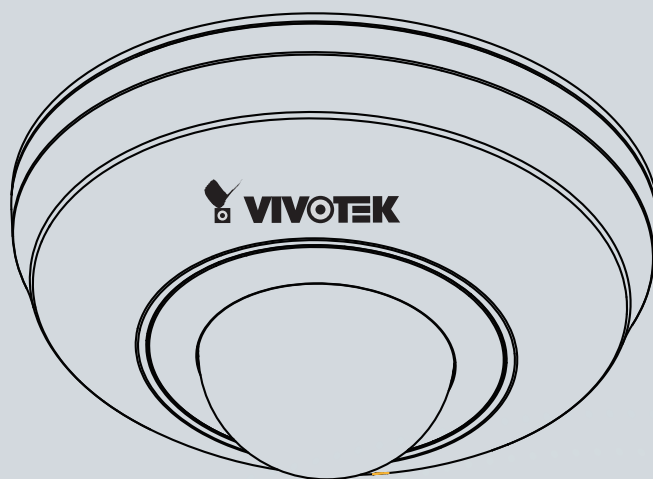




**PD8136** Pan/Tilt Dome  
Network Camera

# User's Manual

1MP • Pan/Tilt • PoE



Rev. 1.0

## ***Table of Contents***

---

<b>Overview</b> .....	<b>4</b>
Read Before Use.....	5
Package Contents.....	5
Symbols and Statements in this Document.....	5
Physical Description .....	6
Restoring defaults .....	7
<b>Installation</b> .....	<b>8</b>
Hardware Installation .....	8
Network Deployment.....	12
Software Installation.....	14
Ready to Use.....	15
<b>Accessing the Network Camera</b> .....	<b>16</b>
Using Web Browsers.....	16
Using RTSP Players.....	18
Using 3GPP-compatible Mobile Devices.....	19
Using VIVOTEK Recording Software .....	20
<b>Main Page</b> .....	<b>21</b>
<b>Client Settings</b> .....	<b>27</b>
<b>Configuration</b> .....	<b>29</b>
System > General settings .....	30
System > Homepage layout .....	32
System > Logs .....	36
System > Parameters .....	37
System > Maintenance.....	38
Media > Image .....	42
Media > Video .....	47
Media > Audio.....	50
Network > General settings.....	51
Network > Streaming protocols .....	58
Network > SNMP (Simple Network Management Protocol) .....	67
Security > User Account.....	68
Security > HTTPS (Hypertext Transfer Protocol over SSL) .....	69
Security > Access List .....	76
PTZ > PTZ settings .....	81
Event > Event settings .....	84
Applications > Motion detection.....	98
Applications > Tampering Detection.....	101
Recording > Recording settings .....	102
Local storage > SD card management.....	107
Local storage > Content management .....	108
<b>Appendix</b> .....	<b>110</b>

URL Commands for the Network Camera.....	110
Technical Specifications .....	112
Technology License Notice.....	113
Electromagnetic Compatibility (EMC).....	114

## Overview

VIVOTEK PD8136 is equipped with a 1MP sensor enabling viewing resolution of 1280x800 at 30 fps. Users need look no further for an all-in-one camera capable of capturing high quality, high resolution video with pan & tilt control. With a stylish design and small footprint to fit most installation environments, it is the best choice for indoor surveillance applications such as retail stores, offices, or homes.

With flexible 360-degree pan and 80-degree tilt, PD8136 gives users comprehensive control over a monitored site. The PD8136 supports the industry-standard H.264 compression technology, drastically reducing file sizes and conserving valuable network bandwidth. In addition, PD8136 is integrated with Power over Ethernet functionality, making installation easier and more cost-efficient. Together with the bundled, multi-lingual 32-channel recording software ST7501, users can set up an easy-to-use IP surveillance system with ease.

## 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

- PD8136
- Ceiling Mount Brackets
- Screws / RJ45 female-female Coupler
- Quick Installation Guide
- Software CD / Warranty Card

## 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 facilitate an installation, function, or process.



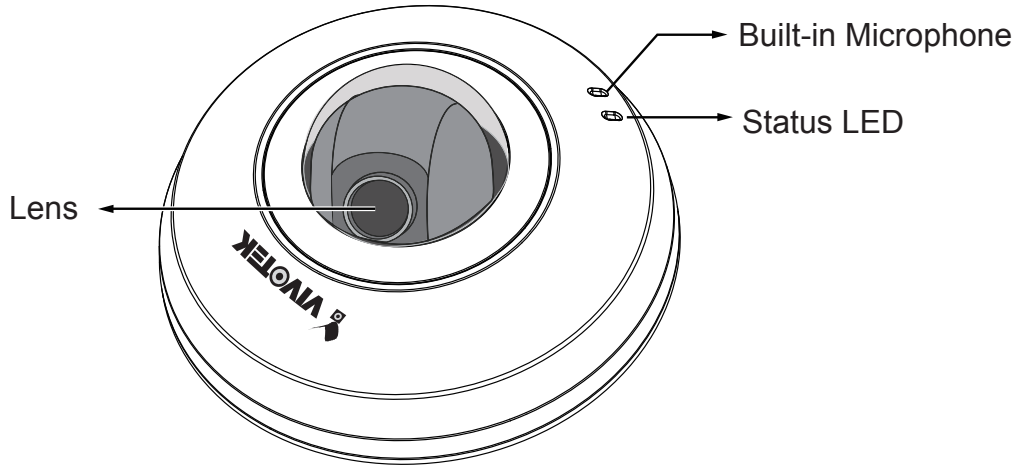
**WARNING! or IMPORTANT!:** These statements indicate situations that can be dangerous or hazardous to the machine or you.



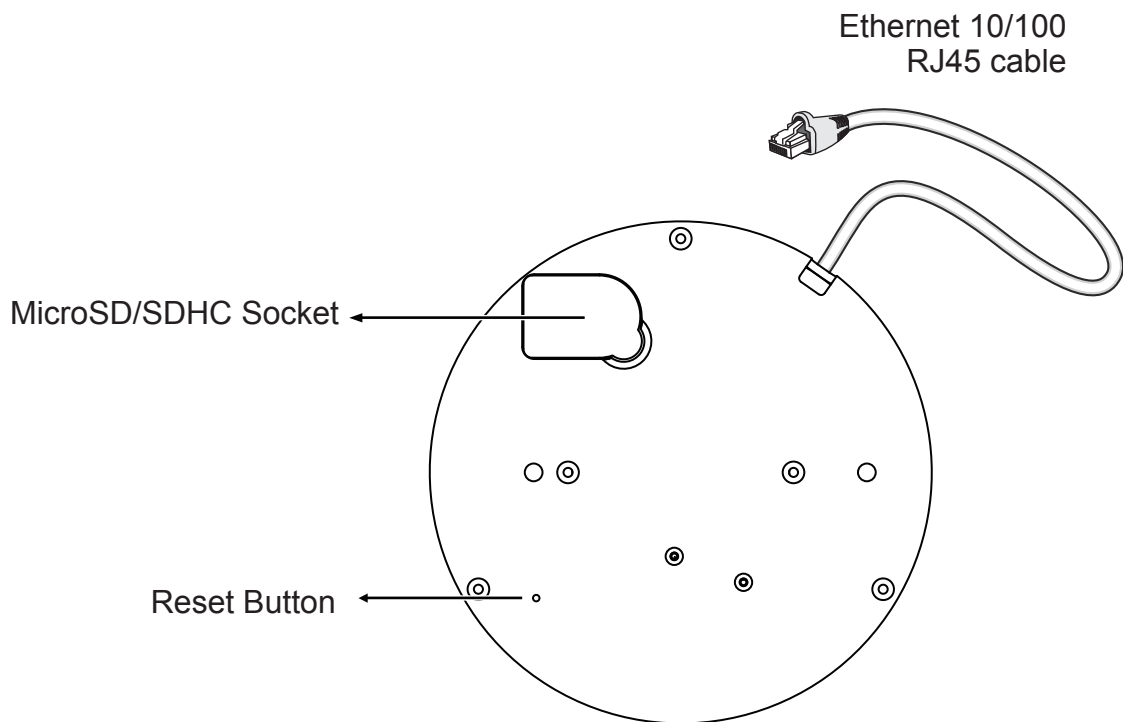
**Electrical Hazard:** This statement appears when high voltage electrical hazards might occur to an operator.

## Physical Description

### ● Top View



### ● Bottom View



## LED Definitions

Item	LED Status	Description
1	Steady <b>Red</b>	Power on and system booting
	<b>Red</b> LED off	Power off
2	Steady <b>Red</b> + blinking <b>Green</b> every 1 sec. (Green LED on for 1 sec and off for another)	Network heartbeat
	Steady <b>Red</b> + <b>Green</b> LED off	Network disconnected
3	Blinking <b>Red</b> every 0.15 sec. + Blinking <b>Green</b> every 1 sec. ( <b>Red</b> LED on for 0.15 sec. and <b>Green</b> LED on for 1 sec. and off for another)	Upgrading firmware
4	Blinking <b>Red</b> every 0.15 sec. + blinking <b>Green</b> every 0.15 sec.	Restoring defaults

## Hardware Reset

The reset button is used to reset the system or to 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.

**Reset:** Press and release the recessed reset button with a paper clip or thin object. Wait for the Network Camera to reboot.

**Restore:** Press and hold the recessed reset button for a while to restore. Note that all settings will be restored to factory default.

## SD/SDHC/SDXC Card Capacity

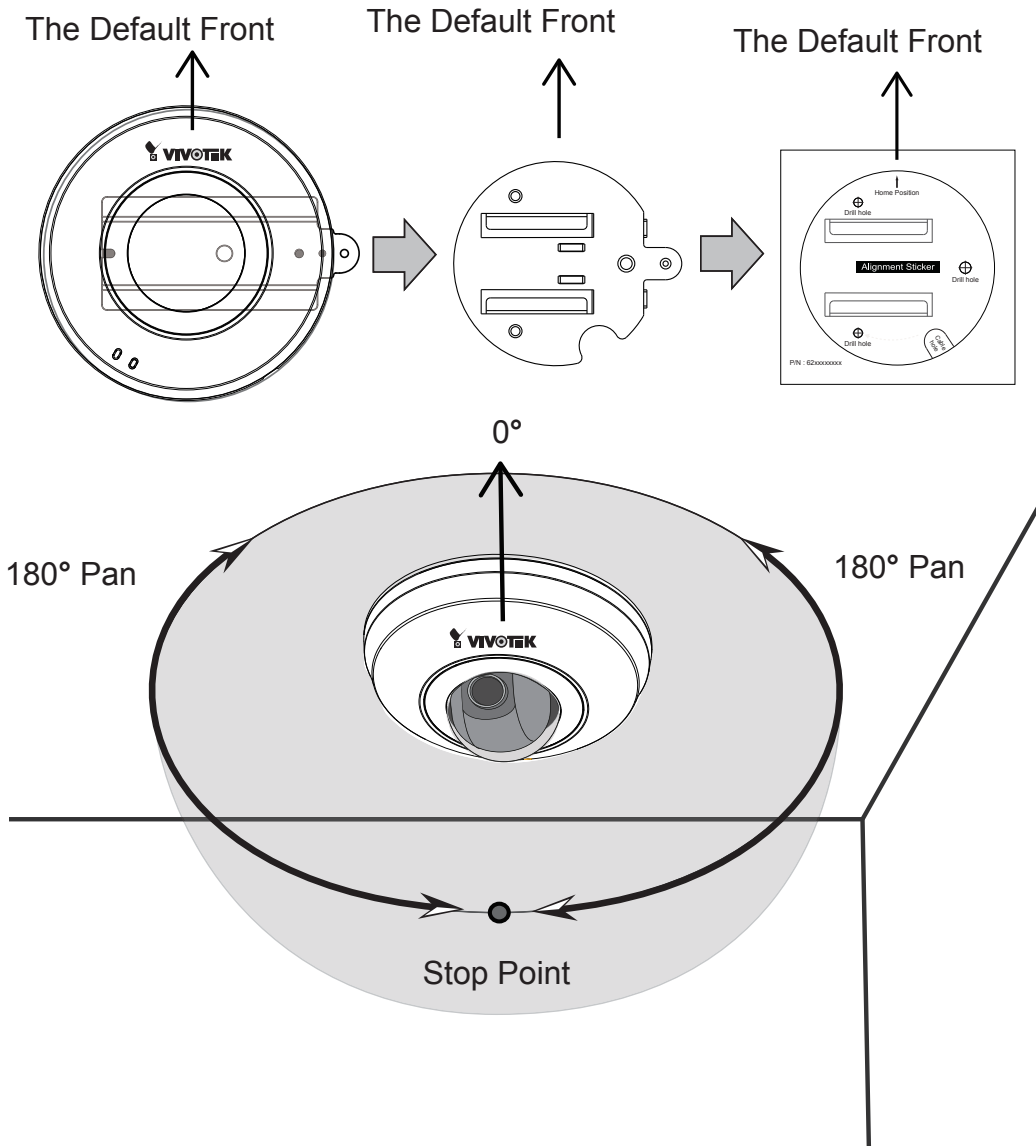
This network camera is compliant with **SD/SDHC/SDXC 32GB, 64GB**, and other preceding standard SD cards.

# Installation

## Hardware Installation

### ● Mounting Plate and Camera Orientation

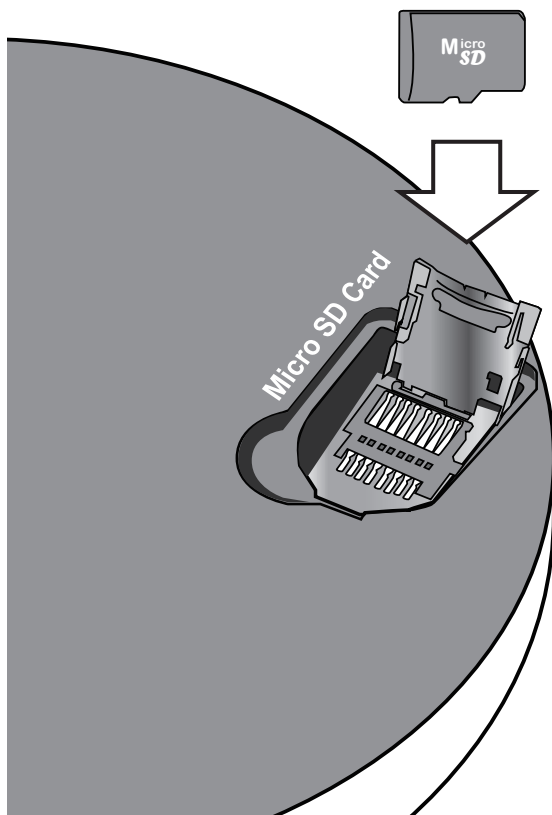
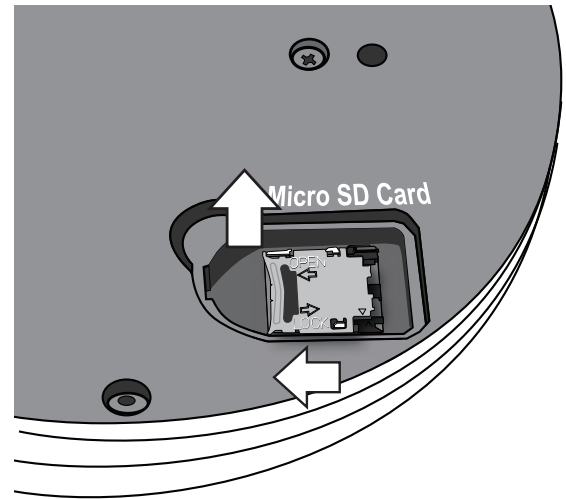
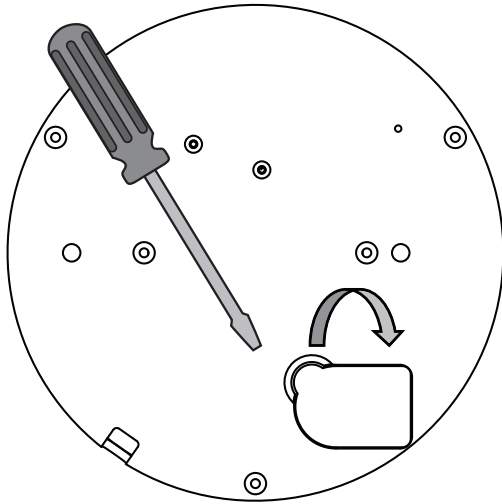
When installing the camera, orient the default front on the mounting plate (illustrated below) towards the area of your interest. The camera lens' central position is aligned with the VIVOTEK logo on the dome cover.





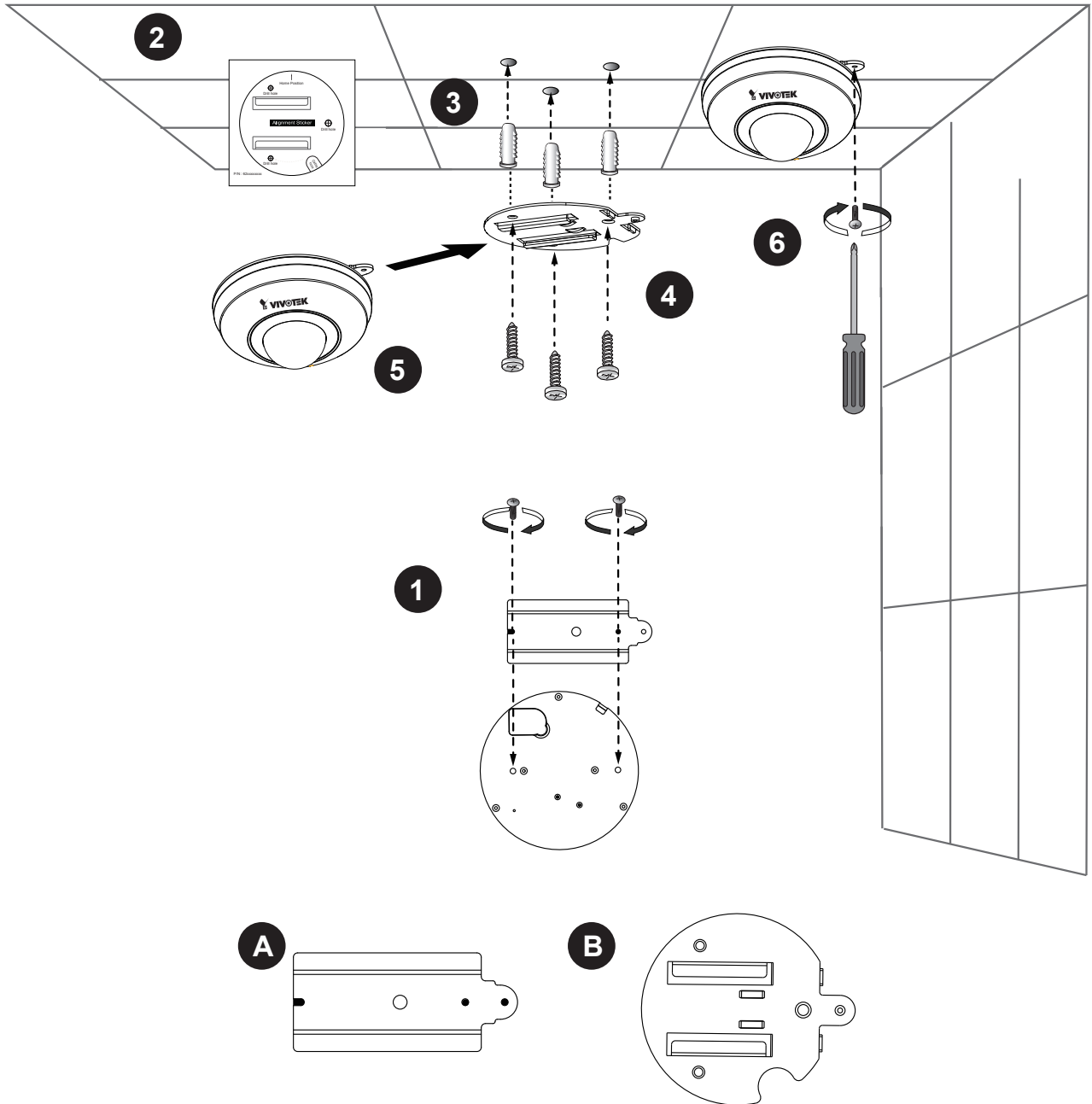
## ● Install MicroSD Card

Open the MicroSD card plastic cover at the bottom using a small flathead screwdriver. Flip the socket cover forward and up. Insert a MicroSD card, close the cover, and push it back to secure the installation. Install the plastic cover by pressing it back to its original position.



## ● Mounting the Network Camera

1. Attach base plate "A" of the ceiling mount bracket to the bottom of camera and secure it with two small round head screws. Note that the guiding edge of the base plate (where a screw hole is available) must protrude from the edge of camera.
2. Use the included alignment sticker, orient the sticker toward the direction you prefer.
3. Drill three holes into the ceiling; hammer the plastic anchors into the holes.
4. Install ceiling mounting plate "B" to the ceiling with three screws.
5. Slide the Network Camera into mounting plate "B."
6. Secure the camera to the mounting plate with a small screw.



## Network Deployment

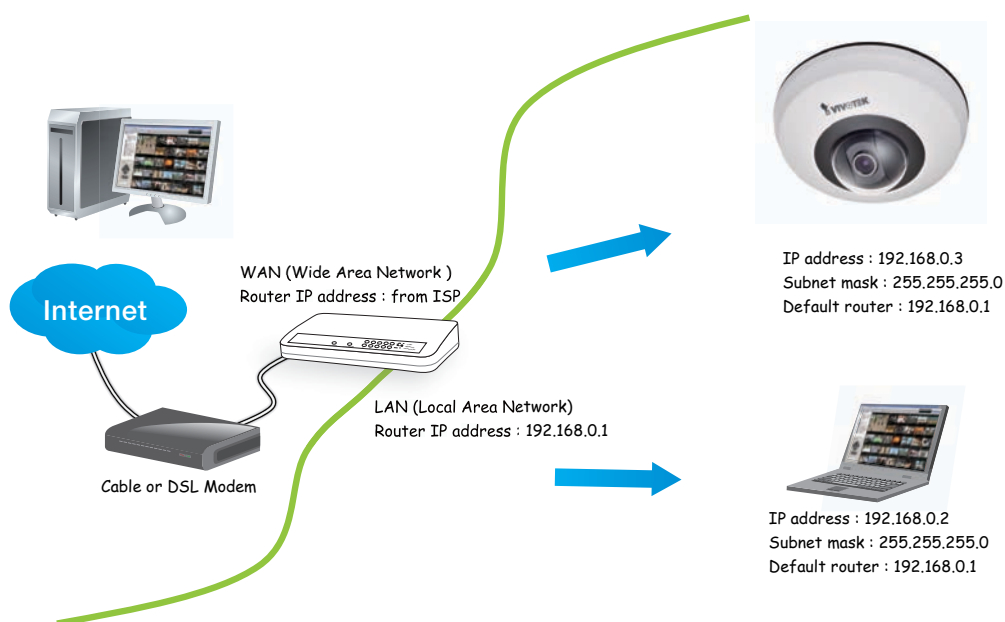
### Setting up the Network Camera over the Internet

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

#### Internet connection via a router

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

1. 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 14 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.

- Secondary HTTP port: 8080
- RTSP port: 554
- RTP port for audio: 5558
- RTCP port for audio: 5559
- RTP port for video: 5556
- RTCP port for video: 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 51 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 on page 51 for details.

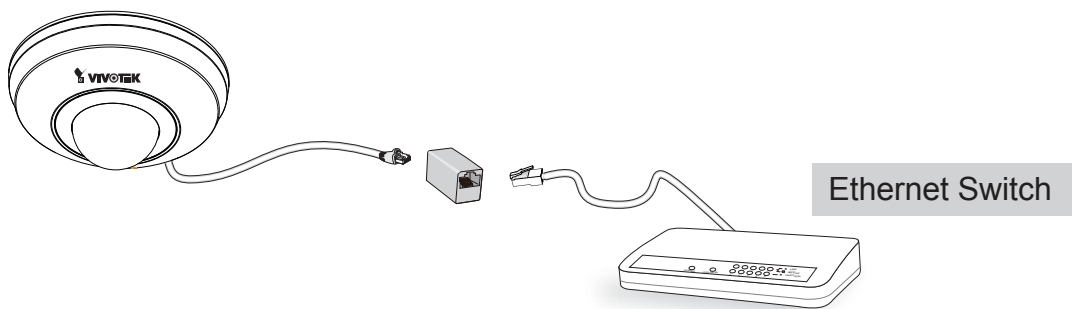
### **Internet connection via PPPoE (Point-to-Point over Ethernet)**

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 49 for details.

## General Connection

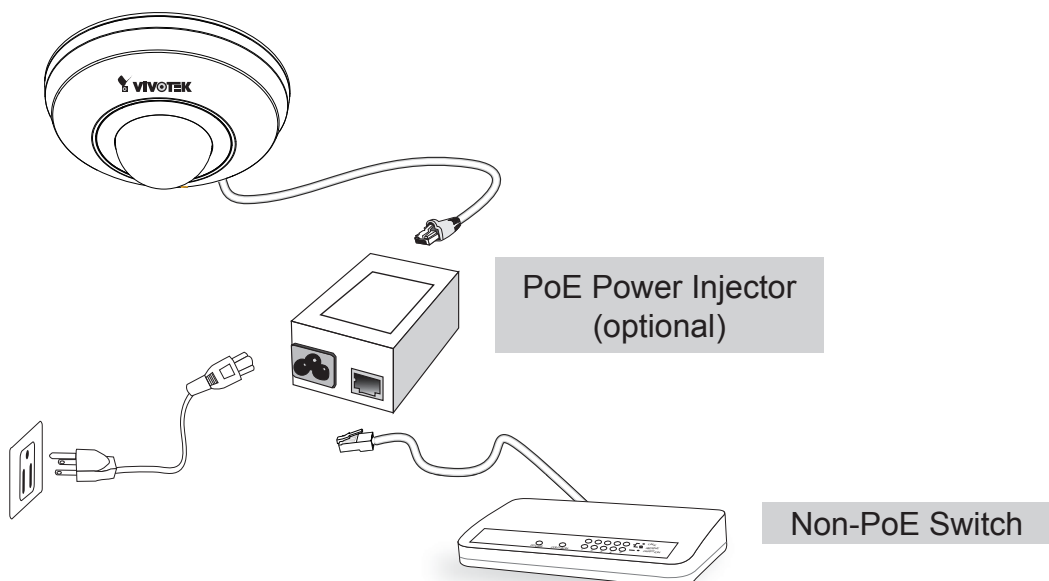
### ● When using a PoE-enabled switch

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



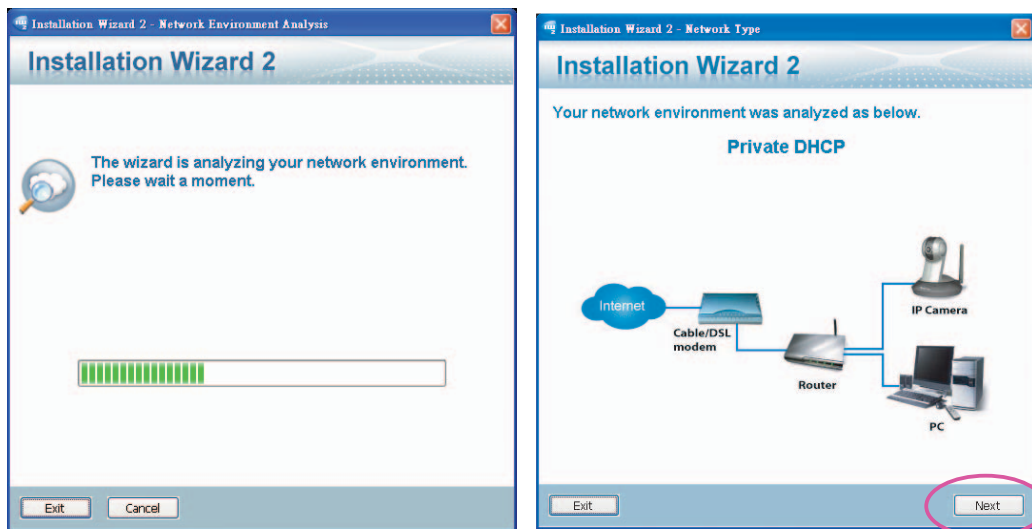
## Software Installation

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

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

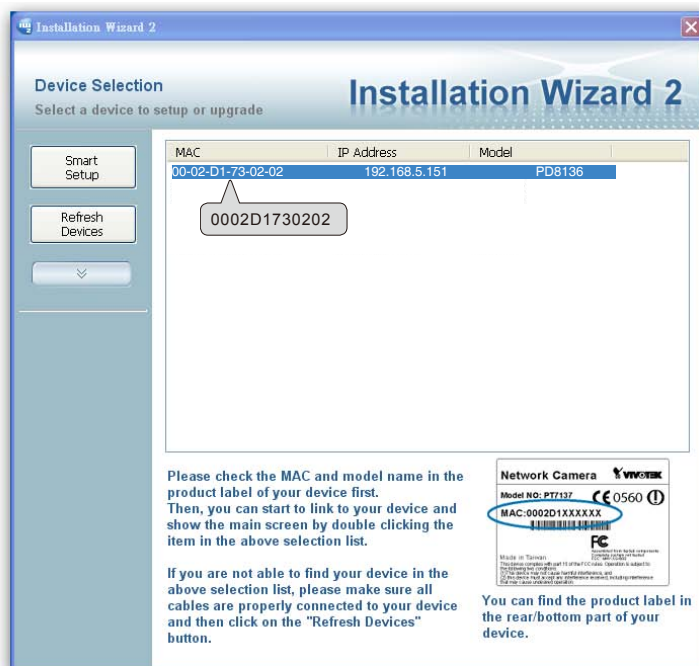


2. The program will conduct an analysis of your network environment.  
 After your network environment is analyzed, please click **Next** to continue the program.



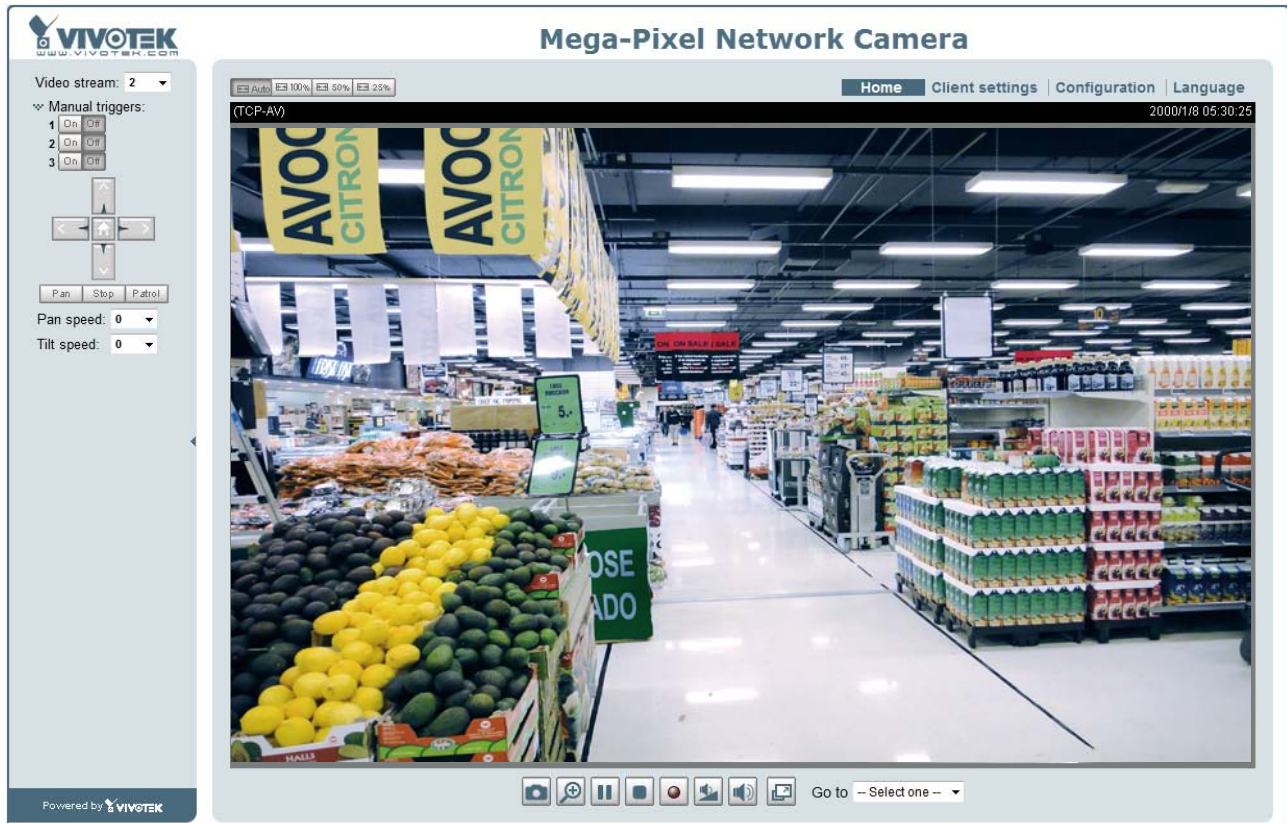
3. The program will search for all VIVOTEK network devices on the same LAN.

