect ratio correction

○ MPEG-4:

● H.264:

Frame size: 4CIF -> 640x480 ▾

Maximum frame rate: 25 fps ▾

Intra frame period:

Video quality:

○ Constant bit rate:

● Fixed quality:

○ JPEG:

Available FPS

D1:	0 FPS
4CIF:	0 FPS
CIF:	0 FPS
QCIF:	0 FPS

Audio settings

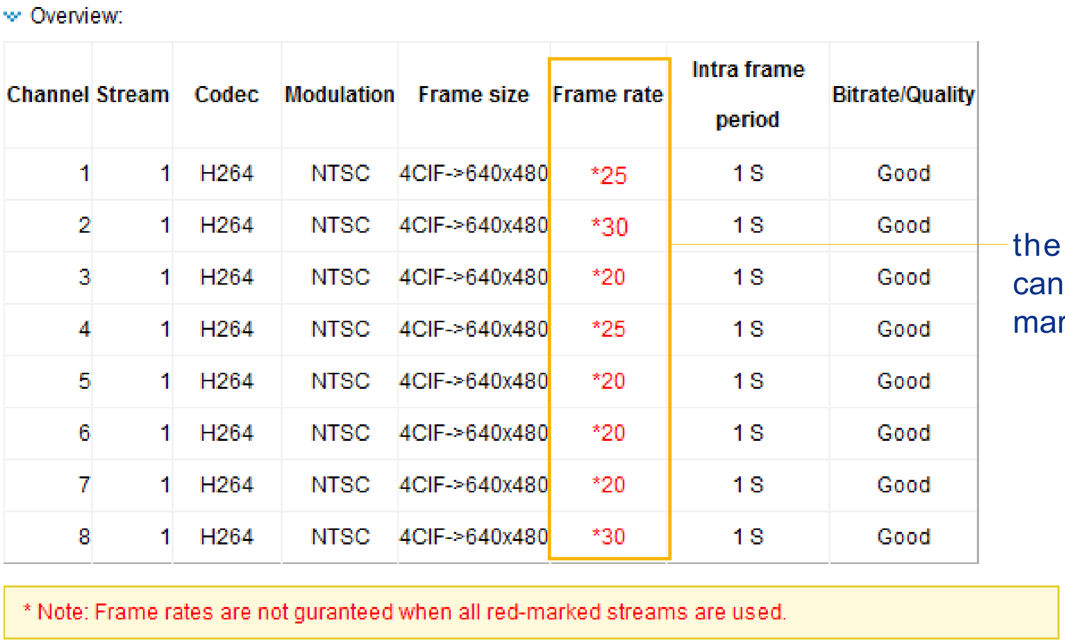
☑ Mute

External microphone input: 0 dB ▾

G.711 Mode: pcmu ▾

*Note: G.711 mode is shared by all channels.

Save to: All channels ▾



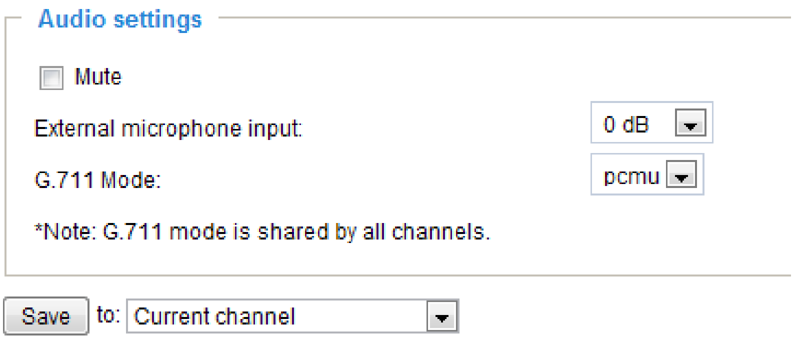
Overview:

Channel	Stream	Codec	Modulation	Frame size	Frame rate	Intra frame period	Bitrate/Quality
1	1	H264	NTSC	4CIF->640x480	*25	1 S	Good
2	1	H264	NTSC	4CIF->640x480	*30	1 S	Good
3	1	H264	NTSC	4CIF->640x480	*20	1 S	Good
4	1	H264	NTSC	4CIF->640x480	*25	1 S	Good
5	1	H264	NTSC	4CIF->640x480	*20	1 S	Good
6	1	H264	NTSC	4CIF->640x480	*20	1 S	Good
7	1	H264	NTSC	4CIF->640x480	*20	1 S	Good
8	1	H264	NTSC	4CIF->640x480	*30	1 S	Good

* Note: Frame rates are not guranteed when all red-marked streams are used.

the frame rate that cannot be reached is marked in red color.

Audio settings



Audio settings

□ Mute

External microphone input: 0 dB

G.711 Mode: pcmu

*Note: G.711 mode is shared by all channels.

Mute: Select this option to disable audio transmission from the video server to all clients. Note that if mute mode is turned on, no audio data will be transmitted even if audio transmission is enabled on the Client Settings page. In that case, the following message is displayed:

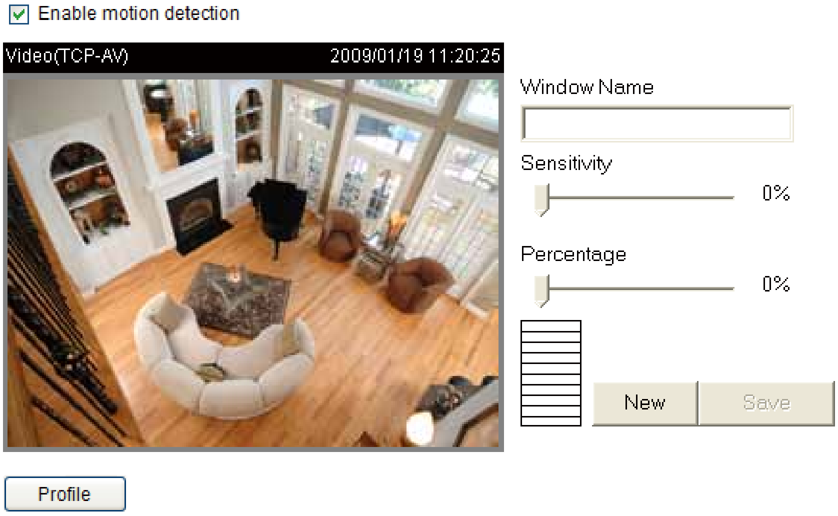
External microphone input: Select the gain of the internal audio input according to ambient conditions. Adjust the gain from +9 db (most sensitive) ~ -12 db (least sensitive).

G.711 Mode: G.711 also provides good sound quality and requires about 64Kbps. Select pcmu (Pulse code Modulation μ-Law) or pcma (A-Law) mode.

Save: When finishing the setting, you can choose to apply the settings to **Current channel, All channels, Current channel and channel 2**, etc. in the drop-down list. Then click **Save** to enable the settings.

Motion detection

This section explains how to configure the Video Server to enable motion detection. A total of three motion detection windows can be configured for each channel.



☑ Enable motion detection

Video(TCP-AV) 2009/01/19 11:20:25

Window Name:

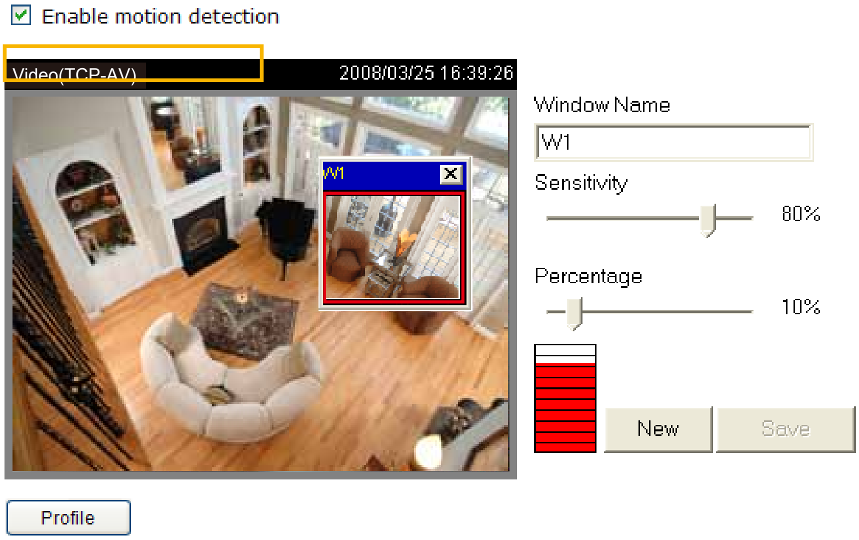
Sensitivity: 0%

Percentage: 0%

Follow the steps below to enable motion detection:

1. Select **Channel**.
2. Click **New** to add a new motion detection window.
3. In the Window Name text box, enter a name for the motion detection window.
   - ■ To move and resize the window, drag and drop your mouse on the window.
   - ■ To delete window, click X on the upper right corner of the window.
4. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slider bar.
5. Click **Save** to enable the settings.
6. Check **Enable motion detection** to enable this function.

For example:



☑ Enable motion detection

Video(TCP-AV) 2008/03/25 16:39:26

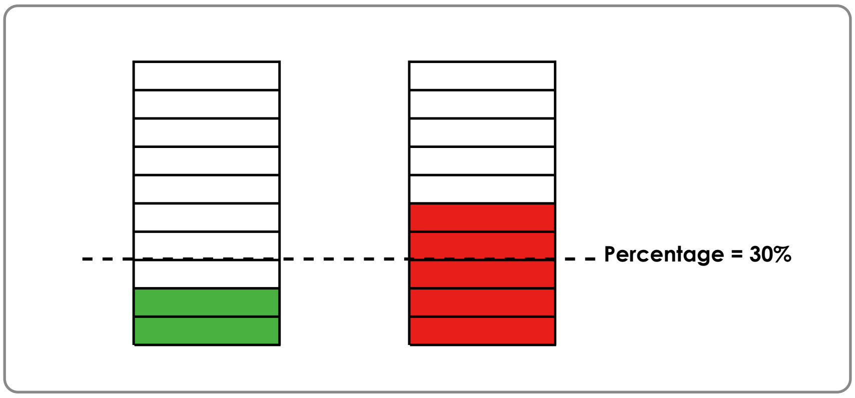
Window Name: W1

Sensitivity: 80%

Percentage: 10%

The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to be sent to a remote server (Email, FTP) by utilizing this feature as a trigger source. For more information on how to set an event, please refer to Application on page 78.

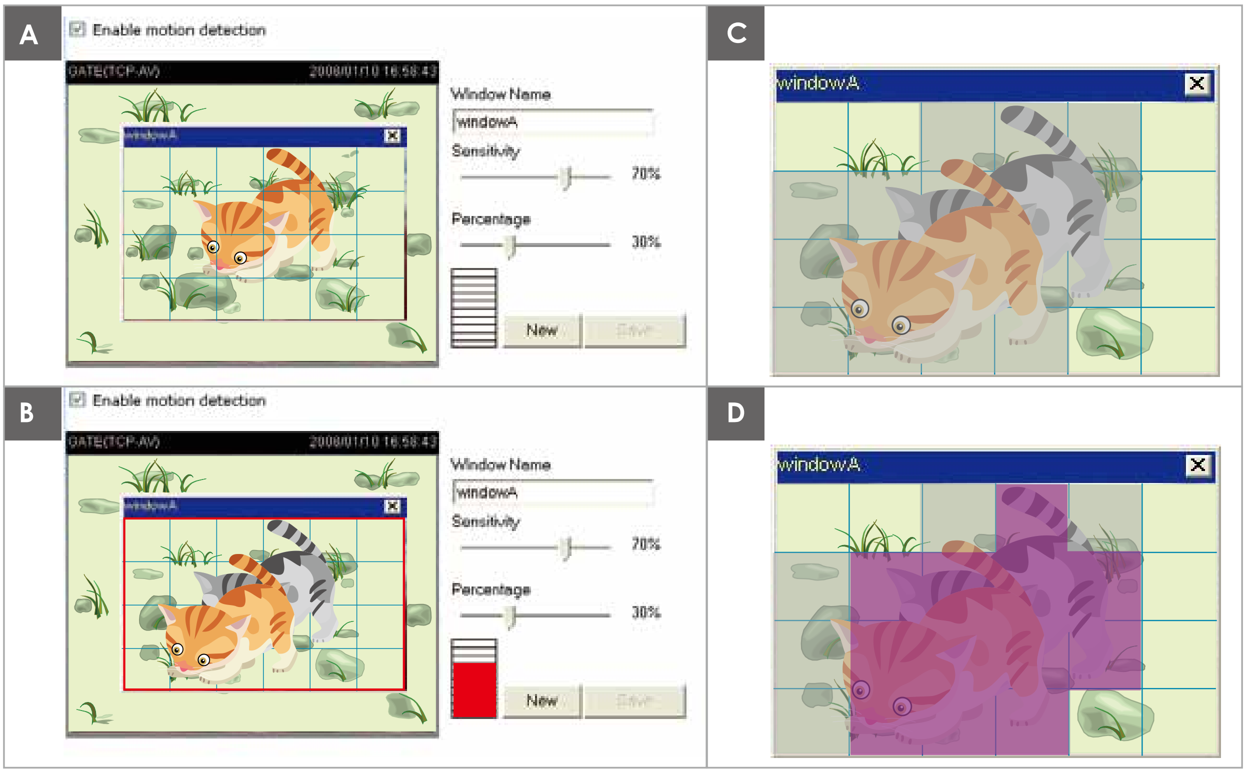
A green bar indicates that even though motions have been detected, the event has not been triggered because the image variations still fall under the defined threshold.



This motion detection window will also be displayed on the Event Settings page. You can go to Application > Event Settings > Trigger to choose it as a trigger source. Please refer to page 79 for detailed information.

NOTE:

► *How does motion detection work?*



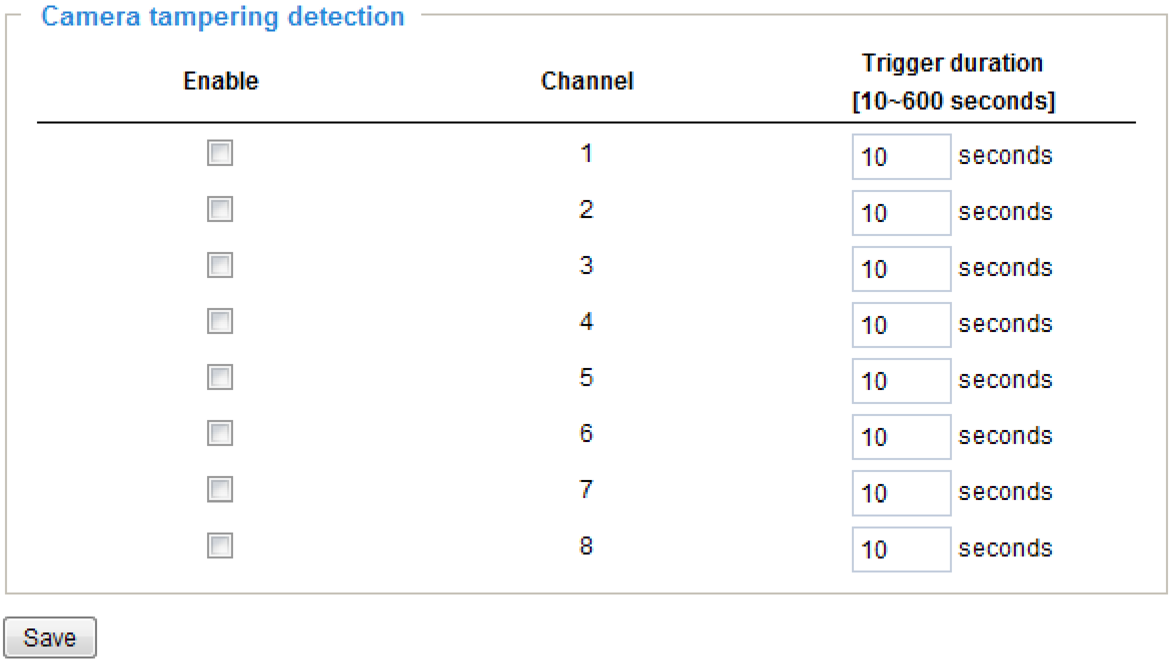
There are two motion detection parameters: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to detect slight movements while smaller sensitivity settings will neglect them. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).

Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.

For applications that require a high level of security management, it is suggested to use higher sensitivity settings and smaller percentage values.

Camera tampering detection

This section explains how to set up camera tempering detection. With tampering detection, the camera is capable of detecting incidents such as **redirection**, **blocking or defocusing**, or even **spray paint**.



Camera tampering detection

Enable	Channel	Trigger duration [10~600 seconds]
☐	1	10 seconds
☐	2	10 seconds
☐	3	10 seconds
☐	4	10 seconds
☐	5	10 seconds
☐	6	10 seconds
☐	7	10 seconds
☐	8	10 seconds

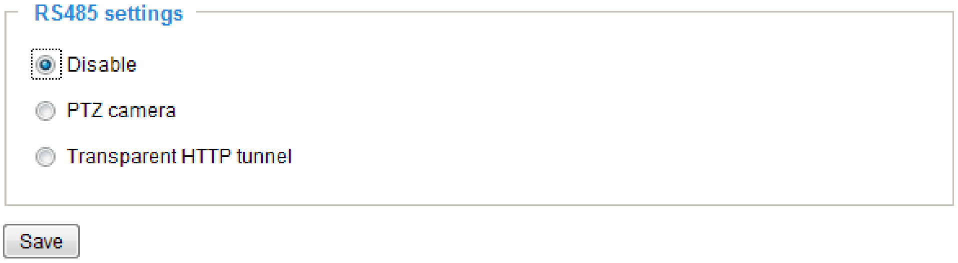
Please follow the steps below to set up the camera tampering detection function:

1. Check **Enable camera tampering detection**.
2. Enter the trigger duration. (10 sec. ~ 10 min.) The alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.
3. Set up the event source as Camera tampering detection on **Application** > **Event settings > Trigger**. Please refer to page 79 for detailed information.
4. Click on **Save** to take effect.

Camera control

This section explains how to control the Network Camera's Pan/Tilt/Zoom operation by connecting to a PTZ driver or scanner via RS485 interface.

RS485 settings



RS485 settings

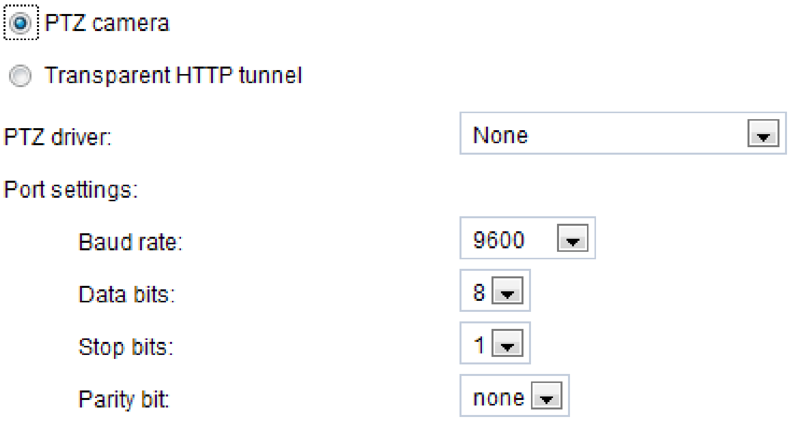
● Disable

○ PTZ camera

○ Transparent HTTP tunnel

Disable: Select this option to disable this function.

PTZ camera: Select this option to enable PTZ operation.
To utilize this feature, please connect the Network Camera to a PTZ driver or scanner via RS485 interface first. Then you can configure the PTZ driver and RS485 port with the following settings.

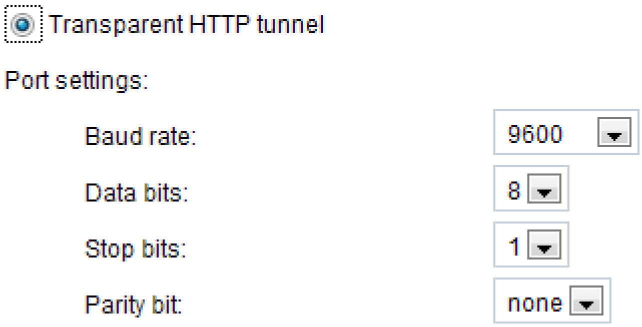


● PTZ camera

○ Transparent HTTP tunnel

PTZ driver:	None
Port settings:	
Baud rate:	9600
Data bits:	8
Stop bits:	1
Parity bit:	none

Transparent HTTP Tunnel: If you want to use your own RS-485 device, you can use UART commands to build a Transparent HTTP Tunnel. The UART commands will be sent through HTTP tunnel established between the RS-485 device and the linked camera. For detailed application notes, please refer to URL Commands on page 105 or http://www.vivotek.com/downloadfiles/support/faq/172_document_2.pdf.



● Transparent HTTP tunnel

Port settings:	
Baud rate:	9600
Data bits:	8
Stop bits:	1
Parity bit:	none

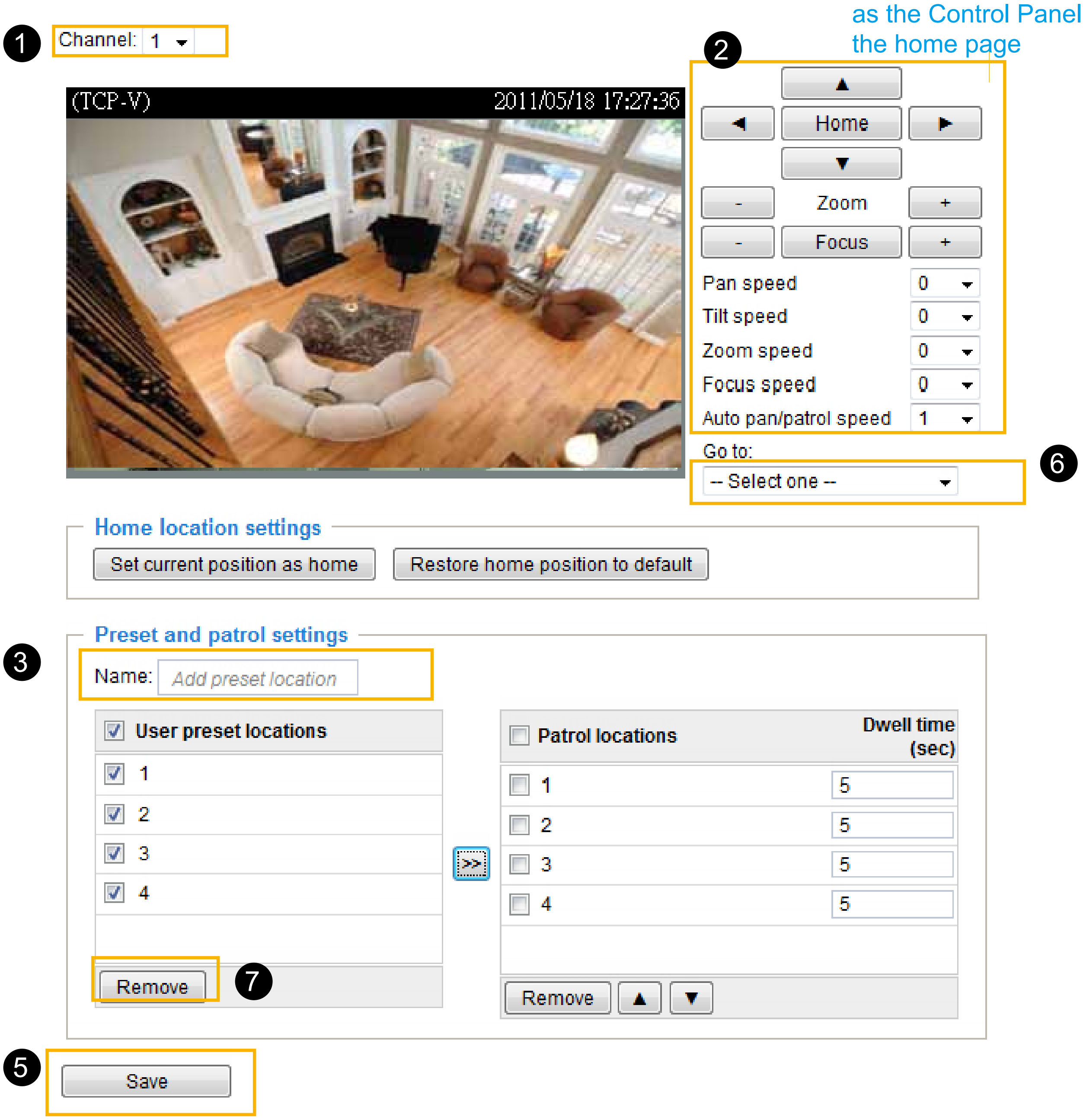
Preset positions

If you select DynaDome/SmartDOME, Lilin PIH-7x00, or Pelco D, Pelco P protocol, Samsung scc643 protocol protocol as the PTZ driver and click the **Save** button, the **Preset Position** button will be enabled. Click **Preset Position** to open the settings page. You can also select preset positions for the camera to patrol. A total of 20 preset positions can be configured.

Please follow the steps below to preset a position:

1. Select **Channel** in the drop-down list.
2. Adjust the shooting area to the desired position by using the buttons on the right. The default **Home** position is set as the center position.
3. Enter a name for the preset position, which allows up to forty characters. Click **Add** to enable the settings. The preset positions will be displayed under **User preset locations**.
4. To add additional preset positions, please repeat steps 1~2.
5. Select the preset positions and click on **Save** to enable the settings.
6. The positions saved will show up in **Go to** drop down list on the Home page. See next page
7. To remove a preset position from the list, select it and click **Remove**.

Functions are the same as the Control Panel on the home page



1 Channel: 1

2

(TCP-V) 2011/05/18 17:27:36

▲
◄ Home ►
▼
- Zoom +
- Focus +

Pan speed 0

Tilt speed 0

Zoom speed 0

Focus speed 0

Auto pan/patrol speed 1

Go to: -- Select one --

6

Home location settings

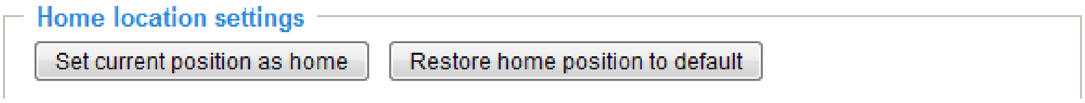
Set current position as home
Restore home position to default

Preset and patrol settings

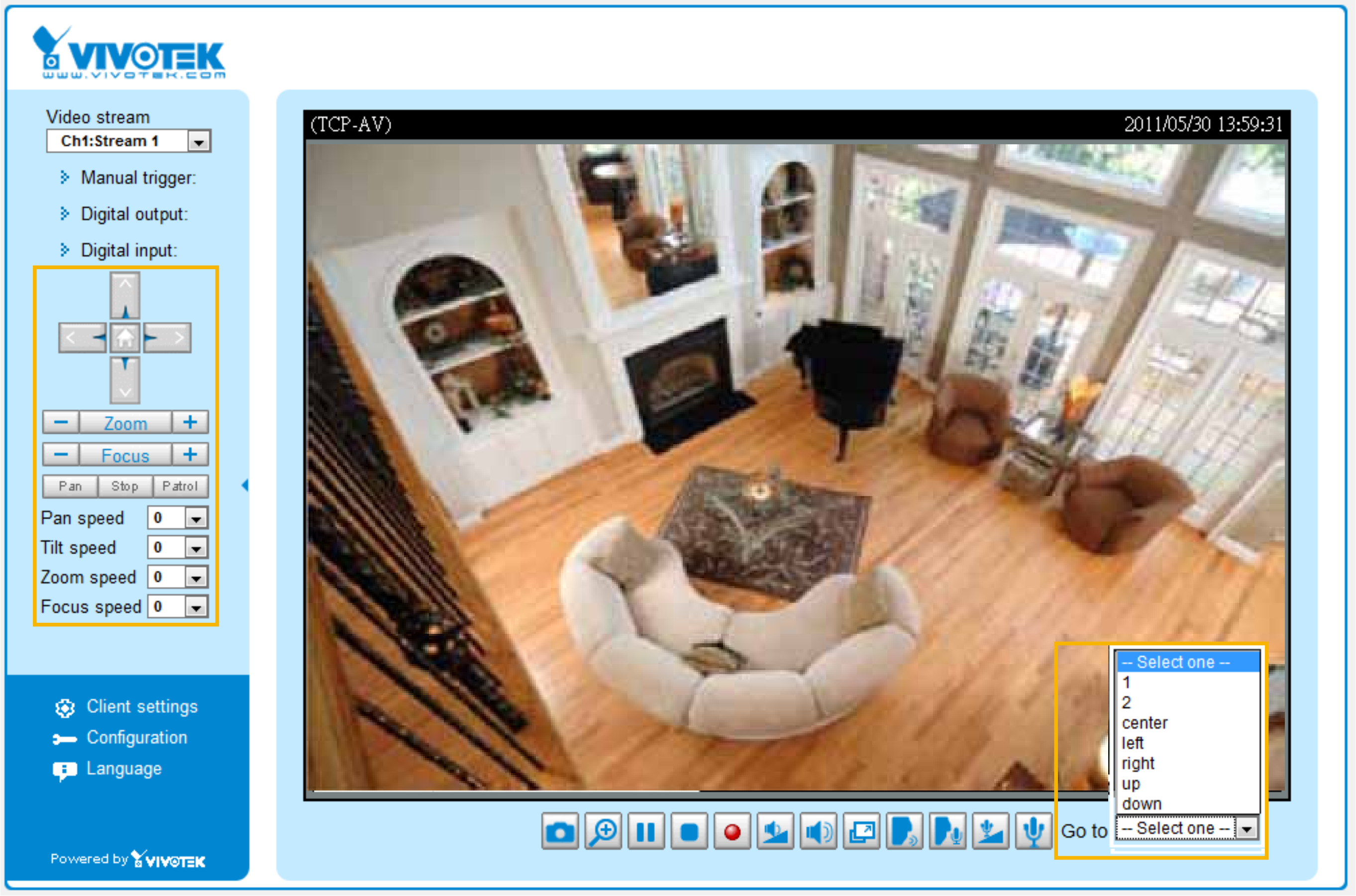
3 Name: Add preset location

☑ User preset locations
☑ 1
☑ 2
☑ 3
☑ 4

□ Patrol locations	Dwell time (sec)
□ 1	5
□ 2	5
□ 3	5
□ 4	5


Home location settings
Set current position as home
Restore home position to default

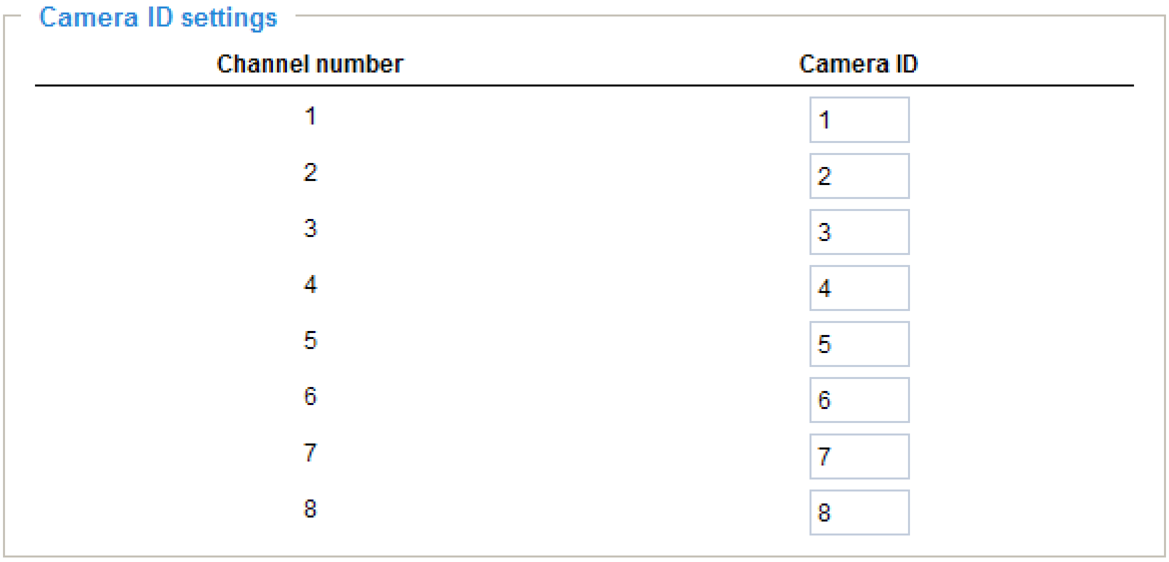
- Home location settings: You can configure the Home location by clicking on **Set current position as home**. Click on **Restore home position to default**, and the Home position will be set as the center position.



- The Camera Control Panel and Preset positions will be displayed on the home page:
- Click Go to: Select one from the drop-down list, and the Network Camera will move to the selected preset position.

Camera ID settings

VIVOTEK offers five PTZ drivers: DynaDome/SmartDOME, Lilin PIH-7x00, Pelco D protocol, Pelco P protocol, and Samsung scc643 protocol. If none of the above PTZ drivers is supported by your PTZ scanner, please select **Custom camera** (scanner). Please refer to the user's manual of your PTZ scanner to determine the Camera ID, PTZ driver, and Port settings. The Camera ID is necessary to control multiple cameras. If you click **Save** to enable this function, the camera control panel will be displayed on the main page. Please refer to the illustration on page 70.



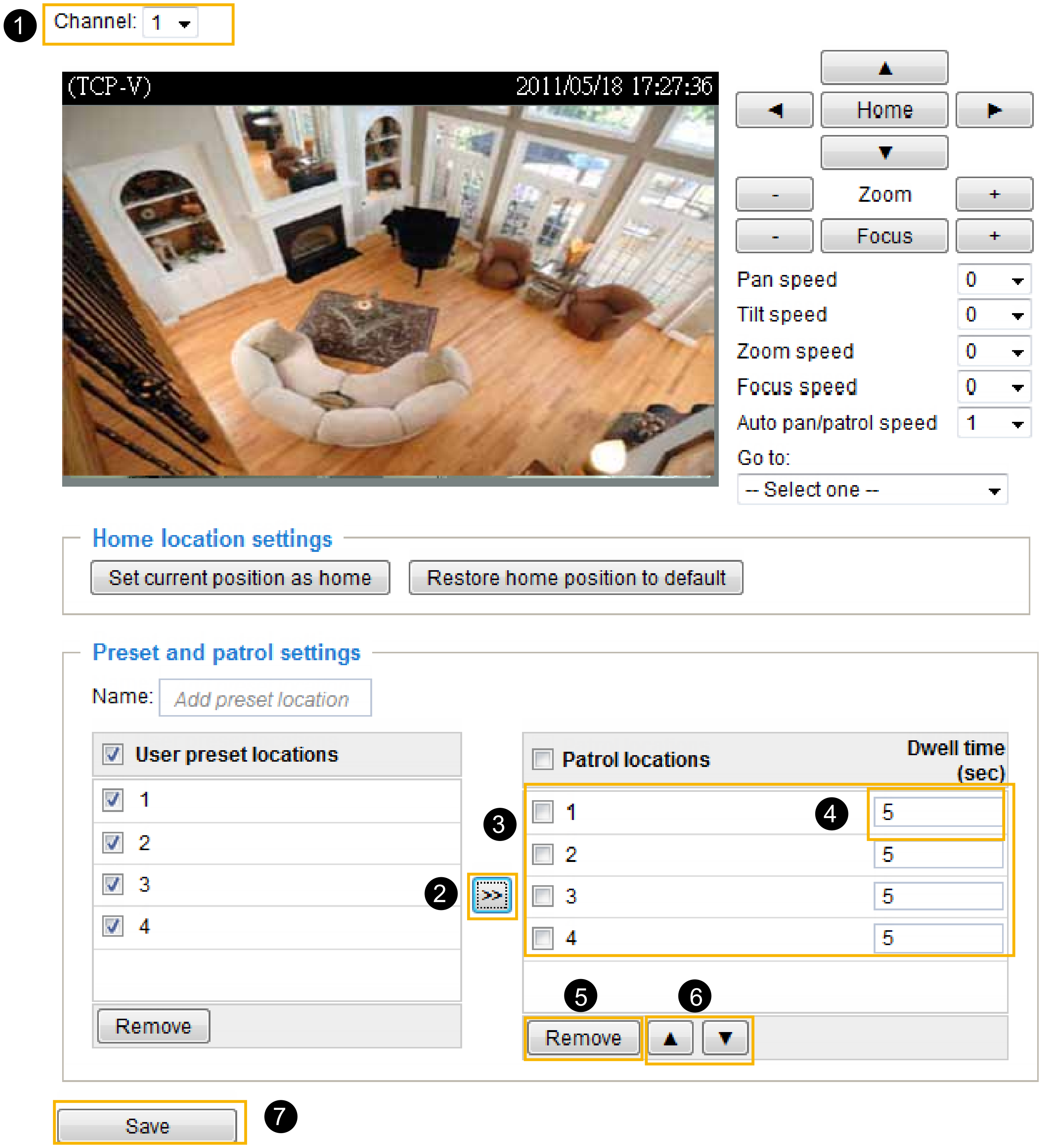
Camera ID settings

Channel number	Camera ID
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8

Patrol settings

You can select some preset positions for the Network Camera to patrol.
Please follow the steps below to set up a patrol schedule:

1. Select **Channel** in the drop-down list.
2. Select the preset locations on the list, and click >> .
3. The selected preset locations will be displayed on the **Patrol locations** list.
4. Set the **Dwelling time** for the preset location during auto patrol.
5. If you want to delete a preset location from the Patrol locations list, select it and click **Remove**.
6. Select a location and click ▲ ▼ to rearrange the patrol order.
7. Select patrol locations you want to save in the list and click **Save** to enable the patrol settings.
8. To implement the patrol schedule, please go to homepage and click on **Patrol** button.



Channel: 1

(TCP-V) 2011/05/18 17:27:36

Pan speed: 0
Tilt speed: 0
Zoom speed: 0
Focus speed: 0
Auto pan/patrol speed: 1
Go to: -- Select one --

Home location settings

Preset and patrol settings

Name: Add preset location

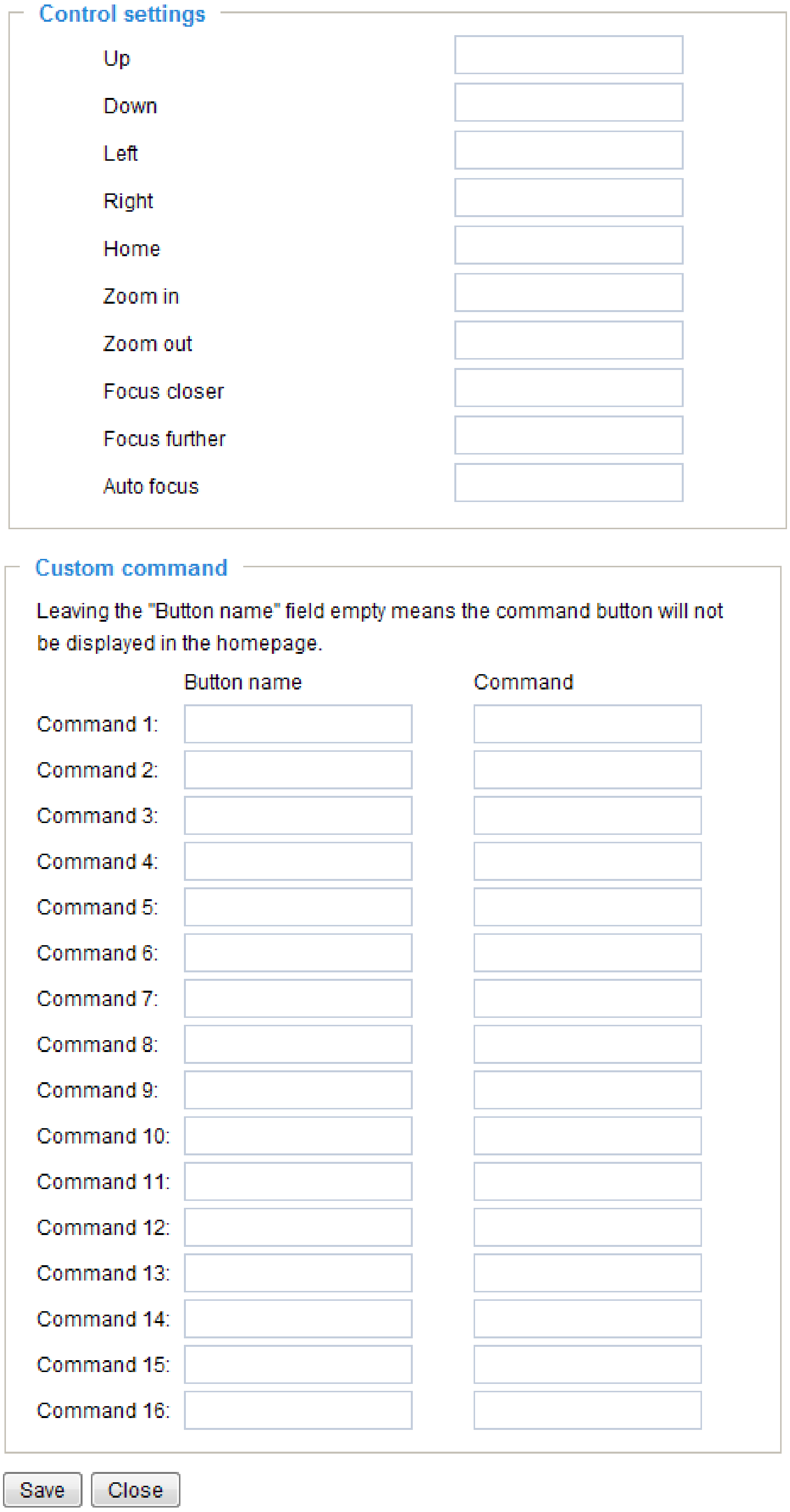
☑ User preset locations
☑ 1
☑ 2
☑ 3
☑ 4

□ Patrol locations	Dwell time (sec)
□ 1	5
□ 2	5
□ 3	5
□ 4	5

1
▲
◀
Home
▶
▼
-
Zoom
+
-
Focus
+
Set current position as home
Restore home position to default
3
4
2
>>
Remove
5
6
Remove
▲
▼
Save
7

Custom Command

If **Custom Camera (scanner)** is selected as the PTZ driver, the **Preset Position** and **PTZ Control Panel** on the main page will be disabled. You will need to configure command buttons to control the PTZ scanner. Click **Custom Command** to open the Custom Command page to set the commands in the Control Settings session. Please refer to your PTZ scanner user's manual to enter the commands in the following fields. Click **Save** to enable the settings and click **Close** to exit the page.



