3GPP/ISMA IP7137

WIRELESS NETWORK CAMERA

User's Manual

VIVOTEK

www.vivotek.com

IP Surveillance

Product name:	Wireless Network Camera (IP7137)
Release Date:	2009/03/25
Manual Revision:	2.3
Web site:	www.vivotek.com
Email:	technical@vivotek.com
	sales@vivotek.com
Made in Taiwan.	

Before You Use This Product

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 also can be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the list in the "Package Contents" chapter. Take notice of the warnings in "Quick installation guide" before the Network Camera is installed, then carefully read and follow the instructions in the "Installation" chapter to avoid damages 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 network knowledge. The "Troubleshooting" chapter in the Appendix provides remedies to the most common errors in set up and configuration. You should consult this chapter first if you run into a system error. The Network Camera is designed for various applications including video sharing, general security/surveillance, etc. The "How to Use" chapter suggests ways to best utilize the Network Camera and ensure proper operations. For the creative and professional developers, the "URL Commands of The Network Camera" chapter serves to be a helpful reference to customize existing homepages or integrating with the current web server.

For paragraphs preceded by ⚠ the reader should use caution to understand completely the warnings. Ignoring the warnings may result in serious hazards or injuries.

Table of Contents

Package Content

IP7137

Software CD

Power adapter

Quick installation guide

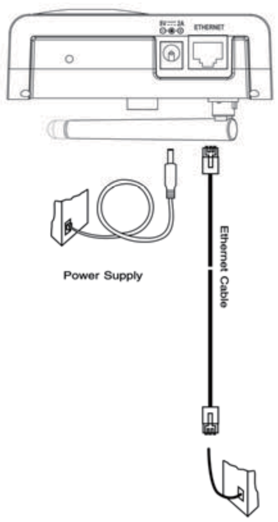
Camera stand

Warranty card

Installation

In this manual, "User" refers to whoever has access to the Network Camera, and "Administrator" refers to the person who can configure the Network Camera and grant user access to the camera.

Hardware installation



Please verify that your product package contains all the accessories listed in the foregoing Package Contents. Depending on the user's application, an Ethernet cable may be needed. The Ethernet cable should meet the specs of UTP Category 5 and not exceed 100 meters in length.

⚠ Connect the power adapter jack to the Network Camera before plugging in to the power socket. This will reduce the risk of accidental electric shock.

Upon powering up, the front blue LED will become lighted first and then the device will go through booting process. During the booting process, both blue and red LEDs will be on and the Network Camera will standby for getting IP address. After getting IP Address, the LED will blink blue every second.

The Network Camera will first detect Ethernet. If it does not connect to Ethernet, the Network Camera will try WLAN. During the searching and connecting process to the wireless access point or station, the red LED of the Network Camera will flash every second. Until the Network Camera connects to the other wireless device, the red LED will become lighted. Operating in either network mode, the blue LED will flash every second as heartbeat to indicate alive.

To install in Ethernet

Make sure the Ethernet is firmly connected to a switch hub. After attaching the Ethernet cable plug in the power adapter. If the LED turns out to be steady blue, go to next paragraph "Software installation". If the Ethernet is not available, Network Camera will switch to wireless LAN mode.

To install in wireless LAN

If the Ethernet is not available while power on, the Network Camera will search for any access point with the SSID “default”. Once any access point is found, the LED will turn blue to wait for installation. If the network environment cannot meet the default settings, install Network Camera in Ethernet to proceed with wireless LAN configuration.

Software installation

At the end of the hardware installation, users can use Installation Wizard program included in the product CDROM to find the location of the Network Camera. There may be many Network Cameras in the local network. Users can differentiate the Network Cameras with the serial number. The serial number is printed on the labels on the carton and the back of the Network Camera body. Please refer to the user’s manual of Installation Wizard for detail.

Once installation is complete, the Administrator should proceed to the next section "Initial access to the Network Camera" for necessary checks and configurations.

Initial Access to the Network Camera

Check Network Settings

The Network Camera can be connected either before or immediately after software installation onto the Local Area Network. The Administrator should complete the network settings on the configuration page, including the correct subnet mask and IP address of gateway and DNS. Ask your network administrator or Internet service provider for the detail information. By default the Network Camera requires the Administrator to run installation every time it reboots. If the network settings are to remain unchanged, disable the Install option. Refer to “Network settings” on the System Configuration page for details. If any setting is entered incorrectly and cannot proceed to setting up the Network Camera, restore the factory settings following the steps in the “Troubleshooting” chapter of the Appendix.

Add Password to prevent Unauthorized Access

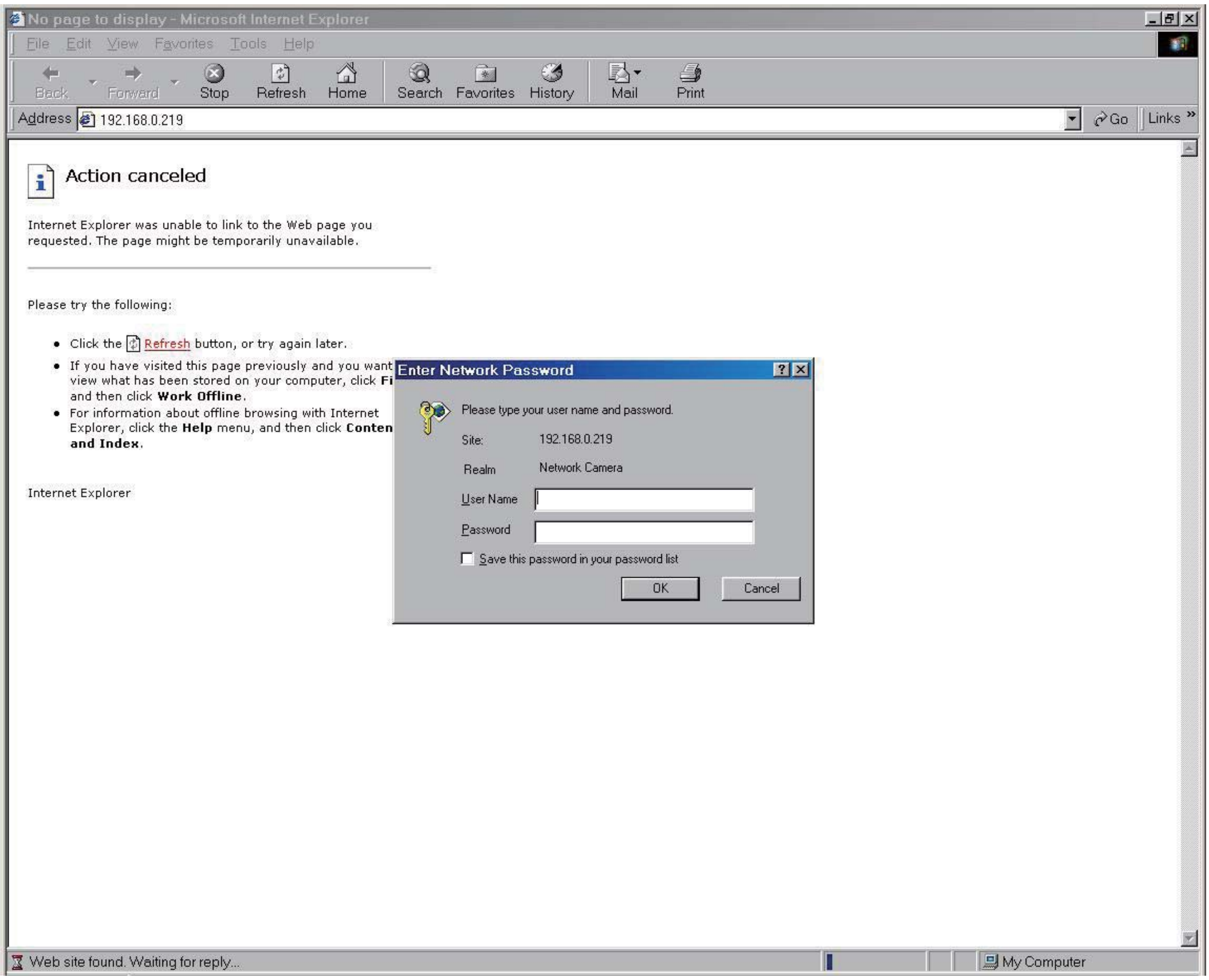
The default Administrator’s password is blank and the Network Camera initially will not ask for any password. The Administrator should immediately implement a new password as a matter of prudent security practice. Once the Administrator’s password is saved, the Network Camera will ask for the user’s name and password before each access. The Administrator can set up a maximum of twenty (20) user accounts. Each user can access the Network Camera except to perform system configuration. Some critical functions are exclusive for the Administrator, such as system configuration, user administration, and software upgrades. The user name for the Administrator is permanently assigned as “root”. Once the password is changed, the browser will display an authentication window to ask for the new password. **Once the password is set, there is no provision to recover the Administrator’s password. The only option is to restore to the original factory default settings.**

How to Use

Authentication

After opening the Web browser and typing in the URL of the Network Camera, a dialogue window pops up to request a username and password. Upon successful authentication, the following figure is displayed.

The foreground is the login window and the background shows the message if authentication fails. The user may check the option box to save the password for future convenience. This option is not available to the Administrator for obvious reason.



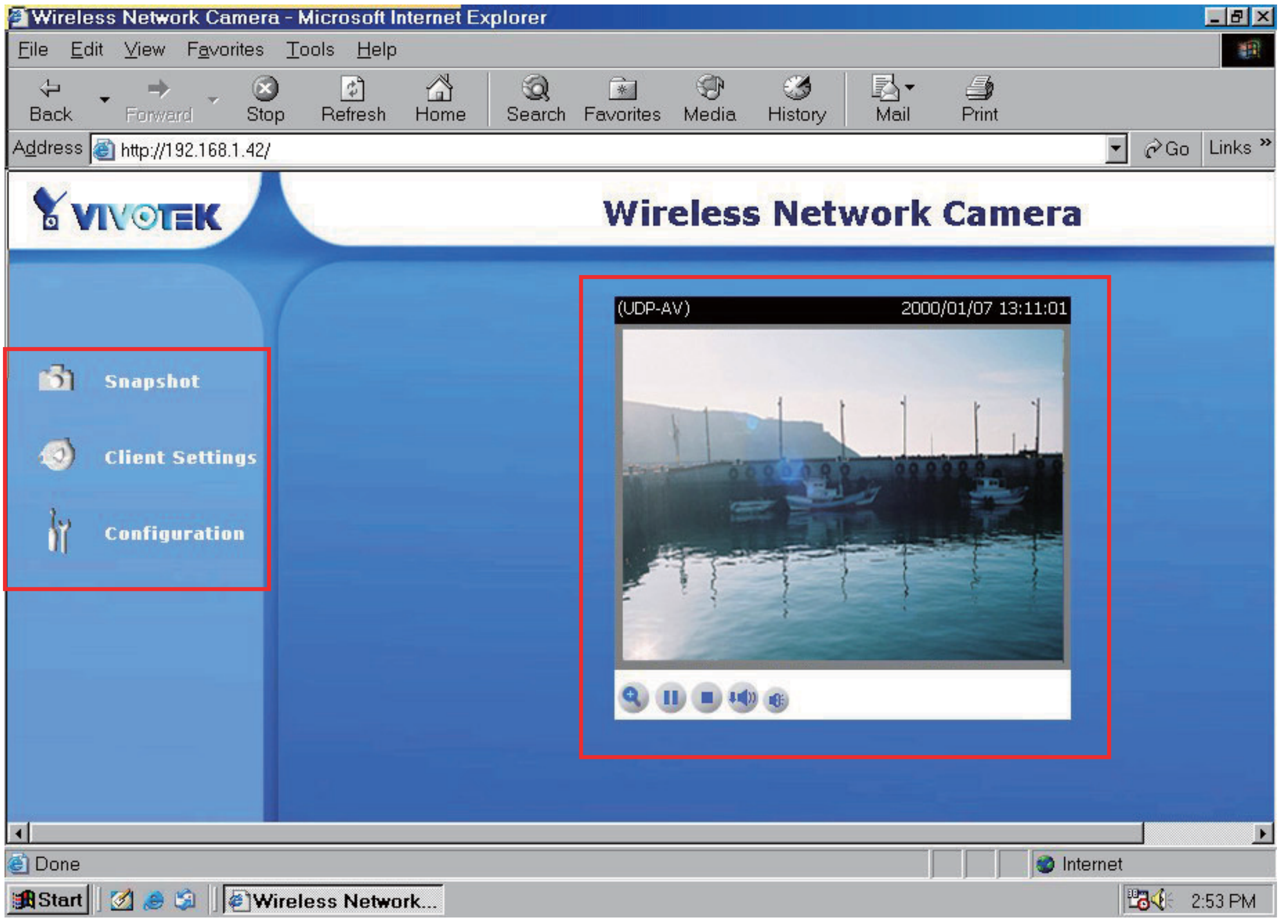
Installing plug-in

For the initial access to the Network Camera in Windows, the web browser may prompt for permission to install a new plug-in for the Network Camera. Permission request depends on the Internet security settings of the user's PC or notebook. If the highest security level is set, the computer may prohibit any installation and execution attempt. This plug-in has been registered for certificate and is used to display the video in the browser. Users may click on Yes to proceed. If the web browser does not allow the user to continue to install, check the Internet security option and lower the security levels or contact your IT or networking supervisor for help.