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



## 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.



### IMPORTANT:

- Currently the Network Camera utilizes a 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`

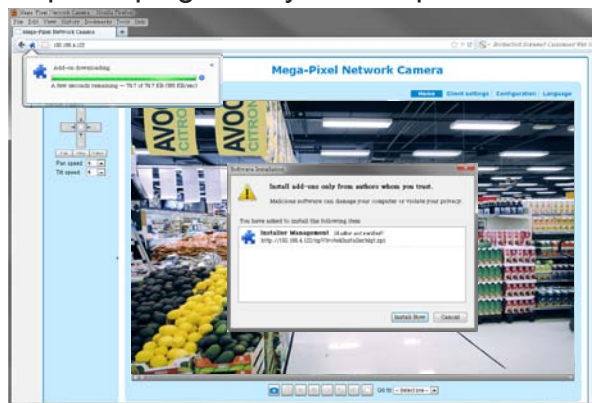
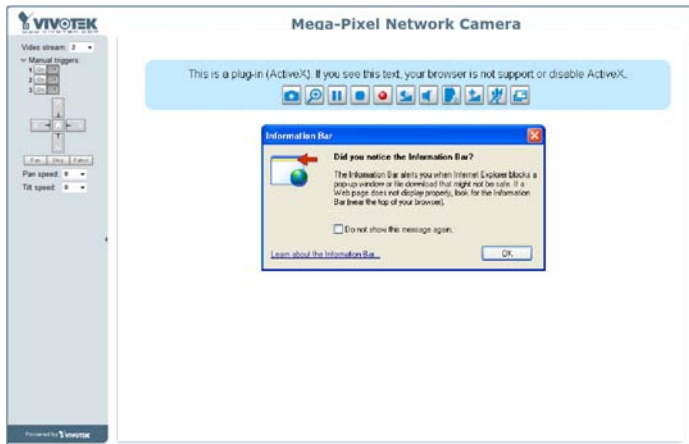
# Accessing the Network Camera


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

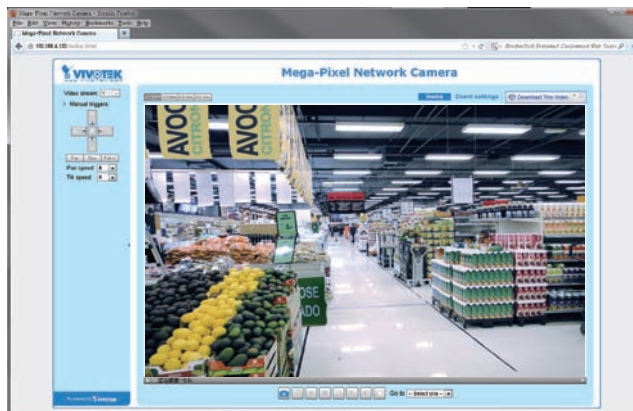
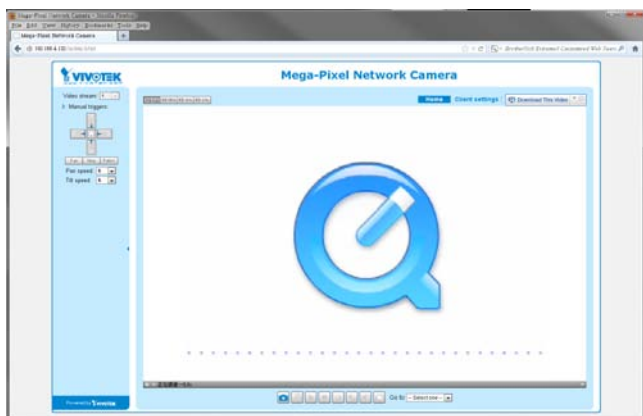
Use Installation Wizard 2 (IW2) to access to the Network Cameras on the LAN. If your network environment is not a LAN, follow these steps to access the Network Camera:

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. (A temporary IP will be generated for the camera. Find it in your Network Neighborhood). Press **Enter**.
3. Live video will display in your web browser.
4. If it is the first time installing the VIVOTEK network camera, an information bar will pop up as shown below. Follow the instructions to install the required plug-in on your computer.



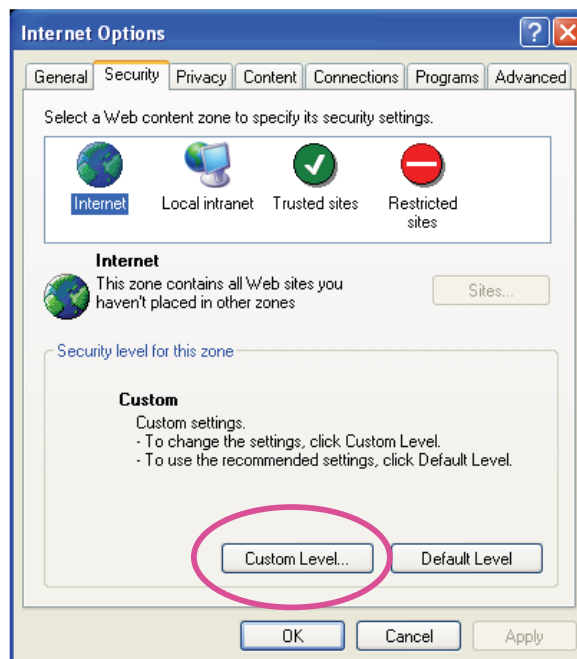
 **NOTE:**

*For Mozilla **Firefox** or **Netscape** users, your browser will use **Quick Time** to stream live video. If you do not have Quick Time on your computer, please download Quick Time from Apple Inc's website, and then launch your web browser.*

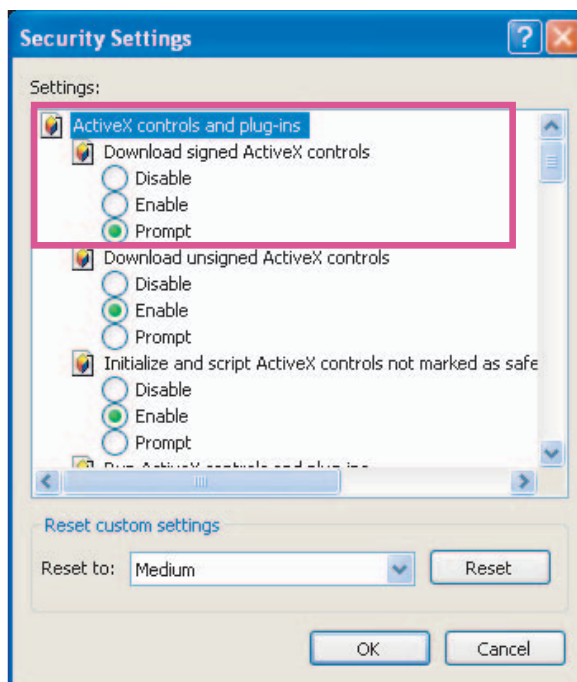


- ▶ *By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera. For more information about how to enable password protection, please refer to Security on page 68.*
- ▶ *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable the ActiveX® Controls for your browser.*

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



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



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



## Using RTSP Players

To view the H.264/MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.



Quick Time Player

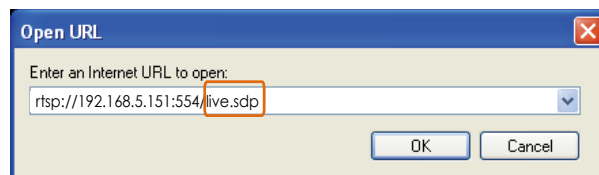


VLC Media Player

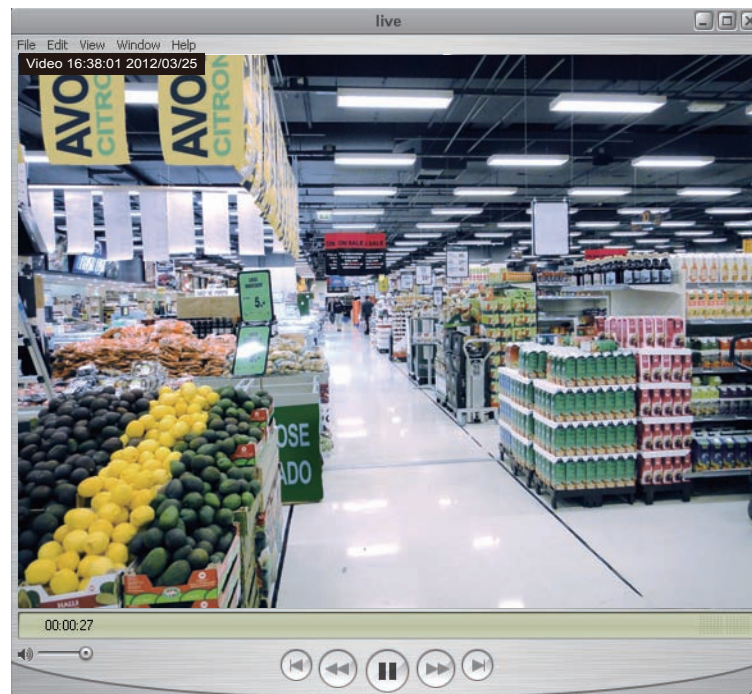
1. Launch the RTSP player.
2. Choose File > Open URL. An URL dialog box will pop up.
3. The address format is `rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>`

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 59.

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 59 for details.



## Using 3GPP-compatible Mobile Devices

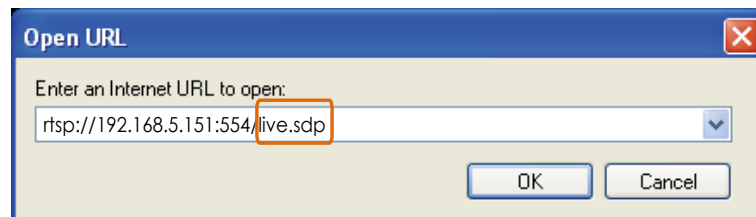
To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 12.

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 59.
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 48.

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 59.
4. Launch the player on the 3GPP-compatible mobile devices (e.g., Quick Time Player).
5. Key in the following URL commands into the player.  
The address format is `rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream 3>`.  
For example:



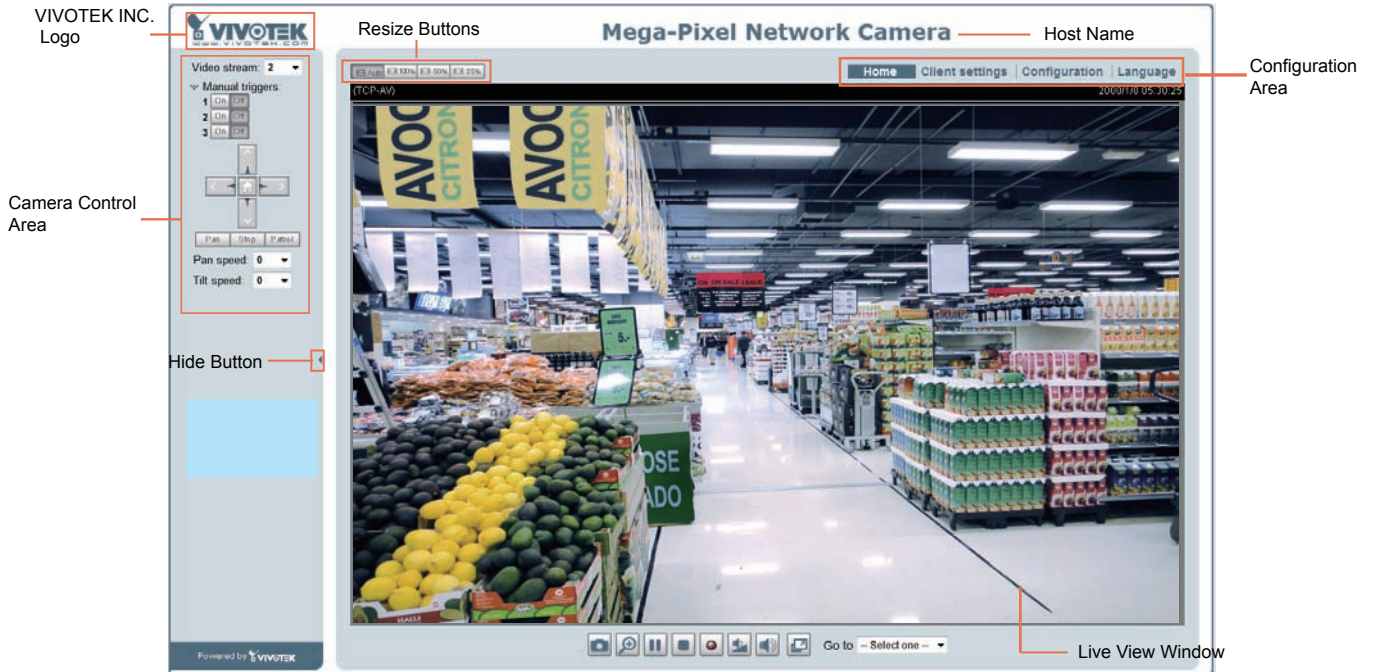
## Using VIVOTEK Recording Software

The product software CD also contains 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>.



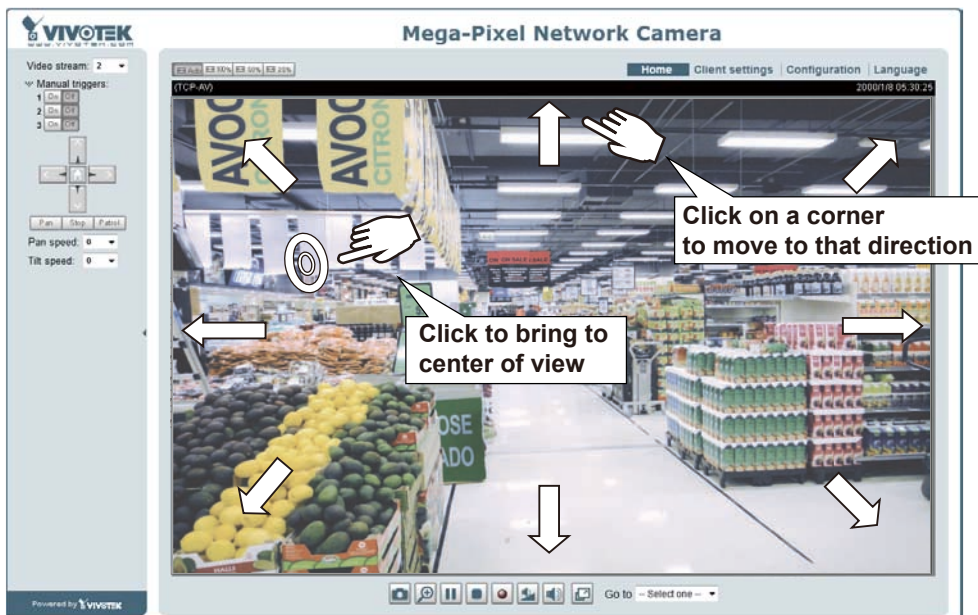
# Main Page

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, and Live Video Window.



## Mouse and Screen Control

In addition to the use of a joystick, mouse control is also supported by the web session. You can click on any spot on the screen to move camera's field of view to that direction. Click on a corner to move to that direction. Note that you can horizontally pan to the right or left by a 180 degrees from the central point, until reaching the stop point.



Note that if your screen control malfunctions, it is possible that the CPU of your current view station can not cope with the HD video feeds or that an incompatibility issue occurred with the ActiveX control plug-ins.

### VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

### Host Name

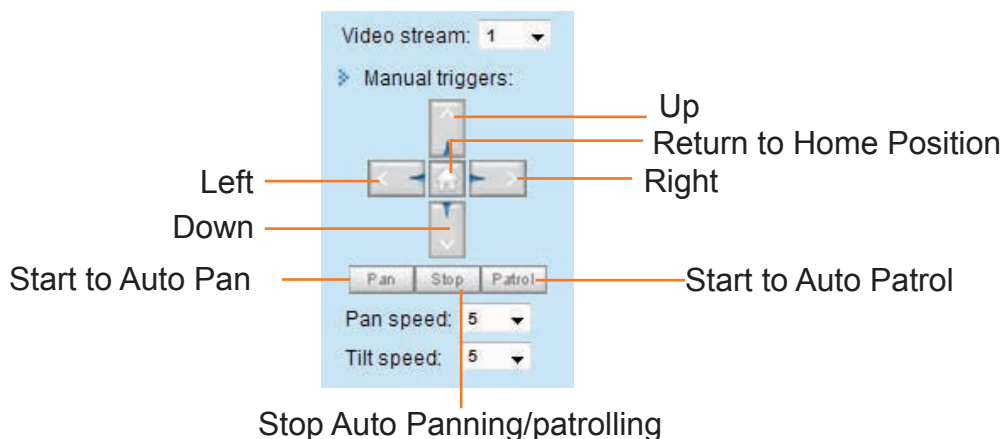
The host name can be customized to fit your needs. For more information, please refer to System on page 30.

### Camera Control Area

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

Manual Triggers: Click to reveal the manual trigger buttons.

### PTZ Control Panel:



Pan: Click this button to start the auto pan (will pan 180° to one side, pan 180° to the other, and then return to the home position).

Stop: Click this button to stop the Auto Pan and Auto Patrol action.

Patrol: Once the Administrator has configured the list of preset positions, click this button to command the camera to patrol among those positions on the Patrol List. The Network Camera will patrol through the preset positions for one time. For more information, please refer to PTZ control on page 81.



### Tips:

The onscreen Java control can malfunction under the following situations:

A PC connects to different cameras that are using the same IP address (or the same camera running different firmware versions).

Removing your browser cookies will solve this problem.

**Pan /Tilt speed:** Adjust the speed of Pan/ Tilt movement:

Pan speed	Tilt speed	Zoom speed	Focus speed	
-5	-5	-5	-5	Slower
-4	-4	-4	-4	
-3	-3	-3	-3	
-2	-2	-2	-2	
-1	-1	-1	-1	
0	0	0	0	
1	1	1	1	
2	2	2	2	
3	3	3	3	Faster
4	4	4	4	
5	5	5	5	

Note that mouse screen control is also supported. You can refer to page 81 for related information.

**Configuration Area**

**Client Settings:** Click this button to access the client setting page. For more information, please refer to Client Settings on page 27.

**Configuration:** 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 29.

**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, 简体中文, and 繁體中文. You can also change a language on the Configuration page; please refer to page 29.

**Hide Button**

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

## Resize Buttons

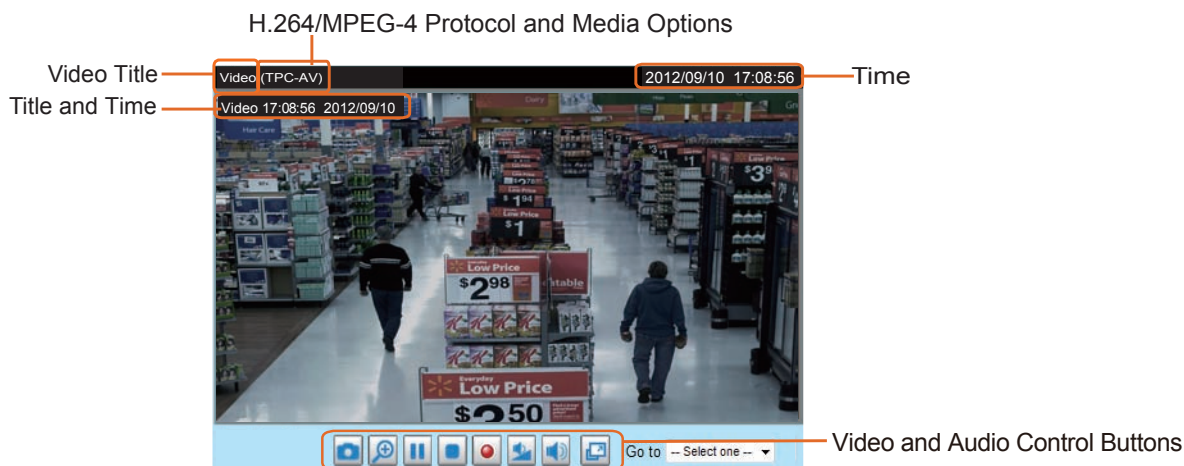


Click the Auto button, the video cell will resize automatically to fit the monitor.  
 Click 100% is to display the original homepage size.  
 Click 50% is to resize the homepage to 50% of its original size.  
 Click 25% is to resize the homepage to 25% of its original size.

## Go to

If you have preset PTZ positions, these positions will be available in the Go to menu. Please refer to page 81 for more information. [Live Video Window](#)

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



Video Title: The video title can be configured. For more information, please refer to Video settings on page 42.


H.264 / MPEG-4 Protocol and Media Options: The transmission protocol and media options for H.264 / MPEG-4 video streaming. For further configuration, please refer to Client Settings on page 27.


Time: Display the current time. For further configuration, please refer to Media > Image > General settings on page 42.

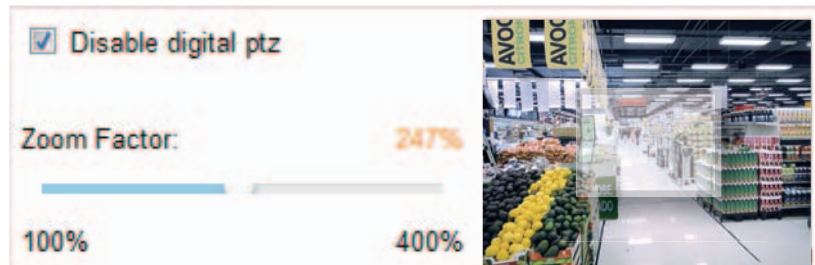
Title and Time: The video title and time can be stamped on the streaming video. For further configuration, please refer to Media > Image > General settings on page 42.



Title 2012/09/05 10:39:08



Video and Audio Control Buttons: 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.



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







 **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 28 for details.

 **Volume:** When the audio  is not muted, move the slider bar to adjust the volume on the local computer.

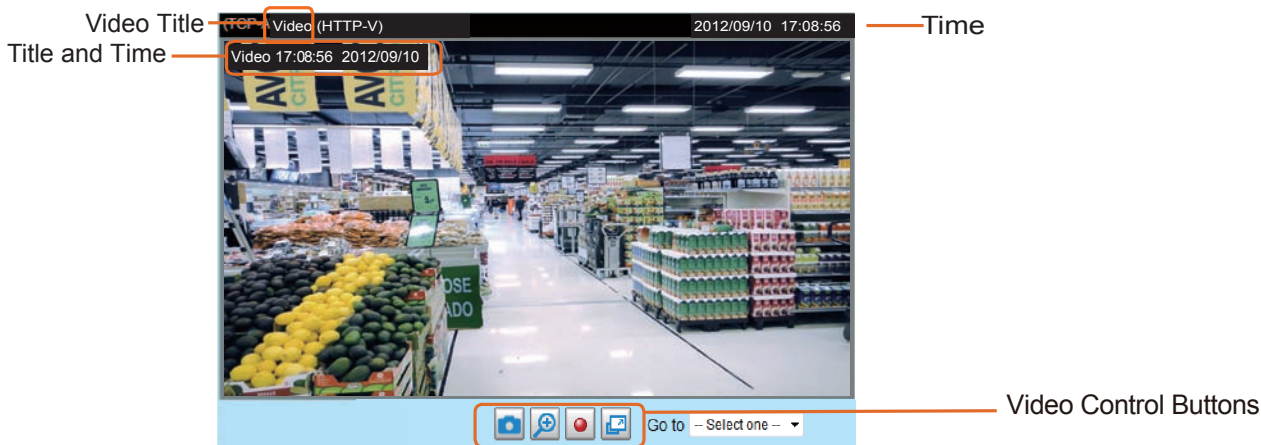
 **Mute:** Turn off the volume on the local computer. The button becomes the  **Audio On** button after clicking the Mute button.

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

 **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:





Video Title: The video title can be configured. For more information, please refer to Media > Image on page 42.

Time: Display the current time. For more information, please refer to Media > Image on page 42.



Title and Time: Video title and time can be stamped on the streaming video. For more information, please refer to Media > Image on page 42.


Video and Audio Control Buttons: 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.

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



 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 28 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

Video and Audio

Video Only

Audio Only

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

## H.264 / MPEG-4 Protocol Options

H.264/MPEG-4 Protocol Options

UDP Unicast

UDP Multicast

TCP

HTTP

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

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

**UDP multicast:** This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps 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 60.

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

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


## MP4 Saving Options

**MP4 Saving Options**

Folder:

File name prefix:

Add date and time suffix to file name

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

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

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

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



## Local Streaming Buffer Time

**Local Streaming Buffer Time**

Millisecond

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. Please refer to page 68 Security > User Account for how to configure access rights for different users.

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.

Show below are the locations of the Basic Mode and the Advanced Mode screen elements:

## Basic Mode

The screenshot displays the VIVOTEK web interface in Basic Mode. The top navigation bar includes 'Home', 'Client settings', 'Configuration', and 'Language'. The main content area is titled 'System > General settings' and contains two sections: 'System' and 'System time'. The 'System' section includes a 'Host name' field (set to 'Mega-Pixel Network Camera') and a checkbox for 'Turn off the LED indicator'. The 'System time' section has radio buttons for 'Keep current date and time' (selected), 'Synchronize with computer time', 'Manual', and 'Automatic'. A 'Save' button is located at the bottom right. On the left, a blue sidebar menu lists 'System', 'General settings', 'Maintenance', 'Media', 'Network', 'Security', and 'Applications'. Below the menu is a '[ Advanced mode ]' button. At the bottom left, the 'Version: 0100e' is displayed.

Annotations in the image point to the following elements:

- Navigation Area:** The top navigation bar containing 'Home', 'Client settings', 'Configuration', and 'Language'.
- Configuration List:** The left sidebar menu containing 'System', 'General settings', 'Maintenance', 'Media', 'Network', 'Security', and 'Applications'.
- Click to switch to Advanced Mode:** The '[ Advanced mode ]' button at the bottom of the sidebar.
- Firmware Version:** The 'Version: 0100e' text at the bottom left of the page.

## 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 tagged with **Advanced Mode**. If you want to configure 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), **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.

### System

**System**

Host name:

Turn off the LED indicator

**Host name:** Enter a desired name for the Network Camera. The text will be displayed at the top of the main page.

## System time

**System time**

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

Note: You can upload your daylight saving time rules on [Maintenance](#) page or use the camera default value.

Keep current date and time  
 Synchronize with computer time  
 Manual  
 Automatic

Save

**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.

**Synchronize with computer time:** 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.

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

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

**NTP server:** Assign the IP address or domain name of an established time server. Leaving the text box blank connects the Network Camera to the default time servers.

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

**Time zone Advanced Mode:** Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules, please refer to **System > Maintenance > Import/ Export files** on page 39 for details.

When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

## 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 homepage 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, such wording will be removed from the homepage.


### Logo graph


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

**Logo graph**

A customized logo (Gif, JPG or PNG) can be uploaded for main page. It will be resized to 160x50 pixels to replace the previous logo.

Default
  Custom





Logo link:

Follow the steps below to upload a new logo:

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

## 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.

General settings | Theme options

Font Color — Video stream 1

Background Color of the Control Area — Manual triggers:

Font Color of the Configuration Area — Powered by VIVOTEK

Background Color of the Configuration Area —

Preset patterns — Themes

Font Color of the Video Title — Mega-Pixel Network

Background Color of the Video Area —

Frame Color —

Color

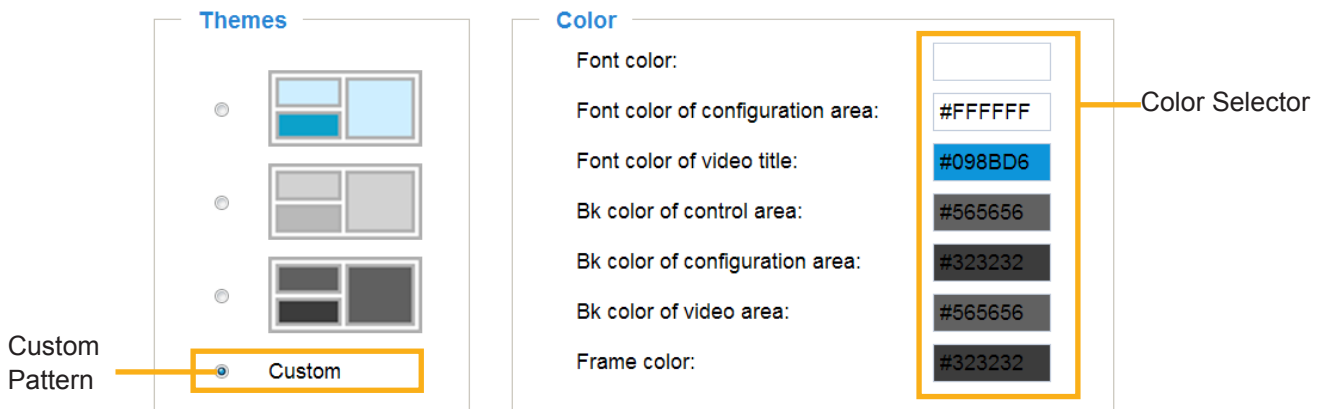
- Font color: #000000
- Font color of configuration area: #FFFFFF
- Font color of video title: #098BD6
- Bk color of control area: #C4EAFF
- Bk color of configuration area: #0186D1
- Bk color of video area: #C4EAFF
- Frame color: #0186D1

Save

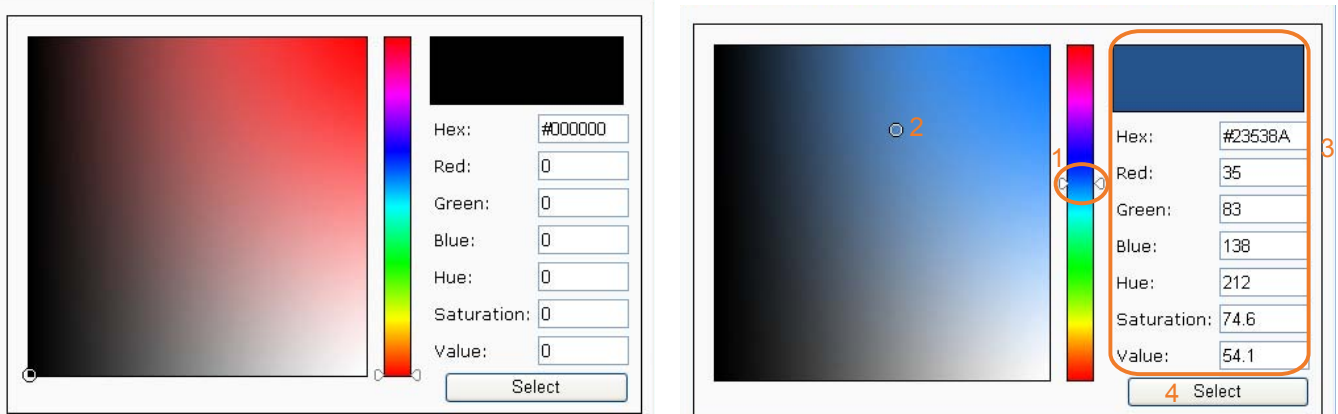




- Follow the steps below to set up the customized homepage:
  - Click **Custom** on the left column.
  - A double-click on the color selection area (the right hand side column) will bring up a color palette window.



- The palette window will pop up as shown below.



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

Below are options for system integrators or VARs. You can use the checkboxes to replace VIVOTEK's company logo, the embedded website address or the slogan "Powered by VIVOTEK." When done, use the Save button to complete the configuration.

**Logo graph**

A customized logo (Gif, JPG or PNG) can be uploaded for main page. It will be resized to 160x50 pixels to replace the previous logo.

Default
  Custom

Logo link:

---

**Customized button**

Show manual trigger button

- Customized button: Deselect the “Show manual trigger button” if you do not need the manual trigger function. System default is enabled.

## System > Logs Advanced Mode

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

### Log server settings

**Log server settings**

Enable remote log

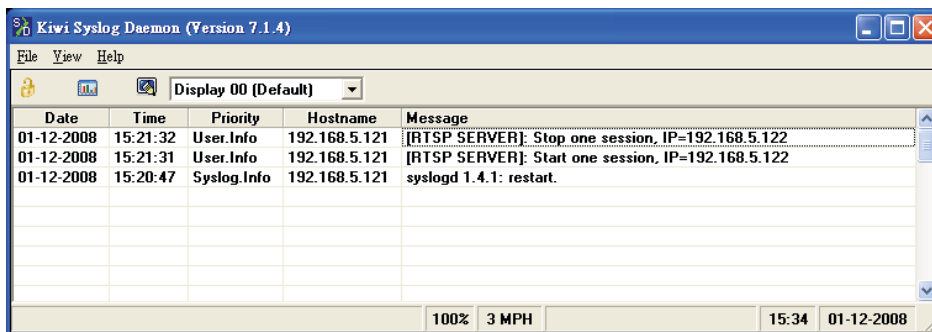
IP address:

port:

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 <http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/>.



