

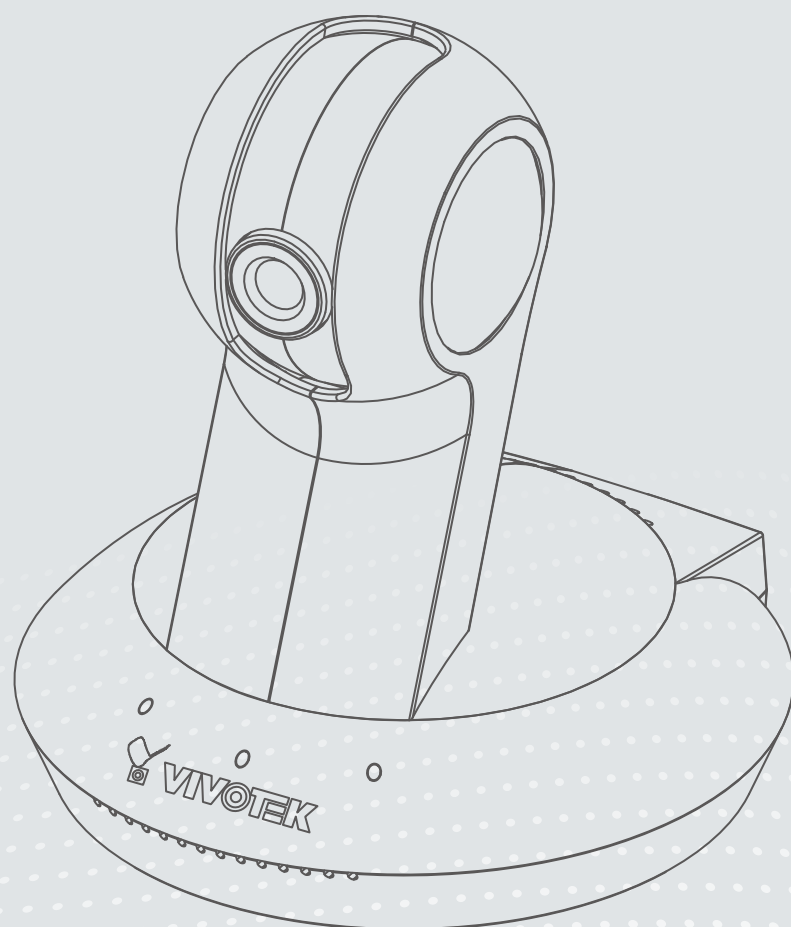


**PT8133/33W** Pan/Tilt  
Network Camera

# User's Manual

PT8133: 1MP • PoE

PT8133W: 1MP • WPS • 802.11n



Rev. 1.0

## Table of Contents

---

Package Contents .....	3
<b>Overview</b> .....	<b>4</b>
Read Before Use.....	4
Package Contents .....	4
Physical Description .....	5
Network Deployment.....	9
Software Installation .....	12
Configure the Wireless Connection (PT8133W) .....	13
<b>Accessing the Network Camera</b> .....	<b>15</b>
Using Web Browsers.....	15
Using RTSP Players.....	18
Using 3GPP-compatible Mobile Devices.....	19
Using VIVOTEK Recording Software .....	20
<b>Main Page</b> .....	<b>21</b>
Camera Control Area.....	21
Onscreen Mouse Control .....	22
<b>Client Settings</b> .....	<b>30</b>
Local Streaming Buffer Time .....	31
<b>Configuration</b> .....	<b>32</b>
System .....	33
Security .....	35
HTTPS (Hypertext Transfer Protocol over SSL) .....	36
SNMP (Simple Network Management Protocol) .....	41
Network .....	42
<b>Network Type</b> .....	<b>42</b>
IEEE 802.1x .....	48
Network > QoS (Quality of Service) .....	50
Network > HTTP .....	52
<b>Wireless (PT8133W only)</b> .....	<b>57</b>
Manual Configuration: .....	57
WPS: .....	62
DDNS .....	63
Access List .....	65
Audio and Video .....	68
Motion Detection .....	77
Camera Control .....	80
Homepage Layout .....	83
Application .....	86
Recording .....	99

System Log .....	103
View Parameters .....	104
Maintenance .....	105
<i>Appendix</i> .....	<i>109</i>
URL Commands for the Network Camera.....	109
Technical Specifications .....	173
Technology License Notice.....	174
Electromagnetic Compatibility (EMC).....	175

## Package Contents

Revision 1.0: Initial release.

## Overview

VIVOTEK PT8133 (PoE)/ 33W (WLAN) 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. The camera is designed for indoor surveillance applications such as retail stores, offices, or banks.

With flexible 350-degree pan and 125-degree tilt, PT8133/33W gives users more comprehensive control over a monitored site. The PT8133/33W supports the industry-standard H.264 compression technology, drastically reducing file sizes and conserving valuable network bandwidth. With MPEG-4 and MJPEG compatibility also included, video streams can also be transmitted in any of these formats for versatile applications. The streams can also be individually configured to meet different constraints, thereby further reducing bandwidth and storage requirements. Users can thus receive multiple streams simultaneously in different resolutions, frame rates, and image qualities for viewing on different platforms.

In addition, PT8133 is integrated with Power over Ethernet functionality, while PT8133W boasts 802.11b/g/n compatible wireless connection, making installation easier and more cost-efficient. The WPS function of PT8133W makes wireless configuration easy and straightforward. Together with the free, 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 and complies with all privacy laws 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 more 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.

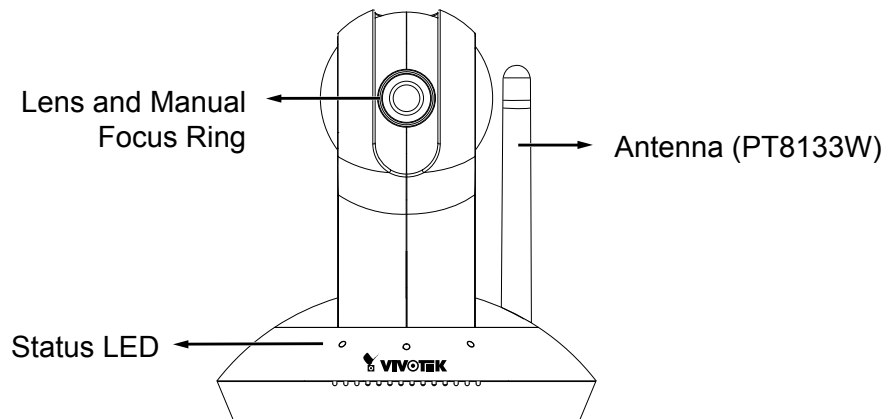
## Package Contents

■ PT8133/PT8133W	■ Warranty Card
■ Power Adapter	■ Software CD
■ Antenna (PT8133W only)	■ Mount kit and Foot Pads
■ Screws	
■ Quick Installation Guide	



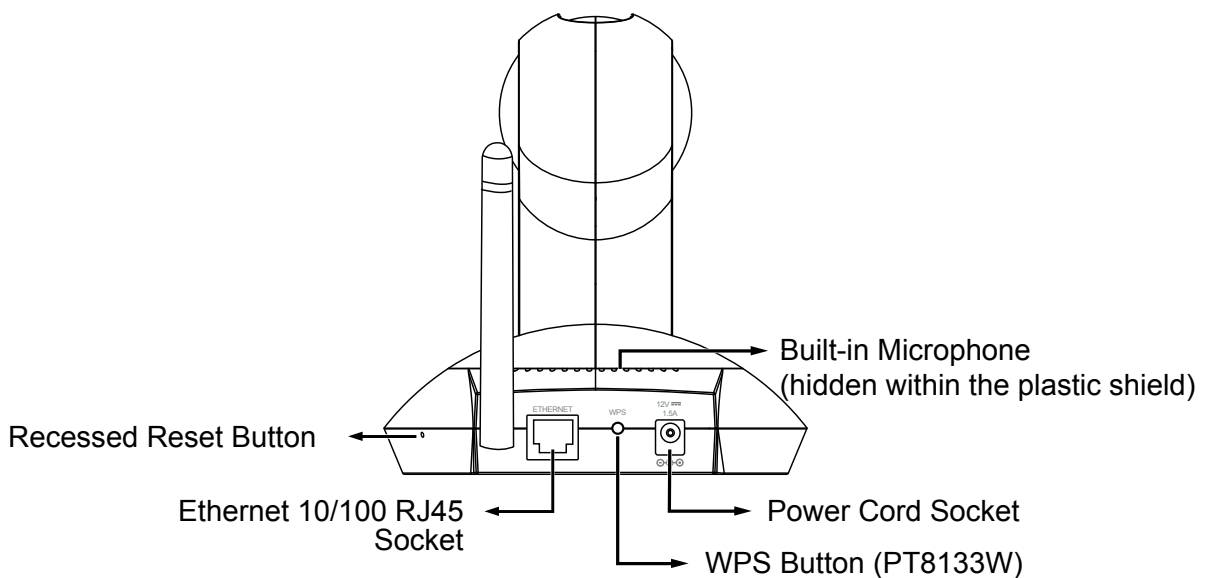
# Physical Description

## Front panel



	Item	LED status	Description
LED Definitions	1	Steady Red	Power on and system boot
		Red LED off	Power off
	2	Blink Green every 1 sec. + Steady Red	Network connected (heartbeat)
		Green LED off + Steady Red	Network failed
	3	Blink Red every 0.15 sec. + Blink Green every 1 sec.	Upgrading firmware
	4	Blink Red every 0.15 sec. + Blink Green every 0.15 sec.	Restoring defaults
	5	Steady Blue	Linked to a wireless AP
		Blue LED off	Not connected to wireless network
	6	Blink Blue every 0.15 sec.	WPS searching

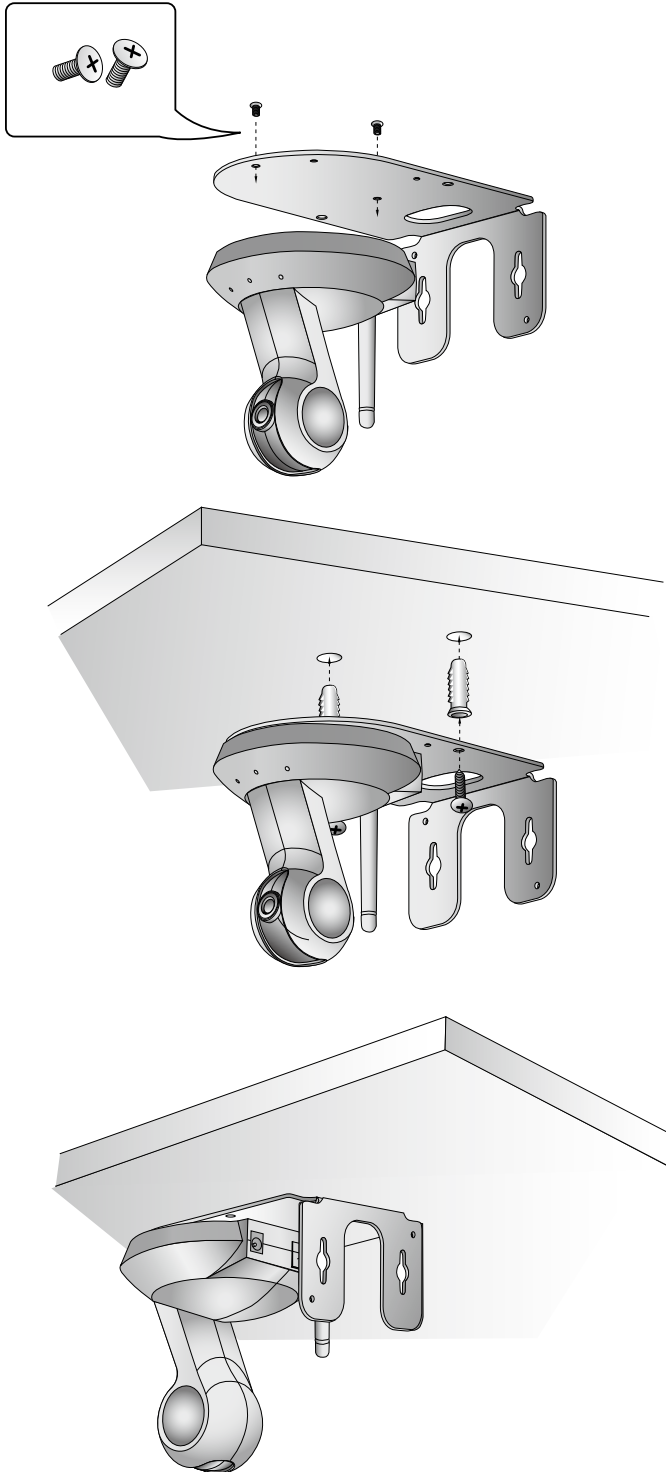
## Rear panel



## Hardware Installation

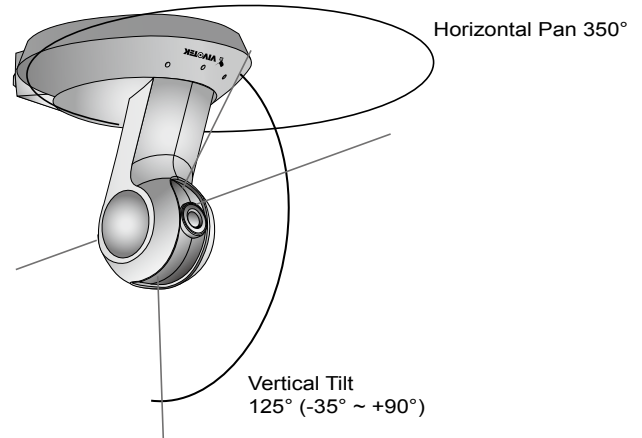
### Mounting the Network Camera - Ceiling Mount

1. Use the holes on the mount bracket as a template to mark where holes will be drilled on the ceiling. Drill two holes into the ceiling; and hammer in the plastic anchors.
2. Attach the Network Camera to the mount bracket using two flathead screws.
3. Secure mount bracket to the ceiling using two panhead screws.
4. You can now proceed with cabling.



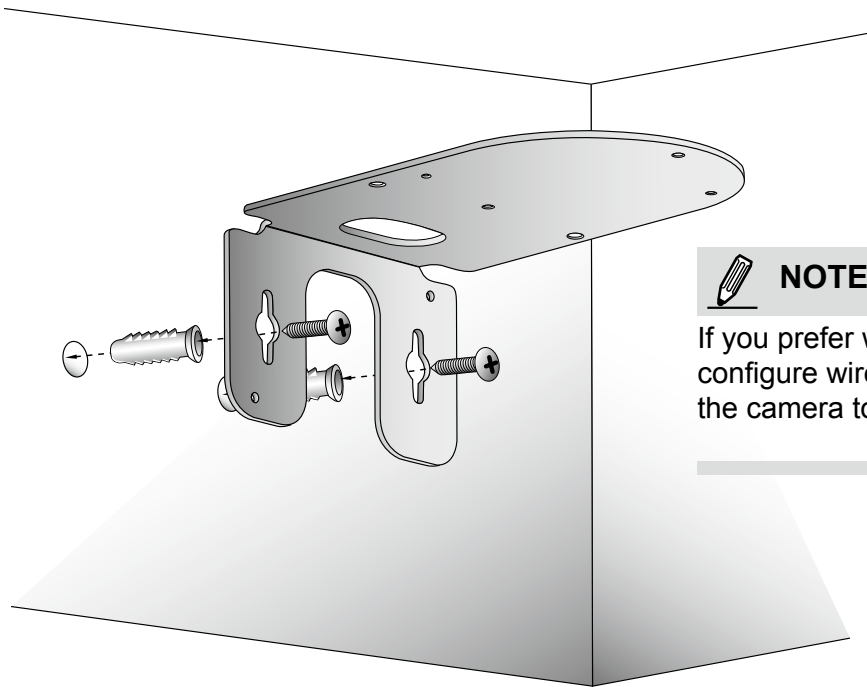
#### NOTE:

- If you prefer wireless configuration, you can configure wireless connection before you mount the camera to bracket.
- The camera can cover a wide surveillance area with its pan and tilt angles. Aim the camera orientation toward area of interest.



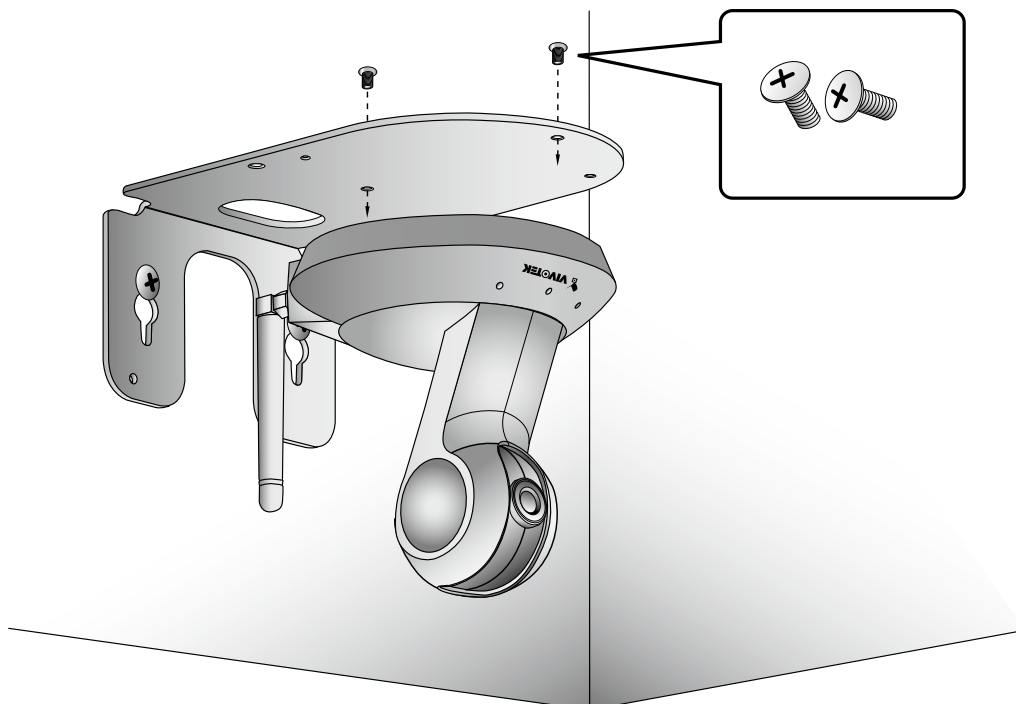
## Mounting the Network Camera - Wall Mount

1. Use the holes on the mount bracket as a template to mark where holes will be drilled on the ceiling. Drill two holes into the wall; and hammer in the plastic anchors.
2. Secure mount bracket to the wall using two included panhead screws.
3. Attach the Network Camera to the mount bracket using two flathead screws.
4. You can now proceed with cabling.



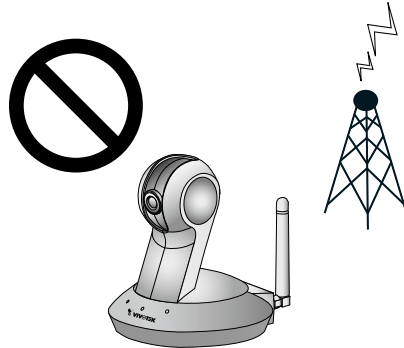
### NOTE:

If you prefer wireless configuration, you can configure wireless connection before you mount the camera to bracket.

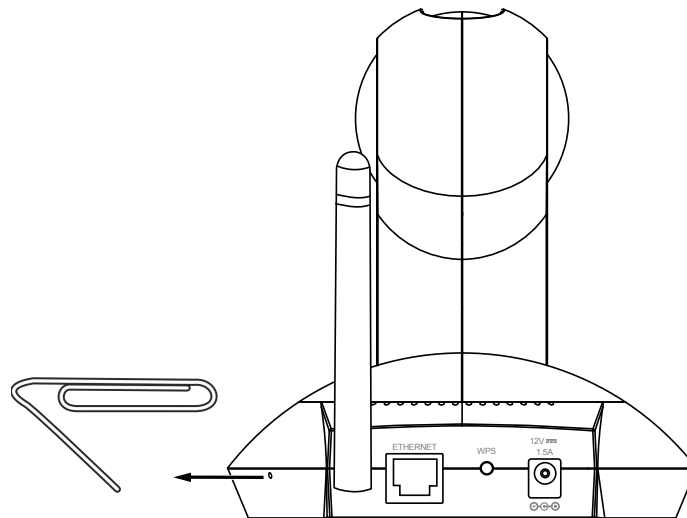


**NOTE:**

- Keep away from interference source to make sure performance integrate, and avoid snow or moiré patterning.



## Hardware Reset



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

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

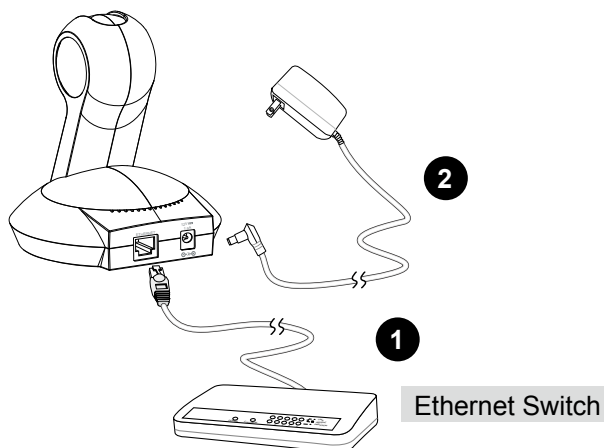
**Restore:** Press and hold the recessed reset button until the status LED rapidly blinks red and green simultaneously. Note that all settings will be restored to factory default.

## Network Deployment

### Setup the Network Camera over the Internet

This section explains how to configure the Network Camera over an Internet connection.

1. Connect the camera to a switch via Ethernet cable.
2. Connect the supplied power cable from the Network Camera to a power outlet.

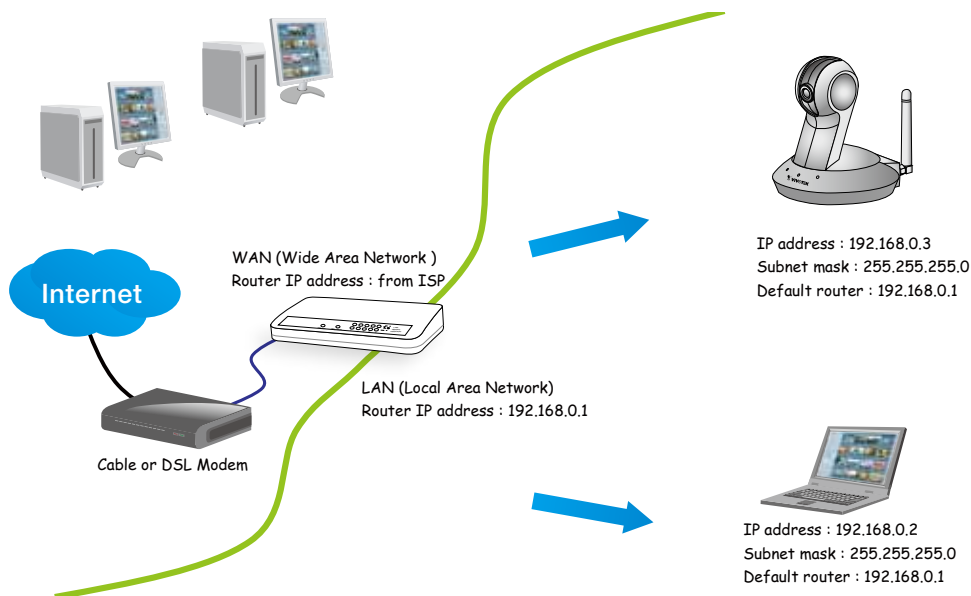


There are several ways to set up the Network Camera over the Internet. The first way is to set up the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

### 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 12 for details.



2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

- HTTP port
- RTSP port
- RTP port for audio
- RTCP port for audio
- RTP port for video
- RTCP port for video

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

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 42 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 42 for details.

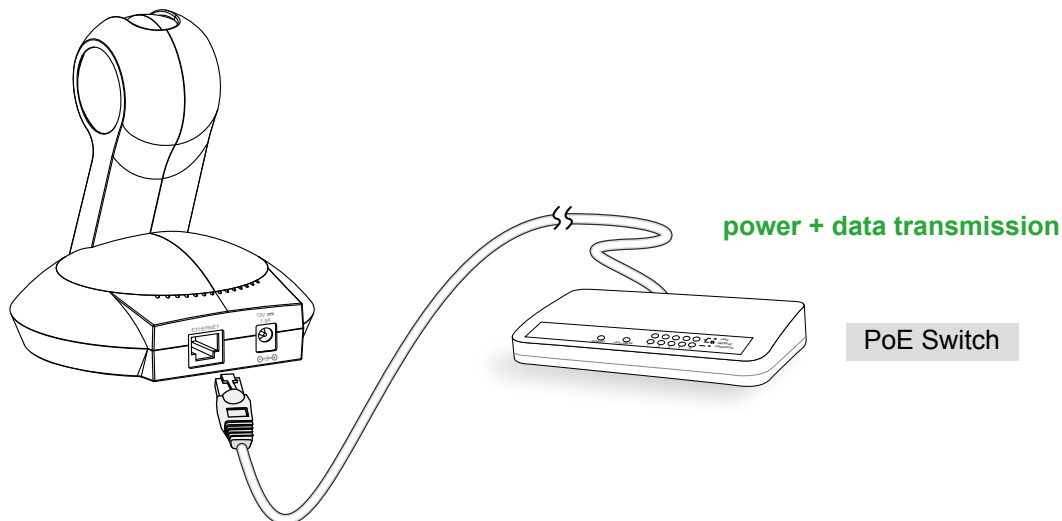
### **Internet connection via PPPoE (Point-to-Point over Ethernet)**

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 43 for details.

## Set up the Network Camera through Power over Ethernet (PoE) (PT8133)

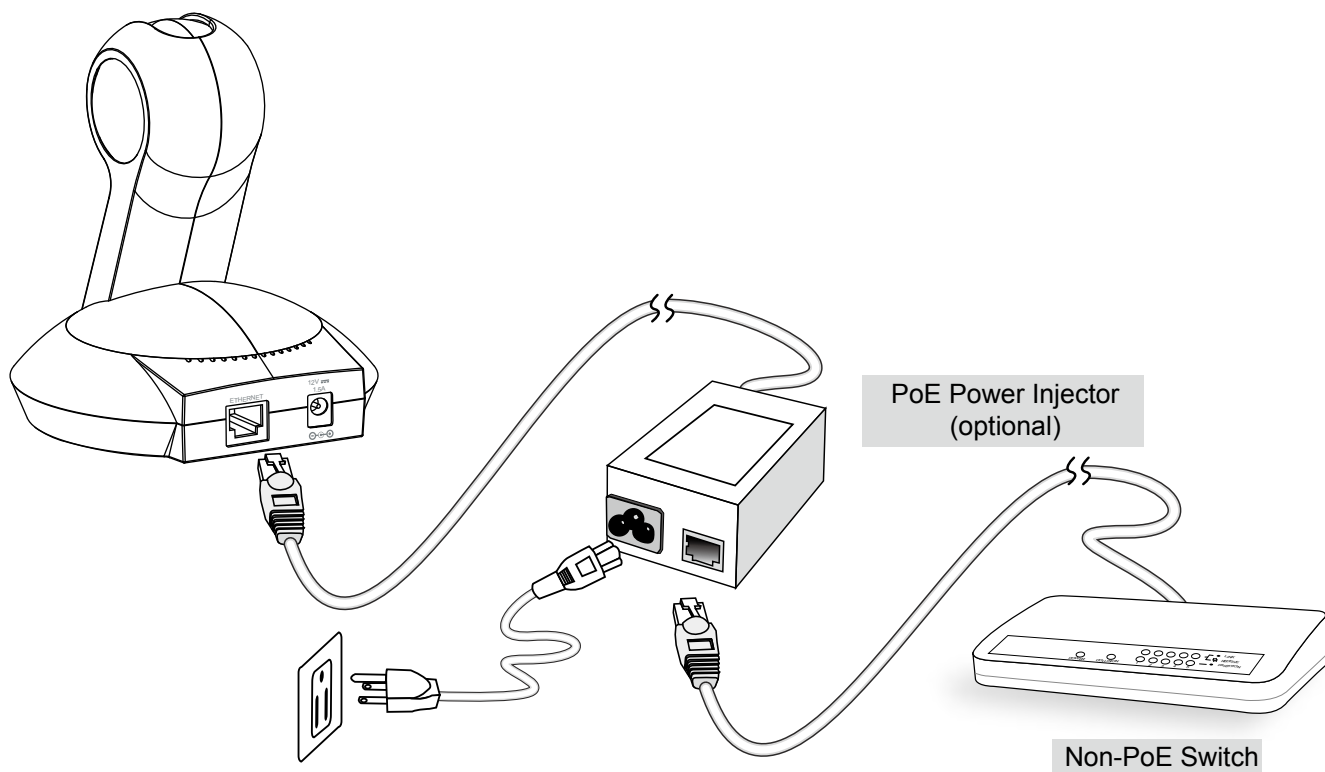
### When using a PoE-enabled switch

The Network Camera is PoE-compliant, which allows it to be powered via a single Ethernet cable. If your switch/router supports PoE, refer to the following illustration to connect the Network Camera to a PoE-enabled switch/router.