Primary user's capability

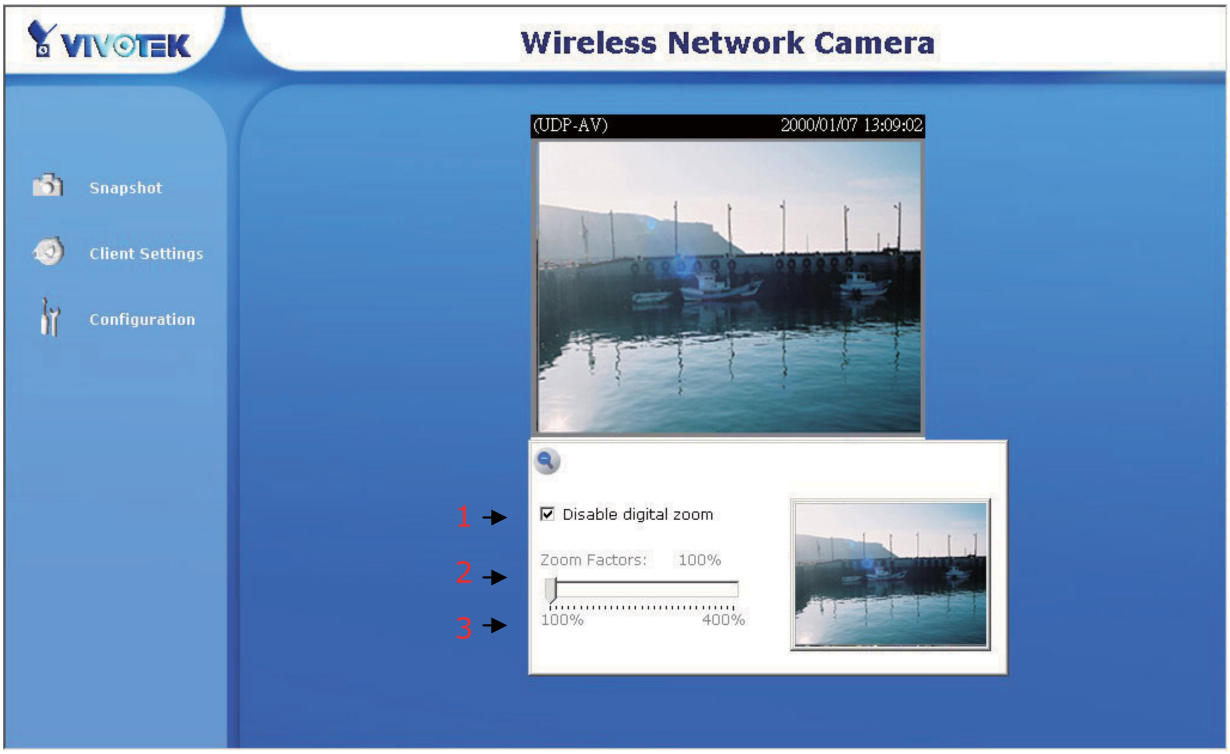
Main Screen with Camera View

The main page layout has two parts:
Configuration functions: The camera can be configured using these user interfaces.
Camera View: What the camera sees.
Click on the configuration link to the left of the image window to enter the configuration page.



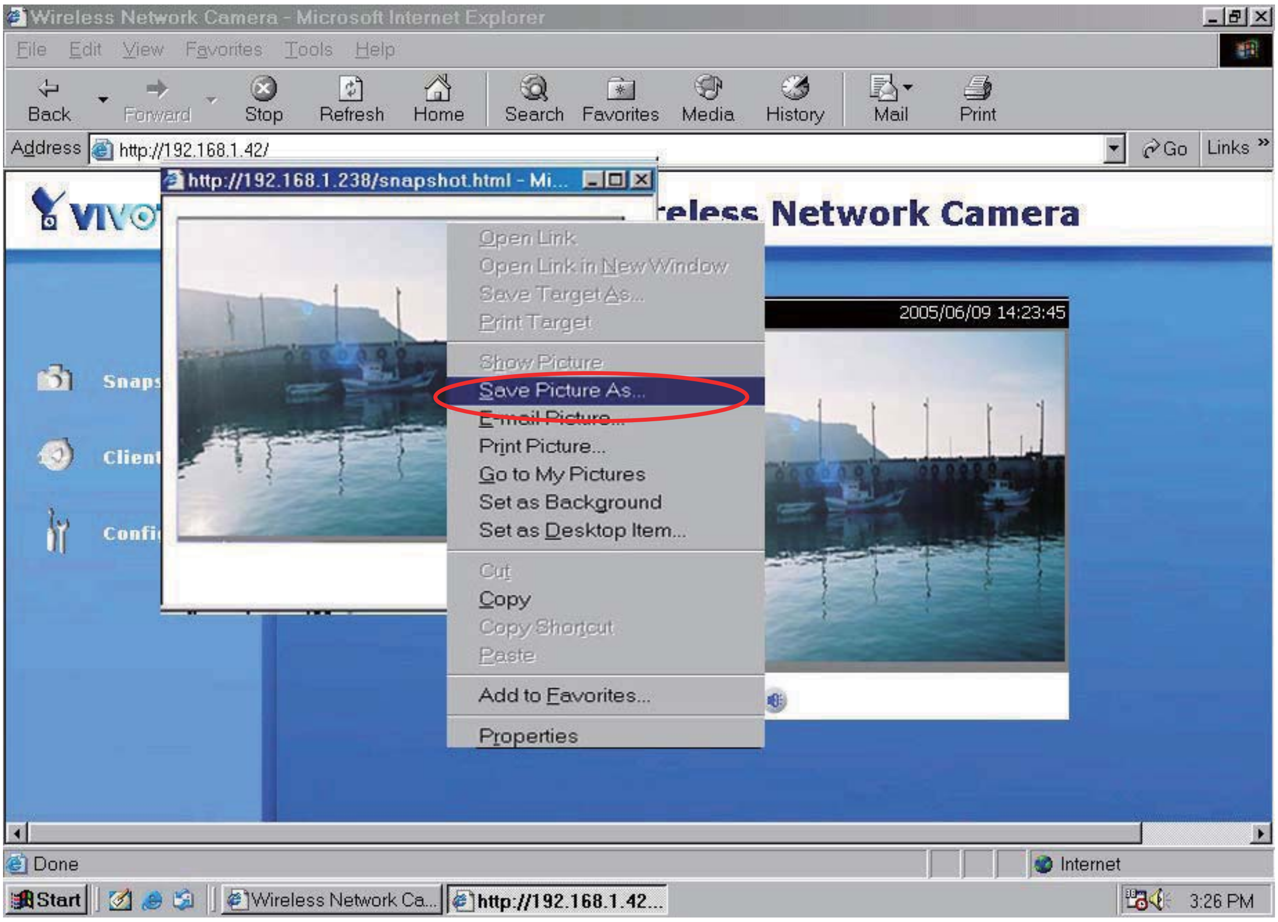
Digital Zoom

Click on the magnifier icon under the camera view then the digital zoom control panel will be shown. Uncheck “Disable digital zoom” and use the slider control to change the zoom factors.



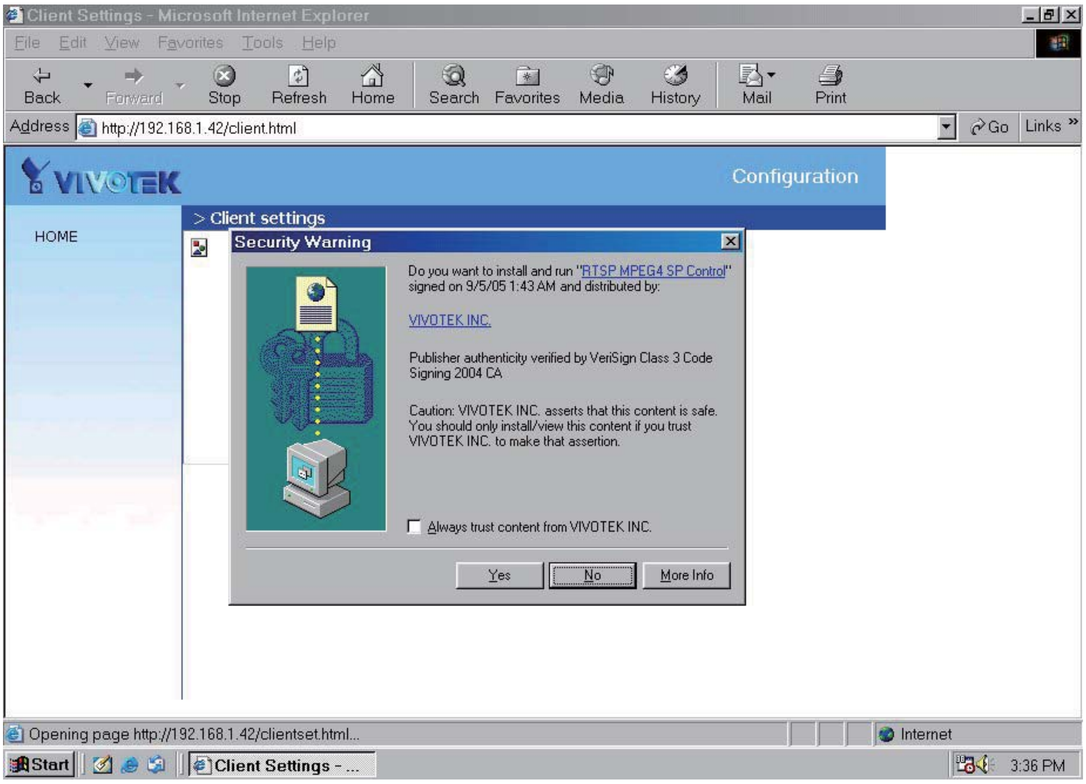
Snapshot

Click on "**Snapshot**", web browser will pop up a new window to show the snapshot. Users can point at the snapshot and click the right button of mouse to save it.



Client settings

At the initial access to the "Connection type" page in Windows, the web browser will ask for a new plug-in installation, the plug-in being the Network Camera. This plug-in has been registered for certification and can be used to change the parameters at the client's site. The user may click on Yes to install the plug-in. If the web browser does not allow the user to complete the installation, check the Internet security to lower the security level or contact your IT or networking supervisor.

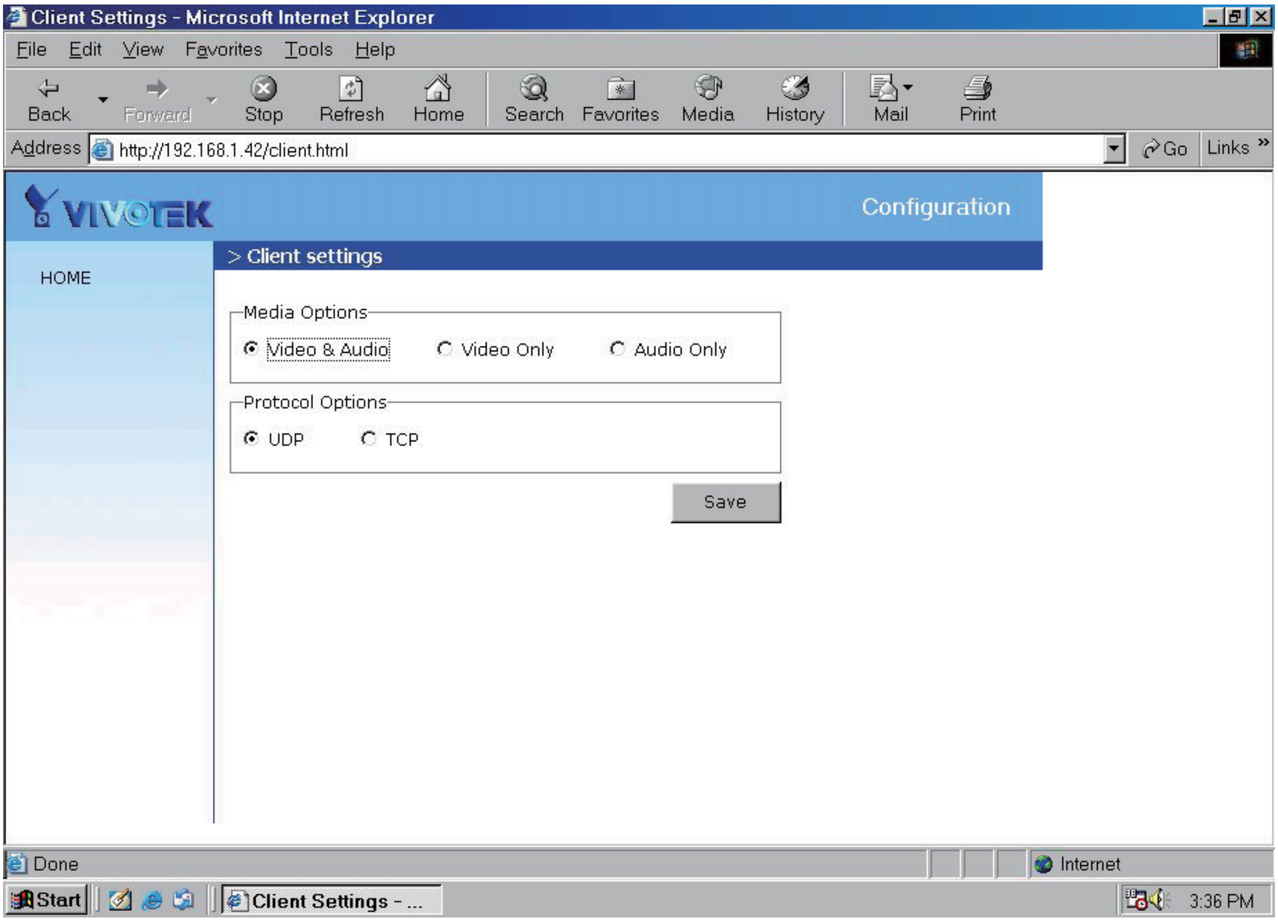


There are two settings for the client side. One is "**Media Options**" for users to determine the type of media to be streaming. The other is "**Protocol Options**" which allows choices on connection protocol between client and server. There are two protocols choices to optimize your usage – UDP and TCP.

The **UDP** protocol allows for more real-time audio and video streams. However, some packets may be lost due to network burst traffic and images may be obscured.

The **TCP** protocol allows for less packet loss and produces a more accurate video display. The downside with this protocol is that the real-time effect is worse than that with the UDP protocol.

If no special need is required, UDP protocol is recommended. Generally speaking, the client's choice will be in the order of UDP → TCP. After the Network Camera is connected successfully, "Protocol Option" will indicate the selected protocol. The selected protocol will be recorded in the user's PC and will be used for the next connection. If the network environment is changed, or the user wants to let the web browser to detect again, manually select the UDP protocol, save, and return HOME to re-connect.