Control settings

Up	
Down	
Left	
Right	
Home	
Zoom in	
Zoom out	
Focus closer	
Focus further	
Auto focus	

Custom command

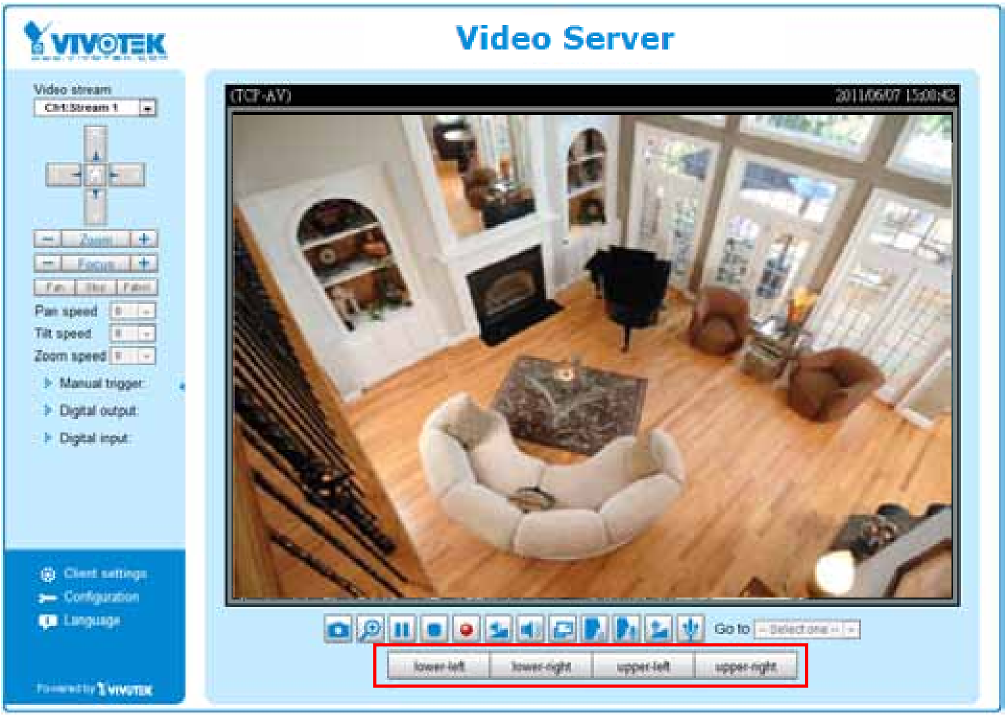
Leaving the "Button name" field empty means the command button will not be displayed in the homepage.

	Button name	Command
Command 1:		
Command 2:		
Command 3:		
Command 4:		
Command 5:		
Command 6:		
Command 7:		
Command 8:		
Command 9:		
Command 10:		
Command 11:		
Command 12:		
Command 13:		
Command 14:		
Command 15:		
Command 16:		

NOTE:

- ►*If you select DynaDome/SmartDOME, Lilin PIH-7x00, or Pelco D protocol as the PTZ driver, the Control Settings column will not be displayed.*
- ►*For all PTZ drivers, a total of five additional command buttons can be configured.*

► *The command buttons will be displayed on the main page:*

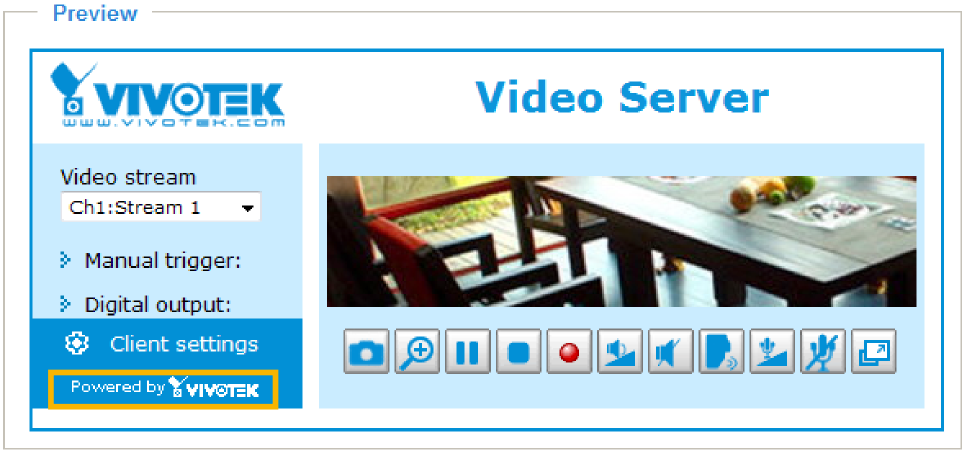


Homepage layout Advanced Mode

This section explains how to set up your own customized homepage layout.

Preview

This column shows the settings of your homepage layout. You can manually select the background and font colors in Theme Options (the third column on this page). The settings will be displayed automatically in this Preview field. The following shows the homepage using the default settings:

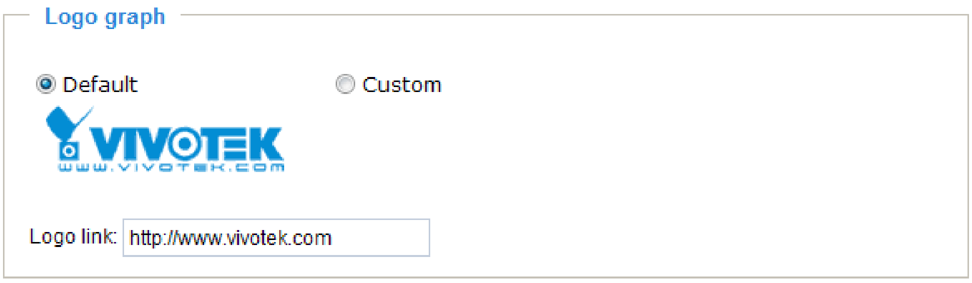


□ Hide Powered by VIVOTEK

■ Hide Powered by VIVOTEK: If you check this item, it will be removed from the homepage.

Logo

Here you can change the logo at the top of your homepage.



● Default ○ Custom

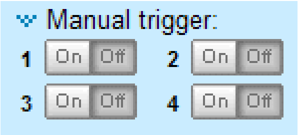
Logo link: http://www.vivotek.com

Follow the steps below to upload a new logo:
1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

Customized button

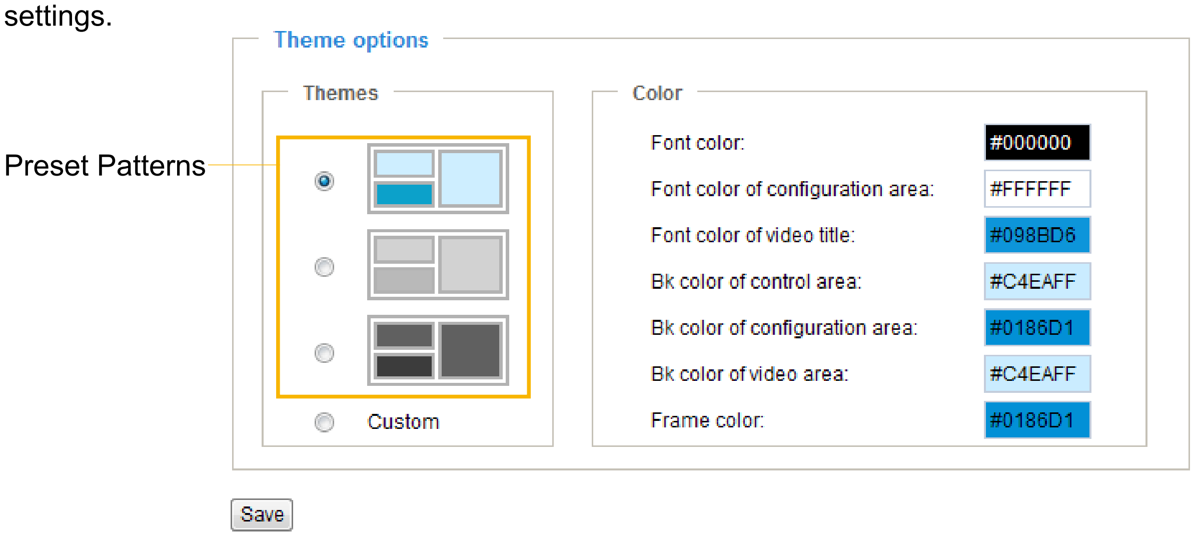
☑ Show manual trigger button

Check **Show manual trigger button**, and it will be displayed on the Home page. Uncheck **Show manual trigger button** to hide this function on the Home page.



Theme options

Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the settings.



Theme options

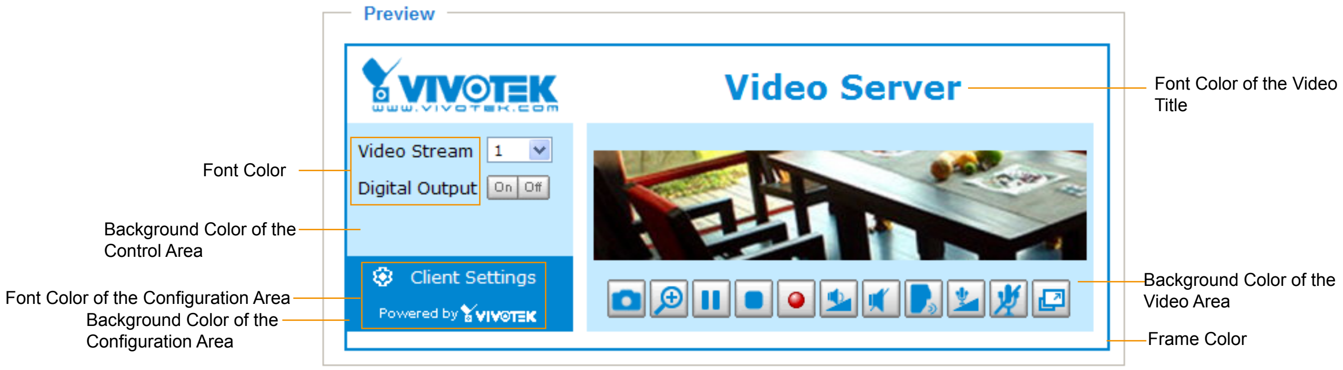
Themes

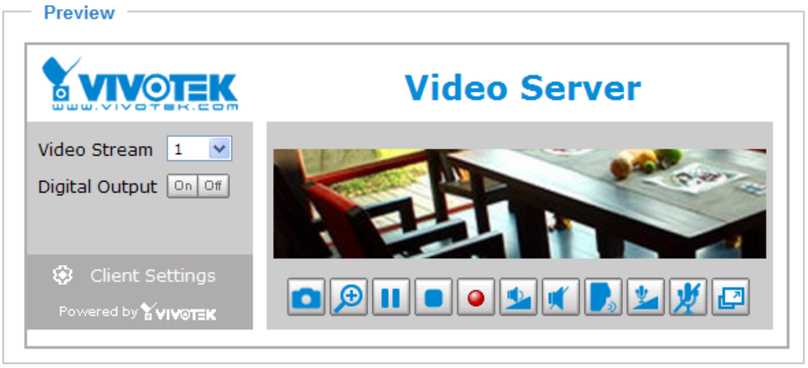
●
○
○
○ Custom

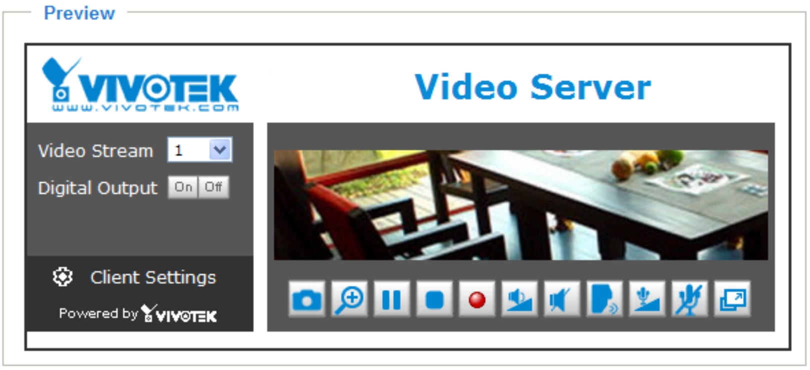
Color

Font color:	#000000
Font color of configuration area:	#FFFFFF
Font color of video title:	#098BD6
Bk color of control area:	#C4EAFF
Bk color of configuration area:	#0186D1
Bk color of video area:	#C4EAFF
Frame color:	#0186D1

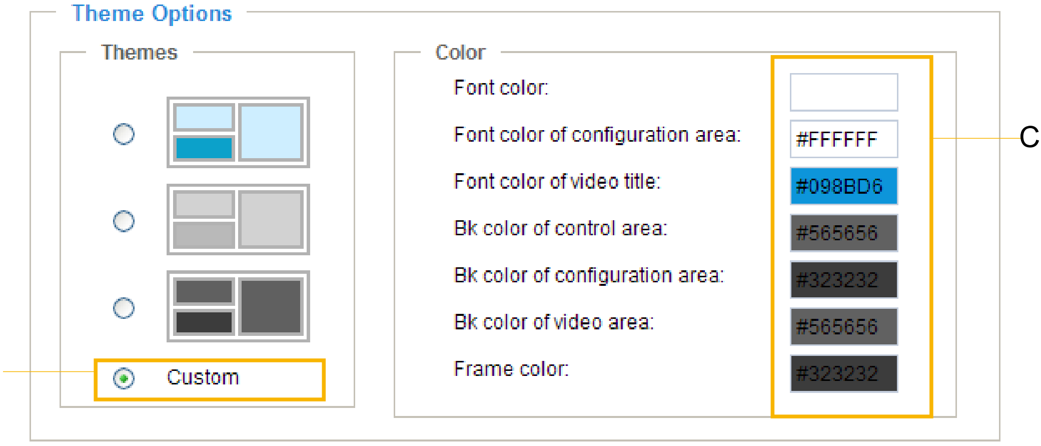
Save


Preview
Video Server
Font Color of the Video Title
Font Color
Video Stream 1
Digital Output On Off
Background Color of the Control Area
Font Color of the Configuration Area
Background Color of the Configuration Area
Client Settings
Powered by VIVOTEK
Background Color of the Video Area
Frame Color





■ Follow the steps below to set up the customed homepage:
1. Click **Custom** on the left column.
2. Click the field where you want to change the color on the right column.



Theme Options

Themes

○

○

○

● Custom

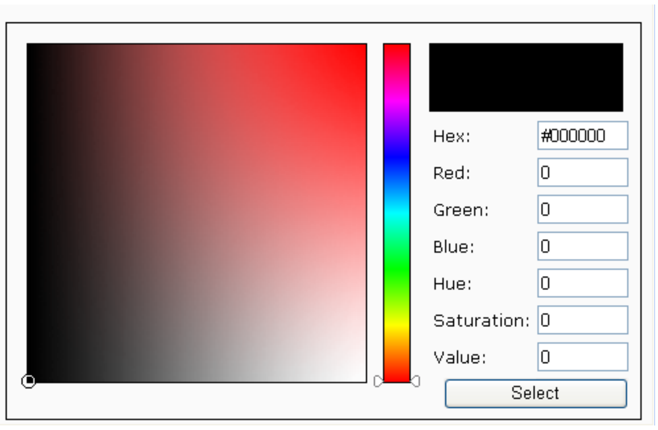
Color

Font color:	
Font color of configuration area:	#FFFFFF
Font color of video title:	#098BD6
Bk color of control area:	#565656
Bk color of configuration area:	#323232
Bk color of video area:	#565656
Frame color:	#323232

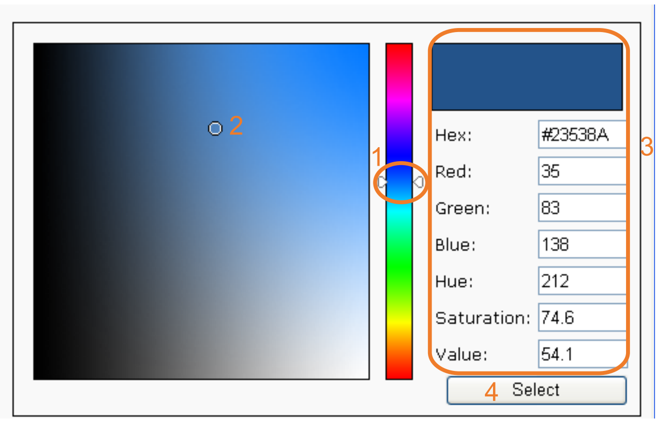
Color Selector

Custom Pattern

3. The palette window will pop up as shown below.



Hex:	#000000
Red:	0
Green:	0
Blue:	0
Hue:	0
Saturation:	0
Value:	0



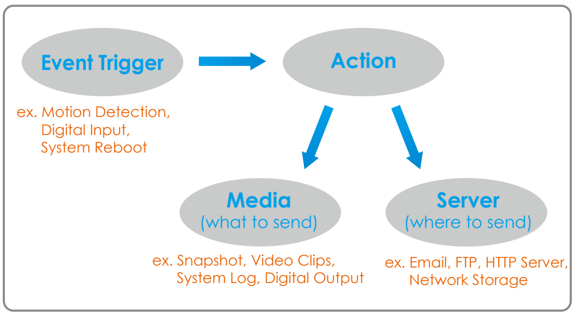
Hex:	#23538A
Red:	35
Green:	83
Blue:	138
Hue:	212
Saturation:	74.6
Value:	54.1

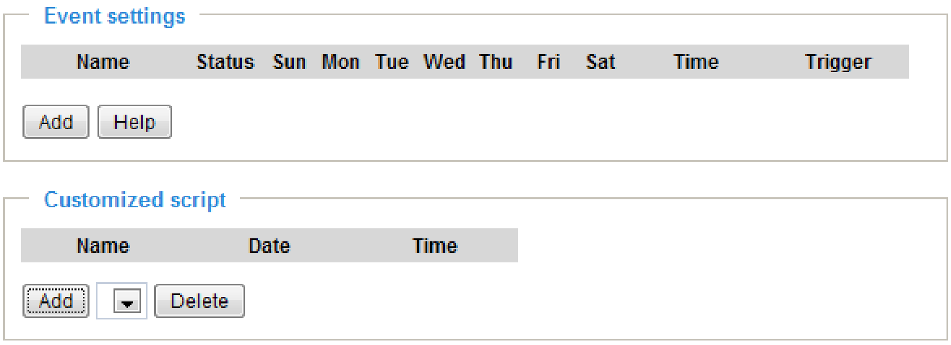
4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

Application Advanced Mode

This section explains how to configure the video server to respond to particular situations (event). A typical application is that when a motion is detected, the video server sends buffered images to an FTP server or e-mail address as notifications.

As illustrated on the right, an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action that will be performed. You can configure the video server to send snapshots or videos to your email address or FTP site.





Event settings

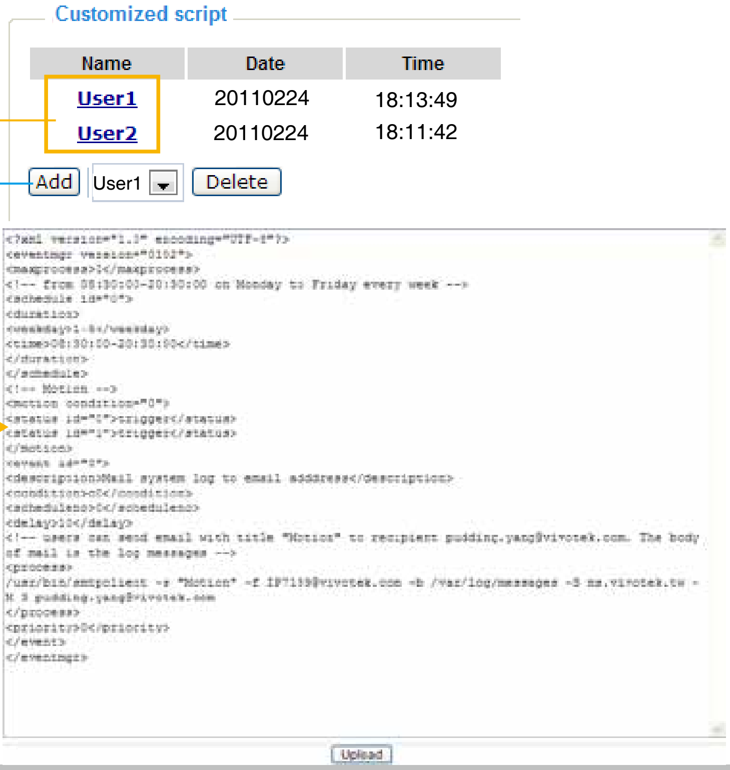
Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger

Customized script

Name	Date	Time

Customized script

This function allows you to upload a sample script (.xml file) to the webpage, which will save your time on configuring the settings. Please note that there is a limited number of customized scripts you can upload; if the current amount of customized scripts has reached the limit, an alert message will pop up. If you need more information, please contact VIVOTEK's technical support.



Customized script

Name	Date	Time
User1	20110224	18:13:49
User2	20110224	18:11:42

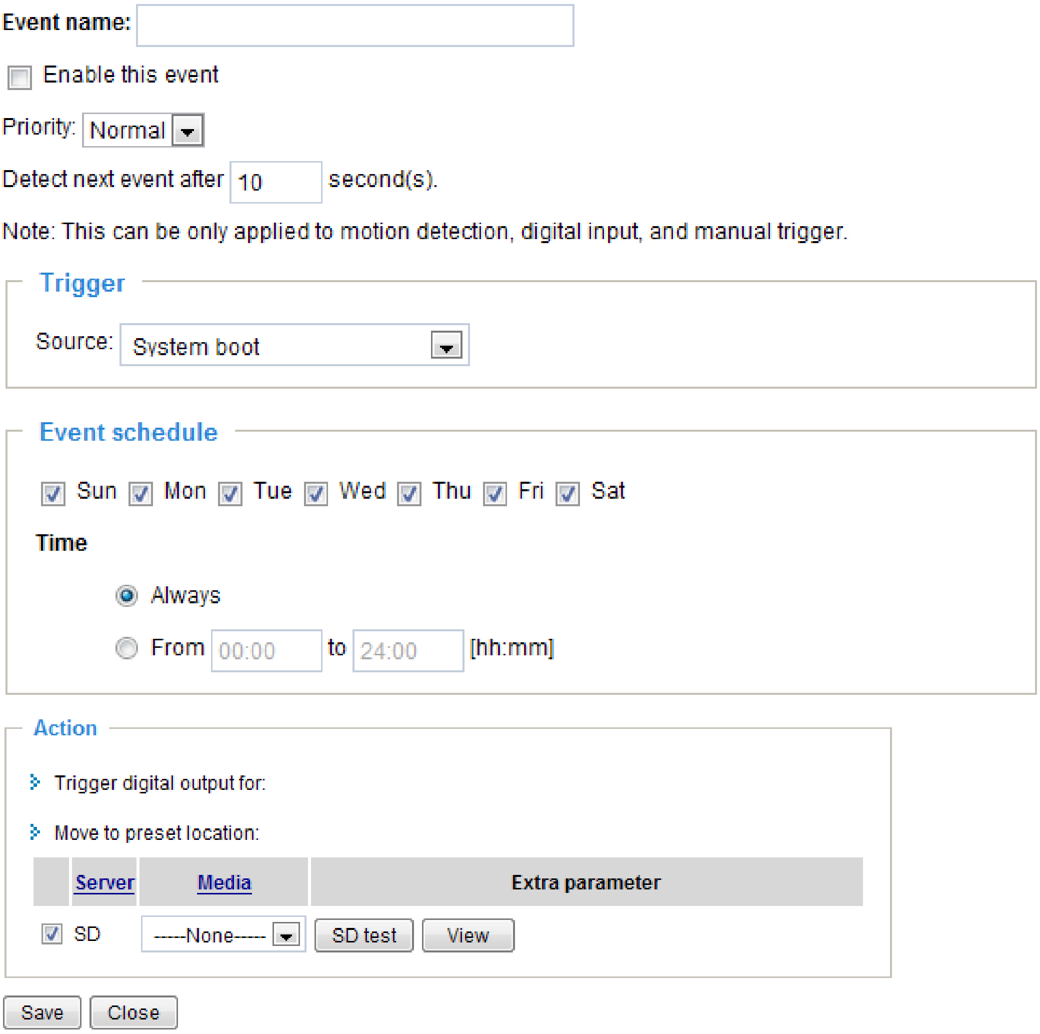
Click to upload a file

Click to modify the script online

```
<?xml version="1.0" encoding="UTF-8"?>
<eventmgr version="0102">
<maxprocess>1</maxprocess>
<!-- from 08:30:00-20:30:00 on Monday to Friday every week -->
<schedule id="0">
<duration>
<weekday>1-5</weekday>
<time>08:30:00-20:30:00</time>
</duration>
</schedule>
<!-- Motion -->
<motion condition="0">
<status id="0">trigger</status>
<status id="1">trigger</status>
</motion>
<event id="0">
<description>Mail system log to email address</description>
<condition>c0</condition>
<scheduleno>0</scheduleno>
<delay>10</delay>
<!-- users can send email with title "Motion" to recipient pudding.yang@vivotek.com. The body
of mail is the log messages -->
<process>
/usr/bin/smtpclient -s "Motion" -f IP7139@vivotek.com -b /var/log/messages -S ms.vivotek.tw -
M 3 pudding.yang@vivotek.com
</process>
<priority>0</priority>
</event>
</eventmgr>
```

Event settings

In the **Event settings** column, click **Add** to open the **Event settings** page. On this page, you can arrange three elements -- Trigger, Schedule, and Action to set an event. A total of 3 event settings can be configured.



Event name:

□ Enable this event

Priority: Normal

Detect next event after 10 second(s).

Note: This can be only applied to motion detection, digital input, and manual trigger.

Trigger

Source: System boot

Event schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

Action

Trigger digital output for:

Move to preset location:

	Server	Media	Extra parameter
☑	SD	-----None-----	SD test View

Event name: Enter a name for the event setting.

Enable this event: Select this option to enable the event setting.

Priority: Select the relative importance of this event (High, Normal, or Low). Events with a higher priority setting will be executed first.

Detect next event after □ seconds: Enter the duration in seconds to pause motion detection after a motion is detected.

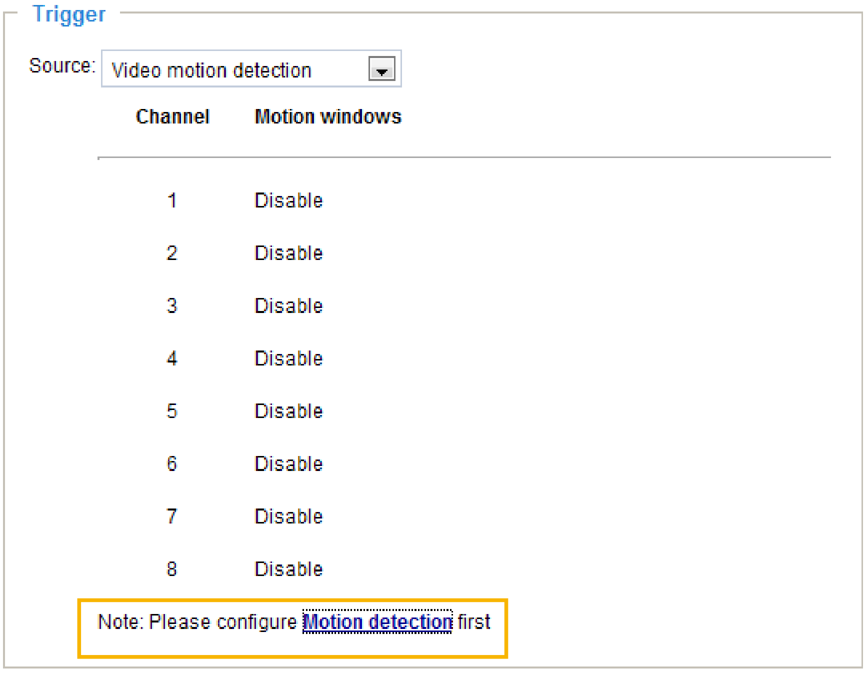
An event is an action initiated by a user-defined trigger source; it is the causal arrangement of the following three elements: Trigger, Event Schedule, and Action.

Trigger

This is the cause or stimulus which defines when to trigger the video server. The trigger source can be configured to use the video server's built-in motion detection mechanism or external digital input devices. There are several choices of trigger sources as shown below. Select the item to display the detailed configuration options.

- System boot
  This option triggers the video server when the power to the video server is disconnected.

- Video motion detection
  This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to **Motion detection** on page 65 for details.



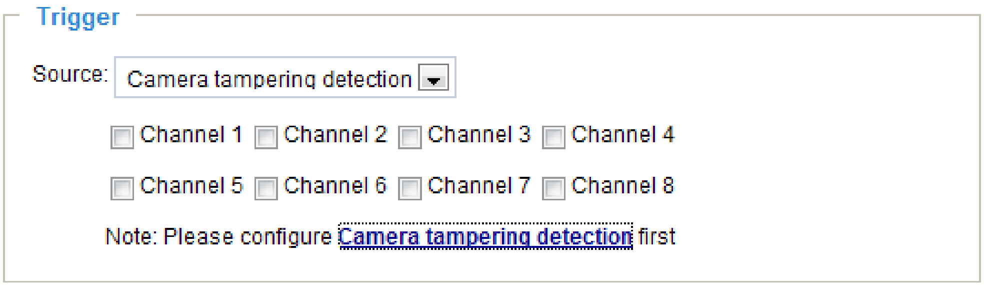
Trigger

Source: Video motion detection

Channel	Motion windows
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable

Note: Please configure Motion detection first

- Camera tampering detection
  This option allows the video server to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Camera tampering detection option first. Please refer to page 67 for detailed information.



Trigger

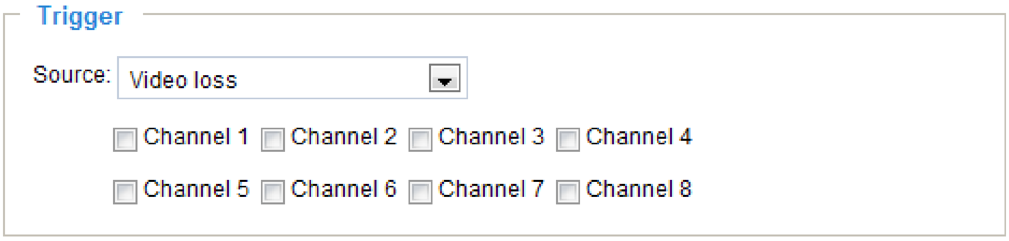
Source: Camera tampering detection

□ Channel 1 □ Channel 2 □ Channel 3 □ Channel 4

□ Channel 5 □ Channel 6 □ Channel 7 □ Channel 8

Note: Please configure Camera tampering detection first

- Video loss
  This option triggers the video server when the transmitted media files are missing. Check to enable the trigger source.



Trigger

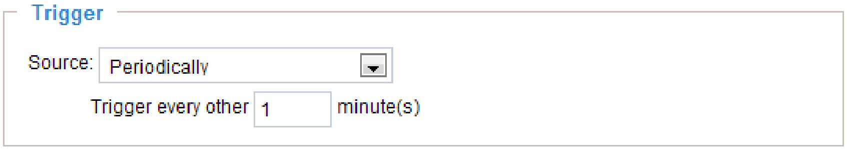
Source: Video loss

□ Channel 1 □ Channel 2 □ Channel 3 □ Channel 4

□ Channel 5 □ Channel 6 □ Channel 7 □ Channel 8

- Video restore
  This option triggers the video server when the camera starts to transmit video files.

- Periodically
  This option allows the video server to trigger periodically for every other defined minute. Up to 999 minutes are allowed.

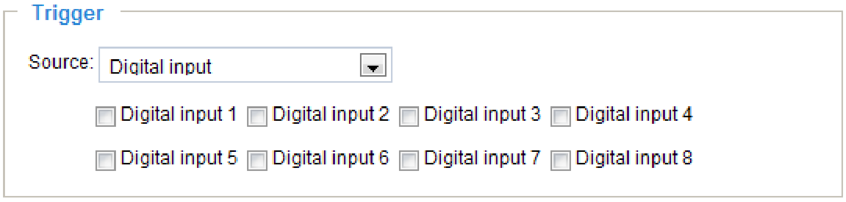


Trigger

Source: Periodically

Trigger every other 1 minute(s)

- Digital input
  This option allows the video server to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices of digital input devices on the market which helps to detect changes in temperature, vibration, sound, and light, etc.



Trigger

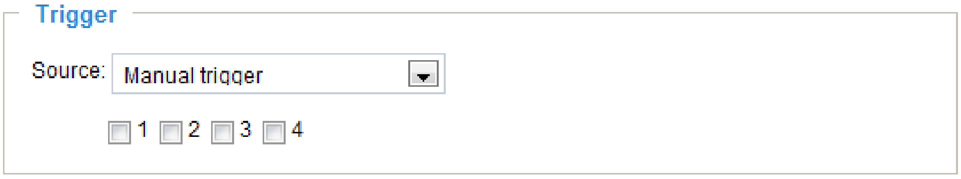
Source: Digital input

□ Digital input 1 □ Digital input 2 □ Digital input 3 □ Digital input 4

□ Digital input 5 □ Digital input 6 □ Digital input 7 □ Digital input 8

- Recording notify
  This option allows the video server to trigger when the recording disk is full or when recording starts to rewrite older data.

- Manual trigger
  This option allows user to enable event triggers manually by clicking the on/off button on the homepage. Please configure 1 ~ 3 events before using this function.



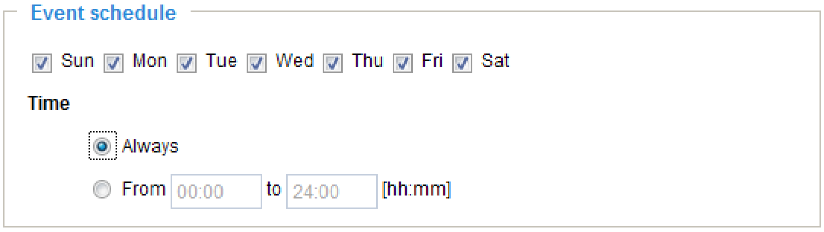
Trigger

Source: Manual trigger

□ 1 □ 2 □ 3 □ 4

Event Schedule

Specify the period for the event.



Event schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

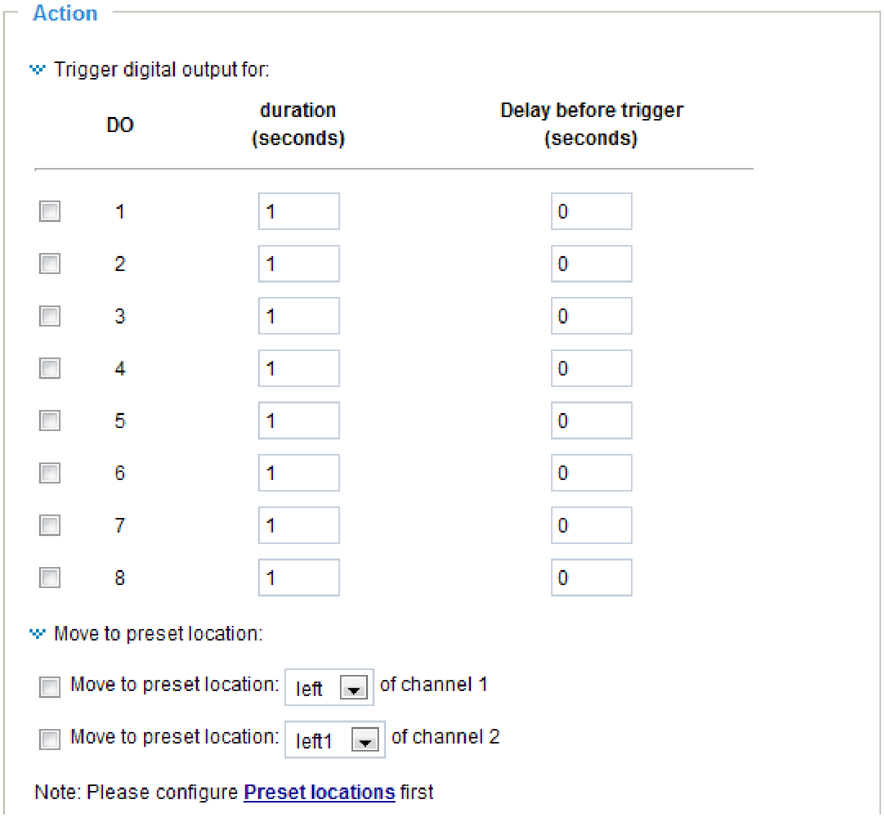
○ From 00:00 to 24:00 [hh:mm]

- Select the days of the week.

- Select the recording schedule in 24-hr time format.

Action

Define the actions to be performed by the video server when a trigger is activated.



Action

Trigger digital output for:

	DO	duration (seconds)	Delay before trigger (seconds)
□	1	1	0
□	2	1	0
□	3	1	0
□	4	1	0
□	5	1	0
□	6	1	0
□	7	1	0
□	8	1	0

Move to preset location:

□ Move to preset location: left of channel 1

□ Move to preset location: left1 of channel 2

Note: Please configure Preset locations first

- Trigger digital output for □ seconds

  Check the desired DO to turn on the external digital output device when a trigger is activated. Specify the length (seconds) of the trigger interval in the text box.

- Delay the trigger for □ seconds

  Check the desired DO to turn on the external digital output device when a trigger is activated. Specify the length (seconds) of the delay for the trigger after the event has been detected.

- Move to preset location

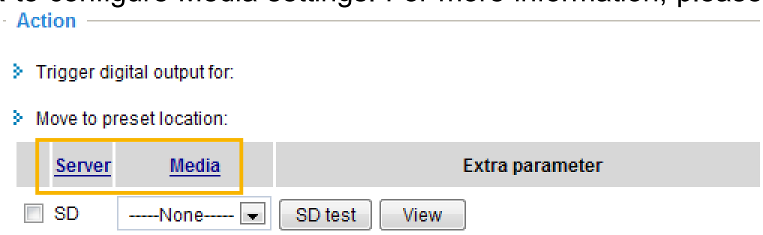
  Select this option, the Network Camera will move to the preset location when a trigger is activated. Please setup the preset locations first. You can setup more preset locations for each channel (Network Camera) by clicking on **Preset locations**. To know more details about preset locations settings please refer to page 69.

To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the video server will know what action to take (such as which server to send the media files to) when a trigger is activated.

- Server / Media

  Click **Server** to configure Server settings. For more information, please refer to Server settings on page 85.

  Click **Media** to configure Media settings. For more information, please refer to Media settings on page 88.



