

Indoor · 3-axis · PoE · PIR

FD7131

# NETWORK CAMERA *User's Manual*



## **Table of Contents**

---

|   |           |
|---|-----------|
| <b>Overview</b> .....                     | <b>3</b>  |
| Read Before Use.....                      | 3         |
| Package Contents.....                     | 3         |
| Physical Description.....                 | 4         |
| <b>Installation</b> .....                 | <b>6</b>  |
| Hardware Installation.....                | 6         |
| Network Deployment.....                   | 9         |
| Software Installation.....                | 12        |
| <b>Accessing the Network Camera</b> ..... | <b>13</b> |
| Using Web Browsers.....                   | 13        |
| Using RTSP Players.....                   | 15        |
| Using 3GPP-compatible Mobile Devices..... | 16        |
| Using VIVOTEK Recording Software.....     | 17        |
| <b>Main Page</b> .....                    | <b>18</b> |
| <b>Client Settings</b> .....              | <b>22</b> |
| <b>Configuration</b> .....                | <b>24</b> |
| System.....                               | 25        |
| Security.....                             | 27        |
| HTTPS.....                                | 28        |
| Network.....                              | 33        |
| DDNS.....                                 | 44        |
| Access List.....                          | 46        |
| Audio and Video.....                      | 49        |
| Motion Detection.....                     | 55        |
| Application.....                          | 61        |
| Recording.....                            | 74        |
| System Log.....                           | 77        |
| View Parameters.....                      | 78        |
| Maintenance.....                          | 79        |
| <b>Appendix</b> .....                     | <b>83</b> |
| URL Commands for the Network Camera.....  | 83        |
| Technical Specifications.....             | 120       |
| Technology License Notice.....            | 121       |
| Electromagnetic Compatibility (EMC).....  | 122       |

# Overview

VIVOTEK FD7131 is a full-featured 3-axis dome network camera designed for indoor surveillance. It comes with a wide-angle, vari-focal lens, allowing you to have a wide open view for maximum coverage. With the sophisticated 3-axis mechanical and industrial design, it offers a very flexible, easy hardware installation for either ceiling or wall mount. To prevent false alarms, it is also equipped with a PIR (Passive Infrared) sensor, which can detect motion causing temperature changes in the infrared range emitted by surrounding objects. When the environment is short of sufficient light source, the built-in white-light illuminators will be activated automatically or manually so as to supplement the low light situation without additional equipment. Embedded with VIVOTEK VVTK-1000 SoC, it simultaneously delivers dual streams with different resolutions up to 30fps in VGA resolution and video qualities upon different multimedia devices for real-time viewing. Additionally, by offering more advanced features such as 3GPP mobile surveillance, built-in 802.3af compliant PoE, two-way audio, and so on, FD7131 allows users to build up a powerful, cost-effective IP surveillance system for various indoor applications with ease.

## Read Before Use

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

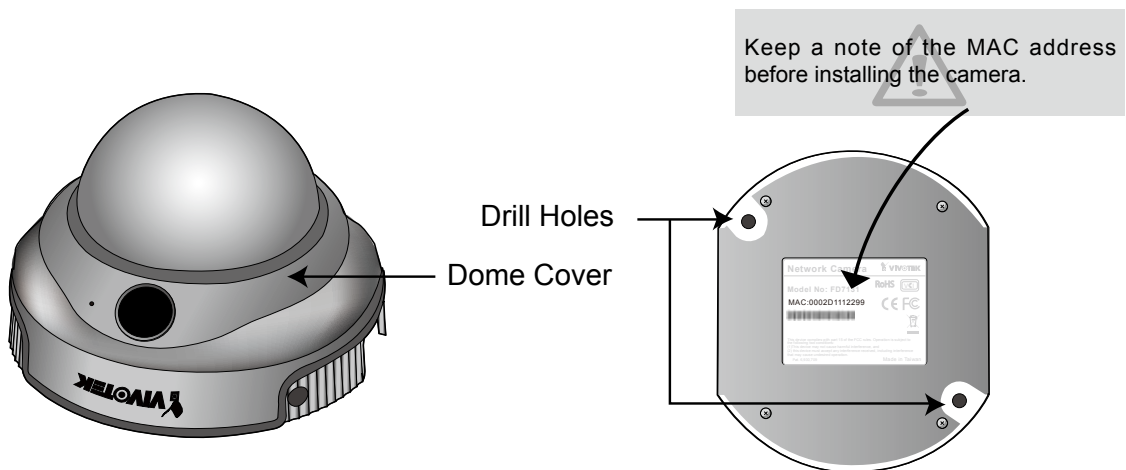
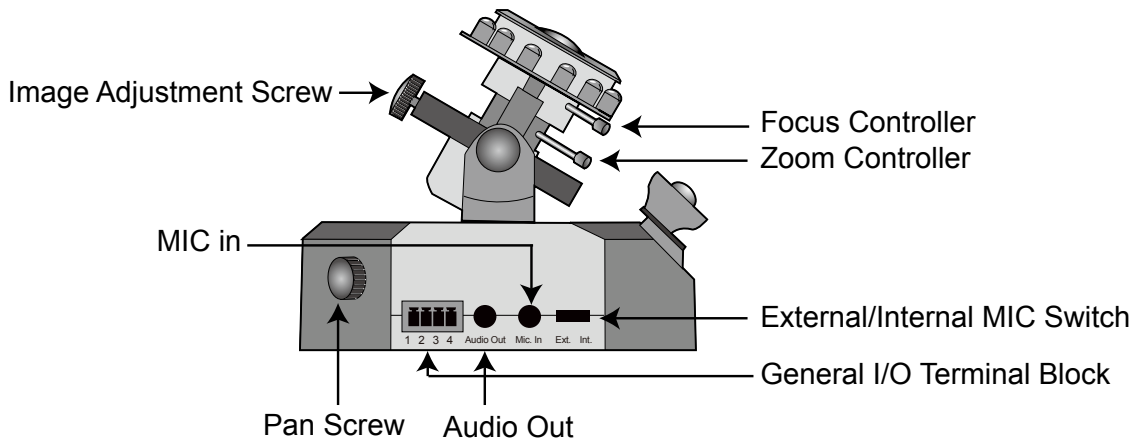
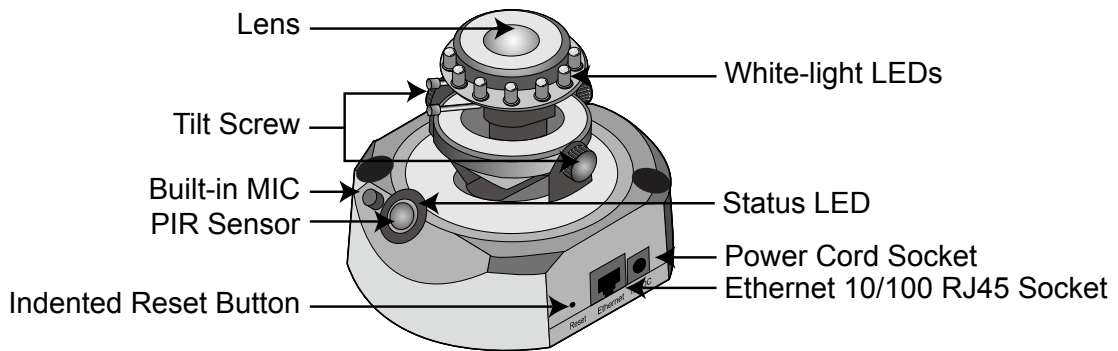
It is important to first verify that all contents received are complete according to the Package Contents listed below. Take note of the warnings in the Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid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

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

## Package Contents

- FD7131
- Power Adapter
- Software CD
- Alignment Sticker
- Warranty Card
- Quick Installation Guide
- Screwdriver
- Screws and I/O Connector

## Physical Description



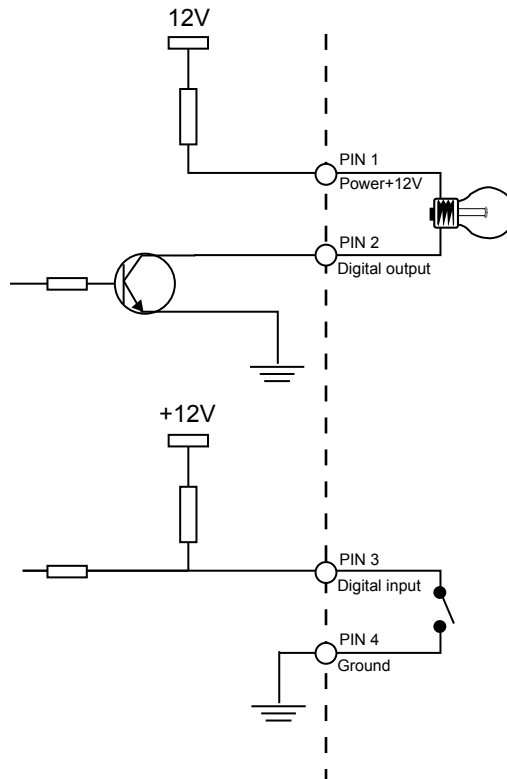
### General I/O Terminal Block

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



## DI/DO Diagram

Refer to the following illustration for the connection method.

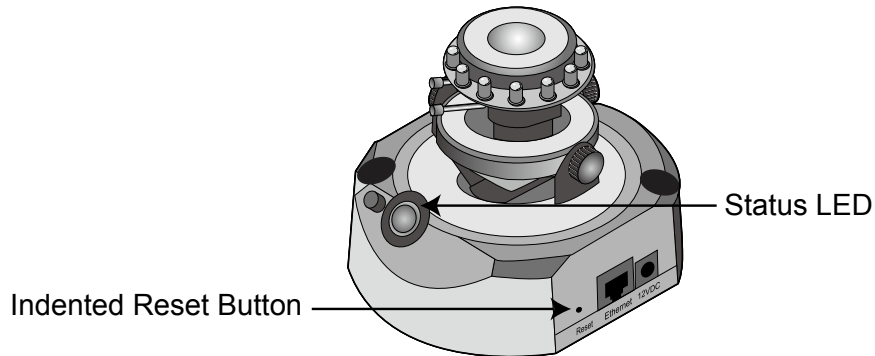


## Status LED

The LED indicates the status of the Network Camera.

| Description                                    | Status LED                          |
|--|-------------------------------------|
| Blinking green and orange (twice)              | Power on or reset                   |
| Non light                                      | During booting procedure            |
| Steady orange till IP address is confirmed     | Detecting and setting network       |
| Blinking orange and red continuously           | After network is setup (system up)  |
| Rapidly blink orange till firmware is upgraded | During the upgrade firmware process |

## Hardware Reset



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

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

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

## Installation

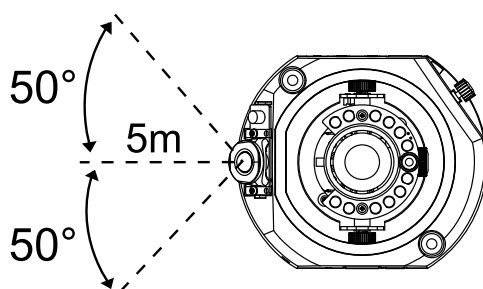
### Hardware Installation

1. Use the supplied screwdriver to detach the dome cover from the camera base. Then, follow the steps below to install the camera; either to a ceiling or to a wall.

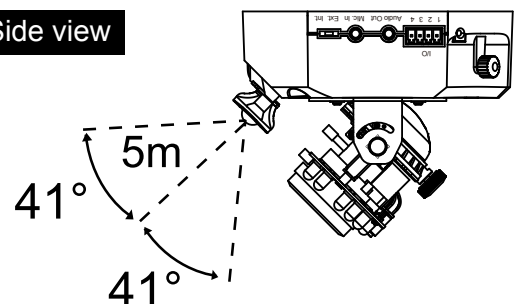
#### Installation Tips

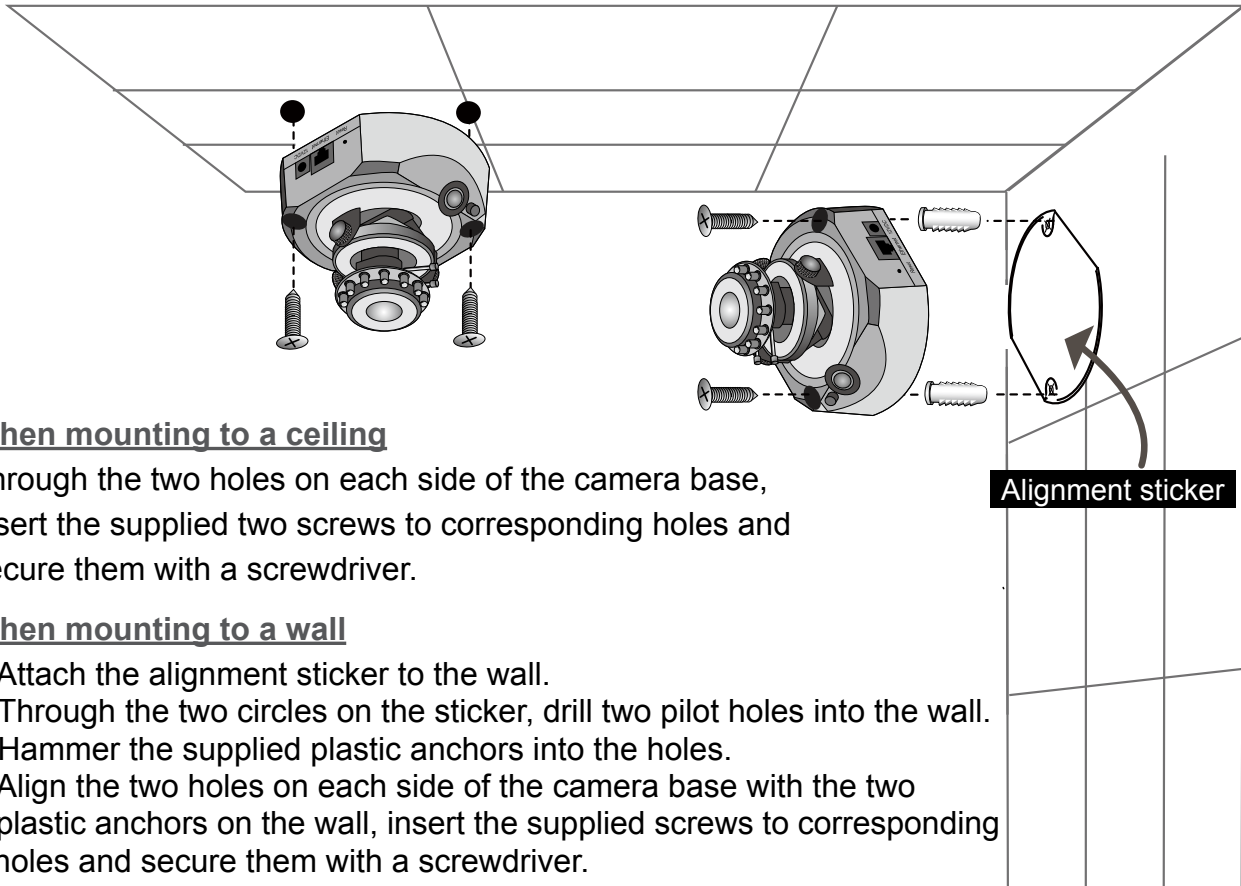
Before installing the camera, look for a spot that best suits your needs. The built-in PIR sensor is designed to be triggered when a person enters its detection range. Therefore, it is crucial to install the camera at a place with the PIR sensor facing the desired direction. (The sensitivity of PIR sensor depends on object size and temperature differences between the object and the background environment.)

Top view



Side view





### When mounting to a ceiling

Through the two holes on each side of the camera base, insert the supplied two screws to corresponding holes and secure them with a screwdriver.

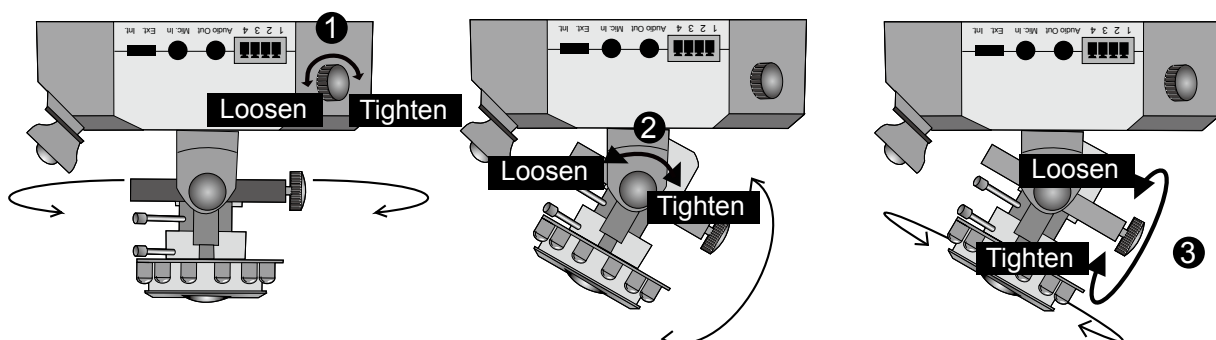
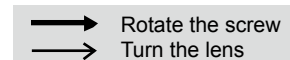
### When mounting to a wall

- Attach the alignment sticker to the wall.
- Through the two circles on the sticker, drill two pilot holes into the wall.
- Hammer the supplied plastic anchors into the holes.
- Align the two holes on each side of the camera base with the two plastic anchors on the wall, insert the supplied screws to corresponding holes and secure them with a screwdriver.

3. Feed power to the Network Camera and connect it to the Internet. For more information, please refer to Network deployment on page 9 for details.
4. Install the "Installation Wizard 2" to assign IP address to the Network Camera. For more information, please refer to Software installation on page 12 for details.
5. Access to the Network Camera from the Internet. For more information, please refer to Accessing the Network Camera on page 13 for details.
6. Based on the live image retrieved from the camera, adjust the camera lens as following steps.

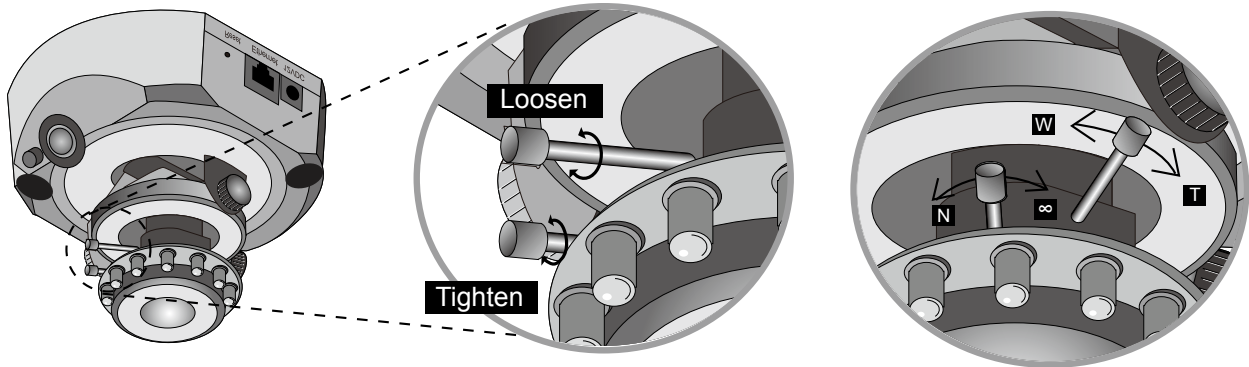
### To adjust the viewing angle

- Loosen the pan screw, then turn the lens module left and right. Upon completion, tighten the pan screw.
- Loosen the tilt screws on both side of the camera, then turn the lens module up and down. Upon completion, tighten the tilt screws.
- Loosen the image adjustment screw, then turn the lens to adjust the image orientation. Upon completion, tighten the image adjustment screw.



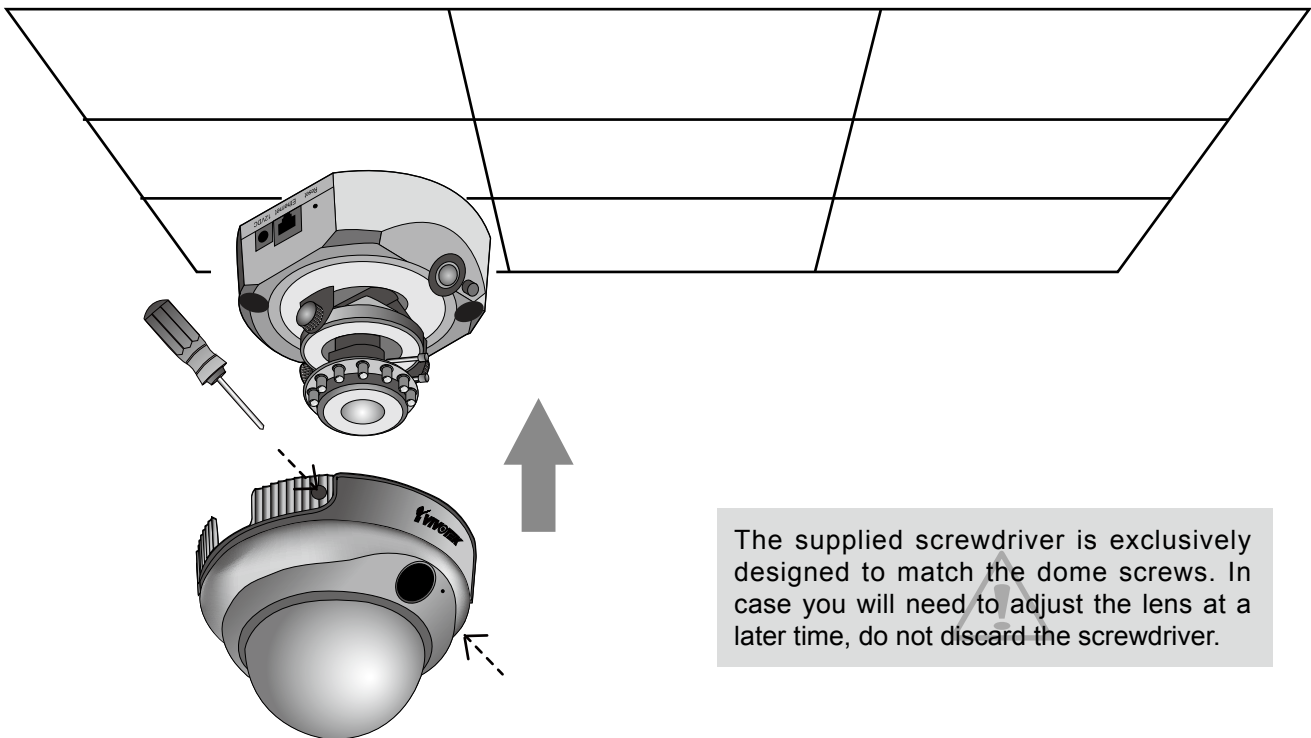
**To adjust the zoom factor and focus range**

- Loosen the zoom controller, then adjust zoom factor by moving the controller left and right. Upon completion, tighten the zoom controller.
- Loosen the focus controller, then adjust focus range by moving the controller left and right. Upon completion, tighten the focus controller.



DO NOT over tighten the controllers. Doing so can damage the structure of camera lens.

7. Attach the dome cover to camera. Secure the two dome screws with a screwdriver. Finally, make sure all parts of the camera are securely installed.



The supplied screwdriver is exclusively designed to match the dome screws. In case you will need to adjust the lens at a later time, do not discard the screwdriver.

