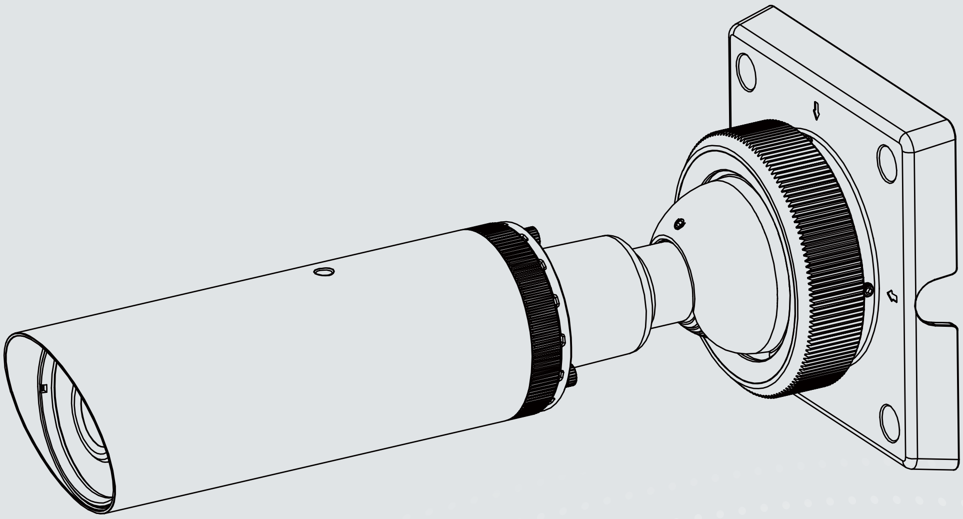
VIVOTEK

IP8332-C Bullet Network Camera

User's Manual

Outdoor • Day & Night • Weather-proof • Cable Management



Rev. 1.0

Table of Contents

Overview

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

- IP8332-C
- Alignment Sticker
- L-type Hex Key Wrench / Desiccant Bag / Screws / RJ45 Female/Female Coupler /Waterproof Connector
- Ball Swivel Mount Bracket
- Quick Installation Guide / Warranty Card
- Software CD

Revision History

- Rev. 1.0: Initial release.

Symbols and Statements in this Document

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

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

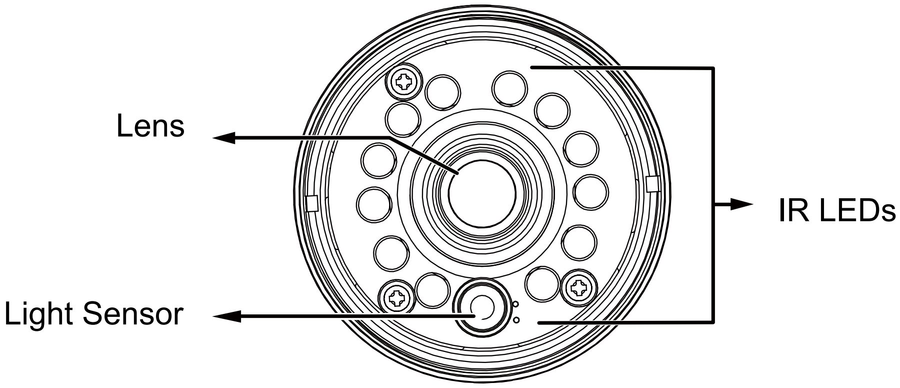
Tips: Tips are useful information that helps enhance or facilitae an installation, function, or process.

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

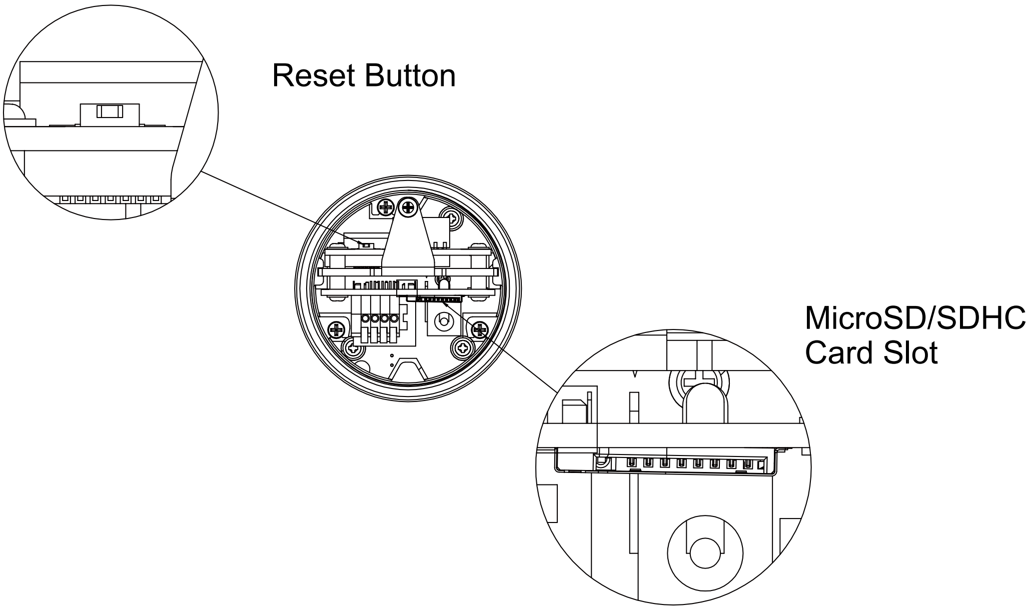
Electrical Hazard: This statement appears when high voltage electrical hazards might occur to an operator.

Physical Description

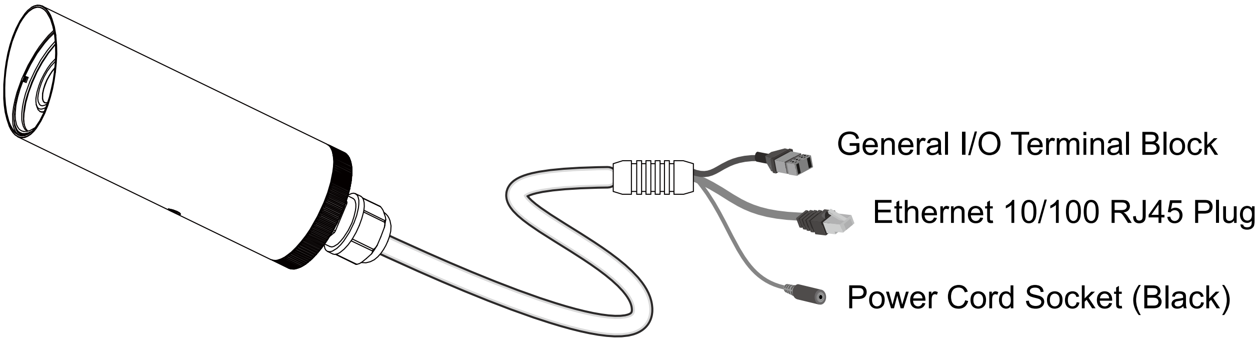
Front Panel



Back Panel

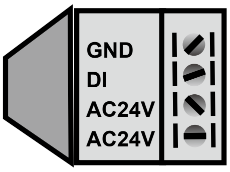


Connectors


General I/O Terminal Block
Ethernet 10/100 RJ45 Plug
Power Cord Socket (Black)

General I/O Terminal Block

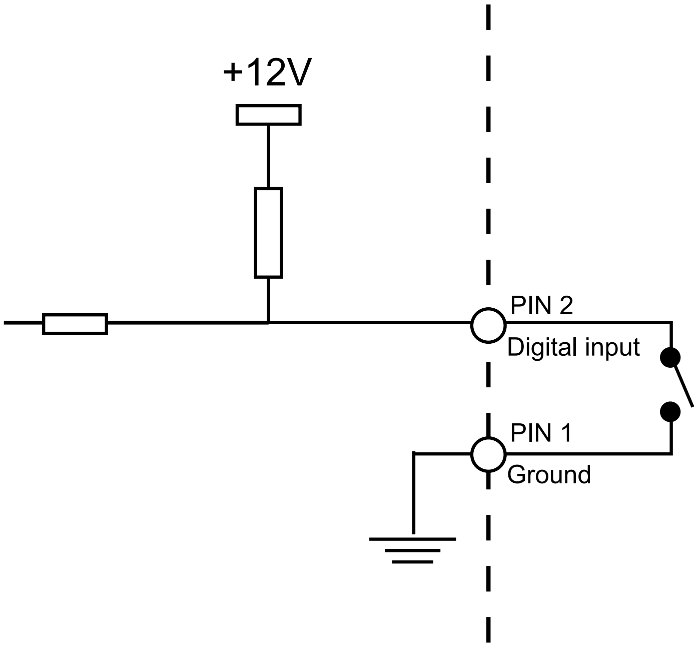
This Network Camera provides a general I/O terminal block which is used to connect external input devices. The pin definitions are described below.



Pin	Name
GND	Ground
DI	Digital Iutput
AC24V	24V
AC24V	24V

DI Diagram

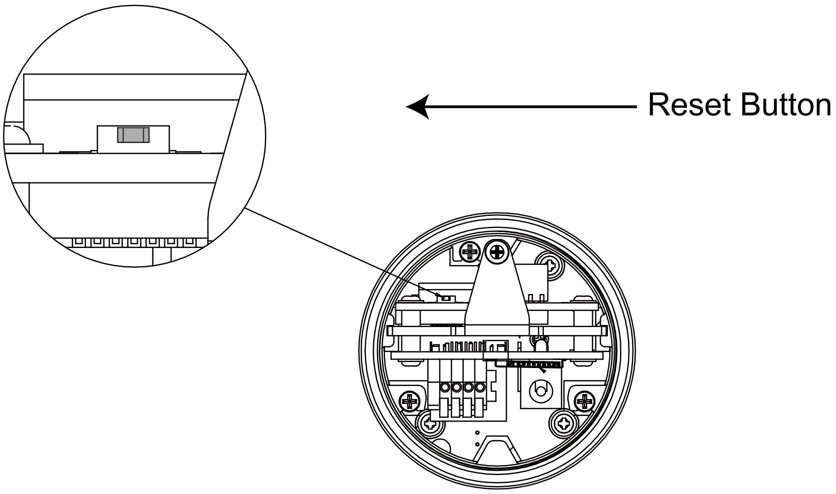
Please refer to the following illustration for the connection method.



MicroSD/SDHC Card Capacity

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

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 recessed reset button with a paper clip or thin object. Wait for the Network Camera to reboot.

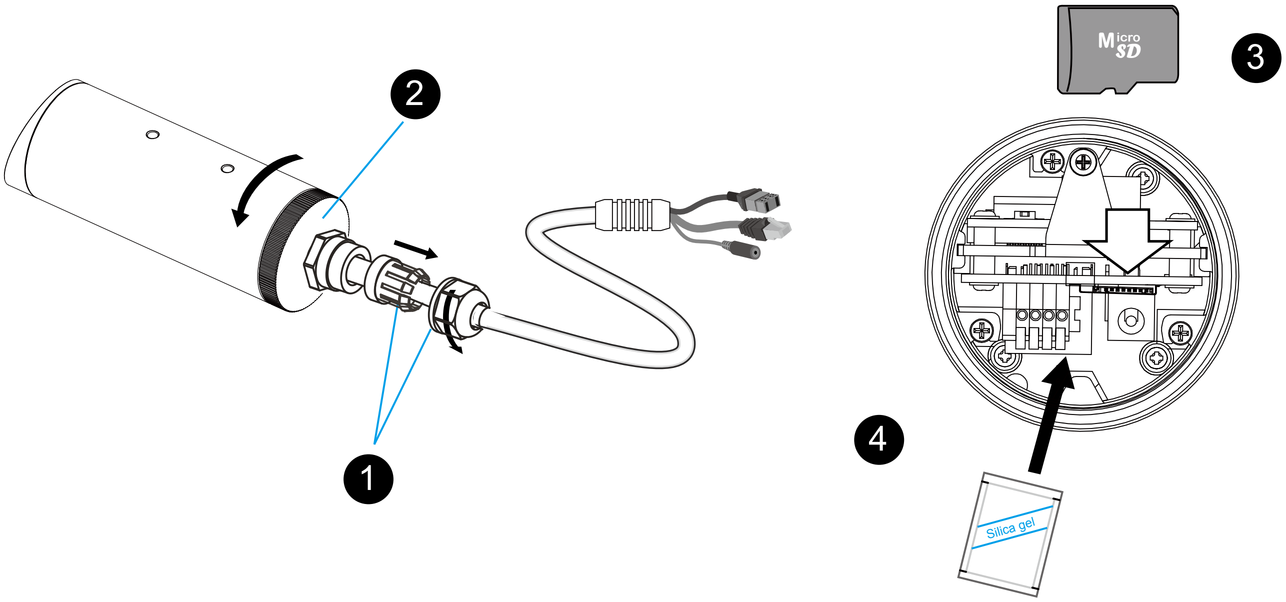
Restore: Press and hold the recessed reset button until the status LED rapidly blinks. Note that all settings will be restored to factory default. Upon successful restore, the status LED will blink green and red during normal operation.

Installation

Hardware Installation

If you prefer installing a MicroSD card as onboard storage:

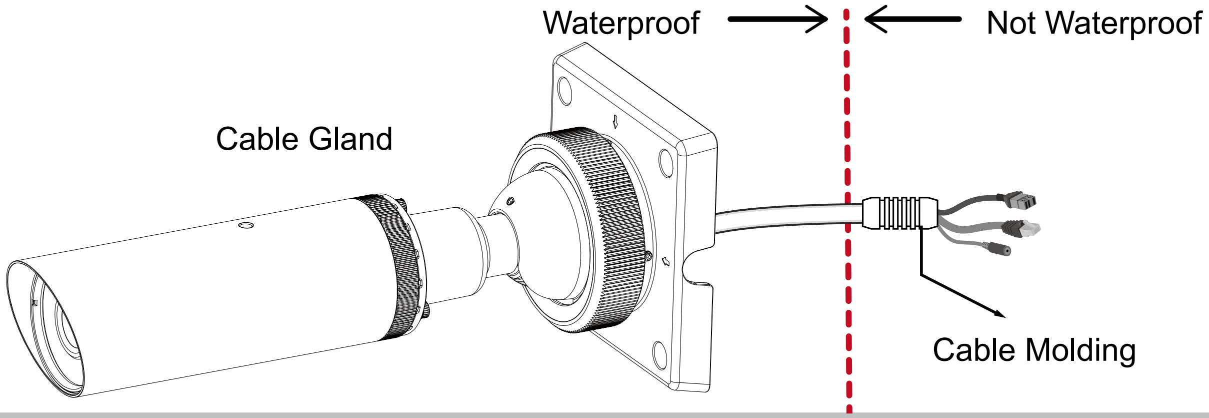
1. Loosen the waterproof connector, and then remove the rubber seal, and the waterproof connector.
2. Loosen and open the rear cover.
3. Install a MicroSD/SDHC card.
4. Tear down the aluminum foil vacuum bag and take out the dessicant bag. Attach the supplied desiccant bag to the inner side of the Network Camera. (Please replace the dessicant bag with a new one every time you open the rear cover.)
5. Make sure all cable lines are securely connected.



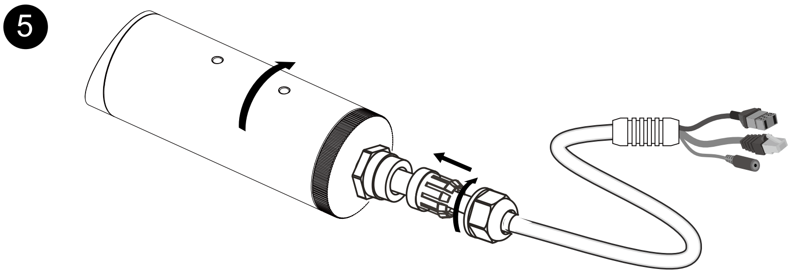
IMPORTANT:

Although the camera and the cable gland on the camera's end are waterproof, the cable molding at the other end is not waterproof.

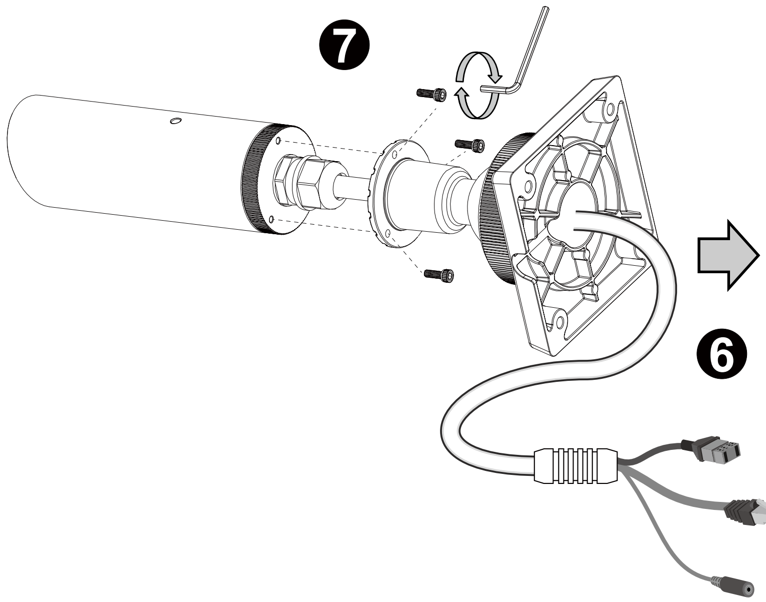
Measures should be taken to prevent water from leaking in through the cable-end molding, such as the use of expanding foam sealant, putties, and so on. Note that the cable gland on the camera should also be securely fastened to attain its waterproof functionality.



5. Tighten the rear cover, rubber seal and waterproof connector.



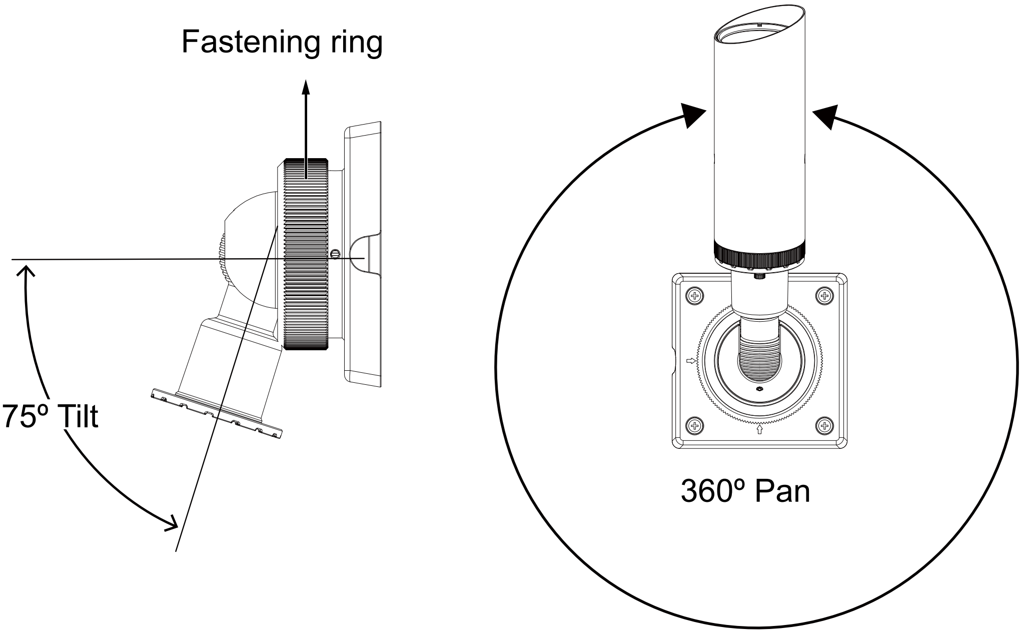
6. Pass the cables through the center of the ball swivel mount bracket, one at a time.
7. Fasten the bracket to the camera using 3 hex socket screws.



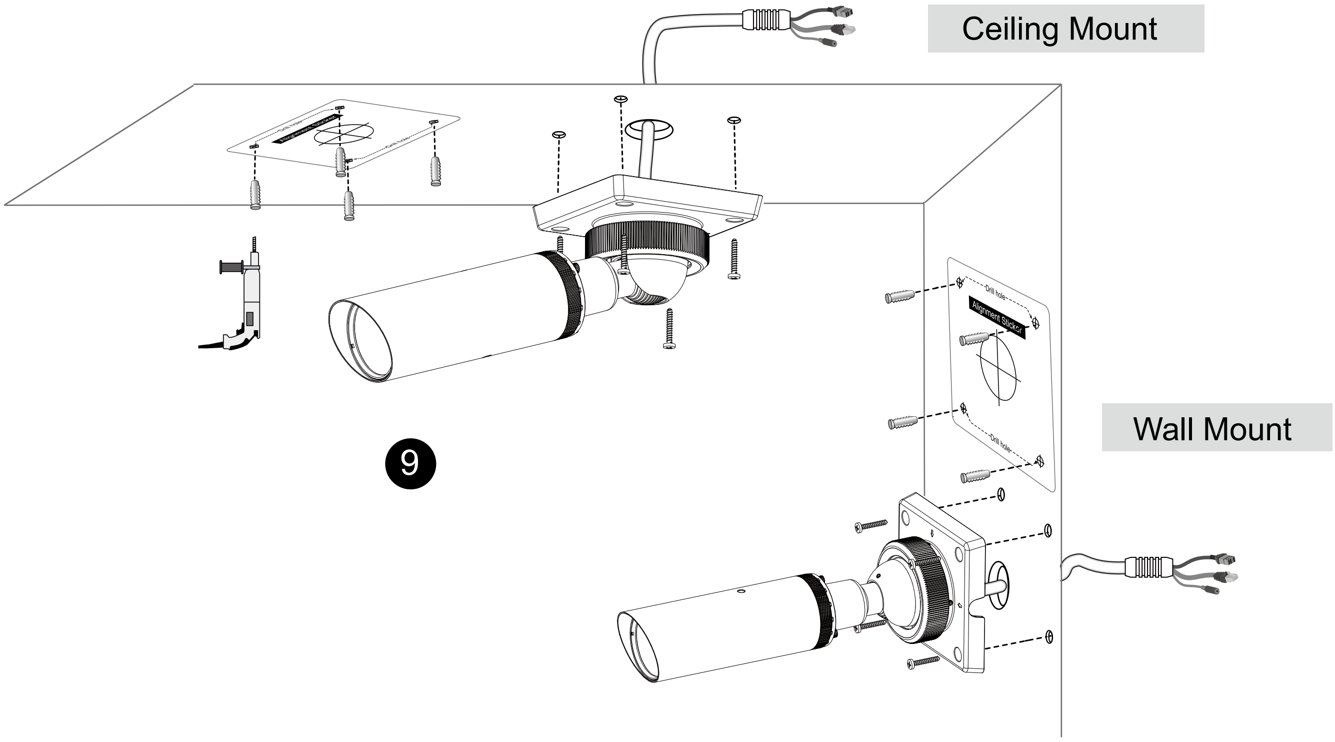
NOTE:

The camera weighs up to 1.28 kgs. Make sure the mounting surface can support this camera.

8. Loosen the fastening ring on the mount bracket, and aim the camera at the area of your interest. When done, tighten the fastening ring.



9. Secure the Network Camera to a wall or ceiling.

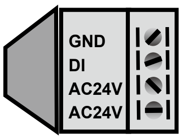


Network Deployment

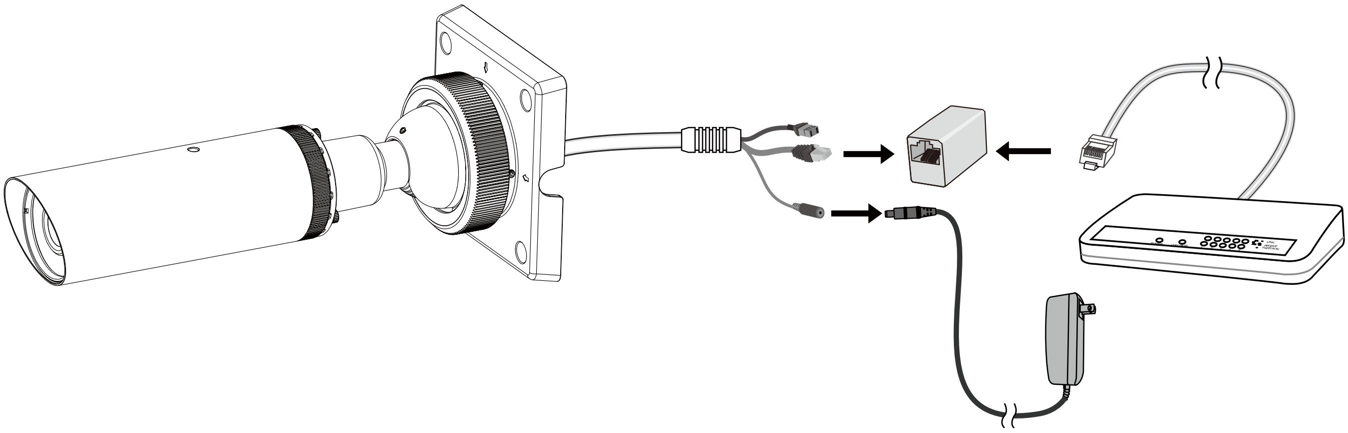
Setting up the Network Camera over the Internet

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. Use the supplied RJ45 female/female coupler to connect the Network Camera to a switch. Use a Category 5 Cross Cable when Network Camera is directly connected to PC.
3. Connect the power cable from the Network Camera to a power outlet.



GND: Ground
DI: Digital Input
AC24V: 24V
AC24V: 24V

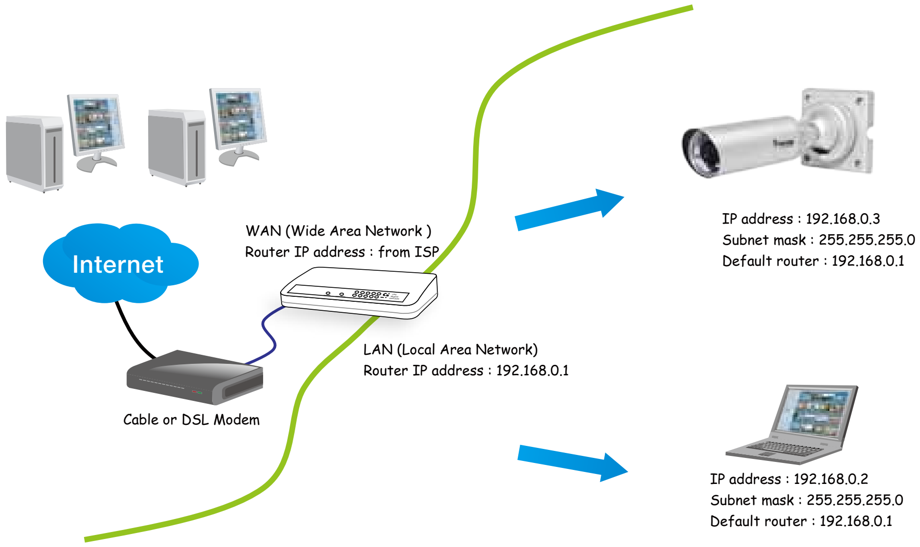


There are several ways to set up the Network Camera over the Internet. The first way is to set up the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

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 13 for details.


Internet
WAN (Wide Area Network)
Router IP address : from ISP
Cable or DSL Modem
LAN (Local Area Network)
Router IP address : 192.168.0.1
IP address : 192.168.0.3
Subnet mask : 255.255.255.0
Default router : 192.168.0.1
IP address : 192.168.0.2
Subnet mask : 255.255.255.0
Default router : 192.168.0.1

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

■ HTTP port: default is 80
■ RTSP port: default is 554
■ RTP port for audio: default is 5558
■ RTCP port for audio: default is 5559
■ RTP port for video: default is 5556
■ RTCP port for video: default is 5557

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

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 37 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 37 for details.

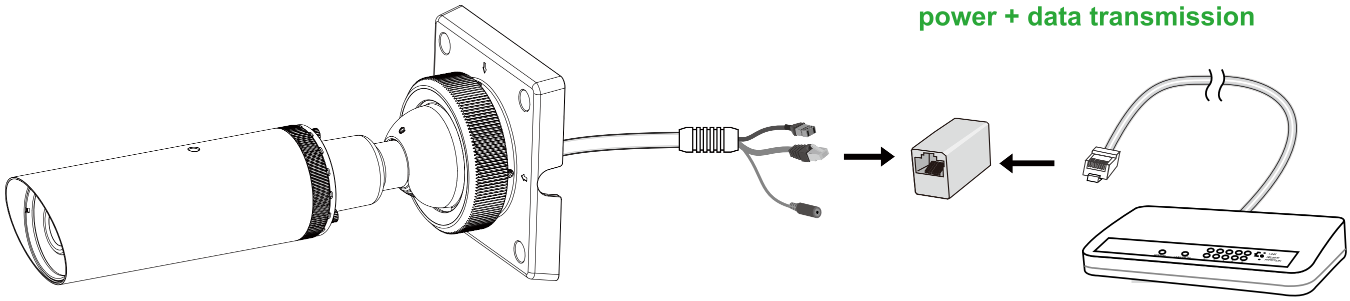
Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 38 for details.

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

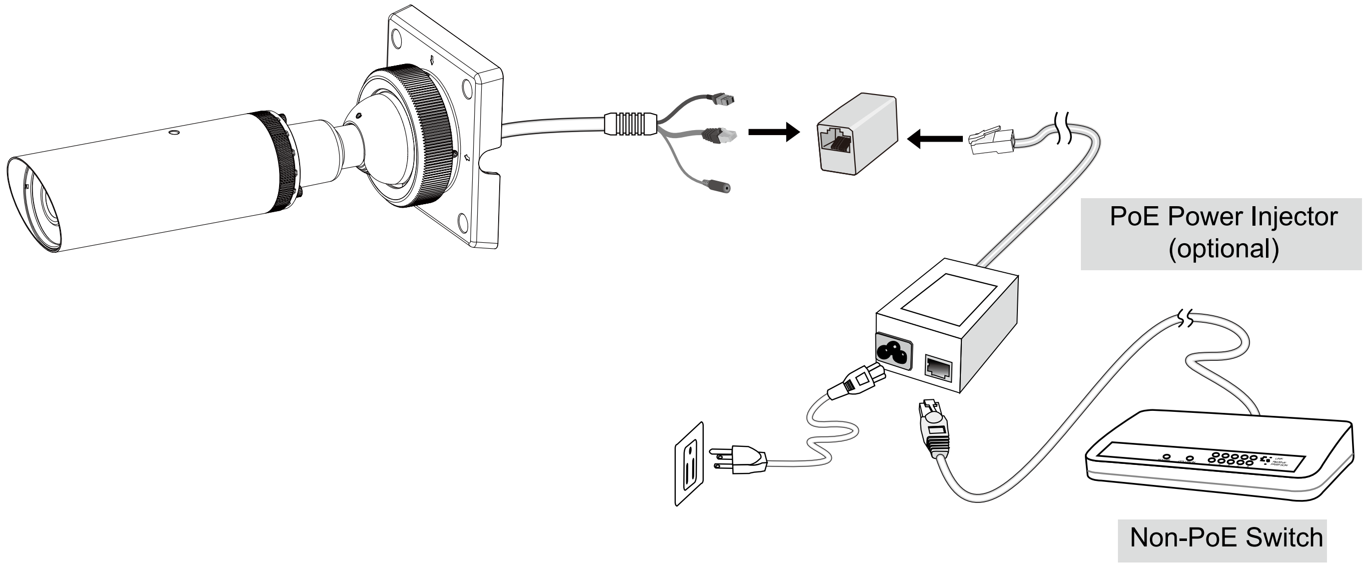
When using a PoE-enabled switch

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



When using a non-PoE switch

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.

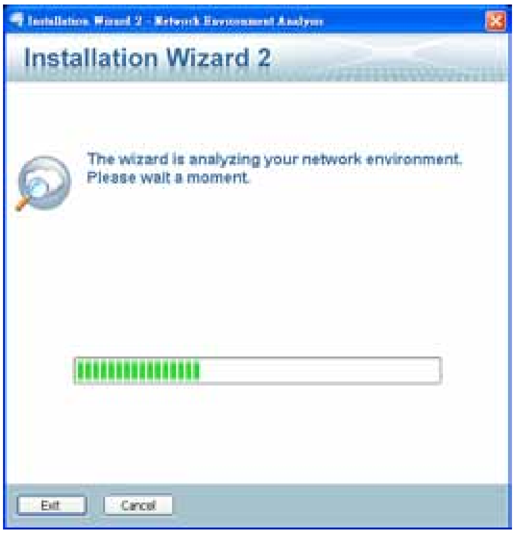


Software Installation

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

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

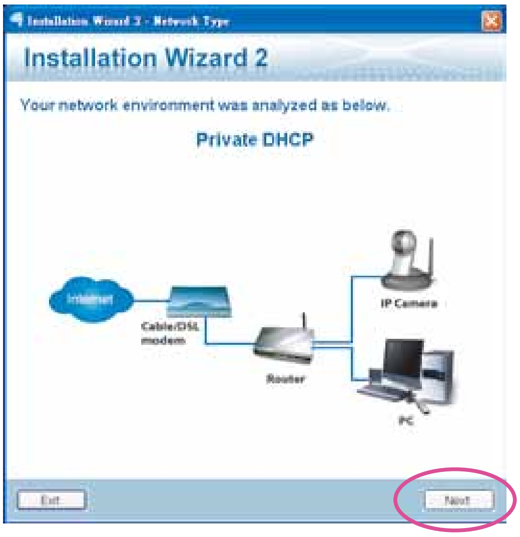
2. The program will conduct an analysis of your network environment.
   After your network environment is analyzed, please click **Next** to continue the program.



Installation Wizard 2 - Network Environment Analyze

Installation Wizard 2

The wizard is analyzing your network environment.
Please wait a moment.



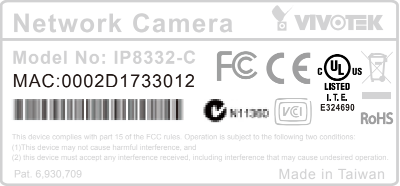
Installation Wizard 2 - Network Type

Installation Wizard 2

Your network environment was analyzed as below.

Private DHCP

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



Network Camera VIVOTEK

Model No: IP8332-C

MAC:0002D1733012

N11360

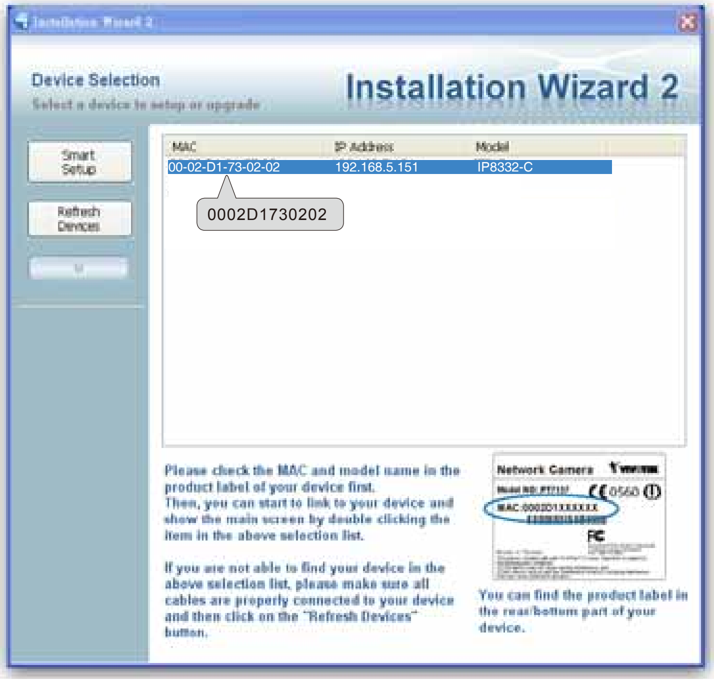
LISTED I. T. E. E324690

RoHS

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:
(1)This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

Pat. 6,930,709

Made in Taiwan



Installation Wizard 2

Device Selection

Select a device to setup or upgrade

Installation Wizard 2

MAC	IP Address	Model
00-02-D1-73-02-02	192.168.5.151	IP8332-C

0002D1730202

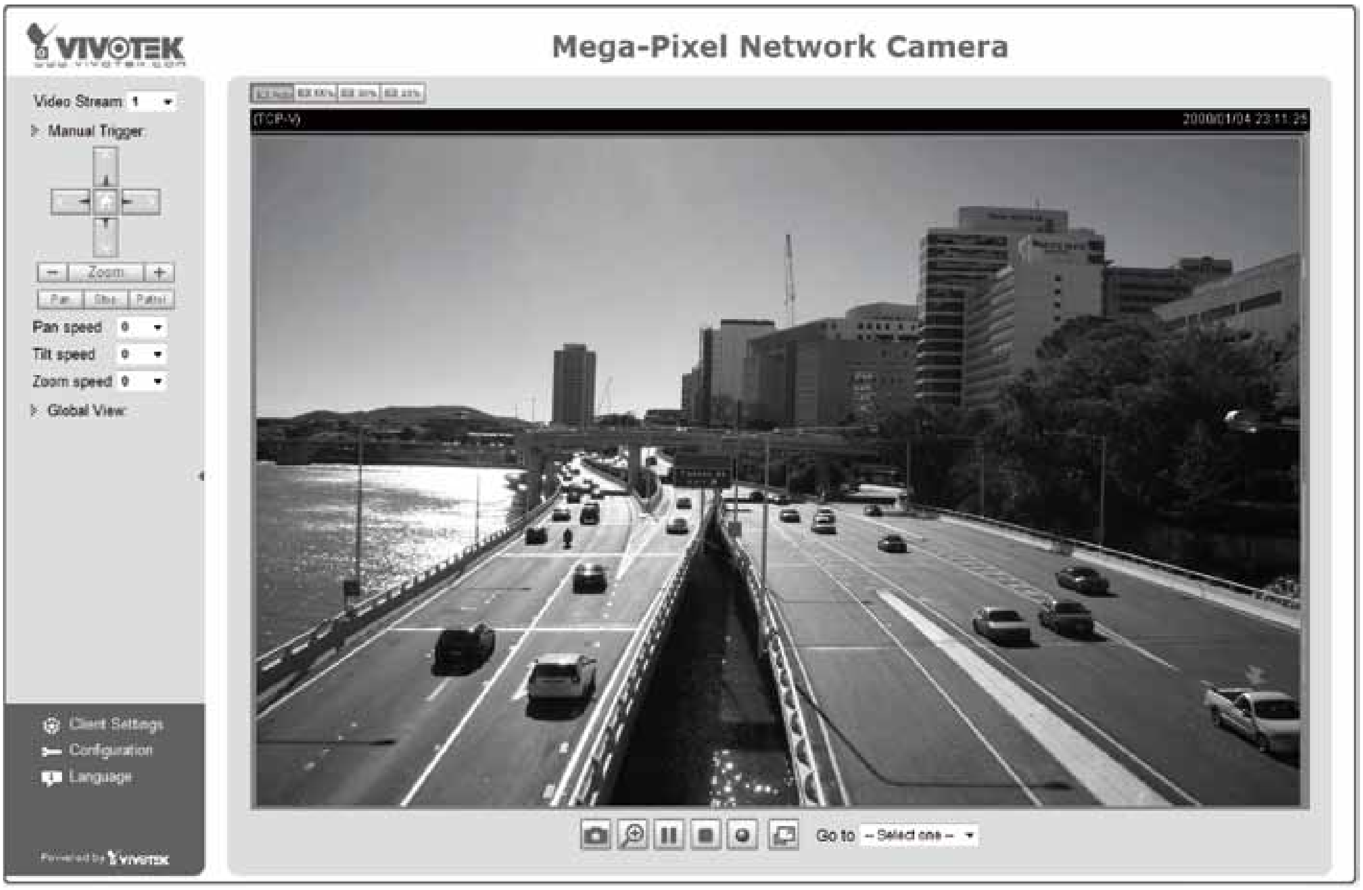
Please check the MAC and model name in the product label of your device first.
Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.

If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.

You can find the product label in the rear/bottom part of your device.

Ready to Use

1. A browser session with the Network Camera should prompt as shown below.
2. You should be able to see live video from your camera. You may also install the 32-channel recording software from the software CD in a deployment consisting of multiple cameras. For its installation details, please refer to its related documents.