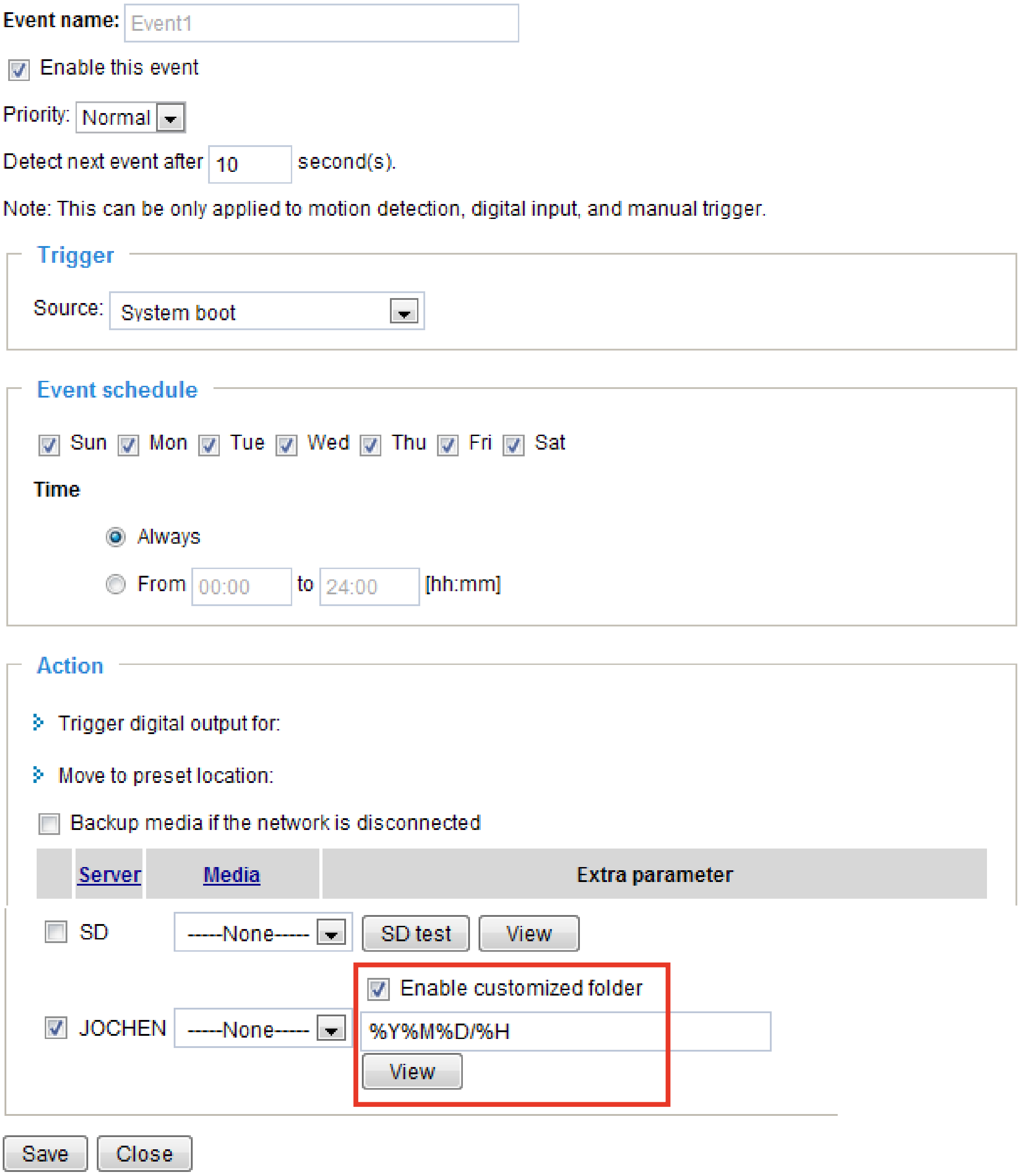
Action

Trigger digital output for:

Move to preset location:

Server	Media	Extra parameter
□ SD	-----None-----	SD test View

Here is an example of the Event settings page:



Event name: Event1

☑ Enable this event

Priority: Normal

Detect next event after 10 second(s).

Note: This can be only applied to motion detection, digital input, and manual trigger.

Trigger

Source: System boot

Event schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

Action

Trigger digital output for:

Move to preset location:

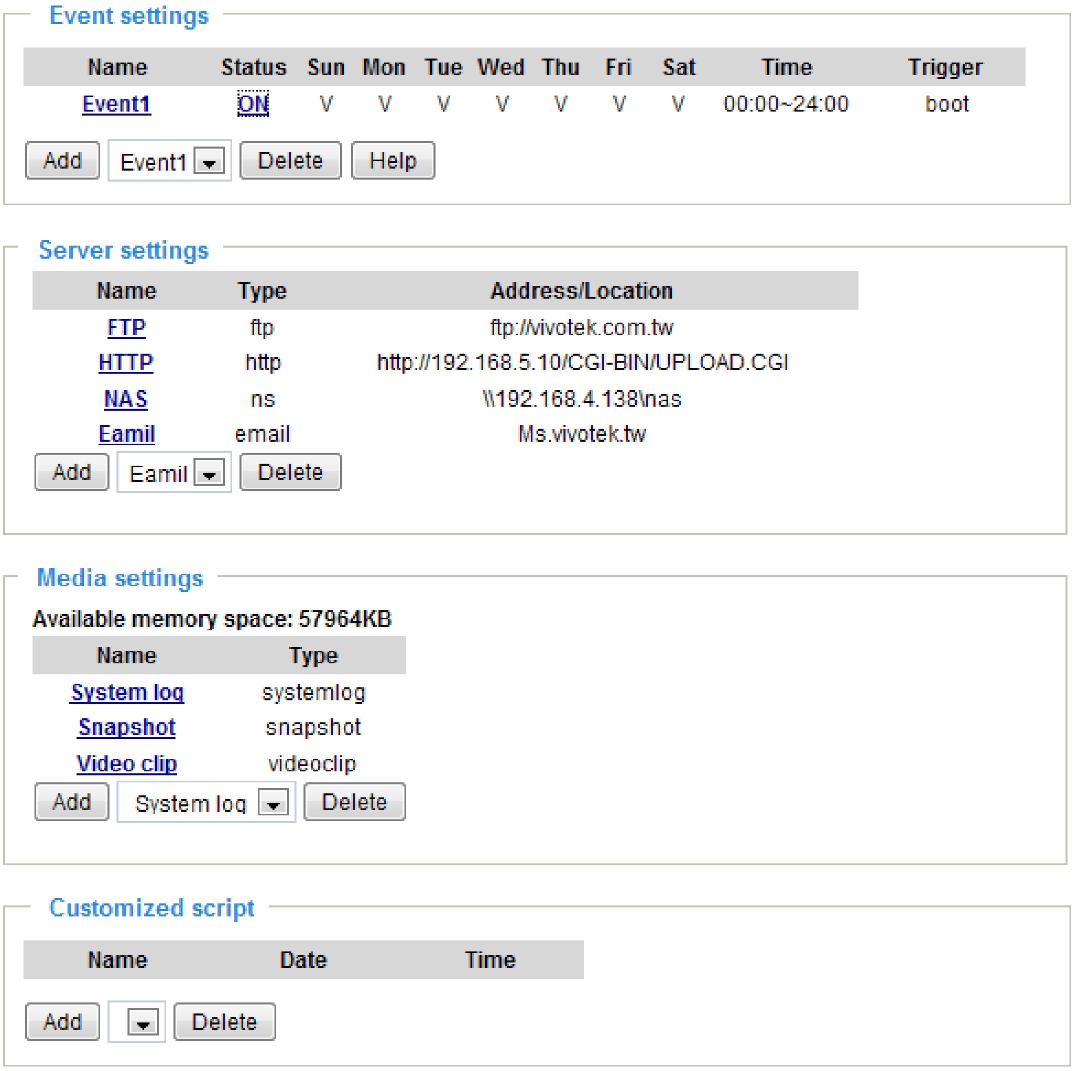
□ Backup media if the network is disconnected

	Server	Media	Extra parameter
□	SD	-----None-----	SD test View
☑	JOCHEN	-----None-----	☑ Enable customized folder %Y%M%D/%H View

When completed, click **Save** to enable the settings and click **Close** to exit Event Settings page. The new Event settings / Server settings / Media settings will appear in the event drop-down list on the Application page.

SD Test: If you have an SD card, click the button to test the availability. Your camera will display a message indicating a success or failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 109 for more information.

Here is an example of the Application page with an event setting:



Event settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger
Event1	ON	V	V	V	V	V	V	V	00:00~24:00	boot

Server settings

Name	Type	Address/Location
FTP	ftp	ftp://vivotek.com.tw
HTTP	http	http://192.168.5.10/CGI-BIN/UPLOAD.CGI
NAS	ns	\\192.168.4.138\nas
Eamil	email	Ms.vivotek.tw

Media settings

Available memory space: 57964KB

Name	Type
System log	systemlog
Snapshot	snapshot
Video clip	videoclip

Customized script

Name	Date	Time

When the Event Status is ON, once an event is triggered by motion detection, the video server will automatically send snapshots via e-mail.

If you want to stop the event trigger, you can click ON to turn it to OFF status or click **Delete** to remove the event setting.

To remove a server setting from the list, select a server name from the drop-down list and click **Delete**. Note that only when the server setting is not being applied to an event setting can it be deleted.

To remove a media setting from the list, select a media name from the drop-down list and click **Delete**. Note that only when the media setting is not being applied to an event setting can it be deleted.

Server settings

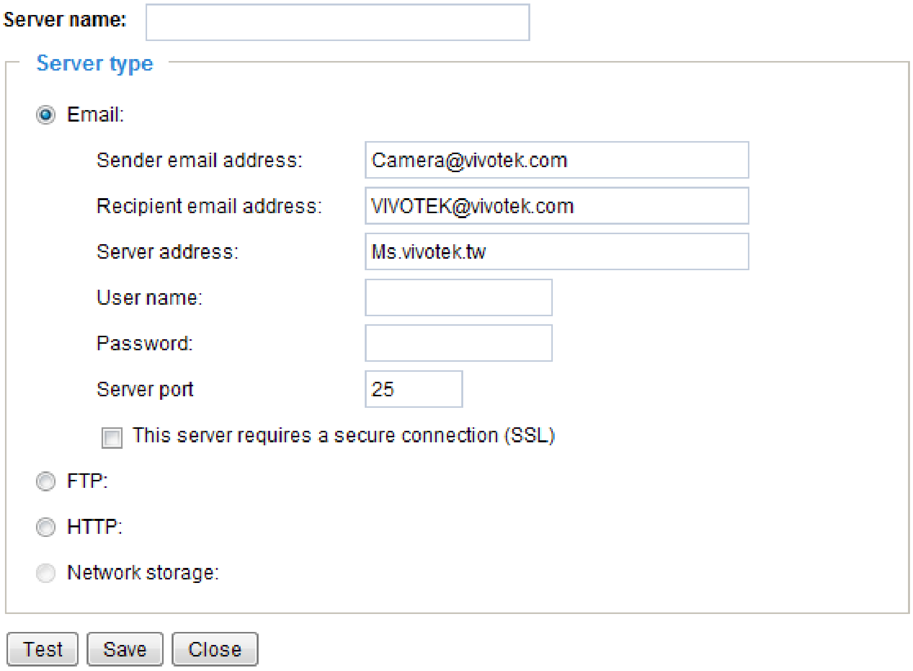
Click **Server** on Event Settings page to open the Server Setting page. On this page, you can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

Server name: Enter a name for the server setting.

Server type

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item to display the detailed configuration options. You can configure either one or all of them.

Email: Select to send the media files via email when a trigger is activated.



Server name:

Server type

● Email:

Sender email address: Camera@vivotek.com

Recipient email address: VIVOTEK@vivotek.com

Server address: Ms.vivotek.tw

User name:

Password:

Server port 25

□ This server requires a secure connection (SSL)

○ FTP:

○ HTTP:

○ Network storage:

■ Sender email address: Enter the email address of the sender.

■ Recipient email address: Enter the email address of the recipient.

■ Server address: Enter the domain name or IP address of the email server.

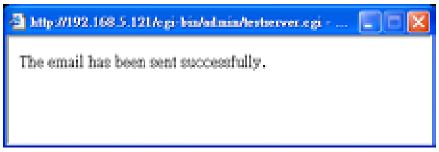
■ User name: Enter the user name of the email account if necessary.

■ Password: Enter the password of the email account if necessary.

■ Server port: The default mail server port is set to 25. You can also manually set another port.

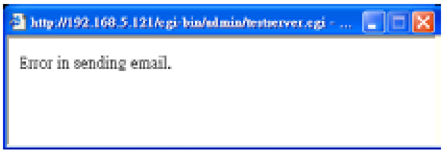
If your SMTP server requires a secure connection (SSL), check **This server requires a secure connection (SSL).**

To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will also receive an email indicating the result.



http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

The email has been sent successfully.

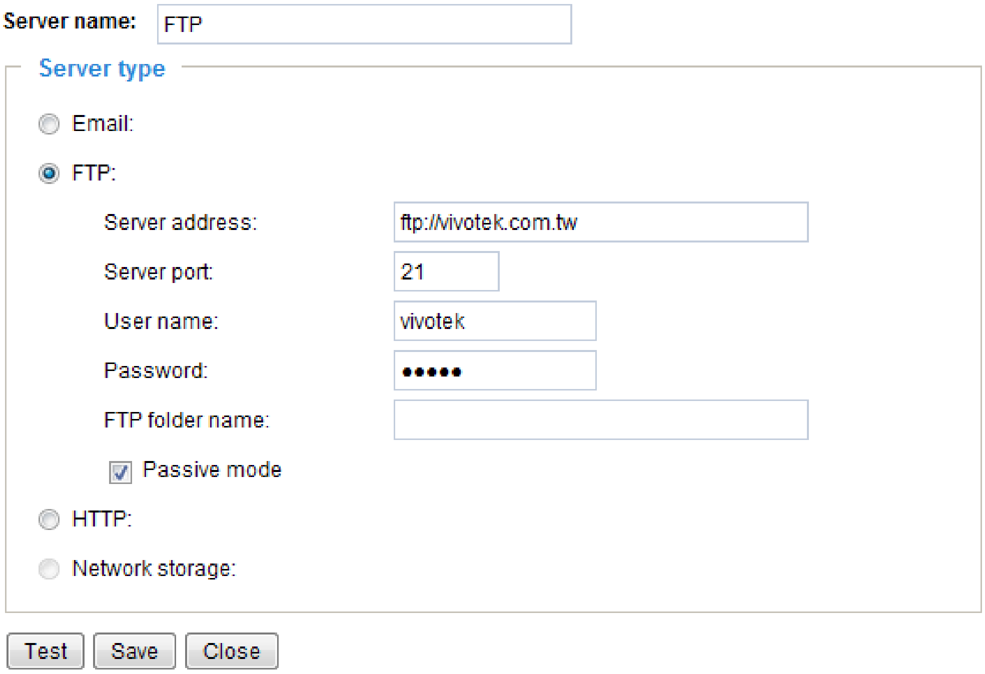


http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

Error in sending email.

Click **Save** to enable the settings, then click **Close** to exit the page.

FTP: Select to send the media files to an FTP server when a trigger is activated.



Server name: FTP

Server type

○ Email:

● FTP:

Server address: ftp://vivotek.com.tw

Server port: 21

User name: vivotek

Password: •••••

FTP folder name:

☑ Passive mode

○ HTTP:

○ Network storage:

■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port
By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.

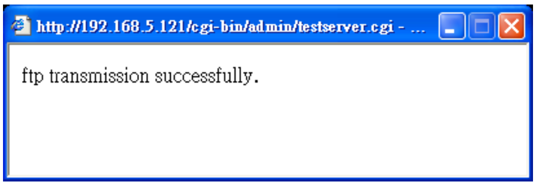
■ User name: Enter the login name of the FTP account.

■ Password: Enter the password of the FTP account.

■ FTP folder name
Enter the folder where the media file will be placed. If the folder name does not exist, the video server will create one on the FTP server.

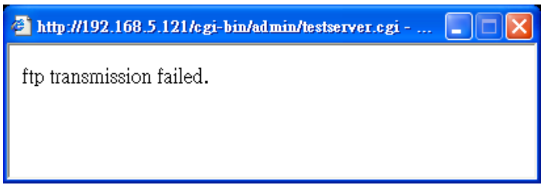
■ Passive mode
Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as shown below. If successful, you will also receive a test.txt file on the FTP server.



http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

ftp transmission successfully.

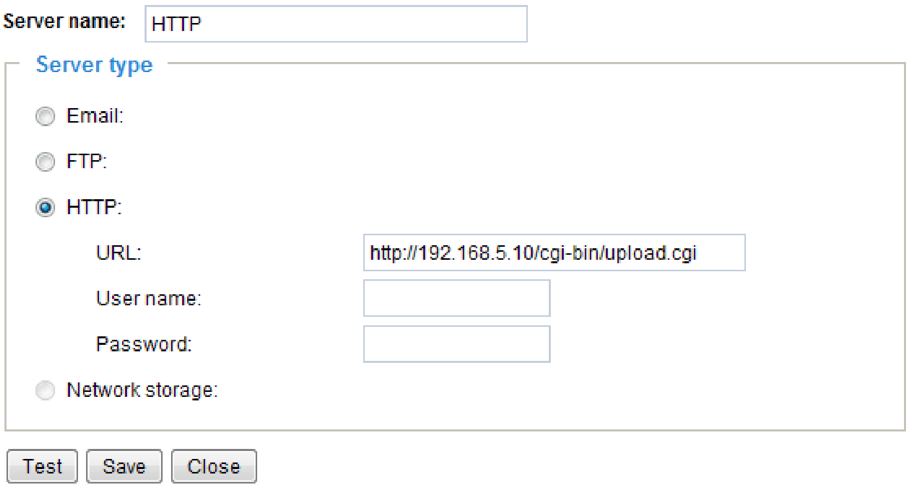


http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

ftp transmission failed.

Click **Save** to enable the settings, then click **Close** to exit the page.

HTTP: Select to send the media files to an HTTP server when a trigger is activated.



Server name: HTTP

Server type

○ Email:

○ FTP:

● HTTP:

URL: http://192.168.5.10/cgi-bin/upload.cgi

User name:

Password:

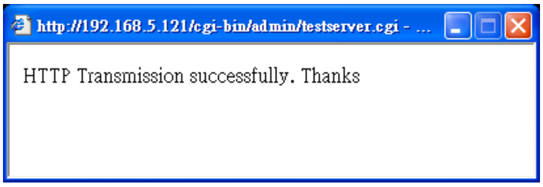
○ Network storage:

■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name if necessary.

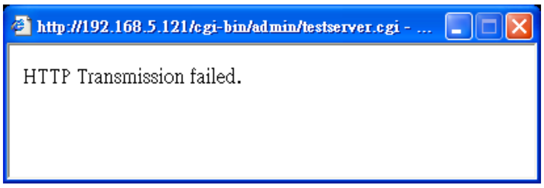
■ Password: Enter the password if necessary.

To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as below. If successful, you will receive a test.txt file on the HTTP server.



http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

HTTP Transmission successfully. Thanks

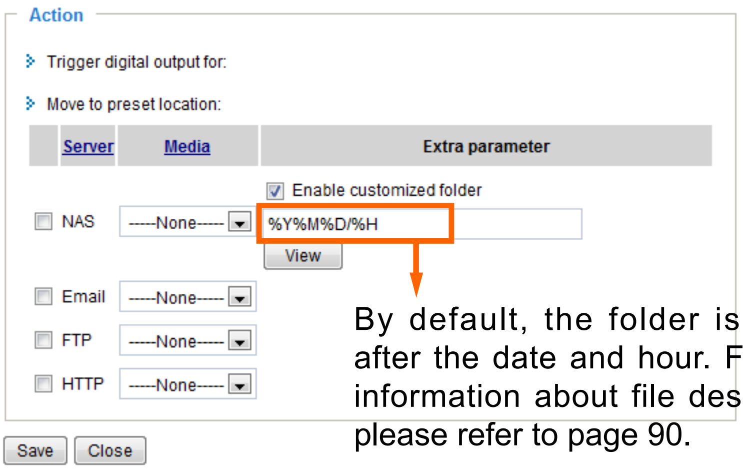


http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

HTTP Transmission failed.

Click **Save** to enable the settings, then click **Close** to exit the page.

When completed, the new server settings will automatically be displayed on the Event Settings page. For example:



Action

Trigger digital output for:

Move to preset location:

	Server	Media	Extra parameter
□	NAS	-----None-----	☑ Enable customized folder %Y%M%D/%H View
□	Email	-----None-----	
□	FTP	-----None-----	
□	HTTP	-----None-----	

By default, the folder is named after the date and hour. For more information about file destination, please refer to page 90.

NOTE:

► *By default, the folder is named after the date and hour; " %Y%M%D%H" refers to Year/ Month/Date/Hour. Your saved media files will be automatically classified in folders named after the date and hour, if you keep the default setting. You may also create the customized folder by any other desired name, but all media files will be saved in the same folder.*

Media settings

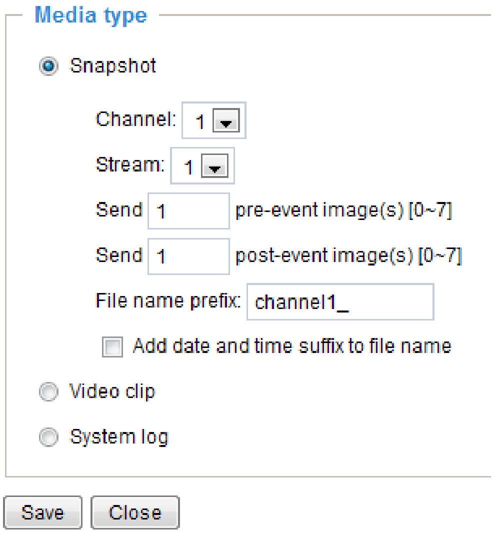
Click **Media** on the Event Settings page to open the Media Settings page. On this page, you can specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be configured.

<u>Media name</u>: Enter a name for the media setting.

Media type

There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.

<u>Snapshot</u>: Select to send snapshots when a trigger is activated.



Media type

● Snapshot

Channel: 1

Stream: 1

Send 1 pre-event image(s) [0~7]

Send 1 post-event image(s) [0~7]

File name prefix: channel1_

□ Add date and time suffix to file name

○ Video clip

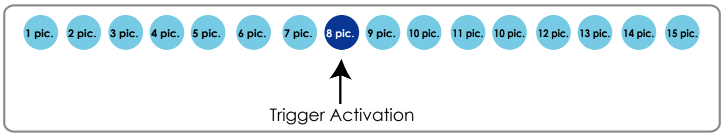
○ System log

■ Channel: Select to take snapshots from stream 1 ~ 4.

■ Send □ pre-event images
The video server has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

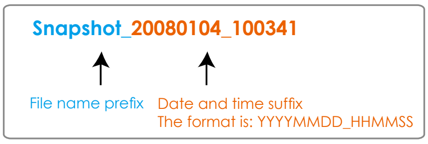
■ Send □ post-event images
Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images are generated after a trigger is activated.



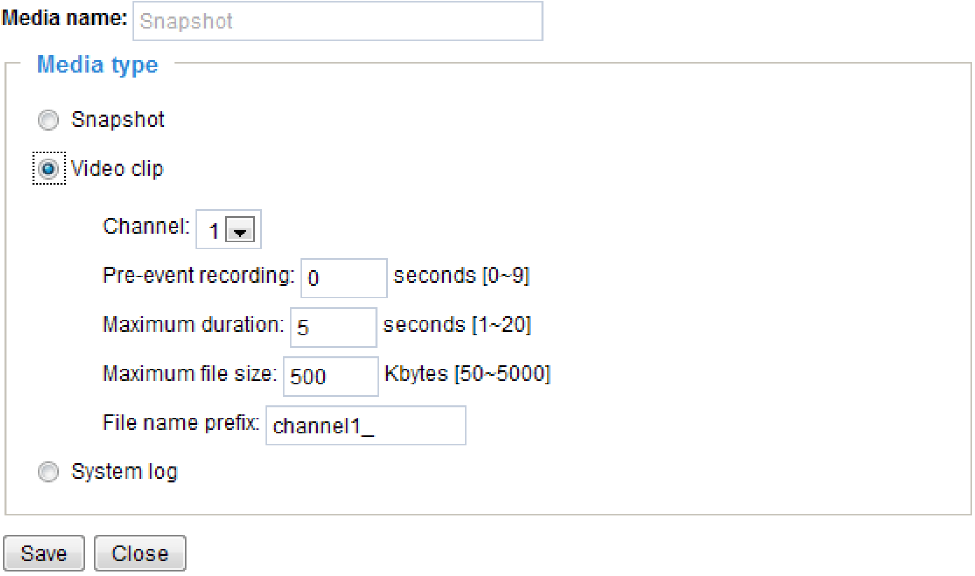
■ File name prefix
Enter the text that will be appended to the front of the file name.

■ Add date and time suffix to the file name
Select this option to add a date/time suffix to the file name.
For example:



Click **Save** to enable the settings, then click **Close** to exit the page.

Video clip: Select to send video clips when a trigger is activated.



Media name: Snapshot

Media type

○ Snapshot

● Video clip

Channel: 1

Pre-event recording: 0 seconds [0~9]

Maximum duration: 5 seconds [1~20]

Maximum file size: 500 Kbytes [50~5000]

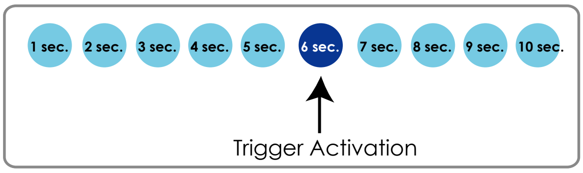
File name prefix: channel1_

○ System log

■ Channel: The video source. The stream source will be identical to the preset time shift caching stream. For more information about time shift caching stream, please refer to page 57.

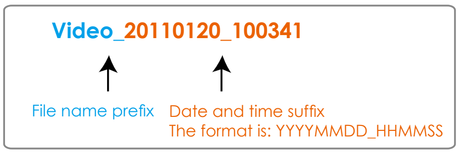
■ Pre-event recording
The video server has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

■ Maximum duration
Specify the maximum recording duration in seconds. Up to 10 seconds can be set.
For example, if pre-event recording is set to five seconds and the maximum duration is set to ten seconds, the video server continues to record for another 4 seconds after a trigger is activated.



■ Maximum file size
Specify the maximum file size allowed.

■ File name prefix
Enter the text that will be appended to the front of the file name.
For example:

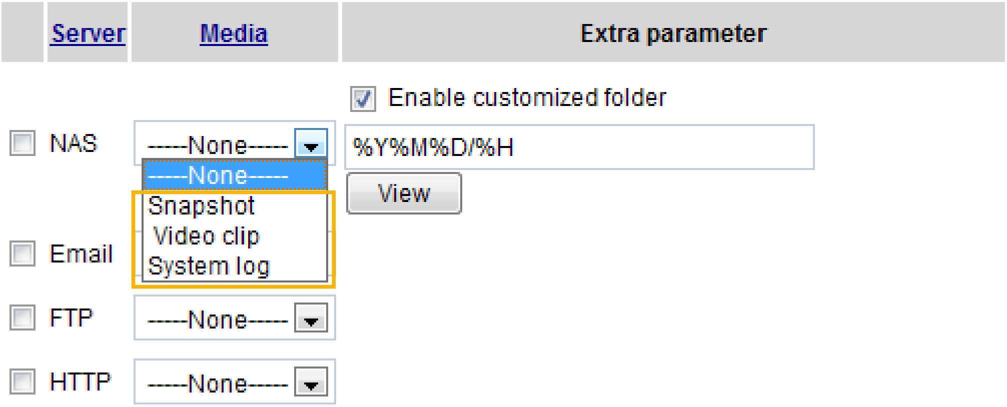


Click **Save** to enable the settings, then click **Close** to exit the page.

System log: Select to send a system log when a trigger is activated.
Click **Save** to enable the settings, then click **Close** to exit the page.

When completed, click **Save** to enable the settings and click **Close** to exit this page. The new media settings will appear on the Event settings page.

You can continue to select a server and media type for the event. Please go back to page 79 for detailed information.

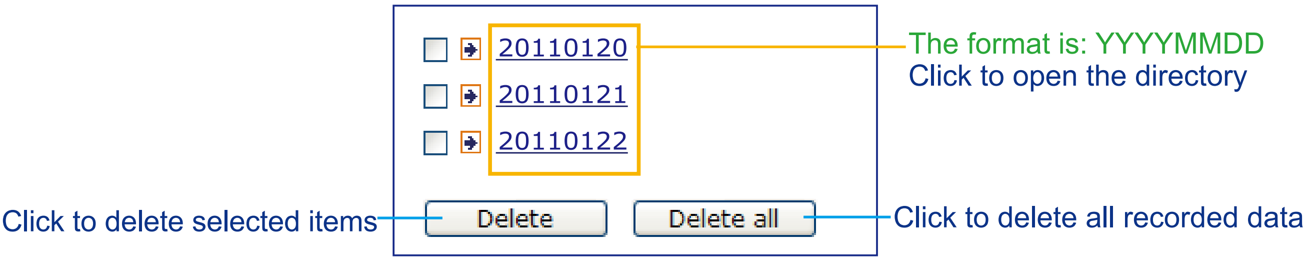


■ Enable customized folder: Create folders by date, time, and hour automatically: If you check this item, the system will generate folders automatically by date.

■ View: Click this button to open a file list window. This function is only for **Network Storage (NAS)** and **SD/SDHC** card.

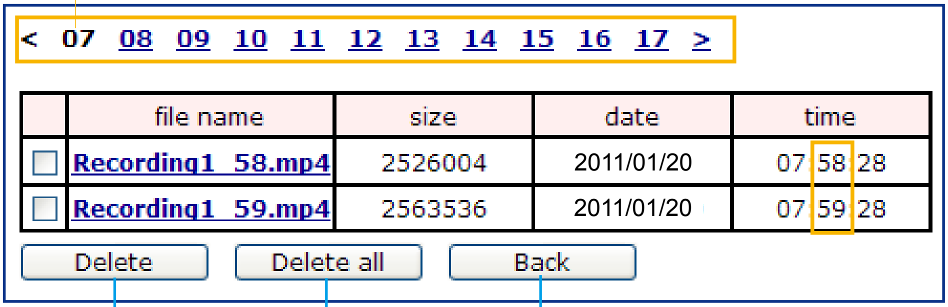
If you click the **View** button of Network storage, a **file directory window** will pop up for you to view recorded data on Network storage.

The following is an example of a file destination with video clips:


□ 20110120
□ 20110121
□ 20110122
Delete
Delete all
The format is: YYYYMMDD
Click to open the directory
Click to delete selected items
Click to delete all recorded data

Click 20110120 to open the directory:

The format is: HH (24r)
Click to open the file list for that hour



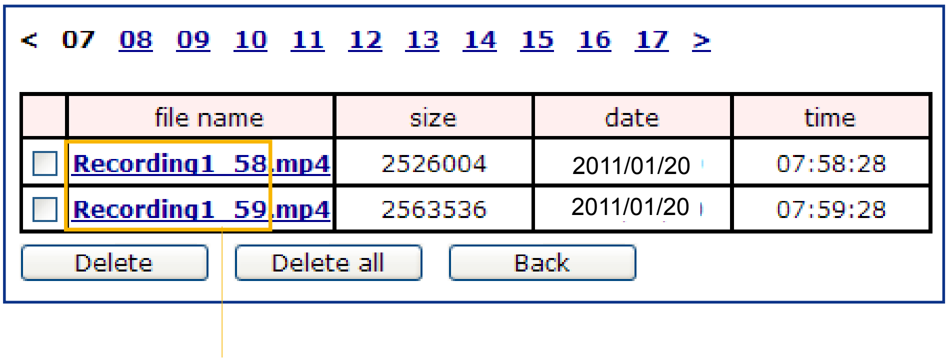
< 07 08 09 10 11 12 13 14 15 16 17 >

	file name	size	date	time
□	Recording1_58.mp4	2526004	2011/01/20	07:58:28
□	Recording1_59.mp4	2563536	2011/01/20	07:59:28

Click to delete selected items

Click to go back to the previous level of the directory

Click to delete all recorded data



< 07 08 09 10 11 12 13 14 15 16 17 >

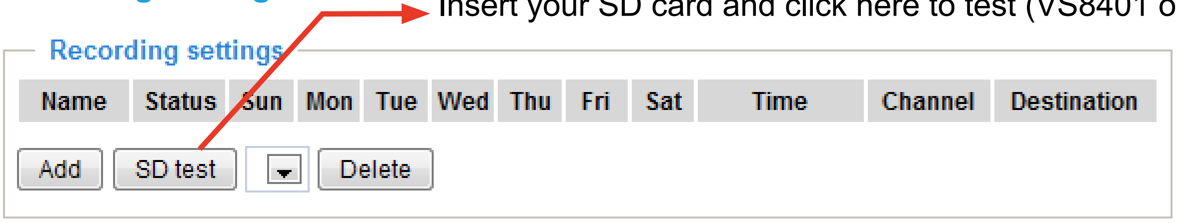
	file name	size	date	time
□	Recording1_58.mp4	2526004	2011/01/20	07:58:28
□	Recording1_59.mp4	2563536	2011/01/20	07:59:28

The format is: File name prefix + Minute (mm)
You can set up the file name prefix on Media Settings page.
Please refer to page 88 for detailed information.

Recording > Recording settings Advanced Mode

This section explains how to configure the recording settings for the Video Server.

Recording Settings



Insert your SD card and click here to test (VS8401 only)

Recording settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Channel	Destination

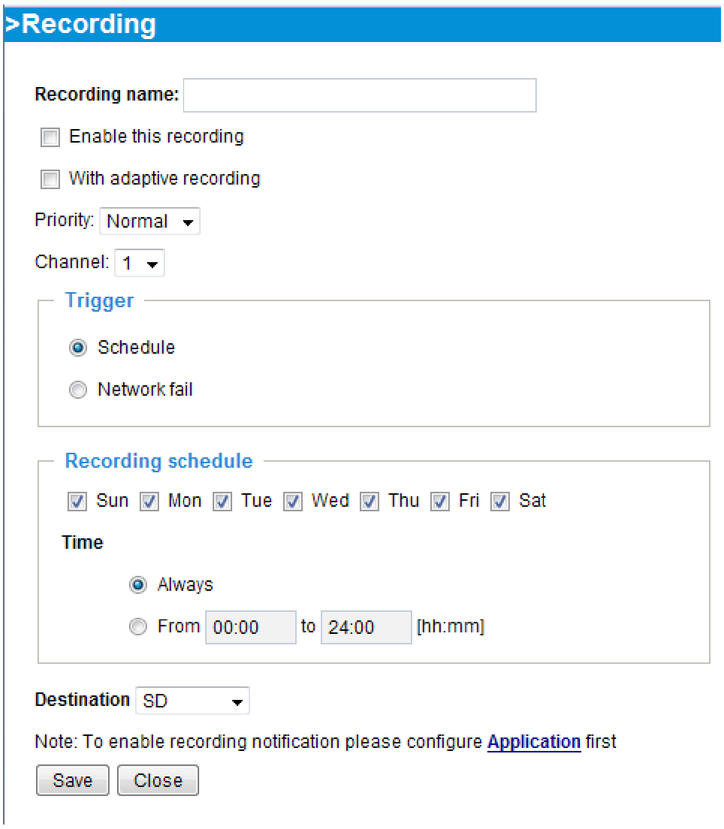
NOTE:

► *Please remember to format your SD card when using it for the first time. Please refer to page 109 for detailed information.*

► *The SD card storage option is only available on the VS8401.*

Recording Settings

Click **Add** to open the recording setting window. On this page, you can define the adaptive recording, recording sources, recording schedule, and recording capacity. A total of 2 recording settings can be configured.



>Recording

Recording name:

□ Enable this recording

□ With adaptive recording

Priority: Normal

Channel: 1

Trigger

● Schedule

○ Network fail

Recording schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

Destination SD

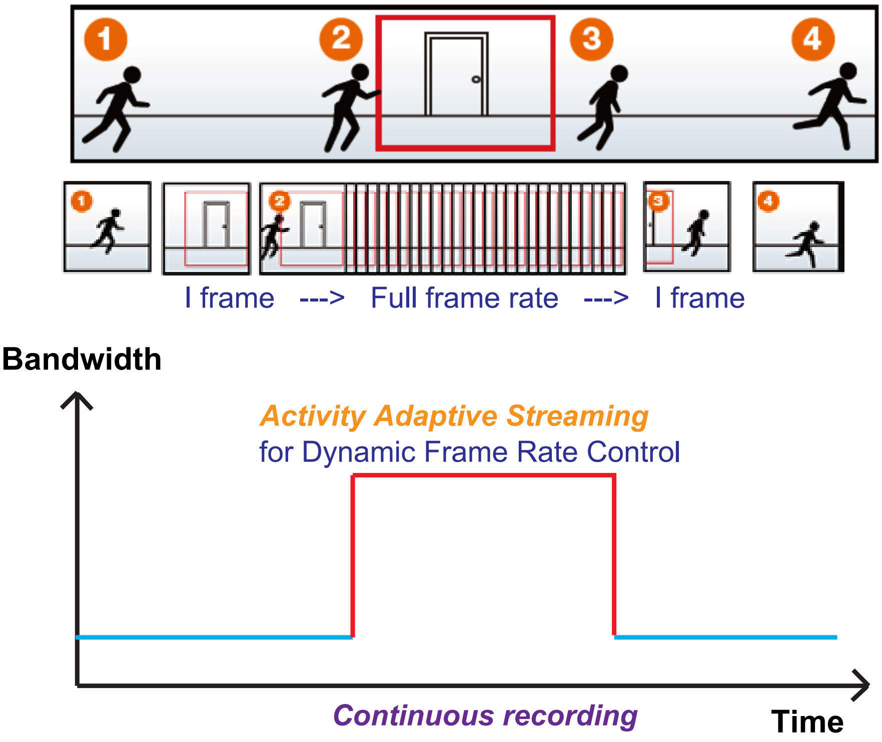
Note: To enable recording notification please configure Application first

■ Recording name: Enter a name for the recording setting.

■ Enable this recording: Select this option to enable video recording.

■ With adaptive recording:
Selecting this option will activate the frame rate control according to alarm trigger. The frame rate control means that when there is a triggered alarm, the frame rate will raise up to the value you've set on Stream setting page. Please refer to page 53 for more information.

If you enalbe the **adaptive recording** and enable time-shift cache stream on Camera A, only when an event takes place on Camera A will the server records the streaming data at the full frame rate. This methodology only requires transferring the Intra frame data during normal operation, and full-frame-rate videos in the occurrences of events, and thus saving users of network bandwidth and storage space.


1
2
3
4
I frame ---> Full frame rate ---> I frame
Bandwidth
Activity Adaptive Streaming
for Dynamic Frame Rate Control
Continuous recording
Time

The alarm trigger includes: motion detection and DI dection. Please refer to Event settings on page 87.

■ Pre-event recording and post-event recording:
The Video Server has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before and after a trigger is activated.

■ Priority: Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.

■ Source: Select a stream as the recording source.

NOTE:

▶ *To enable adaptive recording, please make sure you have setup the triggering sources such as Motion Detection, DI devices, or Manual Triggers.*

▶ *When there is no alarm trigger:*
- JPEG mode: records 1 frame per second.
- H.264 mode: record one I frame only.
- MPEG-4mation.

▶ *When the I frame period is <1s on Video settings page, it should be forced to make the I frame period to 1s when adaptive recording is activated.*

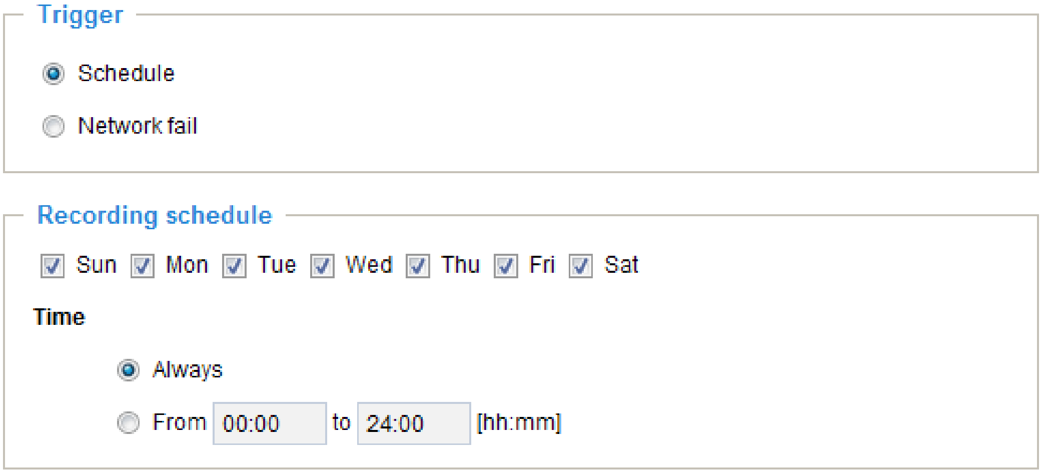
▶ *To enable adaptive recording, please also **enable time shift caching stream** and **select a caching stream** on page 56, **Audio and Video** settings.*

▶ *To enable recording notification please configure **Event Settings** first. Please refer to page 79.*

Please follow steps 1 to 2 below to set up a recording setting:

1. Trigger

Select a triggering condition: For example, event triggers might not make sense in a place full of human traffic during the office hours. You may want to enable the triggering conditions during the night.