### When using a non-PoE switch

If your switch/router does not support PoE, use a PoE power injector (optional) to connect between the Network Camera and a non-PoE switch/router.



## Software Installation

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

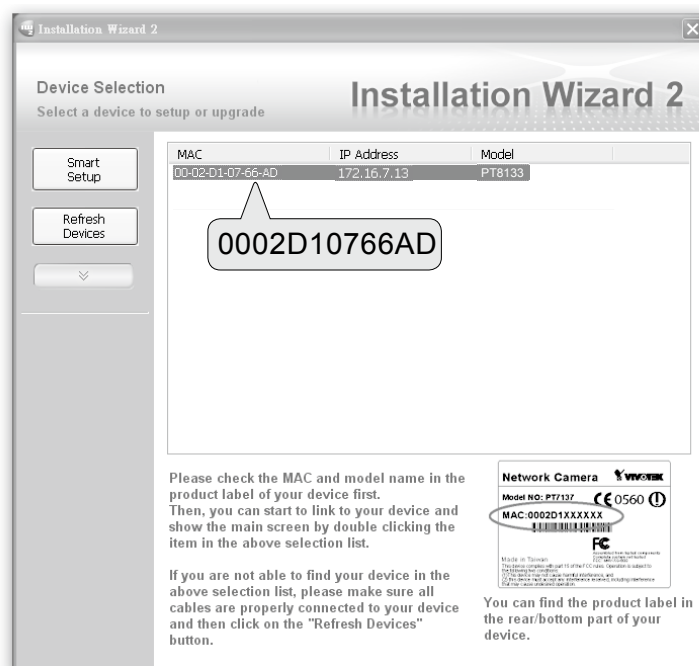
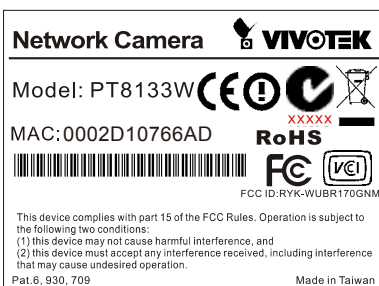
1. Install IW2 from the Software Utility directory on the software CD.  
Double click the IW2 shortcut on your desktop to launch the program.



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



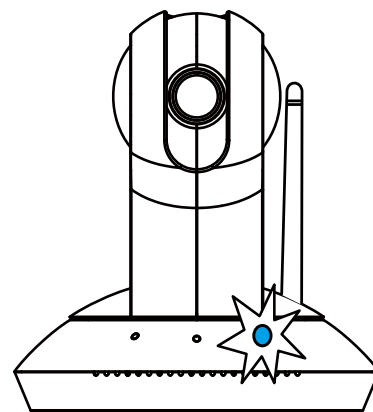
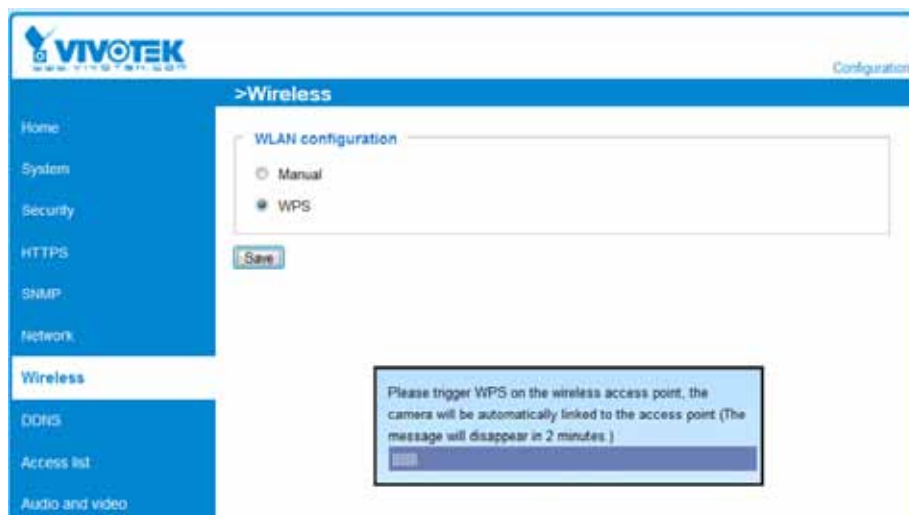
3. The program will search for VIVOTEK Video Receivers, Video Servers, and Network Cameras on the same LAN.
4. After a brief search, the main installer window will pop up. Double-click on the MAC address that matches the one printed on the camera label or the S/N number on the package box label to open a browser management session with the Network Camera.



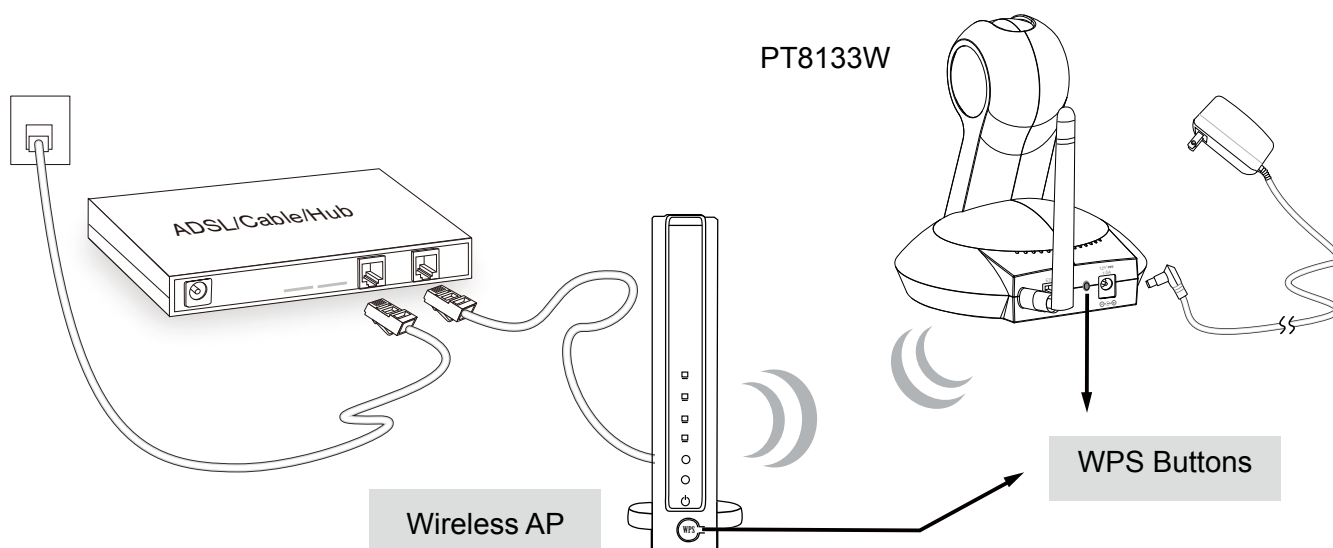


## Configure the Wireless Connection (PT8133W)

1. Make sure your AP (Access Point) and Operating System support the WPS (Wi-Fi Protected Setup) functions. WPS enables easy setup with compatible APs.
2. Connect your camera using a LAN cable, open a web console, and enter the **Configuration** -> **Wireless** page. Select the **WPS** checkbox, and click the **Save** button.



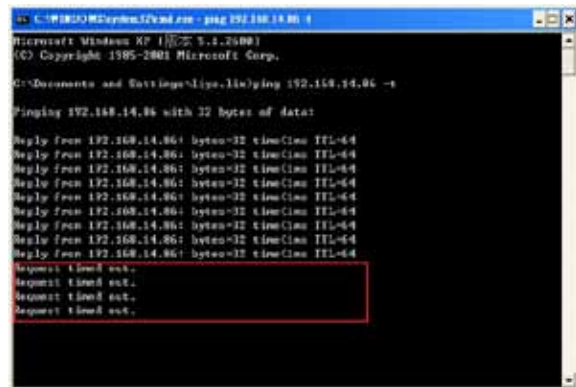
3. The camera's blue LED should start flashing. Press and hold down both of the WPS buttons on your AP and your camera for at least 1 second. (Some router/AP will have a virtual button on their management software instead.) Refer to your AP's documentation for details using its WPS function.
4. Wait for 2 minutes with the onscreen progress bar. The camera should then reboot. When the progress bar disappears, disconnect your LAN cable. You can refresh or re-start your web console to see live video.



When WPS configuration is done, wireless connectivity will be established and the security encryption, such as WEP or WPA-PSK, will be synchronized with the AP. Use the IW2 utility to find the camera. As for IP setting, the camera's use of DHCP or static IP is determined by your configuration on the network camera via the web console. The camera's default is DHCP.

**NOTE:**

1. WPS may not work if your AP is configured with a "hidden" SSID.
2. If the camera can not detect an AP after 2 minutes, the wireless setup will be cancelled.
3. If a camera is assigned with a fixed IP outside the AP's network segment, wireless setup will fail.
4. A wired connection always has a higher priority. Unplug the LAN cable at an appropriate time for the wireless setup to take effect.
5. The camera also supports manual configuration of wireless settings, enter the SSID (Service Set Identifier) and security authentication password in a web console with the camera.



- 5-1. Enter the Configuration page -> Wireless.
  - 5-2. Enter the SSID and password of your AP, select the Wireless mode as "Infrastructure."
  - 5-3. Use the "ping <IP address> -t" command in a DOS prompt to observe wired connectivity. Click the **Save** button. When wired connection is discontinued, unplug the LAN cable.
  - 5-4. After several seconds, the camera will switch to wireless connection. Disconnect and then connect the power cord to restart the camera, and you should be able to see live video from the web console.
6. Select "Ad-Hoc" wireless mode if you prefer direct connection with a PC without the intermediate AP or wireless router.

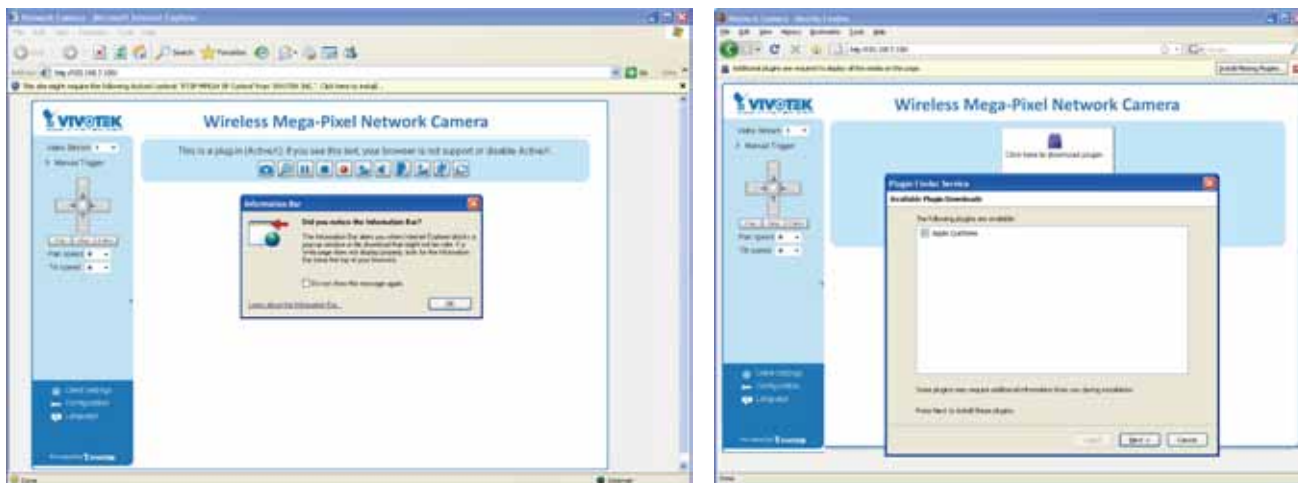
# Accessing the Network Camera

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

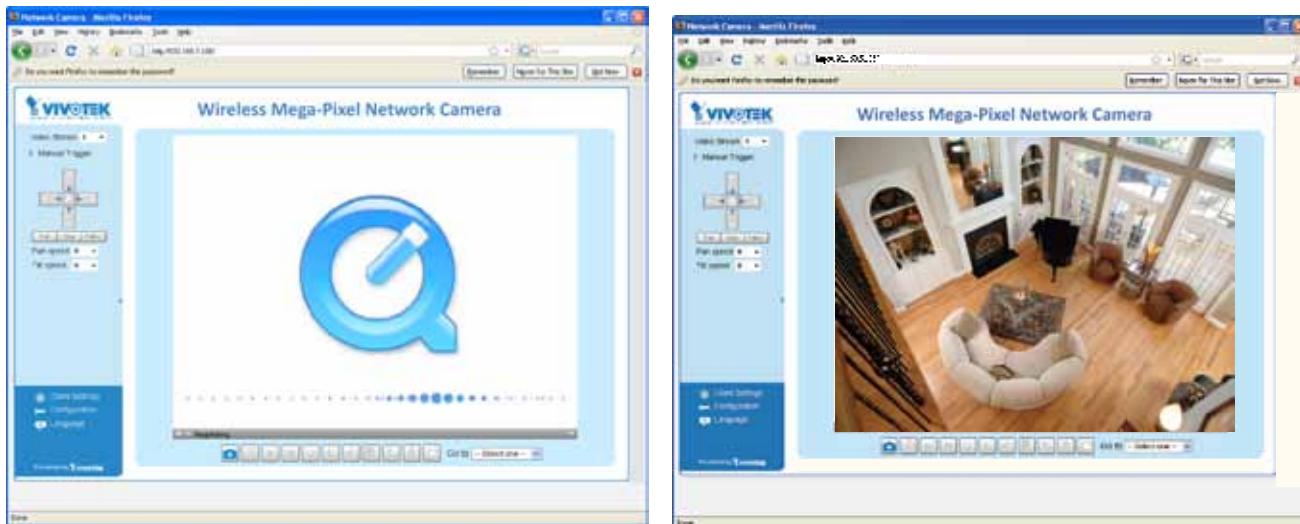
Use Installation Wizard 2 (IW2) to access to the Network Cameras installed on the LAN. If your network environment is not the LAN, follow these steps to access the Network Camera:

1. Launch your web browser (e.g., Microsoft® Internet Explorer or Mozilla Firefox).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If this 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-ins on your computer.



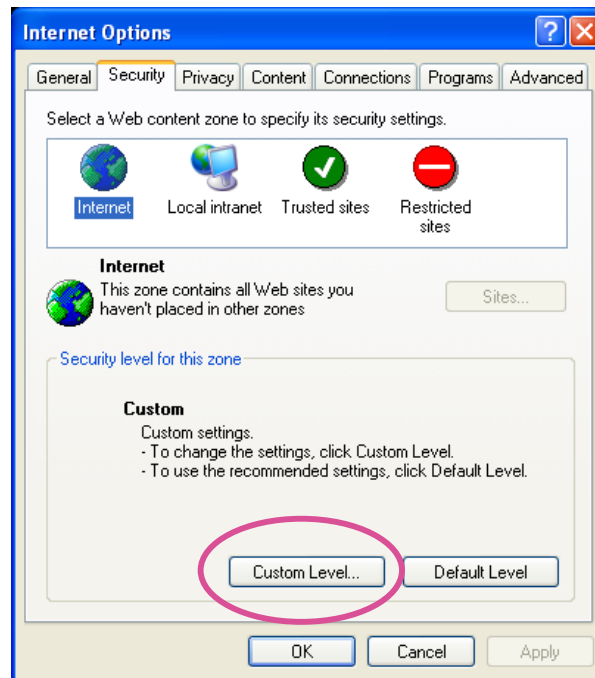
 **NOTE:**

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

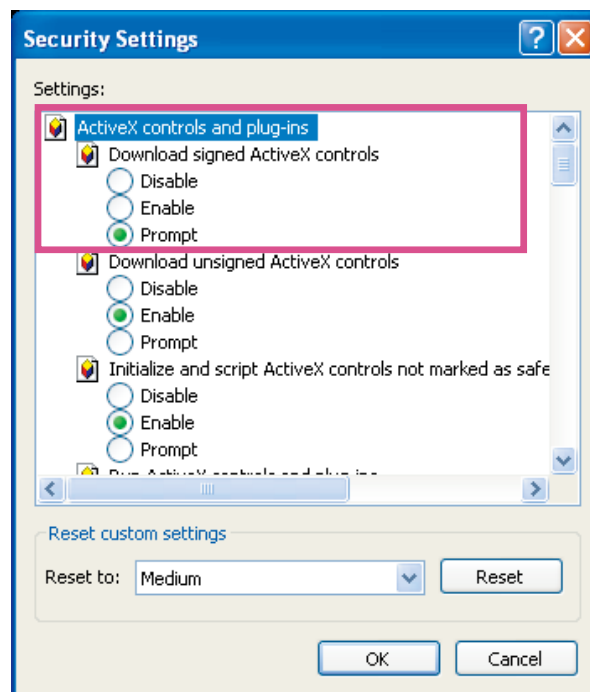


- ▶ *By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera. For more information about how to enable password protection, please refer to Security on page 35.*
- ▶ *If you see a dialog box indicating 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 Active X® control. Follow the instructions to complete installation.

**IMPORTANT!**

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

## Using RTSP Players

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



Quick Time Player

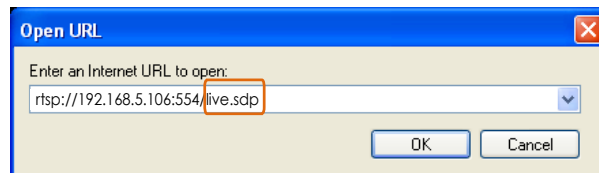


Real Player

1. Launch the RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. The address format is `rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1, 2, 3, or 4>`

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 55.

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 55 for details.



## Using 3GPP-compatible Mobile Devices

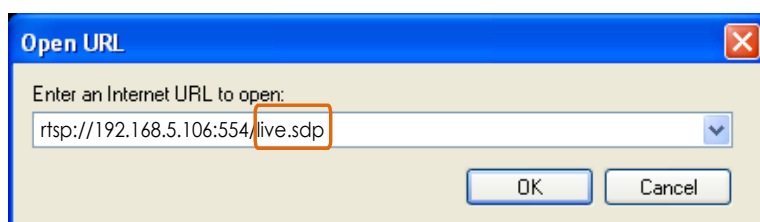
To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 9.

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 disabled.  
For more information, please refer to RTSP Streaming on page 55.
2. As the the bandwidth on 3G networks is limited, larger video sizes are not available. Please set the video and audio streaming parameters as listed below.  
For more information, please refer to Audio and Video on page 68.

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 55.
4. Launch the players on 3GPP-compatible mobile devices (ex. Real Player).
5. Type the following URL commands in the player.  
The address format is `rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream1, 2, or 3>`.  
For example:





## Using VIVOTEK Recording Software

The product software CD also contains VIVOTEK's recording software, ST-7501, 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 the manual 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, PTZ Control Panel, Configuration Area, and Live video window.



## VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

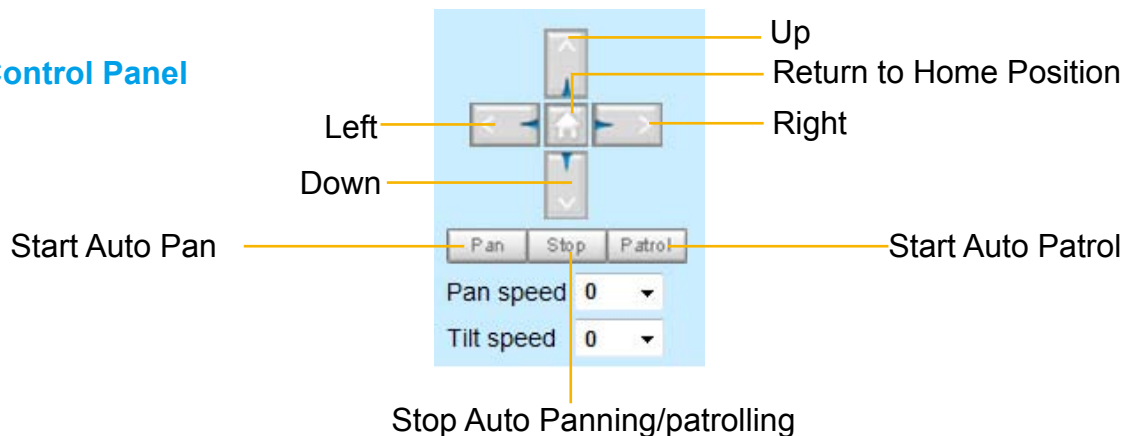
## Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page 33.

## Camera Control Area

Video Stream: This Network Camera supports H.264, MJPEG, or MPEG-4 triple streams simultaneously. You can select any of the 3 streams for live viewing.

## PTZ Control Panel



Pan: Click this button to start the auto pan. When the current position is Home or on the left side of

Home, the camera starts panning from the current position to the left-most position, then to the right-most position, and finally backward to the original position. When the current position is on the right side of Home, the camera starts panning from the current position to the right-most position, then to the left-most position, and finally backward to the original position.

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

**Patrol:** Once the Administrator has determined the list of preset positions, click this button to command the camera to patrol among those positions on the Patrol List. For more information, please refer to Camera Control on page 80.

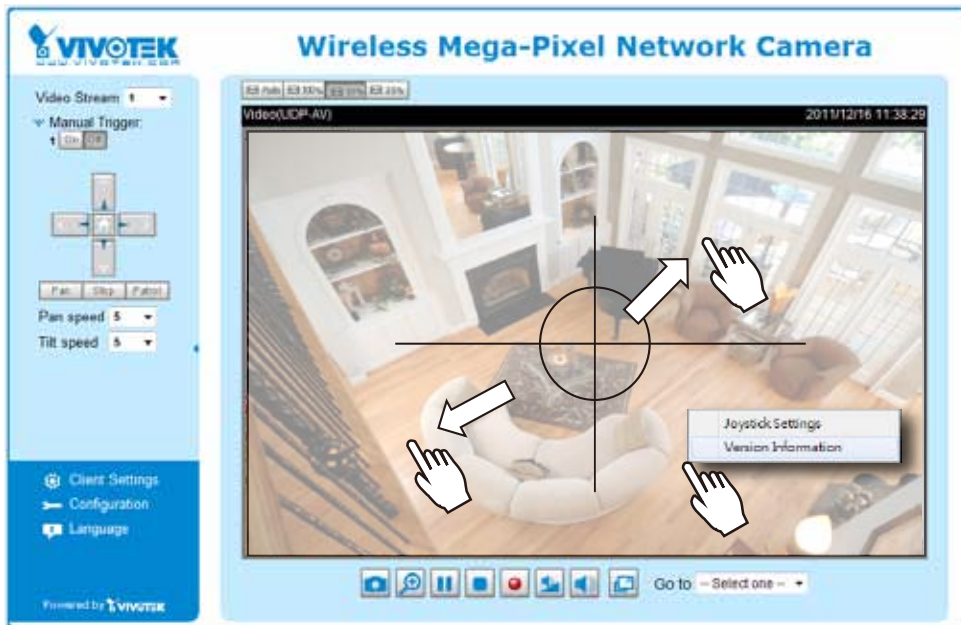
Pan speed	Tilt speed	
-5	-5	Slower
-4	-4	
-3	-3	
-2	-2	
-1	-1	
0	0	
1	1	
2	2	
3	3	
4	4	
5	5	Faster

**Pan /Tilt speed:** Adjust the speed of pan/ tilt movements.



### Onscreen Mouse Control

You can click on a place on the screen to indicate the camera move direction you prefer. For example, you can click on the upper-right corner of the screen, and the camera lens will move toward the upper-right direction. The mouse control also takes effect in the Camera Control window.



You can right-click on the screen to display the joystick and the ActiveX version information. In times of plug-in compatibility conflicts (e.g., your browser might have previously installed plug-ins), you may report this to technical support.

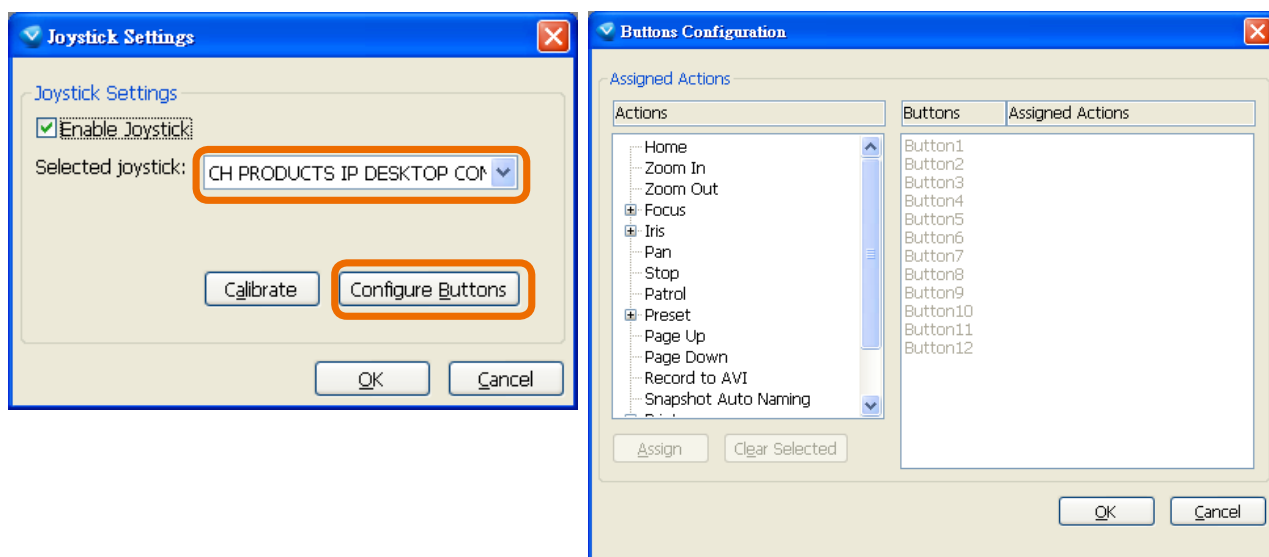
## Joystick Settings

### Enable Joystick

Connect to the USB plug of the joystick to a USB port on your management computer. Supported by the plug-in in the main page (Microsoft's DirectX), once the plug-in in the main page is loaded, it will automatically detect if there is any joystick on the computer. The joystick should work properly without installing any other driver or software.

Then you can begin to configure the joystick settings of connected devices. Please follow the instructions below to enable joystick settings.

1. Right-click on a live view window. Select Joystick Settings. If your joystick is working properly, it will be displayed on the drop-down list.
- c. Select the joystick you want to configure. Check **Enable Joystick**, then click **Configure Buttons** to open Buttons configuration window.