Mega-Pixel Network Camera

Video Stream 1

Pan speed 0

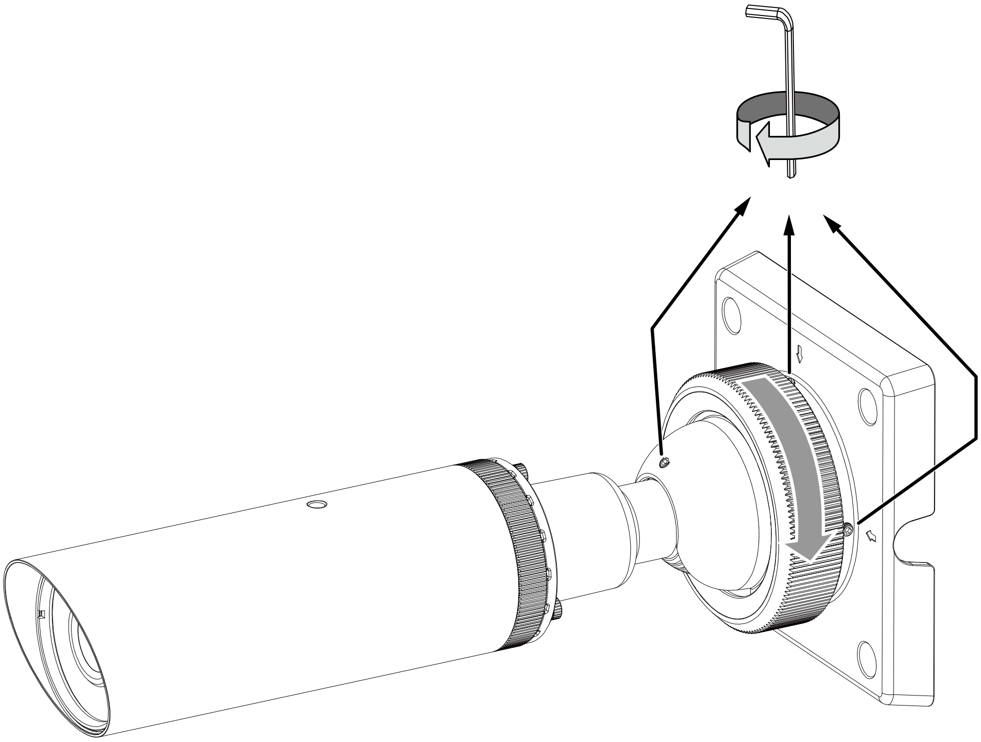
Tilt speed 0

Zoom speed 0

(TCP-V) 2000/01/04 23:11:25

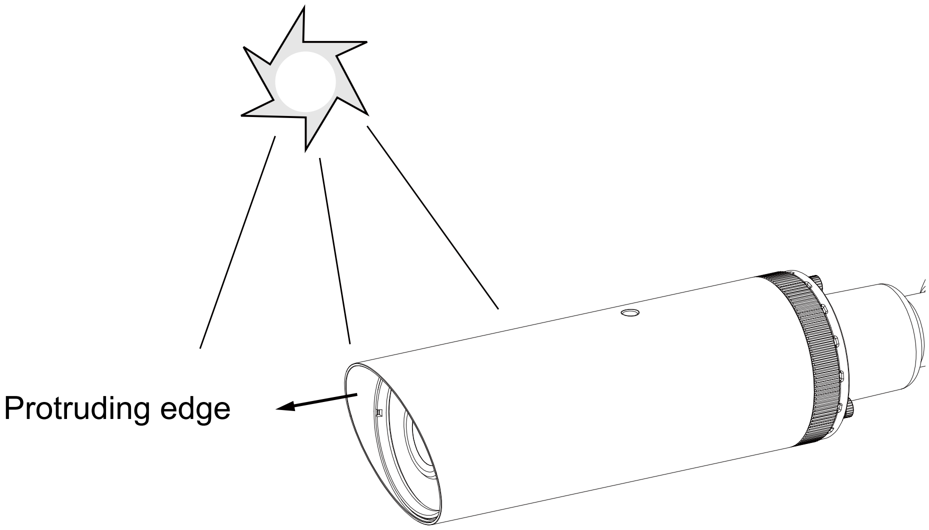
Secure the Shooting Angle

When you are done with tuning the field of view and obtain a satisfactory image, tighten the fastening ring and the 3 small hex screws on the ball-swivel bracket.



NOTE:

Orient the camera so that the protruding edge of its sunshield is positioned against the direction of direct sunlight.



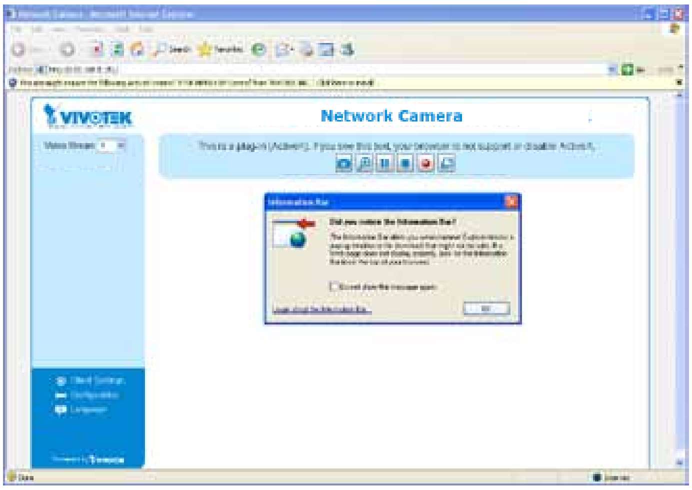
Accessing the Network Camera

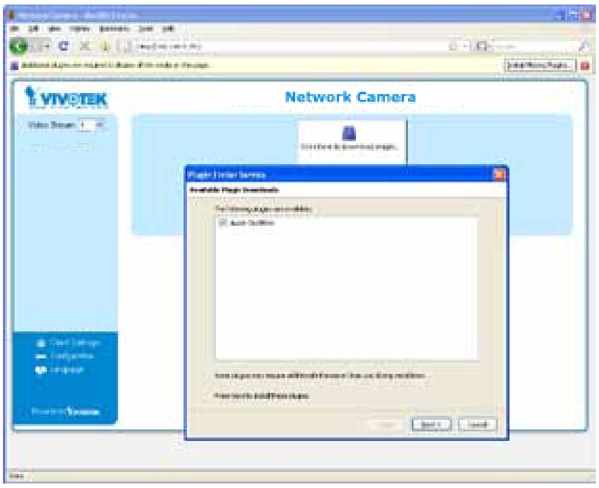
This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

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

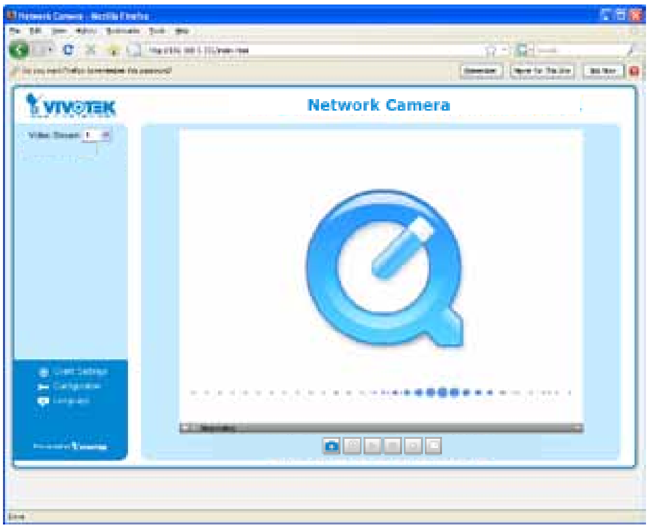
1. Launch your web browser (e.g., Microsoft® Internet Explorer, Mozilla Firefox, or Netscape).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If it is the first time installing the VIVOTEK network camera,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

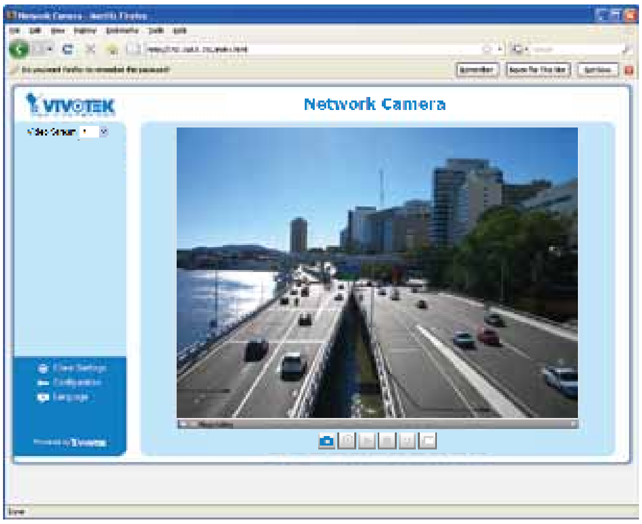




NOTE:

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

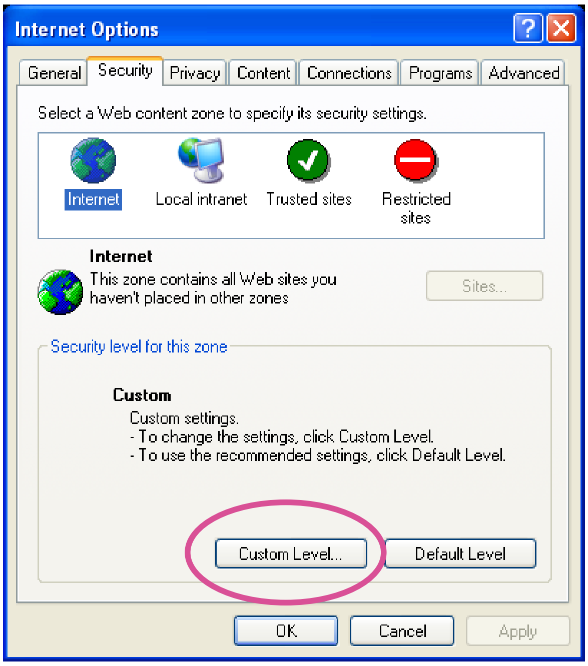




► *By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera.*
For more information about how to enable password protection, please refer to Security on page 30.

► *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable the ActiveX® Controls for your browser.*

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



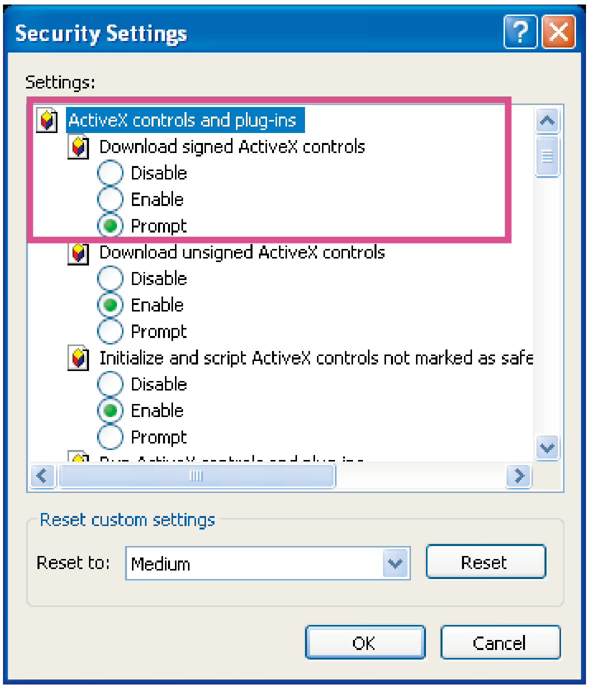
Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

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



Settings:

ActiveX controls and plug-ins
- Download signed ActiveX controls
  - ○ Disable
  - ○ Enable
  - ● Prompt
- Download unsigned ActiveX controls
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Initialize and script ActiveX controls not marked as safe
  - ○ Disable
  - ● Enable
  - ○ Prompt

Reset custom settings

Reset to: Medium

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

⚠ **IMPORTANT:**

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

Using RTSP Players

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

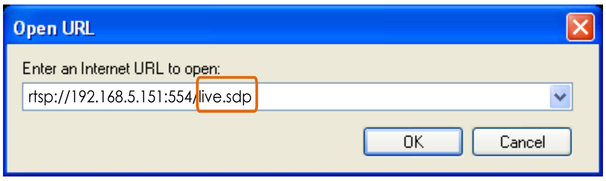
Quick Time Player

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 49.

For example:

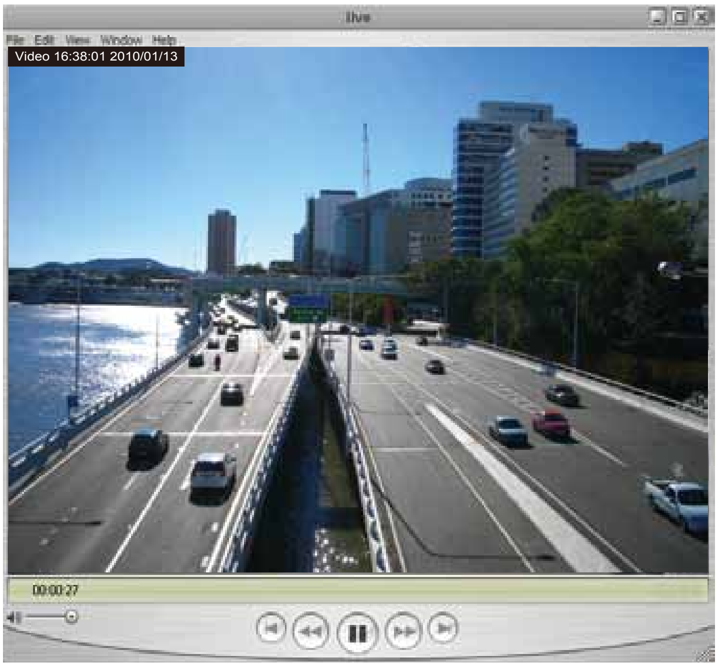


Open URL

Enter an Internet URL to open:

rtsp://192.168.5.151:554/live.sdp

4. The live video will be displayed in your player.
   For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 49 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 10.

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 49.

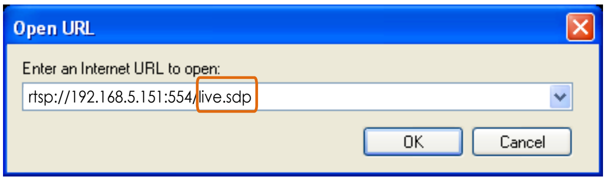
2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video and audio streaming parameters as listed below.
For more information, please refer to Viewing Window on page 61.

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

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 49.

4. Launch the player on the 3GPP-compatible mobile devices (ex. Real Player).

5. Type the following URL commands into the player.
The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream 3>.
For example:

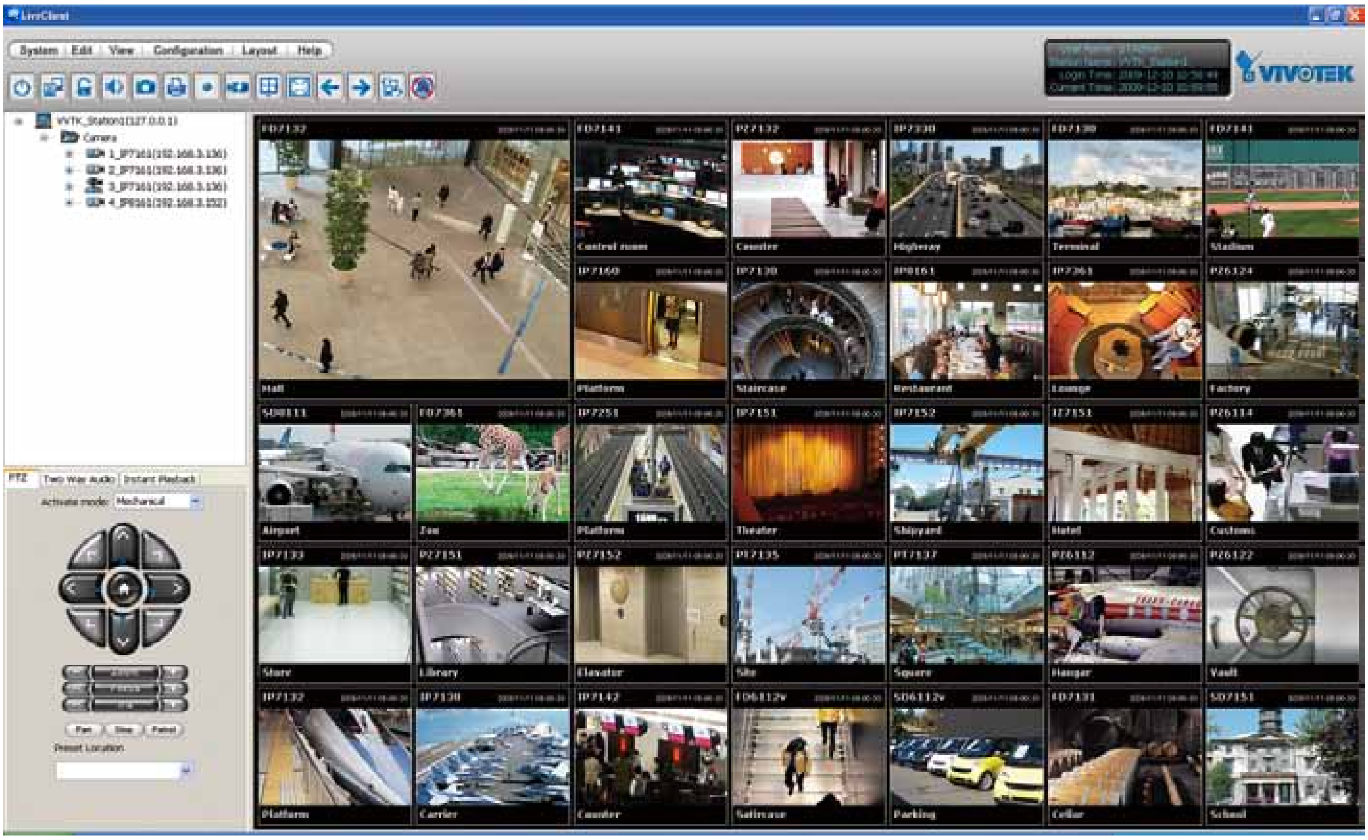


Enter an Internet URL to open:

rtsp://192.168.5.151:554/live.sdp

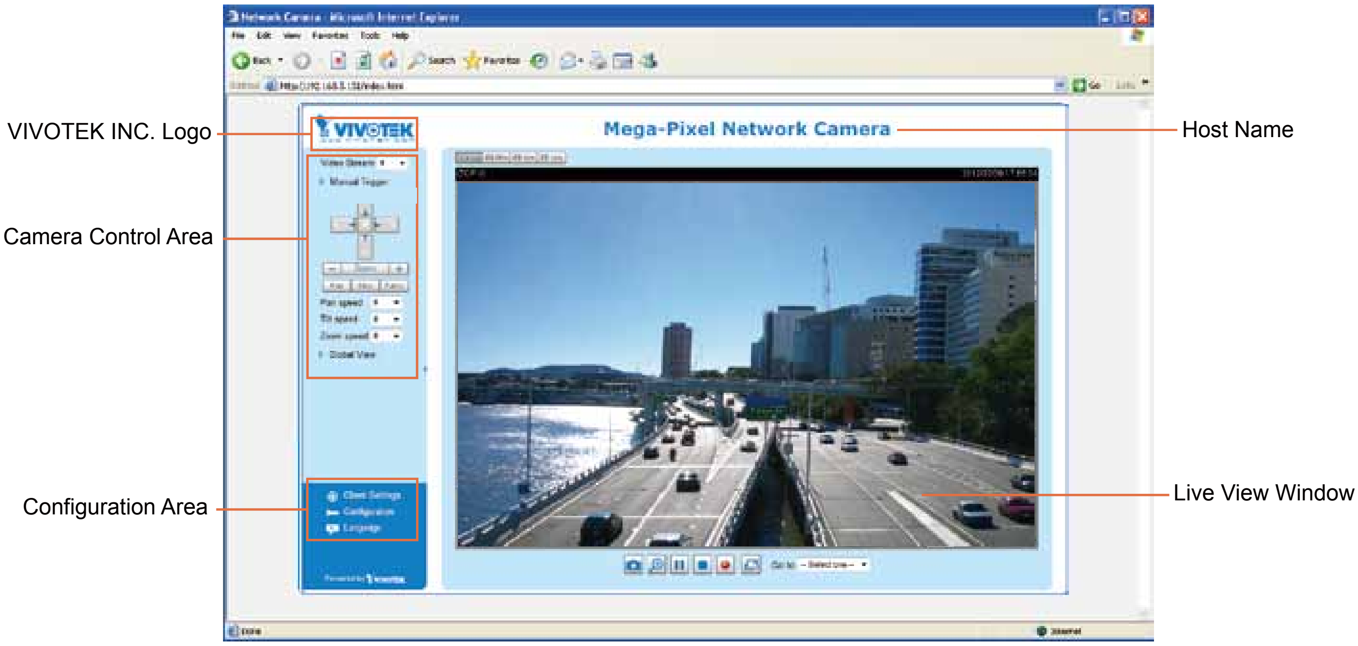
Using VIVOTEK Recording Software

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 the VIVOTEK website.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page 28.

Camera Control Area

Video Stream: This Network Cmera supports multiple streams (stream 1 ~ 4) simultaneously. You can select either one for live viewing. For more information about multiple streams, please refer to page 61 for detailed information.

Configuration Area

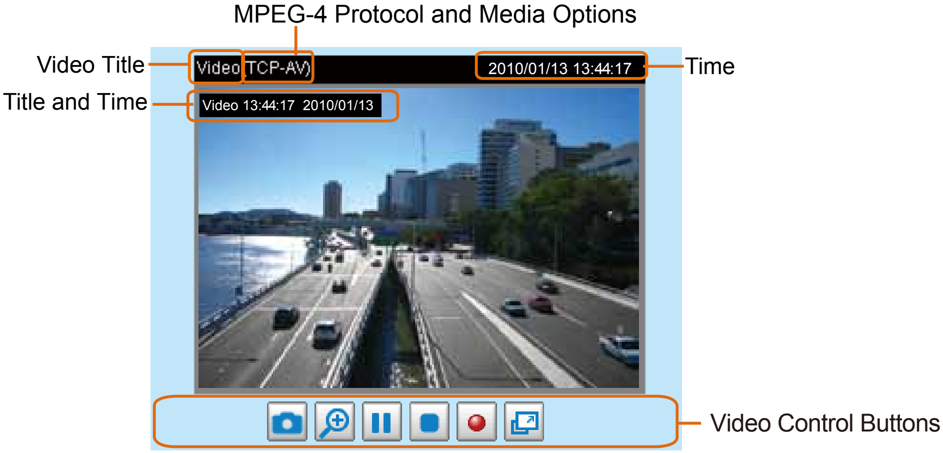
Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 25.

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 27.

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

Live Video Window

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



Video Title: The video title can be configured. For more information, please refer to Video Settings on page 56.

H.264 / MPEG-4 Protocol and Media Options: The transmission protocol and media options for H.264 / MPEG-4 video streaming. For further configuration, please refer to Client Settings on page 25.

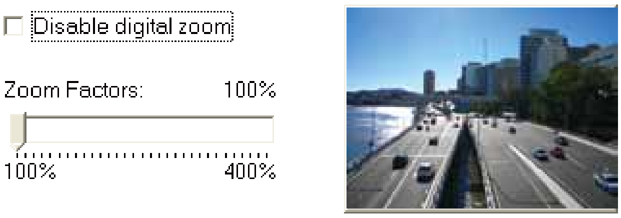
Time: Display the current time. For further configuration, please refer to Video Settings on page 56.

Title and Time: The video title and time can be stamped on the streaming video. For further configuration, please refer to Video Settings on page 56.

Video Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

📷 Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

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



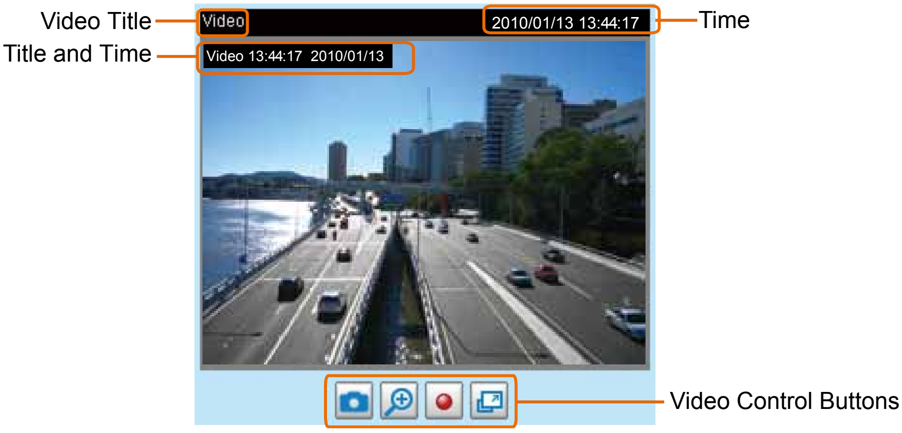
⏸ Pause: Pause the transmission of the streaming media. The button becomes the ▶ Resume button after clicking the Pause button.

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

● Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the ■ Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 26 for details.

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

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



Video Title: The video title can be configured. For more information, please refer to Video Settings on page 56.

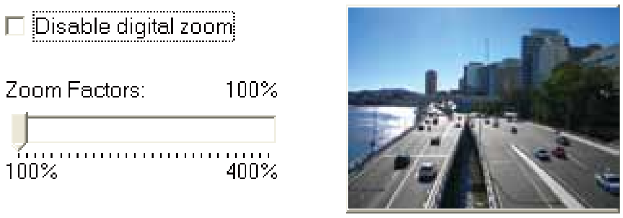
Time: Display the current time. For more information, please refer to Video Settings on page 56.

Title and Time: Video title and time can be stamped on the streaming video. For more information, please refer to Video Settings on page 56.

Video 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%

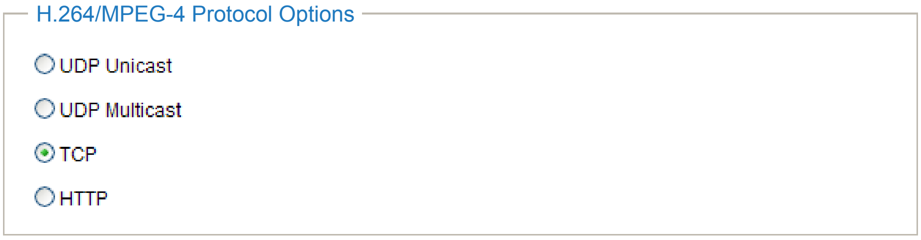
Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the ■ Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 26 for details.

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

Client Settings

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

H.264 / MPEG-4 Protocol Options



H.264/MPEG-4 Protocol Options

○ UDP Unicast

○ UDP Multicast

● TCP

○ HTTP

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

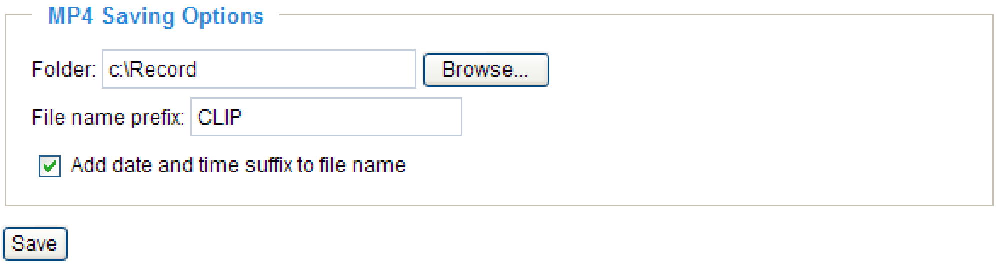
UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast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

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 49.

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: c:\Record [Browse...]

File name prefix: CLIP

☑ Add date and time suffix to file name

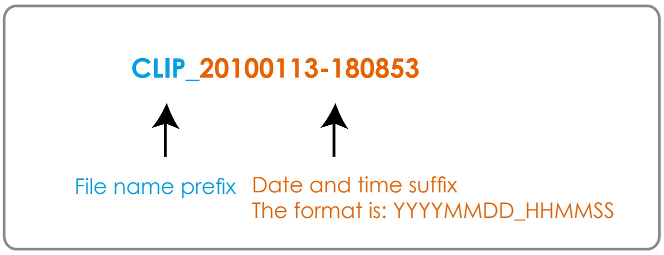
[Save]

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

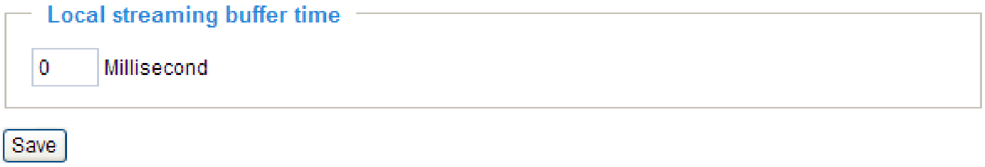
Folder: Specify a storage destination for the recorded video files.

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.



Local Streaming Buffer Time



Local streaming buffer time

0 Millisecond

[Save]

Due to the unsteady bandwidth flow, the live streaming may lag and not be very smoothly. If you enable this option, the live streaming will be stored on the camera's buffer area for a few seconds before playing on the live viewing window. This will help you see the streaming more smoothly. If you enter 3,000 Millisecond, the streaming will delay 3 seconds.

Configuration

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

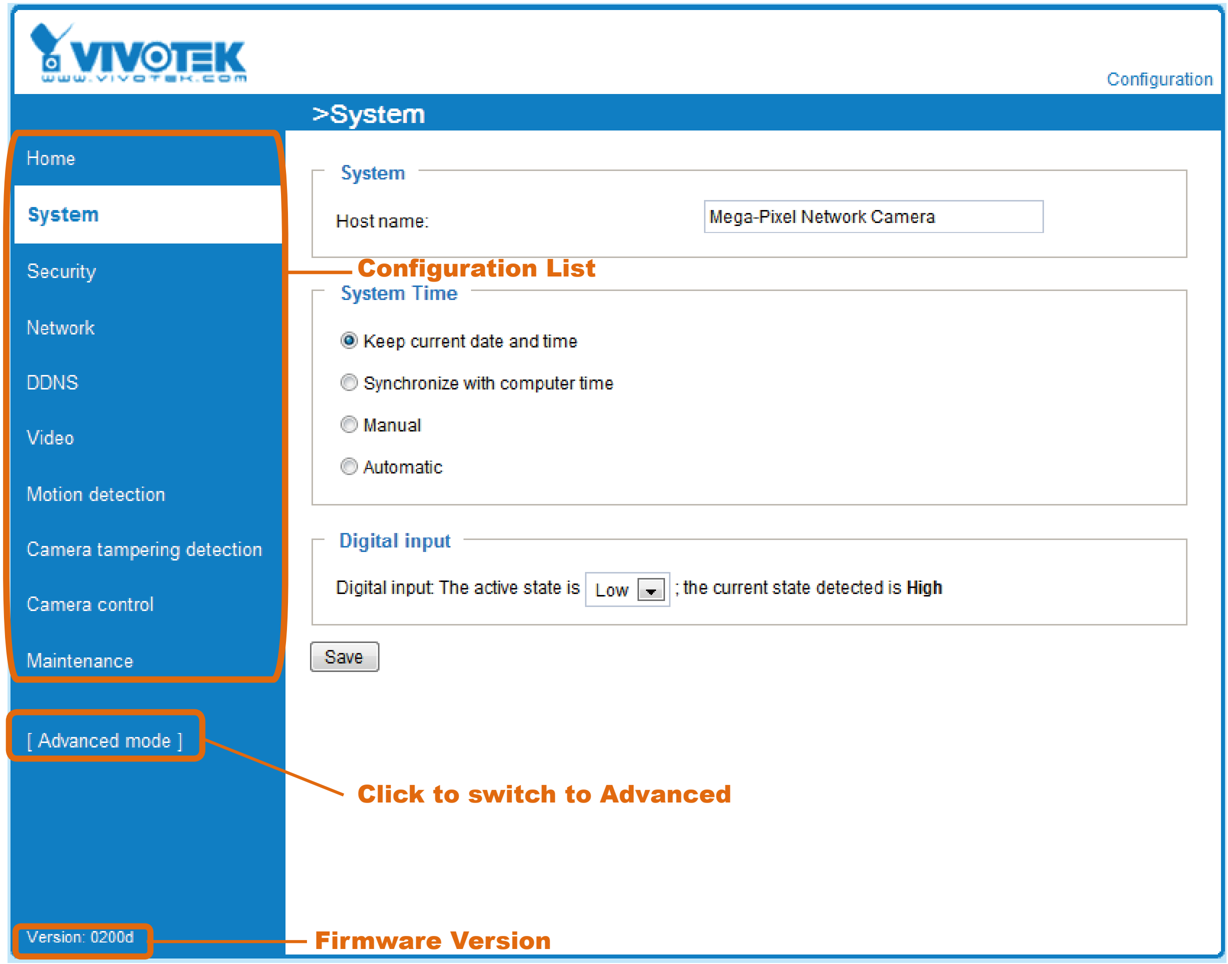
VIVOTEK offers an easy-to-use user interface that helps you set up your network camera with minimal effort. To simplify the setting procedure, two types of user interfaces are available: Advanced Mode for professional users and Basic Mode for entry-level users. Some advanced functions (HTTPS/ Access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

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

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

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

Basic Mode



System

Host name: Mega-Pixel Network Camera

System Time

● Keep current date and time

○ Synchronize with computer time

○ Manual

○ Automatic

Digital input

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

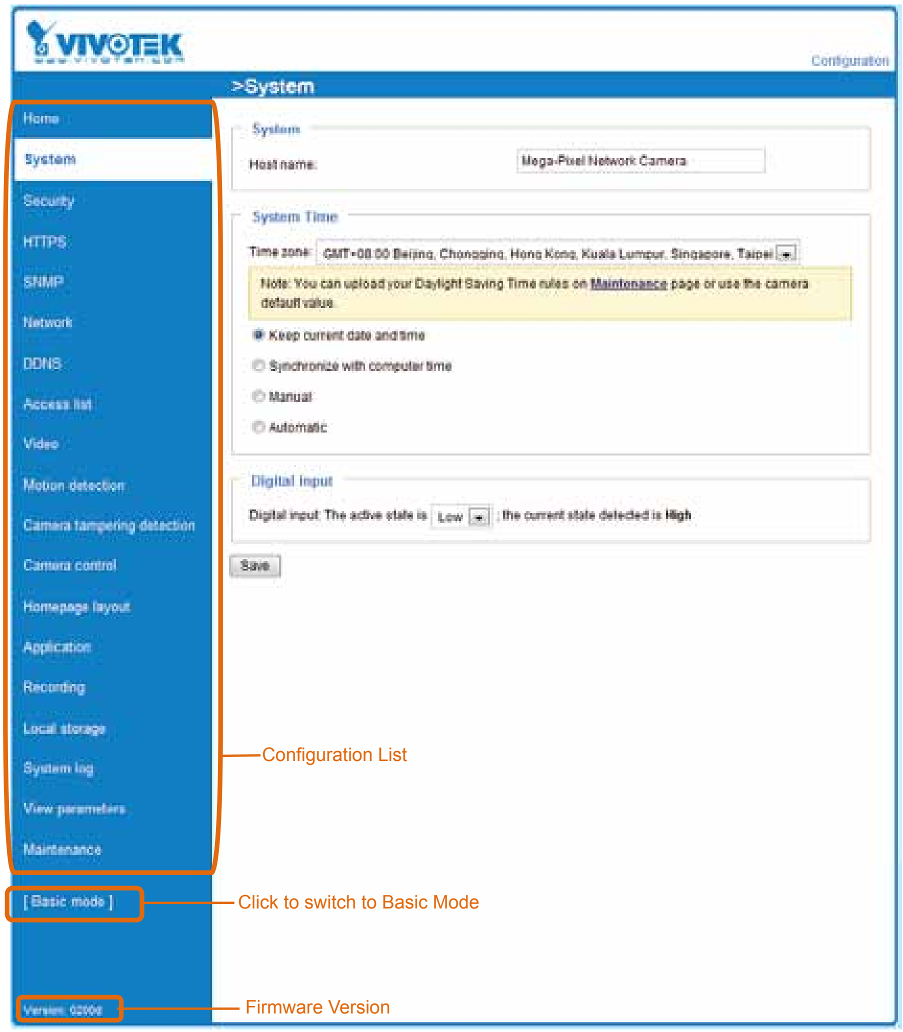
Version: 0200d

Configuration List

Click to switch to Advanced

Firmware Version

Advanced Mode



System

Host name: Mega-Pixel Network Camera

System Time

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

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

● Keep current date and time
○ Synchronize with computer time
○ Manual
○ Automatic

Digital input

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

Configuration List

Click to switch to Basic Mode

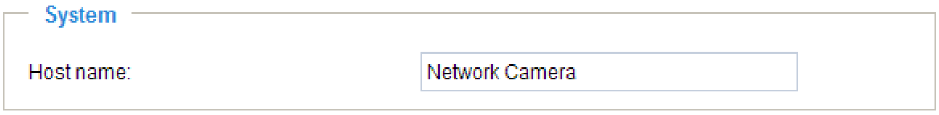
Firmware Version

Each function on the configuration list will be explained in the following sections. Those functions that are displayed only in Advanced Mode are tagged with the 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 finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

System

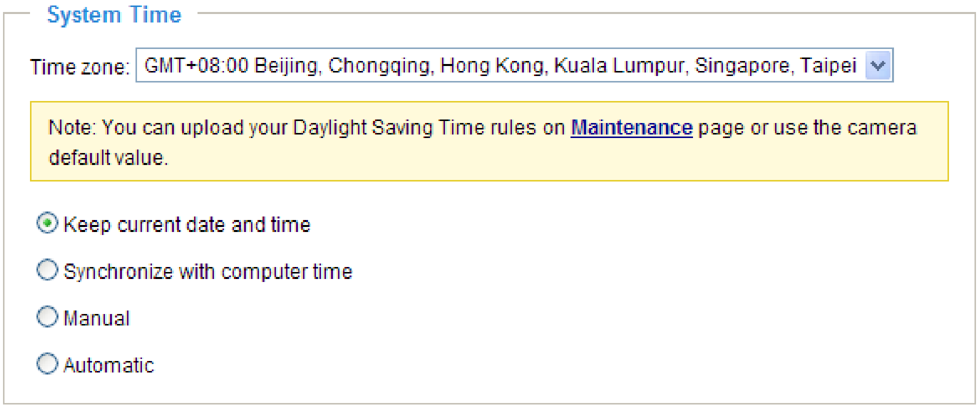


System

Host name: Network Camera

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

System Time



System Time

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

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

● Keep current date and time

○ Synchronize with computer time

○ Manual

○ Automatic

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

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

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

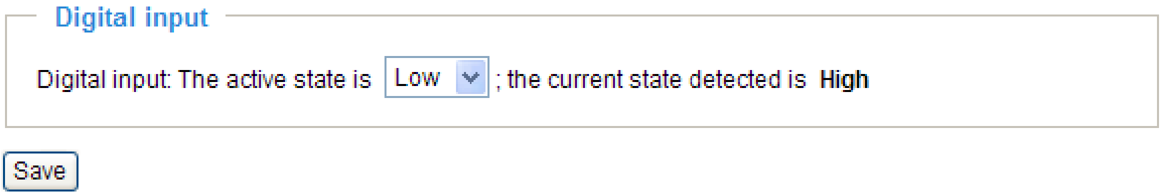
Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of 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 100 for details.

Digital Input



Digital input

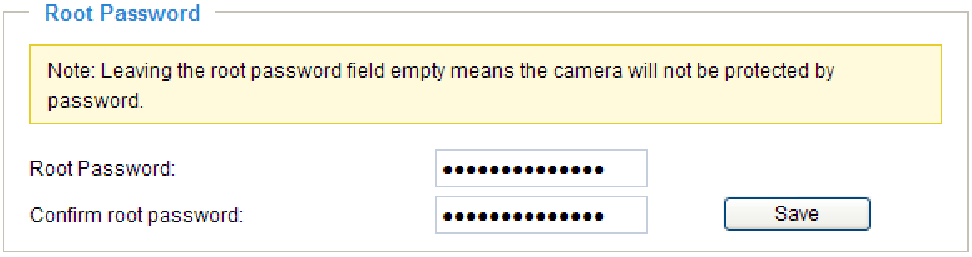
Digital input: The active state is Low ; the current state detected is High

Digital input: Select High or Low to define normal status for the digital input. Connect an external device to the digital input pin, and the Network Camera will automatically report the current status.

Security

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

Root Password



Root Password

Note: Leaving the root password field empty means the camera will not be protected by password.

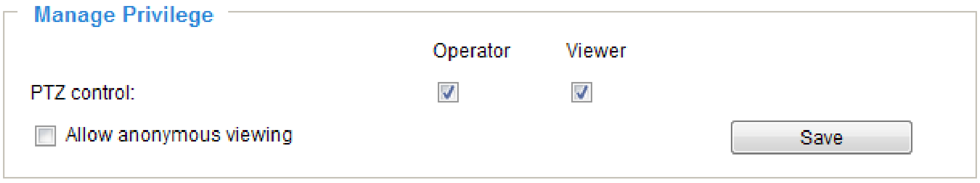
Root Password: ••••••••••••••

Confirm root password: ••••••••••••••

The administrator account name is “root”, which is permanent and can not be deleted. If you want to add more accounts in the Manage User column, please apply the password for the “root” account first.