Trigger

● Schedule

○ Network fail

Recording schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

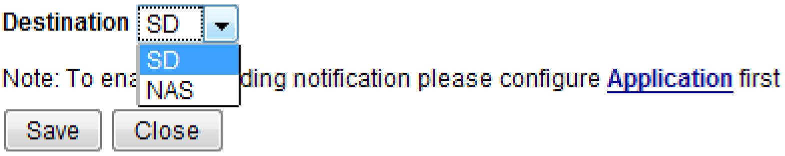
○ From 00:00 to 24:00 [hh:mm]

■ Schedule: The server to start recording files onto local storage or networked storage (NAS).

■ Network fail: Starts recording to the local storage (SD card) in the event of network failures.

2. Destination

You can either select an SD card or a networked storage (NAS) to store the recorded videos.

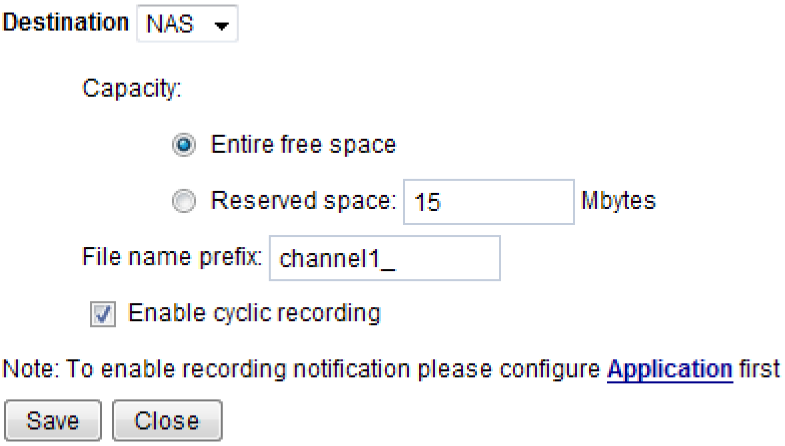


Destination SD

Note: To ena ding notification please configure Application first

To add a NAS server, move to the Application > Event > and Add Event setting page. Please note that only one NAS server can be configured as the recording destination.

If you have selected a NAS server as the recording destination, you should configure the following options: **Capacity**, **File name prefix**, and **Cyclic recording**.



Destination NAS

Capacity:

● Entire free space

○ Reserved space: 15 Mbytes

File name prefix: channel1_

☑ Enable cyclic recording

Note: To enable recording notification please configure Application first

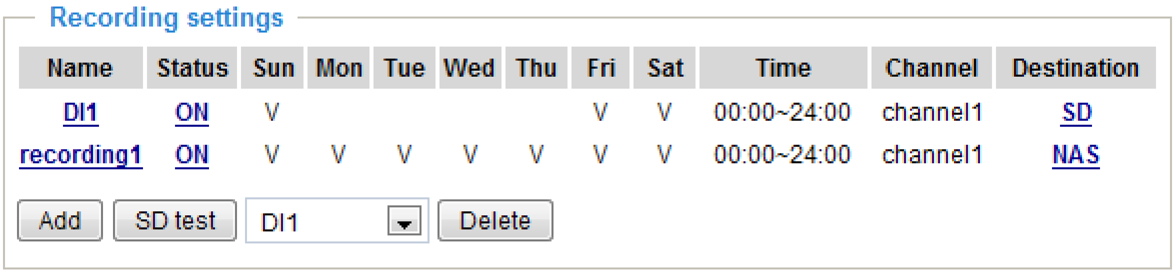
- Capacity: You can select either the entire storage space available or specify a reserved space. The recording size limit must be larger than the reserved space for cyclic recording. The reserved space is used for cyclic recording to prevent malfunctions that might occur during the transaction stage when the video feeds are about to fill up the storage space. This value must be larger than 15 MBytes.

- File name prefix: Enter the text that will be appended to the front of the file name.

- Enable cyclic recording: If your check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest ones.

If you want to enable recording notification, please refer to **Event** > **Event Settings** on page 79 for more details.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit. When the system begins recording, it will send the recorded files to the networked storage or SD card. The new recording configuration will appear on the recording page as shown below. To move a configured setting, click on the **Delete** button.



Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Channel	Destination
DI1	ON	V					V	V	00:00~24:00	channel1	SD
recording1	ON	V	V	V	V	V	V	V	00:00~24:00	channel1	NAS

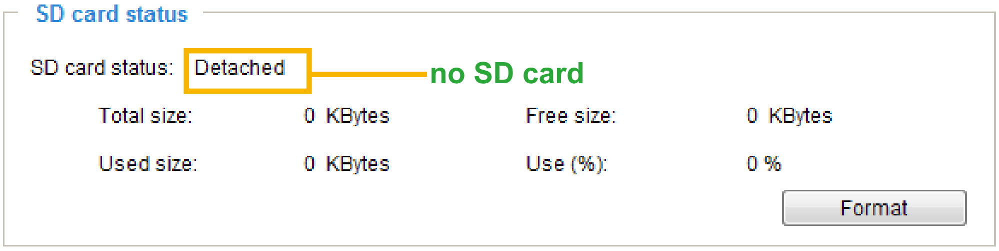
Below are legends on the Recording Settings page:
Name: Click to open and edit an existing configuration.
ON (Status): Click to enable or disable the recording task.
NAS or **SD**: Click to open the file list produced by the recording tasks. For more information about folder naming, please refer to page 90 for details. A file list window will prompt showing previously recorded files.

Local storage > SD card management (for VS8401 only)

This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, and implement SD card control.

SD card staus

This column shows the status and reserved space of your SD card. Please remember to format the SD card when using for the first time.

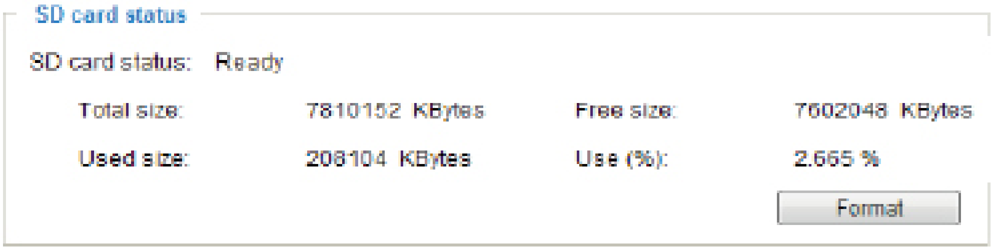


SD card status

SD card status: Detached

no SD card

Total size:	0 KBytes	Free size:	0 KBytes
Used size:	0 KBytes	Use (%):	0 %

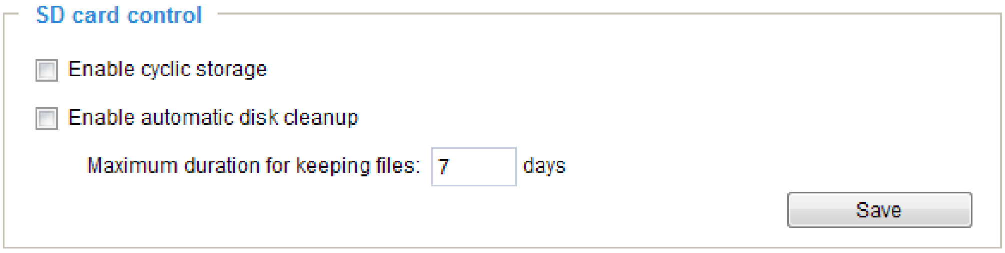


SD card status

SD card status: Ready

Total size:	7810152 KBytes	Free size:	7602048 KBytes
Used size:	208104 KBytes	Use (%):	2.665 %

SD card control



SD card control

□ Enable cyclic storage

□ Enable automatic disk cleanup

Maximum duration for keeping files: 7 days

- Enable cyclic storage: Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.

- Enable automatic disk cleanup: Check this item and enter the number of days you wish to retain a file. For example, if you enter “7 days”, the recorded files will be stored on the SD card for 7 days.

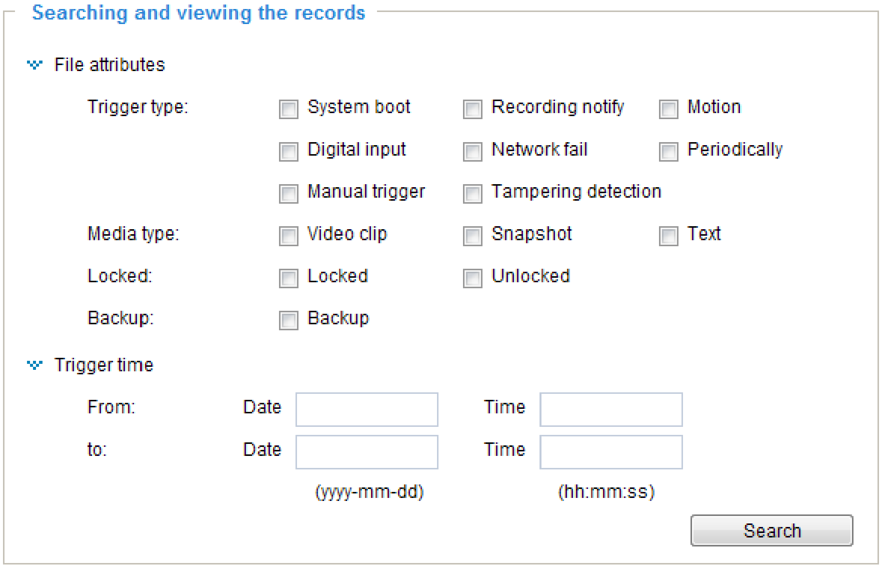
When all settings are completed, click **Save** to enable your settings.

Local storage > Content management

This section explains how to manage the content of recorded videos on the Network Camera. Here you can search and view the records and view the searched results.

Searching and Viewing the Records

This column allows the user to set up search criteria for recorded data. If you do not select any criteria and click **Search** button, all recorded data will be listed in the **Search Results** cloumn.



Searching and viewing the records

File attributes

Trigger type: □ System boot □ Recording notify □ Motion □ Digital input □ Network fail □ Periodically □ Manual trigger □ Tampering detection

Media type: □ Video clip □ Snapshot □ Text

Locked: □ Locked □ Unlocked

Backup: □ Backup

Trigger time

From: Date ____ Time ____

to: Date ____ Time ____

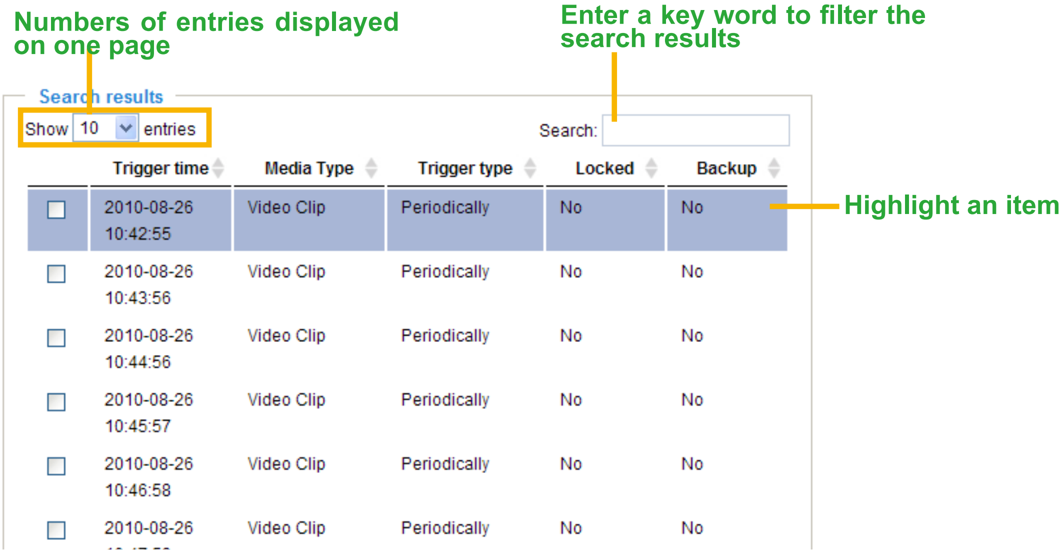
(yyyy-mm-dd) (hh:mm:ss)

■ File attributes: Select one or more items as your search criteria.
■ Trigger time: Manually enter the time range you want to search.

Click **Search** and the recorded data corresponding to the search criteria will be listed in **Search Results** window.

Search Results

The following is an example of search results. There are four columns: Trigger time, Media type, Trigger type, and Locked. Click ⬍ to sort the search results in either direction.



Numbers of entries displayed on one page

Enter a key word to filter the search results

Highlight an item

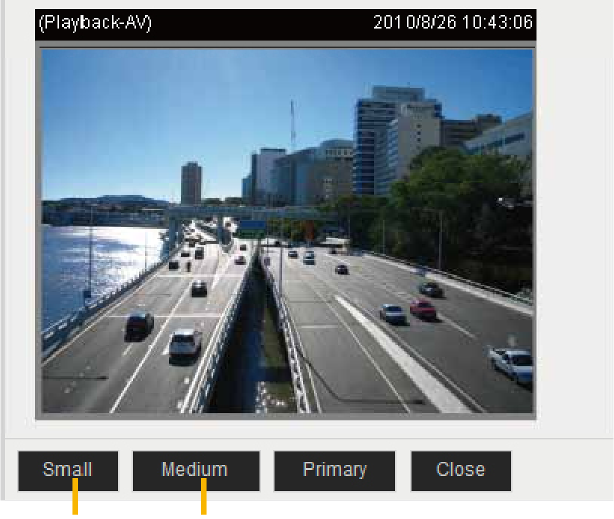
Search results

Show 10 entries

Search: ____

	Trigger time	Media Type	Trigger type	Locked	Backup
□	2010-08-26 10:42:55	Video Clip	Periodically	No	No
□	2010-08-26 10:43:56	Video Clip	Periodically	No	No
□	2010-08-26 10:44:56	Video Clip	Periodically	No	No
□	2010-08-26 10:45:57	Video Clip	Periodically	No	No
□	2010-08-26 10:46:58	Video Clip	Periodically	No	No
□	2010-08-26	Video Clip	Periodically	No	No

- View: Click on a search result which will highlight the selected item in purple as shown above. Click the **View** button and a media window will pop up to play back the selected file.
  For example:

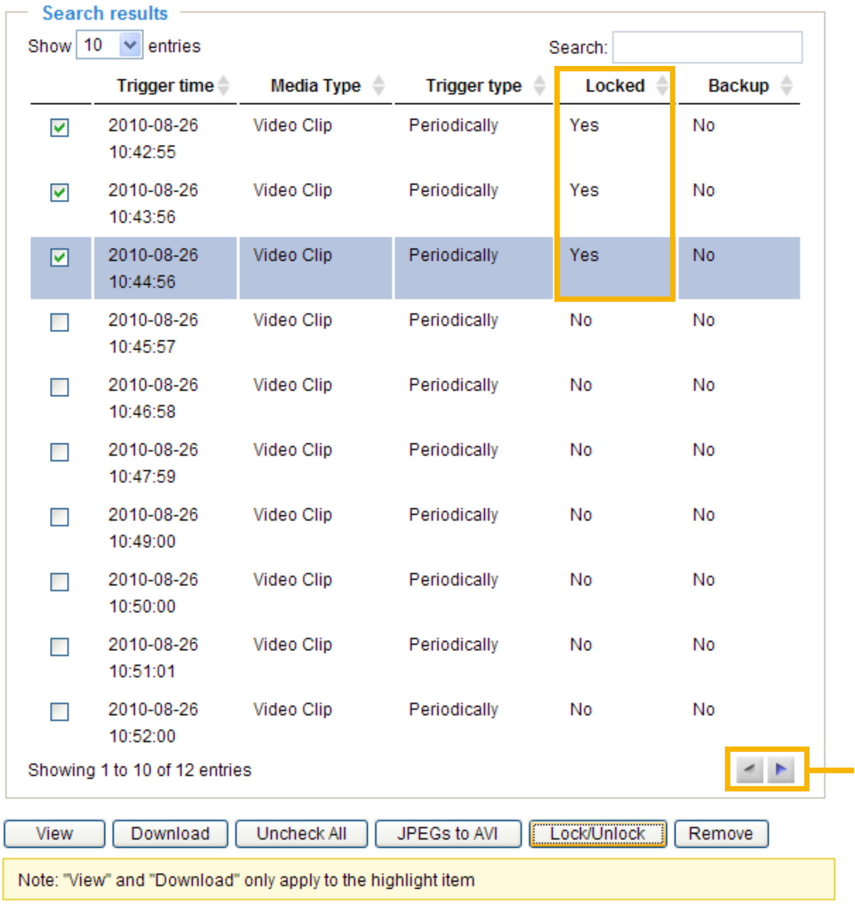


Click to adjust the image size

- Download: Click on a search result to highlight the selected item in purple as shown above. Then click the **Download** button and a file download window will pop up for you to save the file.

- JPEGs to AVI: This functions only applies to “JPEG“ format files such as snapshots. You can select several snapshots from the list, then click this button. Those snapshots will be converted into an AVI file.

- Lock/Unlock: Select the desired search results, then click this button. The selected items will become Locked, which will not be deleted during cyclic recoroding. You can click again to unlock the selections.
  For example:



Search results

Show 10 entries

Search:

	Trigger time	Media Type	Trigger type	Locked	Backup
☑	2010-08-26 10:42:55	Video Clip	Periodically	Yes	No
☑	2010-08-26 10:43:56	Video Clip	Periodically	Yes	No
☑	2010-08-26 10:44:56	Video Clip	Periodically	Yes	No
□	2010-08-26 10:45:57	Video Clip	Periodically	No	No
□	2010-08-26 10:46:58	Video Clip	Periodically	No	No
□	2010-08-26 10:47:59	Video Clip	Periodically	No	No
□	2010-08-26 10:49:00	Video Clip	Periodically	No	No
□	2010-08-26 10:50:00	Video Clip	Periodically	No	No
□	2010-08-26 10:51:01	Video Clip	Periodically	No	No
□	2010-08-26 10:52:00	Video Clip	Periodically	No	No

Showing 1 to 10 of 12 entries

Note: "View" and "Download" only apply to the highlight item

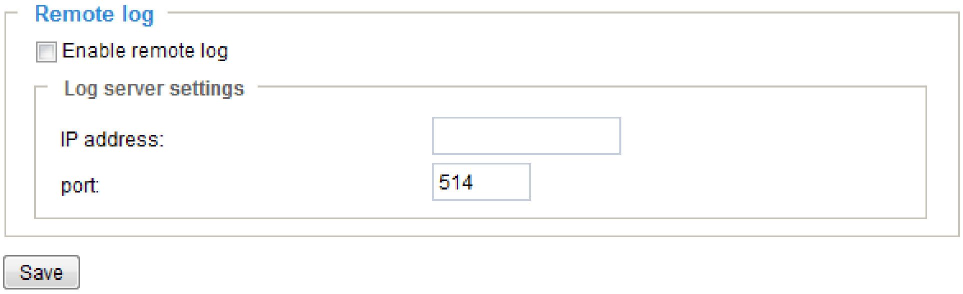
Click to switch pages

- Remove: Select the desired search results, then click this button to delete the files.

System log Advanced Mode

This section explains how to configure the video server to send the system log to the remote server as backup.

Remote log



Remote log

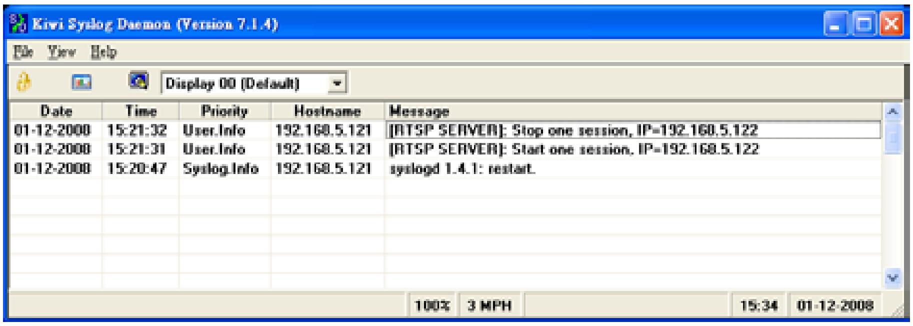
□ Enable remote log

Log server settings

IP address:

port: 514

You can configure the video server to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log messages from the video server. An example is Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.

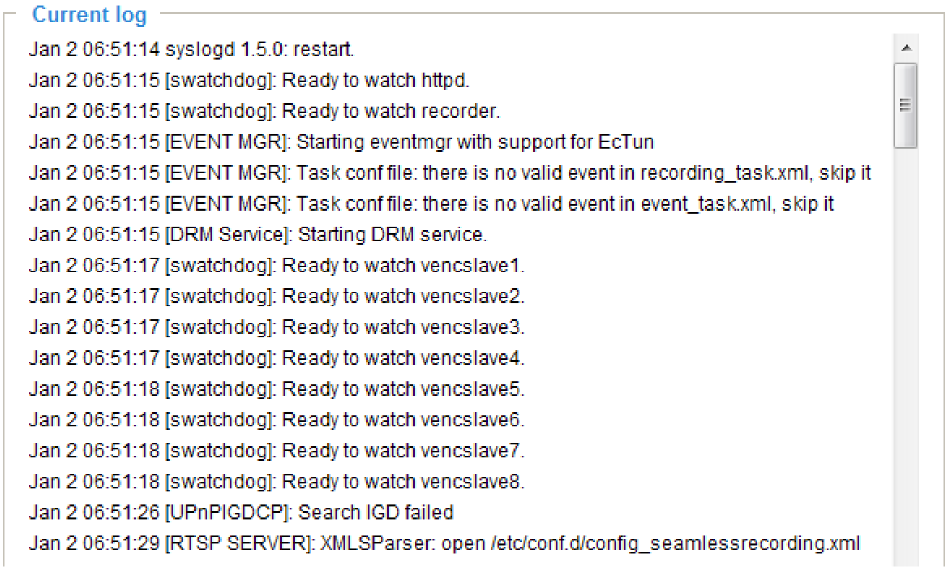


Date	Time	Priority	Hostname	Message
01-12-2008	15:21:32	User.Info	192.168.5.121	[RTSP SERVER]: Stop one session, IP=192.168.5.122
01-12-2008	15:21:31	User.Info	192.168.5.121	[RTSP SERVER]: Start one session, IP=192.168.5.122
01-12-2008	15:20:47	Syslog.Info	192.168.5.121	syslogd 1.4.1: restart.

Follow the steps below to set up the remote log:

1. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, select **Enable remote log** and click **Save** to enable the setting.

Current log



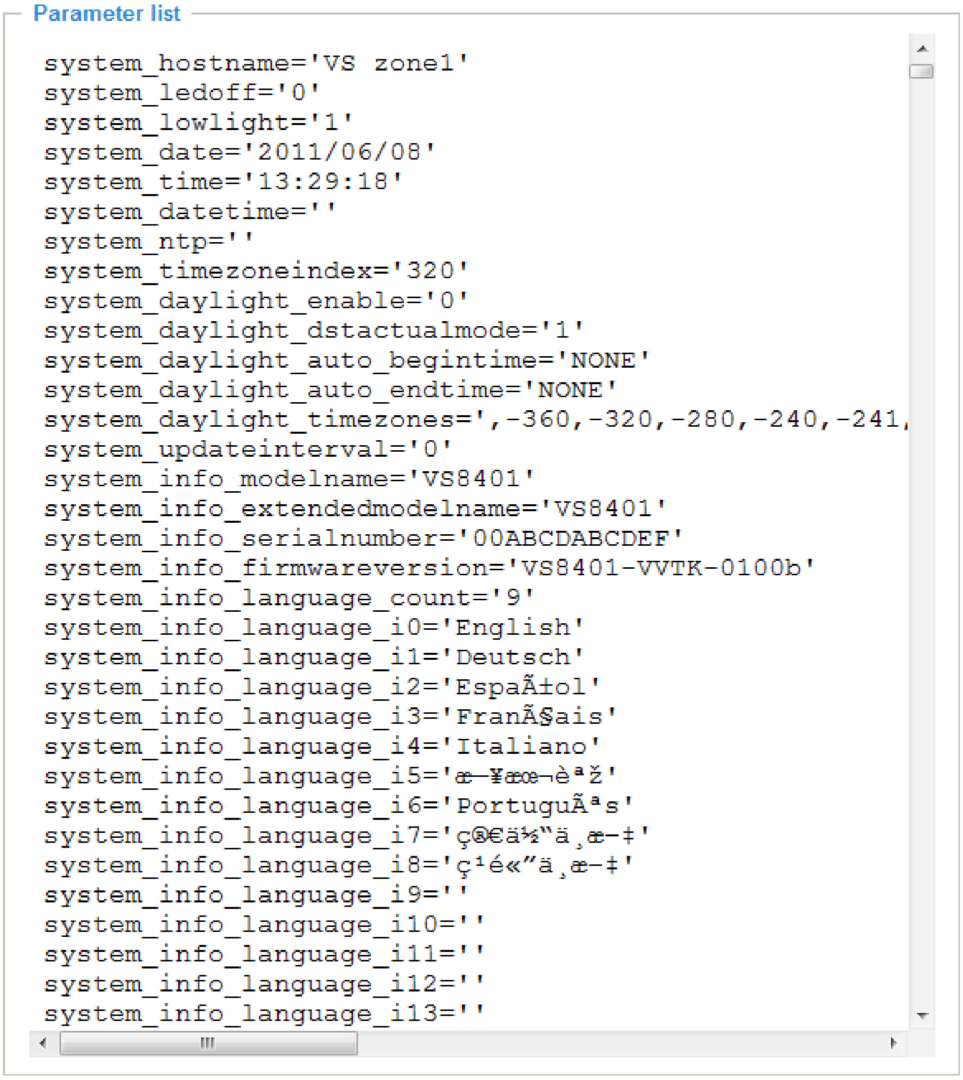
Current log

```
Jan 2 06:51:14 syslogd 1.5.0: restart.
Jan 2 06:51:15 [swatchdog]: Ready to watch httpd.
Jan 2 06:51:15 [swatchdog]: Ready to watch recorder.
Jan 2 06:51:15 [EVENT MGR]: Starting eventmgr with support for EcTun
Jan 2 06:51:15 [EVENT MGR]: Task conf file: there is no valid event in recording_task.xml, skip it
Jan 2 06:51:15 [EVENT MGR]: Task conf file: there is no valid event in event_task.xml, skip it
Jan 2 06:51:15 [DRM Service]: Starting DRM service.
Jan 2 06:51:17 [swatchdog]: Ready to watch vencslave1.
Jan 2 06:51:17 [swatchdog]: Ready to watch vencslave2.
Jan 2 06:51:17 [swatchdog]: Ready to watch vencslave3.
Jan 2 06:51:17 [swatchdog]: Ready to watch vencslave4.
Jan 2 06:51:18 [swatchdog]: Ready to watch vencslave5.
Jan 2 06:51:18 [swatchdog]: Ready to watch vencslave6.
Jan 2 06:51:18 [swatchdog]: Ready to watch vencslave7.
Jan 2 06:51:18 [swatchdog]: Ready to watch vencslave8.
Jan 2 06:51:26 [UPnPIGDCP]: Search IGD failed
Jan 2 06:51:29 [RTSP SERVER]: XMLSParser: open /etc/conf.d/config_seamlessrecording.xml
```

This column displays the system log in chronological order. The system log is stored in the video server's buffer area and will be overwritten when reaching a certain limit.

View parameters Advanced Mode

The View Parameters page lists the entire system’s parameters in alphabetical order. If you need technical assistance, please provide the information listed on this page.



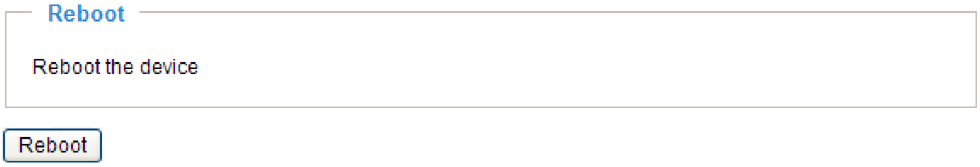
Parameter list

```
system_hostname='VS zone1'
system_ledoff='0'
system_lowlight='1'
system_date='2011/06/08'
system_time='13:29:18'
system_datetime=''
system_ntp=''
system_timezoneindex='320'
system_daylight_enable='0'
system_daylight_dstactualmode='1'
system_daylight_auto_begintime='NONE'
system_daylight_auto_endtime='NONE'
system_daylight_timezones=',-360,-320,-280,-240,-241,
system_updateinterval='0'
system_info_modelname='VS8401'
system_info_extendedmodelname='VS8401'
system_info_serialnumber='00ABCDABCDEF'
system_info_firmwareversion='VS8401-VVTK-0100b'
system_info_language_count='9'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='EspaÃ±ol'
system_info_language_i3='FranÃ§ais'
system_info_language_i4='Italiano'
system_info_language_i5='æ—¥æœ¬èªž'
system_info_language_i6='PortuguÃªs'
system_info_language_i7='ç®€ä½“ä¸æ–‡'
system_info_language_i8='ç¹é«”ä¸æ–‡'
system_info_language_i9=''
system_info_language_i10=''
system_info_language_i11=''
system_info_language_i12=''
system_info_language_i13=''
```

Maintenance

This chapter explains how to restore the video server to factory default, upgrade firmware version, etc.

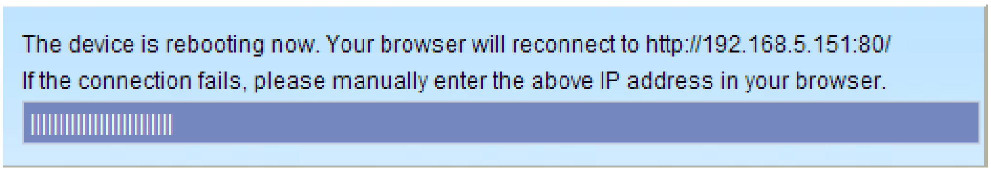
Reboot



Reboot

Reboot the device

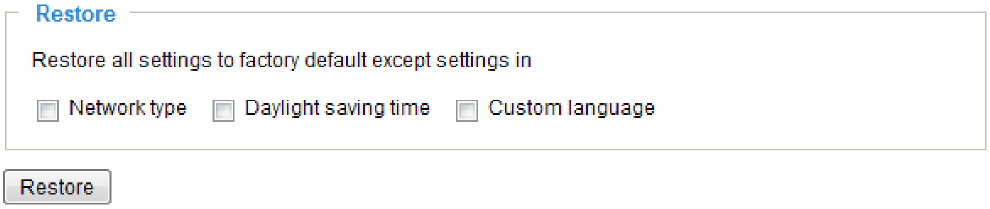
This feature allows you to reboot the video server, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will be displayed during the reboot process.



The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/
If the connection fails, please manually enter the above IP address in your browser.

If the connection fails after rebooting, manually enter the IP address of the video server in the address field to resume the connection.

Restore



Restore

Restore all settings to factory default except settings in

☐ Network type ☐ Daylight saving time ☐ Custom language

This feature allows you to restore the video server to factory default settings.

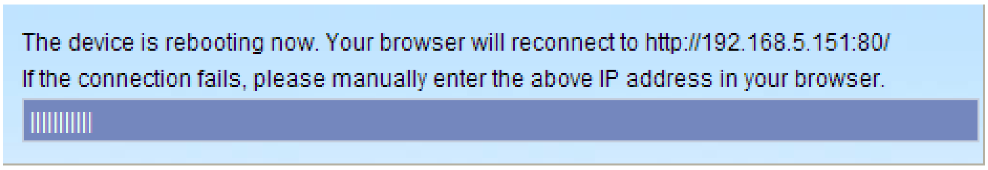
Network type: Select this option to retain the Network type settings (please refer to Network type on page 35).

Daylight saving time: Select this option to retain the Daylight saving time settings (please refer to System on page 26)

Custom language: Select this option to retain the Custom Language settings.

If none of the options is selected, all settings will be restored to factory default.

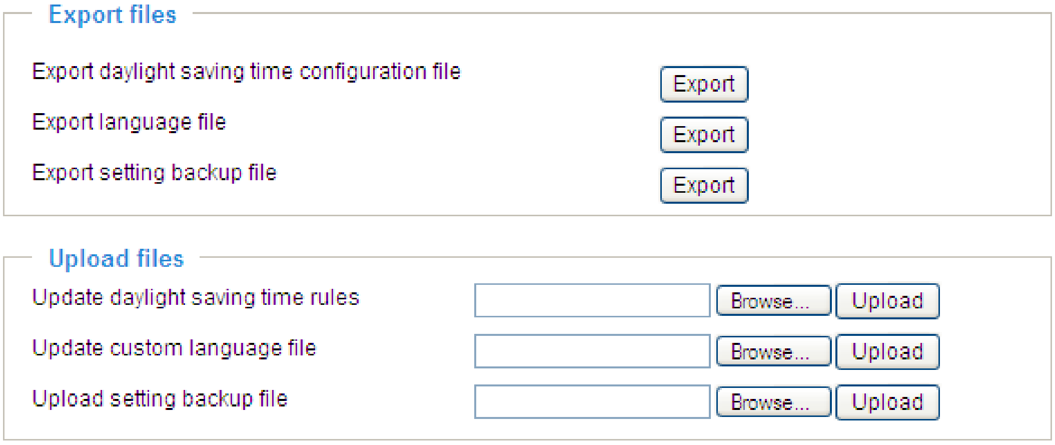
The following message is displayed during the restoring process.



The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/
If the connection fails, please manually enter the above IP address in your browser.

Export / Upload Files Advanced Mode

This feature allows you to Export / Upload daylight saving time rules, custom language files, and setting backup files.



Export files

Export daylight saving time configuration file Export

Export language file Export

Export setting backup file Export

Upload files

Update daylight saving time rules Browse... Upload

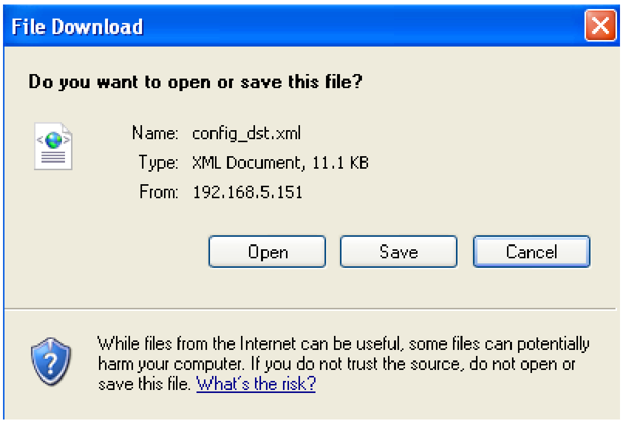
Update custom language file Browse... Upload

Upload setting backup file Browse... Upload

Export daylight saving time configuration file: Click to set the start and end time of DST.

Follow the steps below to export:

1. In the Export files column, click **Export** to export the daylight saving time configuration file from the video server.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.



File Download

Do you want to open or save this file?

Name: config_dst.xml

Type: XML Document, 11.1 KB

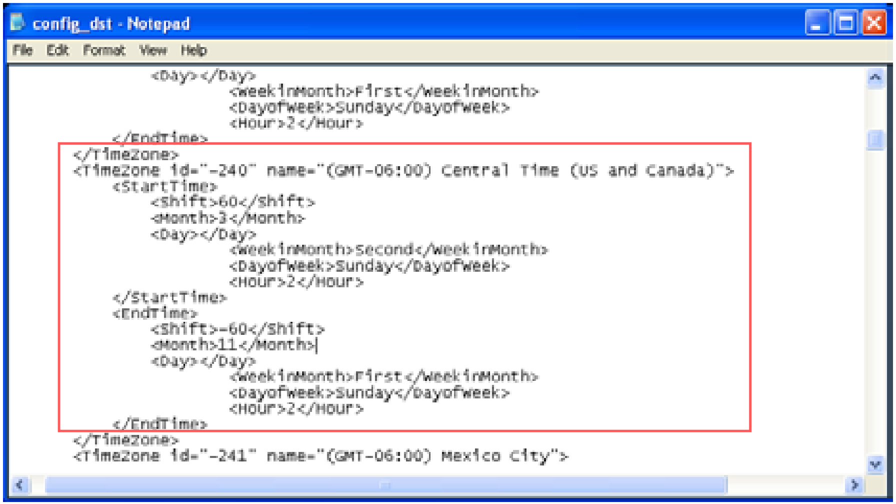
From: 192.168.5.151

Open Save Cancel

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

3. Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST. When completed, save the file.

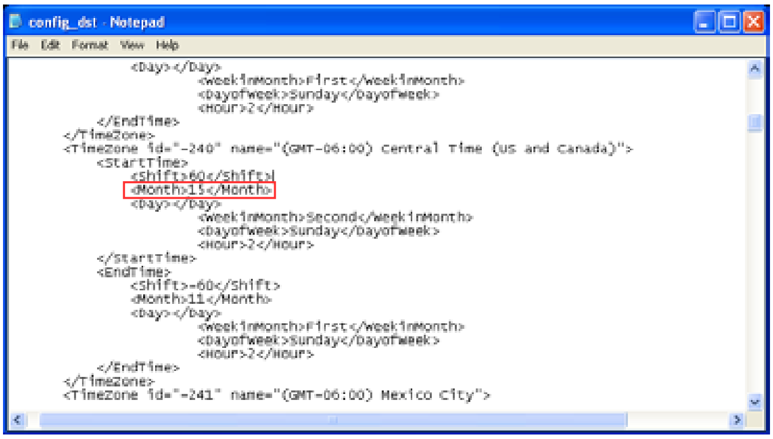
In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.



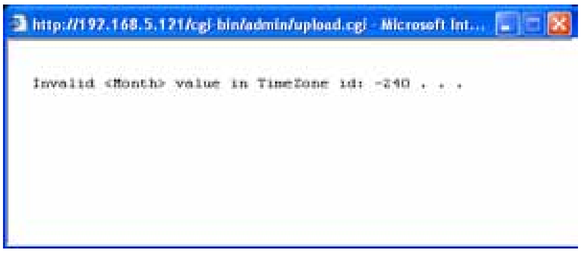
```
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-240" name="(GMT-06:00) Central Time (US and Canada)">
        <StartTime>
            <Shift>60</Shift>
            <Month>3</Month>
            <Day></Day>
                    <WeekInMonth>Second</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </StartTime>
        <EndTime>
            <Shift>-60</Shift>
            <Month>11</Month>
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-241" name="(GMT-06:00) Mexico City">
```

Upload daylight saving time rule: Click **Browse…** and specify the XML file to upload.

If the incorrect date and time are assigned, you will see the following warning message when uploading the file to the video server.

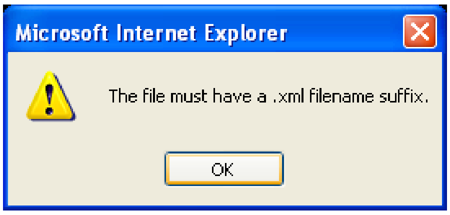


```
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-240" name="(GMT-06:00) Central Time (US and Canada)">
        <StartTime>
            <Shift>60</Shift>
            <Month>15</Month>
            <Day></Day>
                    <WeekInMonth>Second</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </StartTime>
        <EndTime>
            <Shift>-60</Shift>
            <Month>11</Month>
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-241" name="(GMT-06:00) Mexico City">
```


http://192.168.5.121/cgi-bin/admin/upload.cgi - Microsoft Int...

```
Invalid <Month> value in TimeZone id: -240 . . .
```

The following message is displayed when attempting to upload an incorrect file format.



The file must have a .xml filename suffix.

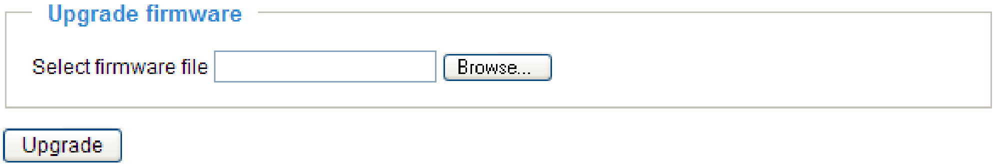
Export language file: Click to export language strings. VIVOTEK provides nine languages: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Upload custom language file: Click **Browse…** and specify your own custom language file to upload.

Export setting backup file: Click to export all parameters for the device and user-defined scripts.

Upload setting backup file: Click **Browse…** to upload a setting backup file. Please note that the model and firmware version of the device should be the same as the setting backup file. If you have set up a fixed IP or other special settings for your device, it is not suggested to upload a settings backup file.

Upgrade firmware

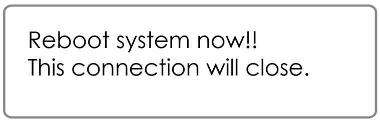


This feature allows you to upgrade the firmware of your video server. It takes a few minutes to complete the process.
Note: Do not power off the video server during the upgrade!

Follow the steps below to upgrade the firmware:
1. Download the latest firmware file from the VIVOTEK website. The file is in .pkg file format.
2. Click **Browse…** and specify the firmware file.
3. Click **Upgrade**. The video server starts to upgrade and will reboot automatically when the upgrade completes.