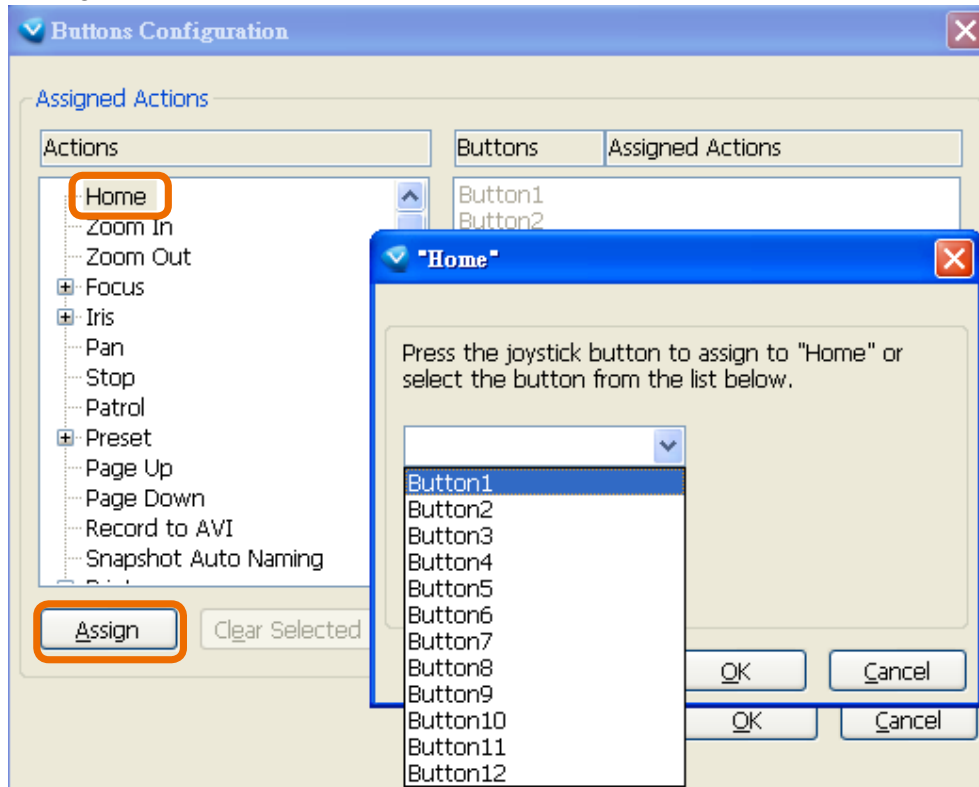
## Buttons Configuration

In Button Configuration window, the left column shows the actions you can assign, and the right column shows the functional buttons and assigned actions. The number of buttons may differ from different joysticks.

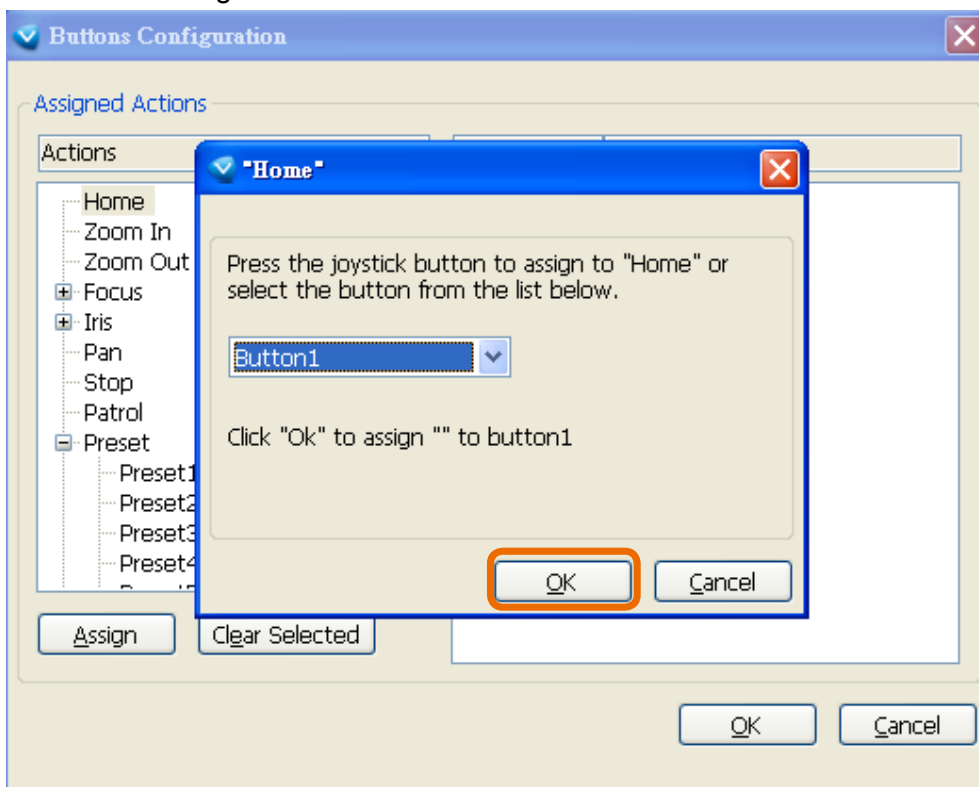
Please follow the steps below to configure your joystick buttons:

1. Choosing one of the actions and click **Assign** will pop up a dialog. Then you can assign this action to a button by pressing the joystick button or select it from the drop-down list.

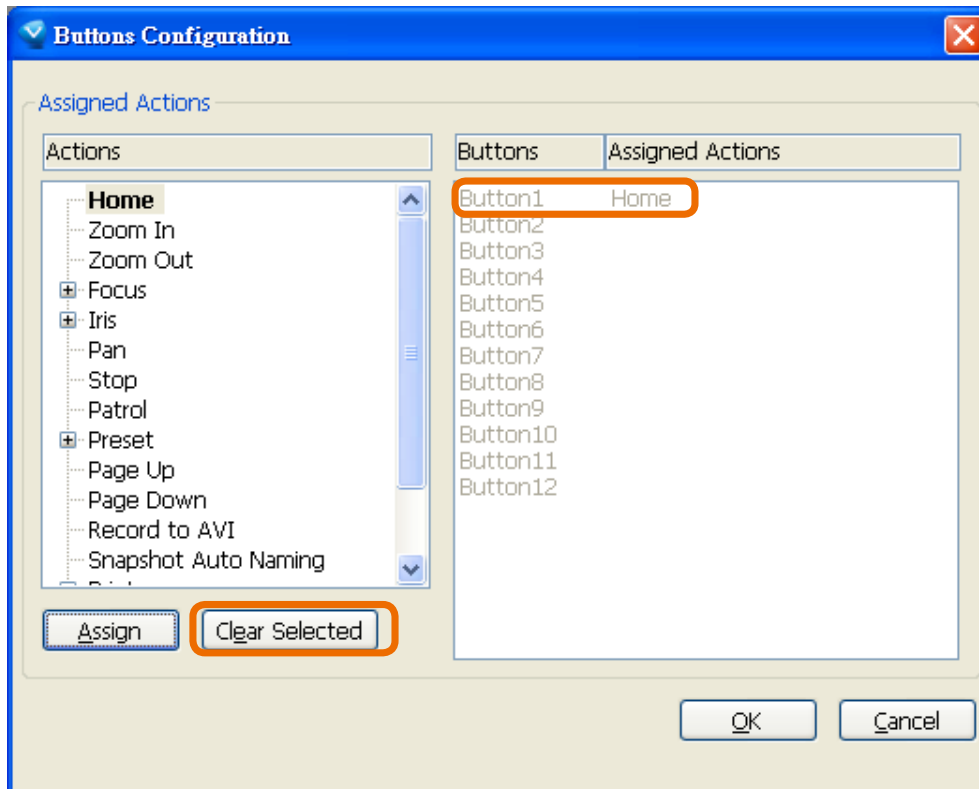
For example: Assign **Home** (move to home position) to Button 1.



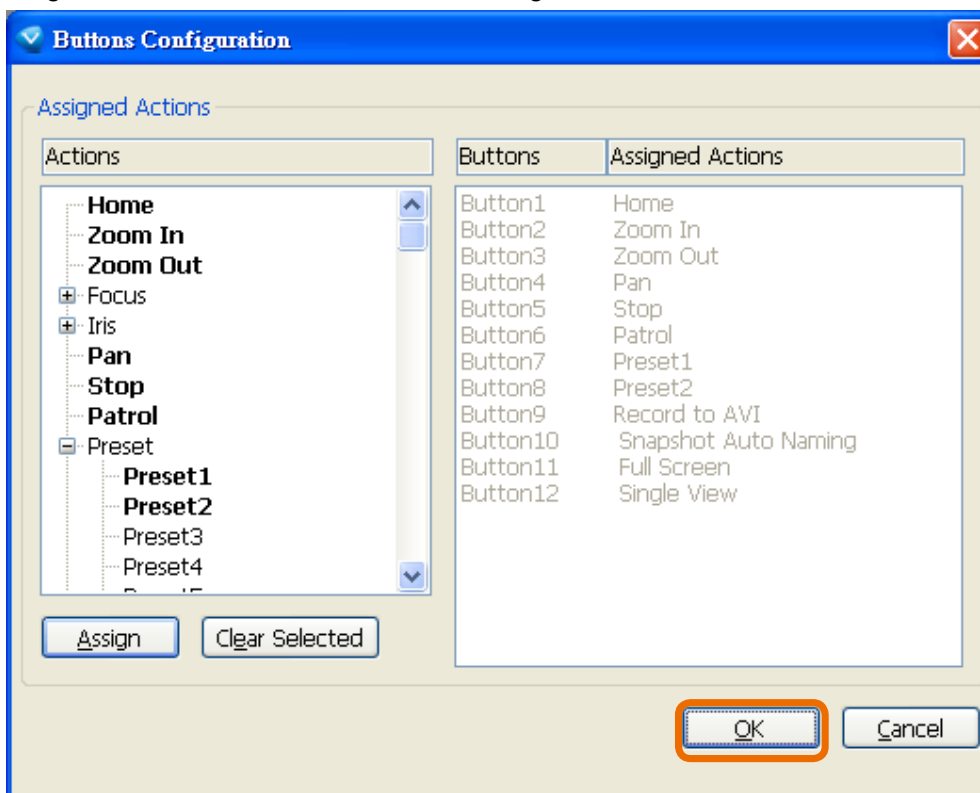
2. Click **OK** to confirm the configuration.



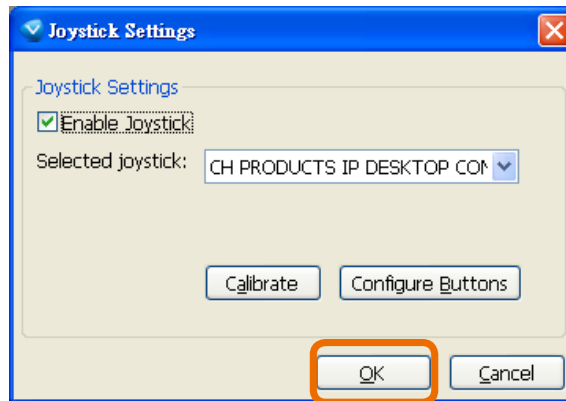
3. The Assigned Action will appear beside Button 1 in the right column as shown in the following diagram. Note that a button can only be assigned with an action. If you want to modify the settings, select the action on the list and click **Clear Selected**.



4. If you want to assign additional actions, repeat step a.~c. When all settings are complete, click **OK** to save the settings or click **Cancel** to discard the settings.

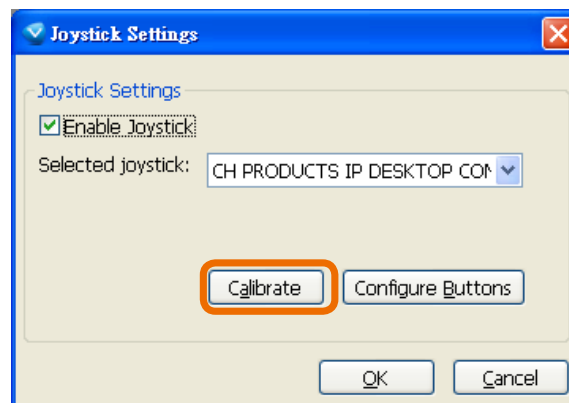


5. Click **OK** to save the settings or click **Cancel** to discard the settings.

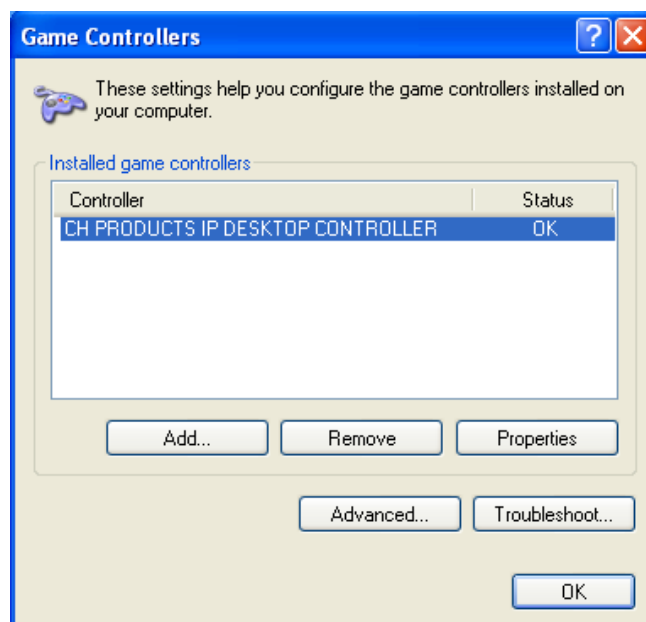


#### NOTE:

- If you want to assign Preset actions to your joystick, the preset locations should be configured in advance.
- If your joystick is not working properly, it may need to be calibrated. Click the Calibrate button to open the Game Controllers window located in Microsoft Windows control panel and follow the instructions for trouble shooting.



- The joystick will appear in the Game Controllers list in the Windows Control panel. If you want to check out for your devices, go to the following page: Start -> Control Panel -> Game Controllers.



## Configuration Area

**Client Settings:** Click this button to access the client settings page. For more information, please refer to Client Settings on page 30.

**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 32.

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

## Live Video Window

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




**Video Title:** The video title can be configured. For more information, please refer to Video Settings on page 68.


**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 30.

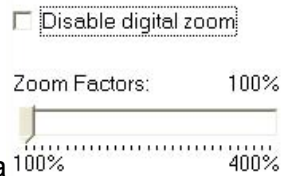
**Time:** Display the current time. For further configuration, please refer to Video Settings on page 68.


**Title and Time:** The video title and time can be stamped on the streaming video. For further configuration, please refer to Audio and Video Settings on page 68.

**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 image.







 **Pause:** Pause the transmission after clicking the Pause button.


becomes the  Resume 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. 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 the file name, please refer to MP4 Saving Options on page 31 for details.

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

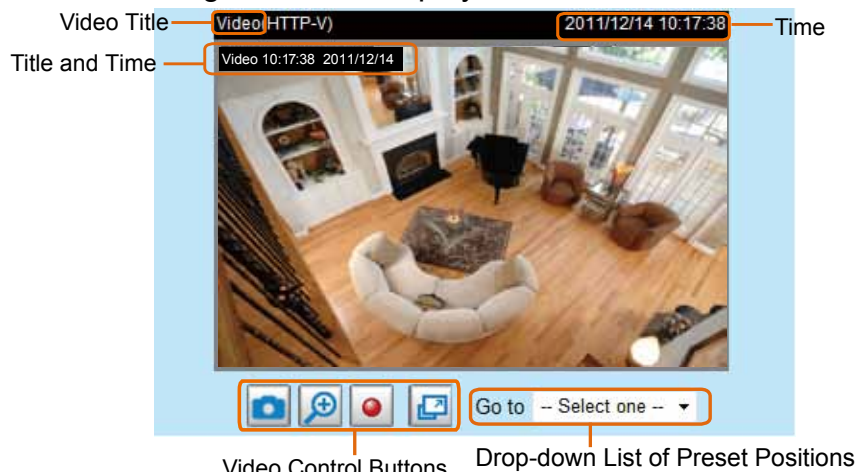
 **Mute:** Turn off the volume on the local computer. The button becomes the  Audio On button after clicking the Mute button.

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

**Go to:** Once the Administrator has configured a list of preset positions, you can quickly move the camera’s view to a preset position using using this command. For more information, please refer to Camera Control on page 80.



■ 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 Video Settings on page 68.

**Time:** Display the current time. For more information, please refer to Video Settings on page 68.



**Title and Time:** The video title and time can be stamped on the streaming video. For more information, please refer to Video Settings on page 68.


**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 image.



 **Start MP4 Recording:** Click this button to record video clips in MP4 file format. 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 31 for details.

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

**Go to:** Once the Administrator has determined the list of preset positions; you can aim the camera using this command. For more information, please refer to Camera Control on page 80.

# Client Settings

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

## H.264/MPEG-4 Media Options

**MPEG-4 Media Options**

Video and Audio

Video Only

Audio Only

Select whether 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

**MPEG-4 Protocol Options**

UDP Unicast

UDP Multicast

TCP

HTTP

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

**UDP unicast:** This protocol allows for better real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate the 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 to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 55.

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

**HTTP:** This protocol allows for the same transmission quality as the 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.

Note that changing the protocol option might bring your camera's focus back to the default home position.

## MP4 Saving Options

**MP4 Saving Options**

Folder:

File name prefix:

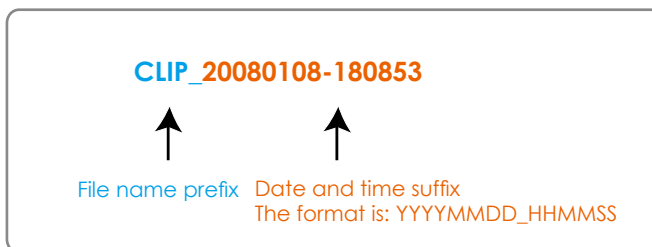
Add date and time suffix to file name

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

Folder: Specify the 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.



## Local Streaming Buffer Time

**Local Streaming Buffer Time**

Millisecond

Due to unsteady bandwidth flow, live streaming may lag and not be very smoothly. If you enable this option, the live streaming will be stored on the camera's memory buffer for a few seconds before being played on the live viewing window. This helps produce a smooth live streaming. If you enter a value of 3000 milliseconds, the streaming will delay for 3 seconds.

# Configuration

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

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

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

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

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

## Basic Mode

The screenshot displays the VIVOTEK configuration web interface. On the left is a blue sidebar menu with the following items: Home, System, Security, Network, Wireless, DDNS, Audio and video, Motion detection, Camera control, and Maintenance. The 'System' menu item is highlighted. Below the menu is a button labeled '[ Advanced mode ]'. At the bottom left of the sidebar, the text 'Version: 0100c' is shown. The main content area has a blue header with the VIVOTEK logo and 'www.vivotek.com' on the left, and 'Configuration' on the right. Below the header is a breadcrumb '>System'. The main content area contains two sections: 'System' and 'System Time'. The 'System' section includes a text input field for 'Host name' containing 'Mega-Pixel Pan/Tilt Wireless Network Camera' and a checkbox for 'Turn off the LED indicator'. The 'System Time' section includes three radio button options: 'Keep current date and time' (selected), 'Synchronize with computer time', and 'Manual'. Below these options is an 'Automatic' radio button and a 'Save' button. Annotations with orange arrows point to the 'System Time' section, the '[ Advanced mode ]' button, and the 'Version: 0100c' text.

## Advanced Mode

The screenshot shows the VIVOTEK configuration interface. On the left is a vertical 'Configuration list' with items like Home, System, Security, HTTPS, SNMP, Network, Wireless, DDNS, Access list, Audio and video, Motion detection, Camera control, Homepage layout, Application, Recording, System log, View parameters, and Maintenance. Below this list are buttons for '[ Basic mode ]' and 'Version: 0100c'. The main area is titled '>System' and contains two sections: 'System' with a 'Host name' field (Mega-Pixel Pan/Tilt Wireless Network Camera) and a 'Turn off the LED indicator' checkbox; and 'System Time' with a 'Time zone' dropdown menu (GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei) and radio buttons for 'Keep current date and time', 'Synchronize with computer time', 'Manual', and 'Automatic'. A 'Save' button is located at the bottom of the System Time section.

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

## System

This section explains how to configure the basic settings for the Network Camera, including System, and System Time. When completed with the settings on this page, click **Save** at the bottom of the page to enable the settings.

### System

**System**

Host name:

Turn off the LED indicator

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

**Turn off the LED indicators:** If you do not want others to know that the network camera is operating, you can select this option to turn off the LED indicators.

## System Time

**System Time**

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

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

Keep current date and time

Sync with computer time:

Manual:

Automatic:

**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 system power 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 when updated.

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

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

**NTP server:** Assign the IP address or domain name of the time-server. Leaving the text box blank connects the 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 on the Maintenance page, please refer to Upload / Export Daylight Saving Time Configuration File on page 106 for details.

## Security

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 set a password for the “root” account first.

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

### Manage Privilege Advanced Mode

**PTZ control:** You can modify the manage privilege of operators or viewers. Check or uncheck the item, then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Main Page on page 21.)

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

### Manage User

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. Operators cannot access the Configuration page but can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands for the Network Camera on page 109. Viewers access only the main page for live viewing.

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

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

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

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

### Enable HTTPS

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

**Enable HTTPS**

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

Enable HTTPS secure connection:

HTTP & HTTPS  
  HTTPS only

**Save**

---

**Create and install certificate method**

Create self-signed certificate automatically

Create self-signed certificate manually:

Create certificate request and install:

### Create and Install Certificate Method

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

#### Create self-signed certificate automatically

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

**Enable HTTPS**

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

Enable HTTPS secure connection:

HTTP & HTTPS  
  HTTPS only

**Save**

---

**Create and install certificate method**

Create self-signed certificate automatically

Create self-signed certificate manually:

Create certificate request and install:

**Certificate Information**

Status: Not installed

Please wait while the certificate is being generated...



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

**Certificate Information**

Status:	Active
Country:	TW
State or province:	Province
Locality:	City Name
Organization:	Organization Name
Organization Unit:	Unit Name
Common Name:	IP Address

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

**https://**



**Security Alert** ✖

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

- The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
- The security certificate date is valid.
- The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

**Security Information** ✖

This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

### Create self-signed certificate manually

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

**Create and install certificate method**

Create self-signed certificate automatically  
 Create self-signed certificate manually:  
     Self-signed certificate:   
 Create certificate request and install:

---

**Create Certificate**

Country:

State or province:

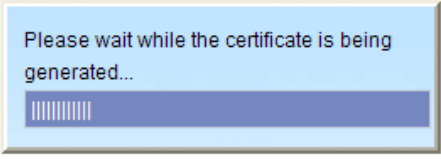
Locality:

Organization:

Organization Unit:

Common Name:

Validity:  days



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

**Certificate Information**

Status:

Country: TW

State or province: Province

Locality: City Name

Organization: Organization Name

Organization Unit: Unit Name

Common Name: IP Address

### Create certificate request and install : Select this option if you want to create an official certificate issued by a CA (Certificate Authority).

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

**Create and install certificate method**

Create self-signed certificate automatically  
 Create self-signed certificate manually:  
 Create certificate request and install:  
     Certificate request:   
     Select certificate file:

**Create Certificate**

Country:

State or province:

Locality:

Organization:

Organization Unit:

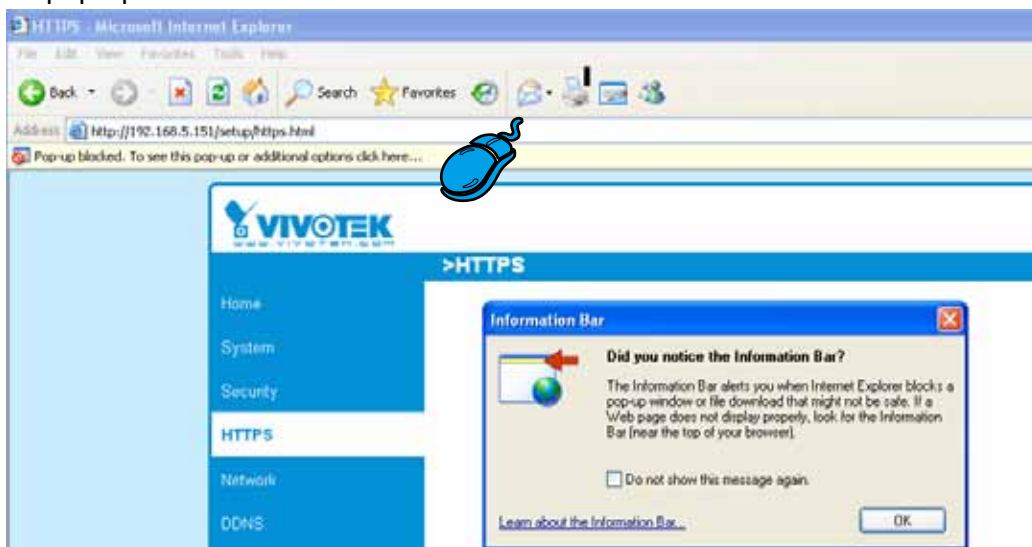
Common Name:

Validity:  days

Please wait while the certificate is being generated...