1. Key in the identical passwords in both text boxes, then click **Save** to enable password protection.
2. A window will prompt for authentication; enter the correct user’s name and password in their respective fields to access the Network Camera.

Manage Privilege Advanced Mode



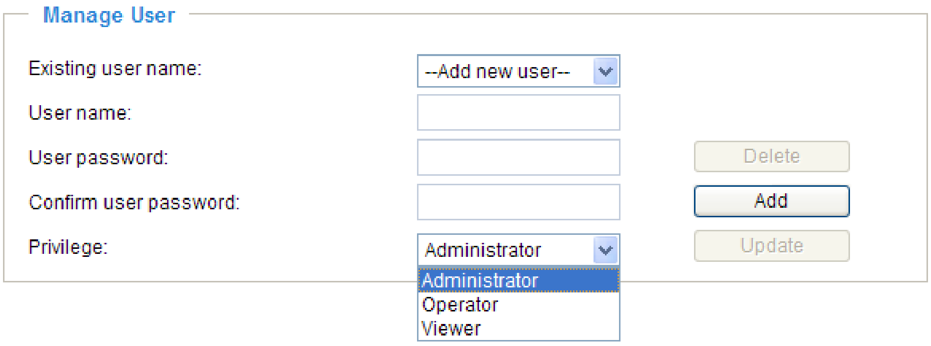
Manage Privilege

	Operator	Viewer
PTZ control:	☑	☑

☐ Allow anonymous viewing

Allow anonymous viewing: If you check this item, any client can access the live stream without entering a User ID and Password. Select or deselect checkboxes to define a user’s rights to the operation and access to the live view.

Manage User



Manage User

Existing user name: --Add new user--

User name:

User password:

Confirm user password:

Privilege: Administrator

Administrators can create up to 20 user accounts.

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

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Although operators cannot access the Configuration page, they can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 103. Viewers access only the main page for live viewing.

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

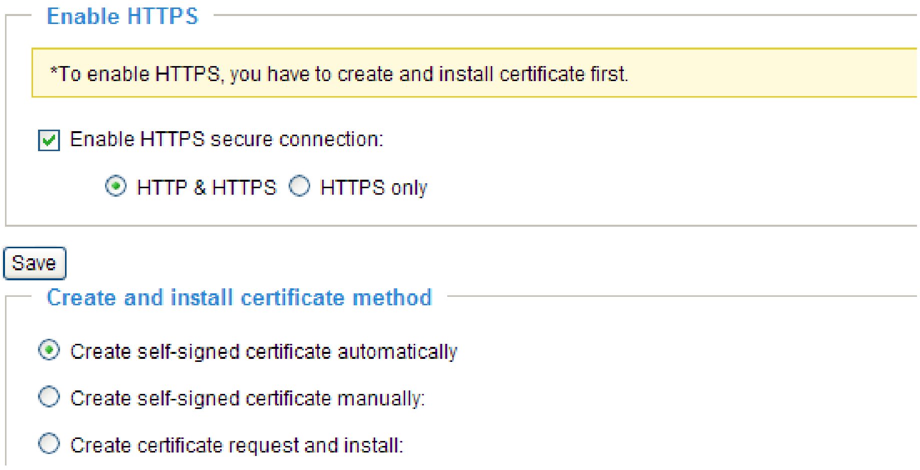
1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

HTTPS (Hypertext Transfer Protocol over SSL) Advanced Mode

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

Enable HTTPS

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



Enable HTTPS

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

☑ Enable HTTPS secure connection:

● HTTP & HTTPS ○ HTTPS only

Create and install certificate method

● Create self-signed certificate automatically

○ Create self-signed certificate manually:

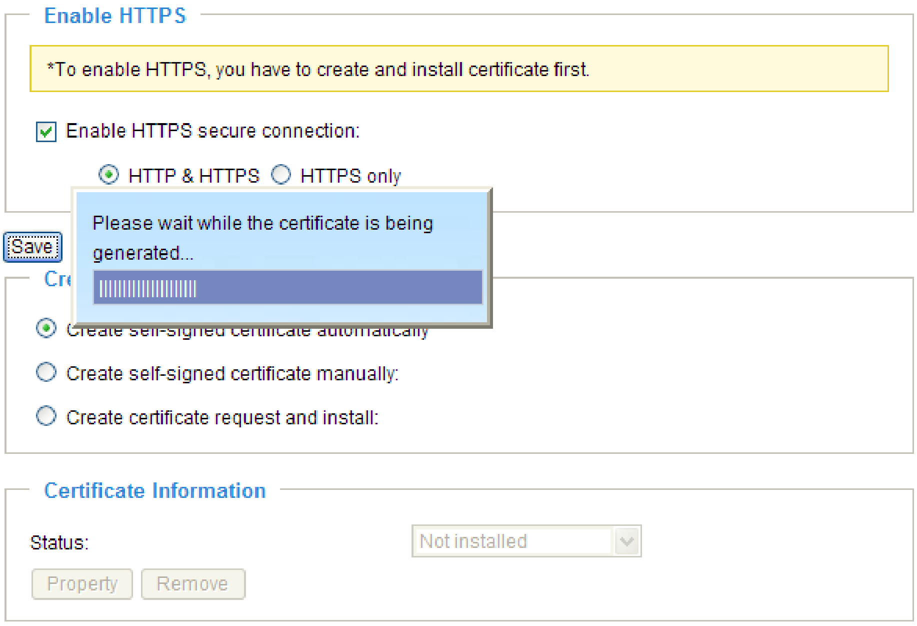
○ Create certificate request and install:

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

Please wait while the certificate is being generated...

● Create self-signed certificate automatically

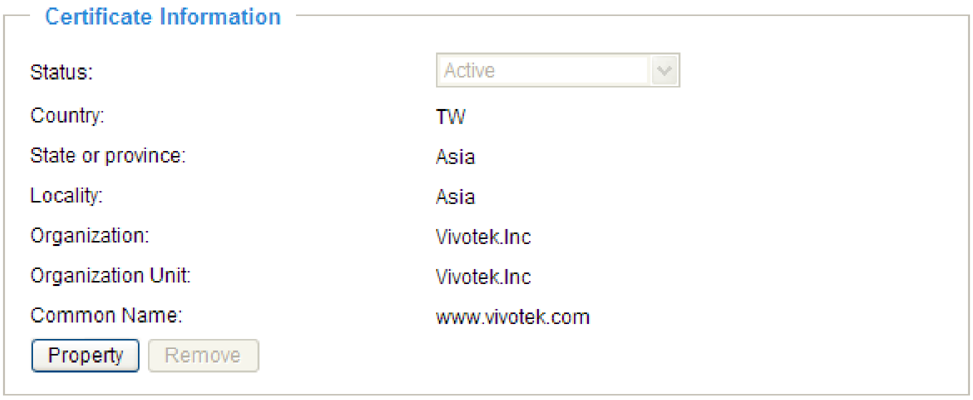
○ Create self-signed certificate manually:

○ Create certificate request and install:

Certificate Information

Status: Not installed

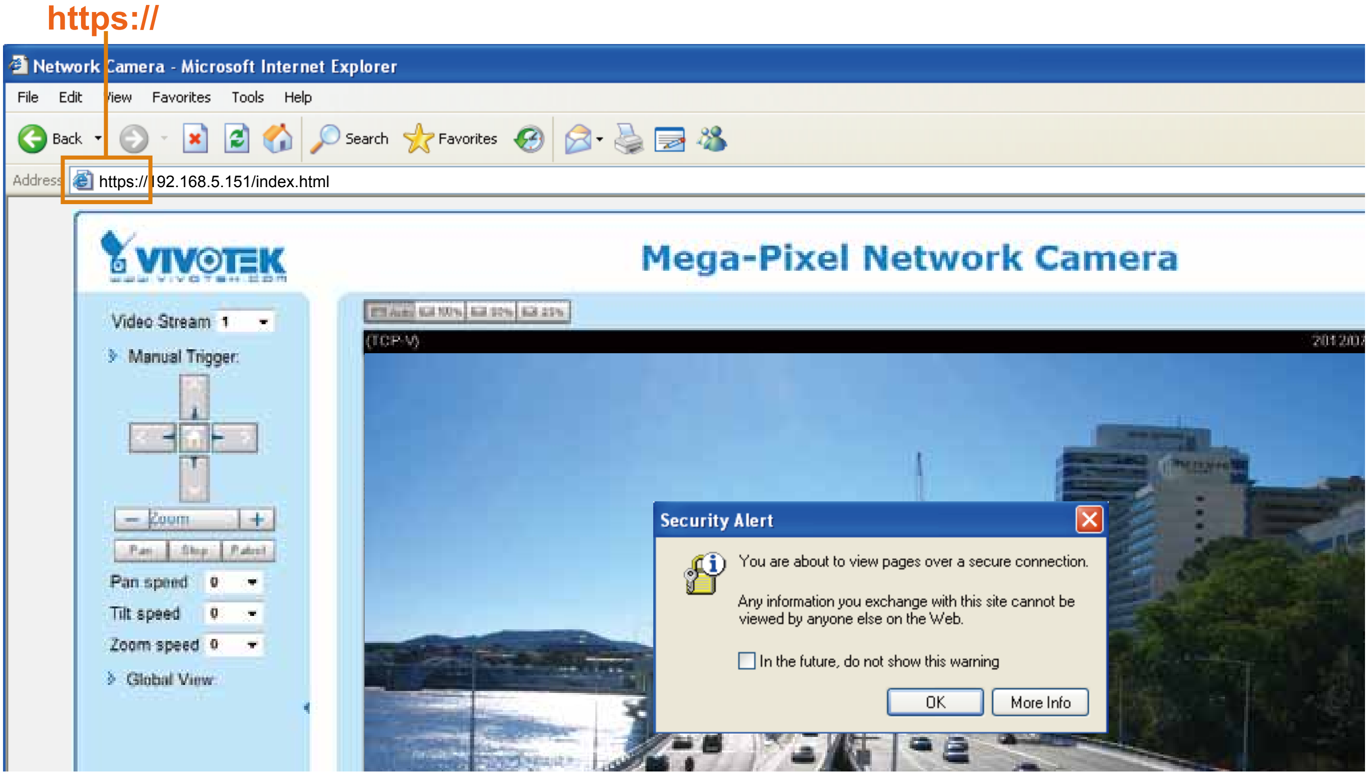
4. The Certificate Information will automatically be displayed in the third column as shown below. You can click **Property** to view detailed information about the certificate.



Certificate Information

Status:	Active
Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	Vivotek.Inc
Organization Unit:	Vivotek.Inc
Common Name:	www.vivotek.com

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.



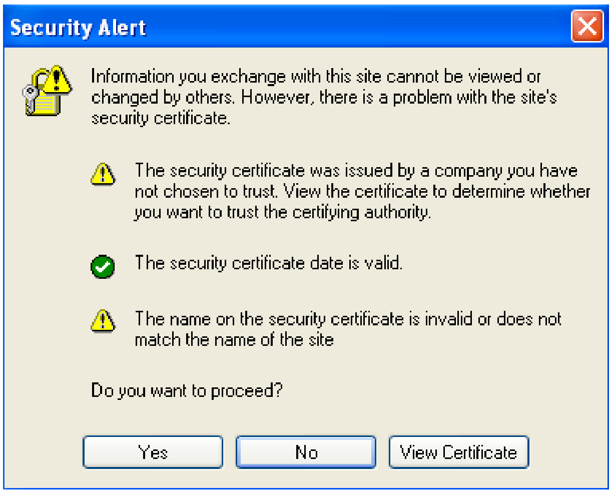
https://
Network Camera - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
https://192.168.5.151/index.html
VIVOTEK
Mega-Pixel Network Camera
Video Stream 1
Manual Trigger
Zoom
Pan speed 0
Tilt speed 0
Zoom speed 0
Global View

Security Alert

You are about to view pages over a secure connection.

Any information you exchange with this site cannot be viewed by anyone else on the Web.

□ In the future, do not show this warning



Security Alert

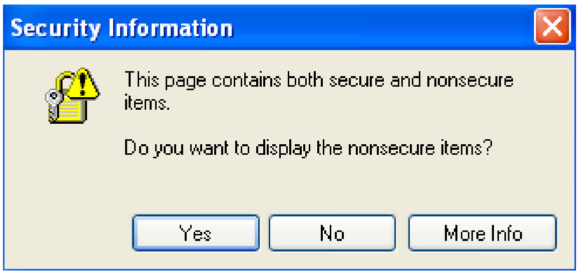
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?



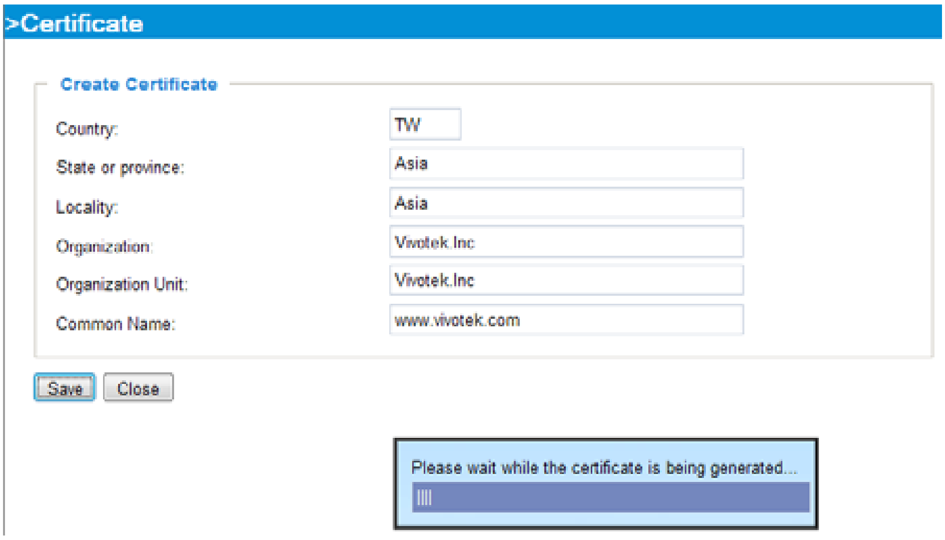
Security Information

This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

Create self-signed certificate manually

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



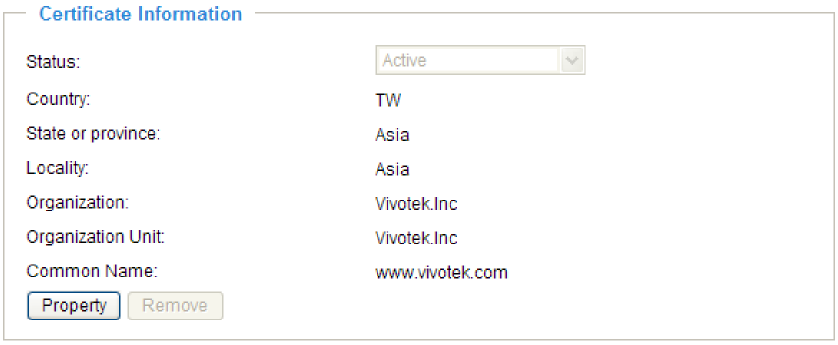
>Certificate

Create Certificate

Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	Vivotek.Inc
Organization Unit:	Vivotek.Inc
Common Name:	www.vivotek.com

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.

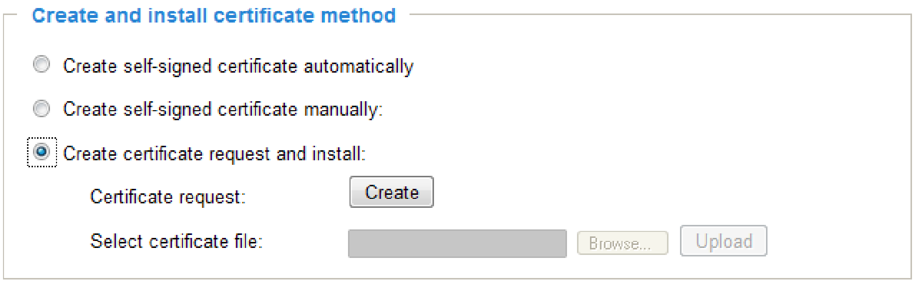


Certificate Information

Status:	Active
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 the Create Certificate page, then click **Save** to generate the certificate.



Create and install certificate method

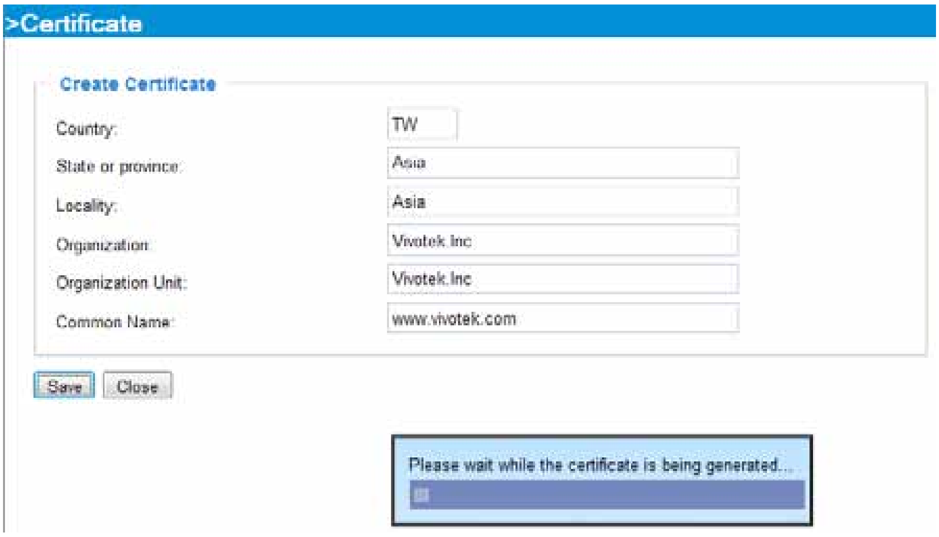
○ Create self-signed certificate automatically

○ Create self-signed certificate manually:

● Create certificate request and install:

Certificate request:

Select certificate file:



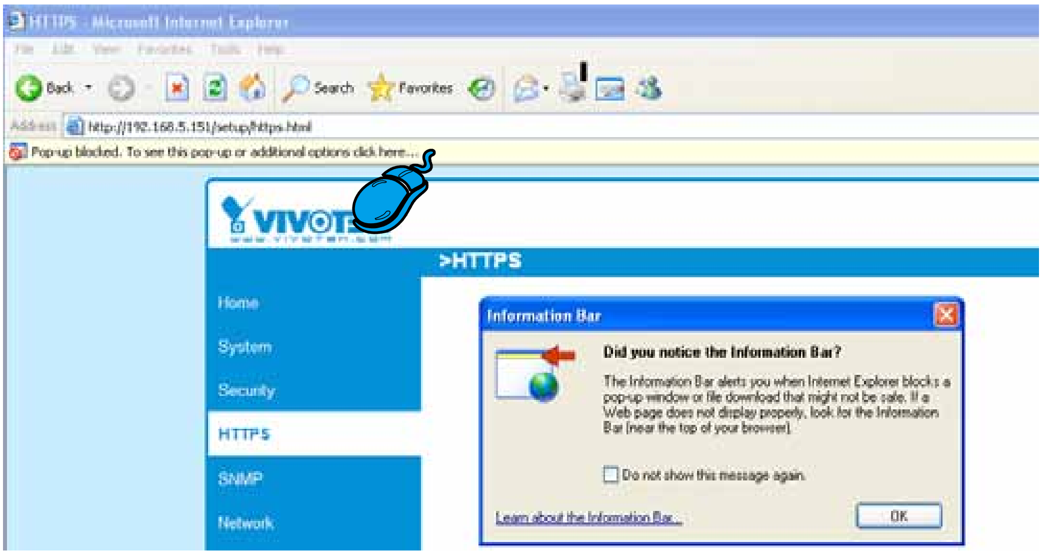
>Certificate

Create Certificate

Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	Vivotek.Inc
Organization Unit:	Vivotek.Inc
Common Name:	www.vivotek.com

Please wait while the certificate is being generated...

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



HTTPS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://192.168.5.151/setup/https.html
VIVOTEK
>HTTPS
Home
System
Security
HTTPS
SNMP
Network
Information Bar
OK

Pop-up blocked. To see this pop-up or additional options click here...

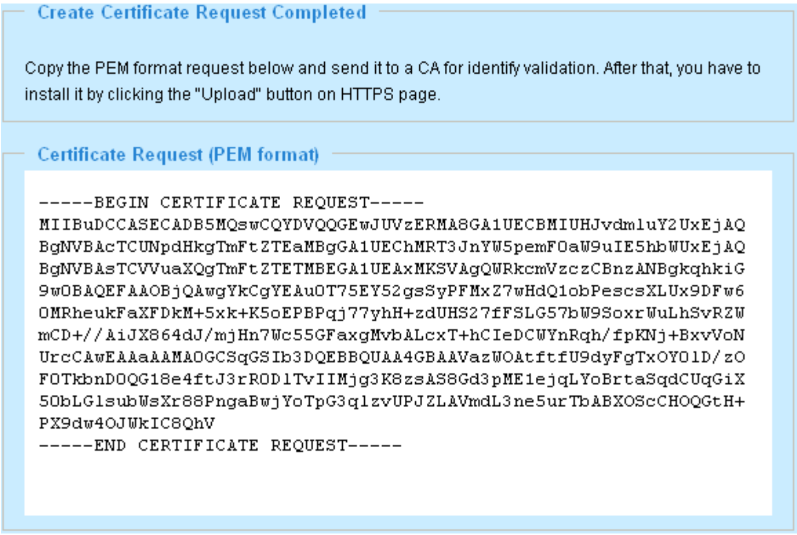
Did you notice the Information Bar?

The Information Bar alerts you when Internet Explorer blocks a pop-up window or file download that might not be safe. If a Web page does not display properly, look for the Information Bar (near the top of your browser).

□ Do not show this message again.

Learn about the Information Bar...

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



Create Certificate Request Completed

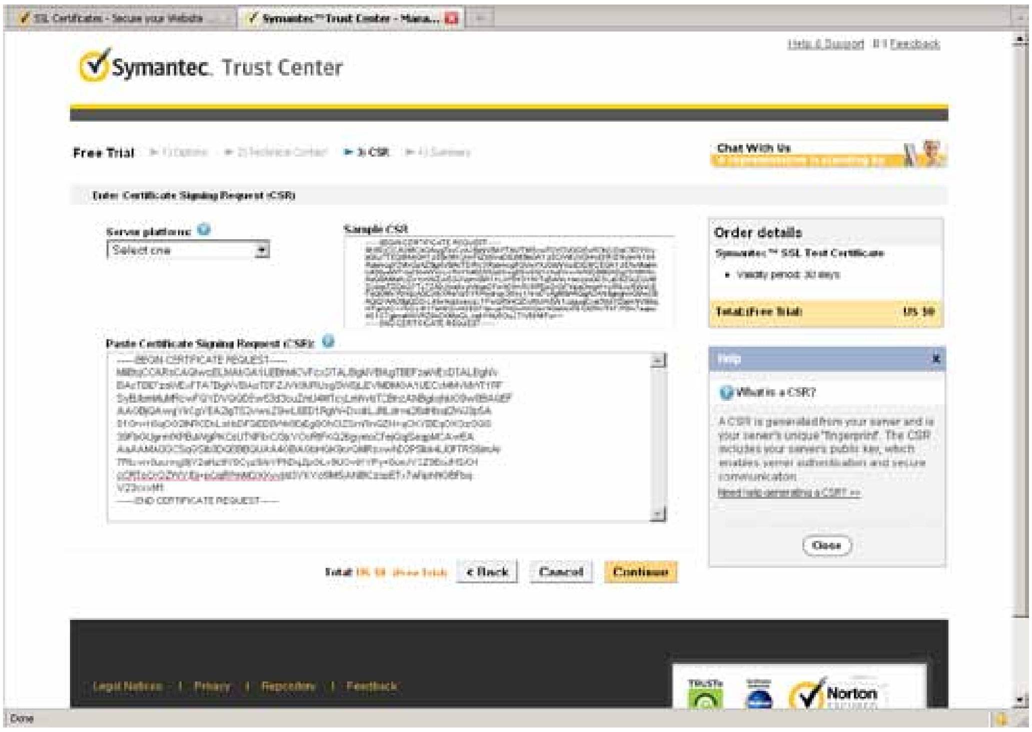
Copy the PEM format request below and send it to a CA for identify validation. After that, you have to install it by clicking the "Upload" button on HTTPS page.

Certificate Request (PEM format)

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBuDCCASECADB5MQswCQYDVQQGEwJUVzERMA8GA1UECBMIUHJvdmluY2UxEjAQ
BgNVBAcTCUNpdHkgTmFtZTEaMBgGA1UEChMRT3JnYW5pemF0aW9uIE5hbWUxEjAQ
BgNVBAsTCVVuaXQgTmFtZTETMBEGA1UEAxMKSVAgQWRkcmVzczCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwgYkCgYEAuOT75EY52gsSyPFMxZ7wHdQ1obPescsXLUx9DFw6
OMRheukFaXFDkM+5xk+K5oEPBPqj77yhH+zdUHS27fFSLG57bW9SoxrWuLhSvRZW
mCD+//AiJX864dJ/mjHn7Wc55GFaxgMvbALcxT+hCIeDCWYnRqh/fpKNj+BxvVoN
UrcCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBAAVazWOAtftfU9dyFgTxOYO1D/zO
FOTkbnDOQG18e4ftJ3rRODlTvIIMjg3K8zsAS8Gd3pME1ejqLYoBrtaSqdCUqGiX
5ObLGlsubWsXr88PngaBwjYoTpG3qlzvUPJZLAVmdL3ne5urTbABXOScCHOQGtH+
PX9dw4OJWkIC8QhV
-----END CERTIFICATE REQUEST-----
```

5. Click **Browse...** to search for the issued certificate, then click Upload in the second column.

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


SSL Certificates - Secure your Website ...
Symantec™ Trust Center - Mana...
Help & Support | Feedback
Symantec. Trust Center
Free Trial ► 1) Options ► 2) Technical Contact ► 3) CSR ► 4) Summary
Chat With Us
< Back
Cancel
Continue
Close
Legal Notices | Privacy | Repository | Feedback
Norton
Done

Enter Certificate Signing Request (CSR)

Server platform: Select one

Sample CSR

Order details

Symantec™ SSL Test Certificate

- Validity period: 30 days

Total (Free Trial) US $0

Paste Certificate Signing Request (CSR):

```
-----BEGIN CERTIFICATE REQUEST-----
[illegible]
-----END CERTIFICATE REQUEST-----
```

Help

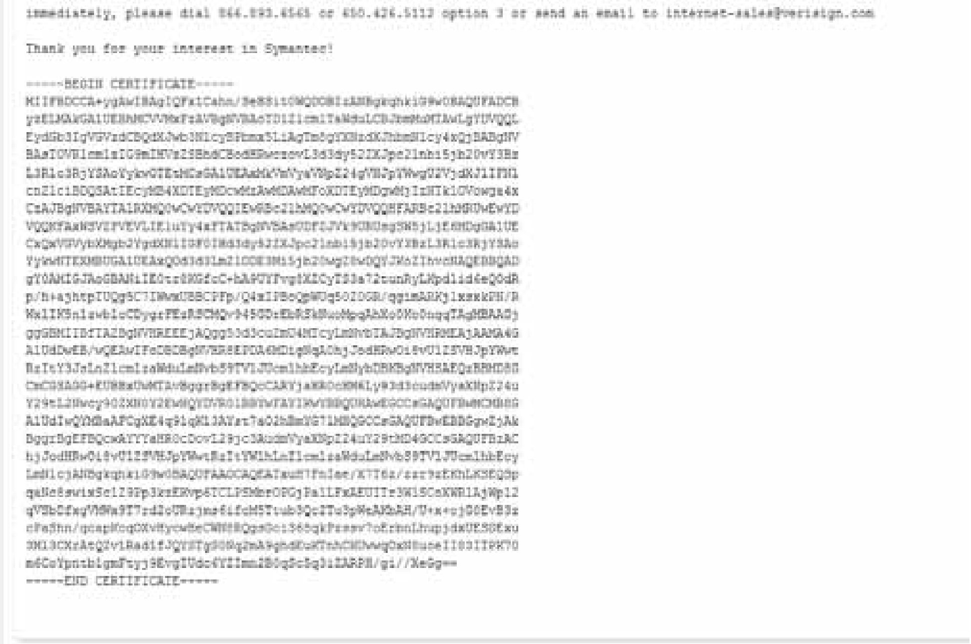
What is a CSR?

A CSR is generated from your server and is your server's unique "fingerprint". The CSR includes your server's public key, which enables server authentication and secure communication.

Need help generating a CSR? »

Total: US $0 (Free Trial)

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

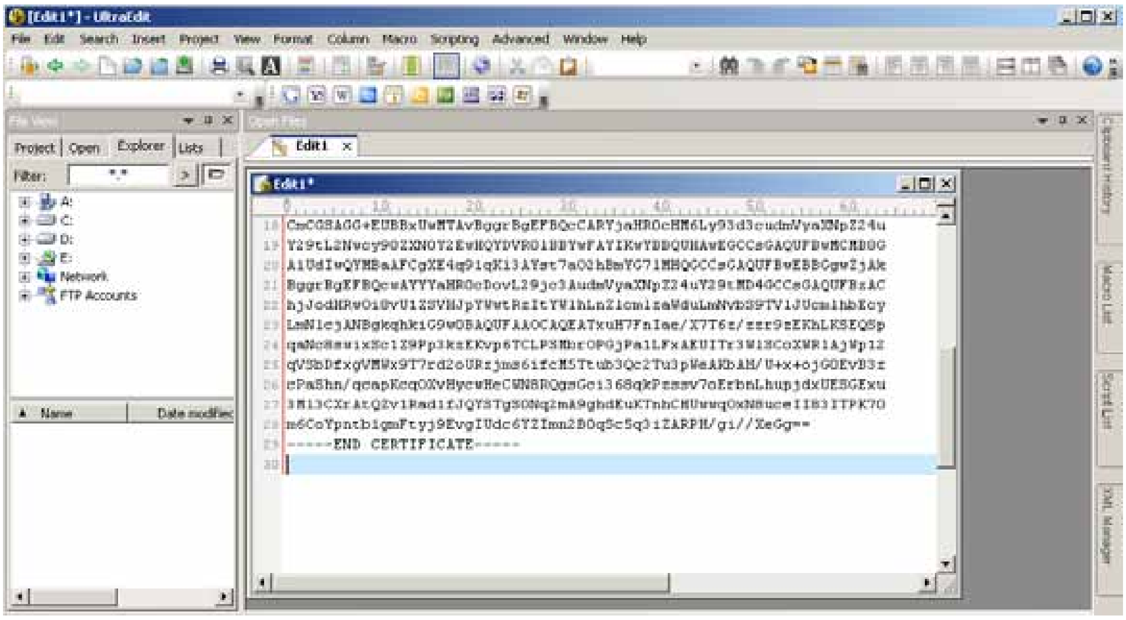


immediately, please dial 866.893.6565 or 650.426.5112 option 3 or send an email to internet-sales@verisign.com

Thank you for your interest in Symantec!

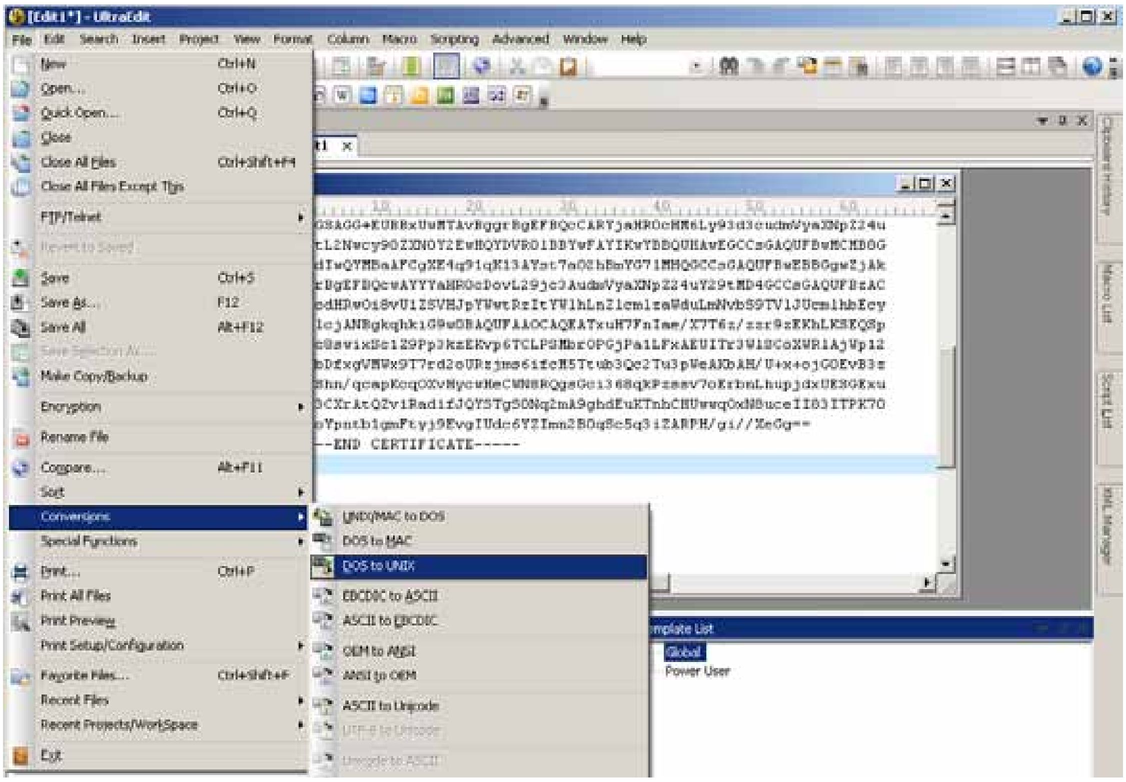
```
-----BEGIN CERTIFICATE-----
MIIFBDCCA+ygAwIBAgIQFx1Cahn/BeB8itOWQDOBIzANBgkqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz
L3Rlc3RjYSAoYykwOTEzMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNl
cnZlciBDQSAtIEcyMB4XDTEyMDcwMzAwMDAwMFoXDTEyMDgwMjIzNTk1OVowgx4x
CzAJBgNVBAYTAlRXMQ0wCwYDVQQIEwRBcZlhMQ0wCwYDVQQHFARBcZlhMRUwEwYD
VQQKFAxNSVIFVEVLIEluYy4xFTATBgNVBAsUDFlJVkVORUmgSW5jLjEMMDgGA1UE
CxQwVGVybXMgb2YgdXNlIGF0IHd3dy52ZXJpc2lnbi5jb20vY3BzL3RlcSRjYSAo
YywwMTEXMBUGA1UEAxQOd3d3LmZ1ODE3Mi5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANiIE0tr8KGfcC+hA8TYFvgtX2CyT93a72tunRyLMpdlid6eQOdR
p/h+ajhtpIUQg5C7IWwmUBBCPFp/Q4xIPBoQgWDq5OZDGB/qgimARKj1xzxkPH/R
Wx1IK5n1swb1oCDygzFEsR5CMQv945GDrEbR5kNuoMpgAAKo0Ko0uqqTAgMBAAGj
ggGBMIIBfTAZBgNVHREEEjAQgg53d3cuZmU4MTcyLmNvbTAJBgNVHRMEAjAAMA4G
A1UdDwEB/wQEAwIFoDBCBgNVHR8EOzA5MDegNaAzhjJodHRwOi8vU1ZSVHJpYWwt
RzItY3JsLnZlcmlzaWduLmNvbS9TVlJUcmlhbEcyLmNybDBKBgNVHSAEQzBBMD8G
CmCGSAGG+EUBBxUwMTAvBggrBgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24u
Y29tL2Nwcy90ZXN0Y2EwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8G
A1UdIwQYMBaAFCgXE4q9lqKL3AYzr7aO2hBmYGT1MHQGCCsGAQUFBwEBBGgwZjAk
BggrBgEFBQcwAYYYaHR0cDovL29jc3AudmVyaXNpZ24uY29tMD4GCCsGAQUFBzAC
hjJodHRwOi8vU1ZSVHJpYWwtRzItYWlhLnZlcmlzaWduLmNvbS9TVlJUcmlhbEcy
LmNlcjANBgkqhkiG9w0BAQUFAAOCAQEATauH7Fnlee/X7T6s/zzr9zEKhLK3EQ3p
qaNc8wvix5c1Z9Pp3xzEKvp6TCLPSMbrOPGjFa1LFxAEUITz3W15CsKWR1AjWp12
qVSbCfxg/MWa9T7zd2oUBzjmz6ifcM5Tuub3QcZTuSpWeAKbAH/U+x+cj00EvB3z
cFa5hn/qcapKcqOXvHycwReCWNHBQgaGci365qkPzssv7oKrbnLhupjdxUE9OExu
3M13CXrAtQ2v1Rad1fJQYSTg90NqZmA9ghdKuKTnhCHDwwqOxNBuceII03IIPK70
m6CoYpntblgmFtyj9EvgIUdc4YIImm2B0q5c5q3iZARPH/gi//XeGg==
-----END CERTIFICATE-----
```

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

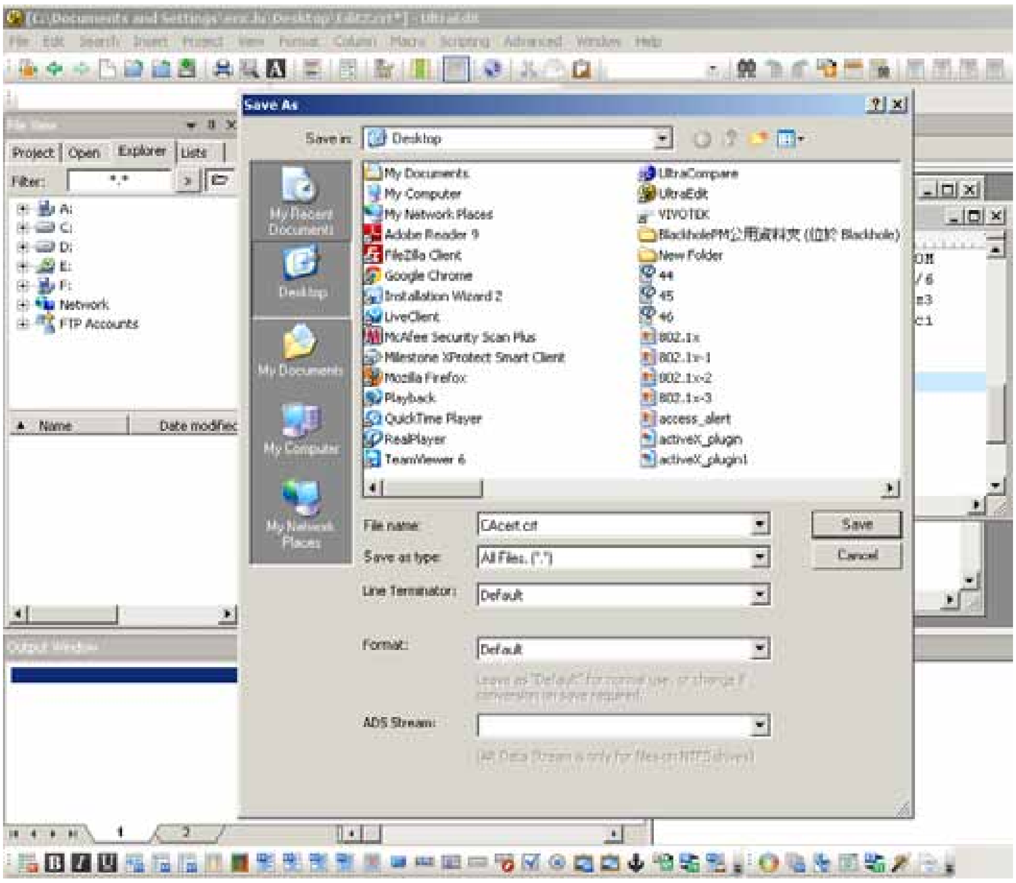