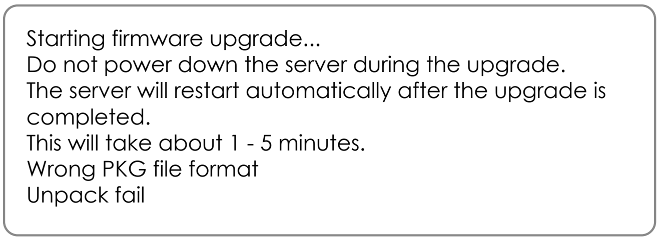
If the upgrade is successful, you will see “Reboot system now!! This connection will close”. After that, re-access the video server.

The following message is displayed when the upgrade has succeeded.



```
Reboot system now!!
This connection will close.
```

The following message is displayed when you have selected an incorrect firmware file.



```
Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is
completed.
This will take about 1 - 5 minutes.
Wrong PKG file format
Unpack fail
```

Appendix

URL Commands for the Network Camera/Video Server

1. Overview

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. The HTTP-based camera interface provides the functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set internal parameter values. The image and CGI-requests are handled by the built-in Web server.

2. Style Convention

In URL syntax and in descriptions of CGI parameters, text within angle brackets denotes content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets should also be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example further down in the page.

URL syntax is denoted with the word "Syntax:" written in bold face followed by a box with the referenced syntax as shown below. For example, name of the server is written as <servername> and is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg
```

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data is returned in HTTP format, i.e., each line is separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

```
HTTP/1.0 <HTTP code> <HTTP text>\r\n
```

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

```
http://mywebserver/cgi-bin/viewer/video.jpg
```

3. General CGI URL Syntax and Parameters

When the CGI request includes internal camera parameters, these parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in functionally-related directories under the cgi-bin directory. The file extension .cgi is required.

Syntax:

http://<*servername*>/cgi-bin/<*subdir*>[/<*subdir*>...]/<*cgi*>.<*ext*>
[?<parameter>=<value>[&<parameter>=<value>...]]

Example: Set digital output #1 to active

http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1

4. Security Level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, camctrl	1. Can view, listen, talk to camera. 2. Can control DI/DO, PTZ of the camera.
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator access rights can modify most of the camera's parameters except some privileges and network options.
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator access rights can fully control the camera's operations.
7	N/A	Internal parameters. Unable to be changed by any external interfaces.

5. Get Server Parameter Values

Note: The access right depends on the URL directory.
Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/viewer/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/operator/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/admin/getparam.cgi?[<*parameter*>]
[&<parameter>…]

Where the <*parameter*> should be <*group*>[_<*name*>]. If you do not specify any parameters, all the parameters on the server will be returned. If you specify only <*group*>, the parameters of the related group will be returned.

When querying parameter values, the current parameter values are returned.
A successful control request returns parameter pairs as follows:
Return:

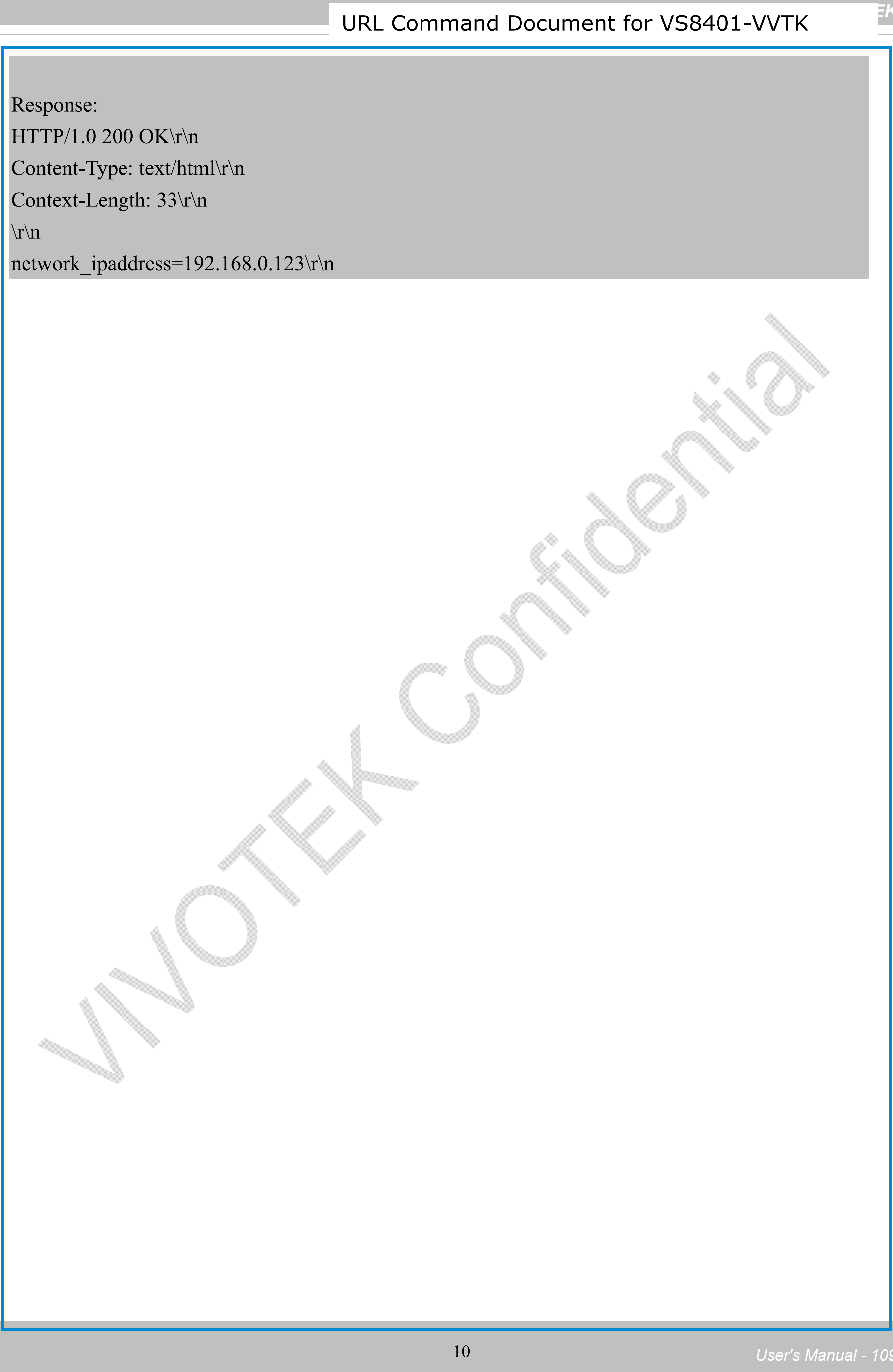
```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is
<parameter>=<value>\r\n
[<parameter pair>]

<length> is the actual length of content.

Example: Request IP address and its response

Request:
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress



```
Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network_ipaddress=192.168.0.123\r\n
```

6. Set Server Parameter Values

Note: The access right depends on the URL directory.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/anonymous/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&return=<return page>]

http://<servername>/cgi-bin/viewer/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&return=<return page>]

http://<servername>/cgi-bin/operator/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&return=<return page>]

http://<servername>/cgi-bin/admin/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign *<value>* to the parameter *<group>_<name>*.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. (Note: The return page can be a general HTML file (.htm, .html). It cannot be a CGI command or have any extra parameters. This parameter must be placed at the end of the parameter list

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is
<parameter>=<value>\r\n
[<parameter pair>]

Only the parameters that you set and are readable will be returned.

Example: Set the IP address of server to 192.168.0.123:

Request:

http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

Response:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network_ipaddress=192.168.0.123\r\n
```

7. Available parameters on the server

This chapter defines all the parameters which can be configured or retrieved from VIVOTEK network camera or video server. The general format of description is listed in the table below

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text strings shorter than 'n' characters. The characters "," , <,>,& are invalid.
string[n~m]	Text strings longer than `n' characters and shorter than `m' characters. The characters "," , <,>,& are invalid.
password[<n>]	The same as string but displays '*' instead.
integer	Any number between (-2^{31} – 1) and (2^{31} – 1).
positive integer	Any number between 0 and (2^{32} – 1).
<m> ~ <n>	Any number between 'm' and 'n'.
domain name[<n>]	A string limited to a domain name shorter than 'n' characters (eg. www.ibm.com).
email address [<n>]	A string limited to an email address shorter than 'n' characters (eg. joe@www.ibm.com).
ip address	A string limited to an IP address (eg. 192.168.1.1).
mac address	A string limited to contain a MAC address without hyphens or colons.
boolean	A boolean value of 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>, <value3>, …	Enumeration. Only given values are valid.
blank	A blank string.
everything inside <>	A description
integer primary key	SQLite data type. A 32-bit signed integer. The value is assigned a unique integer by the server.
text	SQLite data type. The value is a text string, stored using the database encoding (UTF-8, UTF-16BE or UTF-16-LE).
coordinate	x, y coordinate (eg. 0,0)
window size	window width and height (eg. 800x600)

NOTE: The camera should not be restarted when parameters are changed.

7.1 system

Group: **system**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	"Video Server"	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
ledoff	<boolean>	0	6/6	Turn on (0) or turn off (1) all led indicators.
date	<YYYY/MM/DD>, keep, auto	<current date>	6/6	Current date of system. Set to 'keep' to keep date unchanged. Set to 'auto' to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	<current time>	6/6	Current time of the system. Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	<MMDDhhmmYYYY.ss>	<current time>	6/6	Another current time format of the system.
ntp	<domain name>, <ip address>, <blank>	<blank>	6/6	NTP server. *Do not use "skip to invoke default server" for default value.
timezoneindex	-489 ~ 529	0	6/6	Indicate timezone and area. -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00

				Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona -240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan -200: GMT-05:00 Eastern Time, New York, Toronto -201: GMT-05:00 Bogota, Lima, Quito, Indiana -180: GMT-04:30 Caracas -160: GMT-04:00 Atlantic Time, Canada, La Paz, Santiago -140: GMT-03:30 Newfoundland -120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland

				-80: GMT-02:00 Mid-Atlantic -40: GMT-01:00 Azores, Cape_Verde_IS. 0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London 40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris 41: GMT 01:00 Warsaw, Budapest, Bern 80: GMT 02:00 Athens, Helsinki, Istanbul, Riga 81: GMT 02:00 Cairo 82: GMT 02:00 Lebanon, Minsk 83: GMT 02:00 Israel 120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi 121: GMT 03:00 Iraq 140: GMT 03:30 Tehran 160: GMT 04:00 Abu Dhabi, Muscat, Baku,

				Tbilisi, Yerevan 180: GMT 04:30 Kabul 200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00

				Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Auckland, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'alofa
daylight_enable	<boolean>	0	6/6	Enable automatic daylight saving time in time zone.
daylight_auto_begintime	string[19]	NONE	6/7	Display the current daylight saving start time.
daylight_auto_endtime	string[19]	NONE	6/7	Display the current daylight saving end time.
daylight_timezones	string	,-360,-320, -280,-240, -241,-200, -201,-160, -140,-120, -80,-40,0, 40,41,80, 81,82,83, 120,140, 380,400,480	6/6	List time zone index which support daylight saving time.
updateinterval	0, 3600, 86400, 604800, 2592000	0	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.
restore	0, <positive integer>	N/A	7/6	Restore the system parameters to default values after

				<value> seconds.
reset	0, <positive integer>	N/A	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	<Any value>	N/A	7/6	Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
restoreexceptdst	<Any value>	N/A	7/6	Restore the system parameters to default values except all daylight saving time settings. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to default values except for a union of combined results.
restoreexceptlang	<Any Value>	N/A	7/6	Restore the system

				parameters to default values except the custom language file the user has uploaded. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.

7.1.1 system.info

Subgroup of **system**: **info** (The fields in this group are unchangeable.)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	VS8401	0/7	Internal model name of the server (e.g. IP7139)
extendedmodelname	string[40]	VS8401	0/7	ODM specific model name of server (e.g. DCS-5610). If it is not an ODM model, this field will be equal to "modelname"
serialnumber	<mac address>	<product mac address>	0/7	12 characters MAC address (without hyphens).
firmwareversion	string[40]		0/7	Firmware version, including model, company, and version number in the format: <MODEL-BRAND-VERSION>
language_count	<integer>	9	0/7	Number of webpage languages available on the server.
language_i<0~(count-1)>	string[16]	English,	0/7	Available language lists.

		Deutsch, Español, Français, Italiano, 日本語, Português, 简体中文, 繁體中文		
customlanguage_maxcount	<integer>	1	0/6	Maximum number of custom languages supported on the server.
customlanguage_count	<integer>	0	0/6	Number of custom languages which have been uploaded to the server.
customlanguage_i<0~(maxcount-1)>	string	N/A	0/6	Custom language name.

7.2 status

Group: **status**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
signal_c<0~(nvideoin-1)>	<Boolean>	0	1/7	0=> No signal. 1=> Signal detected.
videomode_c<0~(nvideoin-1)>	ntsc, pal	ntsc	1/7	Video modulation type
di_i<0~(ndi-1)>	<boolean>	0	1/7	0 => Inactive, normal 1 => Active, triggered (capability.ndi > 0)
do_i<0~(ndo-1)>	<boolean>	0	1/7	0 => Inactive, normal 1 => Active, triggered (capability.ndo > 0)
onlinenum_rtsp	integer	0	6/7	Current number of RTSP connections.
onlinenum_httppush	integer	0	6/7	Current number of HTTP push server connections.
eth_i0	<string>	<blank>	1/7	Get network information from mii-tool.
vi_i<0~(nvi-1)>	<boolean>	0	1/7	Virtual input

				0 => Inactive 1 => Active (capability.nvi > 0)

7.3 digital input behavior define

Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	high	1/1	Indicates open circuit or closed circuit (inactive status)

7.4 digital output behavior define

Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	open	1/1	Indicate open circuit or closed circuit (inactive status)

7.5 security

Group: **security**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
privilege_do	view, operator, admin	operator	6/6	Indicate which privileges and above can control digital output (capability.ndo > 0)
privilege_camctrl	view, operator, admin	view	6/6	Indicate which privileges and above can control PTZ (capability.ptzenabled > 0 or capability.eptz > 0)
user_i0_name	string[64]	root	6/7	User name of root
user_i<1~20>_name	string[64]	<blank>	6/7	User name
user_i0_pass	password[64]	<blank>	6/6	Root password
user_i<1~20>_pass	password[64]	<blank>	7/6	User password
user_i0_privilege	viewer,	admin	6/7	Root privilege

	operator, admin			
user_i<1~20>_ privilege	viewer, operator, admin	<blank>	6/6	User privilege

7.6 network

Group: **network**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
preprocess	<positive integer>	NULL	7/6	An 32-bit integer, each bit can be set separately as follows: Bit 0 => HTTP service; Bit 1=> HTTPS service; Bit 2=> FTP service; Bit 3 => Two way audio and RTSP Streaming service; To stop service before changing its port settings. It's **recommended** to set this parameter when change a service port to the port occupied by another service currently. Otherwise, the service may fail. Stopped service will auto-start after changing port settings. Ex: Change HTTP port from 80 to 5556, and change RTP port for video from 5556 to 20480. Then, set preprocess=9 to stop both service first. "/cgi-bin/admin/setparam.cgi? network_preprocess=9&network_http_port=5556 & network_rtp_videoport=20480"
type	lan, pppoe	lan	6/6	Network connection type.
resetip	<boolean>	1	6/6	1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot. 0 => Use preset ipaddress, subnet, rounter, dns1, and dns2.

ipaddress	<ip address>	192.168.0.99	6/6	IP address of server.
subnet	<ip address>	<blank>	6/6	Subnet mask.
router	<ip address>	<blank>	6/6	Default gateway.
dns1	<ip address>	<blank>	6/6	Primary DNS server.
dns2	<ip address>	<blank>	6/6	Secondary DNS server.
wins1	<ip address>	<blank>	6/6	Primary WINS server.
wins2	<ip address>	<blank>	6/6	Secondary WINS server.

7.6.1 802.1x

Subgroup of **network: ieee8021x** (capability.protocol.ieee8021x > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable IEEE 802.1x
eapmethod	eap-peap, eap-tls	eap-peap	6/6	Selected EAP method
identity_peap	String[64]	<blank>	6/6	PEAP identity
identity_tls	String[64]	<blank>	6/6	TLS identity
password	String[254]	<blank>	6/6	Password for TLS
privatekeypassword	String[254]	<blank>	6/6	Password for PEAP
ca_exist	<boolean>	0	6/6	CA installed flag
ca_time	<integer>	0	6/7	CA installed time. Represented in EPOCH
ca_size	<integer>	0	6/7	CA file size (in bytes)
certificate_exist	<boolean>	0	6/6	Certificate installed flag (for TLS)
certificate_time	<integer>	0	6/7	Certificate installed time. Represented in EPOCH
certificate_size	<integer>	0	6/7	Certificate file size (in bytes)
privatekey_exist	<boolean>	0	6/6	Private key installed flag (for TLS)
privatekey_time	<integer>	0	6/7	Private key installed time.

				Represented in EPOCH
privatekey_size	<integer>	0	6/7	Private key file size (in bytes)

7.6.2 QOS

Subgroup of **network: qos_cos** (capability.protocol.qos.cos > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable CoS (IEEE 802.1p)
vlanid	1~4095	1	6/6	VLAN ID
video	0~7	0	6/6	Video channel for CoS
audio	0~7	0	6/6	Audio channel for CoS (capability.naudio > 0)
eventalarm	0~7	0	6/6	Event/alarm channel for CoS
management	0~7	0	6/6	Management channel for CoS
eventtunnel	0~7	0	6/6	Event/Control channel for CoS

Subgroup of **network: qos_dscp** (capability.protocol.qos.dscp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable DSCP
video	0~63	0	6/6	Video channel for DSCP
audio	0~63	0	6/6	Audio channel for DSCP (capability.naudio > 0)
eventalarm	0~63	0	6/6	Event/alarm channel for DSCP
management	0~63	0	6/6	Management channel for DSCP
eventtunnel	0~63	0	6/6	Event/Control channel for DSCP

7.6.3 IPV6

Subgroup of **network**: **ipv6** (capability.protocol.ipv6 > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable IPv6.
addonipaddress	<ip address>	<blank>	6/6	IPv6 IP address.
addonprefixlen	0~128	64	6/6	IPv6 prefix length.
addonrouter	<ip address>	<blank>	6/6	IPv6 router address.
addondns	<ip address>	<blank>	6/6	IPv6 DNS address.
allowoptional	<boolean>	0	6/6	Allow manually setup of IP

				address setting.

7.6.4 FTP

Subgroup of **network**: **ftp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	21, 1025~65535	21	6/6	Local ftp server port.

7.6.5 HTTP

Subgroup of **network**: **http**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	80	6/6	HTTP port.
alternateport	1025~65535	8080	6/6	Alternate HTTP port.
authmode	basic, digest	basic	1/6	HTTP authentication mode.
anonymousviewing	<boolean>	0	1/6	Enable anoymous streaming viewing.

Subgroup of **network**: **http_c<0~(n-1)>** for n channel products and c is channel count[1~n]

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
s0_accessname	string[32]	“video.mjpg” for c = 1. ”video2.mjpg” for c = 2. ”video3.mjpg” for c = 3, and so on.	1/6	HTTP server push access name for channel c stream 1. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 0)
s1_accessname	string[32]	“video1-2.mjpg ” for c = 1. ”video2-2.mjpg ” for c = 2, and so on.	1/6	HTTP server push access name for channel c stream 2. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 1)

For compatibility, **network_http_s<0~(t-1)>_accessname** are reserved, t = n*m for n channel products, and m is stream number per channel.

*Note: We can get n by (capability.nvideoin), and get m by (capability.nmediastream).

Besides, we map the first stream of each channel: **network_http_c<0~(n-1)>_s0_accessname** to **network_http_s<0~(n-1)>_accessname** and map the second stream of each channel: **network_http_c<0~(n-1)>_s1_accessname** to **network_http_s<n~(n*2-1)>_accessname** and so on.

Take VS8401 as an example, channel 1 stream 1: **network_http_c0_s0_accessname** is mapped to **network_http_s0_accessname** and channel 1 stream 2: **network_http_c0_s1_accessname** is mapped to **network_http_s4_accessname**.

7.6.6 HTTPS port

Subgroup of **network**: **https_port** (capability.protocol.https > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	443, 1025 ~ 65535	443	6/6	HTTPS port.

7.6.7 RTSP

Subgroup of **network**: **rtsp** (capability.protocol.rtsp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	554	1/6	RTSP port. (capability.protocol.rtsp=1)
anonymousviewing	<boolean>	0	1/6	Enable anoymous streaming viewing.
authmode	disable, basic, digest	disable	1/6	RTSP authentication mode. (capability.protocol.rtsp=1)

Subgroup of **network**: **rtsp_c<0~(n-1)>** for n channel products and c is channel count[1~n] (capability.protocol.rtsp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
s0_accessname	string[32]	"live.sdp" for c = 1. "live2.sdp" for c = 2. "live3.sdp" for c = 3,	1/6	RTSP access name for channel c stream 1. (capability.protocol.rtsp=1 and capability.nmediastream > 0)

		and so on.		
s1_accessname	string[32]	"live1-2.sdp" for c = 1. "live2-2.sdp" for c = 2, and so on.	1/6	RTSP access name for channel c stream 2. (capability.protocol.rtsp=1 and capability.nmediastream > 1)

For compatibility, **network_rtsp_s<0~(t-1)>_accessname** are reserved, t = n*m for n channel products, and m is stream number per channel.
*Note: We can get n by (capability.nvideoin), and get m by (capability.nmediastream).

Besides, we map the first stream of each channel: **network_rtsp_c<0~(n-1)>_s0_accessname** to **network_rtsp_s<0~(n-1)>_accessname** and map the second stream of each channel: **network_rtsp_c<0~(n-1)>_s1_accessname** to **network_rtsp_s<n~(n*2-1)>_accessname** and so on.

Take VS8401 as an example, channel 1 stream 1: **network_rtsp_c0_s0_accessname** is mapped to **network_rtsp_s0_accessname** and channel 1 stream 2: **network_rtsp_c0_s1_accessname** is mapped to **network_rtsp_s4_accessname**.

7.6.7.1 RTSP multicast

Subgroup of **network_rtsp_c<0~(n-1)>_s<0~(m-1)>_multicast** for n channel products, and m is stream number per channel, c is channel count[1~n], s is stream count[1~m]
(capability.protocol.rtp.multicast > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	0	4/4	Enable always multicast.
ipaddress	<ip address>	For stream 1 of all channels: 239.128.1.99 for channel 1 stream 1. 239.128.1.100 for channe 2 stream 1, and so on. For stream 2 of all channels: 239.128.1.(99+n) for channel 1 stream 2. 239.128.1.(100+n) for	4/4	Multicast IP address.

		channel 2 stream 2, and so on. For stream 3 of all channels: 239.128.1.(99+n*2) for channel 1 stream 3. 239.128.1.(100+n*2) for channel 2 stream 3, and so on.		
videoport	1025 ~ 65535	For stream 1 of all channels: 5560+(c-1)*4 For stream 2 of all channels: 5560+n*4*(s-1)+(c-1)*4 And so on.	4/4	Multicast video port.
audioport	1025 ~ 65535	For stream 1 of all channels: 5562+(c-1)*4 For stream 2 of all channels: 5562+n*4+(c-1)*4 And so on.	4/4	Multicast audio port. (capability.naudio > 0)
ttl	1 ~ 255	15	4/4	Mutlicast time to live value.

For compatibility, **network_rtsp_s<0~(t-1)>_multicast** are reserved, t = n*m for n channel products, and m is stream number per channel.
*Note: We can get n by (capability.nvideoin), and get m by (capability.nmediastream).

Besides, we map the first stream of each channel: **network_rtsp_c<0~(n-1)>_s0_multicast** to **network_rtsp_s<0~(n-1)>_multicast** and map the second stream of each channel: **network_rtsp_c<0~(n-1)>_s1_multicast** to **network_rtsp_s<n~(n*2-1)>_multicast** and so on.

Take VS8401 as an example, channel 1 stream 1 is mapped to **network_rtsp_s0_multicast** and channel 1 stream 2 is mapped to **network_rtsp_s4_multicast**.

7.6.8 SIP port

Subgroup of **network**: **sip** (capability.protocol.sip> 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	1025 ~ 65535	5060	1/6	SIP port.

7.6.9 RTP port

Subgroup of **network**: **rtp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	5556	6/6	Video channel port for RTP. (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	5558	6/6	Audio channel port for RTP. (capability.protocol.rtp_unicast=1)

7.6.10 PPPoE

Subgroup of **network**: **pppoe** (capability.protocol.pppoe > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
user	string[128]	<blank>	6/6	PPPoE account user name.
pass	password[64]	<blank>	6/6	PPPoE account password.

7.7 Ipfilter for ONVIF

Group: **ipfilter**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable access list filtering.
admin_enable	<boolean>	0	6/6	Enable administrator IP address.
admin_ip	String[44]	<blank>	6/6	Administrator IP address.
maxconnection	1~10	10	6/6	Maximum number of concurrent streaming connection(s).
type	0, 1	1	6/6	Ipfilter policy :

				0 => allow 1 => deny
ipv4list_i<0~9>	Single address: <ip address> Network address: <ip address / network mask> Range address:<start ip address - end ip address>	<blank>	6/6	IPv4 address list.
ipv6list_i<0~9>	String[44]	<blank>	6/6	IPv6 address list.

7.8 Video input setting per channel

Group: **videoin_c<0~(n-1)>** for n channel products, and m is stream number

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
whitebalance	auto, manual	auto	4/4	"auto" indicates auto white balance. "manual" indicates keep current value.
color	0, 1	1	4/4	0 =>monochrome 1 => color
flip	<boolean>	0	4/4	Flip the image.
mirror	<boolean>	0	4/4	Mirror the image.
ptzstatus	<integer>	2	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support) Bit 3 => Support **tilt**

				operation; 0(not support), 1(support) Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)
text	string[16]	<blank>	1/4	Enclose caption.
imprinttimestamp	<boolean>	0	4/4	Overlay time stamp and enclose caption on video.
s<0~(m-1)>_codectype	mpeg4, mjpeg, h264	h264	1/4	Video codec type.
s<0~(m-1)>_resolution	D1, 4CIF, CIF, QCIF	4CIF	1/4	Video resolution in pixels.
s<0~(m-1)>_ratiocorrect	<boolean>	0	1/4	Change resolution to fit 4:3 ratio. For PAL: D1/4CIF(720/704x576) -> (768x576) CIF(352x288)->(384x288) For NTSC: D1/4CIF(720/704x480) -> (640x480) CIF(352x240)->(320x240)
s<0~(m-1)>_mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_mpeg4_ratecontrolmode	cbr, vbr	vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_quant	0~5 99, 100	3	4/4	Quality of video when choosing vbr in “ratecontrolmode”. 0, 99,100 is the customized manual input setting.

				1 = worst quality, 5 = best quality.
s<0~(m-1)>_mpeg4_qvalue	1~31	7	4/4	Manual video quality level input. (s<0~(m-1)>_mpeg4_quant = 0, 99) *Note: This is reserved for campatibility, and we recommend changing to use "s<0~(m-1)>_mpeg4_qpercent".
s<0~(m-1)>_mpeg4_qpercent	1~100	29	4/4	Set quality by percentage. 1: Worst quality 100: Best quality (s<0~(m-1)>_mpeg4_quant = 100)
s<0~(m-1)>_mpeg4_bitrate	1000~4000000	51200	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_mpeg4_maxframe	1~30	20	1/4	Set maximum frame rate in fps (for MPEG-4).
s<0~(m-1)>_h264_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_h264_ratecontrolmode	cbr, vbr	vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_h264_quant	0~5,99,100	3	4/4	Quality of video when choosing vbr in "ratecontrolmode". 0, 99 and 100 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_h264_qvalue	0~51	26	4/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 0, 99) *Note: This is reserved for

				campatibility, and we recommend changing to use “s<0~(m-1)>_h264_qpercent”.
s<0~(m-1)>_h264_qpercent	1~100	45	4/4	Set quality by percentage. 1: Worst quality 100: Best quality (s<0~(m-1)>_h264_quant = 100)
s<0~(m-1)>_h264_bitrate	1000~4000000	512000	4/4	Set bit rate in bps when choosing cbr in “ratecontrolmode”.
s<0~(m-1)>_h264_maxframe	1~30	20	1/4	Set maximum frame rate in fps (for h264).
s<0~(m-1)>_h264_profile	0~2	1	1/4	Indicate H264 profiles 0: baseline 1: main profile 2: high profile
s<0~(m-1)>_mjpeg_quant	0 ~ 5,99, 100	3	4/4	Quality of JPEG video. 0, 99 and 100 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_mjpeg_qvalue	0~200	50	4/4	Manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 0, 99) *Note: This is reserved for campatibility, we recommend changing to use “s<0~(m-1)>_mjpeg_qpercent”.
s<0~(m-1)>_mjpeg_qpercent	1~100	49	4/4	Set quality by percentage. 1: Worst quality 100: Best quality (s<0~(m-1)>_mjpeg_quant = 100)
s<0~(m-1)>_mjpeg_maxfram	1~30	20	1/4	Set maximum frame rate in

e				fps (for JPEG).

7.9 Image setting per channel

Group: **image_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5 ~ 5, 100	100	4/4	Adjust brightness of image according to mode settings. 100 means using "brightnesspercent". *Note: This is reserved for campatibility, and we recommend changing to use "brightnesspercent".
saturation	-5 ~ 5, 100	100	4/4	Adjust saturation of image according to mode settings. 100 means using "saturationpercent". *Note: This is reserved for campatibility, and we recommend changing to use "saturationpercent".
contrast	-5 ~ 5, 100	100	4/4	Adjust contrast of image according to mode settings. 100 means using "contrastpercent". *Note: This is reserved for campatibility, and we recommend changing to use "contrastpercent".
sharpness	-5 ~ 5, 100	100	4/4	Adjust sharpness of image according to mode settings. 100 means using "sharpnesspercent". *Note: This is reserved for campatibility, and we recommend

				changing to use "sharpnesspercent".
brightnesspercent	0 ~ 100	50	4/4	Adjust brightness of image by percentage. Darker 0 <-> 100 Brighter
saturationpercent	0 ~ 100	50	4/4	Adjust saturation of image by percentage. Less 0 <-> 100 More saturation
contrastpercent	0 ~ 100	50	4/4	Adjust contrast of image by percentage. Less 0 <-> 100 More contrast
sharpnesspercent	0~100	30	4/4	Adjust sharpness of image by percentage. Softer 0 <-> 100 Sharper
xoffset	-4 ~ 4	2	4/4	Change start point of input image in horizontal.
yoffset	-4 ~ 4	2	4/4	Change start point of input image in vertical.
deinterlace_enable	<boolean>	1	4/4	Enable de-interlace
deinterlace_mode	adaptive, blend	adaptive	4/4	Adaptive: Detect moving area and perform de-interlace on it. This mode leads to better image quality, but consumes more resource. Blend: Use blend method to perform de-interlace.
IBPE_edgeenable	<boolean>	0	4/4	Enable edge enhancement.
IBPE_edgestrength	1 ~ 128	14	4/4	Adjust edge enhancement strength. 1 is minimum and 128 is maximum.
IBPE_nrenable	<boolean>	0	4/4	Enable noise reduction.
IBPE_nrmode	1 ~ 3	1	4/4	Adjust noise reduction mode. 1 => DeGaussian 2 => DeImpulse 3 => DeGaussian + DeImpulse
IBPE_nrstrength	1 ~ 63	1	4/4	Adjust noise reduction strength. 1 is minimum and 63 is maximum.

*Note: Saving value between -5~+5 to "brightness" will save its corresponding value to "brightnesspercent" automatically, and then the value of "brightness" will be set back to 100 to take effect..
Saving value to "saturation", "contrast", or "sharpness" has the same behavior.

7.10 Audio input per channel

Group: **audioin_c<0~(n-1)>** for n channel products (capability.audioin>0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
mute	0, 1	1	1/4	Enable audio mute.
gain	0~15	8	4/4	Gain of input.
s0_g711_mode	pcmu, pcma	pcmu	4/4	Set G.711 mode.

7.11 Time Shift settings

Group: **timeshift**, c for n channel products, m is stream number (capability.timeshift > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable time shift streaming.
c<0~(n-1)>_s<0~(m-1)>_allow	<boolean>	0	4/4	Enable time shift streaming for specific stream.

7.12 Motion detection settings

Group: **motion_c<0~(n-1)>** for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable motion detection.
win_i<0~2>_enable	<boolean>	0	4/4	Enable motion window 1~3.
win_i<0~2>_name	string[40]	<blank>	4/4	Name of motion window 1~3.
win_i<0~2>_left	0 ~ 320	0	4/4	Left coordinate of window position.
win_i<0~2>_top	0 ~ 240	0	4/4	Top coordinate of window position.
win_i<0~2>_width	0 ~ 320	0	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	0	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	0	4/4	Percent of motion detection window.

win_i<0~2>_sensitivity	0 ~ 100	0	4/4	Sensitivity of motion detection window.

7.13 Tempering detection settings

Group: **tampering_c<0~(n-1)>** for n channel product (capability.tampering > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable or disable tamper detection.
threshold	0 ~ 255	32	1/99	Threshold of tamper detection.
duration	10 ~ 600	10	4/4	If tampering value exceeds the 'threshold' for more than 'duration' second(s), then tamper detection is triggered.

7.14 DDNS

Group: **ddns** (capability.ddns > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the dynamic DNS.

provider	Safe100,
	DyndnsDynamic,
	DyndnsCustom,
	TZO,
	DHS,
	DynInterfree,
	CustomSafe100
		DyndnsDynamic	6/6	Safe100 => safe100.net
				DyndnsDynamic => dyndns.org (dynamic)
				DyndnsCustom => dyndns.org (custom)
				TZO => tzo.com
				DHS => dhs.org
				DynInterfree =>dyn-interfree.it
				CustomSafe100 =>
				Custom server using safe100 method

<provider>_hostname	string[128]	<blank>	6/6	Your DDNS hostname.
<provider>_usernameemail	string[64]	<blank>	6/6	Your user name or email to login to the DDNS service provider
<provider>_passwordkey	string[64]	<blank>	6/6	Your password or key to login to the DDNS service provider.
<provider>_servername	string[128]	<blank>	6/6	The server name for safe100. (This field only exists if the provider is customsafe100)

7.15 UPnP presentation

Group: **upnppresentation**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	1	6/6	Enable or disable the UPnP presentation service.

7.16 UPnP port forwarding

Group: **upnpportforwarding**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the UPnP port forwarding service.
upnpnatstatus	0~3	0	6/7	The status of UPnP port forwarding, used internally. 0 = OK, 1 = FAIL, 2 = no IGD router, 3 = no need for port forwarding

7.17 Express link

Group:expresslink

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
state	onlycheck, onlyoffline, checkonline, badnetwork	<blank>	6/6	“onlycheck” : You have to input the host name of your camera and press "Register" button to register it. “onlyoffline” : Express link is active, you can now connect to this camera at expresslink_url. “checkonline” : Express link is not active. “badnetwork” : Express Link is not supported under this network environment.
url	string[64]	<blank>	6/6	The URL to connect to this camera

				by express link.

7.18 System log

Group: **syslog**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	0	6/6	Enable remote log.
serverip	<IP address>	<blank>	6/6	Log server IP address.
serverport	514, 1025~65535	514	6/6	Server port used for log.
level	0~7	6	6/6	Levels used to distinguish the importance of the information: 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG

7.19 camera PTZ control

Group: **camctrl** (capability.camctrl.httptunnel > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enablehttptunnel	<boolean>	0	4/4	Enable HTTP tunnel for camera control.

Group: **camctrl_c<0~(n-1)>** for n channel product (capability.ptzenabled)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
panspeed	-5 ~ 5	0	1/4	Pan speed
tiltspeed	-5 ~ 5	0	1/4	Tilt speed
zoomspeed	-5 ~ 5	0	1/4	Zoom speed
focusspeed	-5 ~ 5	0	1/4	Auto focus speed
preset_i<0~(npreset-1)>_name	string[40]	<blank>	1/4	Name of the preset location.
uart	0 ~ (m-1), m	0	1/4	Select corresponding uart

	is UART count			(capability.nuart>0).
cameraid	0~255	1	1/4	Camera ID controlling external PTZ camera.
hometype	<boolean>	0	1/4	The attribute defines whether the HOME command emulation is enabled. 0: Use the preset position 0 as the home position 1: Use HOME command (if the camera supports it.)
isptz	0 ~ 2	0	1/4	0: disable PTZ commands. 1: enable PTZ commands with PTZ driver. 2: enable PTZ commands with UART tunnel.
disablemdonptz	<boolean>	0	1/4	Disable motion detection on PTZ operation.
patrolseq	string[120]	<blank>	1/4	(For external device) The indexes of patrol points, separated by ","
patroldwelling	string[160]	<blank>	1/4	(For external device) The dwelling time of each patrol point, separated by ","

7.20 UART control

Group: **uart** (capability.nuart > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
ptzdrivers_i<0~19, 127>_name	string[40]	<blank>	1/4	Name of the PTZ driver.
ptzdrivers_i<0~19, 127>_location	string[128]	<blank>	1/4	Full path of the PTZ driver.
enablehttptunnel	<boolean>	0	4/4	Enable HTTP tunnel channel to control UART.

Group: **uart_i<0~(n-1)>** n is uart port count (capability.nuart > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION

			(get/set)	
baudrate	110,300,600,1200,2400,3600,4800,7200,9600,19200,38400,57600,115200	9600	4/4	Set baud rate of COM port.
databit	5,6,7,8	8	4/4	Data bits in a character frame.
paritybit	none, odd, even	none	4/4	For error checking.
stopbit	1,2	1	4/4	1 2-1.5 , data bit is 5 2-2
uartmode	rs485, rs232	rs485	4/4	RS485 or RS232.
customdrvcmd_i<0~9>	string[128]	<blank>	1/4	PTZ command for custom camera.
speedlink_i<0~15>_name	string[40]	<blank>	1/4	Additional PTZ command name.
speedlink_i<0~15>_cmd	string[40]	<blank>	1/4	Additional PTZ command list.
ptzdriver	0~19, 127 (custom), 128 (no driver)	128 (no driver)	4/4	The PTZ driver is used by this COM port.

7.21 SNMP

Group: **snmp** (capability.snmp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
v2	0~1	0	6/6	SNMP v2 enabled. 0 for disable, 1 for enable
v3	0~1	0	6/6	SNMP v3 enabled. 0 for disable, 1 for enable
secnamerw	string[31]	Private	6/6	Read/write security name
secnamero	string[31]	Public	6/6	Read only security name
authpwrw	string[8~128]	<blank>	6/6	Read/write authentication password

authpwro	string[8~128]	<blank>	6/6	Read only authentication password
authtyperw	MD5,SHA	MD5	6/6	Read/write authentication type
authtypero	MD5,SHA	MD5	6/6	Read only authentication type
encryptpwrw	string[8~128]	<blank>	6/6	Read/write password
encryptpwro	string[8~128]	<blank>	6/6	Read only password
encrypttyperw	DES	<blank>	6/6	Read/write encryption type
encrypttypero	DES	<blank>	6/6	Read only encryption type
rwcommunity	string[31]	Private	6/6	Read/write community
rocommunity	string[31]	Public	6/6	Ready only community

7.22 Layout configuration

Group: **layout**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
logo_default	<boolean>	1	1/6	0 => Custom logo 1 => Default logo
logo_link	string[40]	http://www.vivotek.com	1/6	Hyperlink of the logo
logo_powerbyvvtk_hidden	<boolean>	0	1/6	0 => display the power by vivotek logo 1 => hide the power by vivotek logo
theme_option	1~4	1	1/6	1~3: One of the default themes. 4: Custom definition.
theme_color_font	string[7]	#ffffff	1/6	Font color
theme_color_configfont	string[7]	#ffffff	1/6	Font color of configuration area.
theme_color_titlefont	string[7]	#098bd6	1/6	Font color of video title.
theme_color_controlbackground	string[7]	#565656	1/6	Background color of control area.
theme_color_configbackground	string[7]	#323232	1/6	Background color of configuration area.

theme_color_videobackground	string[7]	#565656	1/6	Background color of video area.
theme_color_case	string[7]	#323232	1/6	Frame color
custombutton_manualtrigger_show	<boolean>	1	1/6	Show or hide manual trigger (VI) button in homepage 0 -> Hidden 1 -> Visible

7.23 Privacy mask

Group: **privacymask_c<0~(n-1)>** for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable privacy mask.
win_i<0~4>_enable	<boolean>	0	4/4	Enable privacy mask window.
win_i<0~4>_name	string[14]	<blank>	4/4	Name of the privacy mask window.
win_i<0~4>_left	0 ~ 320/352	0	4/4	Left coordinate of window position.
win_i<0~4>_top	0 ~ 240/288	0	4/4	Top coordinate of window position.
win_i<0~4>_width	0 ~ 320/352	0	4/4	Width of privacy mask window.
win_i<0~4>_height	0 ~ 240/288	0	4/4	Height of privacy mask window.

7.24 Capability

Group: **capability**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
api_httpversion	0200a	0200a	0/7	The HTTP API version.
bootuptime	<positive integer>	60	0/7	Server bootup time.
nir	0, <positive integer>	0	0/7	Number of IR interfaces. (Recommend to use ir for built-in IR and extir for external IR)

npir	0, <positive integer>	0	0/7	Number of PIRs.
ndi	0, <positive integer>	4	0/7	Number of digital inputs.
nvi	0, <positive integer>	4	0/7	Number of virtual inputs (manual trigger)
ndo	0, <positive integer>	4	0/7	Number of digital outputs.
naudioin	0, <positive integer>	4	0/7	Number of audio inputs.
naudioout	0, <positive integer>	4	0/7	Number of audio outputs.
nvideoin	<positive integer>	4	0/7	Number of video inputs.
nvideoinprofile	<positive integer>	0	0/7	Number of video input profiles.
nmediastream	<positive integer>	2	0/7	Number of media stream per channels.
nvideosetting	<positive integer>	1	0/7	Number of video settings per channel.
naudiosetting	<positive integer>	1	0/7	Number of audio settings per channel.
nuart	0, <positive integer>	1	0/7	Number of UART interfaces.
nmotionprofile	0, <positive integer>	0	0/7	Number of motion profiles.
ptzenabled	0, <positive integer>	189	0/7	An 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support)

				Bit 1 => Built-in or external camera;
				0(external), 1(built-in)
				Bit 2 => Support pan operation, 0(not support), 1(support)
				Bit 3 => Support tilt operation; 0(not support), 1(support)
				Bit 4 => Support zoom operation;
				0(not support), 1(support)
				Bit 5 => Support focus operation;
				0(not support), 1(support)
				Bit 6 => Support iris operation;
				0(not support), 1(support)
				Bit 7 => External or built-in PT; 0(built-in), 1(external)
				Bit 8 => Invalidate bit 1 ~ 7;
				0(bit 1 ~ 7 are valid),
				1(bit 1 ~ 7 are invalid)
				Bit 9 => Reserved bit;
				Invalidate lens_pan, lens_tilt, lens_zoon, lens_focus, len_iris.
				0(fields are valid),
				1(fields are invalid)

windowless	<boolean>	1	0/7	Indicate whether to support windowless plug-in.
eptz	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => stream 1 supports ePTZ or not. Bit 1 => stream 2 supports ePTZ or not.

				The rest may be deduced by analogy
lens_pan	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support pan. Bit 1 => Support pan in UI. Bit 2 => External or built-in pan function; 0(built-in), 1(external).
lens_tilt	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support tilt. Bit 1 => Support tilt in UI. Bit 2 => External or built-in tilt function; 0(built-in), 1(external).
lens_zoom	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support zoom Bit 1 => Support zoom in UI Bit 2 => External or built-in zoom function; 0(built-in), 1(external).
lens_focus	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support focus. Bit 1 => Support focus in UI. Bit 2 => External or built-in focus function; 0(built-in), 1(external). Bit 3 => Support auto focus in UI.
lens_iris	0, <positive	0	0/7	A 32-bit integer, each bit

	integer>			can be set separately as follows: Bit 0 => Support iris. Bit 1 => Support iris in UI. Bit 2 => External or build-in iris function; 0(build-in), 1(external). Bit 3 => Support auto iris in UI.
npreset	0, <positive integer>	20	0/7	Number of preset locations.
protocol_https	< boolean >	1	0/7	Indicate whether to support HTTP over SSL.
protocol_rtsp	< boolean >	1	0/7	Indicate whether to support RTSP.
protocol_sip	<boolean>	1	0/7	Indicate whether to support SIP.
protocol_maxconnection	<positive integer>	10	0/7	The maximum allowed simultaneous connections.
protocol_maxgenconnection	<positive integer>	10	0/7	The maximum general streaming connections .
protocol_maxmegaconnection	<positive integer>	0	0/7	The maximum megapixel streaming connections.
protocol_rtp_multicast_ scalable	<boolean>	1	0/7	Indicate whether to support scalable multicast.
protocol_rtp_multicast_ backchannel	<boolean>	0	0/7	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	1	0/7	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	1	0/7	Indicate whether to support RTP over HTTP.
protocol_spush_mjpeg	<boolean>	1	0/7	Indicate whether to support server push MJPEG.
protocol_snmp	<boolean>	1	0/7	Indicate whether to support SNMP.
protocol_ipv6	<boolean>	1	0/7	Indicate whether to support IPv6.
protocol_pppoe	<boolean>	1	0/7	Indicate whether to support PPPoE.

protocol_ieee8021x	<boolean>	1	0/7	Indicate whether to support IEEE802.1x.
protocol_qos_cos	<boolean>	1	0/7	Indicate whether to support CoS.
protocol_qos_dscp	<boolean>	1	0/7	Indicate whether to support QoS/DSCP.
protocol_ddns	<boolean>	1	0/7	Indicate whether to support DDNS.
videoin_type	0, 1, 2	0	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_resolution	<a list of available resolution separated by commas>	QCIF, CIF, 4CIF, D1	0/7	Available resolutions list.
videoin_maxframerate	<a list of available maximum frame rate separated by commas>	30, 30, 30, 30	0/7	Available maximum frame list.
videoin_codec	mpeg4. mjpeg, h264	mpeg4, mjpeg, h264	0/7	Available codec list.
timeshift	<boolean>	1	0/7	Indicate whether to support time shift caching stream.
audio_aec	<boolean>	0	0/7	Indicate whether to support acoustic echo cancellation.
audio_extmic	<boolean>	1	0/7	Indicate whether to support external microphone input.
audio_linein	<boolean>	0	0/7	Indicate whether to support external line input. (It will be replaced by audio_mic and audio_extmic.)
audio_lineout	<boolean>	0	0/7	Indicate whether to support line output.
audio_headphoneout	<boolean>	0	0/7	Indicate whether to support

				headphone output.
audioin_codec	aac4, gamr, g711	g711	0/7	Available codec list for audio input.
uart_httptunnel	<boolean>	1	0/7	Indicate whether to support HTTP tunnel for UART transfer.
camctrl_httptunnel	<boolean>	1	0/7	The attribute indicates whether sending camera control commands through HTTP tunnel is supported. 0: Not supported 1: Supported
camctrl_privilege	<boolean>	1	0/7	Indicate whether to support “Manage Privilege” of PTZ control in the Security page. 1: support both /cgi-bin/camctrl/camctrl.cgi and /cgi-bin/viewer/camctrl.cgi 0: support only /cgi-bin/viewer/camctrl.cgi
transmission_mode	Tx, Rx, Both	Tx	0/7	Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both = DVR.
network_wire	<boolean>	1	0/7	Indicate whether to support Ethernet.
network_wireless	<boolean>	0	0/7	Indicate whether to support wireless.
derivative_brand	<boolean>	1	0/7	Indicate whether to support the upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)
evctrlchannel	<boolean>	1	0/7	Indicate whether to support HTTP tunnel for

				event/control transfer.
joystick	<boolean>	0	0/7	Indicate whether to support joystick control.
storage_dbenabled	<boolean>	0	0/7	Media files are indexed in database.
nanystream	0, <positive integer>	0	0/7	number of any media stream per channel
iva	<boolean>	0	0/7	Indicate whether to support Intelligent Video analysis
version_onvifdaemon	<string>	<blank>	0/7	Indicate ONVIF daemon version
version_onvifevent	<string>	<blank>	0/7	Indicate ONVIF event version
media_totalspace	<positive integer>	60000	0/7	Available memory space (KB) for media.
media_snapshot_sizepersecond	<positive integer>	512	0/7	Maximum size (KB) of one snapshot image.
media_snapshot_maxpreevent	<positive integer>	7	0/7	Maximum snapshot number before event occurred.
media_snapshot_maxpostevent	<positive integer>	7	0/7	Maximum snapshot number after event occurred.
media_videoclip_maxsize	<positive integer>	5000	0/7	Maximum size (KB) of a videoclip.
media_videoclip_maxlength	<positive integer>	20	0/7	Maximum length (second) of a videoclip.
media_videoclip_maxpreevent	<positive integer>	9	0/7	Maximum duration (second) after event occurred in a videoclip.

7.25 Customized event script

Group: **event_customtaskfile_i**<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[41]	NULL	6/7	Custom script identification of this entry.
date	string[17]	NULL	6/7	Date of custom script.
time	string[17]	NULL	6/7	Time of custom script.

7.26 Event setting

Group: **event_i**<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry.
enable	0, 1	0	6/6	Enable or disable this event.
priority	0, 1, 2	1	6/6	Indicate the priority of this event: "0" = low priority "1" = normal priority "2" = high priority
delay	1~999	20	6/6	Delay in seconds before detecting the next event.
trigger	boot, di, motion, seq, recnotify, tampering, visignal, virestore, vi	boot	6/6	Indicate the trigger condition: "boot" = System boot "di"= Digital input "motion" = Video motion detection "seq" = Periodic condition "recnotify" = Recording notification. "tampering" = Tamper detection. "visignal" = Video input signal loss. "virestore" = Video input signal restore "vi"= Virtual input (Manual trigger)
triggerstatus	<string>	trigger	6/6	The status for event trigger
di	<integer>	0	6/6	Indicate the source id of di trigger. This field is required when trigger condition is "di". One bit represents one digital input. The LSB indicates DI 0.
vi	<integer>	0	6/6	Indicate the source id of vi trigger. This field is required when trigger condition is "vi". One bit represents one digital input. The LSB indicates VI 0.

tampering	0 ~ 255	0	6/6	Indicate the source of the tampering detection. Each bit represents one channel, and the LSB indicates channel 1.
visignal	0 ~ 255	0	6/6	Indicate the source of video input signal loss. Each bit represents one channel, and the LSB indicates channel 1.
virestore	0 ~ 255	0	6/6	Indicate the source of video input signal restore. Each bit represents one channel, and the LSB indicates channel 1.
mdwin	<integer>	0	6/6	Indicate the source window id of motion detection. This field is required when trigger condition is “md”. One bit represents one window. The LSB indicates the 1st window. For example, to detect the 1st and 3rd windows, set mdwin as 5.
inter	1~999	1	6/6	Interval of snapshots in minutes. This field is used when trigger condition is “seq”.

weekday	0~127	127	6/6	Indicate which weekday is scheduled.
				One bit represents one weekday.
				bit0 (LSB) = Saturday
				bit1 = Friday
				bit2 = Thursday
				bit3 = Wednesday
				bit4 = Tuesday
				bit5 = Monday
				bit6 = Sunday
				For example, to detect events on Friday and Sunday, set weekday as 66.

begintime	hh:mm	00:00	6/6	Begin time of the weekly schedule.
endtime	hh:mm	24:00	6/6	End time of the weekly schedule. (00:00 ~ 24:00 sets schedule as always on)

action_do_i<0~(ndo-1)>_enable	0, 1	0	6/6	Enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	1	6/6	Duration of the digital output trigger in seconds.
action_do_i<0~(ndo-1)>_delay	0~999	0	6/6	The delay time needed before triggering the digital output (in seconds)
action_goto_c<0~(nvideoin-1)>_enable	<boolean>	0	6/6	Indicate whether recalling the preset position is enabled. 0: Disabled 1: Enabled
action_goto_c<0~(nvideoin-1)>_name	string[40]	<blank>	6/6	The preset position name used for recalling.
action_cf_enable	0. 1	0	6/6	Enable media write on CF or other local storage media
action_cf_folder	string[128]	NULL	6/6	Path to store media.
action_cf_media	0~7, 101	NULL	6/6	Index of the attached media.
action_cf_datefolder	<boolean>	1	6/6	Enable this to create folders by date, time, and hour automatically.
action_cf_backup	<boolean>	0	6/6	Enable the capability of backing up recorded files to the SD card when network is lost. 0: Disabled 1: Enabled
action_server_i<0~4>_enable	0, 1	0	6/6	Enable or disable this server action.
action_server_i<0~4>_media	0~7, 101	NULL	6/6	Index of the attached media.
action_server_i<0~4>_datefolder	<boolean>	0	6/6	Enable this to create folders by date, time, and hour automatically. 0: Disabled 1: Enabled

action_server_i<0~4>_foldername	string[40]	%Y%M%D%H	6/6	The template of the folder name to be created. Slashes can be used in the template, and following placeholders can also be used: %Y: Year (e.g. 2010) %M: Month %D: Date %H: Hour

7.27 Server setting for event action

Group: **server_i**<0~4>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	email, ftp, http, ns	email	6/6	Indicate the server type: "email" = email server "ftp" = FTP server "http" = HTTP server "ns" = network storage
http_url	string[128]	http://	6/6	URL of the HTTP server to upload.
http_username	string[64]	NULL	6/6	Username to log in to the server.
http_passwd	string[64]	NULL	6/6	Password of the user.
ftp_address	string[128]	NULL	6/6	FTP server address.
ftp_username	string[64]	NULL	6/6	Username to log in to the server.
ftp_passwd	string[64]	NULL	6/6	Password of the user.
ftp_port	0~65535	21	6/6	Port to connect to the server.
ftp_location	string[128]	NULL	6/6	Location to upload or store the media.
ftp_passive	0, 1	1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode
email_address	string[128]	NULL	6/6	Email server address.
email_sslmode	0, 1	0	6/6	Enable support SSL.
email_port	0~65535	25	6/6	Port to connect to the server.
email_username	string[64]	NULL	6/6	Username to log in to the server.
email_passwd	string[64]	NULL	6/6	Password of the user.

email_senderemail	string[128]	NULL	6/6	Email address of the sender.
email_recipientemail	string[128]	NULL	6/6	Email address of the recipient.
ns_location	string[128]	NULL	6/6	Location to upload or store the media.
ns_username	string[64]	NULL	6/6	Username to log in to the server.
ns_passwd	string[64]	NULL	6/6	Password of the user.
ns_workgroup	string[64]	NULL	6/6	Workgroup for network storage.

7.28 Media setting for event action

Group: **media_i<0~4>** (media_freespace is used internally.)

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	snapshot, systemlog, videoclip, recordmsg	snapshot	6/6	Media type to send to the server or store on the server.
snapshot_source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
snapshot_prefix	string[16]		6/6	Indicate the prefix of the filename.
snapshot_datesuffix	0, 1	0	6/6	Add date and time suffix to filename: 1 = Add date and time suffix. 0 = Do not add.
snapshot_preevent	0 ~ 7	1	6/6	Indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	1	6/6	The number of post-event images.
snapshot_channel	0 ~ 7	0	6/6	Indicates the channel of media source. 0~7 for 8 channels. 0 = channel 1, 1 = channel 2, … 7 = channel 8, etc.

videoclip_source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
videoclip_prefix	string[16]		6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	0	6/6	Indicates the time for pre-event recording in seconds.
videoclip_maxduration	1 ~ 20	5	6/6	Maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 5000	1000	6/6	Maximum size of one video clip file in Kbytes.
videoclip_channel	0 ~ 7	0	6/6	Indicates the channel of media source. 0~7 for 8 channels. 0 = channel 1, 1 = channel 2, … 7 = channel 8, etc.

7.29 Recording

Group: **recording_i**<0~1>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry.
enable	0, 1	0	6/6	Enable or disable this recording.
priority	0, 1, 2	1	6/6	Indicate the priority of this recording: “0” indicates low priority. “1” indicates normal priority. “2” indicates high priority.
channel	0~4	0	6/6	Indicate which channel is used for recording.
source	0	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and so on.
limitsize	0,1	0	6/6	0: Entire free space mechanism 1: Limit recording size mechanism

cyclic	0,1	0	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	0,1	1	6/6	0: Disable recording notification 1: Enable recording notification

notifyserver	0~31	0	6/6	Indicate which notification server is scheduled.
				One bit represents one application server (server_i0~i4).
				bit0 (LSB) = server_i0.
				bit1 = server_i1.
				bit2 = server_i2.
				bit3 = server_i3.
				bit4 = server_i4.
				For example, enable server_i0, server_i2, and server_i4 as notification servers; the notifyserver value is 21.

weekday	0~127	127	6/6	Indicate which weekday is scheduled.
				One bit represents one weekday.
				bit0 (LSB) = Saturday
				bit1 = Friday
				bit2 = Thursday
				bit3 = Wednesday
				bit4 = Tuesday
				bit5 = Monday
				bit6 = Sunday
				For example, to detect events on Friday and Sunday, set weekday as 66.

begintime	hh:mm	00:00	6/6	Start time of the weekly schedule.
endtime	hh:mm	24:00	6/6	End time of the weekly schedule. (00:00~24:00 indicates schedule always on)
prefix	string[16]	<blank>	6/6	Indicate the prefix of the filename.
cyclesize	16~	100	6/6	The maximum size for cycle recording in Kbytes when choosing to limit recording size.

reserveamount	0~15000000	15	6/6	The reserved amount in Mbytes when choosing cyclic recording mechanism.
dest	cf, 0~4	cf	6/6	The destination to store the recorded data. "cf" means local storage (CF or SD card). "0" means the index of the network storage.
cffolder	string[128]	NULL	6/6	Folder name.
trigger	schedule, networkfail	schedule	6/6	The event trigger type schedule: The event is triggered by schedule networkfail: The event is triggered by the failure of network connection.
adaptive_enable	0,1	0	6/6	Indicate whether the adaptive recording is enabled
adaptive_preevent	0~9	5	6/6	Indicate when is the adaptive recording started before the event trigger point (seconds)
adaptive_postevent	0~10	5	6/6	Indicate when is the adaptive recording stopped after the event trigger point (seconds)

7.30 HTTPS

Group: **https** (capability.protocol.https > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	To enable or disable secure HTTP.
policy	<Boolean>	0	6/6	If the value is 1, it will force HTTP connection redirect to HTTPS connection

method	auto,
	manual,
	install
		Auto	6/6	auto => Create self-signed certificate automatically.
				manual => Create self-signed certificate manually.
				install => Create certificate

				request and install.
status	-3 ~ 1	0	6/7	Specify the https status. -3 = Certificate not installed -2 = Invalid public key -1 = Waiting for certificate 0 = Not installed 1 = Active
countryname	string[2]	TW	6/6	Country name in the certificate information.
stateorprovincename	string[128]	Asia	6/6	State or province name in the certificate information.
localityname	string[128]	Asia	6/6	The locality name in the certificate information.
organizationname	string[64]	Vivotek.Inc	6/6	Organization name in the certificate information.
unit	string[32]	Vivotek.Inc	6/6	Organizational unit name in the certificate information.
commonname	string[64]	www.vivotek.com	6/6	Common name in the certificate information.
validdays	0 ~ 3650	3650	6/6	Valid period for the certification.

7.31 Storage management setting

Currently it's for local storage (SD, CF card)

Group: **disk_i<0~(n-1)>** n is the total number of storage devices. (capability.storage.dbenabled > 0)

cyclic_enabled	<boolean>	0	6/6	Enable cyclic storage method.
autocleanup_enabled	<boolean>	0	6/6	Enable automatic clean up method. Expired and not locked media files will be deleted.
autocleanup_maxage	<positive integer>	7	6/6	To specify the expired days for automatic clean up.

8. Useful Functions

8.1 Drive the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/setdo.cgi?do1=<state>[&do2=<state>]
[&do3=<state>][&do4=<state>]
```