|||||||

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



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

**Create Certificate Request Completed**

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

**Certificate Request (PEM format)**

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBuDCASECADB5MQswCQYDVQQGEwJUVzERMAsGA1UECBMIUHJvdmluY2UxUxJlAQ
BgNVBAsTCUNpdHkgTmFtZTEaMBGGA1UEChMRMRT3JnYW5pemFoaW9uIE5hbWUxUxJlAQ
BgNVBAsTCVVueXQgTmFtZTEaMBEGAlUEAxMKSVAgQWRkcmVzcCBnzANBgkqhkiG
9w0BAQEFAA0BjQAwgYkCgYEAuOT75EY52gsSyPFMxZ7wHdQ1obPescsXLUx9DFw6
OMRheukFaXFDkM+5xk+K5oEPBPqj77yhH+zdUHS27ffSLG57bW9SoxrWuLhSvRZW
mCD+//AiJX864dJ/mjHn7Wc55GFaxgMvbALcxT+hCIeDCWYnRqh/fpKNj+BxvVoN
UrcCAwEAaAAAMAGCSqGSIb3DQEBBQUAA4GBAAVazWO&tftfU9dyFgTxOYO1D/zO
FOTkbnDOQG18e4ftJ3rROD1TvIIMjg3K8zsAS8Gd3pME1ejqLYoBrtaSqgGix
50bLG1subWsXr88PngaBwjYoTpG3qlzvUPJZLAVmdL3ne5urTbABXOScCHOQGT+
PX9dw40JWkIC8QhV
-----END CERTIFICATE REQUEST-----

```

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

**Create and install certificate method**


Create self-signed certificate automatically  
 Create self-signed certificate manually:  
 Create certificate request and install:

Certificate request:   
 Select certificate file:

---

**Certificate Information**

Status:

 **NOTE:**

- How do I cancel the HTTPS settings?
  1. Uncheck **Enable HTTPS secure connection** in the first column and click **Save**; a warning dialog will pop up.
  2. Click **OK** to disable HTTPS.

**Enable HTTPS**

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

Enable HTTPS secure connection:

**Create and install certificate method**

Create self-signed certificate automatically  
 Create self-signed certificate manually:

**Microsoft Internet Explorer**

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

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

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

**Certificate Information**

Status:

Country:

State or province:

Locality:

Organization:

Organization Unit:

Common Name:

**Microsoft Internet Explorer**

Are you sure you want to delete the certificate?

## 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:	Private
Read only community:	Public

#### Enable SNMPv3

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

- Security name: According to your NMS settings, choose Read/Write or Read Only and enter the community name.
- Authentication type: Select MD5 or SHA as the authentication method.
- Authentication password: Enter the password for authentication (at least 8 characters).
- Encryption password: Enter a password for encryption (at least 8 characters).

Enable SNMPv3

**SNMPv3 Settings**

Read/Write Security name:	Private
Authentication Type:	MD5 ▼
Authentication Password:	
Encryption Password:	
Read only Security name:	Public
Authentication Type:	MD5 ▼
Authentication Password:	
Encryption Password:	

## Network

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

### Network Type

**Network Type**

LAN:

Get IP address automatically

Use fixed IP address:

Enable UPnP presentation

Enable UPnP port forwarding

PPPoE:

Enable IPv6

Save

### 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. Remember to click **Save** when you complete the Network setting.

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

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

**Network Type**

LAN:

Get IP address automatically

Use fixed IP address:

IP address:

Subnet mask:

Default router:

Primary DNS:

Secondary DNS:

Primary WINS server:

Secondary WINS server:

Enable UPnP presentation

Enable UPnP port forwarding

PPPoE:

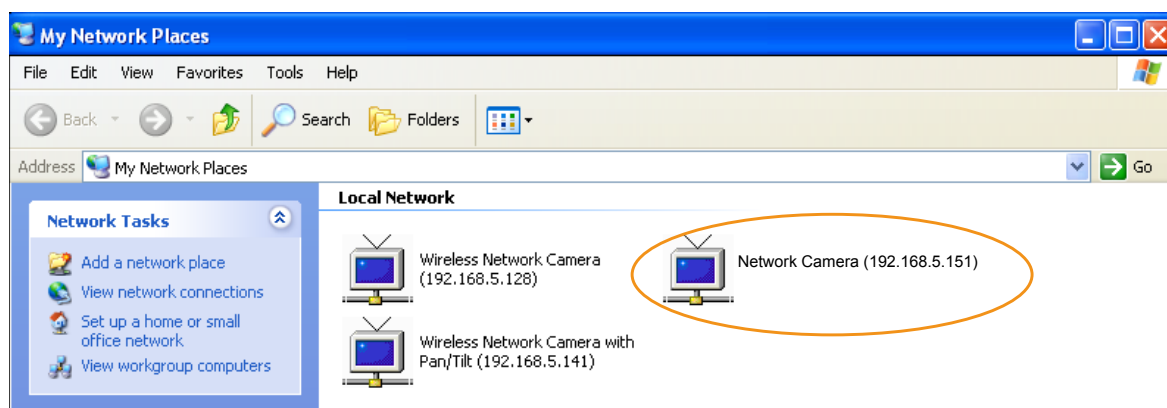
Enable IPv6

Save

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

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

UPnP™ component is installed on your computer.



**Enable UPnP port forwarding:** To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP™ 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 (Internet Service Provider).

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 Home > Configuration > Application > Server Settings (please refer to Server Settings on page 92) to add a new email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 95). Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > Network Type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.

**Network Type**

LAN:

PPPoE:

User name:

Password:

Confirm password:

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



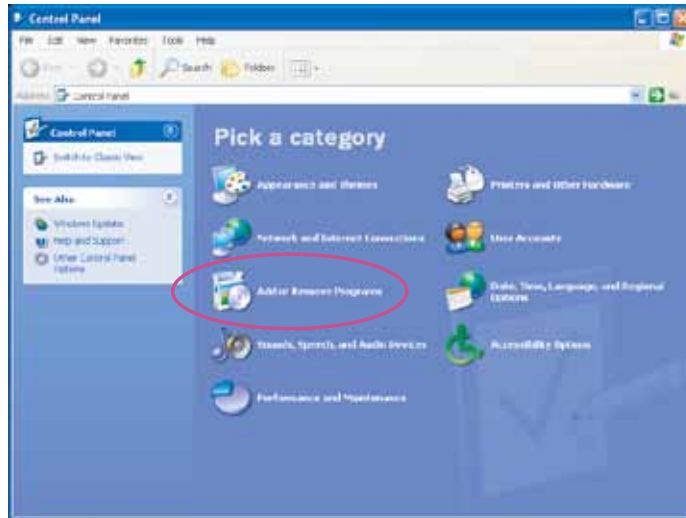
### NOTE:

- ▶ 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.**

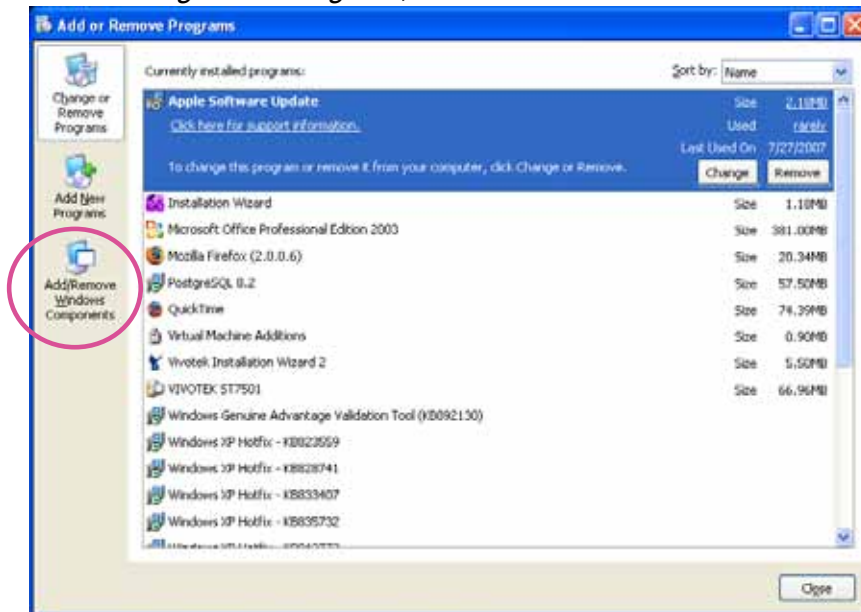


► Following are the steps to enable the UPnP™ user interface on your computer:  
 Note that you must log on to the computer as a system administrator to install the UPnP™ components.

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**.

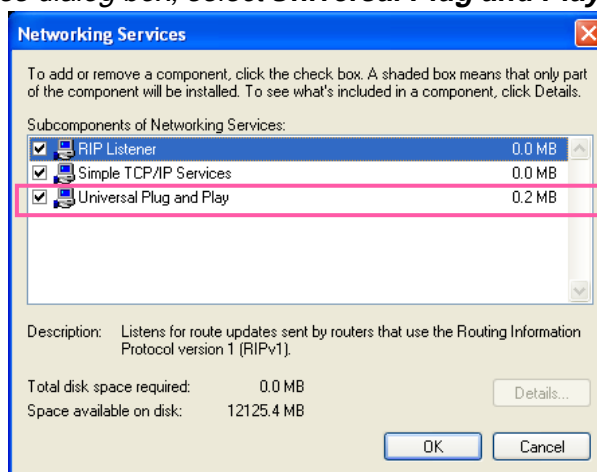


3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.

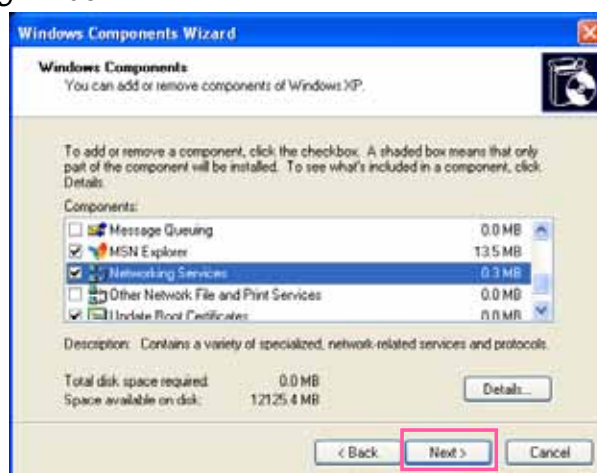




4. In the Networking Services dialog box, select **Universal Plug and Play** and click **OK**.



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 105 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:

- Get IP address automatically
- Use fixed IP address:
- Enable UPnP presentation
- Enable UPnP port forwarding

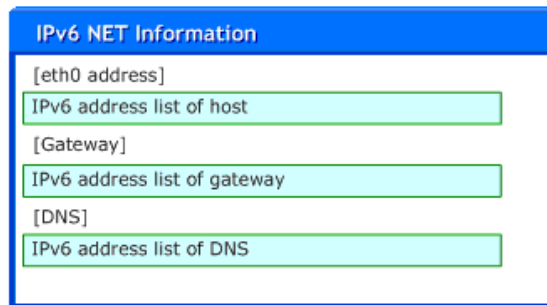
PPPoE:

- Enable IPv6

Manually setup the IP address

When IPv6 is enabled, by default, the 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 will be listed in a pop-up window. The IPv6 address will be displayed as follows:

### Refers to Ethernet

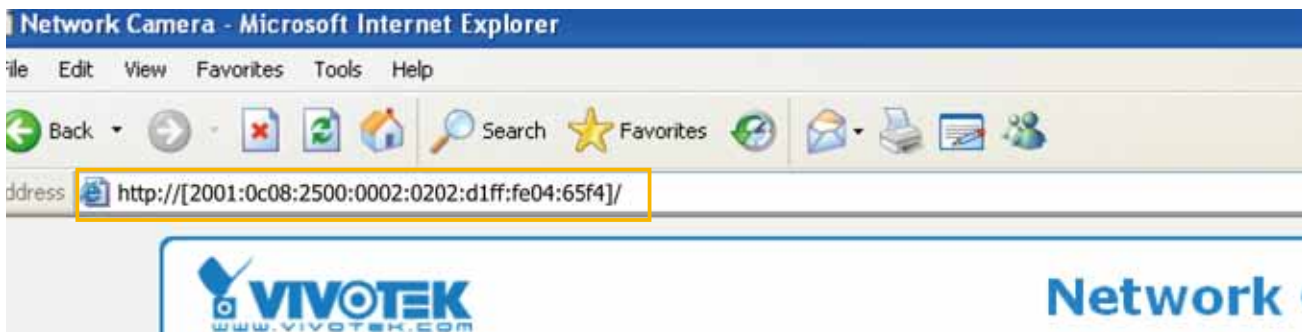
[eth0 address]	
2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global	— Link-global IPv6 address/network mask
fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link	— Link-local IPv6 address/network mask
[Gateway]	
fe80::211:d8ff:fea2:1a2b	
[DNS]	
2010:05c0:978d::	

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:



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** on page 52 for detailed information.)



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

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

**Manually setup the IP address:** Select this option to manually set up IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers.

If you check this item, the following blanks will be displayed for you to enter the corresponding information:

Enable IPv6

**IPv6 Information**

Manually setup the IP address

Optional IP address / Prefix length  / 64

Optional default router

Optional primary DNS

## IEEE 802.1x Advanced Mode

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

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

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



1. Supplicant: A client end user (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 (ie. MIS 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:

Status: no file

client certificate:

Status: no file

Client private key:

Status: no file

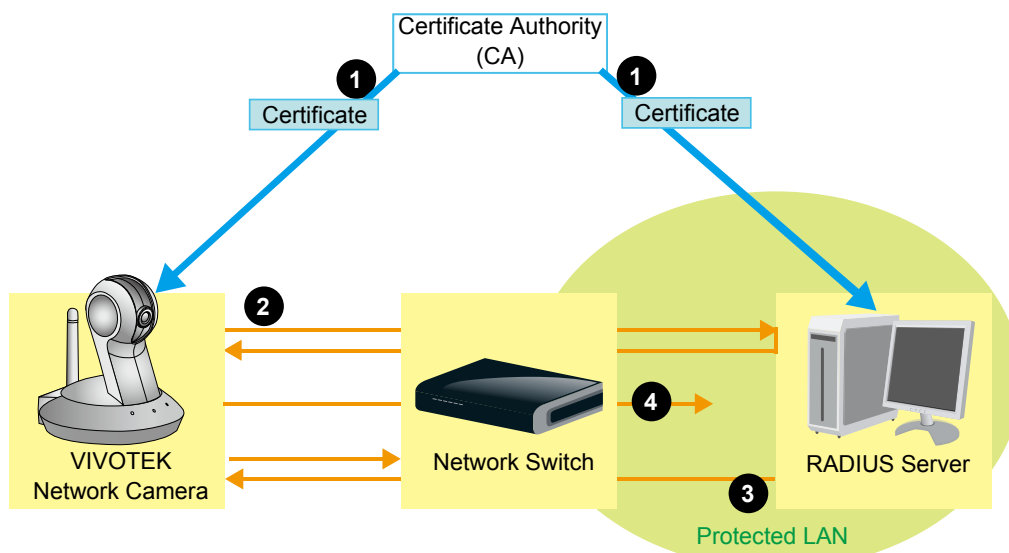
3. When all settings are complete, move the Network Camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.



#### **NOTE:**

► *The authentication process for 802.1x:*

1. *The Certificate Authority (CA) provides the required signed certificates to the Network Camera (the supplicant) and the RADIUS Server (the authentication server).*
2. *A Network Camera requests access to the protected LAN using 802.1X via a switch (the authenticator). The client offers its identity and client certificate, which is then forwarded by the switch to the RADIUS Server, which uses an algorithm to authenticate the Network Camera and returns an acceptance or rejection back to the switch.*
3. *The switch also forwards the RADIUS Server's certificate to the Network Camera.*
4. *Assuming all certificates are validated, the switch then changes the Network Camera's state to authorized and is allowed access to the protected network via a pre-configured port.*



## Network > QoS (Quality of Service) Advanced Mode

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

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

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

### Requirements for QoS

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

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

### QoS models

#### CoS (the VLAN 802.1p model)

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

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

**CoS**

Enable CoS

VLAN ID:

Live video:  ▼

Live audio:  ▼

Event/Alarm:  ▼

Management:  ▼

If you assign Video the highest priority level, your network 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 > HTTP **Advanced Mode**

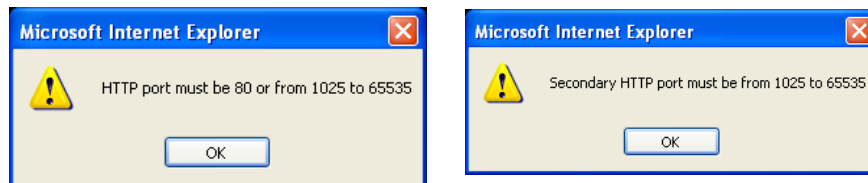
To utilize HTTP authentication, make sure that you have set a password for the Network Camera first; please refer to Security on page 35 for details.

HTTP	
Authentication:	basic ▾
HTTP port:	80
Secondary HTTP port:	8080
Access name for stream 1:	video.mjpg
Access name for stream 2:	video2.mjpg
Access name for stream 3:	video3.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.

In LAN
http://192.168.4.160 or
http://192.168.4.160:8080

**Access name for stream 1 / stream 2 / stream 3:** The access name is used to differentiate the streaming source.

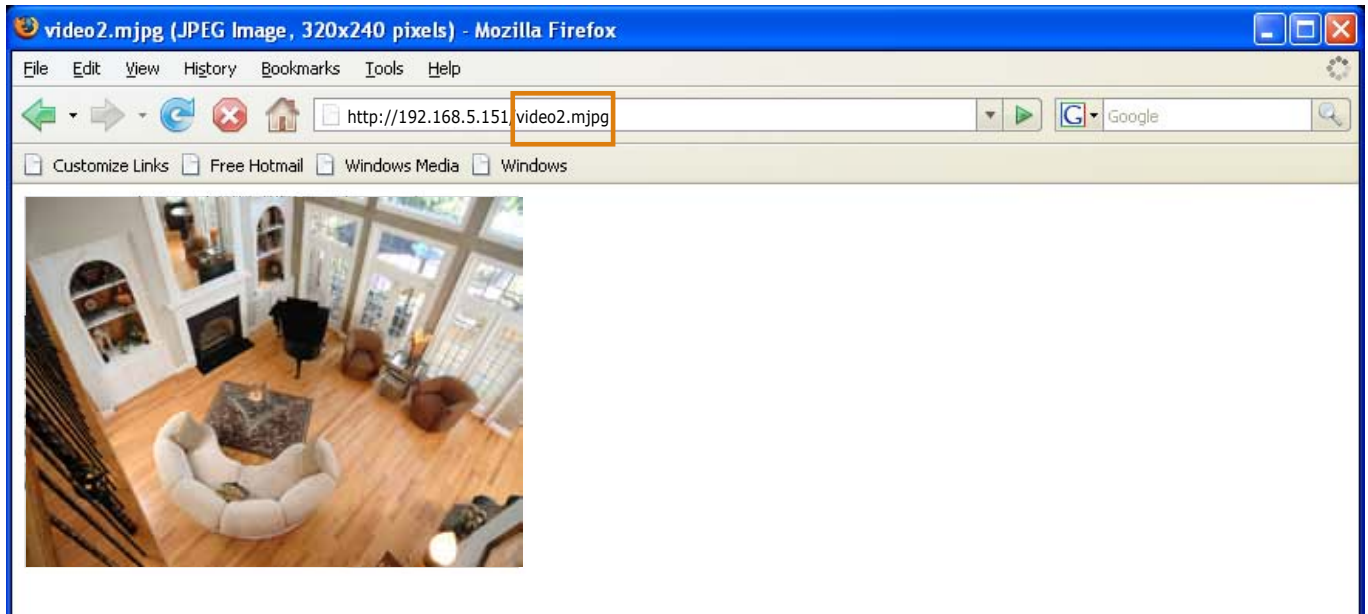
When using Mozilla Firefox or Netscape to access the Network Camera and the video mode is set to JPEG, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.



URL command -- <http://<ip address>:<http port>/<access name for stream1 or stream2>>

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

1. Launch Mozilla Firefox or Netscape.
2. Type the URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.



#### NOTE:

- ▶ Microsoft® Internet Explorer does not support server push technology; therefore, using <http://<ip address>:<http port>/<access name for stream1 or stream2>> will fail to access the Network Camera.

## HTTPS

HTTPS	
HTTPS port:	<input type="text" value="443"/>

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

## FTP

**FTP**

FTP port:

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

## RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for the Network Camera first; please refer to Security on page 35 for details.

**RTSP Streaming**

Authentication:

Access name for stream 1:

Access name for stream 2:

Access name for stream 3:

RTSP port:

RTP port for video:

RTCP port for video:

RTP port for audio:

RTCP port for audio:

✦ Multicast settings for stream 1:

✦ Multicast settings for stream 2:

✦ Multicast settings for stream 3:

**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 in the following table:

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

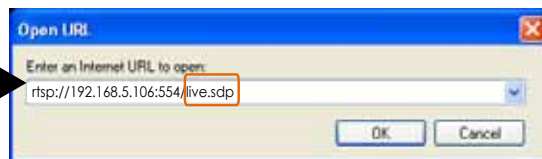
Access name for stream 1 / stream 2 / stream 3: This Network camera supports three simultaneous video streams. The access name is used to differentiate the streaming source.

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

`rtsp://<ip address>:<rtsp port>/<access name for stream1 or stream2>`

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 URL command in the text box. For example:
4. The live video will be displayed in your player as shown below.

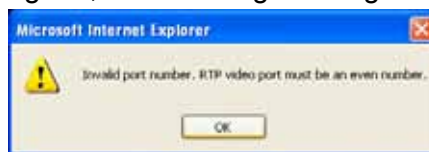


RTSP port /RTP port for video, audio/ RTCP port for video, audio

- 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 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 odd. 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 stream 1 / stream 2 / stream 3: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1, stream 2, or stream 3.

▼ Multicast settings for stream 1: <input type="checkbox"/> Always multicast		▼ Multicast settings for stream 3: <input type="checkbox"/> Always multicast	
Multicast group address:	<input type="text" value="239.128.1.99"/>	Multicast group address:	<input type="text" value="239.128.1.101"/>
Multicast video port:	<input type="text" value="5560"/>	Multicast video port:	<input type="text" value="5568"/>
Multicast RTCP video port:	<input type="text" value="5561"/>	Multicast RTCP video port:	<input type="text" value="5569"/>
Multicast audio port:	<input type="text" value="5562"/>	Multicast audio port:	<input type="text" value="5570"/>
Multicast RTCP audio port:	<input type="text" value="5563"/>	Multicast RTCP audio port:	<input type="text" value="5571"/>
Multicast TTL [1~255]:	<input type="text" value="15"/>	Multicast TTL [1~255]:	<input type="text" value="15"/>
▼ Multicast settings for stream 2: <input type="checkbox"/> Always multicast			
Multicast group address:	<input type="text" value="239.128.1.100"/>		
Multicast video port:	<input type="text" value="5564"/>		
Multicast RTCP video port:	<input type="text" value="5565"/>		
Multicast audio port:	<input type="text" value="5566"/>		
Multicast RTCP audio port:	<input type="text" value="5567"/>		
Multicast TTL [1~255]:	<input type="text" value="15"/>		

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

## Wireless (PT8133W only)

### Manual Configuration:

Setting up wireless cameras' connections can be tricky. The configuration process involves hardwire connection to your LAN for initial setup and wireless connection to AP. To switch between the connection types, you have to physically disconnect the 12VDC connector. For example, when you are finished with initial setup via LAN, you have to remove the RJ-45 LAN cable and disconnect the 12VDC power jack, and then reconnect the power.

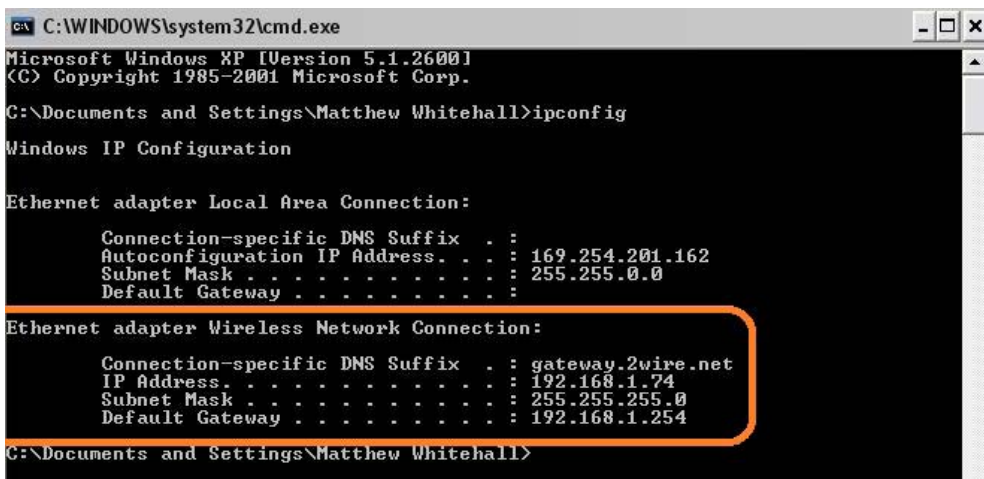
When you are performing the initial setup via LAN, the wireless antenna can be left in place.

To set up a wireless connection with the camera,

1. You must already have a wireless AP and wireless connection available. Find out the name of your wireless network by a click on your Windows System Tray. Jot down the name of the network.



2. You may need to set up static IPs for wireless connections. You can find related information using the "ipconfig" command in a command prompt window.



3. Attach a LAN cable between your wireless camera and router/switch. Use the IW2 utility in the product CD to locate the camera in LAN. Double-click on the IP address to start an IE session with the camera.



4. Enter the **Configuration > Wireless** menu, and enter the name (**SSID**) of the existing wireless network, channel number, and other related information. See the following pages for more details. You may enter the **Configuration > Network** page to setup DHCP or static IP if necessary.
5. Disconnect DC power and LAN cable from camera, and re-connect the DC power to boot the camera. Your IW2 utility should then be able to locate your wireless camera.

For detailed configuration options, please refer to the following pages.

Every time the camera is restarted by reconnecting power, network connection is ready when the camera starts the initial pan/tilt calibration.

**WLAN configuration**

Manual

SSID: default

Wireless mode: infrastructure

Channel: 6

Security: None

WPS

Save

## Manual

**SSID (Service Set Identifier):** This is the name that identifies a wireless network. Access Points and wireless clients attempting to connect to a specific WLAN (Wireless Local Area Network) must use the same SSID. The default setting is “default”. Note: The maximum length for an SSID is 32 single-byte characters and cannot consist of “, <, >, or blank spaces. Note that the SSID is case-sensitive.

**Wireless mode:** Click on the pull-down menu to select from the following options:

- **Infrastructure:** Connect the Network Camera to the WLAN via an Access Point. (default setting)
- **Ad-Hoc:** Connect the Network Camera directly to a host equipped with a wireless adapter in a peer-to-peer environment.

**WLAN configuration**

Manual

SSID: default

Wireless mode: ad-hoc

Channel: 6

Security: None

WPS

**Channel:** While in infrastructure mode, the channel is selected automatically to match the channel setting of the selected Access Point. In Ad-Hoc mode, the channel must be manually set to the same channel for each wireless adapter. The default channel setting depends on the installed region.

**Security:** Select the data encryption method. There are four types, none and WEP, WPA-PSK, and WPA2-PSK.

**WLAN configuration**

Manual

SSID: default

Wireless mode: infrastructure

Channel: 6

Security: None

WPS

Save

1. None: No data encryption.

2. WEP (Wired Equivalent Privacy): This allows communication only with other devices with identical WEP settings.

**WLAN configuration**

Manual

SSID: default

Wireless mode: infrastructure

Channel: 6

Security: WEP

Authentication mode: Open

Key length: 64 bits

Key format: HEX

Default key:

Network key

Shared key

WPS

Network key:

0000000000

0000000000

0000000000

0000000000

Save

- **Authentication Mode:** Choose one of the following modes. The default setting is “Open”.  
Open – Communicates the key across the network.  
Shared – Allows communication only with other devices with identical WEP settings.
- **Key length:** The administrator can set the key length to 64 or 128 bits. The default setting is “64 bits”.
- **Key format:** Hexadecimal or ASCII. The fault setting is “HEX”.  
HEX digits consist of the numbers 0~9 and the letters A-F.  
ASCII is a code for representing English letters as numbers from 0-127 except “, <, > , and the space character which are reserved.
- **Network Key:** Enter a key in either hexadecimal or ASCII format.  
 You can select different key lengths, the acceptable input lengths are as follows:  
 64-bit key length: 10 Hex digits or 5 characters.  
 128-bit key length: 26 Hex digits or 13 characters.



#### NOTE:

- ▶ *When 22(“), 3C(<), or 3E(>) are input as network keys, the key format cannot be changed to ASCII format.*



### 3. WPA-PSK: Use WPA (Wi-Fi Protected Access) pre-shared key.

The screenshot shows the 'WLAN configuration' window with the 'Manual' radio button selected. The settings are as follows:

- SSID: default
- Wireless mode: infrastructure
- Channel: 6
- Security: WPA-PSK
- algorithm: TKIP
- pre-shared key: 0000000000

The 'WPS' radio button is unselected. A 'Save' button is located at the bottom left of the configuration area.

More secure than WEP, the Wi-Fi Alliance developed WPA (Wi-Fi Protected Access) in 2003 to address WEP's weaknesses. Improvements included TKIP, which changes the encryption key for each data transmission.

- **Algorithm:** Choose one of the following algorithms for WPA-PSK and WPA2-PSK modes.

**TKIP (Temporal Key Integrity Protocol):** A security protocol used in IEEE 802.11 wireless networks.

TKIP is a "wrapper" that goes around the existing WEP encryption. TKIP is comprised of the same encryption engine and RC4 algorithm defined for WEP; however, the key used for encryption in TKIP is 128 bits long. This solves the first problem of WEP: a short key length. (From Wikipedia)

**AES (Advanced Encryption Standard):** In cryptography, the Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government.

As of 2006, AES is one of the most popular algorithms used in symmetric key cryptography. (From Wikipedia)

- **Pre-shared Key:** Enter a key in ASCII format. The length of the key can be between 8 to 63 characters.

### 4. WPA2-PSK: Use WPA2 pre-shared key.

This advanced protocol, certified through Wi-Fi Alliance's WPA2 program, implements the mandatory elements of 802.11i. In particular, it introduces a new AES-based algorithm, CCMP, that is considered fully secure. From March 13, 2006, WPA2 certification is mandatory for all new devices wishing to be certified by the Wi-Fi Alliance as "Wi-Fi CERTIFIED." (From Wikipedia)

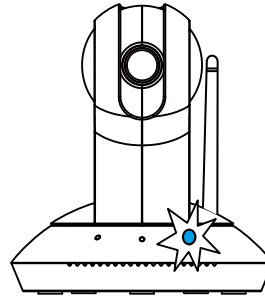
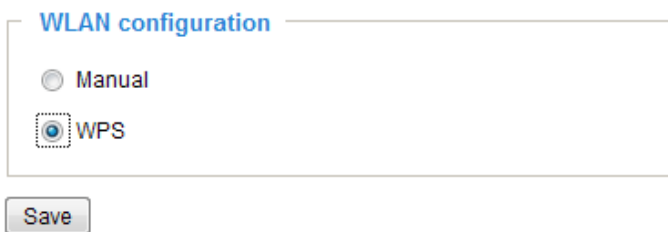


#### NOTE:

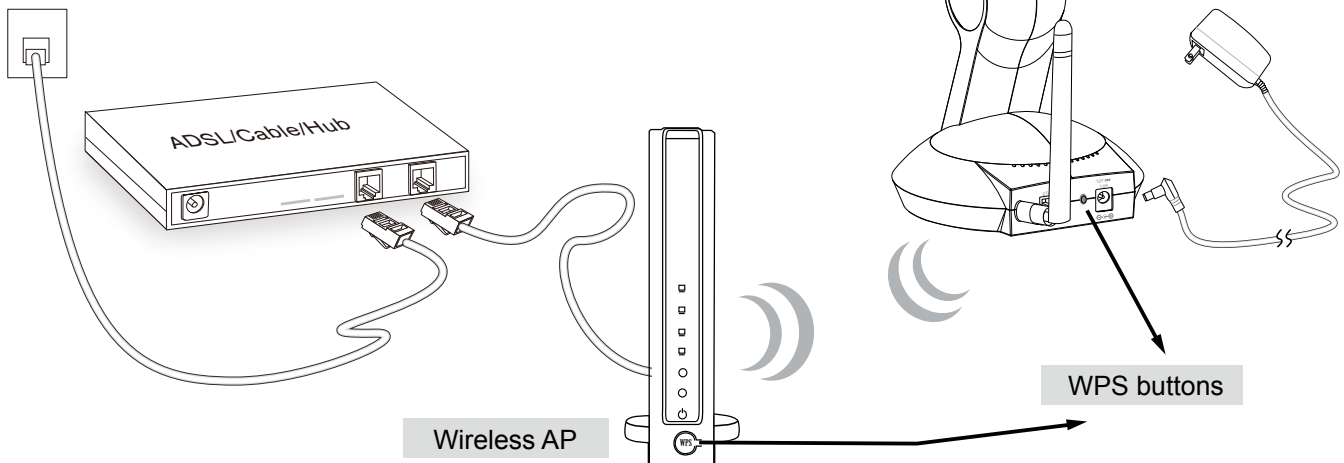
- ▶ *After wireless configurations are completed, click Save and the camera will reboot. Wait for the live image to be reloaded to your browser. For VIVOTEK 81xx-series cameras, you have to unplug the power and Ethernet cables from the camera; then re-plug the power cable to the camera. The camera will then switch to wireless mode.*
- ▶ *Some invalid settings may cause the system to fail to respond. Change the configuration settings only if necessary and consult with your network supervisor or experienced users for correct settings. Once the system has lost contact, please refer to Maintenance on page 105 for reset and restore procedures.*

## WPS:

1. Make sure your AP (Access Point) and Operating System support WPS (Wi-Fi Protected Setup) functions. WPS enables easy setup with compatible APs.
2. Connect your camera using a LAN cable, open a web console, and enter the **Configuration** -> **Wireless** page. Select the **WPS** checkbox, and click the **Save** button.
3. The camera's blue LED should start flashing. Press and hold down both of the WPS buttons on your AP and your camera for at least 1 second. (Some router/AP will have a virtual button on their management software instead.) Refer to your AP's documentation for details using its WPS function.  
If your AP does not support WPS, configure your wireless connection manually.



