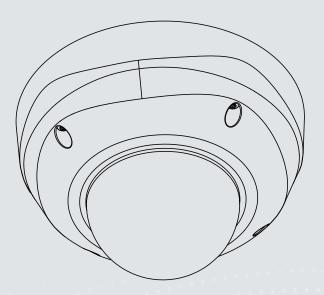


# FD8372 Fixed Dome Network Camera USEr's Vanual

5MP • Full HD • Smart Focus System



## Table of Contents

Overview	4
Revision History	4
Read Before Use	5
Package Contents	5
Symbols and Statements in this Document	5
Physical Description	6
Installation	9
Network Deployment	15
Software Installation	18
Ready to Use	19
Completion	20
Accessing the Network Camera	21
Using Web Browsers	
Using RTSP Players	24
Using 3GPP-compatible Mobile Devices	25
Using VIVOTEK Recording Software	26
Main Page	27
Client Settings	32
Configuration	34
System > General settings	35
System > Homepage layout	37
System > Logs	40
System > Parameters	41
System > Maintenance	
Media > Image	46
Media > Video	55
Media > Video	57
Media > Audio	
Network > General settings	
Network > Streaming protocols	
Network > SNMP (Simple Network Management Protocol)	
Security > User Account	
Security > HTTPS (Hypertext Transfer Protocol over SSL)	
Security > Access List	
PTZ > PTZ settings	
Event > Event settings	
Applications > Motion detection	
Applications > DI and DO	
Applications > Tampering detection	
Recording > Recording settings	
Local storage > SD card management	
Local storage > Content management	
Appendix URL Commands for the Network Camera	
ONE COMMINANCE IN THE INSTRUCTION CAMERIA	141

Technical Specifications	198
Technology License Notice	
Electromagnetic Compatibility (EMC)	200

## **Overview**

VIVOTEK's FD8372 network camera features an HD WDR CMOS sensor to cope with challenging lighting conditions. The WDR feature allows the camera to capture both the dark and bright parts of an image and combines the differences to generate a highly realistic image representative of the original scene, enabling it to provide video quality close to the capabilities of the human eye. This function enables the FD8372 to be widely applicable in high contrast environments such as lobby entrances, parking lots, ATMs, loading areas, and much more. The P-iris lens controls the iris with extreme precision; with its built-in stepper motor, it maintains the iris opening at an optimal level at all times, resulting in superior image clarity and depth of field as well as image quality.

Incorporating an IR-cut filter that can be removed automatically at night and built-in IR illuminators with coverage of up to 20 meters, the FD8372 is an outstanding 24-hour surveillance solution. The vandal-proof and the IP66-rated housing of the FD8372 enables users to easily build a cost-effective IP surveillance system without additional accessories. Its metal vandal-proof housing effectively provides robust protection from vandalism. Meanwhile, the IP66 integrated housing shields the camera from dust and water, allowing it to be applied in the harsh weather conditions of outdoor environments.

## **Revision History**

■ Rev. 1.0: Initial release

#### Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera 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 Network Camera 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 Network Camera 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 Network Camera and ensure proper operations. For creative and professional developers, the URL Commands of the Network Camera section serves as a helpful reference to customizing existing homepages or integrating with the current web server.

## **Package Contents**

- FD8372
- Mounting Plate
- Alignment sticker/Ceiling Hole Template Sticker
- L-type Hex key wrench / Moisture absorber / Screws / Hex Nut / Double-side tape / AV cable
- Software CD
- Warranty Card
- Quick Installation Guide
- Waterproof Connector & bushing

## **Symbols and Statements in this Document**



**INFORMATION:** provides important messages or advices that might help prevent inconvenient or problem situations.



**NOTE**: Notices provide guidance or advices that are related to the functional integrity of the machine.



**Tips**: Tips are useful information that helps enhance or facilitae an installation, function, or process.



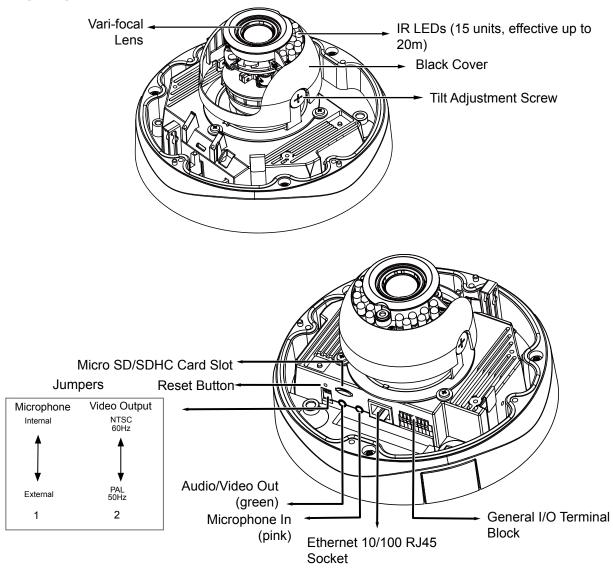
**WARNING!** or **IMPORTANT!**: These statements indicate situations that can be dangerous or hazardous to the machine or you.



**Electrical Hazard**: This statement appears when high voltage electrical hazards might occur to an operator.

## **Physical Description**

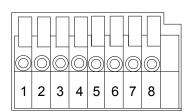
#### **Inner View**



#### **General I/O Terminal Block**

This Network Camera provides a general I/O terminal block which is used to connect external input / output devices. The pin definitions are described below. The 24V AC can be used as an alternate power source.

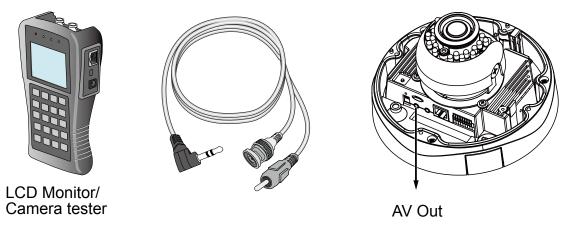
1	DO+ (12V)
2	DO-
3	DI1+
4	DI2+
5	DI3+
6	DI-
7	AC24V_1
8	AC24V 2





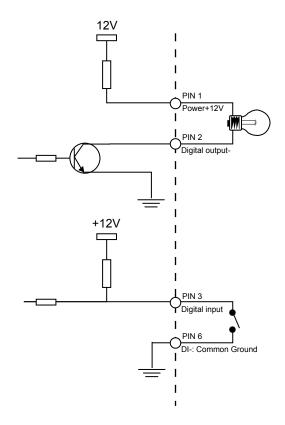
#### NOTE:

- 1. There is no internal microphone. Connect an external microphone if you need audio inputs.
- 2. Use the included AV cable to connect to a camera tester or LCD monitor to begin initial setup.



## **DI/DO Diagram**

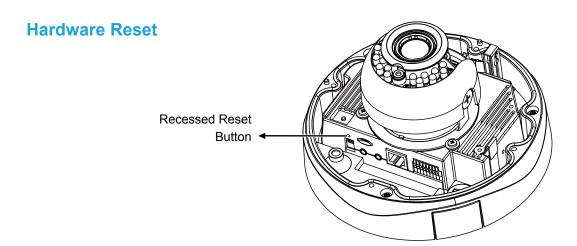
Please refer to the following illustration for the connection method.





#### NOTE:

The maximum output load from pins #1 & 2 is 50mA.



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

<u>Reset</u>: Press and release the recessed reset button with a straightened paper clip. Wait for the Network Camera to reboot.

<u>Restore</u>: Press and hold the recessed reset button until the status LED rapidly blinks. Note that all settings will be restored to factory default. Upon successful restore, the status LED will blink green and red during normal operation.

## **Micro SD/SDHC Card Capacity**

This network camera is compliant with **Micro SD/SDHC 16GB / 8GB** and other preceding standard SD cards.

#### Installation

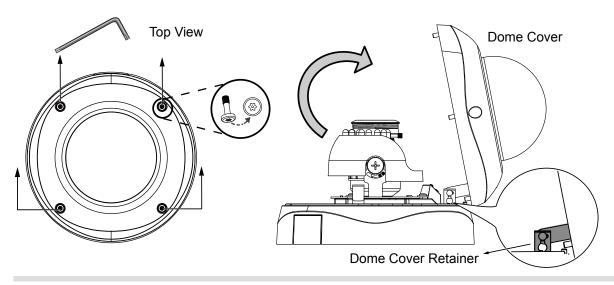
#### **Removing Dome Cover**

First, use the included T20 hex key wrench to loose the four screws and detach the dome cover from the camera base. Follow the steps below to install the camera either to a ceiling or a wall.



#### **IMPORTANT:**

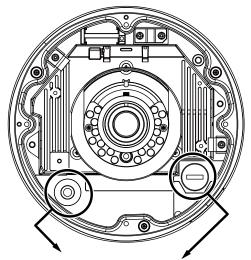
The dome cover should be removed first because if it should fall during the installation process, physical injury could occur to your co-workers.



#### **Cabling Assembly**

Connect power lines and if you have external devices such as sensors and alarms, make the connection from the general I/O terminal block.

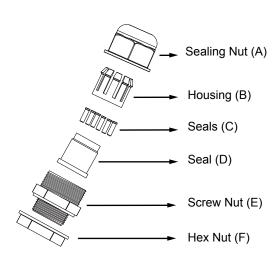
Top View



For Ethernet Cable For Power & IO Cables

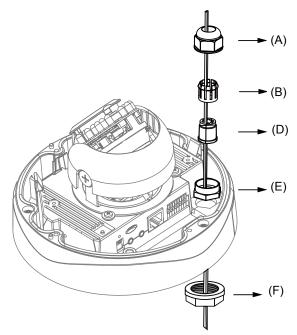
Power and IO cables pass through a waterproof connector. The Ethernet cable should be routed through a rubber seal plug. All cables are user-supplied.

### **Waterproof Connector**



#### Assembling Steps

- Disassemble the components of the waterproof connector into parts (A) ~ (F) as shown above.
- 2. Place the screw nut (E) on the Power and GPIO opening.
- 3. Feed the power cables through the waterproof connector (F --> E --> D --> B --> A) as the illustration shows. Then connect the power cables to the power source. Note: There are 8 holes on the seal (D), and the widest holes with a crack on the side are specific for power cables.
- 4. If you have external devices such as sensors and alarms, feed the cables through the waterproof connector (F --> E --> D --> B --> A) as previously described.



Refer to the pin definition to connect them to the general I/O terminal block. Note: The recommended cable gauge is  $2.0 \sim 2.8 \text{ mm}$ .

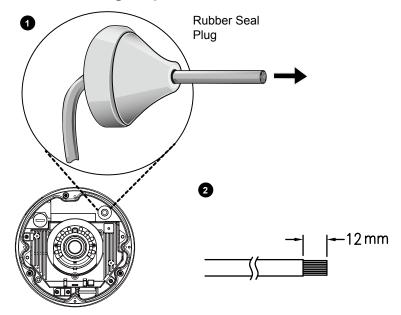
- 5. Push the seal (D) into the housing (B).
- 6. Insert the seals (C) into unused holes on the seal (D) to avoid moisture.
- 7. Secure the sealing nut (A) tightly and hex nut (F) from the bottom of the camera.

#### **Connecting RJ45 Ethernet Cable**

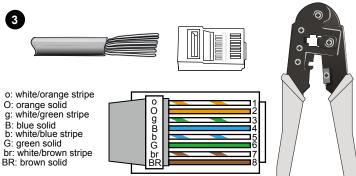
RJ45 Cable Dimension (unit: mm)

Recommended cable gauge: 24AWG (0.51 mm)

#### Assembling Steps

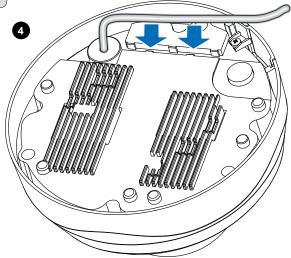


- 1. Drill a hole on the rubber seal plug and insert an Ethernet cable through the opening.
- 2. Strip part of the sheath from the Ethernet cable.



3. You will need an RJ45 crimping tool to attach the Ethernet wires to a connector. When done, connect the cable to the camera's Ethernet RJ45 socket.

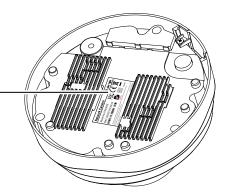
4. Press the Ethernet cable into the routing path at the bottom of the camera so that the cable will not get in the way when the metal mounting plate is attached.





## \ IMPORTANT:

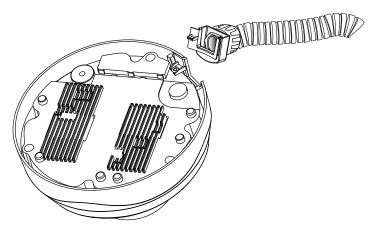
Record the MAC address under the camera base before installing the camera.





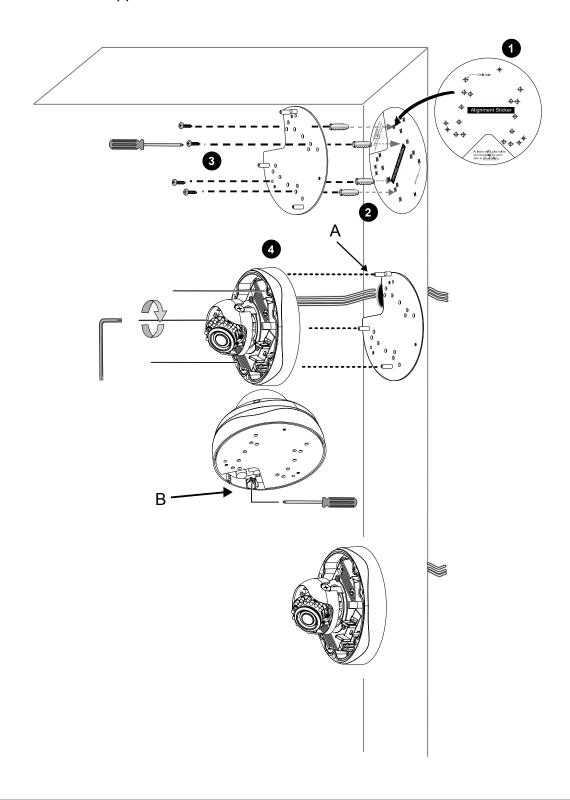
## \_\_\_\_Tips:

Replace the side opening cover with the included side outlet bushing if you want to route cables from the side of camera. The 1/2" protection conduits and tubing, if applied, are separately purchased.



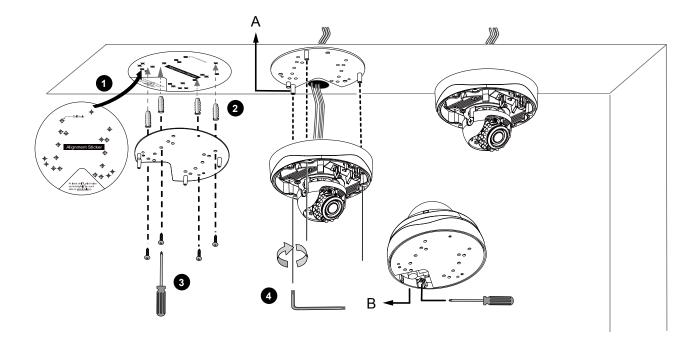
#### Wall mount

- 1. Attach the supplied alignment sticker to the wall.
- 2. Using the circle marks on the sticker, drill at least 2 pilot holes symmetrically on each side into the wall. Then hammer the four supplied plastic anchors into the holes.
- 3. Through three or four holes on the mounting plate, insert the supplied screws into the corresponding holes and secure the mounting plate with a screwdriver.
- 4. Feed the cables through the triangular cutout A or side opening B. If you want to use hole B, remove the side cover using a screwdriver. Secure the camera base to the mounting plate with three supplied screws.



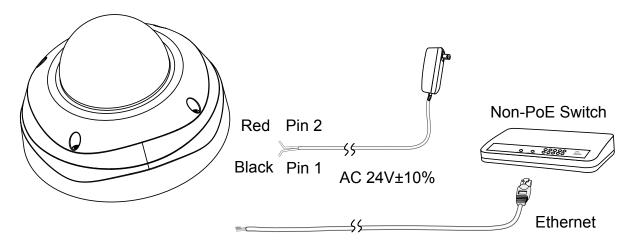
#### **Ceiling mount**

- 1. Attach the supplied alignment sticker to the ceiling.
- 2. Using the circle marks on the sticker, drill at least 2 pilot holes symmetrically on each side into the ceiling. Then hammer the four supplied plastic anchors into the holes.
- 3. Through three or four holes on the mounting plate, insert the supplied screws into the corresponding holes and secure the mounting plate with a screwdriver.
- 4. Feed the cables through the triangular cutout A or side opening B. If you want to use hole B, remove the side cover using a screwdriver. Secure the camera base to the mounting plate with three supplied screws.



## **Network Deployment**

#### **General Connection (without PoE)**

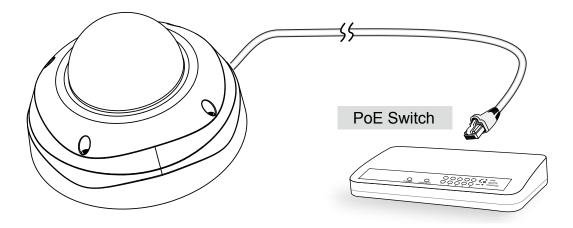


- 1. Connect RJ45 Ethernet cable to a switch.
- Connect the AC cables from the terminal block as an alternate power source. The IO cables are user-supplied.

#### Power over Ethernet (PoE)

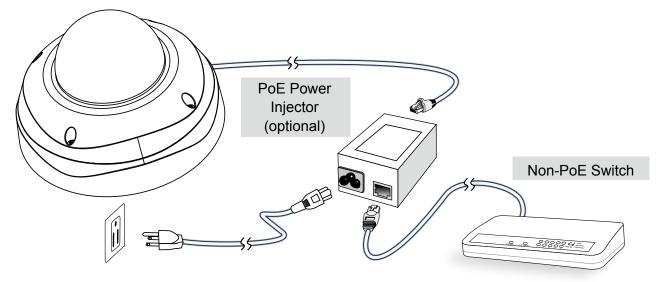
## When using a PoE-enabled switch

The Network Camera is PoE-compliant, allowing transmission of power and data via a single Ethernet cable. Follow the below illustration to connect the Network Camera to a PoE-enabled switch via Ethernet cable.



## When using a non-PoE switch

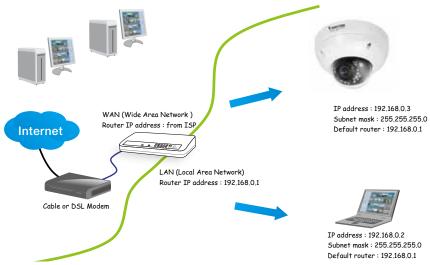
Use a PoE power injector (optional) to connect between the Network Camera and a non-PoE switch.



#### Internet connection via a router

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

 Connect your Network Camera behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 18 for details.



- 2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.
  - HTTP port: default is 80RTSP port: default is 554
  - RTP port for audio: default is 5558
    RTCP port for audio: default is 5559
    RTP port for video: default is 5556
    RTCP port for video: default is 5557

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 Network Camera from the Internet. Please refer to Network Type on page 63 for details.

#### Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN setting on page 62 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 63 for details.

#### Software Installation

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

- 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

- 3. The program will search for all VIVOTEK network devices on the same LAN.
- 4. After a brief search, the installer window will prompt. Click on the MAC and model name that matches the one printed on the product label. You can then double-click on the address to open a management session with the Network Camera.





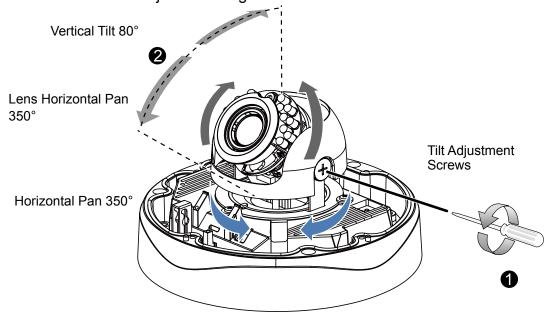
## Ready to Use

- 1. A browser session with the Network Camera 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.



#### To adjust the viewing angle -- 3-axis mechanism design

- 1. Loosen the tilt adjustment screws and then turn the lens module up or down, or swing left or right. Upon completion, tighten the screw.
- 2. Turn the lens to adjust the image orientation.



#### To adjust the zoom factor and focus range

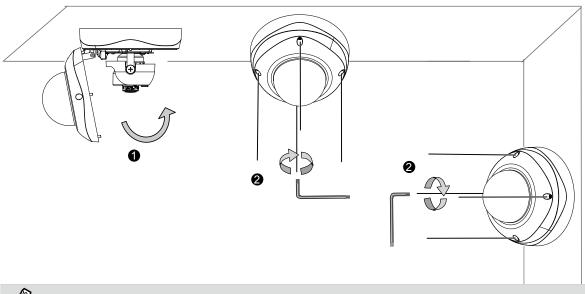


- The camera comes with a motorized varifocal lens module. With a web console, you can enter the Configuration > Media > Image > Focus page to tune the image zoom and focus.
- 2. On this page, you can pull the **Zoom** and **Focus** pointers, set up a **Focus window**, and use the **Perform auto focus** button to automatically obtain an optimal focus result. You may also manually fine-tune zoom and focus using the various functional buttons.

Please refer to page 52, Media > Image > Focus for more information.

## Completion

- 1. Attach the dome cover to the camera by combining it to the retainer and aligning with the mounting holes.
- 2. Secure the four dome screws with the supplied hex key wrench. Make sure all parts of the camera are securely installed.



NOTE:

You will find a moisture absorber bag attached to the dome cover. Replace the moisture absorber included in the camera with the one shipped within the accessory bag.

# **Accessing the Network Camera**

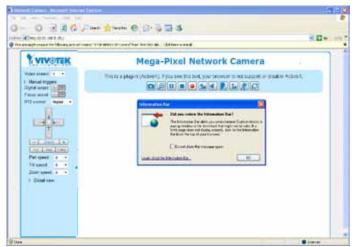
This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

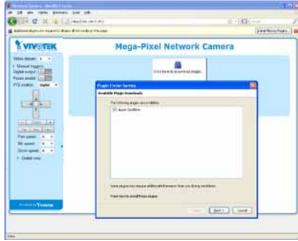
## **Using Web Browsers**

Use Installation Wizard 2 (IW2) to access the Network Cameras on LAN.

If your network environment is not a LAN, follow these steps to access the Network Camera:

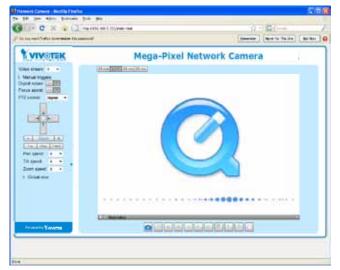
- 1. Launch your web browser (e.g., Microsoft® Internet Explorer or Mozilla Firefox).
- 2. Enter the IP address of the Network Camera in the address field. Press Enter.
- 3. The live video will be displayed in your web browser.
- 4. If it is the first time installing the VIVOTEK network camera, an information bar will prompt as shown below. Follow the instructions to install the required plug-in on your computer.





#### NOTE:

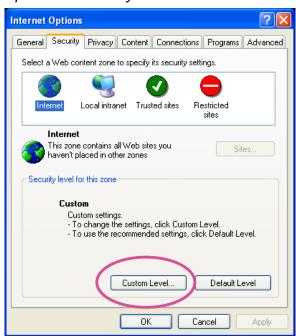
► For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video. If you don't have Quick Time on your computer, please download it first, then launch the web browser.



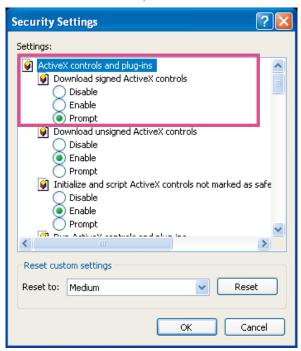


- ▶ By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera.

  For more information about how to enable password protection, please refer to Security on page 80.
- ► If you see a dialog box indicating that your security settings prohibit running ActiveX<sup>®</sup> Controls, please enable the ActiveX<sup>®</sup> Controls for your browser.
- 1. Choose Tools > Internet Options > Security > Custom Level.



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



3. Refresh your web browser, then install the ActiveX<sup>®</sup> control. Follow the instructions to complete installation.