```
CmCGSAGG+EUBBxUwMTAvBggrBgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24u
Y29tL2Nwcy90ZXN0Y2EvMQYDVR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB0G
A1UdIwQYMBaAFCgXE4q91qKi3AYst7aO2hBmYG71MHQGCCsGAQUFBwEBBGgwZjAk
BggrBgEFBQcwAYYYaHR0cDovL29jc3AudmVyaXNpZ24uY29tMD4GCCsGAQUFBzAC
hjJodHRwOi8vU1ZSVHJpYWwtRzItYW1hLnZlcmlzaWduLmNvbS9TV1JUcm1hbEcy
LmNlcjANBgkqhkiG9w0BAQUFAAOCAQEATxuH7FnIae/X7T6z/zzr9zEKhLKSEQSp
qaNc8swixSc1Z9Pp3kzEKvp6TCLPSMbrOPGjPa1LFxAKUITr3W1SCoXWR1AjWp12
qVSbDfxgVMWx9T7rd2oURzjms6ifcM5Ttub3Qc2Tu3pWeAKbAH/U+x+ojG0EvB3z
cPaShn/qcapKcqOXVHycwHeCWNBRQgsGci368qkPzmsv7oErbnLhupjdxUE3GExu
3M13CXrAtQ2v1RadifJQYSTgS0Nq2mA9ghdEuKTnhCHUwwqOxN8uceII83ITPK70
m6CoYpntb1gmFtyj9EvgIUdc6YZImn2B0q5c5q3iZARPH/gi//XeGg==
-----END CERTIFICATE-----
```

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



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



Save As

Save in: Desktop

File name: CAcert.crt

Save as type: All Files. (*.*)

Line Terminator: Default

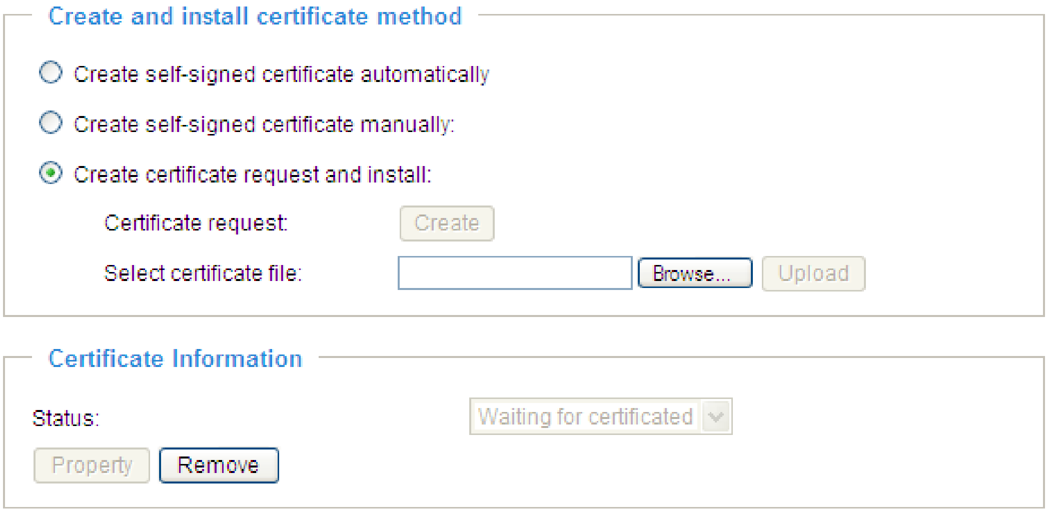
Format: Default

Leave as "Default" for normal use, or change if conversion on save required.

ADS Stream:

(Alt Data Stream is only for files on NTFS drives)

10. Return to the original firmware session.



Create and install certificate method

○ Create self-signed certificate automatically

○ Create self-signed certificate manually:

● Create certificate request and install:

Certificate request: Create

Select certificate file: Browse... Upload

Certificate Information

Status: Waiting for certificated

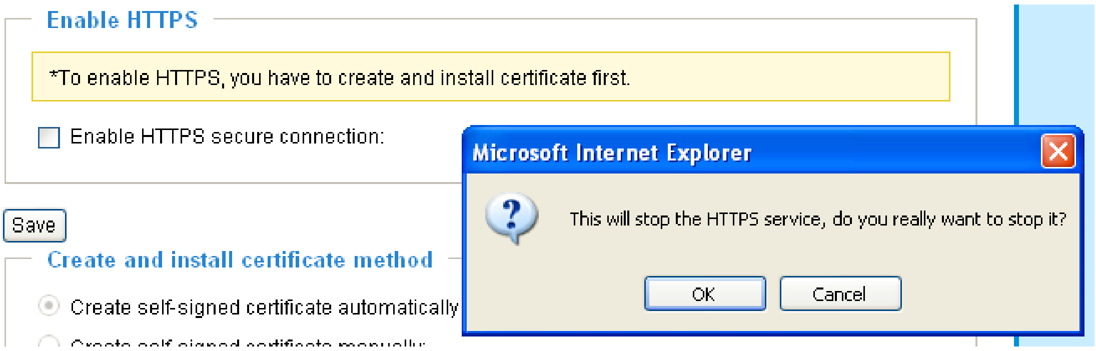
Property Remove

NOTE:

► *How do I cancel the HTTPS settings?*

*1. Uncheck **Enable HTTPS secure connection** in the first column and click **Save**; a warning dialog will pop up.*

*2. Click **OK** to disable HTTPS.*



Enable HTTPS

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

□ Enable HTTPS secure connection:

Save

Create and install certificate method

○ Create self-signed certificate automatically

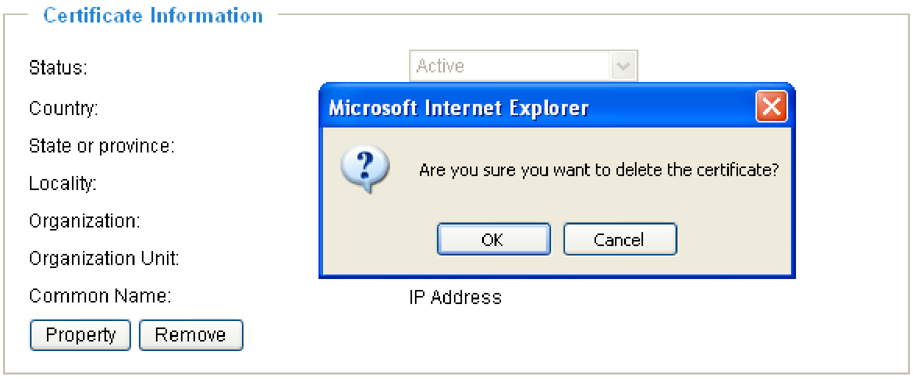
Microsoft Internet Explorer

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

OK Cancel

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

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



Certificate Information

Status: Active

Country:

State or province:

Locality:

Organization:

Organization Unit:

Common Name: IP Address

Property Remove

Microsoft Internet Explorer

Are you sure you want to delete the certificate?

OK Cancel

SNMP (Simple Network Management Protocol) Advanced Mode

This section explains how to use the SNMP on the network camera. The Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices. It helps network administrators to remotely manage network devices and find, solve network problems with ease.

■ The SNMP consists of the following three key components:

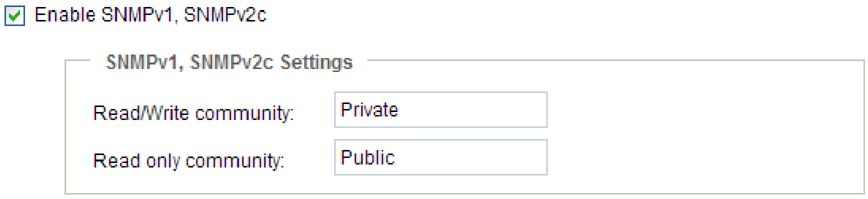
1. Manager: Network-management station (NMS), a server which executes applications that monitor and control managed devices.
2. Agent: A network-management software module on a managed device which transfers the status of managed devices to the NMS.
3. Managed device: A network node on a managed network. For example: routers, switches, bridges, hubs, computer hosts, printers, IP telephones, network cameras, web server, and database.

Before configuring SNMP settings on the this page, please enable your NMS first.

SNMP Configuration

Enable SNMPv1, SNMPv2c

Select this option and enter the names of Read/Write community and Read Only community according to your NMS settings.



☑ Enable SNMPv1, SNMPv2c

SNMPv1, SNMPv2c Settings

Read/Write community:	Private
Read only community:	Public

Enable SNMPv3

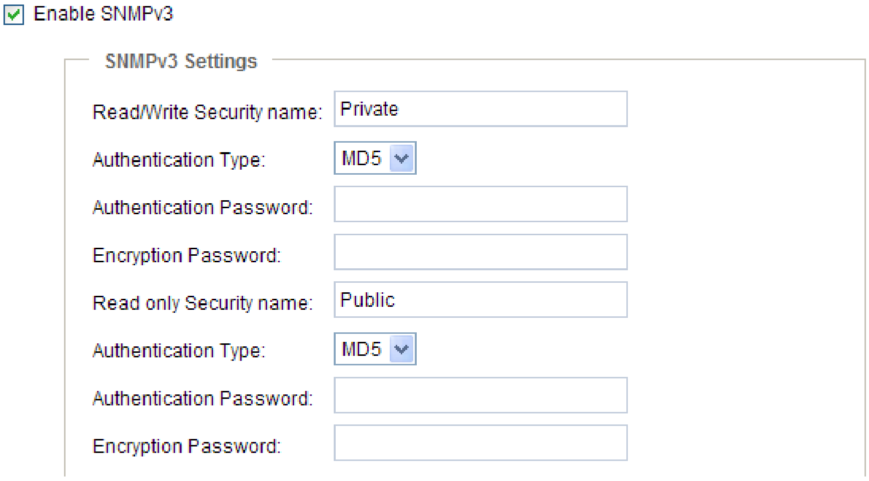
This option contains cryptographic security, a higher security level, which allows you to set the Authentication password and the Encryption password.

■ Security name: According to your NMS settings, choose Read/Write or Read Only and enter the community name.

■ Authentication type: Select MD5 or SHA as the authentication method.

■ Authentication password: Enter the password for authentication (at least 8 characters).

■ Encryption password: Enter a password for encryption (at least 8 characters).



☑ Enable SNMPv3

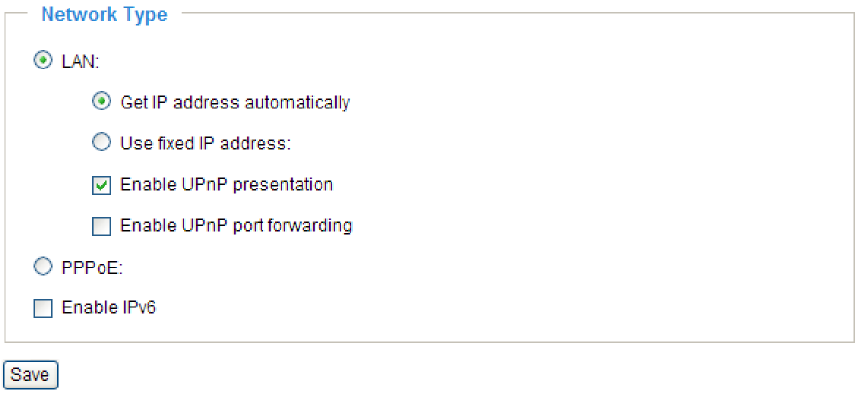
SNMPv3 Settings

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

Network

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

Network Type



Network Type

● LAN:

● Get IP address automatically

○ Use fixed IP address:

☑ Enable UPnP presentation

□ Enable UPnP port forwarding

○ PPPoE:

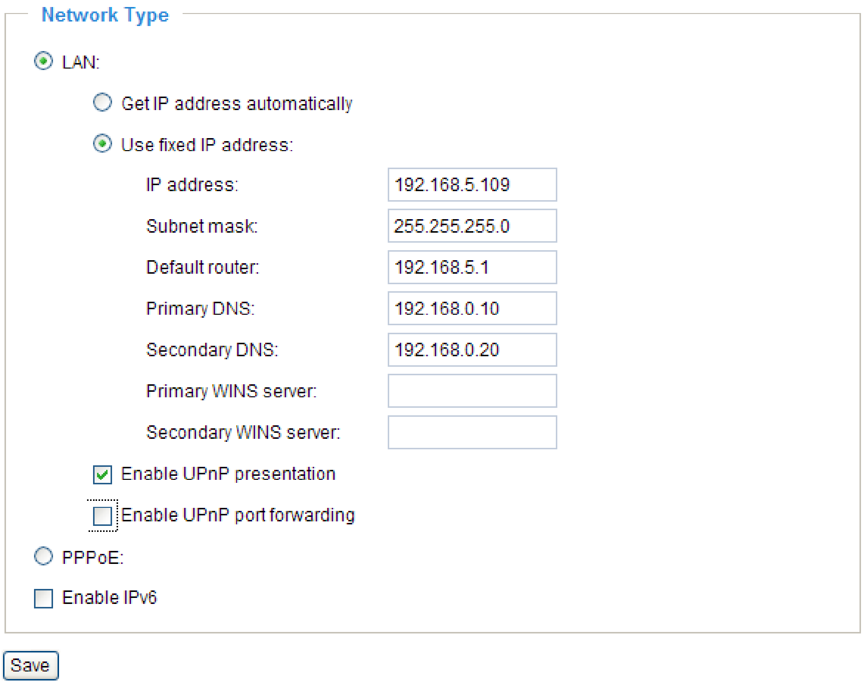
□ Enable IPv6

LAN

Select this option when the Network Camera is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. Rememer to click **Save** when you complete the Network setting.

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

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:	192.168.5.109
Subnet mask:	255.255.255.0
Default router:	192.168.5.1
Primary DNS:	192.168.0.10
Secondary DNS:	192.168.0.20
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 14 for details.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP.

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

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

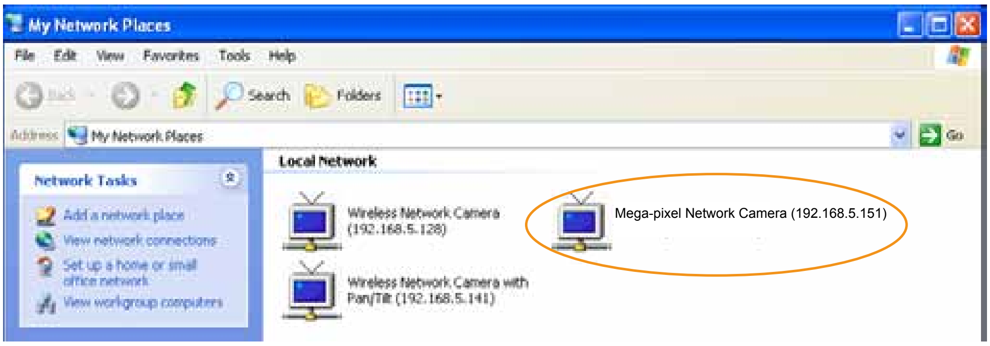
Primary DNS: The primary domain name server that translates hostnames into IP addresses.

Secondary DNS: Secondary domain name server that backups the Primary DNS.

Primary WINS server: The primary WINS server that maintains the database of computer name and IP address.

Secondary WINS server: The secondary WINS server that maintains the database of computer name and IP address.

Enable UPnP presentation: Select this option to enable UPnP^{TM} 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^{TM} is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP^{TM} component is installed on your computer.

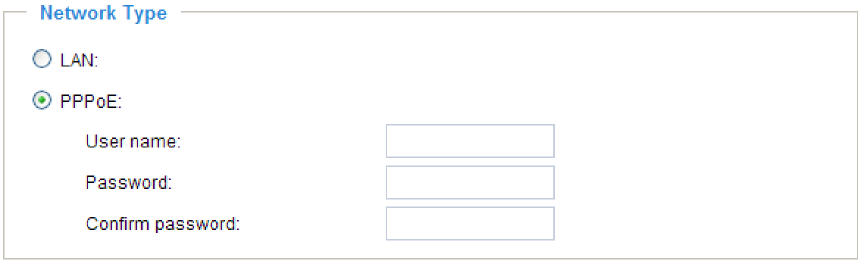


Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP^{TM} and it is activated.

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 82) to add a new email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 85). Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > Network Type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.



Network Type

○ LAN:

● PPPoE:

User name:

Password:

Confirm password:

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

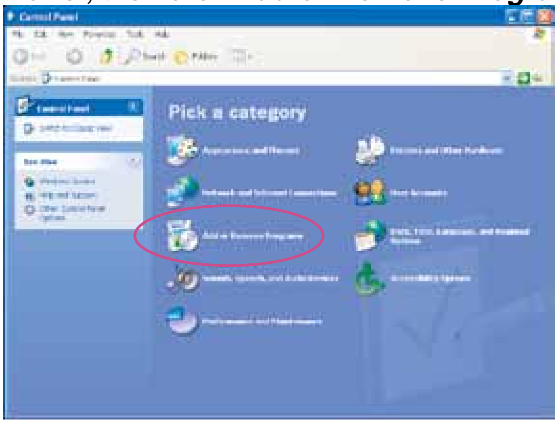
NOTE:

- ► *If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.*

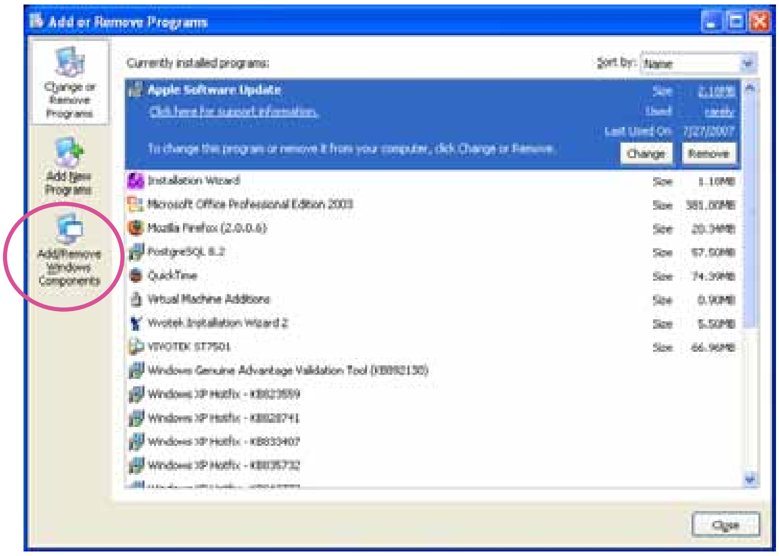
- ► *If UPnP™ is not supported by your router, you will see the following message:*
  Error: Router does not support UPnP port forwarding.

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

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



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

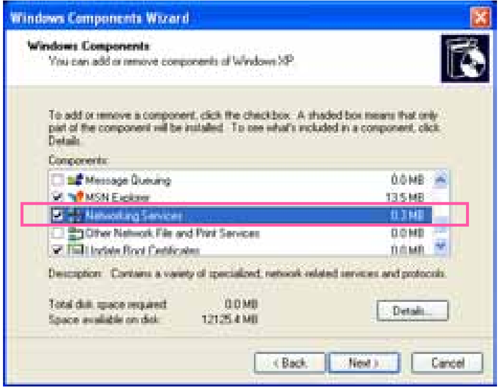


Currently installed programs:

Sort by: Name

Apple Software Update Click here for support information. To change this program or remove it from your computer, click Change or Remove.	Size Used Last Used On	2.10MB rarely 7/27/2007
Installation Wizard	Size	1.10MB
Microsoft Office Professional Edition 2003	Size	381.00MB
Mozilla Firefox (2.0.0.6)	Size	20.34MB
PostgreSQL 8.2	Size	57.50MB
QuickTime	Size	74.39MB
Virtual Machine Additions	Size	0.90MB
Vivotek Installation Wizard 2	Size	5.50MB
VIVOTEK ST7501	Size	66.96MB
Windows Genuine Advantage Validation Tool (KB892130)		
Windows XP Hotfix - KB823559		
Windows XP Hotfix - KB828741		
Windows XP Hotfix - KB833407		
Windows XP Hotfix - KB835732		

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



Windows Components

You can add or remove components of Windows XP

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

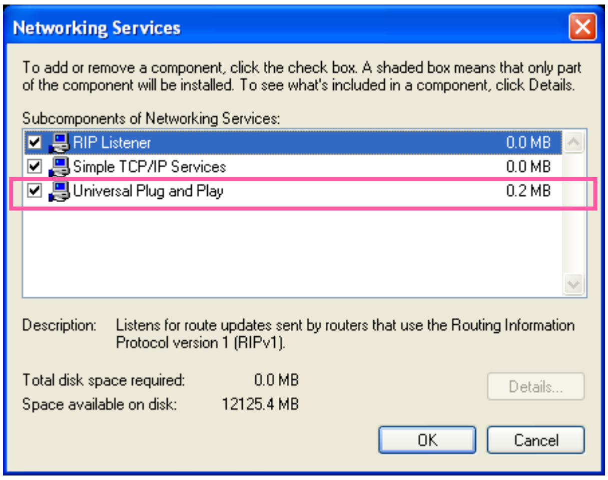
□	Message Queuing	0.0 MB
☑	MSN Explorer	13.5 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB
☑	Update Root Certificates	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 12125.4 MB

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



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

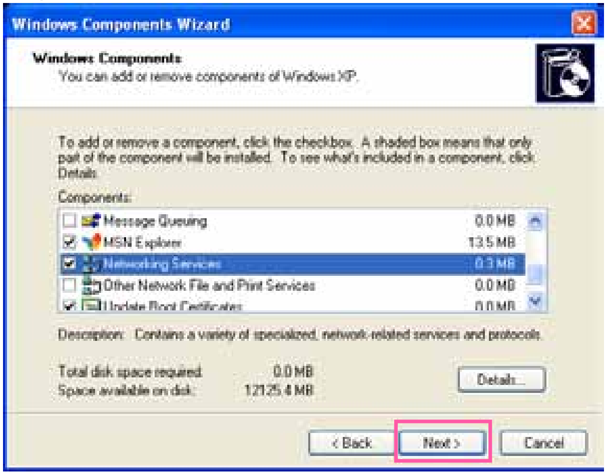
☑	RIP Listener	0.0 MB
☑	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Listens for route updates sent by routers that use the Routing Information Protocol version 1 (RIPv1).

Total disk space required: 0.0 MB

Space available on disk: 12125.4 MB

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



Windows Components Wizard

Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

□	Message Queuing	0.0 MB
☑	MSN Explorer	13.5 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB
☑	Update Root Certificates	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 12125.4 MB

6. *Click* ***Finish****. UPnP^{TM} is enabled.*

► *How does UPnP^{TM} work?*
UPnP^{TM} networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.

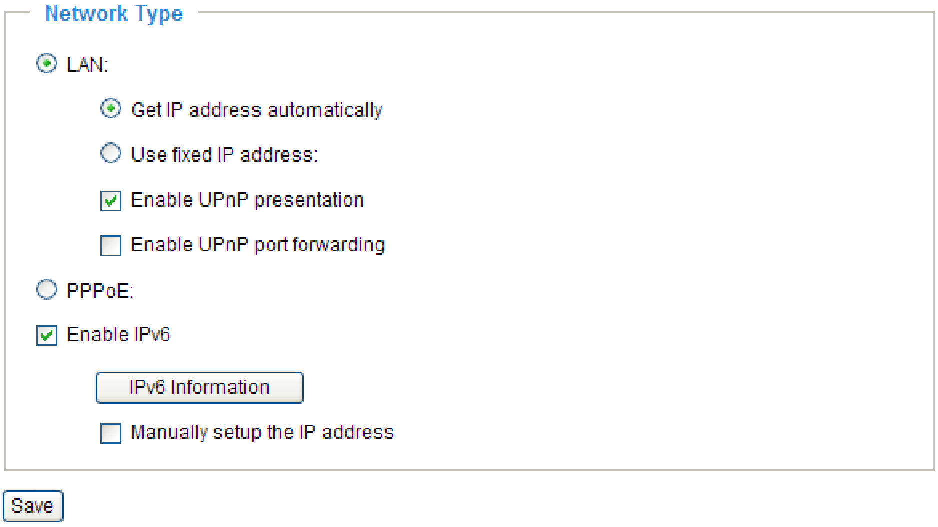
► *Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.*

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

► *If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 99 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.*

Enable IPv6

Select this option and click **Save** to enable IPv6 settings.
Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.



Network Type

● LAN:

● Get IP address automatically

○ Use fixed IP address:

☑ Enable UPnP presentation

□ Enable UPnP port forwarding

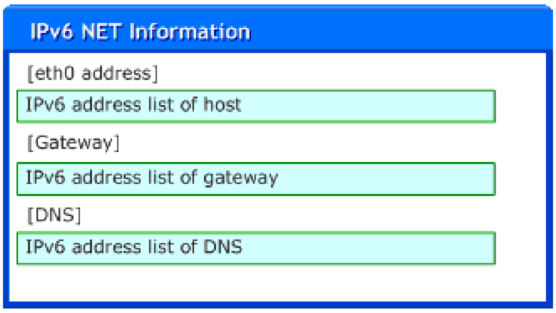
○ PPPoE:

☑ Enable IPv6

□ Manually setup the IP address

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

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



IPv6 NET Information

[eth0 address]

IPv6 address list of host

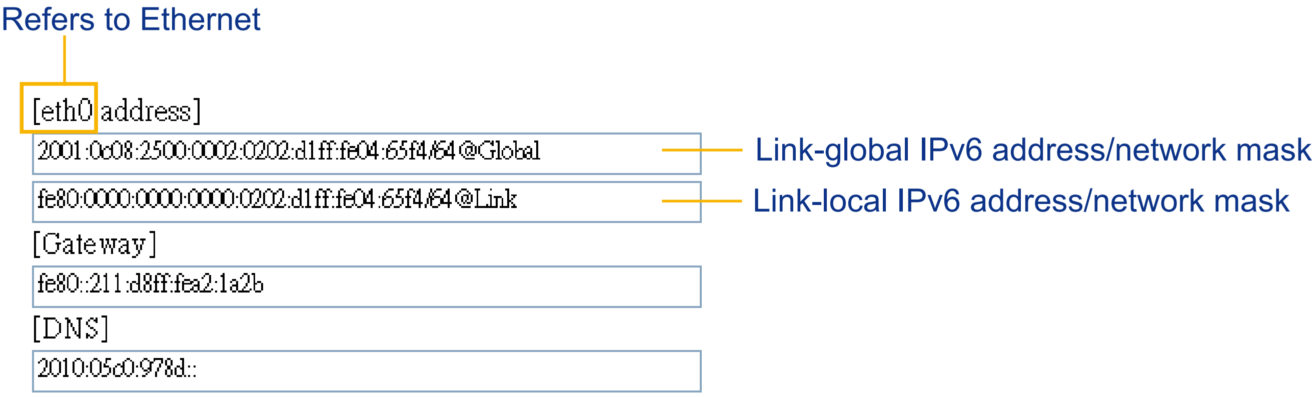
[Gateway]

IPv6 address list of gateway

[DNS]

IPv6 address list of DNS

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



Refers to Ethernet

[eth0 address]

2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global

fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link

[Gateway]

fe80::211:d8ff:fea2:1a2b

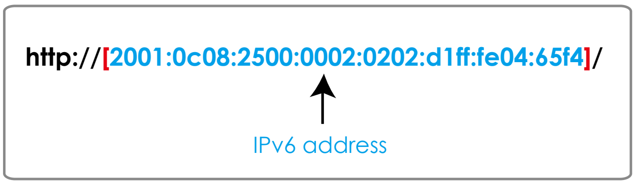
[DNS]

2010:05c0:978d::

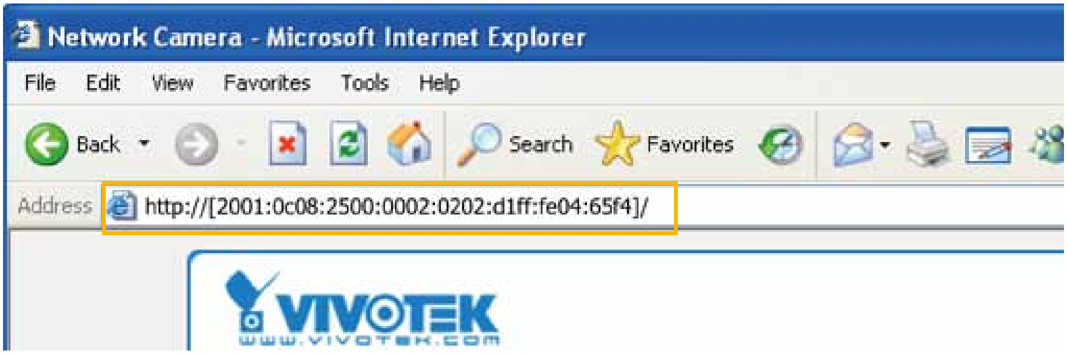
Link-global IPv6 address/network mask

Link-local IPv6 address/network mask

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


http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/

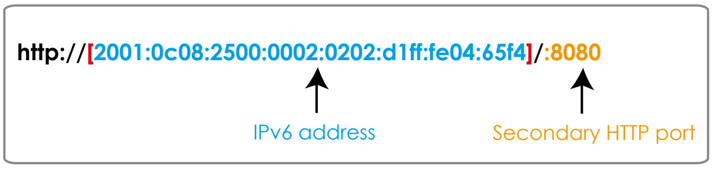
4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.
For example:



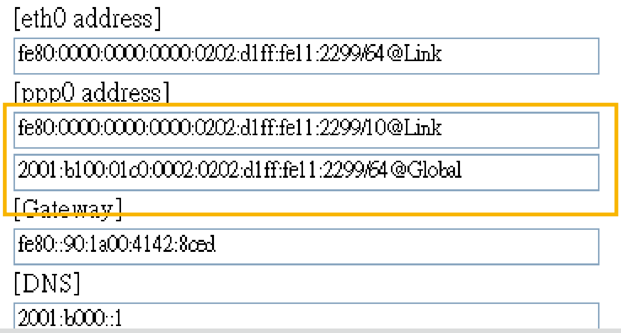
http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/

NOTE:

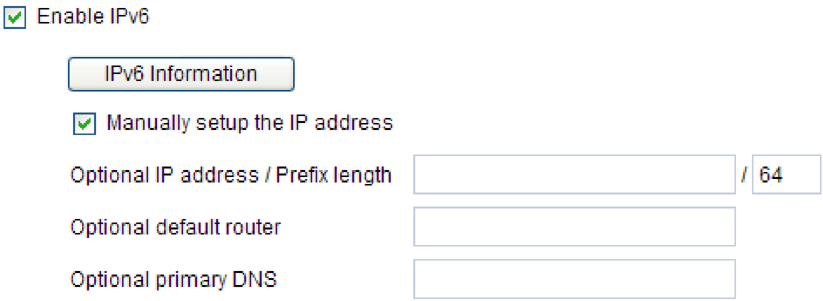
► *If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to* ***HTTP*** *on page 47 for detailed information.)*


http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/:8080

► *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:b100:01c0:0002:0202:d1ff:fe11:2299/64@Global
[Gateway]
fe80::90:1a00:4142:8ced
[DNS]
2001:b000::1

Manually set up the IP address: Select this option to manually set up IPv6 settings if your network environment does not have DHCPv6 server and advertisements-enabled routers.
If you check this item, the following blanks will be displayed for you to enter the corresponding information:


☑ Enable IPv6

☑ Manually setup the IP address

Optional IP address / Prefix length / 64

Optional default router

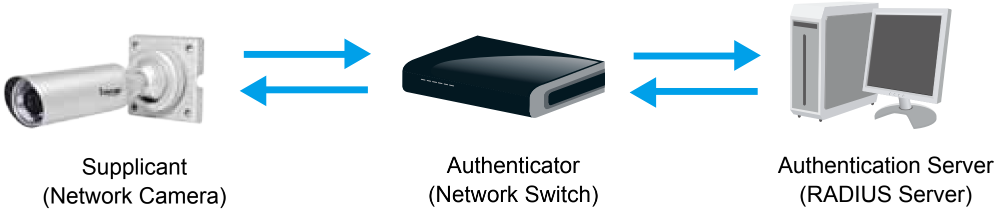
Optional primary DNS

IEEE 802.1x Advanced Mode

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

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

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

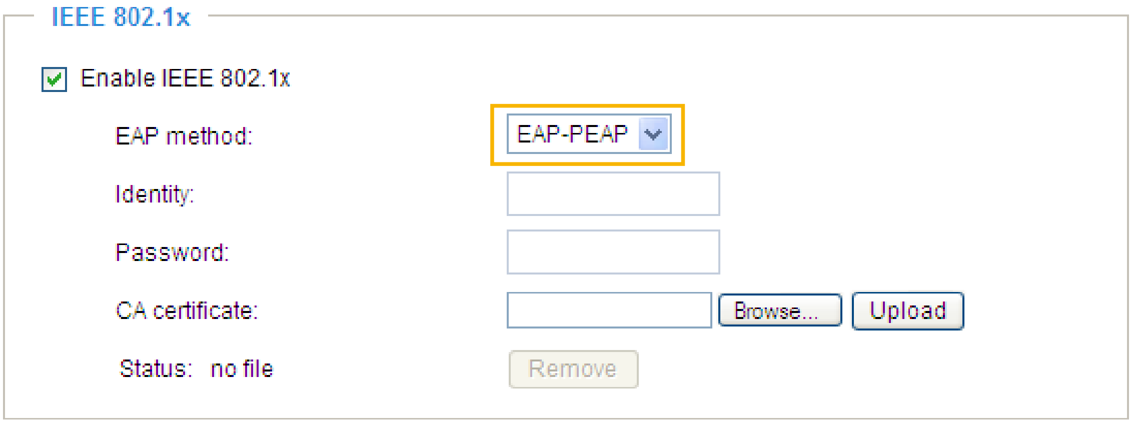


1. Supplicant: A client end user (camera), which requests authentication.
2. Authenticator (an access point or a switch): A “go between” which restricts unauthorized end users from communicating with the authentication server.
3. Authentication server (usually a RADIUS server): Checks the client certificate and decides whether to accept the end user’s access request.

■ VIVOTEK Network Cameras support two types of EAP methods to perform authentication: **EAP-PEAP** and **EAP-TLS**.

Please follow the steps below to enable 802.1x settings:

1. Before connecting the Network Camera to the protected network with 802.1x, please apply a digital certificate from a Certificate Authority (ie. MIS of your company) which can be validated by a RADIUS server.
2. Connect the Network Camera to a PC or notebook outside of the protected LAN. Open the configuration page of the Network Camera as shown below. Select **EAP-PEAP** or **EAP-TLS** as the EAP method. In the following blanks, enter your ID and password issued by the CA, then upload related certificate(s).



IEEE 802.1x

☑ Enable IEEE 802.1x

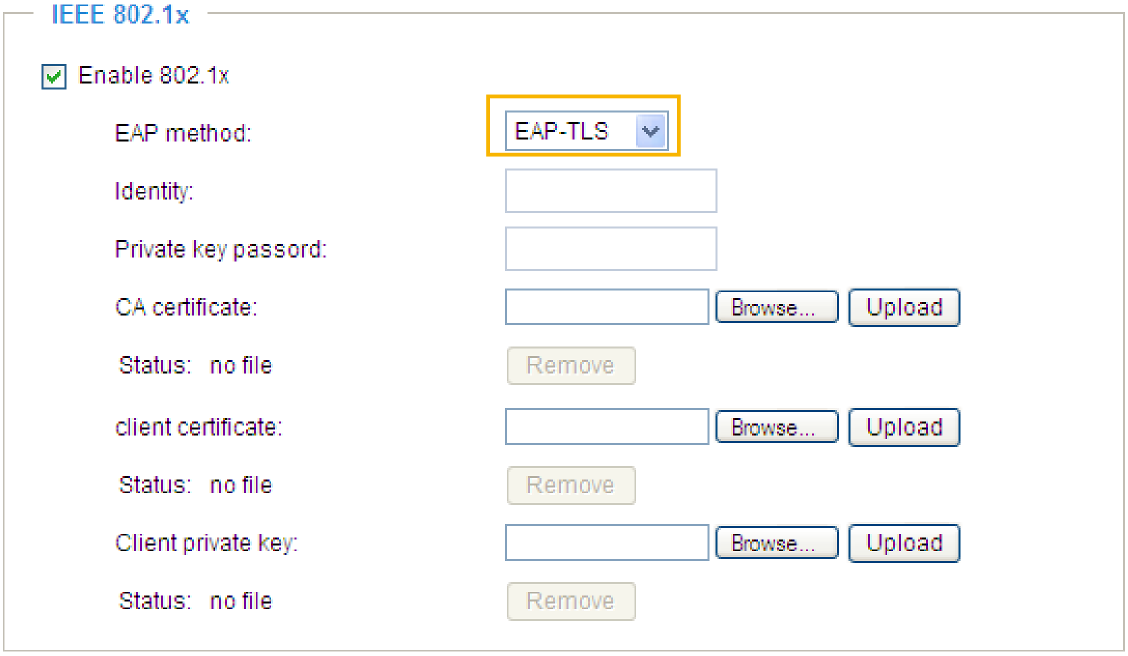
EAP method: EAP-PEAP

Identity:

Password:

CA certificate:

Status: no file



IEEE 802.1x

☑ Enable 802.1x

EAP method:	EAP-TLS		
Identity:			
Private key passord:			
CA certificate:		Browse...	Upload
Status: no file	Remove		
client certificate:		Browse...	Upload
Status: no file	Remove		
Client private key:		Browse...	Upload
Status: no file	Remove		

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

NOTE:

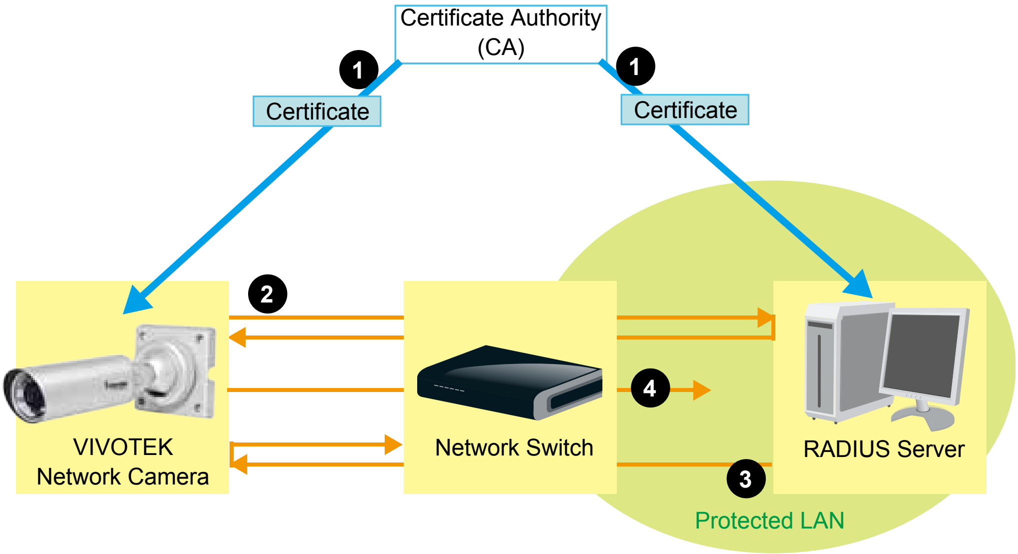
► *The authentication process for 802.1x:*

1. The Certificate Authority (CA) provides the required signed certificates to the Network Camera (the supplicant) and the RADIUS Server (the authentication server).

2. A Network Camera requests access to the protected LAN using 802.1X via a switch (the authenticator). The client offers its identity and client certificate, which is then forwarded by the switch to the RADIUS Server, which uses an algorithm to authenticate the Network Camera and returns an acceptance or rejection back to the switch.

3. The switch also forwards the RADIUS Server's certificate to the Network Camera.

4. Assuming all certificates are validated, the switch then changes the Network Camera's state to authorized and is allowed access to the protected network via a pre-configured port.



QoS (Quality of Service) Advanced Mode

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

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