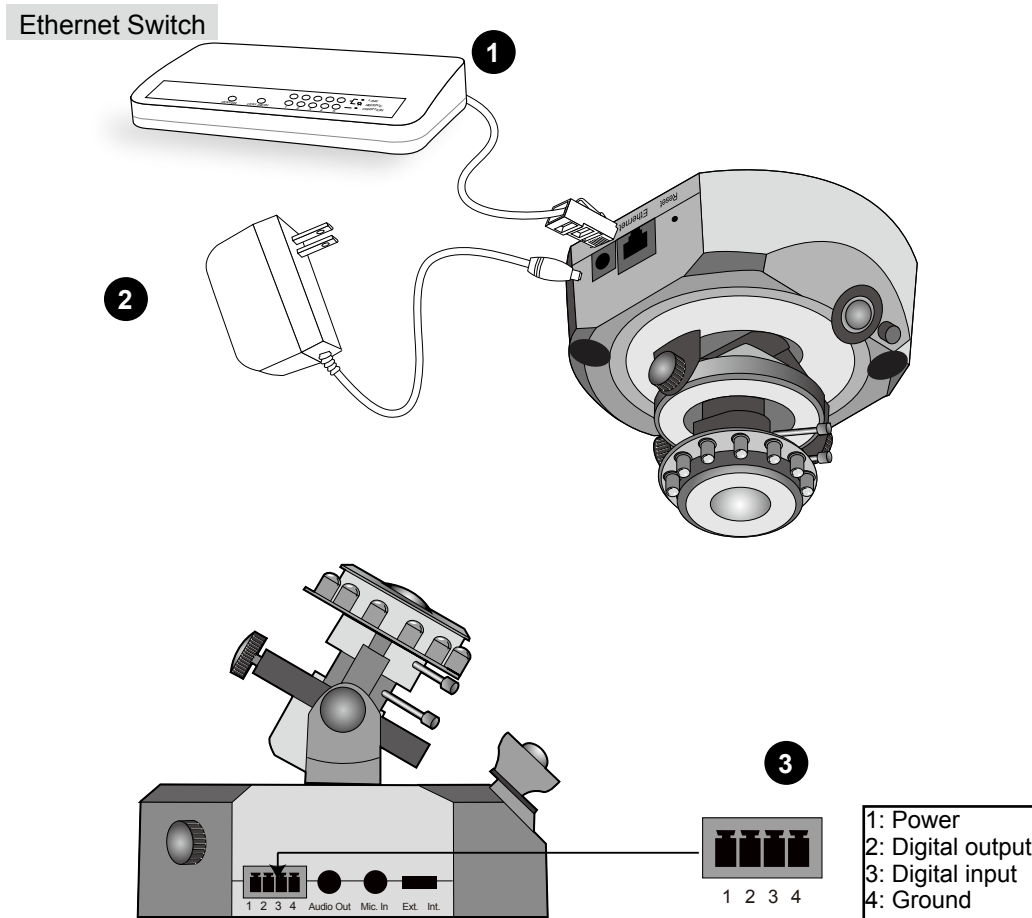


## Network Deployment

### Setting up the Network Camera over the Internet

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

1. If you have external devices such as sensors and alarms, make the connection from the general I/O terminal block.
2. Connect the camera to a switch via Ethernet cable.
3. Connect the supplied power cable from the Network Camera to a power outlet.

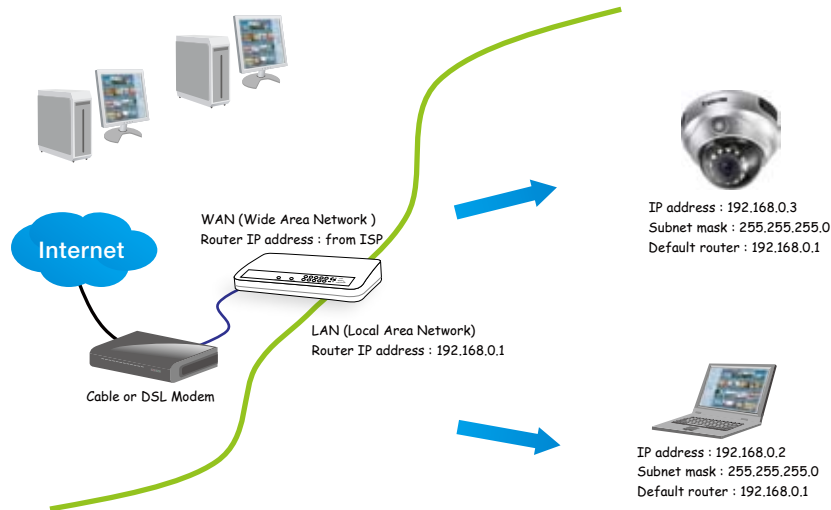


There are several ways to set up the Network Camera over the Internet. The first way is to set up the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

### 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 33 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 33 for details.

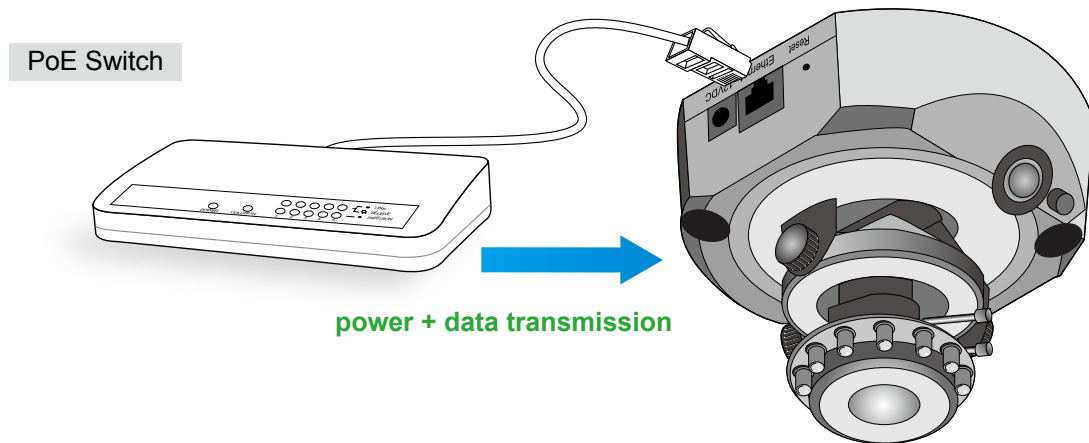
### **Internet connection via PPPoE (Point-to-Point over Ethernet)**

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 34 for details.

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

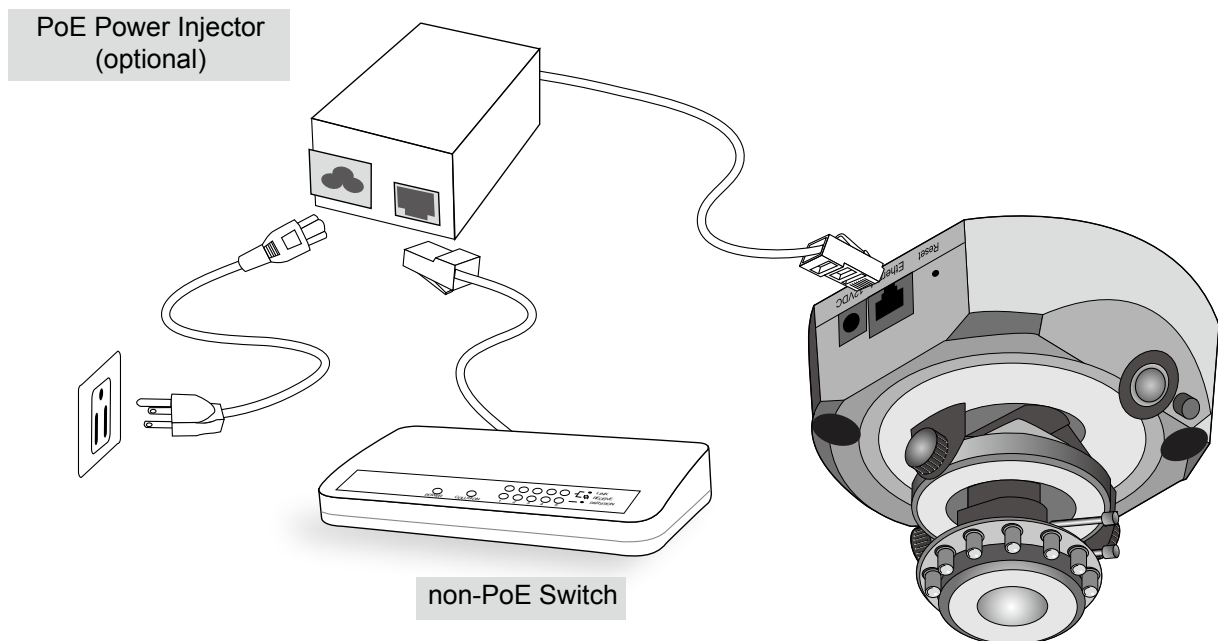
### When using a PoE-enabled switch

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

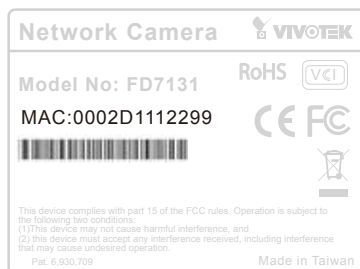


2. The program will conduct an analysis of your network environment.  
After your network environment is analyzed, please click **Next** to continue the program.



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

4. After searching, the main installer window will pop up. Click on the MAC and model name which matches the product label on your device to connect to the Network Camera via Internet Explorer.



# Accessing the Network Camera

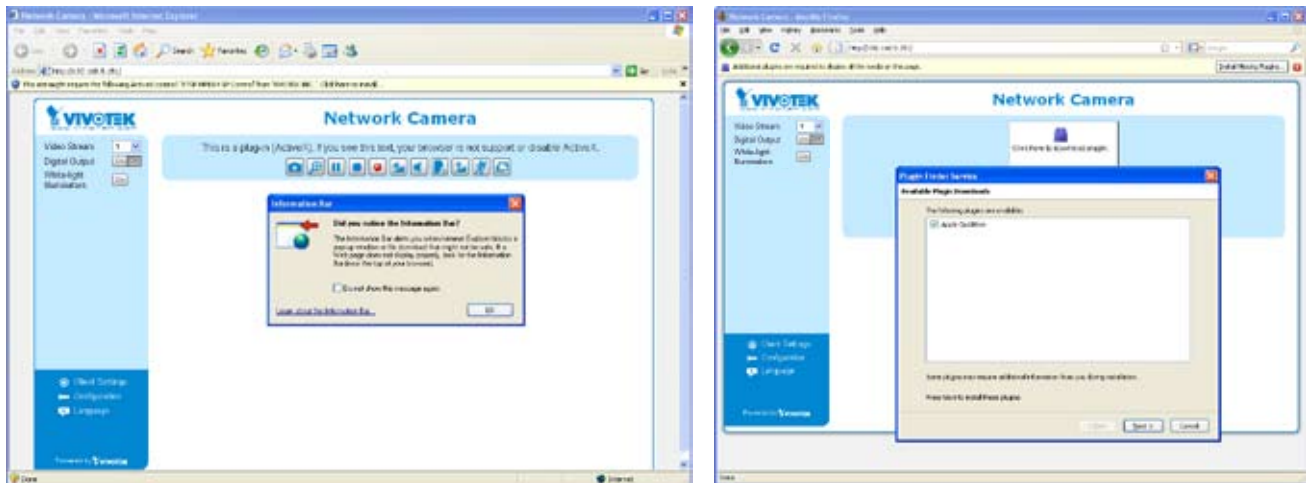
This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

## Using Web Browsers

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

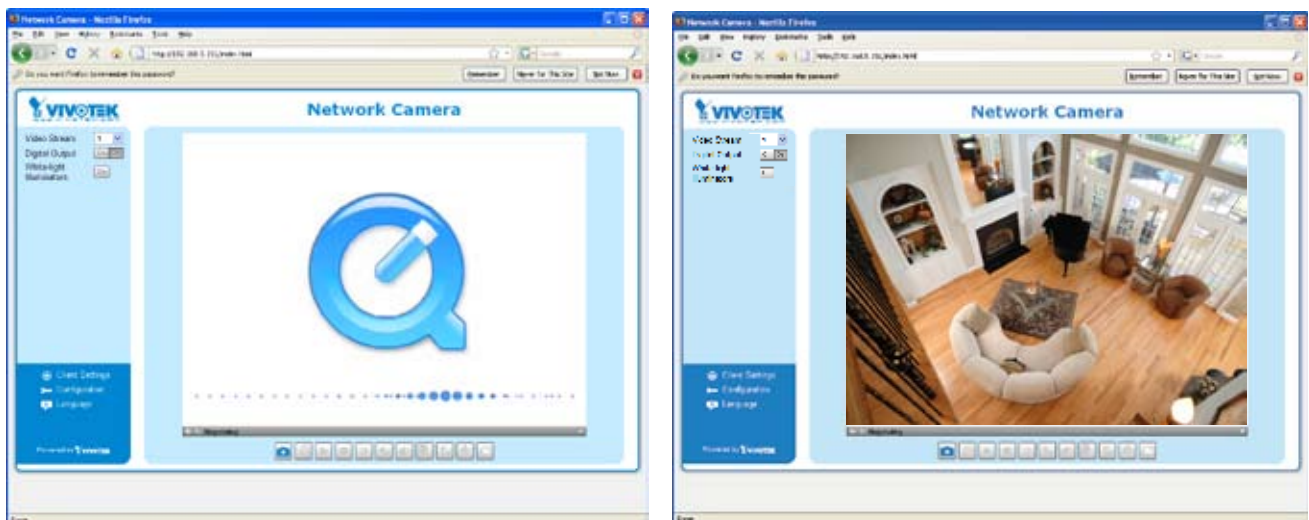
If your network environment is not a LAN, follow these steps to access the Network Camera:

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



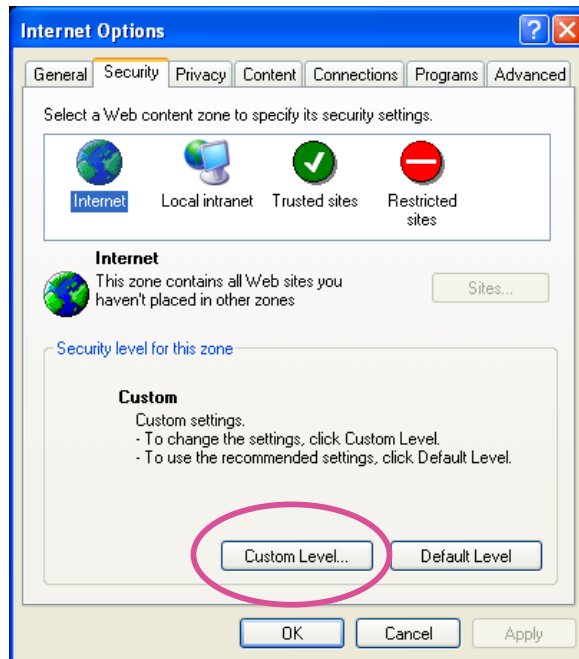
### **NOTE**

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

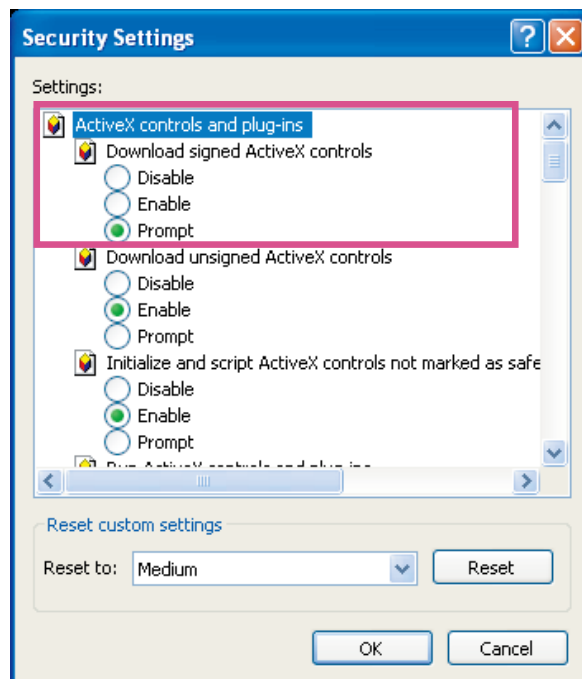


- ▶ *By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera. For more information about how to enable password protection, please refer to Security on page 27.*
- ▶ *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable your 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.

## Using RTSP Players

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



Quick Time Player

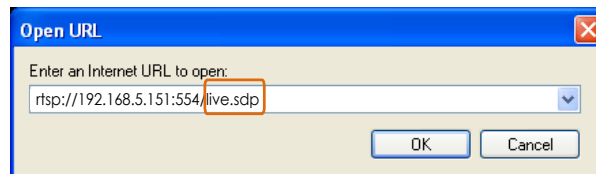


Real Player

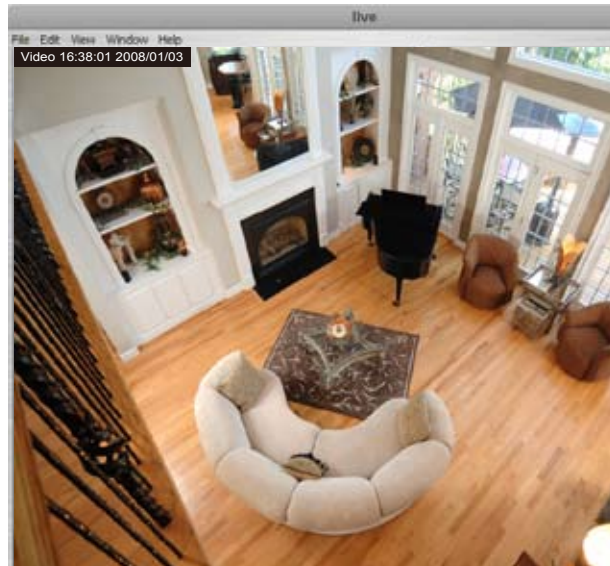
1. Launch the RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. The address format is `rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>`

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 42.

For example:



4. The live video will be displayed in your player.  
For more information on how to configure RTSP access name, please refer to RTSP Streaming on page 42 for details.



## Using 3GPP-compatible Mobile Devices

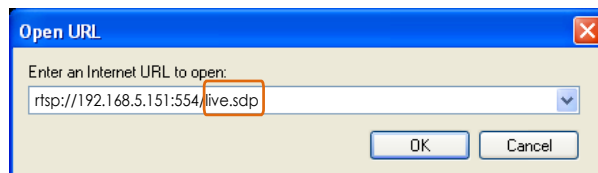
To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 9.

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 disable.  
For more information, please refer to RTSP Streaming on page 42.
2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video and audio streaming parameters as listed below.  
For more information, please refer to Audio and Video on page 49.

|                                   |           |
|-----------------------------------|-----------|
| 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 42.
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 or stream2>`.  
For example:





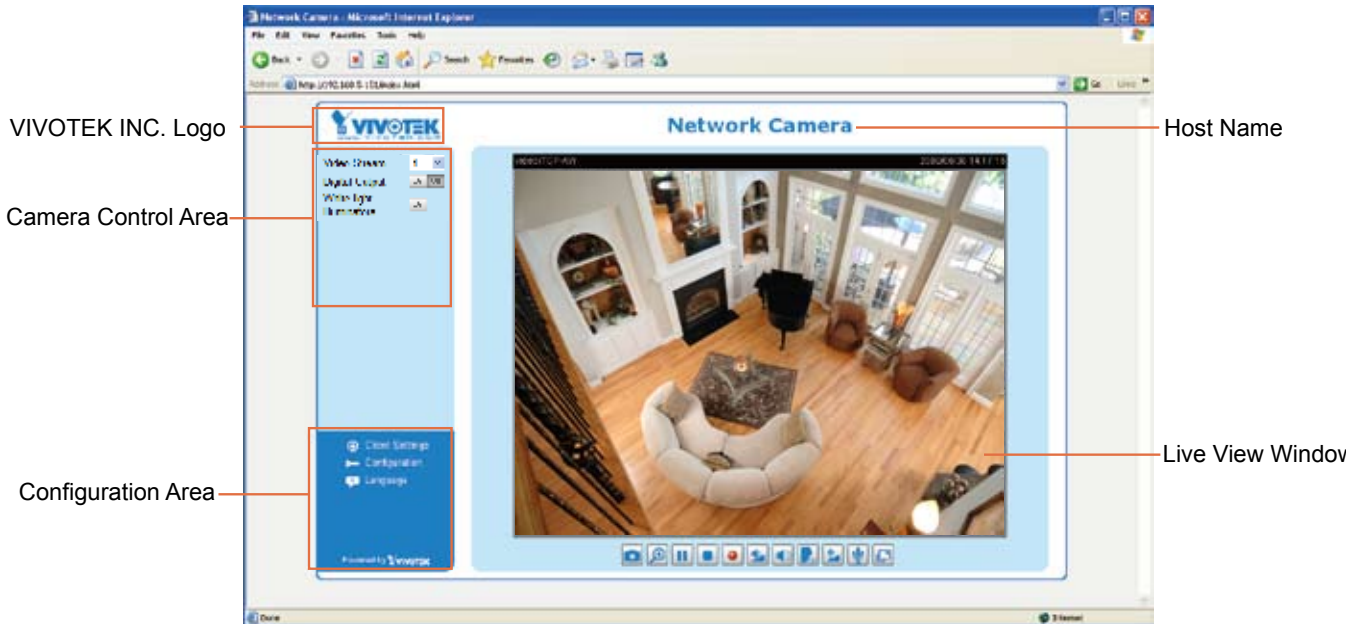
## Using VIVOTEK Recording Software

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



# Main Page

This chapter explains the layout of the main page. It is composed of the following sections: VIVOTEK INC. Logo, Host Name, Camera Control Area, Configuration Area, Menu, and Live Video Window.



## VIVOTEK INC. Logo

Click this logo to visit VIVOTEK website.

## Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page 25.

## Camera Control Area

Video Stream: This Network Camera supports MJPEG or MPEG-4 dual streams simultaneously. You can select either one for live viewing.

Digital Output: Click to turn the digital output device on or off.

White-light illuminators: Click to turn on the White-light LEDs for 20 seconds.

## Configuration Area

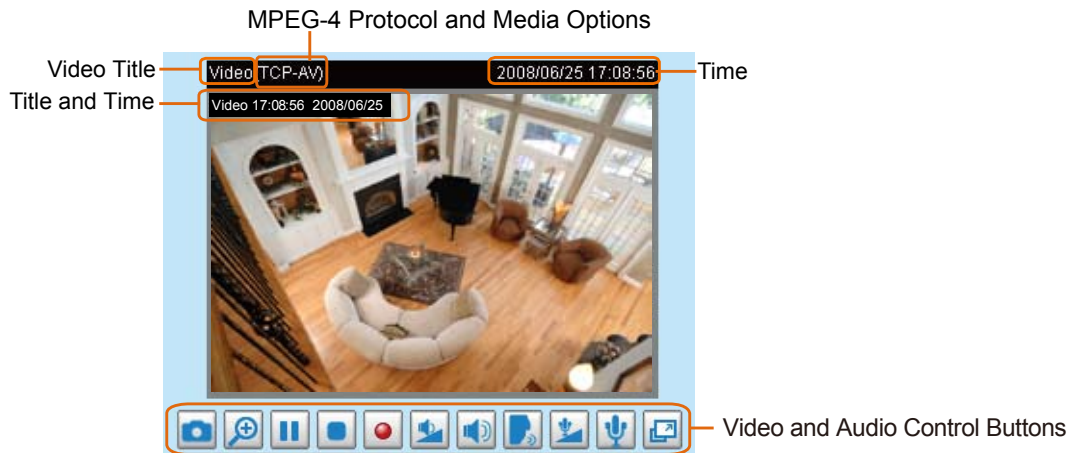
Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 22.

Configuration: Click this button to access the configuration page of the 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 24.