### 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 the number of events reaches a preset limit.

```

Sep 19 16:44:31 syslogd 1.5.0: restart.
Sep 19 16:44:32 [EVENT MGR]: Starting eventmgr with support for EcTun
Sep 19 16:44:32 [EVENT MGR]: Task conf file: there is no valid event in recording_task.xml, skip it
Sep 19 16:44:32 [EVENT MGR]: Task conf file: there is no valid event in event_task.xml, skip it
Sep 19 16:44:33 udhcpd: deconfig
Sep 19 16:44:34 udhcpd: IP 192.168.4.135 netmask 255.255.255.0
Sep 19 16:44:34 udhcpd: router 192.168.4.1
Sep 19 16:44:34 udhcpd: dns 192.168.0.21 192.168.0.22
Sep 19 16:44:37 [swatcdog]: Ready to watch vncslave1.
Sep 19 16:44:37 [swatcdog]: Ready to watch vncslave2.
Sep 19 16:44:39 [swatcdog]: Ready to watch configer.
Sep 19 16:44:39 [ectun]: receiver value of x-path : "camctrl_c0_isptz" from configer failed!
Sep 19 16:44:39 [ectun]: Get Notify parameter "camctrl_c0_isptz" value failed
Sep 19 16:44:40 [swatcdog]: Ready to watch httpd.
Sep 19 16:44:41 [swatcdog]: Ready to watch recorder.
Sep 19 16:44:42 [DRM Service]: Starting DRM service.
Sep 19 16:44:43 [swatcdog]: Ready to watch rtsp.
Sep 19 16:44:43 automount[807]: [fnbuf]/usr/lib/autofs/mount_vfat.so
Sep 19 16:44:43 automount[807]: 1
Sep 19 16:44:43 automount[807]: [fnbuf]/usr/lib/autofs/mount_generic.so
Sep 19 16:44:43 automount[807]: do_mount /dev/localstorage1 /mnt/auto/CF type vfat options (null) using
    
```

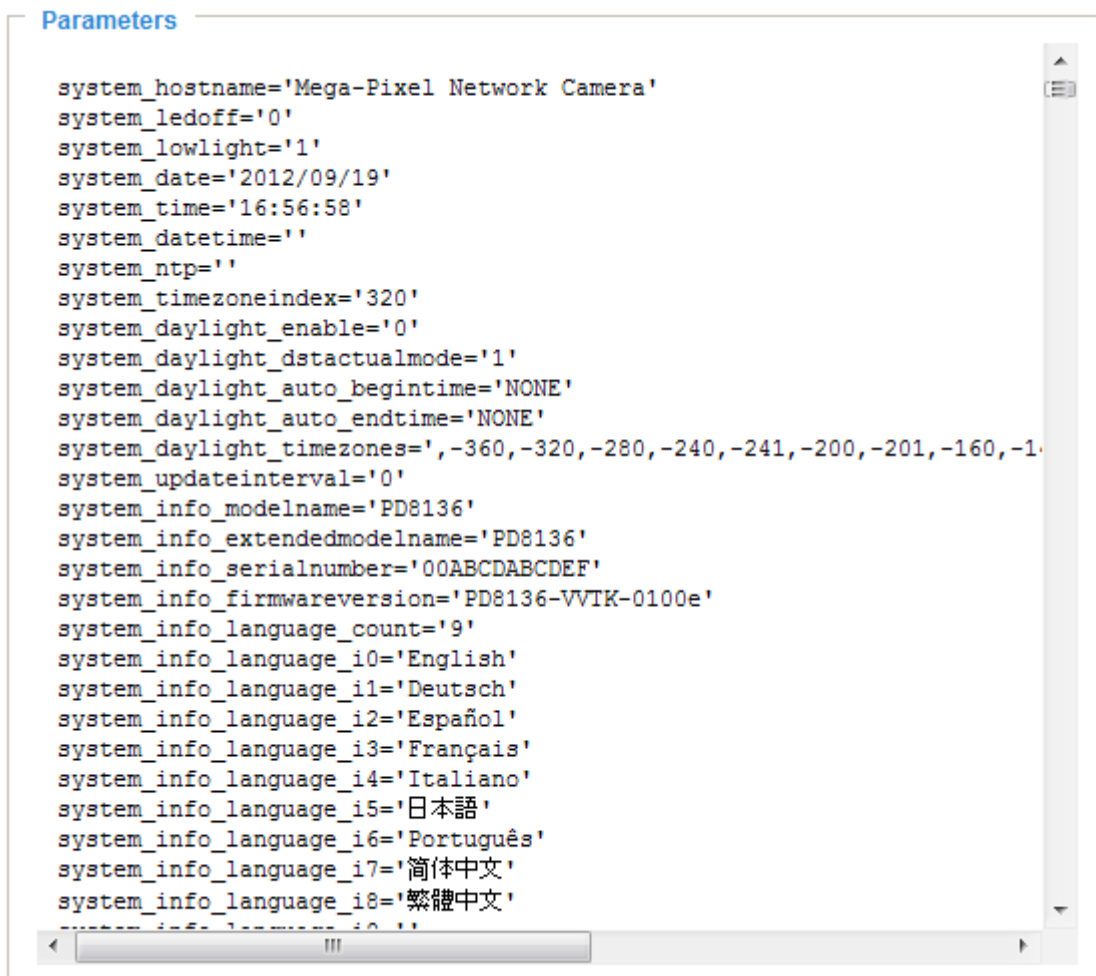
## Access log

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

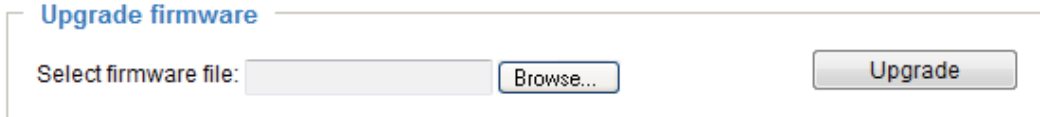
The View Parameters page lists the entire system's parameters in an alphabetical order. If you need technical assistance, please provide the information listed on this page.



## System > Maintenance

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

### General settings > Upgrade firmware



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

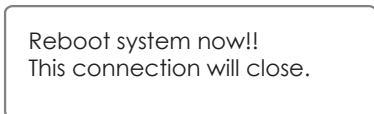
**Note: Do not power off the Network Camera during the upgrade!**

Follow the steps below to upgrade the firmware:

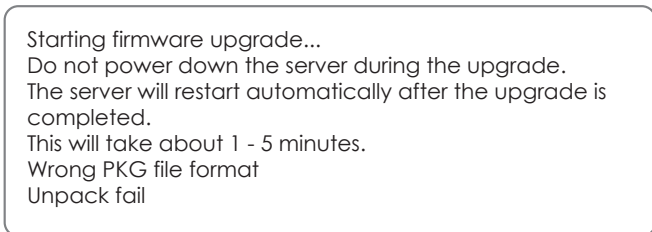
1. Download the latest firmware file from the VIVOTEK website. The file is in .pkg file format.
2. Click **Browse...** and specify the firmware file.
3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

If the upgrade is successful, you will see “Reboot system now!! This connection will close”. After that, refresh the management session with the Network Camera.

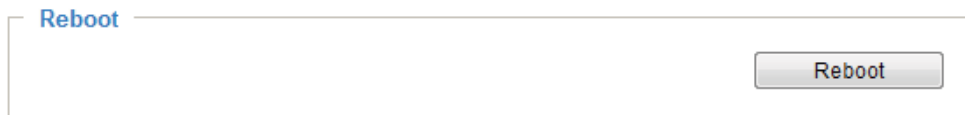
The following message is displayed when the upgrade has succeeded.



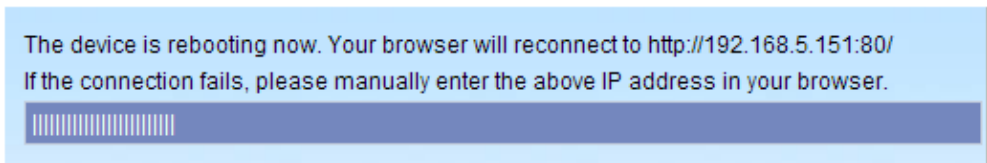
The following message is displayed when you have selected an incorrect firmware file.



### 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.



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

**Restore**

Restore all settings to factory default except settings in

Network
  Daylight saving time
  Custom language

This feature allows you to restore the Network Camera's factory defaults.

**Network:** Select this option to retain the Network Type settings (please refer to Network Type on page 51).

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

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

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

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

|||||||

## Import/Export files Advanced Mode

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

General settings
Import/Export files

**Export files**

Export daylight saving time configuration file	<input type="button" value="Export"/>
Export language file	<input type="button" value="Export"/>
Export configuration file	<input type="button" value="Export"/>
Export server status report	<input type="button" value="Export"/>

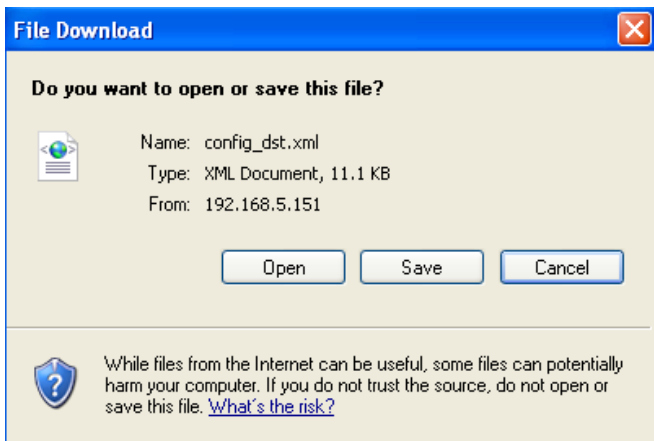
**Upload files**

Update daylight saving time rules:	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Upload"/>
Update custom language file:	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Upload"/>
Upload configuration file:	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Upload"/>

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

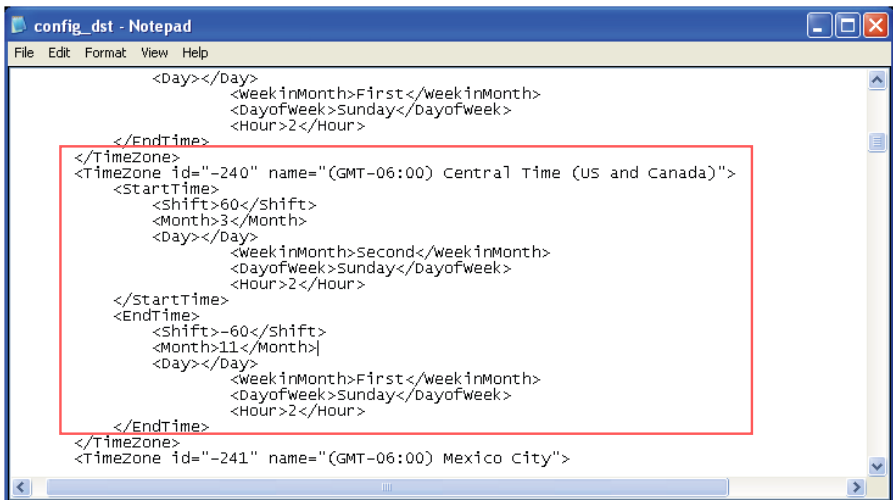
Follow the steps below to export:

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



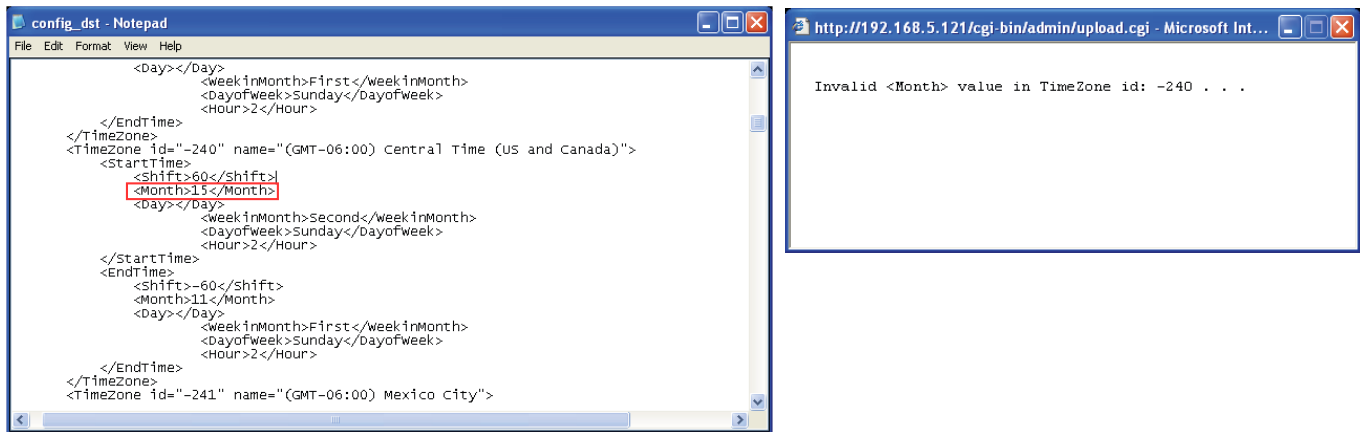
3. Open and edit the file using Microsoft® Notepad and locate your time zone in the strings; set the start and end time of DST. When completed, save the file.

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.

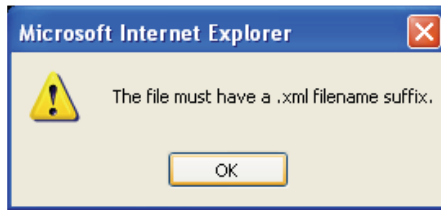


Update daylight saving time rules: Click **Browse...** and specify the XML file to update.

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, 簡體中文, 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.

Update configuration file: Click **Browse...** to update a configuration file. Please note that the model and firmware version of the device should be identical to those specified for 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.

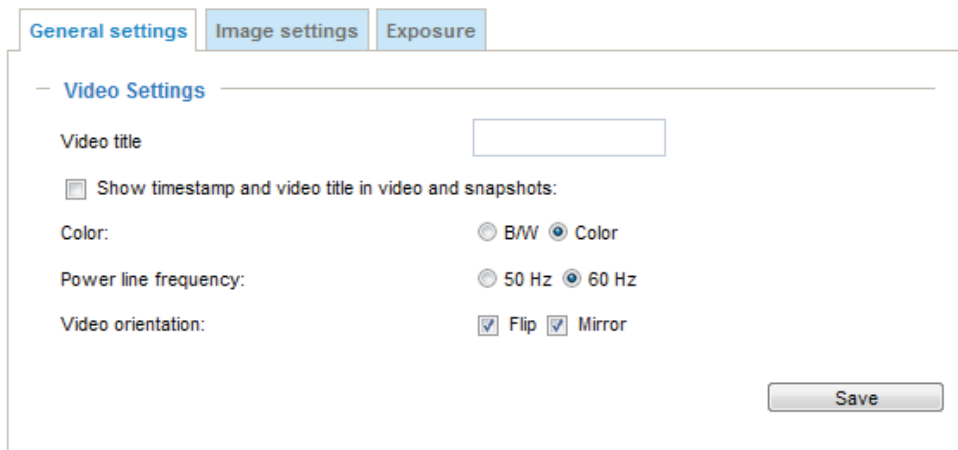
Export server status report: Click to export the current server status report, such as time, logs, parameters, process status, memory status, file system status, network status, kernel message..., and so on.



## 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

Show timestamp and video title in video and snapshots: 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.

Power line frequency: 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.

Video orientation: Flip - vertically reflect the display of the live video; Mirror - horizontally reflect the display of the live video. Change the settings if the Network Camera is installed in a different orientation to correct the image orientation. Please note that if you have preset locations, those locations will be cleared after a change in the flip/mirror setting.

## Image settings

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

Sensor Setting 1:  
For normal situations

Sensor Setting 2:  
For special situations

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

■ **Auto:** The Network Camera automatically adjusts the color temperature of the light in response to different light sources. The white balance setting defaults to **Auto** and works well in most situations.

### ■ Fix current value

Follow the steps below to manually set the white balance to compensate for the ambient lighting conditions.

1. Set the White balance to **Auto** and click **Save**.
2. Place a sheet of white paper in front of the lens, (or a color of cool color temperature, such as blue), click the **Off** button, then allow the Network Camera to adjust the color temperature automatically.
3. Click the **On** button on the Fix Current Value to confirm the setting while the white balance is being measured.
4. Click **Save** to enable the new setting.

### 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%.
- **Enable low light compensation:** When selected, the camera will provide electronic gains during low light conditions.

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.

— **Activated period** —

Enable and apply this profile to

Schedule mode

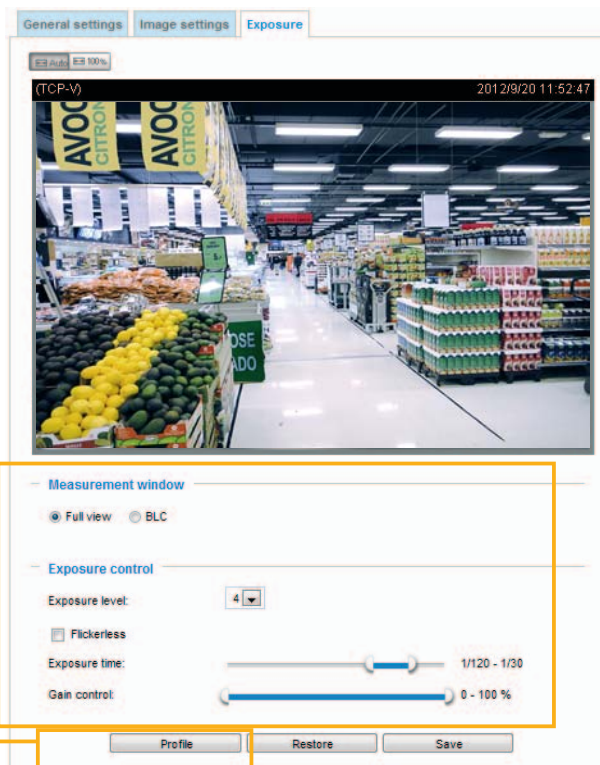
From  to  [hh:mm]

## Exposure Advanced Mode

On this page, you can set the Exposure level, Exposure time, and Gain control settings. Detailed configurations will be automatically adjusted since the sensor library will automatically adjust the value according to the ambient light.

Sensor Setting 1:  
For normal situations

Sensor Setting 2:  
For special situations



### Measurement window:

- Full view: Calculate the full range of view and offer appropriate light compensation.
- BLC (Back Light Compensation): This option will automatically add a “weighted region“ in the middle of the window and give the necessary light compensation. Camera firmware then adopts the weighted averages method to calculate the value and provides necessary light compensation.

### Exposure control:

- **Exposure level:** You can manually set the Exposure level, which ranges from 0 to 8 (dark to bright). You can also select other values from the Exposure mode menus and select a preferred scenario or manually configure the associated settings. You may prefer a shorter shutter time to better capture moving objects, while a faster shutter reduces light and needs to be compensated by electrical brightness gains.

- **Flickerless:** This function helps avoid the flickering on images because of the fast shutter movement. When selected, the exposure time will be forced to stay longer than 1/120 second.
- **Exposure time:** The Exposure time allows tuning for more or less light to enter the lens. The configurable value ranges from 1/32000 to 1/5 of a second. An optimum shutter speed should be maintained as long as the light level of the scene permits.
- **Gain control:** Tune the slider bar to set the Gain Control to the best image quality. Higher gain control value will generate a certain amount of noise, and that the gain control, lighting levels, and picture performance are closely related.

Note that you can split the round pointers on the **Exposure time** and **Gain control** slide bars into two halves and drag them on the bars to designate a range of values in which firmware can automatically adapt to. Firmware will then automatically tune the Gain control and Exposure time within the ranges you specified.

— **Exposure control** —

Exposure level:

Flickerless

Exposure time:

Gain control:

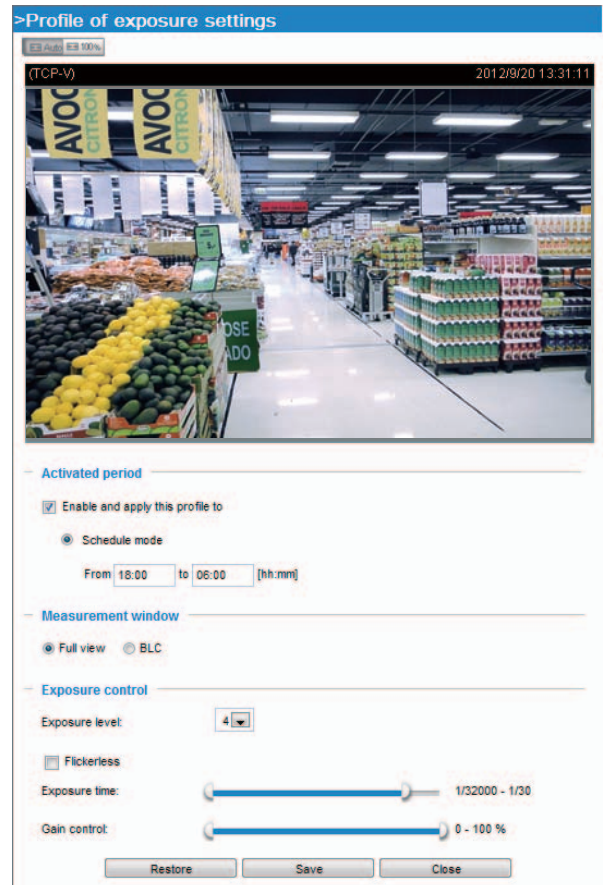
### Exposure Profile:

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

Activated period: You can select the Schedule mode to this profile. Please manually enter a range of time if you choose Schedule mode. Then check **Save** to take effect.

Please follow the steps below to set up a profile:

1. Select the **Enable and apply this profile to** checkbox.
2. Select the applicable period of time this profile will apply to.
3. Configure Exposure control settings in the following columns. Please refer to previous discussions for detailed information.
4. Click **Save** to enable the setting and click **Close** to exit the window.



## Media > Video Advanced Mode

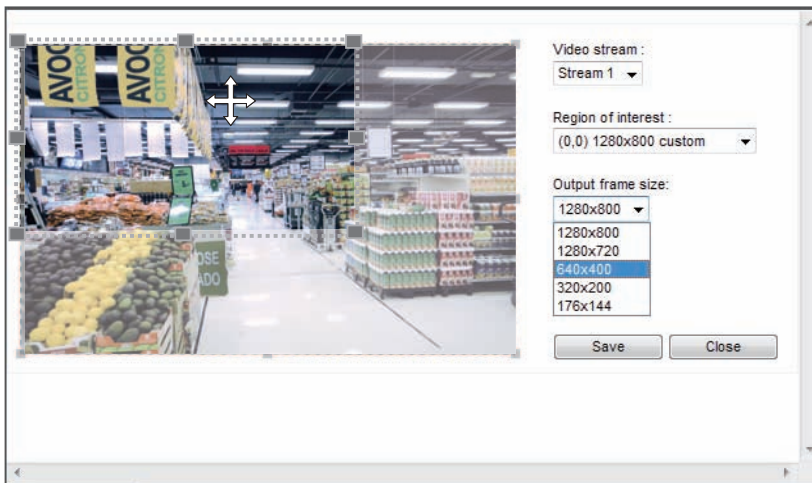
### Stream settings

**Stream settings**

- ▶ Video settings for stream 1 [Viewing Window](#)
- ▶ Video settings for stream 2

This Network Camera supports multiple streams with frame sizes ranging from 176 x 144 to 1280 x 800 pixels.

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 stream 1.



Please follow the steps below to set up those settings for stream #1:

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 Global 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.

The definition of multiple streams:

- Stream 1: Users can define the Frame sizes, compression format, image quality, etc. Only stream 1 supports Viewing Window configuration.
- Stream 2: The default frame size for stream 2 is also configured to 1280x800.

Click the stream item to display the detailed information. .

**Stream settings**

Video settings for stream 1 [Viewing Window](#)

MPEG-4  
 H.264

Frame size: 1280x800  
 Maximum frame rate: 30 fps  
 Intra frame period: 1 S

Video quality

Constant bit rate: 3 Mbps  
 Fixed quality: Good

JPEG

Video settings for stream 2

MPEG-4  
 H.264

Frame size: 1280x800  
 Maximum frame rate: 30 fps  
 Intra frame period: 1 S

Video quality

Constant bit rate: 3 Mbps  
 Fixed quality: Good

JPEG

Save

This Network Camera offers real-time H.264, MPEG-4, and MJPEG compression standards (Triple Codec) for real-time viewing. If the **H.264 / MPEG-4** mode is selected, the video is streamed via RTSP protocol. There are several parameters through which you can adjust the video performance:

MPEG-4  
 H.264

Frame size: 1280x800  
 Maximum frame rate: 30 fps  
 Intra frame period: 1 S

Video quality

Constant bit rate: 3 Mbps  
 Fixed quality: Good

JPEG

#### ■ 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.

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.

#### ■ Intra frame period

Determine how often for firmware 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, and 8Mbps. You can also select **Customize** and manually enter a value.
- Fixed quality: 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.



#### NOTE:

- ▶ *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 occurrence, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*




## Media > Audio **Advanced Mode**

### Audio Settings

**Audio settings**

Mute

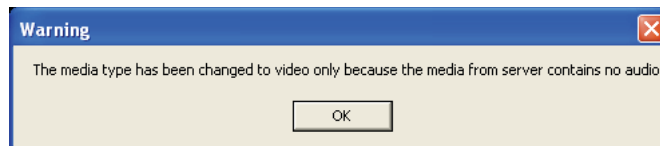
Internal microphone input gain: 

Audio type

G.711: pcmu ▾

Save...

**Mute:** 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:



**Internal microphone input gain:** Select the gain of the embedded audio input (microphone) according to ambient conditions. Adjust the gain by dragging pointer on the slide bar.

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

- G.711 also provides good sound quality and requires about 64Kbps. Select pcmu ( $\mu$ -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. Please remember to click on the **Save** button when you complete the Network setting.

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

Use fixed IP address: Select this option to manually assign a static IP address to the 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 14 for details.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP or network administrator.

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

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

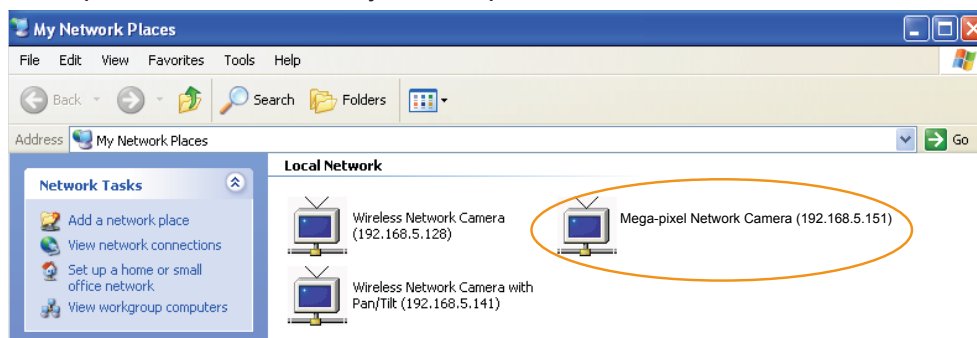
**Primary DNS:** The primary domain name server that translates host names into IP addresses.

**Secondary DNS:** Secondary domain name server that backs up the Primary DNS.

**Primary WINS server:** The primary WINS server that maintains the database of computer names and IP addresses.

**Secondary WINS server:** 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, the shortcuts to 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™ 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 104) to add a new email or FTP server.
3. Go to Configuration > Event > Event settings > Add media (please refer to Add media on page 109). 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.

**Network type**

LAN

PPPoE

User name:

Password:

Confirm password:

Enable IPv6

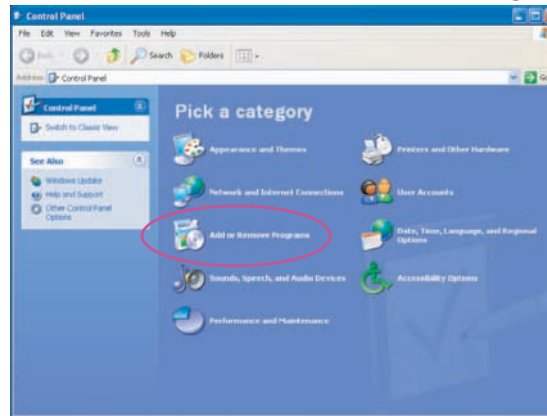
5. The Network Camera will reboot.

6. Disconnect the power to the Network Camera; remove it from the LAN environment.

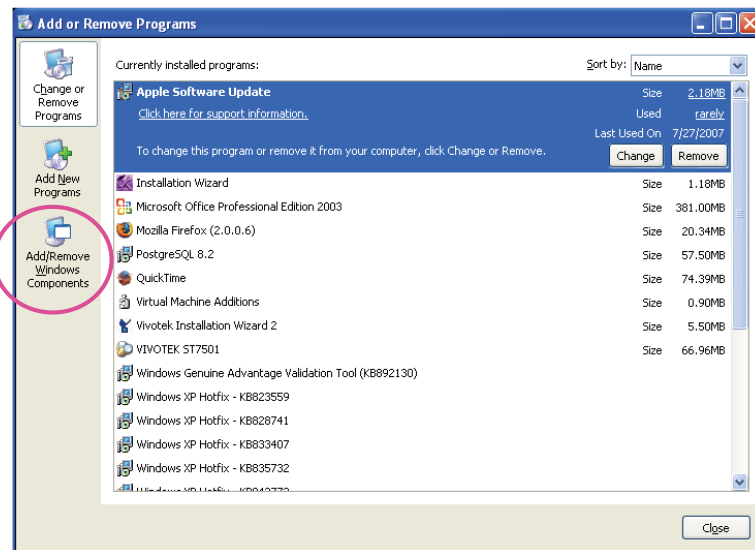
**NOTE:**

- ▶ 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™ 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™ user interface on your computer:  
Note that you must log on to the computer as a system administrator to install the UPnP™ components.

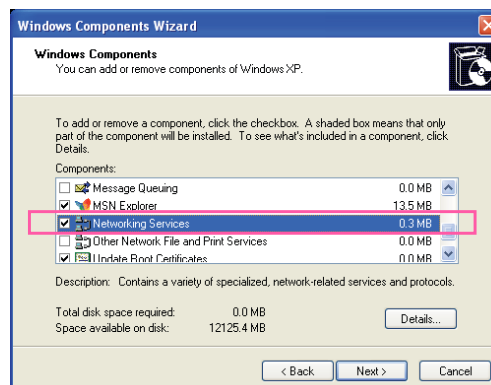
1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.



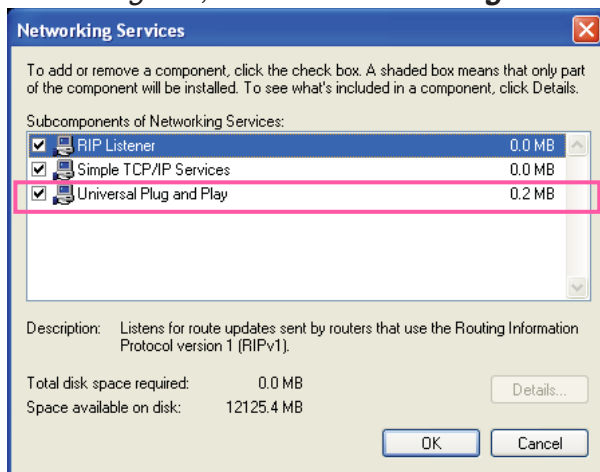
2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.



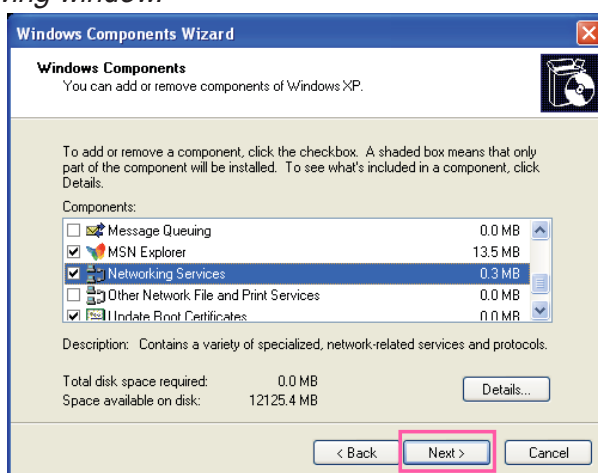
3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.



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™ is enabled.

- ▶ **How does UPnP™ work?**  
 UPnP™ 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 44 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® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.