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

Requirements for QoS

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

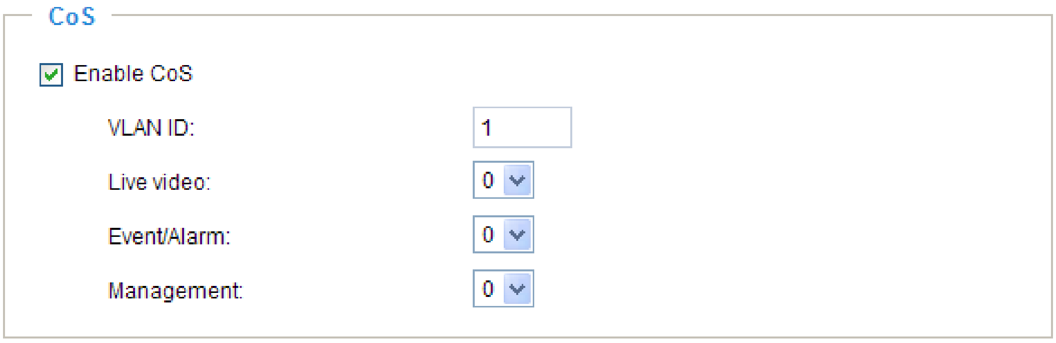
- All network switches and routers in the network must include support for QoS.
- The network video devices used in the network must be QoS-enabled.

QoS models

CoS (the VLAN 802.1p model)

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

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



CoS

☑ Enable CoS

VLAN ID: 1

Live video: 0

Event/Alarm: 0

Management: 0

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

NOTE:

► *A VLAN -capable Switch (802.1p) is required. A web session may fail if the CoS setting is incorrect.*

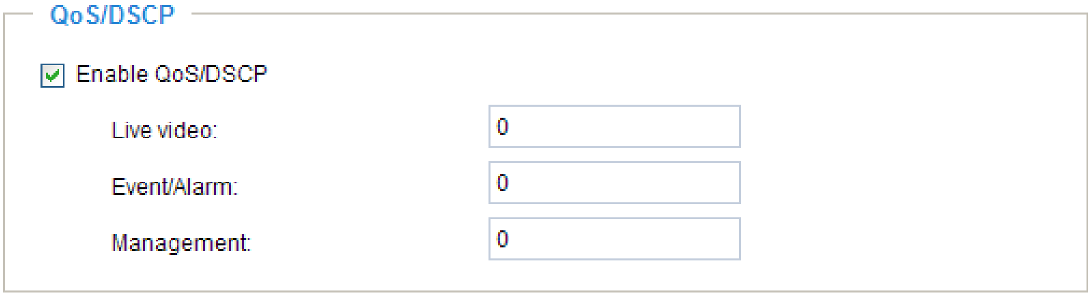
► *Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.*

► *Although CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.*

QoS/DSCP (the DiffServ model)

DSCP-ECN defines QoS at Layer 3 (Network Layer). The Differentiated Services (DiffServ) model is based on packet marking and router queuing disciplines. The marking is done by adding a field to the IP header, called the DSCP (Differentiated Services Codepoint). This is a 6-bit field that provides 64 different class IDs. It gives an indication of how a given packet is to be forwarded, known as the Per Hop Behavior (PHB). The PHB describes a particular service level in terms of bandwidth, queueing theory, and dropping (discarding the packet) decisions. Routers at each network node classify packets according to their DSCP value and give them a particular forwarding treatment; for example, how much bandwidth to reserve for it.

Below are the setting options of DSCP (DiffServ Codepoint). Specify the DSCP value for each application (0~63).



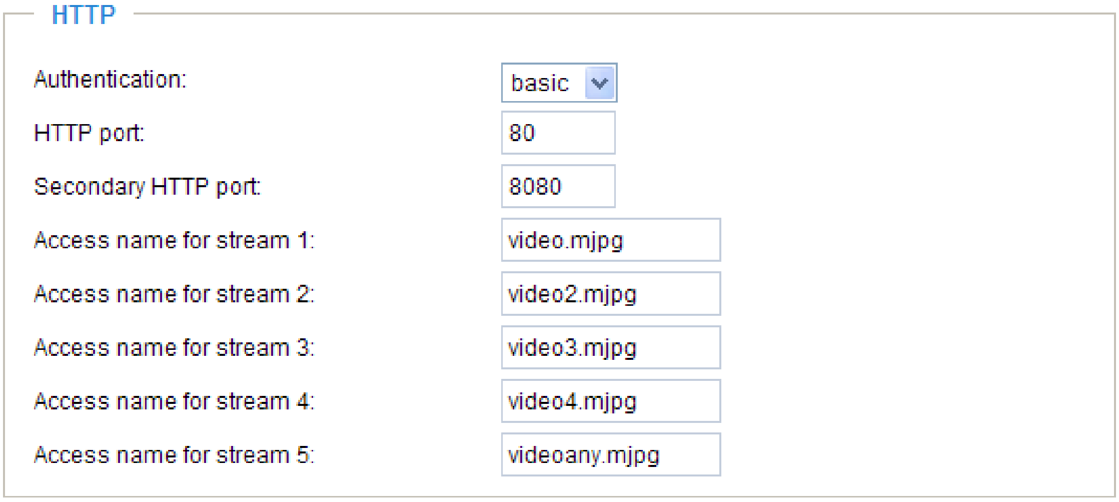
QoS/DSCP

☑ Enable QoS/DSCP

Live video:	0
Event/Alarm:	0
Management:	0

HTTP Advanced Mode

To utilize HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security on page 30 for details.

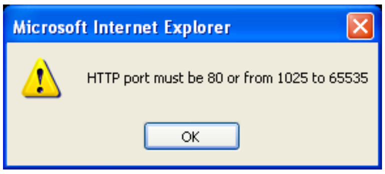


HTTP

Authentication:	basic
HTTP port:	80
Secondary HTTP port:	8080
Access name for stream 1:	video.mjpg
Access name for stream 2:	video2.mjpg
Access name for stream 3:	video3.mjpg
Access name for stream 4:	video4.mjpg
Access name for stream 5:	videoany.mjpg

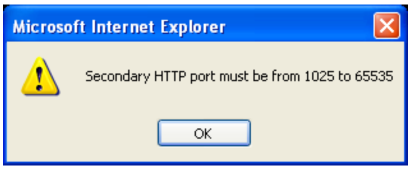
Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest.
If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. 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:



Microsoft Internet Explorer

HTTP port must be 80 or from 1025 to 65535



Microsoft Internet Explorer

Secondary HTTP port must be from 1025 to 65535

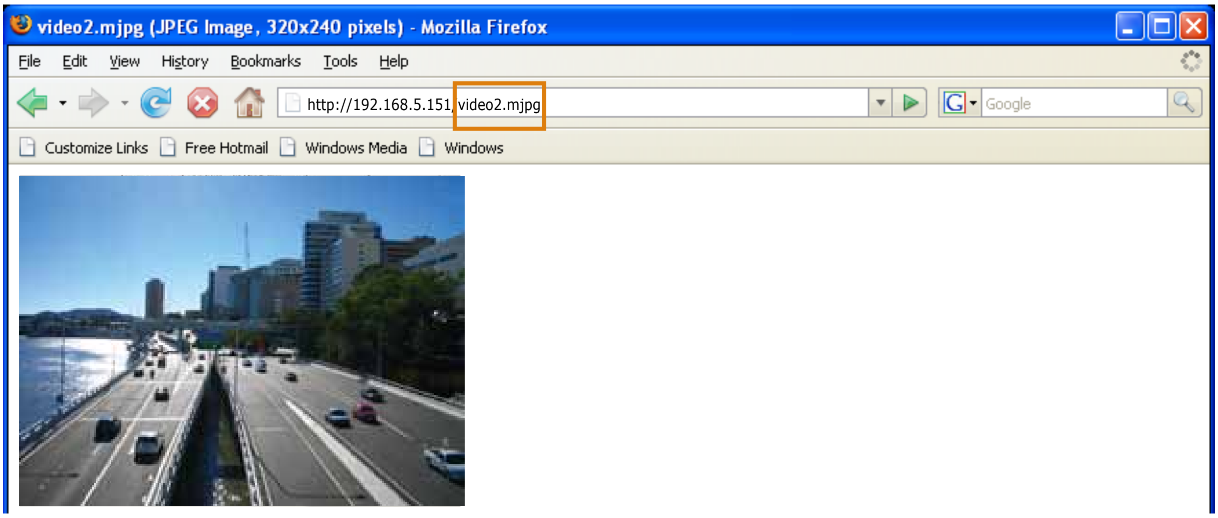
To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

On the LAN
http://192.168.4.160 or http://192.168.4.160:8080

Access name for stream 1 ~ 5: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. Users can click **Configuration > Video > Video Settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Viewing Windows on page 61.

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

URL command -- http://<ip address>:<http port>/<access name for stream 1 ~ 5>
For example, when the Access name for stream 2 is set to video2.mjpg:
1. Launch Mozilla Firefox or Netscape.
2. Type the above URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.



video2.mjpg (JPEG Image, 320x240 pixels) - Mozilla Firefox

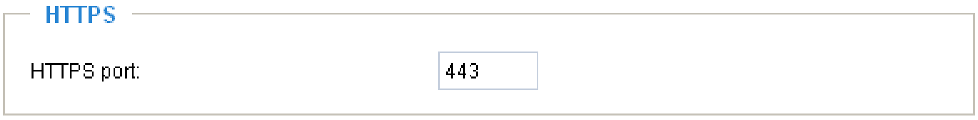
http://192.168.5.151/video2.mjpg

NOTE:

► *Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream 1 ~ 5> will fail to access the Network Camera.*

► *Users can only use URL commands to request the stream 5. For more information about URL commands, please refer to page 103.*

HTTPS

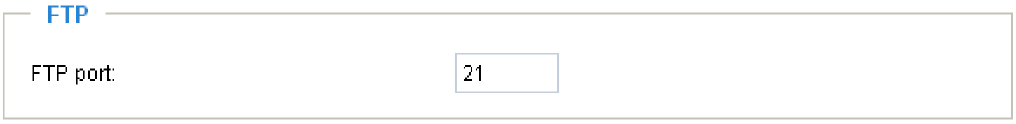


HTTPS

HTTPS port: 443

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

FTP



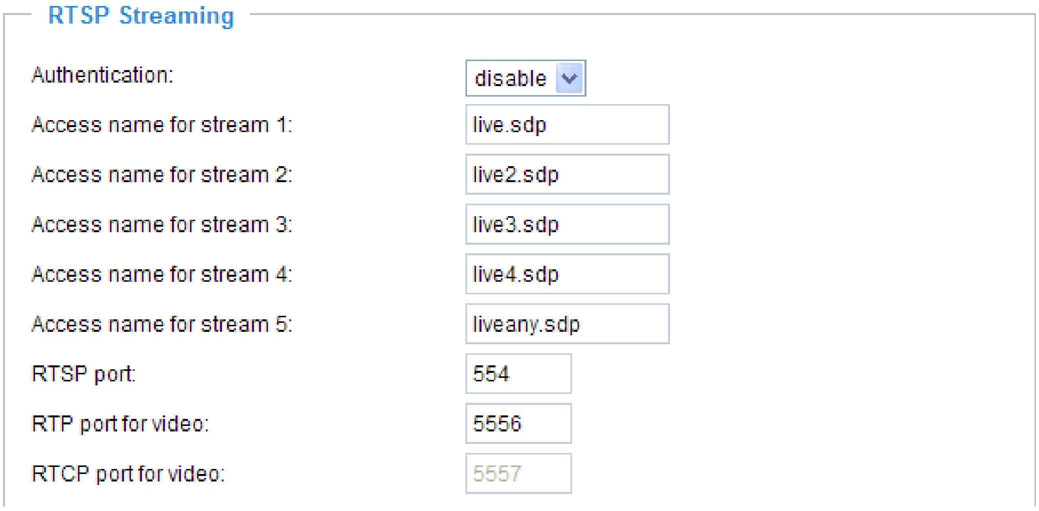
FTP

FTP port: 21

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

RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for the Network Camera first; please refer to Security on page 30 for details.



RTSP Streaming

Authentication:	disable
Access name for stream 1:	live.sdp
Access name for stream 2:	live2.sdp
Access name for stream 3:	live3.sdp
Access name for stream 4:	live4.sdp
Access name for stream 5:	liveany.sdp
RTSP port:	554
RTP port for video:	5556
RTCP port for video:	5557

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

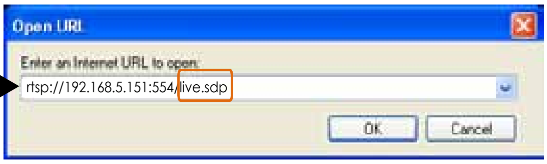
Access name for stream 1 ~ 5: This Network Camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.

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

rtsp://<ip address>:<rtsp port>/<access name for stream1 ~ 5>

For example, when the access name for stream 1 is set to live.sdp:

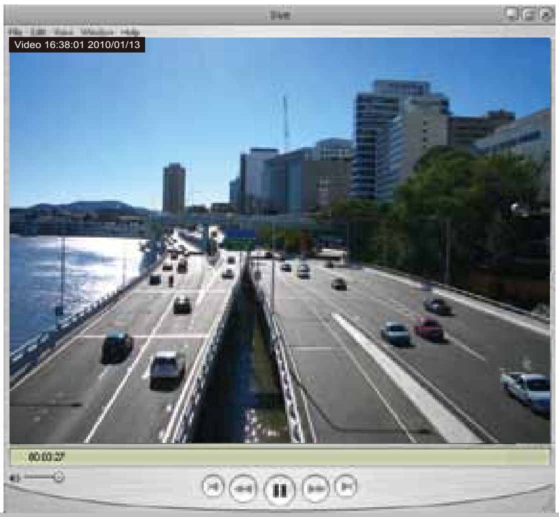
1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the above URL command in the text box.
4. The live video will be displayed in your player as shown below.



Open URL

Enter an Internet URL to open:

rtsp://192.168.5.151:554/live.sdp



RTSP port /RTP port for video/ RTCP port for video

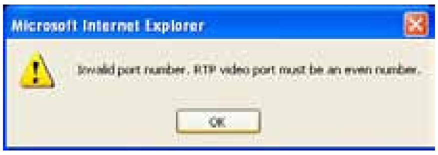
- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

- The RTP (Real-time Transport Protocol) is used to deliver video data to the clients. By default, the RTP port for video is set to 5556.

- The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557.

The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always an odd number. When the RTP port changes, the RTCP port will change accordingly.

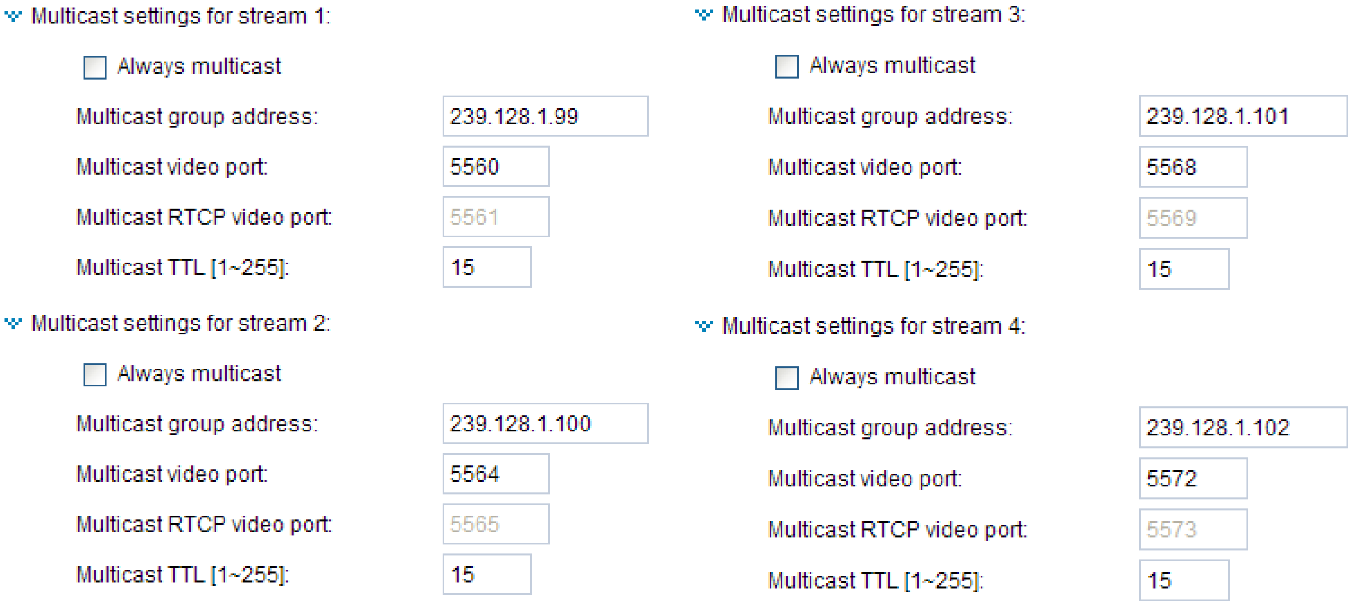
If the RTP ports are incorrectly assigned, the following warning message will be displayed:



Microsoft Internet Explorer

Invalid port number. RTP video port must be an even number.

Multicast settings for stream 1 ~ 4: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1 ~ 4.



Multicast settings for stream 1:

□ Always multicast

Multicast group address: 239.128.1.99

Multicast video port: 5560

Multicast RTCP video port: 5561

Multicast TTL [1~255]: 15

Multicast settings for stream 2:

□ Always multicast

Multicast group address: 239.128.1.100

Multicast video port: 5564

Multicast RTCP video port: 5565

Multicast TTL [1~255]: 15

Multicast settings for stream 3:

□ Always multicast

Multicast group address: 239.128.1.101

Multicast video port: 5568

Multicast RTCP video port: 5569

Multicast TTL [1~255]: 15

Multicast settings for stream 4:

□ Always multicast

Multicast group address: 239.128.1.102

Multicast video port: 5572

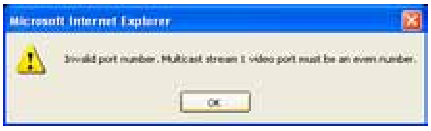
Multicast RTCP video port: 5573

Multicast TTL [1~255]: 15

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

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus is always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:



Microsoft Internet Explorer

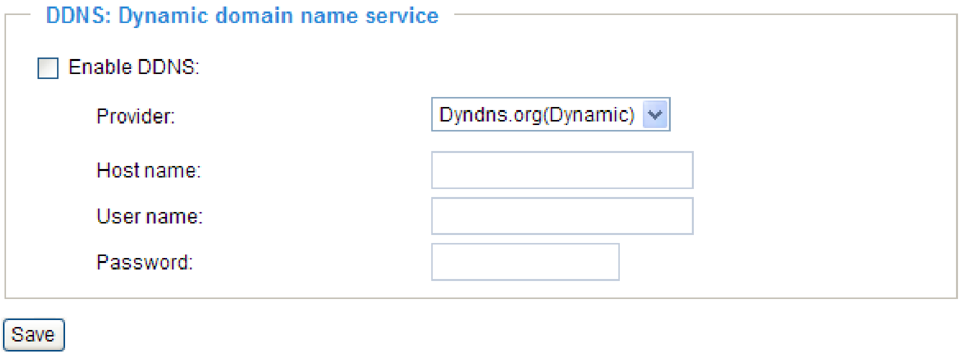
Invalid port number. Multicast stream 1 video port must be an even number.

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

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



DDNS: Dynamic domain name service

□ Enable DDNS:

Provider: Dyndns.org(Dynamic)

Host name:

User name:

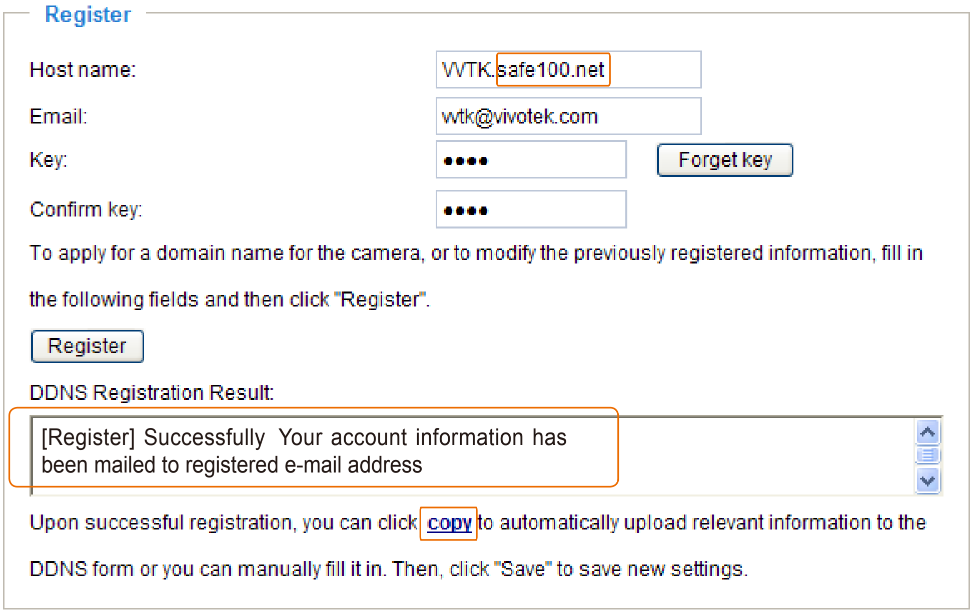
Password:

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

Provider: Select a DDNS provider from the provider drop-down list.
VIVOTEK offers **Safe100.net**, a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's Network Cameras from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it.
Note that before utilizing this function, please apply for a dynamic domain account first.

■ Safe100.net

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



Register

Host name: VVTK.safe100.net

Email: vvtk@vivotek.com

Key: ●●●●

Confirm key: ●●●●

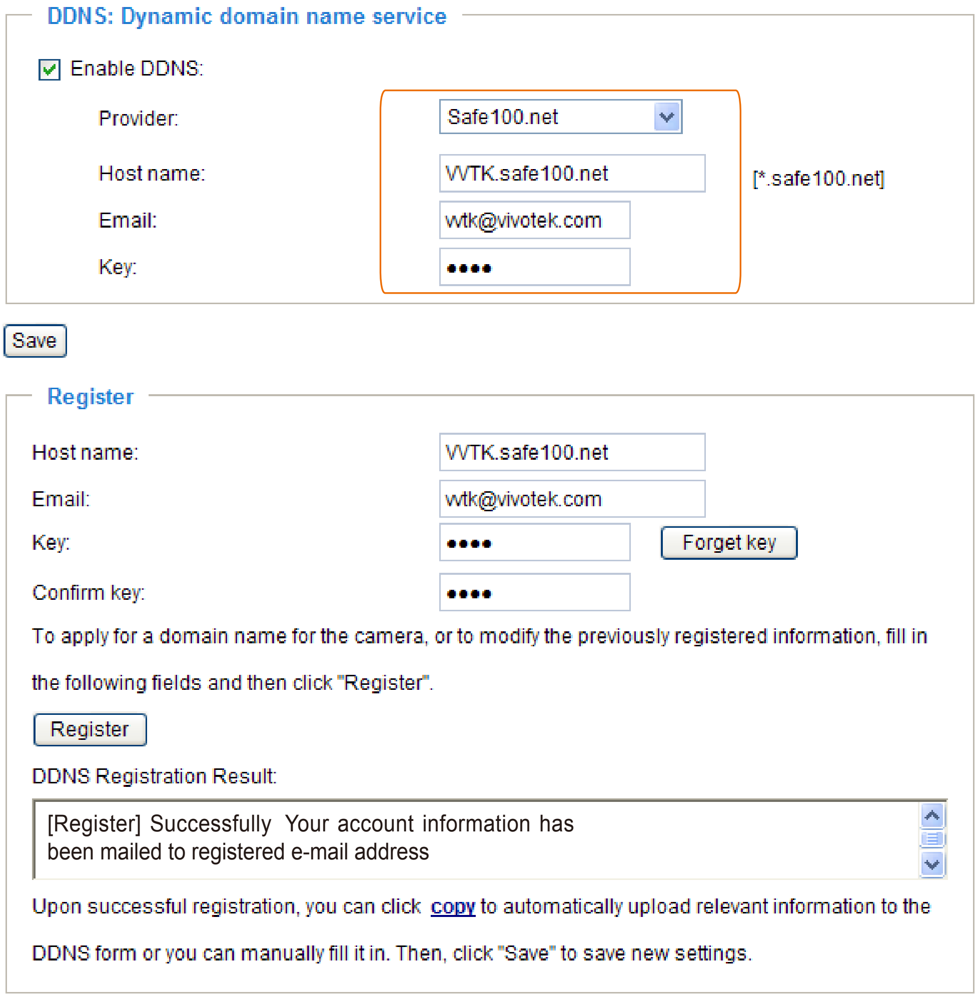
To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".

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.

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:	VVTK.safe100.net	[*.safe100.net]
Email:	wtk@vivotek.com	
Key:	••••	

Save

Register

Host name:	VVTK.safe100.net	
Email:	wtk@vivotek.com	
Key:	••••	Forget 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".

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 and click **Save** to enable the setting.

■ CustomSafe100

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

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

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

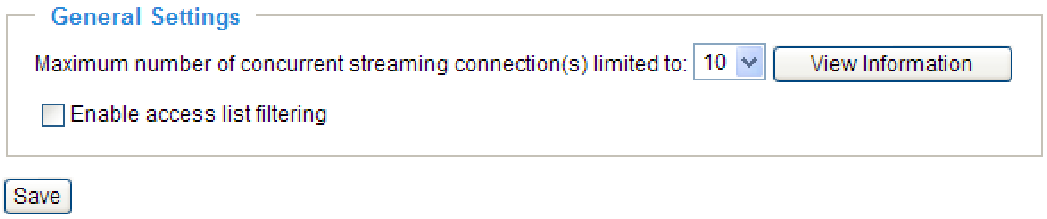
Refer to the following links to apply for a dynamic domain account when selecting other DDNS providers:

■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/
■ TZO.com: visit http://www.tzo.com/
■ DHS.org: visit http://www.dhs.org/
■ dyn-interfree.it: visit http://dyn-interfree.it/

Access List Advanced Mode

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

General Settings



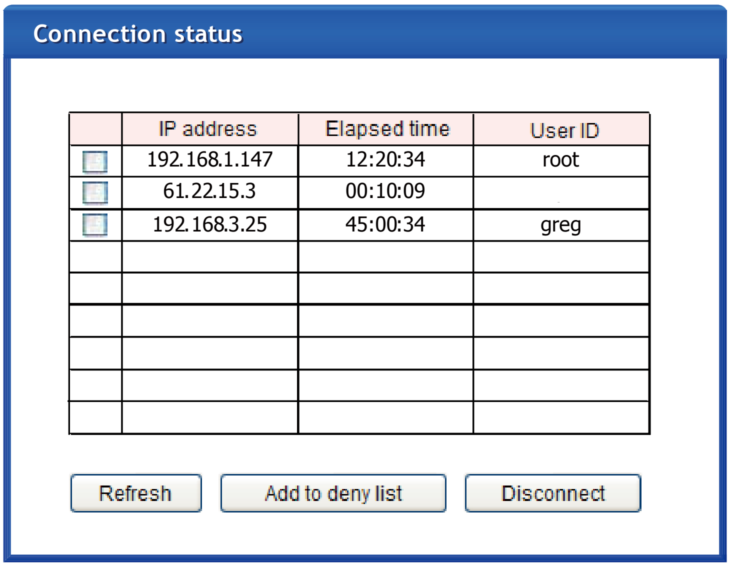
General Settings

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

□ Enable access list filtering

Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 ~ stream 5). 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. Note that only computers currently having a live view session will be listed here.
For example:



Connection status

	IP address	Elapsed time	User ID
□	192.168.1.147	12:20:34	root
□	61.22.15.3	00:10:09	
□	192.168.3.25	45:00:34	greg

■ 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 30.
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 49.
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 30.

■ 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).

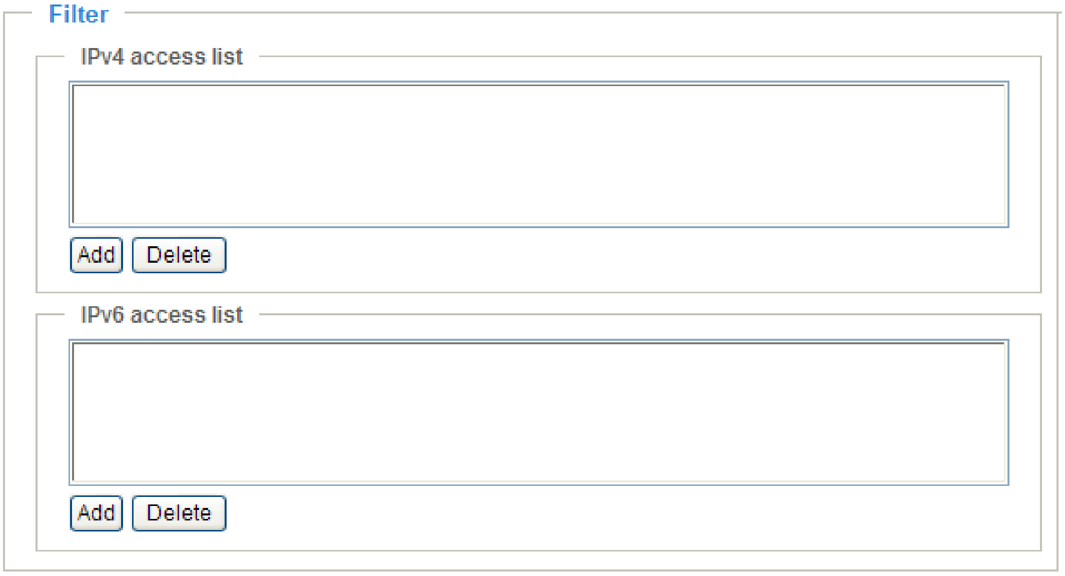
Enable access list filtering: Check this item and click **Save** if you want to enable the access list filtering function.

Filter Type

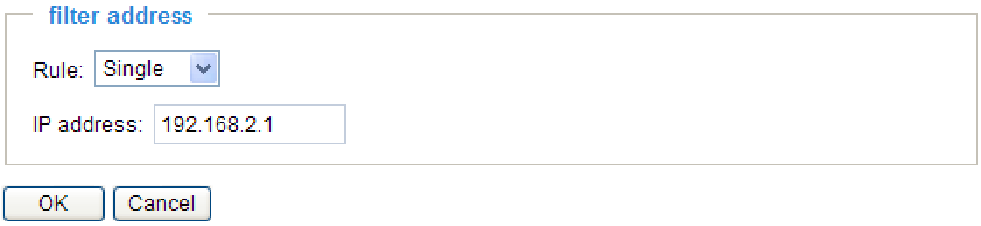
Select **Allow** or **Deny** as the filter type. If you choose **Allow Type**, only those clients whose IP addresses are on the Access List below can access the Network Camera, and the others cannot access. On the contrary, if you choose **Deny Type**, those clients whose IP addresses are on the Access List below will not be allowed to access the Network Camera, and the others can access.

Filter

Then you can add a rule to the following Access List. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to page 41 for detailed information.

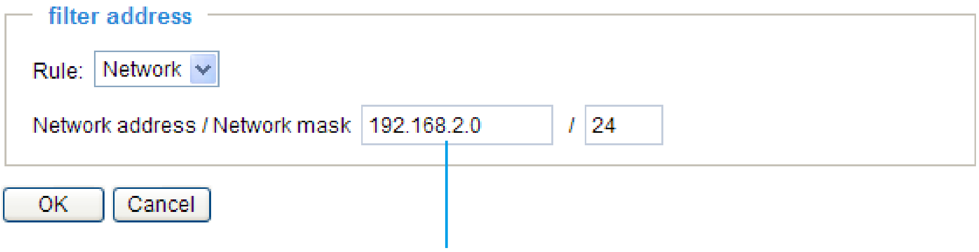


There are three types of rules:
Single: This rule allows the user to add an IP address to the Allowed/Denied list.
For example:



Rule: Single
IP address: 192.168.2.1

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



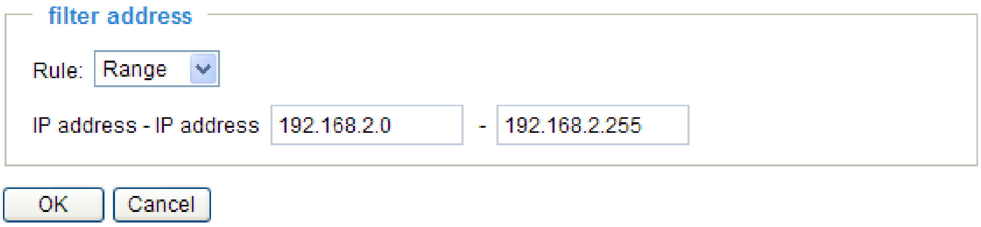
Rule: Network

Network address / Network mask 192.168.2.0 / 24

IP address 192.168.2.x will be blocked.

This column is also available with IPv6 addresses. Only that a prefix length is entered in the network mask field.

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

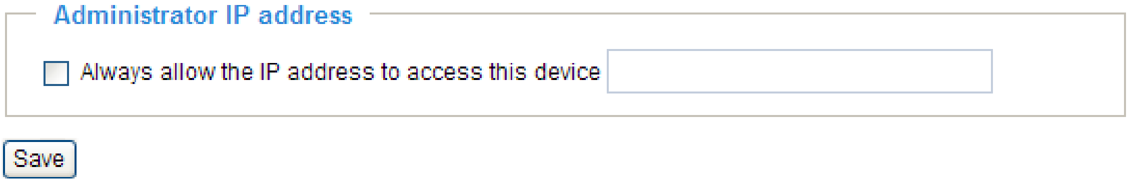


Rule: Range

IP address - IP address 192.168.2.0 - 192.168.2.255

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.

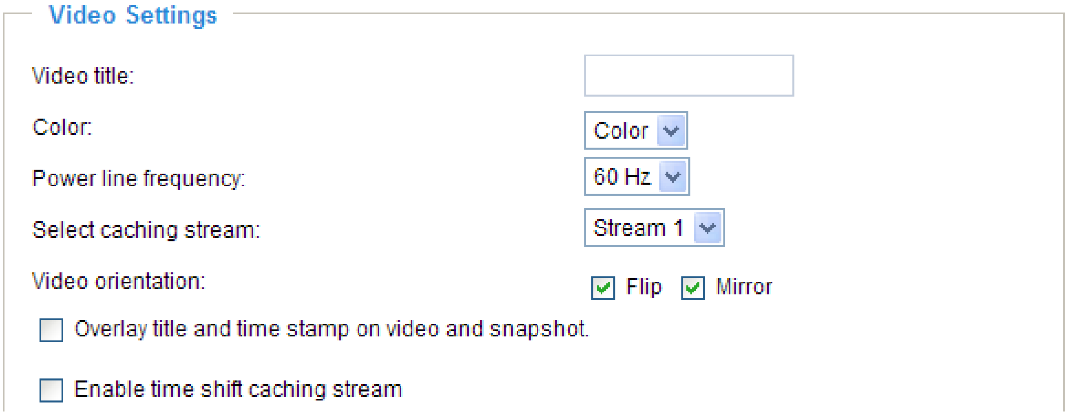


□ Always allow the IP address to access this device

Video

This section explains how to configure the video settings of the Network Camera.

Video Settings



Video Settings

Video title:

Color: Color

Power line frequency: 60 Hz

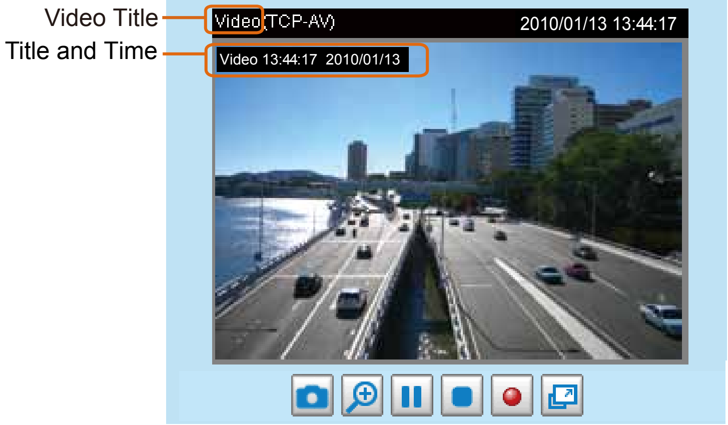
Select caching stream: Stream 1

Video orientation: ☑ Flip ☑ Mirror

□ Overlay title and time stamp on video and snapshot.

□ Enable time shift caching stream

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 in order for the new setting to take effect.

Select caching stream: This Network Camera supports time shift cache stream on the Network Camera. Select one stream and check the below option **Enable time shift caching stream**.

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. Please note that the preset locations will be cleared after flip/mirror.

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

Enable time shift caching stream Advanced Mode : Check this item to enable the time shift cache stream on the Network Camera, which will stores video in the camera's embedded memory for a period of time depending on the cache memory of each Network Camera. This function can work seamlessly with VIVOTEK's recording software. When an event occurs, the recording software can request time shift cache stream from the camera, which allows the user to acquire video data recorded before an event.

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.

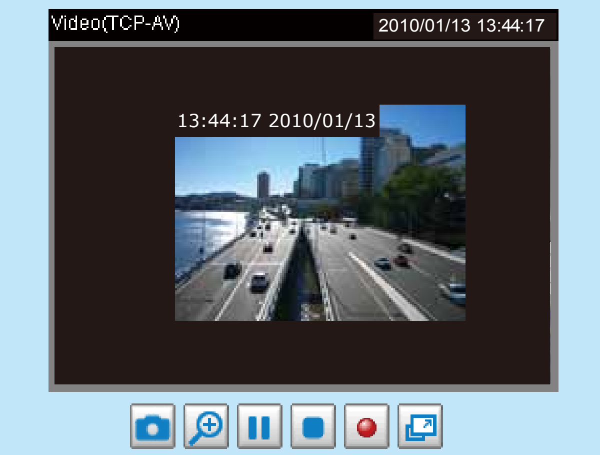
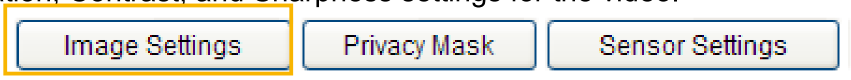
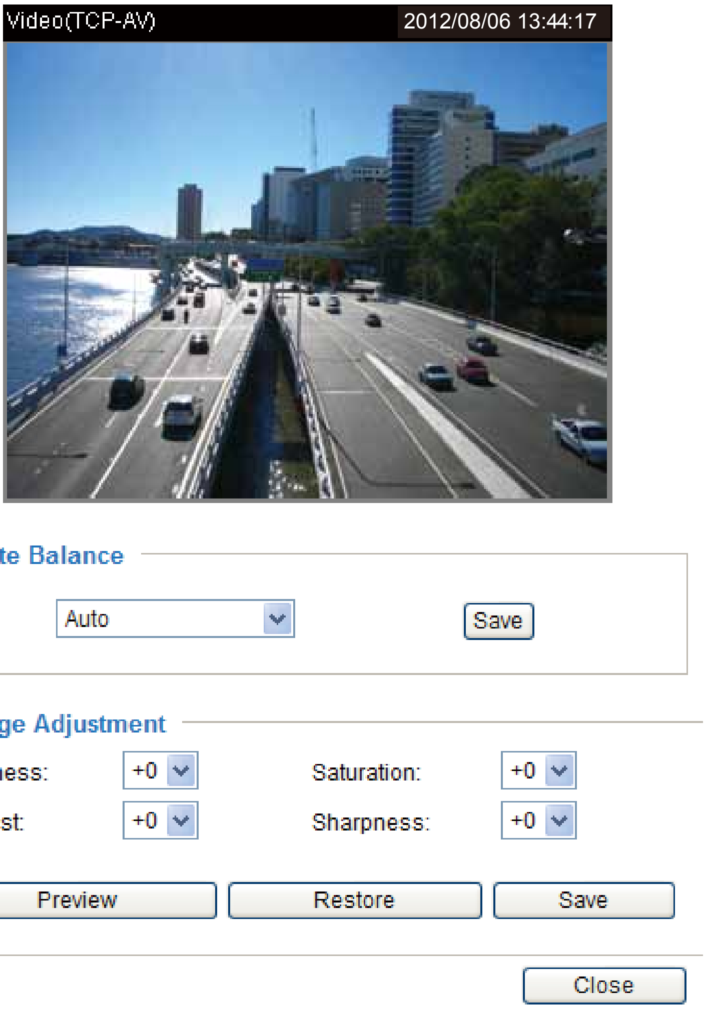


Image Settings Advanced Mode

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: +0

Saturation: +0

Contrast: +0

Sharpness: +0

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

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

■ 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 new setting.

Image Adjustment

■ Brightness: Adjust the image brightness level, which ranges from -5 to +5.

■ Saturation: Adjust the image saturation level, which ranges from -5 to +5.

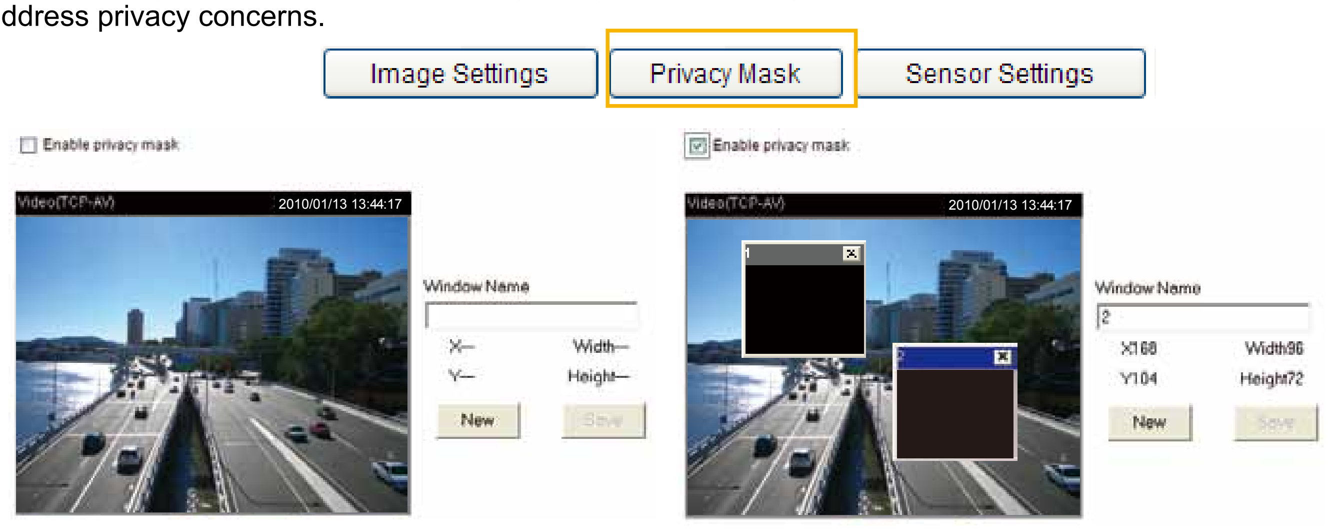
■ Contrast: Adjust the image contrast level, which ranges from -5 to +5.

■ Sharpness: Adjust the image sharpness level, which ranges from -3 to +3.

You can click **Preview** to fine-tune the image, or click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the setting and click **Close** to exit the page.

Privacy Mask Advanced Mode

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



☐ Enable privacy mask

Window Name

X— Width—

Y— Height—

☑ Enable privacy mask

Window Name 2

X168 Width96

Y104 Height72

■ 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.

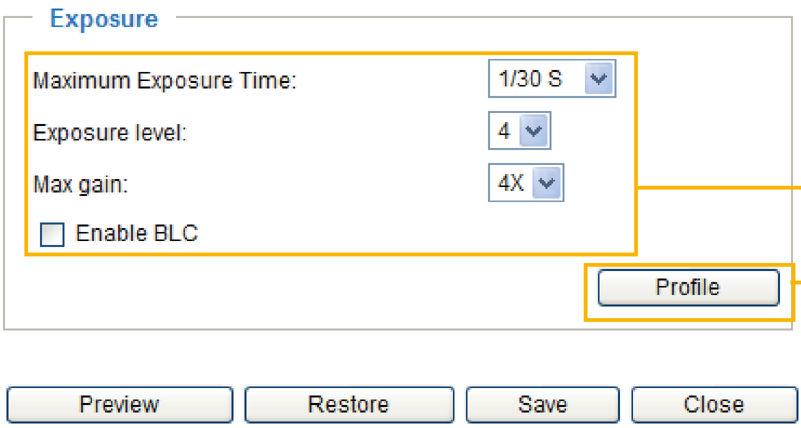
NOTE:

► *Up to 5 privacy mask windows can be configured on the same screen.*

► *If you want to delete the privacy mask window, please click the 'x' mark on the upper right-hand corner of the window.*

Sensor Settings Advanced Mode