## **IMPORTANT!**

- Currently the Network Camera utilizes 32-bit ActiveX plugin. You CAN NOT open a management/view session with the camera using a 64-bit IE browser.
- If you encounter this problem, try execute the lexplore.exe program from C:\ Windows\SysWOW64. A 32-bit version of IE browser will be installed.
- On Windows 7, the 32-bit explorer browser can be accessed from here:
   C:\Program Files (x86)\Internet Explorer\iexplore.exe

## **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** 

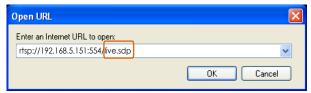


Real Player

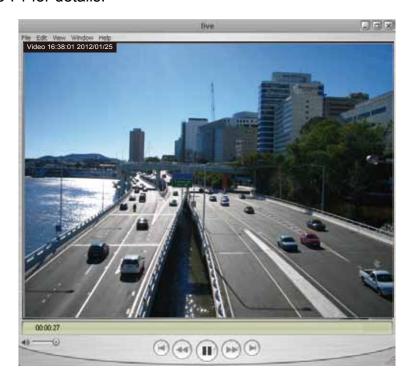
- 1. Launch the RTSP player.
- 2. Choose File > Open URL. A URL dialog box will pop up.
- 3. The address format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>

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 71.

For example:



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 71 for details.



## **Using 3GPP-compatible Mobile Devices**

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 15.

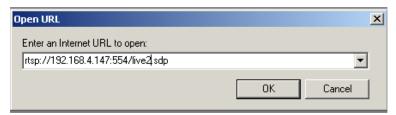
To utilize this feature, please check the following settings on your Network Camera:

- 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 71.
- 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. For more information, please refer to Stream settings on page 56.

Video Mode	MPEG-4
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (GSM-AMR)	12.2kbps

- 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 71.
- 4. Launch the player on the 3GPP-compatible mobile devices (e.g., 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 # with small frame size and frame rate>. For example:



You can configure Stream #2 into the suggested stream settings as listed above for live viewing on a mobile device.

## **Using VIVOTEK Recording Software**

The product software CD also contains an ST7501 recording software, allowing simultaneous monitoring and video recording for multiple Network Cameras. Please install the recording software; then launch the program to add the Network Camera 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.



#### **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 on page 35.

#### **Camera Control Area**

<u>Video Stream</u>: This Network Camera supports multiple streams (stream  $1 \sim 4$ ) simultaneously. You can select either one for live viewing. For more information about multiple streams, please refer to page 56 for detailed information.

<u>Manual Trigger</u>: Click to enable/disable an event trigger manually. Please configure an event setting on Application page before enable this function. A total of 3 event settings can be configured. For more information about event setting, please refer to page 94. If you want to hide this item on the homepage, please go to **Configuration> System > Homepage Layout > General settings > Customized button** to deselect "show manual trigger button".

<u>Digital Output</u>: Click to turn the digital output device on or off.

#### **Configuration Area**

<u>Client Settings</u>: Click this button to access the client setting page. For more information, please refer to Client Settings on page 32.

<u>Configuration</u>: Click this button to access the configuration page of the Network Camera. It is suggested that a password be applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 34.

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. Please note that you can also change a language on the Configuration page; please refer to page 34.

#### **Hide Button**

You can click the hide button to hide the control panel or display the control panel.

#### **Resize Buttons**



Click the Auto button, the video cell will resize automatically to fit the monitor.

Click 100% is to display the original homepage size.

Click 50% is to resize the homepage to 50% of its original size.

Click 25% is to resize the homepage to 25% of its original size.

#### **Live Video Window**

■ The following window is displayed when the video mode is set to H.264 / MPEG-4:



<u>Video Title</u>: The video title can be configured. For more information, please refer to Video Settings on page 46.

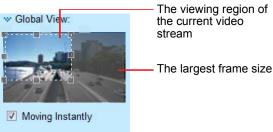
<u>H.264 / MPEG-4 Protocol and Media Options</u>: The transmission protocol and media options for H.264 / MPEG-4 video streaming. For further configuration, please refer to Client Settings on page 32.

<u>Time</u>: Display the current time. For further configuration, please refer to Media > Image > Genral settings on page 46.

<u>Title and Time</u>: The video title and time can be stamped on the streaming video. For further configuration, please refer to Media > Image > General settings on page 48.

<u>PTZ Panel</u>: This Network Camera supports "digital" (e-PTZ) pan/tilt/zoom control, which allows roaming a smaller view frame within a large view frame. Please refer to PTZ settiings on page 91 for detailed information.

<u>Global View</u>: Click on this item to display the Global View window. The Global View window contains a full view image (the largest frame size of the captured video) and a floating frame (the viewing region of the current video stream). The floating frame allows users to control the e-PTZ function (Electronic Pan/Tilt/Zoom). For more information about e-PTZ operation, please refer to E-PTZ Operation on page 91. For more information about how to set up the viewing region of the current video stream, please refer to page 91.





#### NOTE:

- 1. For a megapixel camera, it is recommended to use monitors of the 24" size or larger, and are capable of 1600x1200 or better resolutions.
- The video input is "muted" by default. To receive audio into from external microphone, you need to enable the audio input from Media > Audio. Refer to page 61 for more information.

<u>Video and Audio Control Buttons</u>: Depending on the Network Camera model and Network Camera 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.

<u>Digital Zoom</u>: 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.



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 33 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 Network Camera. Audio will project from the external speaker connected to the Network Camera. Click this button again to end talking transmission.

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.

■ The following window is displayed when the video mode is set to MJPEG:



<u>Video Title</u>: The video title can be configured. For more information, please refer to Media > Image on page 48.

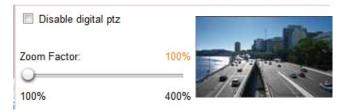
<u>Time</u>: Display the current time. For more information, please refer to Media > Image on page 48.

<u>Title and Time</u>: Video title and time can be stamped on the streaming video. For more information, please refer to Media > Image on page 48.

<u>Video and Audio Control Buttons</u>: Depending on the Network Camera model and Network Camera 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.

<u>Digital Zoom</u>: 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.



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 33 for details.

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

# **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
O Video Only
O 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	
O UDP Unicast	
O UDP Multicast	
▼TCP	
○HTTP	

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

<u>UDP unicast</u>: 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 Network Camera allows up to ten simultaneous accesses.

<u>UDP multicast</u>: 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 Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 71.

<u>TCP</u>: 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.

<u>HTTP</u>: 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**



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.

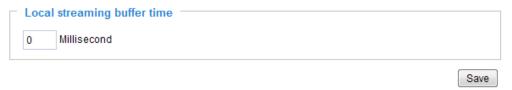
<u>Folder</u>: Specify a storage destination for the recorded video files. The location can be changed.

<u>File name prefix</u>: Enter the text that will be appended to the front of the video file name. A specified folder will be automatically created on your local hard disk.

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.



#### **Local Streaming Buffer Time**



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 for 3 seconds.

## **Configuration**

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

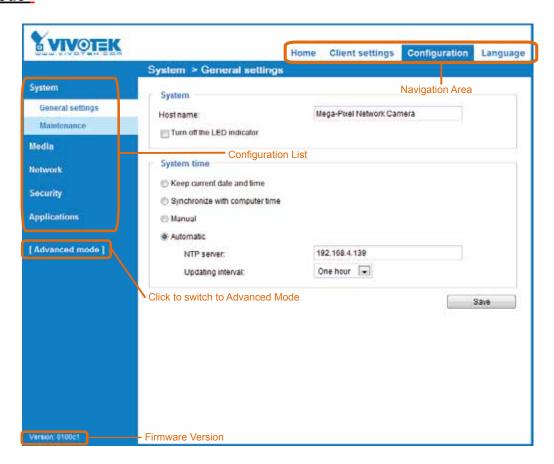
VIVOTEK offers an easy-to-use user interface that helps you set up your network camera with minimal effort. To simplify the setting procedure, two types of user interfaces are available: Advanced Mode for professional users and Basic Mode for entry-level users. Some advanced functions (PTZ/ Event/ Recording/ Local storage) 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.

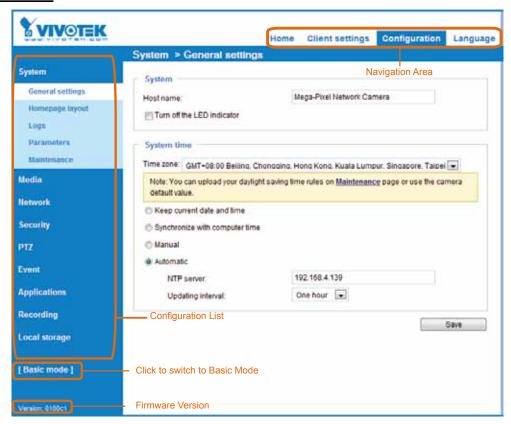
In order to simplify the user interface, the detailed information will be hidden unless you click on the function item. When you click on the first sub-item, the detailed information for the first sub-item will be displayed; when you click on the second sub-item, the detailed information for the second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



#### **Advanced Mode**



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] on the bottom of the configuration list to quickly switch over.

Navigation Area provides an instant switch among **Home** page (the monitoring page for live viewing), **Client settings**, **Configuration** page, and multi-language selection.

## System > General settings

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

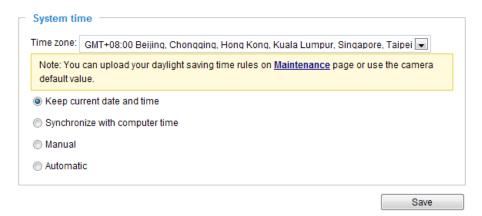
#### **System**



<u>Host name</u>: Enter a desired name for the Network Camera. The text will be displayed at the top of the main page, and also on the view cell of ST7501 and VAST management software.

<u>Turn off the LED indicators</u>: If you do not want others to notice the network camera is in operation, you can select this option to turn off the LED indicators.

#### **System time**



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

<u>Synchronize with computer time</u>: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

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

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

<u>NTP server</u>: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time servers.

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

<u>Time zone</u> Advanced Mode: Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules, please refer to **System > Maintenance > Import/ Export files** on page 43 for details.

# System > Homepage layout Advanced Mode

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

# **General settings**

This column shows the settings of your hompage layout. You can manually select the background and font colors in Theme Options (the second tab 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: If you check this item, it will be removed from the homepage.

### Logo graph

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



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.

Show manual trigger button

- 4. Enter a website link if necessary.
- 5. Click **Save** to enable the settings.

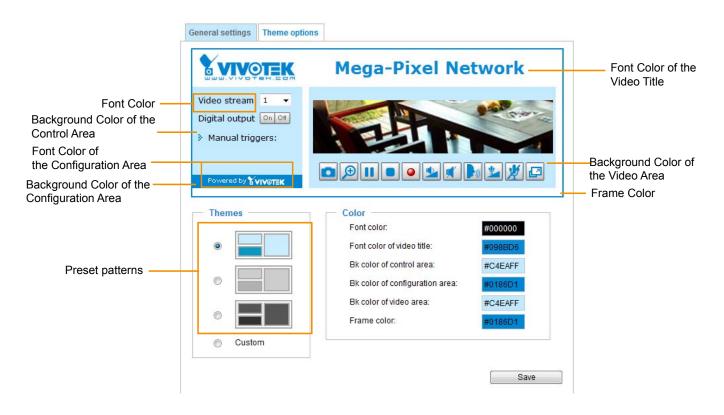
### Customized button

If you want to hide manual trigger buttons on the homepage, please uncheck this item. This item is checked by default.

— Customized button

## **Theme Options**

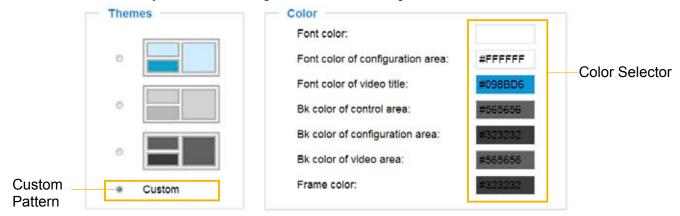
Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the settings.



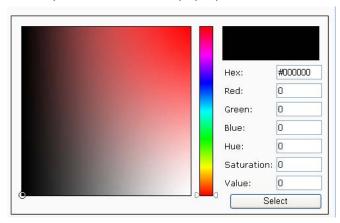


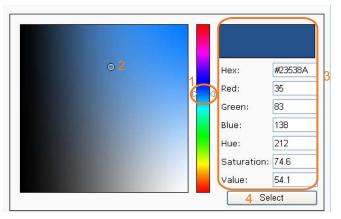


- Follow the steps below to set up the customed homepage:
- 1. Click **Custom** on the left column.
- 2. Click the field where you want to change the color on the right column.



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





- 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.

# System > Logs Advanced Mode

This section explains how to configure the Network Camera to send the system log to a remote server as backup.

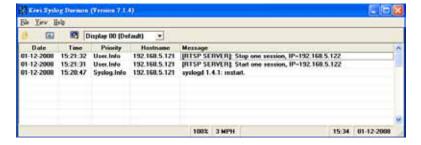
# Log server settings



Follow the steps below to set up the remote log:

- 1. Select Enable remote log.
- 2. 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, click **Save** to enable the setting.

You can configure the Network Camera 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 Network Camera. An example is Kiwi Syslog Daemon. Visit <a href="http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/">http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/</a>.



# System log



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

# **Access log**

```
Jan 5 11:36:28 [RTSP SERVER]: Start one session, IP=172.16.2.52

Jan 5 11:49:15 [RTSP SERVER]: Start one session, IP=192.168.4.105

Jan 5 13:11:20 [RTSP SERVER]: Start one session, IP=192.168.4.105
```

Access log displays the access time and IP address of all viewers (including operators and administrators) in a chronological order. The access log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain limit.

# System > Parameters Advanced Mode

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

```
Parameters
 system hostname='Mega-Pixel Network Camera'
                                                                   (E)
 system ledoff='0'
 system lowlight='1'
 system_date='2012/04/03'
system_time='17:40:54'
 system datetime=''
 system ntp='192.168.4.139'
 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,-200,-201,-1
 system updateinterval='3600'
 system info modelname='FD8372'
 system_info_extendedmodelname='FD8372'
 system info serialnumber='0002D117DED0'
 system info firmwareversion='FD8372-VVTK-0100c1'
 system info language count='9'
 system info language i0='English'
 system_info_language_i1='Deutsch'
 system_info_language_i2='Español'
 system info language i3='Français'
 system info language i4='Italiano'
 system_info_language i5='日本語'
 system info language i6='Português'
 system_info_language_i7='简体中文'
 system_info_language_i8='繁體中文'
```

# System > Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.

# **General settings > Upgrade firmware**

Upgrade firmware		
Select firmware file:	Browse	Upgrade

This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.

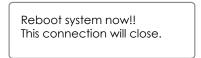
Note: Do not power off the Network Camera during the upgrade!

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 Network Camera 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, reaccess the Network Camera.

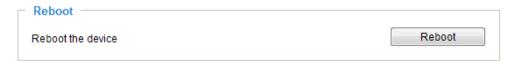
The following message is displayed when the upgrade has succeeded.



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

# **General settings > Reboot**



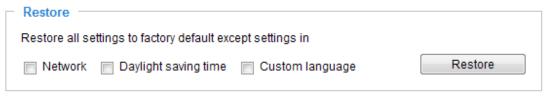
This feature allows you to reboot the Network Camera, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will be displayed during the reboot process.

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 Network Camera in the address field to resume the connection.

# **General settings > Restore**



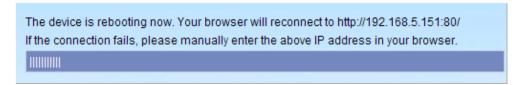
This feature allows you to restore the Network Camera to factory default settings.

<u>Network</u>: Select this option to retain the Network Type settings (please refer to Network Type on page 63).

<u>Daylight Saving Time</u>: Select this option to retain the Daylight Saving Time settings (please refer to Import/Export files below on this page).

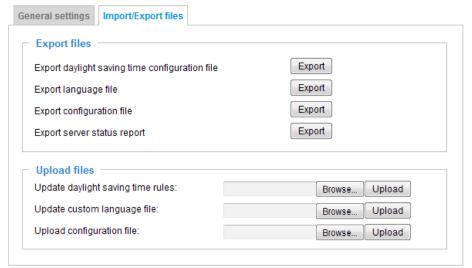
<u>Custom Language</u>: Select this option to retain the Custom Language settings.

If none of the options is selected, all settings will be restored to factory default. The following message is displayed during the restoring process.



# Import/Export files Advanced Mode

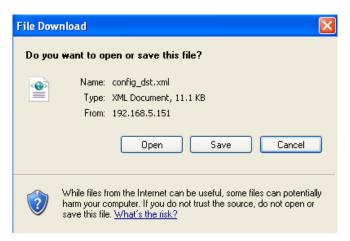
This feature allows you to Export / Update daylight saving time rules, custom language file, configuration file, and server status report.



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

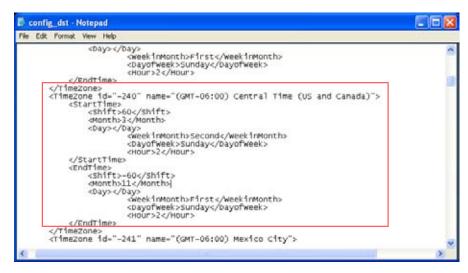
Follow the steps below to export:

- 1. In the Export files column, click **Export** to export the daylight saving time configuration file from the Network Camera.
- 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.



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.



<u>Update daylight saving time rules</u>: Click **Browse...** and specify the XML file to update.

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

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



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.

Update custom language file: Click Browse... and specify your own custom language file to upload.

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

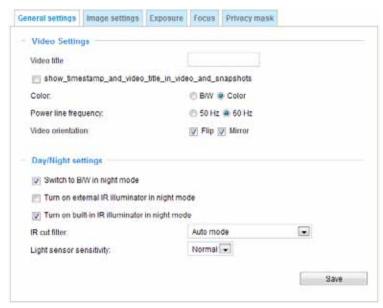
<u>Update configuration file</u>: Click **Browse...** to update a configuration file. Please note that the model and firmware version of the device should be the same as the configuration file. If you have set up a fixed IP or other special settings for your device, it is not suggested to update a configuration file.

<u>Export server staus report</u>: Click to export the current server status report, such as time, logs, parameters, process status, memory status, file system status, network status, kernel message ... and so on.

# Media > Image Advanced Mode

This section explains how to configure the image settings of the Network Camera. It is composed of the following four columns: General settings, Picture settings, Exposure, and Privacy mask.

# **General settings**



### Video title

<u>Show timestamp and video title in video and snapshots</u>: Enter a name that will be displayed on the title bar of the live video as the picture shown below.



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

<u>Power line frequency</u>: Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

<u>Video orientation</u>: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (e.g., on the ceiling) to correct the image orientation. Please note that if you have preset locations, those locations will be cleared after flip/mirror setting.

### **Day/Night Settings**

### Switch to B/W in night mode

Select this to enable the Network Camera to automatically switch to Black/White during night mode.

### Turn on external IR illuminator in night mode

Select this to turn on an external IR illuminator (connected via Digital Output lines) when the camera detects low light condition and enters the night mode.

### Turn on built-in IR illuminator in night mode

Select this to turn on the built-in IR illuminators (effective range up to 20 meters) when the camera detects low light condition and enters the night mode.

### IR cut filter

With a removable IR-cut filter, this Network Camera can automatically remove the filter to let IR light enter the light sensor during low light conditions.

#### Auto mode

The Network Camera automatically removes the filter by judging the level of ambient light.

### ■ Day mode

In day mode, the Network Camera switches on the IR cut filter at all times to block infrared light from reaching the sensor so that the colors will not be distorted.

### ■ Night mode

In night mode, the Network Camera switches off the IR cut filter at all times for the sensor to accept infrared light, thus helping to improve low light sensitivity.

### ■ Synchronize with digital input (1~3)

The Network Camera automatically removes the IR cut filter when a Digital Input is triggerred.

### ■ Schedule mode

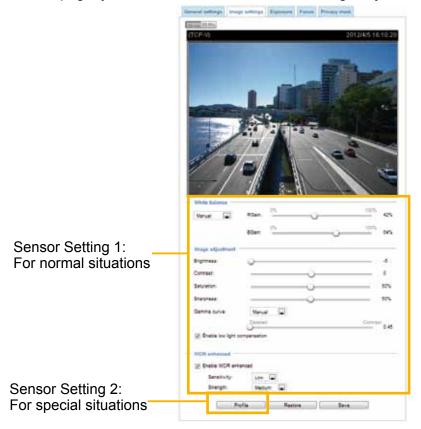
The Network Camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and end time of day mode are set to 07:00 and 18:00.

### <u>Light sensor sensitivity</u>

Select Low, Normal, or High sensitivity for the light sensor.

## **Image settings**

On this page, you can tune the White balance, Image adjustment and WDR enhanced.



White balance: Adjust the value for the best color temperature.

- You may follow the steps below to adjust the white balance to the best color temperature.
- 1. Place a sheet of paper of white or cooler-color temperature paper, such as blue, in front of the lens, then allow the Network Camera to automatically adjust the color temperature.
- 2. Click the **On** button to **Fix current value** and confirm the setting while the white balance is being measured.
- You may also manually tune the color temperature by pulling the RGain and BGain slide bards.

### **Image Adjustment**

- Brightness: Adjust the image brightness level, which ranges from -5 to +5.
- Contrast: Adjust the image contrast level, which ranges from -5 to +5.
- Saturation: Adjust the image saturation level, which ranges from 0% to 100%.
- Sharpness: Adjust the image sharpness level, which ranges from 0% to 100%.
- Gamma curve: Adjust the image sharpness level, which ranges from 0% to 100%. You may let firmware **Optimize** your display or select the **Manual** mode, and pull the slide bar pointer to change the preferred level of Gamma correction towards higher contrast or towards the higher luminance for detailed expression for both dark and lighted areas of an image.
- Enable low light compensation: Select this option in low light mode, and the values of sharpness and brightness will change automatically. This function also benefits from an automated noise reduction feature.

<u>WDR enchanced</u>: This function allows users to identify more details of objects in the high contrast environment especially for details in the shaded area. You may check the **Enable WDR enhanced** checkbox, and then adjust the sensitivity (low, high) and the strength (low, medium, high) to reach the best image quality.

WDR enhanced ———			
Enable WDR enhanced			
Sensitivity:	Low 💌		
Strength:	Medium <b>▼</b>		
Profile	Restore	Save	

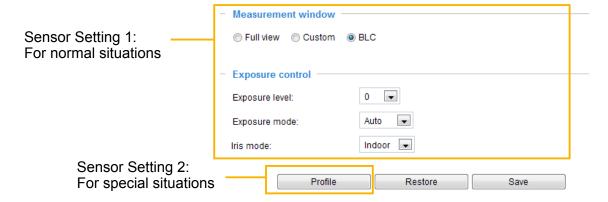
Note that the **Preview** button has been cancelled, all changes made to image settings is directly shown on screen. You can click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the setting. You can also click on **Profile** to adjust all settings above in a pop-up window for special lighting conditions.



<u>Activated period</u>: Select the mode this profile to apply to: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose Schedule mode. Then check **Save** to take effect.

# Exposure Advanced Mode

On this page, you can set the Measurement window, Exposure level, Exposure mode, and Iris mode. Detailed configurations will be automatically adjusted since the sensor library will automatically adjust the value according to the ambient light.



<u>Measurement Window</u>: This function allows users to configure measurement window(s) for low light compesation.

■ Full view: Calculate the full range of view and offer appropriate light compesation.

■ Custom: This option allows you to manually add specific windows as measuring areas. The measuring window refers to "weighed window" where the lighting condition within the particular area is taken into account. Camera firmware then adopts the weighed averages method to calculate the value.

A total of 9 inclusive and exclusive windows can be created for a view. You can create Exclude windows for the camera to ignore the lighting condition of certain areas.

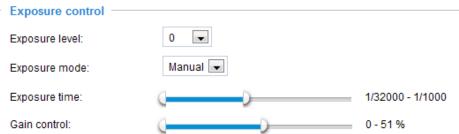
Note that the title pane of the Include/ Exclude windows is not included into the calculation.

■ BLC: When selected, a BLC window will appear on screen meaning that the center of the scene will be taken as a weighed area. This option enables light compensation for images that are too dark or too bright to recognize; for example, for the dark side of objects that is posed against bright sunlight.



### Exposure control:

- Exposure level: You can manually set the Exposure level, which ranges from -2.0 to +2.0 (dark to bright).
- Exposure mode: Select **Auto** or **Manual** mode according to your needs. **Manual**: Select **Manual** to set a fixed exposure time and gain. Then, tune the slide bar to set the Exposure time and Gain Control to the best image quality. A shorter exposure time allows less amount of light to enter the sensor; while a higher gain control value generates certain amount of noises.