Where state is 0 or 1; "0" means inactive or normal state, while "1" means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – Inactive, normal state
		1 – Active, triggered state

Example: Drive the digital output 1 to triggered state and redirect to an empty page.
http://myserver/cgi-bin/dido/setdo.cgi?do1=1

8.2 Query Status of the Digital Input (capability.ndi > 0)

Note: This request requires Viewer privileges
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]
```

If no parameter is specified, all of the digital input statuses will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[di0=<state>]\r\n
[di1=<state>]\r\n
[di2=<state>]\r\n
[di3=<state>]\r\n
```

where <*state*> can be 0 or 1.

Example: Query the status of digital input 1 .

```
Request:
http://myserver/cgi-bin/dido/getdi.cgi?di1

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
di1=1\r\n
```

8.3 Query Status of the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]
```

If no parameter is specified, all the digital output statuses will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[do0=<state>]\r\n
[do1=<state>]\r\n
[do2=<state>]\r\n
[do3=<state>]\r\n
```

where <*state*> can be 0 or 1.

Example: Query the status of digital output 1.

```
Request:
http://myserver/cgi-bin/dido/getdo.cgi?do1

Response:
HTTP/1.0 200 OK\r\n
```

```
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
do1=1\r\n
```

8.4 Capture Single Snapshot

Note: This request requires Normal User privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>][&streamid=<value>]
```

If the user requests a size larger than all stream settings on the server, this request will fail.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	The channel number of the video source.
resolution	<available resolution>	0	The resolution of the image.
quality	1~5	3	The quality of the image.
streamid	0~(m-1)	0	The stream number.

The server will return the most up-to-date snapshot of the selected channel and stream in JPEG format. The size and quality of the image will be set according to the video settings on the server.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]

<binary JPEG image data>
```

8.5 Account Management

Note: This request requires Administrator privileges.
Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<*name*>[&userpass=<*value*>][&privilege=<*value*>]
[&privilege=<value>][…][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to the server. When using this method, the "username" field is necessary. It will use the default value of other fields if not specified.
	Delete	Remove an account from the server. When using this method, the "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, the "username" field is necessary, and other fields are optional. If not specified, it will keep the original settings.
username	<name>	The name of the user to add, delete, or edit.
userpass	<value>	The password of the new user to add or that of the old user to modify. The default value is an empty string.
Privilege	<value>	The privilege of the user to add or to modify.
	viewer	Viewer privilege.
	operator	Operator privilege.
	admin	Administrator privilege.
Return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.6 System Logs

Note: This request require Administrator privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/syslog.cgi
```

Server will return the most up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n
```

8.7 Upgrade Firmware

Note: This request requires Administrator privileges.

Method: POST

Syntax:

```
http://<servername>/cgi-bin/admin/upgrade.cgi
```

Post data:

```
fimage=<file name>[&return=<return page>]\r\n
\r\n
<multipart encoded form data>
```

Server will accept the file named <file name> to upgrade the firmware and return with <return page> if indicated.

8.8 Camera Control (capability.ptzenabled)

Note: This request requires Viewer privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/camctrl.cgi?[channel=<value>][&camid=<value>]
[&move=<value>] – Move home, up, down, left, right
[&focus=<value>] – Focus operation
[&iris=<value>] – Iris operation
[&auto=<value>] – Auto pan, patrol
[&zoom=<value>] – Zoom in, out
[&zooming=<value>&zs=<value>] – Zoom without stopping, used for joystick
[&vx=<value>&vy=<value>&vs=<value>] – Shift without stopping, used for joystick
[&x=<value>&y=<value>&videosize=<value>&resolution=<value>&stretch=<value>] – Click on image
(Move the center of image to the coordination (x,y) based on resolution or videosize.)
[ [&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>][&speedlink=<value>] ] – Set speeds
[&return=<return page>]
```

Example:

http://myserver/cgi-bin/viewer/camctrl.cgi?channel=0&camid=1&move=right
http://myserver/cgi-bin/viewer/camctrl.cgi?channel=0&camid=1&zoom=tele
http://myserver/cgi-bin/viewer/camctrl.cgi?channel=0&camid=1&x=300&y=200&resolution=704x480&videosize=704x480&strech=1

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
camid	0,<positive integer>	Camera ID.
move	home	Move to camera to home position.
	up	Move camera up.
	down	Move camera down.
	left	Move camera left.
	right	Move camera right.
speedpan	-5 ~ 5	Set the pan speed.

speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.
speedfocus	-5 ~ 5	Set the focus speed.
speedapp	-5 ~ 5	Set the auto pan/patrol speed.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop camera.
zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.
	stop	Stop zoom.
zooming	wide or tele	Zoom without stopping for larger view or further view with zs speed, used for joystick control.
zs	0 ~ 11	Set the speed of zooming, “0” means stop.
vx	<integer , excluding 0>	The slope of movement = vy/vx, used for joystick control.
vy	<integer>	
vs	0 ~ 11	Set the speed of movement, “0” means stop.
x	<integer>	x-coordinate clicked by user. It will be the x-coordinate of center after movement.
y	<integer>	y-coordinate clicked by user. It will be the y-coordinate of center after movement.
videosize	<window size>	The size of plug-in (ActiveX) window in web page
resolution	<window size>	The resolution of streaming.
stretch	<boolean>	0 indicates that it uses **resolution** (streaming size) as the range of the coordinate system. 1 indicates that it uses **videosize** (plug-in size) as the range of the coordinate system.
focus	auto	Auto focus.
	far	Focus on further distance.
	near	Focus on closer distance.
iris	auto	Let the Network Camera control iris size.
	open	Manually control the iris for bigger size.
	close	Manually control the iris for smaller size.

speedlink	0 ~ 4	Issue speed link command.
gaptime	0~32768	The gaptime between two consecutive ptz commands for device. (unit: ms)
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.9 Recall (capability.ptzenabled)

Note: This request requires Viewer privileges.
Method: GET

Syntax:

```
http://<servername>/cgi-bin/viewer/recall.cgi?
recall=<value>[&channel=<value>][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
recall	Text string less than 30 characters	One of the present positions to recall.
channel	<0~(n-1)>	Channel of the video source.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.10 Preset Locations (capability.ptzenabled)

Note: This request requires Operator privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/operator/preset.cgi?[channel=<value>]
[&addpos=<value>][&delpos=<value>][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
addpos	<Text string less than 30 characters>	Add one preset location to the preset list.
channel	<0~(n-1)>	Channel of the video source.
delpos	<Text string less than 30 characters>	Delete preset location from preset list.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.11 IP Filtering

Note: This request requires Administrator access privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/ipfilter.cgi?
method=<value>&[start=<ipaddress>&end=<ipaddress>][&index=<value>]
[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
method	addallow	Add allowed IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.

	adddeny	Add denied IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	deleteallow	Remove allowed IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
	deletedeny	Remove denied IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start	<ip address>	The starting IP address to add or to delete.
end	<ip address>	The ending IP address to add or to delete.
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.11.1 IP Filtering for ONVIF

Syntax: <product dependent>

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?type[=<value>]
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=add<v4/v6>&ip=<*ipaddress*>[&index=<value>][&return=<*return page*>]
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=del<v4/v6>&index=<value>[&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
type	NULL	Get IP filter type
	allow, deny	Set IP filter type
method	addv4	Add IPv4 address into access list.
	addv6	Add IPv6 address into access list.
	delv4	Delete IPv4 address from access list.
	delv6	Delete IPv6 address from access list.

ip	<IP address>	Single address: <IP address> Network address: <IP address / network mask> Range address:<start IP address - end IP address>
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.12 UART HTTP Tunnel Channel (capability.nuart > 0)

Note: This request requires Operator privileges.
Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/operator/uartchannel.cgi?[channel=<value>]
------------------------------------------------------------------------
GET /cgi-bin/operator/uartchannel.cgi?[channel=<value>]
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache

------------------------------------------------------------------------
POST /cgi-bin/operator/uartchannel.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
```

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through a proxy server.

This channel will help to transfer the raw data of UART over the network.
Please see UART tunnel spec for detail information

PARAMETER	VALUE	DESCRIPTION
channel	0 ~ (n-1)	The channel number of UART.

8.13 Event/Control HTTP Tunnel Channel (capability. evctrlchannel > 0)

Note: This request requires Administrator privileges.
Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/admin/ctrlevent.cgi
------------------------------------------------------------------------
GET /cgi-bin/admin/ctrlevent.cgi
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache

------------------------------------------------------------------------
POST /cgi-bin/admin/ ctrlevent.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
```

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through the proxy server.

This channel will help perform real-time event subscription and notification as well as camera control more efficiently. The event and control formats are described in another document.

See Event/control tunnel spec for detail information

8.14 Get SDP of Streams

Note: This request requires Viewer access privileges.
Method: GET/POST

Syntax:

```
http://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

"m" is the stream number.
"network_accessname_<0~(m-1)>" is the accessname for stream "1" to stream "m". Please refer to the "subgroup of network: rtsp" for setting the accessname of SDP.
You can get the SDP by HTTP GET.
When using scalable multicast, Get SDP file which contains the multicast information via HTTP.

8.15 Open the Network Stream

Note: This request requires Viewer access privileges.

Syntax:
For HTTP push server (MJPEG):

```
http://<servername>/<network_http_s<0~m-1>_accessname>
```

For RTSP (MP4), the user needs to input the URL below into an RTSP compatible player.

```
rtsp://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

"m" is the stream number.
For details on streaming protocol, please refer to the "control signaling" and "data format" documents.

8.16 Senddata (capability.nuart > 0)

Note: This request requires Viewer privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/senddata.cgi?
[com=<value>][&data=<value>][&flush=<value>] [&wait=<value>] [&read=<value>]
```

PARAMETER	VALUE	DESCRIPTION
com	1 ~ <max. com port number>	The target COM/RS485 port number.
data	<hex decimal data>[,<hex decimal data>]	The <hex decimal data> is a series of digits from 0 ~ 9, A ~ F. Each comma separates the commands by 200 milliseconds.
flush	yes,no	yes: Receive data buffer of the COM port will be cleared before read. no: Do not clear the receive data buffer.
wait	*1 ~ 65535*	Wait time in milliseconds before read data.
read	*1 ~ 128*	The data length in bytes to read. The read data will be in the return page.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
<hex decimal data>\r\n
```

Where hexadecimal data is digits from 0 ~ 9, A ~ F.

8.17 Storage managements (capability.storage.dbenabled > 0)

Note: This request requires administrator privileges.

Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=<cmd_type>[&<parameter>=<value>…]
```

The commands usage and their input arguments are as follows.

PARAMETER	VALUE	DESCRIPTION
cmd_type	<string>	Required. Command to be executed, including *search*, *insert*, *delete*, *update*, and *queryStatus*.

Command: **search**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Optional. The integer primary key column will automatically be assigned a unique integer.
triggerType	<text>	Optional. Indicate the event trigger type. Please embrace your input value with single quotes. Ex. mediaType='motion' Support trigger types are product dependent.
mediaType	<text>	Optional. Indicate the file media type. Please embrace your input value with single quotes. Ex. mediaType='videoclip' Support trigger types are product dependent.
destPath	<text>	Optional. Indicate the file location in camera. Please embrace your input value with single quotes. Ex. destPath ='/mnt/auto/CF/NCMF/abc.mp4'
resolution	<text>	Optional. Indicate the media file resolution. Please embrace your input value with single quotes. Ex. resolution='800x600'

isLocked	<boolean>	Optional. Indicate if the file is locked or not. 0: file is not locked. 1: file is locked. A locked file would not be removed from UI or cyclic storage.
triggerTime	<text>	Optional. Indicate the event trigger time. (not the file created time) Format is "YYYY-MM-DD HH:MM:SS" Please embrace your input value with single quotes. Ex. triggerTime='2008-01-01 00:00:00' If you want to search for a time period, please apply "TO" operation. Ex. triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59' is to search for records from the start of Jan 1st 2008 to the end of Jan 1st 2008.
limit	<positive integer>	Optional. Limit the maximum number of returned search records.
offset	<positive integer>	Optional. Specifies how many rows to skip at the beginning of the matched records. Note that the offset keyword is used after limit keyword.

To increase the flexibility of search command, you may use "OR" connectors for logical "OR" search operations. Moreover, to search for a specific time period, you can use "TO" connector.
Ex. To search records triggered by motion or di or sequential and also triggered between 2008-01-01 00:00:00 and 2008-01-01 23:59:59.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=search&triggerType='motion'+OR+'di'+OR+'seq'
&triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59'
```

Command: **delete**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1

Ex. Delete records whose key numbers are 1, 4, and 8.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=delete&label=1&label=4&label=8
```

Command: **update**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1
isLocked	<boolean>	Required. Indicate if the file is locked or not.

Ex. Update records whose key numbers are 1 and 5 to be locked status.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=1&label=1&label=5
```

Ex. Update records whose key numbers are 2 and 3 to be unlocked status.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=0&label=2&label=3
```

Command: queryStatus

PARAMETER	VALUE	DESCRIPTION
retType	xml or javascript	Optional. Ex. retype=javascript The default return message is in XML format.

Ex. Query local storage status and call for javascript format return message.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=queryStatus&retType=javascript
```

8.18 Virtual input (capability.nvi > 0)

Note: Change virtual input (manual trigger) status.

Method: GET

Syntax:

```
http://<servername>/cgi-bin/admin/setvi.cgi?vi0=<value>[&vi1=<value>][&vi2=<value>]
[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
vi<num>	state[(duration)nstate]	Ex: vi0=1 Setting virtual input 0 to trigger state

	Where "state" is 0, 1. “0” means inactive or normal state while “1” means active or triggered state. Where "nstate" is next state after duration.	Ex: vi0=0(200)1 Setting virtual input 0 to normal state, waiting 200 **milliseconds**, setting it to trigger state. Note that when the virtual input is waiting for next state, it cannot accept new requests.
return	*<return page>*	Redirect to the page *<return page>* after the request is completely assigned. The *<return page>* can be a full URL path or relative path according the current path. If you omit this parameter, it will redirect to an empty page.

Return Code	Description
200	The request is successfully executed.
400	The request cannot be assigned, ex. incorrect parameters. Examples: 1. setvi.cgi?vi0=0(10000)1(15000)0(20000)1 No multiple duration. 2. setvi.cgi?vi3=0 VI index is out of range. 3. setvi.cgi?vi=1 No VI index is specified.
503	The resource is unavailable, ex. Virtual input is waiting for next state. Examples: 1. setvi.cgi?vi0=0(15000)1 2. setvi.cgi?vi0=1 Request 2 will not be accepted during the execution time(15 seconds).

8.19 Open Timeshift Stream (capability.timeshift > 0, timeshift_enable=1, timeshift_c<n>_s<m>_allow=1)

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

```
http://<servername>/<network_http_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&refti
me=<value>&forcechk&minsft=<value>]
```

For RTSP (MP4 and H264), the user needs to input the URL below into an RTSP compatible player.

```
rtsp://<servername>/<network_rtsp_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&refti
me=<value>&forcechk&minsft=<value>]
```

"n" is the channel index.

"m" is the timeshift stream index.

For details on timeshift stream, please refer to the "TimeshiftCaching" documents.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
maxsft	<positive integer>	0	Request cached stream at most how many seconds ago.
tsmode	normal, adaptive	normal	Streaming mode: normal => Full FPS all the time. adaptive => Default send only I-frame for MP4 and H.264, and send 1 FPS for MJPEG. If DI , VI or motion window are triggered, the streaming is changed to send full FPS for 10 seconds. (*Note: this parameter also works on non-timeshift streams.)
reftime	mm:ss	The time camera receives the request.	Reference time for maxsft and minsft. (This provides more precise time control to eliminate the inaccuracy due to network latency.) Ex: Request the streaming from 12:20 rtsp://10.0.0.1/live.sdp?maxsft=10&reftime=12:30
forcechk	N/A	N/A	Check if the requested stream enables timeshift, feature and if minsft is achievable. If false, return "415 Unsupported Media Type".

minsft	<positive integer>	0	How many seconds of cached stream client can accept at least. (Used by forcechk)

Return Code	Description
400 Bad Request	Request is rejected because some parameter values are illegal.
415 Unsupported Media Type	Returned, if forcechk appears, when minsft is not achievable or the timeshift feature of the target stream is not enabled.

<End of document>

3. General CGI URL Syntax and Parameters

When the CGI request includes internal camera parameters, these parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in functionally-related directories under the cgi-bin directory. The file extension .cgi is required.

Syntax:

```
http://<servername>/cgi-bin/<subdir>[/<subdir>...]/<cgi>.<ext>
[?<parameter>=<value>[&<parameter>=<value>...]]
```

Example: Set digital output #1 to active

```
http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1
```

4. Security Level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, camctrl	1. Can view, listen, talk to camera. 2. Can control DI/DO, PTZ of the camera.
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator access rights can modify most of the camera's parameters except some privileges and network options.
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator access rights can fully control the camera's operations.
7	N/A	Internal parameters. Unable to be changed by any external interfaces.

5. Get Server Parameter Values

Note: The access right depends on the URL directory.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/anonymous/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/viewer/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/operator/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/admin/getparam.cgi?[<parameter>]
[&<parameter>…]
```

Where the <*parameter*> should be <*group*>[_<*name*>]. If you do not specify any parameters, all the parameters on the server will be returned. If you specify only <*group*>, the parameters of the related group will be returned.