Click **Sensor Settings** to open the Sensor Settings page. On this page, you can set the maximum exposure time, exposure level, and AGC (Auto Gain Control) settings. You can configure two sets of sensor settings: one for normal situations, the other for special situations, such as day/night/schedule mode.



Exposure

Maximum Exposure Time: 1/30 S

Exposure level: 4

Max gain: 4X

□ Enable BLC

Sensor Setting 1:
For normal situations

Sensor Setting 2:
For special situations

Exposure

■ Maximum Exposure Time: Select a proper maximum exposure time according to the light source of the surroundings. Shorter exposure times result in less light. The exposure times are selectable for the following durations:
1/480 second, 1/240 second, 1/120 second, 1/60 second, 1/30 second, 1/15 second, and 1/5 second. If you want to set up 60 fps, please select 1/60 second.

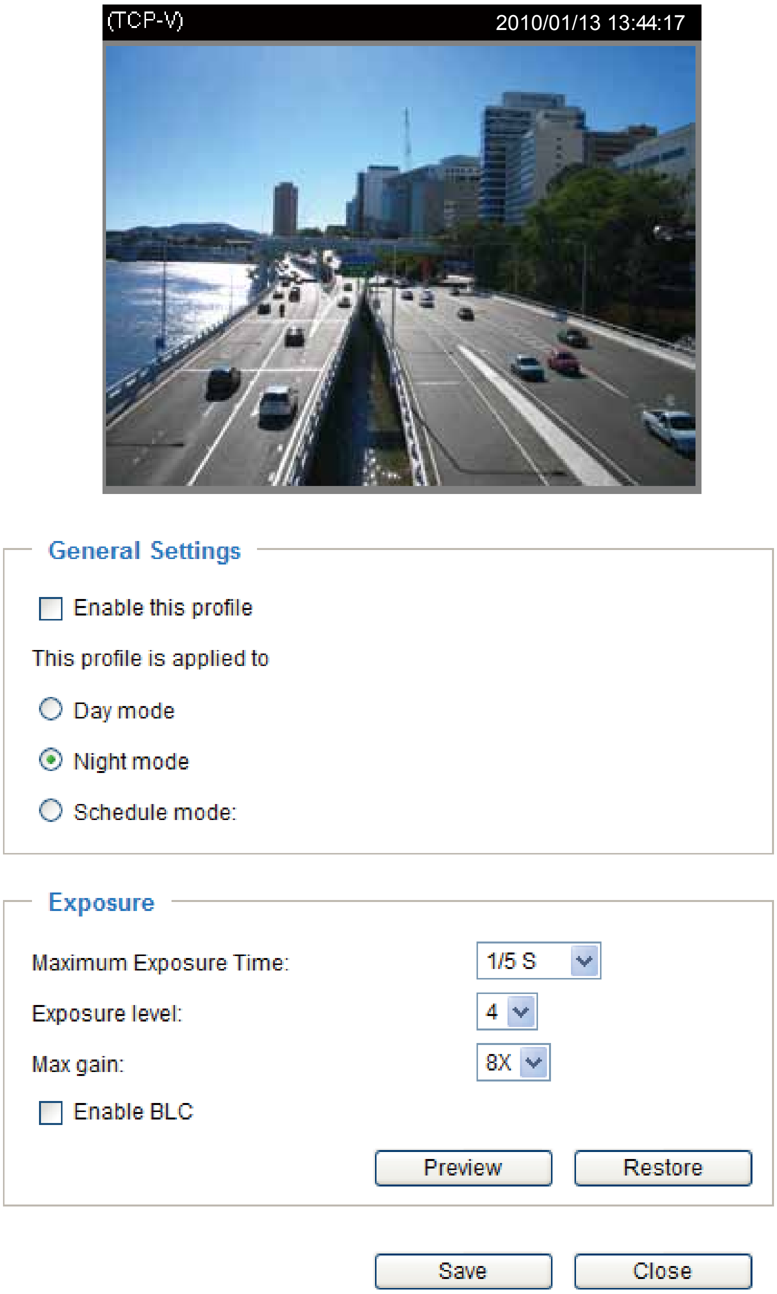
■ Exposure level: You can manually set the Exposure level, which ranges from 1 to 8 (dark to bright).The default value is 4.

■ Max gain (Auto Gain Control): You can manually set the AGC level (2X, 4X, or 8X). The default value is 4X.

■ Enable BLC (Back Light Compensation): Enable this option when the object is too dark or too bright to recognize. It allows the camera to adjust to the best light conditions in any environment and automatically give the necessary light compensation.

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.

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



General Settings

□ Enable this profile

This profile is applied to

○ Day mode

● Night mode

○ Schedule mode:

Exposure

Maximum Exposure Time: 1/5 S

Exposure level: 4

Max gain: 8X

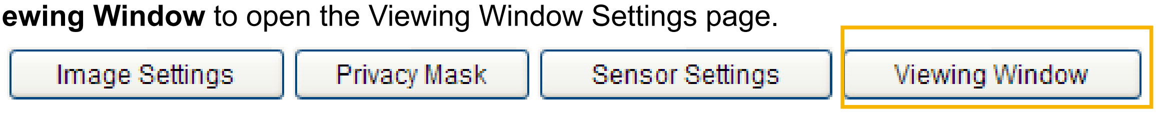
□ Enable BLC

Please follow the steps beolw to setup a profile:

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

Viewing Window Advanced Mode

Click **Viewing Window** to open the Viewing Window Settings page.



The IP8332 supports multiple streams with frame size ranging from 176 x 144 to 1280 x 800.

The definition of multiple streams:

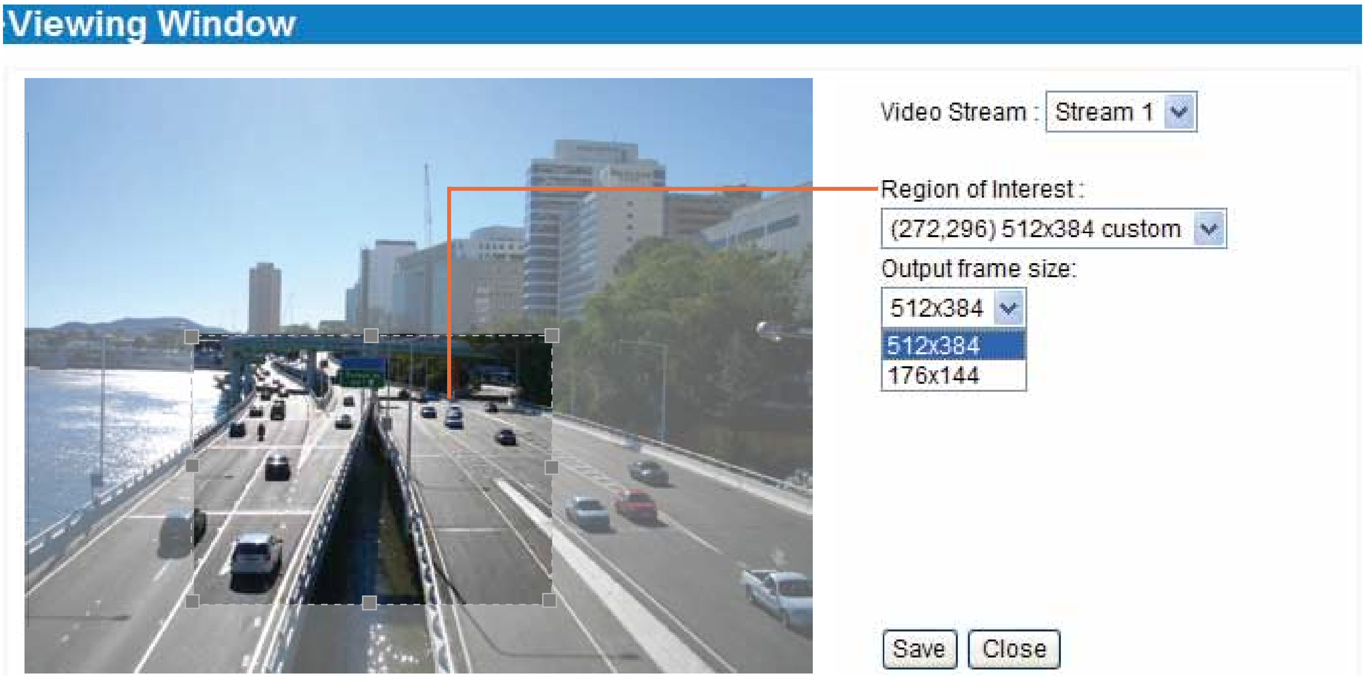
- ■ Stream 1: Users can define the "Region of Interest" (viewing region) and the "Output Frame Rate" (size of the live view window).

- ■ Stream 2: Users can define the "Region of Interest" (viewing region) and the "Output Frame Rate" (size of the live view window).

- ■ Stream 3: Users can define the "Region of Interest" (viewing region) and the "Output Frame Rate" (size of the live view window).

- ■ Stream 4 (Global view stream): This stream captures the full view of the video and users can also define the "Output Frame Rate" (size of the live view window).

Click **Viewing Window** to open the viewing region settings page. On this page, you can set the **Region of Interest** and the **Output Frame Size** for streams 1 ~ 3.



Video Stream : Stream 1

Region of Interest : (272,296) 512x384 custom

Output frame size: 512x384

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

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

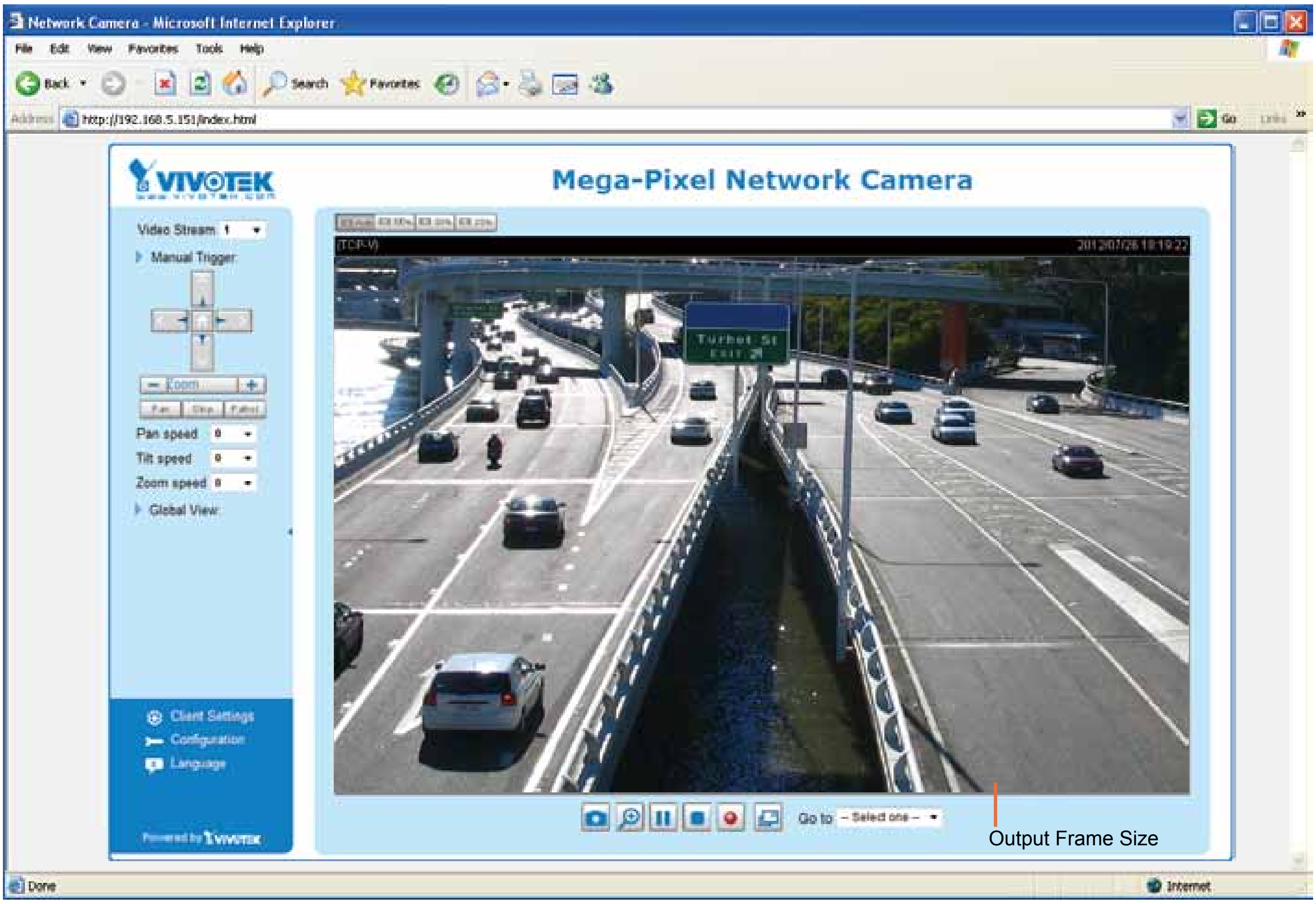
NOTE:

► *All the items in the “Region of Interest” should not be greater than the “Output Frame Size“ (current maximum resolution).*

■ The parameters of the multiple streams:

	Region of Interest	Output frame size
Stream 1	1280 X 800 ~ 176 x 144 (Selectable)	1280 X 800 ~ 176 x 144 (Selectable)
Stream 2	1280 X 800 ~ 176 x 144 (Selectable)	1280 X 800 ~ 176 x 144 (Selectable)
Stream 3	1280 X 800 ~ 176 x 144 (Selectable)	1280 X 800 ~ 176 x 144 (Selectable)
Stream 4	1280 X 800 (Fixed)	1280 X 800 ~ 176 x 144 (Selectable)

When completed with the settings in the Viewing Window, click **Save** to enable the settings and click **Close** to exit the window. The selected **Output Frame Size** will immediately be applied to the **Frame size** of video stream. Then you can go back to the home page to test the settings.

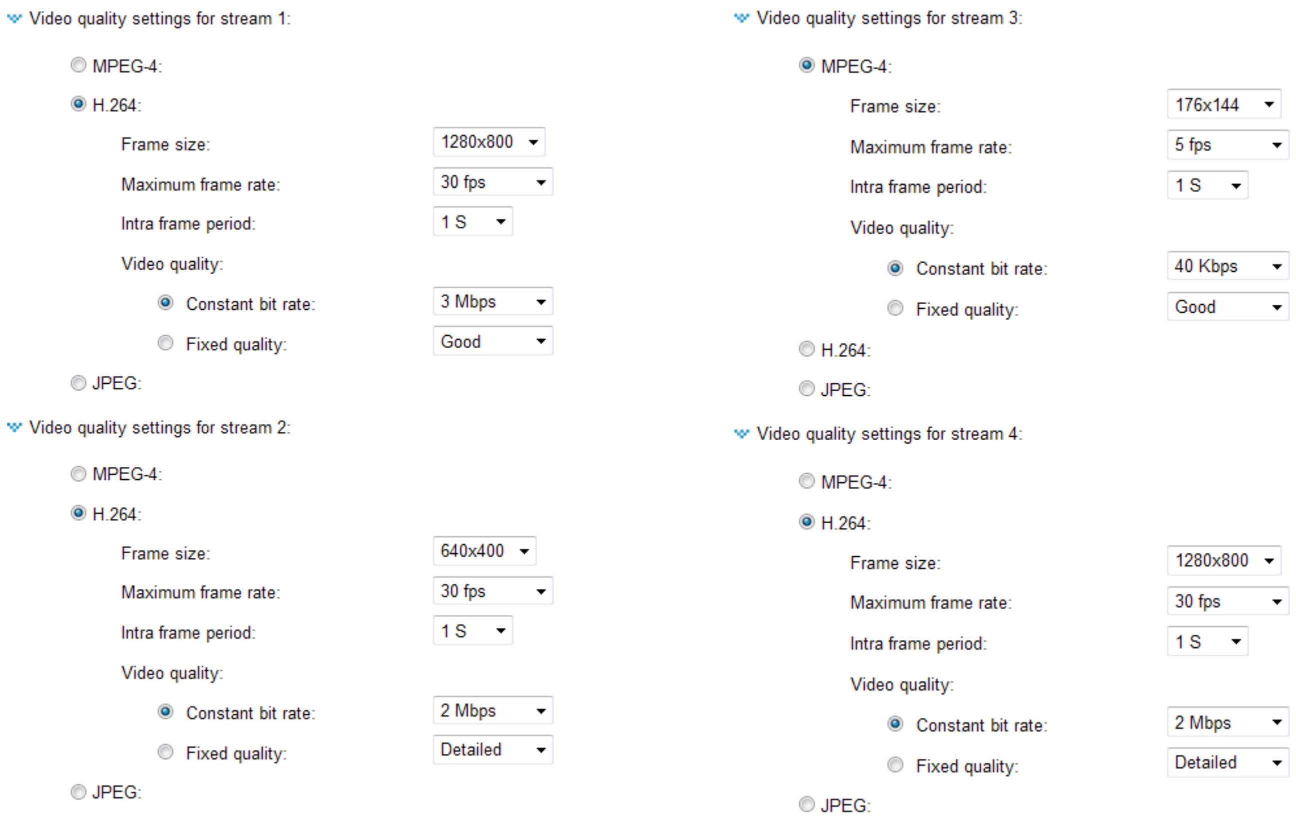


Video Quality Settings Advanced Mode

Click the stream item to display the detailed information. This Network Camera offers real-time H.264, MPEG-4 and MJEPG compression standards (Triple Codec) for real-time viewing.

The IP8332-C supports multiple streams with frame size ranging from 176 x 144 to 1280 x 800.

The maximum frame size will follow your settings in the above Viewing Window sections.



Video quality settings for stream 1:

○ MPEG-4:

● H.264:

Frame size:	1280x800
Maximum frame rate:	30 fps
Intra frame period:	1 S
Video quality:	
● Constant bit rate:	3 Mbps
○ Fixed quality:	Good

○ JPEG:

Video quality settings for stream 2:

○ MPEG-4:

● H.264:

Frame size:	640x400
Maximum frame rate:	30 fps
Intra frame period:	1 S
Video quality:	
● Constant bit rate:	2 Mbps
○ Fixed quality:	Detailed

○ JPEG:

Video quality settings for stream 3:

● MPEG-4:

Frame size:	176x144
Maximum frame rate:	5 fps
Intra frame period:	1 S
Video quality:	
● Constant bit rate:	40 Kbps
○ Fixed quality:	Good

○ H.264:

○ JPEG:

Video quality settings for stream 4:

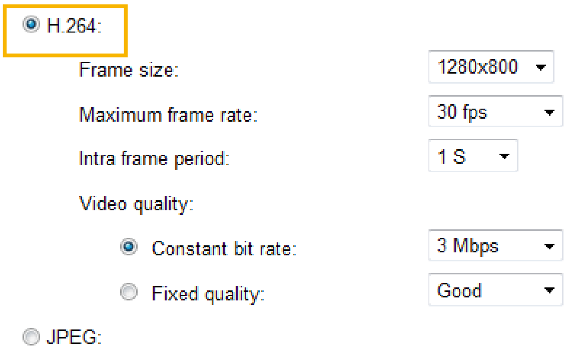
○ MPEG-4:

● H.264:

Frame size:	1280x800
Maximum frame rate:	30 fps
Intra frame period:	1 S
Video quality:	
● Constant bit rate:	2 Mbps
○ Fixed quality:	Detailed

○ JPEG:

If **H.264 / MPEG-4** mode is selected, the video is streamed via RTSP protocol. There are four parameters for you to adjust the video performance:



● H.264:

Frame size:	1280x800
Maximum frame rate:	30 fps
Intra frame period:	1 S
Video quality:	
● Constant bit rate:	3 Mbps
○ Fixed quality:	Good

○ JPEG:

■ Frame size

You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate

This places a limitation on the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.

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

■ Intra frame period

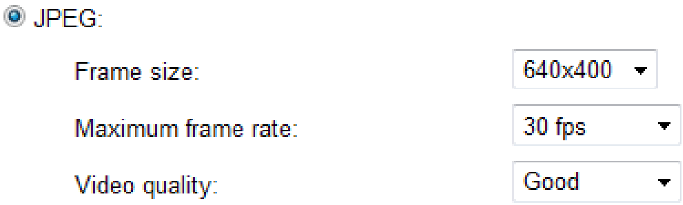
Determine how often to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

■ Video quality

A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. Therefore, if **Constant bit rate** is selected, the bandwidth utilization is fixed at a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 1.5Mbps, 2Mbps, 3Mbps, 4Mbps, 6Mbps, and 8Mbps. You can also select **Customize** and manually enter a value.

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

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:



● JPEG:

Frame size:	640x400
Maximum frame rate:	30 fps
Video quality:	Good

■ Frame size

You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate

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

■ Video quality

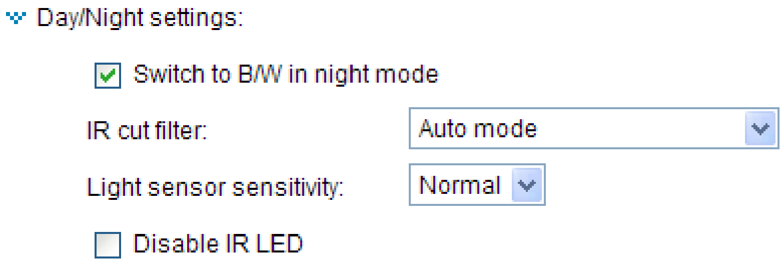
The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

NOTE:

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

► *Converting high-quality video may significantly increase the CPU loading, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the above does occur, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

Day/Night Settings



Day/Night settings:

☑ Switch to B/W in night mode

IR cut filter: Auto mode

Light sensor sensitivity: Normal

□ Disable IR LED

Switch to B/W in night mode
Select this to enable the Network Camera to automatically switch to B/W during night mode.

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

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

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

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

■ Synchronize with digital input
The Network Camera automatically removes the IR cut filter when DI triggers. When the camera is installed with external IR lights, you may let the digital input from the external devices determine when to turn the IR cut filter on or off.

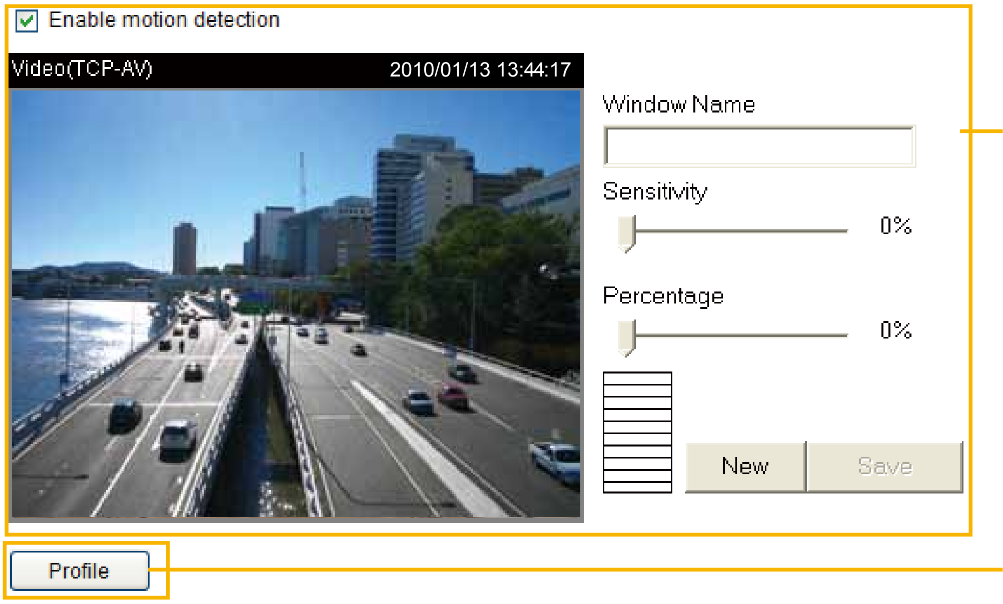
■ Schedule mode
The Network Camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and end time of day mode are set to 07:00 and 18:00.

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

Disable IR LED
If you do not want to use the IR illuminators, you can select this option to turn it off.

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.



☑ Enable motion detection

Video(TCP-AV) 2010/01/13 13:44:17

Window Name

Sensitivity 0%

Percentage 0%

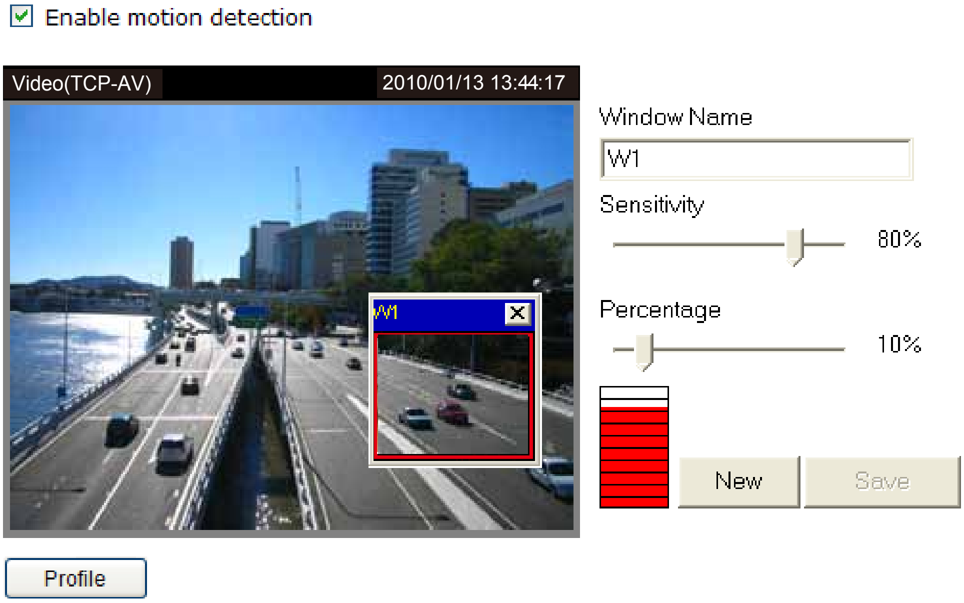
Motion Detection Setting 1:
For normal situations

Motion Detection Setting 2:
For special situations

Follow the steps below to enable motion detection:

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



☑ Enable motion detection

Video(TCP-AV) 2010/01/13 13:44:17

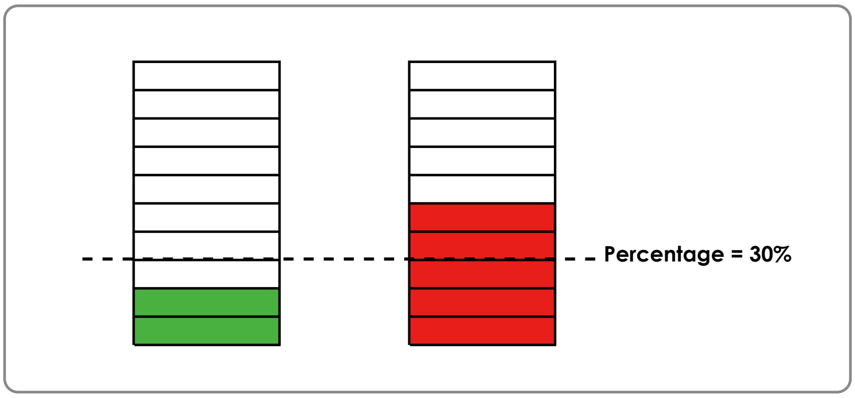
Window Name: W1

Sensitivity 80%

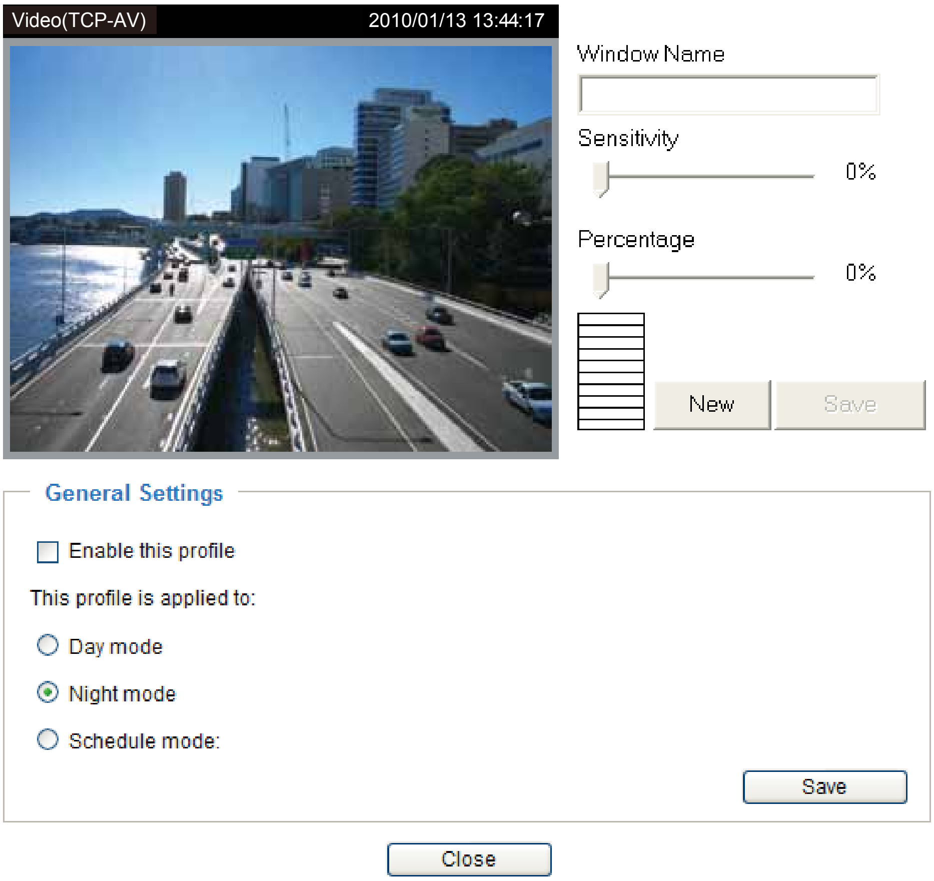
Percentage 10%

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 76.

A green bar indicates that even though motions have been detected, the event has not been triggered because the image variations still fall under the defined threshold.



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


Video(TCP-AV) 2010/01/13 13:44:17

Window Name

Sensitivity 0%

Percentage 0%

General Settings

□ Enable this profile

This profile is applied to:

○ Day mode

● Night mode

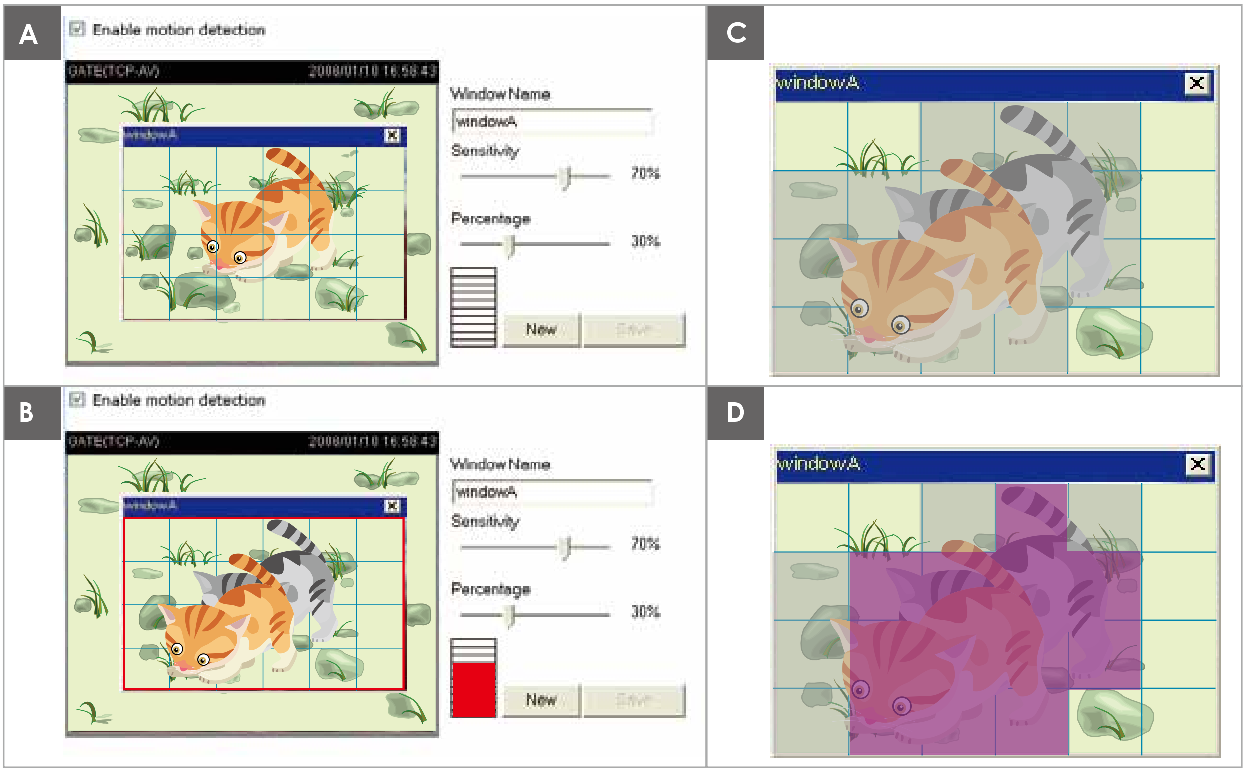
○ Schedule mode:

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

This motion detection window will also be displayed on the Event Settings page. You can go to Application > Event Settings > Trigger to choose it as a trigger source. Please refer to page 78 for detailed information.

NOTE:

► *How does motion detection work?*



☑ Enable motion detection

Window Name: windowA

Sensitivity 70%

Percentage 30%

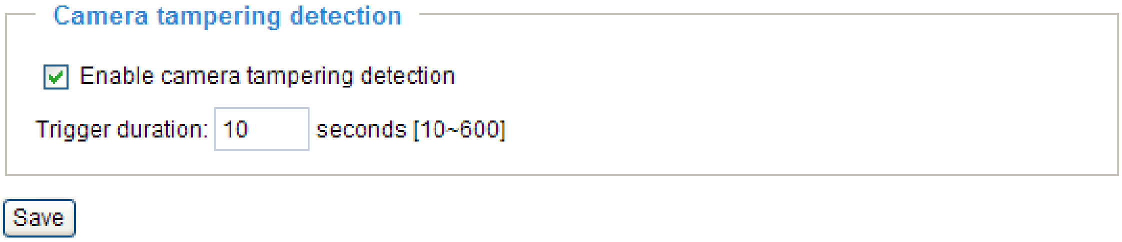
There are two motion detection parameters: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity is a 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 tamper 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: 10 seconds [10~600]

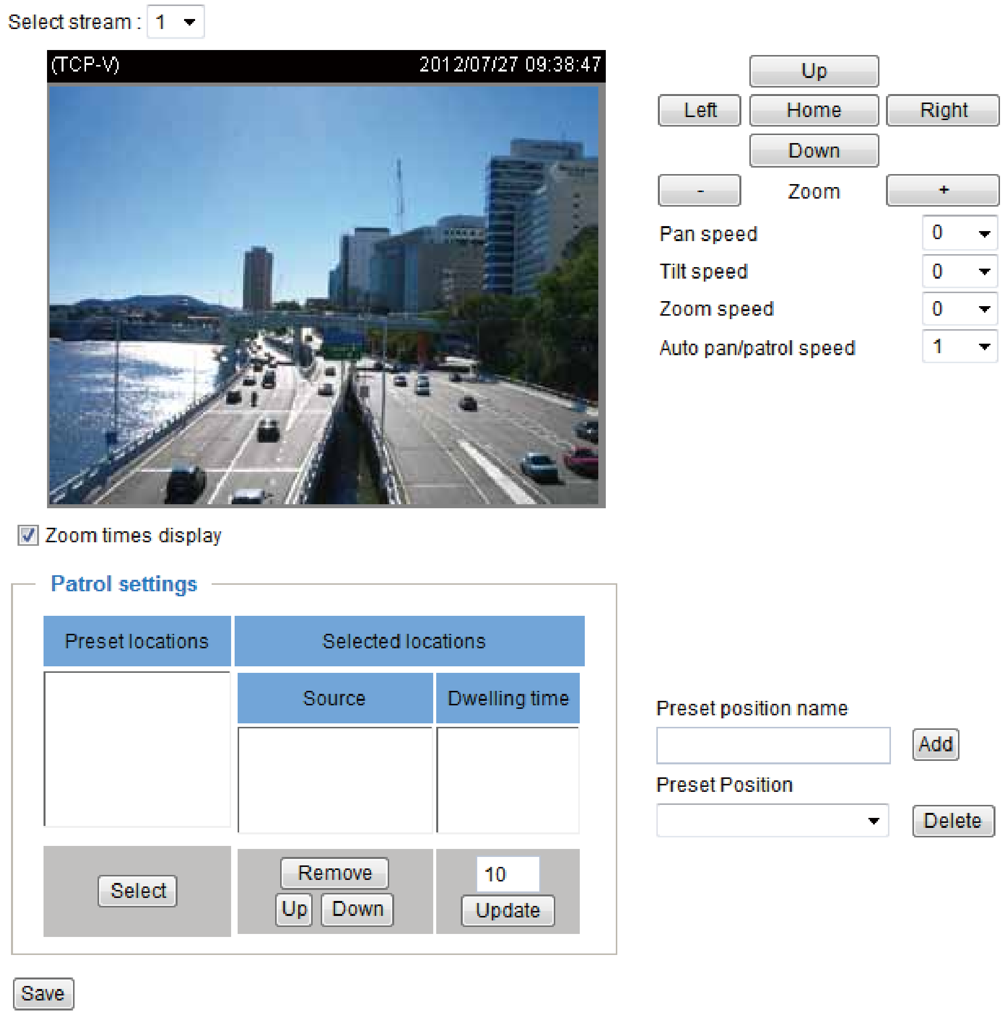
Please follow the steps below to set up the camera tamper detection function:

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 78 for detailed information.

Camera Control

This section explains how to control the Network Camera’s Pan/Tilt/Zoom operation. The Camera Control works **only when** a streaming view **is not** showing the full of the camera’s largest frame size. For example, when showing a 640x400 frame out of the 1280x800 maximum size frame.

The onscreen control allows users to quickly move the focus to a pre-configured target area for close-up viewing without physically zooming the camera.



Select stream : 1

(TCP-V) 2012/07/27 09:38:47

Pan speed 0

Tilt speed 0

Zoom speed 0

Auto pan/patrol speed 1

☑ Zoom times display

Patrol settings

Preset locations	Selected locations	
	Source	Dwelling time
Select	Remove Up Down	10 Update

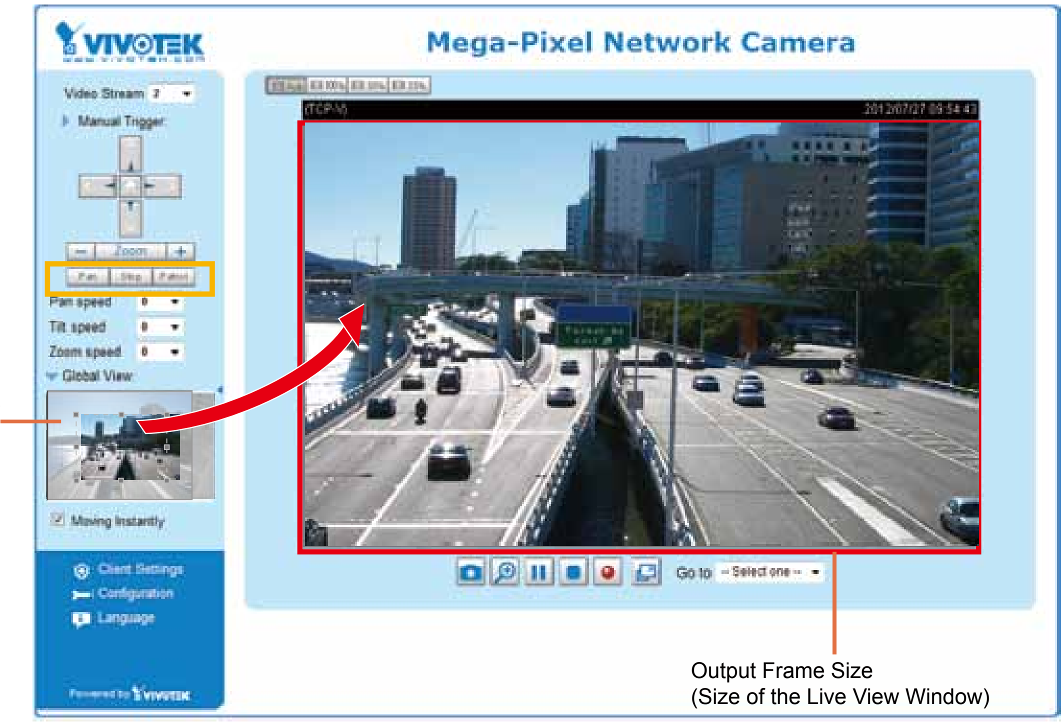
Preset position name

Preset Position

Select stream: You can only apply e-PTZ control on stream #1. Refer to the following page for details about how to set up preset and patrol settings.

Auto pan/patrol speed: Select the speed from 1~5 (from slow to fast) to set up the Auto pan/patrol speed control. When completed with the settings of e-PTZ, click **Save** to enable the settings on this page.

Camera Control on the Home page



Video Stream 2

Pan speed 0

Tilt speed 0

Zoom speed 0

☑ Moving Instantly

Region of Interest
(Viewing Region)

Output Frame Size
(Size of the Live View Window)

■ The Preset Positions will also be displayed on the home page. Select one from the drop-down list, and the Network Camera will move to the selected e-preset position.

■ If you have set up different preset positions for stream #1, you can select another video stream to display its different preset positions.

Global View

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

Moving Instantly

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

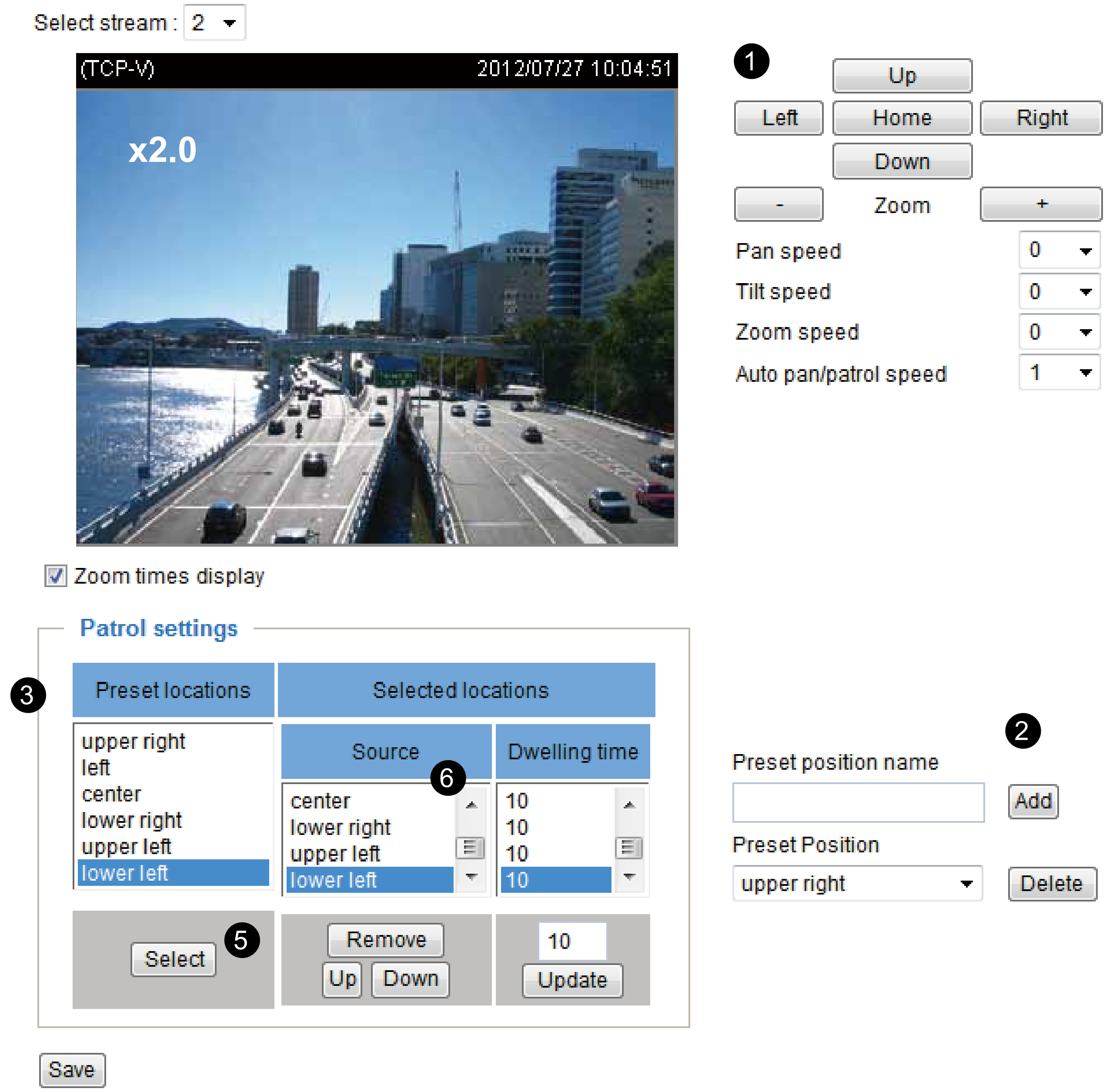
Click on Image

The Camera Control function also supports “Click on Image“. When you click on any point of the Global View Window or Live View Window, the viewing region will also move to that point.

Patrol settings

You can select some preset positions for the Network Camera to patrol.
Please follow the steps below to set up a patrol schedule:

1. Use mouse clicks on the screen or the PTZ panel to move the current view to a desired position.
2. Enter a name as the Preset position name, and then click the Add button.
3. The position you created will be listed in the Preset locations column.
4. Repeat the above process by moving to different positions and mark those positions as Preset positions.
5. Select a location each by a mouse click and click the Select button.
6. Selection locations will be listed in the Selected locations column.
7. You may then use the Up or Down button to change the patrolling order, or change the dwelling time for the camera's field of view to stay on a specific location.
8. When done with all configuration details, click on the Save button.



Select stream : 2

(TCP-V) 2012/07/27 10:04:51

x2.0

☑ Zoom times display

Pan speed 0

Tilt speed 0

Zoom speed 0

Auto pan/patrol speed 1

Patrol settings

Preset locations	Selected locations	
	Source	Dwelling time
upper right left center lower right upper left lower left	center lower right upper left lower left	10 10 10 10

Preset position name

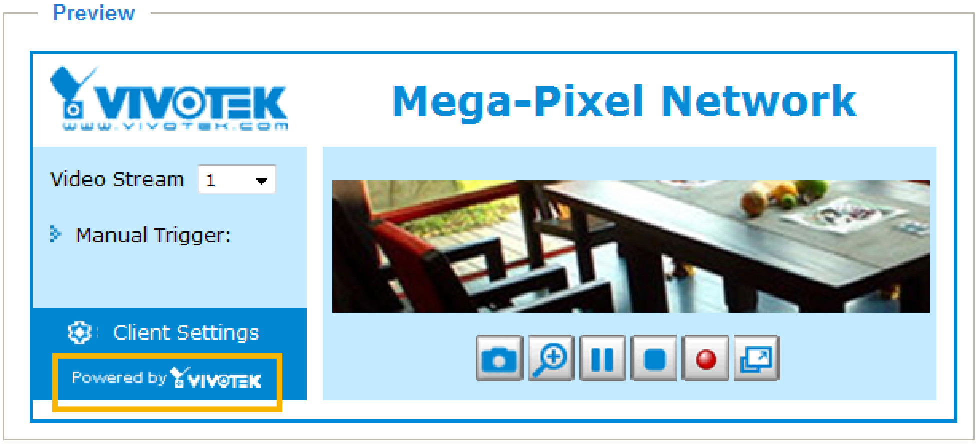
Preset Position: upper right

Homepage Layout Advanced Mode

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

Preview

This column shows the settings of your hompage 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:

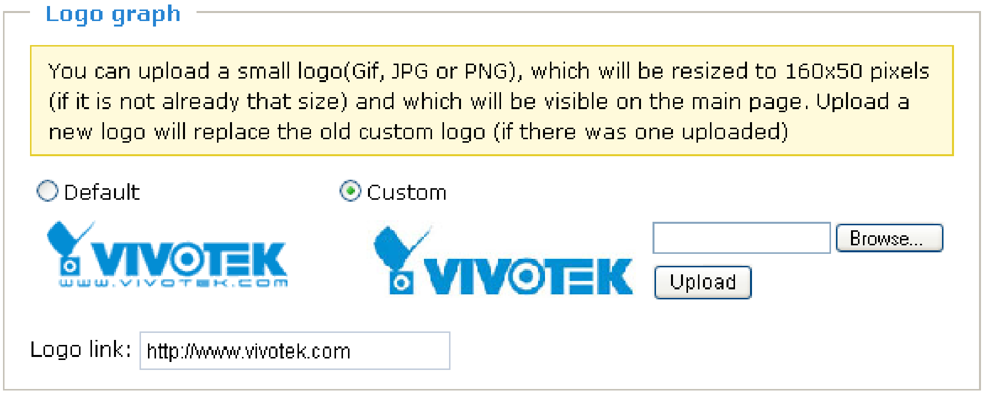


□ Hide Powered by VIVOTEK

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

Logo

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



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)

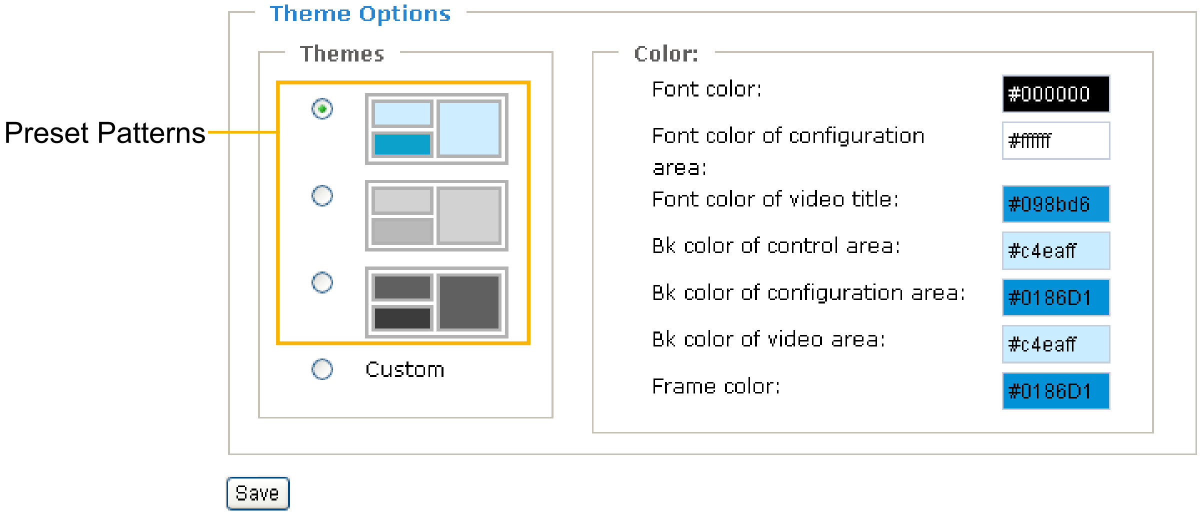
○ Default ● Custom

Logo link: http://www.vivotek.com

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

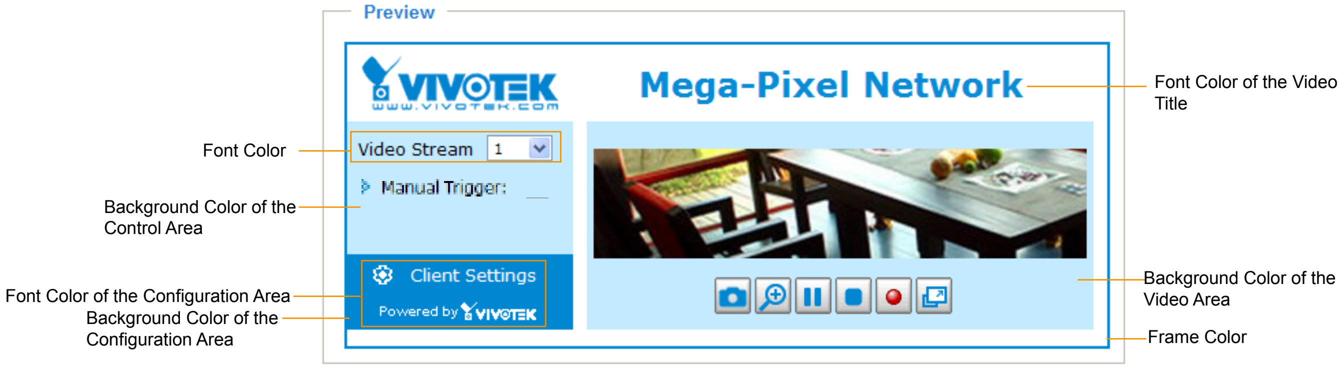
Themes

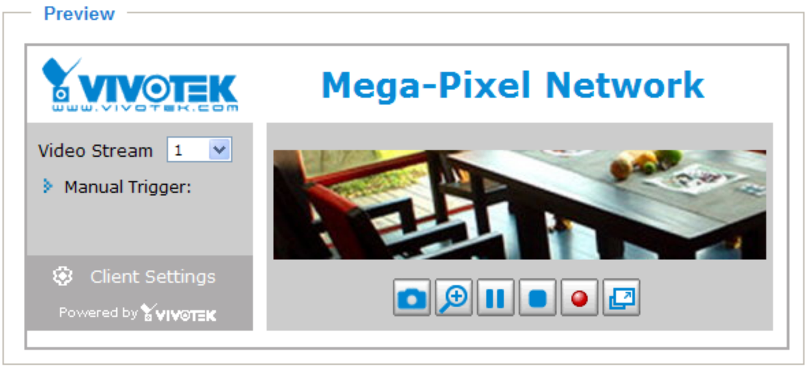
●
○
○
○ Custom

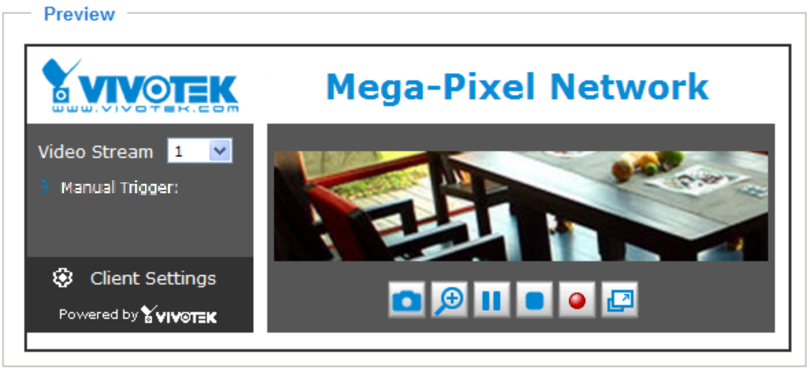
Color:

Font color:	#000000
Font color of configuration area:	#ffffff
Font color of video title:	#098bd6
Bk color of control area:	#c4eaff
Bk color of configuration area:	#0186D1
Bk color of video area:	#c4eaff
Frame color:	#0186D1

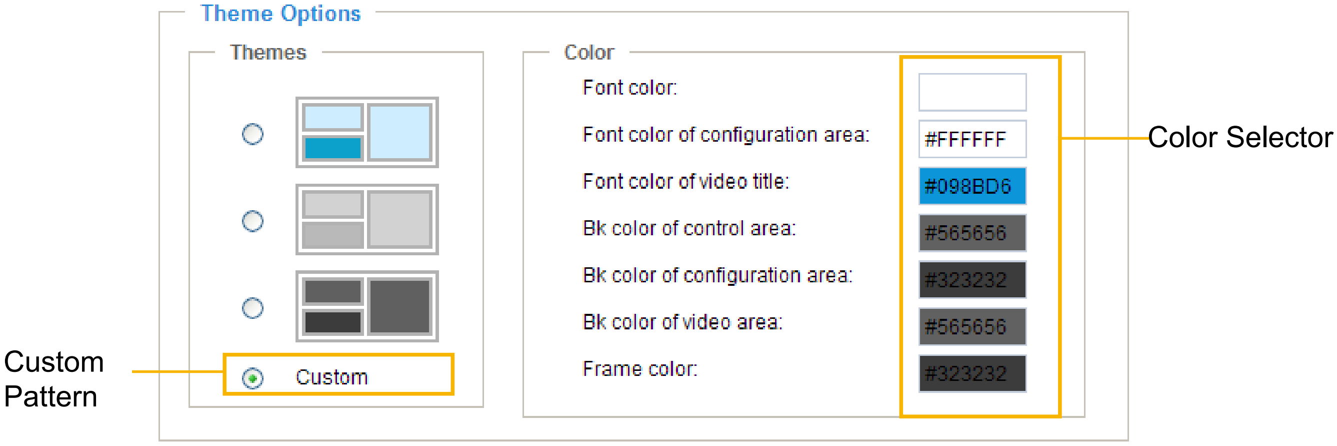
Save


Preview
VIVOTEK
www.vivotek.com