**Auto**: If you set Exposure mode as **Auto**, the Exposure time and Gain control will not be configurable since the sensor library will automatically adjust the value according to the ambient light. Then you can set iris mode as "indoor" or "outdoor" to reach the best image quality.

■ Iris mode: Select Indoor or Outdoor iris mode to adapt to the installation. The preset iris aperture setting will apply.

You can click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the settings.

If you want to configure another sensor setting for day/night/schedule mode, please click **Profile** to open the Profile of exposure settings page as shown below.

<u>Activated period</u>: Select the mode this profile to apply to: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose Schedule mode. Then check **Save** to take effect.

Please follow the steps below to setup a profile:

- 1. Check Enable this profile.
- 2. Select the applied mode: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose Schedule mode.
- Configure Exposure control settings in the following columns. Please refer to previous dicussions for detailed information.
- 4. Click **Save** to enable the setting and click **Close** to exit the page.



# Focus Advanced Mode

The camera comes with a motorized vari-focal lens, and therefore a smart focus function panel is provided to facilitate zoom and focus configuration.



- Zoom: If you need to zoom in to a field of view, click and drag the pointer to the right to zoom in. Note that the size of the field of view will also be reduced.
- Focus: Whenever the zoom factor is changed or you see the live image is out of focus, you can click and drag its pointer to find the best focus by draging it along the slide bar. You can also use the Perform Auto Focus button to help achieve best image focus.

### **Auto Focus:**

Click the **Perform auto focus** button for the camera to automatically find the best focus. The process takes about 1 or 2 minutes to complete. A color bar will appear below the Focus slide bar. When the scan is completed, the Focus pointer will stay at the optimal location on the slide bar.

You may still need to use the "+" or "-" buttons to fine-tune the focus depending on the live image on your screen. "+" means moving from wide to tele end; and "-" tele to wide.

■ Full-range scan: If selected, the auto focus scan will be performed throughout the complete

range of focus. The full-range scan takes a longer time to complete. A full-range scan usually takes approximately 3 minutes or longer.

■ Fully-open Iris: By default, this checkbox is selected for performing an auto scan and should provide an optimal scan result.

### **Focus window:**

By default, the optimal focus is found on a full view window. You may designate a custom window within your current field of view to acquire the best focus out of it. However, you can not place a focus window on a distant background, e.g., a hall way that stretches away for 3 meters or farther. Doing so you will not benefit from the Focus window function.

- Full view: The focus tuning takes place by referring to the full view.
- Custom: You can create a focus window and drag it to a place of interest in your view window. Note that it is recommended to use this function only when you have a solid object in your view window that is showing a consistent color or texture. This function will not take effect if you set the focus window on a distant background.

# 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.



- To set the privacy mask windows, follow the steps below:
- 1. Click **New** to add a new window.
- 2. You can use the mouse cursor 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. Click on the **Enable privacy mask** checkbox to enable this function.



### NOTE:

- ▶ Up to 5 privacy mask windows can be set up on the same screen.
- ▶ If you want to delete the privacy mask window, please click the 'x' on the upper right corner of the window.

# Media > Video | Advanced Mode

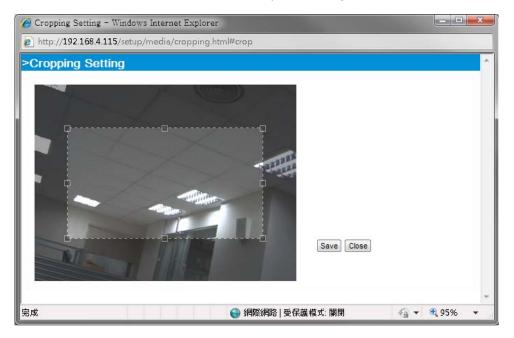
# **FOV** (Field of View)



Select a resolution from the list. The default is 5 Megapixels, and if bandwidth or frame rate per second is of the concern you can select a lower resolution. The configurable options are: 5MP (4:3) at 10fps, 3MP (4:3) 20fps, 2MP (4:3) 30fps, 1080P (16:9) 30fps, and 720P (16:9) at 60fps.

### **Cropping Setting:**

When you select a resolution other than the default 5MP, a Cropping Setting window will prompt. You then need to place the cropped window on a place of your interest by dragging it over the field of view. Note that you **CAN NOT** enlarge or shrink the cropping window. When done with selecting the field of view, click Save to preserve your setting and click Close to end the process.



# Stream settings

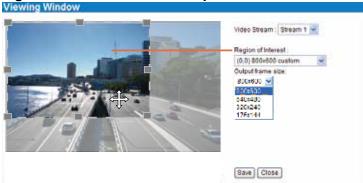


This Network Camera supports multiple streams with frame size ranging from 176 x 144 to 2560 x 1920 pixels.

The definition of multiple streams:

- Stream 1: Users can define the "Region of Interest" (viewing region) and the "Output Frame Size" (size of the live view window).
- Stream 2: The default frame size for Stream 2 is set to the minimized 176 x 144 for viewing on mobile devices.
- Stream 3: Stream 3 does not support the "Region of Interest" configuration.

Click **Viewing Window** to open the viewing region settings page. On this page, you can set the **Region of Interest** and the **Output Frame Size** for streams 1 and 2.



Please follow the steps below to set up those settings for a stream:

- 1. Select a stream for which you want to set up the viewing region.
- 2. Select a **Region of Interest** from the drop-down list. The floating frame, the same as the one in the Gloabl View window on the home page, will resize accordingly. If you want to set up a customized viewing region, you can also resize and drag the floating frame to a desired position with your mouse.
- 3. Choose a proper **Output Frame Size** from the drop-down list according to the size of your monitoring device.

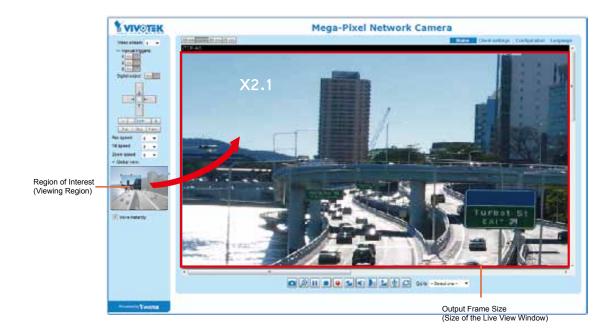


# NOTE:

- ▶ All the items in the "Region of Interest" should not be larger than the "Output Frame Size" (current maximum resolution).
- The parameters of the multiple streams:

	Region of Interest	Output frame size
Stream 1	2560 X 1920 ~ 176 x 144 (Selectable)	2560 X 1920 ~ 176 x 144 (Selectable)
Stream 2	2560 X 1920 ~ 176 x 144 (Selectable)	2560 X 1920 ~ 176 x 144 (Selectable)
	fixed	fixed

When completed with the settings in the Viewing Window, click **Save** to enable the settings and click **Close** to exit the window. The selected **Output Frame Size** will immediately be applied to the **Frame size** of each video stream. Then you can go back to the home page to test the e-PTZ function. For more information about the e-PTZ function, please refer to page 91.





Click the stream item to display the detailed information. The maximum frame size will follow your settings in the above Viewing Window sections.

This Network Camera 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 several parameters for you to adjust the video performance:



### ■ 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.

### ■ Maximum frame rate

This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality and for recognizing moving objects in the field of view.

The below frame rates apply when the lowest resolution, 720P, is selected for a stream:

If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, 0fps, 40fps, 45fps, and 50fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, 30fps, 40fps, 45fps, 50fps, 55fps, and 60fps. 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

#### Constant bit rate:

- Constant bit rate: A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. The bandwidth utilization is configurable to match 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, 4Mbps, 6Mbps, 8Mbps, 10Mbps, 12Mbps, 14Mbps, 16Mbps, 18Mbps, and 20Mbps. You can also select Customize and manually enter a value.
  - You should specifiy the bit rate setting either as an Average restriction or as an Upper bound threshold. If set to the Average, video bit rate will fluctuate around the Target bit rate setting.
- <u>Fixed quality</u>: 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 enter a value.

If JPEG mode is selected, the Network Camera sends consecutive 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:



#### ■ 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.

#### Maximum frame rate

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

If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps. You can also select **Customize** and manually enter a value. The frame rate will decrease if you select a higher resolution.

### ■ Video quality

Refer to the previous page setting an average or upper bound threshold for controlling the bandwidth consumed for transmitting motion jpegs. The configuration method is identical to that for MPEG4 and H.264.

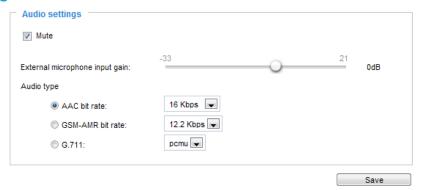


### NOTE:

- ► 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.

# Media > Audio | Advanced Mode

# **Audio Settings**



<u>Mute</u>: Select this option to disable audio transmission from the Network Camera to all clients. Note that if muted, 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 gain: Select the gain of the external audio input according to ambient conditions. Adjust the gain from +24 db (most sensitive) or -33db (least sensitive).

Audio type: Select audio codec AAC or GSM-AMR and the bit rate Advanced Mode

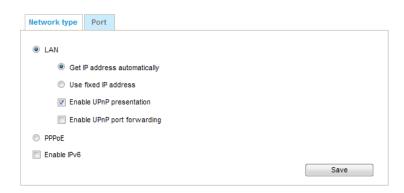
- AAC provides good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable from: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps, and 128Kbps.
- GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable from: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps, and 12.2Kbps.
- G.711 also provides good sound quality and requires about 64Kbps. Select pcmu (µ-Law) or pcma (A-Law) mode.

When completed with the settings on this page, click **Save** to enable the settings.

# **Network > General settings**

This section explains how to configure a wired network connection for the Network Camera.

# **Network Type**

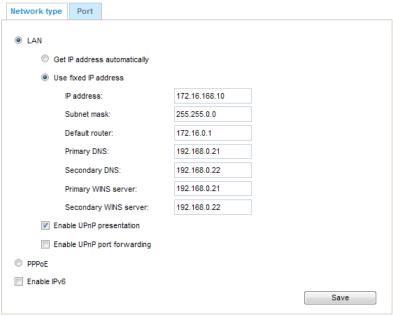


### LAN

Select this option when the Network Camera 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.

<u>Use fixed IP address</u>: Select this option to manually assign a static IP address to the Network Camera.



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 18 for details.

2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP.

<u>Subnet mask</u>: This is used to determine if the destination is in the same subnet. The default value is "255.255.25.0".

<u>Default router</u>: 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.

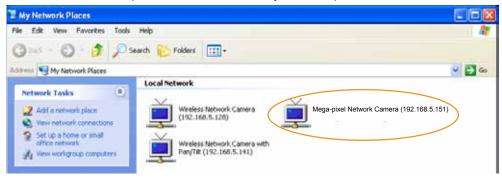
<u>Primary DNS</u>: The primary domain name server that translates hostnames into IP addresses.

<u>Secondary DNS</u>: Secondary domain name server that backups the Primary DNS.

<u>Primary WINS server</u>: The primary WINS server that maintains the database of computer names and IP addresses.

<u>Secondary WINS server</u>: The secondary WINS server that maintains the database of computer names and IP addresses.

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



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

### PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera 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 Network Camera's public IP address.

- 1. Set up the Network Camera on the LAN.
- 2. Go to Configuration > Event > Event settings > Add server (please refer to Add server on page 98) to add a new email or FTP server.
- 3. Go to Configuration > Event > Event settings > Add media (please refer to Add media on page 103).
  - 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 > General settings > Network type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.



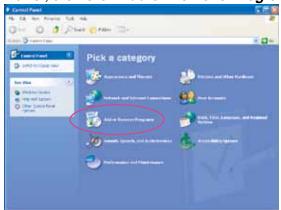
- 5. The Network Camera will reboot.
- 6. Disconnect the power to the Network Camera; remove it from the LAN environment.



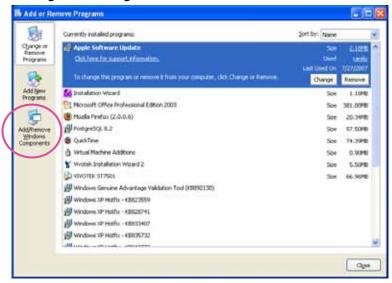
### NOTE:

- ▶ If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.
- ► If UPnP<sup>™</sup> 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<sup>™</sup> user interface on your computer:

  Note that you must log on to the computer as a system administrator to install the UPnP<sup>™</sup> components.
  - 1. Go to Start, click Control Panel, then click Add or Remove Programs.

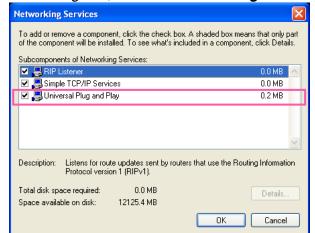


2. In the Add or Remove Programs dialog box, click Add/Remove Windows Components.



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

Details.



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

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



- 6. Click **Finish**.  $UPnP^{TM}$  is enabled.
- ► How does UPnP<sup>TM</sup> work?

  UPnP<sup>TM</sup> 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 Network Cameras, you will see Network Camera shortcuts under My Network Places.
- ▶ Enabling UPnP port forwarding allows the Network Camera 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 Network Camera's public address in order to access the Network Camera 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 Network Camera's IP address.

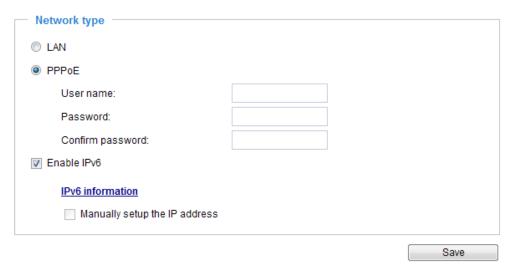
From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or
	http://192.168.4.160:8080

▶ If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 43 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.

### Enable IPv6

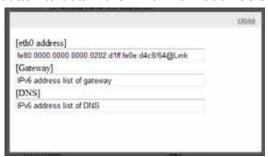
Select this option and click **Save** to enable IPv6 settings.

Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft<sup>®</sup> Internet Explorer 6.5, Mozilla Firefox 3.0 or above.



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

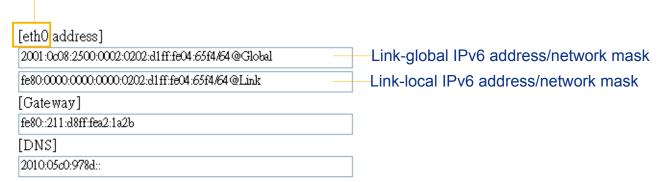
IPv6 Information: Click this button to obtain the IPv6 information as shown below.



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



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:



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

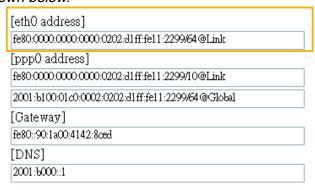




▶ If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to **HTTP** streaming on page 70 for detailed information.)



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



<u>Manually setup the IP address</u>: 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			
IPv6 information			
Manually setup the IP address			
Optional IP address / Prefix length	ı	1	64
Optional default router			
Optional primary DNS			

#### **Port**

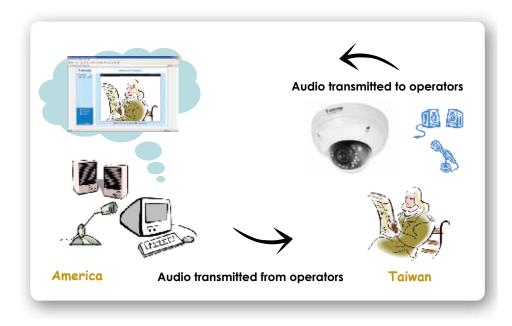
port —		
HTTPS port:	443	
Two way audio port:	5060	
FTP port:	21	
rir poit.	21	
		Save

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

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 Media > Video > Stream settings page and the media option is set to "Media > Video > Stream settings" on the Client Settings page. Please refer to Client Settings on page 32 and Stream settings on page 56.





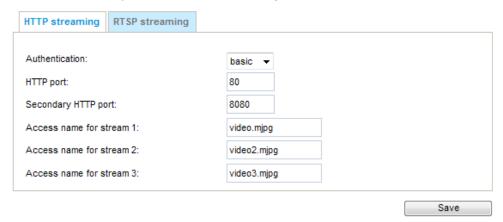
Click to enable audio transmission to the Network Camera; click to adjust the volume of microphone; click to turn off the audio. To stop talking, click again.

<u>FTP port</u>: 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.

# Network > Streaming protocols | Advanced Mode

### **HTTP streaming**

To utilize HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security > User account on page 80 for details.



<u>Authentication</u>: Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest.

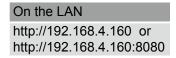
If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

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:





To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. 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 Network Camera's IP address.



Access name for stream  $1 \sim 3$ : This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. Users can click **Media > Video > Stream settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Stream settings on page 56.

When using **Mozilla Firefox** or **Netscape** to access the Network Camera 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 Network Camera to feed live pictures to Mozilla Firefox and Netscape.

URL command -- http://<ip address>:<http port>/<access name for stream 1, 2, or 3> 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.



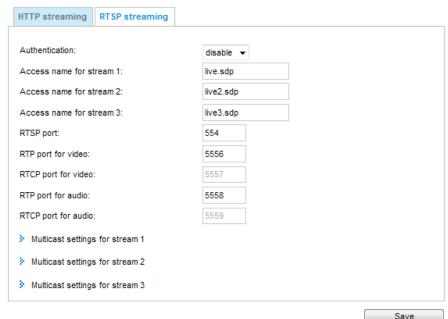


## NOTE:

- ▶ Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream 1, 2, or 3> will fail to access the Network Camera.
- ▶ Users can only use URL commands to request the stream 5. For more information about URL commands, please refer to page 121.

### **RTSP Streaming**

To utilize RTSP streaming authentication, make sure that you have set a password for controlling the access to video stream first. Please refer to Security > User account on page 80 for details.



<u>Authentication</u>: Depending on your network security requirements, the Network Camera 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	0	0
Basic	0	0
Digest	0	X

Access name for stream  $1 \sim 3$ : This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.

If you want to use an RTSP player to access the Network Camera, you have to set the video mode to H.264 / MPEG-4 and use the following RTSP URL command to request transmission of the streaming data.

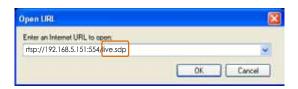
rtsp://<ip address>:<rtsp port>/<access name for stream 1 to 3>

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.





### 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 Network Camera 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:



<u>Multicast settings for stream 1, 2, and 3</u>: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1 or 2.

Multicast settings for stream 1:		Multicast settings for stream 3		
Always multicast		Always multicast		
Multicast group address:	239.128.1.99	Multicast group address:	239.128.1.101	
Multicast video port:	5560	Multicast video port:	5568	
Multicast RTCP video port:	5561	Multicast RTCP video port:	5569	
Multicast audio port:	5562	Multicast audio port:	5570	
Multicast RTCP audio port:	5563	Multicast RTCP audio port:	5571	
Multicast TTL [1~255]:	15	Multicast TTL [1~255]:	15	
w Multicast settings for stream 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:

It wast port number. Multicast stream 1 video port must be an even number.

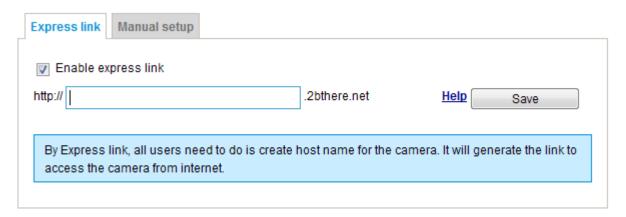
Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

# Network > DDNS

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

# **Express link**

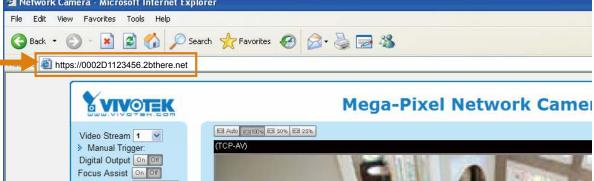
Express Link is a free service provided by VIVOTEK server, which allows users to register a domain name for a network device. One URL can only be mapped to one MAC address. This service will check out if the host name is valid and automatically open a port on your router. Unlike DDNS, the user has to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



Please follow the steps below to enable Express Link:

- 1. Make sure that your router supports UPnP port forwarding and it is activated.
- 2. Check Enable express link.
- 3. Enter a host name for the network device and click **Save**. 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 a message as shown below.





# Manual setup

# DDNS: Dynamic domain name service

DDNS: Dynamic domain name se	ervice ————————————————————————————————————
Enable DDNS:	
Provider:	Dyndns.org(Dynamic)
Host name:	
User name:	
Password:	

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

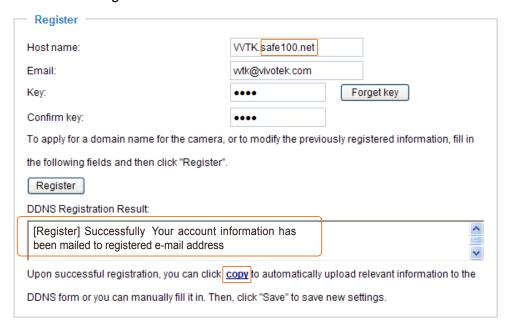
<u>Provider</u>: Select a DDNS provider from the provider drop-down list.

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 Network Cameras 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.

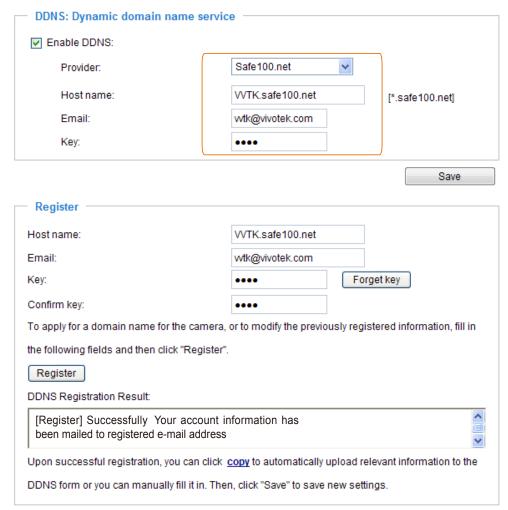
Note that before utilizing this function, please apply for a dynamic domain account first.

#### ■ 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.



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.



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.

<u>Forget key</u>: 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/

# Network > 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 the frame priority level from 0 (lowest) to 7 (highest). 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  $(0\sim4095)$  and choose the priority for each application  $(0\sim7)$ .



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



#### NOTE:

- ▶ A VLAN Switch (802.1p) is required. 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 guarantees 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).



# Network > SNMP (Simple Network Management Protocol) Advanced Mode

This section explains how to use the SNMP on the network camera. 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, network cameras, 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 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 authentication (at least 8 characters).
- Encryption password: Enter a password for encryption (at least 8 characters).



# **Security > User Account**

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

#### **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.

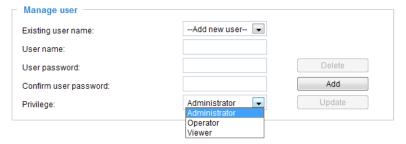
- 1. Type the password identically in both text boxes, then click **Save** to enable password protection.
- 2. A window will be prompted for authentication; type the correct user's name and password in their respective fields to access the Network Camera.

# Root password Privilege management Root password Privilege management Account management Allow anonymous viewing Operator: Digital output PTZ control Viewer: Digital output PTZ control Save

<u>Digital Output & PTZ control</u>: You can modify the management privilege for operators or viewers. Select or deselect the checkboxes, then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Configuration on page 34).

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

## **Account Management**



Administrators can create 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. Although 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 Network Camera on page 121. Viewers can only access 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.

# Security > HTTPS (Hypertext Transfer Protocol over SSL) Advanced Mode

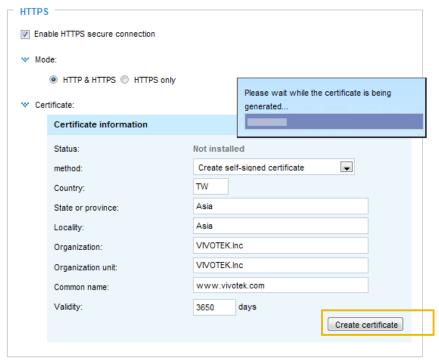
This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

#### **Create and Install Certificate Method**

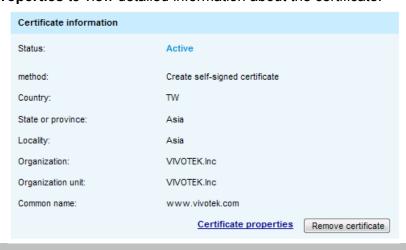
Before using HTTPS for communication with the Network Camera, a **Certificate** must be created first. There are three ways to create and install a certificate:

# **Create self-signed certificate**

- 1. Select this option from a pull-down menu.
- 2. In the first column, select **Enable HTTPS secure connection**, then select a connection option: "HTTP & HTTPS" or "HTTPS only".
- 3. Click Create certificate to generate a certificate.