4. Wait for 2 minutes with the onscreen progress bar. The camera should then reboot. When the progress bar disappears, disconnect your LAN cable. You can refresh or re-start your web console to see live video.



When WPS configuration is done, wireless connectivity will be established and the security encryption, such as WEP or WPA-PSK, will be synchronized with the AP. Use the IW2 utility to find the camera. As for IP setting, the camera's use of DHCP or static IP is determined by your configuration on the network camera via the web-based configuration of firmware. The camera's default is DHCP.

## 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.

### 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, then 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 a dynamic domain account when selecting other DDNS providers:

- [Dyndns.org\(Dynamic\) / Dyndns.org\(Custom\)](http://www.dyndns.com/): 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/>

## Access List Advanced Mode

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

### General Settings

**Filter Type**

Allow  Deny

Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream #1, #2, and #3). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (IE Explore or Quick Time Player).

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

Connection status

	IP address	Elapsed time	User ID
<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 has the client been at the webpage.
- User ID: If the administrator has set a password for the webpage, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to access the webpage without a user name and password, the User ID column will be empty.

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

1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security on page 35.
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 55.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing**, please refer to Security on page 35.

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

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

## Filter

Select the checkbox in the Filter Type panel as permission control: Allowed or Deny list. Only those clients whose IP addresses are on the Allowed list and not on the Denied list can access the Network Camera. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to page 46 for detailed information.

The image shows two panels from a software interface. The top panel, titled "Filter Type", contains two radio buttons: "Allow" (which is selected) and "Deny". Below these buttons is a "Save" button. The bottom panel, titled "Filter", contains a sub-panel titled "IPv4 access list". Inside this sub-panel is a text box containing the IP address "192.168.4.101". Below the text box are two buttons: "Add" and "Delete".

- **Add a rule to configure an Allowed/Denied list:** Click **Add** to add a rule to Allowed/Denied list.

There are three types of rules for user to set up:

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

For example:

The image shows a dialog box titled "filter address". It contains a "Rule:" dropdown menu with "Single" selected. Below it is an "IP address:" text box containing "192.168.2.1". At the bottom of the dialog are two buttons: "OK" and "Cancel".

**Network:** This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List. The IP address is written in the CIDR format.

For example:

**filter address**

Rule: Network ▼

Network address / Network mask  /

IP address 192.168.2.x will be blocked.

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

For example:

**filter address**

Rule: Range ▼

IP address - IP address  -

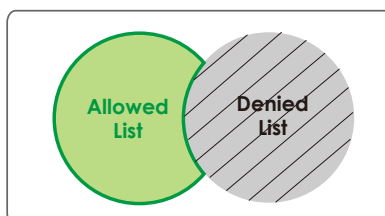
■ Delete Allowed/Denied list:

In the Delete Allowed List or Delete Denied List column, make a selection and click **Delete**.



**NOTE:**

► For example, when the range of IP addresses in the allowed list is set from 1.1.1.0 to 192.255.255.255 and the range in the denied list is set from 1.1.1.0 to 170.255.255.255, only users' IP located between 171.0.0.0 and 192.255.255.255 can access the Network Camera.



**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

## Audio and Video

This section explains how to configure the audio and video settings of the Network Camera. It is composed of the following two columns: Video Settings and Audio Settings.

### Video Settings

**Video Settings**

Video title:

Color:

Power line frequency:

Video orientation:  Flip  Mirror

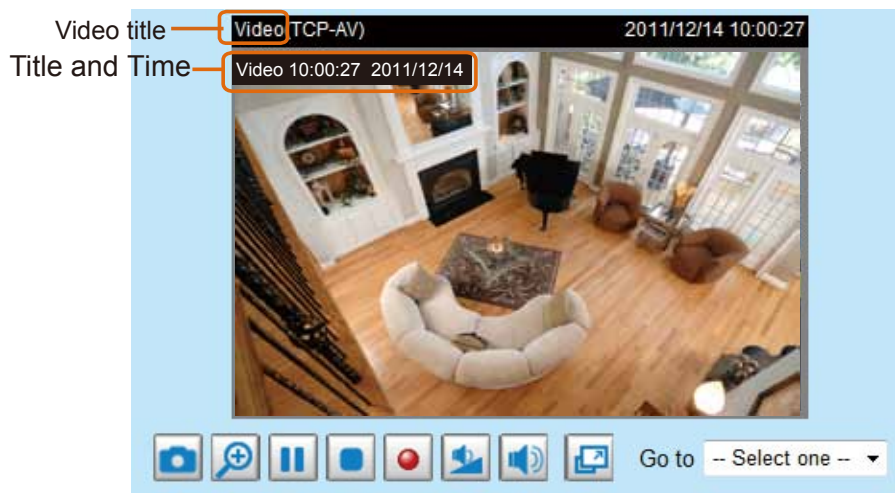
Overlay title and time stamp on video and snapshot.

▶ Video quality settings for stream 1:

▶ Video quality settings for stream 2:

▶ Video quality settings for stream 3:

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



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

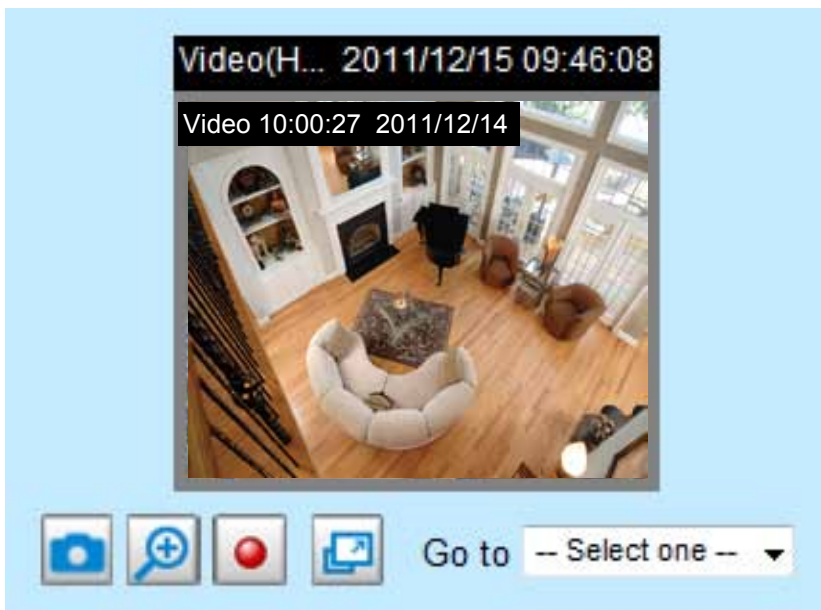
**Power line frequency:** Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the Network Camera in order for the 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. The camera's default is to be mounted up-side down to the included bracket as a ceiling mount. Select both options if the Network Camera is installed on a desktop or flat surface (i.e., sitting on its flat bottom) to correct the image orientation.

**Overlay title and time stamp on video:** Select this option to place the video title and time on the video streaming view cells.

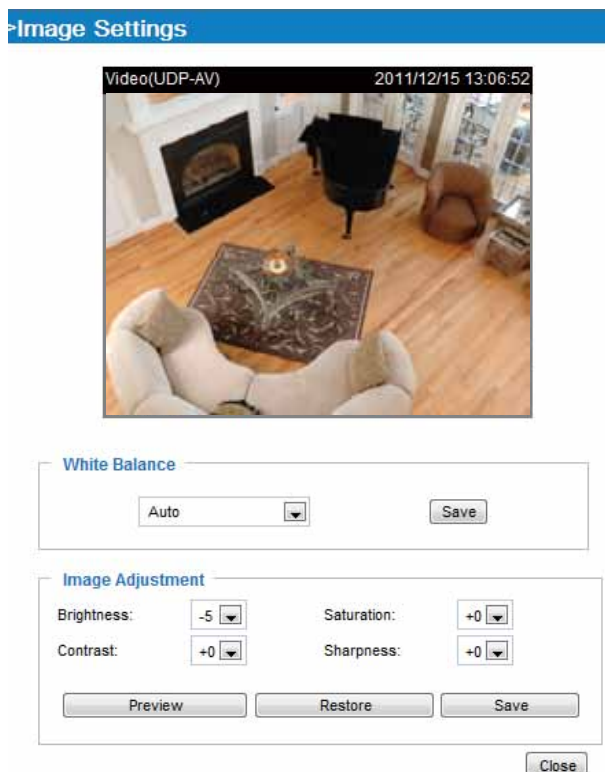


Note that when the frame size is set to 176 x 144 as shown in the picture below, only the time will be stamped on the video streams.



[Image Settings](#) **Advanced Mode**

Click **Image Settings** to open the Image Settings page. On this page, you can tune the White Balance, Brightness, Saturation, Contrast, and Sharpness for the video.



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

- Auto: The camera will automatically adjust the color temperature of the light in response to different light sources. You may follow the steps below to adjust the white balance to the best color temperature.
  1. Set the White balance to **Auto**.

- Place a sheet of paper of white or cooler color temperature, such as blue, in front of the lens, then allow the Network Camera to adjust the color temperature automatically.
- Select **Keep current value**, and click the **Save** button to preserve current configuration.

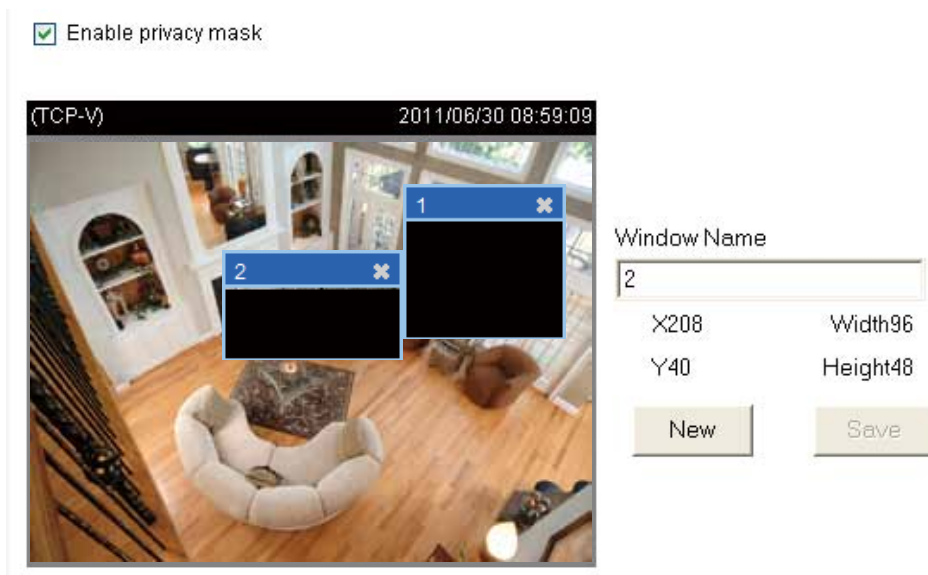
### Image Adjustment

- **Brightness:** Adjust the image brightness level, which ranges from -5 to +5. The default value is set to 0.
- **Saturation:** Adjust the image saturation level, which ranges from -5 to +5. The default value is set to 0.
- **Contrast:** Adjust the image contrast level, which ranges from -5 to +5. The default value is set to 0.
- **Sharpness:** Adjust the image sharpness level, which ranges from -3 to +3. The default value is set to +3.

You can click **Preview** to fine-tune the image, or 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 and click **Close** to exit the page.

### Privacy mask Advanced Mode

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



- To set the privacy mask windows, follow the steps below:
  - Click **New** to add a new window.
  - Use the mouse to size and drag-drop the window, which is recommended to be at least twice the size of the object (height and width) you want to cover.
  - Enter a Window Name and click **Save** to enable the setting.
  - Check **Enable privacy mask** to enable this function.



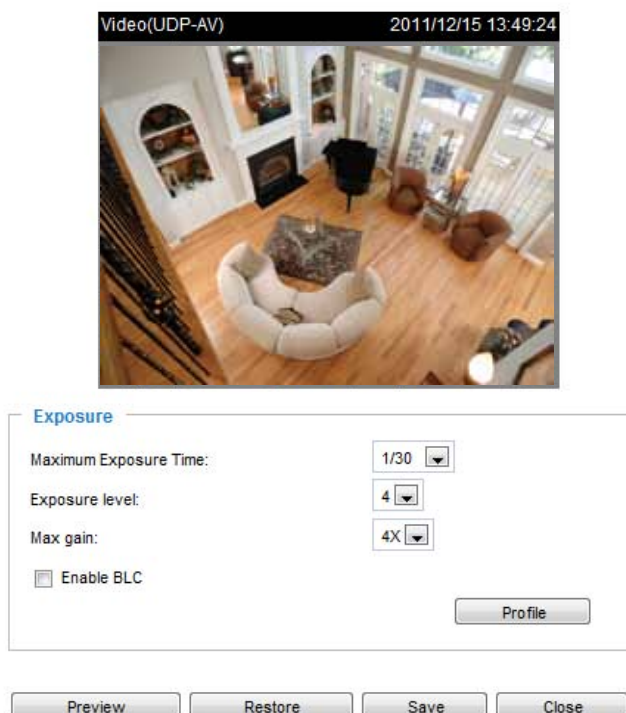
#### **NOTE:**

- ▶ *Up to 5 privacy mask windows can be configured on the same screen.*
- ▶ *If you want to delete a configured mask window, click on the 'X' button at the upper right corner of the window.*

## Sensor Settings **Advanced Mode**

Click **Sensor settings** to open the Sensor Settings page. On this page, you can set the Maximum Exposure Time, Exposure level, BLC settings, and an image profile for a different period of time.

### >Sensor Settings



The screenshot shows a video preview window at the top with the text "Video(UDP-AV)" and a timestamp "2011/12/15 13:49:24". The video displays a living room with a fireplace, a piano, and a large window. Below the video is a settings panel titled "Exposure" with the following controls:

- Maximum Exposure Time: 1/30
- Exposure level: 4
- Max gain: 4X
- Enable BLC
- Profile button

At the bottom of the settings panel are four buttons: Preview, Restore, Save, and Close.

**Maximum Exposure Time:** The default iris setting of the sensor is fixed mode, and the AES option will be **1/30**. There are several options for AES: 1/5, 1/15, 1/30, 1/60, 1/120, 1/240, and 1/480 second. Faster electronic shutter would enable the Network Camera to capture fast-moving objects more clearly.

**Exposure level:** Select a value ranging from 1 to 8 to determine the exposure level depending on the lighting condition of the installation site.


**Max gain:** Select 2X, 4X, or 8X for exposure gain values should the need arises for low lighting conditions. While the signal gains increase, noises will also increase.

**Enable BLC (Back Light Compensation):** Select it when the object is too dark or too bright to be recognized, e.g., an object of interest is posed against a bright background. It will give the captured images the necessary light compensation.

If you want to configure another sensor setting for day/night/schedule mode, please click the **Profile** button to open the Profile Settings window as shown below.

>Sensor Setting Profile

Video(UDP-AV) 2011/12/15 14:24:50



**General Settings**

Enable this profile

This profile is applied to

Schedule mode:

From  to  [hh:mm]

**Exposure**

Maximum Exposure Time:  ▾

Exposure level:  ▾

Max gain:  ▾

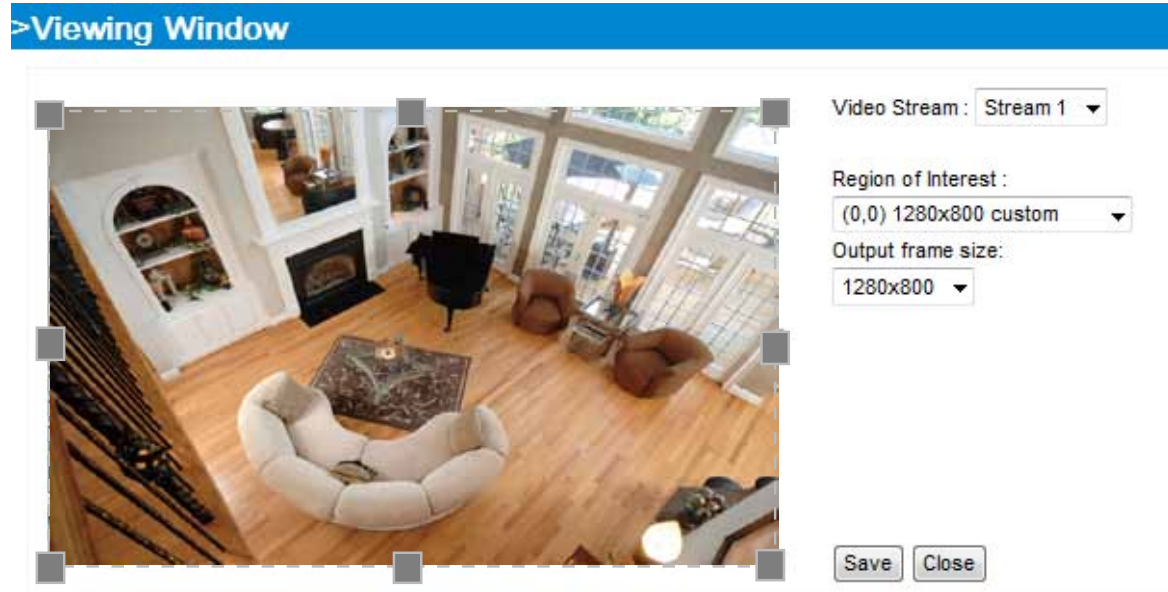
Enable BLC

Please follow the steps below to setup a profile:

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

## Viewing Window **Advanced Mode**

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 ~ 3.



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

1. Select a stream which you want to set up the viewing region. If you want to stream out the video to a mobile device, please select stream 3.
2. Select a **Region of Interest** from the drop-down list. The floating frame, 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.

	NTSC	PAL
WXGA	1280 x 800	-
hd720	1280 x 720	-
XVGA	1024 x 768	-
SVGA	800 x 600	-
D1	720 x 480	720 x 576
4CIF	704 x 480	704 x 576
VGA	640 x 480	-
CIF	352 x 240	352 x 288
QVGA	320 x 240	-
QCIF	176 x 144	-

3. Choose a proper **Output Frame Size** from the drop-down list according to the size of your monitoring device.

## Video quality settings for multiple streams Advanced Mode

The Network Camera offers three choices of video compression standards for real-time viewing: MPEG-4, H.264, and MJPEG.

Click the items to display the detailed configuration settings. You can set up three separate streams for the Network Camera 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.

If **MPEG-4** mode is selected, it is streamed in RTSP protocol.

▼ Video quality settings for stream 1:

MPEG-4:

Frame size:

Maximum frame rate:

Intra frame period:

Video quality:

Constant bit rate:

Fixed quality:

▼ Video quality settings for stream 2:

MPEG-4:

Frame size:

Maximum frame rate:

Intra frame period:

Video quality:

Constant bit rate:

Fixed quality:

▼ Video quality settings for stream 3:

MPEG-4:

H.264:

JPEG:

Frame size:

Maximum frame rate:

Video quality:

There are four parameters provided in MPEG-4 mode which allow you to adjust the video performance:

- **Frame size**  
Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions: 1280 x 800, 1280 x 720, 640 x 400, 320 x 200, and 176 x 144.
- **Maximum frame rate**  
This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video quality. 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 to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.
- **Video quality**  
A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. Therefore, if **Constant bit rate** is selected, the bandwidth utilization is fixed at a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, 4Mbps, 6Mbps, and 8Mbps. You can also select **Customize** and manually enter a value.



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

The **H.264** mode has similar settings with that of the MPEG-4 mode as previously mentioned, yet it offers a higher compression rate for saving storage and network bandwidth. On the other hand, it requires higher computing resources to decode the video on the receiver's side.

If **JPEG** mode is selected, the Network Camera continuously sends JPEG images to the client, producing a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents are a combination of JPEG images, no audio data is transmitted to the client.

There are three parameters provided in MJPEG mode to control the video performance:

■ **Frame size**

Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions:

WXGA	1280 x 800
hd720	1280 x 720
Custom	640 x 400
Custom	320 x 200

■ **Maximum frame rate**

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

■ **Video quality**

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



**NOTE:**

- The **Custom** value you enter for Video quality here is related the **Compression rate** of each still JPEG image. A lower value produces higher JPEG image quality.

## Audio Settings

**Audio Settings**

Mute

Internal microphone input gain: +3 dB ▾

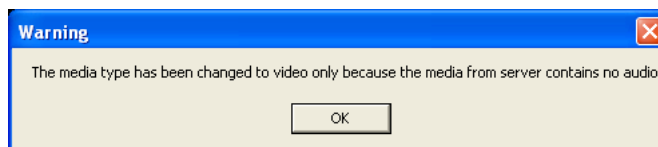
Audio type:

GSM-AMR:

G.711:

Mode: pcmu ▾

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



**Internal microphone input gain:** Select the gain of the internal audio input according to ambient conditions. Adjust the gain from +21 db (most sensitive) ~ -33 db (least sensitive).

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

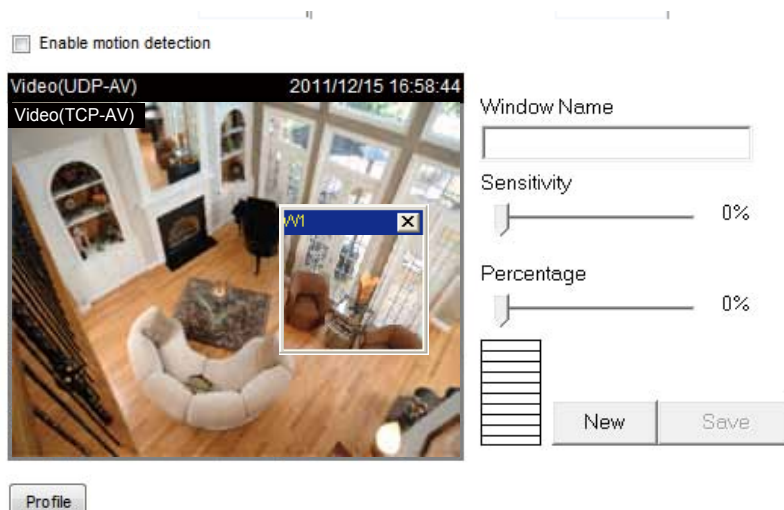
- GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable from: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps, and 12.2Kbps.
- G.711 also provides good sound quality and requires about 64Kbps. Select pcmu ( $\mu$ -Law) or pcma (A-Law) mode.

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



## Motion Detection

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



Follow the steps below to enable motion detection:

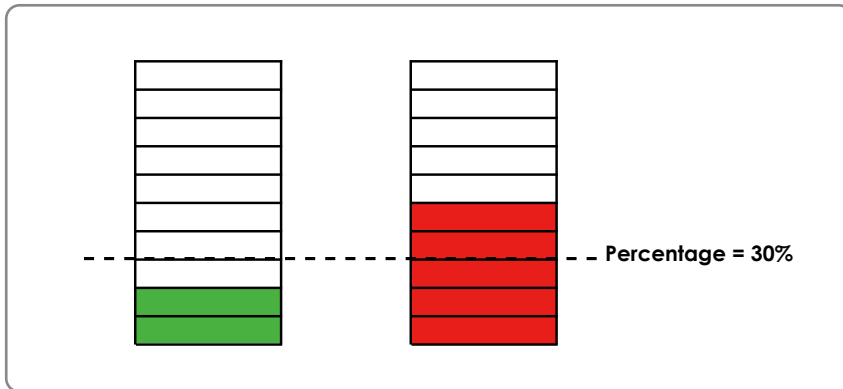
1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
  - To move and resize the window, drag and drop your mouse on the window.
  - To delete window, click X on the top right corner of the window.
3. Define the sensitivity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

For example:



The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to be sent to a remote server (Email, FTP) by utilizing this feature as a trigger source. For more information on how to set an event, please refer to Application on page 86.

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.



**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.

## Motion Detection Profile

You may create additional Motion Detection profile for different application scenarios, e.g., a different setting for the off-office hours.

### > Motion Detection Profile Settings

Video(UDP-AV)
2011/12/15 17:07:51



Window Name

Sensitivity

Percentage


**General Settings**

Enable this profile

This profile is applied to:

Schedule mode:

From  to  [hh:mm]

Configure the period of time during which this profile will apply. Set up a detection window, and then click the **Save** button and the **Close** button to finish the configuration. The Motion Detection takes effect even when it is panning or patrolling through points of interest in its surveillance area.

## Camera Control

This section explains how to control the Network Camera's Pan/Tilt/Zoom/Focus operation via the control panel and how to create preset positions.

### Preset Locations

On this page, you can create preset positions for the Network Camera to go to directly or patrol consecutively from one position to another. A total of 128 preset positions can be configured.

Please follow the steps below to create preset positions:

1. Adjust the shooting area to a desired position using the buttons on the upper-right corner of the window. You can also use mouse clicks on the view cell to move the camera shooting direction.
2. Click **Set Current position as home** or **Restore home position to default** to define your home position.
3. Enter a name for the preset position, which allows for up to forty characters. Click **Add** to enable the settings. The preset positions will be displayed under the Preset Location list on the left-hand side.
4. To add additional preset positions, please repeat step 1~3.
5. To remove a preset position, select its checkbox from the drop-down list and click **Remove**.
6. Click **Save** to enable the settings.



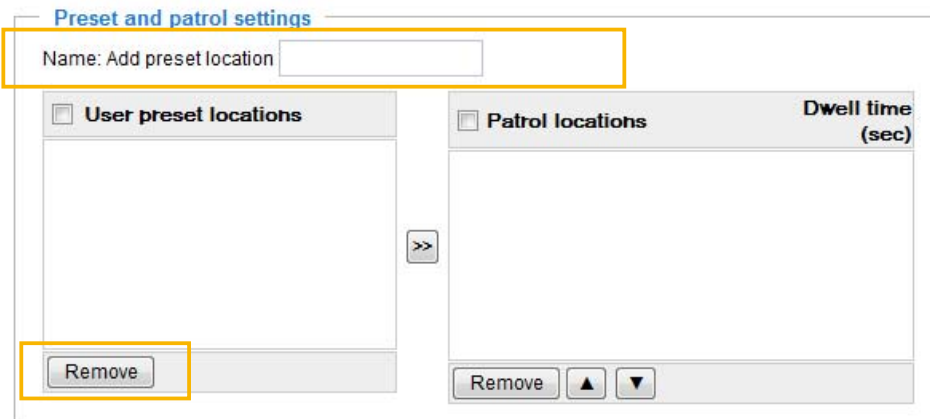
1

functions are the same as the control panel on home page

2



3



5



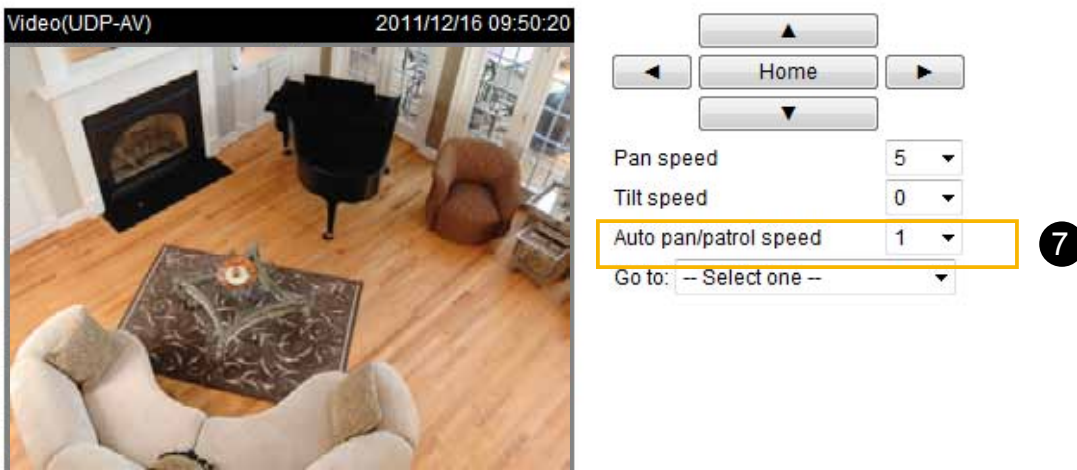
6



## Patrol Settings

You can select preset locations to arrange the patrolling tour for the Network Camera. Please follow the steps below to set up a patrolling tour:

1. Click to select one or multiple preset locations by checking their checkboxes.
2. Click the >> (Move) button to move them to the Patrol locations column.
3. Click to select a position, and manually enter a **Dwelling time** for the camera to stay during an auto patrol. The default value is 5 seconds.
4. Repeat step 1 and 3 to select and configure individual patrol locations.
5. If you want to delete a selected location, select it from the list and click **Remove**.
6. Select a location and click **Up** or **Down** to rearrange the patrolling order.
7. Adjust the **Auto pan/patrol speed**. (1~5 scale determining how fast moving to the next position)
8. Click **Save** to enable the settings.



### Home location settings

Set current position as home

Restore home position to default

### Preset and patrol settings

Name: Add preset location

#### User preset locations

- upper right
- right
- center
- top
- left

Remove

#### Patrol locations

Dwell time (sec)

- upper right 5
- right 5
- center 5
- top 5
- left 5

Remove

▲ ▼

### Misc settings

Return to home position while idle

Save



### NOTE:

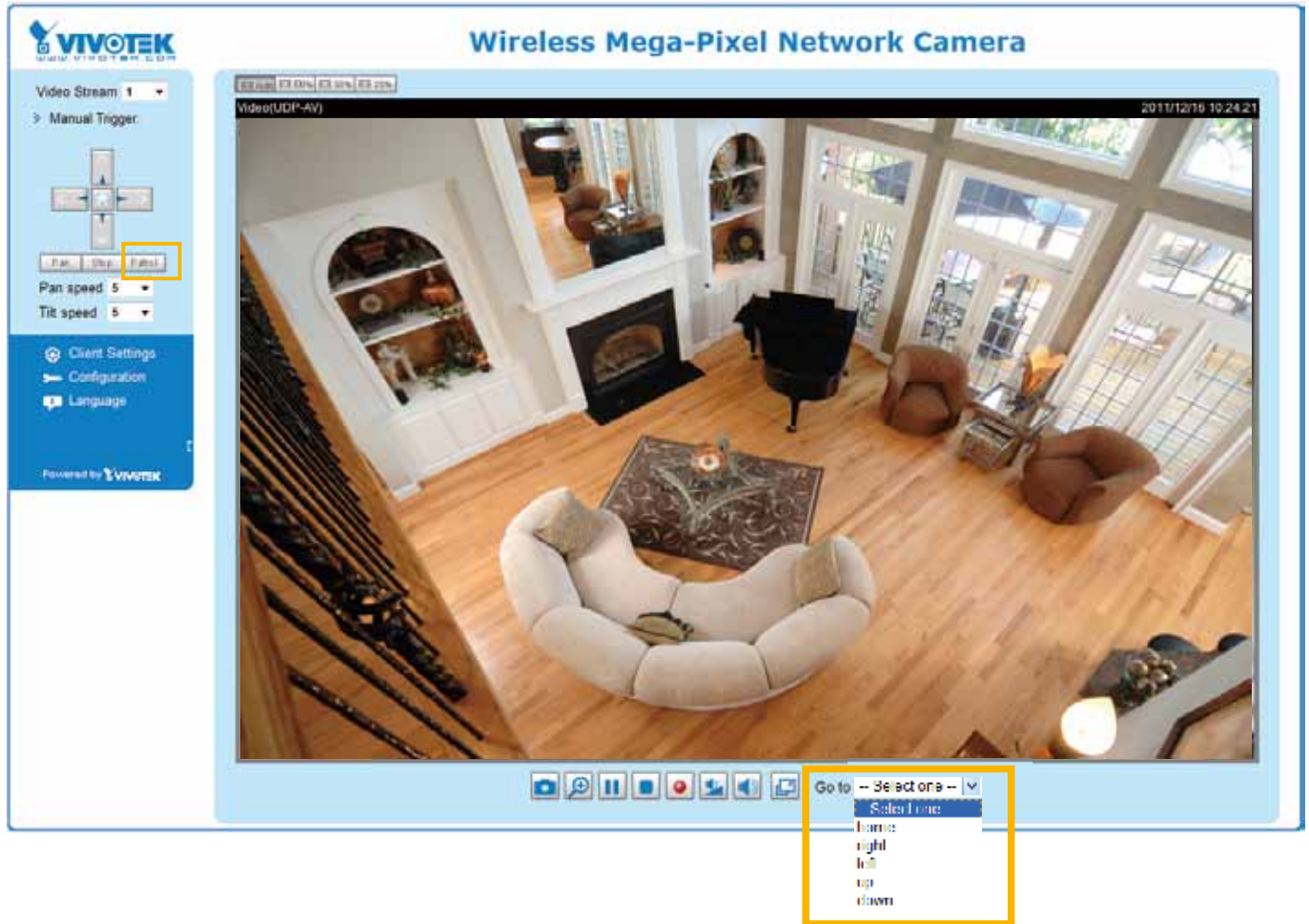
A patrol takes place by clicking the **Patrol** button on the home page, and ends when the last position is reached.



## Return to Home Position while Idle

If you select this option, the Network Camera will automatically return to the home position after idling for a specific time span. Please remember to click **Save** to enable the settings.

- The Preset Locations will be displayed on the Home page:



- Click **Go to**: The Network Camera will move to the preset location.
- Click **Patrol**: The Network Camera will patrol among the selected preset positions (from right to left) for once.

## Homepage Layout Advanced Mode

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

### Preview

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



Hide Powered by VIVOTEK

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


### Logo


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

**Logo graph**

You can upload a small logo(Gif, JPG or PNG), which will be resized to 160x50 pixels (if it is not already that size) and which will be visible on the main page. Upload a new logo will replace the old custom logo (if there was one uploaded)

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.

### Theme Options

**Themes**







Custom

**Color:**

Font color:

Font color of configuration area:

Font color of video title:

Bk color of control area:

Bk color of configuration area:

Bk color of video area:

Frame color:

Preview

Font color

Background Color of the Control Area

Font Color of the Configuration Area

Background Color of the Configuration Area



Font Color of the Video Title

Background Color of the Video Area

Frame Color

Preview

Video Stream 1

Manual Trigger:

Client Settings

Powered by VIVOTEK



Preview

Video Stream 1

Manual Trigger:

Client Settings

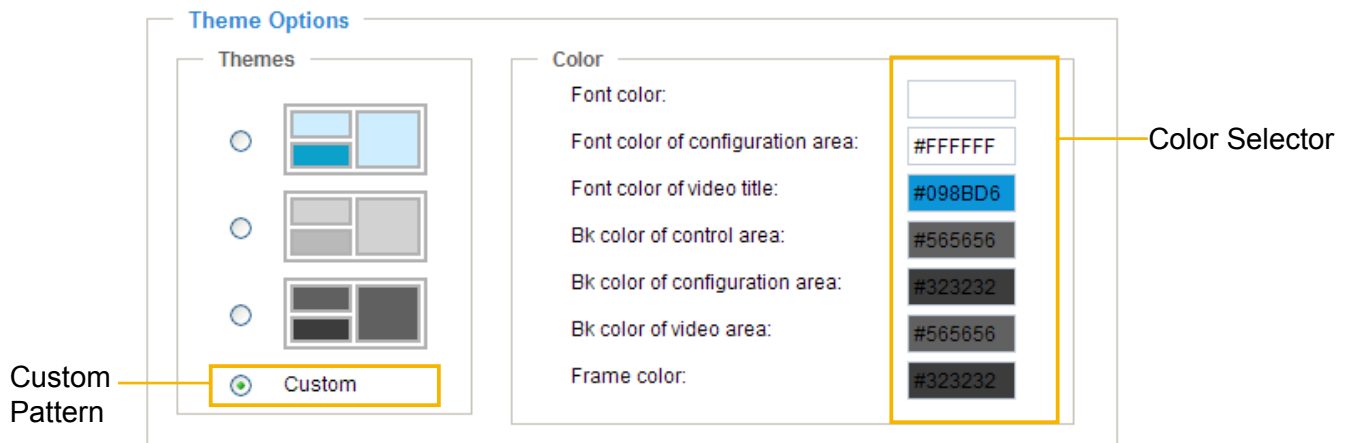
Powered by VIVOTEK



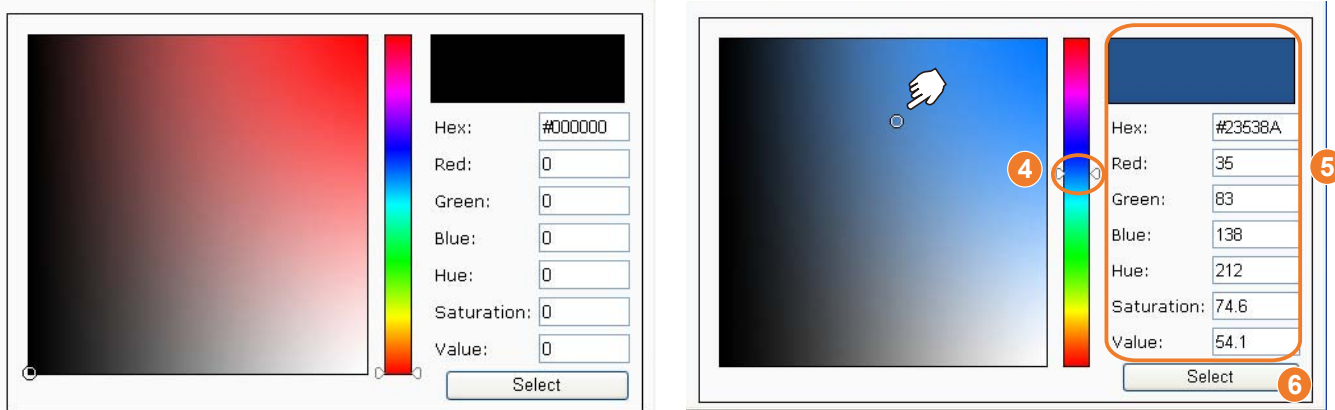


■ Follow the steps below to set up the customized homepage:

1. Click **Custom** on the left column.
2. Click the field where you want to change the color on the right column.



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

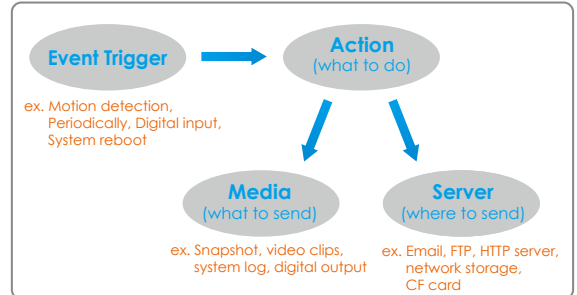


4. Drag the slider bar and/or click on the left square to select a desired color.
5. The selected color will show up in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

## Application Advanced Mode

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

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



**Event Settings**

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger
<input type="button" value="Add"/> <input type="button" value="Help"/>										

**Customized Script**

Name	Date	Time
<input type="button" value="Add"/> <input type="button" value="▼"/> <input type="button" value="Delete"/>		

### Customized Script

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

**Customized Script**

Name	Date	Time
<a href="#">User1</a>	20081113	18:13:46
<a href="#">User2</a>	20081113	18:11:32