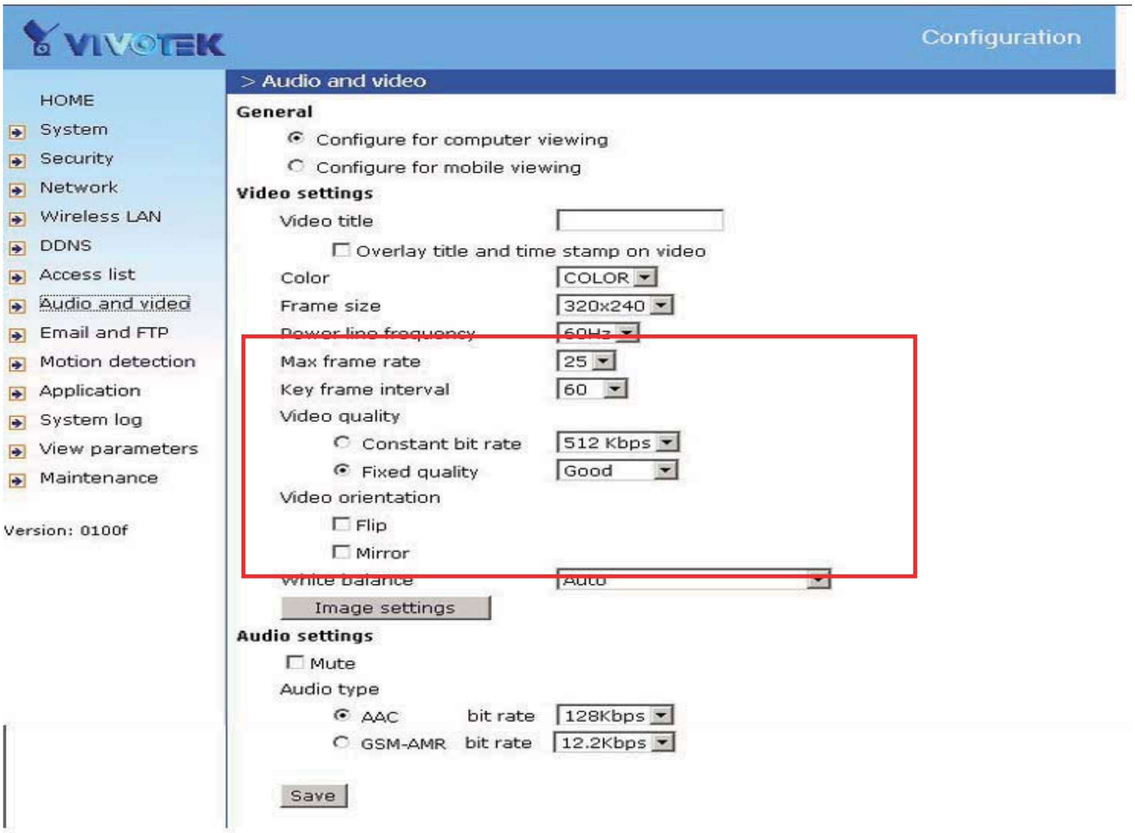
<url> *http://<Network Camera>/client.html*

<Network Camera> is the domain name or the original IP address of the Network Camera.

Administrator's capability

Fine-tuning for Best Performance

Best performance generally equates to the fastest image refresh rate with the best video quality, and at the lowest network bandwidth as possible. The three factors, "Maximum frame rate", "Constant bit rate", and "Fix quality" on the Audio and Video Configuration page, are correlative to allow for achieving the best performance possible.



For Viewing by Mobile Phone

Most 3GPP cell phone supports media streaming with MPEG4 video and GSM-AMR audio. Due to the limitation of the bandwidth for 3GPP, only 176x144 video solution will be supported for cell phone viewing. Select the "Configure for mobile viewing" option will change the range of other related video settings.

For Best Real-time Video Images

To achieve good real-time visual effect, the network bandwidth should be large enough to allow a transmission rate of greater than 20 image frames per second. If the broadband network is over 1 Mbps, set the "Fix bit rate" to 1000Kbps or 1200Kbps, and set "Fix quality" at the highest quality. The maximum frame rate is 30. If your network bandwidth is more than 512Kbps, you can fix the bit rate according to your bandwidth and set the maximum frame rate to 30 fps. If the images vary dramatically in your environment, you may want to slow the maximum frame rate down to 20 fps in order to lower the rate of data transmission. This allows for better video quality and the human eyes cannot readily detect the differences between those of 20, 25, or 30 frames per second. If your network bandwidth is below 512 Kbps, set the "Fix bit rate" according to your bandwidth and try to get the best performance by fine-tuning with the "Maximum frame rate". In a slow network, greater frame rate results in blur images. Another work-around is to choose "160x120" in the "Size" option for better images. Video quality performance will vary somewhat due to the number of users viewing on the network; even when the parameters have initially been finely tuned. Performance will also suffer due to poor connectivity because of the network's burst constraint.

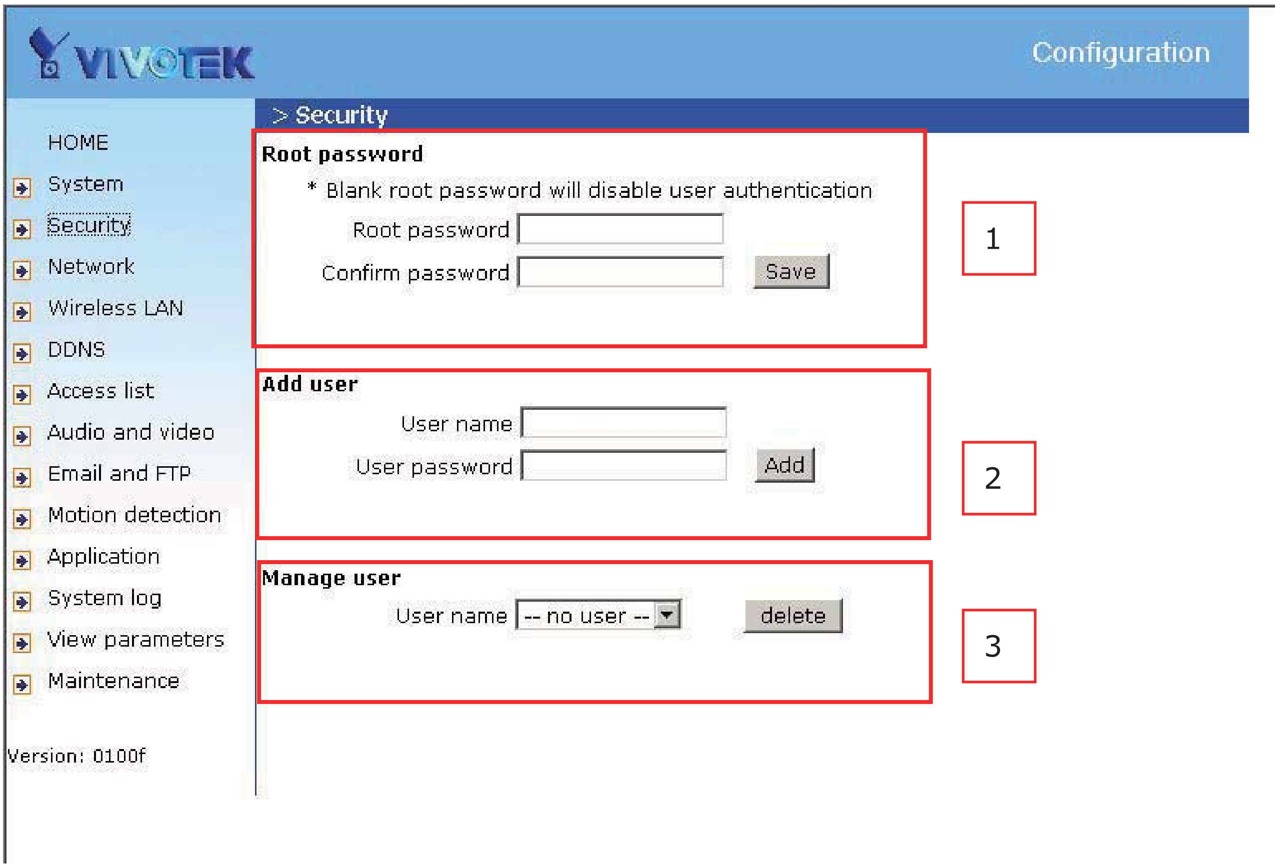
Only Quality Images Will Do

To have the best video quality, you should set "Fix quality" at "Detailed" or "Excellent" and adjust the "Maximum frame rate" to match your network's bandwidth. If your network is slow and you receive "broken" pictures, go to the TCP protocol in "Connection type" and choose a more appropriate mode of transmission. The images may suffer a time delay due to a slower connection. The delay will also increase with added number of users.

Somewhere Between Real-time and Clear Images

If you have a broadband network, set "Fix quality" at "Normal" or better, rather than setting "Fix bit rate". You can also fix the bandwidth according to your actual network speed and adjust the frame rate. Start from 30 fps down for best results but not below 15 fps. If the image qualities are not improved, select a lower bandwidth setting.

Opening accounts for new users



Protect Network Camera by passwords

The Network Camera is shipped without any password by default. That means everyone can access the Network Camera including the configuration as long as the IP address is known. It is necessary to assign a password if the Network Camera is intended to be accessed by others. Type a new word twice in ① to enable protection. This password is used to identify the administrator. Then add an account with user name and password for your friends in ②. Network Camera can provide twenty accounts for your valuable customers or friends. You may delete some users from ③.

Build a security application

The Administrator can use the built-in motion detection to monitor any movement to perform many useful security applications. To upload the snapshots, users can choose either email or FTP according to user's needs. Both e-mail and FTP use the network settings on the Email and FTP page. Refer to the definition section for detail configuration.

1. Click on "**Configuration**" on homepage,
2. Click on "**Motion detection**" at the left column,
3. Check "Enable motion detection",
4. Click on new to have a new window to monitor video,
5. Type in a name to identify the new window,
6. Use the mouse to click, hold, and drag the window corner to resize or the title bar to move,
7. Fine-tune using the "Sensitivity" and "Percentage" fields to best suit the camera's environment. Higher "Sensitivity" detects the slighter motion. Higher "Percentage" discriminates smaller objects,
8. Clicking on "Save" enables the activity display. Green means the motion in the window is under the watermark set by Administrator and red means it is over the watermark,
9. Click on "**Application**" at the left column,
10. Check the weekdays as you need and give the time interval to monitor the motion detection every day,
11. Select the Trigger on Motion detection.
12. Set the **delay before detecting next motion** to avoid continuous false alarms following the original event,
13. Set the number of pre-event and post-event images to be uploaded,
14. Check the window name set in step 5,
15. Check the way to upload snapshot,

Click on save to validate.

Software revision upgrade

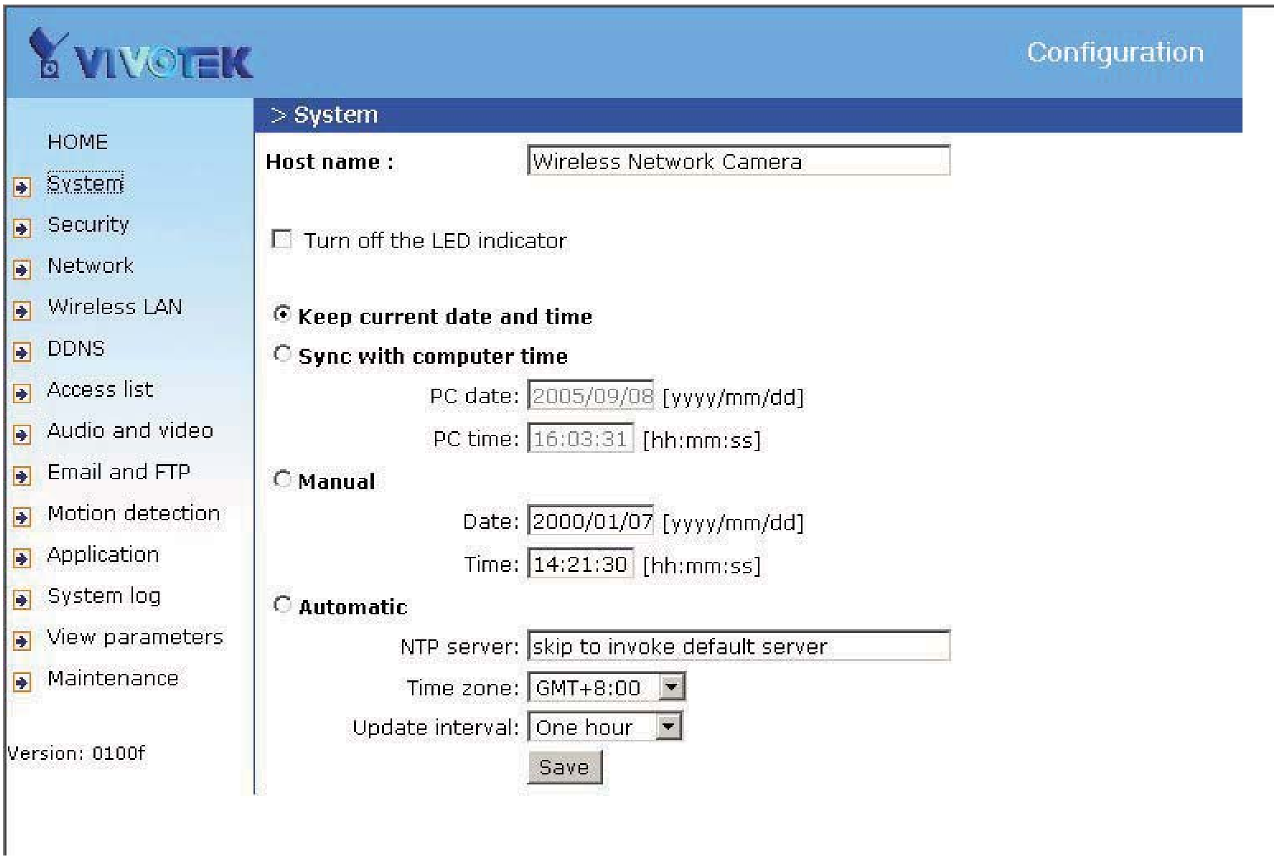
Customers can obtain the up-to-date software from the web site of VIVOTEK. An easy-to-use Upgrade Wizard is provided to upgrade the Network Camera with just a few clicks. The upgrade function is opened to the Administrator only. To upgrade the system, follow the procedures below.

1. Download the firmware file named “xxx.pkg” from the appropriate product folder.
2. Run the Upgrade Wizard and proceed following the prompts. Refer to the instructions of the Upgrade Wizard for details.
3. Or upgrade firmware from HTTP web page directly
3. The whole process will finish in a few minutes and it will automatically restart the system.

> ⚠ If power fails during the writing process of Flash memory, the program in the memory of the Network Camera may be destroyed permanently. If the Network Camera cannot restart properly, ask your dealer for technical service.

Definitions in Configuration

Only the Administrator can access system configuration. Each category in the left column will be explained in the following pages. The bold texts are the specific phrases on the Option pages. The Administrator may type the URL below the figure to directly enter the frame page of configuration. If the Administrator also wants to set certain options through the URL, read the reference appendix for details.



<url> http://<Network Camera>/setup/config.html
<Network Camera> is the domain name or original IP address of the Network Camera.
<url> http://<Network Camera>/setup/system.html
<Network Camera> is the domain name or original IP address of the Network Camera.

System parameters

"Host name" The text displays the title at the top of the main page.
“Turn off the LED indicator” Check this option to shut off the LED on the rear. It can prevent the camera’s operation being noticed.
"Keep current date and time" Click on this to reserve the current date and time of the Network Camera. An internal real-time clock maintains the date and time even when the power of the system is turned off.
"Sync with computer time" Synchronizes the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.
“Manual” Adjust the date and time according to what is entered by the Administrator. Notice the format in the related fields while doing the entry.
“Automatic” Synchronize with the NTP server over the Internet whenever the Network Camera starts up. It will fail if the assigned time-server cannot be reached.
“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.
"Time zone" Adjust the time with that of the time-servers for local settings.
“**Update interval**” Select hourly, daily, weekly, or monthly update with the time on the NTP server.