**Network type**

LAN  
 PPPoE

User name:   
 Password:   
 Confirm password:

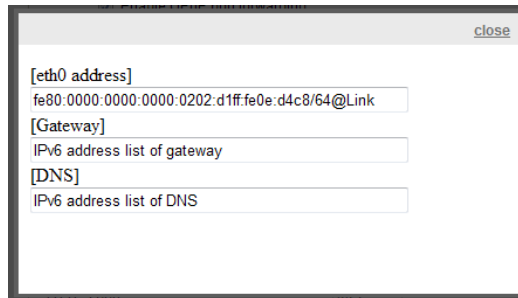
Enable IPv6

[IPv6 information](#)

Manually setup the IP address

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

[eth0 address]	
2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global	— Link-global IPv6 address/network mask
fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link	— Link-local IPv6 address/network mask
[Gateway]	
fe80::211:d8ff:fea2:1a2b	
[DNS]	
2010:05c0:978d::	

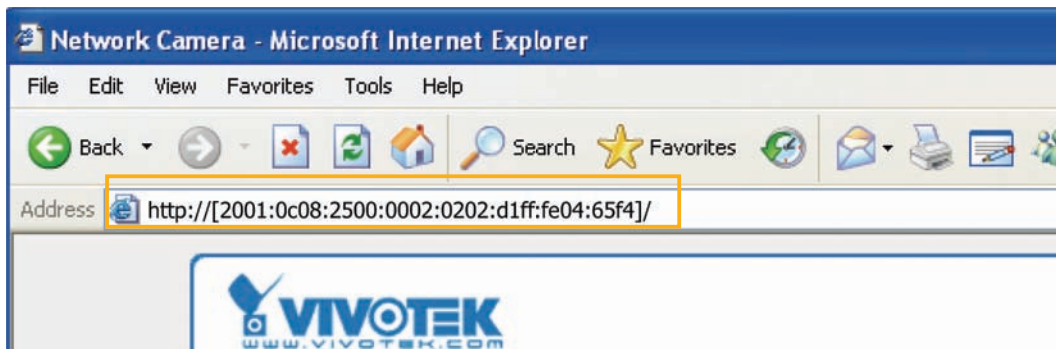
Please follow the steps below to link to an IPv6 address:

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

```

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

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



**NOTE:**

- ▶ If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to **HTTP** streaming on page 58 for detailed information.)

```

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

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

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

**Manually setup the IP address:** Select this option to manually configure 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 addressOptional IP address / Prefix length  / 64Optional default router Optional primary DNS **Port**

Network type	Port
HTTPS port:	<input type="text" value="443"/>
FTP port:	<input type="text" value="21"/>

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

FTP port: 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

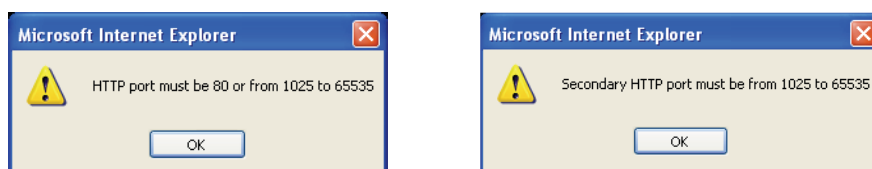
To utilize HTTP authentication, make sure that you have set a password for the Network Camera first; please refer to Security > User account on page 68 for details.

HTTP streaming	RTSP streaming
Authentication:	basic ▼
HTTP port:	80
Secondary HTTP port:	8080
Access name for stream 1:	video.mjpg
Access name for stream 2:	video2.mjpg

Authentication: 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.

On the LAN

http://192.168.4.160 or  
http://192.168.4.160:8080

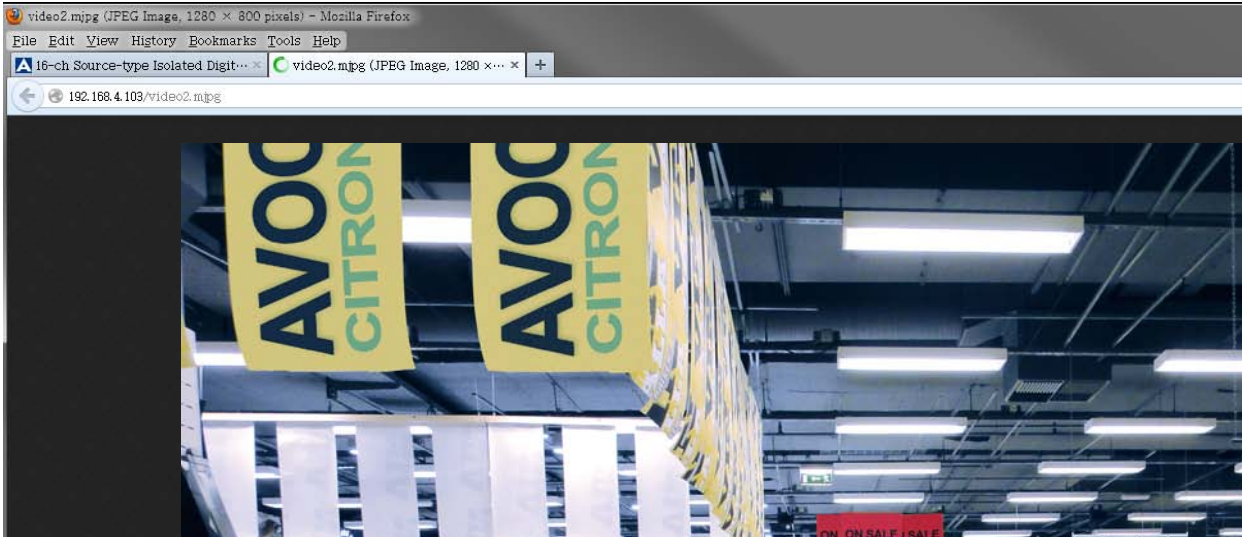
Access name for streams 1 ~ 2: This Network camera supports multiple streams simultaneously. The access name is used to identify different video streams. Users can click **Media > Video > Stream settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Stream settings on page 47.

When using **Mozilla Firefox** 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.

URL command -- [http://<ip address>:<http port>/<access name for stream 1 or 2>](#)

For example, when the Access name for stream 2 is set to [video2.mjpg](#):

1. Launch the Mozilla Firefox browser.
2. Type the above URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser. The precondition is that the source stream must be configured into the MJPG mode.



**NOTE:**

► *Microsoft® Internet Explorer does not support server push technology; therefore, using [http://<ip address>:<http port>/<access name for stream 1 or 2>](#) will not work.*

**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 68 for details.

HTTP streaming	RTSP streaming
Authentication: <input type="text" value="disable"/>	
Access name for stream 1: <input type="text" value="live.sdp"/>	
Access name for stream 2: <input type="text" value="live2.sdp"/>	
RTSP port: <input type="text" value="554"/>	
RTP port for video: <input type="text" value="5556"/>	
RTCP port for video: <input type="text" value="5557"/>	
RTP port for audio: <input type="text" value="5558"/>	
RTCP port for audio: <input type="text" value="5559"/>	
▶ Multicast settings for stream 1	
▶ Multicast settings for stream 2	
<input type="button" value="Save"/>	

**Authentication:** 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 below:

	Quick Time player	VLC
Disable	O	O
Basic	O	O
Digest	O	X

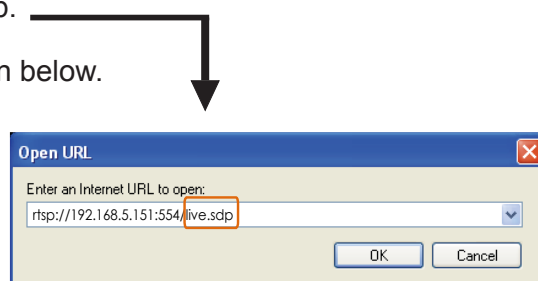
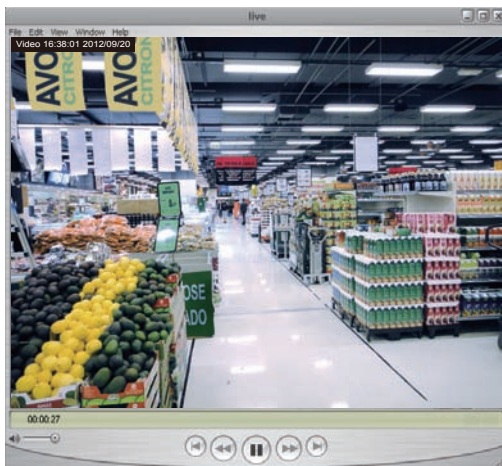
**Access name for stream 1 ~ 2:** This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.

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 2>`

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.

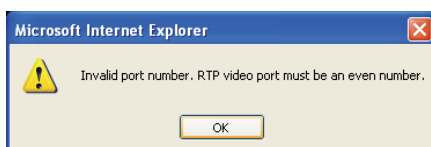


RTSP port / RTP port for video, audio / RTCP port for video, audio

- 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:



Multicast settings for streams 1 and 2: Click the items to display the detailed configuration information. Select the Always multicast option to enable cast for video streams.

▼ Multicast settings for stream 1

Always multicast

Multicast group address:

Multicast video port:

Multicast RTCP video port:

Multicast audio port:

Multicast RTCP audio port:

Multicast TTL [1~255]:

▼ Multicast settings for stream 2

Always multicast

Multicast group address:

Multicast video port:

Multicast RTCP video port:

Multicast audio port:

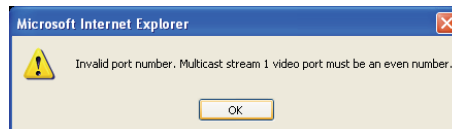
Multicast RTCP audio port:

Multicast TTL [1~255]:

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 bandwidth.

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:



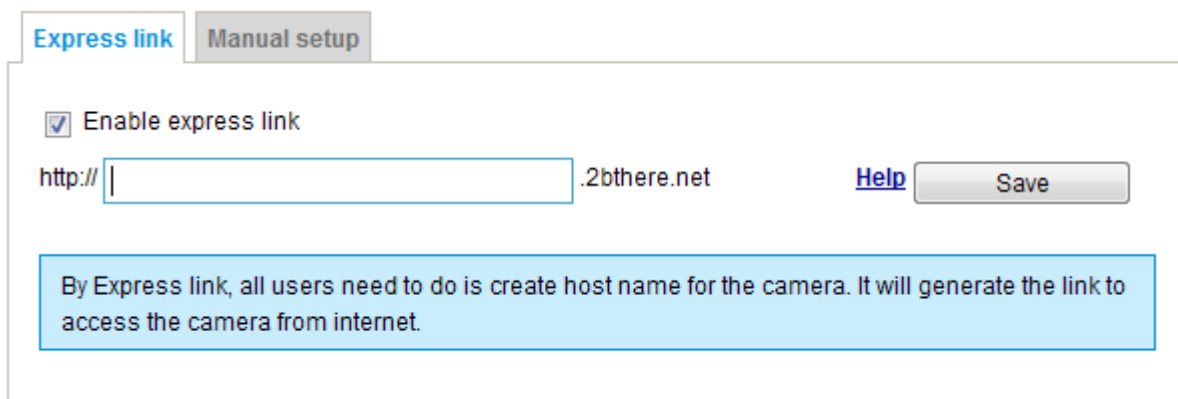
Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

## 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 examine if the host name is valid and automatically open a port on your router. If using DDNS, the user has to manually configure UPnP port forwarding. Express Link is more convenient and easier to set up.



**Express link** Manual setup

Enable express link

http://  .2bthere.net [Help](#)

By Express link, all users need to do is create host name for the camera. It will generate the link to access the camera from internet.

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 prompt. If the host name is valid, it will display a message as shown below.

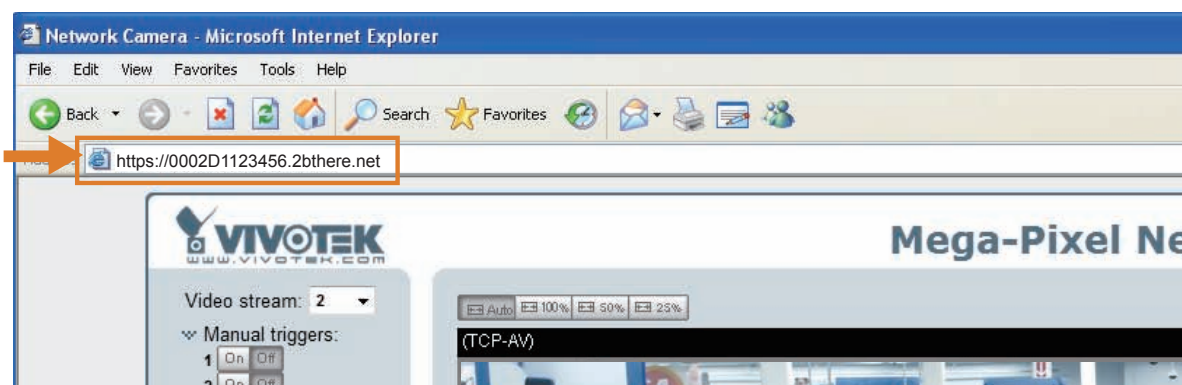


**Express link** Manual setup

Enable express link

http:// 0002D1123456 .2bthere.net [Help](#)

The camera can now be accessed at <http://0002D1123456.2bthere.net>



## Manual setup

### DDNS: Dynamic domain name service

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

**Provider:** Select a DDNS provider from the provider drop-down list.

VIVOTEK offers **Safe100.net**, a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's 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.

**DDNS: Dynamic domain name service**

Enable DDNS:

Provider:

Host name:  [\*.safe100.net]

Email:

Key:

---

**Register**

Host name:

Email:

Key:

Confirm key:

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

DDNS Registration Result:

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

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

#### ■ CustomSafe100

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

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

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

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

- [Dyndns.org\(Dynamic\) / Dyndns.org\(Custom\)](http://www.dyndns.org/): visit <http://www.dyndns.com/>
- [TZO.com](http://www.tzo.com/): visit <http://www.tzo.com/>
- [DHS.org](http://www.dns.org/): visit <http://www.dns.org/>
- [dyn-interfree.it](http://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 via a web console with the network switches, which then use different queuing disciplines to forward the packets.

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

**CoS**

Enable CoS

VLAN ID:	<input style="width: 60px;" type="text" value="1"/>
Live video:	<input style="width: 40px;" type="text" value="0"/> ▼
Live audio:	<input style="width: 40px;" type="text" value="0"/> ▼
Event/Alarm:	<input style="width: 40px;" type="text" value="0"/> ▼
Management:	<input style="width: 40px;" type="text" value="0"/> ▼

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



#### NOTE:

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

#### QoS/DSCP

Enable QoS/DSCP

Live video:	<input type="text" value="0"/>
Live audio:	<input type="text" value="0"/>
Event/Alarm:	<input type="text" value="0"/>
Management:	<input type="text" value="0"/>

## 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 SNMPv1, SNMPv2c

**SNMPv1, SNMPv2c Settings**

Read/Write community:

Read only community:

#### 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).

Enable SNMPv3

**SNMPv3 Settings**

Read/Write Security name:

Authentication Type:

Authentication Password:

Encryption Password:

Read only Security name:

Authentication Type:

Authentication Password:

Encryption Password:

## 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 prompt for authentication; type the correct user’s name and password in their respective fields to access the Network Camera.

### Privilege management **Advanced Mode**

**PTZ control:** You can modify the manage privileges of 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 29).

**Allow anonymous viewing:** If this checkbox is selected, any client can access the live stream without entering a User ID and Password.

### Account management

Administrators can add up to 20 user accounts.

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

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Although operators cannot access the Configuration page, they can use the URL Commands to get and set the camera parameters. For more information, please refer to URL Commands of the Network Camera at the Appendix of this manual. Viewers access only the main page for live viewing.

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

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

## 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.

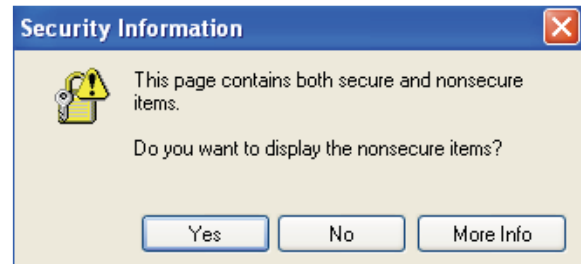
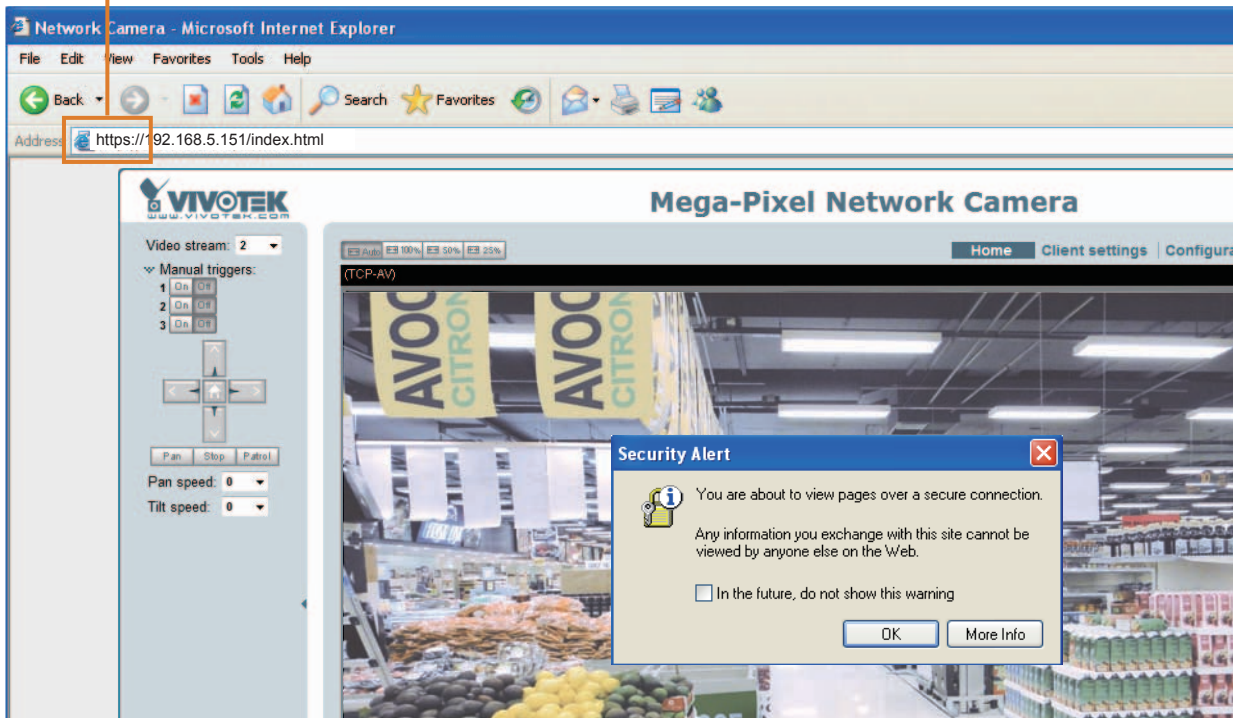
The screenshot shows the 'HTTPS' configuration page. The 'Enable HTTPS secure connection' checkbox is checked. Under 'Mode', 'HTTP & HTTPS' is selected. Under 'Certificate', the 'Create self-signed certificate' method is chosen. The 'Certificate information' section is expanded, showing fields for Country (TW), State or province (Asia), Locality (Asia), Organization (VIVOTEK.Inc), Organization unit (VIVOTEK.Inc), Common name (www.vivotek.com), and Validity (3650 days). A blue progress bar with the text 'Please wait while the certificate is being generated...' is visible. The 'Create certificate' button is highlighted with an orange border.

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

The screenshot shows the 'Certificate information' panel. The status is 'Active'. The method is 'Create self-signed certificate'. The fields for Country (TW), State or province (Asia), Locality (Asia), Organization (VIVOTEK.Inc), Organization unit (VIVOTEK.Inc), and Common name (www.vivotek.com) are displayed. At the bottom, there is a link for 'Certificate properties' and a 'Remove certificate' button.

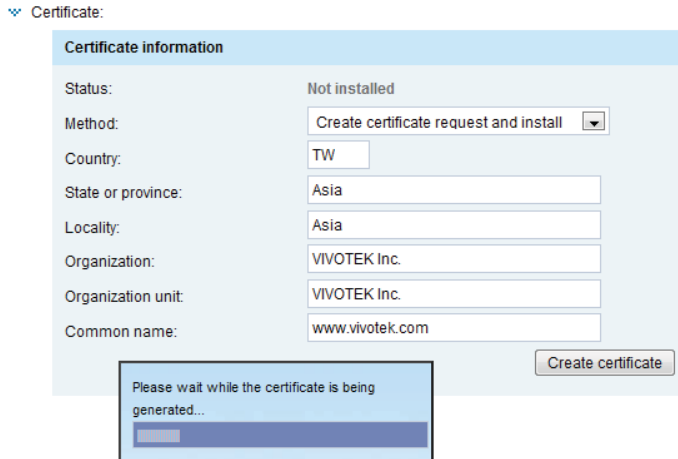
5. Click **Save** to preserve your configuration, and your current session with the camera will change to the encrypted connection.
6. If your web session does not automatically change to an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from “<http://>” to “<https://>” in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.

**https://**

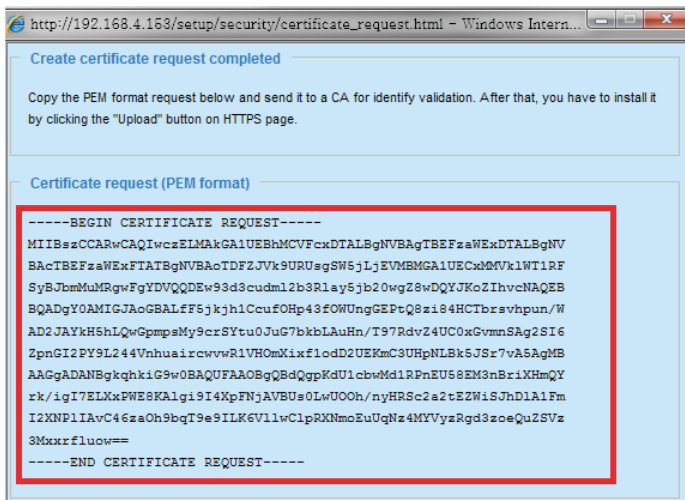


### Create certificate request and install

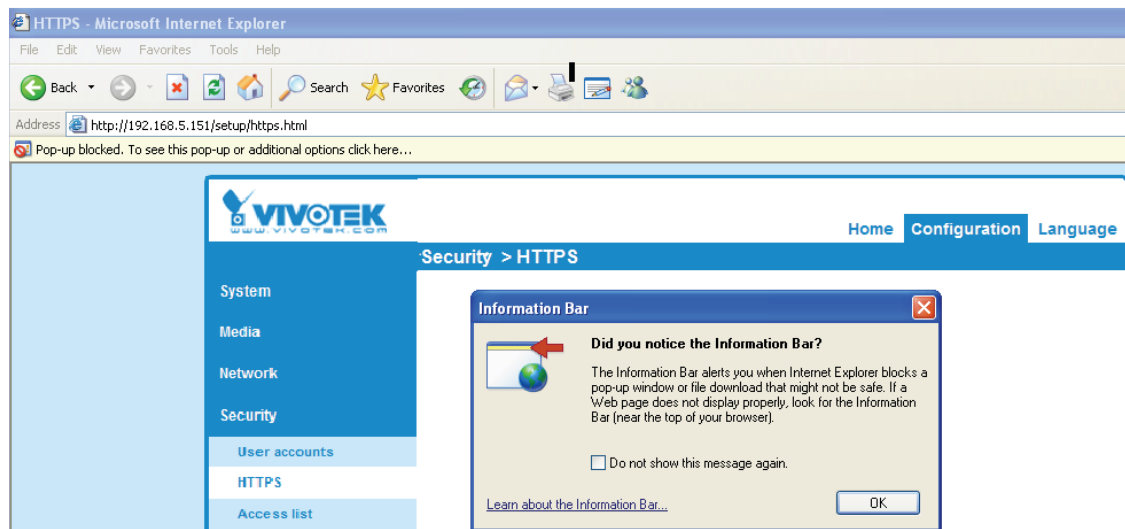
1. Select the option from the **Method** pull-down menu.
2. Click **Create certificate** to proceed.
3. The following information will show up in a pop-up window after clicking **Create**. Then click **Save** to generate the certificate request.



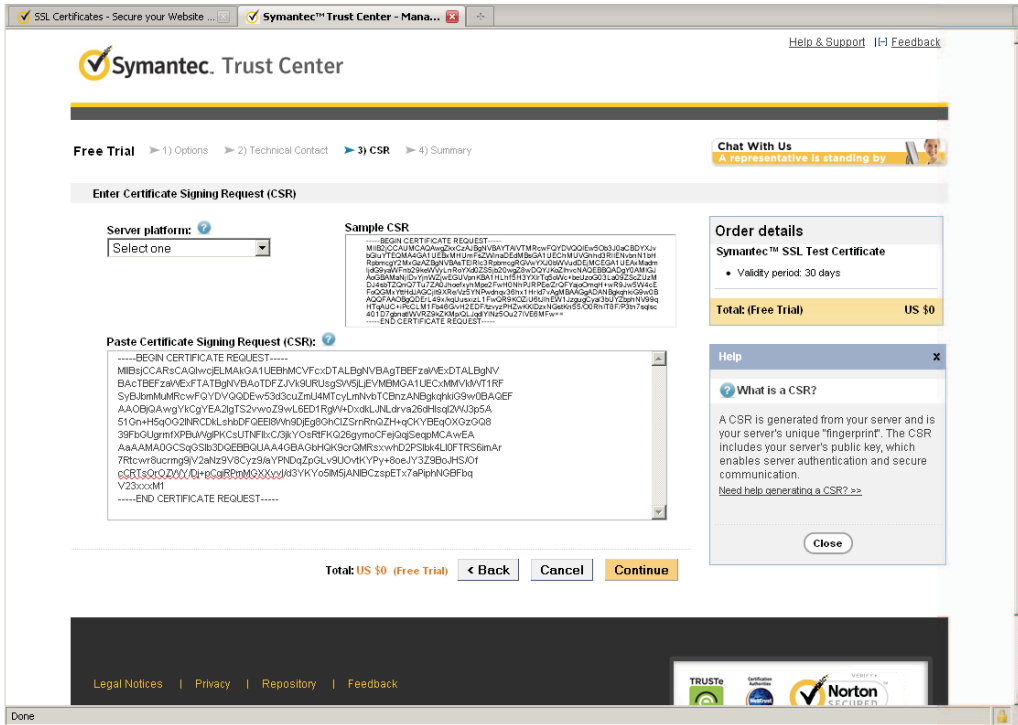
4. The Certificate request window will prompt.



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.



5. Look for a trusted certificate authority, such as Symantec’s VeriSign Authentication Services, that issues digital certificates. Sign in and purchase the SSL certification service. Copy the certificate request from your request prompt and paste it in the CA’s signing request window. Proceed with the rest of the process as CA’s instructions on their webpage.



6. Once completed, your SSL certificate should be delivered to you via an email or other means. Copy the contents of the certificate in the email and paste it in a text/HTML/hex editor/converter, such as IDM Computer Solutions’ UltraEdit.

```

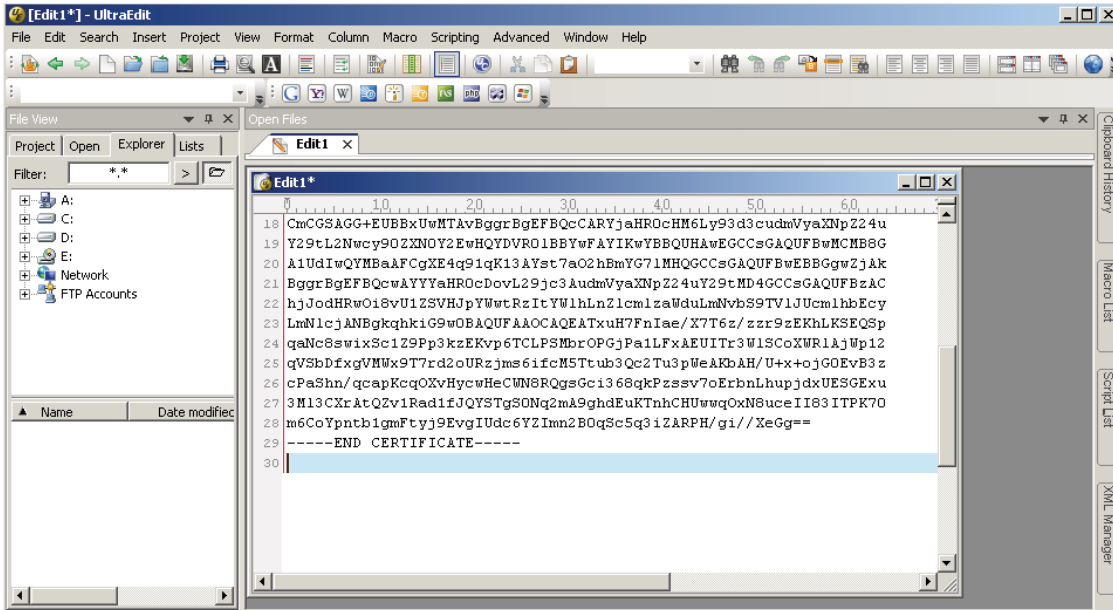
immediately, please dial 866.893.6565 or 650.426.5112 option 3 or send an email to internet-sales@verisign.com

Thank you for your interest in Symantec!

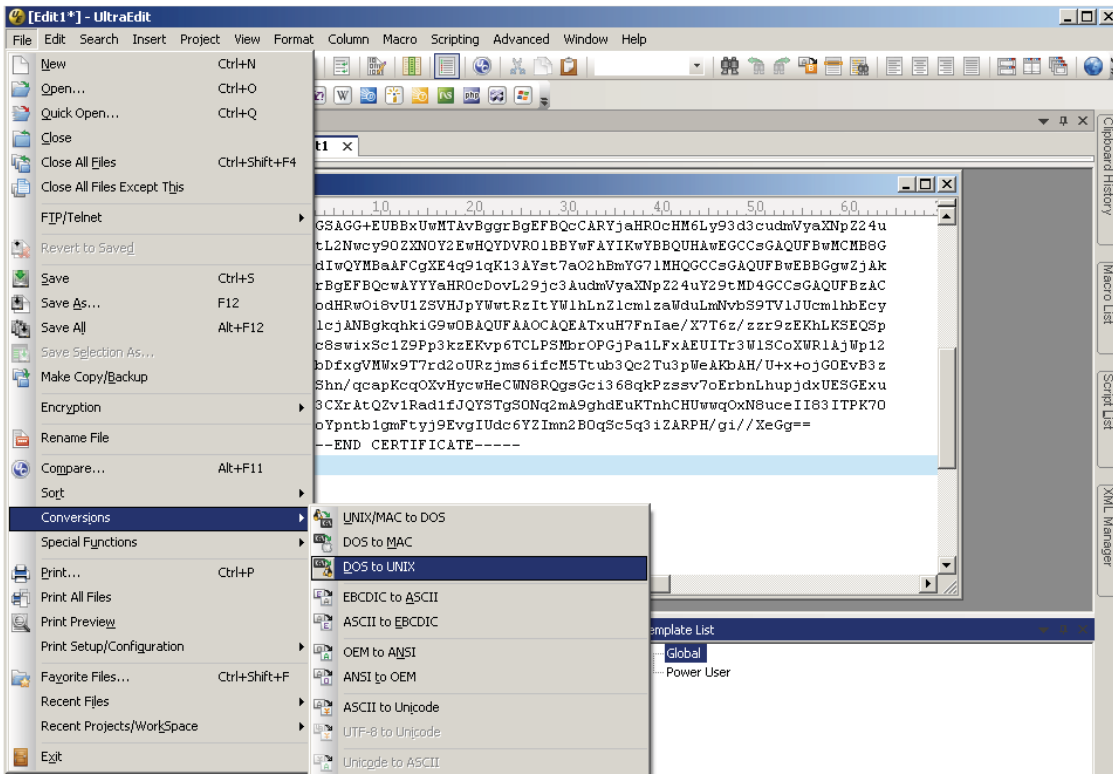
-----BEGIN CERTIFICATE-----
MIIFBDCCA+ygAwIBAgIQFxlCahn/SeBS1t0WQDOBIzANBgkqhkiG9w0BAQUFADCB
yzEIMAAkGA1UEBHMCMVVMxZzAvVjBkaWVBAoTDIzLm1tZWduLmVBAQIBAQIBAQIB
EydGbz3IgdGVzZCBQdXJwb3N1cyBFBm5LiAgTm8gYXNzdKXJhbmN1cy4xQjBAGgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovLj3d3dy52Zkxpc21nb15jb20vY3Bz
L3Rlc3RjYSAoYykwOTFtMCA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1
cnZlciBDQSA1IEcyMB4XDTExMDcwMzAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
CzAubG9uVBA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1
VQKFAxNSVzPVEVLE1uY4xFTATBGNVBAoUDFZJVk9URUg5W5jLjE6MDgGA1UE
CxqxVGVybXMgb2YgdXN1IGF0IHd3dy52Zkxpc21nb15jb20vY3BzL3Rlc3RjYSAo
YykwNTExMCA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1
g0RMIIGJABGABBI1E0tr8KGFc+hA9UYFvg8XZCYTs3a72unRyLkPd1d6eQ0dR
p/h+ajhtpUqG5C7IwaxUBBcFp/Q4xIPBoQpWUg5020Rg/qqimARKjlxskxkEN/R
Wx1IK5n1zwb1cDygrFEzRSCMq945SGdrEbRSknUoMpqhXo0Ko0noqTAgMBAAGj
ggGRMIIBFTAZBGNVHREEEjAqgg53d3cu2m4MTcyLmVBAQIBAQIBAQIBAQIBAQIBAQ
A1UdDwEB/wQEAwIFoDBDBGNVHREEDPA6MD1gNgA0hJodHRwOi8vU1ZSVHJpYwtr
RzItY3JlLnZlcm1zaWduLmVBAQIBAQIBAQIBAQIBAQIBAQIBAQIBAQIBAQIBAQIB
CmCGSAGG+EUBBxUwMTAvBggzBgEFAQ1UEA1UEA1UEA1UEA1UEA1UEA1UEA1UEA1
Y29tL2Nwcy90ZXN0Y2EwHQDYDVR01BBYwFAYIKwYBBQUHAwEGCCAGAUFBwMCMBAQ
A1UdIwYMBaAFcG4e4q91qK13AYst7a02BmYg71MHQGCCAGAUFBwEBBGGwZjAk
BggrBgEFBQcwAYYHR0cDovL29jczAudmVyaXNpc2Z4Y29tMD4GCCAGAUFBzAC
hJodHRwOi8vU1ZSVHJpYwtrRzItYw1hLnZlcm1zaWduLmVBAQIBAQIBAQIBAQIB
LmN1cyBkqhkiG9w0BAQUFAQAOCQAERTxuH7FnIae/X7I6z/zr9zEKhLKSEQSp
qaNc8sw1xSc129Fp3kzEkVp6TCLP5MbrOPGjPa1LfxAEUITr3WL5CoXWR1ajWp12
qV5bDFxgVMWx9T7rd2oUrzms61fMSTtub3Qc2Tu3PwEAKdAH/U+X+oJG0EvB3z
cPaShn/qcapKcOxYhycwHeCWN8RQqsGc1368qPzssv7oErbnLhupjdxUESGEXu
3M13CXrAtQ2v1Rad1fJQYSTg50Nq2mAg9hdEuKtNhCHUWwqOxN8uceII83ITP70
m6CoYpntb1gmFtyj9EvgYUdc6YZImn2B0qS5c53i2ARPH/gi//XeGg==
-----END CERTIFICATE-----

```

- Open a new edit, paste the certificate contents, and press ENTER at the end of the contents to add an empty line.