```

<?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>
<weekdays>1-5</weekdays>
<time>08:30:00-20:30:00</time>
</duration>
</schedule>
<!-- Motion -->
<action condition="0">
<status id="1">trigger</status>
<status id="1">trigger</status>
</action>
<event id="2">
<description>Mail system log to email address</description>
<condition>0</condition>
<scheduleid>0</scheduleid>
<delay>1</delay>
<!-- users can send email with title "Motion" to recipient guiding.yang@vivotek.com. The body of mail is the log messages -->
<process>
/usr/bin/ampollent -r "Motion" -f IP@vivotek.com -b /var/log/messages -s mv.vivotek.tw -N 3 guiding.yang@vivotek.com
</process>
<priority>0</priority>
</event>
</eventmgr>
          
```

## Event Settings

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

> Event Settings

Event name:

Enable this event

Priority:

Detect next event after  second(s).

Note: This can only applied to motion detection and digital input

**Trigger**

Video motion detection

Manual Trigger

Periodically

System boot

Recording notify

**Event Schedule**

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Time**

Always

From  to  [hh:mm]

**Action**

Move to preset location:

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

Server	Media	Extra parameter

Event name: Enter a name for the event setting.

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

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

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

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

### Trigger

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

There are several choices of trigger sources as shown below. Select the items 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 77 for details.

The screenshot shows a configuration window titled "Trigger". It contains several radio button options: "Video motion detection" (selected), "Manual Trigger", "Periodically", "System boot", and "Recording notify". Under "Video motion detection", there are two sub-options: "Normal" with a checkbox and the text "entrance", and "Profile" with a checkbox and the text "corridor". A note below these options reads: "Note: Please configure [Motion detection](#) first".

#### ■ Manual Trigger

Users can manually trigger an event using the Manual Trigger button on the home page.

#### ■ Periodically

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

The screenshot shows a configuration window titled "Trigger". It contains several radio button options: "Video motion detection:", "Periodically:" (selected), "Digital input", "System boot", and "Recording notify". Under "Periodically:", there is a text input field with the value "1" and the text "Trigger every other" and "minutes".

#### ■ System boot

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

#### ■ Recording notify

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

### Event Schedule

Specify the period for the event.

**Event Schedule**

Sun
  Mon
  Tue
  Wed
  Thu
  Fri
  Sat

**Time**

Always

From  to  [hh:mm]

- Select the days of the week. For example, some detection might not need to be applied during the office hours, while they are necessary during the off-office hours.
- Select the recording schedule in 24-hr time format.

### Action

Define the actions to be performed by the Network Camera when an event is triggered.

**Action**

Move to preset location:

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

Server	Media	Extra parameter

- Move to preset location  
Select this option, the Network Camera will move to the preset location when a trigger is activated. Please setup the preset locations first. Please refer to Preset Locations on page 80 for detailed information.

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

- Add Server / Add Media  
Click **Add Server** to configure [Server Settings](#). For more information, please refer to Server Settings on page 92.  
Click **Add Media** to configure [Media Settings](#). For more information, please refer to Media Settings on page 95.

Here is an example of Event Settings page:

Event name:

Enable this event

Priority:

Detect next event after  second(s).

Note: This can only applied to motion detection and digital input

**Trigger**

Video motion detection

Manual Trigger

Periodically

System boot

Recording notify

**Event Schedule**

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Time**

Always

From  to  [hh:mm]

**Action**

Move to preset location:

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

Server	Media	Extra parameter
<input type="checkbox"/> NAS	<input type="text" value="----None----"/>	<input type="checkbox"/> Create folders by date time and hour automatically
		<input type="button" value="View"/>
<input type="checkbox"/> Email	<input type="text" value="----None----"/>	
<input type="checkbox"/> FTP	<input type="text" value="----None----"/>	

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

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

**Event Settings**

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	motion

**Server Settings**

Name	Type	Address/Location
<a href="#">NAS</a>	ns	\\192.168.5.122\nas
<a href="#">FTP</a>	ftp	ftp.vivotek.com
<a href="#">Email</a>	email	Ms.vivotek.tw
<a href="#">HTTP</a>	http	http://192.168.3.10/cgi-bin/upload.cgi

**Media Settings**

Available memory space: 3550KB

Name	Type
<a href="#">Snapshot</a>	snapshot
<a href="#">Video Clip</a>	videoclip
<a href="#">System log</a>	systemlog

**Customized Script**

Name	Date	Time
------	------	------

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

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

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

To remove a media setting from the list, select a media name from the drop-down list and click **Delete**. Note that a media setting can be deleted when the media setting is not currently associated with an event setting.

## Server Settings

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

Server name: Enter a name for the server setting.

### Server Type

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

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

Server name:

**Server Type**

Email:

Sender email address:

Recipient email address:

Server address:

User name:

Password:

Server port:

This server requires a secure connection (SSL)

FTP:

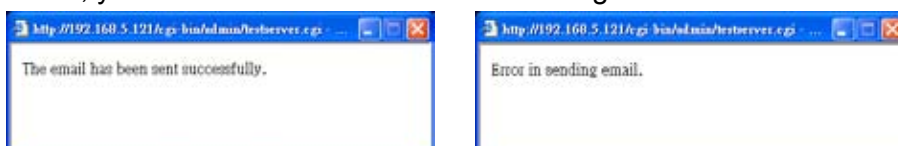
HTTP:

Network storage:

- Sender email address: Enter the email address of the sender.
- Recipient email address: Enter the email address of the recipient.
- Server address: Enter the domain name or IP address of the email server.
- User name: Enter the user name of the email account if necessary.
- Password: Enter the password of the email account if necessary.
- Server port: The default mail server port is set to 25. You can also manually set another port.

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

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



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



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

Server name:

**Server Type**

Email:

**FTP:**

Server address:

Server port:

User name:

Password:

FTP folder name:

Passive mode

HTTP:

Network storage:

- **Server address:** Enter the domain name or IP address of the FTP server.
- **Server port**  
By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.
- **User name:** Enter the login name of the FTP account.
- **Password:** Enter the password of the FTP account.
- **FTP folder name**  
Enter the folder where the media file will be placed. If the folder name does not exist, the 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** to enable the settings, then click **Close** to exit the page.

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

Server name:

**Server Type**

Email:

FTP:

HTTP:

URL:

User name:

Password:

Network storage:

- URL: Enter the URL of the HTTP server.
- User name: Enter the user name if necessary.
- Password: Enter the password if necessary.

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



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

**Network storage:** Select to send the media files to a network storage location when a trigger is activated. Please refer to **Network Storage Setting** on page 99 for details.

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

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

	Server	Media	Extra parameter
<input type="checkbox"/>	FTP	----None----	
<input type="checkbox"/>	NAS	----None----	<input type="checkbox"/> Create folders by date time and hour automatically <input type="button" value="View"/>
<input type="checkbox"/>	Email	----None----	
<input type="checkbox"/>	HTTP	----None----	

## Media Settings

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

**Media name:** Enter a name for the media setting.

### Media Type

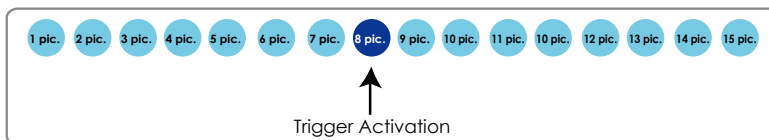
There are three choices of media types available: Snapshot, Video clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.

**Snapshot:** Select to send snapshots when a trigger is activated.

The screenshot shows a web form for configuring a media setting. At the top, there is a text input field labeled "Media name:" containing the word "Snapshot". Below this is a section titled "Media Type" with three radio button options: "Snapshot" (which is selected), "Video Clip", and "System log". Under the "Snapshot" option, there are several fields: a "Source:" dropdown menu set to "Stream 1", two "Send" input fields (both containing "1") labeled "pre-event image(s) [0~7]" and "post-event image(s) [0~7]", and a "File name prefix:" input field containing "Snapshot\_". There is also a checked checkbox labeled "Add date and time suffix to file name". At the bottom of the form are "Save" and "Close" buttons.

- **Source:** Select to take snapshots from stream 1 or stream 2.
- **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** to enable the settings, then click **Close** to exit the page.

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

Media name:

**Media Type**

Snapshot

Video Clip

Source:

Pre-event recording:  seconds [0~9]

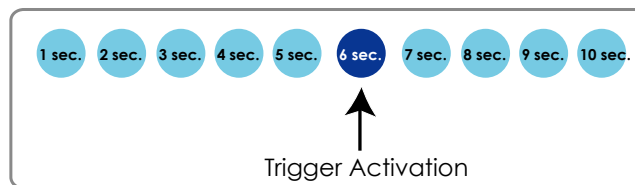
Maximum duration:  seconds [1~10]

Maximum file size:  Kbytes [50~800]

File name prefix:

System log

- **Source:** Select to record video clips from stream 1 or stream 2.
- **Pre-event recording**  
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.
- **Maximum duration**  
Specify the maximum recording duration in seconds. Up to 10 seconds can be set.  
For example, if pre-event recording is set to five seconds and the maximum duration is set to ten seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.



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



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

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

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

You can continue to select a server and media type for the event.

The screenshot shows a configuration window with two buttons at the top: "Add Server" and "Add Media". Below them is a table with three columns: "Server", "Media", and "Extra parameter".

	Server	Media	Extra parameter
<input type="checkbox"/> NAS		<input type="checkbox"/> Create folders by date time and hour -----None----- automatically <input type="button" value="View"/>	
<input type="checkbox"/> FTP		Video clip snapshot system log -----None-----	
<input type="checkbox"/> HTTP		-----None-----	
<input type="checkbox"/> Email		-----None-----	

- **Create folders by date, time, and hour automatically:** If you check this item, the system will generate folders automatically by date.
- **View:** Click this button to open a file list window. This function is only available when a Networked Storage is applied.

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

The screenshot shows a file list window with a list of directories. Each directory name is a date in YYYYMMDD format, preceded by a checkbox and a right-pointing arrow. Below the list are two buttons: "Delete" and "Delete all".

<input type="checkbox"/>	→	20111120	The format is: YYYYMMDD Click to open the directory
<input type="checkbox"/>	→	20111121	
<input type="checkbox"/>	→	20111122	

Click to delete selected items →        → Click to delete all recorded data

Click [20111120](#) to open the directory:

**The format is: HH (24r)**

Click to open the file list for that hour

< [07](#) [08](#) [09](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) >

	file name	size	date	time
<input type="checkbox"/>	<a href="#">Recording1 58.mp4</a>	2526004	2011/11/20	07:58:28
<input type="checkbox"/>	<a href="#">Recording1 59.mp4</a>	2563536	2011/11/20	07:59:28

Click to delete selected items

Click to go back to the previous level of the directory

Click to delete all recorded data

< [07](#) [08](#) [09](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) >

	file name	size	date	time
<input type="checkbox"/>	<a href="#">Recording1 58.mp4</a>	2526004	2011/11/20	07:58:28
<input type="checkbox"/>	<a href="#">Recording1 59.mp4</a>	2563536	2011/11/20	07:59:28

**The format is: File name prefix + Minute (mm)**

You can set up the file name prefix on Media Settings page. Please refer to page 95 for detailed information.

## Recording Advanced Mode

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

### Recording Settings

Recording Settings

Note: Before setup recording, you have to setup network storage first via [Server](#) page

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Add</span> <span>▼</span> <span>Delete</span> </div>											



#### NOTE:

► Before setting up this page, please set up the Network Storage on the Server Settings (Add Server) page first.

### Network Storage Setting

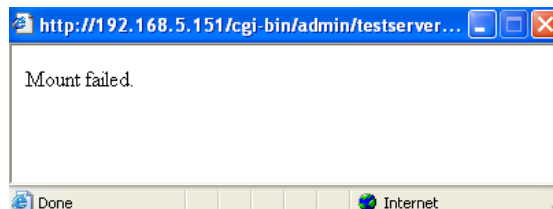
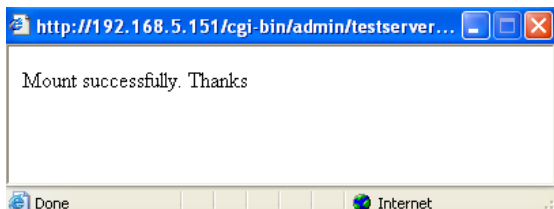
Click [Server](#) on the message bar to open the Server Settings page (if you have not) and follow the steps below to set up:

1. Fill in the information for your server.

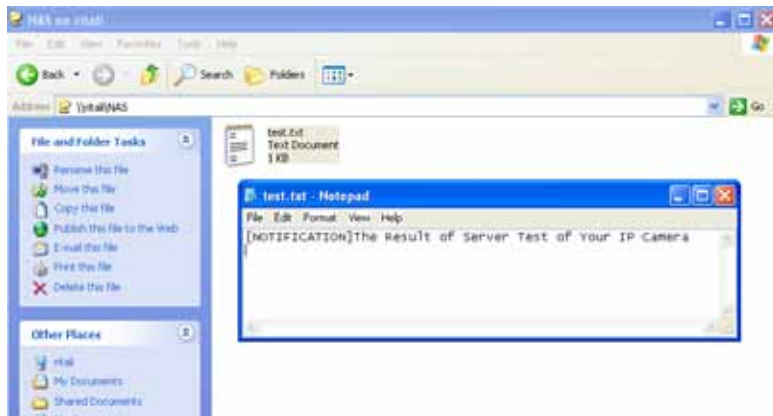
For example:

The screenshot shows the 'Server Settings' page. The 'Server name' field contains 'NAS'. Under the 'Server Type' section, 'Network storage' is selected. The 'Network storage location' field contains '\192.168.5.122\nas'. Below this, there are fields for 'Workgroup' (vivotek), 'User name' (ritali), and 'Password' (masked with dots). At the bottom, there are 'Test', 'Save', and 'Close' buttons. Annotations with numbers 1, 2, 3, and 4 point to the 'Network storage' section, the 'Test' button, the 'Server name' field, and the 'Save' button respectively. A note points to the 'Network storage location' field with the text 'Network storage path (\\server name or IP address\folder name)'. Another note points to the 'User name' and 'Password' fields with the text 'User name and password for your server'.

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



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



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

### Recording Settings

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

**>Recording**

Recording name:

Enable this recording

With adaptive recording

Pre-event recording:  seconds [0-9]

Post-event recording:  seconds [0-10]

Priority:

Source:

Trigger

Schedule

Recording Schedule

Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time

Always

From  to  [hh:mm]

Destination:

Capacity:

Entire free space

Reserved space:  Mbytes

File name prefix:

Enable cyclic recording

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

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

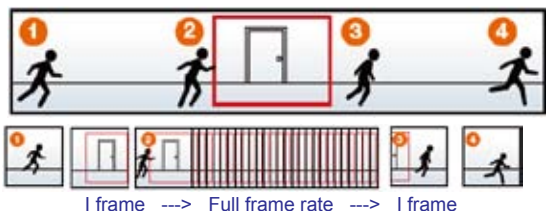
**Enable this recording:** Select this option to enable video recording.



With adaptive recording:

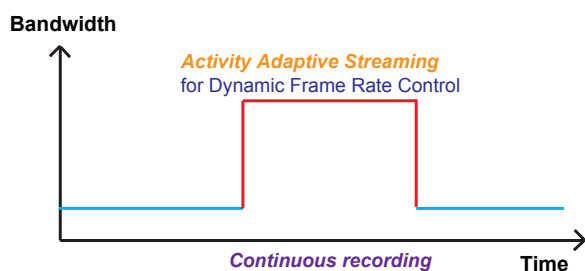
Select this option will activate the frame rate control according to alarm trigger. The frame control means that when there is a triggered alarm/event, the frame rate will raise up to the value you've set on the Stream setting page. Please refer to page 74 for more information.

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



**NOTE:**

- ▶ To enable adaptive recording, please make sure you've set up the trigger sources such as Motion Detection or Manual Trigger.
- ▶ When there is no alarm trigger:
  - JPEG mode: record 1 frame per second.
  - H.264 mode: record the I frame only.
  - MPEG-4 mode: record the I frame only.
- ▶ When the Intra frame period has been set to larger than >1s on Video settings page, the Intra frame period will be forced into 1s when the adaptive recording is activated.



The alarm trigger includes: motion detection and manual trigger, etc. Please refer to Event settings on page 87.

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

**NOTE:**

- To enable recording notification, please configure the associated Event Settings first, please refer to page 87.

**Trigger:** Select the trigger of recording action either as a planned schedule.

**Recording Schedule:**

- Select the days of the week.
- Select the recording to be **Always** recording or starting and ending between two points in time in a 24-hr format.

**Destination:** You can select the network storage to store the recorded video files.

**Capacity:** You can choose either the “entire free space” or “reserved space”. The reserved space must be larger than 15MB, and that space is important if you select the cyclic recording option. The reserved space will be a turn-around buffer during the transaction stage when a networked storage is about to be filled up and old data is to be overwritten.

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

**Enable cyclic recording:** If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for cyclic recording to prevent malfunction. This value must be larger than 15 MBytes.

If you want to enable recording notification, please click [Application](#) to set up. Please refer to **Trigger > Recording notify** on page 88 for detailed information.

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

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

**Recording Settings**

Note: Before setup recording, you have to setup network storage first via [Server](#) page

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination
<a href="#">Video</a>	<a href="#">ON</a>	V	V	V	V	V	V	V	00:00~24:00	stream1	<a href="#">NAS</a>

Add Video

- Click [Video \(Name\)](#): Opens the Recording Settings page to modify.
- Click [ON \(Status\)](#): The Status will become [OFF](#) and stop recording.
- Click [NAS \(Destination\)](#): Opens the file list of recordings as shown below. For more information about folder naming rule, please refer to page 98 for details.

[20111120](#)

[20111121](#)

[20111122](#)

The recorded video clips are playable using the VMSMediaPlayer.exe that comes with the ST-7501 recording software. When the software is installed, the media player can be found in C:\Program Files\VIVOTEK Inc\ST-7501\Client\Playback.

## System Log Advanced Mode

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

### Remote Log

**Remote Log**

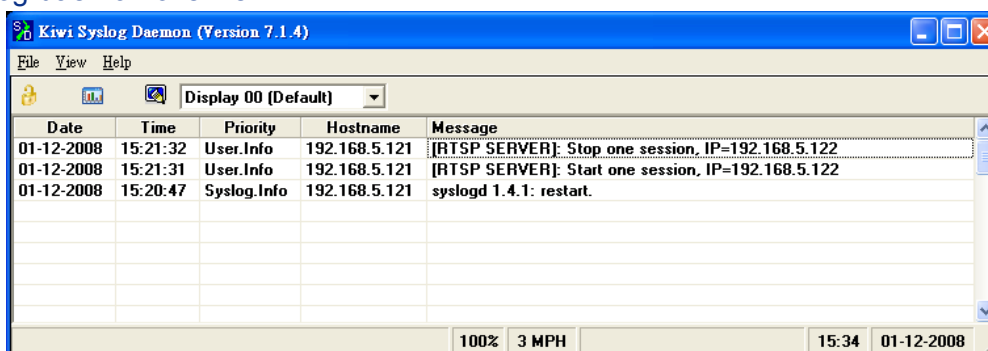
Enable remote log

Log server settings

IP address:

port:

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/>.



Follow the steps below to set up the remote log:

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

### Current Log

**Current Log**