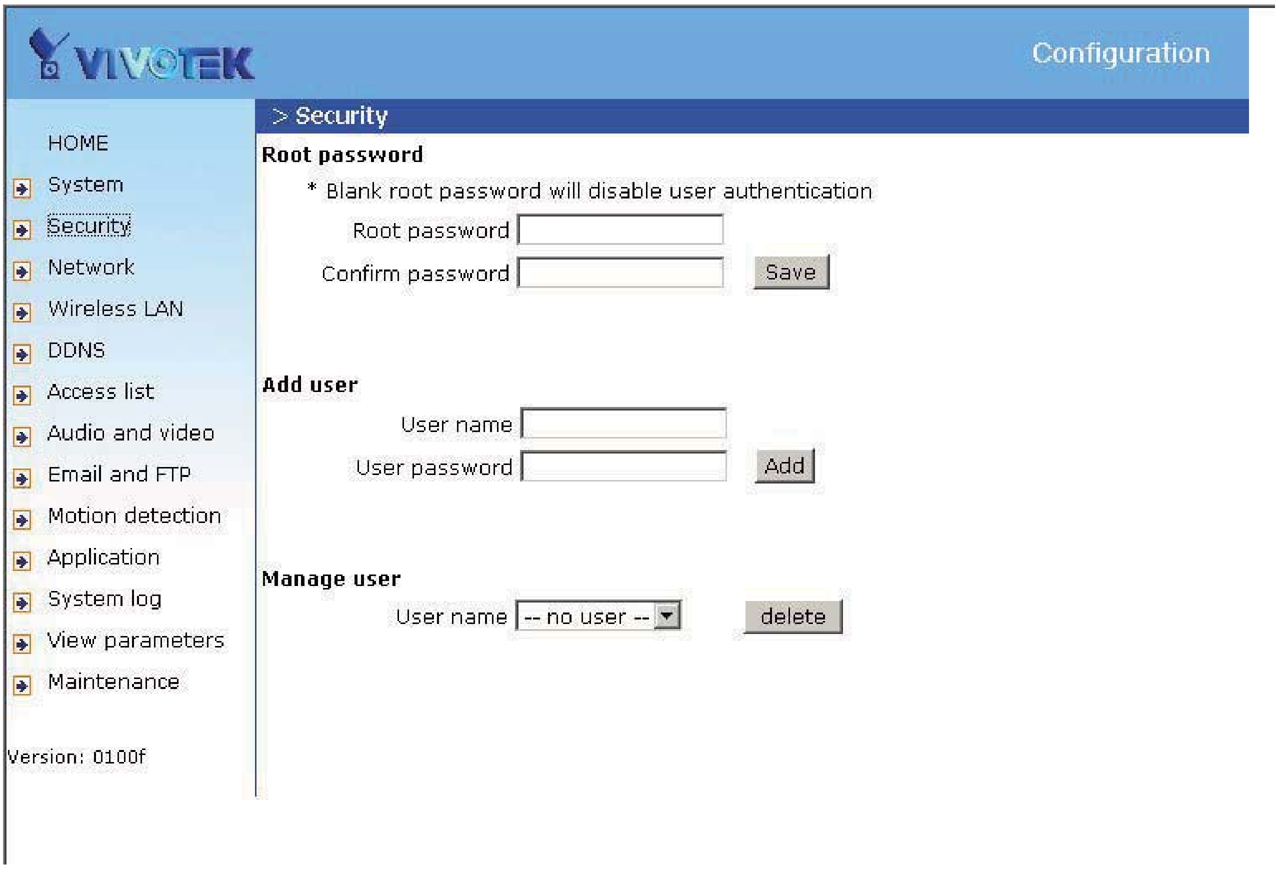
Remember to click on Save to immediately validate the changes. Otherwise, the correct time will not be synchronized.

Security settings

"Root password" Change the Administrator's password by typing in the new password identically in both text boxes. The typed entries will be displayed as asterisks for security purposes. After pressing Save, the web browser will ask the Administrator for the new password for access.

"Add user" Type the new user's name and password and press Add to insert the new entry. The new user will be displayed in the user name list. There is a maximum of twenty user accounts.

"Manager user" Pull down the user list to find the user's name and press Delete to complete.



<url> http://<Network Camera>/setup/security.html

<Network Camera> is the domain name or original IP address of the Network Camera.

Network settings

Any changes made on this page will restart the system in order to validate the changes. Make sure every field is entered correctly before clicking on Save.

Network type

“LAN” & **“PPPoE”**

The default type is LAN. Select PPPoE if using ADSL

"Get IP address automatically" & “Use fixed IP address”

The default status is “**Get IP address automatically**”. This can be tedious having to perform software installation whenever the Network Camera starts. Therefore, once the network settings, especially the IP address, have been entered correctly, select “**Use fixed IP address**” then the Network Camera will skip installation at the next boot. The Network Camera can automatically restart and operate normally after a power outage. Users can run IP installer to check the IP address assigned to the Network Camera if the IP address is forgotten or using the UPnP function provided by the Network Camera (MS Windows XP provides UPnP function at **My Network Place**).

“IP address” This is necessary for network identification.

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

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

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

“Secondary DNS” Secondary domain name server that backups the Primary DNS.

“Enable UPnP presentation” Enable the UPnP camera short cut

“**Enable UPnP port forwarding**” Enable uPnP port forwarding

“PPPoE” If using the PPPoE interface , fill the following settings from ISP

“User name” The login name of PPPoE account

“Password” The password of PPPoE account

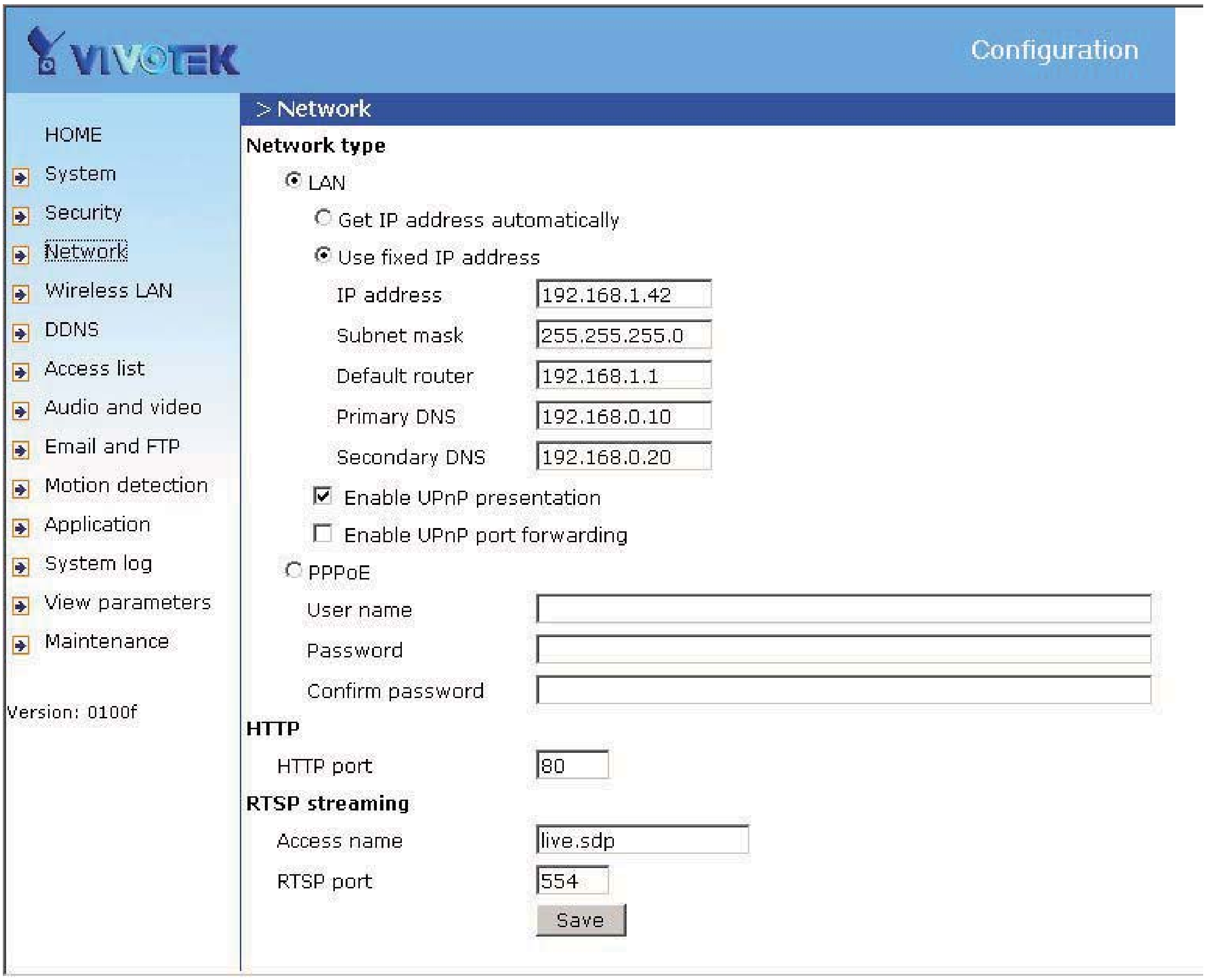
“Confirm password” Input password again for confirmation

HTTP

"Http port" This can be other than the default Port 80. Once the port is changed, the users must be notified the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the Network Camera whose IP address is 192.168.0.100 from 80 to 8080, the users must type in the web browser "http://192.168.0.100:8080" instead of "http://192.168.0.100".

RTSP Streaming

"Access name" This is the access URL for making connection from client software. Using rtsp://<ip address>/<access name> to make connection
"RTSP port" This can be other than the default Port 554



<url> *http://<Network Camera>/setup/network.html*

<Network Camera> is the domain name or original IP address of the Network Camera.

WLAN Configuration

“SSID” (Service Set Identifier), it is a 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 of SSID is 32 single-byte characters and SSID can’t be any of “, <, > and space character.*

“Wireless mode” Clicking on the pull-down menu to select from the following options:

▶ **“Infrastructure”** Make the Network Camera connect to the WLAN via an Access Point. (The default setting)

▶ **“Ad-Hoc”** Make the Network Camera connect directly to a host equipped with a wireless adapter in a peer-to-peer environment.

“Channel” While in infrastructure mode, the channel is selected automatically to match the channel setting for 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.

“TX rate” This field is for selecting the maximum transmission rate on the network. The default setting is “auto”, that is the Network Camera will try to connect to the other wireless device with highest transmitting rate.

“Security” Select the data encrypt method

▶ **“None”** – No data encryption.

▶ **“WEP”** – allows communication only with other devices with identical WEP settings.

▶ **“WPA-PSK”** – Use WPA pre-shared key.

“Auth Mode” Choosing one of the following modes, (Open is the default setting).

▶ **“Open”** – communicates the key across the network.

▶ **“Shared”** – allows communication only with other devices with identical WEP settings.

“Key length” The administrator can select the key length among 64 or 128 bits. 64bits is the default setting.

“Key format” Hexadecimal or ASCII. “**HEX**” is the default setting.

▶ **“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 space characters that are reserved.

“Network Key” Entering a key in either hexadecimal or ASCII format. When selecting

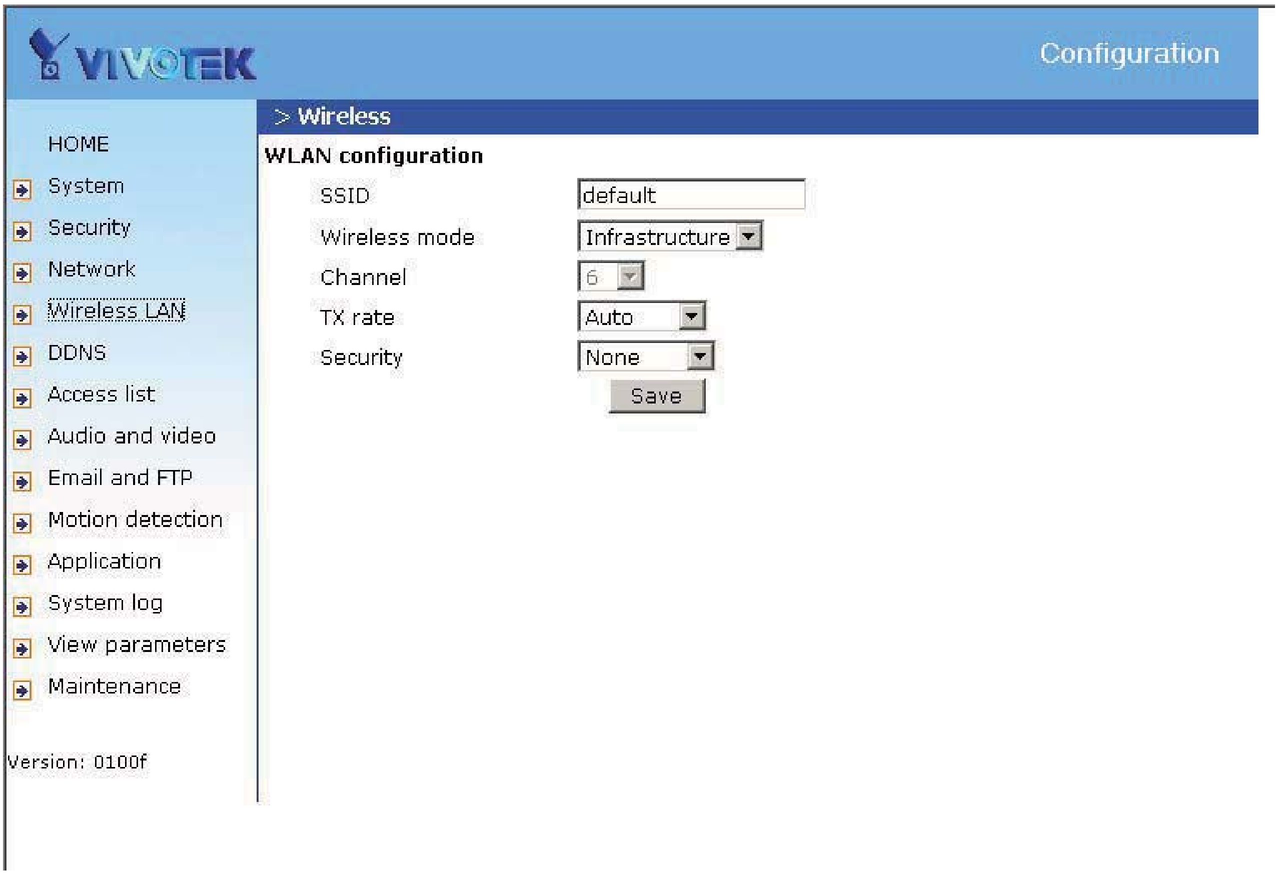
different key length, acceptable input length is listed as following:
64 bits key length: 10 Hex digits or 5 characters.
128 bites key length: 26 Hex digits or 13 characters.
Note: When 22(“), 3C(<) or 3E(>) are input in network key, the key format can’t be changed to ASCII format.