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

## Live Video Window

- The following window is displayed when the video mode is set to MPEG-4:




**Video Title:** The video title can be configured. For more information, please refer to Video Settings on page 49.


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

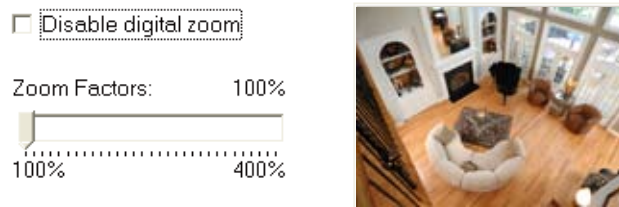
**Time:** Display the current time. For further configuration, please refer to Video settings on page 49.



**Title and Time:** Video title and time can be stamped on the streaming video. For further configuration, please refer to Video settings on page 49.



**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 which part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.







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



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




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


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

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

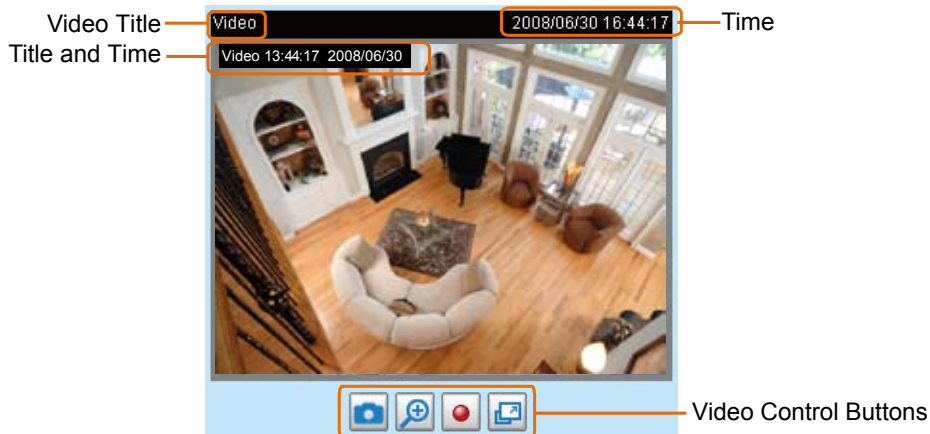
 **Talk:** Click this button to talk to people around the Network Camera. Audio will project from the external speaker connected to the Network Camera. Click this button  again to end talking transmission.

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

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

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

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





**Video Title:** The video title can be configured. For more information, please refer to Video Settings on page 49.

**Time:** Display the current time. For more information, please refer to Video Settings on page 49.

**Title and Time:** Video title and time can be stamped on the streaming video. For more information, please refer to Video Settings on page 49.

**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.

Disable digital zoom

Zoom Factors: 100%



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

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

# Client Settings

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

## MPEG-4 Media Options

**MPEG-4 Media Options**

Video and Audio

Video Only

Audio Only

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

## MPEG-4 Protocol Options

**MPEG-4 Protocol Options**

UDP Unicast

UDP Multicast

TCP

HTTP

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

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

**UDP multicast:** This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps 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, see RTSP Streaming on page 34.

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

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


## MP4 Saving Options

**MP4 Saving Options**

Folder:

File name prefix:

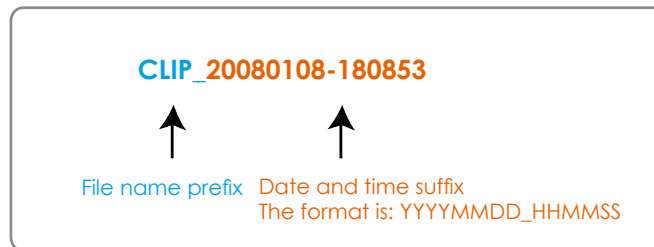
Add date and time suffix to file name

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

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

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

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



# Configuration

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

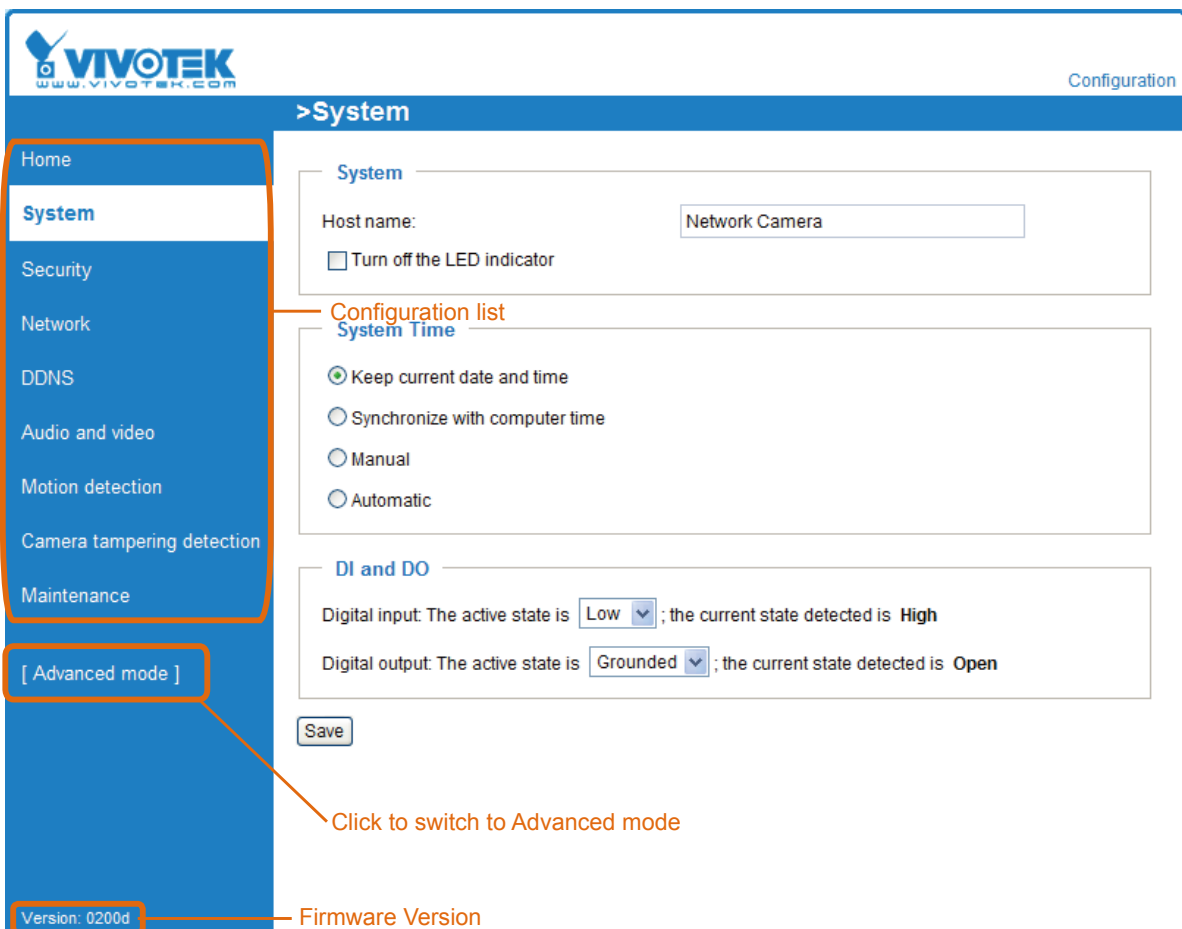
VIVOTEK offers an easy-to-use user interface that helps you set up your network camera with minimal effort. To simplify the setting procedure, two types of user interfaces are available: Advanced Mode for professional users and Basic Mode for entry-level users. Some advanced functions (ex. HTTPS/ Access 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 subitem will be displayed; when you click on the second sub-item, the detailed information for the second sub-item will be displayed and that of the first sub-item will be hidden.

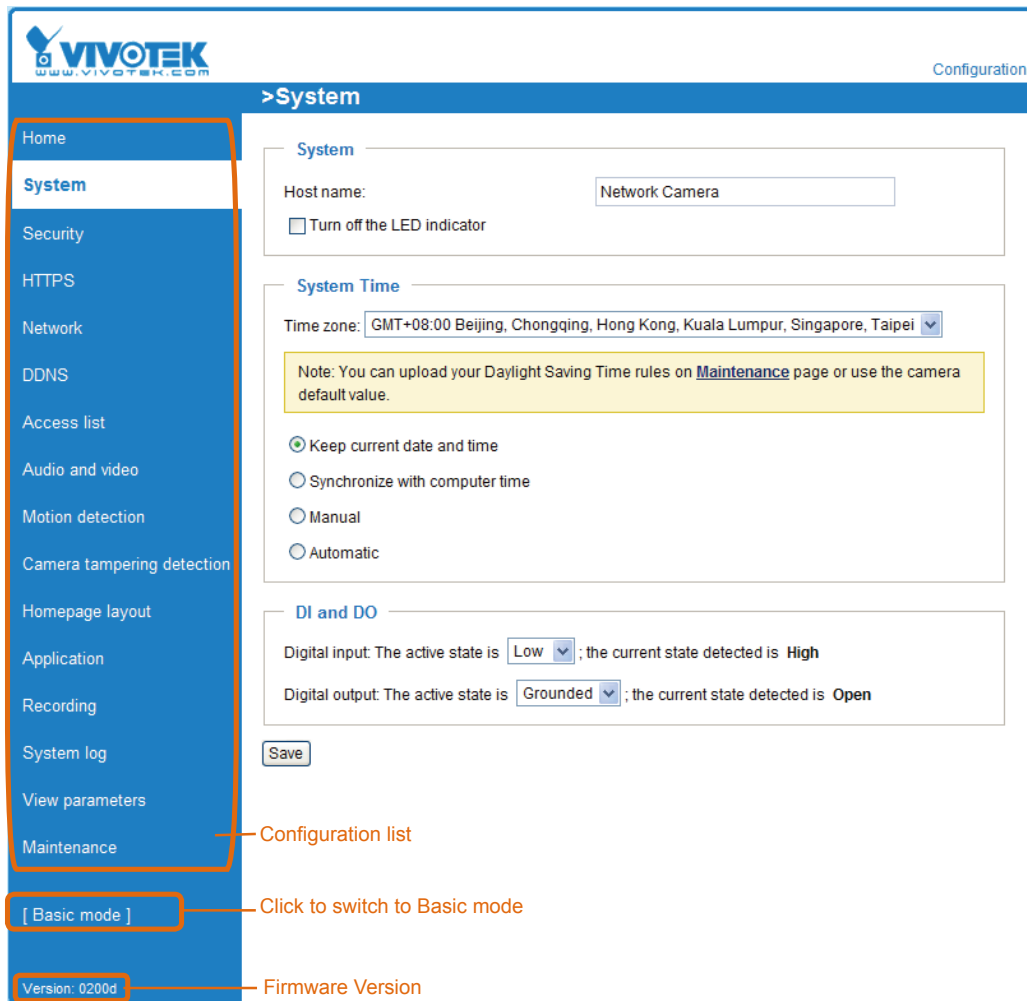
The following is the interface of the Basic Mode and the Advanced Mode:

## Basic mode





## Advanced Mode



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

## System

This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following three columns: System, System Time and DI and DO. 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 a 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 don't want to let others know that the network camera is working, you can select this option to turn off the LED indicators.

## System Time

**System Time**

Time zone: GMT+08:00 Beijing, Chongging, 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 power of the system is turned off.

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

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

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

**NTP server:** Assign the IP address or domain name of 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 80 for details.

## DI and DO

**DI and DO**

Digital input: The active state is Low ▼ ; the current state detected is **High**

Digital output: The active state is Grounded ▼ ; the current state detected is **Open**

**Digital input:** Select High or Low to define normal status of the digital input. The Network Camera will report the current status.

**Digital output:** Select Grounded or Open to define normal status of the digital output. The Network Camera will show whether the trigger is activated or not.

## 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 Manage User column, please apply a password for the “root” account first.

1. Type the password identically in both text boxes, and 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

Digital Output & IR illuminators: 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 18.)

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 settings.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Though operators cannot access the Configuration page, they can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 83. Viewers access only the main page for live viewing.

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

1. Select an existing account to modify.
2. Make necessary changes, then click **Update** or **Delete** to enable the settings.

## 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 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

---

**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

---

**Create and install certificate method**

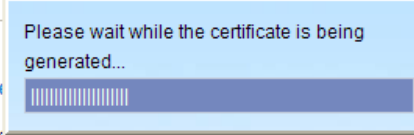
Create self-signed certificate automatically

Create self-signed certificate manually:

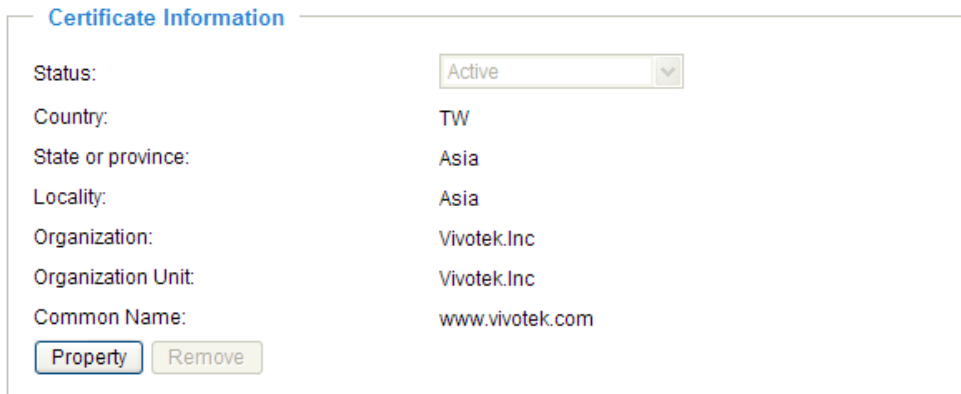
Create certificate request and install:

**Certificate Information**

Status: Not installed

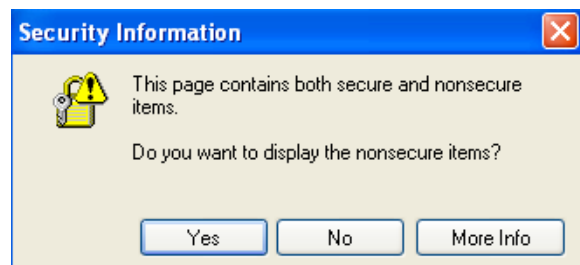
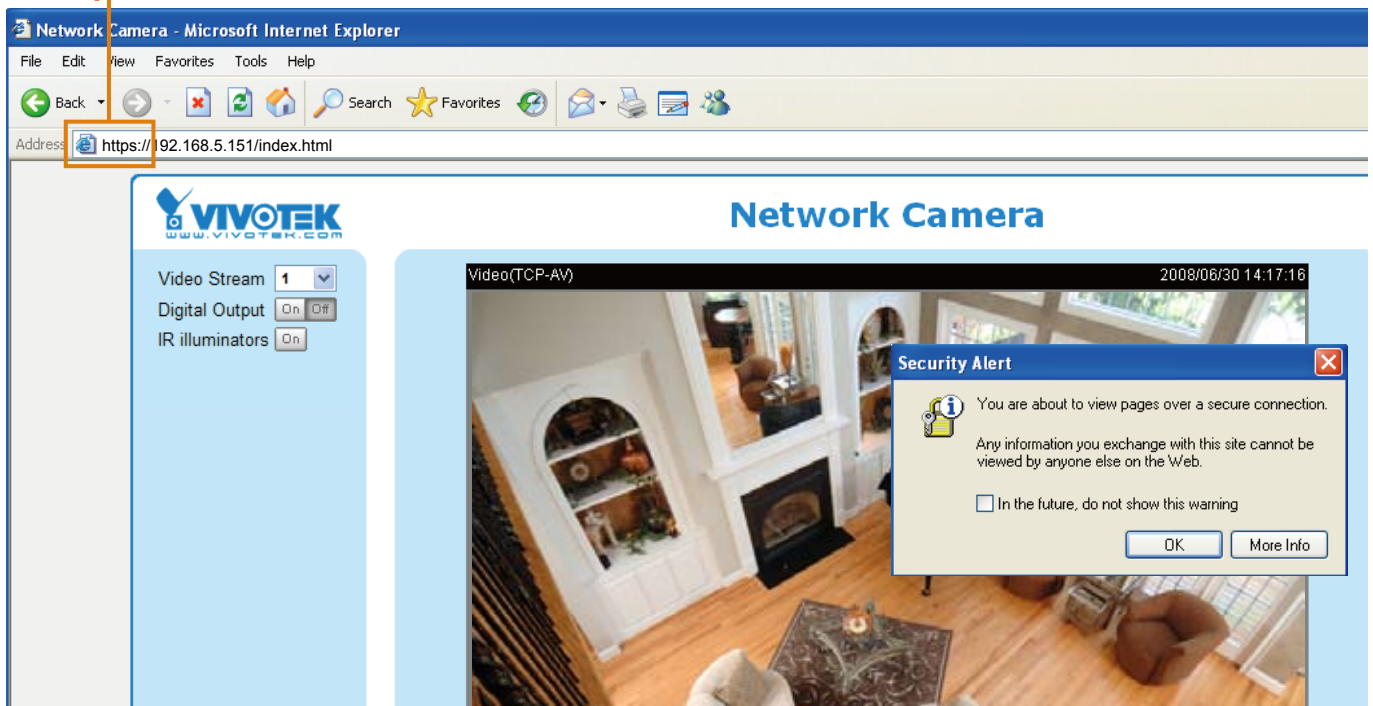


4. The Certificate Information will automatically be displayed in the third column as shown below. You can click **Property** to view detailed information about the certificate.



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://



**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

Please wait while the certificate is being generated...

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

**Certificate Information**

Status:

Country: TW

State or province: Asia

Locality: Asia

Organization: Vivotek.Inc

Organization Unit: Vivotek.Inc

Common Name: www.vivotek.com

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

1. Select this option.
2. Click **Create** to open 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:  
 Create certificate request and install:

Certificate request:

Select certificate file:

**Create Certificate**

Country:

State or province:

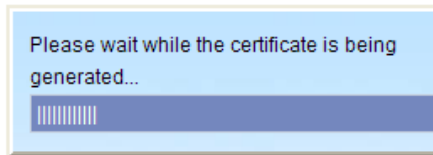
Locality:

Organization:

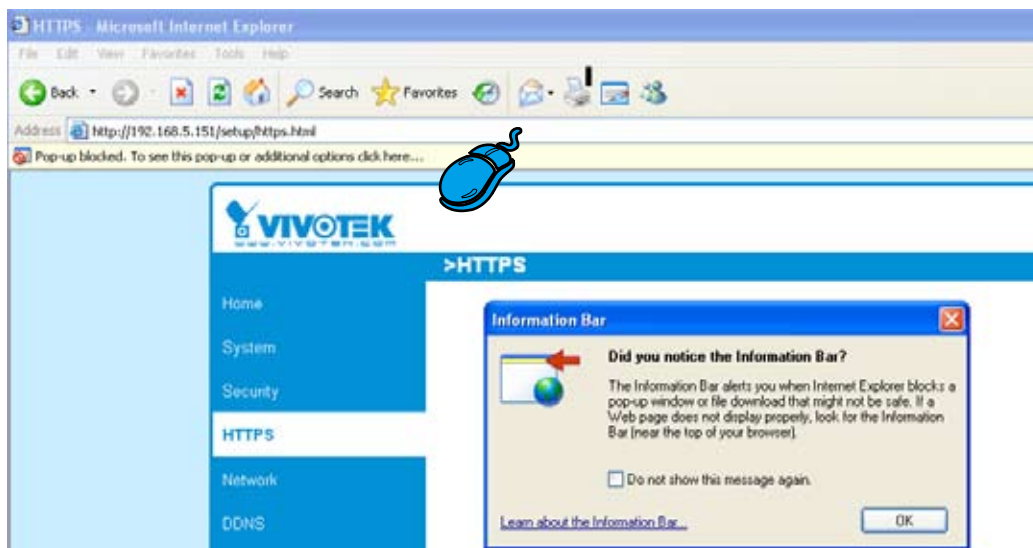
Organization Unit:

Common Name:

Validity:  days



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)**

```

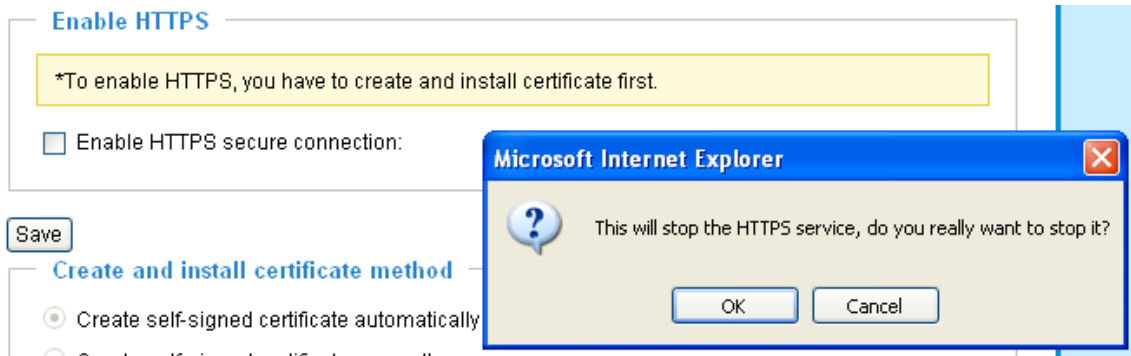
-----BEGIN CERTIFICATE REQUEST-----
MIIBuDCCASECADB5MQswCQYDVQQGEwJVUzERMAsGA1UECBMIUHJvdmluY2UxLjAQ
BgNVBACTCUNpdHkgTmFtZTEaMBGGA1UEChMRMT3JnYW5pemF0aW9uIE5hbWUxLjAQ
BgNVBAsTCVUuaXQgTmFtZTEaMBGGA1UEAxMKSVAgQWRkcmVzcCBnzANBgkqhkiG
9w0BAQEFAAQBjQAwgYkCgYEAuOT75EY52gsSyPFMxZ7wHdQ1obPescsXLUx9DFw6
OMRheukFaXFDkM+5xk+K5oEPBPqj77yhH+zdUHS27fFSLG57bW9SoxrWuLhSvR2W
mCD+//AiJX864dJ/mjHn7Wc55GFaxgMvb&LcxT+hCIeDCWYnRqh/fpKNj+BxvVoN
UrcCAwEAAaAAMAOGCSqGSIb3DQEBBQUAA4GBAAVazW0AtftfU9dyFgTxOYO1D/zO
FOTkbnD0QG18e4ftJ3rROD1TvIIMjg3K8zaAS8Gd3pME1ejqLYoBrtaSqdcUqGIX
50bLG1subWsxR88PngaBwjYoTpG3q1zvUPJZLAVmdL3ne5urTbABXOScCHOQgtH+
PX9dw4OJWkIC8QhV
-----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.

**NOTE**

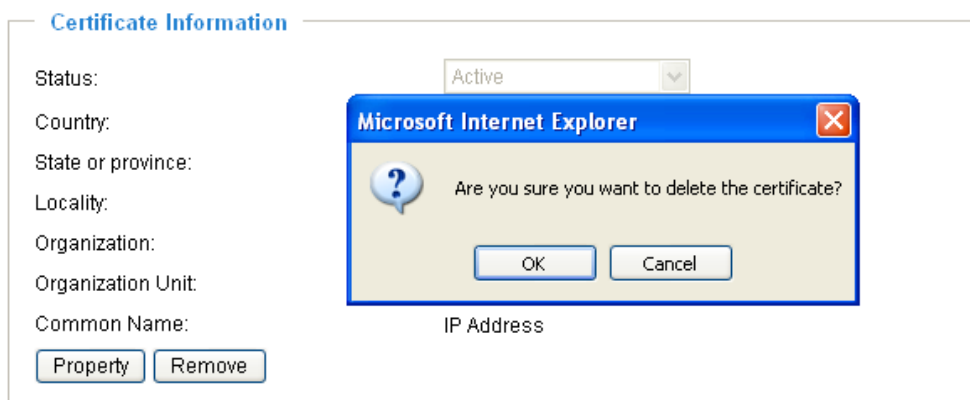
► *How to cancel HTTPS settings?*

1. Uncheck **Enable HTTPS secure connection** in the first column, then click **Save**, then a warning dialog will pop up.
2. Click **OK** to disable HTTPS.



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.*





## Network

This section explains how to configure 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

### LAN

Select this option when the Network Camera is deployed in 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 Settings.

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:

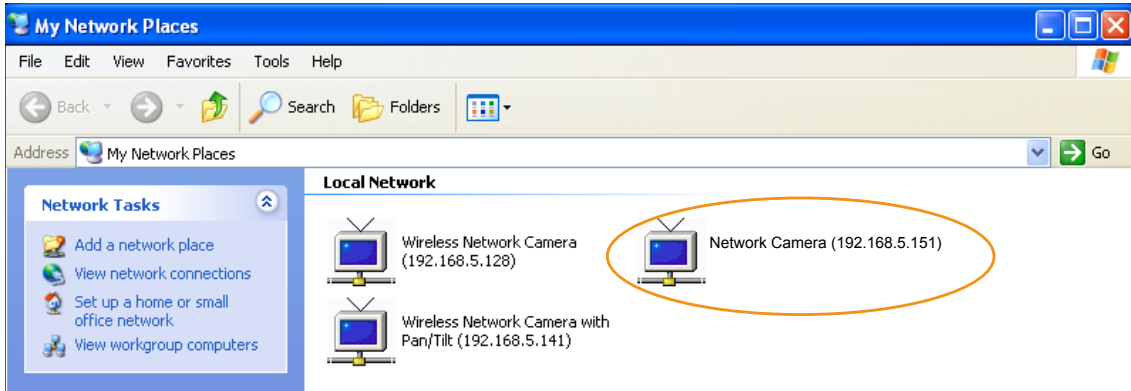
- Enable UPnP presentation
- Enable UPnP port forwarding

PPPoE:

- Enable IPv6

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, 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.

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 67) to add a new server -- email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 70). 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 settings.

**Network Type**

LAN:

PPPoE:

User name:

Password:

Confirm password:

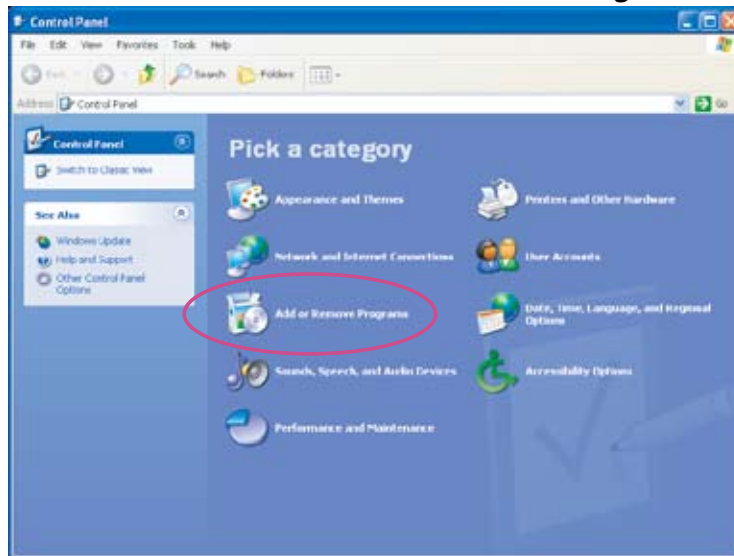
5. The Network Camera will reboot.
6. Disconnect the power to the Network Camera; remove it from the LAN environment.

### **NOTE**

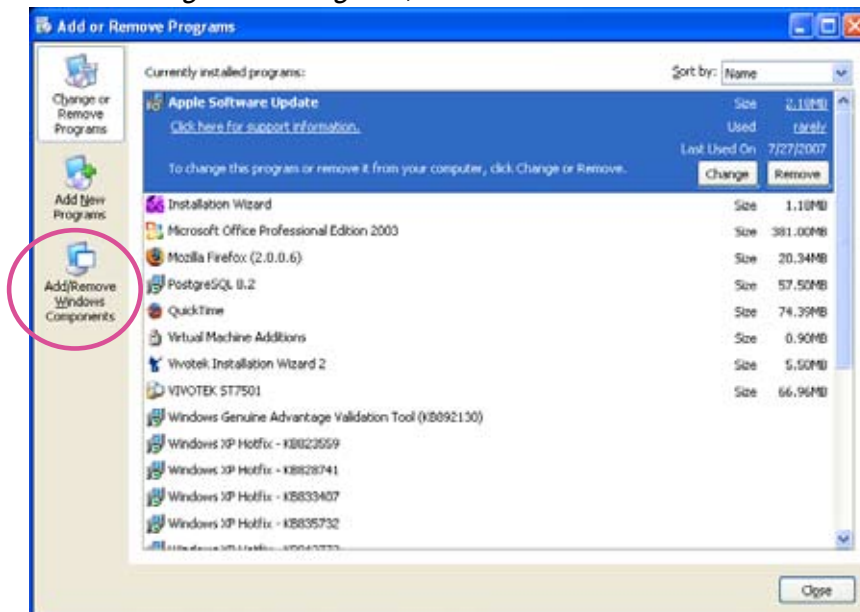
- ▶ If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.
- ▶ If UPnP™ is not supported by your router, you will see the following message:  
**Error: Router does not support UPnP port forwarding.**

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

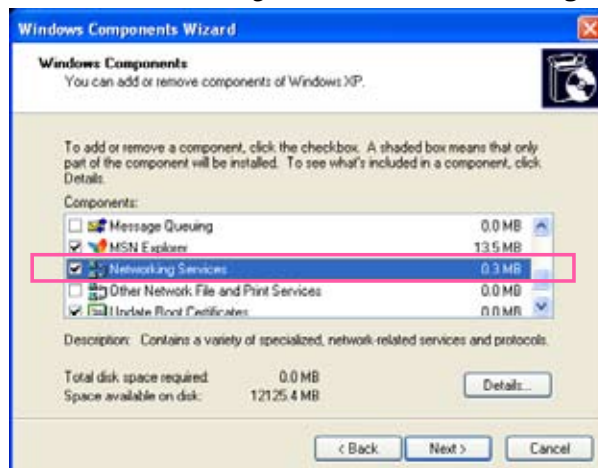
1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.



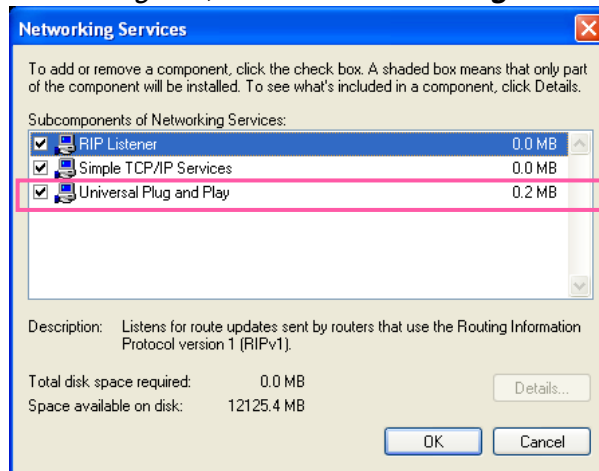
2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.



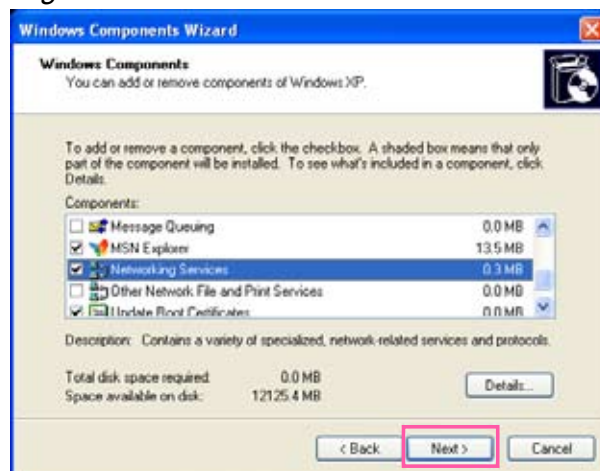
3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.



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<br>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 79 for details. After the Network Camera is reset to factory default, it is 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.

**IPv6 NET Information**

[eth0 address]

IPv6 address list of host

[Gateway]

IPv6 address list of gateway

[DNS]

IPv6 address list of DNS

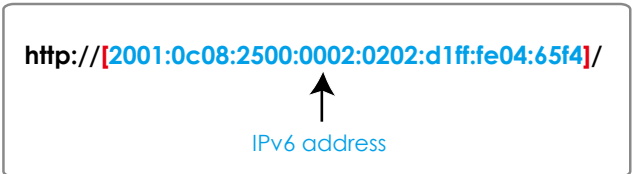
If your IPv6 settings are successful, the IPv6 address list will listed in the pop-up window. The IPv6 address will be displayed as follows:

### Refers to Ethernet

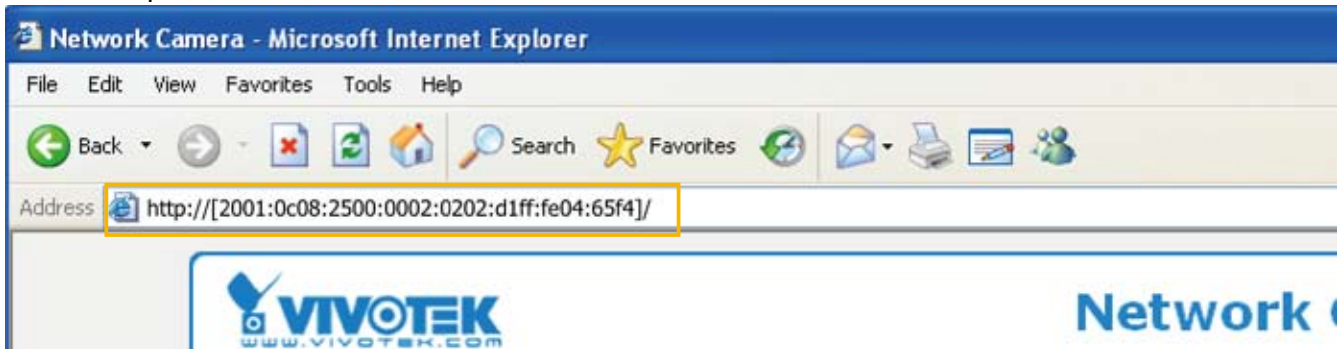
|                |   |   |
|----------------|---|---|
| [eth0 address] |   |   |
|                | 2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global | — Link-global IPv6 address/network mask |
|                | fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link   | — Link-local IPv6 address/network mask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

Please follow the steps below to link to 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 the 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 39 for detailed information.)



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

|                |   |
|----------------|---|
| [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:b100:01e0:0002:0202:d1ff:fe11:2299/64@Global |
| [Gateway]      | fe80:90:1a00:4142:8ca3                            |
| [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

## HTTP **Advanced Mode**

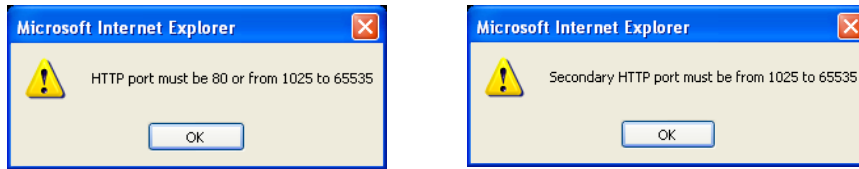
To utilize HTTP authentication, make sure that you have set a password for the Network Camera first; please refer to Security on page 27 for details.

| HTTP                      |             |
|---------------------------|-------------|
| Authentication:           | basic       |
| HTTP port:                | 80          |
| Secondary HTTP port:      | 8080        |
| Access name for stream 1: | video.mjpg  |
| Access name for stream 2: | video2.mjpg |

**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

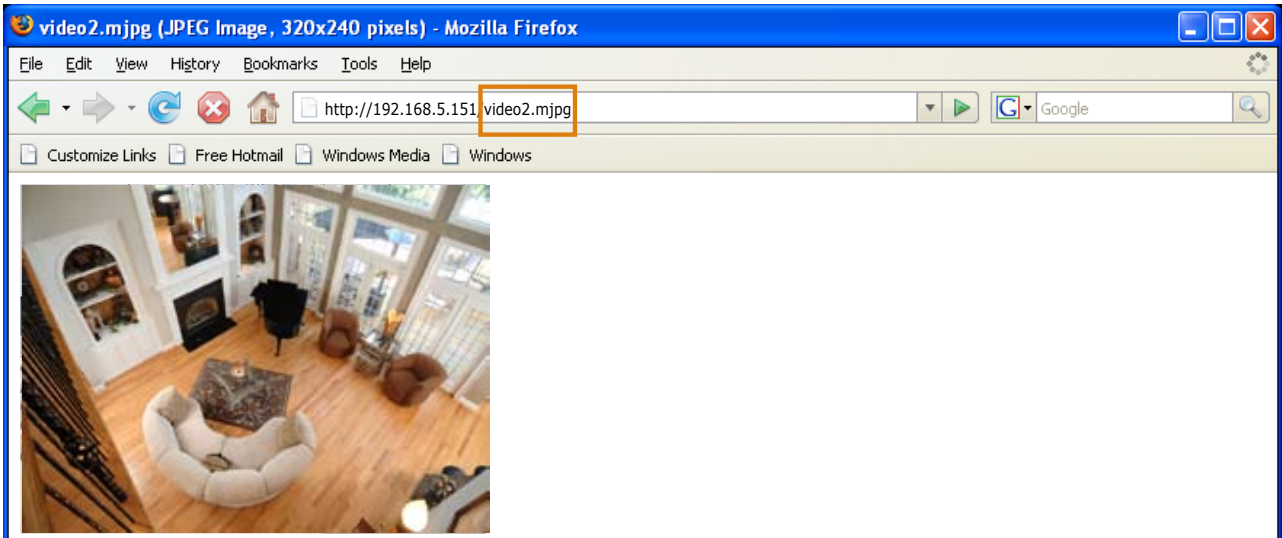
**Access name for stream 1 / Access name for stream 2:** The access name is used to differentiate the streaming source.

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:

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

**Two Way Audio**

**Two way audio**

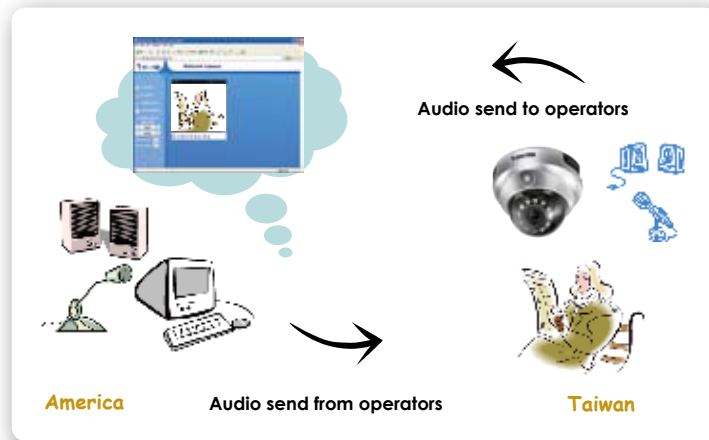
Two way audio port:

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

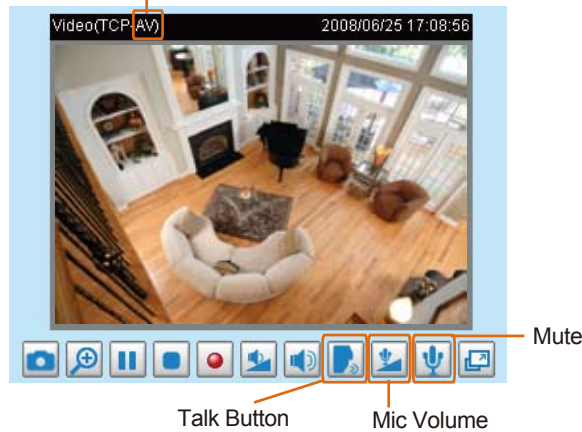
The Network Camera supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the Network Camera's built-in or external microphone and an external speaker, you can communicate with people around the Network Camera.







Note that as JPEG only transmits a series of JPEG images to the client, to enable the two-way audio function, make sure the video mode is set to "MPEG-4" on the Audio and Video Settings page and the media option is set to "Video and Audio" on the Client Settings page. Please refer to Client Settings on page 22 and Audio and Video Settings on page 49.



Audio is being transmitted to the Network Camera



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

## 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 also can be assigned to another port number between 1025 and 65535.

## RTSP Streaming

To utilize the RTSP streaming authentication, make sure that you have set a password for the Network Camera first; please refer to Security on page 27 for details.

**RTSP Streaming**

Authentication:

Access name for stream 1:

Access name for stream 2:

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:

**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           |

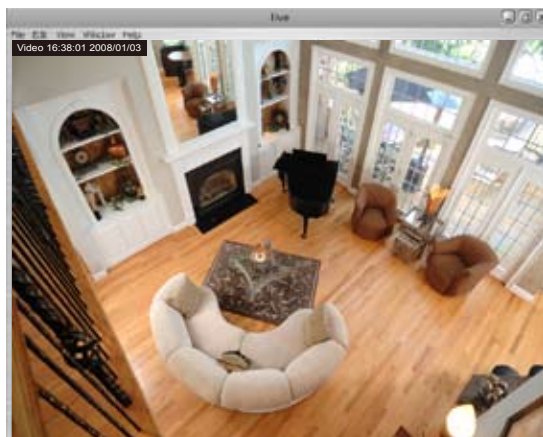
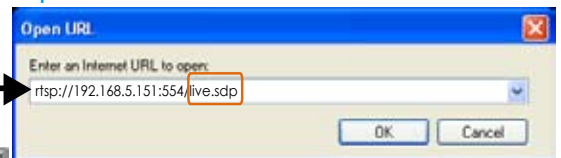
**Access name for stream 1 / Access name for stream 2:** This Network camera supports dual streams simultaneously. The access name is used to differentiate the streaming source.

If you want to use an **RTSP player** to access the Network Camera, you have to set the video mode to **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.



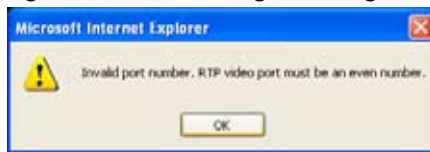
RTSP port /RTP port for video, audio/ RTCP port for video, audio

The 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 five 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 / Multicast settings for stream 2: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1 or stream 2.

Multicast settings for stream 1:
   
 Always multicast
   
 Multicast group address: 
  
 Multicast video port: 
  
 Multicast RTCP video port: 
  
 Multicast audio port: 
  
 Multicast RTCP audio port: 
  
 Multicast TTL [1~255]:

Multicast settings for stream 2:
   
 Always multicast
   
 Multicast group address: 
  
 Multicast video port: 
  
 Multicast RTCP video port: 
  
 Multicast audio port: 
  
 Multicast RTCP audio port: 
  
 Multicast TTL [1~255]:

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

The five 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 a packet can be forwarded.

## 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 camera 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 a dynamic domain account first.

#### ■ [Safe100.net](#)

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

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

**DDNS: Dynamic domain name service**

Enable DDNS:

Provider: Safe100.net

Host name: WTK.safe100.net [\* .safe100.net]

Email: wtk@vivotek.com

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:

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

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

4. Select Enable DDNS, then click **Save** to enable the settings.

#### ■ CustomSafe100

VIVOTEK offers documents to establish 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

**General Settings**

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

Enable access list filtering

Save

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

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

Connection status

|                          | IP address    | Elapsed time | User ID |
|--------------------------|---------------|--------------|---------|
| <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    |
|                          |               |              |         |
|                          |               |              |         |
|                          |               |              |         |
|                          |               |              |         |
|                          |               |              |         |
|                          |               |              |         |

Refresh
Add to deny list
Disconnect

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

There are some situations 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 27.
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 42.
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 27.

- 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

There are two lists for permission control: Allowed list and Denied 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 37 for detailed information.

**General Settings**

Maximum number of concurrent streaming connection(s) limited to:

Enable access list filtering

---

**Filter**

**IPv4 access list**

| Allowed list   | Denied list  |
|--|--|
| 1.0.0.0-255.255.255.255  |  |
| <input type="button" value="Add"/> <input type="button" value="Delete"/> | <input type="button" value="Add"/> <input type="button" value="Delete"/> |

**IPv6 access list**

| Allowed list   | Denied list  |
|--|--|
| ::/0   |  |
| <input type="button" value="Add"/> <input type="button" value="Delete"/> | <input type="button" value="Add"/> <input type="button" value="Delete"/> |

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

There are three types of rules:

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

For example:

**filter address**

Rule:

IP address:

**Network:** This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List.  
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

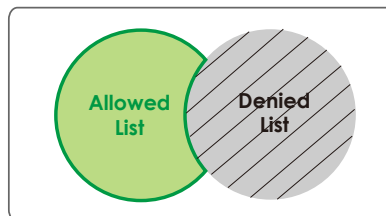
IP address - IP address:  -

■ **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: Color ▾

Power line frequency: 60 Hz ▾

Video orientation:  Flip  Mirror

Maximum Exposure Time: 1/5 S ▾

Overlay title and time stamp on video and snapshot.

➤ Video quality settings for stream 1:

➤ Video quality settings for stream 2:

**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.

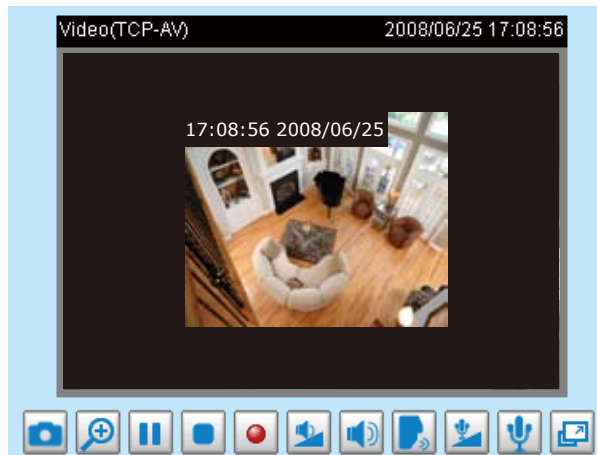
**Power line frequency:** Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the Network Camera in order for the 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. Select both options if the Network Camera is installed upside-down (ex. on the ceiling) to correct the image orientation.

**Maximum exposure time:** 1/30 S, 1/15 S, and 1/5 S.

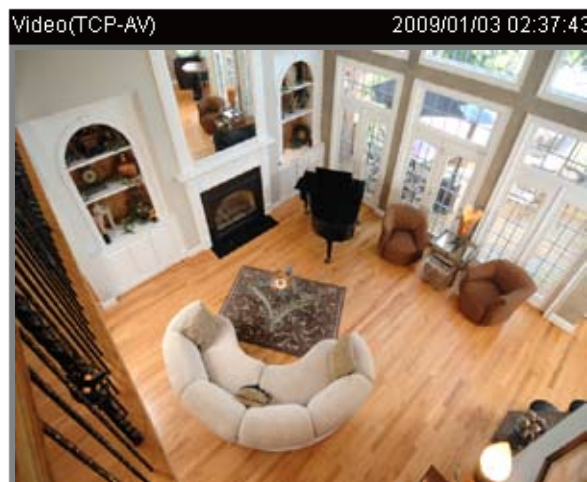
**Overlay title and time stamp on video:** Select this option to place the video title and time on video streams.

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 settings for the video.



**White Balance**

Auto

**Image Adjustment**

Brightness:  Saturation:   
Contrast:  Sharpness:

White balance: Adjust the value for best color temperature.

#### ■ Auto

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

■ **Keep current value**

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

1. Set the White balance to **Auto** and click **Save**.
2. Place a sheet of white paper in front of the lens, then allow the Network Camera to adjust the color temperature automatically.
3. Select Keep Current Value to confirm the setting while the white balance is being measured.
4. Click **Save** to enable the settings.

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 settings 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 sensitive zones to address privacy concerns.



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

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

**NOTE**

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

[Video quality settings for stream 1 / stream 2](#) **Advanced Mode**

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

Click the items to display the detailed configuration settings. You can set up two 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, the video is streamed via RTSP protocol. There are four parameters provided in MPEG-4 mode which allow you to adjust the video performance:

▼ Video quality settings for stream 1:

MPEG-4:

Frame size:

Maximum frame rate:   fps [1~30]

Intra frame period:

Video quality:

Constant bit rate:   Kbps [1~4000]

Fixed quality:   [1~31]

JPEG:

▼ Video quality settings for stream 2:

MPEG-4:

JPEG:

Frame size:

Maximum frame rate:   fps [1~30]

Video quality:   [10~200]

■ **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: 176 x 144, 320 x 240 and 640 x 480.

■ **Maximum frame rate**  
This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video quality.

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

- Intra frame period

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

- Video quality

A complex scene generally produces 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 performances. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, and 4Mbps. You can also select **Customize** and manually enter a value.

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

If **JPEG** mode is selected, the Network Camera 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: 176 x 144, 320 x 240, and 640 x 480.

- Maximum frame rate

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

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

- Video quality

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

### **NOTE**

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

## Audio Settings

**Audio Settings**

Mute

Internal microphone input gain: -10.5 dB

External microphone input: 0db

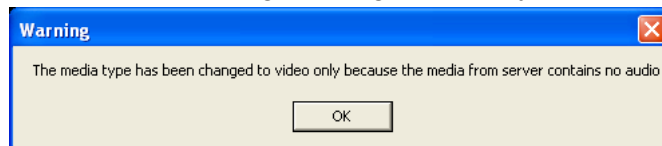
Audio type:

AAC:

GSM-AMR:

GSM-AMR bit rate: 12.2 Kbps

**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 +12 db (most sensitive) ~ -34.5 db (least sensitive).

**External microphone input:** Select the gain of the external audio input according to ambient conditions. Adjust the gain from +20 db (most sensitive) or 0 db (least sensitive).

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

- AAC provides good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable from: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps, and 128Kbps.
- GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable from: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps, and 12.2Kbps.

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

### **NOTE**

- ▶ *The Network Camera offers two inputs to capture audio - internal microphone or external microphone. The internal/external microphone switch is located on the side of the Network Camera.*

## 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:

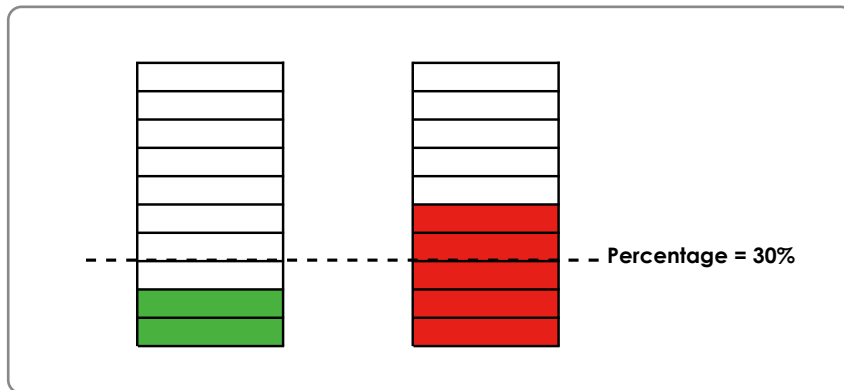
1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
  - To move and resize the window, drag and drop your mouse on the window.
  - To delete window, click X on the top right corner of the window.
3. Define the sensitivity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



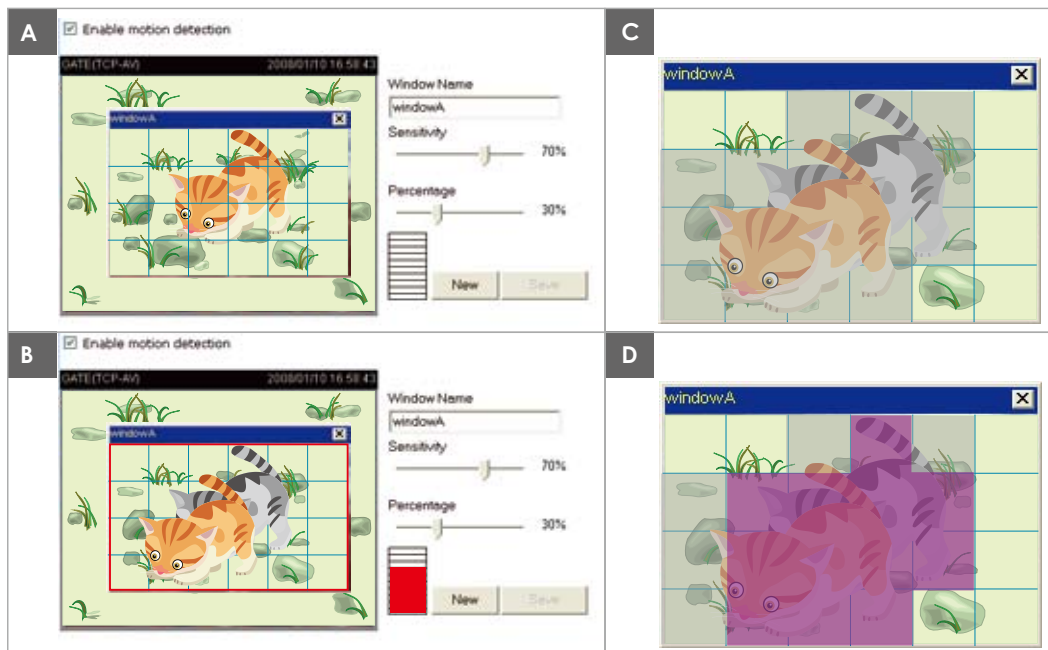
The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured 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 61.

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.



## Camera Tampering Detection

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

**Camera tampering detection**

Enable camera tampering detection

Trigger duration:  seconds [10~600]

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

1. Check **Enable camera tampering detection**.
2. Enter the tamper trigger duration. (10 sec. ~ 10 min.) The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.
3. Set up the event source as Camera Tampering Detection on **Application page > Event Settings / Server Settings (how to send alarm message) / Media Settings (send what type of alarm message)**. Please refer to page 65 for detailed information.

## Homepage Layout Advanced Mode

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

### Preview

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





### 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**

**VIVOTEK**  
www.vivotek.com

Video Stream

Digital Output

Client Settings

Powered by **VIVOTEK**

**Network Camera**

**Preview**

**VIVOTEK**  
www.vivotek.com

Video Stream

Digital Output

Client Settings

Powered by **VIVOTEK**

**Network Camera**

**Preview**

**VIVOTEK**  
www.vivotek.com

Video Stream

Digital Output

Client Settings

Powered by **VIVOTEK**

**Network Camera**

Preset Patterns

Font Color

Background Color of the Control Area

Font Color of the Configuration Area  
Background Color of the Configuration Area

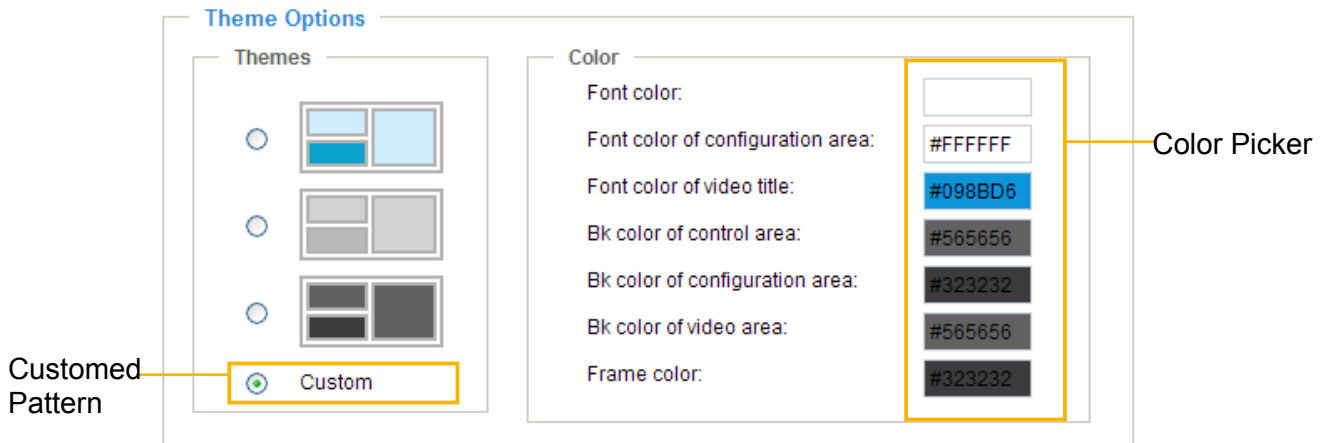
Font Color of the Video Title

Background Color of the Video Area

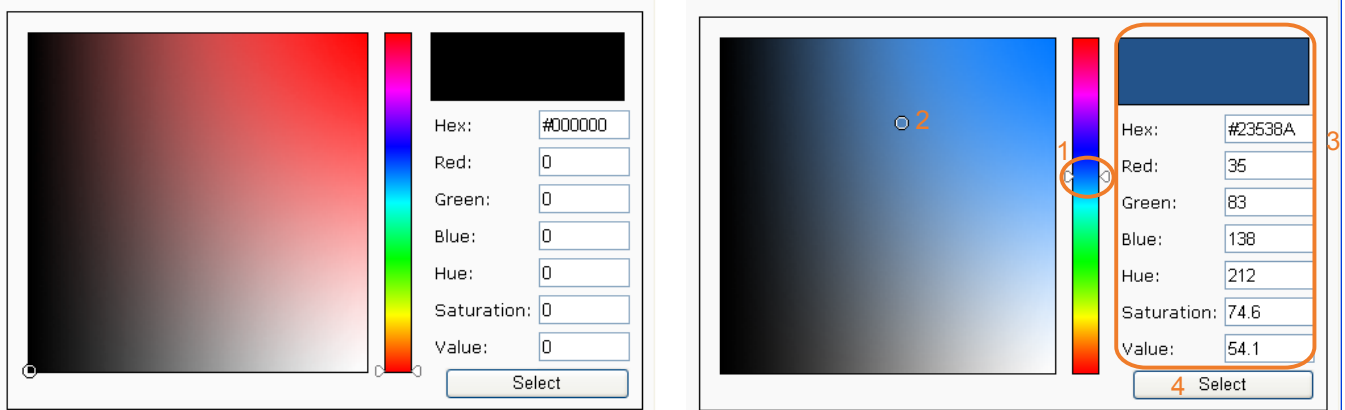
Frame Color

User's Manual - 59

- 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.

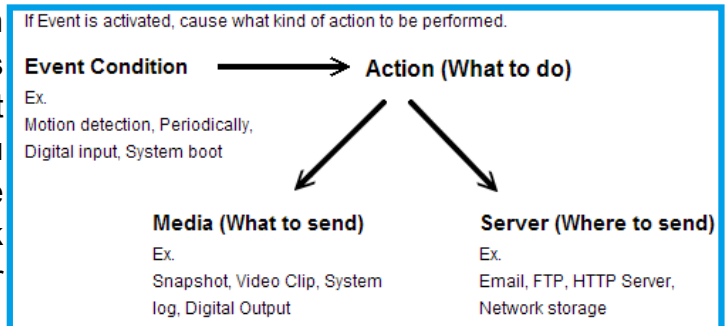


4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

## Application Advanced Mode

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

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 videos to your email address or FTP site.



**Event Settings**

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

**Customized Script**

| Name   | Date | Time |
|--|------|------|
| <div style="display: flex; justify-content: space-between; align-items: center;"> <span>Add</span> <span>▼</span> <span>Delete</span> </div> |      |      |

### 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 technical support.

**Customized Script**

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

Add
User1 ▼
Delete