When querying parameter values, the current parameter values are returned.
A successful control request returns parameter pairs as follows:
Return:

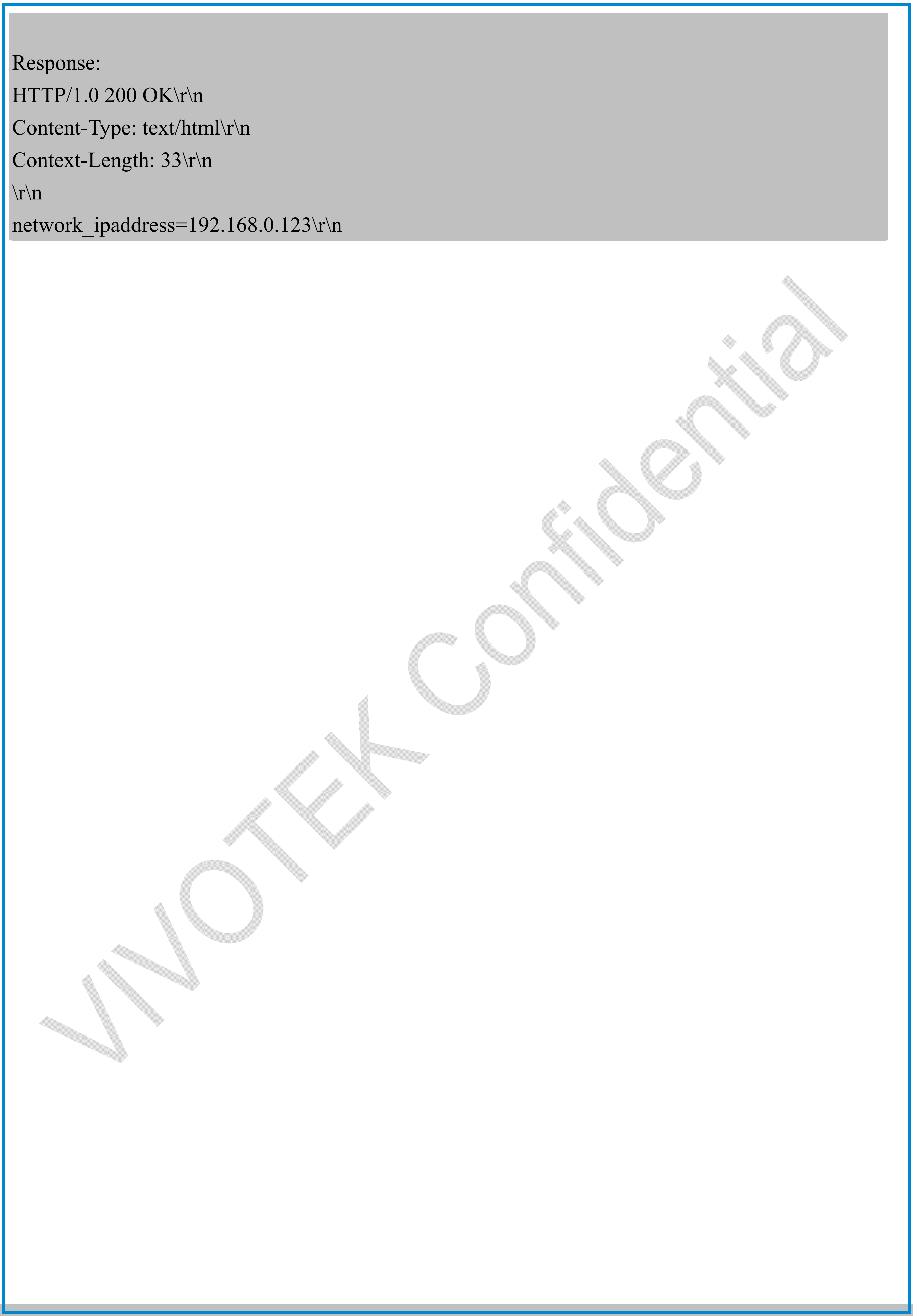
```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is
<parameter>=<value>\r\n
[<parameter pair>]

<length> is the actual length of content.

Example: Request IP address and its response

Request:
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress



```
Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network_ipaddress=192.168.0.123\r\n
```

6. Set Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/anonymous/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&return=<return page>]

http://<servername>/cgi-bin/viewer/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&return=<return page>]

http://<servername>/cgi-bin/operator/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&return=<return page>]

http://<servername>/cgi-bin/admin/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign *<value>* to the parameter *<group>*_*<name>*.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. (Note: The return page can be a general HTML file (.htm, .html). It cannot be a CGI command or have any extra parameters. This parameter must be placed at the end of the parameter list

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

Only the parameters that you set and are readable will be returned.

Example: Set the IP address of server to 192.168.0.123:

```
Request:
http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network_ipaddress=192.168.0.123\r\n
```

7. Available parameters on the server

This chapter defines all the parameters which can be configured or retrieved from VIVOTEK network camera or video server. The general format of description is listed in the table below

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text strings shorter than 'n' characters. The characters ",', <,>,& are invalid.
string[n~m]	Text strings longer than \`n' characters and shorter than \`m' characters. The characters ",', <,>,& are invalid.
password[<n>]	The same as string but displays '*' instead.
integer	Any number between (-2^{31} – 1) and (2^{31} – 1).
positive integer	Any number between 0 and (2^{32} – 1).
<m> ~ <n>	Any number between 'm' and 'n'.
domain name[<n>]	A string limited to a domain name shorter than 'n' characters (eg. www.ibm.com).
email address [<n>]	A string limited to an email address shorter than 'n' characters (eg. joe@www.ibm.com).
ip address	A string limited to an IP address (eg. 192.168.1.1).
mac address	A string limited to contain a MAC address without hyphens or colons.
boolean	A boolean value of 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>, <value3>, …	Enumeration. Only given values are valid.
blank	A blank string.
everything inside <>	A description
integer primary key	SQLite data type. A 32-bit signed integer. The value is assigned a unique integer by the server.
text	SQLite data type. The value is a text string, stored using the database encoding (UTF-8, UTF-16BE or UTF-16-LE).
coordinate	x, y coordinate (eg. 0,0)
window size	window width and height (eg. 800x600)

NOTE: The camera should not be restarted when parameters are changed.

7.1 system

Group: **system**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	"Video Server"	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
ledoff	<boolean>	0	6/6	Turn on (0) or turn off (1) all led indicators.
date	<YYYY/MM/DD>, keep, auto	<current date>	6/6	Current date of system. Set to 'keep' to keep date unchanged. Set to 'auto' to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	<current time>	6/6	Current time of the system. Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	<MMDDhhmmYYYY.ss>	<current time>	6/6	Another current time format of the system.
ntp	<domain name>, <ip address>, <blank>	<blank>	6/6	NTP server. *Do not use "skip to invoke default server" for default value.
timezoneindex	-489 ~ 529	0	6/6	Indicate timezone and area. -480: GMT-12:00

				Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona -240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan -200: GMT-05:00 Eastern Time, New York, Toronto -201: GMT-05:00 Bogota, Lima, Quito, Indiana -180: GMT-04:30 Caracas -160: GMT-04:00 Atlantic Time, Canada, La Paz, Santiago -140: GMT-03:30 Newfoundland -120: GMT-03:00 Brasilia, Buenos

				Aires, Georgetown, Greenland -80: GMT-02:00 Mid-Atlantic -40: GMT-01:00 Azores, Cape_Verde_IS. 0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London 40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris 41: GMT 01:00 Warsaw, Budapest, Bern 80: GMT 02:00 Athens, Helsinki, Istanbul, Riga 81: GMT 02:00 Cairo 82: GMT 02:00 Lebanon, Minsk 83: GMT 02:00 Israel 120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi 121: GMT 03:00 Iraq 140: GMT 03:30 Tehran

				160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan 180: GMT 04:30 Kabul 200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra,

				Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Auckland, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'alofa
daylight_enable	<boolean>	0	6/6	Enable automatic daylight saving time in time zone.
daylight_auto_begintime	string[19]	NONE	6/7	Display the current daylight saving start time.
daylight_auto_endtime	string[19]	NONE	6/7	Display the current daylight saving end time.
daylight_timezones	string	,-360,-320, -280,-240, -241,-200, -201,-160, -140,-120, -80,-40,0, 40,41,80, 81,82,83, 120,140, 380,400,480	6/6	List time zone index which support daylight saving time.
updateinterval	0, 3600, 86400, 604800, 2592000	0	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.

restore	0, <positive integer>	N/A	7/6	Restore the system parameters to default values after <value> seconds.
reset	0, <positive integer>	N/A	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	<Any value>	N/A	7/6	Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
restoreexceptdst	<Any value>	N/A	7/6	Restore the system parameters to default values except all daylight saving time settings. This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to default values except for a

				union of combined results.
restoreexceptlang	<Any Value>	N/A	7/6	Restore the system parameters to default values except the custom language file the user has uploaded. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.

7.1.1 system.info

Subgroup of **system**: **info** (The fields in this group are unchangeable.)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	VS8801	0/7	Internal model name of the server (e.g. IP7139)
extendedmodelname	string[40]	VS8801	0/7	ODM specific model name of server (e.g. DCS-5610). If it is not an ODM model, this field will be equal to "modelname"
serialnumber	<mac address>	<product mac address>	0/7	12 characters MAC address (without hyphens).
firmwareversion	string[40]		0/7	Firmware version, including model, company, and version number in the format: <MODEL-BRAND-VERSION>
language_count	<integer>	9	0/7	Number of webpage languages

				available on the server.
language_i<0~(count-1)>	string[16]	English, Deutsch, Español, Français, Italiano, 日本語, Português, 简体中文, 繁體中文	0/7	Available language lists.
customlanguage_maxcount	<integer>	1	0/6	Maximum number of custom languages supported on the server.
customlanguage_count	<integer>	0	0/6	Number of custom languages which have been uploaded to the server.
customlanguage_i<0~(maxcount-1)>	string	N/A	0/6	Custom language name.

7.2 status

Group: **status**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
signal_c<0~(nvideoin-1)>	<Boolean>	0	1/7	0=> No signal. 1=> Signal detected.
videomode_c<0~(nvideoin-1)>	ntsc, pal	ntsc	1/7	Video modulation type
di_i<0~(ndi-1)>	<boolean>	0	1/7	0 => Inactive, normal 1 => Active, triggered (capability.ndi > 0)
do_i<0~(ndo-1)>	<boolean>	0	1/7	0 => Inactive, normal 1 => Active, triggered (capability.ndo > 0)
onlinenum_rtsp	integer	0	6/7	Current number of RTSP connections.
onlinenum_httppush	integer	0	6/7	Current number of HTTP push server connections.
eth_i0	<string>	<blank>	1/7	Get network information from

				mii-tool.
vi_i<0~(nvi-1)>	<boolean>	0	1/7	Virtual input 0 => Inactive 1 => Active (capability.nvi > 0)

7.3 digital input behavior define

Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	high	1/1	Indicates open circuit or closed circuit (inactive status)

7.4 digital output behavior define

Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	open	1/1	Indicate open circuit or closed circuit (inactive status)

7.5 security

Group: **security**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
privilege_do	view, operator, admin	operator	6/6	Indicate which privileges and above can control digital output (capability.ndo > 0)
privilege_camctrl	view, operator, admin	view	6/6	Indicate which privileges and above can control PTZ (capability.ptzenabled > 0 or capability.eptz > 0)
user_i0_name	string[64]	root	6/7	User name of root
user_i<1~20>_name	string[64]	<blank>	6/7	User name
user_i0_pass	password[64]	<blank>	6/6	Root password

user_i<1~20>_pass	password[64]	<blank>	7/6	User password
user_i0_privilege	viewer, operator, admin	admin	6/7	Root privilege
user_i<1~20>_ privilege	viewer, operator, admin	<blank>	6/6	User privilege

7.6 network

Group: **network**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
preprocess	<positive integer>	NULL	7/6	An 32-bit integer, each bit can be set separately as follows: Bit 0 => HTTP service; Bit 1=> HTTPS service; Bit 2=> FTP service; Bit 3 => Two way audio and RTSP Streaming service; To stop service before changing its port settings. It's **recommended** to set this parameter when change a service port to the port occupied by another service currently. Otherwise, the service may fail. Stopped service will auto-start after changing port settings. Ex: Change HTTP port from 80 to 5556, and change RTP port for video from 5556 to 20480. Then, set preprocess=9 to stop both service first. "/cgi-bin/admin/setparam.cgi? network_preprocess=9&network_http_port=5556 & network_rtp_videoport=20480"
type	lan, pppoe	lan	6/6	Network connection type.
resetip	<boolean>	1	6/6	1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot.

				0 => Use preset ipaddress, subnet, rounter, dns1, and dns2.
ipaddress	<ip address>	192.168.0.99	6/6	IP address of server.
subnet	<ip address>	<blank>	6/6	Subnet mask.
router	<ip address>	<blank>	6/6	Default gateway.
dns1	<ip address>	<blank>	6/6	Primary DNS server.
dns2	<ip address>	<blank>	6/6	Secondary DNS server.
wins1	<ip address>	<blank>	6/6	Primary WINS server.
wins2	<ip address>	<blank>	6/6	Secondary WINS server.

7.6.1 802.1x

Subgroup of **network: ieee8021x** (capability.protocol.ieee8021x > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable IEEE 802.1x
eapmethod	eap-peap, eap-tls	eap-peap	6/6	Selected EAP method
identity_peap	String[64]	<blank>	6/6	PEAP identity
identity_tls	String[64]	<blank>	6/6	TLS identity
password	String[254]	<blank>	6/6	Password for TLS
privatekeypassword	String[254]	<blank>	6/6	Password for PEAP
ca_exist	<boolean>	0	6/6	CA installed flag
ca_time	<integer>	0	6/7	CA installed time. Represented in EPOCH
ca_size	<integer>	0	6/7	CA file size (in bytes)
certificate_exist	<boolean>	0	6/6	Certificate installed flag (for TLS)
certificate_time	<integer>	0	6/7	Certificate installed time. Represented in EPOCH
certificate_size	<integer>	0	6/7	Certificate file size (in bytes)
privatekey_exist	<boolean>	0	6/6	Private key installed flag (for

				TLS)
privatekey_time	<integer>	0	6/7	Private key installed time. Represented in EPOCH
privatekey_size	<integer>	0	6/7	Private key file size (in bytes)

7.6.2 QOS

Subgroup of **network: qos_cos** (capability.protocol.qos.cos > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable CoS (IEEE 802.1p)
vlanid	1~4095	1	6/6	VLAN ID
video	0~7	0	6/6	Video channel for CoS
audio	0~7	0	6/6	Audio channel for CoS (capability.naudio > 0)
eventalarm	0~7	0	6/6	Event/alarm channel for CoS
management	0~7	0	6/6	Management channel for CoS
eventtunnel	0~7	0	6/6	Event/Control channel for CoS

Subgroup of **network: qos_dscp** (capability.protocol.qos.dscp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable DSCP
video	0~63	0	6/6	Video channel for DSCP
audio	0~63	0	6/6	Audio channel for DSCP (capability.naudio > 0)
eventalarm	0~63	0	6/6	Event/alarm channel for DSCP
management	0~63	0	6/6	Management channel for DSCP
eventtunnel	0~63	0	6/6	Event/Control channel for DSCP

7.6.3 IPV6

Subgroup of **network**: **ipv6** (capability.protocol.ipv6 > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable IPv6.
addonipaddress	<ip address>	<blank>	6/6	IPv6 IP address.
addonprefixlen	0~128	64	6/6	IPv6 prefix length.
addonrouter	<ip address>	<blank>	6/6	IPv6 router address.

addondns	<ip address>	<blank>	6/6	IPv6 DNS address.
allowoptional	<boolean>	0	6/6	Allow manually setup of IP address setting.

7.6.4 FTP

Subgroup of **network**: **ftp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	21, 1025~65535	21	6/6	Local ftp server port.

7.6.5 HTTP

Subgroup of **network**: **http**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	80	6/6	HTTP port.
alternateport	1025~65535	8080	6/6	Alternate HTTP port.
authmode	basic, digest	basic	1/6	HTTP authentication mode.
anonymousviewing	<boolean>	0	1/6	Enable anoymous streaming viewing.

Subgroup of **network**: **http_c<0~(n-1)>** for n channel products and c is channel count[1~n]

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
s0_accessname	string[32]	"video.mjpg" for c = 1. "video2.mjpg" for c = 2. "video3.mjpg" for c = 3, and so on.	1/6	HTTP server push access name for channel c stream 1. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 0)
s1_accessname	string[32]	"video1-2.mjpg" for c = 1. "video2-2.mjpg" for c = 2, and so on.	1/6	HTTP server push access name for channel c stream 2. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 1)

For compatibility, **network_http_s<0~(t-1)>_accessname** are reserved, t = n*m for n channel

products, and m is stream number per channel.
*Note: We can get n by (capability.nvideoin), and get m by (capability.nmediastream).

Besides, we map the first stream of each channel: **network_http_c<0~(n-1)>_s0_accessname** to **network_http_s<0~(n-1)>_accessname** and map the second stream of each channel: **network_http_c<0~(n-1)>_s1_accessname** to **network_http_s<n~(n*2-1)>_accessname** and so on.

Take VS8401 as an example, channel 1 stream 1: **network_http_c0_s0_accessname** is mapped to **network_http_s0_accessname** and channel 1 stream 2: **network_http_c0_s1_accessname** is mapped to **network_http_s4_accessname**.

7.6.6 HTTPS port

Subgroup of **network**: **https_port** (capability.protocol.https > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	443, 1025 ~ 65535	443	6/6	HTTPS port.

7.6.7 RTSP

Subgroup of **network**: **rtsp** (capability.protocol.rtsp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	554	1/6	RTSP port. (capability.protocol.rtsp=1)
anonymousviewing	<boolean>	0	1/6	Enable anoymous streaming viewing.
authmode	disable, basic, digest	disable	1/6	RTSP authentication mode. (capability.protocol.rtsp=1)

Subgroup of **network**: **rtsp_c<0~(n-1)>** for n channel products and c is channel count[1~n] (capability.protocol.rtsp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
s0_accessname	string[32]	"live.sdp" for c = 1. "live2.sdp" for c = 2.	1/6	RTSP access name for channel c stream 1. (capability.protocol.rtsp=1 and capability.nmediastream > 0)

		"live3.sdp" for c = 3, and so on.		
s1_accessname	string[32]	"live1-2.sdp" for c = 1. "live2-2.sdp" for c = 2, and so on.	1/6	RTSP access name for channel c stream 2. (capability.protocol.rtsp=1 and capability.nmediastream > 1)

For compatibility, **network_rtsp_s<0~(t-1)>_accessname** are reserved, t = n*m for n channel products, and m is stream number per channel.
*Note: We can get n by (capability.nvideoin), and get m by (capability.nmediastream).

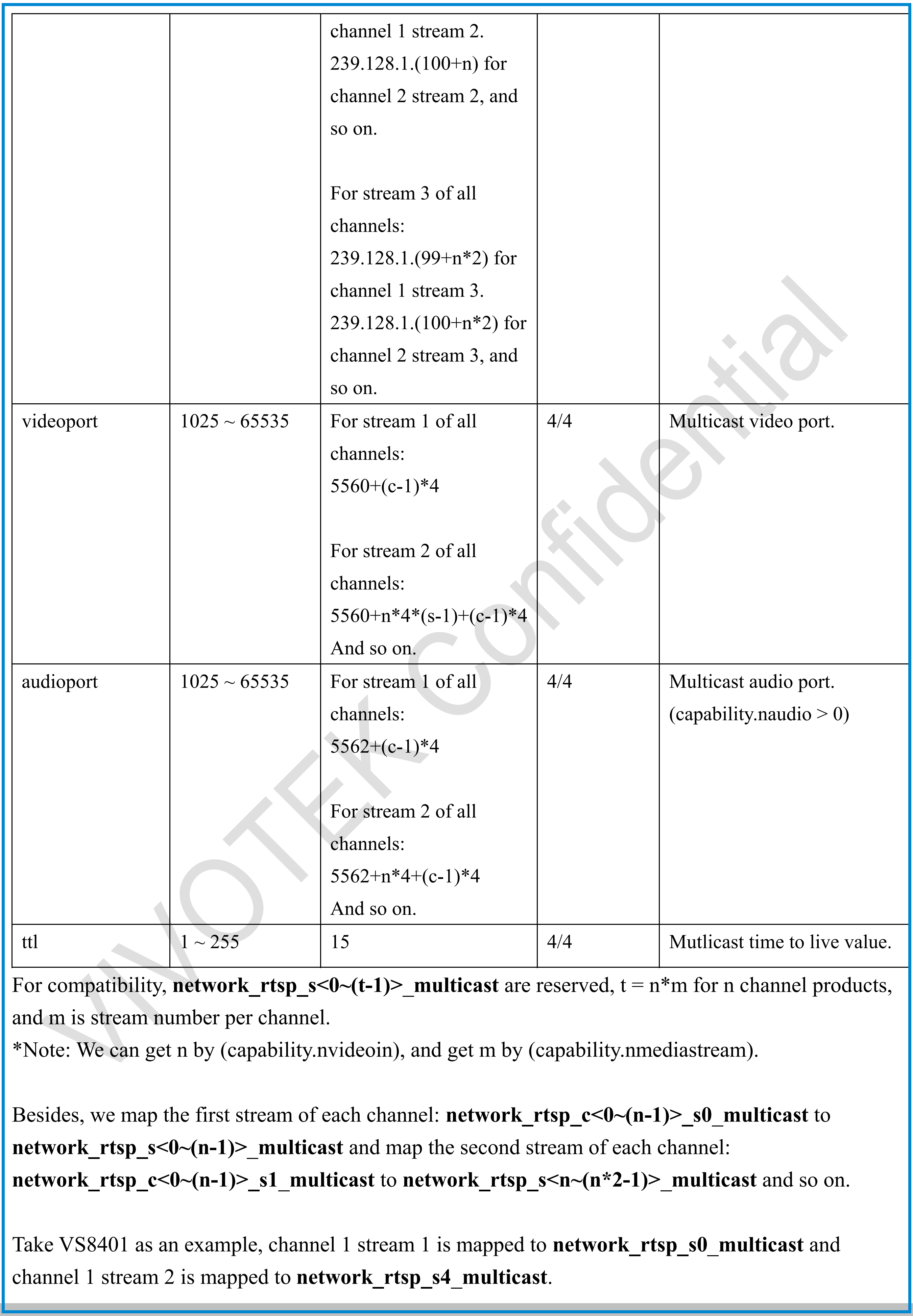
Besides, we map the first stream of each channel: **network_rtsp_c<0~(n-1)>_s0_accessname** to **network_rtsp_s<0~(n-1)>_accessname** and map the second stream of each channel: **network_rtsp_c<0~(n-1)>_s1_accessname** to **network_rtsp_s<n~(n*2-1)>_accessname** and so on.

Take VS8401 as an example, channel 1 stream 1: **network_rtsp_c0_s0_accessname** is mapped to **network_rtsp_s0_accessname** and channel 1 stream 2: **network_rtsp_c0_s1_accessname** is mapped to **network_rtsp_s4_accessname**.

7.6.7.1 RTSP multicast

Subgroup of **network_rtsp_c<0~(n-1)>_s<0~(m-1)>_multicast** for n channel products, and m is stream number per channel, c is channel count[1~n], s is stream count[1~m] (capability.protocol.rtp.multicast > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	0	4/4	Enable always multicast.
ipaddress	<ip address>	For stream 1 of all channels: 239.128.1.99 for channel 1 stream 1. 239.128.1.100 for channe 2 stream 1, and so on. For stream 2 of all channels: 239.128.1.(99+n) for	4/4	Multicast IP address.



		channel 1 stream 2. 239.128.1.(100+n) for channel 2 stream 2, and so on. For stream 3 of all channels: 239.128.1.(99+n*2) for channel 1 stream 3. 239.128.1.(100+n*2) for channel 2 stream 3, and so on.		
videoport	1025 ~ 65535	For stream 1 of all channels: 5560+(c-1)*4 For stream 2 of all channels: 5560+n*4*(s-1)+(c-1)*4 And so on.	4/4	Multicast video port.
audioport	1025 ~ 65535	For stream 1 of all channels: 5562+(c-1)*4 For stream 2 of all channels: 5562+n*4+(c-1)*4 And so on.	4/4	Multicast audio port. (capability.naudio > 0)
ttl	1 ~ 255	15	4/4	Mutlicast time to live value.

For compatibility, **network_rtsp_s<0~(t-1)>_multicast** are reserved, t = n*m for n channel products, and m is stream number per channel.
*Note: We can get n by (capability.nvideoin), and get m by (capability.nmediastream).

Besides, we map the first stream of each channel: **network_rtsp_c<0~(n-1)>_s0_multicast** to **network_rtsp_s<0~(n-1)>_multicast** and map the second stream of each channel: **network_rtsp_c<0~(n-1)>_s1_multicast** to **network_rtsp_s<n~(n*2-1)>_multicast** and so on.

Take VS8401 as an example, channel 1 stream 1 is mapped to **network_rtsp_s0_multicast** and channel 1 stream 2 is mapped to **network_rtsp_s4_multicast**.

7.6.8 SIP port

Subgroup of **network**: **sip** (capability.protocol.sip> 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	1025 ~ 65535	5060	1/6	SIP port.

7.6.9 RTP port

Subgroup of **network**: **rtp**

NAME	VALUE	DEFAULT	SECURIT Y (get/set)	DESCRIPTION
videoport	1025 ~ 65535	5556	6/6	Video channel port for RTP. (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	5558	6/6	Audio channel port for RTP. (capability.protocol.rtp_unicast=1)

7.6.10 PPPoE

Subgroup of **network**: **pppoe** (capability.protocol.pppoe > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
user	string[128]	<blank>	6/6	PPPoE account user name.
pass	password[64]	<blank>	6/6	PPPoE account password.

7.7 Ipfilter for ONVIF

Group: **ipfilter**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable access list filtering.
admin_enable	<boolean>	0	6/6	Enable administrator IP address.
admin_ip	String[44]	<blank>	6/6	Administrator IP address.
maxconnection	1~10	10	6/6	Maximum number of concurrent streaming connection(s).

type	0, 1	1	6/6	Ipfilter policy : 0 => allow 1 => deny
ipv4list_i<0~9>	Single address: <ip address> Network address: <ip address / network mask> Range address:<start ip address - end ip address>	<blank>	6/6	IPv4 address list.
ipv6list_i<0~9>	String[44]	<blank>	6/6	IPv6 address list.

7.8 Video input setting per channel

Group: **videoin_c<0~(n-1)>** for n channel products, and m is stream number

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
whitebalance	auto, manual	auto	4/4	"auto" indicates auto white balance. "manual" indicates keep current value.
color	0, 1	1	4/4	0 =>monochrome 1 => color
flip	<boolean>	0	4/4	Flip the image.
mirror	<boolean>	0	4/4	Mirror the image.
ptzstatus	<integer>	2	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support)

				Bit 3 => Support **tilt** operation; 0(not support), 1(support) Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)
text	string[16]	<blank>	1/4	Enclose caption.
imprinttimestamp	<boolean>	0	4/4	Overlay time stamp and enclose caption on video.
s<0~(m-1)>_codectype	mpeg4, mjpeg, h264	h264	1/4	Video codec type.
s<0~(m-1)>_resolution	D1, 4CIF, CIF, QCIF	4CIF	1/4	Video resolution in pixels.
s<0~(m-1)>_ratiocorrect	<boolean>	0	1/4	Change resolution to fit 4:3 ratio. For PAL: D1/4CIF(720/704x576) -> (768x576) CIF(352x288)->(384x288) For NTSC: D1/4CIF(720/704x480) -> (640x480) CIF(352x240)->(320x240)
s<0~(m-1)>_mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_mpeg4_ratecontrolmode	cbr, vbr	vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_quant	0~5 99, 100	3	4/4	Quality of video when choosing vbr in "ratecontrolmode". 0, 99,100 is the customized

				manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_mpeg4_qvalue	1~31	7	4/4	Manual video quality level input. (s<0~(m-1)>_mpeg4_quant = 0, 99) *Note: This is reserved for campatibility, and we recommend changing to use "s<0~(m-1)>_mpeg4_qpercent".
s<0~(m-1)>_mpeg4_qpercent	1~100	29	4/4	Set quality by percentage. 1: Worst quality 100: Best quality (s<0~(m-1)>_mpeg4_quant = 100)
s<0~(m-1)>_mpeg4_bitrate	1000~4000000	51200	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_mpeg4_maxframe	1~30	20	1/4	Set maximum frame rate in fps (for MPEG-4).
s<0~(m-1)>_h264_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_h264_ratecontrolmode	cbr, vbr	vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_h264_quant	0~5,99,100	3	4/4	Quality of video when choosing vbr in "ratecontrolmode". 0, 99 and 100 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_h264_qvalue	0~51	26	4/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 0, 99)

				*Note: This is reserved for campatibility, and we recommend changing to use "s<0~(m-1)>_h264_qpercent".
s<0~(m-1)>_h264_qpercent	1~100	45	4/4	Set quality by percentage. 1: Worst quality 100: Best quality (s<0~(m-1)>_h264_quant = 100)
s<0~(m-1)>_h264_bitrate	1000~4000000	512000	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_h264_maxframe	1~30	20	1/4	Set maximum frame rate in fps (for h264).
s<0~(m-1)>_h264_profile	0~2	1	1/4	Indicate H264 profiles 0: baseline 1: main profile 2: high profile
s<0~(m-1)>_mjpeg_quant	0 ~ 5,99, 100	3	4/4	Quality of JPEG video. 0, 99 and 100 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_mjpeg_qvalue	0~200	50	4/4	Manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 0, 99) *Note: This is reserved for campatibility, we recommend changing to use "s<0~(m-1)>_mjpeg_qpercent".
s<0~(m-1)>_mjpeg_qpercent	1~100	49	4/4	Set quality by percentage. 1: Worst quality 100: Best quality (s<0~(m-1)>_mjpeg_quant = 100)

s<0~(m-1)>_mjpeg_maxframe	1~30	20	1/4	Set maximum frame rate in fps (for JPEG).

7.9 Image setting per channel

Group: **image_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5 ~ 5, 100	100	4/4	Adjust brightness of image according to mode settings. 100 means using "brightnesspercent". *Note: This is reserved for campatibility, and we recommend changing to use "brightnesspercent".
saturation	-5 ~ 5, 100	100	4/4	Adjust saturation of image according to mode settings. 100 means using "saturationpercent". *Note: This is reserved for campatibility, and we recommend changing to use "saturationpercent".
contrast	-5 ~ 5, 100	100	4/4	Adjust contrast of image according to mode settings. 100 means using "contrastpercent". *Note: This is reserved for campatibility, and we recommend changing to use "contrastpercent".
sharpness	-5 ~ 5, 100	100	4/4	Adjust sharpness of image according to mode settings. 100 means using "sharpnesspercent". *Note: This is reserved for

				campatibility, and we recommend changing to use "sharpnesspercent".
brightnesspercent	0 ~ 100	50	4/4	Adjust brightness of image by percentage. Darker 0 <-> 100 Brighter
saturationpercent	0 ~ 100	50	4/4	Adjust saturation of image by percentage. Less 0 <-> 100 More saturation
contrastpercent	0 ~ 100	50	4/4	Adjust contrast of image by percentage. Less 0 <-> 100 More contrast
sharpnesspercent	0~100	30	4/4	Adjust sharpness of image by percentage. Softer 0 <-> 100 Sharper
xoffset	-4 ~ 4	2	4/4	Change start point of input image in horizontal.
yoffset	-4 ~ 4	2	4/4	Change start point of input image in vertical.
deinterlace_enable	<boolean>	1	4/4	Enable de-interlace
deinterlace_mode	adaptive, blend	adaptive	4/4	Adaptive: Detect moving area and perform de-interlace on it. This mode leads to better image quality, but consumes more resource. Blend: Use blend method to perform de-interlace.
IBPE_edgeenable	<boolean>	0	4/4	Enable edge enhancement.
IBPE_edgestrength	1 ~ 128	14	4/4	Adjust edge enhancement strength. 1 is minimum and 128 is maximum.
IBPE_nrenable	<boolean>	0	4/4	Enable noise reduction.
IBPE_nrmode	1 ~ 3	1	4/4	Adjust noise reduction mode. 1 => DeGaussian 2 => DeImpulse 3 => DeGaussian + DeImpulse
IBPE_nrstrength	1 ~ 63	1	4/4	Adjust noise reduction strength. 1 is minimum and 63 is maximum.

*Note: Saving value between -5~+5 to "brightness" will save its corresponding value to "brightnesspercent" automatically, and then the value of "brightness" will be set back to 100 to take effect..

Saving value to “saturation”, “contrast”, or “sharpness” has the same behavior.

7.10 Audio input per channel

Group: **audioin_c<0~(n-1)>** for n channel products (capability.audioin>0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
mute	0, 1	1	1/4	Enable audio mute.
gain	0~15	8	4/4	Gain of input.
s0_g711_mode	pcmu, pcma	pcmu	4/4	Set G.711 mode.

7.11 Time Shift settings

Group: **timeshift**, c for n channel products, m is stream number (capability.timeshift > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable time shift streaming.
c<0~(n-1)>_s<0~(m-1)>_allow	<boolean>	0	4/4	Enable time shift streaming for specific stream.

7.12 Motion detection settings

Group: **motion_c<0~(n-1)>** for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable motion detection.
win_i<0~2>_enable	<boolean>	0	4/4	Enable motion window 1~3.
win_i<0~2>_name	string[40]	<blank>	4/4	Name of motion window 1~3.
win_i<0~2>_left	0 ~ 320	0	4/4	Left coordinate of window position.
win_i<0~2>_top	0 ~ 240	0	4/4	Top coordinate of window position.
win_i<0~2>_width	0 ~ 320	0	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	0	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	0	4/4	Percent of motion detection

				window.
win_i<0~2>_sensitivity	0 ~ 100	0	4/4	Sensitivity of motion detection window.

7.13 Tempering detection settings

Group: **tampering_c<0~(n-1)>** for n channel product (capability.tampering > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable or disable tamper detection.
threshold	0 ~ 255	32	1/99	Threshold of tamper detection.
duration	10 ~ 600	10	4/4	If tampering value exceeds the 'threshold' for more than 'duration' second(s), then tamper detection is triggered.

7.14 DDNS

Group: **ddns** (capability.ddns > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the dynamic DNS.

provider	Safe100,
	DyndnsDynamic,
	DyndnsCustom,
	TZO,
	DHS,
	DynInterfree,
	CustomSafe100
		DyndnsDynamic	6/6	Safe100 => safe100.net
				DyndnsDynamic => dyndns.org (dynamic)
				DyndnsCustom => dyndns.org (custom)
				TZO => tzo.com
				DHS => dhs.org
				DynInterfree =>dyn-interfree.it
				CustomSafe100 =>
				Custom server using safe100 method

<provider>_hostname	string[128]	<blank>	6/6	Your DDNS hostname.
<provider>_usernameemail	string[64]	<blank>	6/6	Your user name or email to login to the DDNS service provider
<provider>_passwordkey	string[64]	<blank>	6/6	Your password or key to login to the DDNS service provider.
<provider>_servername	string[128]	<blank>	6/6	The server name for safe100. (This field only exists if the provider

				is customsafe100)

7.15 UPnP presentation

Group: **upnppresentation**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	1	6/6	Enable or disable the UPnP presentation service.

7.16 UPnP port forwarding

Group: **upnpportforwarding**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the UPnP port forwarding service.
upnpnatstatus	0~3	0	6/7	The status of UPnP port forwarding, used internally. 0 = OK, 1 = FAIL, 2 = no IGD router, 3 = no need for port forwarding

7.17 Express link

Group:expresslink

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
state	onlycheck, onlyoffline, checkonline, badnetwork	<blank>	6/6	“onlycheck” : You have to input the host name of your camera and press "Register" button to register it. “onlyoffline” : Express link is active, you can now connect to this camera at expresslink_url. “checkonline” : Express link is not active. “badnetwork” : Express Link is not supported under this network environment.

url	string[64]	<blank>	6/6	The URL to connect to this camera by express link.

7.18 System log

Group: **syslog**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	0	6/6	Enable remote log.
serverip	<IP address>	<blank>	6/6	Log server IP address.
serverport	514, 1025~65535	514	6/6	Server port used for log.
level	0~7	6	6/6	Levels used to distinguish the importance of the information: 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG

7.19 camera PTZ control

Group: **camctrl** (capability.camctrl.httptunnel > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enablehttptunnel	<boolean>	0	4/4	Enable HTTP tunnel for camera control.

Group: **camctrl_c<0~(n-1)>** for n channel product (capability.ptzenabled)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
panspeed	-5 ~ 5	0	1/4	Pan speed
tiltspeed	-5 ~ 5	0	1/4	Tilt speed
zoomspeed	-5 ~ 5	0	1/4	Zoom speed
focusspeed	-5 ~ 5	0	1/4	Auto focus speed
preset_i<0~(npreset-1)>_name	string[40]	<blank>	1/4	Name of the preset location.

uart	0 ~ (m-1), m is UART count	0	1/4	Select corresponding uart (capability.nuart>0).
cameraid	0~255	1	1/4	Camera ID controlling external PTZ camera.
hometype	<boolean>	0	1/4	The attribute defines whether the HOME command emulation is enabled. 0: Use the preset position 0 as the home position 1: Use HOME command (if the camera supports it.)
isptz	0 ~ 2	0	1/4	0: disable PTZ commands. 1: enable PTZ commands with PTZ driver. 2: enable PTZ commands with UART tunnel.
disablemdonptz	<boolean>	0	1/4	Disable motion detection on PTZ operation.
patrolseq	string[120]	<blank>	1/4	(For external device) The indexes of patrol points, separated by ","
patroldwelling	string[160]	<blank>	1/4	(For external device) The dwelling time of each patrol point, separated by ","

7.20 UART control

Group: **uart** (capability.nuart > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
ptzdrivers_i<0~19, 127>_name	string[40]	<blank>	1/4	Name of the PTZ driver.
ptzdrivers_i<0~19, 127>_location	string[128]	<blank>	1/4	Full path of the PTZ driver.
enablehttptunnel	<boolean>	0	4/4	Enable HTTP tunnel channel to control UART.

Group: **uart_i<0~(n-1)>** n is uart port count (capability.nuart > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
baudrate	110,300,600,1200,2400,3600,4800,7200,9600,19200,38400,57600,115200	9600	4/4	Set baud rate of COM port.
databit	5,6,7,8	8	4/4	Data bits in a character frame.
paritybit	none, odd, even	none	4/4	For error checking.
stopbit	1,2	1	4/4	1 2-1.5 , data bit is 5 2-2
uartmode	rs485, rs232	rs485	4/4	RS485 or RS232.
customdrvcmd_i<0~9>	string[128]	<blank>	1/4	PTZ command for custom camera.
speedlink_i<0~15>_name	string[40]	<blank>	1/4	Additional PTZ command name.
speedlink_i<0~15>_cmd	string[40]	<blank>	1/4	Additional PTZ command list.
ptzdriver	0~19, 127 (custom), 128 (no driver)	128 (no driver)	4/4	The PTZ driver is used by this COM port.

7.21 SNMP

Group: **snmp** (capability.snmp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
v2	0~1	0	6/6	SNMP v2 enabled. 0 for disable, 1 for enable
v3	0~1	0	6/6	SNMP v3 enabled. 0 for disable, 1 for enable
secnamerw	string[31]	Private	6/6	Read/write security name
secnamero	string[31]	Public	6/6	Read only security name

authpwrw	string[8~128]	<blank>	6/6	Read/write authentication password
authpwro	string[8~128]	<blank>	6/6	Read only authentication password
authtyperw	MD5,SHA	MD5	6/6	Read/write authentication type
authtypero	MD5,SHA	MD5	6/6	Read only authentication type
encryptpwrw	string[8~128]	<blank>	6/6	Read/write password
encryptpwro	string[8~128]	<blank>	6/6	Read only password
encrypttyperw	DES	<blank>	6/6	Read/write encryption type
encrypttypero	DES	<blank>	6/6	Read only encryption type
rwcommunity	string[31]	Private	6/6	Read/write community
rocommunity	string[31]	Public	6/6	Ready only community

7.22 Layout configuration

Group: **layout**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
logo_default	<boolean>	1	1/6	0 => Custom logo 1 => Default logo
logo_link	string[40]	http://www.vivotek.com	1/6	Hyperlink of the logo
logo_powerbyvvtk_hidden	<boolean>	0	1/6	0 => display the power by vivotek logo 1 => hide the power by vivotek logo
theme_option	1~4	1	1/6	1~3: One of the default themes. 4: Custom definition.
theme_color_font	string[7]	#ffffff	1/6	Font color
theme_color_configfont	string[7]	#ffffff	1/6	Font color of configuration area.
theme_color_titlefont	string[7]	#098bd6	1/6	Font color of video title.
theme_color_controlbackground	string[7]	#565656	1/6	Background color of control area.
theme_color_configbackground	string[7]	#323232	1/6	Background color of

				configuration area.
theme_color_videobackground	string[7]	#565656	1/6	Background color of video area.
theme_color_case	string[7]	#323232	1/6	Frame color
custombutton_manualtrigger_show	<boolean>	1	1/6	Show or hide manual trigger (VI) button in homepage 0 -> Hidden 1 -> Visible

7.23 Privacy mask

Group: **privacymask_c<0~(n-1)>** for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable privacy mask.
win_i<0~4>_enable	<boolean>	0	4/4	Enable privacy mask window.
win_i<0~4>_name	string[14]	<blank>	4/4	Name of the privacy mask window.
win_i<0~4>_left	0 ~ 320/352	0	4/4	Left coordinate of window position.
win_i<0~4>_top	0 ~ 240/288	0	4/4	Top coordinate of window position.
win_i<0~4>_width	0 ~ 320/352	0	4/4	Width of privacy mask window.
win_i<0~4>_height	0 ~ 240/288	0	4/4	Height of privacy mask window.

7.24 Capability

Group: **capability**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
api_httpversion	0200a	0200a	0/7	The HTTP API version.
bootuptime	<positive integer>	60	0/7	Server bootup time.
nir	0, <positive	0	0/7	Number of IR interfaces. (Recommend to use ir for

	integer>			built-in IR and extir for external IR)
npir	0, <positive integer>	0	0/7	Number of PIRs.
ndi	0, <positive integer>	8	0/7	Number of digital inputs.
nvi	0, <positive integer>	4	0/7	Number of virtual inputs (manual trigger)
ndo	0, <positive integer>	8	0/7	Number of digital outputs.
naudioin	0, <positive integer>	8	0/7	Number of audio inputs.
naudioout	0, <positive integer>	8	0/7	Number of audio outputs.
nvideoin	<positive integer>	8	0/7	Number of video inputs.
nvideoinprofile	<positive integer>	0	0/7	Number of video input profiles.
nmediastream	<positive integer>	1	0/7	Number of media stream per channels.
nvideosetting	<positive integer>	1	0/7	Number of video settings per channel.
naudiosetting	<positive integer>	1	0/7	Number of audio settings per channel.
nuart	0, <positive integer>	1	0/7	Number of UART interfaces.
nmotionprofile	0, <positive integer>	0	0/7	Number of motion profiles.
ptzenabled	0, <positive integer>	189	0/7	An 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera

				control function;
				0(not support), 1(support)
				Bit 1 => Built-in or external camera;
				0(external), 1(built-in)
				Bit 2 => Support pan operation, 0(not support), 1(support)
				Bit 3 => Support tilt operation; 0(not support), 1(support)
				Bit 4 => Support zoom operation;
				0(not support), 1(support)
				Bit 5 => Support focus operation;
				0(not support), 1(support)
				Bit 6 => Support iris operation;
				0(not support), 1(support)
				Bit 7 => External or built-in PT; 0(built-in), 1(external)
				Bit 8 => Invalidate bit 1 ~ 7;
				0(bit 1 ~ 7 are valid),
				1(bit 1 ~ 7 are invalid)
				Bit 9 => Reserved bit; Invalidate lens_pan, lens_tilt, lens_zoon, lens_focus, len_iris.
				0(fields are valid),
				1(fields are invalid)

windowless	<boolean>	1	0/7	Indicate whether to support windowless plug-in.
eptz	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => stream 1 supports ePTZ or not.

				Bit 1 => stream 2 supports ePTZ or not. The rest may be deduced by analogy
lens_pan	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support pan. Bit 1 => Support pan in UI. Bit 2 => External or built-in pan function; 0(built-in), 1(external).
lens_tilt	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support tilt. Bit 1 => Support tilt in UI. Bit 2 => External or built-in tilt function; 0(built-in), 1(external).
lens_zoom	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support zoom Bit 1 => Support zoom in UI Bit 2 => External or built-in zoom function; 0(built-in), 1(external).
lens_focus	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support focus. Bit 1 => Support focus in UI. Bit 2 => External or built-in focus function; 0(built-in), 1(external). Bit 3 => Support auto focus

				in UI.
lens_iris	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support iris. Bit 1 => Support iris in UI. Bit 2 => External or build-in iris function; 0(build-in), 1(external). Bit 3 => Support auto iris in UI.
npreset	0, <positive integer>	20	0/7	Number of preset locations.
protocol_https	< boolean >	1	0/7	Indicate whether to support HTTP over SSL.
protocol_rtsp	< boolean >	1	0/7	Indicate whether to support RTSP.
protocol_sip	<boolean>	1	0/7	Indicate whether to support SIP.
protocol_maxconnection	<positive integer>	10	0/7	The maximum allowed simultaneous connections.
protocol_maxgenconnection	<positive integer>	10	0/7	The maximum general streaming connections .
protocol_maxmegaconnection	<positive integer>	0	0/7	The maximum megapixel streaming connections.
protocol_rtp_multicast_scalable	<boolean>	1	0/7	Indicate whether to support scalable multicast.
protocol_rtp_multicast_backchannel	<boolean>	0	0/7	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	1	0/7	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	1	0/7	Indicate whether to support RTP over HTTP.
protocol_spush_mjpeg	<boolean>	1	0/7	Indicate whether to support server push MJPEG.
protocol_snmp	<boolean>	1	0/7	Indicate whether to support SNMP.
protocol_ipv6	<boolean>	1	0/7	Indicate whether to support IPv6.

protocol_pppoe	<boolean>	1	0/7	Indicate whether to support PPPoE.
protocol_ieee8021x	<boolean>	1	0/7	Indicate whether to support IEEE802.1x.
protocol_qos_cos	<boolean>	1	0/7	Indicate whether to support CoS.
protocol_qos_dscp	<boolean>	1	0/7	Indicate whether to support QoS/DSCP.
protocol_ddns	<boolean>	1	0/7	Indicate whether to support DDNS.
videoin_type	0, 1, 2	0	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_resolution	<a list of available resolution separated by commas>	QCIF, CIF, 4CIF, D1	0/7	Available resolutions list.
videoin_maxframerate	<a list of available maximum frame rate separated by commas>	30, 30, 30, 30	0/7	Available maximum frame list.
videoin_codec	mpeg4. mjpeg, h264	mpeg4, mjpeg, h264	0/7	Available codec list.
timeshift	<boolean>	1	0/7	Indicate whether to support time shift caching stream.
audio_aec	<boolean>	0	0/7	Indicate whether to support acoustic echo cancellation.
audio_extmic	<boolean>	1	0/7	Indicate whether to support external microphone input.
audio_linein	<boolean>	0	0/7	Indicate whether to support external line input. (It will be replaced by audio_mic and audio_extmic.)
audio_lineout	<boolean>	0	0/7	Indicate whether to support

				line output.
audio_headphoneout	<boolean>	0	0/7	Indicate whether to support headphone output.
audioin_codec	aac4, gamr, g711	g711	0/7	Available codec list for audio input.
uart_httptunnel	<boolean>	1	0/7	Indicate whether to support HTTP tunnel for UART transfer.
camctrl_httptunnel	<boolean>	1	0/7	The attribute indicates whether sending camera control commands through HTTP tunnel is supported. 0: Not supported 1: Supported
camctrl_privilege	<boolean>	1	0/7	Indicate whether to support “Manage Privilege” of PTZ control in the Security page. 1: support both /cgi-bin/camctrl/camctrl.cgi and /cgi-bin/viewer/camctrl.cgi 0: support only /cgi-bin/viewer/camctrl.cgi
transmission_mode	Tx, Rx, Both	Tx	0/7	Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both = DVR.
network_wire	<boolean>	1	0/7	Indicate whether to support Ethernet.
network_wireless	<boolean>	0	0/7	Indicate whether to support wireless.
derivative_brand	<boolean>	1	0/7	Indicate whether to support the upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)

evctrlchannel	<boolean>	1	0/7	Indicate whether to support HTTP tunnel for event/control transfer.
joystick	<boolean>	0	0/7	Indicate whether to support joystick control.
storage_dbenabled	<boolean>	0	0/7	Media files are indexed in database.
nanystream	0, <positive integer>	0	0/7	number of any media stream per channel
iva	<boolean>	0	0/7	Indicate whether to support Intelligent Video analysis
version_onvifdaemon	<string>	<blank>	0/7	Indicate ONVIF daemon version
version_onvifevent	<string>	<blank>	0/7	Indicate ONVIF event version
media_totalspace	<positive integer>	60000	0/7	Available memory space (KB) for media.
media_snapshot_sizepersecond	<positive integer>	512	0/7	Maximum size (KB) of one snapshot image.
media_snapshot_maxpreevent	<positive integer>	7	0/7	Maximum snapshot number before event occurred.
media_snapshot_maxpostevent	<positive integer>	7	0/7	Maximum snapshot number after event occurred.
media_videoclip_maxsize	<positive integer>	5000	0/7	Maximum size (KB) of a videoclip.
media_videoclip_maxlength	<positive integer>	20	0/7	Maximum length (second) of a videoclip.
media_videoclip_maxpreevent	<positive integer>	9	0/7	Maximum duration (second) after event occurred in a videoclip.

7.25 Customized event script

Group: **event_customtaskfile_i**<0~2>

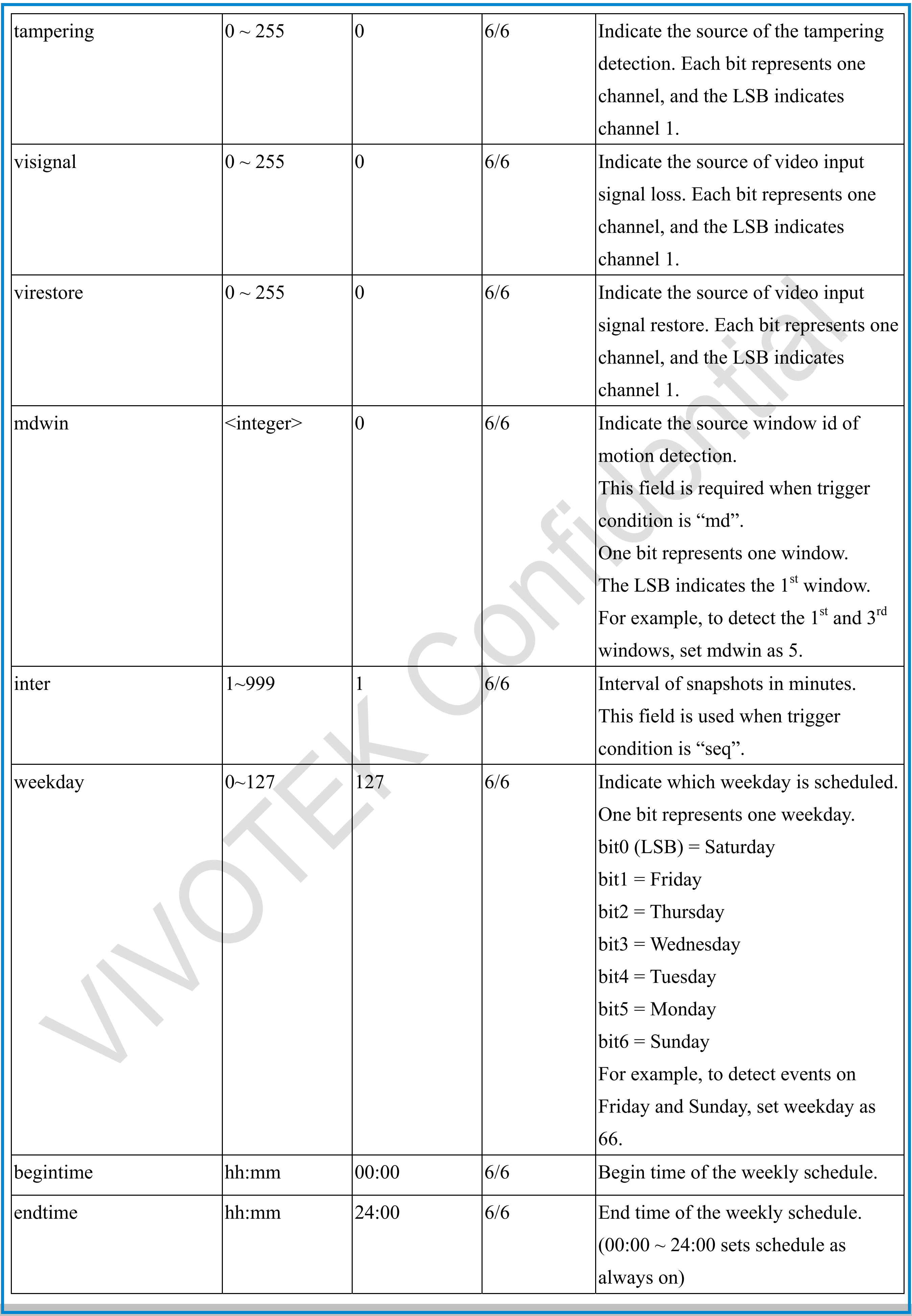
PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[41]	NULL	6/7	Custom script identification of this entry.
date	string[17]	NULL	6/7	Date of custom script.

time	string[17]	NULL	6/7	Time of custom script.

7.26 Event setting

Group: **event_i**<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry.
enable	0, 1	0	6/6	Enable or disable this event.
priority	0, 1, 2	1	6/6	Indicate the priority of this event: "0" = low priority "1" = normal priority "2" = high priority
delay	1~999	20	6/6	Delay in seconds before detecting the next event.
trigger	boot, di, motion, seq, tampering, visignal, virestore, vi	boot	6/6	Indicate the trigger condition: "boot" = System boot "di"= Digital input "motion" = Video motion detection "seq" = Periodic condition "tampering" = Tamper detection. "visignal" = Video input signal loss. "virestore" = Video input signal restore "vi"= Virtual input (Manual trigger)
triggerstatus	<string>	trigger	6/6	The status for event trigger
di	<integer>	0	6/6	Indicate the source id of di trigger. This field is required when trigger condition is "di". One bit represents one digital input. The LSB indicates DI 0.
vi	<integer>	0	6/6	Indicate the source id of vi trigger. This field is required when trigger condition is "vi". One bit represents one digital input. The LSB indicates VI 0.



tampering	0 ~ 255	0	6/6	Indicate the source of the tampering detection. Each bit represents one channel, and the LSB indicates channel 1.
visignal	0 ~ 255	0	6/6	Indicate the source of video input signal loss. Each bit represents one channel, and the LSB indicates channel 1.
virestore	0 ~ 255	0	6/6	Indicate the source of video input signal restore. Each bit represents one channel, and the LSB indicates channel 1.
mdwin	<integer>	0	6/6	Indicate the source window id of motion detection. This field is required when trigger condition is “md”. One bit represents one window. The LSB indicates the 1st window. For example, to detect the 1st and 3rd windows, set mdwin as 5.
inter	1~999	1	6/6	Interval of snapshots in minutes. This field is used when trigger condition is “seq”.

weekday	0~127	127	6/6	Indicate which weekday is scheduled.
				One bit represents one weekday.
				bit0 (LSB) = Saturday
				bit1 = Friday
				bit2 = Thursday
				bit3 = Wednesday
				bit4 = Tuesday
				bit5 = Monday
				bit6 = Sunday
				For example, to detect events on Friday and Sunday, set weekday as 66.

begintime	hh:mm	00:00	6/6	Begin time of the weekly schedule.
endtime	hh:mm	24:00	6/6	End time of the weekly schedule. (00:00 ~ 24:00 sets schedule as always on)

action_do_i<0~(ndo-1)>_enable	0, 1	0	6/6	Enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	1	6/6	Duration of the digital output trigger in seconds.
action_do_i<0~(ndo-1)>_delay	0~999	0	6/6	The delay time needed before triggering the digital output (in seconds)
action_goto_c<0~(nvideoin-1)>_enable	<boolean>	0	6/6	Indicate whether recalling the preset position is enabled. 0: Disabled 1: Enabled
action_goto_c<0~(nvideoin-1)>_name	string[40]	<blank>	6/6	The preset position name used for recalling.
action_server_i<0~4>_enable	0, 1	0	6/6	Enable or disable this server action.
action_server_i<0~4>_media	0~7, 101	NULL	6/6	Index of the attached media.
action_server_i<0~4>_datefolder	<boolean>	0	6/6	Enable this to create folders by date, time, and hour automatically. 0: Disabled 1: Enabled
action_server_i<0~4>_foldername	string[40]	%Y%M%D%H	6/6	The template of the folder name to be created. Slashes can be used in the template, and following placeholders can also be used: %Y: Year (e.g. 2010) %M: Month %D: Date %H: Hour

7.27 Server setting for event action

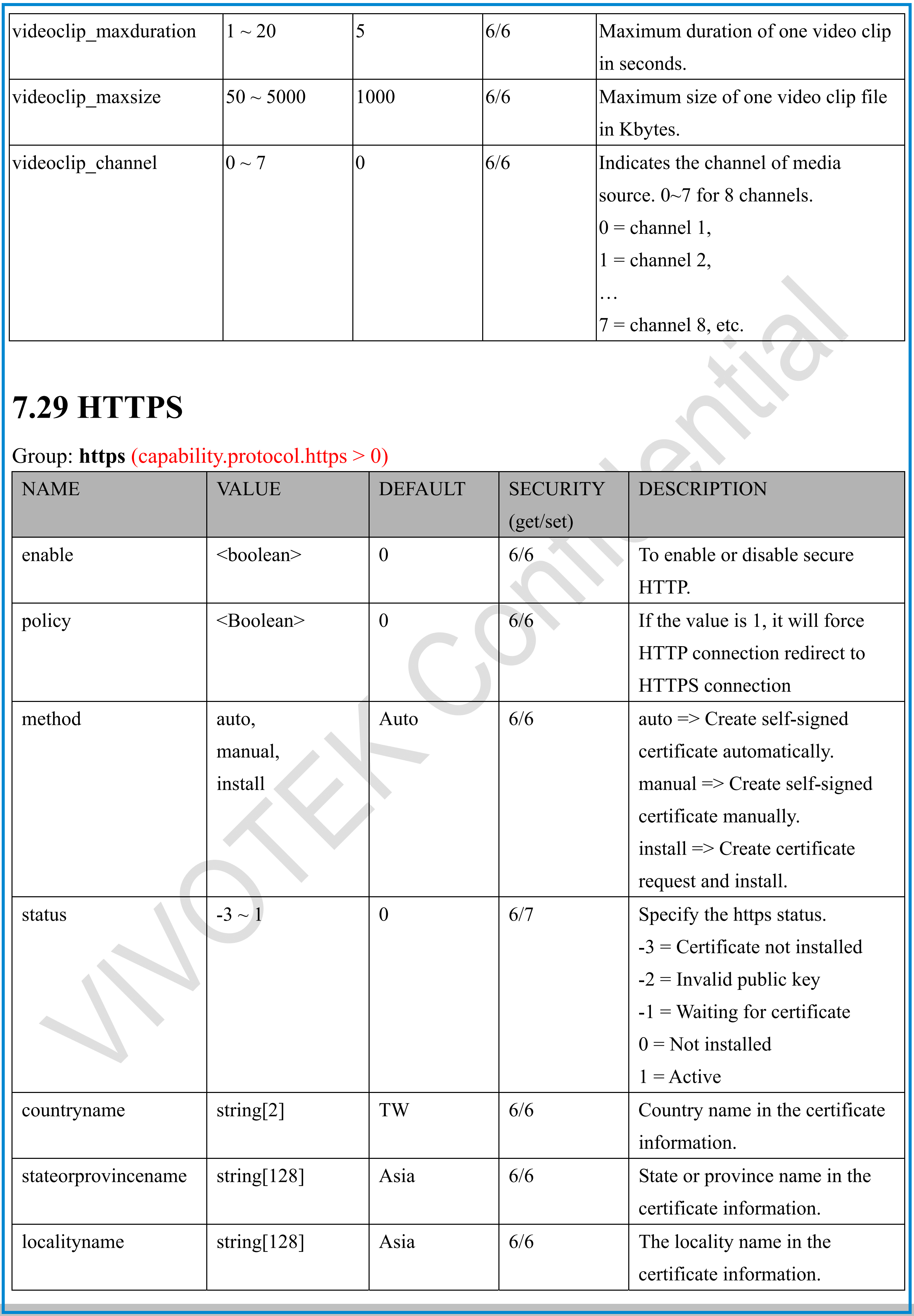
Group: **server_i**<0~4>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	email, ftp, http, ns	email	6/6	Indicate the server type: “email” = email server “ftp” = FTP server “http” = HTTP server “ns” = network storage
http_url	string[128]	http://	6/6	URL of the HTTP server to upload.
http_username	string[64]	NULL	6/6	Username to log in to the server.
http_passwd	string[64]	NULL	6/6	Password of the user.
ftp_address	string[128]	NULL	6/6	FTP server address.
ftp_username	string[64]	NULL	6/6	Username to log in to the server.
ftp_passwd	string[64]	NULL	6/6	Password of the user.
ftp_port	0~65535	21	6/6	Port to connect to the server.
ftp_location	string[128]	NULL	6/6	Location to upload or store the media.
ftp_passive	0, 1	1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode
email_address	string[128]	NULL	6/6	Email server address.
email_sslmode	0, 1	0	6/6	Enable support SSL.
email_port	0~65535	25	6/6	Port to connect to the server.
email_username	string[64]	NULL	6/6	Username to log in to the server.
email_passwd	string[64]	NULL	6/6	Password of the user.
email_senderemail	string[128]	NULL	6/6	Email address of the sender.
email_recipientemail	string[128]	NULL	6/6	Email address of the recipient.
ns_location	string[128]	NULL	6/6	Location to upload or store the media.
ns_username	string[64]	NULL	6/6	Username to log in to the server.
ns_passwd	string[64]	NULL	6/6	Password of the user.
ns_workgroup	string[64]	NULL	6/6	Workgroup for network storage.

7.28 Media setting for event action

Group: **media_i<0~4>** (media_freespace is used internally.)

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	snapshot, systemlog, videoclip, recordmsg	snapshot	6/6	Media type to send to the server or store on the server.
snapshot_source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
snapshot_prefix	string[16]		6/6	Indicate the prefix of the filename.
snapshot_datesuffix	0, 1	0	6/6	Add date and time suffix to filename: 1 = Add date and time suffix. 0 = Do not add.
snapshot_preevent	0 ~ 7	1	6/6	Indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	1	6/6	The number of post-event images.
snapshot_channel	0 ~ 7	0	6/6	Indicates the channel of media source. 0~7 for 8 channels. 0 = channel 1, 1 = channel 2, … 7 = channel 8, etc.
videoclip_source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
videoclip_prefix	string[16]		6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	0	6/6	Indicates the time for pre-event recording in seconds.



videoclip_maxduration	1 ~ 20	5	6/6	Maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 5000	1000	6/6	Maximum size of one video clip file in Kbytes.
videoclip_channel	0 ~ 7	0	6/6	Indicates the channel of media source. 0~7 for 8 channels. 0 = channel 1, 1 = channel 2, … 7 = channel 8, etc.

7.29 HTTPS

Group: **https** (capability.protocol.https > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	To enable or disable secure HTTP.
policy	<Boolean>	0	6/6	If the value is 1, it will force HTTP connection redirect to HTTPS connection

method	auto,
	manual,
	install
		Auto	6/6	auto => Create self-signed certificate automatically.
				manual => Create self-signed certificate manually.
				install => Create certificate request and install.

status	-3 ~ 1	0	6/7	Specify the https status. -3 = Certificate not installed -2 = Invalid public key -1 = Waiting for certificate 0 = Not installed 1 = Active
countryname	string[2]	TW	6/6	Country name in the certificate information.
stateorprovincename	string[128]	Asia	6/6	State or province name in the certificate information.
localityname	string[128]	Asia	6/6	The locality name in the certificate information.

organizationname	string[64]	Vivotek.Inc	6/6	Organization name in the certificate information.
unit	string[32]	Vivotek.Inc	6/6	Organizational unit name in the certificate information.
commonname	string[64]	www.vivotek .com	6/6	Common name in the certificate information.
validdays	0 ~ 3650	3650	6/6	Valid period for the certification.

8. Useful Functions

8.1 Drive the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/setdo.cgi?do1=<state>[&do2=<state>]
[&do3=<state>][&do4=<state>]
```