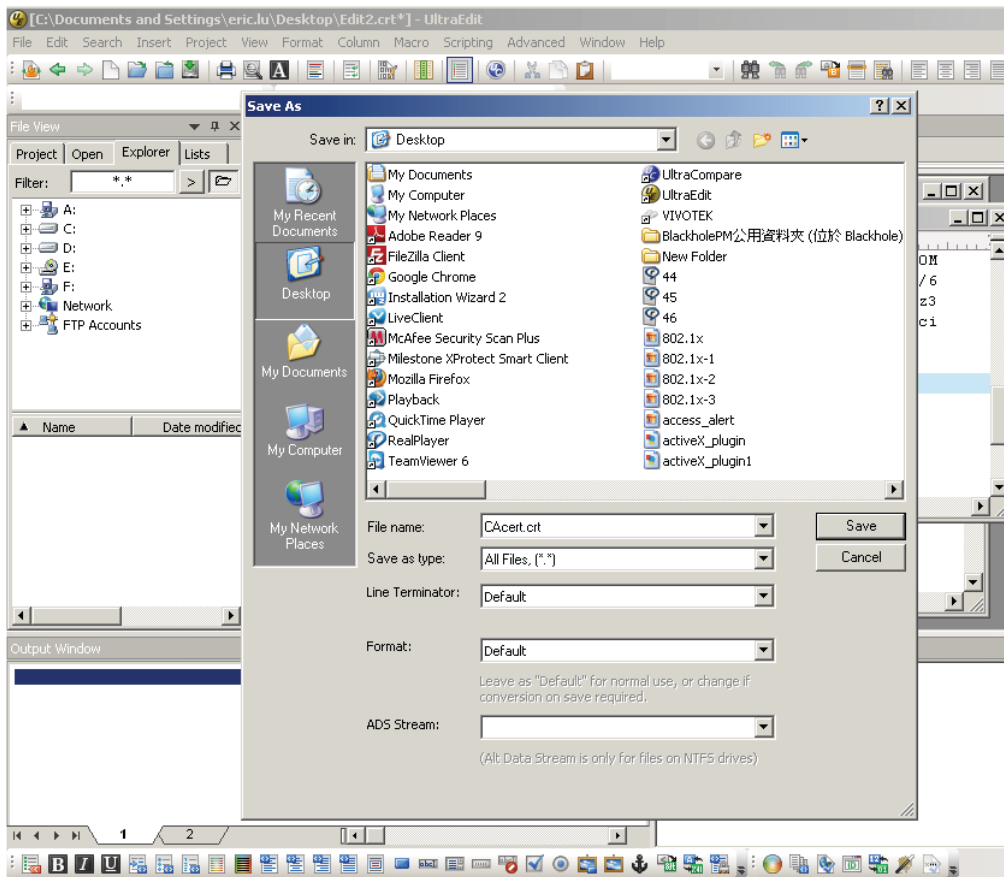


- Convert file format from DOS to UNIX. Open File menu > Conversions > DOS to Unix.

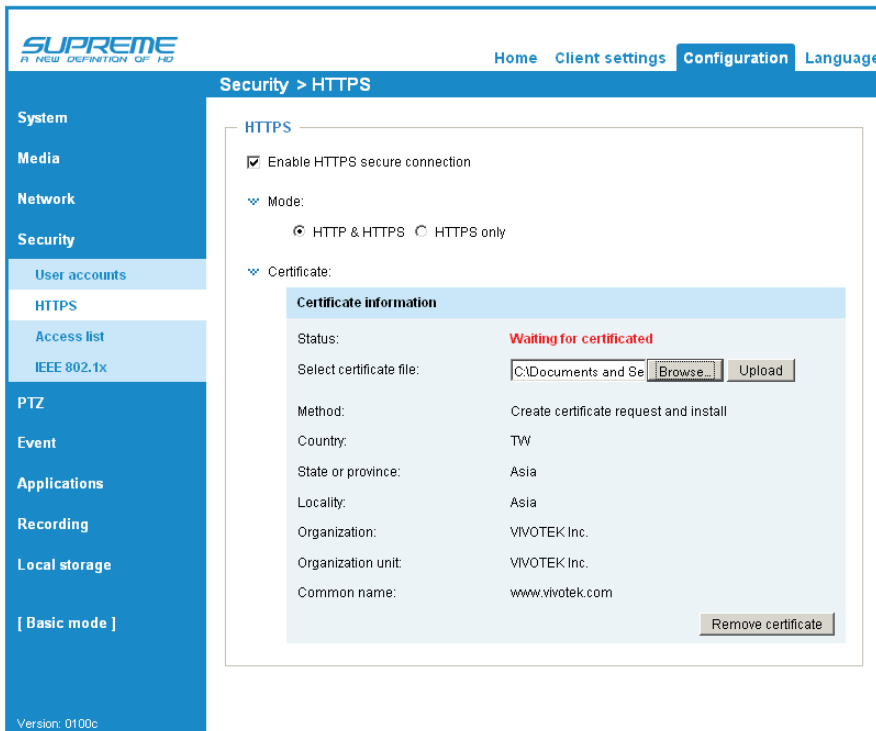




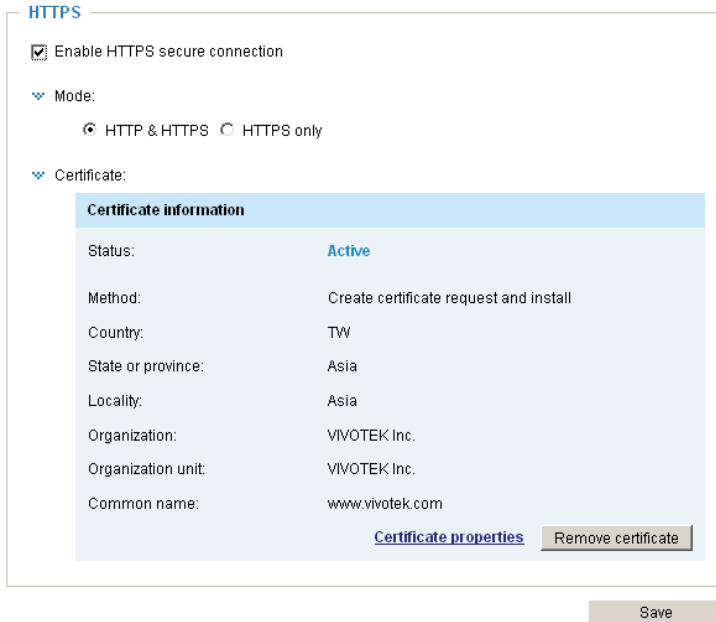
9. Save the edit using the “.crt” extension, using a file name like “CAcert.crt.”



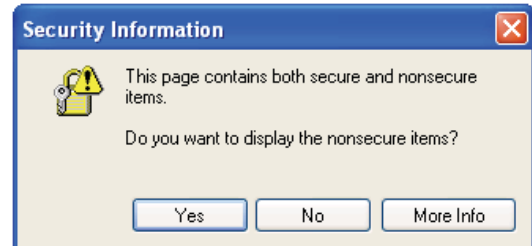
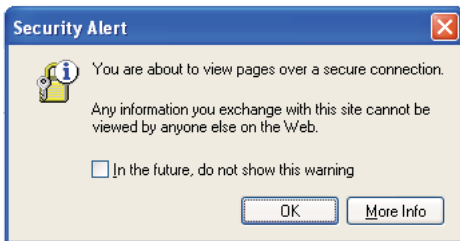
10. Return to the original firmware session, use the **Browse** button to locate the crt certificate file, and click **Upload** to enable the certification.



11. When the certificate file is successfully loaded, its status will be stated as **Active**. Note that a certificate must have been created and installed before you can click on the **“Save”** button for the configuration to take effect.



12. To begin an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from **“http://”** to **“https://”** in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.



## Security > Access List Advanced Mode

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

### General Settings

**General settings**

Maximum number of concurrent streaming:  Connection management

Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including all streams). 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).

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

	IP address	Elapsed time	User ID
<input type="checkbox"/>	192.168.1.147	12:20:34	root
<input type="checkbox"/>	61.22.15.3	00:10:09	
<input type="checkbox"/>	192.168.3.25	45:00:34	greg

- IP address: Current connections to the Network Camera.
- Elapsed time: How long the client has been at the live view webpage (note that only clients currently at the live view window will be listed here).
- 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 make a connection without a user name and password, the User ID column will be empty.

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

1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security > User account on page 68.
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 59.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing**, please refer to page 68.

- 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 their access. Please note that those checked connections will only be disconnected temporarily and they will automatically retry a connection (IE Explorer 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 they will automatically retry a connection (IE Explorer or Quick Time Player).

## Filter

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

**Filter type:** Select **Allow** or **Deny** as the filter type. If you choose **Allow Type**, only those clients whose IP addresses are on the Access List below can access the Network Camera, and exclude the access from those that are not on the list. 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, while those that are not on the list can.

**Filter**

Filter type:  Allow  Deny

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 > Enable IPv6 on page 55 for detailed information.

**IPv4 access list**

**IPv6 access list**

There are three types of rules:

**Single:** This rule allows the user to add an IP address to the Allowed/Denied list.

For example:

> Add ipv4 filter list

**Filter address**

Rule:  ▼

IP address:

**Network:** This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List in the CIDR format, e.g. 192.168.xx.xx/24.  
 For example:

**Filter address**

Rule: Network

Network address / Network mask: 192.168.2.0 / 24

OK Cancel

IP address 192.168.2.x will be blocked.

In an IPv6 filter list, the subnet mask is replaced by a prefix length.

**>Add ipv6 filter list**

**Filter address**

Rule: Network

Network address / Network mask: /

OK Cancel

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

**Filter address**

Rule: Range

IP address - IP address: 192.168.2.0 - 192.168.2.255

OK Cancel

**Administrator IP address**

**Always allow the IP address to access this device:** 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.

**Administrator IP address**

Always allow the IP address to access this device

Save

## 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 have their 802.1x settings enabled.

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., network administrator of your company) which can be validated by a RADIUS server.
2. 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).

**IEEE 802.1x**

Enable IEEE 802.1x

EAP method: EAP-PEAP ▼

Identity:

Password:

CA certificate:

Status: no file

**IEEE 802.1x**

Enable 802.1x

EAP method: EAP-TLS ▾

Identity:

Private key password:

CA certificate:  Browse... Upload

Status: no file Remove

client certificate:  Browse... Upload

Status: no file Remove

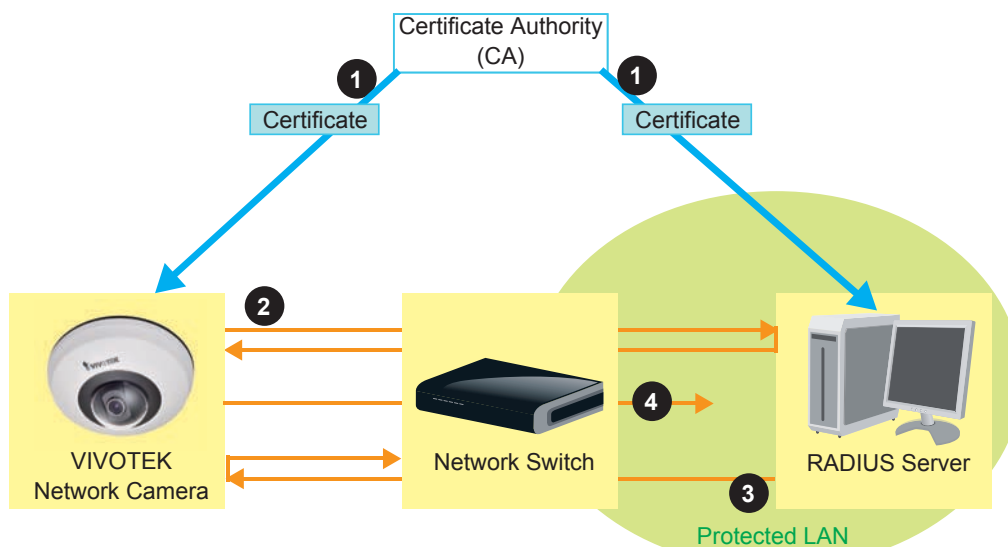
Client private key:  Browse... Upload

Status: no file Remove

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.

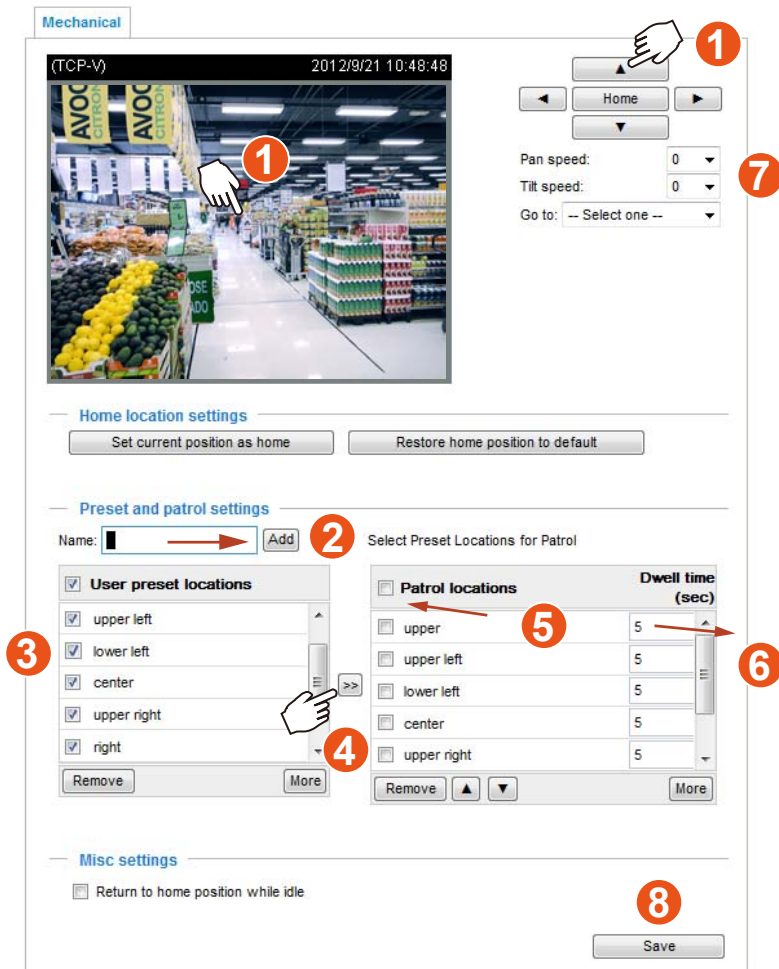
 **NOTE:**

- Below is 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. The camera comes with built-in PTZ mechanisms.



### Preset positions and patrol settings

In the PTZ settings page, you can select preset positions for the camera to patrol. A total of 20 preset positions can be configured.

Please follow the steps below to configure preset positions and arrange them in a pan/tilt/zoom tour:

1. Adjust the shooting area to the desired position using the keypad on the upper right side of the window. The default **Home** position refers to the center position defaulted in the factory. You might as well select another area of interest as the "Home" position. You should also select the speeds for the actions that occur during the patrol; i.e., pan and tilt speeds.
2. Enter a name for a new preset position, which can contain up to forty characters. Click **Add** to enable the settings. The preset positions will be listed on the **User preset locations**. (To add positions you wish, please repeat steps 1~2.)
3. Select the preset positions and click on the **Save** button at the bottom of the screen.
4. Click on the move button (>>) >> to move positions to the Patrol locations window.
5. You may select some or all of the imported positions as the stop points during the tour.
6. Enter a preferred dwell time before moving to the next position.
7. Select a **speed** level for the **auto patrol tour**.
8. Click on the **Save** button to preserve your configuration.

To remove a preset position from the list, select it and click **Remove**.

You can re-arrange the patrol order of the positions on the list using the   buttons.



**Misc. settings:** Use the checkboxes and the pull-down menus for the camera to automatically return to the home position after the camera has stayed idle for a period of time.

**Misc settings**

Return to home position while idle

Time span for idle duration:  (1~999) seconds

**Time span for idle duration: \_\_ (1~999) seconds:** You can assign an action to be taken when the camera sits idle for a configurable period time. You can let the camera return to the home position. The idle state does not include the situations when the camera is performing pan or patrol action.

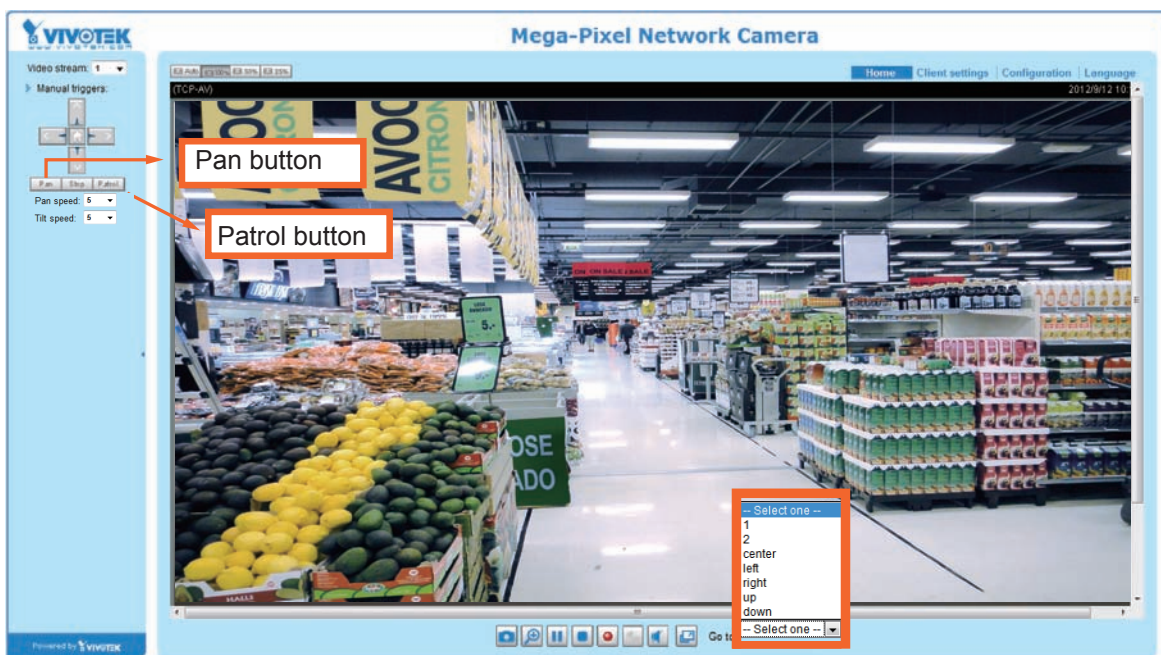
Note that if your screen control malfunctions, it is possible that the CPU of your current view station can not cope with the HD video feeds or that an incompatibility issue occurred with the ActiveX control plug-ins.

The **Zoom factor display:** This option is enabled by default, and zoom ratio is displayed along with the video title on the upper left corner of a view cell.

### Positions on the Home page

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 position.

**Patrol button:** Click this button, then the Network Camera will patrol among the selected positions for one time.



**PTZ > Calibrate**

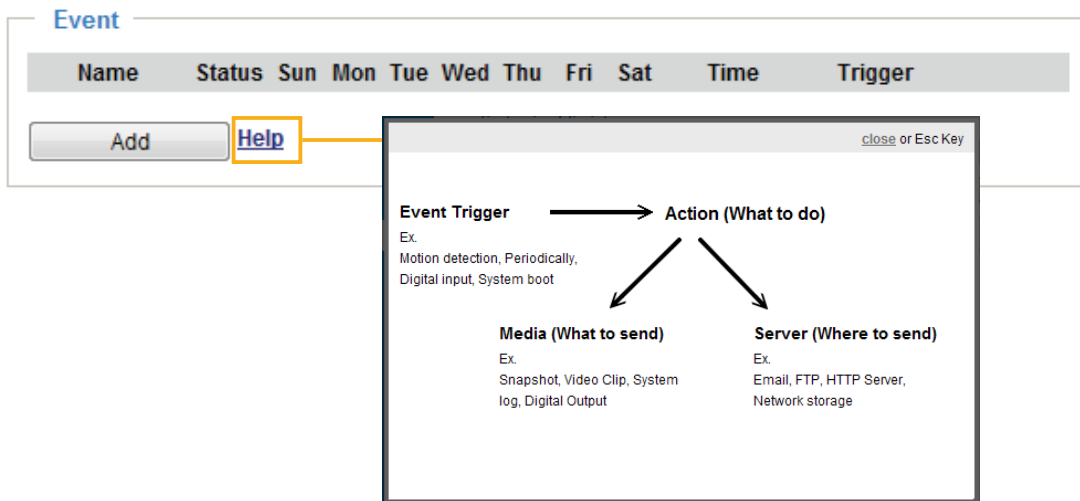
This function re-calibrates the home position to the default center to recover any displacement caused by external forces. Please note that there is no confirm message after using the function, and the calibration immediately takes place. If, after a long use, a user finds it is difficult to move camera's field of view to a specific point, use this function to restore the camera's original coordinates in pan and tilt motions.

**PTZ > Calibrate****Calibrate**

Recalibrate the home position to the default center to recover the tolerance caused by some external forces.

## 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 will be performed.



### Event

An event is an action initiated by a user-defined trigger source. In the **Event** column, click **Add** to open the event settings window.

The screenshot shows the 'Event settings' window. At the top is a table with columns: Name, Status, Sun, Mon, Tue, Wed, Thu, Fri, Sat, Time, and Trigger. Below the table are 'Add' and 'Help' buttons. The main area contains the following fields:

- Event name:
- Enable this event
- Priority:
- Detect next motion detection or digital input after  second(s).

**Event schedule**

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Time**

Always

From  to  [hh:mm]

At the bottom are 'Close' and 'Save event' buttons.

A flowchart on the left side of the window shows three steps: 1. Schedule, 2. Trigger, and 3. Action, connected by downward arrows.

- **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 motion detection or digital input after  seconds:** Enter the duration in seconds to pause motion detection after a motion is detected.

Follow the steps 1~3 to arrange the three elements -- Schedule, Trigger, and Action to configure an action to take when an event is triggered. You can configure 3 event-triggered conditions.

### 1. Schedule

Specify the time span for the event-triggering condition. Please select the days in a week and the time in a day (in a 24-hr time format) for the recording 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 98 for details.

Video motion detection

Normal:  door

Profile:  hallway

Note: Please configure Motion detection first

- **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  minutes

- **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 it is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 103 for detailed information.

**Camera tampering detection**

Enable camera tampering detection

Trigger duration  seconds [10~600]

### ■ Manual triggers

An event can be manually triggered by the manual trigger buttons on the main page.

### 3. Action

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

1. Schedule

↓

2. Trigger

↓

3. Action

**Action**

Backup media if the network is disconnected

Move to preset location:  ▼

Note: Please configure [Preset locations](#) first

Server	Media	Extra parameter
<input type="checkbox"/> SD	<input type="text" value="----None----"/> ▼	<a href="#">SD test</a> <a href="#">View</a>
<input type="checkbox"/> NAS	<input type="text" value="----None----"/> ▼	<input type="checkbox"/> Create folders by date time and hour automatically <a href="#">View</a>

▼  ▼

### ■ Backup media if the network is disconnected

Select this option to backup media file onto SD card if the network is disconnected. Please note that this function will only be displayed after you configure a networked storage (NAS). For more information about how to configure the connection to a network share by a networked storage, please refer to page 104.

### ■ Move to preset location

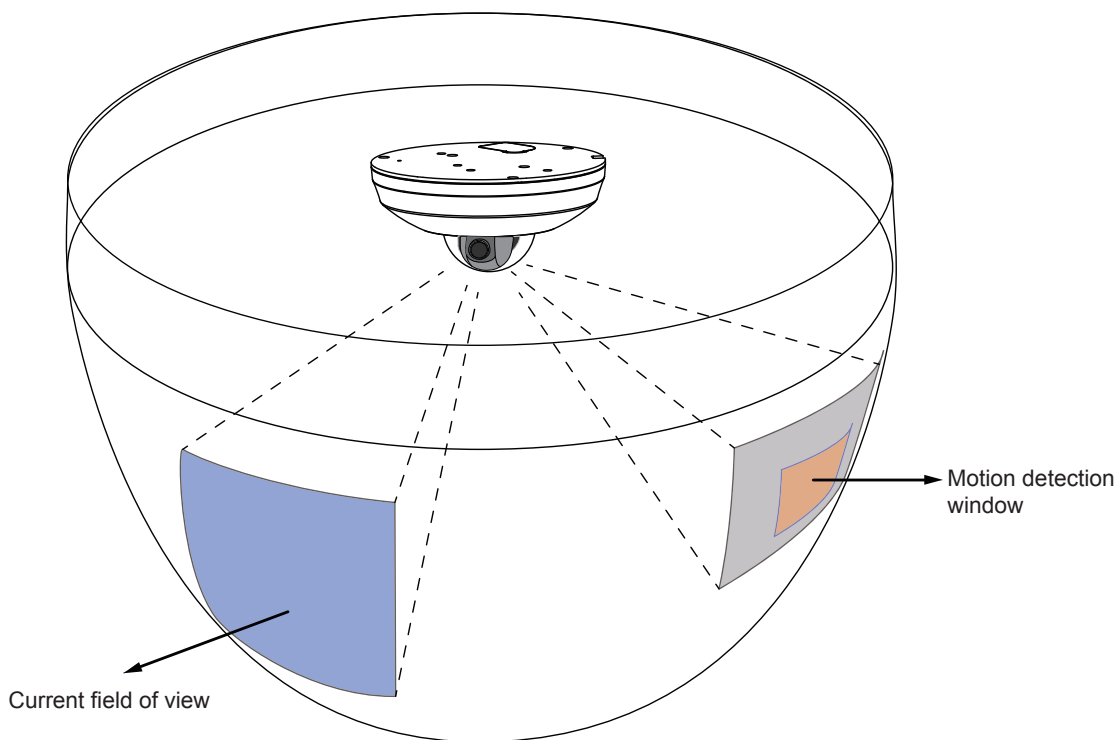
Select a preset location you've configured. Note that please configure **Preset locations** first. For detailed information, please refer to page 82. Another checkbox will appear, **Capture media after moving to the location**. You can select to record associated snapshot, video clip or system event once the event is triggered and the camera moves to the preset location. See Add Media in the following discussion.

To configure an event with the action to record video or snapshots, it is necessary to configure both 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.

**NOTE:**

If you configured a motion detection window as a trigger, the motion detection may become invalid then the camera's field of view moved away from the detection window.

You can let camera return to the motion detection position to detect the coming event by re-configuring your Home position in **PTZ > PTZ settings** (see page 81) or turn the camera to a preset position.



## Add server

Click **Add server** to unfold 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.



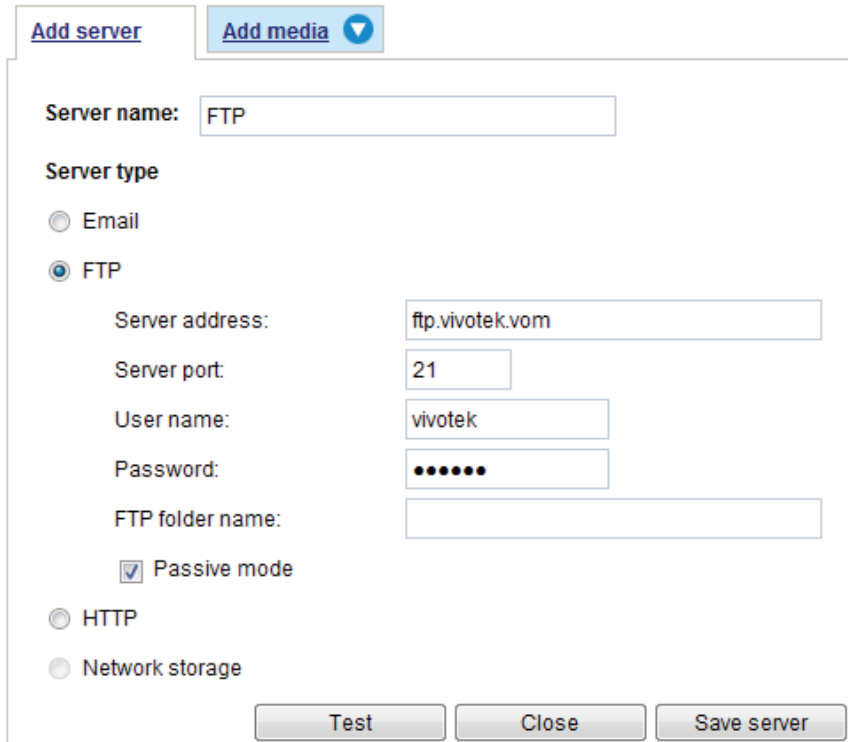
Click **Save server** to enable the settings, then click **Close** to exit the Add server page.

After you set up the first event server, a new item for event server will automatically show up on the Server list. If you wish to add more server options, click **Add server**.



Server type - FTP

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



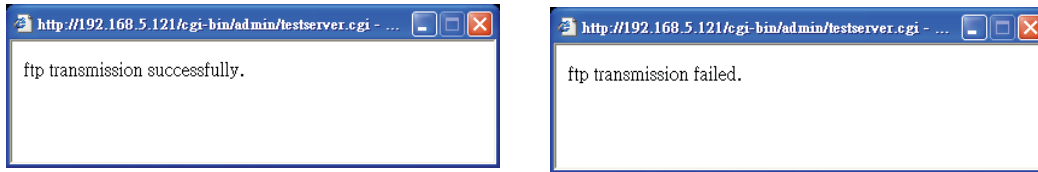
- Server name: Enter a name for the server setting.
- Server address: Enter the domain name or IP address of the FTP server.
- Server port: By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.
- User name: Enter the login name of the FTP 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 create one on the FTP server.



#### ■ Passive mode

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

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



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

#### 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 and click **Close** to exit the Add server page.

Network storage:

Select to send the media files to a networked storage location when a trigger is activated. Please refer to **NAS server** on page 104 for details.

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

**Action**

Backup media if the network is disconnected

Move to preset location:  ▾

Note: Please configure [Preset locations](#) first

	Server	Media	Extra parameter
<input type="checkbox"/>	SD	-----None----- ▾	<a href="#">SD test</a> <a href="#">View</a>
<input type="checkbox"/>	Email	Snapshot Video clip System log	
<input type="checkbox"/>	FTP	-----None----- ▾	
<input type="checkbox"/>	HTTP	-----None----- ▾	
<input type="checkbox"/>	NAS	-----None----- ▾	<a href="#">View</a>

Create folders by date time and hour automatically

▾  ▾

- 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 107 for detailed information.