Mega-Pixel Network
Video Stream 1
Manual Trigger:
Client Settings
Powered by VIVOTEK
Font Color of the Video Title
Font Color
Background Color of the Control Area
Font Color of the Configuration Area
Background Color of the Configuration Area
Background Color of the Video Area
Frame Color





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



Theme Options

Themes

○

○

○

● Custom

Color

Font color:

Font color of configuration area: #FFFFFF

Font color of video title: #098BD6

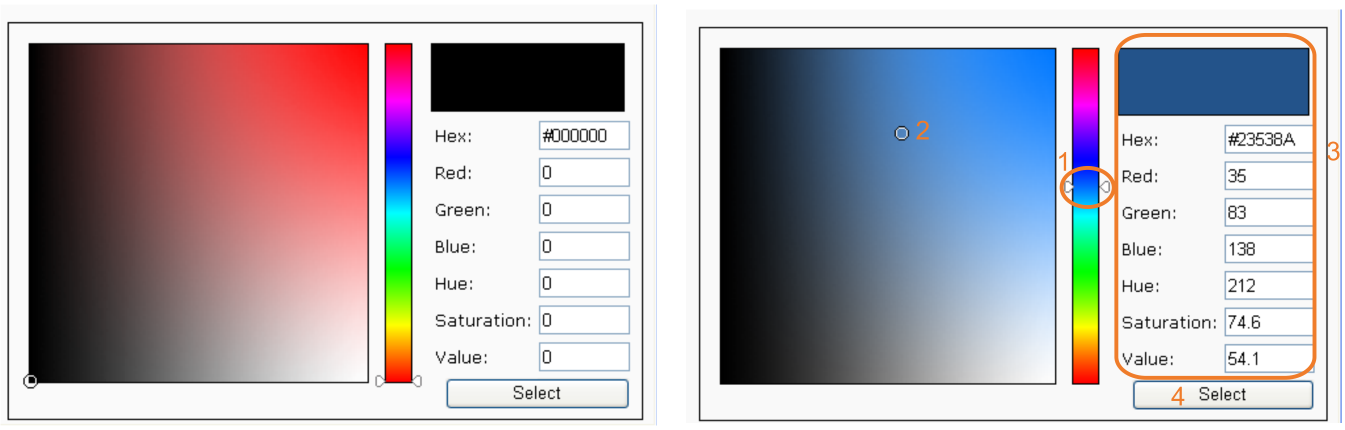
Bk color of control area: #565656

Bk color of configuration area: #323232

Bk color of video area: #565656

Frame color: #323232

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



Hex: #000000
Red: 0
Green: 0
Blue: 0
Hue: 0
Saturation: 0
Value: 0
Select

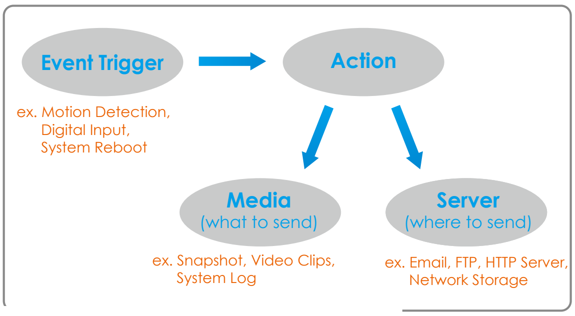
Hex: #23538A
Red: 35
Green: 83
Blue: 138
Hue: 212
Saturation: 74.6
Value: 54.1
Select

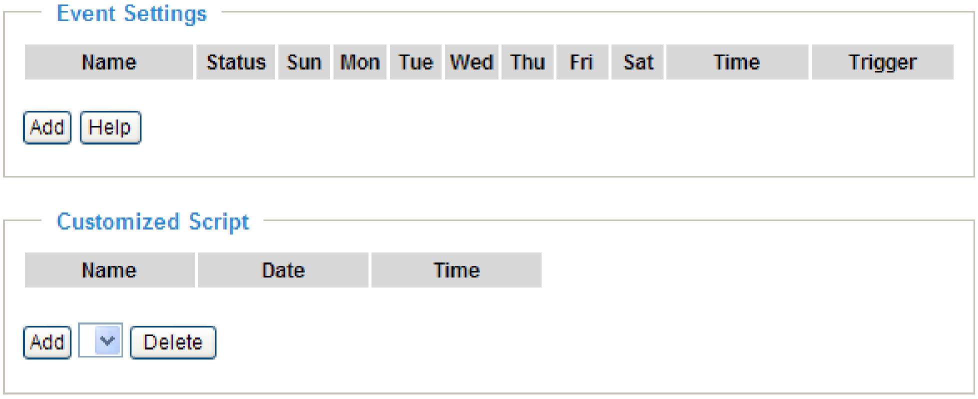
4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

Application Advanced Mode

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

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 will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.




Event Settings

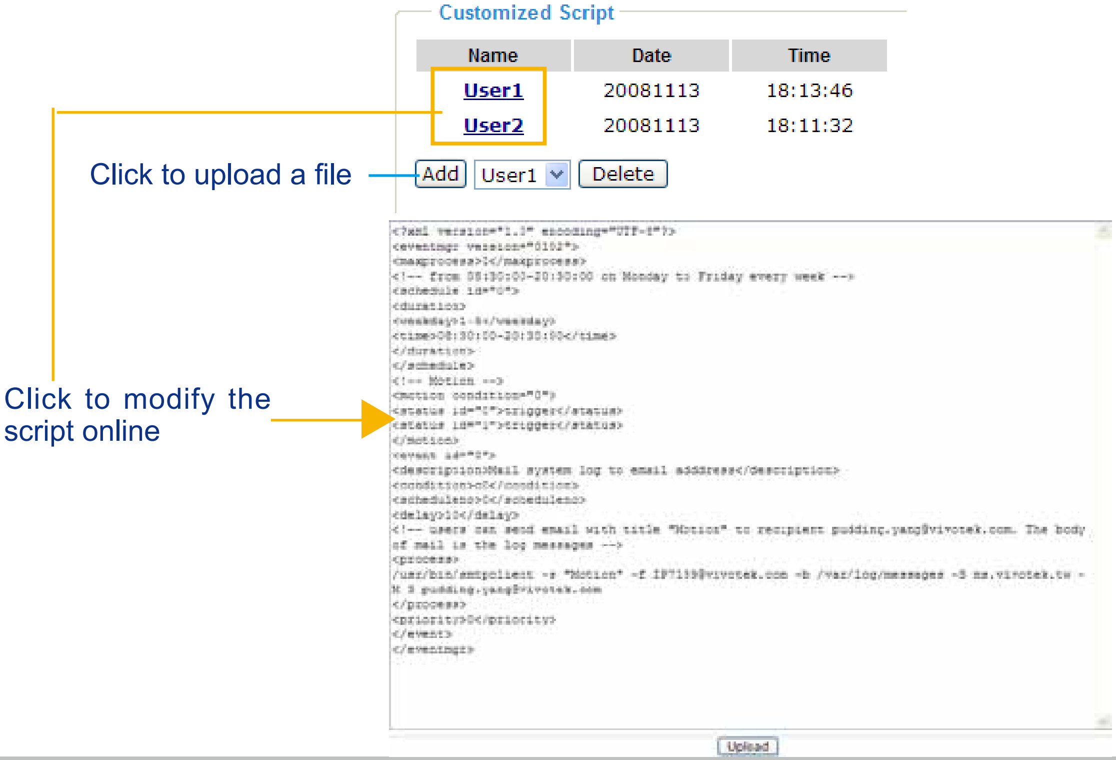
Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger

Customized Script

Name	Date	Time

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.

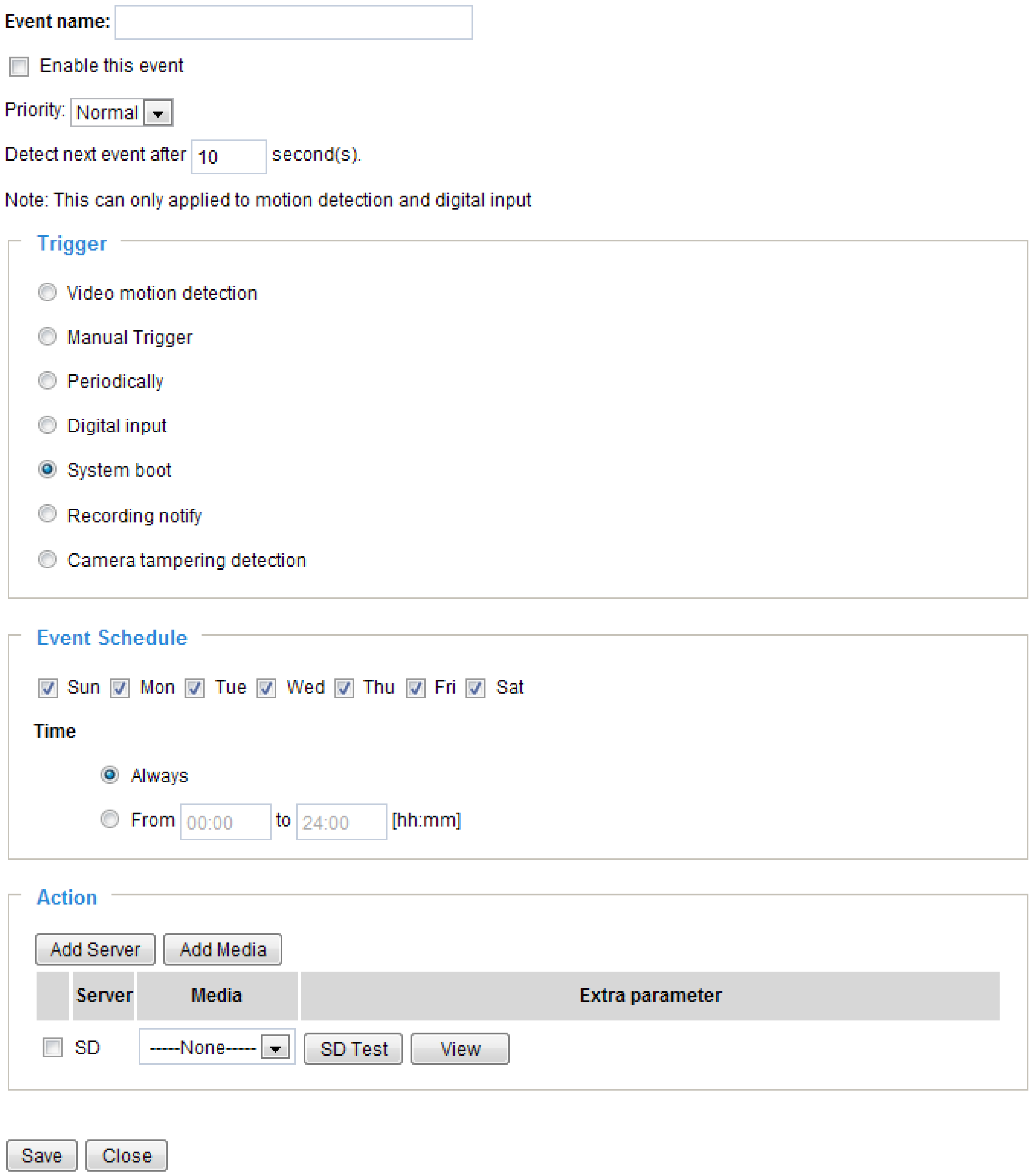

Customized Script

Name	Date	Time
User1	20081113	18:13:46
User2	20081113	18:11:32

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

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: Normal

Detect next event after 10 second(s).

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

Trigger

○ Video motion detection
○ Manual Trigger
○ Periodically
○ Digital input
● System boot
○ Recording notify
○ Camera tampering detection

Event Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always
○ From 00:00 to 24:00 [hh:mm]

Action

Add Server | Add Media

	Server	Media	Extra parameter
□	SD	-----None-----	SD Test View

Save | Close

Event name: Enter a name for the event setting.

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

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

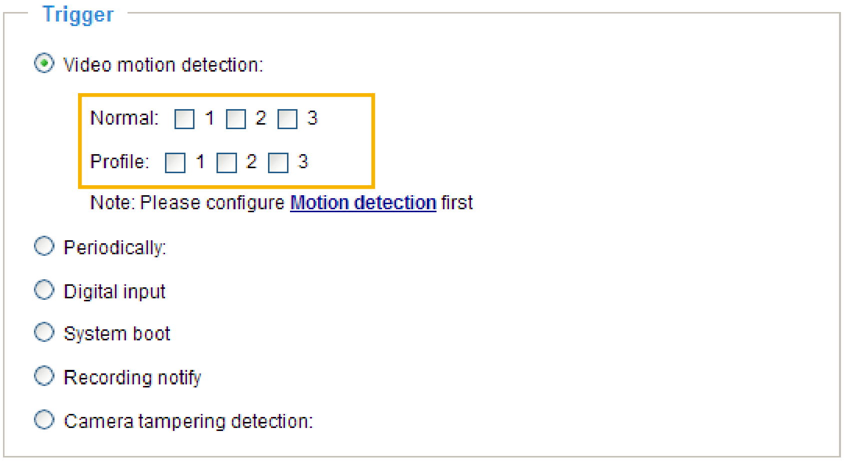
Detect next event after □ seconds: Enter the duration in seconds to pause motion detection after a motion is detected.

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 with 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 66 for details.



Trigger

● Video motion detection:

Normal: □ 1 □ 2 □ 3

Profile: □ 1 □ 2 □ 3

Note: Please configure Motion detection first

○ Periodically:

○ Digital input

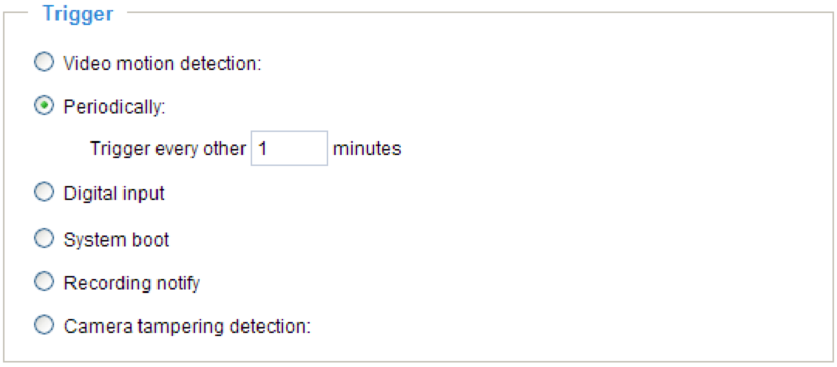
○ System boot

○ Recording notify

○ Camera tampering detection:

■ Manual Trigger
This option allows an event to be manually triggered using the Manual Trigger buttons on the home page.

■ Periodically
This option allows the Network Camera to trigger periodically for every other defined minute. The maximum duration is to 999 minutes.



Trigger

○ Video motion detection:

● Periodically:

Trigger every other 1 minutes

○ Digital input

○ System boot

○ Recording notify

○ Camera tampering detection:

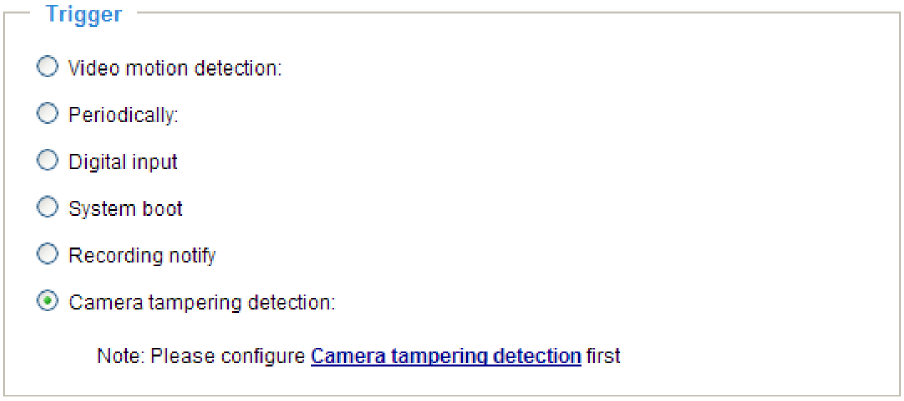
■ Digital input
This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices of digital input devices on the market which helps to detect changes in temperature, vibration, sound, and light, etc.

■ System boot
This option triggers the Network Camera when the power to the Network Camera is disconnected and restored.

■ Recording notify
This option allows the Network Camera to trigger when the recording disk is full or when recording

starts to rewrite older data.

■ Camera tampering detection
This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 69 for detailed information.



Trigger

○ Video motion detection:

○ Periodically:

○ Digital input

○ System boot

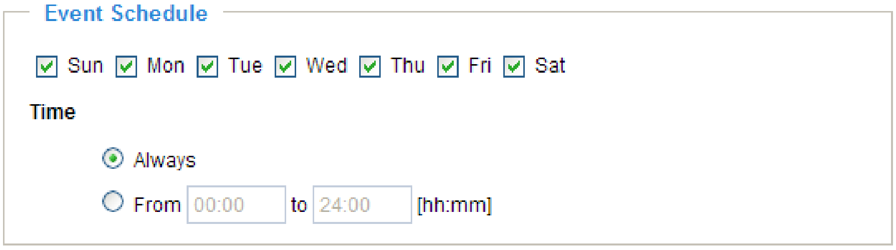
○ Recording notify

● 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

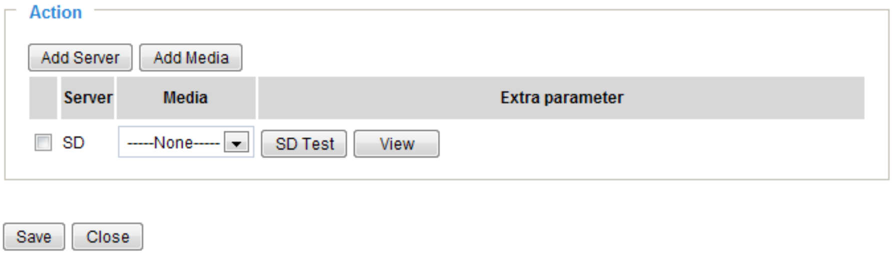
○ From 00:00 to 24:00 [hh:mm]

■ Select the days in a 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.



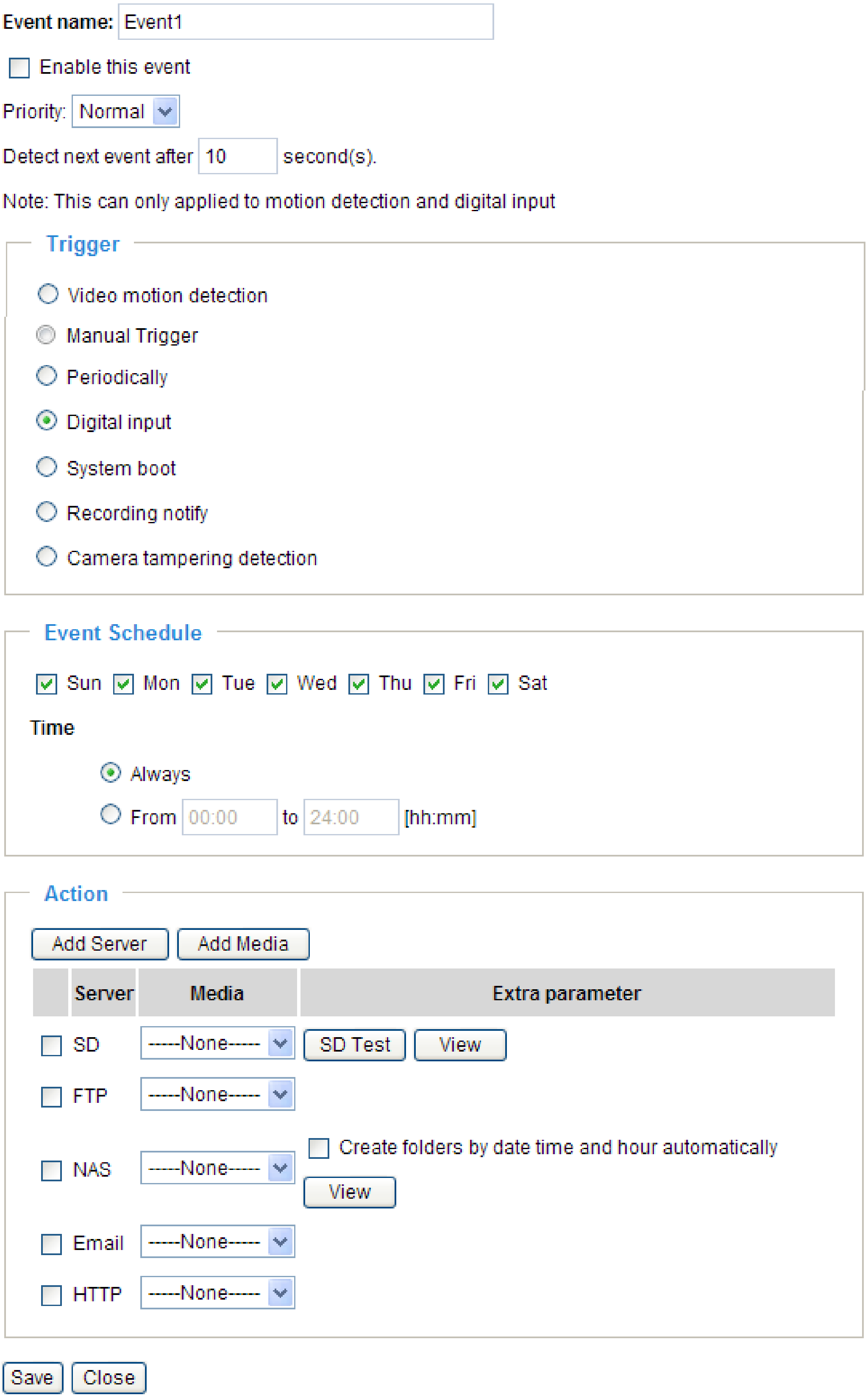
Action

	Server	Media	Extra parameter
□	SD	-----None-----	SD Test View

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 82.
Click **Add Media** to configure Media Settings. For more information, please refer to Media Settings on page 85.

Here is an example of the Event Settings page:



Event name: Event1

□ Enable this event

Priority: Normal

Detect next event after 10 second(s).

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

Trigger

○ Video motion detection

○ Manual Trigger

○ Periodically

● Digital input

○ System boot

○ Recording notify

○ Camera tampering detection

Event Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

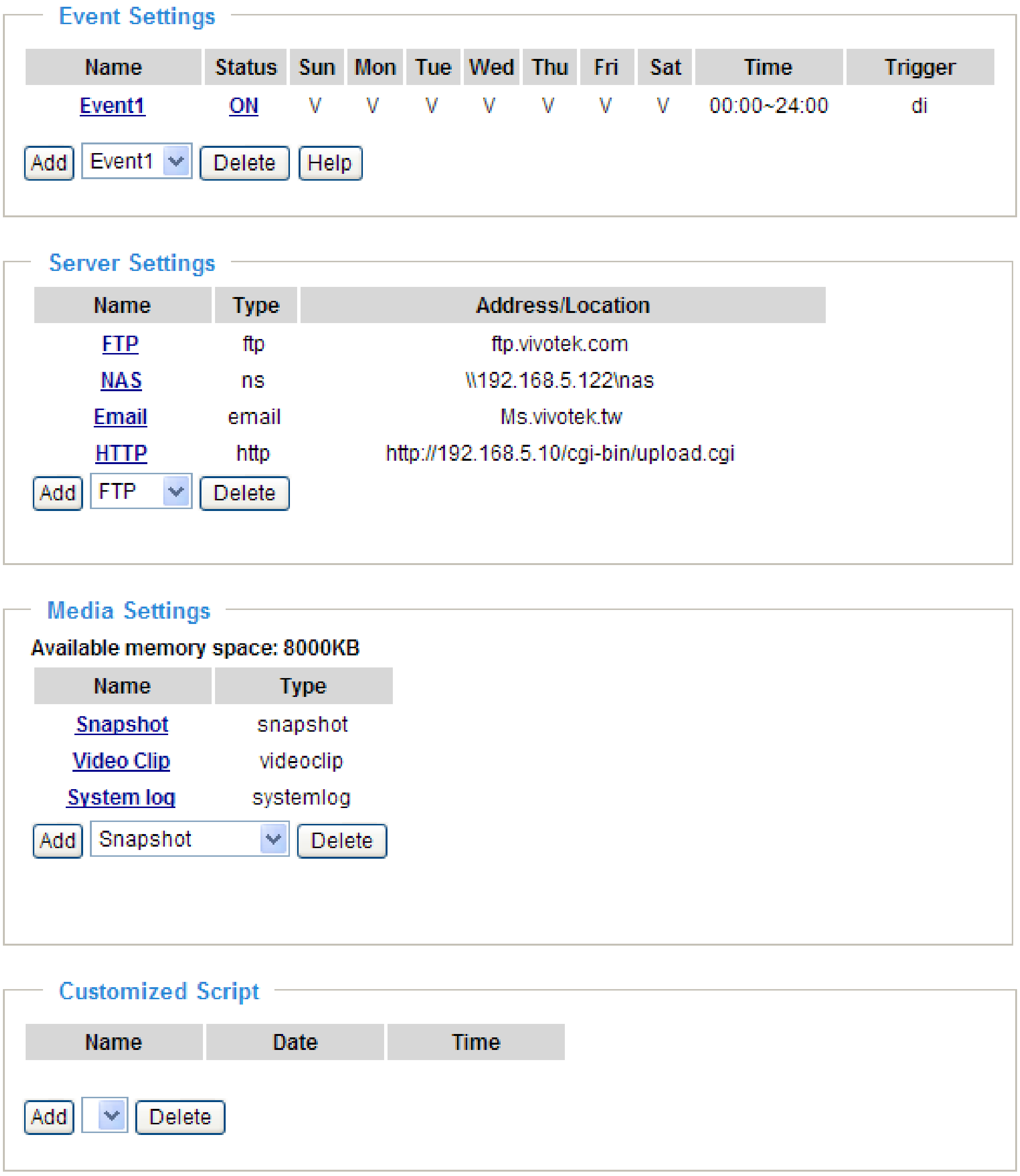
○ From 00:00 to 24:00 [hh:mm]

Action

	Server	Media	Extra parameter
□	SD	-----None-----	SD Test View
□	FTP	-----None-----	
□	NAS	-----None-----	□ Create folders by date time and hour automatically View
□	Email	-----None-----	
□	HTTP	-----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
Event1	ON	V	V	V	V	V	V	V	00:00~24:00	di

Server Settings

Name	Type	Address/Location
FTP	ftp	ftp.vivotek.com
NAS	ns	\\192.168.5.122\nas
Email	email	Ms.vivotek.tw
HTTP	http	http://192.168.5.10/cgi-bin/upload.cgi

Media Settings

Available memory space: 8000KB

Name	Type
Snapshot	snapshot
Video Clip	videoclip
System log	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 you can only delete a server when it is not involed in an event setting.

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

Server Settings

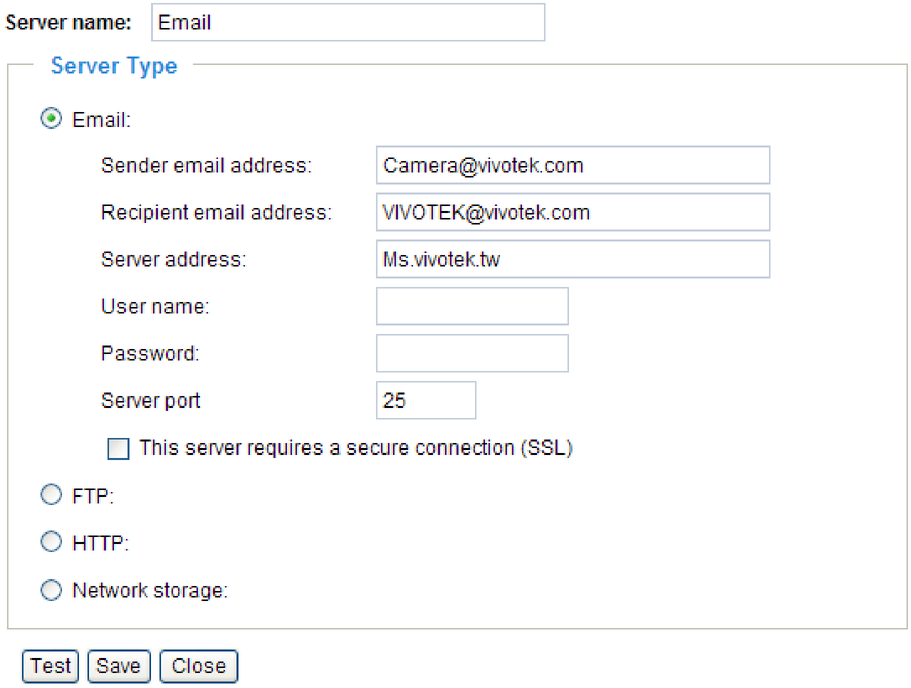
Click **Add Server** on Event Settings page to open the Server Setting page. On this page, you can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

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: Email

Server Type

● Email:

Sender email address: Camera@vivotek.com

Recipient email address: VIVOTEK@vivotek.com

Server address: Ms.vivotek.tw

User name:

Password:

Server port: 25

□ 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.

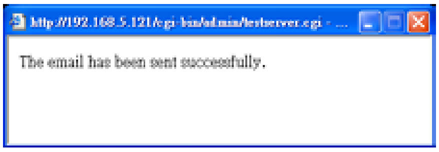
■ User name: Enter the user name of the email account if necessary.

■ 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.

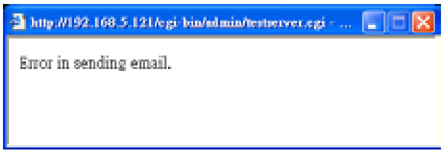
If your SMTP server requires a secure connection (SSL), check **This server requires a secure connection (SSL).**

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.



http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

The email has been sent successfully.

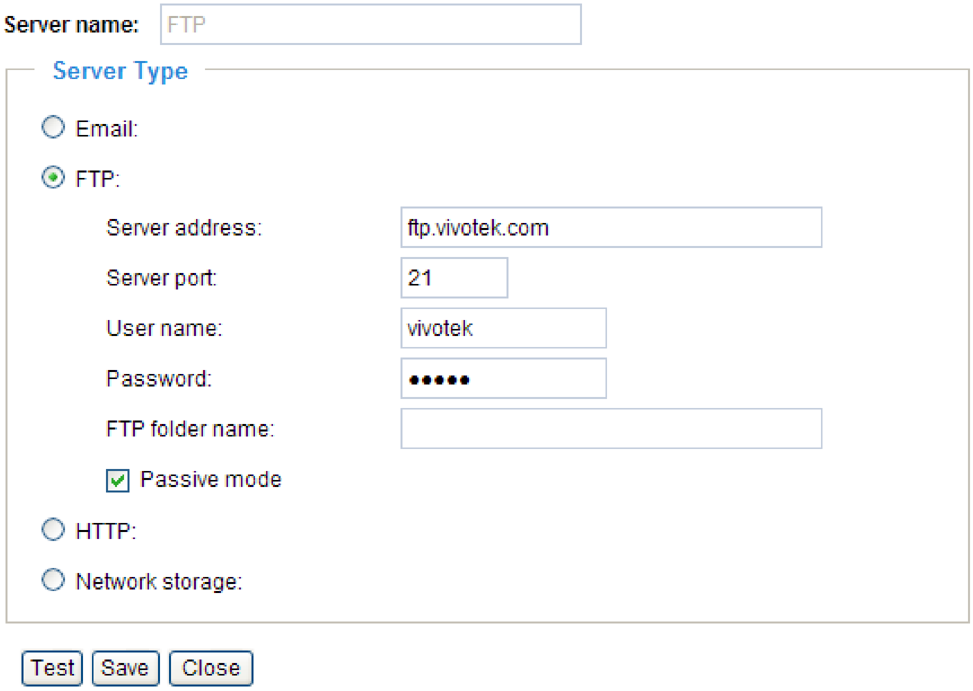


http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

Error in sending email.

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: FTP

Server Type

○ Email:

● FTP:

Server address: ftp.vivotek.com

Server port: 21

User name: vivotek

Password: •••••

FTP folder name:

☑ Passive mode

○ HTTP:

○ Network storage:

■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port:
By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.

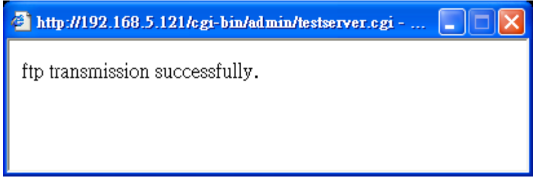
■ User name: Enter the login name of the FTP account.

■ Password: Enter the password of the FTP account.

■ FTP folder name
Enter the folder where the media file will be placed. If the folder name does not exist, the Network Camera will create one on the FTP server.

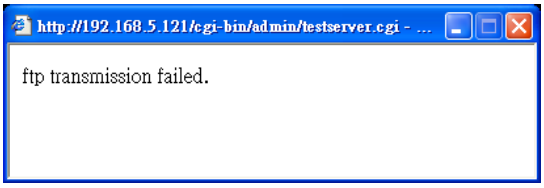
■ Passive mode
Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

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



http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

ftp transmission successfully.

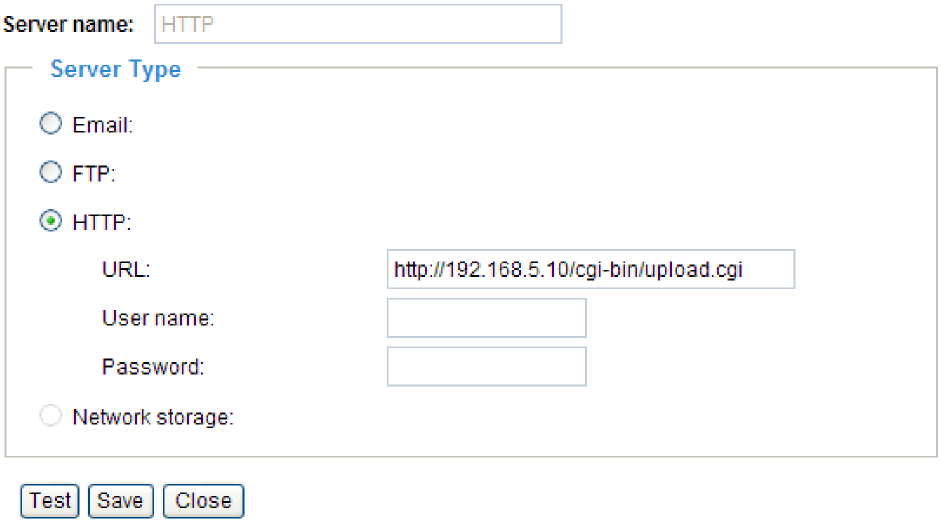


http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

ftp transmission failed.

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: HTTP

Server Type

○ Email:

○ FTP:

● HTTP:

URL: http://192.168.5.10/cgi-bin/upload.cgi

User name:

Password:

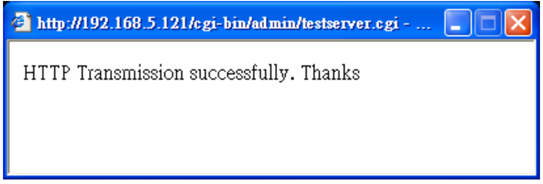
○ Network storage:

■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name if necessary.

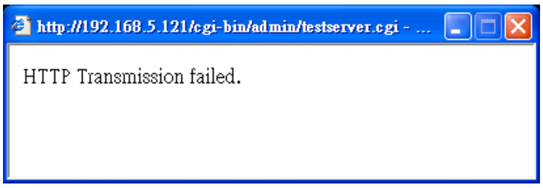
■ Password: Enter the password if necessary.

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.



http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

HTTP Transmission successfully. Thanks



http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

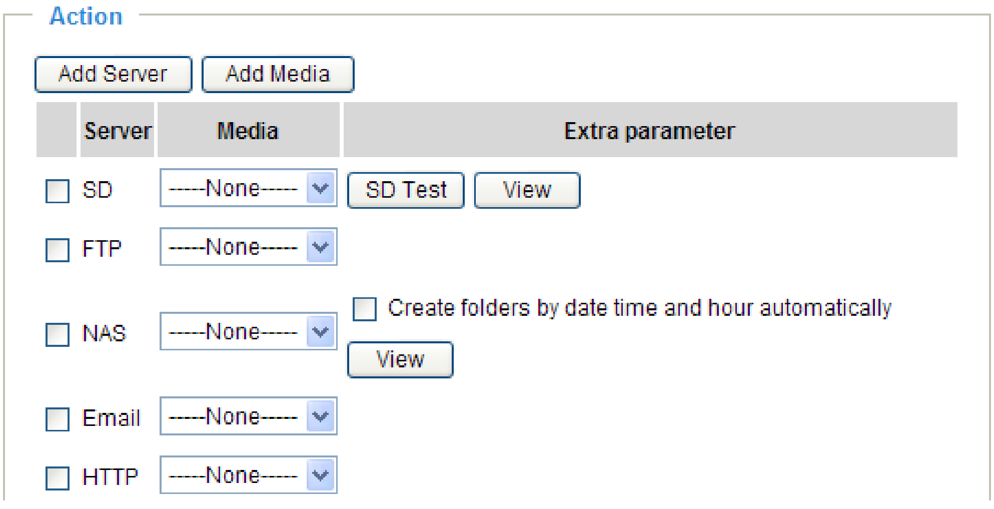
HTTP Transmission failed.

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 89 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:



Action

	Server	Media	Extra parameter
□	SD	-----None-----	SD Test View
□	FTP	-----None-----	
□	NAS	-----None-----	□ Create folders by date time and hour automatically View
□	Email	-----None-----	
□	HTTP	-----None-----	

Media Settings

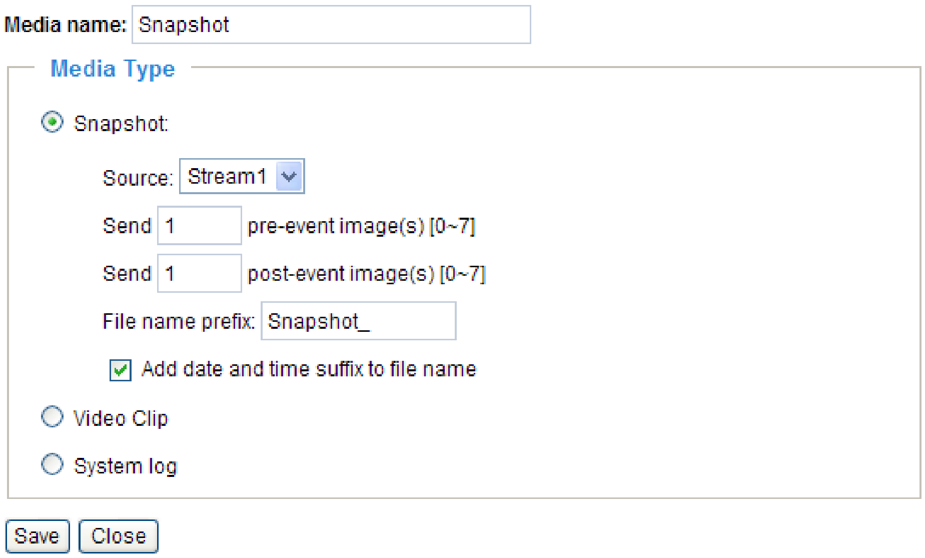
Click **Add Media** on the Event Settings page to open the Media Settings page. On this page, you can specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be configured.

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: Snapshot

Media Type

● Snapshot:

Source: Stream1

Send 1 pre-event image(s) [0~7]

Send 1 post-event image(s) [0~7]

File name prefix: Snapshot_

☑ Add date and time suffix to file name

○ Video Clip

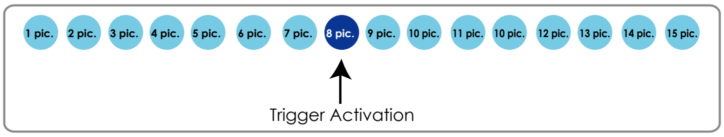
○ System log

■ Source: Select to take snapshots from stream 1 ~ 4.

■ 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.

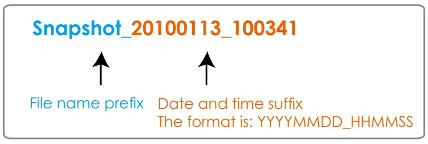
■ Send □ post-event images
Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

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.



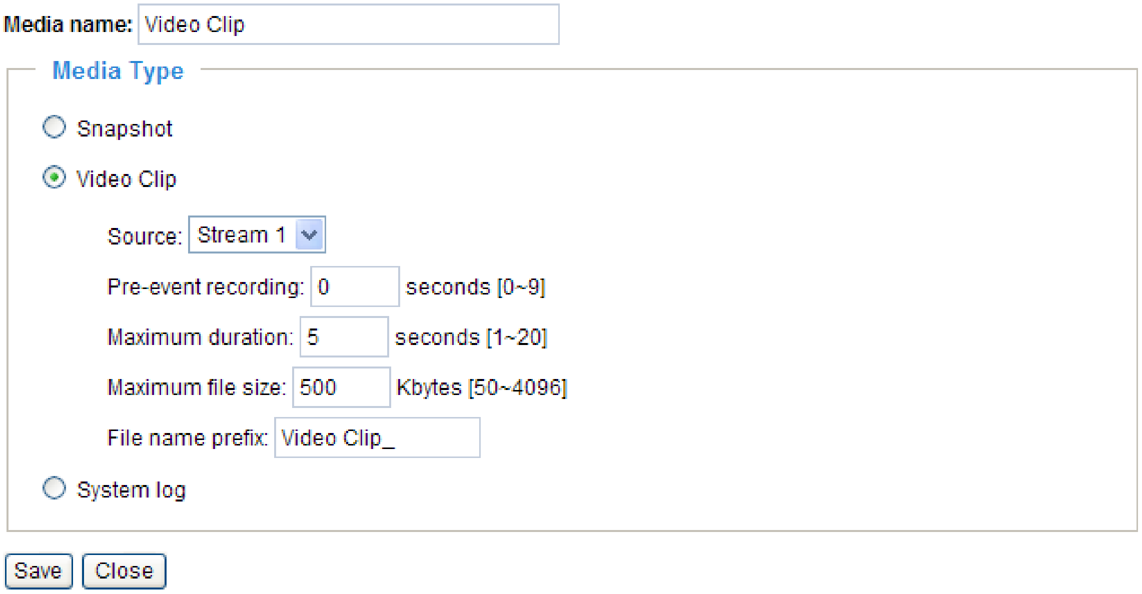
■ File name prefix
Enter the text that will be appended to the front of the file name.

■ 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: Video Clip

Media Type

○ Snapshot

● Video Clip

Source: Stream 1

Pre-event recording: 0 seconds [0~9]

Maximum duration: 5 seconds [1~20]

Maximum file size: 500 Kbytes [50~4096]

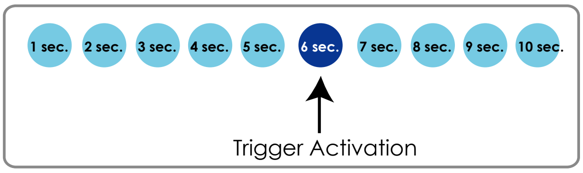
File name prefix: Video Clip_

○ System log

■ Source: Select a source of video clip.

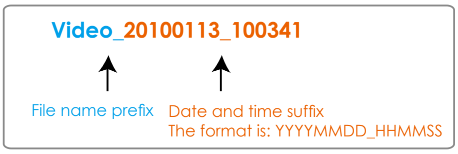
■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

■ Maximum duration
Specify the maximum recording duration in seconds. Up to 10 seconds can be set.
For example, if pre-event recording is set to five seconds and the maximum duration is set to ten seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.



■ Maximum file size
Specify the maximum file size allowed.

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

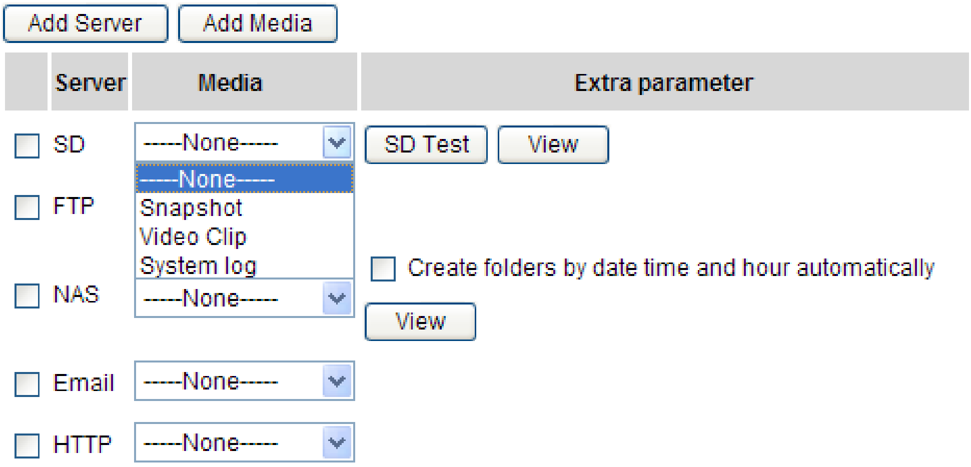


Click **Save** to enable the settings, then click **Close** to exit the page.

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

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

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



■ SD Test: Click to test your SD card. The system will display a message indicating success or failure. If you want to use your SD card for on board storage, please format it before use. Please refer to page 89 for detailed information.

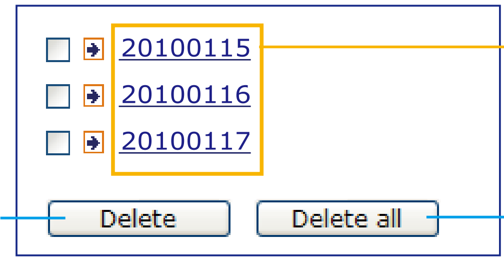
■ Create folders by date, time, and hour automatically: If you check this item, the system will generate folders automatically by date.

■ View: Click this button to open a file list window. This function is only for **SD card** and **Network Storage**.

If you click **View** button of SD card, a **Local storage** page will prompt for you to manage recorded files on SD card. For more information about Local storage, please refer to page 93 for illustration.

If you click **View** button of Network storage, a **file directory window** will pop up for you to view recorded data on Network storage. For detailed illustration, please refer to the next page.

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



□ 20100115
□ 20100116
□ 20100117

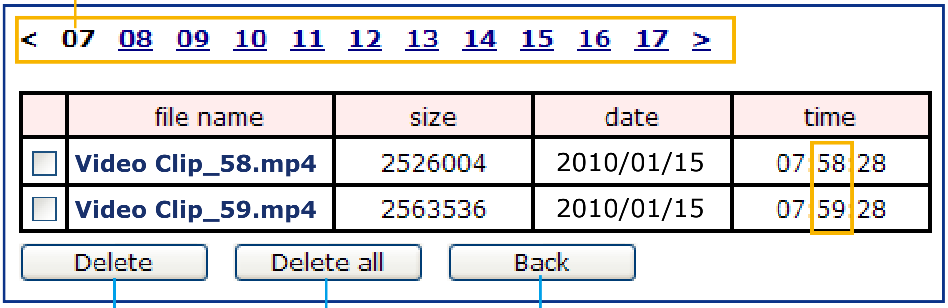
The format is: YYYYMMDD
Click to open the directory

Click to delete selected items

Click to delete all recorded data

Click **20100115** to open the directory:

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



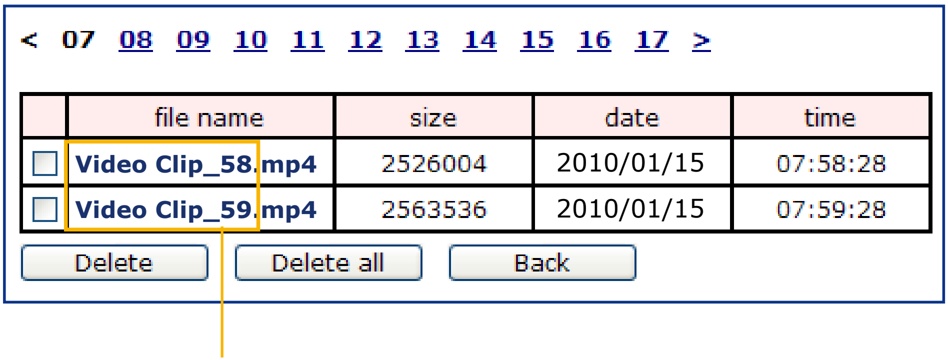
< 07 08 09 10 11 12 13 14 15 16 17 >

	file name	size	date	time
□	**Video Clip_58.mp4**	2526004	2010/01/15	07:58:28
□	**Video Clip_59.mp4**	2563536	2010/01/15	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 >

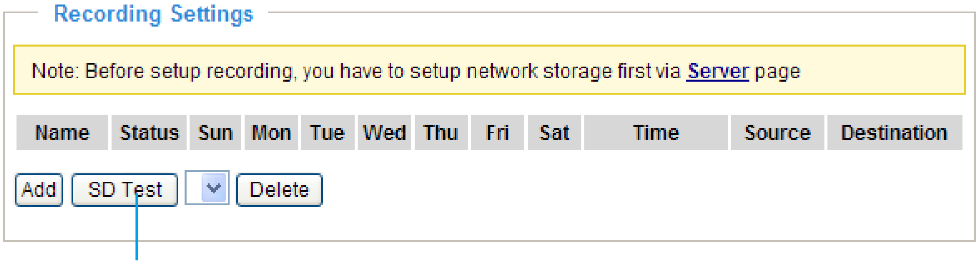
	file name	size	date	time
□	**Video Clip_58.mp4**	2526004	2010/01/15	07:58:28
□	**Video Clip_59.mp4**	2563536	2010/01/15	07:59:28

The format is: File name prefix + Minute (mm)
You can set up the file name prefix on Media Settings page. Please refer to page 85 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

Insert your SD card and click here to test

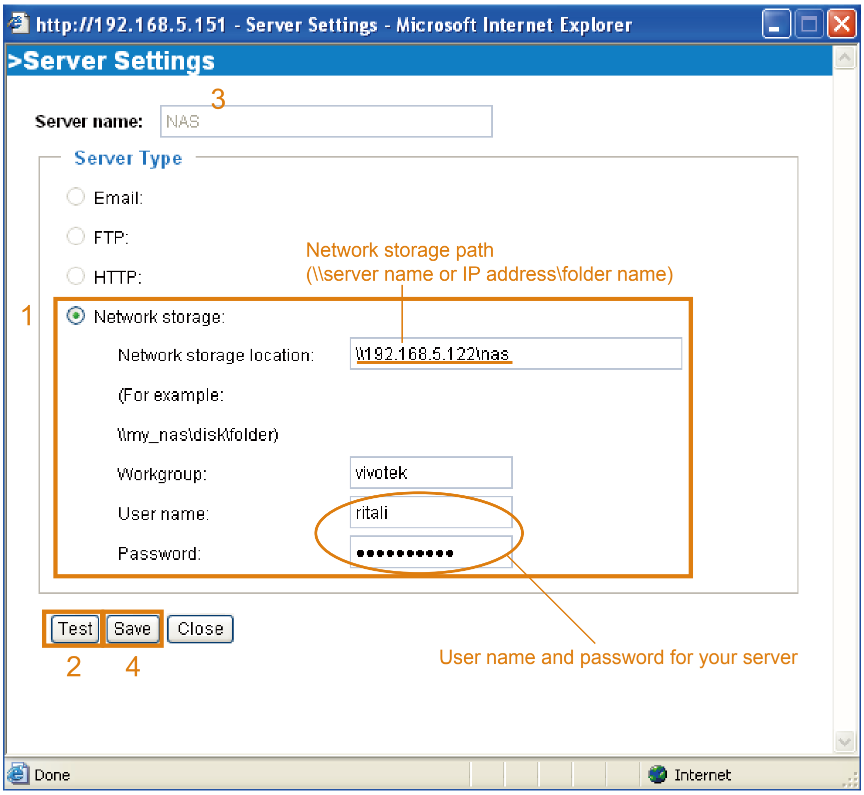
NOTE:

- ► *Before setting up this page, please set up the Network Storage on the Server Settings page first.*
- ► *Please remember to format your SD card when using for the first time. Please refer to page 93 for detailed information.*

Network Storage Setting

If you have not configured a networked storage, click Server to open the Server Settings page and follow the steps below:

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



http://192.168.5.151 - Server Settings - Microsoft Internet Explorer

>Server Settings

Server name: NAS

Server Type

○ Email:

○ FTP:

○ HTTP:

● Network storage:

Network storage location: \\192.168.5.122\nas

(For example:

\\my_nas\disk\folder)

Workgroup: vivotek

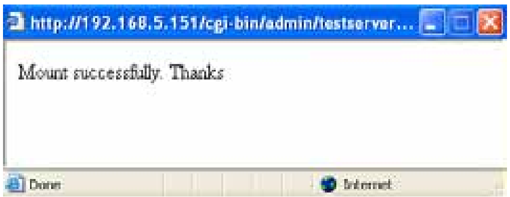
User name: ritali

Password: ●●●●●●●●●●●

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

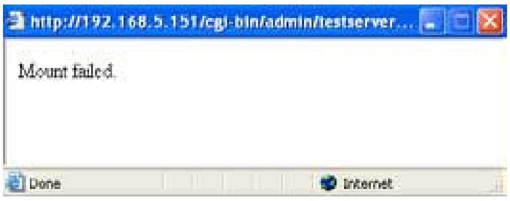
User name and password for your server

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



http://192.168.5.151/cgi-bin/admin/testserver...

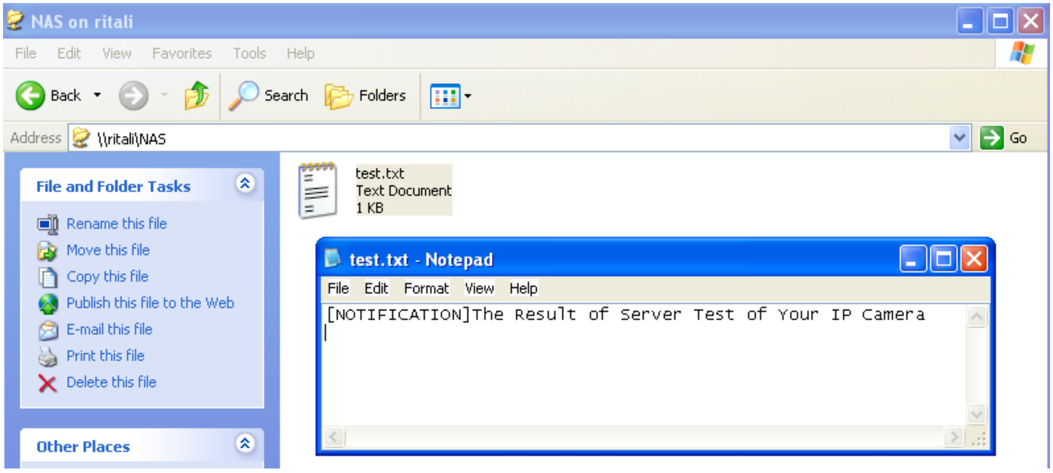
Mount successfully. Thanks



http://192.168.5.151/cgi-bin/admin/testserver...

Mount failed.

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

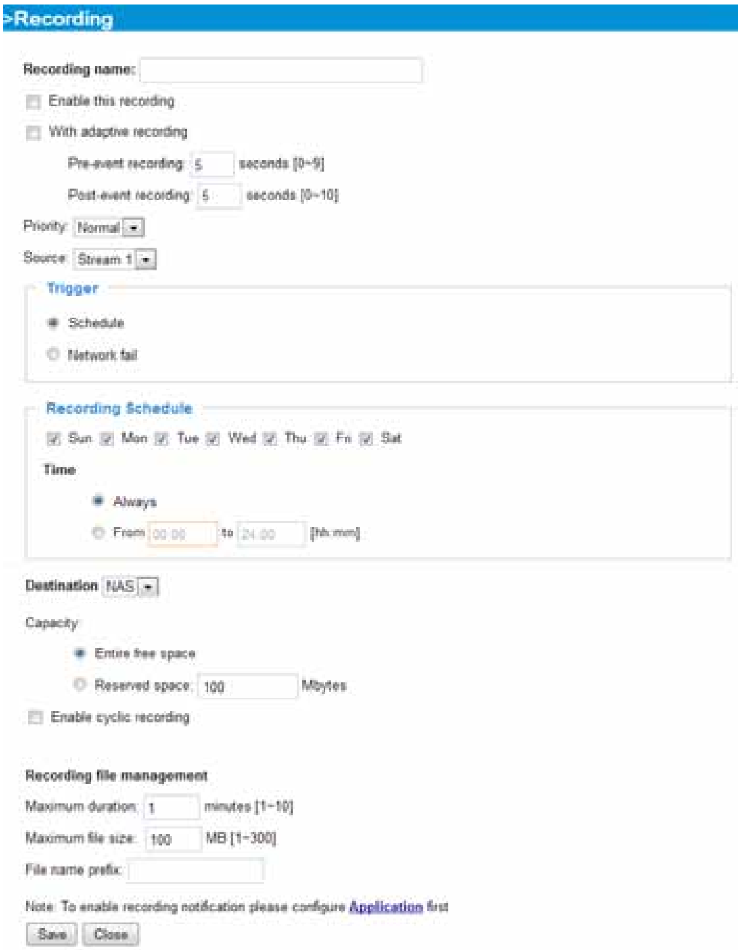