“Algorithm” Choosing one of the following algorithm for WPA-PSK modes

- **“TKIP”**
- **“AES”**

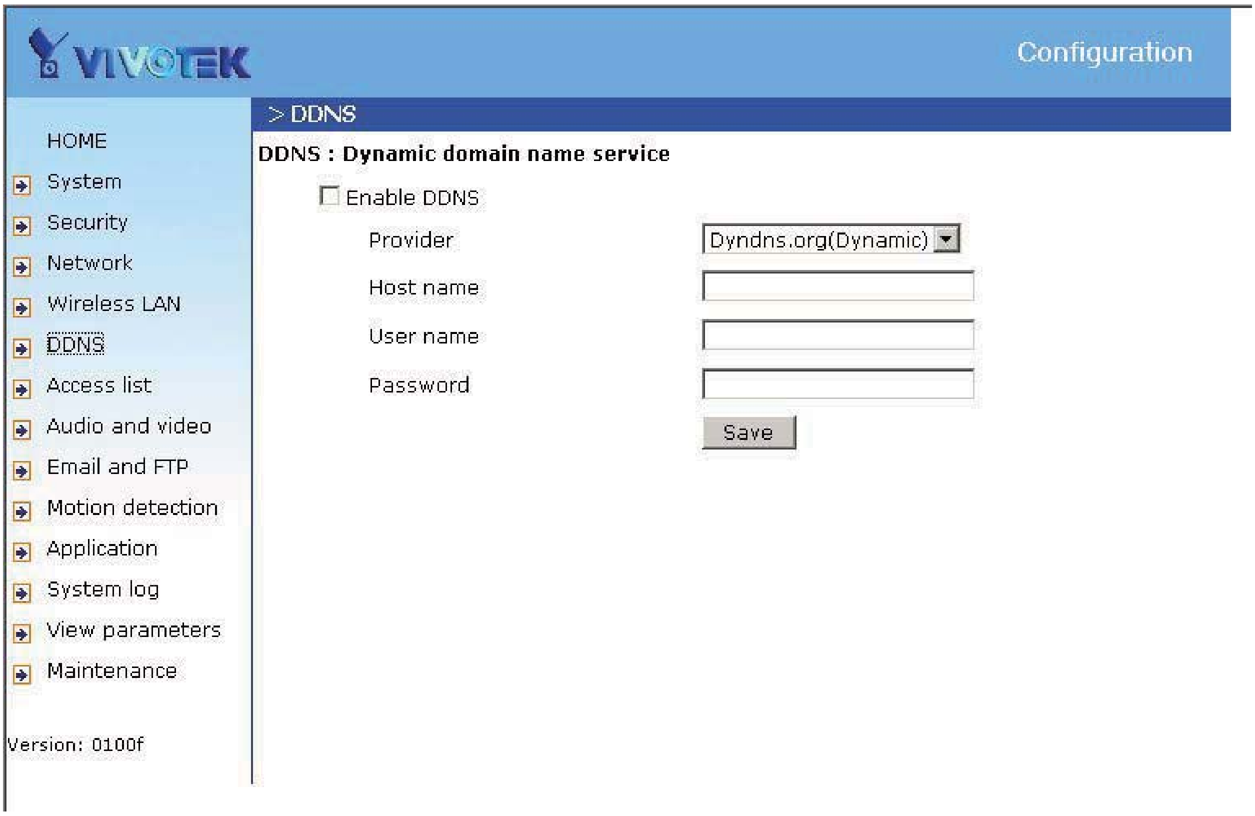
“Pre-shared Key” Entering a key in ASCII format. The length of the key is 8 ~ 63

⚠ Some invalid settings may cause the system failing to respond. Change the configuration only if necessary and consult with your network supervisor or experienced users for correct settings. Once the system has lost contact, refer to Appendix A for reset and restore procedures.



DDNS

"Enable DDNS" This option turns on the DDNS function.
"Provider" The provider list contains four hosts that provide DDNS services. Please connect to the service provider's website to make sure the service charges.
"Host Name" If the User wants to use DDNS service, this field must be filled. Please input the hostname that is registered in the DDNS server.
"Username/E-mail" The Username or E-mail field is necessary for logging in the DDNS server or notify the User of the new IP address. Note: when this field is input as "Username" the following field must be input as "Password".
"Password/Key" Please input the password or key to get the DDNS service.
"**Save**" Click on this button to save current settings for the DDNS service and UPnP function.



<url> http://<Network Camera>/setup/ddns.html
<Network Camera> is the domain name or original IP address of the Network Camera.

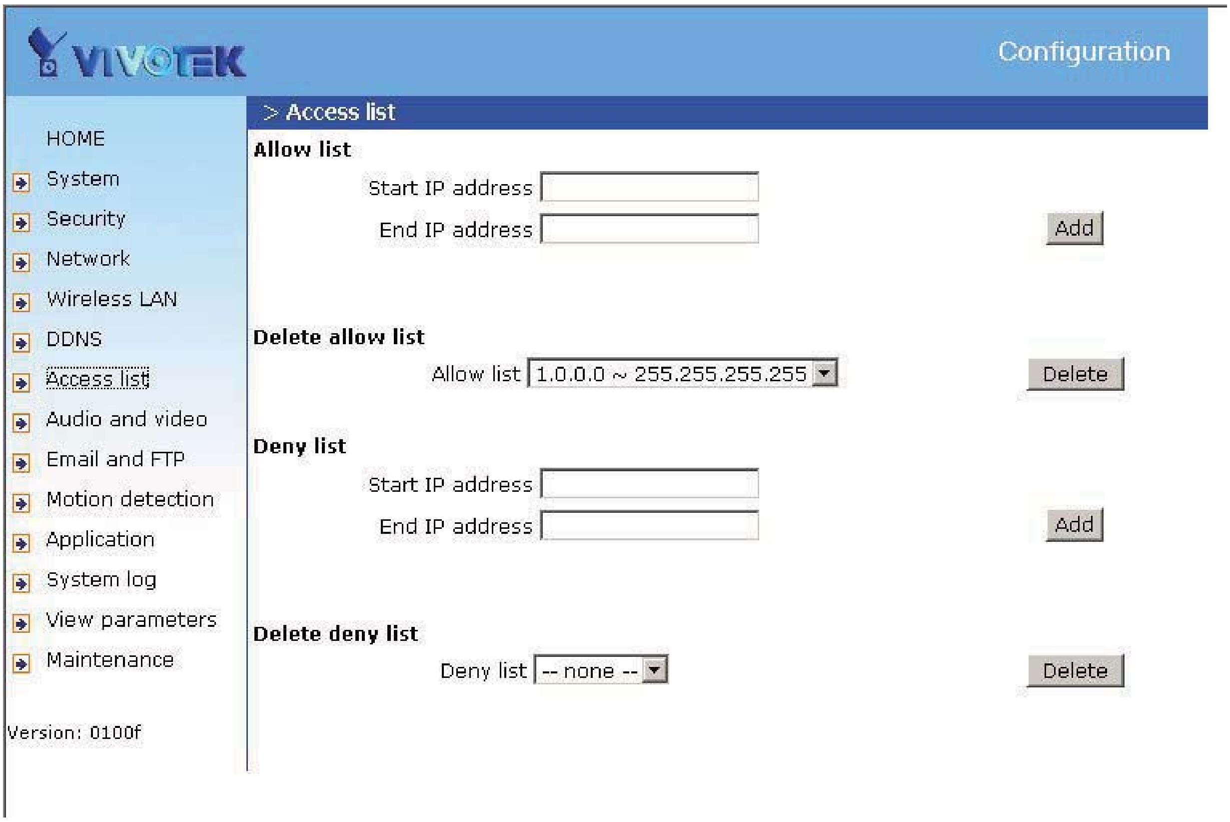
Access List

The access list is to control the access permission of clients by checking the client IP address.

There are two lists for permission control: **Allow List** and **Deny List**. Only those clients whose IP address is in the **Allow List** and not in the **Deny List** can connect to the Video Server or Network Camera for receiving the audio/video streaming.

Both **Allow List** and **Deny List** consist of a list of IP ranges. If you want to add a new IP address range, type the **Start IP Address** and **End IP Address** in the text boxes and click on the **Add** button. If you want to remove an existing IP address range, just select from the pull-down menu and click on the **Delete** button.

Both the Allow List and Deny List can have 20 entries.



<url> http://<Network Camera>/setup/accesslist.html

<Network Camera> is the domain name or original IP address of the Network Camera.

Audio and Video

General

"Configure for computer viewing" To make quick setting for computer viewing
"Configure for mobile viewing" To make quick setting for cell phone viewing

Video Settings

"Video title" The text string can be displayed on video
"Color" Select either for color or monochrome video display.
"Frame Size" There are four options for video sizes. **"160x120"**. **"176x144", "320x240", "640x480"**.
"Power line frequency (for fluorescent light)", the fluorescent light will flash according to the power line frequency that depends on local utility. Change the frequency setting to eliminate uncomfortable flash image when the light source is only fluorescent light.
There are three dependent parameters provided for video performance adjustment.
"key frame interval"
"Max frame rate" This limits the maximal refresh frame rate, which can be combined with the **"Video quality"** to optimize bandwidth utilization and video quality. Choose "**Constant bit rate**" If the user wants to fix the bandwidth utilization regardless of the video quality, choose **"Fixed quality"** and select the desired bandwidth. The video quality may be poor due to the sending of maximal frame rate within the limited bandwidth when images are moving rapidly. Consequently, to ensure detailed video quality (quantization rate) regardless of the network, it will utilize more bandwidth to send the maximal frames when images change drastically.
"Maximum Exposure Time" Select a proper maximum exposure time according to the light source of the surroundings. The exposure time are selectable at the following duration: 1/120 second, 1/60 second, 1/30 second, and 1/15 second. Shorter exposure time would accept less light amount.

Video orientation

“Flip” Vertically rotate the video.
“Mirror” Horizontally rotate the video. Check options both if the Network Camera is installed upside down.
“White balance” Adjust the value for best color temperature.

Audio settings

“mute” Audio mute
“Audio type” Select audio codec **“AAC”** or **“GSM-AMR”** and the bit rate

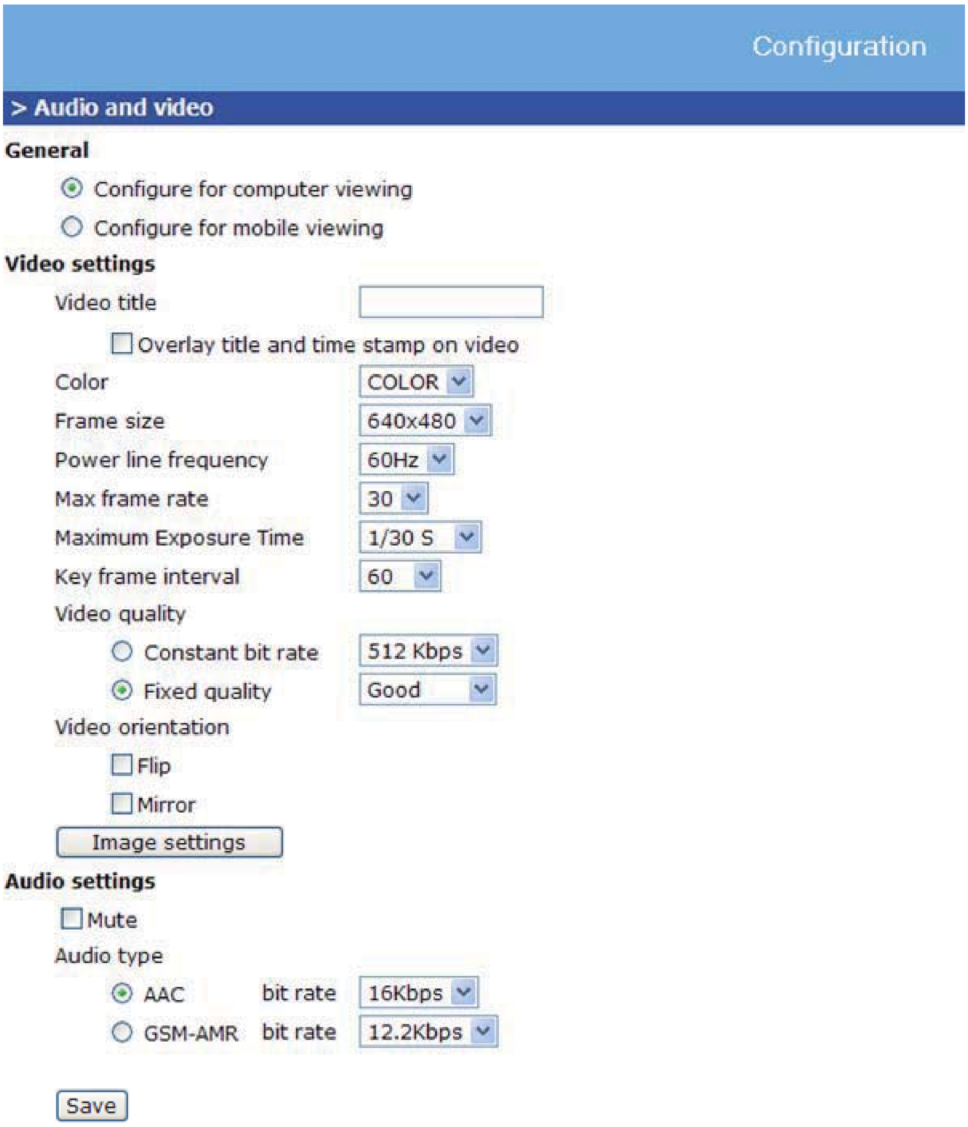


Image Settings

[Image settings] Click on this button to pop up another window to tune **"Brightness"**, **"Contrast"**, **"Hue"** and **"Saturation"** for video compensation. Each field has eleven levels ranged from -5 to +5. In **"Brightness"** and **"Contrast"** fields the value 0 indicates auto tuning. The user may press [Preview] to fine-tune the image. When the image is O.K., press [Save] to set the image settings. [Restore] Click on this to recall the original settings without incorporating the changes.

Email & FTP

Email

When the SMTP server support SMTP authentication, users need to give the valid user name and password to send email via the server.
“Sender email address”, the email address of the sender.

There are two external mail server can be configured, primary and secondary email server, The network camera will use primary server as default , and use secondary server when primary server is unreachable.
“Server address” The domain name or IP address of the external email server.
“User name” This granted user name on the external email server.
“Password” This granted password on the external email server.
“Recipient email address” The email address of the recipients for snapshots or log file. Multiple recipients must be separated by semicolon, ‘;’.