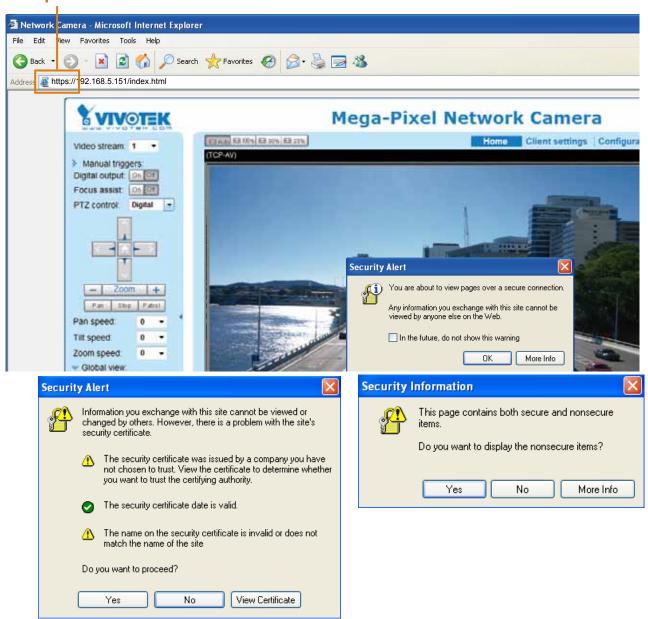


4. The Certificate Information will automatically be displayed as shown below. You can click **Certificate properties** to view detailed information about the certificate.



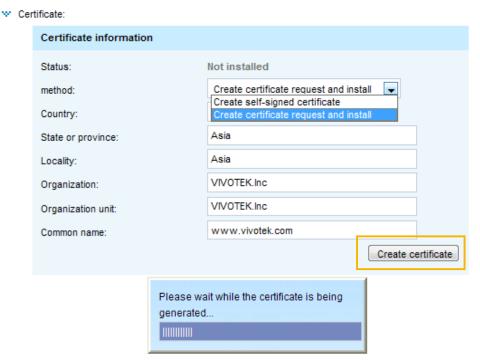
5. Click **Home** to return to the main page. Change the address from "<a href="http://">http://</a>" to "<a href="https://">https://</a>" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.

https://

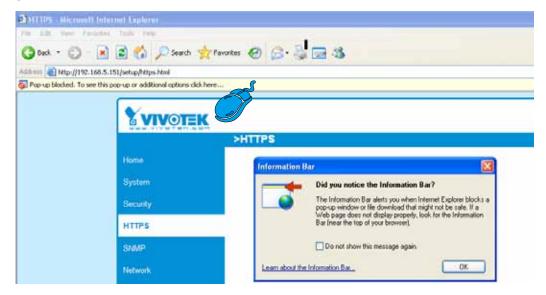


<u>Create certificate and install</u>: Select this option if you want to create a certificate from a certification authority.

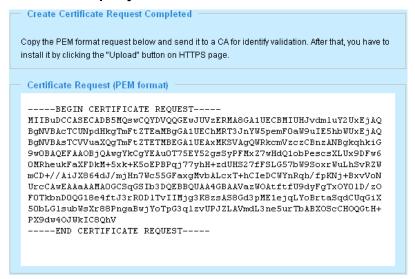
- 1. Select this option from a method pull-down menu.
- 2. Click **Create certificate** to generate the certificate.



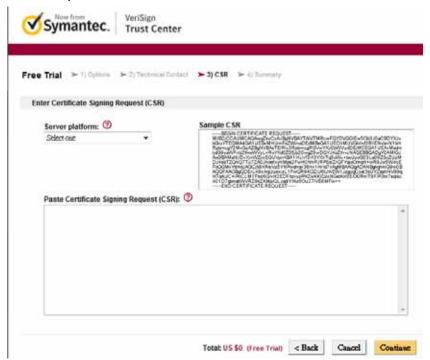
3. The following information will appear in a pop-up window after clicking **Create**. If you see the following Information bar, click **OK** and click on the Information bar at the top of the page to allow pop-ups.



4. 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.



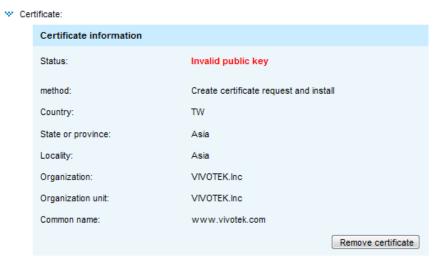
5. Copy the contents of the Certificate request (in PEM format). Use the contents to apply for a 3rd-party certification authority such as Symantec VeriSign. Wait for the certificate authority to issue an SSL certificate; click Browse to search for the issued certificate, and then click Upload to finish the process.





# NOTE:

- ► How do I cancel the HTTPS settings?
  - 1. Click on the Remove certificate button.



政治

2. If you are currently running a secure connection The webpage will redirect to a non-HTTPS page automatically.

# **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 before clicking the **Save** button.

被定



# Security > Access List Advanced Mode

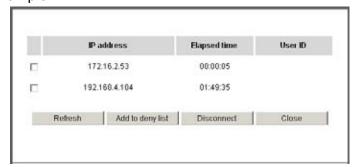
This section explains how to control access permission by verifying the client PC's IP address.

# **General Settings**



Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 to stream 3). 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 Explorer or Quick Time Player).

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



Note that only consoles that are currently displaying live streaming will be listed in the View Information list.

- IP address: Current connections to the Network Camera.
- 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 that 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 > User account on page 80.
- 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 71.
- 3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing**, please refer to page 80.

- 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).

#### **Filter**

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

<u>Filter type</u>: 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. 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.



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 Network > General settings on page 62 for detailed information.

There are three types of rules:

<u>Single</u>: This rule allows the user to add an IP address to the Allowed/Denied list. For example:



<u>Network</u>: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List. The address and network mask are written in CIDR format. For example:



IP address range 192.168.2.x will be bolcked.

Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List. Note: This rule only applies to IPv4 addresses. For example:



## **Administrator IP address**

<u>Always allow the IP address to access this device</u>: You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.



# Security > 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.

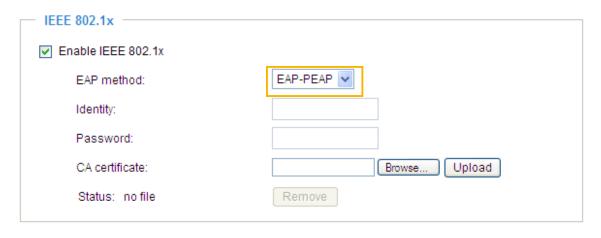
■ The components of a protected network with 802.1x authentication:

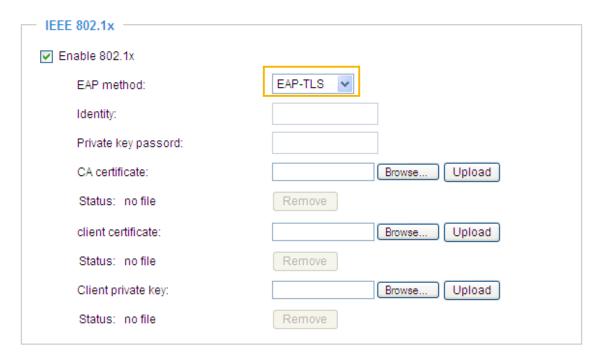


- 1. Supplicant: A client end user (camera), which requests authentication.
- 2. Authenticator (an access point or a switch): A "go between" which restricts unauthorized end users from communicating with the authentication server.
- 3. Authentication server (usually a RADIUS server): Checks the client certificate and decides whether to accept the end user's access request.
- VIVOTEK Network Cameras 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 Network Camera to the protected network with 802.1x, please apply a digital certificate from a Certificate Authority (i.e., your network administrator) which can be validated by a RADIUS server.
- Connect the Network Camera to a PC or notebook outside of the protected LAN. Open the
  configuration page of the Network Camera 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).



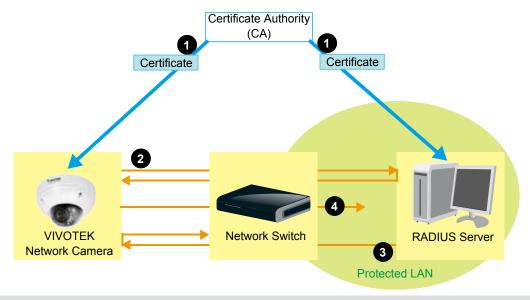


3. When all settings are complete, move the Network Camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.



# NOTE:

- ► The authentication process for 802.1x:
- 1. The Certificate Authority (CA) provides the required signed certificates to the Network Camera (the supplicant) and the RADIUS Server (the authentication server).
- 2. A Network Camera 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 Network Camera and returns an acceptance or rejection back to the switch.
- 3. The switch also forwards the RADIUS Server's certificate to the Network Camera.
- 4. Assuming all certificates are validated, the switch then changes the Network Camera's state to authorized and is allowed access to the protected network via a pre-configured port.

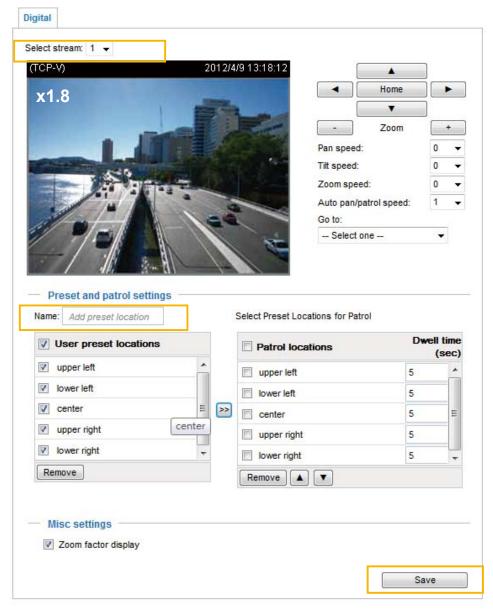


# PTZ > PTZ settings Advanced Mode

This section explains how to control the Network Camera's Pan/Tilt/Zoom operation.

# **Digital PTZ Operation (E-PTZ Operation)**

The e-PTZ control settings section will be displayed as shown below:



<u>Select Stream</u>: Select a video stream to set up the e-PTZ control. Please note that each stream can possess its own preset and patrol settings. For detailed information about how to set up preset and patrol settings, please refer to page 91.

Auto pan/patrol speed: Select the speed from 1~5 (slow/fast) to set up the Auto pan/patrol speed control.

When completed with the e-PTZ settings, click **Save** to enable the settings on this page.

# Home page in E-PTZ Mode



- The e-Preset Positions will also be displayed on the home page. Select one from the drop-down list, and the Network Camera will move to the selected position.
- If you have set up different preset positions for different streams, you can select one of the video streams to display its separate preset positions.

#### **Global View**

In addition to using the e-PTZ control panel, you can also use the mouse to drag or resize the floating frame to pan/tilt/zoom the viewing region. The live view window will also move to the viewing region accordingly.

#### Moving Instantly

If you check this item, the live view window will switch to the new viewing region instantly after you move the floating frame.

# Click on Image

The e-PTZ function also supports "Click on Image". When you click on any point of the Global View Window or Live View Window, the viewing region will also move to that point.

Note that the "Click on Image" function only applies when you have configured a smaller "Region of Interest" out of the maximum output frame! e.g., a 1600x1200 region from the camera's 2560x1920 maximum frame size.

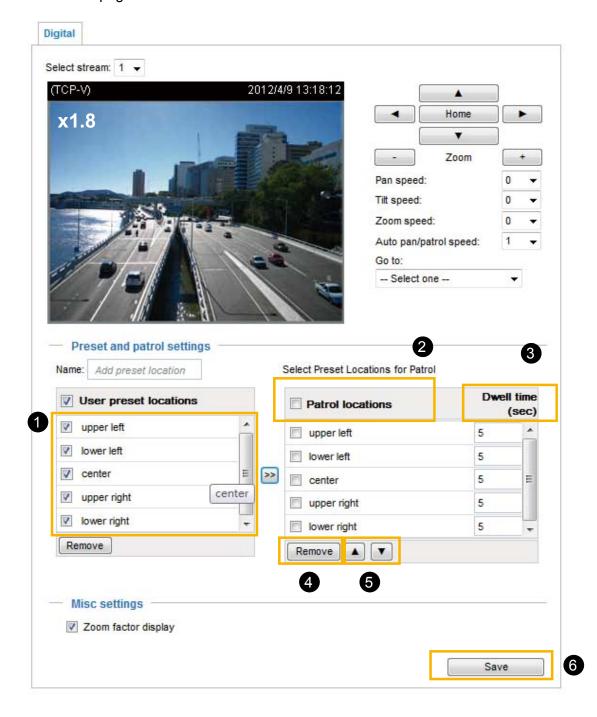
Patrol button: Click this button, then the Network Camera will patrol among the selected preset positions continuously.

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





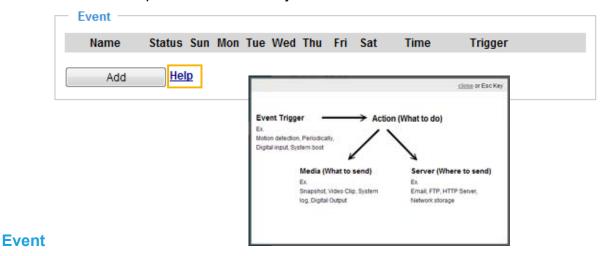
# NOTE:

- ▶ The Preset Positions will also be displayed on the home page. Select one from the Go to drop-down list, and the Network Camera will move to the selected preset position.
- ► Click Patrol: The Network Camera will patrol along the selected positions repeatedly. Please refer to page 93 to see more details.

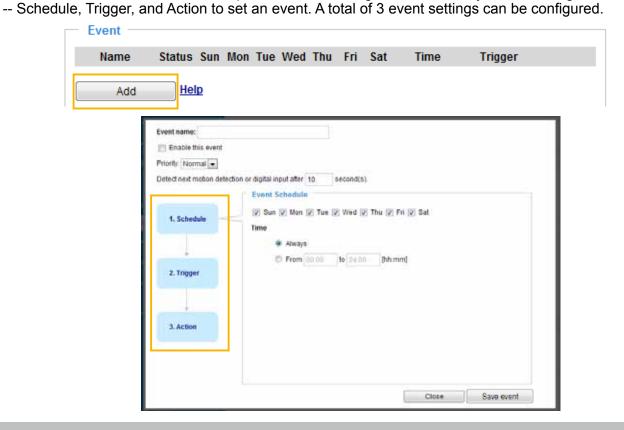
# **Event > Event settings**

Advanced Mode

This section explains how to configure the Network Camera to responds to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or e-mail address as notifications. Click on **Help**, there is an illustration shown in the pop-up window explaining that 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 Network Camera to send snapshots or videos to your email address or FTP site.



To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated. An event is an action initiated by a user-defined trigger source. In the **Event** column, click **Add** to open the event settings window. Here you can arrange three elements



- 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. This can prevent event-related actions to be too frequently performed.

## 1. Schedule

Specify the period of them during which the event trigger will take place. Please select the days of the week and the time in a day (in 24-hr time format) for the event triggering schedule.

# 2. Trigger

This is the cause or stimulus which defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.

There are several choices of trigger sources as shown on next page. Select the item to display the detailed configuration options.

#### ■ 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 108 for details.

Video motion detection		
Normal: door		
Profile: nallway		
Note: Please configure	Motion detection firs	st

#### ■ Periodically

This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.

Periodically		
Trigger every other	1	minutes

#### ■ Digital input

This option allows the Network Camera 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.

#### ■ System boot

This option triggers the Network Camera when the power to the Network Camera is disconnected.

# Recording notify

This option allows the Network Camera to trigger when the recording disk is full or when recording starts to rewrite older data.

■ Camera tampering detection

This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 111 for detailed information.



■ Manual Trigger

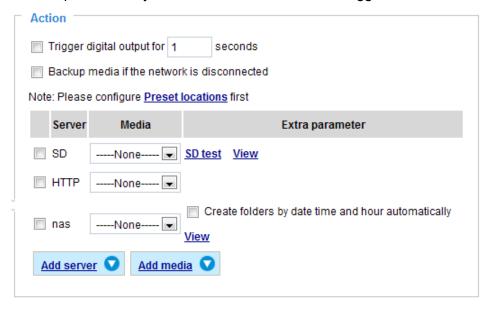
This option allows users to enable event triggers manually by clicking the on/off button on the homepage. Please configure 1 to 3 associated events before using this function.





## 3. Action

Define the actions to be performed by the Network Camera when a trigger is activated.

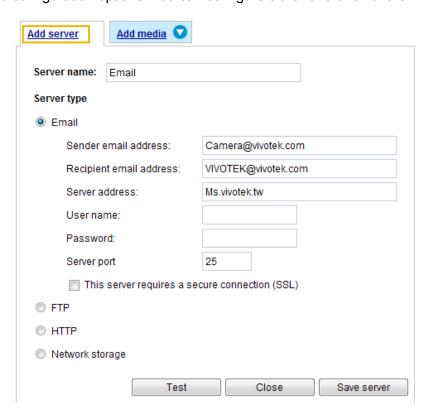


- Trigger digital output for □ seconds
  Select this option to turn on the external digital output device when a trigger is activated. Specify the length of the trigger interval in the text box.
- Backup media if the network is disconnected Select this option to backup media file on SD card if the network is disconnected. This function will only be displayed after you set up a network storage (NAS).

#### **Add server**

To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated. Click **Add server** to open the server setting window. You can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

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.



#### Server type - Email

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

- Server name: Enter a name for the server setting.
- 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.



Click **Save server** to enable the settings.

Note that after you set up the first event server, the new event server will automatically display on the Server list. If you wish to add other server options, click **Add server**.



#### Server type - FTP

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



- Server name: Enter a name for the server setting.
- 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 Network

  Camera will automatically 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. The firmware default has the Passive mode checkbox selected.

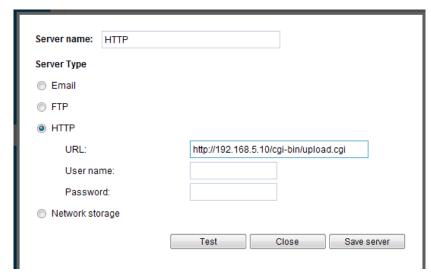
To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as shown below. If successful, you will also receive a test.txt file on the FTP server.



Click Save server to enable the settings.

## Server type - HTTP

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



- Server name: Enter a name for the server setting.
- 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.





Click **Save server** to enable the settings.

#### Network storage:

Select to send the media files to a network storage location when a trigger is activated. Please refer to **NAS server** on page 115 for details.

Click **Save server** to enable the settings.



- SD Test: Click to test your SD card. The system will display a message indicating success or failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 103 for detailed information.
- View: Click this button to open a file list window. This function is only for SD card and Network Storage. If you click the View button of SD card, a Local storage page will pop up for you to manage recorded files on SD card. For more information about Local storage, please refer to page 117. If you click the View button of Network storage, a file directory window will prompt for you to view recorded data on Network storage. For detailed illustration, please refer to the next page.
- Create folders by date, time, and hour automatically: If you check this item, the system will generate folders automatically by the date when video footages are stored onto the networked storage.

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



# Click 20110220 to open the directory:

The format is: HH (24r)

Click to open the file list for that hour

< 07 <u>08 09 10 11 12 13 14 15 16 17 ≥</u>					
file name	size	date	time		
Recording 1 58.mp4	2526004	2011/02/20	07 58 28		
Recording 1 59.mp4	2563536	2011/02/20	07 59 28		
Delete Delete all Back					
Click to delete selected items		o go back to the	e previous		

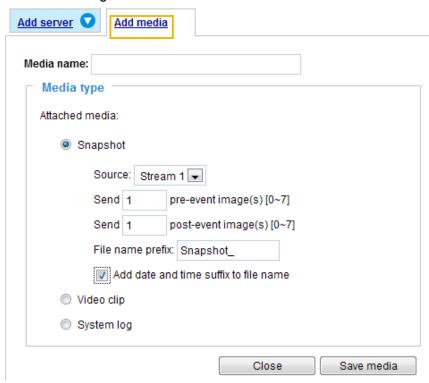
Click to delete all recorded data

< 07 <u>08 09 10 11 12 13 14 15 16 17 &gt;</u>					
	file nam	ie	size	date	time
	Recording 1 5	8 <u>.mp4</u>	2526004	2011/02/20	07:58:28
	Recording 1 5	9 <u>mp4</u>	2563536	2011/02/20	07:59:28
Delete all Back					

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

#### Add media

Click **Add media** to open the media setting window. 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. 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.

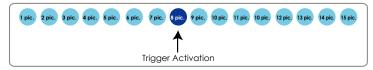


# Media type - Snapshot

Select to send snapshots when a trigger is activated.

- Media name: Enter a name for the media setting.
- Source: Select to take snapshots from any of the video streams.
- Send ☐ pre-event images
  The Network Camera 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.

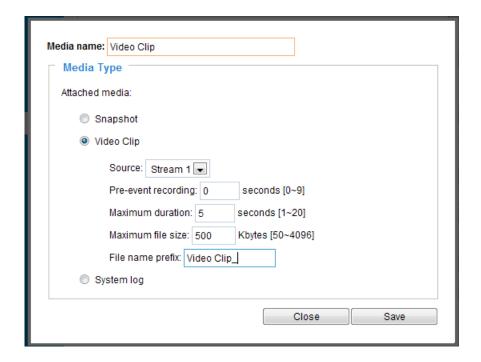
■ Add date and time suffix to the file name Select this option to add a date/time suffix to the file name. For example:

Click **Save media** to enable the settings.

To note that after you set up the first media server, a new column for media server will automatically show up on the Media list. If you wish to add more other media options, click **Add media**.

### Media type - Video clip

Select to send video clips when a trigger is activated.



- Media name: Enter a name for the media setting.
- Source: Select the source of video clip.
- Pre-event recording

The Network Camera 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 Network Camera continues to record for another 4 seconds after a trigger is activated.



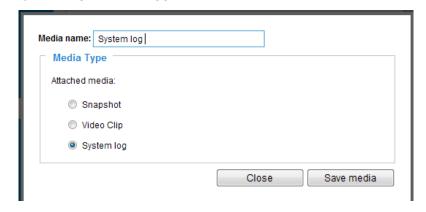
- Maximum file size Specify the maximum file size allowed.
- File name prefix Enter the text that will be appended to the front of the file name. For example:



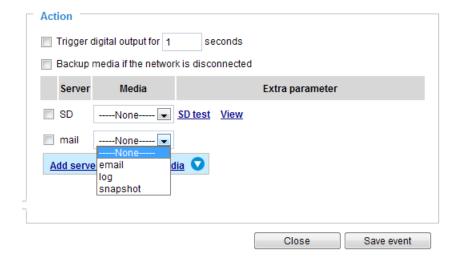
Click **Save media** to enable the settings.

# Media type - System log

Select to send a system log when a trigger is activated.



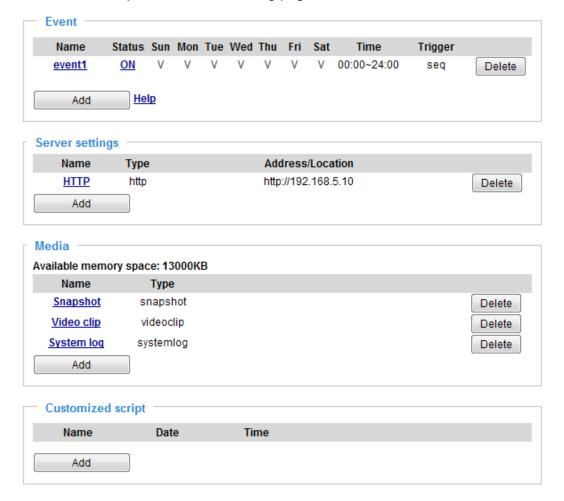
Click Save media to enable the settings, then click Close to exit the page.