## Add media

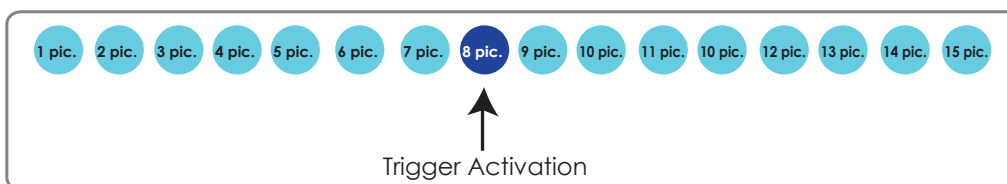
Click **Add media** to open the media setting window. You can specify the type of media that will be sent and preserved when a trigger is activated. A total of 5 media settings can be configured. There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to 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.

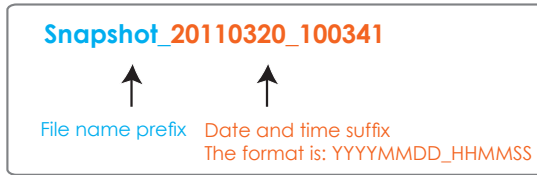
- Media name: Enter a name for the media setting.
- Source: Select to take snapshots from stream 1 ~ 2. (The following options are available when the check circle is selected.)
- Send  pre-event images  
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number 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.



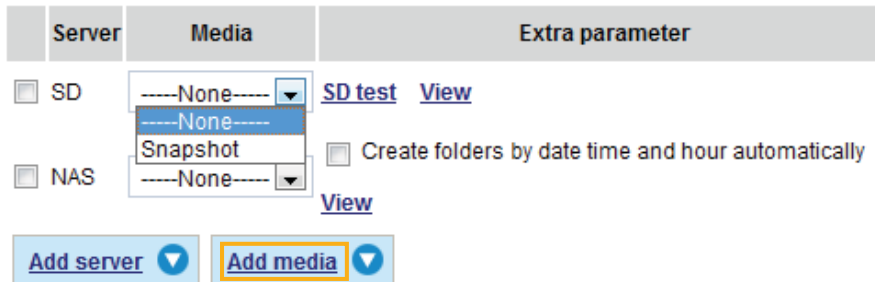
- File name prefix  
Enter the text that will be appended to the front of the file name.

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



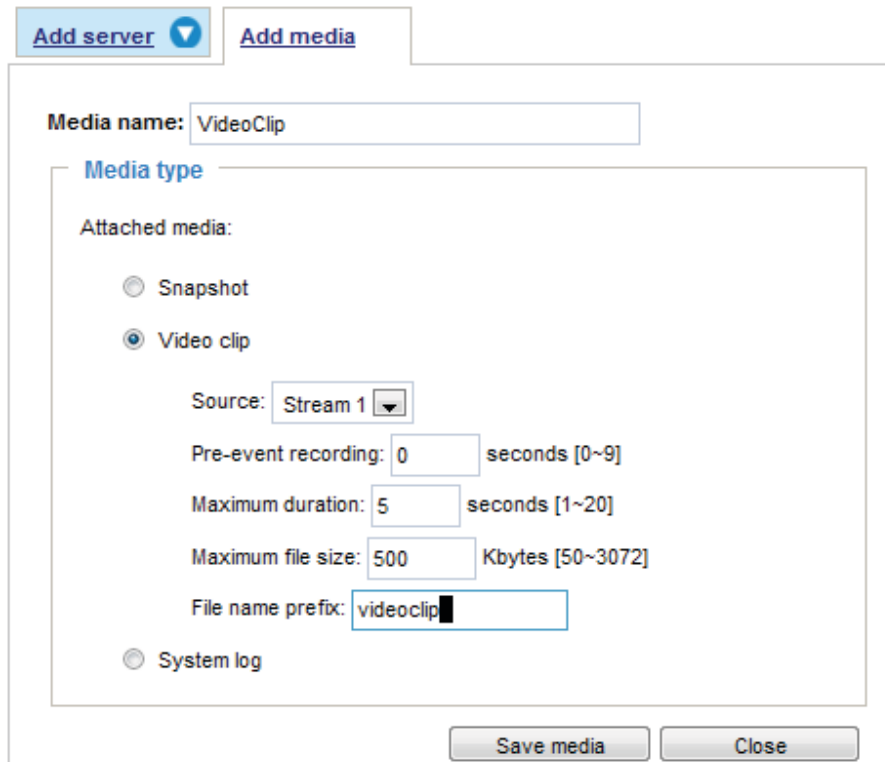
Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

After you set up the first media server, a drop-down menu of existing medias will be available on the Media list. If you wish to add more media options, click **Add media** again.



Media type - Video clip

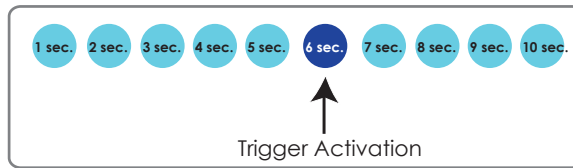
Select to send video clips when a trigger is activated.



- 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 20 seconds can be set.  
 For example, if pre-event recording is set to 5 seconds and the maximum duration is set to 10 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 for each clip.

■ **File name prefix**

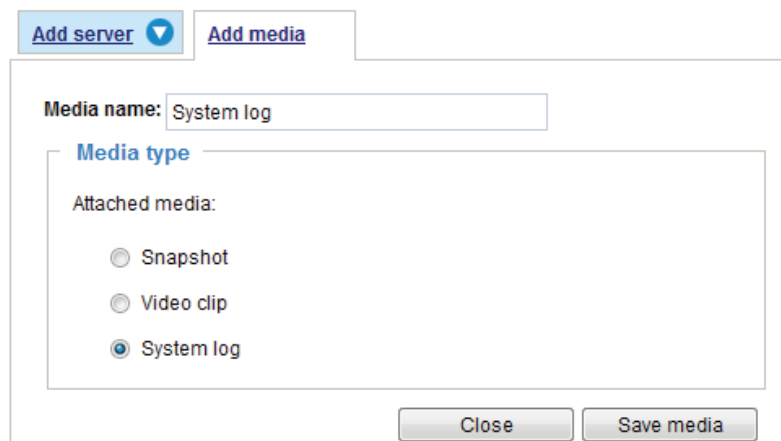
Enter the text that will be appended to the front of the file name.  
 For example:



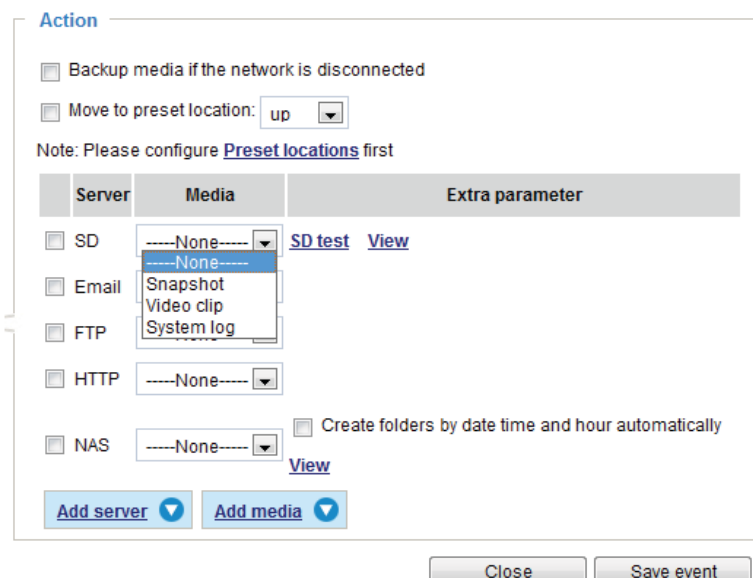
Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

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 Add media page.

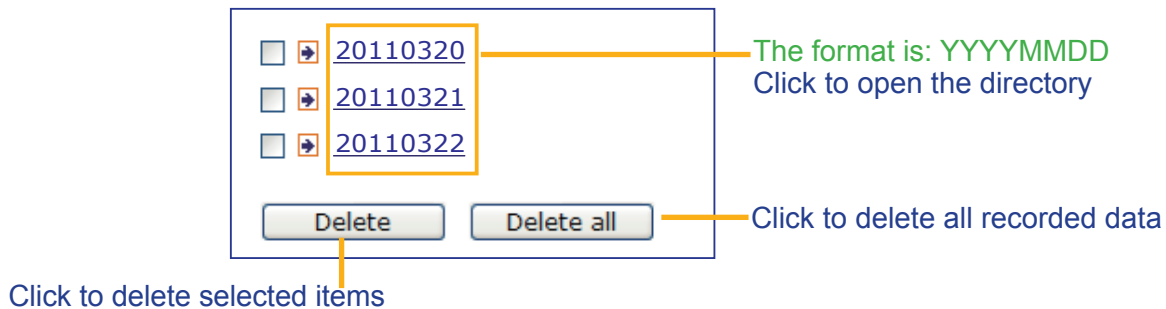


- **View:** Click this button to open a file list window. This function only applies when an SD card or a networked storage are available.

If you click **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 107. If you click **View** button of Network storage, a file directory window will pop up for you to view recorded data on Network storage.

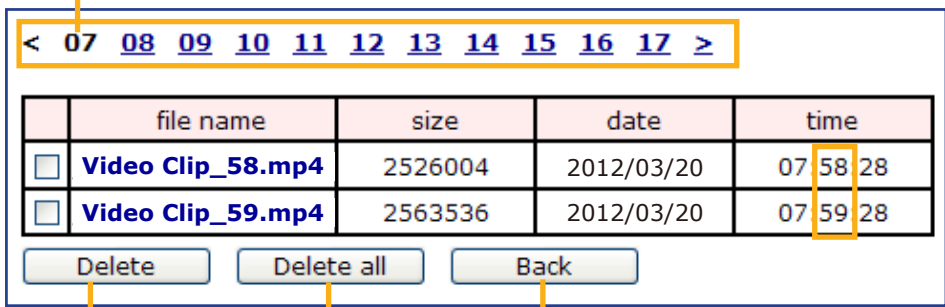
- **Create folders by date, time, and hour automatically:** If you check this item, the system will automatically create sub-folders named by the date.

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



Click [20120320](#) to open the directory:

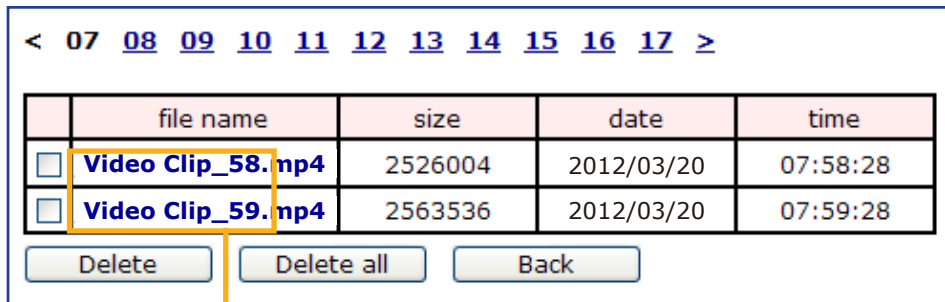
The format is: HH (24r)  
Click to open the file list for that hour



Click to delete selected items

Click to delete all recorded data

Click to go back to the previous level of the directory



The format is: File name prefix + Minute (mm)  
You can set up the file name prefix on Add media page.

Here is an example of the Event setting:

Event name:

Enable this event

Priority:

Detect next motion detection or digital input after  second(s).

1. Schedule

↓

2. Trigger

↓

3. Action

**Action**

Backup media if the network is disconnected

Move to preset location:

Capture media after moving to the location

Note: Please configure [Preset locations](#) first

Server	Media	Extra parameter
<input type="checkbox"/> SD	<input type="text" value="----None----"/>	<a href="#">SD test</a> <a href="#">View</a>
<input checked="" type="checkbox"/> NAS	<input type="text" value="video"/>	<input checked="" type="checkbox"/> Create folders by date time and hour automatically <a href="#">View</a>
<input type="checkbox"/> email	<input type="text" value="----None----"/>	

When completed the settings with steps 1~3 to arrange Schedule, Trigger, and Action of an event, click **Save event** to enable the settings and click **Close** to exit the page.

The following is an example of the Event setting page:

**Event**

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger	
<a href="#">Event1</a>	<a href="#">ON</a>	V	V	V	V	V	V	V	00:00~24:00	boot	<input type="button" value="Delete"/>

[Help](#)

**Server settings**

Name	Type	Address/Location	
<a href="#">NAS</a>	ns	\\172.16.4.39\nas	<input type="button" value="Delete"/>

**Media**

Available memory space: 13000KB

Name	Type	
<a href="#">Snapshot</a>	snapshot	<input type="button" value="Delete"/>
<a href="#">Video clip</a>	videoclip	<input type="button" value="Delete"/>
<a href="#">System log</a>	systemlog	<input type="button" value="Delete"/>

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

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 and click **Delete**. Note that you can only delete a server setting when the server setting is currently not applied to an event setting.

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

### Customized Script

This function allows you to upload a sample script (.xml file) to the camera, 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.

#### Customized Script

Name	Date	Time
<a href="#">User1</a>	20120813	18:13:46
<a href="#">User2</a>	20120813	18:11:32

Click to upload a file

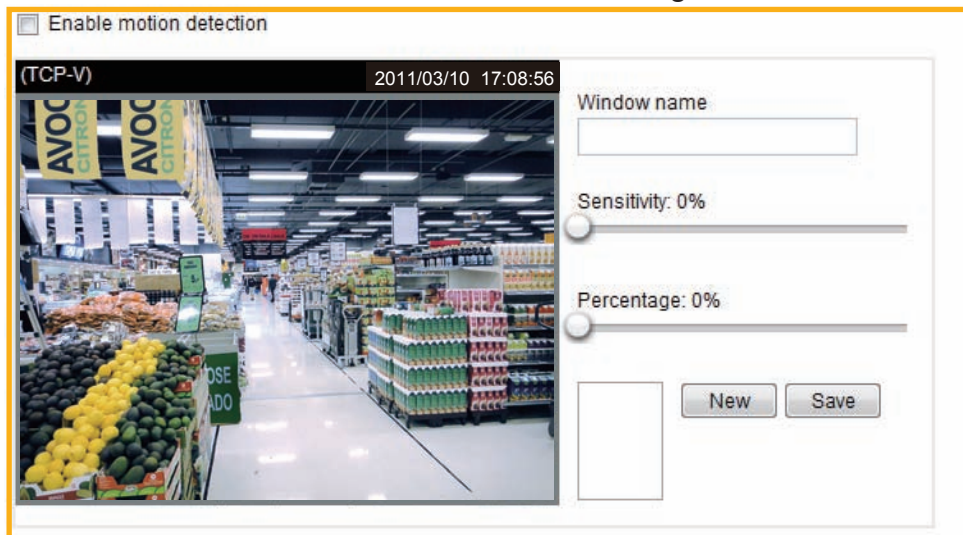
```

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



## 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.



Motion Detection Setting 1:  
For normal situations

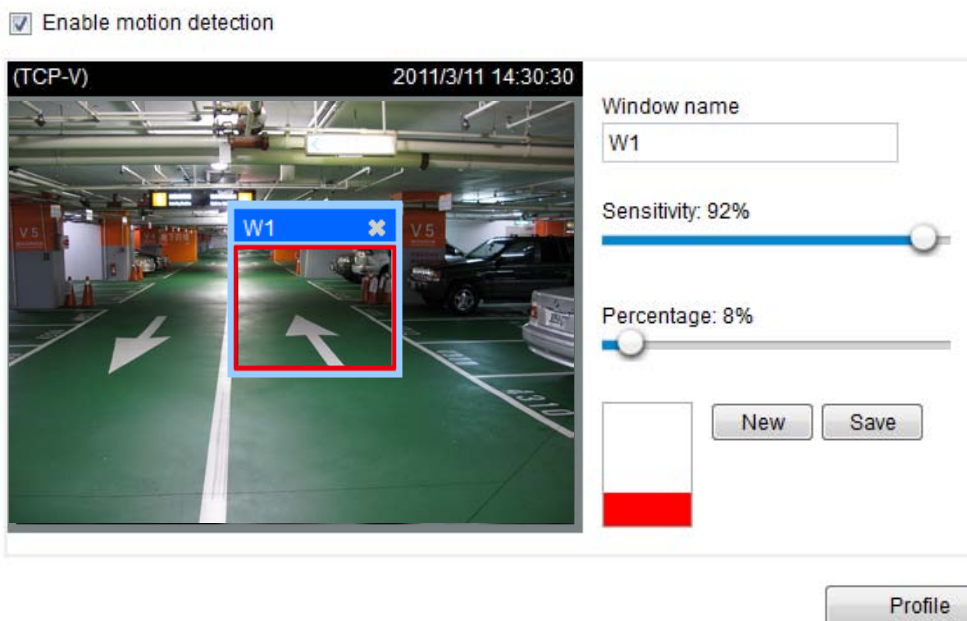


Motion Detection Setting 2:  
For special situations

Follow the steps below to enable motion detection:

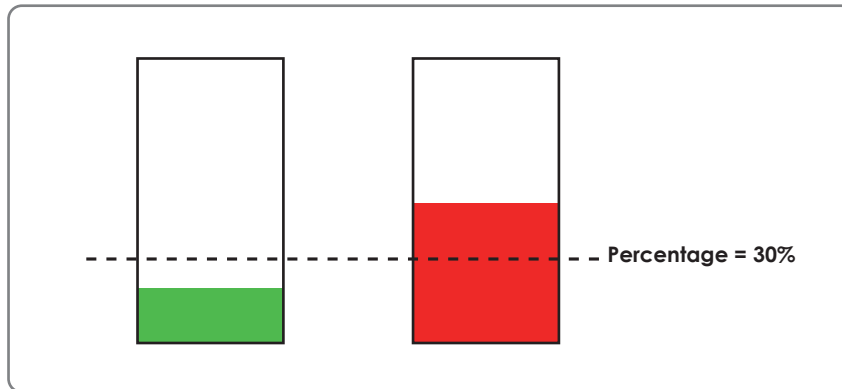
1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
  - To move and resize the window, drag and drop your mouse on the window.
  - To delete window, click the X mark on the upper right corner of the window.
3. Define the 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 considered 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 84.

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.

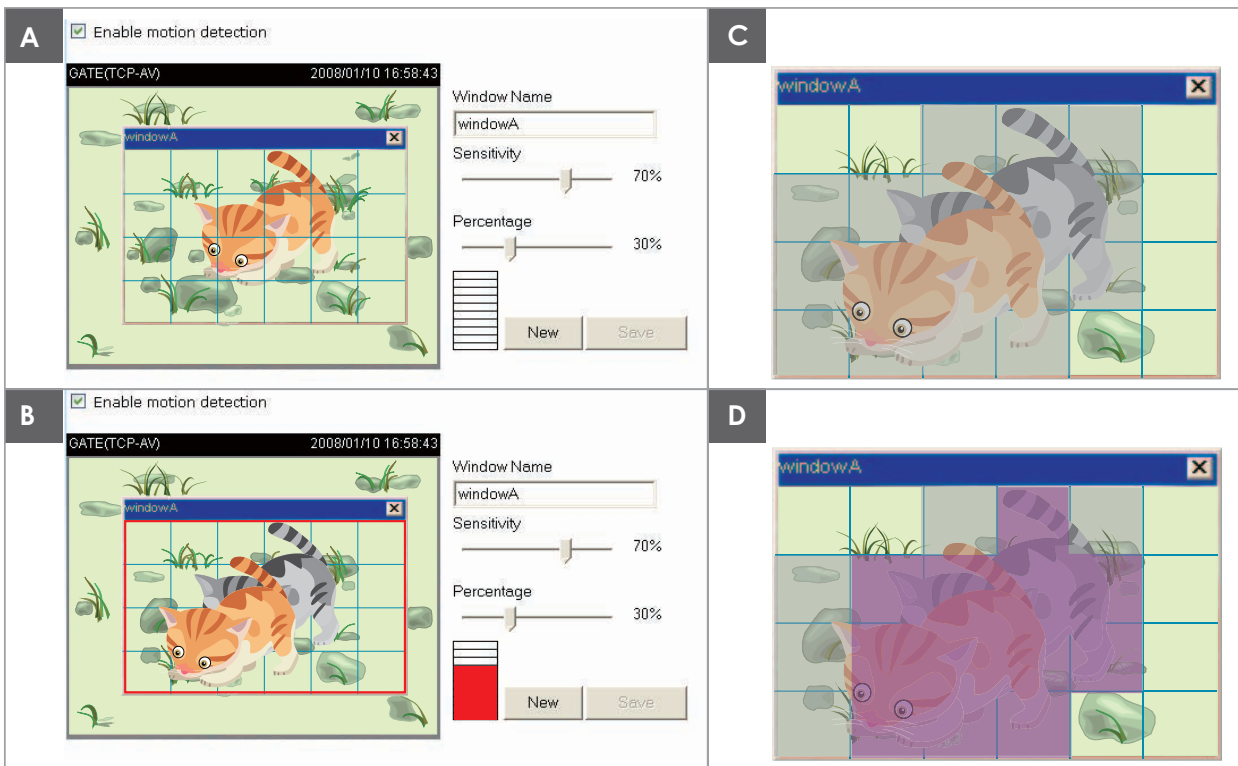
>Motion detection profile settings

The screenshot displays the "Motion detection profile settings" interface. At the top left is a video feed of a parking garage with a timestamp of "2012/10/08 17:08:56". To the right of the video are input fields for "Window name:", "Sensitivity: 0%", and "Percentage: 0%", each with a corresponding slider. Below these are "New" and "Save" buttons. The "General settings" section includes a checked "Enable this profile" checkbox, a "This profile is applied to:" label, a selected "Schedule mode" radio button, and time selection fields showing "From 18:00 to 06:00 [hh:mm]". At the bottom right are "Save" and "Close" buttons.

Please follow the steps below to set up a profile:

1. Create a new motion detection window.
2. Check **Enable this profile**.
3. Select and enter the time frame from the Schedule mode time fields. Please manually enter a range of during which the profile will apply.
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 configure it as a trigger source. Please refer to page 85 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 > 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**.

### Applications > Tampering detection

Camera tampering detection

Enable camera tampering detection

Trigger duration  seconds [10~600]

Save

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. You can configure Tampering Detection as a trigger element to the proactive event configurations in **Event -> Event settings -> Trigger**. For example, when the camera is tampered with, camera can be configured to send pre- and post-event video clips to a networked storage device. Please refer to page 105 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
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Add</span> <span><a href="#">SD test</a></span> </div>												

**NOTE:**

► Please remember to format your SD card when using it for the first time. Please refer to page 107 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:

Enable this recording

With adaptive recording

Pre-event recording:  seconds [0~9]

Post-event recording:  seconds [0~10]

Priority:

Source:

**Trigger**

Schedule

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Time**

Always

From  to  [hh:mm]

Network fail

1. Trigger

↓

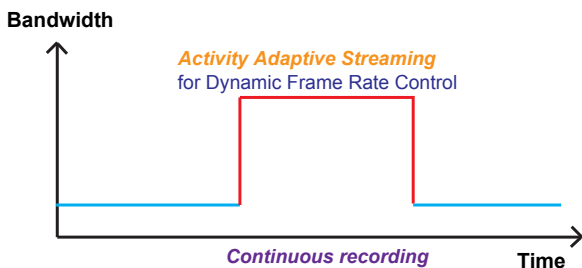
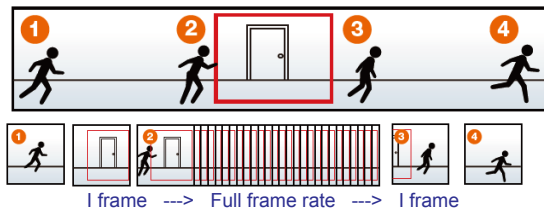
2. Destination

Note: To enable recording notification please configure [Event](#) first

- 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 alarm trigger, the frame rate will raise up to the value you've set on Stream setting page. Please refer to page 49 for more information.

If you enable adaptive recording on the camera, only when an event is triggered on the camera will the server record video streams in the full frame rate; otherwise, it will only request the I frame data during normal monitoring, thus effectively save lots of bandwidth and storage.



**NOTE:**

- ▶ To enable adaptive recording, please make sure you've set up the trigger source such as Motion Detection, DI Device, Audio detection, 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 I frame only.
- ▶ When the I frame period is >1s on Video settings page, it should be forced to make the I frame period to 1s when adaptive recording is activated.

The alarm trigger includes: motion detection and DI detection. Please refer to Event settings on page 84.

- Pre-event recording and post-event recording  
The Network Camera has a buffer area; it temporarily holds data for up to a certain limit. Enter a number to decide the duration of recording that will take place before and after a trigger is activated.
- Priority: Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.
- Source: Select a stream as the recording source.

**NOTE:**

- ▶ To enable recording notification, please configure **Event settings** first. Please refer to page 84.

Please follow steps 1~2 below to set up the recording:

**1. Trigger**

Select a trigger source.

**Trigger**

Schedule

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Time**

Always

From  to  [hh:mm]

Network fail

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

## 2. Destination

You can select the SD card or network attached storage (NAS) for recording video files.

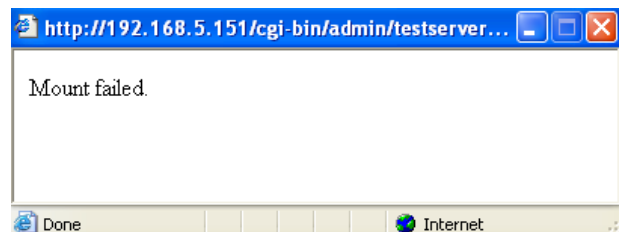
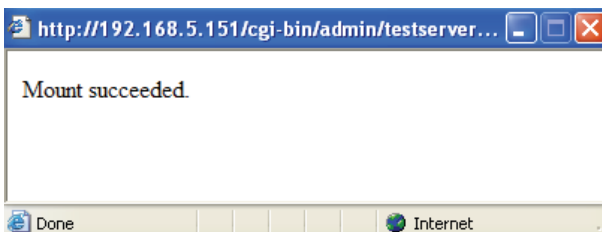
## NAS server

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

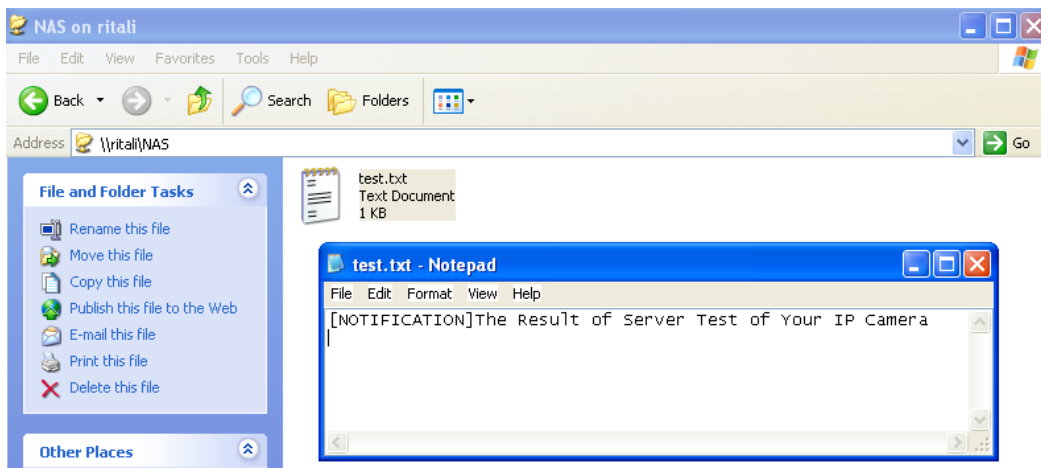
1. Fill in the information for your server.

For example:

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.

Recording name:

Enable this recording

With adaptive recording ([Help](#))

Pre-event recording:  seconds [0~9]

Post-event recording:  seconds [0~10]

Priority:

Source:

**Destination**

Destination:

Capacity:

Entire free space

Reserved space:  Mbytes

Enable cyclic recording

**Recording file management**

Maximum duration:  minutes [1~30]

Maximum file size:  MB [1~900]

File name prefix:

Note: To enable recording notification please configure [Event](#) first

- **Capacity:** You can select either the entire storage space available or specify a reserved space. The recording size limit must be larger than the reserved space for cyclic recording. The reserved space is used during cyclic recording to prevent malfunctions that might occur during the transaction stage when the video feeds are about to fill up the storage space, and new data is still coming. This value must be larger than 15 MBytes.
- **File name prefix:** Enter the text that will be appended to the front of the file name.
- **Enable cyclic recording:** If you check this item, when the maximum capacity is reached, the oldest files will be overwritten by the latest ones.

If you want to enable recording notification, please click [Event](#) to set up. Please refer to **Event > Event settings** on page 84 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 a networked storage or SD card. The new recording name will appear on the recording page as shown below. To remove a recording setting from the list, select it and click **Delete**.

Recording settings												
Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination	Delete
<a href="#">Video</a>	<a href="#">ON</a>	V	V	V	V	V	V	V	00:00~24:00	stream1	<a href="#">SD</a>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>		<a href="#">SD test</a>										

- **[Video](#) (Name)**: Click to open the Recording settings page to modify its details.
- **[ON](#) (Status)**: Click to manually adjust the Status. ([ON](#): start recording; [OFF](#): stop recording)
- **[NAS](#) or [SD](#) (Destination)**: Click to open the file list of recordings as shown below. For more information about folder naming rules, please refer to page 95 or page 95 for details.

## Local storage > SD card management

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 status

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

**SD card status**

SD card status: **Detached** — no SD card

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

**SD card status**

SD card status: Ready

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

### SD card control

**SD card control**

Enable cyclic storage

Enable automatic disk cleanup

Maximum duration for keeping files:  days

- **Enable cyclic storage:** Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest files will be overwritten by the latest ones.
- **Enable automatic disk cleanup:** Check this item and enter the number of days you wish to retain a file. For example, if you enter “7 days”, the recorded files will be stored on the SD card for 7 days.

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

## Local storage > Content management

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

**Searching and viewing the records**

**File attributes**

Trigger type:  System boot  Recording notify  Motion  
 Network fail  Periodically  Manual triggers  
 Tampering detection

Media type:  Video clip  Snapshot  Text

Locked:  Locked  Unlocked

Backup:  Backup


**Trigger time**

From: Date  Time   
to: Date  Time   
(yyyy-mm-dd) (hh:mm:ss)

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






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

### Search Results

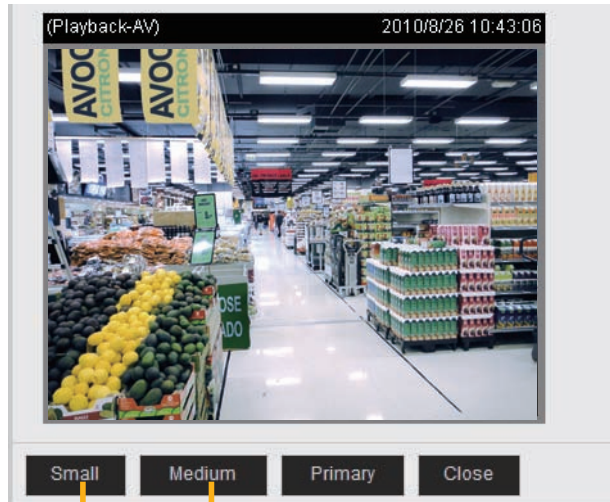
The following is an example of search results. There are four columns: Trigger time, Media type, Trigger type, and Locked. Click  to sort the search results in either direction.

**Search results**

Show 10 entries Search:

<input type="checkbox"/>	Trigger time 	Media Type 	Trigger type 	Locked 	Backup 
<input checked="" type="checkbox"/>	2010-08-26 10:42:55	Video Clip	Periodically	No	No
<input type="checkbox"/>	2010-08-26 10:43:56	Video Clip	Periodically	No	No
<input type="checkbox"/>	2010-08-26 10:44:56	Video Clip	Periodically	No	No
<input type="checkbox"/>	2010-08-26 10:45:57	Video Clip	Periodically	No	No
<input type="checkbox"/>	2010-08-26 10:46:58	Video Clip	Periodically	No	No
<input type="checkbox"/>	2010-08-26 .....	Video Clip	Periodically	No	No

- **View:** Click on a search result. The entry will be highlighted 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 select an entry as shown above. Then click the **Download** button and a file download window will prompt for you to save the file.
- **JPEGs to AVI:** This function only applies to “JPEG” format files such as snapshots. You can select several snapshots from the list, then click this button. The series of 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:

Search results

Show  entries

Search:

<input type="checkbox"/>	Trigger time	Media type	Trigger type	Locked	Backup
<input checked="" type="checkbox"/>	2012-07-11 17:56:12	Video clip	Boot	Yes	No
<input checked="" type="checkbox"/>	2012-07-11 17:35:10	Snapshot	Boot	Yes	No
<input checked="" type="checkbox"/>	2012-07-11 17:35:10	Snapshot	Boot	Yes	No
<input type="checkbox"/>	2012-07-11 17:35:10	Snapshot	Boot	No	No
<input type="checkbox"/>	2012-07-11 17:35:10	Snapshot	Boot	No	No
<input type="checkbox"/>	2012-07-11 17:35:10	Snapshot	Boot	No	No

Showing 1 to 6 of 6 entries

View Download JPEGs to AVI **Lock/Unlock** Remove

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

Click to switch pages

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

# 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

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
```

VIVOTEK Confidential

## 4. Security Level

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

## 5. Get Server Parameter Values

**Note:** The access right depends on the URL directory.

**Method:** GET/POST

Syntax:

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

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

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

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

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

When querying parameter values, the current parameter values are returned.