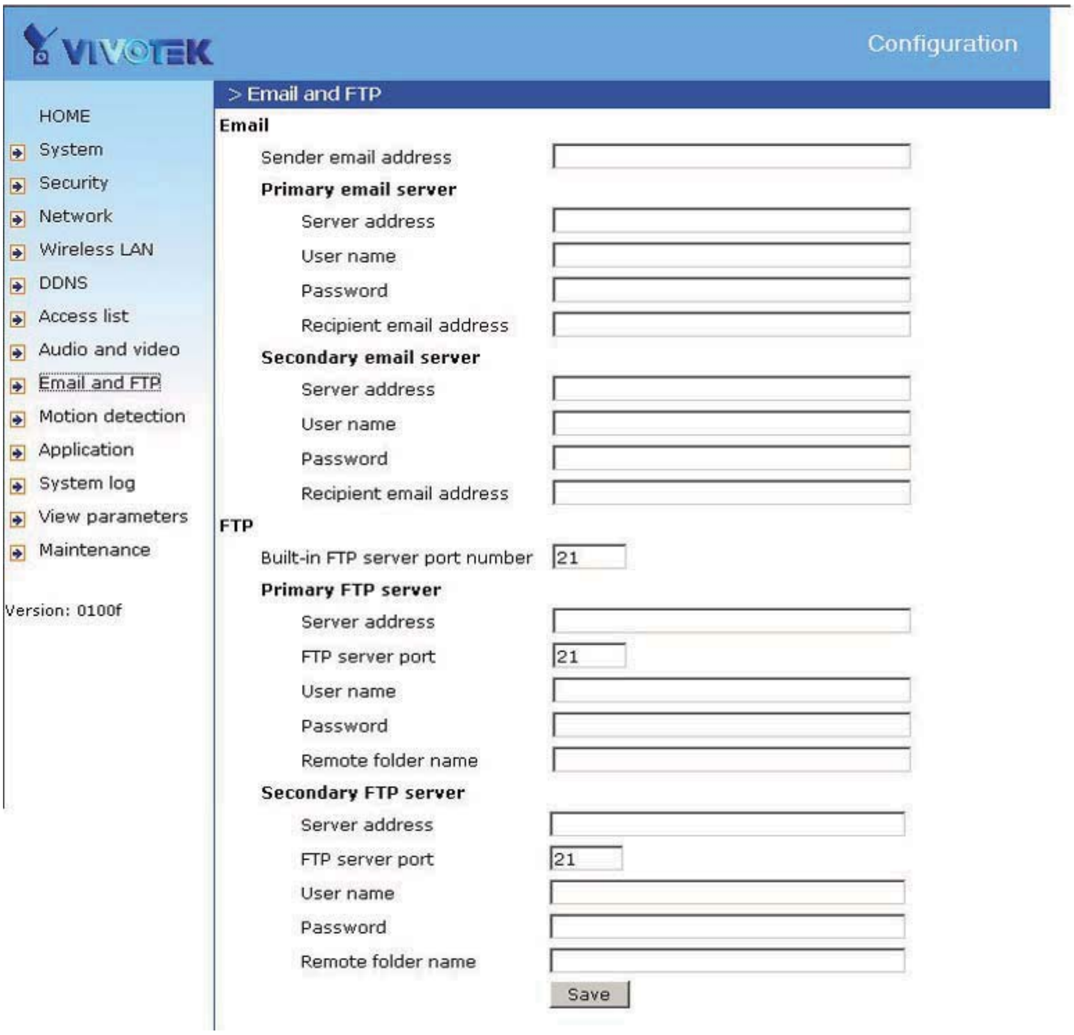
FTP

“Built-in FTP server port number” This can be other than the default port 21. The user can change this value from 1025 to 65535. After the changed, the external FTP client program must change the server port of connection accordingly.

There are two external FTP server can be configured, primary and secondary FTP server, The network camera will use primary server as default , and use secondary server when primary server is unreachable.

“Server address” The domain name or the IP address of the external FTP server. The following user settings must be correctly configured for remote access.
“FTP server port” This can be other than the default port 21. The user can change this value from 1025 to 65535.
“User name” Granted user name on the external FTP server.
“Password” Granted password on the external FTP server.

"Remote folder name" Granted folder on the external FTP server. The string must conform to that of the external FTP server. Some FTP servers cannot accept preceding slash symbol before the path without virtual path mapping. Refer to the instructions for the external FTP server for details. The folder privilege must be open for upload.



<url> *http://<Network Camera>/setup/mailftp.html*

<Network Camera> is the domain name or original IP address of the Network Camera.

Motion detection

"Enable motion detection" Check this option to turn on motion detection.

New Click on this button to add a new window. At most three windows can exist simultaneously. Use the mouse to click, hold, and drag the window frame to resize or the title bar to move. Clicking on the 'x' at the upper right-hand corner of the window to delete the window. Remember to save in order to validate the changes.

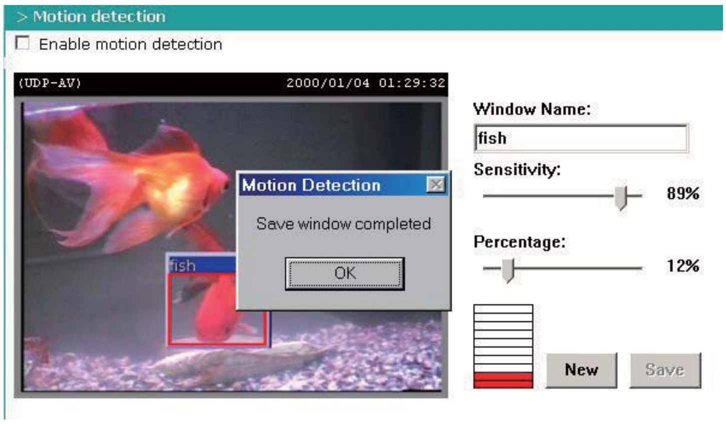
Save Click on this button to save the related window settings. A graphic bar will rise or fall depending on the image variation. A green bar means the image variation is under monitoring level and a red bar means the image variation is over monitoring level. When the bar goes red, the detected window will also be outlined in red. Going back to the homepage, the monitored window is hidden but the red frame shows when motion is detected.

"Window Name" The text will show at the top of the window.

"Sensitivity" This sets the endurable difference between two sequential images.

"Percentage" This sets the space ratio of moving objects in the monitoring window. Higher sensitivity and small percentage will allow easier motion detection.

The following figure shows the screen when Save is clicked. The monitoring window has been outlined in red and the graphic bar goes red since the goldfish is moving.



Application settings

The server provides two kinds of applications, snapshot and videoclip. There are two independent snapshot items to set, and they are named as Snapshot #1 and Snapshot #2. The status, schedule, trigger condition, and action of three applications are summaried in the application page. The user can click on Snapshot #1, Snapshot #2 or Video Clip to enter the detail setting page.

> Application

	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger	Send
Snapshot #1	OFF								always	motion	mail
Snapshot #2	OFF								always	motion	mail
Video Clip	OFF								always	motion	mail

Snapshot

"Enable snapshot" Enable/Disable snapshot application.

Weekly schedule

"Sun" ~ "Sat" Select the days of the week to perform the application.
Select **"Always"** or input the time interval.

Snapshot file name prefix

The prefix name will be added on the file name of the snapshot images.

Send out the snapshot while motion detection

There are three windows for motion detection each can be assigned a name. Select the windows which need to be monitored. If motion detection has not been set up, "**undefined**" will be shown instead of the window title. If this happens, clicking on "Motion detection" and a note will show to direct the User to the configuration page for motion detection.
"Send pre-event image(s)" The number of pre-snapshots will be captured and send when a condition is triggered.

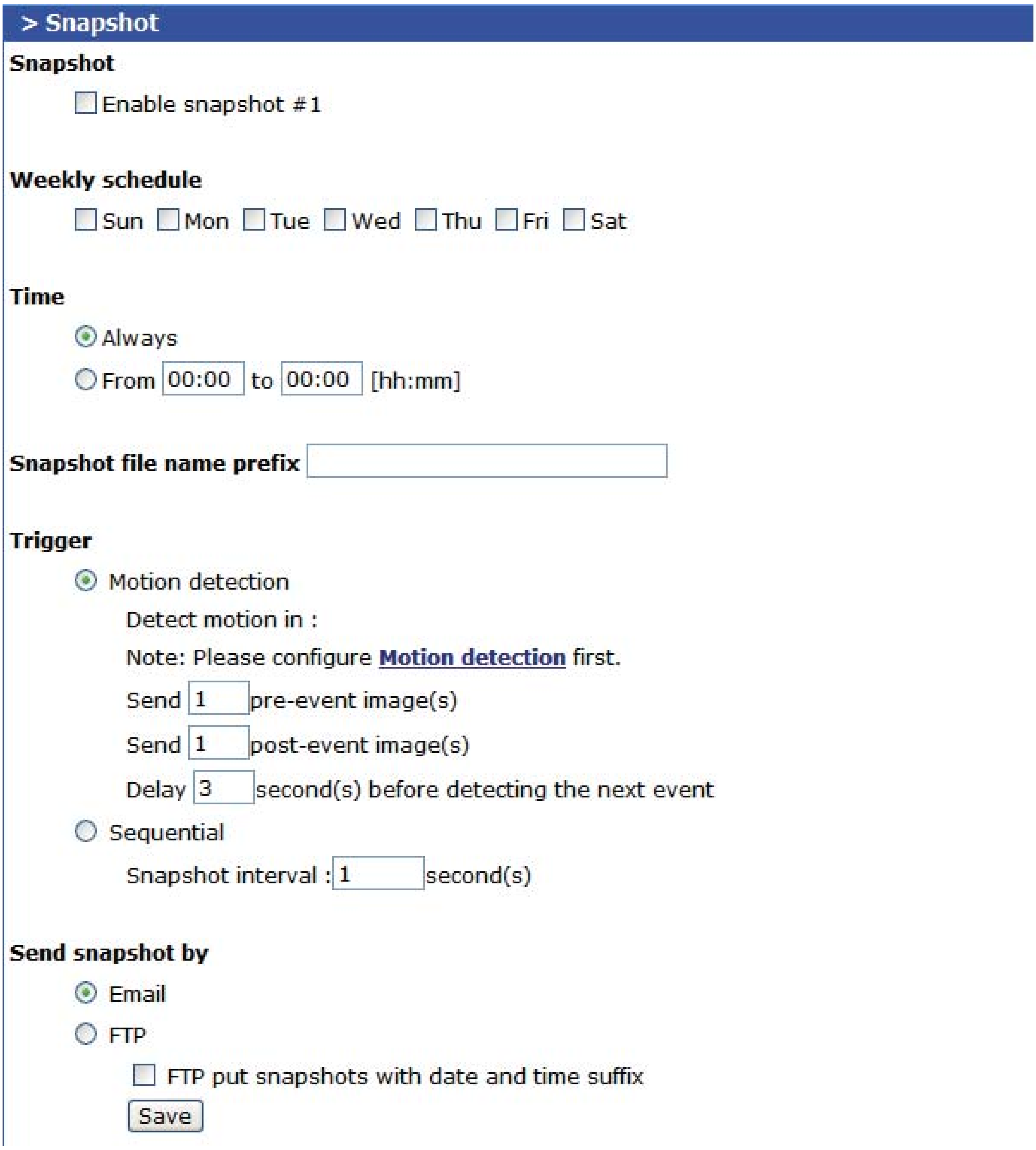
"Send post-event image(s)" The number of post-snapshots will be captured and send when a condition is triggered.
"Delay second(s) before detecting next motion" Set the time delay before restarting to check on the triggering condition when the current condition is triggered.

Sequential operation

"Snapshot interval (seconds)" Network Camera will send snapshots at the specified intervals to the external server using the method selected below. Remember: This operation is still subject to the conditions set in the weekly schedule.

Method for sending snapshot

"Email" This selects the uploading method following the intervals set above. The snapshot named "prefix-yyyymmdd-hhmmss.jpg" will be attached in the email.
"FTP" The snapshots will be uploaded to the external FTP server with the file name defined in the next option. This can also be used to refresh the captured images stored in the external web server to build creative homepages.
"FTP put snapshots with date and time suffix" This option sets up the snapshot capture date and time, which can be used to easily differentiate the snapshot file names in the sequential operation. For instance, "prefix-20030102-030405.jpg" means the JPEG image was captured in the year 2003, January the 2nd, at 3 o'clock, 4 minute, and 5 second. If this suffix is omitted, the file named "video.jpg" on the external FTP server will be refreshed at the specified interval.


> Snapshot
Snapshot
Enable snapshot #1
Weekly schedule
Sun Mon Tue Wed Thu Fri Sat
Time
Always
From 00:00 to 00:00 [hh:mm]
Snapshot file name prefix
Trigger
Motion detection
Detect motion in :
Note: Please configure Motion detection first.
Send 1 pre-event image(s)
Send 1 post-event image(s)
Delay 3 second(s) before detecting the next event
Sequential
Snapshot interval : 1 second(s)
Send snapshot by
Email
FTP
FTP put snapshots with date and time suffix
Save

> Videoclip

Video Clip

☐ Enable videoclip

Weekly schedule

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Time

◉ Always

○ From 00:00 to 00:00 [hh:mm]

Video clip file name prefix

Video clip max file size 500 **KB**

Trigger

◉ Motion detection

Detect motion in :

Note: Please configure **Motion detection** first.