In the Event settings column, the Servers and Medias you configured will be listed; please make sure the Event -> Status is indicated as **ON**, in order to enable the event triggering action.

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

Please see the example of the Event setting page below:



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

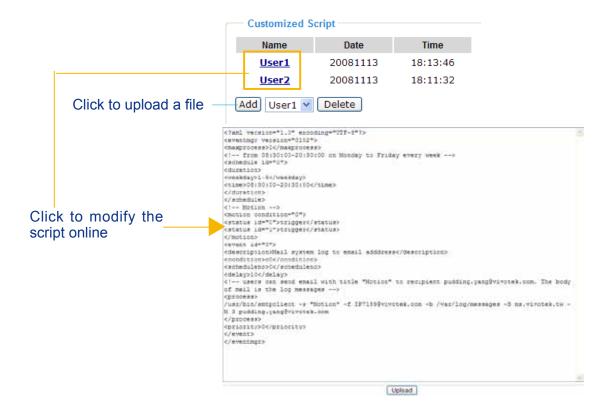
If you want to stop the event trigger, you can click **ON** to turn it to **OFF** status or click **Delete** to remove the event setting.

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

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

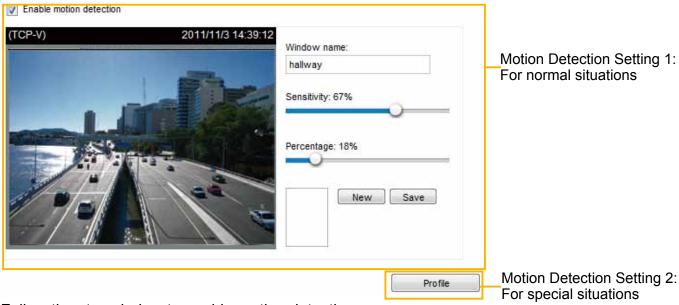
# **Customized Script**

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 prompt. If you need more information, please contact VIVOTEK technical support.



# **Applications > Motion detection**

This section explains how to configure the Network Camera to enable motion detection. A total of three motion detection windows can be configured.



Follow the steps below to enable motion detection:

- 1. Click **New** to add a new motion detection window.
- 2. 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 a window, click X on the upper right corner of the window.
- 3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slider bar.
- 4. Click **Save** to enable the settings.
- 5. Select **Enable motion detection** to enable this function.

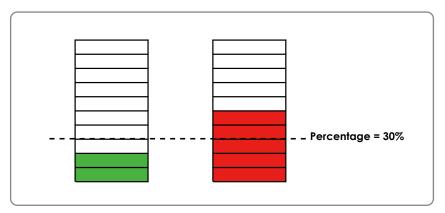
For example:



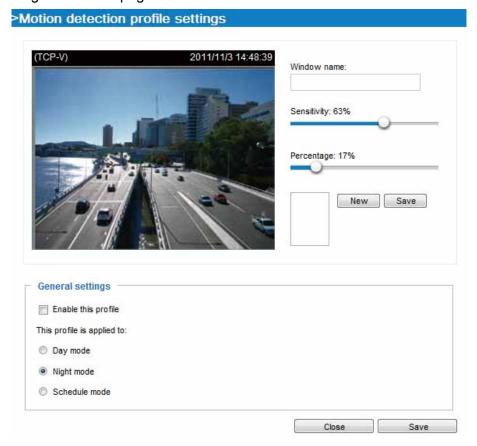
The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured 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 Event settings on page 95.

Profile

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.



If you want to configure other motion detection settings for day/night/schedule mode, please click **Profile** to open the Motion Detection Profile Settings page as shown below. A total of three motion detection windows can be configured on this page as well.



Please follow the steps below to set up a profile:

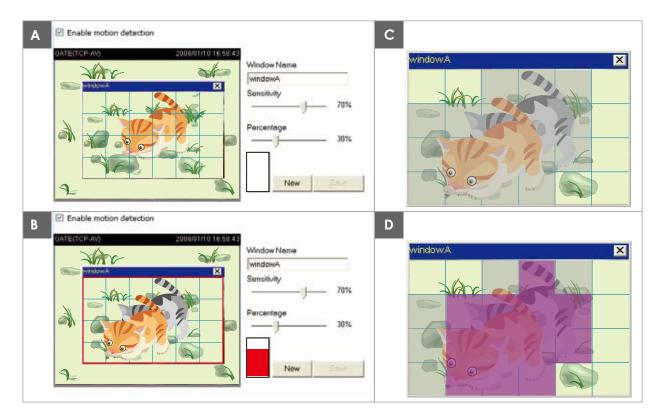
- 1. Create a new motion detection window.
- 2. Check Enable this profile.
- 3. Select the applicable mode: Day mode, Night mode, or Schedule mode. Please manually enter a time range if you choose Schedule mode.
- 4. Click **Save** to enable the settings and click **Close** to exit the page.

This motion detection window will also be displayed on the Event Settings page. You can go to Event > Event settings > Trigger to choose it as a trigger source. Please refer to page 113 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.

## Applications > DI and DO Advanced Mode



Connect DI or DO devices to the camera's terminal block, the camera will automatically detect the current connection state as pulled-high or pulled-low. You may then define the triggering condition.

<u>Digital input</u>: Select High or Low to define the "Normal status" for the digital input. The Network Camera will report the current status.

<u>Digital output</u>: Select Grounded or Open to define the "Normal status" for the digital output. The Network Camera will show whether the trigger is activated or not.

## **Applications > Tampering detection**

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



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

- 1. Check **Enable camera tampering detection**.
- 2. Enter the tamper trigger duration. (10 sec. ~ 10 min.) The tamper 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 **Event > Event settings > Trigger.** Please refer to page 113 for detailed information.

## Recording > Recording settings | Advanced Mode

This section explains how to configure the recording settings for the Network Camera.

#### **Recording Settings**

# Insert your SD card and click here to test Recording settings Name Status Sun Mon Tue Wed Thu Fri Sat Time Source Destination Delete Add SD test Note: Before setup recording, you may setup network storage via NAS server page



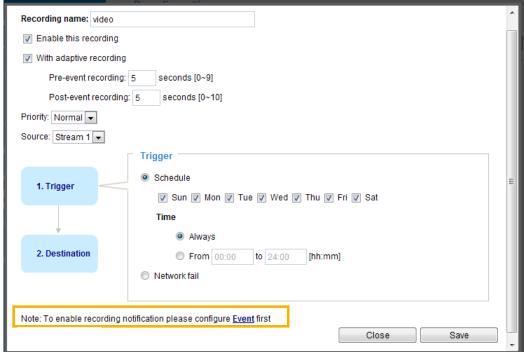
#### NOTE:

▶ Please remember to format your SD card when using it for the first time. Please refer to page 117 for detailed information.

#### **Recording Settings**

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

configured.

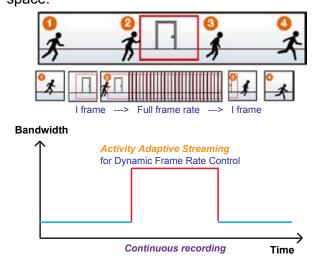


- Recording name: Enter a name for the recording setting.
- Enable this recording: Select this option to enable video recording.
- With adaptive recording:

  Select this option will activate the frame rate control according to alarm trigger.

  The frame control means that when there is a triggered alarm, the frame rate will raise up to the value you've set on Video quality page. Please refer to page 59 for more information.

If you enable adaptive recording and enable time-shift cache stream on Camera A, only when an event is triggered on Camera A will the server record the full frame rate streaming data; otherwise, it will only request the I frame data during normal monitoring, thus effectively save lots of bandwidths and storage space.





- ➤ To enable adaptive recording, please make sure you've set up the trigger source such as Motion Detection, DI Device, or Manual Trigger.
- ▶ When there is no alarm trigger:
  - JPEG mode: record 1 frame per second.
  - H.264 mode: record I frame only.
  - MPEG-4 mode: record the I frame only.
- ► When the I frame period is >1s on Video settings page, firmware will force decrease the I frame period to 1s when adaptive recording is enabled.

The alarm trigger includes: motion detection and DI detection. Please refer to Event Settings on page 95.

- Pre-event recording and post-event recording The Network Camera 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 for the recording source.

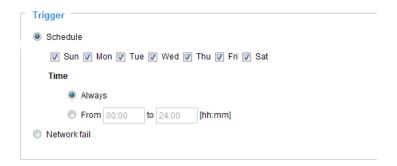


#### NOTE:

▶ To enable recording notification please configure **Event settings** first . Please refer to page 95.

Please follow the steps below to set up the recording.

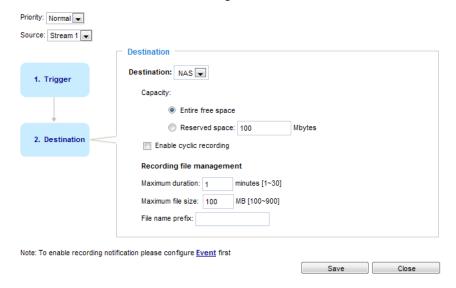
# Trigger Select a trigger source.



- Schedule: The server will start to record files on the local storage or network storage (NAS).
- Network fail: Since network fail, the server will start to record files on the local storage (SD card).

#### 2. Destination

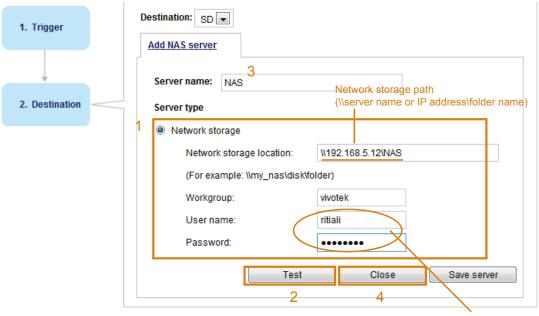
You can select the SD card or network storage (NAS) for the recorded video files. If you have not configured a NAS server, see details in the following.



#### **NAS** server

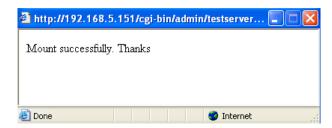
Click **Add NAS server** to open the server setting window and follow the steps below to set up:

1. Fill in the information for your server. For example:



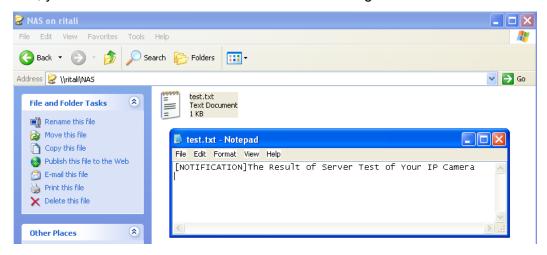
User name and password for your server

2. Click **Test** to check the setting. The result will be shown in the pop-up window.

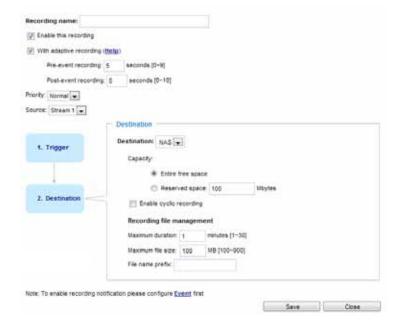




If successful, you will receive a test.txt file on the network storage server.



- 3. Enter a server name.
- 4. Click **Save** to complete the settings and click **Close** to exit the page.

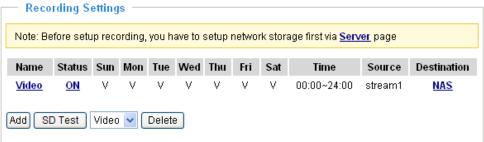


- Capacity: You can choose either the entire free space available or limit the reserved space. The recording size limit must be larger than the reserved amount for cyclic recording.
- File name prefix: Enter the text that will be appended to the front of the file name.
- Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for the transaction stage when the storage space is about to be full and new data arrives. The minimum for the Reserved space must be larger than 15 MBytes.
- Recording file management: You can manually assign the Maximum duration and the Maximum file size for each recording footage. You may need to stitch individual files together under some circumstances. You may also designate a file name prefix by filling in the responsive text field.

f you want to enable recording notification, please click **<u>Event</u>** to configure event triggering settings. Please refer to **Event > Event settings** on page 95 for more details.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the network storage. The new recording name will appear in the drop-down list on the recording page as shown below.

To remove a recording setting from the list, select a recording name from the drop-down list and click **Delete**.



- Click <u>Video</u> (Name): Opens the Recording Settings page to modify.
- Click ON (Status): The Status will become OFF and stop recording.
- Click <u>NAS</u> (**Destination**): Opens the file list of recordings as shown below. For more information about folder naming rules, please refer to page 101 for details.





#### IMPORTANT:

Due to the limitations of file system and video recording format, a video recording interrupted by sabotage or power outage will produce inaccessible video fragments. And the loss of video makes it difficult to identify who sabotaged the camera and the assets it aims to protect.

This revision of firmware (0100d0 and above) supports "**Recoverable Recording**," a feature that enables the usability of video footages taken immediately before (less than 1 second) an interruption. By inserting meta tags and pointers to videos, videos recorded to the onboard SD card or networked storage is viewable even when it is abnormally discontinued. Some video frames will still be lost, yet it is now possible to retrieve important footages taken before a camera is destroyed or its power disconnected.

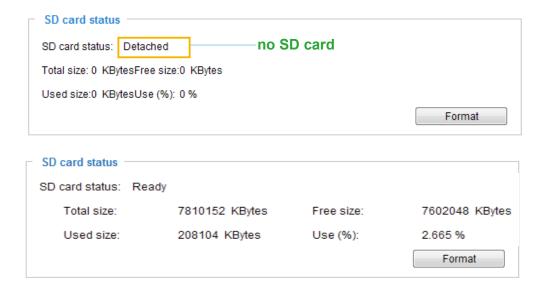
You can select the **Recovered** checkbox to search for the videos particularly affected by an interruption.

## Local storage > SD card management Advanced Mode

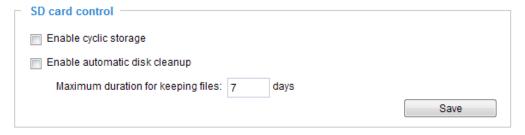
This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, and implement SD card control.

#### 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 control



- 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.

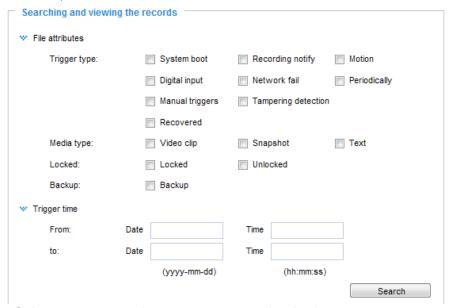
Click **Save** to enable your settings.

## Local storage > Content management | Advanced Mode

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** column.

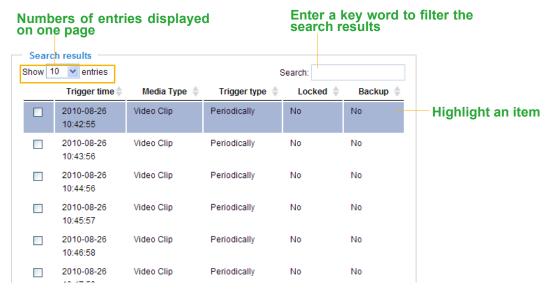


- File attributes: Select one or more items as your search criteria.
- Trigger time: Manually enter the time range you want to search.

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.



■ 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:

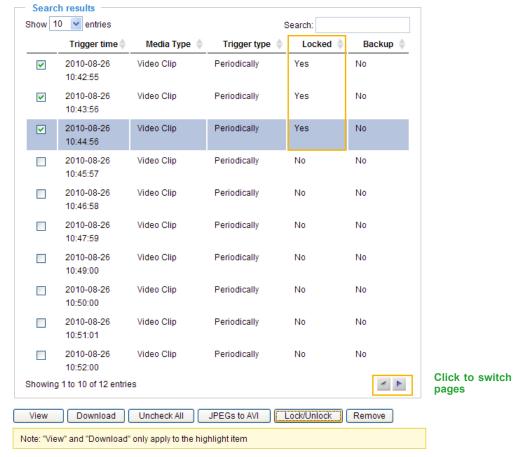


Click to adjust the image size

- 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 recording. You can click again to unlock the selections.

For example:



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

# **Appendix**

#### **URL Commands for the Network Camera**

#### 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

CGI parameters are written in lower-case and as one word without any underscores or other separators. 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,	1. Can view, listen, talk to camera.
	dido, camctrl	2. Can control DI/DO, PTZ of the camera.
4 [operator]	anonymous, viewer,	Operator access rights can modify most of the camera's
	dido, camctrl, operator	parameters except some privileges and network options.
6 [admin]	anonymous, viewer,	Administrator access rights can fully control the camera's
	dido, camctrl, operator,	operations.
	admin	
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>*] or *<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>...][&update=<value>][&return=<return page>]

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

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

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

[&<parameter>=<value>...][&update=<value>] [&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION	
<group>_<name></name></group>	value to assigned	Assign <i><value></value></i> to the parameter <i><group>_<name></name></group></i> .	
update	<boolean></boolean>	Set to 1 to update all fields (no need to update parameter in	
		each group).	
return	<return page=""></return>	Redirect to the page < return page > after the parameter is	
		assigned. The <return page=""> can be a full URL path or relative</return>	
		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)	
		or a VIVOTEK server script executable (.vspx) file. 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

 $r\n$ 

# 7. Available parameters on the server

#### Valid values:

VALID VALUES	DESCRIPTION		
string[ <n>]</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>]</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></n></m>	Any number between 'm' and 'n'.		
domain name[ <n>]</n>	A string limited to a domain name shorter than `n' characters (eg.		
	www.ibm.com).		
email address [ <n>]</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>,</value1>	Enumeration. Only given values are valid.		
<value2>,</value2>			
<value3>,</value3>			

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]	Mega-Pixel Network Camera	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
ledoff	<boolean></boolean>	0	6/6	Turn on (0) or turn off (1) all led indicators.
lowlight	<boolean></boolean>	1	6/6	Turn on white light LED under all conditions.  Only turn on white light LED in low light conditions.
date	<yyyy <br="" mm="">DD&gt;, keep, auto</yyyy>	<current date=""></current>	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:s s&gt;, keep, auto</hh:mm:s 	<current time=""></current>	6/6	Current time of the system.  Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	<mmddhh mmYYYY.ss &gt;</mmddhh 	<blank></blank>	6/6	Another current time format of the system.
ntp	<domain name="">, <ip address="">, <blank></blank></ip></domain>	<blank></blank>	6/6	NTP server.  *Do not use "skip to invoke default server" for default value.
timezoneindex	-489 ~ 529	320	6/6	Indicate timezone and area480: 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 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is.

				520: GMT 13:00 Nuku'Alofa
daylight_enable	<boolean></boolean>	0	6/6	Enable automatic daylight
				saving time in time zone.
daylight_dstactualmode	<boolean></boolean>	1	6/7	Check if current time is under
				daylight saving time.
				(Used internally)
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,	6/6	List time zone index which
		-280,-240,		support daylight saving time.
		-241,-200,		
		-201,-160,		
		-140,-120,		
		-80,-40,0,		
		40,41,80,		
		81,82,83,		
		120,140,		
		380,400,48		
		0		
updateinterval	0,	0	6/6	0 to Disable automatic time
	3600,			adjustment, otherwise, it
	86400,			indicates the seconds
	604800,			between NTP automatic
	2592000			update intervals.
restore	0,	N/A	7/6	Restore the system
	<positive< td=""><td></td><td></td><td>parameters to default values</td></positive<>			parameters to default values
	integer>			after <value> seconds.</value>
reset	0,	N/A	7/6	Restart the server after
	<positive< td=""><td></td><td></td><td><value> seconds if <value></value></value></td></positive<>			<value> seconds if <value></value></value>
	integer>			is non-negative.
restoreexceptnet	<any< td=""><td>N/A</td><td>7/6</td><td>Restore the system</td></any<>	N/A	7/6	Restore the system
	value>			parameters to default values
				except (ipaddress, subnet,
				router, dns1, dns2, pppoe).
	i	1		
1				This command can cooperate
				This command can cooperate with other

commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.  restoreexceptdst <pre></pre>			1		I
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					commands. When
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 for a union of combined results. This command can cooperate with other 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					cooperating with others, the
restoreexceptdst <pre></pre>					system parameters will be
restoreexceptdst <pre></pre>					restored to the default value
restoreexceptdst <pre></pre>					except for a union of the
value>  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.
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.  Testoreexceptlang	restoreexceptdst	<any< td=""><td>N/A</td><td>7/6</td><td>Restore the system</td></any<>	N/A	7/6	Restore the system
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 <a href="#">Any</a> 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		value>			parameters to default values
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					except all daylight saving time
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					settings.
"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					This command can cooperate
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					with other
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					"restoreexceptXYZ"
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					commands. When
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					cooperating with others, the
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					system parameters will be
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					restored to default values
restoreexceptlang <pre></pre>					except for a union of
Value>  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.
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	restoreexceptlang	<any< td=""><td>N/A</td><td>7/6</td><td>Restore the system</td></any<>	N/A	7/6	Restore the system
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		Value>			parameters to default values
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					except the custom language
with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the					file the user has uploaded.
"restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the					This command can cooperate
commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the					with other
cooperating with others, the system parameters will be restored to the default value except for a union of the					"restoreexceptXYZ"
system parameters will be restored to the default value except for a union of the					commands. When
restored to the default value except for a union of the					cooperating with others, the
except for a union of the					system parameters will be
					restored to the default value
combined results.					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]	FD8372	0/7	Internal model name of the server (eg. IP7139)
extendedmodelname	string[40]	FD8372	0/7	ODM specific model name of server (eg. DCS-5610). If it is not an ODM model, this field will be equal to "modelname"
serialnumber	<mac address&gt;</mac 	<pre><pre><pre><pre>mac address&gt;</pre></pre></pre></pre>	0/7	12 characters MAC address (without hyphens).
firmwareversion	string[40]	<pre><pre><pre><pre>dependent &gt;</pre></pre></pre></pre>	0/7	Firmware version, including model, company, and version number in the format: <model-brand-version></model-brand-version>
language_count	<integer></integer>	9	0/7	Number of webpage languages available on the server.
language_i<0~(count-1)>	string[16]	<pre><pre><pre><pre>dependent</pre>&gt;</pre></pre></pre>	0/7	Available language lists.
customlanguage_maxcoun t	<integer></integer>	1	0/6	Maximum number of custom languages supported on the server.
customlanguage_count	<integer></integer>	0	0/6	Number of custom languages which have been uploaded to the server.
customlanguage_i<0~(ma xcount-1)>	string	<blank></blank>	0/6	Custom language name.