```

<?xml version="1.0" encoding="UTF-8"?>
<eventmgr version="0102">
<maxprocess>1</maxprocess>
<!-- From 08:30:00-20:30:00 on Monday to Friday every week -->
<schedule id="0">
<duration>
<weekday>1-5</weekday>
<time>08:30:00-20:30:00</time>
</duration>
</schedule>
<!-- Motion -->
<action condition="0">
<status id="0">trigger</status>
<status id="1">trigger</status>
</motion>
<event id="0">
<description>Mail system log to email address</description>
<condition>0</condition>
<scheduleid>0</scheduleid>
<delay>10</delay>
<!-- users can send email with title "Motion" to recipient gudding.yang@vivotek.com. The body of mail is the log messages -->
<process>
/usr/bin/sempollent -s "Motion" -f IP@159@vivotek.com -b /var/log/messages -S ma.vivotek.tw -H S gudding.yang@vivotek.com
</process>
<priority>0</priority>
</event>
</eventmgr>
                
```

Upload

Click to upload a file. →

Click to modify the script online →

## Event Settings

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

Event name:

Enable this event

Priority:  ▼

Detect next event after  second(s).

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

**Trigger**

Video motion detection:

Periodically:

Digital input

PIR

System boot

Recording notify

Camera tampering detection:

**Event Schedule**

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Time**

Always

From  to  [hh:mm]

**Action**

Trigger digital output for  seconds

Turn on IR illuminators for  seconds  ▼

| Server | Media | Extra parameter |
|--------|-------|-----------------|
|        |       |                 |

Event name: Enter a name for the event setting.

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

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

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

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

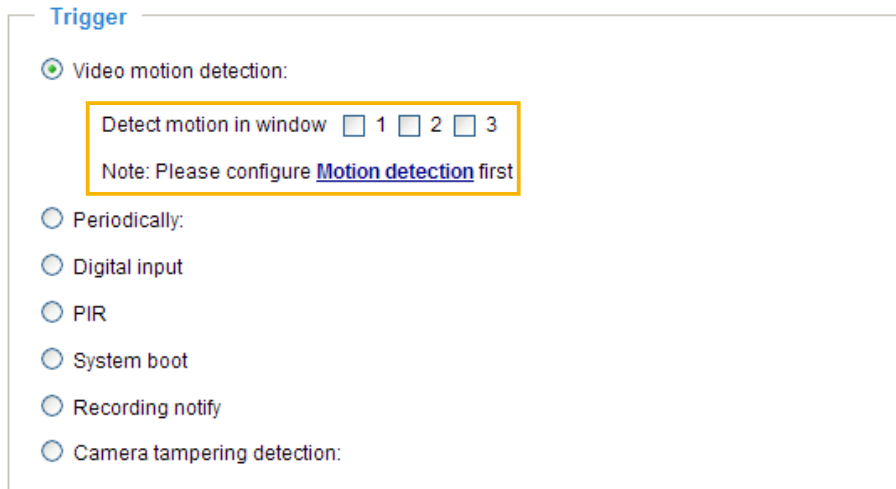
**Trigger**

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

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

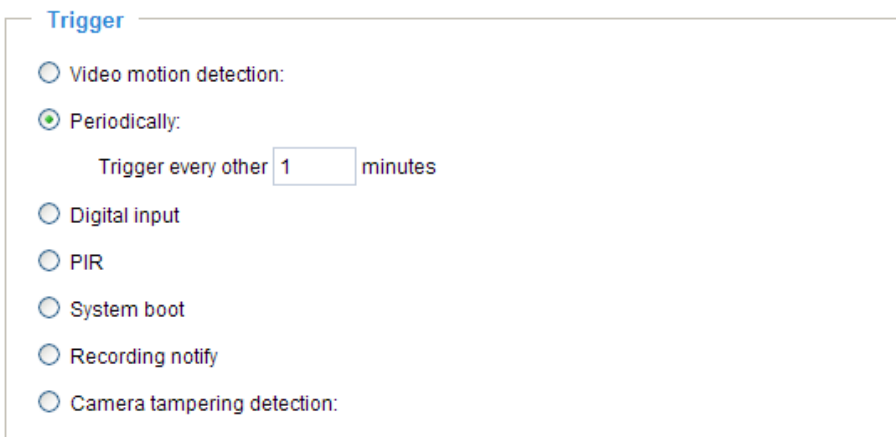
■ **Video motion detection**

This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to Motion detection on page 55 for details.



■ **Periodically**

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



■ **Digital input**

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

■ **PIR**

This option allows the Network Camera to trigger when the built-in PIR (Passive Infrared) sensor detects any motion objects by their thermal to prevent occurrences of false alarms.

■ **System boot**

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

■ Recording notify

This option allows the Network Camera to trigger when the recording disk is full or when recording starts to rewrite older data. If you want receive **Recording notify message**, please refer to page 72 for detailed information.

■ Camera tampering detection

This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 57 for detailed information.

**Trigger**

- Video motion detection:
- Periodically:
- Digital input
- PIR
- System boot
- Recording notify
- Camera tampering detection:

Note: Please configure [Camera tampering detection](#) first

**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.

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

**Action**

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

**Action**

Trigger digital output for  seconds

Turn on IR illuminators for  seconds in low-light conditions ▼

in low-light conditions

at all times

| Server | Media | Extra parameter |
|--------|-------|-----------------|
|        |       |                 |

■ Trigger digital output for  seconds

Select this option to turn on the external digital output device when a trigger is activated. Specify the length of the trigger interval in the text box.

■ Turn on IR Illuminators for  seconds

Select this to turn on IR Illuminators when a trigger is activated every time or only in low light conditions. Specify the length of trigger interval in the text box.



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

■ Add Server / Add Media

Click **Add Server** to configure [Server Settings](#). For more information, please refer to Server Settings on page 67.

Click **Add Media** to configure [Media Settings](#). For more information, please refer to Media Settings on page 70.

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:

Periodically:

Digital input

PIR

System boot

Recording notify

Camera tampering detection:

Note: Please configure [Camera tampering detection](#) first

**Event Schedule**

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Time**

Always

From  to  [hh:mm]

**Action**

Trigger digital output for  seconds

Turn on IR illuminators for  seconds

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

**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="#">Recording notify</a> | recordmsg |
| <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 only when the media setting is not being applied to an event setting can it be deleted.

## Server Settings

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

Server name: Enter a name for the server setting.

### Server Type

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

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

Server name:

**Server Type**

Email:

Sender email address:

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.
- **Remote 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 74 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 checked="" type="checkbox"/> | NAS    | Video Clip     | <input checked="" type="checkbox"/> Create folders by date time and hour automatically<br><input type="button" value="View"/> |
| <input type="checkbox"/>            | FTP    | -----None----- |   |
| <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.

Media name:

**Media Type**

Snapshot

Source:  ▼

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

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

File name prefix:

Add date and time suffix to file name

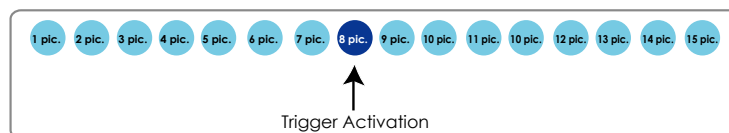
Video Clip

System log

Recording notify message

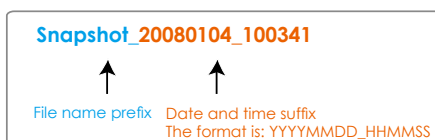
- Source: Select to take snapshots from stream 1 or stream 2.
- Send  pre-event images  
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.
- Send  post-event 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]

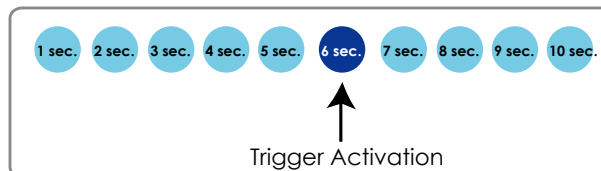
Maximum file size:  Kbytes [50~800]

File name prefix:

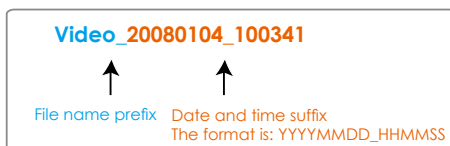
System log

Recording notify message

- **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.



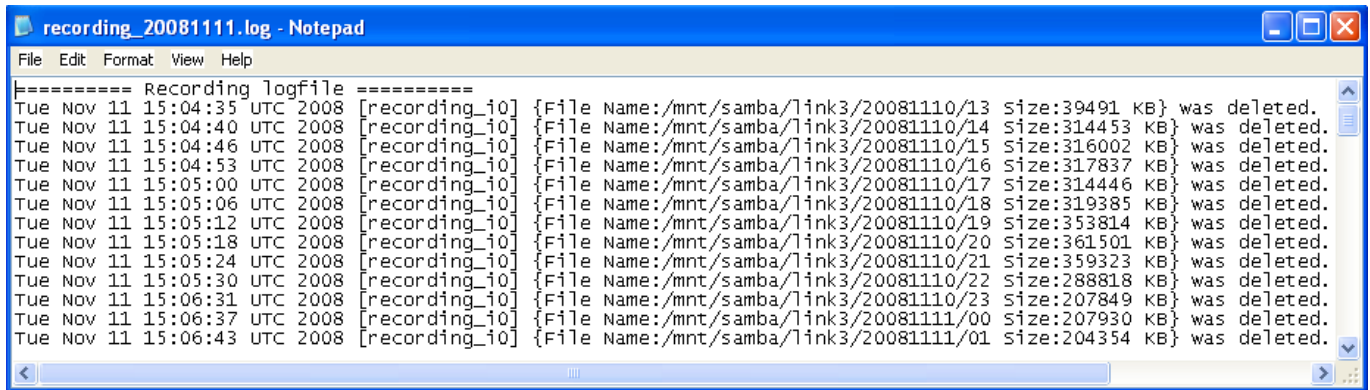
- **Maximum file size**  
Specify the maximum file size allowed.
- **File name prefix**  
Enter the text that will be appended to the front of the file name.  
For example:



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.

**Recording notify message:** Select to send a recording notification message when a trigger is activated. The following is an example of a recording notification message (.txt file), which shows a list of deleted previously-recorded data due to cycle recording.



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

You can continue to select a server and media type for the event. Please go back to page 66 for detailed information.

| Server                         | Media  | Extra parameter   |
|--------------------------------|--|---|
| <input type="checkbox"/> FTP   | -----None-----   |   |
| <input type="checkbox"/> Email | Snapshot<br>Video Clip<br>System log<br>Recording notify |   |
| <input type="checkbox"/> HTTP  |  |   |
| <input type="checkbox"/> NAS   | -----None-----   | <input type="checkbox"/> Create folders by date time and hour automatically |

- **Create folders by date, time, and hour automatically:** If you check this item, the system will generate folders automatically by date.
- **View:** Click this button to open a file list window. This function is only for Network Storage. The following is an example of a file destination with video clips:

|  |  |
|--|--|
| <input type="checkbox"/> <input type="button" value="▶"/> 20081120<br><input type="checkbox"/> <input type="button" value="▶"/> 20081121<br><input type="checkbox"/> <input type="button" value="▶"/> 20081122 | The format is: YYYYMMDD<br>Click to open the directory |
| <input type="button" value="Delete"/> <input type="button" value="Delete all"/>  | Click to delete selected items                         |



Click [20081120](#) 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 | 2008/11/20 | 07:58:28 |
| <input type="checkbox"/> | <a href="#">Recording1_59.mp4</a> | 2563536 | 2008/11/20 | 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 | 2008/11/20 | 07:58:28 |
| <input type="checkbox"/> | <a href="#">Recording1_59.mp4</a> | 2563536 | 2008/11/20 | 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 70 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 |
|---|--------|-----|-----|-----|-----|-----|-----|-----|------|--------|-------------|
| <input type="button" value="Add"/> <input type="button" value="▼"/> <input type="button" value="Delete"/> |        |     |     |     |     |     |     |     |      |        |             |

#### **NOTE**

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

#### **Network Storage Setting**

Click [Server](#) to open the Server Settings page and follow the steps below to set up:

1. Fill in the information for your server.

For example:

**>Server Settings**

Server name:  <sup>3</sup>

**Server Type**

Email:

FTP:

HTTP:

**1**  Network storage:

Network storage location:  (For example: \\my\_nas\diskfolder)

Workgroup:

User name:

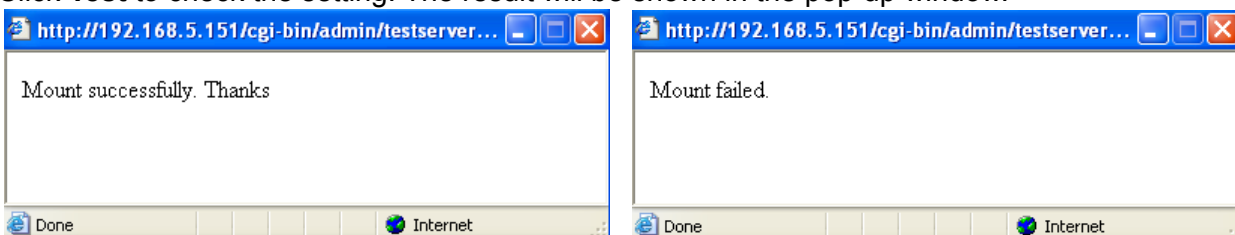
Password:

<sup>2</sup> <sup>4</sup>

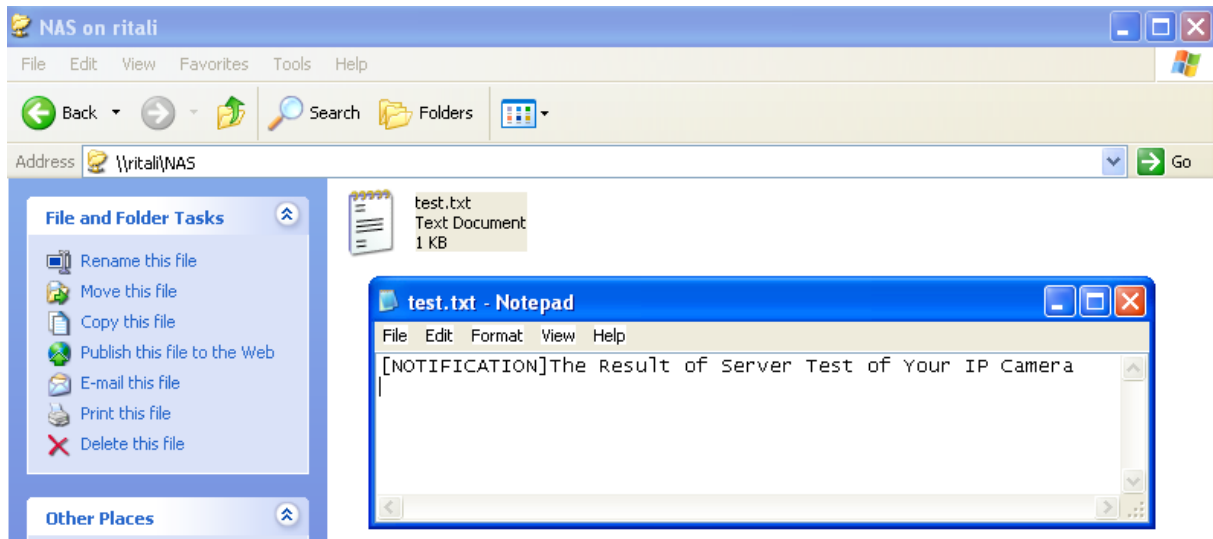
Network storage path (\\server name or IP address\folder name)

User name and password for your server

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



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



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

### Recording Settings

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

Recording name:

Enable this recording

Priority:

Source:

**Recording Schedule**

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Time**

Always

From  to  [hh:mm]

Destination:

Capacity:

Entire free space

Limit recording size in  Mbytes

File name prefix:

Enable cyclic recording

Reserved amount:  Mbytes

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.

**Priority:** Select the relative importance of this recording setting (High, Normal, and Low).

**Source:** Select the recording source (stream 1 or stream 2).

**Recording Schedule:** Specify the recording duration.

- Select the days of the week.
- Select the recording start and end times in 24-hr time format.

**Destination:** You can select the SD card or network storage that was set up for the recorded video files.

**Capacity:** You can choose either the entire free space available or limit the recording size. The recording size limit must be larger than the reserved amount for cyclic recording.

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

**Enable cyclic recording:** If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for 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 64 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 ▾ Delete

- 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 rules, please refer to page 72 for details.

- [➔ 20081120](#)
- [➔ 20081121](#)
- [➔ 20081122](#)

Delete Delete all

## 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**

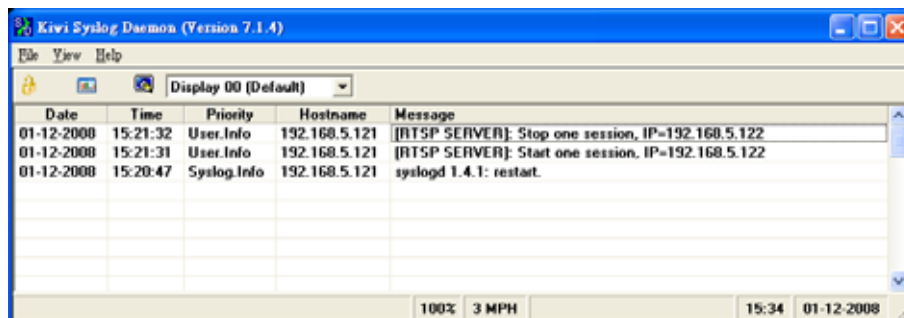
Enable remote log

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**