A successful control request returns parameter pairs as follows:

Return:

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

where *<parameter pair>* is

```
<parameter>=<value>\r\n
```

```
[<parameter pair>]
```

*<length>* is the actual length of content.

**Example:** Request IP address and its response

Request:

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



Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Content-Length: 33\r\n

\r\n

network\_ipaddress=192.168.0.123\r\n

VIVOTEK Confidential

## 6. Set Server Parameter Values

**Note:** The access right depends on the URL directory.

**Method:** GET/POST

Syntax:

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

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

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

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

PARAMETER	VALUE	DESCRIPTION
<b>&lt;group&gt;_&lt;name&gt;</b>	value to assigned	Assign <i>&lt;value&gt;</i> to the parameter <i>&lt;group&gt;_&lt;name&gt;</i> .
<b>return</b>	<i>&lt;return page&gt;</i>	Redirect to the page <i>&lt;return page&gt;</i> after the parameter is assigned. The <i>&lt;return page&gt;</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.  (Note: The return page can be a general HTML file (.htm, .html). It cannot be a CGI command or have any extra parameters. This parameter must be placed at the end of the parameter list

Return:

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

where *<parameter pair>* is

```
<parameter>=<value>\r\n
[<parameter pair>]
```

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

**Example:** Set the IP address of server to 192.168.0.123:

Request:

[http://myserver/cgi-bin/admin/setparam.cgi?network\\_ipaddress=192.168.0.123](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

Content-Length: 33\r\n

\r\n

network\_ipaddress=192.168.0.123\r\n

VIVOTEK Confidential

## 7. Available parameters on the server

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

Valid values:

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

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

## 7.1 system

Group: system

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
hostname	string[64]	Mega-Pixel Network Camera	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
ledoff	<boolean>	0	6/6	Turn on (0) or turn off (1) all led indicators.
date	<YYYY/MM/DD >, keep, auto	<current date>	6/6	Current date of system. Set to 'keep' to keep date unchanged. Set to 'auto' to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	<current time>	6/6	Current time of the system. Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	<MMDDhhmmY YYY.ss>	<current time>	6/6	Another current time format of the system.
ntp	<domain name>, <ip address>, <blank>	<blank>	6/6	NTP server. *Do not use "skip to invoke default server" for default value.
timezoneindex	-489 ~ 529	320	6/6	Indicate timezone and area. -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time,

			<p>Denver</p> <p>-281: GMT-07:00 Arizona</p> <p>-240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan</p> <p>-200: GMT-05:00 Eastern Time, New York, Toronto</p> <p>-201: GMT-05:00 Bogota, Lima, Quito, Indiana</p> <p>-180: GMT-04:30 Caracas</p> <p>-160: GMT-04:00 Atlantic Time, Canada, La Paz, Santiago</p> <p>-140: GMT-03:30 Newfoundland</p> <p>-120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland</p> <p>-80: GMT-02:00 Mid-Atlantic</p> <p>-40: GMT-01:00 Azores, Cape_Verde_IS.</p> <p>0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London</p> <p>40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris</p> <p>41: GMT 01:00 Warsaw, Budapest, Bern</p> <p>80: GMT 02:00 Athens, Helsinki, Istanbul, Riga</p> <p>81: GMT 02:00 Cairo</p> <p>82: GMT 02:00 Lebanon, Minsk</p> <p>83: GMT 02:00 Israel</p> <p>120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi</p> <p>121: GMT 03:00 Iraq</p> <p>140: GMT 03:30 Tehran</p> <p>160: GMT 04:00 Abu Dhabi, Muscat, Baku,</p>
--	--	--	---

				<p>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,  Chongqing, Hong Kong, Kuala  Lumpur, Singapore, Taipei  360: GMT 09:00 Osaka, Sapporo,  Tokyo, Seoul, Yakutsk  380: GMT 09:30 Adelaide, Darwin  400: GMT 10:00 Brisbane, Canberra,  Melbourne, Sydney, Guam,  Vladivostok  440: GMT 11:00 Magadan, Solomon  Is., New Caledonia  480: GMT 12:00 Auckland,  Wellington, Fiji, Kamchatka,  Marshall Is.  520: GMT 13:00 Nuku'Alofa</p>
daylight_enable	<boolean>	0	6/6	Enable automatic daylight saving time in time zone.
daylight_auto_begintime	string[19]	NONE	6/7	Display the current daylight saving start time.
daylight_auto_endtime	string[19]	NONE	6/7	Display the current daylight saving end time.
daylight_timezones	string	,-360,-320, -280,-240, -241,-200, -201,-160, -140,-120,	6/6	List time zone index which support daylight saving time.

		-80,-40,0, 40,41,80, 81,82,83, 120,140, 380,400,480		
updateinterval	0, 3600, 86400, 604800, 2592000	0	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.
restore	0, <positive integer>	N/A	7/6	Restore the system parameters to default values after <value> seconds.
reset	0, <positive integer>	N/A	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	<Any value>	N/A	7/6	Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
restoreexceptdst	<Any value>	N/A	7/6	Restore the system parameters to default values except all daylight saving time settings. This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to default values except for a union of combined results.



restoreexceptlanguage	<Any Value>	N/A	7/6	Restore the system parameters to default values except the custom language file the user has uploaded. This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
-----------------------	-------------	-----	-----	---

### 7.1.1 system.info

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	PD8136	0/7	Internal model name of the server (eg. IP7139)
extendedmodelname	string[40]	PD8136	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>	<product mac address>	0/7	12 characters MAC address (without hyphens).
firmwareversion	string[40]	<product dependent>	0/7	Firmware version, including model, company, and version number in the format: <MODEL-BRAND-VERSION>
language_count	<integer>	<product dependent>	0/7	Number of webpage languages available on the server.
language_i<0~(count-1)>	string[16]	<product dependent>	0/7	Available language lists.
customlanguage_maxcount	<integer>	<product dependent>	0/6	Maximum number of custom languages supported on the

				server.
customlanguage_count	<integer>	1	0/6	Number of custom languages which have been uploaded to the server.
customlanguage_i<0~(max count-1)>	string	N/A	0/6	Custom language name.

## 7.2 status

Group: **status**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
daynight <product dependent>	day, night	0	7/7	Current status of day, 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>	<blank>	1/7	Get network information from mii-tool.
vi_i<0~(nvi-1)> <product dependent>	<boolean>	0	1/7	Virtual input 0 => Inactive 1 => Active (capability.nvi > 0)
signal_c<0~(nvideoin-1)> <product dependent>	<Boolean>	0	1/7	0=> No signal. 1=> Signal detected.
videomode_c<0~(nvideoin-1)> <product dependent>	ntsc, pal	<product dependent>	1/7	Video modulation type

## 7.3 security

Group: **security**

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

## 7.4 network

Group: **network**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
preprocess	<positive integer>	NULL	7/6	<p>An 32-bit integer, each bit can be set separately as follows:</p> <ul style="list-style-type: none"> <li>Bit 0 =&gt; HTTP service;</li> <li>Bit 1=&gt; HTTPS service;</li> <li>Bit 2=&gt; FTP service;</li> <li>Bit 3 =&gt; Two way audio and RTSP Streaming service;</li> </ul> <p>To stop service before changing its port settings. It's <b>recommended</b> to set this parameter when</p>

				<p>change a service port to the port occupied by another service currently. Otherwise, the service may fail.</p> <p>Stopped service will auto-start after changing port settings.</p> <p>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&amp;network_http_port=5556 &amp; network_rtp_videoport=20480”</p>
type	lan, pppoe	lan	6/6	Network connection type.
resetip	<boolean>	1	6/6	<p>1 =&gt; Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot.</p> <p>0 =&gt; Use preset ipaddress, subnet, router, dns1, and dns2.</p>
ipaddress	<ip address>	<product dependent>	6/6	IP address of server.
subnet	<ip address>	<blank>	6/6	Subnet mask.
router	<ip address>	<blank>	6/6	Default gateway.
dns1	<ip address>	<blank>	6/6	Primary DNS server.
dns2	<ip address>	<blank>	6/6	Secondary DNS server.
wins1	<ip address>	<blank>	6/6	Primary WINS server.
wins2	<ip address>	<blank>	6/6	Secondary WINS server.

## 7.4.1 802.1x

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

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

## 7.4.2 QOS

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

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

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

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

## 7.4.3 IPV6

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

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

## 7.4.4 FTP

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

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

## 7.4.5 HTTP

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	80	6/6	HTTP port.
alternateport	1025~65535	8080	6/6	Alternate HTTP port.
authmode	basic, digest	basic	1/6	HTTP authentication mode.
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 for stream 2. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 1)
anonymousviewing	<boolean>	0	1/6	Enable anonymous streaming viewing.

## 7.4.6 HTTPS port

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

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

## 7.4.7 RTSP

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	554	1/6	RTSP port. ( <code>capability.protocol.rtsp=1</code> )
anonymousviewing	<boolean>	0	1/6	Enable anonymous streaming viewing.
authmode	disable, basic, digest	disable	1/6	RTSP authentication mode. ( <code>capability.protocol.rtsp=1</code> )
s0_accessname	string[32]	live.sdp	1/6	RTSP access name for stream1. ( <code>capability.protocol.rtsp=1</code> and <code>capability.nmediastream &gt; 0</code> )
s1_accessname	string[32]	live2.sdp	1/6	RTSP access name for stream2. ( <code>capability.protocol.rtsp=1</code> and <code>capability.nmediastream &gt; 1</code> )

### 7.4.7.1 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>	0	4/4	Enable always multicast.
ipaddress	<ip address>	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	1025 ~ 65535	$5562+n*2$	4/4	Multicast audio port. ( <code>capability.naudio &gt; 0</code> )
ttl	1 ~ 255	15	4/4	Multicast time to live value.



## 7.4.8 RTP port

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	5556	6/6	Video channel port for RTP. (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	5558	6/6	Audio channel port for RTP. (capability.protocol.rtp_unicast=1)

## 7.4.9 PPPoE

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

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

## 7.5 ipfilter

Group: **ipfilter**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable access list filtering.
admin_enable	<boolean>	0	6/6	Enable administrator IP address.
admin_ip	String[44]	<blank>	6/6	Administrator IP address.
maxconnection	1~10	10	6/6	Maximum number of concurrent streaming connection(s).
type	0, 1	1	6/6	Ipfilter policy : 0 => allow 1 => deny
ipv4list_i<0~9>	Single address: <ip address>	<blank>	6/6	IPv4 address list.

	Network address: <ip address / network mask> Range address:<start ip address - end ip address>			
ipv6list_i<0~9>	String[44]	<blank>	6/6	IPv6 address list.

## 7.6 video input

Group: **videoin**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
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	0~8	4	4/4	Exposure level
irismode	fixed	fixed	4/4	Video Iris or DC Iris.
enableblc	<boolean>	0	4/4	Enable backlight compensation.

## 7.6.1 video input setting per channel

Group: **videoin\_c<0~(n-1)>** for n channel products, and m is stream number

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
whitebalance	auto, manual,	auto	4/4	“auto” indicates auto white balance. “manual” indicates keep current value.
exposurelevel	0~8	4	4/4	Exposure level
irismode	fixed	fixed	4/4	Video Iris mode for DC Iris.
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>	0	4/4	Flip the image.
mirror	<boolean>	0	4/4	Mirror the image.
ptzstatus	<integer>	2	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => <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),

				1(support)
text	string[60]	<blank>	1/4	Enclose caption.
imprinttimestamp	<boolean>	0	4/4	Overlay time stamp on video.
flickless	<boolean>	0	4/4	Enable flickless mode or not. Enable flickless mode will limit the parameters: minexposure and maxexposure between 5~120.
minexposure	5,15,25,30,50,60,100,120,240,250,480,500,1000,2000,4000,8000,16000,32000	32000	4/4	Minimum exposure time.
maxexposure	5,15,25,30,50,60,100,120,240,250,480,500,1000,2000,4000,8000,16000,32000	30	4/4	Maximum exposure time.
enableblc	0~1	0	4/4	Enable backlight compensation
s<0~(m-1)>_codectype	mpeg4, mjpeg, h264	h264	1/4	Video codec type. svc is only supported with stream 0.
s<0~(m-1)>_resolution	"176~1280"x"144~800"	1280x800	1/4	Video resolution in pixels.
s<0~(m-1)>_mpeg4_intra period	250, 500, 1000, 2000, 3000, 4000	1000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_mpeg4_ratecontrolmode	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". 99,100 is the customized manual input setting.

				1 = worst quality, 5 = best quality.
s<0~(m-1)>_mpeg4_qvalue	1~31	7	4/4	Manual video quality level input. (s<0~(m-1)>_mpeg4_quant = 99)
s<0~(m-1)>_mpeg4_qpercent	1~100	29	4/4	Set quality by percentage. 1: Worst quality 100: Best quality (s<0~(m-1)>_mpeg4_quant = 100)
s<0~(m-1)>_mpeg4_bitrate	1000~8000000	3000000	4/4	Set bit rate in bps when choosing cbr in “ratecontrolmode”.
s<0~(m-1)>_mpeg4_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	30	1/4	Set maximum frame rate in fps (for MPEG-4).
s<0~(m-1)>_h264_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_h264_ratecontrolmode	cbr, vbr	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”. 99,100 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_h264_qpercent	1~100	45	4/4	Set quality by percentage. 1: Worst quality 100: Best quality (s<0~(m-1)>_h264_quant = 100)
s<0~(m-1)>_h264_qvalue	0~51	26	4/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 99)

s<0~(m-1)>_h264_bitrate	1000~8000000	3000000	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_h264_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	30	1/4	Set maximum frame rate in fps (for h264).
s<0~(m-1)>_h264_profile	0~2	1	1/4	Indicate H264 profiles 0: baseline 1: main profile 2: high profile
s<0~(m-1)>_mjpeg_quant	1~5,99,100	3	4/4	Quality of JPEG video. 99, 100 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_mjpeg_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	30	1/4	Set maximum frame rate in fps (for JPEG).
s<0~(m-1)>_mjpeg_qvalue	10~200	50	4/4	Manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 0)
s<0~(m-1)>_mjpeg_qpercent	1~100	49	4/4	Set quality by percentage. 1: Worst quality 100: Best quality (s<0~(m-1)>_mjpeg_quant = 100)
s<0~(m-1)>_forcei	1	N/A	7/6	Force I frame.
maxgain	1~100	100	4/4	Manual set maximum gain value
mingain	1~100	0	4/4	Manual set minimum gain value

## 7.6.1.1 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\_profile\_i<0~(m-1)>** (capability. nvideoinprofile > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable/disable this profile setting
policy	schedule	schedule	4/4	The mode which the profile is applied to.
begintime	hh:mm	18:00	4/4	Begin time of schedule mode.
endtime	hh:mm	06:00	4/4	End time of schedule mode.
minexposure	1~32000	32000	4/4	Minimum exposure time.
maxexposure	1~32000	30	4/4	Maximum exposure time.
flickless	<boolean>	0	4/4	Enable flickless mode or not. Enable flickless mode will limit the parameters: minexposure and maxexposure between 5~120.
exposurelevel	0~8	4	4/4	Exposure level
maxexposure	5,15,25,30,50,60, 100,120,240,250, 480,500,1000,200 0,4000,8000,1600 0,32000	30	4/4	Maximum exposure time.
minexposure	5,15,25,30,50,60, 100,120,240,250, 480,500,1000,200 0,4000,8000,1600 0,32000	32000	4/4	Minimum exposure time.
maxgain	0~100	100	4/4	Manual set maximum gain value.
mingain	0~100	0	4/4	Manual set minimum gain value.
enableblc	<boolean>	0	4/4	Enable backlight compensation.
whitebalance	auto, manual	manual	4/4	“auto” indicates auto white balance. “manual” indicates keep current value.

irismode	fixed	fixed	4/4	Video Iris mode for DC Iris.
maxgain	0~100	100	4/4	Manual set maximum gain value
mingain	0~100	0	4/4	Manual set minimum gain value

## 7.7 video input preview

The temporary settings for video preview

Group: **videoinpreview**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
minexposure	5,15,25,30,50,60,100,120,240,250,480,500,1000,2000,4000,8000,16000,32000	32000	4/4	Minimum exposure time.
maxexposure	5,15,25,30,50,60,100,120,240,250,480,500,1000,2000,4000,8000,16000,32000	30	4/4	Maximum exposure time.
irismode	fixed	fixed	4/4	Video Iris mode for DC Iris.
exposurelevel	0~8	4	4/4	Preview of exposure level
enableble	0~1	0	4/4	Enable backlight compensation
maxgain	0~100	100	4/4	Manual set maximum gain value
mingain	0~100	0	4/4	Manual set minimum gain value

## 7.8 image setting per channel

Group: **image\_c<0~(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	100	4/4	Adjust saturation of image according to mode settings. 100 means using the parameter "saturationpercent".
contrast	-5 ~ 5	0	4/4	Adjust contrast of image



				according to mode settings.
sharpness	-3~3,100	100	4/4	Adjust sharpness of image according to mode settings. 100 means using the parameter "sharpnesspercent"
Saturationpercent	0 ~ 100	50	4/4	Adjust saturation of image by percentage. Less 0 <-> 100 More saturation
sharpnesspercent	0~100	50	4/4	Adjust sharpness of image by percentage. Softer 0 <-> 100 Sharper
lowlightmode	<boolean>	1	4/4	Enable/disable low light mode.

## 7.9 image setting for preview

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5~5	-5	4/4	Preview of brightness adjustment of image according to mode settings.
saturation	-5~5,100	100	4/4	Preview of saturation adjustment of image according to mode settings. 100 means using the parameter "saturationpercent"
contrast	-5 ~ 5	0	4/4	Preview of contrast adjustment of image according to mode settings.
sharpness	-3~3,100	100	4/4	Preview of sharpness adjustment of image according to mode settings. 100 means using the parameter "sharpnesspercent"
saturationpercent	0 ~ 100	50	4/4	Adjust saturation of image by percentage. Less 0 <-> 100 More

				saturation
sharpnesspercent	0~100	50	4/4	Adjust sharpness of image by percentage. Softer 0 <-> 100 Sharper
lowlightmode	<boolean>	1	4/4	Enable/disable low light mode.

## 7.10 Audio input per channel

Group: **audioin\_c<0~(n-1)>** for n channel products (capability.audioin>0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
source	micin	micin	4/4	micin => use built-in microphone input.
mute	0, 1	0	4/4	Enable audio mute.
gain	1,5,9,13,17,21,25,29, 33,37,41,45,49,53,57, 61	61	4/4	Gain of input.
s<0~(m-1)>_codectype	g711	g711	4/4	Set audio codec type for input.
s<0~(m-1)>_g711_mode	pcmu, pcma	pcmu	4/4	Set G.711 mode.

## 7.11 Motion detection settings

Group: **motion\_c<0~(n-1)>** for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable motion detection.
win_i<0~2>_enable	<boolean>	0	4/4	Enable motion window 1~3.
win_i<0~2>_name	string[40]	<blank>	4/4	Name of motion window 1~3.
win_i<0~2>_left	0 ~ 320	0	4/4	Left coordinate of window position.
win_i<0~2>_top	0 ~ 240	0	4/4	Top coordinate of window position.
win_i<0~2>_width	0 ~ 320	0	4/4	Width of motion detection window.

win_i<0~2>_height	0 ~ 240	0	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	0	4/4	Percent of motion detection window.
win_i<0~2>_sensitivity	0 ~ 100	0	4/4	Sensitivity of motion detection window.

Group: **motion\_c<0~(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>	0	4/4	Enable profile 1 ~ (m-1).
i<0~(m-1)>_policy	schedule	schedule	4/4	The mode which the profile is 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>	0	4/4	Enable motion window.
i<0~(m-1)>_win_i<0~2>_name	string[40]	<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.
-----------------------------------	---------	---	-----	---

## 7.12 Tampering detection settings

Group: **tampering\_c<0~(n-1)>** for n channel product (capability.tampering > 0)

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

## 7.13 DDNS

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the dynamic DNS.
provider	Safe100, DyndnsDynamic, DyndnsCustom, TZO, DHS, DynInterfree, CustomSafe100, PeanutHull	DyndnsDynamic <product dependent>	6/6	Safe100 => safe100.net DyndnsDynamic => dyndns.org (dynamic) DyndnsCustom => dyndns.org (custom) TZO => tzo.com DHS => dhs.org DynInterfree => dyn-interfree.it CustomSafe100 => Custom server using safe100 method PeanutHull => PeanutHull
<provider>_hostname	string[128]	<blank>	6/6	Your DDNS hostname.
<provider>_usernameemail	string[64]	<blank>	6/6	Your user name or email to login to the DDNS service provider
<provider>_passwordkey	string[64]	<blank>	6/6	Your password or key to login to the DDNS service provider.
<provider>_server	string[128]	<blank>	6/6	The server name for safe100.

vername				(This field only exists if the provider is customsafel00)
---------	--	--	--	---

## 7.13.1 Express link

Group: expresslink

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable express link.
state	onlycheck, onlyoffline, checkonline, badnetwork	<blank>	6/6	<p>“onlycheck” : You have to input the host name of your camera and press "Register" button to register it.</p> <p>“onlyoffline” : Express link is active, you can now connect to this camera at expresslink_url.</p> <p>“checkonline” : Express link is not active.</p> <p>“badnetwork” : Express Link is not supported under this network environment.</p>
url	string[64]	<blank>	6/6	The URL to connect to this camera by express link.

## 7.14 UPnP presentation

Group: upnppresentation

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

## 7.15 UPnP port forwarding

Group: upnpportforwarding

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the UPnP port forwarding service.
upnpnatstatus	0~3	0	6/7	The status of UPnP port forwarding, used internally.

				0 = OK, 1 = FAIL, 2 = no IGD router, 3 = no need for port forwarding
--	--	--	--	--

## 7.16 System log

Group: **syslog**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	0	6/6	Enable remote log.
serverip	<IP address>	<blank>	6/6	Log server IP address.
serverport	514, 1025~65535	514	6/6	Server port used for log.
level	0~7	6	6/6	Levels used to distinguish the importance of the information: 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG
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.

## 7.17 camera PTZ control

Group: **camctrl\_c<0~(n-1)>** for n channel product (**capability.ptzenabled**)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
panspeed	-5 ~ 5	0	1/4	Pan speed
tiltspeed	-5 ~ 5	0	1/4	Tilt speed
axisx	-175 ~ 175	0	1/4	Axis X coordinate, used internally.
axisy	-80 ~ 0	0	1/4	Axis Y coordinate, used internally.
returnhome	<boolean>	0	1/4	Enable/disable auto return home while idle
returnhomeinterval	<integer>	1	1/4	Wait interval return home
defaulthome	<boolean>	1	1/4	This field tells system to use default home position or not.
preset_i<0~19>_name	string[40]	<blank>	1/4	Name of the preset location.
patrol_i<0~39>_name	string[40]	<blank>	1/4	(For internal device) The name of patrol location
patrol_i<0~39>_dwelling	0 ~ 255	<blank>	1/4	(For internal device) The dwelling time of each patrol location
patrolseq	string[64]	<blank>	1/4	(For external device) The indexes of patrol points, separated by “,”
patroldwelling	string[128]	<blank>	1/4	(For external device) The dwelling time of each patrol point, separated by “,”

## 7.18 SNMP

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
v2	0~1	0	6/6	SNMP v2 enabled. 0 for disable, 1 for enable
v3	0~1	0	6/6	SNMP v3 enabled. 0 for disable, 1 for enable
secnamerw	string[31]	Private	6/6	Read/write security name
secnamero	string[31]	Public	6/6	Read only security name
authpwrw	string[8~128]	<blank>	6/6	Read/write authentication password
authpwro	string[8~128]	<blank>	6/6	Read only authentication password
authtyperw	MD5,SHA	MD5	6/6	Read/write authentication type
authtypero	MD5,SHA	MD5	6/6	Read only authentication type
encryptpwrw	string[8~128]	<blank>	6/6	Read/write passwr
encryptpwro	string[8~128]	<blank>	6/6	Read only password
encrypttyperw	DES	<blank>	6/6	Read/write encryption type
encrypttypero	DES	<blank>	6/6	Read only encryption type
rwcommunity	string[31]	Private	6/6	Read/write community
rocommunity	string[31]	Public	6/6	Ready only community



## 7.19 Layout configuration

Group: **layout**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
logo_default	<boolean>	1	1/6	0 => Custom logo 1 => Default logo
logo_link	string[64]	<a href="http://www.vivotek.com">http://www.vivotek.com</a>	1/6	Hyperlink of the logo
logo_powerbyvvtk_hidden	<boolean>	0	1/6	0 => display the power by vivotek logo 1 => hide the power by vivotek logo
theme_option	1~4	1	1/6	1~3: One of the default themes. 4: Custom definition.
theme_color_font	string[7]	#000000	1/6	Font color
theme_color_configfont	string[7]	#ffffff	1/6	Font color of configuration area.
theme_color_titlefont	string[7]	#098bd6	1/6	Font color of video title.
theme_color_controlbackground	string[7]	#c4eaff	1/6	Background color of control area.
theme_color_configbackground	string[7]	#0186d1	1/6	Background color of configuration area.
theme_color_videobackground	string[7]	#c4eaff	1/6	Background color of video area.
theme_color_case	string[7]	#0186d1	1/6	Frame color
custombutton_manualtrigger_show	<boolean>	1	1/6	Show or hide manual trigger (VI) button in homepage 0 -> Hidden 1 -> Visible

## 7.20 Capability

 Group: **capability**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
api_httpversion	0100a	0100a	0/7	The HTTP API version.
bootuptime	<positive integer>	60	0/7	Server bootup time.
nir	0, <positive integer>	0	0/7	Number of IR interfaces. (Recommend to use ir for built-in IR and extir for external IR)
npir	0, <positive integer>	0	0/7	Number of PIRs.
ndi	0, <positive integer>	0	0/7	Number of digital inputs.
nvi	0, <positive integer>	3	0/7	Number of virtual inputs (manual trigger)
ndo	0, <positive integer>	0	0/7	Number of digital outputs.
naudioin	0, <positive integer>	1	0/7	Number of audio inputs.
naudioout	0, <positive integer>	0	0/7	Number of audio outputs.
nvideoin	<positive integer>	1	0/7	Number of video inputs.
nvideoinprofile	<positive integer>	1	0/7	Number of video input profiles.
nmediastream	<positive integer>	2	0/7	Number of media stream per channels.
nvideosetting	<positive integer>	2	0/7	Number of video settings per channel.
naudiosetting	<positive integer>	1	0/7	Number of audio settings per channel.
nuart	0, <positive integer>	0	0/7	Number of UART interfaces.
nmotionprofile	0, <positive integer>	1	0/7	Number of motion profiles.
ptzenabled	0, <positive integer>	15	0/7	An 32-bit integer, each bit

	integer>			<p>can be set separately as follows:</p> <p>Bit 0 =&gt; Support camera control function; 0(not support), 1(support)</p> <p>Bit 1 =&gt; Built-in or external camera; 0(external), 1(built-in)</p> <p>Bit 2 =&gt; Support pan operation, 0(not support), 1(support)</p> <p>Bit 3 =&gt; Support tilt operation; 0(not support), 1(support)</p> <p>Bit 4 =&gt; Support zoom operation; 0(not support), 1(support)</p> <p>Bit 5 =&gt; Support focus operation; 0(not support), 1(support)</p> <p>Bit 6 =&gt; Support iris operation; 0(not support), 1(support)</p> <p>Bit 7 =&gt; External or built-in PT; 0(built-in), 1(external)</p> <p>Bit 8 =&gt; Invalidate bit 1 ~ 7; 0(bit 1 ~ 7 are valid), 1(bit 1 ~ 7 are invalid)</p> <p>Bit 9 =&gt; Reserved bit; Invalidate lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris. 0(fields are valid), 1(fields are invalid)</p>
windowless	<boolean>	1	0/7	Indicate whether to support windowless plug-in.
eptz	0, <positive	0	0/7	A 32-bit integer, each bit

	integer>			<p>can be set separately as follows:</p> <p>Bit 0 =&gt; stream 1 supports ePTZ or not.</p> <p>Bit 1 =&gt; stream 2 supports ePTZ or not.</p> <p>The rest may be deduced by analogy</p>
lens_pan	0, <positive integer>	3	0/7	<p>A 32-bit integer, each bit can be set separately as follows:</p> <p>Bit 0 =&gt; Support pan.</p> <p>Bit 1 =&gt; Support pan in UI.</p> <p>Bit 2 =&gt; External or built-in pan function; 0(built-in), 1(external).</p>
lens_tilt	0, <positive integer>	3	0/7	<p>A 32-bit integer, each bit can be set separately as follows:</p> <p>Bit 0 =&gt; Support tilt.</p> <p>Bit 1 =&gt; Support tilt in UI.</p> <p>Bit 2 =&gt; External or built-in tilt function; 0(built-in), 1(external).</p>
lens_zoom	0, <positive integer>	0	0/7	<p>A 32-bit integer, each bit can be set separately as follows:</p> <p>Bit 0 =&gt; Support zoom</p> <p>Bit 1 =&gt; Support zoom in UI</p> <p>Bit 2 =&gt; External or built-in zoom function; 0(built-in), 1(external).</p>
lens_focus	0, <positive integer>	0	0/7	<p>A 32-bit integer, each bit can be set separately as follows:</p> <p>Bit 0 =&gt; Support focus.</p> <p>Bit 1 =&gt; Support focus in UI.</p>

				Bit 2 => External or built-in focus function; 0(built-in), 1(external). Bit 3 => Support auto focus in UI.
lens_iris	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support iris. Bit 1 => Support iris in UI. Bit 2 => External or built-in iris function; 0(built-in), 1(external). Bit 3 => Support auto iris in UI.
npreset	0, <positive integer>	20	0/7	Number of preset locations.
protocol_https	<boolean >	1	0/7	Indicate whether to support HTTP over SSL.
protocol_rtsp	<boolean >	1	0/7	Indicate whether to support RTSP.
protocol_sip	<boolean>	0	0/7	Indicate whether to support SIP.
protocol_maxconnection	<positive integer>	10	0/7	The maximum allowed simultaneous connections.
protocol_maxgenconnection	<positive integer>	10	0/7	The maximum general streaming connections .
protocol_maxmegaconnection	<positive integer>	0	0/7	The maximum megapixel streaming connections.
protocol_rtp_multicast_scalable	<boolean>	1	0/7	Indicate whether to support scalable multicast.
protocol_rtp_multicast_backchannel	<boolean>	0	0/7	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	1	0/7	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	1	0/7	Indicate whether to support RTP over HTTP.

protocol_spush_mjpg	<boolean>	1	0/7	Indicate whether to support server push MJPEG.
protocol_snmp	<boolean>	1	0/7	Indicate whether to support SNMP.
protocol_ipv6	<boolean>	1	0/7	Indicate whether to support IPv6.
videoin_type	0, 1, 2	2	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_resolution	<a list of available resolution separated by commas>	320x200, 640x400, 1280x800	0/7	Available resolutions list.
videoin_maxframe rate	<a list of available maximum frame rate separated by commas>	30, 30, 30, 30, 30	0/7	Available maximum frame list.
videoin_codec	mpeg4, mjpeg, h264	mpeg4, mjpeg, h264	0/7	Available codec list.
videoout_codec	<a list of the available codec types separated by commas>	7,7	0/7	Available codec list.
audioin_codec	g711	g711	0/7	Available codec list for audio input.
uart_http tunnel	<boolean>	0	0/7	Indicate whether to support HTTP tunnel for UART transfer.
camctrl_http tunnel	<boolean>	0	0/7	The attribute indicates whether sending camera control commands through HTTP tunnel is supported. 0: Not supported 1: Supported
camctrl_privilege	<boolean>	1	0/7	Indicate whether to support

				<p>“Manage Privilege” of PTZ control in the Security page.</p> <p>1: support both /cgi-bin/camctrl/camctrl.cgi and /cgi-bin/viewer/camctrl.cgi 0: support only /cgi-bin/viewer/camctrl.cgi</p>
transmission_mode	Tx	TX	0/7	Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both = DVR.
network_wire	<boolean>	1	0/7	Indicate whether to support Ethernet.
network_wireless	<boolean>	0	0/7	Indicate whether to support wireless.
wireless_s802dot11b	<boolean>	0	0/7	Indicate whether to support wireless 802.11b+.
wireless_s802dot11g	<boolean>	0	0/7	Indicate whether to support wireless 802.11g.
wireless_encrypt_wep	<boolean>	0	0/7	Indicate whether to support wireless WEP.
wireless_encrypt_wpa	<boolean>	0	0/7	Indicate whether to support wireless WPA.
wireless_encrypt_wpa2	<boolean>	0	0/7	Indicate whether to support wireless WPA2.
derivative_brand	<boolean>	1	0/7	Indicate whether to support the upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)
evctrlchannel	<boolean>	1	0/7	Indicate whether to support HTTP tunnel for event/control transfer.
joystick	<boolean>	0	0/7	Indicate whether to support

				joystick control.
storage_dbenabled	<boolean>	1	0/7	Media files are indexed in database.
nanystream	0, <positive integer>	0	0/7	number of any media stream per channel
iva	<boolean>	0	0/7	Indicate whether to support Intelligent Video analysis
ir	<boolean>	0	0/7	Indicate whether to support built-in IR led.
tampering	<boolean>	1	0/7	Indicate whether to support tampering detection.
image_wdrc	<Boolean>	0	0/7	Indicate whether to support WDRC
image_iris	<string>	dciris	0/7	Indicate iris type.
image_focusassist	<Boolean>	0	0/7	Indicate whether to support focus assist.
adaptiverecording	<boolean>	1	0/7	Indicate whether to support adaptive recording.
adaptivestreaming	<boolean>	1	0/7	Indicate whether to support adaptive streaming.