## 7.2 Status

Group: status

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
videoactualmodulation	ntsc,	1	4/7	The actual modulation
<pre><pre><pre>oduct dependent&gt;</pre></pre></pre>	pal			type
				(videoin.type=0).
di_i<0~(ndi-1)>	<boolean></boolean>	0	1/7	0 => Inactive, normal
<pre><pre><pre>oduct dependent&gt;</pre></pre></pre>				1 => Active, triggered
				(capability.ndi > 0)
do_i<0~(ndo-1)>	<boolean></boolean>	0	1/7	0 => Inactive, normal
<pre><pre><pre>oduct dependent&gt;</pre></pre></pre>				1 => Active, triggered
				(capability.ndo > 0)
daynight	day, night	<pre><pre><pre><pre></pre></pre></pre></pre>	7/7	Current status of day,
<pre><pre><pre><pre>oduct dependent&gt;</pre></pre></pre></pre>		dependent>		night.
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></string>	<pre><pre><pre><pre></pre></pre></pre></pre>	1/7	Get network information
		dependent>		from mii-tool.
vi_i<0~(nvi-1)>	<boolean></boolean>	0	1/7	Virtual input
<pre><pre><pre>oduct dependent&gt;</pre></pre></pre>				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	DESCRIPTION
			(get/set)	
normalstate	high,	high	1/1	Indicates open circuit or
	low			closed circuit (inactive
				status)

# 7.4 digital output behavior define

Group:  $do_i < 0 \sim (ndo-1) > (capability.ndo > 0)$ 

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

# 7.5 security

Group: security

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
privilege_do	view, operator,	operator	6/6	Indicate which privileges
<pre><pre><pre><pre>oduct dependent&gt;</pre></pre></pre></pre>	admin			and above can control
				digital output
				(capability.ndo > 0)
privilege_camctrl	view, operator,	view	6/6	Indicate which privileges
<pre><pre><pre>oduct dependent&gt;</pre></pre></pre>	admin			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></blank>	6/7	User name
user_i0_pass	password[64]	<blank></blank>	6/6	Root password
user_i<1~20>_pass	password[64]	<blank></blank>	7/6	User password
user_i0_privilege	viewer,	admin	6/7	Root privilege
	operator,			
	admin			
user_i<1~20>_ privilege	viewer,	<blank></blank>	6/6	User privilege
	operator,			
	admin			

## 7.6 network

Group: network

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
preproces	<positive< td=""><td><black></black></td><td>7/6</td><td>An 32-bit integer, each bit can be set separately</td></positive<>	<black></black>	7/6	An 32-bit integer, each bit can be set separately
s	integer>			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 <b>recommended</b> 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=55
				56& network_rtp_videoport=20480"
type	lan,	lan	6/6	Network connection type.
	pppoe			
	<pre><pre><pre><pre></pre></pre></pre></pre>			
	dependent>			
resetip	<boolean></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< td=""><td><pre><pre><pre><pre></pre></pre></pre></pre></td><td>6/6</td><td>IP address of server.</td></ip<>	<pre><pre><pre><pre></pre></pre></pre></pre>	6/6	IP address of server.
	address>	dependent>		
subnet	<ip< td=""><td><blank></blank></td><td>6/6</td><td>Subnet mask.</td></ip<>	<blank></blank>	6/6	Subnet mask.

	address>			
router	<ip< td=""><td><blank></blank></td><td>6/6</td><td>Default gateway.</td></ip<>	<blank></blank>	6/6	Default gateway.
	address>			
dns1	<ip< td=""><td><blank></blank></td><td>6/6</td><td>Primary DNS server.</td></ip<>	<blank></blank>	6/6	Primary DNS server.
	address>			
dns2	<ip< td=""><td><blank></blank></td><td>6/6</td><td>Secondary DNS server.</td></ip<>	<blank></blank>	6/6	Secondary DNS server.
	address>			
wins1	<ip< td=""><td><blank></blank></td><td>6/6</td><td>Primary WINS server.</td></ip<>	<blank></blank>	6/6	Primary WINS server.
	address>			
wins2	<ip< td=""><td><blank></blank></td><td>6/6</td><td>Secondary WINS server.</td></ip<>	<blank></blank>	6/6	Secondary WINS server.
	address>			

## 7.6.1 802.1x

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean></boolean>	0	6/6	Enable/disable IEEE 802.1x
eapmethod	eap-peap,	еар-реар	6/6	Selected EAP method
identity_peap	String[64]	<black></black>	6/6	PEAP identity
identity_tls	String[64]	<black></black>	6/6	TLS identity
password	String[254]	<black></black>	6/6	Password for TLS
privatekeypassword	String[254]	<black></black>	6/6	Password for PEAP
ca_exist	<boolean></boolean>	0	6/6	CA installed flag
ca_time	<integer></integer>	0	6/7	CA installed time.
				Represented in EPOCH
ca_size	<integer></integer>	0	6/7	CA file size (in bytes)
certificate_exist	<boolean></boolean>	0	6/6	Certificate installed flag (for
				TLS)
certificate_time	<integer></integer>	0	6/7	Certificate installed time.
				Represented in EPOCH
certificate_size	<integer></integer>	0	6/7	Certificate file size (in bytes)
privatekey_exist	<boolean></boolean>	0	6/6	Private key installed flag (for
				TLS)
privatekey_time	<integer></integer>	0	6/7	Private key installed time.
				Represented in EPOCH
privatekey_size	<integer></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	DESCRIPTION
			(get/set)	
enable	<boolean></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
<pre><pre><pre><pre></pre></pre></pre></pre>				(capability.naudio > 0)
dependent>				
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	DESCRIPTION
			(get/set)	
enable	<boolean></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	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	6/6	Enable IPv6.
addonipaddress	<ip address=""></ip>	<blank></blank>	6/6	IPv6 IP address.
addonprefixlen	0~128	64	6/6	IPv6 prefix length.
addonrouter	<ip address=""></ip>	<blank></blank>	6/6	IPv6 router address.
addondns	<ip address=""></ip>	<blank></blank>	6/6	IPv6 DNS address.
allowoptional	<boolean></boolean>	0	6/6	Allow manually setup of IP
				address setting.

## 7.6.4 FTP

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

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

## 7.6.5 HTTP

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

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
port	80, 1025 ~	80	1/6	HTTP port.
	65535			
alternateport	1025~65535	8080	6/6	Alternate HTTP port.
authmode	basic,	basic	1/6	HTTP authentication mode.
	digest			
s0_accessname	string[32]	video.mjpg	1/6	HTTP server push access name
				for stream 1.
				(capability.protocol.spush_mjpeg
				=1 and capability.nmediastream
				> 0)
s1_accessname	string[32]	video2.mjpg	1/6	HTTP server push access name
<pre><pre><pre><pre></pre></pre></pre></pre>				for stream 2.
dependent>				(capability.protocol.spush_mjpeg
				=1 and capability.nmediastream
				> 1)
s2_accessname	string[32]	video3.mjpg	1/6	Http server push access name for
<pre><pre><pre><pre></pre></pre></pre></pre>				stream 3
dependent>				(capability.protocol.spush_mjpeg
				=1 and capability.nmediastream
				> 2)
anonymousviewing	<boolean></boolean>	0	1/6	Enable anonymous streaming
				viewing.

## **7.6.6 HTTPS port**

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

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
port	443, 1025 ~	443	1/6	HTTPS port.
	65535			

## 7.6.7 RTSP

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~	554	1/6	RTSP port.
	65535			(capability.protocol.rtsp=1)
anonymousviewing	<boolean></boolean>	0	1/6	Enable anoymous
				streaming viewing.
authmode	disable,	disable	1/6	RTSP authentication mode.
	basic,			(capability.protocol.rtsp=1)
	digest			
s0_accessname	<boolean></boolean>	live.sdp	1/6	RTSP access name for
				stream1.
				(capability.protocol.rtsp=1
				and
				capability.nmediastream >
				0)
s1_accessname	<boolean></boolean>	live2.sdp	1/6	RTSP access name for
				stream2.
				(capability.protocol.rtsp=1
				and
				capability.nmediastream >
				1)
s2_accessname	<boolean></boolean>	live3.sdp	1/6	RTSP access name for
				stream3
				(capability.protocol.rtsp=1
				and
				capability.nmediastream >
				2)

s0_audiotrack	<boolean></boolean>	-1	1/6	Enable audio for stream1.
s1_audiotrack	<boolean></boolean>	-1	1/6	Enable audio for stream2.
s2_audiotrack	<boolean></boolean>	-1	1/6	Enable audio for stream3.

## 7.6.7.1 RTSP multicast

Subgroup of **network\_rtsp\_s<0~(n-1)>**: **multicast,** n is stream count (capability.protocol.rtp.multicast > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean></boolean>	0	4/4	Enable always multicast.
ipaddress	<ip address=""></ip>	For n=0, 239.128.1.99 For n=1, 239.128.1.100, and so on.	4/4	Multicast IP address.
videoport	1025 ~ 65535	5560+n*2	4/4	Multicast video port.
audioport <pre><pre><pre><pre>dependent&gt;</pre></pre></pre></pre>	1025 ~ 65535	5562+n*2	4/4	Multicast audio port. (capability.naudio > 0)
ttl	1 ~ 255	15	4/4	Mutlicast time to live value.

## **7.6.8 SIP port**

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

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
port	1025 ~ 65535	5060	1/6	SIP port.

## **7.6.9 RTP port**

Subgroup of **network**: **rtp** 

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
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	DESCRIPTION
			(get/set)	
user	string[128]	<black></black>	6/6	PPPoE account user name.
pass	password[64]	<blank></blank>	6/6	PPPoE account password.

## 7.7 IP Filter

Group: ipfilter

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	6/6	Enable access list
				filtering.
admin_enable	<boolean></boolean>	0	6/6	Enable administrator IP
				address.
admin_ip	String[44]	<black></black>	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:	<black></black>	6/6	IPv4 address list.
	<ip address=""></ip>			
	Network address:			
	<ip <="" address="" td=""><td></td><td></td><td></td></ip>			
	network mask>			
	Range			
	address: <start ip<="" td=""><td></td><td></td><td></td></start>			
	address - end ip			
	address>			
ipv6list_i<0~9>	String[44]	<blank></blank>	6/6	IPv6 address list.

# 7.8 Video input

Group: videoin

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
cmosfreq	50, 60	60	4/4	CMOS frequency.
				(capability.videoin.type=2)
whitebalance	auto, manual	auto	4/4	"auto" indicates auto white
				balance.
				"manual" indicates keep current
				value.
exposurelevel	0~12	6	4/4	Exposure level
autoiris	<boolean></boolean>	0	4/4	Enable auto Iris.
irismode	fixed, indoor,	indoor	4/4	Video Iris for DC Iris.
	outdoor			
enablewdr	<boolean></boolean>	0	4/4	Enable/disable wield dynamic
				range.
enableblc	<boolean></boolean>	0	4/4	Enable backlight compensation.
agc	0,1,2	1	4/4	Set auto gain control to normal
				level or MAX level.
				0->2x,
				1->4x,
				2->8x
color	0, 1	1	4/4	0 =>monochrome
55.5.	3, 2	-	,, .	1 => color
flip	<boolean></boolean>	0	4/4	Flip the image.
mirror	<boolean></boolean>	0	4/4	Mirror the image.
ptzstatus	<integer></integer>	2	1/7	A 32-bit integer, each bit can be
ptzotatas	vinteger 2		1,7	set separately as follows:
				Bit 0 => Support camera
				control function; 0(not
				support), 1(support)
				Bit 1 => <b>Built-in</b> or <b>external</b>
				camera; 0 (external),
				1(built-in)
				Bit 2 => Support <b>pan</b>

				operation; 0(not support), 1(support) Bit 3 => Support <b>tilt</b> operation; 0(not support), 1(support) Bit 4 => Support <b>zoom</b>
				operation; 0(not support), 1(support)
				Bit 5 => Support <b>focus</b>
				operation; 0(not support),
text	string[16]	<black></black>	1/4	1(support) Enclose caption.
- CAC	String[10]	Column	1/1	Enclose caption.
imprinttimestamp	<boolean></boolean>	0	4/4	Overlay time stamp on video.
maxexposure	1, 15, 30,	30	4/4	Maximum exposure time.
	60, 120, 240,			
	480			
	<pre><pre><pre><pre></pre></pre></pre></pre>			
	dependent>			
options	quality,	crop	4/4	Video input option:
	framerate, crop			(1) video quality first mode
				(2) video frame rate first mode
				(3) cropping mode
				(not used in FD8372)
enablepreview	<boolean></boolean>	0	1/4	Usage for UI of exposure
				settings. Preview settings of
				video profile.

## 7.8.1 Video input setting per channel

Group:  $videoin_c<0\sim(n-1)>$  for n channel products, and m is stream number

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
cmosfreq	50, 60	60	4/4	CMOS frequency.
				(capability.videoin.type=2)
whitebalance	auto, manual	auto	4/4	"auto" indicates auto white
				balance.
				"manual" indicates keep
				current value.
rgain	0~100	30	4/4	Manual set rgain value of

				gain control setting.
bgain	0~100	30	4/4	Manual set bgain value of
				gain control setting.
exposurelevel	0~12	6	4/4	Exposure level
autoiris	0~1	0	4/4	set 1 to enable auto iris, set
				0 to disable auto iris.
irismode	fixed, indoor,	indoor	4/4	Video Iris for DC Iris.
	outdoor			
enablewdr	<boolean></boolean>	0	4/4	Enable/disable wield
				dynamic range.
enableblc	0~1	0	4/4	Enable backlight
				compensation
agc	0,1,2	1	4/4	Set auto gain control to
				normal level or MAX level.
				0->2x,
				1->4x,
				2->8x
agcmode	auto,fixed	auto	4/4	Set auto gain control
				mode.
maxgain	0~100	100	4/4	Manual set maximum gain
				value.
mingain	0~100	0	4/4	Manual set minimum gain
				value.
color	0, 1	1	4/4	0 =>monochrome
				1 => color
flip	<boolean></boolean>	0	4/4	Flip the image.
mirror	<boolean></boolean>	0	4/4	Mirror the image.
text	string[16]	<blank></blank>	1/4	Enclose caption.
imprinttimestamp	<boolean></boolean>	0	4/4	Overlay time stamp on
				video.
exposuremode	auto,fixed	auto	4/4	Exposure mode
maxexposure	1~32000	32000	4/4	Maximum exposure time.
maxexposure	1~32000	30	4/4	Maximum exposure time.
enablepreview	<boolean></boolean>	0	1/4	Usage for UI of exposure
				settings. Preview settings
				of video profile.
crop_position	<coordinate></coordinate>	-1,-1	1/4	Crop left-top corner

	(x,y)			coordinate.
crop_size	<window size=""></window>	2560×1920	1/4	Crop width and height.  (width must be 16x or 32x and height must be 8x)
crop_preview	< boolean >	0	1/4	Usage for UI of crop setting
s<0~(m-1)>_codectype	mpeg4, mjpeg, h264 <product dependent&gt;</product 	H264	1/4	Video codec type.
s<0~(m-1)>_resolution	Reference capability_vide oin_resolution	2560×1920	1/4	Video resolution in pixels.
s<0~(m-1)>_mpeg4_intrap eriod	250, 500, 1000, 2000, 3000, 4000	1000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_mpeg4_rateco ntrolmode	cbr, vbr	cbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_quant	1~5, 99, 100	3	4/4	Quality of video when choosing vbr in "ratecontrolmode".  99 is the customized manual input setting.  1 = worst quality, 5 = best quality.  100 is percentage mode.
s<0~(m-1)>_mpeg4_qvalue	2~31	7	4/4	Manual video quality level input. (s<0~(m-1)>_mpeg4_qua nt = 99)
s<0~(m-1)>_mpeg4_qperce nt	1~100	29	4/4	Manual video quality level input. (s<0~(m-1)>_mpeg4_qua nt = 100)
s<0~(m-1)>_mpeg4_bitrate	1000~260000 00 <pre>product</pre>	6000000	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".

	dependent>			
s<0~(m-1)>_mpeg4_maxfr ame s<0~(m-1)>_h264_intraperi	1~50, 51~60 (only for NTSC or 60Hz CMOS)	1000	1/4	Set maximum frame rate in fps (for MPEG-4).  5M: 1~10fps  3M: 1~20fps  2M: 1~30fps  1080P: 1~25fps  720P: 1~60fps  (for NTSC or 60Hz CMOS)  Intra frame period in
od	1000, 2000, 3000, 4000	1000	7/7	milliseconds.
s<0~(m-1)>_h264_ratecont rolmode	cbr, vbr	cbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_h264_quant	1~5, 99, 100	3	4/4	Quality of video when choosing vbr in "ratecontrolmode".  99 is the customized manual input setting.  1 = worst quality, 5 = best quality.  100 is percentage mode.
s<0~(m-1)>_h264_qvalue	0~51	7	4/4	Manual video quality level input. (s<0~(m-1)>_h264_quan t = 99)
s<0~(m-1)>_h264_qpercen t	1~100	44	4/4	Manual video quality level input. (s<0~(m-1)>_h264_quan t = 100)
s<0~(m-1)>_h264_bitrate	1000~260000	6000000	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_h264_maxfra me	1~50, 51~60 (only for NTSC or 60Hz CMOS)	10	1/4	Set maximum frame rate in fps (for h264).  5M: 1~10fps  3M: 1~20fps  2M: 1~30fps  1080P: 1~30fps

				720P: 1~60fps
				(for NTSC or 60Hz CMOS)
s<0~(m-1)>_h264_profile	0~2	1	1/4	Indicate H264 profiles
<pre><pre><pre><pre>oduct dependent&gt;</pre></pre></pre></pre>				0: baseline
				1: main profile
				2: high profile
s<0~(m-1)>_mjpeg_quant	1~5,	3	4/4	Quality of JPEG video.
	99, 100			99 is the customized
				manual input setting.
				1 = worst quality, 5 = best
				quality.
				100 is percentage mode.
s<0~(m-1)>_mjpeg_qvalue	2~97	49	4/4	Manual video quality level
				input.
				(s<0~(m-1)>_mjpeg_qua
				nt = 99)
s<0~(m-1)>_mjpeg_qperce	1~100	49	4/4	Manual video quality level
nt				input.
				(s<0~(m-1)>_mjpeg_qua
				nt = 100)
s<0~(m-1)>_mjpeg_maxfra	1~50,	13	1/4	Set maximum frame rate in
me	51~60 (only			fps (for JPEG).
	for NTSC or			5M:1~13fps
	60Hz CMOS)			3M:1~20fps
				2M:1~30fps
				1080P: 1~30fps
				720P: 1~60fps
				(for NTSC or 60Hz CMOS)
wdrc_mode	0~3	1	4/4	WDR enhanced.
				0: off
				1: auto
				2: always on
				3: keep current value
wdrc_strength	0~2	1	4/4	WDR enhanced.
				0: low
				1: medium
				2: high

### 7.8.1.1 Alternative video input profiles per channel

In addition to the primary setting of video input, there can be alternative profile video input setting for each channel which might be for different scene of light (daytime or nighttime).

Group: videoin\_c0\_profile\_i<0~(m-1)> (capability. nvideoinprofile > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	4/4	Enable/disable this profile
				setting
policy	day,	night	4/4	The mode which the profile is
	night,			applied to.
	schedule			
begintime	hh:mm	18:00	4/4	Begin time of schedule mode.
endtime	hh:mm	06:00	4/4	End time of schedule mode.
exposuremode	auto,fixed	auto	4/4	Exposure Mode
minexposure	1~32000	32000	4/4	Minimum exposure time.
maxexposure	1~32000	30	4/4	Maximum exposure time.
enableblc	<boolean></boolean>	0	4/4	Enable backlight compensation.
exposurelevel	0~12	6	4/4	Exposure level
agc	0,1,2	2	4/4	Set auto gain control to normal
				level or MAX level.
				0->2x,
				1->4x,
				2->8x
agcmode	auto,fixed	auto	4/4	Set auto gain control mode.
maxgain	0~100	100	4/4	Manual set maximum gain
				value.
mingain	0~100	0	4/4	Manual set minimum gain
				value.
autoiris	<boolean></boolean>	0	4/4	Enable auto Iris.
enablewdr	<boolean></boolean>	0	4/4	Enable/disable wield dynamic
				range.
whitebalance	auto, manual	manual	4/4	"auto" indicates auto white
				balance.
				"manual" indicates keep current
				value.

rgain	0~100	52	4/4	Manual set rgain value of gain
				control setting.
bgain	0~100	30	4/4	Manual set bgain value of gain
				control setting.
irismode	fixed, indoor,	indoor	4/4	Video Iris for DC Iris.
	outdoor			
wdrc_mode	0~3	0	4/4	WDR enhanced.
				0: off
				1: auto
				2: always on
				3: keep current value
wdrc_strength	0~2	1	4/4	WDR enhanced.
				0: low
				1: medium
				2: high

# 7.9 Video input preview

The temporary settings for video preview

Group: videoinpreview

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
exposuremode	auto,fixed	auto	4/4	Exposure Mode
minexposure	1~32000	32000	4/4	Minimum exposure time.
maxexposure	1~32000	30	4/4	Maximum exposure time.
exposurelevel	0~12	6	4/4	Exposure level
enableblc	<boolean></boolean>	0	4/4	Enable backlight compensation.
enablewdr	<boolean></boolean>	0	4/4	Enable/disable wield dynamic
				range.
irismode	fixed, indoor,	indoor	4/4	Video Iris for DC Iris.
	outdoor			
wdrc_mode	0~3	1	4/4	WDR enhanced.
				0: off
				1: auto
				2: always on
				3: keep current value
wdrc_strength	0~2	0	4/4	WDR enhanced.
				0: low
				1: medium

				2: high
agc	0,1,2	1	4/4	Set auto gain control to normal
				level or MAX level.
				0->2x,
				1->4x,
				2->8x
agcmode	auto,fixed	auto	4/4	Set auto gain control mode.
maxgain	0~100	100	4/4	Manual set maximum gain
				value.
mingain	0~100	0	4/4	Manual set minimum gain
				value.
autoiris	<boolean></boolean>	0	4/4	Enable auto Iris.

### 7.10 IR cut control

Group: **ircutcontrol** (capability.nvideoinprofile > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
mode	auto,	auto	6/6	Set IR cut control mode
	day,			
	night,			
	di,			
	schedule			
	<pre><pre><pre><pre></pre></pre></pre></pre>			
	dependent>			
daymodebegintime	00:00~23:59	07:00	6/6	Day mode begin time
daymodeendtime	00:00~23:59	18:00	6/6	Day mod end time
bwmode	<boolean></boolean>	1	6/6	Switch to B/W in night mode if
				enabled
sensitivity	low,	normal	6/6	Sensitivity of light sensor
	normal,			
	high			

# 7.11 Image setting per channel

Group:  $image_c<0\sim(n-1)>$  for n channel products

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
brightness	-5~5	-5	4/4	Adjust brightness of image
				according to mode settings.
saturation	-5~5,100	0	4/4	Adjust saturation of image
				according to mode settings.
				100 for saturation
				percentage mode.
saturationpercent	0~100	50	4/4	Adjust saturation value of
				percentage when
				saturation=100
contrast	-5 ~ 5	0	4/4	Adjust contrast of image
				according to mode settings.
sharpness	-3~3,100	0	4/4	Adjust sharpness of image
				according to mode settings.
sharpnesspercent	0~100	50	4/4	Adjust sharpness value of
				percentage when
				sharpness=100
gammacurve	0~100	0	4/4	Gamma curve.
lowlightmode	<boolean></boolean>	1	4/4	Enable/disable low light
				mode.
profile_i0_enable	<boolean></boolean>	0	4/4	Enable/disable this profile
				setting
profile_i0_policy	day,	night	4/4	The mode which the profile is
	night,			applied to.
	schedule			
profile_i0_begintime	hh:mm	18:00	4/4	Begin time of schedule mode.
profile_i0_endtime	hh:mm	06:00	4/4	End time of schedule mode.
profile_i0_brightness	-5~5	-5	4/4	Adjust brightness of image
				according to mode settings.
profile_i0_contrast	-5 ~ 5	0	4/4	Adjust contrast of image
				according to mode settings.
profile_i0_sharpness	-3~3	0	4/4	Adjust sharpness of image
				according to mode settings.
profile_i0_sharpnesspercent	0~100	50	4/4	Adjust sharpness value of

				percentage when
				sharpness=100
profile_i0_gammacurve	0~100	0	4/4	Gamma curve
profile_i0_lowlightmode	<boolean></boolean>	1	4/4	Enable/disable low light
				mode.
profile_i0_wdrcstrength	0~2	1	4/4	WDR enhanced
				0: low
				1: medium
				2: high
profile_i0_wdrcmode	0~3	1	4/4	WDR enhanced
				0: off
				1: auto
				2: always on
				3:keep current value

# 7.12 Image setting for preview

Group:  $imagepreview_c<0\sim(n-1)>$  for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5~5	-5	4/4	Adjust brightness of image
				according to mode settings.
saturation	-5~5,100	0	4/4	Adjust saturation of image
				according to mode settings.
				100 for saturation
				percentage mode.
saturationpercent	0~100	50	4/4	Adjust saturation value of
				percentage when
				saturation=100
contrast	-5 ~ 5	0	4/4	Adjust contrast of image
				according to mode settings.
sharpness	-3~3,100	0	4/4	Adjust sharpness of image
				according to mode settings.
sharpnesspercent	0~100	50	4/4	Adjust sharpness value of
				percentage when
				sharpness=100
gammacurve	0~100	0	4/4	Gamma curve
lowlightmode	<boolean></boolean>	0	4/4	Enable/disable low light
				mode.

Group: imagepreview

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
videoin_whitebalance	auto,	auto	4/4	Preview of adjusting white balance of
	manual,			image according to mode settings
	rbgain			
videoin_restoreatwb	0, 1~	0	4/4	Restore of adjusting white balance of
				image according to mode settings
videoin_rgain	0~100	0	4/4	Manual set rgain value of gain control
				setting.
videoin_bgain	0~100	0	4/4	Manual set bgain value of gain control
				setting.

# 7.13 Exposure window setting per channel

Group: exposure\_c<0~(n-1)> for n channel products

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
mode	auto, custom,	auto	4/4	The mode indicates how to
	blc			decide the exposure.
				auto: Use full view as the only
				one exposure window.
				custom: Use inclusive and
				exclusive window.
				blc: Use BLC.
win_i<0~9>_enable	<boolean></boolean>	0	4/4	Enable or disable the window.
win_i<0~9>_policy	0~1	0	4/4	0: Indicate exclusive.
				1: Indicate inclusive.
win_i<0~9>_home	<coordinate></coordinate>	(150,110)	4/4	Left-top corner coordinate of
				the window.
win_i<0~9>_size	<window size=""></window>	(100x75)	4/4	Width and height of the
				window.