```

Dec 31 10:33:34 syslogd 1.5.0: restart.
Dec 31 10:33:36 [swatchdog][102]: Ready to watch httpd.
Dec 31 10:33:37 [EVENT MGR]: Starting eventmgr with support for EcTun
Dec 31 10:33:38 [DRM Service]: Starting DRM service.
Dec 31 10:33:44 [swatchdog][102]: Ready to watch vncslave1.
Dec 31 10:33:46 [swatchdog][102]: Ready to watch vncslave2.
Dec 31 10:33:50 [RTSP SERVER]: XMLSParser: open failed^M
Dec 31 10:33:55 [IR Cut Control]: Day mode
Dec 31 10:33:55 [RTSP SERVER]: Start one session, IP=192.168.5.122
Dec 31 10:33:56 [SYS]: Serial number = 0002D107258A
Dec 31 10:33:57 [SYS]: System starts at Wed Dec 31 10:33:56 UTC 2008
Dec 31 10:33:57 [NET]: === NET INFO ===
Dec 31 10:33:57 [NET]: Host IP = 192.168.5.108
Dec 31 10:33:57 [NET]: Subnet Mask = 255.255.255.0
Dec 31 10:33:57 [NET]: Gateway = 192.168.5.1
Dec 31 10:33:57 [NET]: Primary DNS = 192.168.0.10
Dec 31 10:33:57 [NET]: Secondary DNS = 192.168.0.20

```

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 certain limit.

## View Parameters Advanced Mode

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

**Parameter List**