Where state is 0 or 1; “0” means inactive or normal state, while “1” means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – Inactive, normal state
		1 – Active, triggered state

Example: Drive the digital output 1 to triggered state and redirect to an empty page.

http://myserver/cgi-bin/dido/setdo.cgi?do1=1

8.2 Query Status of the Digital Input (capability.ndi > 0)

Note: This request requires Viewer privileges
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]
```

If no parameter is specified, all of the digital input statuses will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[di0=<state>]\r\n
[di1=<state>]\r\n
[di2=<state>]\r\n
[di3=<state>]\r\n
```

where <*state*> can be 0 or 1.

Example: Query the status of digital input 1 .

```
Request:
http://myserver/cgi-bin/dido/getdi.cgi?di1

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
di1=1\r\n
```

8.3 Query Status of the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]
```

If no parameter is specified, all the digital output statuses will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[do0=<state>]\r\n
[do1=<state>]\r\n
[do2=<state>]\r\n
[do3=<state>]\r\n
```

where <*state*> can be 0 or 1.

Example: Query the status of digital output 1.

```
Request:
http://myserver/cgi-bin/dido/getdo.cgi?do1

Response:
HTTP/1.0 200 OK\r\n
```

```
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
do1=1\r\n
```

8.4 Capture Single Snapshot

Note: This request requires Normal User privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>][&streamid=<value>]
```

If the user requests a size larger than all stream settings on the server, this request will fail.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	The channel number of the video source.
resolution	<available resolution>	0	The resolution of the image.
quality	1~5	3	The quality of the image.
streamid	0~(m-1)	0	The stream number.

The server will return the most up-to-date snapshot of the selected channel and stream in JPEG format. The size and quality of the image will be set according to the video settings on the server.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]

<binary JPEG image data>
```

8.5 Account Management

Note: This request requires Administrator privileges.
Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<*name*>[&userpass=<*value*>][&privilege=<*value*>]
[&privilege=<value>][…][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to the server. When using this method, the "username" field is necessary. It will use the default value of other fields if not specified.
	Delete	Remove an account from the server. When using this method, the "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, the "username" field is necessary, and other fields are optional. If not specified, it will keep the original settings.
username	<name>	The name of the user to add, delete, or edit.
userpass	<value>	The password of the new user to add or that of the old user to modify. The default value is an empty string.
Privilege	<value>	The privilege of the user to add or to modify.
	viewer	Viewer privilege.
	operator	Operator privilege.
	admin	Administrator privilege.
Return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.6 System Logs

Note: This request require Administrator privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/syslog.cgi
```

Server will return the most up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n
```

8.7 Upgrade Firmware

Note: This request requires Administrator privileges.
Method: POST

Syntax:

```
http://<servername>/cgi-bin/admin/upgrade.cgi
```

Post data:

```
fimage=<file name>[&return=<return page>]\r\n
\r\n
<multipart encoded form data>
```

Server will accept the file named <file name> to upgrade the firmware and return with <return page> if indicated.

8.8 Camera Control (capability.ptzenabled)

Note: This request requires Viewer privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/camctrl.cgi?[channel=<value>][&camid=<value>]
[&move=<value>] – Move home, up, down, left, right
[&focus=<value>] – Focus operation
[&iris=<value>] – Iris operation
[&auto=<value>] – Auto pan, patrol
[&zoom=<value>] – Zoom in, out
[&zooming=<value>&zs=<value>] – Zoom without stopping, used for joystick
[&vx=<value>&vy=<value>&vs=<value>] – Shift without stopping, used for joystick
[&x=<value>&y=<value>&videosize=<value>&resolution=<value>&stretch=<value>] – Click on image
(Move the center of image to the coordination (x,y) based on resolution or videosize.)
[ [&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>][&speedlink=<value>] ] – Set speeds
[&return=<return page>]
```

Example:

http://myserver/cgi-bin/viewer/camctrl.cgi?channel=0&camid=1&move=right
http://myserver/cgi-bin/viewer/camctrl.cgi?channel=0&camid=1&zoom=tele
http://myserver/cgi-bin/viewer/camctrl.cgi?channel=0&camid=1&x=300&y=200&resolution=704x480&videosize=704x480&strech=1

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
camid	0,<positive integer>	Camera ID.
move	home	Move to camera to home position.
	up	Move camera up.
	down	Move camera down.
	left	Move camera left.
	right	Move camera right.
speedpan	-5 ~ 5	Set the pan speed.

speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.
speedfocus	-5 ~ 5	Set the focus speed.
speedapp	-5 ~ 5	Set the auto pan/patrol speed.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop camera.
zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.
	stop	Stop zoom.
zooming	wide or tele	Zoom without stopping for larger view or further view with zs speed, used for joystick control.
zs	0 ~ 11	Set the speed of zooming, “0” means stop.
vx	<integer , excluding 0>	The slope of movement = vy/vx, used for joystick control.
vy	<integer>	
vs	0 ~ 11	Set the speed of movement, “0” means stop.
x	<integer>	x-coordinate clicked by user. It will be the x-coordinate of center after movement.
y	<integer>	y-coordinate clicked by user. It will be the y-coordinate of center after movement.
videosize	<window size>	The size of plug-in (ActiveX) window in web page
resolution	<window size>	The resolution of streaming.
stretch	<boolean>	0 indicates that it uses **resolution** (streaming size) as the range of the coordinate system. 1 indicates that it uses **videosize** (plug-in size) as the range of the coordinate system.
focus	auto	Auto focus.
	far	Focus on further distance.
	near	Focus on closer distance.
iris	auto	Let the Network Camera control iris size.
	open	Manually control the iris for bigger size.
	close	Manually control the iris for smaller size.

speedlink	0 ~ 4	Issue speed link command.
gaptime	0~32768	The gaptime between two consecutive ptz commands for device. (unit: ms)
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.9 Recall (capability.ptzenabled)

Note: This request requires Viewer privileges.
Method: GET

Syntax:

http://<*servername*>/cgi-bin/viewer/recall.cgi?
recall=<value>[&channel=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
recall	Text string less than 30 characters	One of the present positions to recall.
channel	<0~(n-1)>	Channel of the video source.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.10 Preset Locations (capability.ptzenabled)

Note: This request requires Operator privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/operator/preset.cgi?[channel=<value>]
[&addpos=<value>][&delpos=<value>][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
addpos	<Text string less than 30 characters>	Add one preset location to the preset list.
channel	<0~(n-1)>	Channel of the video source.
delpos	<Text string less than 30 characters>	Delete preset location from preset list.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.11 IP Filtering

Note: This request requires Administrator access privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/ipfilter.cgi?
method=<value>&[start=<ipaddress>&end=<ipaddress>][&index=<value>]
[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
method	addallow	Add allowed IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.

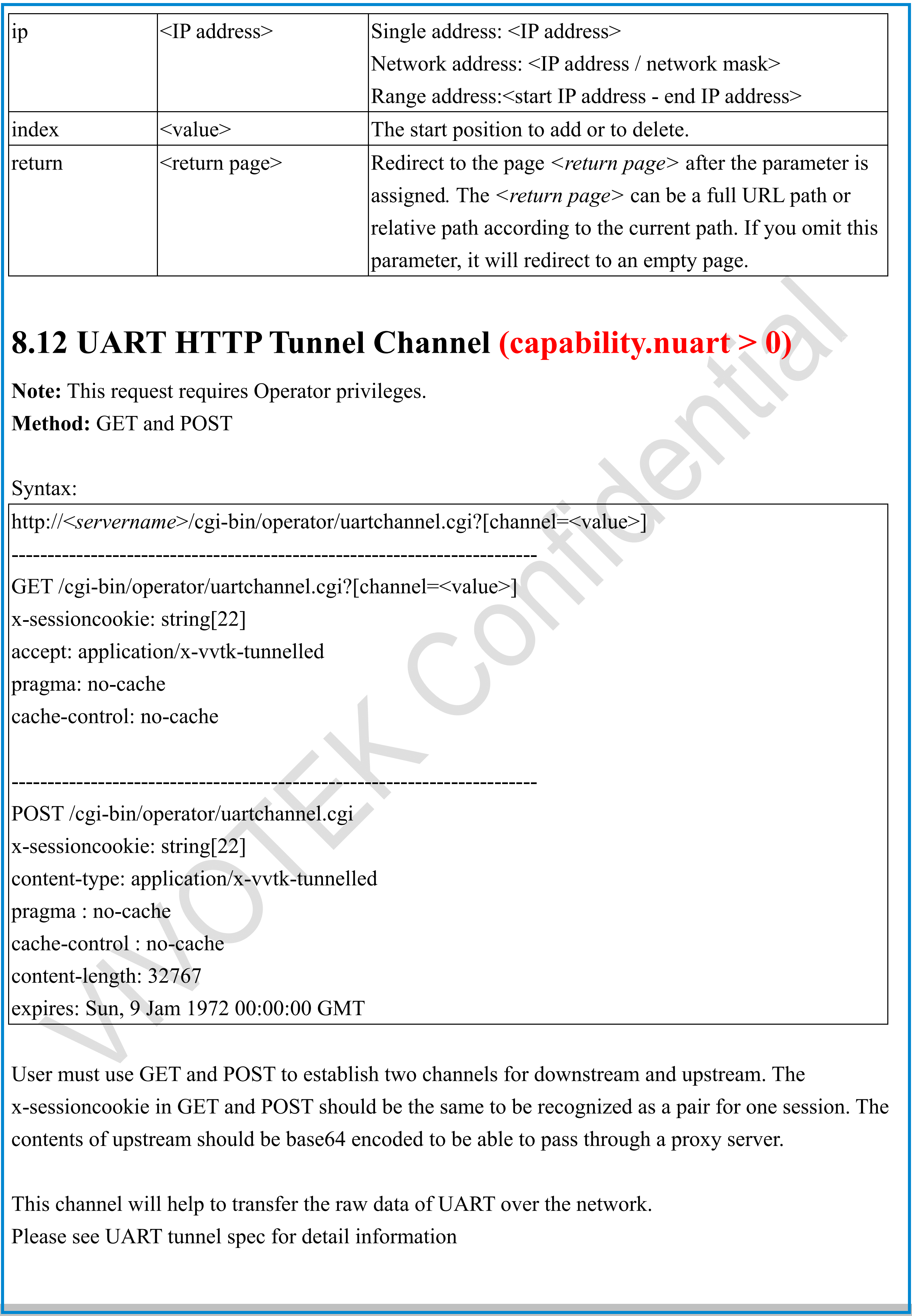
	adddeny	Add denied IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	deleteallow	Remove allowed IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
	deletedeny	Remove denied IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start	<ip address>	The starting IP address to add or to delete.
end	<ip address>	The ending IP address to add or to delete.
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.11.1 IP Filtering for ONVIF

Syntax: <product dependent>

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?type[=<value>]
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=add<v4/v6>&ip=<*ipaddress*>[&index=<value>][&return=<*return page*>]
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=del<v4/v6>&index=<value>[&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
type	NULL	Get IP filter type
	allow, deny	Set IP filter type
method	addv4	Add IPv4 address into access list.
	addv6	Add IPv6 address into access list.
	delv4	Delete IPv4 address from access list.
	delv6	Delete IPv6 address from access list.



ip	<IP address>	Single address: <IP address> Network address: <IP address / network mask> Range address:<start IP address - end IP address>
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.12 UART HTTP Tunnel Channel (capability.nuart > 0)

Note: This request requires Operator privileges.
Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/operator/uartchannel.cgi?[channel=<value>]
------------------------------------------------------------------------
GET /cgi-bin/operator/uartchannel.cgi?[channel=<value>]
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache

------------------------------------------------------------------------
POST /cgi-bin/operator/uartchannel.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
```

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through a proxy server.

This channel will help to transfer the raw data of UART over the network.
Please see UART tunnel spec for detail information

PARAMETER	VALUE	DESCRIPTION
channel	0 ~ (n-1)	The channel number of UART.

8.13 Event/Control HTTP Tunnel Channel (capability. evctrlchannel > 0)

Note: This request requires Administrator privileges.
Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/admin/ctrlevent.cgi
------------------------------------------------------------------------
GET /cgi-bin/admin/ctrlevent.cgi
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache

------------------------------------------------------------------------
POST /cgi-bin/admin/ ctrlevent.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
```

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through the proxy server.

This channel will help perform real-time event subscription and notification as well as camera control more efficiently. The event and control formats are described in another document.

See Event/control tunnel spec for detail information

8.14 Get SDP of Streams

Note: This request requires Viewer access privileges.
Method: GET/POST

Syntax:

```
http://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

“m” is the stream number.
“network_accessname_<0~(m-1)>” is the accessname for stream “1” to stream “m”. Please refer to the “subgroup of network: rtsp” for setting the accessname of SDP.
You can get the SDP by HTTP GET.
When using scalable multicast, Get SDP file which contains the multicast information via HTTP.

8.15 Open the Network Stream

Note: This request requires Viewer access privileges.

Syntax:
For HTTP push server (MJPEG):

```
http://<servername>/<network_http_s<0~m-1>_accessname>
```

For RTSP (MP4), the user needs to input the URL below into an RTSP compatible player.

```
rtsp://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

“m” is the stream number.
For details on streaming protocol, please refer to the “control signaling” and “data format” documents.

8.16 Senddata (capability.nuart > 0)

Note: This request requires Viewer privileges.
Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/senddata.cgi?
[com=<value>][&data=<value>][&flush=<value>] [&wait=<value>] [&read=<value>]
```

PARAMETER	VALUE	DESCRIPTION
com	1 ~ <max. com port number>	The target COM/RS485 port number.
data	<hex decimal data>[,<hex decimal data>]	The <hex decimal data> is a series of digits from 0 ~ 9, A ~ F. Each comma separates the commands by 200 milliseconds.
flush	yes,no	yes: Receive data buffer of the COM port will be cleared before read. no: Do not clear the receive data buffer.
wait	*1 ~ 65535*	Wait time in milliseconds before read data.
read	*1 ~ 128*	The data length in bytes to read. The read data will be in the return page.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
<hex decimal data>\r\n
```

Where hexadecimal data is digits from 0 ~ 9, A ~ F.

8.17 Virtual input (capability.nvi > 0)

Note: Change virtual input (manual trigger) status.
Method: GET

Syntax:

```
http://<servername>/cgi-bin/admin/setvi.cgi?vi0=<value>[&vi1=<value>][&vi2=<value>]
[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
vi<num>	state[(duration)nstate] Where "state" is 0, 1. “0” means inactive or normal state while “1” means active or triggered state. Where "nstate" is next state after duration.	Ex: vi0=1 Setting virtual input 0 to trigger state Ex: vi0=0(200)1 Setting virtual input 0 to normal state, waiting 200 **milliseconds**, setting it to trigger state. Note that when the virtual input is waiting for next state, it cannot accept new requests.
return	*<return page>*	Redirect to the page *<return page>* after the request is completely assigned. The *<return page>* can be a full URL path or relative path according the current path. If you omit this parameter, it will redirect to an empty page.

Return Code	Description
200	The request is successfully executed.
400	The request cannot be assigned, ex. incorrect parameters. Examples: 1. setvi.cgi?vi0=0(10000)1(15000)0(20000)1 No multiple duration. 2. setvi.cgi?vi3=0 VI index is out of range. 3. setvi.cgi?vi=1 No VI index is specified.

503	The resource is unavailable, ex. Virtual input is waiting for next state. Examples: 1. setvi.cgi?vi0=0(15000)1 2. setvi.cgi?vi0=1 Request 2 will not be accepted during the execution time(15 seconds).

8.18 Open Timeshift Stream (capability.timeshift > 0, timeshift_enable=1, timeshift_c<n>_s<m>_allow=1)

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

```
http://<servername>/<network_http_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&refti
me=<value>&forcechk&minsft=<value>]
```

For RTSP (MP4 and H264), the user needs to input the URL below into an RTSP compatible player.

```
rtsp://<servername>/<network_rtsp_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&refti
me=<value>&forcechk&minsft=<value>]
```

"n" is the channel index.

"m" is the timeshift stream index.

For details on timeshift stream, please refer to the "TimeshiftCaching" documents.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
maxsft	<positive integer>	0	Request cached stream at most how many seconds ago.
tsmode	normal, adaptive	normal	Streaming mode: normal => Full FPS all the time. adaptive => Default send only I-frame for MP4 and H.264, and send 1 FPS for MJPEG. If DI , VI or motion window are triggered, the streaming is changed to send full FPS for 10 seconds. (*Note: this parameter also works on non-timeshift streams.)
reftime	mm:ss	The time camera receives the	Reference time for maxsft and minsft. (This provides more precise time control to eliminate the inaccuracy due to network latency.)

		request.	Ex: Request the streaming from 12:20 rtsp://10.0.0.1/live.sdp?maxsft=10&reftime=12:30
forcechk	N/A	N/A	Check if the requested stream enables timeshift, feature and if minsft is achievable. If false, return “415 Unsupported Media Type”.
minsft	<positive integer>	0	How many seconds of cached stream client can accept at least. (Used by forcechk)

Return Code	Description
400 Bad Request	Request is rejected because some parameter values are illegal.
415 Unsupported Media Type	Returned, if forcechk appears, when minsft is not achievable or the timeshift feature of the target stream is not enabled.

<End of document>

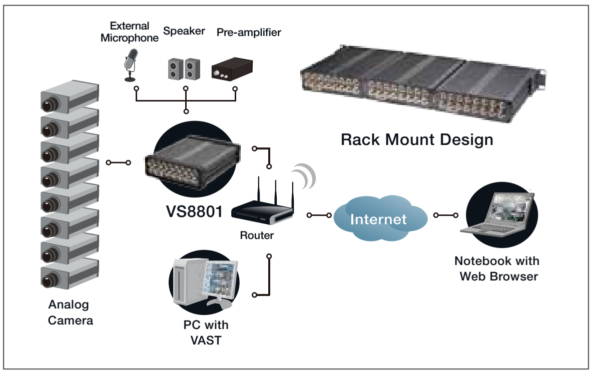
Technical Specifications

Specifications

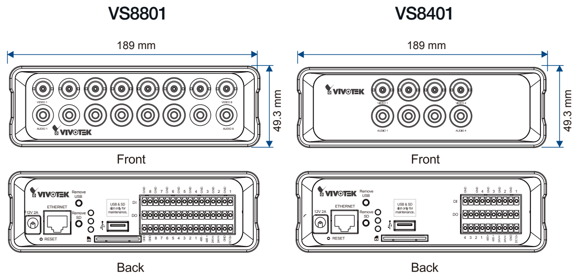
Ver. 1.0

System	· CPU: Mozart 380 SoC · Flash: 32MB · RAM: 512MB · Embedded OS: Linux 2.6
Camera Control	· PTZ camera control through RS-485 · Supported devices and protocols: DynaDome/ SmartDome Pelco D LiLin Pelco P Samsung scc643 and customized types · Supports CGI command serial driver
Video	· Compression: H.264/MJPEG/MPEG-4 · Streaming: Single Stream (VS8801) or Dual Streams (VS8401) H.264 streaming over UDP, TCP, HTTP or HTTPS MPEG-4 streaming over UDP, TCP, HTTP or HTTPS H.264/MPEG-4 multicast streaming MJPEG streaming over HTTP or HTTPS · Supports activity adaptive streaming for dynamic frame rate control · Supports 3GPP mobile surveillance · Frame rates: H.264: Up tp 180 fps at D1 MJPEG: Up to 240 fps at D1 MPEG-4: Up to 80 fps at D1 · Interface: BNC connector for video output
Image Settings	· Adjustable image size, quality and bit rate · Time stamp and text caption overlay · Flip & mirror · Configurable brightness, contrast, saturation, sharpness · Supports privacy masks
Audio	· Compression: G.711 audio encoding, bit rate: 64 kbps, µ -Law, or A-Law mode selectable · Interface: Audio input, up to 1Vrms, 3.5 mm Phone Jack Audio output, Terminal block x 8 · Supports two-way audio (Per channel) · Supports audio mute
Networking	· 10/100/1000 Mbps Gigabit Ethernet, RJ-45 · Onvif support · Protocols: IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP and 802.1X
Alarm and Event Management	· Triple-window video motion detection · Tamper detection · Four D/I and four D/O for external sensor and alarm (VS8401) · Eight D/I and eight D/O for external sensor and alarm (VS8801) · Event notification using HTTP, SMTP or FTP · Local recording of MP4 file
Security	· Multi-level user access with password protection · IP address filtering · HTTPS encrypted data transmission · 802.1X port-based authentication for network protection
Users	· Live viewing for up to 10 clients
Weight	· Net: 837 g (VS8801)
Dimension	· 189 mm (L) x 153 mm (W) x 49.3 mm (H)
LED Indicator	· System power and status indicator · System activity and network link indicator
Power	· Power input: 12V DC/24V AC · Power consumption: Max. 24 W
Approvals	· CE, LVD, FCC, VCCI, C-Tick
Operating Environments	· Temperature: -10° C ~ 50 ° C · Humidity: 20 ~ 80% RH
Viewing System Requirements	· OS: Microsoft Windows 2000/XP/Vista/Win7 · Browser: Internet Explorer 6 or above · Cell phone: 3GPP player · Real Player: 10.5 or above · Quick Time: 6.5 or above
Installation, Management, and Maintenance	· Installation Wizard 2 · 32-CH ST7501 recording software · Supports firmware upgrade
Interface	· RS-485: Half Duplex
Applications	· SDK available for application development and system integration
Warranty	· 24 months

System Overview



External View



The USB socket and SD card slot are only for maintenance.

Distributed by:

VIVOTEK
www.vivotek.com

VIVOTEK INC.
6F, No.192, Lien-Cheng Rd., Chung-Ho, New Taipei City, 235, Taiwan, R.O.C.
| **T:** +886-2-82455282 | **F:** +886-2-82455532 | **E:** sales@vivotek.com

VIVOTEK USA, INC.
470 Lakeside Drive Suite C, Sunnyvale, CA 94085 USA
| **T:** 408-773-8686 | **F:** 408-773-8298 | **E:** salesusa@vivotek.com

Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT WITH REGARD TO PC SOFTWARE, OF WHICH YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

■ This device may not cause harmful interference, and

■ This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

CE Mark Warning CE

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Warning

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあいます。この場合には使用者が適切な対策を講ずるよう要求されることたがあります。

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.