Group:  $exposure_c<0\sim(n-1)>_profile$  for m profile and n channel product

	•		•	
NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
i<0~(m-1)>_mode	auto, custom,	auto	4/4	The mode indicates how
	blc			to decide the exposure.

	1			
				auto: Use full view as
				the only one exposure
				window.
				custom: Use inclusive
				and exclusive window.
				blc: Use BLC.
i<0~(m-1)>_win_i<0~9>_enable	<boolean></boolean>	0	4/4	Enable or disable the
				window.
i<0~(m-1)>_win_i<0~9>_policy	0~1	0	4/4	0: Indicate exclusive.
				1: Indicate inclusive.
i<0~(m-1)>_win_i<0~9>_home	<coordinate></coordinate>	(150,110)	4/4	Left-top corner
				coordinate of the
				window.
i<0~(m-1)>_win_i<0~9>_size	<window size=""></window>	(100x75)	4/4	Width and height of the
				window.

# 7.14 Audio input per channel

Group:  $audioin_c<0\sim(n-1)>$  for n channel products (capability.audioin>0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
source	linein	linein	4/4	micin => use built-in
				microphone input.
				linein => use external
				microphone input.
mute	0, 1	1	4/4	Disable audio mute.
gain	9~108	69	4/4	Gain of input.
				(audioin_c<0~(n-1)>_source =
				linein)
boostmic	9~108	69	4/4	Enable microphone boost.
				0 => +0dB
				1 => +20dB
				2 => +40dB
				Or
				Gain of input.
				(audioin_c<0~(n-1)>_source
				= micin)
s<0~(m-1)>_codectype	aac4,	aac4	4/4	Set audio codec type for input.
	gamr, g711			

s<0~(m-1)>_aac4_bitrate	16000,	16000	4/4	Set AAC4 bitrate in bps.
<pre><pre><pre><pre>oduct dependent&gt;</pre></pre></pre></pre>	32000,			
	48000,			
	64000,			
	96000,			
	128000			
s<0~(m-1)>_gamr_bitrate	4750,	12200	4/4	Set AMR bitrate in bps.
<pre><pre><pre><pre>oduct dependent&gt;</pre></pre></pre></pre>	5150,			
	5900,			
	6700,			
	7400,			
	7950,			
	10200,			
	12200			
s<0~(m-1)>_g711_mode	pcmu,	pcmu	4/4	Set G.711 mode.
<pre><pre><pre><pre>oduct dependent&gt;</pre></pre></pre></pre>	pcma			

7.15

### 7.16 Motion detection settings

Group:  $motion_c<0\sim(n-1)>$  for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean></boolean>	0	4/4	Enable motion detection.
win_i<0~2>_enable	<boolean></boolean>	0	4/4	Enable motion window 1~3.
win_i<0~2>_name	string[14]	<blank></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.

Group:  $motion_c<0\sim(n-1)>profile$  for m profile and n channel product (capability.nmotionprofile > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
i<0~(m-1)>_enable	<boolean></boolean>	0	4/4	Enable profile 1
				~ (m-1).
i<0~(m-1)>_policy	day,	night	4/4	The mode which
	night,			the profile is
	schedule			applied to.
i<0~(m-1)>_begintime	hh:mm	18:00	4/4	Begin time of
				schedule mode.
i<0~(m-1)>_endtime	hh:mm	06:00	4/4	End time of
				schedule mode.
i<0~(m-1)>_win_i<0~2>_enable	<boolean></boolean>	0	4/4	Enable motion
				window.
i<0~(m-1)>_win_i<0~2>_name	string[14]	<blank></blank>	4/4	Name of motion
				window.
i<0~(m-1)>_win_i<0~2>_left	0 ~ 320	0	4/4	Left coordinate
				of window
				position.
i<0~(m-1)>_win_i<0~2>_top	0 ~ 240	0	4/4	Top coordinate
				of window
				position.
i<0~(m-1)>_win_i<0~2>_width	0 ~ 320	0	4/4	Width of motion
				detection
				window.
i<0~(m-1)>_win_i<0~2>_height	0 ~ 240	0	4/4	Height of
				motion
				detection
				window.
i<0~(m-1)>_win_i<0~2>_objsize	0 ~ 100	0	4/4	Percent of
				motion
				detection
				window.
i<0~(m-1)>_win_i<0~2>_sensitivity	0 ~ 100	0	4/4	Sensitivity of
				motion
				detection
				window.

### 7.17 Tampering detection settings

Group:  $tampering_c<0\sim(n-1)>$  for n channel product (capability.tampering > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	4/4	Enable or disable tamper detection.
threshold	0 ~ 255	32	4/4	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.

#### **7.18 DDNS**

Group: **ddns** (capability.ddns > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	6/6	Enable or disable the dynamic DNS.
provider	Safe100,	DyndnsDyn	6/6	Safe100 => safe100.net
	DyndnsDynamic,	amic		DyndnsDynamic => dyndns.org
	DyndnsCustom,			(dynamic)
	TZO,			DyndnsCustom => dyndns.org
	DHS,			(custom)
	DynInterfree,			TZO => tzo.com
	CustomSafe100,			DHS => dhs.org
	PeanutHull,			DynInterfree =>dyn-interfree.it
	IODATA,			CustomSafe100 =>
	DO_JP,			Custom server using safe100
	MYDNS_JP,			method
	customizeddyndns,			PeanutHull => PeanutHull
	DP21,			IODATA => iodata.jp
	NetHome,			DO JP => ddo.jp
	ADAMA_LAND,			MYDNS JP => mydns.jp
	AddressNet,			Customizeddyndns => Custom
	Luna_VC,			server using dyndns method
	Mars_VC,			DP21 => dp-21.net
	Planex_VC,			NetHome => NetHome Co.,Ltd
	Sun_VC,			ADAMA_LAND => non-functional
	Nexus_Control,			service provider

	DO_JP_FREE,			Address.net => non-functional
	EPolice,			service provider
	PCCW,			Luna_VC => cybergate ddns
	MegaChips,			Mars_VC => cybergate ddns
	DLink,			Planex_VC => cybergate ddns
	DLinkCN			Sun_VC => cybergate ddns
	Logitec,			Nexus_Control => nexus control
	GE_Security,			DO_JP_FREE => dp-21.net (free)
	HUAGAI,			Epolice => epolice.com.tw
	3322,			PCCW => pccw.com
	ALARM,			MegaChips => megachips.co.jp
	ChangeIP,			Dlink =>D-LINK
	NOIP			DlinkCN => D-LINK CN
	SWISSCOM			Logitec => logitec.co.jp
	CustomizedTZO			GE_Security =>GE Security
	<pre><pre><pre><pre></pre></pre></pre></pre>			HUAGAI => huagai.com
	dependent>			3322 => 3322.net
				ALARM => alarm.com
				ChangeIP => TOSHIBA
				NOIP => TOSHIBA
				SWISSCOM =>swiss.com
				CustomizedTZO => Customized
				server using TZO method
				<pre><pre><pre><pre></pre></pre></pre></pre>
<pre><pre><pre>ovider&gt;_ho</pre></pre></pre>	string[128]	<blank></blank>	6/6	Your DDNS hostname.
stname				
<pre><pre><pre><pre>ovider&gt;_us</pre></pre></pre></pre>	string[64]	<blank></blank>	6/6	Your user name or email to login to
ernameemail				the DDNS service provider
<pre><pre><pre>ovider&gt;_pa</pre></pre></pre>	string[64]	<blank></blank>	6/6	Your password or key to login to the
sswordkey				DDNS service provider.
<pre><pre><pre><pre>se</pre></pre></pre></pre>	string[128]	<blank></blank>	6/6	The server name for safe100.
rvername				(This field only exists if the provider
				is customsafe100)

### 7.19 Express link

Group: expresslink

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	6/6	Enable or disable express link.
state	onlycheck,	NULL	6/6	Camera will check the status of
	onlyoffline,			network environment and express link
	checkonline,			URL
	badnetwork			
url	string[64]	NULL	6/6	The url user define to link to camera

### 7.20 UPnP presentation

Group: upnppresentation

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	1	6/6	Enable or disable the UPnP
				presentation service.

## 7.21 UPnP port forwarding

Group: upnpportforwarding

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></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

# 7.22 System log

Group: syslog

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enableremotelog	<boolean></boolean>	0	6/6	Enable remote log.
serverip	<ip address=""></ip>	<black></black>	6/6	Log server IP address.
serverport	514,	514	6/6	Server port used for log.
	1025~65535			
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
setparamlevel	0~2	0	6/6	Show log of parameter
				setting.
				0: disable
				1: Show log of parameter
				setting set from external.
				2. Show log of parameter
				setting set from external and
				internal.

#### **7.23 SNMP**

Group: **snmp** (capability.snmp > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
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></blank>	6/6	Read/write authentication password
authpwro	string[8~128]	<blank></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></blank>	6/6	Read/write passwrd
encryptpwro	string[8~128]	<blank></blank>	6/6	Read only password
encrypttyperw	DES	DES	6/6	Read/write encryption type
encrypttypero	DES	DES	6/6	Read only encryption type
rwcommunity	string[31]	Private	6/6	Read/write community
rocommunity	string[31]	Public	6/6	Read only community
syslocation	0~128	<blank></blank>	6/6	System location
syscontact	0~128	<blank></blank>	6/6	System contact

# 7.24 Layout configuration

Group: layout (New version)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
logo_default	<boolean></boolean>	1	1/6	0 => Custom logo
				1 => Default logo
logo_link	string[40]	http://ww	1/6	Hyperlink of the logo
		w.vivotek.c		
		<u>om</u>		
logo_powerbyvvtk_hidden	<boolean></boolean>	0	1/6	0 => display the power by
				vivotek logo
				1 => hide the power by
				vivotek logo
custombutton_manualtrigger_s	<boolean></boolean>	1	1/6	Show or hide manual trigger
how				(VI) button in homepage
<pre><pre><pre><pre>oduct dependent&gt;</pre></pre></pre></pre>				0 -> Hidden
				1 -> Visible
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_controlbackgroun	string[7]	#565656	1/6	Background color of control
d				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

# 7.25 Privacy mask

Group:  $privacymask_c<0\sim(n-1)>$  for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean></boolean>	0	4/4	Enable privacy mask.
win_i<0~4>_enable	<boolean></boolean>	0	4/4	Enable privacy mask window.
win_i<0~4>_name	string[14]	<black></black>	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.

# 7.26 Capability

Group: capability

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
api_httpversion	<string></string>	0100a	0/7	The HTTP API version.
bootuptime	<positive< td=""><td>60</td><td>0/7</td><td>Server bootup time.</td></positive<>	60	0/7	Server bootup time.
	integer>			
nir	0,	0	0/7	Number of IR interfaces.
	<positive< td=""><td></td><td></td><td>(Recommand to use ir for</td></positive<>			(Recommand to use ir for
	integer>			built-in IR and extir for
				external IR)
npir	0,	0	0/7	Number of PIRs.
	<positive< td=""><td></td><td></td><td></td></positive<>			
	integer>			
ndi	0,	3	0/7	Number of digital inputs.
	<positive< td=""><td></td><td></td><td></td></positive<>			
	integer>			
nvi	0,	3	0/7	Number of virtual inputs
	<positive< td=""><td></td><td></td><td>(manual trigger)</td></positive<>			(manual trigger)
	integer>			
ndo	0,	1	0/7	Number of digital outputs.
	<positive< td=""><td></td><td></td><td></td></positive<>			
	integer>			
naudioin	0,	1	0/7	Number of audio inputs.
	<positive< td=""><td></td><td></td><td></td></positive<>			
	integer>			
naudioout	0,	1	0/7	Number of audio outputs.
	<positive< td=""><td></td><td></td><td></td></positive<>			
	integer>			
nvideoin	<positive< td=""><td>1</td><td>0/7</td><td>Number of video inputs.</td></positive<>	1	0/7	Number of video inputs.
	integer>			
nmediastream	<positive< td=""><td>3</td><td>0/7</td><td>Number of media stream</td></positive<>	3	0/7	Number of media stream
	integer>			per channels.
nvideosetting	<positive< td=""><td>3</td><td>0/7</td><td>Number of video settings</td></positive<>	3	0/7	Number of video settings
	integer>			per channel.
naudiosetting	<positive< td=""><td>1</td><td>0/7</td><td>Number of audio settings</td></positive<>	1	0/7	Number of audio settings
	integer>			per channel.

nuart	0,	0	0/7	Number of UART
	<positive< td=""><td></td><td></td><td>interfaces.</td></positive<>			interfaces.
	integer>			
nvideoinprofile	<positive< td=""><td>1</td><td>0/7</td><td>Number of video input</td></positive<>	1	0/7	Number of video input
	integer>			profiles.
nmotionprofile	0, <positive< td=""><td>1</td><td>0/7</td><td>Number of motion profiles.</td></positive<>	1	0/7	Number of motion profiles.
·	integer>			·
ptzenabled	0, <positive< td=""><td>189</td><td>0/7</td><td>An 32-bit integer, each bit</td></positive<>	189	0/7	An 32-bit integer, each bit
	integer>			can be set separately as
				follows:
				Bit 0 => Support camera
				control function;
				O(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; O(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;
				O(not support),
				1(support)
				Bit 7 => External or
				built-in PT; 0(built-in),
				1(external)
				Bit 8 => Invalidate bit 1 ~
				7;

				0(bit $1 \sim 7$ are valid),
				1(bit 1 ~ 7 are invalid)
				Bit 9 => Reserved bit;
				Invalidate lens_pan,
				Lens_tilt, lens_zoon,
				lens_focus, len_iris.
				O(fields are valid),
				1(fields are invalid)
evctrlchannel	<boolean></boolean>	1	0/7	Indicate whether to
				support HTTP tunnel for
				event/control transfer.
joystick	<boolean></boolean>	1	0/7	Indicate whether to
				support joystick control.
storage_dbenabled	<boolean></boolean>	1	0/7	Media files are indexed in
				database.
ptzenabledclient	<boolean></boolean>	0	0/7	Indicate whether to
				support ptz client
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></boolean>	1	0/7	Indicate whether to
				support SIP.
protocol_maxconnection	<positive< td=""><td>10</td><td>0/7</td><td>The maximum allowed</td></positive<>	10	0/7	The maximum allowed
. –	integer>			simultaneous connections.
protocol_maxgenconnection	<positive< td=""><td>10</td><td>0/7</td><td>The maximum general</td></positive<>	10	0/7	The maximum general
, <b>5</b>	integer>		',	streaming connections .
protocol_maxmegaconnection	<positive< p=""></positive<>	0	0/7	The maximum megapixel
F	integer>			streaming connections.
protocol_rtp_multicast_	<boolean></boolean>	1	0/7	Indicate whether to
scalable				support scalable
Scalabic				multicast.
protocol_rtp_multicast_	<boolean></boolean>	0	0/7	Indicate whether to
backchannel	1200104117			support backchannel
				multicast.
protocol_rtp_tcp	<boolean></boolean>	1	0/7	Indicate whether to
p. 0.0000i_i.cp_tcp	- Dooreans	_		support RTP over TCP.
protocol_rtp_http	<boolean></boolean>	1	0/7	Indicate whether to
protocoi_rtp_nttp	\DOUIE all>	1	0, 7	support RTP over HTTP.
				Support KIF Over IIIIF.

			1	
protocol_spush_mjpeg	<boolean></boolean>	1	0/7	Indicate whether to
				support server push
				MJPEG.
protocol_snmp	<boolean></boolean>	1	0/7	Indicate whether to
				support SNMP.
protocol_ipv6	<boolean></boolean>	1	0/7	Indicate whether to
				support IPv6.
videoin_type	0, 1, 2	2	0/7	0 => Interlaced CCD
				1 => Progressive CCD
				2 => CMOS
videoin_resolution	<a list="" of<="" td=""><td>176x144,</td><td>0/7</td><td>Available resolutions list.</td></a>	176x144,	0/7	Available resolutions list.
	available	320x240,		
	resolution	384x216,		
	separated by	640x360,		
	commas>	640x480,		
	<pre><pre><pre><pre></pre></pre></pre></pre>	800x600,		
	dependent>	1280x720,		
		1360x768,		
		1600x904,		
		1600×1200,		
		1920×1080,		
		2048x1536,		
		2560x1920		
videoin_resolution16x9	<a list="" of<="" td=""><td>176x144,</td><td>0/7</td><td>Available resolutions list.</td></a>	176x144,	0/7	Available resolutions list.
	available	384x216,		
	resolution	640x360,		
	separated by	1280x720,		
	commas>	1360x768,		
	<pre><pre><pre><pre></pre></pre></pre></pre>	1600x904,		
	dependent>	1920x1080,		
videoin_resolution4x3	<a list="" of<="" td=""><td>176x144,</td><td>0/7</td><td>Available resolutions list.</td></a>	176x144,	0/7	Available resolutions list.
	available	320x240,		
	resolution	640x480,		
	separated by	800x600,		
	commas>	1600x1200,		
	<pre><pre><pre><pre></pre></pre></pre></pre>	2048x1536,		
	dependent>	2560x1920		
videoin_maxframerate	<a list="" of<="" td=""><td>30,</td><td>0/7</td><td>Available maximum frame</td></a>	30,	0/7	Available maximum frame
	available	30,		list.
•	•	•	•	

	maximum frame	30,		
	rate separated by	30,		
	commas>	30,		
	<pre><pre><pre><pre></pre></pre></pre></pre>	30		
	dependent>	30		
maxcodecfps	<a list="" of<="" td=""><td>(60,60,60),</td><td>0/7</td><td>Available maximum codec</td></a>	(60,60,60),	0/7	Available maximum codec
	available	(60,60,60),		frame list.
	maximum codec	(60,60,60),		For example:
	frame rate	(60,60,60),		(10,13,10) means
	separated by	(60,60,60),		In 2560x1920,
	commas>	(60,60,60),		Mpeg4 maximum fps is
	<pre><pre><pre><pre></pre></pre></pre></pre>	(60,60,60),		10,
	dependent>	(30,30,30),		Jpeg maximum fps is 13,
		(30,30,30),		H.264 maximum fps is 10.
		(30,30,30),		
		(25,30,30),		
		(20,20,20),		
		(10,13,10)		
videoin_codec	mpeg4. mjpeg,	mpeg4,	0/7	Available codec list.
	h264	mjpeg,		
	<pre><pre><pre><pre></pre></pre></pre></pre>	h264		
	dependent>			
videoout_codec	<a list="" of="" td="" the<=""><td><blank></blank></td><td>0/7</td><td>Available codec list.</td></a>	<blank></blank>	0/7	Available codec list.
	available codec			
	types separated			
	by commas)			
	<pre><pre><pre><pre></pre></pre></pre></pre>			
	dependent>			
audio_aec	<boolean></boolean>	0	0/7	Indicate whether to
				support acoustic echo
				cancellation.
audio_extmic	<boolean></boolean>	1	0/7	Indicate whether to
				support external
				microphone input.
audio_linein	<boolean></boolean>	1	0/7	Indicate whether to
				support external line
				input.
				(It will be replaced by
				audio_mic and

	1			
audio_lineout	<boolean></boolean>	1	0/7	Indicate whether to
				support line output.
audio_headphoneout	<boolean></boolean>	0	0/7	Indicate whether to
				support headphone
				output.
audioin_codec	aac4, gamr, g711	aac4, gamr,	0/7	Available codec list for
	<pre><pre><pre><pre></pre></pre></pre></pre>	g711		audio input.
	dependent>			
audioout_codec	g711	g711	0/7	Available codec list for SIP.
	<pre><pre><pre><pre></pre></pre></pre></pre>			
	dependent>			
camctrl_httptunnel	<boolean></boolean>	0	0/7	Indicate whether to
				support httptunnel.
camctrl_httptunnelclient	<boolean></boolean>	0	0/7	Indicate whether to
				support httptunnel client.
camctrl_privilege	<boolean></boolean>	1	0/7	Indicate whether to
				support "Manage
				Privilege" of PTZ control in
				the Security page.
				1: support both
				/cgi-bin/camctrl/camctrl.c
				gi and
				/cgi-bin/viewer/camctrl.c
				gi
				0: support only
				/cgi-bin/viewer/camctrl.c
				gi
uart_httptunnel	<boolean></boolean>	0	0/7	Indicate whether to
				support HTTP tunnel for
				UART transfer.
transmission_mode	Tx,	Тх	0/7	Indicate transmission
	Rx,			mode of the machine: TX
	Both			= server, Rx = receiver
				box, Both = DVR.
network_wire	<boolean></boolean>	1	0/7	Indicate whether to
				support Ethernet.
notwork wireless	<boolean></boolean>	0	0/7	Indicate whether to
network_wireless		1	i	i .
Hetwork_wireless				support wireless.

				support wireless
				802.11b+.
wireless_s802dot11g	<boolean></boolean>	0	0/7	Indicate whether to
				support wireless 802.11g.
wireless_encrypt_wep	<boolean></boolean>	0	0/7	Indicate whether to
				support wireless WEP.
wireless_encrypt_wpa	<boolean></boolean>	0	0/7	Indicate whether to
				support wireless WPA.
wireless_encrypt_wpa2	<boolean></boolean>	0	0/7	Indicate whether to
				support wireless WPA2.
derivative_brand	<boolean></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)
npreset	0, <positive< td=""><td>20</td><td>0/7</td><td>Number of preset</td></positive<>	20	0/7	Number of preset
	integer>			locations
eptz	0, <positive< td=""><td>3</td><td>0/7</td><td>A 32-bit integer, each bit</td></positive<>	3	0/7	A 32-bit integer, each bit
	integer>			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
nanystream	0, <positive< td=""><td>0</td><td>0/7</td><td>number of any media</td></positive<>	0	0/7	number of any media
	integer>			stream per channel
iva	<boolean></boolean>	0	0/7	Indicate whether to
				support Intelligent Video
				analysis
tampering	<boolean></boolean>	1	0/7	Indicate whether to
				support tampering
				detection.
test_ac	<boolean></boolean>	1	0/7	Indicate whether to
				support test ac key.
				support test de key.

version_onvifdaemon	<string></string>	1.5.0.0	0/7	Indicate ONVIF daemon
				version
image_wdrc	<boolean></boolean>	0	0/7	Indicate whether to
				support WDR enhanced.
image_ iristype	<string></string>	dciris	0/7	Indicate iris type.
image_ focusassist	<boolean></boolean>	0	0/7	Indicate whether to
				support focus assist.

## 7.27 Customized event script

Group: event\_customtaskfile\_i<0~2>

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
name	string[41]	<blank></blank>		Custom script identification of this entry.
date	string[17]	<black></black>	6/7	Date of custom script.
time	string[17]	<black></black>	6/7	Time of custom script.

### 7.28 Event setting

Group: **event\_i**<0~2>

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
name	string[40]	<black></black>	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.

ndicate the trigger condition:
boot" = System boot
di"= Digital input
motion" = Video motion detection
seq" = Periodic condition
visignal" = Video input signal loss.
recnotify" = Recording notification.
tampering" = Tamper detection.
"vi"= Virtual input (Manual trigger)
The status for event trigger
The status for event DI 1 trigger
The status for event by I thingger
The status for event DI 2 trigger
The status for event D1 2 trigger
The state of the second DI 2 to the second
he status for event DI 3 trigger
ndicate the source id of di trigger.
his field is required when trigger
condition is "di".
One bit represents one digital input.
he LSB indicates DI 0.
ndicate the source window id of
notion detection.
his field is required when trigger
condition is "md".
One bit represents one window.
The LSB indicates the 1 <sup>st</sup> window.
For example, to detect the 1st and
<sup>3rd</sup> windows, set mdwin as 5.
Similar to mdwin. The parameter
akes effect when profile 1 of motion
letection is enabled.