```

system_hostname='Network Camera'
system_ledoff='0'
system_lowlight='1'
system_date='2000/01/01'
system_time='19:28:41'
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_info_modelname='FD7131'
system_info_extendedmodelname='FD7131'
system_info_serialnumber='0002D1112299'
system_info_firmwareversion='FD7131-VVTK-0200c'
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=''

```

## 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 reboot process.

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

|||||

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

### 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 33).

**Daylight Saving Time:** Select this option to retain the Daylight Saving Time settings (please refer to System on page 25).

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

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

The following message is displayed during the restoring process.

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

|||||

## Export / Upload Files Advanced Mode

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

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

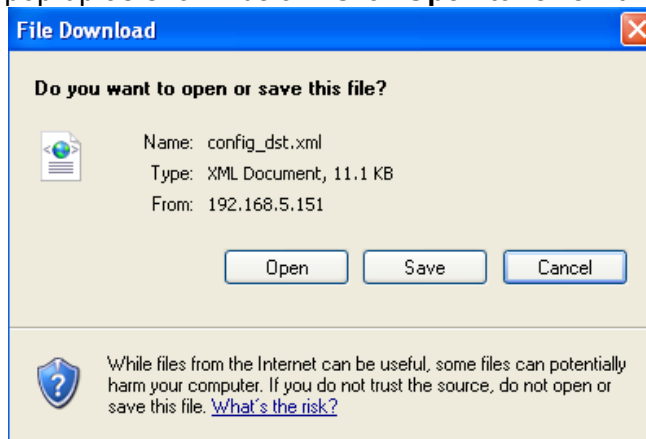
  

| Upload files                      |   |
|-----------------------------------|---|
| Update daylight saving time rules | <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/> |
| Update custom language file       | <input type="text"/> <input type="button"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

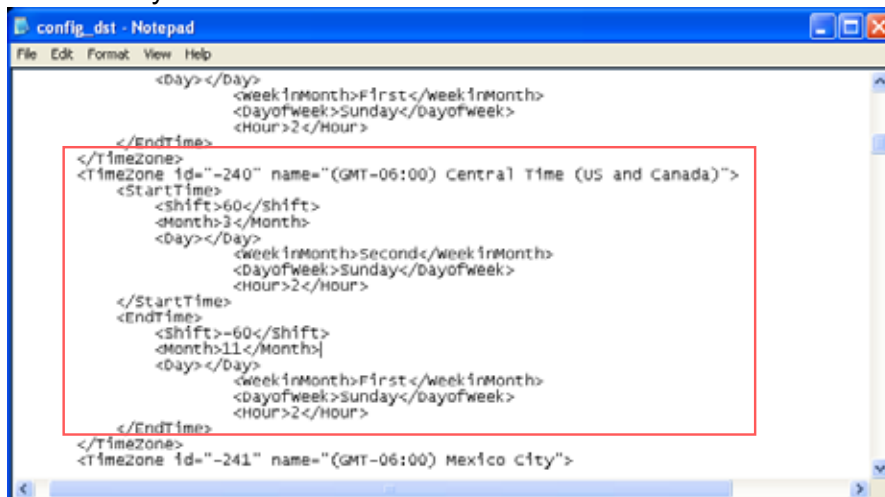
Follow the steps below to export:

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.

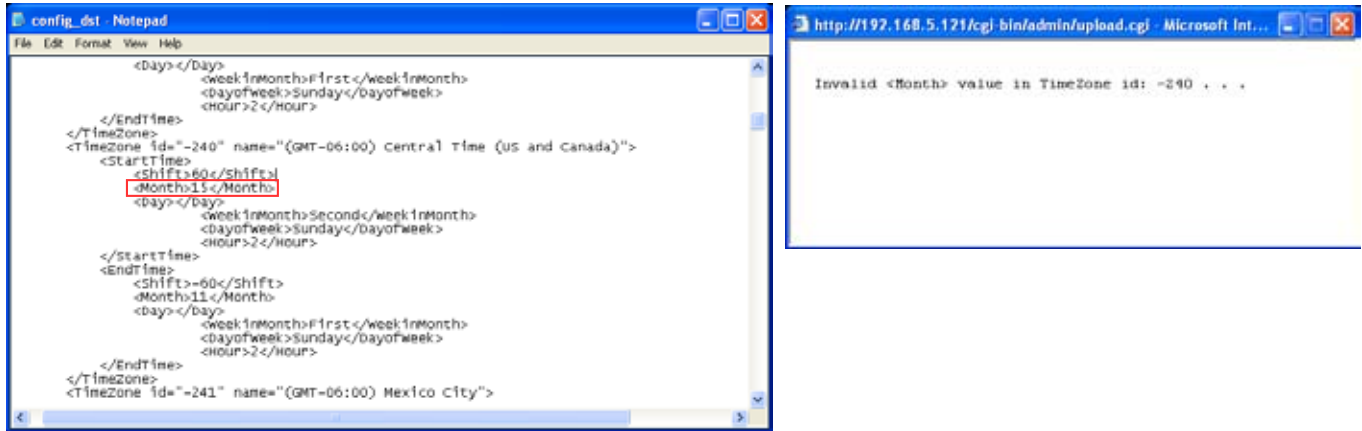
In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.



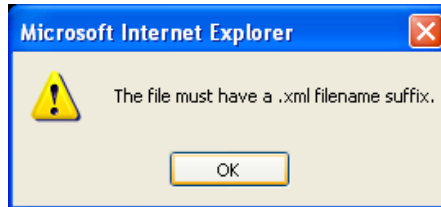


Upload daylight saving time rule: Click **Browse...** and specify the XML file to upload.

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, 簡體中文, 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.

The screenshot shows the VIVOTEK Configuration web interface. The top left features the VIVOTEK logo and website URL. The top right shows the 'Configuration' tab. The main content area is titled '>Maintenance' and contains a progress bar on the right side, ranging from 77% to 100%. On the left, there is a navigation menu with items like Home, System, Security, HTTPS, Network, DDNS, Access list, Audio and video, Motion detection, Homepage layout, Application, Recording, System log, and View parameters. The 'Maintenance' section is currently selected. The main content area displays a list of maintenance tasks, each followed by a percentage and three dots. The tasks include: 'written 77 % ...', 'written 78 % ...', 'written 79 % ...', 'written 80 % ...', 'written 81 % ...', 'written 82 % ...', 'written 83 % ...', 'written 84 % ...', 'written 85 % ...', 'written 86 % ...', 'written 87 % ...', 'written 88 % ...', 'written 89 % ...', 'written 90 % ...', 'written 91 % ...', 'written 92 % ...', 'written 93 % ...', 'written 94 % ...', 'written 95 % ...', 'written 96 % ...', 'written 97 % ...', 'written 98 % ...', 'written 99 % ...', and 'written 100 % ...'. Below the progress bar, there is a list of maintenance tasks: 'Update system image success', 'Clear boot specific data', 'Write boot environment', 'Updating armboot environment if necessary', 'Copied 8192 bytes from /mnt/ramdisk/bootenv to address 0x00004000 in flash', 'Copied 8192 bytes from address 0x00004000 in flash to /mnt/ramdisk/checkbootenv', 'Update armboot env success', 'Set JFFS2 upgrading mode', 'Set flash status 0', 'FlashStatus=0', 'Reboot system now !!', and 'This connection will close'. The last two lines are highlighted with a red box. At the bottom left, the version number 'Version: 0200c' is displayed.

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.  
 It will takes about 1 - 5 minutes.  
 Wrong PKG file format  
 Unpack fail

# Appendix

## URL Commands for the Network Camera

### 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.

### Style Convention

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

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

**Syntax:**

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

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

**Return:**

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

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

**Example:** request a single snapshot image

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

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

Syntax:

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

**Example:** Setting digital output #1 to active

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

## Security level

| SECURITY LEVEL | SUB-DIRECTORY                                     | DESCRIPTION  |
|----------------|---|--|
| 0              | anonymous   | Unprotected.   |
| 1 [view]       | anonymous, viewer, dido, camctrl                  | 1. Can view, listen, talk to camera<br>2. Can control dido, ptz of camera                                |
| 4 [operator]   | anonymous, viewer, dido, camctrl, operator        | Operator's access right can modify most of camera's parameters except some privilege and network options |
| 6 [admin]      | anonymous, viewer, dido, camctrl, operator, admin | Administrator's access right can fully control the camera's operation.                                   |
| 7              | N/A   | Internal parameters. Unable to be changed by any external interface.                                     |

## 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 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 request 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:** 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 <value> to the parameter <group>_<name>  |
| <b>update</b>                     | <boolean>         | set to 1 to actually update all fields (no need to use update parameter in each group)  |
| <b>return</b>                     | <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.<br><br>(note: The return page can be a general HTML file (.htm, .html) or a Vivotek server script executable (.vsp) 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](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

Valid values:

| VALID VALUES          | DESCRIPTION   |
|-----------------------|---|
| string[<n>]           | Text string shorter than 'n' characters. The characters ",', <, >, & are invalid.             |
| password[<n>]         | The same as string but display '*' 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 contain a domain name shorter than 'n' characters (eg. www.ibm.com)       |
| email address [ <n> ] | A string limited to contain a email address shorter than 'n' characters (eg. joe@www.ibm.com) |
| ip address            | A string limited to contain an ip address (eg. 192.168.1.1)                                   |
| mac address           | A string limited to contain mac address without hyphen or colon connected                     |
| boolean               | A boolean value 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].          |

|  |   |
|--|---|
| <value1>,<br><value2>,<br><value3>,<br>... | Enumeration. Only given values are valid. |
| blank                                      | A blank string                            |
| everything inside <>                       | As description                            |

NOTE: The camera should prevent to restart when parameter changed.

Group: **system**

| NAME          | VALUE   | SECURITY<br>(get/set) | DESCRIPTION  |
|---------------|---|-----------------------|--|
| hostname      | string[40]                                    | 1/6                   | host name of server  |
| ledoff        | <boolean>                                     | 6/6                   | turn on(0) or turn off(1) all led indicators   |
| lowlight      | <boolean>                                     | 6/6                   | (0) Turn on white light LED in all condition<br>(1) Only turn on white light LED in low light condition  |
| date          | <yyyy/mm/dd<br>>,<br>keep,<br>auto            | 6/6                   | Current date of system. Set to 'keep' keeping date unchanged. Set to 'auto' to use NTP to synchronize date.  |
| time          | <hh:mm:ss>,<br>keep,<br>auto                  | 6/6                   | Current time of system. Set to 'keep' keeping time unchanged. Set to 'auto' to use NTP to synchronize time.  |
| datetime      | <MMDDhhmmY<br>YY.ss>                          | 6/6                   | Another current time format of system.   |
| ntp           | <domain<br>name>,<br><ip address>,<br><blank> | 6/6                   | NTP server<br>*do not use "skip to invoke default server" for default  |
| timezoneindex | -489 ~ 529                                    | 6/6                   | Indicate timezone and area<br>-480: GMT-12:00 Eniwetok, Kwajalein<br>-440: GMT-11:00 Midway Island, Samoa<br>-400: GMT-10:00 Hawaii<br>-360: GMT-09:00 Alaska<br>-320: GMT-08:00 Las Vegas, San_Francisco, Vancouver |



|  |  |  |  |   |
|--|--|--|--|---|
|  |  |  |  | <p>-280: GMT-07:00 Mountain Time, Denver</p> <p>-281: GMT-07:00 Arizona</p> <p>-240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan</p> <p>-200: GMT-05:00 Eastern Time, New York, Toronto</p> <p>-201: GMT-05:00 Bogota, Lima, Quito, Indiana</p> <p>-160: GMT-04:00 Atlantic Time, Canada, Caracas, La Paz, Santiago</p> <p>-140: GMT-03:30 Newfoundland</p> <p>-120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland</p> <p>-80: GMT-02:00 Mid-Atlantic</p> <p>-40: GMT-01:00 Azores, Cape_Verde_IS.</p> <p>0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London</p> <p>40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris</p> <p>41: GMT 01:00 Warsaw, Budapest, Bern</p> <p>80: GMT 02:00 Athens, Helsinki, Istanbul, Riga</p> <p>81: GMT 02:00 Cairo</p> <p>82: GMT 02:00 Lebanon, Minsk</p> <p>83: GMT 02:00 Israel</p> <p>120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi</p> <p>121: GMT 03:00 Iraq</p> <p>140: GMT 03:30 Tehran</p> <p>160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan</p> <p>180: GMT 04:30 Kabul</p> <p>200: GMT 05:00 Ekaterinburg,</p> |
|--|--|--|--|---|

|                          |   |     |  |
|--------------------------|---|-----|--|
|                          |   |     | <p>Islamabad, Karachi, Tashkent<br/>                 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi<br/>                 230: GMT 05:45 Kathmandu<br/>                 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura<br/>                 260: GMT 06:30 Rangoon<br/>                 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk<br/>                 320: GMT 08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei<br/>                 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk<br/>                 380: GMT 09:30 Adelaide, Darwin<br/>                 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok<br/>                 440: GMT 11:00 Magadan, Solomon Is., New Caledonia<br/>                 480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is.<br/>                 520: GMT 13:00 Nuku'Alofa</p> |
| daylight_enable          | <boolean>                                   | 6/6 | enable automatic daylight saving to time zone  |
| daylight_dstactualmode   | <boolean>                                   | 6/7 | check if current time is under daylight saving time.   |
| daylight_auto_beginntime | string[19]                                  | 6/7 | display the current daylight saving begin time.  |
| daylight_auto_endntime   | string[19]                                  | 6/7 | display the current daylight saving end time.  |
| daylight_timezones       | strings                                     | 6/7 | list of time zone which has daylight saving time   |
| updateinterval           | 0,<br>3600,<br>86400,<br>604800,<br>2592000 | 6/6 | 0 to disable automatic time adjustment, otherwise, it means the seconds between NTP automatic update interval.   |
| restore                  | 0,<br><positive integer>                    | 7/6 | Restore the system parameters to default value after <value> seconds.  |

|                       |                             |     |  |
|-----------------------|-----------------------------|-----|--|
| reset                 | 0,<br><positive<br>integer> | 7/6 | Restart the server after <value><br>seconds if <value> is non-negative.  |
| restoreexceptn<br>et  | <Any value>                 | 7/6 | Restore the system parameters to<br>default value except (ipaddress,<br>subnet, router, dns1, dns2, pppoe).<br>This command can cooperate with<br>other "restoreexceptXYZ" commands.<br>When cooperating with others, the<br>system parameters will be restored to<br>default value except a union of<br>combined results. |
| restoreexceptd<br>st  | <Any value>                 | 7/6 | Restore the system parameters to<br>default value except all daylight saving<br>time settings.<br>This command can cooperate with<br>other "restoreexceptXYZ" commands.<br>When cooperating with others, the<br>system parameters will be restored to<br>default value except a union of<br>combined results.              |
| restoreexceptl<br>ang | <Any Value>                 | 7/6 | Restore the system parameters to<br>default value except custom language<br>file user uploaded.<br>This command can cooperate with<br>other "restoreexceptXYZ" commands.<br>When cooperating with others, the<br>system parameters will be restored to<br>default value except a union of<br>combined results.             |

SubGroup of **system: info**

| NAME              | VALUE            | SECURITY<br>(get/set) | DESCRIPTION  |
|-------------------|------------------|-----------------------|--|
| modelname         | string[40]       | 0/7                   | model name of server   |
| extendedmodelname | string[40]       | 0/7                   | equal to "modelname"   |
| serialnumber      | <mac<br>address> | 0/7                   | 12 characters mac address without<br>hyphen connected                    |
| firmwareversion   | string[40]       | 0/7                   | The version of firmware, including<br>model, company, and version number |

|                                  |            |     |   |
|----------------------------------|------------|-----|---|
|                                  |            |     | in the format<br><MODEL-BRAND-VERSION>                          |
| language_count                   | <integer>  | 0/7 | Default number of webpage language available on the server      |
| language_i<0~(count-1)>          | string[16] | 0/7 | Available default language lists                                |
| customlanguage_maxcount          | <integer>  | 0/7 | Maximum number of custom language supported on the server       |
| customlanguage_count             | <integer>  | 0/7 | Number of custom language which has been uploaded to the server |
| customlanguage_i<0~(maxcount-1)> | string     | 0/7 | Custom language name  |

Group: **status**

| NAME               | VALUE     | SECURITY (get/set) | DESCRIPTION                                     |
|--------------------|-----------|--------------------|---|
| di_i<0~(ndi-1)>    | <boolean> | 1/7                | 0 => Inactive, normal<br>1 => Active, triggered |
| do_i<0~ndi-1)>     | <boolean> | 1/7                | 0 => Inactive, normal<br>1 => Active, triggered |
| onlinenum_rtsp     | integer   | 6/7                | current RTSP connection numbers                 |
| onlinenum_httppush | integer   | 6/7                | current HTTP push server connection numbers     |
| eth_i0             | <string>  | 1/99               | Get network information from mii-tool           |

Group: **di\_i<0~(ndi-1)>**

| NAME        | VALUE        | SECURITY (get/set) | DESCRIPTION  |
|-------------|--------------|--------------------|--|
| normalstate | high,<br>low | 1/1                | indicate whether open circuit or closed circuit represents inactive status |

Group: **do\_i<0~(ndo-1)>**

| NAME        | VALUE             | SECURITY (get/set) | DESCRIPTION  |
|-------------|-------------------|--------------------|--|
| normalstate | open,<br>grounded | 1/1                | indicate whether open circuit or closed circuit represents inactive status |

Group: **security**

| NAME                       | VALUE                         | SECURITY<br>(get/set) | DESCRIPTION  |
|----------------------------|-------------------------------|-----------------------|--|
| privilege_do               | view, operator,<br>admin      | 6/6                   | Indicate which privilege and above<br>can control digital output |
| user_i0_name               | string[64]                    | 6/7                   | User's name of root  |
| user_i<1~20>_name          | string[64]                    | 6/7                   | User's name  |
| user_i0_pass               | password[64]                  | 6/6                   | root's password  |
| user_i<1~20>_pass          | password[64]                  | 7/6                   | User's password  |
| user_i0_privilege          | viewer,<br>operator,<br>admin | 6/7                   | root's privilege   |
| user_i<1~20>_<br>privilege | viewer,<br>operator,<br>admin | 6/6                   | User's privilege.  |

Group: **network**

| NAME       | VALUE         | SECURITY<br>(get/set) | DESCRIPTION   |
|------------|---------------|-----------------------|---|
| type       | lan,<br>pppoe | 6/6                   | Network connection type   |
| preprocess | 0~15          | 6/6                   | Stop related process before set port value  |
| resetip    | <boolean>     | 6/6                   | 1 => get ipaddress, subnet, router, dns1,<br>dns2 from DHCP server at next reboot<br>0 => use preset ipaddress, subnet,<br>router, dns1, and dns2 |
| ipaddress  | <ip address>  | 6/6                   | IP address of server  |
| subnet     | <ip address>  | 6/6                   | subnet mask   |
| router     | <ip address>  | 6/6                   | default gateway   |
| dns1       | <ip address>  | 6/6                   | primary DNS server  |
| dns2       | <ip address>  | 6/6                   | secondary DNS server  |
| wins1      | <ip address>  | 6/6                   | primary WINS server   |
| wins2      | <ip address>  | 6/6                   | secondary WINS server   |

Subgroup of **network: ipv6**

| NAME           | VALUE        | SECURITY<br>(get/set) | DESCRIPTION     |
|----------------|--------------|-----------------------|-----------------|
| enable         | <boolean>    | 6/6                   | Enable IPv6     |
| addonipaddress | <ip address> | 6/6                   | IPv6 IP address |

|                |              |     |   |
|----------------|--------------|-----|---|
| addonprefixlen | 0~128        | 6/6 | IPv6 prefix length                          |
| addonrouter    | <ip address> | 6/6 | IPv6 router address                         |
| addondns       | <ip address> | 6/6 | IPv6 DNS address                            |
| allowoptional  | <boolean>    | 6/6 | Allow Manually setup the IP address setting |

Subgroup of **network: sip**

| NAME | VALUE            | SECURITY<br>(get/set) | DESCRIPTION |
|------|------------------|-----------------------|-------------|
| port | 554, 1025~ 65535 | 6/6                   | SIP port    |

Subgroup of **network: ftp**

| NAME | VALUE          | SECURITY<br>(get/set) | DESCRIPTION           |
|------|----------------|-----------------------|-----------------------|
| port | 21, 1025~65535 | 6/6                   | local ftp server port |

Subgroup of **network: http**

| NAME          | VALUE            | SECURITY<br>(get/set) | DESCRIPTION                               |
|---------------|------------------|-----------------------|---|
| port          | 80, 1025~ 65535  | 6/6                   | HTTP port                                 |
| alternateport | 1025~65535       | 6/6                   | Alternative HTTP port                     |
| authmode      | basic,<br>digest | 1/6                   | HTTP authentication mode                  |
| s0_accessname | string[32]       | 1/6                   | Http server push access name for stream 1 |
| s1_accessname | string[32]       | 1/6                   | Http server push access name for stream 2 |

Subgroup of **network: https**

| NAME | VALUE            | SECURITY<br>(get/set) | DESCRIPTION |
|------|------------------|-----------------------|-------------|
| port | 443, 1025~ 65535 | 6/6                   | HTTPS port  |

Subgroup of **network: rtsp**

| NAME     | VALUE              | SECURITY<br>(get/set) | DESCRIPTION              |
|----------|--------------------|-----------------------|--------------------------|
| port     | 554, 1025 ~ 65535  | 1/6                   | RTSP port                |
| authmode | disable,<br>basic, | 1/6                   | RTSP authentication mode |

|               |            |     |  |
|---------------|------------|-----|--|
|               | digest     |     |  |
| s0_accessname | string[32] | 1/6 | RTSP access name for stream1                             |
| s1_accessname | string[32] | 1/6 | RTSP access name for stream2                             |
| s0_audiotrack | <integer>  | 6/6 | The current audio track for stream1.<br>-1 => audio mute |
| s1_audiotrack | <integer>  | 6/6 | The current audio track for stream2.<br>-1 => audio mute |

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

| NAME            | VALUE        | SECURITY<br>(get/set) | DESCRIPTION                  |
|-----------------|--------------|-----------------------|------------------------------|
| alwaysmulticast | <boolean>    | 4/4                   | Enable always multicast      |
| ipaddress       | <ip address> | 4/4                   | Multicast IP address         |
| videoport       | 1025 ~ 65535 | 4/4                   | Multicast video port         |
| audioport       | 1025 ~ 65535 | 4/4                   | Multicast audio port         |
| ttl             | 1 ~ 255      | 4/4                   | Multicast time to live value |

Subgroup of **network: rtp**

| NAME      | VALUE       | SECURITY<br>(get/set) | DESCRIPTION                |
|-----------|-------------|-----------------------|----------------------------|
| videoport | 1025~ 65535 | 6/6                   | video channel port for RTP |
| audioport | 1025~ 65535 | 6/6                   | audio channel port for RTP |

Subgroup of **network: pppoe**

| NAME | VALUE        | SECURITY<br>(get/set) | DESCRIPTION             |
|------|--------------|-----------------------|-------------------------|
| user | string[128]  | 6/6                   | PPPoE account user name |
| pass | password[64] | 6/6                   | PPPoE account password  |

Group: **ipfilter**

| NAME          | VALUE      | SECURITY<br>(get/set) | DESCRIPTION                     |
|---------------|------------|-----------------------|---------------------------------|
| enable        | <boolean>  | 6/6                   | Enable access list filtering    |
| admin_enable  | <boolean>  | 6/6                   | Enable administrator IP address |
| admin_ip      | String[44] | 6/6                   | Administrator IP address        |
| maxconnection | 1~10       | 6/6                   | Maximum number of concurrent    |

|                    |                           |     |  |
|--------------------|---------------------------|-----|--|
|                    |                           |     | streaming connection(s)                      |
| allow_i<0~9>_start | 1.0.0.0 ~ 255.255.255.255 | 6/6 | Allowed starting IPv4 address for connection |
| allow_i<0~9>_end   | 1.0.0.0 ~ 255.255.255.255 | 6/6 | Allowed ending IPv4 address for connection   |
| deny_i<0~9>_start  | 1.0.0.0 ~ 255.255.255.255 | 6/6 | Denied starting IPv4 address for connection  |
| deny_i<0~9>_end    | 1.0.0.0 ~ 255.255.255.255 | 6/6 | Denied ending IPv4 address for connection    |
| ipv6_allow_i<0~9>  | String[44]                | 6/6 | Allowed IPv6 address for connection          |
| ipv6_deny_i<0~9>   | String[44]                | 6/6 | Denied IPv6 address for connection           |

Group: **videoin**

| NAME         | VALUE        | SECURITY (get/set) | DESCRIPTION                     |
|--------------|--------------|--------------------|---------------------------------|
| cmosfreq     | 50, 60       | 4/4                | CMOS frequency                  |
| whitebalance | auto, manual | 4/4                | auto, auto white balance manual |
| atwbvalue    | 0 ~ 65535    | 4/4                | The auto white balance value.   |

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

| NAME      | VALUE     | SECURITY (get/set) | DESCRIPTION  |
|-----------|-----------|--------------------|--|
| color     | 0, 1      | 4/4                | 0 => monochrome<br>1 => color  |
| flip      | <boolean> | 4/4                | flip the image   |
| mirror    | <boolean> | 4/4                | mirror the image   |
| ptzstatus | <integer> | 1/7                | An 32-bits integer, each bit can be set separately as follows:<br>Bit 0 => Support camera control function 0(not support), 1(support)<br>Bit 1 => <b>Build-in</b> or <b>external</b> camera. 0(external), 1(build-in)<br>Bit 2 => Support <b>pan</b> operation. 0(not support), 1(support)<br>Bit 3 => Support <b>tilt</b> operation. 0(not support), 1(support) |



|                                      |   |     |   |
|--------------------------------------|---|-----|---|
|                                      |   |     | Bit 4 => Support <b>zoom</b> operation. 0(not support), 1(support)<br>Bit 5 => Support <b>focus</b> operation. 0(not support), 1(support) |
| text                                 | string[16]  | 1/4 | enclosed caption  |
| imprinttimestamp                     | <boolean>   | 4/4 | Overlay time stamp on video   |
| maxexposure                          | 1~120   | 4/4 | Maximum exposure time   |
| s<0~(m-1)>_codec<br>type             | mpeg4,<br>mjpeg   | 4/4 | video codec type  |
| s<0~(m-1)>_resol<br>ution            | 176x144,<br>320x240,<br>640x480   | 4/4 | Video resolution in pixel   |
| s<0~(m-1)>_mpeg<br>4_intraperiod     | 250, 500,<br>1000, 2000,<br>3000, 4000                                  | 4/4 | The period of intra frame in milliseconds   |
| s<0~(m-1)>_mpeg<br>4_ratecontrolmode | cbr, vbr  | 4/4 | cbr, constant bitrate<br>vbr, fix quality   |
| s<0~(m-1)>_mpeg<br>4_quant           | 1~5   | 4/4 | quality of video when choosing vbr in "ratecontrolmode".<br>1 is worst quality and 5 is the best quality.                                 |
| s<0~(m-1)>_mpeg<br>4_qvalue          | 1~31  | 7/4 | Quality parameter of mpeg4 encoder.<br>1 is best quality and 31 is the worst quality.   |
| s<0~(m-1)>_mpeg<br>4_bitrate         | 1000~4000<br>000  | 4/4 | Set bit rate in bps when choose cbr in "ratecontrolmode"  |
| s<0~(m-1)>_mpeg<br>4_maxframe        | 1, 2, 3, 5,<br>10, 15, 20,<br>25, 30 (only<br>for NTSC or<br>60Hz CMOS) | 4/4 | set maximum frame rate in fps (for MPEG-4)  |
| s<0~(m-1)>_mjpe<br>g_quant           | 1 ~ 5   | 4/4 | quality of jpeg video.<br>1 is worst quality and 5 is the best quality.   |
| s<0~(m-1)>_mjpe<br>g_qvalue          | 10~200  | 7/4 | The specific quality parameter of jpeg encoder.<br>10 is best quality and 200 is the worst quality.                                       |
| s<0~(m-1)>_mjpe                      | 1~25,   | 4/4 | set maximum frame rate in fps (for  |

|                   |                                    |     |               |
|-------------------|------------------------------------|-----|---------------|
| g_maxframe        | 26~30 (only for NTSC or 60Hz CMOS) |     | JPEG)         |
| s<0~(m-1)>_forcei | 1                                  | 7/6 | Force I frame |

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

| NAME                    | VALUE  | SECURITY (get/set) | DESCRIPTION  |
|-------------------------|--|--------------------|--|
| source                  | micin, linein                                    | 4/4                | micin => use external microphone input<br>linein => use line input |
| mute                    | 0, 1   | 1/4                | Enable audio mute  |
| gain                    | 0~31   | 4/4                | Gain of input  |
| boostmic                | 0, 1   | 4/4                | Enable microphone boost  |
| s<0~(m-1)>_codectype    | aac4, gamr                                       | 4/4                | set audio codec type for input                                     |
| s<0~(m-1)>_aac4_bitrate | 16000, 32000, 48000, 64000, 96000, 128000        | 4/4                | set AAC4 bitrate in bps  |
| s<0~(m-1)>_gamr_bitrate | 4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200 | 4/4                | set AMR bitrate in bps   |

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

| NAME       | VALUE  | SECURITY (get/set) | DESCRIPTION  |
|------------|--------|--------------------|--|
| brightness | -5 ~ 5 | 4/4                | Adjust brightness of image according to mode settings. |
| saturation | -5 ~ 5 | 4/4                | Adjust saturation of image according to mode settings. |
| contrast   | -5 ~ 5 | 4/4                | Adjust contrast of image according to mode settings.   |

|           |        |     |   |
|-----------|--------|-----|---|
| sharpness | -3 ~ 3 | 4/4 | Adjust sharpness of image according to mode settings. |
|-----------|--------|-----|---|

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

| NAME                 | VALUE           | SECURITY<br>(get/set) | DESCRIPTION  |
|----------------------|-----------------|-----------------------|--|
| brightness           | -5 ~ 5          | 4/4                   | Preview of adjusting brightness of image according to mode settings.   |
| saturation           | -5 ~ 5          | 4/4                   | Preview of adjusting saturation of image according to mode settings.   |
| contrast             | -5 ~ 5          | 4/4                   | Preview of adjusting contrast of image according to mode settings.     |
| sharpness            | -3 ~ 3          | 4/4                   | Preview of adjusting sharpness of image according to mode settings.    |
| videoin_whitebalance | auto,<br>manual | 4/4                   | Preview of adjusting white balance of image according to mode settings |
| videoin_restoreatwb  | 0, 1~           | 4/4                   | Restore of adjusting white balance of image according to mode settings |

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

| NAME                   | VALUE      | SECURITY<br>(get/set) | DESCRIPTION                             |
|------------------------|------------|-----------------------|---|
| enable                 | <boolean>  | 4/4                   | enable motion detection                 |
| win_i<0~2>_enable      | <boolean>  | 4/4                   | enable motion window 1~3                |
| win_i<0~2>_name        | string[14] | 4/4                   | name of motion window 1~3               |
| win_i<0~2>_left        | 0 ~ 320    | 4/4                   | Left coordinate of window position.     |
| win_i<0~2>_top         | 0 ~ 240    | 4/4                   | Top coordinate of window position.      |
| win_i<0~2>_width       | 0 ~ 320    | 4/4                   | Width of motion detection window.       |
| win_i<0~2>_height      | 0 ~ 240    | 4/4                   | Height of motion detection window.      |
| win_i<0~2>_objsize     | 0 ~ 100    | 4/4                   | Percent of motion detection window.     |
| win_i<0~2>_sensitivity | 0 ~ 100    | 4/4                   | Sensitivity of motion detection window. |

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

| NAME      | VALUE     | SECURITY<br>(get/set) | DESCRIPTION                            |
|-----------|-----------|-----------------------|--|
| enable    | <boolean> | 4/4                   | Enable or disable tampering detection. |
| threshold | 0 ~ 255   | 4/4                   | Threshold of tampering detection       |

|          |          |     |  |
|----------|----------|-----|--|
| duration | 10 ~ 600 | 4/4 | If tampering value exceeds the 'threshold' for more than 'duration' then tampering detection is triggered. |
|----------|----------|-----|--|

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

| NAME              | VALUE       | SECURITY<br>(get/set) | DESCRIPTION                         |
|-------------------|-------------|-----------------------|-------------------------------------|
| enable            | <boolean>   | 4/4                   | Enable the privacy mask             |
| win_i<0~4>_enable | <boolean>   | 4/4                   | Enable the privacy mask window      |
| win_i<0~4>_name   | string[14]  | 4/4                   | The name of privacy mask window     |
| win_i<0~4>_left   | 0 ~ 320/352 | 4/4                   | Left coordinate of window position. |
| win_i<0~4>_top    | 0 ~ 240/288 | 4/4                   | Top coordinate of window position.  |
| win_i<0~4>_width  | 0 ~ 320/352 | 4/4                   | Width of privacy mask window        |
| win_i<0~4>_height | 0 ~ 240/288 | 4/4                   | Height of privacy mask window       |

Group: **ddns**

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

|            |  |  |  |
|------------|--|--|--|
| servername |  |  | (This field only exists for provider is customsafel00) |
|------------|--|--|--|

Group: **upnpresentation**

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

Group: **upnpportforwarding**

| NAME          | VALUE     | SECURITY<br>(get/set) | DESCRIPTION  |
|---------------|-----------|-----------------------|--|
| enable        | <boolean> | 6/6                   | Enable or disable the UPNP port forwarding service.  |
| upnpnatstatus | 0~3       | 6/7                   | The status of UpnP port forwarding, used internally.<br>0 is OK, 1 is FAIL, 2 is no IGD router, 3 is no need to do port forwarding |

Group: **syslog**

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

Group: **capability**

| NAME            | VALUE                 | SECURITY<br>(get/set) | DESCRIPTION  |
|-----------------|-----------------------|-----------------------|--|
| api_httpversion | 0100a                 | 0/7                   | The HTTP API version.  |
| bootuptime      | <positive integer>    | 0/7                   | The server bootup time   |
| nir             | 0, <positive integer> | 0/7                   | number of IR interface   |
| npir            | 0, <positive integer> | 0/7                   | number of PIR  |
| ndi             | 0, <positive integer> | 0/7                   | number of digital input  |
| ndo             | 0, <positive integer> | 0/7                   | number of digital output   |
| naudioin        | 0, <positive integer> | 0/7                   | number of audio input  |
| naudioout       | 0, <positive integer> | 0/7                   | number of audio output   |
| nvideoin        | <positive integer>    | 0/7                   | number of video input  |
| nmediastream    | <positive integer>    | 0/7                   | number of media stream per channel   |
| nvideosetting   | <positive integer>    | 0/7                   | number of video settings per channel   |
| naudiosetting   | <positive integer>    | 0/7                   | number of audio settings per channel   |
| nuart           | 0, <positive integer> | 0/7                   | number of UART interface   |
| ptzenabled      | < positive integer >  | 0/7                   | An 32-bits integer, each bit can be set separately as follows:<br>Bit 0 => Support camera control function<br>0(not support), 1(support)<br>Bit 1 => Build-in or external camera.<br>0(external), 1(build-in)<br>Bit 2 => Support pan operation. 0(not support), 1(support)<br>Bit 3 => Support tilt |

|                                    |  |     |  |
|------------------------------------|--|-----|--|
|                                    |  |     | operation. 0(not support), 1(support)<br>Bit 4 => Support zoom operation.<br>0(not support), 1(support)<br>Bit 5 => Support focus operation.<br>0(not support), 1(support) |
| protocol_https                     | < boolean >                                      | 0/7 | indicate whether to support http over SSL  |
| protocol_rtsp                      | < boolean >                                      | 0/7 | indicate whether to support rtsp   |
| protocol_sip                       | <boolean>  | 0/7 | indicate whether to support sip  |
| protocol_maxconnection             | <positive integer>                               | 0/7 | The maximum allowed simultaneous connections   |
| protocol_maxgenconnection          | <positive integer>                               | 0/7 | The maximum general streaming connections  |
| protocol_maxmegacconnection        | <positive integer>                               | 0/7 | The maximum mega-pixels streaming connections  |
| protocol_rtp_multicast_scalable    | <boolean>  | 0/7 | indicate whether to support scalable multicast   |
| protocol_rtp_multicast_backchannel | <boolean>  | 0/7 | indicate whether to support backchannel multicast  |
| protocol_rtp_tcp                   | <boolean>  | 0/7 | indicate whether to support rtp over tcp   |
| protocol_rtp_http                  | <boolean>  | 0/7 | indicate whether to support rtp over http  |
| protocol_spush_mjpeg               | <boolean>  | 0/7 | indicate whether to support server push motion jpeg  |
| protocol_snmp                      | <boolean>  | 0/7 | indicate whether to support snmp   |
| protocol_ipv6                      | <boolean>  | 0/7 | indicate whether to support IPv6   |
| videoin_type                       | 0, 1, 2  | 0/7 | 0 => Interlaced CCD<br>1 => Progressive CCD<br>2 => CMOS   |
| videoin_resolution                 | <a list of the available resolution separates by | 0/7 | available resolutions list   |

|                          |   |     |   |
|--------------------------|---|-----|---|
|                          | comma)  |     |   |
| videoin_maxframe<br>rate | <a list of available maximum frame rate separates by comma> | 0/7 | available maximum frame list  |
| videoin_codec            | <a list of the available codec types separators by comma)   | 0/7 | available codec list  |
| videoout_codec           | <a list of the available codec types separators by comma)   | 0/7 | available codec list  |
| audio_aec                | <boolean>   | 0/7 | indicate whether to support acoustic echo cancellation  |
| audio_extmic             | <boolean>   | 0/7 | indicate whether to support external microphone input   |
| audio_linein             | <boolean>   | 0/7 | indicate whether to support external line input   |
| audio_lineout            | <boolean>   | 0/7 | indicate whether to support line output   |
| audio_headphoneout       | <boolean>   | 0/7 | indicate whether to support headphone output  |
| audioin_codec            | <a list of the available codec types separators by comma)   | 0/7 | available codec list  |
| audioout_codec           | <a list of the available codec types separators by comma)   | 0/7 | available codec list  |
| uart_httptunnel          | <boolean>   | 0/7 | Indicate whether to support the http tunnel for uart transfer                                       |
| transmission_mode        | Tx,<br>Rx,<br>Both  | 0/7 | Indicate what kind of transmission mode the machine used. TX: server, Rx: receiver box, Both: DVR?. |



|                       |           |     |   |
|-----------------------|-----------|-----|---|
| network_wire          | <boolean> | 0/7 | Indicate whether to support the Ethernet          |
| network_wireless      | <boolean> | 0/7 | Indicate whether to support the wireless          |
| wireless_802dot11b    | <boolean> | 0/7 | Indicate whether to support the wireless 802.11b+ |
| wireless_802dot11g    | <boolean> | 0/7 | Indicate whether to support the wireless 802.11g  |
| wireless_encrypt_wep  | <boolean> | 0/7 | Indicate whether to support the wireless WEP      |
| wireless_encrypt_wpa  | <boolean> | 0/7 | Indicate whether to support the wireless WPA      |
| wireless_encrypt_wpa2 | <boolean> | 0/7 | Indicate whether to support the wireless WPA2     |

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

| PARAMETER | VALUE      | SECURITY<br>(get/set) | DESCRIPTION                                     |
|-----------|------------|-----------------------|---|
| name      | string[41] | 6/6                   | The custom scripts identification of this entry |
| date      | string[17] | 6/6                   | Date of custom scripts                          |

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

| PARAMETER | VALUE      | SECURITY<br>(get/set) | DESCRIPTION   |
|-----------|------------|-----------------------|---|
| name      | string[40] | 6/6                   | The identification of this entry  |
| enable    | 0, 1       | 6/6                   | To enable or disable this event.  |
| priority  | 0, 1, 2    | 6/6                   | Indicate the priority of this event.<br>"0" indicates low priority.<br>"1" indicates normal priority.<br>"2" indicates high priority. |
| delay     | 1~999      | 6/6                   | Delay seconds before detect next event.   |

|           |  |     |   |
|-----------|--|-----|---|
| trigger   | boot,<br>di,<br>motion,<br>seq,<br>pir,<br>reconfirm,<br>audioswitch,<br>tampering | 6/6 | Indicate the trigger condition.<br>"boot" indicates system boot.<br>"di" indicates digital input.<br>"motion" indicates video motion detection.<br>"seq" indicates periodic condition.<br>"pir" indicates PIR detection.<br>"reconfirm" indicates recording notify.<br>"audioswitch" indicates audio switch.<br>"tampering" indicates tampering detection.                        |
| di        | <integer>  | 6/6 | Indicate which di detected.<br>This field is required when trigger condition is "di".<br>One bit represents one digital input. The LSB indicates DI 0.  |
| mdwin     | <integer>  | 6/6 | Indicate which motion detection windows detected.<br>This field is required when trigger condition is "motion"<br>One bit represents one window.<br>The LSB indicates the 1 <sup>st</sup> window.<br>For example, to detect the 1 <sup>st</sup> and 3 <sup>rd</sup> windows, set mdwin as 5.  |
| inter     | 1~999  | 6/6 | Interval of period snapshot in minute.<br>This field is used when trigger condition is "seq".   |
| weekday   | <integer>  | 6/6 | Indicate which weekday is scheduled.<br>One bit represents one weekday.<br>The bit0 (LSB) indicates Saturday.<br>The bit1 indicates Friday.<br>The bit2 indicates Thursday.<br>The bit3 indicates Wednesday.<br>The bit4 indicates Tuesday.<br>The bit5 indicates Monday.<br>The bit6 indicates Sunday.<br>For example, to detect events on Friday and Sunday, set weekday as 66. |
| begintime | hh:mm  | 6/6 | Begin time of weekly schedule.  |
| endtime   | hh:mm  | 6/6 | End time of weekly schedule.<br>(00:00 ~ 24:00 means always.)   |

|                                  |             |      |   |
|----------------------------------|-------------|------|---|
| lowlightcondition                | 0, 1        | 6/6  | 0 => Do action at all times<br>1 => Do action in low-light conditions |
| action_do_i<0~(n do-1)>_enable   | 0, 1        | 6/6  | To enable or disable trigger digital output.                          |
| action_do_i<0~(n do-1)>_duration | 1~999       | 6/6  | The duration of digital output is triggered in seconds.               |
| action_cf_enable                 | 0, 1        | 6/6  | To enable put media on CF.  |
| action_cf_folder                 | string[128] | 6/6  | The path to store media.  |
| action_cf_media                  | NULL, 0~4   | 6/6  | The index of attached media.  |
| action_cf_datefolder             | <boolean>   | 6/6  | Enable this to create folders by date time and hour automatically.    |
| action_server_i<0~4>_enable      | 0, 1        | 6/6  | To enable or disable this server action.<br>The default value is 0.   |
| action_server_i<0~4>_media       | NULL, 0~4   | 6/6  | The index of attached media.  |
| action_server_i<0~4>_datefolder  | <boolean>   | 6/s6 | Enable this to create folders by date time and hour automatically.    |

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

| PARAMETER     | VALUE                         | SECURITY<br>(get/set) | DESCRIPTION   |
|---------------|-------------------------------|-----------------------|---|
| name          | string[40]                    | 6/6                   | The identification of this entry  |
| type          | email,<br>ftp,<br>http,<br>ns | 6/6                   | Indicate the server type.<br>"email" is email server.<br>"ftp" is ftp server.<br>"http" is http server.<br>"ns" is network storage. |
| http_url      | string[128]                   | 6/6                   | The url of http server to upload.   |
| http_username | string[64]                    | 6/6                   | The username to login in the server.  |
| http_passwd   | string[64]                    | 6/6                   | The password of the user.   |
| ftp_address   | string[128]                   | 6/6                   | The ftp server address  |
| ftp_username  | string[64]                    | 6/6                   | The username to login in the server.  |
| ftp_passwd    | string[64]                    | 6/6                   | The password of the user.   |
| ftp_port      | 0~65535                       | 6/6                   | The port to connect the server.   |
| ftp_location  | string[128]                   | 6/6                   | The location to upload or store the media.  |

|                      |             |     |   |
|----------------------|-------------|-----|---|
| ftp_passive          | 0, 1        | 6/6 | To enable or disable the passive mode.<br>0 is to disable the passive mode.<br>1 is to enable the passive mode. |
| email_address        | string[128] | 6/6 | The email server address  |
| email_sslmode        | 0, 1        | 6/6 | Enable support SSL  |
| email_port           | 0~65535     | 6/6 | The port to connect the server.   |
| email_username       | string[64]  | 6/6 | The username to login in the server.  |
| email_passwd         | string[64]  | 6/6 | The password of the user.   |
| email_senderemail    | string[128] | 6/6 | The email address of sender.  |
| email_recipientemail | string[128] | 6/6 | The email address of recipient.   |
| ns_location          | string[128] | 6/6 | The location to upload or store the media.  |
| ns_username          | string[64]  | 6/6 | The username to login in the server.  |
| ns_passwd            | string[64]  | 6/6 | The password of the user.   |
| ns_workgroup         | string[64]  | 6/6 | The workgroup for network storage.  |

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

| PARAMETER           | VALUE  | SECURITY<br>(get/set) | DESCRIPTION   |
|---------------------|--|-----------------------|---|
| name                | string[40]   | 6/6                   | The identification of this entry  |
| type                | snapshot,<br>systemlog,<br>videoclip,<br>recordmsg | 6/6                   | The media type to send to the server or store by the server.  |
| snapshot_source     | <integer>  | 6/6                   | Indicate the source of media stream.<br>0 means the first stream.<br>1 means the second stream and etc.           |
| snapshot_prefix     | string[16]   | 6/6                   | Indicate the prefix of the filename.  |
| snapshot_datesuffix | 0, 1   | 6/6                   | To add date and time suffix to filename or not.<br>1 means to add date and time suffix.<br>0 means not to add it. |
| snapshot_preevent   | 0 ~ 7  | 6/6                   | It indicates the number of pre-event images.  |
| snapshot_postevent  | 0 ~ 7  | 6/6                   | The number of post-event images.  |

|                       |            |     |   |
|-----------------------|------------|-----|---|
| videoclip_source      | <integer>  | 6/6 | Indicate the source of media stream.<br>0 means the first stream.<br>1 means the second stream and etc. |
| videoclip_prefix      | string[16] | 6/6 | Indicate the prefix of the filename.  |
| videoclip_preevent    | 0 ~ 9      | 6/6 | It indicates the time of pre-event recording in seconds.  |
| videoclip_maxduration | 1 ~ 10     | 6/6 | The time of maximum duration of one video clip in seconds.  |
| videoclip_maxsize     | 50 ~ 1500  | 6/6 | The maximum size of one video clip file in Kbytes.  |

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

| PARAMETER | VALUE      | SECURITY<br>(get/set) | DESCRIPTION  |
|-----------|------------|-----------------------|--|
| name      | string[40] | 6/6                   | The identification of this entry   |
| enable    | 0, 1       | 6/6                   | To enable or disable this recoding.  |
| priority  | 0, 1, 2    | 6/6                   | Indicate the priority of this recoding.<br>"0" indicates low priority.<br>"1" indicates normal priority.<br>"2" indicates high priority. |
| source    | <integer>  | 6/6                   | Indicate the source of media stream.<br>0 means the first stream.<br>1 means the second stream and etc.                                  |
| limitsize | 0,1        | 6/6                   | 0: Entire free space mechanism<br>1: Limit recording size mechanism  |
| cyclic    | 0,1        | 6/6                   | 0: Disable cyclic recording<br>1: Enable cyclic recording  |
| notify    | 0,1        | 6/6                   | 0: Disable recording notification<br>1: Enable recording notification  |

|               |             |     |   |
|---------------|-------------|-----|---|
| notifyserver  | 0~31        | 6/6 | <p>Indicate which notification server is scheduled.</p> <p>One bit represents one application server (server_i0~i4).</p> <p>The bit0 (LSB) indicates server_i0.</p> <p>The bit1 indicates server_i1.</p> <p>The bit2 indicates server_i2.</p> <p>The bit3 indicates server_i3.</p> <p>The bit4 indicates server_i4.</p> <p>For example, enable server_i0, server_i2 and server_i4 to be notification server.</p> <p>The notifyserver value is 21.</p> |
| weekday       | <interger>  | 6/6 | <p>Indicate which weekday is scheduled.</p> <p>One bit represents one weekday.</p> <p>The bit0 (LSB) indicates Saturday.</p> <p>The bit1 indicates Friday.</p> <p>The bit2 indicates Thursday.</p> <p>The bit3 indicates Wednesday.</p> <p>The bit4 indicates Tuesday.</p> <p>The bit5 indicates Monday.</p> <p>The bit6 indicates Sunday.</p> <p>For example, to detect events on Friday and Sunday, set weekday as 66.</p>                          |
| begintime     | hh:mm       | 6/6 | Begin time of weekly schedule.  |
| endtime       | hh:mm       | 6/6 | End time of weekly schedule.<br>(00:00~24:00 means always.)   |
| prefix        | string[16]  | 6/6 | Indicate the prefix of the filename.  |
| cyclesize     | 20~         | 6/6 | The maximum size for cycle recording in Kbytes when choose limit recording size.  |
| reserveamount | 15~         | 6/6 | The reserved amount in Mbytes when choose cyclic recording mechanism.   |
| dest          | cf,<br>0~4  | 6/6 | <p>The destination to store the recording data.</p> <p>"cf" means CF card.</p> <p>"0~4" means the index of network storage.</p>   |
| cffolder      | string[128] | 6/6 | folder name.  |

Group: **https** (product dependent)

| NAME                | VALUE                       | SECURITY<br>(get/set) | DESCRIPTION  |
|---------------------|-----------------------------|-----------------------|--|
| connect             | 1025 ~ 65535                | 7/7                   | Specify the stunnel connect port   |
| enable              | <boolean>                   | 6/6                   | To enable or disable this secure http  |
| policy              | <Boolean>                   | 6/6                   | If the value is 1, it will force http connection redirect to https connection  |
| method              | auto,<br>manual,<br>install | 6/6                   | auto => Create self-signed certificate automatically<br>manual => Create self-signed certificate manually<br>install => Create certificate request and install |
| status              | -2 ~ 1                      | 6/6                   | Specify the https status.<br>-2=>invalid public key<br>-1=>waiting for certificated<br>0=>not installed<br>1=>active   |
| countryname         | string[2]                   | 6/6                   | country name in certificate information  |
| stateorprovincename | string[128]                 | 6/6                   | state or province name in in certificate information   |
| localityname        | string[128]                 | 6/6                   | the locality name in certificate information   |
| organizationname    | string[64]                  | 6/6                   | organization naem in certificate information   |
| unit                | string[32]                  | 6/6                   | organizational unit name in certificate information  |
| commonname          | string[64]                  | 6/6                   | common name in certificate information   |
| validdays           | 0 ~ 9999                    | 6/6                   | certificatation valid period   |

Group: **layout**

| NAME         | VALUE      | SECURITY<br>(get/set) | DESCRIPTION                           |
|--------------|------------|-----------------------|---------------------------------------|
| logo_default | <boolean>  | 1/6                   | 0 => Custom logo<br>1 => Default logo |
| logo_link    | string[40] | 1/6                   | Hyperlink of the logo                 |

|                               |           |     |  |
|-------------------------------|-----------|-----|--|
| theme_option                  | 1~4       | 1/6 | 1~3: One of the default themes<br>4: Custom definition |
| theme_color_font              | string[7] | 1/6 | Font color   |
| theme_color_configfont        | string[7] | 1/6 | Font color of configuration area                       |
| theme_color_titlefont         | string[7] | 1/6 | Font color of video title                              |
| theme_color_controlbackground | string[7] | 1/6 | Background color of control area                       |
| theme_color_configbackground  | string[7] | 1/6 | Background color of configuration area                 |
| theme_color_videobackground   | string[7] | 1/6 | Background color of video area                         |
| theme_color_case              | string[7] | 1/6 | Frame color  |

## Drive the digital output

**Note:** This request requires the privilege of viewer.

**Method:** GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/setdo.cgi?do1=<state>[&do2=<state>]
[&do3=<state>][&do4=<state>][&return=<return page>]
```