Delay 60 second(s) before detecting the next event

○ Sequential

Video clip interval: 60 second(s)

Send videoclip by

◉ Email

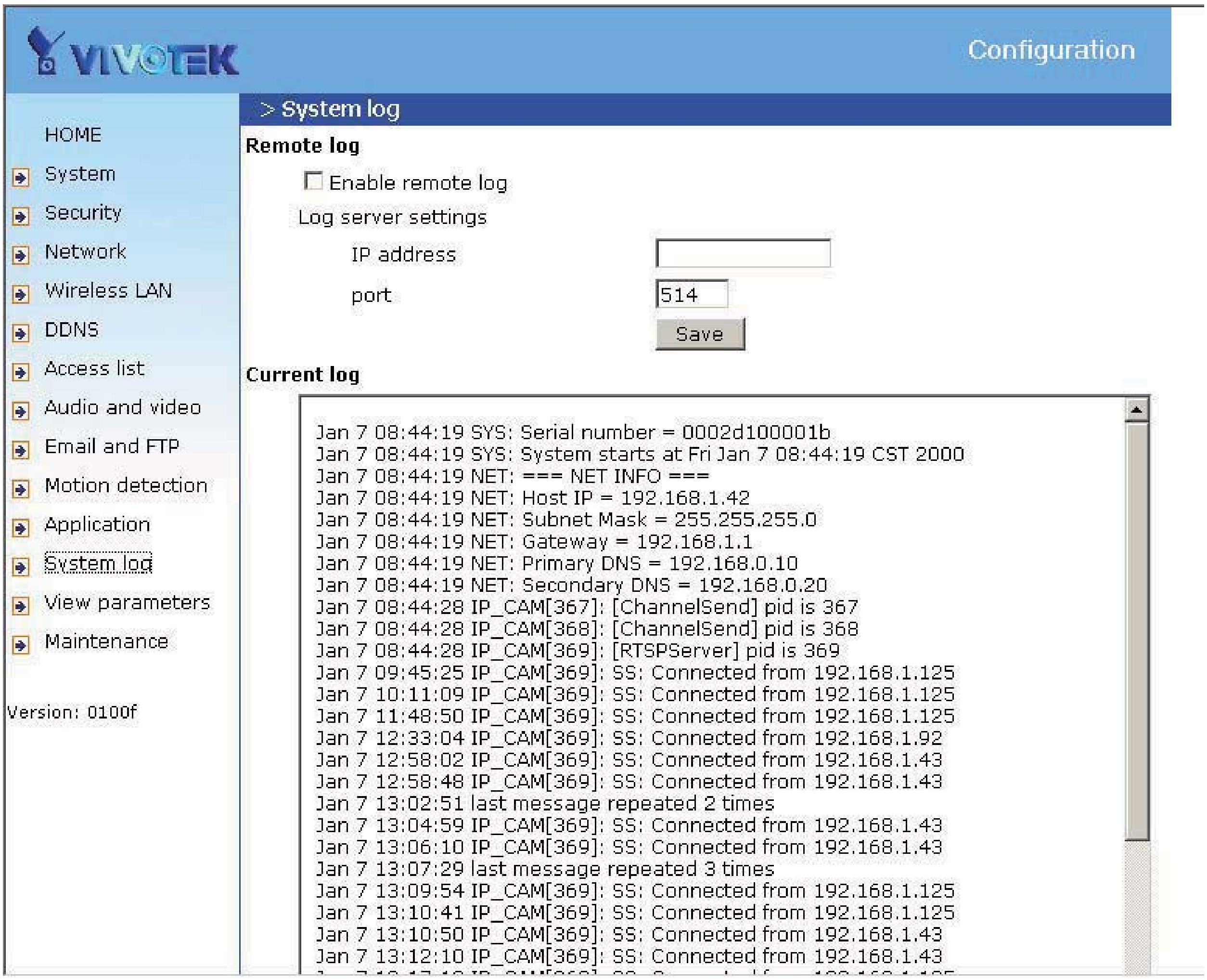
○ FTP

☐ FTP put Video clips with date and time suffix

Save

System log

The Network camera support log the system messages on remote server. The protocol is compliant to RFC 3164. If you have external Linux server with syslogd service, use “-r” option to turn on the facility for receiving log from remote machine. Or you can use some software on Windows which is compliant to RFC 3164.
Check **“Enable remote log**” and input the **“IP address**” and **“port”** number of the log server to enable the remote log facility.
In the **“Current log”**, it displays the current system log file. The content of the log provides useful information about configuration and connection after system boot- up.



Viewing system parameters

Click on this link on the configuration page to view the entire system's parameter set. The content is the same as those in CONFIG.INI.

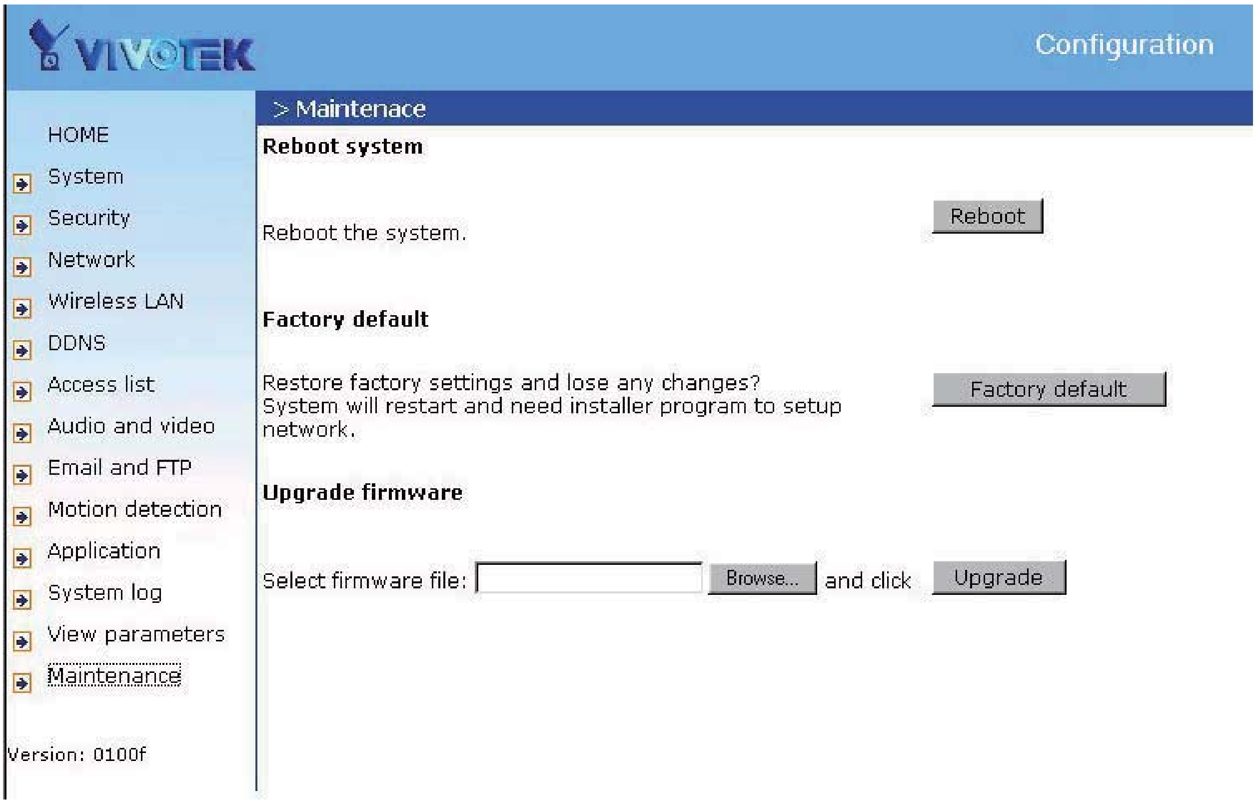
Maintenance

Three actions can be selected

"reboot" click the reboot button to restart system

"factory default" Click on Factory default button on the configuration page to restore the factory default settings. Any changes made so far will be lost and the system will be reset to the initial factory settings. The system will restart and require the installer program to set up the network again.

"upgrade firmware" Select the firmware file and click upgrade button



Appendix

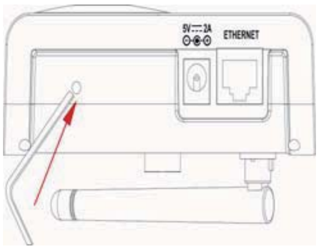
A. Troubleshooting

Status LED

The following table lists the LED patterns in general.

Condition	LED color
Loading system after power on	Steady blue
During booting procedure	Steady blue and red
Detecting and setting network	Steady blue and blink red till IP address is confirmed
After network is setup (system up)	Blink blue every second and steady red
During the upgrade firmware process	Blink blue every second and fast blink red

Reset and restore



There is a button in the back of the Network Camera. It is used to reset the system or restore the factory default settings. Sometimes resetting the system sets the system back to normal state. If the system problems remain after reset, restore the factory settings and install again.

RESET: Click on the button.

RESTORE: 1. Press on the button continuously.

2. Wait for self-diagnostic to run twice.

3. Free the button as soon as the second self-diagnostic starts.

Restoring the factory defaults will erase any previous settings. Reset or restore the system after power on.

B. URL commands of the Network Camera

For some customers who already have their own web site or web control application, the Network Camera can be easily integrated through convenient URLs. This section lists the commands in URL format corresponding to the basic functions of the erase Network Camera.

Get server parameter values

Note: This request require administrator access
Method: GET/POST

Syntax:

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

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

When query parameter values, the current parameter value are returned.
Successful control requests returns paramter 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 it's response

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

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

```
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n
```

Set server parameter values

Note: This request require administrator access
Method: GET/POST

Syntax:

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

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

Return:

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

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

[<parameter pair>]

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

Example: Set the IP address of server to 192.168.0.123

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

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

Available parameters on the server

NOTE: The bold characters in table are the default value of each parameter.

Group: **System**

NAME	VALUE	DESCRIPTION
hostname (r/w)	<text string shorter than 40 characters>	host name of server **<<Wireless>Network Camera >**
ledoff (r/w)	**0**	Do not turn off the led indicator
	1	Turn off the led indicator
date (r/w)	**<yyyy/mm/dd>**	year, month and date separated by slash.
	<keep>	keep date unchanged
	<auto>	Using NTP to sync date/time automatically
time (r/w)	**<hh:mm:ss>**	hour, minute and second separated by colon.
	<keep>	keep date unchanged
	<auto>	Using NTP to sync date/time automatically

ntp (r/w)	<domain name or IP address>	NTP server **<skip to invoke default server>**
timezone (r/w)	-12 ~ 12	time zone, 8 means GMT +8:00 **<8>**
updateinterval (r/w)	0 ~ 2592000	0 to Disable automatic time adjustment, otherwise, it means the seconds between NTP automatic update interval. **<0>**
serialnumber (r)	<mac address>	12 characters mac address without hyphen connected
firmwareversion (r)	<text string shorter than 39 characters>	The version of firmware, including model, company, and version number
restore (w)	0	Restore the system parameters to default value.
	Positive integer	Restore the system parameters to default value and restart the server after <value> seconds.
reset (w)	0 ~ 65535	Restart the server after <value> seconds.
	-1	Not restart the server.
viewmode (r/w)	**0**	Using the profile of viewing by computer
	1	Using the profile of viewing by mobile phone

Group: **Security**

NAME	VALUE	DESCRIPTION
username_<1~20> (r/w)	<text string shorter than 16 characters>	change user name. ***<blank>***
userpass_<0~20> (r/w)	<text string shorter than 14 characters>	change user's password. The UserPass_0 is root's password. ***<blank>***
userattr_<1~20> (r)	[conf]	show user's privilege. The privilege can be <blank> - only permit to view live media conf – Permit to change server's configuration

		<blank>
usercount (r)	1 ~ 21	The current account number on the server including root.**<1>**

Group: **Network**

NAME	VALUE	DESCRIPTION
type (r/w)	**0**	LAN
	1	PPPoE
pppoeuser (r/w)	<text string shorter than 80 characters>	PPPoE account user name **<blank>**
pppoepass (r/w)	<text string shorter than 15 characters>	PPPoE account password **<blank>**
resetip (r/w)(restart)	**1**	enable to get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot
	0	Using preset ipaddress, subnet, router, dns1, dns2
ipaddress (r/w) (restart)	<IP address>	IP address of server **<192.168.0.99>**
subnet (r/w) (restart)	<IP address>	subnet mask **<255.255.255.0>**
router (r/w) (restart)	<IP address>	default gateway ***<blank>***
dns1 (r/w) (restart)	<IP address>	primary DNS server ***<blank>***
dns2 (r/w) (restart)	<IP address>	secondary DNS server ***<blank>***
smtp1 (r/w)	<domain name or IP address, string shorter than 40 characters>	primary SMTP server ***<blank>***
mailto1 (r/w)	<string shorter than 80 characters>	mail recipient address ***<blank>***
mailuser1 (r/w)	<text string shorter than 63 characters>	User name of primary smtp server ***<blank>***
mailpass1 (r/w)	<text string shorter than 15 characters>	Password of primary smtp server ***<blank>***
smtp2 (r/w)	<domain name or IP address, string shorter than 40 characters>	secondary SMTP server ***<blank>***

mailto2 (r/w)	<text string shorter than 80 characters>	mail recipient address ***<blank>***
mailuser2 (r/w)	<text string shorter than 63 characters>	User name of secondary smtp server ***<blank>***
mailpass2 (r/w)	<text string shorter than 15 characters>	Password of secondary smtp server ***<blank>***
returnemail (r/w)	<text string shorter than 80 characters>	return email address ***<blank>***
localftpport (r/w)	<positive number less than 65535>	FTP port **<21>**
ftp1 (r/w)	<domain name or IP address, string shorter than 40 characters >	primary FTP server ***<blank>***
ftpport1 (r/w)	<positive number less than 65535>	primary FTP port **<21>**
ftpuser1 (r/w)	<text string shorter than 63 characters>	user name for primary FTP server ***<blank>***
ftppass1 (r/w)	<text string shorter than 15 characters>	password for primary FTP server ***<blank>***
ftpfolder1 (r/w)	<text string shorter than 40 characters>	upload folder in primary FTP server ***<blank>***
ftppasvmode1 (r/w)	1	Enable passive mode of primary FTP server
	0	Disable passive mode of primary FTP server
ftp2 (r/w)	<domain name or IP address, string shorter than 40 characters >	secondary FTP server
ftpport2 (r/w)	<positive number less than 65535>	secondary FTP port **<21>**
ftpuser2 (r/w)	<text string shorter than 63 characters>	user name for secondary FTP server ***<blank>***
ftppass2 (r/w)	<text string shorter than 15 characters>	password for secondary FTP server ***<blank>***
ftpfolder2 (r/w)	<text string shorter than 40 characters>	upload folder in secondary FTP server ***<blank>***
ftppasvmode2 (r/w)	1	Enable passive mode of primary FTP server
	0	Disable passive mode of primary FTP server
httpport (r/w) (restart)	<positive number less than 65535>	HTTP port **<80>**

rtspport (r/w) (restart)	<positive number less than 65535>	RTSP port **<554>**
videoport (r)	<positive number less than 65535>	video Channel port for RTP **<5558>**
audioport (r)	<positive number less than 65535>	audio Channel port for RTP **<5556>**
accessname (r/w)	<text string shorter than 20 characters>	RTSP access name **<live.sdp>**

Group: **Wireless (restart)**

ssid (r/w)	<text string shorter than 32 characters>	SSID for wireless lan settings **<default>**
wlmode (r/w)	**0**	Infrastructure mode
	1	Adhoc mode
txrate (r/w)	"NONE", "1M", "2M", "5.5M", "11M", "22M" for 802.11b+ "NONE", "1M", "2M", "5.5M", "11M", "6M", "9M", "12M", "18M", "24M", "36M", "48M", "54M", "Auto" for 802.11g	Transmit rate in Mbps **<Auto>**
encrypt (r/w)	**0**	None data encryption
	1	WEP data encryption
	2	WPA-PSK data encryption
authmode (r/w)	**Open**	Open mode
	Shared	Shared mode
keylength (r/w)	(**64**, 128) for 802.11g	Key length in bits **<64>**
keyformat (r/w)	**HEX**	Key1 ~ Key4 will be represented in HEX format
	ASCII	Key1 ~ Key4 will be represented in ASCII format
keyselect (r/w)	1 ~ 4	Default key number **<1>**

key1 (r/w)	<text string shorter than 58 characters> (depends on keyformat & keylength)	WEP key1 for encryption **<0000000000>**
key2 (r/w)	<text string shorter than 58 characters> (depends on keyformat & keylength)	WEP key2 for encryption **<0000000000>**
key3 (r/w)	<text string shorter than 58 characters> (depends on keyformat & keylength)	WEP key3 for encryption **<0000000000>**
key4 (r/w)	<text string shorter than 58 characters> (depends on keyformat & keylength)	WEP key4 for encryption **<0000000000>**
algorithm (r/w)	**TKIP**	TKIP data encryption algorithm for WPA-PSK
	AES	AES data encryption algorithm for WPA-PSK
presharedkey (r/w)	<text string shorter than 58 characters>	WPA-PSK key for encryption **<00000000>**