## 7.21 Customized event script

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

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



## 7.22 Event setting

Group: event\_i<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry.
enable	0, 1	0	6/6	Enable or disable this event.
priority	0, 1, 2	1	6/6	Indicate the priority of this event: “0” = low priority “1” = normal priority “2” = high priority
delay	1~999	20	6/6	Delay in seconds before detecting the next event.
trigger	boot, di, motion, seq, renotify, tampering, vi	boot	6/6	Indicate the trigger condition: “boot” = System boot “di” = Digital input “motion” = Video motion detection “seq” = Periodic condition “renotify” = Recording notification. “tampering” = Tamper detection. “vi” = Virtual input (Manual trigger)
triggerstatus	String[40]	trigger	6/6	The status for event trigger
di	<integer>	1	6/6	Indicate the source id of di trigger. This field is required when trigger condition is “di”. One bit represents one digital input. The LSB indicates DI 0.
vi	<integer>	0	6/6	Indicate the source id of vi trigger. This field is required when trigger condition is “vi”. One bit represents one digital input. The LSB indicates VI 0.

mdwin	<integer>	0	6/6	<p>Indicate the source window id of motion detection.</p> <p>This field is required when trigger condition is “md”.</p> <p>One bit represents one window.</p> <p>The LSB indicates the 1<sup>st</sup> window.</p> <p>For example, to detect the 1<sup>st</sup> and 3<sup>rd</sup> windows, set mdwin as 5.</p>
mdwin0	<integer>	0	6/6	<p>Similar to mdwin. The parameter takes effect when profile 1 of motion detection is enabled.</p>
inter	1~999	1	6/6	<p>Interval of snapshots in minutes.</p> <p>This field is used when trigger condition is “seq”.</p>
weekday	0~127	127	6/6	<p>Indicate which weekday is scheduled.</p> <p>One bit represents one weekday.</p> <p>bit0 (LSB) = Saturday</p> <p>bit1 = Friday</p> <p>bit2 = Thursday</p> <p>bit3 = Wednesday</p> <p>bit4 = Tuesday</p> <p>bit5 = Monday</p> <p>bit6 = Sunday</p> <p>For example, to detect events on Friday and Sunday, set weekday as 66.</p>
begintime	hh:mm	00:00	6/6	<p>Begin time of the weekly schedule.</p>
endtime	hh:mm	24:00	6/6	<p>End time of the weekly schedule.</p> <p>(00:00 ~ 24:00 sets schedule as always on)</p>
lowlightcondition	0, 1	1	6/6	<p>Switch on white light LED in low light condition</p> <p>0 =&gt; Do action at all times</p> <p>1 =&gt; Do action in low-light conditions</p>
action_cf_enable	0, 1	0	6/6	<p>Enable media write on CF or other local storage media</p>
action_cf_folder	string[128]	NULL	6/6	<p>Path to store media.</p>

action_cf_media	NULL, 0~4	NULL	6/6	Index of the attached media.
action_cf_datefolder	<boolean>	0	6/6	Enable this to create folders by date, time, and hour automatically.
action_cf_backup	<boolean>	0	6/6	Enable the capability of backing up recorded files to the SD card when network is lost. 0: Disabled 1: Enabled
action_server_i<0~4>_enable	0, 1	0	6/6	Enable or disable this server action.
action_server_i<0~4>_media	NULL, 0~4	NULL	6/6	Index of the attached media.
action_server_i<0~4>_datefolder	<boolean>	0	6/6	Enable this to create folders by date, time, and hour automatically.

## 7.23 Server setting for event action

Group: server\_i<0~4>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	email, ftp, http, ns	email	6/6	Indicate the server type: “email” = email server “ftp” = FTP server “http” = HTTP server “ns” = network storage
http_url	string[128]	http://	6/6	URL of the HTTP server to upload.
http_username	string[64]	NULL	6/6	Username to log in to the server.
http_passwd	string[64]	NULL	6/6	Password of the user.
ftp_address	string[128]	NULL	6/6	FTP server address.
ftp_username	string[64]	NULL	6/6	Username to log in to the server.
ftp_passwd	string[64]	NULL	6/6	Password of the user.
ftp_port	0~65535	21	6/6	Port to connect to the server.
ftp_location	string[128]	NULL	6/6	Location to upload or store the media.
ftp_passive	0, 1	1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode

email_address	string[128]	NULL	6/6	Email server address.
email_sslmode	0, 1	0	6/6	Enable support SSL.
email_port	0~65535	25	6/6	Port to connect to the server.
email_username	string[64]	NULL	6/6	Username to log in to the server.
email_passwd	string[64]	NULL	6/6	Password of the user.
email_senderemail	string[128]	NULL	6/6	Email address of the sender.
email_recipientemail	string[640]	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.

## 7.24 Media setting for event action

Group: **media\_i<0~4>** (media\_freespace is used internally.)

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	snapshot, systemlog, videoclip, recordmsg	snapshot	6/6	Media type to send to the server or store on the server.
snapshot_source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
snapshot_prefix	string[16]	NULL	6/6	Indicate the prefix of the filename.
snapshot_datesuffix	0, 1	0	6/6	Add date and time suffix to filename: 1 = Add date and time suffix. 0 = Do not add.
snapshot_preevent	0 ~ 7	1	6/6	Indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	1	6/6	The number of post-event images.

videoclip_source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
videoclip_prefix	string[16]	NULL	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	50~3072	500	6/6	Maximum size of one video clip file in Kbytes.

## 7.25 Recording

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

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry.
enable	0, 1	0	6/6	Enable or disable this recording.
priority	0, 1, 2	1	6/6	Indicate the priority of this recording: “0” indicates low priority. “1” indicates normal priority. “2” indicates high priority.
source	0,1	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	<p>Indicate which notification server is scheduled.</p> <p>One bit represents one application server (server_i0~i4).</p> <p>bit0 (LSB) = server_i0.</p> <p>bit1 = server_i1.</p> <p>bit2 = server_i2.</p> <p>bit3 = server_i3.</p> <p>bit4 = server_i4.</p> <p>For example, enable server_i0, server_i2, and server_i4 as notification servers; the notifyserver value is 21.</p>
weekday	0~127	127	6/6	<p>Indicate which weekday is scheduled.</p> <p>One bit represents one weekday.</p> <p>bit0 (LSB) = Saturday</p> <p>bit1 = Friday</p> <p>bit2 = Thursday</p> <p>bit3 = Wednesday</p> <p>bit4 = Tuesday</p> <p>bit5 = Monday</p> <p>bit6 = Sunday</p> <p>For example, to detect events on Friday and Sunday, set weekday as 66.</p>
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]	NULL	6/6	Indicate the prefix of the filename.
cyclesize	100~	100	6/6	The maximum size for cycle recording in Kbytes when choosing to limit recording size.
reserveamount	0~15000000	100	6/6	The reserved amount in Mbytes when choosing cyclic recording mechanism.

dest	cf, 0	cf	6/6	The destination to store the recorded data. “cf” means local storage (CF or SD card). “0” means the index of the network storage.
cffolder	string[128]	NULL	6/6	Folder name.
maxsize	100~900	100	6/6	Unit: Mega bytes. When this condition is reached, recording file is truncated.
maxduration	60~1800	60	6/6	Unit: Second When this condition is reached, recording file is truncated.
trigger	schedule, networkfail	schedule	6/6	The event trigger type schedule: The event is triggered by schedule networkfail: The event is triggered by the failure of network connection.
adaptive_enable	0,1	0	6/6	Indicate whether the adaptive recording is enabled
adaptive_preevent	0~9	5	6/6	Indicate when is the adaptive recording started before the event trigger point (seconds)
adaptive_postevent	0~10	5	6/6	Indicate when is the adaptive recording stopped after the event trigger point (seconds)

## 7.26 HTTPS

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	To enable or disable secure HTTP.
policy	<Boolean>	0	6/6	If the value is 1, it will force HTTP connection redirect to HTTPS connection
method	auto, manual, install	auto	6/6	auto => Create self-signed certificate automatically. manual => Create self-signed certificate manually. install => Create certificate request and install.
status	-3 ~ 1	0	6/7	Specify the https status. -3 = Certificate not installed -2 = Invalid public key -1 = Waiting for certificate 0 = Not installed 1 = Active
countryname	string[2]	TW	6/6	Country name in the certificate information.
stateorprovincename	string[128]	Asia	6/6	State or province name in the certificate information.
localityname	string[128]	localityname	6/6	The locality name in the certificate information.
organizationname	string[64]	VIVOTEK Inc.	6/6	Organization name in the certificate information.
unit	string[32]	>VIVOTEK Inc.	6/6	Organizational unit name in the certificate information.
commonname	string[64]	www.vivotek .com	6/6	Common name in the certificate information.
validdays	0 ~ 3650	3650	6/6	Valid period for the certification.



## 7.27 Storage management setting

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

Group: **disk\_i<0~(n-1)>** n is the total number of storage devices. (capability.storage.dbenabled > 0)

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

## 7.28 Region of interest

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

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
s<0~(m-1)>_home	"0~1104", "0~656"	0,0	6/6	ROI left-top corner coordinate.
s<0~(m-1)>_size	"176~1280"x"144~800"	1280x800	6/6	ROI width and height. The width value must be multiples of 16 and the height value must be multiples of 8

## 8. Useful Functions

### 8.1 Capture Single Snapshot

**Note:** This request requires Normal User privileges.

**Method:** GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>][&streamid=<value>]
```

If the user requests a size larger than all stream settings on the server, this request will fail.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	The channel number of the video source.
resolution	<available resolution>	0	The resolution of the image.
quality	1~5	3	The quality of the image.
streamid	0~(m-1)	<product dependent>	The stream number.

The server will return the most up-to-date snapshot of the selected channel and stream in JPEG format. The size and quality of the image will be set according to the video settings on the server.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]
<binary JPEG image data>
```

### 8.2 Account Management

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

**Method:** GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<name>[&userpass=<value>][&privilege=<value>]
[&privilege=<value>][...][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to the server. When using this method, the “username” field is necessary. It will use the default value of other fields if not specified.
	Delete	Remove an account from the server. When using this method, the “username” field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, the “username” field is necessary, and other fields are optional. If not specified, it will keep the original settings.
username	<name>	The name of the user to add, delete, or edit.
userpass	<value>	The password of the new user to add or that of the old user to modify. The default value is an empty string.
Privilege	<value>	The privilege of the user to add or to modify.
	viewer	Viewer privilege.
	operator	Operator privilege.
	admin	Administrator privilege.
Return	<return page>	Redirect to the page <return page> after the parameter is assigned. The <return page> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

## 8.3 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\nContent-Type: text/plain\r\nContent-Length: <syslog length>\r\n\r\n<system log information>\r\n
```

## 8.4 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.

## 8.5 Camera Control (capability.ptzenabled)

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

**Method:** GET/POST

Syntax:

```
http://<servername>/cgi-bin/camctrl/camctrl.cgi[channel=<value>][&camid=<value>]
[&move=<value>] – Move home, up, down, left, right
[&auto=<value>] – Auto pan, patrol
[ [&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>][&speedlink=<value>] ] – Set speeds
[&return=<return page>]
```

**Example:**

```
http://myserver/cgi-bin/camctrl/camctrl.cgi?channel=0&camid=1&move=right
http://myserver/cgi-bin/camctrl/camctrl.cgi?channel=0&camid=1&x=300&y=200&resolution=704x480&videosize=704x480&stretch=1
```

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
camid	0,<positive integer>	Camera ID.
move	home	Move to camera to home position.
	up	Move camera up.
	down	Move camera down.
	left	Move camera left.
	right	Move camera right.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop camera.
return	<return page>	Redirect to the page <return page> after the parameter is assigned. The <return page> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

## 8.6 Recall (capability.ptzenabled)

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

Method: GET/POST

Syntax:

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

PARAMETER	VALUE	DESCRIPTION
recall	Text string less than 30 characters	One of the present positions to recall.
channel	<0~(n-1)>	Channel of the video source.
return	<return page>	Redirect to the page <return page> after the parameter is assigned. The <return page> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

## 8.7 Preset Locations (capability.ptzenabled)

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

Method: GET/POST

Syntax:

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

PARAMETER	VALUE	DESCRIPTION
addpos	<Text string less than 30 characters>	Add one preset location to the preset list.
channel	<0~(n-1)>	Channel of the video source.
delpos	<Text string less than 30 characters>	Delete preset location from preset list.
return	<return page>	Redirect to the page <return page> after the parameter is

assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

## 8.8 IP Filtering

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

**Method:** GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/ipfilter.cgi?
method=<value>&[start=<ipaddress>&end=<ipaddress>][&index=<value>]
[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
method	addallow	Add allowed IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	adddeny	Add denied IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	deleteallow	Remove allowed IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
	deletedeny	Remove denied IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start	<ip address>	The starting IP address to add or to delete.
end	<ip address>	The ending IP address to add or to delete.
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <i>&lt;return page&gt;</i> after the parameter is assigned. The <i>&lt;return page&gt;</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.

## 8.8.1 IP Filtering for ONVIF

Syntax: <product dependent>

http://<servername>/cgi-bin/admin/ipfilter.cgi?type[=<value>]

http://<servername>/cgi-bin/admin/ipfilter.cgi?method=add<v4/v6>&ip=<ipaddress> [&index=<value>][&return=<return page>]

http://<servername>/cgi-bin/admin/ipfilter.cgi?method=del<v4/v6>&index=<value> [&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
type	NULL	Get IP filter type
	allow, deny	Set IP filter type
method	addv4	Add IPv4 address into access list.
	addv6	Add IPv6 address into access list.
	delv4	Delete IPv4 address from access list.
	delv6	Delete IPv6 address from access list.
ip	<IP address>	Single address: <IP address> Network address: <IP address / network mask> Range address: <start IP address - end IP address>
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <return page> after the parameter is assigned. The <return page> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.



## 8.9 Event/Control HTTP Tunnel Channel (capability.

### evctrlchannel > 0)

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

**Method:** GET and POST

Syntax:

```
http://<servername>/cgi-bin/admin/ctrllevent.cgi
```

---

```
GET /cgi-bin/admin/ctrllevent.cgi
```

```
x-sessioncookie: string[22]
```

```
accept: application/x-vvtek-tunnelled
```

```
pragma: no-cache
```

```
cache-control: no-cache
```

---

```
POST /cgi-bin/admin/ctrllevent.cgi
```

```
x-sessioncookie: string[22]
```

```
content-type: application/x-vvtek-tunnelled
```

```
pragma : no-cache
```

```
cache-control : no-cache
```

```
content-length: 32767
```

```
expires: Sun, 9 Jan 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

## 8.10 Get SDP of Streams

**Note:** This request requires Viewer access privileges.

**Method:** GET

Syntax:

```
http://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

“m” is the stream number.

“network\_accessname\_<0~(m-1)>” is the accessname for stream “1” to stream “m”. Please refer to the “subgroup of network: rtsp” for setting the accessname of SDP.

You can get the SDP by HTTP GET.

When using scalable multicast, Get SDP file which contains the multicast information via HTTP.

## 8.11 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.

## 8.12 Storage managements (capability.storage.dbenabled > 0)

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

**Method:** GET and POST

Syntax:

```
http://<servername>/cgi-bin/admin/lscrtl.cgi?cmd=<cmd_type>[&<parameter>=<value>...]
```

The commands usage and their input arguments are as follows.

PARAMETER	VALUE	DESCRIPTION
cmd_type	<string>	Required. Command to be executed, including <i>search</i> , <i>insert</i> , <i>delete</i> , <i>update</i> , and <i>queryStatus</i> .

Command: **search**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Optional. The integer primary key column will automatically be assigned a unique integer.
triggerType	<text>	Optional. Indicate the event trigger type. Please embrace your input value with single quotes. Ex. mediaType='motion' Support trigger types are product dependent.
mediaType	<text>	Optional. Indicate the file media type. Please embrace your input value with single quotes. Ex. mediaType='videoclip' Support trigger types are product dependent.
destPath	<text>	Optional. Indicate the file location in camera. Please embrace your input value with single quotes. Ex. destPath ='mnt/auto/CF/NCMF/abc.mp4'
resolution	<text>	Optional. Indicate the media file resolution. Please embrace your input value with single quotes. Ex. resolution='800x600'

isLocked	<boolean>	Optional. Indicate if the file is locked or not. 0: file is not locked. 1: file is locked. A locked file would not be removed from UI or cyclic storage.
triggerTime	<text>	Optional. Indicate the event trigger time. (not the file created time) Format is “YYYY-MM-DD HH:MM:SS” Please embrace your input value with single quotes. Ex. triggerTime='2008-01-01 00:00:00' If you want to search for a time period, please apply “TO” operation. Ex. triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59' is to search for records from the start of Jan 1 <sup>st</sup> 2008 to the end of Jan 1 <sup>st</sup> 2008.
limit	<positive integer>	Optional. Limit the maximum number of returned search records.
offset	<positive integer>	Optional. Specifies how many rows to skip at the beginning of the matched records. Note that the offset keyword is used after limit keyword.

To increase the flexibility of search command, you may use “OR” connectors for logical “OR” search operations. Moreover, to search for a specific time period, you can use “TO” connector.

Ex. To search records triggered by motion or di or sequential and also triggered between 2008-01-01 00:00:00 and 2008-01-01 23:59:59.

```
http://<servername>/cgi-bin/admin/lscrtl.cgi?cmd=search&triggerType='motion'+OR+'di'+OR+'seq'
&triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59'
```

**Command: delete**

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

Ex. Delete records whose key numbers are 1, 4, and 8.

```
http://<servername>/cgi-bin/admin/lscrtl.cgi?cmd=delete&label=1&label=4&label=8
```

Command: **update**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1
isLocked	<boolean>	Required. Indicate if the file is locked or not.

Ex. Update records whose key numbers are 1 and 5 to be locked status.

```
http://<servername>/cgi-bin/admin/lscrtl.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/lscrtl.cgi?cmd=update&isLocked=0&label=2&label=3
```

### 8.12.1 Return Message

The returned results are always in XML format, except for storage status related elements that can be returned in javascript format. (i.e. status, totalSize, freeSize, and usedSize.)

The elements are listed as follows.

Group: **stormgr**

Element name	Type	Description	
counts	<Positive Integer>	Total number of matched records.	
limit	<Positive Integer>	Limit the maximum number of returned search records. Could be empty if not specified.	
offset	<Positive Integer>	Specifies how many rows to skip at the beginning of the matched records. Could be empty if not specified.	
statusCode	<Integer>	The reply status (see table below)	
		Value of return-code	Description
		200	OK
		400	Unrecognized Message Type/Content
		500	Server executes command error.
		501	Parse Input Message Failed.
		502	Error Occurs When Searching Database.
503	Storage is Not Ready.		
statusString	string	Return string describing the reason that status code is not	

		OK.
--	--	-----

Subgroup of **stormgr: i<0~(n-1)>**: n is the total number of displayed records.

Element name	Type	Description
label	<Integer Primary Key>	A unique integer.
triggerType	<Text>	Indicate the event trigger type.
mediaType	<Text>	Indicate the file media type.
destPath	<Text>	Indicate the file location in camera.
resolution	<Text>	Indicate the media file resolution.
isLocked	<Boolean>	Indicate if the file is locked or not.
triggerTime	<Text>	Indicate the event trigger time. Format is "YYYY-MM-DD HH:MM:SS"
backup	<Boolean>	Indicate if the file is generated when network loss.

Subgroup of **stormgr\_disk: i<0~(n-1)>**: n is the total number of storage devices.

Element name	Type	Description
name	string	Description of specified storage device.
status	ready, detached, error, and readonly	The storage device status. ready: storage is ready for access. detached: storage is not mounted. error: failed to open storage device. readonly: storage is write protected.
totalSize	<Positive Integer>	The overall storage size in kilobytes.
freeSize	<Positive Integer>	The available storage size in kilobytes.
usedSize	<Positive Integer>	The used storage size in kilobytes.
path	string	Location of database of storage sink

Ex. Returned results of search command

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<stormgr version="0.0.0.1">
  <counts>5</counts>
  <limit>2</limit>
  <offset>0</offset >
  <i0>
    <label>1</label>
    <triggerType>motion</triggerType>
    <mediaType>videoclip</mediaType>
    <destPath>/mnt/auto/NCMF/abc/abc.jpg</destPath>
    <resolution>800x600</resolution>
```

```

<isLocked>0</isLocked>
<triggerTime>2009-01-24 12:00:00</triggerTime>
<backup>0</backup>
</i0>
<i1>
  <label>2</label>
  <triggerType>di</triggerType>
  <mediaType>snapshot</mediaType>
  <destPath>/mnt/auto/NCMF/123/123.jpg</destPath>
  <resolution>800x600</resolution>
  <isLocked>0</isLocked>
  <triggerTime>2009-01-24 12:01:00</triggerTime>
  <backup>0</backup>
</i1>
</stormgr>

```

Ex. Local storage status in XML format.

```

<?xml version="1.0" encoding="ISO-8859-1" ?>
<stormgr version="0.0.0.1">
  <disk>
    <i0>
      <name>SDcard</name>
      <status>ready</status>
      <totalSize>7824444</totalSize>
      <freeSize>7824388</freeSize>
      <usedSize>56</usedSize>
    </i0>
  </disk>
</stormgr>

```

Ex. Local storage status in javascript format.

```

disk_i0_name='SDcard'
disk_i0_status='ready'
disk_i0_totalSize='7824444'
disk_i0_freeSize='7824388'
disk_i0_usedSize='56'
disk_i0_path=i0/NCMF/.db/.localStorage.db

```

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/lscrtl.cgi?cmd=queryStatus&retType=javascript
```

There are two cgi commands for download and composing jpegs to avi format.

For download single selected file, you can use “/cgi-bin/admin/**downloadMedias.cgi**”. Just assign the request file path to this cgi.

Syntax:

```
http://<servername>/cgi-bin/admin/downloadMedias.cgi?<File_Path>
```

The <File\_Path> is in queryStatus return message.

Ex.

```
http://<servername>/cgi-bin/admin/downloadMedias.cgi?/mnt/auto/CF/NCMF/20090310/07/02.mp4
```

For creating an AVI file by giving a list of JPEG files, you can use “/cgi-bin/admin/**jpegtoavi.cgi**”.

Syntax:

```
http://<servername>/cgi-bin/admin/jpegtoavi.cgi?<resolution>=<width>x<height>&<fps>=<num>&<list>=<fileList>
```

PARAMETER	VALUE	DESCRIPTION
resolution	<width>x<height>	Resolution
fps	<positive integer>	Frame rate
list	<fileList>	The JPEG file list. The file path should be embraced by single quotation marks

Ex.



```
http:// <servername>/cgi-bin/admin/
jpegtoavi.cgi?resolution=800x600&fps=1&list='/mnt/auto/CF/NCMF/video1650.jpg', '/mnt/auto/C
F/NCMF/video1651.jpg', '/mnt/auto/CF/NCMF/video1652.jpg',
```

## 8.13 Virtual input (capability.nvi > 0)

**Note:** Change virtual input (manual trigger) status.

**Method:** GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/setvi.cgi?vi0=<value>[&vi1=<value>][&vi2=<value>]
[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
vi<num>	state[(duration)nstate]  Where "state" is 0, 1. "0" means inactive or normal state while "1" means active or triggered state.  Where "nstate" is next state after duration.	Ex: vi0=1  Setting virtual input 0 to trigger state  Ex: vi0=0(200)1  Setting virtual input 0 to normal state, waiting 200 <b>milliseconds</b> , setting it to trigger state.  Note that when the virtual input is waiting for next state, it cannot accept new requests.
return	<return page>	Redirect to the page <return page> after the request is completely assigned. The <return page> can be a full URL path or relative path according the current path. If you omit this parameter, it will redirect to an empty page.

Return Code	Description
200	The request is successfully executed.
400	The request cannot be assigned, ex. incorrect parameters. Examples: 1. setvi.cgi?vi0=0(10000)1(15000)0(20000)1 No multiple duration. 2. setvi.cgi?vi3=0

	<p>VI index is out of range.</p> <p>3. setvi.cgi?vi=1</p> <p>No VI index is specified.</p>
503	<p>The resource is unavailable, ex. Virtual input is waiting for next state.</p> <p>Examples:</p> <p>1. setvi.cgi?vi0=0(15000)1</p> <p>2. setvi.cgi?vi0=1</p> <p>Request 2 will not be accepted during the execution time(15 seconds).</p>

### 8.14 Open Timeshift Stream (capability.timeshift > 0, timeshift\_enable=1, timeshift\_c<n>\_s<m>\_allow=1)

**Note:** This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

```
http://<servername>/<network_http_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&reftime=<value>&forcechk&minsft=<value>]
```

For RTSP (MP4 and H264), the user needs to input the URL below into an RTSP compatible player.

```
rtsp://<servername>/<network_rtsp_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&reftime=<value>&forcechk&minsft=<value>]
```

“n” is the channel index.

“m” is the timeshift stream index.

For details on timeshift stream, please refer to the “TimeshiftCaching” documents.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
maxsft	<positive integer>	0	Request cached stream at most how many seconds ago.
tsmode	normal, adaptive	normal	Streaming mode: normal => Full FPS all the time. adaptive => Default send only I-frame for MP4 and H.264, and send 1 FPS for MJPEG. If DI or motion window are triggered, the streaming is changed to send full FPS for 10 seconds. (*Note: this parameter also works on non-timeshift streams.)

reftime	mm:ss	The time camera receives the request.	Reference time for maxsft and minsft. (This provides more precise time control to eliminate the inaccuracy due to network latency.) Ex: Request the streaming from 12:20 rtsp://10.0.0.1/live.sdp?maxsft=10&reftime=12:30
forcechk	N/A	N/A	Check if the requested stream enables timeshift, feature and if minsft is achievable. If false, return "415 Unsupported Media Type".
minsft	<positive integer>	0	How many seconds of cached stream client can accept at least. (Used by forcechk)

Return Code	Description
400 Bad Request	Request is rejected because some parameter values are illegal.
415 Unsupported Media Type	Returned, if forcechk appears, when minsft is not achievable or the timeshift feature of the target stream is not enabled.

## 8.15 Export Files

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

**Method:** GET

Syntax:

For daylight saving time configuration file:

`http://<servername>/cgi-bin/admin/exportDst.cgi`

For language file:

`http://<servername>/cgi-bin/admin/export_language.cgi?currentlanguage=<value>`

PARAMETER	VALUE	DESCRIPTION
currentlanguage	0~20	Available language lists. Please refer to: system_info_language_i0 ~ system_info_language_i19.

For setting backup file:

`http://<servername>/cgi-bin/admin/export_backup.cgi?backup`

## 8.16 Upload Files

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

**Method:** POST

Syntax:

For daylight saving time configuration file:

```
http://<servername>/cgi-bin/admin/upload_dst.cgi
```

Post data:

```
filename =<file name>\r\n\r\n<multipart encoded form data>
```

For language file:

```
http://<servername>/cgi-bin/admin/upload_lan.cgi
```

Post data:

```
filename =<file name>\r\n\r\n<multipart encoded form data>
```

For setting backup file:

```
http://<servername>/cgi-bin/admin/upload_backup.cgi
```

Post data:

```
filename =<file name>\r\n\r\n<multipart encoded form data>
```

Server will accept the file named <file name> to upload this one to camera.

**<End of document>**

# Technical Specifications

## Technical Specifications

System Information		Intelligent Video	
CPU	Multimedia SoC (System-on-Chip)	Video Motion Detection	Triple-window video motion detection
Flash	16 MB	<b>Alarm and Event</b>	
RAM	128 MB	Alarm Triggers	Video motion detection, manual trigger, periodical trigger, system boot, recording notification, camera tampering detection
<b>Camera Features</b>		Alarm Events	Event notification using digital output, HTTP, SMTP, FTP and NAS server File upload via HTTP, SMTP, FTP and NAS server
Image Sensor	1/4" Progressive CMOS	<b>General</b>	
Maximum Resolution	1280x800	Connectors	RJ-45 for Network/PoE connection
Lens Type	Fixed-focal	LED Indicator	System power and status indicator
Focal Length	f = 3.6 mm	Power Input	IEEE 802.3af PoE Class 2
Aperture	F1.8	Power Consumption	Max. 6.24 W
Field of View	56° (horizontal) 41° (vertical) 71° (diagonal)	Dimensions	Ø: 120 mm x 55 mm
Shutter Time	1/5 sec. to 1/32,000 sec.	Weight	Net: 180 g
Minimum Illumination	0.47 Lux, 50 IRE	Safety Certifications	CE, LVD, FCC Class B, VCCI, C-Tick
Pan Speed	100° / sec.	Operating Temperature	0°C ~ 45°C (32°F ~ 113°F)
Pan Range	360° (-180° ~ + 180°)	Warranty	24 months
Tilt Speed	100° / sec.	<b>System Requirements</b>	
Tilt Range	80° (10° ~ 90°)	Operating System	Microsoft Windows 7/Vista/XP/2000
Pan/tilt/zoom	ePTZ:	Web Browser	Mozilla Firefox 7~10 (streaming only) Internet Explorer 7.x or 8.x
Functionalities	16x digital zoom (4x on IE plug-in, 4x built-in)	Other Players	VLC: 1.1.11 or above QuickTime: 7 or above
On-board Storage	MicroSD/SDHC card slot	<b>Included Accessories</b>	
<b>Video</b>		CD	User's manual, quick installation guide, Installation Wizard 2, ST7501 32-channel recording software
Compression	H.264, MJPEG & MPEG-4	Others	Quick installation guide, warranty card, camera mounting kit
Maximum Frame Rate	H.264: 30 fps at 1280x800 MPEG-4: 30 fps at 1280x800 MJPEG: 30 fps at 1280x800	<b>Dimensions</b>	
Maximum Streams	2 simultaneous streams		
S/N Ratio	Above 50 dB		
Video Streaming	Adjustable resolution, quality and bitrate Configurable video cropping for bandwidth saving		
Image Settings	Adjustable image size, quality and bit rate Time stamp, text overlay, flip & mirror Configurable brightness, contrast, saturation, sharpness, white balance, exposure control, gain, backlight compensation, privacy masks Scheduled profile settings		
<b>Audio</b>			
Audio Capability	Audio input		
Compression	G.711		
Interface	Built-in microphone		
Effective Range	5 meters		
<b>Network</b>			
Users	Live viewing for up to 10 clients		
Protocols	IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP, 802.1X		
Interface	10Base-T/100 BaseTX Ethernet (RJ-45)		
ONVIF	Supported, specification available at <a href="http://www.onvif.org">www.onvif.org</a>		

## Compatible Accessories

### PoE Kits



**MS-POE-IJAF**  
PoE injector, 802.3af compliant

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

Distributed by:



#### VIVOTEK INC.

6F, No.192, Lien-Cheng Rd., Chung-Ho, New Taipei City, 235, Taiwan, R.O.C.  
| T: +886-2-82455282 | F: +886-2-82455532 | E: [sales@vivotek.com](mailto:sales@vivotek.com)

#### VIVOTEK USA, INC.

2050 Ringwood Avenue, San Jose, CA 95131  
| T: 408-773-8686 | F: 408-773-8298 | E: [salesusa@vivotek.com](mailto:salesusa@vivotek.com)

Ver 1.0

## Technology License Notice

### MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT WITH REGARD TO PC SOFTWARE, OF WHICH YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO [HTTP://WWW.VIALICENSING.COM](http://www.vialicensing.com).

### MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

### AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT. 0516621; US PAT. 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT [HTTP://WWW.VOICEAGE.COM](http://www.voiceage.com).

## Electromagnetic Compatibility (EMC)

### FCC Statement

This device complies with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

### CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

### VCCI Warning

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス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.