Where state is 0, 1. "0" means inactive or normal state while "1" means active or triggered state.

| PARAMETER            | VALUE         | DESCRIPTION  |
|----------------------|---------------|--|
| <b>do&lt;num&gt;</b> | 0, 1          | 0 - inactive, normal state   |
|                      |               | 1 - active, triggered state  |
| <b>return</b>        | <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. |

**Example:** Drive the digital output 1 to triggered state and redirect to an empty page

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



## Query status of the digital input

**Note:** This request requires the privilege of viewer.

**Method:** GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]
```

If no parameter is specified, all the status of digital input will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[di0= <state>]\r\n
[di1= <state>]\r\n
[di2= <state>]\r\n
[di3= <state>]\r\n
```

where <state> can be 0 or 1.

**Example:** Query the status of digital input 1

Request:

```
http://myserver/cgi-bin/dido/getdi.cgi?di1
```

Response:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
di1=1\r\n
```

## Query status of the digital output

**Note:** This request requires the privilege of viewer.

**Method:** GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]
```

If no parameter is specified, all the status of digital output will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[do0=<state>]\r\n
[do1=<state>]\r\n
[do2=<state>]\r\n
[do3=<state>]\r\n
```

where <state> can be 0 or 1.

**Example:** Query the status of digital output 1

Request:

```
http://myserver/cgi-bin/dido/getdo.cgi?do1
```

Response:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
do1=1\r\n
```

## Capture single snapshot

**Note:** This request require normal user privilege

**Method:** GET/POST

Syntax:

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

If the user requests the size larger than all stream setting on the server, this request will failed!

| PARAMETER         | VALUE                  | DEFAULT | DESCRIPTION                        |
|-------------------|------------------------|---------|------------------------------------|
| <b>channel</b>    | 0~(n-1)                | 0       | the channel number of video source |
| <b>resolution</b> | <available resolution> | 0       | The resolution of image            |
| <b>quality</b>    | 1~5                    | 3       | The quality of image               |

Server will return the most up-to-date snapshot of selected channel and stream 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.  |
|           | viewer        | viewer's privilege  |
|           | operator      | operator's privilege  |
|           | admin         | administrator's 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 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
```

## 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.

## IP filtering

**Note:** This request requires administrator access privilege

**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 a set of allow IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.  |
|           | adddeny     | Add a set of deny IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.   |
|           | deleteallow | Remove a set of allow IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter. |

|        |               |  |
|--------|---------------|--|
|        | deletedeny    | Remove a set of deny IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter. |
| start  | <ip address>  | The start IP address to add or to delete.  |
| end    | <ip address>  | The end 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 current path. If you omit this parameter, it will redirect to an empty page.  |

## Event/Control HTTP tunnel channel

**Note:** This request requires **admin** privilege

**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 the 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 some proxy server.

This channel will help to do real-time event notification and control. The event and control format are described in another document.

## Get SDP of Streamings

**Note:** This request requires viewer access privilege

**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 method.

## Open the network streamings

**Note:** This request requires viewer access privilege

Syntax:

For http push server (mjpeg):

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

For rtsp (mp4), user needs to input the url below for a rtsp compatible player.

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

"m" is the stream number.

For detailed streaming protocol, please refer to "control signaling" and "data format" documents.

# Technical Specifications

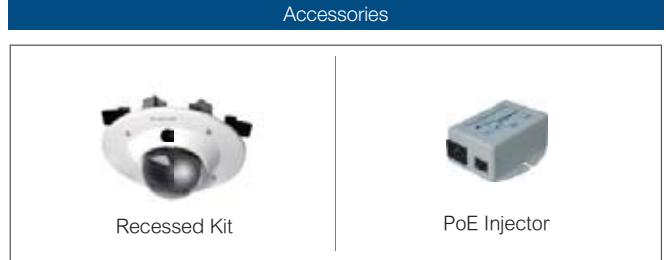
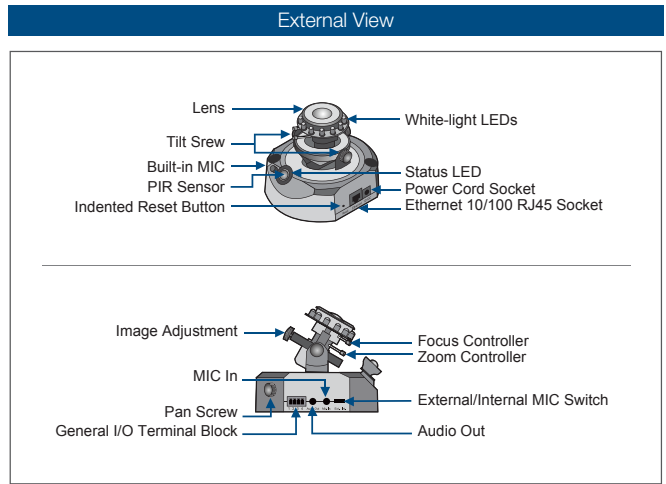
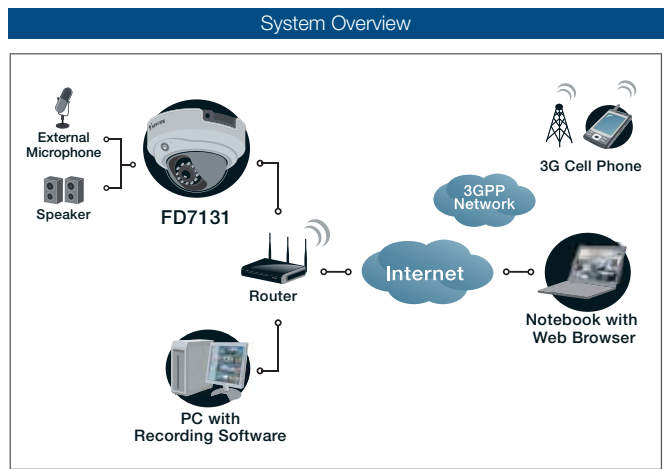
|                                   |  |
|-----------------------------------|--|
| <b>System</b>                     | <ul style="list-style-type: none"> <li>· CPU: VVTK-1000 SoC</li> <li>· Flash: 8MB</li> <li>· RAM: 64MB</li> <li>· Embedded OS: Linux 2.4</li> </ul>  |
| <b>Lens</b>                       | <ul style="list-style-type: none"> <li>· Board lens, vari-focal, f=2 ~ 4 mm, F1.4 (wide), F1.8 (tele), focus range: 50 cm to infinity</li> </ul>   |
| <b>Angle of View</b>              | <ul style="list-style-type: none"> <li>· 53.2° ~ 105.1° (horizontal)</li> <li>· 39.8° ~ 77.4° (vertical)</li> </ul>  |
| <b>Shutter Time</b>               | <ul style="list-style-type: none"> <li>· 1/5, 1/15, 1/30 sec.</li> </ul>   |
| <b>Image sensor</b>               | <ul style="list-style-type: none"> <li>· 1/4" CMOS sensor in VGA resolution</li> </ul>   |
| <b>Minimum Illumination</b>       | <ul style="list-style-type: none"> <li>· 1.5 Lux / F1.4</li> </ul>   |
| <b>Video</b>                      | <ul style="list-style-type: none"> <li>· Compression: MJPEG &amp; MPEG-4</li> <li>· Streaming: Simultaneous dual-streaming</li> <li>· MPEG-4 streaming over UDP, TCP, HTTP or HTTPS</li> <li>· MPEG-4 multicast streaming</li> <li>· MJPEG streaming over HTTP or HTTPS</li> <li>· Supports 3GPP mobile surveillance</li> <li>· Frame rates:                             <ul style="list-style-type: none"> <li>· MPEG-4: Up to 30/25 fps at 640x480</li> <li>· MJPEG: Up to 30/25 fps at 640x480</li> </ul> </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, and white balance</li> <li>· AWB</li> <li>· Supports privacy masks</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>· MPEG-4 AAC audio encoding, bit rate: 16 kbps to 128 kbps</li> </ul> </li> <li>· Interface:                             <ul style="list-style-type: none"> <li>· Built-in microphone</li> <li>· External microphone input</li> <li>· Audio output</li> <li>· External/Internal microphone switch</li> </ul> </li> <li>· Supports two-way audio via SIP protocol</li> <li>· Supports audio mute</li> </ul> |
| <b>Networking</b>                 | <ul style="list-style-type: none"> <li>· 10/100 Mbps Ethernet, RJ-45</li> <li>· Protocols: IPv4, TCP/IP, HTTP, HTTPS, UPnP, RTSP/ RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, and PPPoE</li> </ul>  |
| <b>Alarm and Event Management</b> | <ul style="list-style-type: none"> <li>· Triple-window video motion detection</li> <li>· One D/I and one D/O for external sensor and alarm</li> <li>· Passive infrared sensor (PIR) for human detection</li> <li>· White-light illuminators for low light condition when event triggered</li> <li>· Event notification using HTTP, SMTP, or FTP</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> </ul>  |
| <b>Users</b>                      | <ul style="list-style-type: none"> <li>· Camera live viewing for up to 10 clients</li> </ul>   |
| <b>Dimension</b>                  | <ul style="list-style-type: none"> <li>· Ø 143 mm x 106 mm</li> </ul>  |
| <b>Weight</b>                     | <ul style="list-style-type: none"> <li>· Net: 575.5 g</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> </ul>  |
| <b>Power</b>                      | <ul style="list-style-type: none"> <li>· 12V DC</li> <li>· Power consumption: Max. 3.6 W</li> <li>· 802.3af compliant Power-over-Ethernet</li> </ul>   |
| <b>Approvals</b>                  | <ul style="list-style-type: none"> <li>· CE, LVD, FCC, VCCI, C-Tick</li> </ul>   |
| <b>Operating Environments</b>     | <ul style="list-style-type: none"> <li>· Temperature: 0 ~ 50 °C (32 ~ 122 °F)</li> <li>· Humidity: 20% ~ 80% RH</li> </ul>   |

|                                    |   |
|------------------------------------|---|
| <b>Viewing System Requirements</b> | <ul style="list-style-type: none"> <li>· OS: Microsoft Windows 2000/XP/Vista</li> <li>· Browser: Internet Explorer 6.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>Installation, Management, and Maintenance</b> | <ul style="list-style-type: none"> <li>· 3-axis mechanism for flexible ceiling and wall mount installation</li> <li>· Installation Wizard 2</li> <li>· 16-CH recording software</li> <li>· Supports firmware upgrade</li> </ul> |
|--|---|

|                     |  |
|---------------------|--|
| <b>Applications</b> | <ul style="list-style-type: none"> <li>· SDK available for application development and system integration</li> </ul> |
|---------------------|--|

|                 |   |
|-----------------|---|
| <b>Warranty</b> | <ul style="list-style-type: none"> <li>· 24 months</li> </ul> |
|-----------------|---|



All specifications are subject to change without notice. Copyright©2009 VIVOTEK INC. All rights reserved.



## Technology License Notice

### MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT WITH REGARD TO PC SOFTWARE, OF WHICH YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO [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.mpeg-la.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.

### 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.