Group: **IPFilter**

NAME	VALUE	DESCRIPTION
allowstart_<0~9> (r/w)	1.0.0.0 ~ 255.255.255.255	Allowed starting RTSP connection IP address **<1.0.0.0>**
allowend_<0~9> (r/w)	1.0.0.0 ~ 255.255.255.255	Allowed ending RTSP connection IP address **<255.255.255.255>**
denystart_<0~9> (r/w)	1.0.0.0 ~ 255.255.255.255	Denied starting RTSP connection IP address ***<blank>***
denyend_<0~9> (r/w)	1.0.0.0 ~ 255.255.255.255	Denied ending RTSP connection IP address ***<blank>***

Group: **Video**

NAME	VALUE	DESCRIPTION
text (r/w)	<text string shorter than 14 characters>	enclosed caption ***<blank>***
codectype (r/w)	**0**	MPEG4

keyinterval (r/w)	1, 3, 5, 10, 30, 60, 90, 120	Key frame interval **<60>**
size	1	half
(r)	2	half x 2
	3	normal
	4	normal x 2
	5	double
	256	This field is obsolete (use resolution)
resolution	**176x144 (for mobile)**	Video resolution 176 x 144
(r/w)	160x120	Video resolution 160 x 120
	320x240	Video resolution 320 x 240
	640x480 (for computer)	Video resolution 640 x 480
color	0	monochrome
(r/w)	**1**	color
quality	0	fix bit rate
(r/w)	**1**	fix quantization
quant	1	lowest quality of video
(r/w)	2	lower quality of video
	3	normal quality of video
	4	higher quality of video
	5	highest quality of video
bitrate	20000	set bit rate to 20K bps
(r/w)	30000	set bit rate to 30K bps
	40000	set bit rate to 40K bps
	50000	set bit rate to 50K bps
	64000	set bit rate to 64K bps
	128000	set bit rate to 128K bps
	256000	set bit rate to 256K bps
	512000	set bit rate to 512K bps
	768000	set bit rate to 768K bps
	1000000	set bit rate to 1000K bps
	1500000	set bit rate to 1500K bps
	2000000	set bit rate to 2000K bps
	3000000	set bit rate to 3000K bps
	4000000	set bit rate to 4000K bps
maxframe	1	set maximum frame rate to 1 fps

(r/w)	2	set maximum frame rate to 2 fps
	3	set maximum frame rate to 3 fps
	5	set maximum frame rate to 5 fps
	10	set maximum frame rate to 10 fps
	15	set maximum frame rate to 15 fps
	20	set maximum frame rate to 20 fps
	25	set maximum frame rate to 25 fps
	30 (for 60Hz only)	set maximum frame rate to 30 fps
mode (r/w) (in CMOS version only)	50	synchronize with 50Hz utility
	60	synchronize with 60Hz utility
whitebalance (r/w) (in CMOS version only)	**0**	auto white balance
	1	fixed indoor(3200K)
	2	fixed fluorescent (5500K)
	3	fixed outdoor(> 5500K)
flip (r/w)	1	flip image
	0	normal image
mirror (r/w)	1	mirror image
	0	normal image
imprinttimestamp (r/w)	1	Overlay time stamp on video
	0	Do not overlay time stamp on video

Group: **Audio**

NAME	VALUE	DESCRIPTION
type (r/w)	**AAC4 (for computer)**	set codec to AAC
	GAMR (for mobile)	set codec to GSM-AMR
aacbitrate (r/w)	16000	set AAC bitrate to 16K bps
	32000	set AAC bitrate to 32K bps
	48000	set AAC bitrate to 48K bps
	64000	set AAC bitrate to 64K bps
	96000	set AAC bitrate to 96K bps
	128000	set AAC bitrate to 128K bps
amrbitrate (r/w)	4750	set AMR bitrate to 4.75K bps
	5150	set AMR bitrate to 5.15K bps
	5900	set AMR bitrate to 5.9K bps
	6700	set AMR bitrate to 6.7K bps

	7400	set AMR bitrate to 7.4K bps
	7950	set AMR bitrate to 7.95K bps
	10200	set AMR bitrate to 10.2K bps
	12200	set AMR bitrate to 12.2K bps

Group: **Image**

NAME	VALUE	DESCRIPTION
brightness (r/w)	<-5 ~ 5>	Adjust brightness of image according to mode settings. **<0>**
saturation (r/w)	<-5 ~ 5>	Adjust saturation of image according to mode settings. **<0>**
contrast (r/w)	<-5 ~ 5>	Adjust contrast of image according to mode settings. **<0>**
hue (r/w)	<-5 ~ 5>	Adjust hue of image according to mode settings. **<0>**

Group: **Motion**

NAME	VALUE	DESCRIPTION
enabled (r/w)	**0**	disable motion detection
	1	enable motion detection
winenabled_<0~2> (r/w)	**0**	disable motion window #1
	1	enable motion window #1
winname_<0~2> (r/w)	<text string shorter than 14 characters >	name of motion window #1 ***<blank>***
winleft_<0~2> (r/w)	0 ~ 320	Left coordinate of window position. **<0>**
wintop_<0~2> (r/w)	0 ~ 240	Top coordinate of window position. **<0>**
winwidth_<0~2> (r/w)	0 ~ 320	Width of motion detection window. **<0>**
winheight_<0~2> (r/w)	0 ~ 240	Height of motion detection window. **<0>**
winobjsize_<0~2> (r/w)	0 ~ 100	Percent of motion detection window **<0>**
winsensitivity_<0~2> (r/w)	0 ~ 100	Sensitivity of motion detection window **<0>**

update (w)	1	Update the above motion detection settings to take effect

Group: **DDNS**

NAME	VALUE	DESCRIPTION
enable (r/w)	0, 1	Enable or disable the dynamic dns. **<0>**
provider (r/w)	1 ~ 6	dyndns.org (dynamic) dyndns.org (custom) tzo.com dhs.org safe100.net dyn-interfree.it **<1>**
hostname (r/w)	Text string shorter than 127 characters.	Your dynamic hostname. ***<blank>***
usernameemail (r/w)	Text string shorter than 63 characters.	Your user or email to login ddns service provider ***<blank>***
passwordkey (r/w)	Text string shorter than 20 characters.	Your password or key to login ddns service provider ***<blank>***
update (w)	0, 1	Update the above ddns settings to take effect

Group: **UPNP**

NAME	VALUE	DESCRIPTION
enable (r/w)	0, 1	Enable or disable the UPNP presentation service. **<1>**

Group: **UPNPfor**

NAME	VALUE	DESCRIPTION
enable (r/w)	0, 1	Enable or disable the UPNP port forwarding service. **<0>**

Group: **App**

NAME	VALUE	DESCRIPTION
scriptname (r)	<text string shorter than 255 characters>	File name of script **<script.vssx>**
enablescript (r/w)	0	Disable script
	1	Enable script

Group: **Syslog**

NAME	VALUE	DESCRIPTION
enableremotelog (r/w)	**0**	disable remote log
	1	enable remote log
serverip (r/w)	**<IP address>**	Log server IP address
serverport (r/w)	**<514>**	Server port used for log

Application page CGI command

Note: This request requires administrator privilege.
Method: GET/POST

Syntax (For snapshot):

```
http://<servername>/cgi-bin/admin/gen-new-eventd-conf.cgi?
[<prefix_app_index>_snapshot_enable=<value>]
[&<prefix_app_index>_weekday=<value>]
[&<prefix_app_index>_time_method=<value>]
[&<prefix_app_index>_begin_time=<value>]
[&<prefix_app_index>_end_time=<value>]
[&<prefix_app_index>_prefix=<value>]
[&<prefix_app_index>_trigger_type=<value>]
[&<prefix_app_index>_md_win=<value>]
[&<prefix_app_index>_md_prenum=<value>]
[&<prefix_app_index>_md_postnum=<value>]
[&<prefix_app_index>_md_delay=<value>]
[&<prefix_app_index>_sq_interval=<value>]
[&<prefix_app_index>_send_method=<value]
[&<prefix_app_index>_ftp_suffix=<value>]
```

Syntax (For videoclip):

```
http://<servername>/cgi-bin/admin/gen-new-eventd-conf.cgi?
[<prefix_app_index>_videoclip_enable=<value>]
[&<prefix_app_index>_weekday=<value>]
[&<prefix_app_index>_time_method=<value>]
[&<prefix_app_index>_begin_time=<value>]
[&<prefix_app_index>_end_time=<value>]
[&<prefix_app_index>_prefix=<value>]
[&<prefix_app_index>_trigger_type=<value>]
[&<prefix_app_index>_maxsize=<value>]
[&<prefix_app_index>_md_win=<value>]
[&<prefix_app_index>_md_delay=<value>]
[&<prefix_app_index>_sq_interval=<value>]
[&<prefix_app_index>_send_method=<value>]
[&<prefix_app_index>_ftp_suffix=<value>]
```

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
Application page contents
```

parameter	Value	description
prefix_app_index	sn1, sn2, vc	Index of application
snapshot_enable	0	Enable snapshot application
	1	Disable snapshot application
videoclip_enable	0	Disable videoclip application
	1	Enable videoclip application
weekday	*0,1,2,3,4,5,6*	The array indicate weekly schedule
time_method	*always*	24 hours full day
	interval	Select begin time and end time
begin_time	*hh:mm*	Begin time of weekly schedule
end_time	*hh:mm*	End time of weekly schedule
prefix	*<text string shorter than 60 characters>*	Snapshot/Videoclip file name prefix for both event and sequential operation

trigger_type	*motion*	Set trigger by motion detect
	sequential	Snapshot/Videoclip sequentially
maxsize	*0~500*	Video clip max file size
md_win	*0,1,2*	The array indicate which motion windows are used
md_prenum	*1~5*	The numbers of snapshot before event
md_postnum	*1~5*	The numbers of snapshot after event
md_delay	*1~999*	The delay seconds for detecting next motion event
sq_interval	*1~999*	The interval seconds of sequential snapshot
send_method	*mail*	Send snapshot by mail
	ftp	Send snapshot by ftp
ftp_suffix	*0/1*	Enable/Disable file name prefix

Capture single snapshot

Note: This request require normal user privilege
Method: GET/POST

Syntax:

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

Server will return the most up-to-date snapshot in JPEG format. The size and quality of 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>
```

Account management

Note: This request requires administrator privilege
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 server. When using this method, "username" field is necessary. It will use default value of other fields if not specified.
	delete	Remove an account from server. When using this method, "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, "username" field is necessary, and other fields are optional. If not specified, it will keep original settings.
username	<name>	The name of user to add, delete or edit
userpass	<value>	The password of new user to add or that of old user to modify. The default value is an empty string.
privilege	<value>	The privilege of user to add or to modify. The privilege can be the addition of the following values. Ex: A user with configure access can be assigned privilege as **privilege=conf**.
	conf	configuration 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 the the current path. If you omit this parameter, it will redirect to an empty page.

System logs

Note: This request require administrator privilege
Method: GET/POST

Syntax:

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

Server will return the 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
```

Configuration file

Note: This request requires administrator privilege
Method: GET/POST

Syntax:

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

Server will return the up-to-date configuration file.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <configuration file length>\r\n
\r\n
<configuration data>\r\n
```

Upgrade firmware

Note: This request requires administrator privilege
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 upload file named <file name> to be upgraded the firmware and return with <return page> if indicated.

D. Technical specifications

Specifications

Models
- IP7135 (Wired)
- IP7137 (WLAN)

System
- CPU: VVTK-1000 SoC
- FLASH: 4MB
- RAM: 32MB SDRAM
- Embedded OS: Linux 2.4

Lens
- Board lens, f=4.0 mm, F2.0, Fixed

Shutter Time
- 1/60 sec. to 1/15000 sec.

Image Sensor
- 1/4" CMOS senser in VGA resolution

Minimum Illumination
- 1.5 Lux/F2.0

Video
- Compression:
  MPEG-4 for streaming video.
  JPEG for still image.
- Streaming:
  MPEG-4 streaming over UDP, TCP, or HTTP
- Supports 3GPP mobile surveillance
- Frame rates:
  MPEG-4: Up to 30/25 fps at 640x480

Image Settings
- Adjustable image size, quality, and bit rate
- Time stamp and text caption overlay
- Flip & mirror
- Configurable brightness, saturation, contrast and sharpness
- AGC, AWB, AES

Audio
- Compression:
  GSM-AMR speech compression, bit rate: 4.75 kbps ~12.2 kbps
  MPEG-4 AAC audio encoding, bit rate: 16 kbps ~32 kbps
- Interface: Built-in microphone
- Supports audio mute

Networking
- 10/100 Mbps Ethernet, RJ-45
- Protocols: IPv4, TCP/IP, HTTP, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP,DHCP, NTP, DNS, DDNS, and PPPoE

Alarm and Event Management
- Triple-window video for motion detection
- Event notification using HTTP, SMTP, or FTP

Security
- User access with password protection
- IP address filtering

Users
- Camera live viewing for up to 10 clients

Dimensions
- 34.8 mm (D) x109.5 mm (W) x 77.2 mm (H)

Weight
- Net: 150 g (IP7135)
- Net: 165 g (IP7137)

LED Indicator
- System power and status indicator
- System activity and network link indicator
- Microphone status indicator

Power
- 5V DC
- Power consumption: 2.6 W (IP7135)
- Power consumption: 3.7 W (IP7137)

Approvals
- CE, FCC

Operating Environments
- Temperature: 0° ~ 50° C (32° ~ 122° F)
- Humidity: 20 % ~ 80 % RH

Viewing System Requirements
- OS: Microsoft Windows 2000/XP/Vista
- Browser: Mozilla Firefox, Internet Explorer 6.x or above
- Cell phone: 3GPP player
- Real Player: 10.5 or above
- Quick Time: 6.5 or above

Installation, Management, and Maintenance
- Installation Wizard 2
- 16-CH recording software
- Supports firmware upgrade

Applications
- SDK available for application development and system integration

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 REGARD TO PC SOFTWARE, YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

MPEG-4 Visual Technology

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

AMR-NB Standard

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

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

Electromagnetic Compatibility (EMC)

FCC Statement

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

■ This device may not cause harmful interference, and

■ This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class 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 CE

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 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 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 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.