```

Jun 30 13:46:52 syslogd 1.4.1: restart.
Jun 30 13:46:56 [DRM Service]: Starting DRM service.
Jun 30 13:47:06 [IR Cut Control]: Day mode
Jun 30 13:47:08 [IR Cut Control]: Day mode
Jun 30 13:47:09 [SYS]: Serial number = 0002D107258A
Jun 30 13:47:09 [SYS]: System starts at Mon Jun 30 13:47:09 UTC 2008
Jun 30 13:47:09 [NET]: === NET INFO ===
Jun 30 13:47:09 [NET]: Host IP = 192.168.5.151
Jun 30 13:47:09 [NET]: Subnet Mask = 255.255.255.0
Jun 30 13:47:09 [NET]: Gateway = 192.168.5.1
Jun 30 13:47:09 [NET]: Primary DNS = 192.168.0.10
Jun 30 13:47:09 [NET]: Secondary DNS = 192.168.0.20
Jun 30 13:47:10 [SYS]: Recording entry 0 stop
Jun 30 13:47:10 [SYS]: Recording entry 1 stop
Jun 30 13:47:11 [EVENT MGR]: reload config file
Jun 30 13:47:34 [Chronos]: Sync with NTP server failed!

```

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

## View Parameters Advanced Mode

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

Parameter List

```

system_hostname='Wireless Mega-Pixel Network Camera'
system_ledoff='0'
system_date='2011/12/16'
system_time='16:39:25'
system_datetime=''
system_ntp=''
system_timezoneindex='320'
system_daylight_enable='0'
system_daylight_dstactualmode='1'
system_daylight_auto_begintime='NONE'
system_daylight_auto_endtime='NONE'
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-1
system_updateinterval='0'
system_dailyreboot='07:00'
system_info_modelname='PT8133W'
system_info_extendedmodelname='PT8133W'
system_info_serialnumber='0002D11633D0'
system_info_firmwareversion='PT8133-VVTK-0100c'
system_info_language_count='9'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system_info_language_i3='Français'
system_info_language_i4='Italiano'
system_info_language_i5='日本語'
system_info_language_i6='Português'
system_info_language_i7='简体中文'
system_info_language_i8='繁體中文'
system_info_language_i9=''
system_info_language_i10=''
system_info_language_i11=''
system_info_language_i12=''
system_info_language_i13=''
system_info_language_i14=''
system_info_language_i15=''
system_info_language_i16=''
system_info_language_i17=''

```

## Maintenance

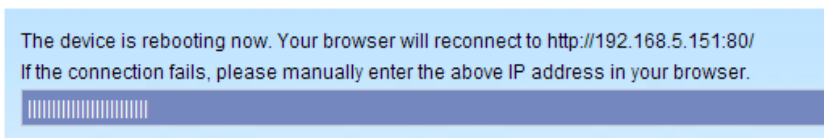
This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.

### Reboot

**Reboot**

Reboot the device

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 rebooting process.



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

### Restore

**Restore**

Restore all settings to factory default except settings in

Network Type    Daylight Saving Time    Custom language

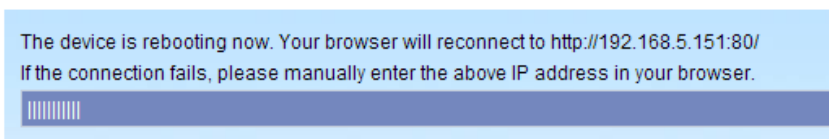
This feature allows you to restore the Network Camera to factory default settings.

**Network Type:** Select this option to retain the Network Type settings. (Please refer to Network Type on page 42.)

**Daylight Saving Time:** Select this option to retain the Daylight Saving Time settings. (Please refer to System on page 33.)

**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.



### Calibrate

**Calibrate**

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

This feature re-calibrate the home position to the default center to recover any displacement caused by external forces. Please note that there is no confirm message box after clicking on Calibrate, and the Network Camera will calibrate immediately.

## Export / Upload Files Advanced Mode

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

**Export files**

Export daylight saving time configuration file	<input type="button" value="Export"/>
Export language file	<input type="button" value="Export"/>
Export setting backup file	<input type="button" value="Export"/>

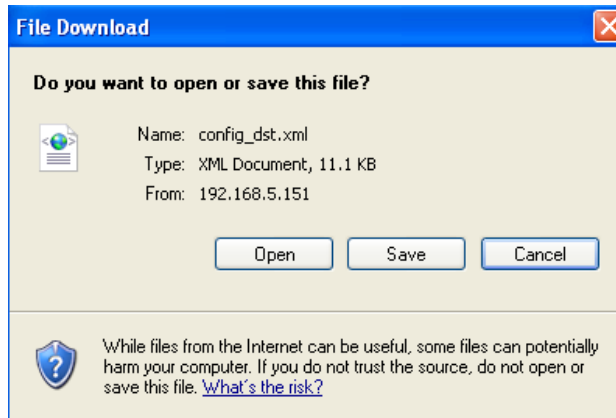
**Upload files**

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 setting backup 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.

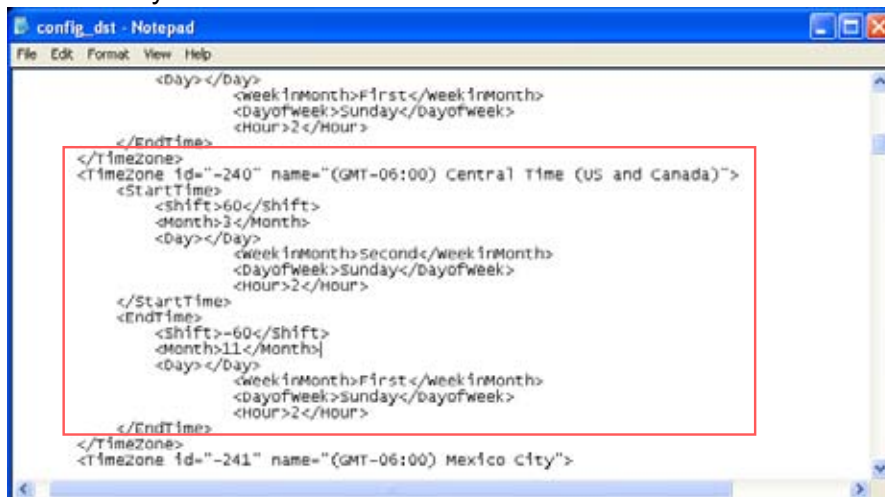
Follow the steps below to export:

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.



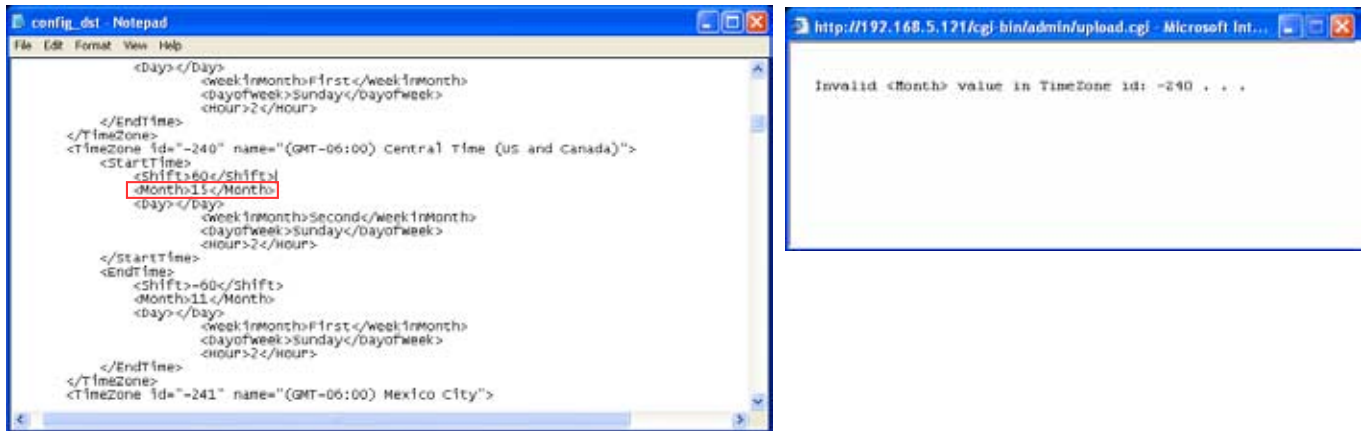
3. Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST. When completed, save the file.

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

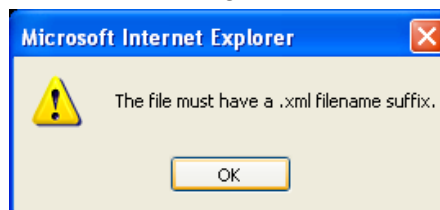


Upload daylight saving time rule: Click **Browse...** and specify the XML file to upload.

If the incorrect date and time are assigned, you will see the following warning message when uploading the file to the 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, 简体中文, and 繁體中文.

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

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

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

## Upgrade Firmware

**Upgrade firmware**

Select firmware file

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, re-access the Network Camera.



The following message is displayed when the upgrade has succeeded.

Reboot system now!!  
This connection will close.

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

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

# Appendix

## URL Commands for the Network Camera

### 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 returned as HTTP formatted, i.e., starting with the string HTTP is line separated with a Carriage Return and Line Feed (CRLF) printed as `\r\n`.

Return:

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

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

**Example:** request a single snapshot image

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

### 3. General CGI URL Syntax and Parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators.

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

Syntax:

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

**Example:** Set hostname