	1	1	T	T
vi	<integer></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.
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)
lowlightcondition <product dependent=""></product>	0, 1	1	6/6	Switch on white light LED in low light condition  0 => Do action at all times  1 => Do action in low-light conditions
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_goto_enable <product dependent=""></product>	<boolean></boolean>	0	6/6	Enable/disable ptz goto preset position on event triggered.
action_goto_name <pre><pre><pre>continue</pre></pre></pre>	string[40]	<blank></blank>	6/6	Specify the preset name that ptz goto on event triggered.

action_cf_enable	<boolean></boolean>	0	6/6	Enable or disable sending media to SD card.
action_cf_folder	string[128]	<black></black>	6/6	Path to store media.
action_cf_media	NULL, 0~4	<black></black>	6/6	Index of the attached media.
action_cf_datefolder	<boolean></boolean>	0	6/6	Enable this to create folders by date,
				time, and hour automatically.
action_cf_backup	<boolean></boolean>	0	6/6	Enable or disable the function that
				send media to SD card for backup if
				network is disconnected.
action_server_i<0~4>_e	0, 1	0	6/6	Enable or disable this server action.
nable				
action_server_i<0~4>_	NULL, 0~4	<black></black>	6/6	Index of the attached media.
media				
action_server_i<0~4>_	<boolean></boolean>	0	6/6	Enable this to create folders by date,
datefolder				time, and hour automatically.
action_patrol_enable	<boolean></boolean>	0	6/6	Enable/disable ptz patrol when
(only for VS series)				event triggered.
<pre><pre><pre>oduct dependent&gt;</pre></pre></pre>				
action_ patrol _server	0~255	0	6/6	Indicate the target servers to which
(only for VS series)				the snapshots taken during patrol
<pre><pre><pre>oduct dependent&gt;</pre></pre></pre>				dwelling time should be sent.
				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.
action_autofocus_enable	<boolean></boolean>	0	6/6	Enable/disable auto focus when
(only for FD series with				event triggered.
remote focus function)				

# 7.29 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,	email	6/6	Indicate the server type:
	ftp,			"email" = email server
	http,			"ftp" = FTP server
	ns			"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.
----------------------------------	--------------------------------

# 7.30 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,	snapshot	6/6	Media type to send to the server or
	systemlog,			store on the server.
	videoclip,			
	recordmsg			
snapshot_source	<integer></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]	Snapshot1_	6/6	Indicate the prefix of the filename.
				media_i0=> Snapshot1_
				media_i1=> Snapshot2_
				media_i2=> Snapshot3_
				media_i3=> Snapshot4_
				media_i4=> Snapshot5_
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.
videoclip_source	<integer></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]	VideoClip1_	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 ~ 6144	1000	6/6	Maximum size of one video clip file
				in Kbytes.

# 7.31 Recording

Group: **recording\_i**<0~1>

PARAMETER	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
name	string[40]	NULL	6/6	Identification of this entry.
trigger	schedule,	schedule	6/6	The event trigger type
	networkfail			schedule: The event is triggered by
				schedule
				networkfail: The event is triggered
				by the failure of network
				connection.
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.
source	0~2	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></blank>	6/6	Indicate the prefix of the filename.
cyclesize	200~	100	6/6	The maximum size for cycle recording in Kbytes when choosing to limit recording size.
reserveamount	0~	100	6/6	The reserved amount in Mbytes when choosing cyclic recording mechanism.

dest	cf,	cf	6/6	The destination to store the
	0~4			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.
maxsize	100~900	100	6/6	Unit: Mega bytes.
<pre><pre><pre>oduct dependent&gt;</pre></pre></pre>	<pre><pre><pre>oduct</pre></pre></pre>	<pre><pre><pre>oduct</pre></pre></pre>		When this condition is reached,
	dependent>	dependent>		recording file is truncated.
maxduration	60~1800	60	6/6	Uuit: Second
<pre><pre><pre>oduct dependent&gt;</pre></pre></pre>	<pre><pre><pre>oduct</pre></pre></pre>	<pre><pre><pre>oduct</pre></pre></pre>		When this condition is reached,
	dependent>	dependent>		recording file is truncated.
adaptive_enable	0,1	0	6/6	Indicate whether the adaptive
<pre><pre><pre>oduct dependent&gt;</pre></pre></pre>				recording is enabled
adaptive_preevent	0~9	1	6/6	Indicate when is the adaptive
<pre><pre><pre>oduct dependent&gt;</pre></pre></pre>				recording started before the event
				trigger point (seconds)
adaptive_postevent	0~10	1	6/6	Indicate when is the adaptive
<pre><pre><pre><pre>oduct dependent&gt;</pre></pre></pre></pre>				recording stopped after the event
				trigger point (seconds)

### **7.32 HTTPS**

Group: **https** (capability.protocol.https > 0)

creap: meps (capasine	, ,	,		
NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	6/6	To enable or disable secure
				НТТР.
policy	<boolean></boolean>	0	6/6	If the value is 1, it will force
				HTTP connection redirect to
				HTTPS connection
method	auto,	auto	6/6	auto => Create self-signed
	manual,			certificate automatically.
	install			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.	6/6	Common name in the
		com		certificate information.
validdays	0 ~ 3650	3650	6/6	Valid period for the
				certification.

### 7.33 Storage management setting

Currently it's for local storage (SD, CF card)

Group:  $disk_i < 0 \sim (n-1) > n$  is the total number of storage devices. (capability.storage.dbenabled > 0)

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
cyclic_enabled	<boolean></boolean>	0	6/6	Enable cyclic storage method.
autocleanup_enabled	<boolean></boolean>	0	6/6	Enable automatic clean up method.
				Expired and not locked media files will
				be deleted.
autocleanup_maxage	<positive< td=""><td>7</td><td>6/6</td><td>To specify the expired days for</td></positive<>	7	6/6	To specify the expired days for
	integer>			automatic clean up.

### 7.34 Region of interest

Group:  $roi_c<0\sim(n-1)>$  for n channel product, and m is the number of streams which support ROI. (capability.eptz > 0)

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
s<0~(m-1)>_home	<coordinate></coordinate>	<pre><pre><pre>oduct</pre></pre></pre>	6/6	ROI left-top corner coordinate.
		dependent>		
s<0~(m-1)>_size	<window size=""></window>	<pre><pre><pre>oduct</pre></pre></pre>	6/6	ROI width and height. The width
		dependent>		value must be multiples of 16 and the
				height value must be multiples of 8

### 7.35 ePTZ setting

Group:  $eptz_c<0\sim(n-1)>$  for n channel product. (capability.eptz > 0)

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
osdzoom	<boolean></boolean>	1	1/4	Indicates multiple of zoom in is
				"on-screen display" or not
smooth	<boolean></boolean>	1	1/4	Enable the ePTZ "move smoothly"
				feature
tiltspeed	-5 ~ 5	0	1/7	Tilt speed
				(It should be set by eCamCtrl.cgi
				rather than by setparam.cgi.)
panspeed	-5 ~ 5	0	1/7	Pan speed
				(It should be set by eCamCtrl.cgi
				rather than by setparam.cgi.)
zoomspeed	-5 ~ 5	0	1/7	Zoom speed
				(It should be set by eCamCtrl.cgi
				rather than by setparam.cgi.)
autospeed	1 ~ 5	1	1/7	Auto pan/patrol speed
				(It should be set by eCamCtrl.cgi
				rather than by setparam.cgi.)

Group:  $eptz_c<0\sim(n-1)>_s<0\sim(m-1)>$  for n channel product and m is the number of streams which support ePTZ. (capability.eptz > 0)

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
patrolseq	string[120]	<black></black>	1/4	The patrol sequence of ePTZ. All the
				patrol position indexes will be
				separated by ","
patroldwelling	string[160]	<black></black>	1/4	The dwelling time (unit: second) of
				each patrol point, separated by ",".
preset_i<0~19>_name	string[40]	<black></black>	1/7	Name of ePTZ preset.
				(It should be set by ePreset.cgi
				rather than by setparam.cgi.)
preset_i<0~19>_pos	<coordinate></coordinate>	<black></black>	1/7	Left-top corner coordinate of the
				preset.
				(It should be set by ePreset.cgi
				rather than by setparam.cgi.)
preset_i<0~19>_size	<window size=""></window>	<blank></blank>	1/7	Width and height of the preset.
				(It should be set by ePreset.cgi
				rather than by setparam.cgi.)

# 7.36 Focus Window setting

Group:  $focuswindow_c<0\sim(n-1)>$  for n channel product.

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
win_i0_enable	<boolean></boolean>	0	4/4	Enable or disable the window.
win_i0_home	<coordinate></coordinate>	(300,180)	-	Left-top corner coordinate of the window.
win_i0_size	<window size=""></window>	(1280x720)	4/4	Width and height of the window.

# 7.37 Exposure window setting per channel

Group: exposurewin\_c<0~(n-1)> for n channel products product dependent>

(capability\_videoin\_supportexpwin = 1)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
mode	auto, custom, blc	auto	4/4	The mode indicates how to decide the exposure. auto: Use full view as the only one exposure window.

				custom: Use inclusive and
				exclusive window.
				blc: Use BLC.
win_i<0~9>_enable	<boolean></boolean>	0	4/4	Enable or disable the window.
win_i<0~9>_policy	0~1	0	4/4	0: Indicate exclusive.
				1: Indicate inclusive.
win is 0 . 0 > home	(150 110)	4/4	Left-top corner coordinate of	
win_i<0~9>_home	<coordinate></coordinate>	(150,110) 4/4	the window.	
in i 40 0> aima	autodou sies	(100,75)	4/4	Width and height of the
wiii_i <u~y>_Size</u~y>	win_i<0 $\sim$ 9>_size   <window size="">   (100x75)  </window>		4/4	window.

Group:  $exposurewin_c<0\sim(n-1)>profile$  for m profile and n channel product

(capability\_videoin\_supportexpwin = 1)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
				The mode indicates how
				to decide the exposure.
				auto: Use full view as
i<0~(m-1)>_mode	auto, custom,	auto	4/4	the only one exposure
	blc	auto	4/4	window.
				custom: Use inclusive
				and exclusive window.
				blc: Use BLC.
i<0~(m-1)>_win_i<0~9>_enable	<boolean></boolean>	0	4/4	Enable or disable the
1 to the second	\boolean>	Ü	-1/ -1	window.
i<0~(m-1)>_win_i<0~9>_policy	0~1	0	4/4	0: Indicate exclusive.
1<0.0 (m-1)>_wm_1<0.0 3>_poncy	0.01	U		1: Indicate inclusive.
				Left-top corner
i<0~(m-1)>_win_i<0~9>_home	<coordinate></coordinate>	(150,110)	4/4	coordinate of the
				window.
i<0~(m-1)>_win_i<0~9>_size	<window size=""></window>	(100x75)	4/4	Width and height of the
1/01/2 (111-1)/ WIII 1/01/2/ 2/2/2/2	William Size>	(100X/3)	4/4	window.

### 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></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

 $[do0=<state>]\r\n$ 

 $\lceil do1 = \langle state \rangle \rceil \ r \ n$ 

[do2=<state>]\r\n

 $\lceil do3 = \langle state \rangle \rceil \backslash r \backslash n$ 

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 3D Privacy Mask

Note: This request requires admin user privilege

<SD81X1> You can set privacy mask only at zoom 1x. To go back to zoom 1x directly, please send this cgi command: "/cgi-bin/camctrl/camposition.cgi?setzoom=0"

Method: GET/POST

### Syntax:

http://<servername>/cgi-bin/admin/setpm3d.cgi?method=<value>&name=<value>&[maskheight=<value>&maskwidth=<value>&return page>]

PARAMETER	VALUE	DESCRIPTION
method	add	Add a 3D privacy mask at current location
	delete	Delete a 3D privacy mask
	edit	Edit a 3D privacy mask
maskname	string[40]	3D privacy mask name
maskheight	integer	3D privacy mask height
maskwidth	integer	3D privacy mask width
return	<return page=""></return>	Redirect to page < return page > after the 3D privacy mask is
		configured. The <return page=""> can be a full URL path or</return>
		relative path according to the current path. If you omit this
		parameter, it will redirect to an empty page.

## 8.5 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< td=""><td>0</td><td>The resolution of the image.</td></available<>	0	The resolution of the image.

	resolution>		
quality	1~5	3	The quality of the image.
streamid	0~(m-1)	<pre><pre><pre><pre></pre></pre></pre></pre>	The stream number.
		dependent>	

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]

<br/>
<br/>
dinary JPEG image data>

# 8.6 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></name>	The name of the user to add, delete, or edit.
userpass	<value></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></value>	The privilege of the user to add or to modify.
	viewer	Viewer privilege.

	operator	Operator privilege.
	admin	Administrator privilege.
Return	<return page=""></return>	Redirect to the page < return page > after the parameter is
		assigned. The < <i>return page</i> > 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.

## 8.7 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

## 8.8 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.

# 8.10 ePTZ Camera Control (capability.eptz > 0)

Note: This request requires camctrl privileges.

Method: GET/POST

#### Syntax:

http://<servername>/cgi-bin/camctrl/eCamCtrl.cgi?channel=<value>&stream=<value>

[&move=<value>] - Move home, up, down, left, right

videosize=640x480&resolution=640x480&stretch=0

[&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>] ] - Set

speeds

[&return=<return page>]

#### Example:

 $\label{lem:http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=0&move=right \\ http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&vx=2&vy=2&vz=2\\ http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&x=100&y=100& \\ \end{array}$ 

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
stream	<0~(m-1)>	Stream.
move	home	Move to home ROI.
	up	Move up.
	down	Move down.
	left	Move left.
	right	Move right.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop auto pan/patrol.
zoom	wide	Zoom larger view with current speed.

	tele	Zoom further with current speed.
zooming	wide or tele	Zoom without stopping for larger view or further view with zs speed, used for joystick control.
zs	0 ~ 6	Set the speed of zooming, "0" means stop.
vx	<integer></integer>	The direction of movement, used for joystick control.
vy	<integer></integer>	
vs	0 ~ 7	Set the speed of movement, "0" means stop.
х	<integer></integer>	x-coordinate clicked by user.
		It will be the x-coordinate of center after movement.
У	<integer></integer>	y-coordinate clicked by user.
		It will be the y-coordinate of center after movement.
videosize	<window size=""></window>	The size of plug-in (ActiveX) window in web page
resolution	<window size=""></window>	The resolution of streaming.
stretch	<boolean></boolean>	0 indicates that it uses <b>resolution</b> (streaming size) as the range of the coordinate system.
		1 indicates that it uses <b>videosize</b> (plug-in size) as the range of
		the coordinate system.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.
speedapp	1 ~ 5	Set the auto pan/patrol speed.
return	<return page=""></return>	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.

# 8.12 ePTZ Recall (capability.eptz > 0)

Note: This request requires camctrl privileges.

Method: GET/POST

### Syntax:

http://<servername>/cgi-bin/camctrl/eRecall.cgi?channel=<value>&stream=<value>&recall=<value>[&return = < return page>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.
recall	Text string less than 40	One of the present positions to recall.
	characters	
return	<return page=""></return>	Redirect to the page < return page > after the parameter is
		assigned. The < <i>return page</i> > can be a full URL path or relative
		path according to the current path.

# 8.14 ePTZ Preset Locations (capability.eptz > 0)

Note: This request requires Operator privileges.

Method: GET/POST

#### Syntax:

http://<*servername*>/cgi-bin/operator/ePreset.cgi?channel=<value>&stream=<value> [&addpos=<value>][&delpos=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.
addpos	<text less="" string="" td="" than<=""><td>Add one preset location to the preset list.</td></text>	Add one preset location to the preset list.
	40 characters>	
delpos	<text less="" string="" td="" than<=""><td>Delete preset location from the preset list.</td></text>	Delete preset location from the preset list.
	40 characters>	
return	<return page=""></return>	Redirect to the page < return page > after the parameter is
		assigned. The <i><return page=""></return></i> can be a full URL path or relative
		path according to the current path.

# 8.15 IP Filtering

Note: This request requires Administrator access privileges.

Method: GET/POST

Syntax: cproduct 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=""></ip>	Single address: <ip address=""></ip>
		Network address: <ip address="" mask="" network=""></ip>
		Range address: <start -="" address="" end="" ip=""></start>
index	<value></value>	The start position to add or to delete.
return	<return page=""></return>	Redirect to the page < return page > after the parameter is
		assigned. The <return page=""> can be a full URL path or relative</return>
		path according to the current path. If you omit this parameter, it
		will redirect to an empty page.

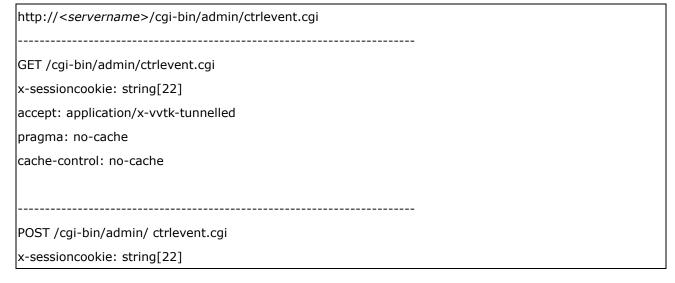
# 8.17 Event/Control HTTP Tunnel Channel (capability.

# evctrlchannel > 0)

Note: This request requires Administrator privileges.

Method: GET and POST

#### Syntax:



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

## 8.18 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\_ $<0\sim(m-1)>$ " 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.

# 8.19 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.

# 8.21 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></string>	Required.
		Command to be executed, including search, insert, delete,
		update, and queryStatus.

#### Command: search

PARAMETER	VALUE	DESCRIPTION
label	<integer key="" primary=""></integer>	Optional.
		The integer primary key column will automatically be assigned
		a unique integer.
triggerType	<text></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></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></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></text>	Optional.
		Indicate the media file resolution.

		Please embrace your input value with single quotes.
		Ex. resolution='800x600'
isLocked	<boolean></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></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 $1^{\text{st}}$ 2008
		to the end of Jan $1^{st}$ 2008.
limit	<positive integer=""></positive>	Optional.
		Limit the maximum number of returned search records.
offset	<positive integer=""></positive>	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'&trigge rTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59'

#### Command: delete

PARAMETER	VALUE	DESCRIPTION
label	<integer key="" primary=""></integer>	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 key="" primary=""></integer>	Required.
		Identify the designated record.
		Ex. label=1
isLocked	<boolean></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

# 8.22 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></num>	state[(duration)nstate]	Ex: vi0=1
		Setting virtual input 0 to trigger state
	Where "state" is 0, 1. "0"	

	means inactive or normal	Ex: vi0=0(200)1
	state while "1" means	Setting virtual input 0 to normal state, waiting 200
	active or triggered state.	milliseconds, setting it to trigger state.
	Where "nstate" is next	Note that when the virtual input is waiting for next state,
	state after duration.	it cannot accept new requests.
return	<return page=""></return>	Redirect to the page < return page > after the request is
		completely assigned. The <return page=""> can be a full</return>
		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:			
	setvi.cgi?vi0=0(10000)1(15000)0(20000)1			
	No multiple duration.			
	setvi.cgi?vi3=0			
	VI index is out of range.			
	setvi.cgi?vi=1			
	No VI index is specified.			
503	The resource is unavailable, ex. Virtual input is waiting for next state.			
	Examples:			
	setvi.cgi?vi0=0(15000)1			
	setvi.cgi?vi0=1			
	Request 2 will not be accepted during the execution time(15 seconds).			

### 8.23Remote Focus

**Note:** This request requires Administrator privileges.

Method: GET/POST

### Syntax:

http://<servername>/cgi-bin/admin/remoefocus.cgi?function=<value>[&direction=<value>] [&position=<value>][&steps=<value>][&iris]

PARAMETER	VALUE	DESCRIPTION		
function	zoom,	Function type		
	focus,	zoom – Move zoom motor		
	auto,	focus – Move focus motor		
	scan,	auto – Perform auto focus		
	stop,	scan – Perform focus scan		
	positioning	stop – Stop current operation		
		positioning – Position the motors		
direction	direct,	Motor's moving direction.		
	forward,	It works only if function=zoom   focus.		
	backward			
position	0 ~ 150 if	Motor's position.		
	function=zoom.	It works only if function=zoom   focus and direction=direct.		
	75 ~ 290 if			
	function=focus.			
steps	1 ~ 5	Motor's moving steps.		
		It works only if function=zoom   focus and direction=forward		
		backward.		
iris	N/A	Open iris or not.		
		It works only if function=auto   scan.		

# **Technical Specifications**

System Information		Intelligent Video	
CPU	Multimedia SoC (System-on-Chip)	Video Motion Detection	Triple-window video motion detection
Flash	16 MB	Alarm and Event	
RAM	128 MB		Video motion detection manual trigger digital input
Camera Features		Alarm Triggers	Video motion detection, manual trigger, digital input, periodical trigger, system boot, recording notify
Image Sensor	1/2.7" Progressive CMOS	Alarm Events	Event notification using digital output, HTTP, SMTP,
Maximum Resolution	1280x800		FTP and NAS server
Lens Type	Vari-focal		File upload via HTTP, SMTP, FTP and NAS server
Focal Length	f = 3 ~ 9 mm	0	•
Aperture	F1.2 (wide), F2.1 (tele)	General	
Iris	P-iris	Smart Focus System	Focus assist OSD (Network streaming)
Field of View	102.68° ~ 35.4° (horizontal)	Connectors	RJ-45 for Network/PoE connection
	61.93° ~ 22.80° (vertical)		3.5 mm phone jack*2 for audio input/output
	122.56° ~ 41.11° (diagonal)		Terminal block*2 for AC 24V power input
Shutter Time	1/15 sec. to 1/25,000 sec.		Terminal block*4 for digital input
WDR Technology	WDR Pro		Terminal block*2 for digital output
Day/Night	Removable IR-cut filter for day & night function	LED Indicator	System power and status indicator
Minimum Illumination	0.8 Lux @ F1.2, 50 IRE (Color)	Power Input	24V AC
	0.001 Lux @ F1.2, 50 IRE (B/W)		IEEE 802.3af PoE Class 3
Pan/tilt/zoom	ePTZ:	Power Consumption	Max. 8.0W
Functionalities	16x digital zoom (4x on IE plug-in, 4x built-in)	Dimensions	Ø: 173 mm x 115 mm
IR Illuminators	Built-in IR illuminators, effective up to 20 meters	Weight	Net: 1266 g
	IR LED*18	Casing	Vandal-proof IK10-rated metal housing
On-board Storage	MicroSD/SDHC card slot		Weather-proof IP66-rated housing
VC-1		Safety Certifications	CE, LVD, FCC Class A, VCCI, C-Tick
Video		Operating Temperature	-20°C ~ 50°C (-4°F ~ 122°F)
Compression	H.264, MJPEG & MPEG-4	Warranty	24 months
Maximum Frame Rate	H.264: 30 fps at 1280x800	System Begyirements	
	MPEG-4: 30 fps at 1280x800	System Requirements	
	MJPEG: 30 fps at 1280x800	Operating System	Microsoft Windows 7/Vista/XP/2000
Maximum Streams	2 simultaneous streams	Web Browser	Mozilla Firefox 7~10
S/N Ratio	Above 60.5 dB		Internet Explorer 7.x or above
TV Line	1235 TVL (Horizontal)	Other Players	VLC: 1.1.11 or above
Dynamic Range	110.4 dB		QuickTime: 7 or above
Video Streaming	Adjustable resolution, quality and bitrate	Included Accessories	
	Configurable video cropping for bandwidth saving	included Accessories	
Image Settings	Adjustable image size, quality and bit rate	CD	User's manual, quick installation guide, Installation
	Time stamp, text overlay, flip & mirror		Wizard 2, ST7501 32-channel recording software
	Configurable brightness, contrast, saturation,	Others	Quick installation guide, warranty card, mounting pla
	sharpness, white balance, exposure control, gain,		alignment sticker, ceiling hole template sticker, L-type
	backlight compensation, privacy masks		hex key wrench, silica gel, screws, hex nut,
	Scheduled profile settings		double-sided tape, AV cable, waterproof connector &
Audio			bushing, software CD
Audio Capability	Audio input/output (half duplex)		
Compression	GSM-AMR, AAC, G.711	Dimensions	
Interface	External microphone input		
Network			
Users	Live viewing for up to 10 clients		E .
Protocols	IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP,		/// ///
	RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP,	Ø173 mm	
	DNS, DDNS, PPPoE, CoS, QoS, SNMP, 802.1X	[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]	
Interface	10Base-T/100 BaseTX Ethernet (RJ-45)		
ONVIF	Ver. 1.02		
Compatible Acce	occarios		
WT 0 1 0 0 1 0 12 1 0 1 1 0 1 1 0 W 4 Y 0 1 0 1 4	ASSIGNATION AND ADDRESS OF THE PROPERTY OF THE		
Companion Acce			



All specifications are subject to change without notice. Copyright @ 2012 VIVOTEK INC. All rights reserved.

### **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 <a href="http://www.vialicensing.com">http://www.vialicensing.com</a>.

### **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; 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 B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

### **CE Mark Warning**

This is a Class B 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、情報処理装置等電波障害自主規制協議会(VCCI)の基準にづくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい

### 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.