```
http://mywebserver/cgi-bin/admin/setparam.cgi?system\_hostname=vivotek
```

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

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

A successful control request returns parameter pairs as follows:

Return:

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

where *<parameter pair>* is

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

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

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

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

Request:

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

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Content-Length: 33\r\n

\r\n

network.ipaddress=192.168.0.123\r\n

## 6. Set Server Parameter Values

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

**Method:** GET/POST

Syntax:

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

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

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

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

PARAMETER	VALUE	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>update</b>	<boolean>	Set to 1 to update all fields (no need to update parameter in each group).
<b>return</b>	<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.  (Note: The return page can be a general HTML file (.htm, .html) or a VIVOTEK server script executable (.vsp) file. It cannot be a CGI command or have any extra parameters. This parameter must be placed at the end of the parameter list

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Content-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

## 7. Available parameters on the server

Valid values:

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

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

## 7.1 System

Group: **system**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	<product dependent >	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
ledoff	<boolean>	0	6/6	Turn on (0) or turn off (1) all led indicators.
date	<yyyy/mm/dd>, keep, auto	<current date>	6/6	Current date of system. Set to 'keep' to keep date unchanged. Set to 'auto' to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	<current time>	6/6	Current time of the system. Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	<MMDDhhmmYYYY.ss>	<current time>	6/6	Another current time format of the system.
ntp	<domain name>, <ip address>, <blank>	<blank>	6/6	NTP server. *Do not use "skip to invoke default server" for default value.
timezoneindex	-489 ~ 529	320	6/6	Indicate timezone and area. -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00

					<p>Midway Island, Samoa</p> <p>-400: GMT-10:00</p> <p>Hawaii</p> <p>-360: GMT-09:00</p> <p>Alaska</p> <p>-320: GMT-08:00 Las Vegas, San_Francisco, Vancouver</p> <p>-280: GMT-07:00</p> <p>Mountain Time, Denver</p> <p>-281: GMT-07:00</p> <p>Arizona</p> <p>-240: GMT-06:00</p> <p>Central America, Central Time, Mexico City, Saskatchewan</p> <p>-200: GMT-05:00</p> <p>Eastern Time, New York, Toronto</p> <p>-201: GMT-05:00</p> <p>Bogota, Lima, Quito, Indiana</p> <p>-180: GMT-04:30</p> <p>Caracas</p> <p>-160: GMT-04:00</p> <p>Atlantic Time, Canada, La Paz, Santiago</p> <p>-140: GMT-03:30</p> <p>Newfoundland</p> <p>-120: GMT-03:00</p> <p>Brasilia, Buenos Aires, Georgetown, Greenland</p> <p>-80: GMT-02:00</p> <p>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, Tbilisi, Yerevan</p> <p>180: GMT 04:30 Kabul</p> <p>200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent</p> <p>220: GMT 05:30</p>
--	--	--	--	---

				<p>Calcutta, Chennai, Mumbai, New Delhi</p> <p>230: GMT 05:45</p> <p>Kathmandu</p> <p>240: GMT 06:00</p> <p>Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura</p> <p>260: GMT 06:30</p> <p>Rangoon</p> <p>280: GMT 07:00</p> <p>Bangkok, Hanoi, Jakarta, Krasnoyarsk</p> <p>320: GMT 08:00</p> <p>Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei</p> <p>360: GMT 09:00</p> <p>Osaka, Sapporo, Tokyo, Seoul, Yakutsk</p> <p>380: GMT 09:30</p> <p>Adelaide, Darwin</p> <p>400: GMT 10:00</p> <p>Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok</p> <p>440: GMT 11:00</p> <p>Magadan, Solomon Is., New Caledonia</p> <p>480: GMT 12:00</p> <p>Aucklan, Wellington, Fiji, Kamchatka, Marshall Is.</p> <p>520: GMT 13:00</p> <p>Nuku'Alofa</p>
daylight_enable	<boolean>	0	6/6	Enable <b>automatic</b> daylight saving time

				in time zone.
daylight_dstactualmode	<boolean>	1	6/7	Check if current time is under daylight saving time. (Used internally)
daylight_auto_begintime	string[19]	NONE	6/7	Display the current daylight saving start time. (product dependent)
daylight_auto_endtime	string[19]	NONE	6/7	Display the current daylight saving end time. (product dependent)
daylight_timezones	string	<product dependent >	6/6	List time zone index which support daylight saving time.
updateinterval	0, 3600, 86400, 604800, 2592000	0	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.
restore	0, <positive integer>	N/A	7/6	Restore the system parameters to default values after <value> seconds.
reset	0, <positive integer>	N/A	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	<Any value>	N/A	7/6	Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other



				<p>“restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.</p>
restoreexceptdst	<Any value>	N/A	7/6	<p>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.</p>
restoreexceptlang	<Any Value>	N/A	7/6	<p>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</p>

				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]	<product depende nt>	0/7	Internal model name of the server (eg. IP7139)
extendedmodelname	string[40]	<product depende nt>	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 depende nt>	0/7	Firmware version, including model, company, and version number in the format: <MODEL-BRAND-VERSION>
language_count	<integer>	9	0/7	Number of webpage languages available on the server.
language_i<0~(count-1)>	string[16]	<product depende nt>	0/7	Available language lists.
customlanguage_maxcount	<integer>	1	0/6	Maximum number of custom languages supported on the server.
customlanguage_count	<integer>	0	0/6	Number of custom languages which have been uploaded to the server.
customlanguage_i<0~(max count-1)>	string	N/A	0/6	Custom language name.

## 7.2 Status

Group: **status**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
videoactualmodulation <product dependent>	ntsc, pal	1	4/7	The actual modulation type (videoin.type=0).
vi_i0	<boolean>	0	1/7	0 => Inactive, normal 1 => Active, triggered
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.

## 7.3 Security

Group: **security**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
privilege_camctrl	view, operator, admin	view	6/6	Indicate which privileges and above can control PTZ
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
type	lan, pppoe	lan	6/6	Network connection type.
preprocess	0~15	<blank>	6/6	Stop related process before setting port value.
resetip	<boolean>	1	6/6	1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot. 0 => Use preset ipaddress, subnet, router, dns1, and dns2.
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.

### 7.5.1 802.1x

Subgroup of **network: ieee8021x**

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)

## 7.5.2 QoS

Subgroup of **network: qos**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
cos_enable	<boolean>	0	6/6	Enable/disable CoS (IEEE 802.1p)
cos_vlanid	1~4095	1	6/6	VLAN ID
cos_video	0~7	0	6/6	Video channel for CoS
cos_audio	0~7	0	6/6	Audio channel for CoS
cos_eventalarm	0~7	0	6/6	Event/alarm channel for CoS
cos_management	0~7	0	6/6	Management channel for CoS
cos_eventtunnel	0~7	0	6/6	Event/Control channel for CoS
dscp_enable	<boolean>	0	6/6	Enable/disable DSCP
dscp_video	0~63	0	6/6	Video channel for DSCP
dscp_audio	0~63	0	6/6	Audio channel for DSCP
dscp_eventalarm	0~63	0	6/6	Event/alarm channel for DSCP
dscp_management	0~63	0	6/6	Management channel for DSCP

## 7.5.3 IPv6

Subgroup of **network: ipv6**

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.
--	--	--	--	------------------

## 7.5.4 FTP

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

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

## 7.5.5 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 video.stream.count>0)
s1_accessname	string[32]	video2.mjpg	1/6	HTTP server push access name for stream 2. (capability.protocol.spush_mjpeg =1 and video.stream.count>1)
s2_accessname	string[32]	Video3.mjpg	1/6	Http server push access name for stream 3 (capability.protocol.spush_mjpeg =1 and video.stream.count>2)
anonymousviewing	<boolean>	0	1/6	Enable anoymous streaming viewing.

## 7.5.6 HTTPS port

Subgroup of **network**: **https\_port**

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

## 7.5.7 RTSP

Subgroup of **network**: **rtsp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	554	1/6	RTSP port. (capability.protocol.rtsp=1)
anonymousviewing	<boolean>	0	1/6	Enable anonymous streaming viewing.
authmode	disable, basic, digest	disable	1/6	RTSP authentication mode. (capability.protocol.rtsp=1)
s0_accessname	string[32]	live.sdp	1/6	RTSP access name for stream1. (capability.protocol.rtsp=1 and video.stream.count>0)
s1_accessname	string[32]	live2.sdp	1/6	RTSP access name for stream2. (capability.protocol.rtsp=1 and video.stream.count>1)
s2_accessname	string[32]	live3.sdp	1/6	RTSP access name for stream3 (capability.protocol.rtsp=1 and video.stream.count>2)
s0_audiotrack	<integer>	-1	6/6	The current audio track for stream1. -1 => audio mute
s1_audiotrack	<integer>	-1	6/6	The current audio track for stream2. -1 => audio mute
s2_audiotrack	<integer>	-1	6/6	The current audio track for stream3. -1 => audio mute

## 7.6.7.1 RTSP multicast

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

(**capability.protocol.rtp.multicast=1**)

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.
ttl	1 ~ 255	15	4/4	Mutlicast time to live value.

## 7.5.8 RTP port

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

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

## 7.5.9 PPPoE

Subgroup of **network**: **pppoe**

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



## 7.7 IP Filter

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).
allow_i<0~9>_start	1.0.0.0 ~ 255.255.255.2 55	allow_0_start => 1.0.0.0  allow_<1~9>_start => <blank>	6/6	Allowed starting IPv4 address for connection.
allow_i<0~9>_end	1.0.0.0 ~ 255.255.255.2 55	allow_0_end => 255.255.255.255  allow_<1~9>_end => <blank>	6/6	Allowed ending IPv4 address for connection.
deny_i<0~9>_start	1.0.0.0 ~ 255.255.255.2 55	<blank>	6/6	Denied starting IPv4 address for connection.
deny_i<0~9>_end	1.0.0.0 ~ 255.255.255.2 55	<blank>	6/6	Denied ending IPv4 address for connection.
ipv6_allow_i<0~9>	String[44]	ipv6_allow_i0 => ::/0 ipv6_allow_i<1~9> => <blank>	6/6	Allowed IPv6 address for connection.
ipv6_deny_i<0~9>	String[44]	<blank>	6/6	Denied IPv6 address for connection.

## 7.8 Video input

### 7.8.1 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
cmosfreq	50, 60	60	4/4	CMOS frequency. (videoin.type=2) (product dependent)
whitebalance	auto, manual	auto	4/4	"auto" indicates auto white balance. "manual" indicates keep current value.
exposurelevel	1~8	4	4/4	Exposure level (product dependent)
enableblc	<boolean>	0	4/4	Enable backlight compensation.
enablewdr	<boolean>	0	4/4	Enable/disable wide dynamic range.
agc	0~2	1	4/4	Set auto gain control to normal level or MAX level.
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[16]	<blank>	1/4	Enclose caption.
imprinttimestamp	<boolean>	0	4/4	Overlay time stamp on video.
maxexposure	1~500	30	4/4	Maximum exposure time.
enablepreview	<boolean>	0	1/4	Usage for UI of exposure settings. Preview settings of video profile.
s<0~(m-1)>_codectype	mpeg4, mjpeg, h264	H264	1/4	Video codec type.
s<0~(m-1)>_resolution	176x144, 320x200 640x400 1280x720 1280x800	s0:1280x800 s1:176x144 s2:1280x800	1/4	Video resolution in pixels.
s<0~(m-1)>_mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_mpeg4_ratecontrol mode	cbr, vbr	s0,s1 :cbr s2: vbr	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". 0 is the customized manual input setting. 1 = worst quality, 5 = best

				quality, 99 = customized manual input setting, 100 = percentage mode.
s<0~(m-1)>_mpeg4_qvalue	2~31	7	4/4	Manual video quality level input. (s<0~(m-1)>_mpeg4_quant = 99)
s<0~(m-1)>_mpeg4_bitrate	1000~800000	s0,s2: 3000000 s1:4000	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)	s0,s2:30 s1:5	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	s0,s1 :cbr s2: vbr	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". 0 is the customized manual input setting. 1 = worst quality, 5 = best quality, 99 = customized manual input setting, 100 = percentage mode.
s<0~(m-1)>_h264_qvalue	0~51	30	4/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 99)
s<0~(m-1)>_h264_bitrate	1000~800000	s0,s2: 3000000 s1:4000	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_h264_maxframe	1~25, 26~30 (only	s0,s2:30 s1:5	1/4	Set maximum frame rate in fps (for MPEG-4).

	for NTSC or 60Hz CMOS)			
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 is the customized manual input setting. 1 = worst quality, 5 = best quality. 100 is percentage mode.
s<0~(m-1)>_mjpeg_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	s0,s2:30 s1:5	1/4	Set maximum frame rate in fps (for JPEG).
s<0~(m-1)>_mjpeg_qvalue	2~97	50	4/4	Manual video quality level input. (s<0~(m-1)>_mjpeg_qua nt = 99)
s<0~(m-1)>_forcei	1	<blank>	7/6	Force I frame.

## 7.8.2 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)>** (product dependent)

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.
exposurelevel	1~8	4	4/4	Exposure level
maxexposure	1~500	5	4/4	Maximum exposure time.
agc	0~2	2	4/4	Auto gain control
enableblc	<boolean>	0	4/4	Enable backlight compensation.
enablewdr	<boolean>	0	4/4	Enable/disable wide dynamic range.

## 7.9 video input preview

The temporary settings for video preview

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
maxexposure	1~500	30	4/4	Maximum exposure time
exposurelevel	1~8	4	4/4	Preview of exposure level (product dependent)
enableblc	<boolean>	0	4/4	Enable backlight compensation.
agc	0~2	1	4/4	Preview of set auto gain control to normal level or MAX level. 0->normal, 1->max
enablewdr	<boolean>	0	4/4	Enable/disable wide dynamic range.

## 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	linein, micin	micin	4/4	micin => use built-in microphone input. linein => use external microphone input.
mute	<boolean>	1	4/4	Enable audio mute.
gain	9~108	60	4/4	Gain of line input.
boostmic	9~108	69	4/4	Gain of mic input.
s<0~(m-1)>_codectype	gamr,g711	gamr	4/4	Set audio codec type for input.
s<0~(m-1)>_gamr_bitrate	4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200	12200	4/4	Set AMR bitrate in bps.
s<0~(m-1)>_g711_mode	pcmu, pcma	pcmu	4/4	Set G.711 mode.

## 7.11 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	0	4/4	Adjust saturation of image according to mode settings.
contrast	-5 ~ 5	0	4/4	Adjust contrast of image according to mode settings.
sharpness	-5 ~ 5	0	4/4	Adjust sharpness of image

				according to mode settings.
--	--	--	--	-----------------------------

## 7.12 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	0	4/4	Preview of saturation adjustment of image according to mode settings.
contrast	-5 ~ 5	0	4/4	Preview of contrast adjustment of image according to mode settings.
sharpness	-5 ~ 5	0	4/4	Preview of sharpness adjustment of image according to mode settings.

Group: **imagepreview**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
videoin_whitebalance	auto, manual	auto	4/4	Preview of adjusting white balance of image according to mode settings
videoin_restoreatwb	0, 1~	0	4/4	Restore of adjusting white balance of image according to mode settings



## 7.13 Motion detection settings

Group: **motion\_c<0~(n-1)>** for m profile and 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[14]	<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.

profile_i<0~(m-1)>_enable	<boolean>	0	4/4	Enable profile 1 ~ (m-1).
profile_i<0~(m-1)>_policy	schedule	schedule	4/4	The mode which the profile is applied to.
profile_i<0~(m-1)>_begintime	hh:mm	18:00	4/4	Begin time of schedule

				mode.
profile_i<0~(m-1)>_endtime	hh:mm	06:00	4/4	End time of schedule mode.
profile_i<0~(m-1)>_win_i<0~2>_enable	<boolean>	0	4/4	Enable motion window.
profile_i<0~(m-1)>_win_i<0~2>_name	string[14]	<blank>	4/4	Name of motion window.
profile_i<0~(m-1)>_win_i<0~2>_left	0 ~ 320	0	4/4	Left coordinate of window position.
profile_i<0~(m-1)>_win_i<0~2>_top	0 ~ 240	0	4/4	Top coordinate of window position.
profile_i<0~(m-1)>_win_i<0~2>_width	0 ~ 320	0	4/4	Width of motion detection window.
profile_i<0~(m-1)>_win_i<0~2>_height	0 ~ 240	0	4/4	Height of motion detection window.
profile_i<0~(m-1)>_win_i<0~2>_objsize	0 ~ 100	0	4/4	Percent of motion detection window.
profile_i<0~(m-1)>_win_i<0~2>_sensitivity <product dependent>	0 ~ 100	0	4/4	Sensitivity of motion detection window.

## 7.14 DDNS

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the dynamic DNS.
provider	Safe100, DyndnsDynamic, DyndnsCustom, TZO, DHS,	DyndnsD ynamic	6/6	Safe100 => safe100.net DyndnsDynamic => dyndns.org (dynamic) DyndnsCustom => dyndns.org (custom)

	DynInterfree, CustomSafe100			TZO => tzo.com DHS => dhs.org DynInterfree =>dyn-interfree.it CustomSafe100 => Custom server using safe100 method
<provider>_hostname	string[128]	<blank>	6/6	Your dynamic hostname.
<provider>_usernameemail	string[64]	<blank>	6/6	Your user or email to login to the DDNS service provider
<provider>_passwordkey	string[64]	<blank>	6/6	Your password or key to login to the DDNS service provider.
<provider>_servername	string[128]	<blank>	6/6	The server name for safe100. (This field only exists if the provider is customsaf100)

## 7.15 UPnP presentation

Group: **upnppresentation**

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

## 7.16 UPnP port forwarding

Group: **upnpportforwarding**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the UPNP port forwarding service.
upnppnatstatus	0~3	0	6/7	The status of UpnP port forwarding, used internally. 0 = OK, 1 = FAIL, 2 = no IGD router, 3 = no need for port forwarding

## 7.17 System log

Group: **syslog**

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

## 7.18 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
autospeed	-5 ~ 5	1	1/4	Auto pan speed
dwelling	0 ~ 9999	0	1/4	Dwelling time during patrol
defaulthome	<boolean>	1	1/4	This field tells system to use default home position or not.
axisx	1 ~ 20800	0	1/4	Axis X coordinate, used internally.
axisy	0 ~ 6400	0	1/4	Axis Y coordinate, used internally.
axisz	0 ~ 16384	0	1/4	Axis Z coordinate, used internally.
pantilt_port	<integer>	<blank>	1/4	Pan and tilt channel.
pantilt_camid	0 ~ 255	<blank>	1/4	ID of camera on pan/tilt channel.
returnhome	<boolean>	0	1/4	Enable/disable auto return home while idle
returnhomeinterval	<integer>	5	1/4	Wait interval return home
preset_i<0~(npreset-1)>_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

## 7.19 SNMP

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
v2	<boolean>	0	6/6	SNMP v2 enabled. 0 for disable, 1 for enable
v3	<boolean>	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 passwrd
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
syslocation	string[128]	<blank>	6/6	Description of Camera location (Ex. Address)
syscontact	string[128]	<blank>	6/6	Description of Camera contactor (Ex. E-mail)

## 7.20 Layout configuration

Group: **layout**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
logo_default	<boolean>	1	1/6	0 => Custom logo 1 => Default logo
logo_link	string[40]	<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]	#ffffff	1/6	Font color
theme_color_configfont	string[7]	#ffffff	1/6	Font color of configuration area.
theme_color_titlefont	string[7]	#098bd6	1/6	Font color of video title.
theme_color_controlbackground	string[7]	#565656	1/6	Background color of control area.
theme_color_configbackground	string[7]	#323232	1/6	Background color of configuration area.
theme_color_videobackground	string[7]	#565656	1/6	Background color of video area.
theme_color_case	string[7]	#323232	1/6	Frame color
custombutton_manualtrigger_s how	<boolean>	1	1/6	Show or hide manual trigger (VI) button in homepage 0 -> Hidden 1 -> Visible

## 7.21 Privacy mask

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

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

## 7.22 Capability

Group: **capability**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
api_httpversion	<string>	0100a	0/7	The HTTP API version.
bootuptime	<positive integer>	60	0/7	Server bootup time.
nvi	0, <positive integer>	1	0/7	Number of digital inputs.
naudioin	0, <positive integer>	1	0/7	Number of audio inputs.
nvideoin	<positive integer>	1	0/7	Number of video inputs.
nmediastream	<positive integer>	3	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>	1	0/7	Number of UART interfaces.
nvideoinprofile	<positive integer>	0	0/7	Number of videoin profiles.
nmotionprofile	<positive integer>	1	0/7	Number of motion profiles.
ptzenabled	<positive integer>	15	0/7	<p>An 32-bit integer, each bit 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;</p>

				0(bit 1 ~ 7 are valid), 1(bit 1 ~ 7 are invalid) Bit 9 => Reserved bit; Invalidate lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris. 0(fields are valid), 1(fields are invalid)
npreset	<positive integer>	20	0/7	Number of preset locations.
ptzenabledclient	<boolean>	0	0/7	Indicate whether to support ptz client
protocol_https	< boolean >	1	0/7	Indicate whether to support HTTP over SSL.
protocol_rtsp	< boolean >	1	0/7	Indicate whether to support RTSP.
protocol_maxconnection	<positive integer>	10	0/7	The maximum allowed simultaneous connections.
protocol_maxgenconnection	<positive integer>	10	0/7	The maximum general streaming connections .
protocol_maxmegaconnection	<positive integer>	0	0/7	The maximum megapixel streaming connections.
protocol_rtp_multicast_ scalable	<boolean>	1	0/7	Indicate whether to support scalable multicast.
protocol_rtp_multicast_ backchannel	<boolean>	0	0/7	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	1	0/7	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	1	0/7	Indicate whether to support RTP over HTTP.
protocol_spush_mjpeg	<boolean>	1	0/7	Indicate whether to support server push MJPEG.
protocol_snmp	<boolean>	1	0/7	Indicate whether to support SNMP.
protocol_ipv6	<boolean>	1	0/7	Indicate whether to support IPv6.
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>	176x144, 320x200, 640x400, 1280x800	0/7	Available resolutions list.
videoin_maxframerate	<a list of available maximum frame rate separated by commas>	30,30,30,30	0/7	Available maximum frame list.
videoin_codec	<a list of available codec types separated by commas>	Mpeg4, mjpeg, h264	0/7	Available codec list.
audio_aec	<boolean>	0	0/7	Indicate whether to support acoustic echo cancellation.
audio_extmic	<boolean>	0	0/7	Indicate whether to support external microphone input.
audio_linein	<boolean>	0	0/7	Indicate whether to support external line input.
audio_lineout	<boolean>	0	0/7	Indicate whether to support line output.
audio_headphoneout	<boolean>	0	0/7	Indicate whether to support headphone output.
audioin_codec	<a list of the available codec types separated by	gamr, g711	0/7	Available codec list.

	commas)			
uart_httptunnel	<boolean>	0	0/7	Indicate whether to support HTTP tunnel for UART transfer.
camctrl_httptunnel	<boolean>	0	0/7	Indicate whether to support httptunnel.
camctrl_httptunnelclient	<boolean>	0	0/7	Indicate whether to support httptunnel client.
camctrl_privilege	<boolean>	1	0/7	Indicate whether to support "Manage Privilege" of PTZ control in the Security page.
transmission_mode	Tx, Rx, Both	Tx	0/7	Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both = DVR.
network_wire	<boolean>	1	0/7	Indicate whether to support Ethernet.
network_wireless	<boolean>	<product dependent >	0/7	Indicate whether to support wireless.
wireless_s802dot11b	<boolean>	<product dependent >	0/7	Indicate whether to support wireless 802.11b+.
wireless_s802dot11g	<boolean>	<product dependent >	0/7	Indicate whether to support wireless 802.11g.
wireless_s802dot11n	<boolean>	<product dependent >	0/7	Indicate whether to support wireless 802.11g.
wireless_beginchannel	1 ~ 14	1	0/7	Indicate the begin channel of wireless network
wireless_endchannel	1 ~ 14	13	0/7	Indicate the end channel of wireless network
wireless_encrypt_wep	<boolean>	<product dependent >	0/7	Indicate whether to support wireless WEP.
wireless_encrypt_wpa	<boolean>	<product dependent >	0/7	Indicate whether to support wireless WPA.

		>		
wireless_encrypt_wpa2	<boolean>	<product dependent >	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>	1	0/7	Indicate whether to support joystick control.
nanystream	<positive integer>	0	0/7	number of any media stream per channel
iva	<boolean>	0	0/7	Indicate whether to support Intelligent Video analysis
test_ac	<boolean>	1	0/7	Indicate whether to support test ac key.
version_onvifdaemon	<string>	1.6.0.8	0/7	Indicate ONVIF daemon version

## 7.23 Customized event script

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

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	<blank>	6/6	Custom script identification of this entry.
date	string[20]	<blank>	6/6	Date of custom script.
time	string[20]	<blank>	6/6	Time of custom script.

## 7.24 Event setting

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

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	<blank>	6/6	Identification of this entry.
enable	<boolean>	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	10	6/6	Delay in seconds before detecting the next event.
trigger	boot, di, motion, seq, reconfirm, vi	boot	6/6	Indicate the trigger condition: "boot" = System boot "di" = Digital input "motion" = Video motion detection "seq" = Periodic condition "reconfirm" = Recording notification. "vi" = Virtual input (Manual trigger)
triggerstatus	String[40]	trigger	6/6	The status for event trigger
mdwin	<integer>	0	6/6	Indicate which motion detection windows detect. This field is required when trigger condition is "md". One bit represents one window. The LSB indicates the 1 <sup>st</sup> window. For example, to detect the 1 <sup>st</sup> and 3 <sup>rd</sup> windows, set mdwin as 5.
mdwin0	<integer>	0	6/6	Similar to mdwin. The parameter takes effect when profile 1 of motion detection is enabled.
vi	<boolean>	0	6/6	Indicate whether to detect virtual input.
inter	1~999	1	6/6	Interval of snapshots in minutes. This field is used when trigger condition is "seq".

weekday	0~127	127	6/6	<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	Begin time of the weekly schedule.
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>
action_server_i<0~4>_enable	<boolean>	0	6/6	<p>Enable or disable this server action.</p> <p>The default value is 0.</p>
action_server_i<0~4>_media	NULL, 0~4	<blank>	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.
action_goto_enable	<boolean>	0	6/6	Enable/disable ptz goto preset on event triggered.
action_goto_name	string[40]	<blank>	6/6	Preset name that ptz goto on event triggered.

## 7.25 Server setting for event action

Group: **server\_i<0~4>**

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	<blank>	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]	<blank>	6/6	Username to log in to the server.
http_passwd	string[64]	<blank>	6/6	Password of the user.
ftp_address	string[128]	<blank>	6/6	FTP server address.
ftp_username	string[64]	<blank>	6/6	Username to log in to the server.
ftp_passwd	string[64]	<blank>	6/6	Password of the user.
ftp_port	0~65535	21	6/6	Port to connect to the server.
ftp_location	string[128]	<blank>	6/6	Location to upload or store the media.
ftp_passive	<boolean>	1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode
email_address	string[128]	<blank>	6/6	Email server address.
email_sslmode	<boolean>	0	6/6	Enable support SSL.
email_port	0~65535	25	6/6	Port to connect to the server.
email_username	string[64]	<blank>	6/6	Username to log in to the server.
email_passwd	string[64]	<blank>	6/6	Password of the user.
email_senderemail	string[128]	<blank>	6/6	Email address of the sender.
email_recipientemail	string[128]	<blank>	6/6	Email address of the recipient.
ns_location	string[128]	<blank>	6/6	Location to upload or store the media.
ns_username	string[64]	<blank>	6/6	Username to log in to the server.



ns_passwd	string[64]	<blank>	6/6	Password of the user.
ns_workgroup	string[64]	<blank>	6/6	Workgroup for network storage.

## 7.26 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]	<blank>	6/6	Identification of this entry
type	snapshot, systemlog, videoclip	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]	<product dependent>	6/6	Indicate the prefix of the filename.
snapshot_datesuffix	<boolean>	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]	<product dependent>	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 ~ 10	5	6/6	Maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 1500	500	6/6	Maximum size of one video clip file in Kbytes.

## 7.27 Recording

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

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	<blank>	6/6	Identification of this entry.
trigger	schedule	schedule	6/6	Trigger type of this entry.
enable	<boolean>	0	6/6	Enable or disable this recording.
priority	0, 1, 2	1	6/6	Indicate the priority of this recording: "0" indicates low priority. "1" indicates normal priority. "2" indicates high priority.
source	0~2	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and so on.
limitsize	<boolean>	0	6/6	0: Entire free space mechanism 1: Limit recording size mechanism
cyclic	<boolean>	0	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	<boolean>	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.  bit1 = server_i1.  bit2 = server_i2.  bit3 = server_i3.  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  bit1 = Friday  bit2 = Thursday  bit3 = Wednesday  bit4 = Tuesday  bit5 = Monday  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]	<product dependent>	6/6	Indicate the prefix of the filename.
cyclesize	200~	100	6/6	The maximum size for cycle recording in Kbytes when choosing to limit recording size.
reserveamount	0~	100	6/6	The reserved amount in Mbytes when choosing cyclic recording mechanism.

dest	cf, 0~4	cf	6/6	The destination to store the recorded data. "cf" means CF card. "0~4" means the index of the network storage.
cffolder	string[128]	<blank>	6/6	Folder name.
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)

## 7.28 HTTPS

Group: **https** (product dependent)

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	6/6	Specify the https status. -3 = Certificate not installed -2 = Invalid public key -1 = Waiting for certificate 0 = Not installed 1 = Active

countryname	string[2]	<product dependent>	6/6	Country name in the certificate information.
stateorprovincename	string[128]	<product dependent>	6/6	State or province name in the certificate information.
localityname	string[128]	<product dependent>	6/6	The locality name in the certificate information.
organizationname	string[64]	<product dependent>	6/6	Organization name in the certificate information.
unit	string[32]	<product dependent>	6/6	Organizational unit name in the certificate information.
commonname	string[64]	<product dependent>	6/6	Common name in the certificate information.
validdays	0 ~ 3650	<product dependent>	6/6	Valid period for the certification.

## 7.29 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	<coordinate>	0,0 0,0	1/6	ROI left-top corner coordinate.
s<0~(m-1)>_size	<window size>	1280x800 1280x800	1/6	ROI width and height. The width value must be multiples of 16 and the height value must be multiples of 8

## 7.30 Wireless setting

Group: **wireless** ([capability.network.wireless > 0](#))

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
ssid	string[32]	default	6/6	SSID for wireless lan settings. The valid characters are [A-Z] [a-z] [0-9] [/] [.] [_] [=] [ ] [-] [+] [*].
wlmode	Infra, Adhoc	Infra	6/6	Wireless mode. Infra: Infrastructure
channel	1~11 or 1 ~ 13 or 10~11 or 10~13 or 1~14	6	6/6	USA and Canada Europe Spain France All
txrate	NONE, 1M, 2M, 5.5M, 11M, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M, Auto	Auto	6/6	Maximum transmit rate in Mbps.
encrypt	0~3	NONE	6/6	Encryption method: 0=> NONE, 1 => WEP, 2 => WPA, 3 => WPA2PSK <product dependent>
authmode	OPEN, SHARED	OPEN	6/6	Authentication mode.
keylength	64, 128	64	6/6	Key length in bits.
keyformat	HEX, ASCII	HEX	6/6	Key1 ~ key4 presentation format.
keyselect	1 ~ 4	1	6/6	Default key number.
key1	password [32]	0000000000	6/6	WEP key1 for encryption. The valid characters are [A-Z] [a-z] [0-9].
key2	password [32]	0000000000	6/6	WEP key2 for encryption. The valid characters are [A-Z] [a-z] [0-9].
key3	password [32]	0000000000	6/6	WEP key3 for encryption.

				The valid characters are [A-Z] [a-z] [0-9].
key4	password [32]	0000000000	6/6	WEP key4 for encryption. The valid characters are [A-Z] [a-z] [0-9].
domain	'U' for USA 'C' for Canada 'E' for Euro 'S' for Spain 'F' for France 'I' for Isrel 'A' for All	U	6/7	Wireless domain.
algorithm	AES, TKIP	TKIP	6/6	Algorithm
presharedkey	password [63]	00000000	6/6	WPA mode pre-shared key. The valid characters are [A-Z] [a-z] [0-9].
connecttype	manual,wps	manual	6/6	WiFi connect method

## 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
<b>channel</b>	0~(n-1)	0	The channel number of the video source.
<b>resolution</b>	<available resolution>	0	The resolution of the image.
<b>quality</b>	1~5	3	The quality of the image.
<b>streamid</b> <product dependent>	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\n
Content-Type: text/plain\r\n
Content-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/viewer/camctrl.cgi?[channel=<value>][&camid=<value>]
[&move=<value>] - Move home, up, down, left, right
[&auto=<value>] - Auto pan, patrol
[&vx=<value>&vy=<value>&vs=<value>] - Shift without stopping, used for joystick
[&x=<value>&y=<value>&videosize=<value>&resolution=<value>&stretch=<value>] - Click on image
(Move the center of image to the coordination (x,y) based on resolution or videosize.)
[ [&speedpan=<value>][&speedtilt=<value>][&speedapp=<value>][&speedlink=<value>] ] - Set speeds
[&return=<return page>]
```

Example:

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

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
camid	0,<positive integer>	Camera ID.
move	home	Move to camera to home position.
	up	Move camera up.
	down	Move camera down.
	left	Move camera left.
	right	Move camera right.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedapp	-5 ~ 5	Set the auto pan/patrol speed.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop camera.
vx	<integer , excluding 0>	The slope of movement = vy/vx, used for joystick control.

vy	<integer>	
vs	0 ~ 7 0 ~ 15 <SD81X1>	Set the speed of movement, "0" means stop.
x	<integer>	x-coordinate clicked by user. It will be the x-coordinate of center after movement.
y	<integer>	y-coordinate clicked by user. It will be the y-coordinate of center after movement.
videosize	<window size>	The size of plug-in (ActiveX) window in web page
resolution	<window size>	The resolution of streaming.
stretch	<boolean>	0 indicates that it uses <b>resolution</b> (streaming size) as the range of the coordinate system. 1 indicates that it uses <b>videosize</b> (plug-in size) as the range of the coordinate system.
speedlink	0 ~ 4	Issue speed link command.
gaptime	0~32768	The gaptime between two consecutive ptz commands for device. (unit: ms)
return	<return page>	Redirect to the page <return page> after the parameter is assigned. The <return page> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

## 8.6 Recall (**capability.ptzenabled**)

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

Method: GET

Syntax:

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

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

## 8.7 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 System Information

**Note:** This request requires Normal User privileges. (obsolete)

**Method:** GET/POST

Syntax:

<http://<servername>/cgi-bin/sysinfo.cgi>

Server will return the system information. In HTTP API version 2, the CapVersion will be 0200. All fields in the previous version (0100) are obsolete. Please use "getparam.cgi?capability" instead.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
Model=<model name of server>\r\n
CapVersion=0200\r\n
```

PARAMETER(supported capability version)	VALUE	DESCRIPTION
Model	system.firmwareversion	Model name of the server. Ex:IP3133-VVTK-0100a
CapVersion	<i>MMmm, MM is major version from 00 ~ 99 mm is minor version from 00 ~ 99</i>  <i>ex: 0100</i>	Capability field version.

## 8.9 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 than 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 than the [index] parameter.
start	<ip address>	The starting IP address to add or to delete.
end	<ip address>	The ending IP address to add or to delete.
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <return page> after the parameter is assigned. The <return page> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

## 8.10 UART HTTP Tunnel Channel (**capability.nuart > 0**)

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

**Method:** GET and POST

Syntax:

```
http://<servername>/cgi-bin/operator/uartchannel.cgi?[channel=<value>]
```

```
-----
```

```
GET /cgi-bin/operator/uartchannel.cgi?[channel=<value>]
```

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

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

```
pragma: no-cache
```

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

```
-----
```

```
POST /cgi-bin/operator/uartchannel.cgi
```

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

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

```
pragma : no-cache
```

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

```
content-length: 32767
```

```
expires: Sun, 9 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 a proxy server.

This channel will help to transfer the raw data of UART over the network.

Please see UART tunnel spec for detail information

PARAMETER	VALUE	DESCRIPTION
channel	0 ~ (n-1)	The channel number of UART.



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

### evctrlchannel > 0)

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

**Method:** GET and POST

Syntax:

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

```
-----
```

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

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

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

```
pragma: no-cache
```

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

```
-----
```

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

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

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

```
pragma : no-cache
```

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

```
content-length: 32767
```

```
expires: Sun, 9 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

## 8.12 Get SDP of Streams

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

**Method:** GET/POST

Syntax:

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

"m" is the stream number.

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

You can get the SDP by HTTP GET.

## 8.13 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.

## 8.14 Virtual input (**capability.nvi > 0**)

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

Method: GET






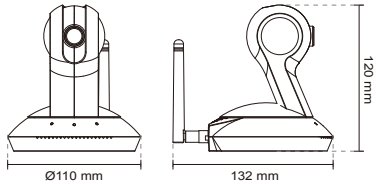
Syntax:

http://<servername>/cgi-bin/admin/setvi.cgi?vi0=<value>[&vi1=<value>][&vi2=<value>] [&return=<return page>]		
PARAMETER	VALUE	DESCRIPTION
vi<num>	state[(duration)nstate]  Where "state" is 0, 1. "0" means inactive or normal state while "1" means active or triggered state.  Where "nstate" is next state after duration.	Ex: vi0=1  Setting virtual input 0 to trigger state  Ex: vi0=0(200)1  Setting virtual input 0 to normal state, waiting 200 <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:  setvi.cgi?vi0=0(10000)1(15000)0(20000)1  No multiple duration.  setvi.cgi?vi3=0  VI index is out of range.  setvi.cgi?vi=1  No VI index is specified.
503	The resource is unavailable, ex. Virtual input is waiting for next state.  Examples:  setvi.cgi?vi0=0(15000)1 setvi.cgi?vi0=1  Request 2 will not be accepted during the execution time(15 seconds).

# Technical Specifications

## Technical Specifications

<b>Models</b> <ul style="list-style-type: none"> <li>PT8133 (PoE)</li> <li>PT8133W (WLAN)</li> </ul>	<b>Alarm and Event Management</b> <ul style="list-style-type: none"> <li>Triple-window video motion detection</li> <li>Tamper detection</li> <li>Event notification using HTTP, SMTP or FTP</li> <li>Local recording of MP4 file</li> </ul>
<b>Pan/Tilt/Zoom</b> <ul style="list-style-type: none"> <li>Pan range: 350° (-175° ~ +175°)</li> <li>Tilt range: 125° (-35° ~ +90°)</li> <li>Auto pan mode</li> <li>Auto patrol mode</li> </ul>	<b>Security</b> <ul style="list-style-type: none"> <li>Multi-level user access with password protection</li> <li>IP address filtering</li> <li>HTTPS encrypted data transmission</li> <li>802.1X port-based authentication for network protection</li> </ul>
<b>Lens</b> <ul style="list-style-type: none"> <li>Board lens, Fixed-focal, f = 3.6mm, F1.8</li> </ul>	<b>Users</b> <ul style="list-style-type: none"> <li>Live viewing for up to 10 clients</li> </ul>
<b>Field of View</b> <ul style="list-style-type: none"> <li>58.39° (horizontal)</li> <li>35.58° (vertical)</li> <li>69.34° (diagonal)</li> </ul>	<b>Weight</b> <ul style="list-style-type: none"> <li>Net: 293 g</li> </ul>
<b>Shutter Time</b> <ul style="list-style-type: none"> <li>1/5 sec. to 1/32,000 sec.</li> </ul>	<b>LED Indicator</b> <ul style="list-style-type: none"> <li>System power and status indicator</li> <li>System activity and network link indicator</li> <li>WPS indicator</li> </ul>
<b>Image Sensor</b> <ul style="list-style-type: none"> <li>1/4" CMOS sensor in 1280x800 resolution</li> </ul>	<b>Power</b> <ul style="list-style-type: none"> <li>12V DC</li> <li>Power consumption:               <ul style="list-style-type: none"> <li>Max: 5.52W (PoE)</li> <li>Max: 5.1W (Wireless)</li> </ul> </li> <li>802.3af compliant Power-over-Ethernet (Class 3)</li> </ul>
<b>Minimum Illumination</b> <ul style="list-style-type: none"> <li>0.3 Lux @ F1.8</li> </ul>	<b>Approvals</b> <ul style="list-style-type: none"> <li>CE, LVD, FCC, VCCI, C-Tick</li> </ul>
<b>Video</b> <ul style="list-style-type: none"> <li>Compression: H.264, MJPEG &amp; MPEG-4</li> <li>Streaming:               <ul style="list-style-type: none"> <li>Multiple simultaneous streams</li> <li>H.264 streaming over UDP, TCP, HTTP or HTTPS</li> <li>MPEG-4 streaming over UDP, TCP, HTTP or HTTPS</li> <li>H.264/MPEG-4 multicast streaming</li> <li>MJPEG streaming over HTTP or HTTPS</li> </ul> </li> <li>Supports activity adaptive streaming for dynamic frame rate control</li> <li>Supports 3GPP mobile surveillance</li> <li>Frame rates:               <ul style="list-style-type: none"> <li>H.264:                   <ul style="list-style-type: none"> <li>Up to 30 fps at 1280x800</li> </ul> </li> <li>MPEG-4:                   <ul style="list-style-type: none"> <li>Up to 30 fps at 1280x800</li> </ul> </li> <li>MJPEG:                   <ul style="list-style-type: none"> <li>Up to 30 fps at 1280x800</li> </ul> </li> </ul> </li> </ul>	<b>Operating Environments</b> <ul style="list-style-type: none"> <li>Temperature: 0°C ~ 50°C (32°F ~ 122°F)</li> <li>Humidity: 90% RH</li> </ul>
<b>Image Settings</b> <ul style="list-style-type: none"> <li>Adjustable image size, quality and bit rate</li> <li>Time stamp and text caption overlay</li> <li>Flip &amp; mirror</li> <li>Configurable brightness, contrast, saturation, sharpness, white balance and exposure</li> <li>AGC, AWB, AES</li> <li>BLC (Backlight Compensation)</li> <li>Supports privacy masks</li> </ul>	<b>Viewing System Requirements</b> <ul style="list-style-type: none"> <li>OS: Microsoft Windows 7/Vista/XP/2000</li> <li>Browser: Mozilla Firefox, Internet Explorer 7.x or above</li> <li>Cell phone: 3GPP player</li> <li>Real Player: 10.5 or above</li> <li>Quick Time: 6.5 or above</li> </ul>
<b>Audio</b> <ul style="list-style-type: none"> <li>Compression:               <ul style="list-style-type: none"> <li>GSM-AMR speech encoding, bit rate: 4.75 kbps to 12.2 kbps</li> <li>G.711 audio encoding, bit rate: 64 kbps, <math>\mu</math>-Law, or A-Law mode selectable</li> </ul> </li> <li>Interface:               <ul style="list-style-type: none"> <li>Built-in microphone</li> <li>Supports one-way audio</li> <li>Supports audio mute</li> </ul> </li> </ul>	<b>Installation, Management, and Maintenance</b> <ul style="list-style-type: none"> <li>Installation Wizard 2</li> <li>32-CH ST7501 recording software</li> <li>Supports firmware upgrade</li> </ul>
<b>Networking</b> <ul style="list-style-type: none"> <li>10/100 Mbps Ethernet, RJ-45</li> <li>ONVIF support</li> <li>Protocols: IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP, and 802.1X</li> </ul>	<b>Applications</b> <ul style="list-style-type: none"> <li>SDK available for application development and system integration</li> </ul>
<b>Accessories</b> <ul style="list-style-type: none"> <li>  <b>AE-101</b> Indoor camera enclosure with transparent cover (PT8133 Only)         </li> <li>  <b>AE-102</b> Indoor camera enclosure with smoke cover (PT8133 Only)         </li> <li>  <b>AE-131</b> Outdoor dome housing with transparent cover (PT8133 Only)         </li> <li>  <b>AE-132</b> Outdoor dome housing with smoked cover (PT8133 Only)         </li> <li>  <b>AM2000</b> Wall mount kit         </li> </ul>	<b>Warranty</b> <ul style="list-style-type: none"> <li>24 months</li> </ul>
	<b>Dimension</b> <ul style="list-style-type: none"> <li>Ø 110 mm x 120 mm</li> </ul> 

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

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

VIVOTEK USA, INC.  
2050 Ringwood Avenue, San Jose, CA 95131  
T: 408-773-8686 | F: 408-773-8298 | E: 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 B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

### CE Mark Warning

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

This device (PT8133/PT8133W) complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC.

This device (PT8133/PT8133W) is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device (PT8133/PT8133W) may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

### 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.

## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>