```
[NOTIFICATION]The Result of Server Test of Your IP Camera
```

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

Recording name:

□ Enable this recording

□ With adaptive recording

Pre-event recording: 5 seconds [0~9]

Post-event recording: 5 seconds [0~10]

Priority: Normal

Source: Stream 1

Trigger

● Schedule

○ Network fail

Recording Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

Destination NAS

Capacity:

● Entire free space

○ Reserved space: 100 Mbytes

□ Enable cyclic recording

Recording file management

Maximum duration: 1 minutes [1~10]

Maximum file size: 100 MB [1~300]

File name prefix:

Note: To enable recording notification please configure Application first

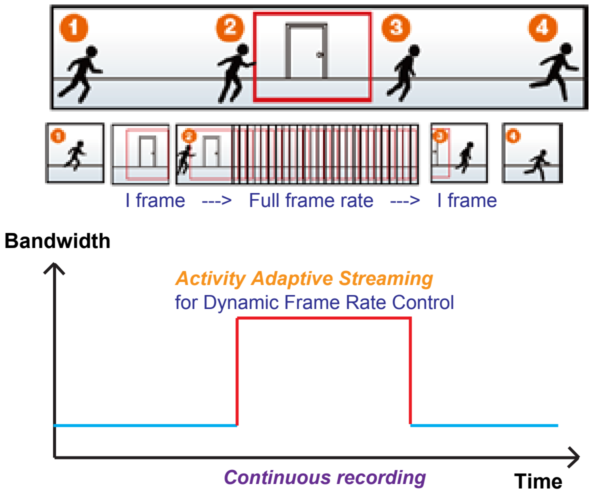
Save Close

Recording name: Enter a name for the recording setting.

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

With adaptive recording: You can specify the length of video recording to be taken before and after an event. When enabled, the network camera will record only the I frame during normal situation, and raise the video frame rate to full on the occurrence of an event. Doing so can save the bandwidth and storage requirements.

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


1
2
3
4
I frame ---> Full frame rate ---> I frame
Bandwidth
Activity Adaptive Streaming
for Dynamic Frame Rate Control
Continuous recording
Time

NOTE:

► To enable adaptive recording, please make sure you've set up the trigger sources such as Motion Detection, DI Device, or Manual Trigger.

► When there is no alarm trigger:
- JPEG mode: record 1 frame per second.
- H.264 mode: record the I frame only.
- MPEG-4 mode: record the I frame only.

► When the Intra frame period has been set to larger than >1s on Video settings page, the Intra frame period will be forced down to 1s when the adaptive recording is activated.

The alarm trigger includes: motion detection and DI detection. Please refer to Event settings on page 77.

■ Pre-event recording and post-event recording
The Network Camera comes with a buffer area. The buffer temporarily holds data up to a certain limit. This enables the camera to record pre- and post-event videos. Enter a number in each text box.

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

■ Source: Select a stream for the recording source.

NOTE:

► *To enable adaptive recording, please also* ***enable time shift caching stream*** *and* ***select a caching stream*** *on Media > Video > Stream settings. Please refer to page 63 for detailed instruction.*

► *To enable recording notification please configure* ***Event settings*** *first. Please refer to page 77.*

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

Source: Select the recording source (stream 1 ~ 4).

Trigger: Select a trigger source.

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

Recording Schedule: Specify the recording duration.

- Select the days in a week as the time when the recording will take place.
- 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 reserved space. The recording size limit must be larger than the reserved amount for cyclic recording.

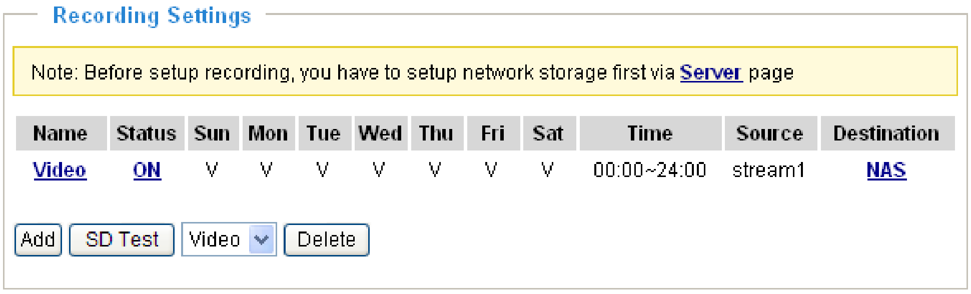
File name prefix: Enter the text that will be appended to the front of the file name.

Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for 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 79 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**.

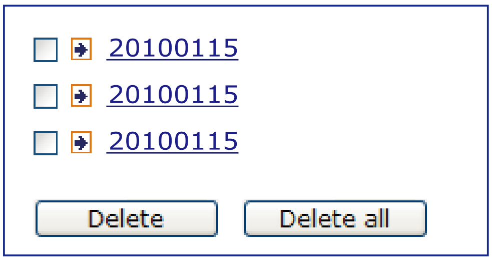


Recording Settings

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
Video	ON	V	V	V	V	V	V	V	00:00~24:00	stream1	NAS

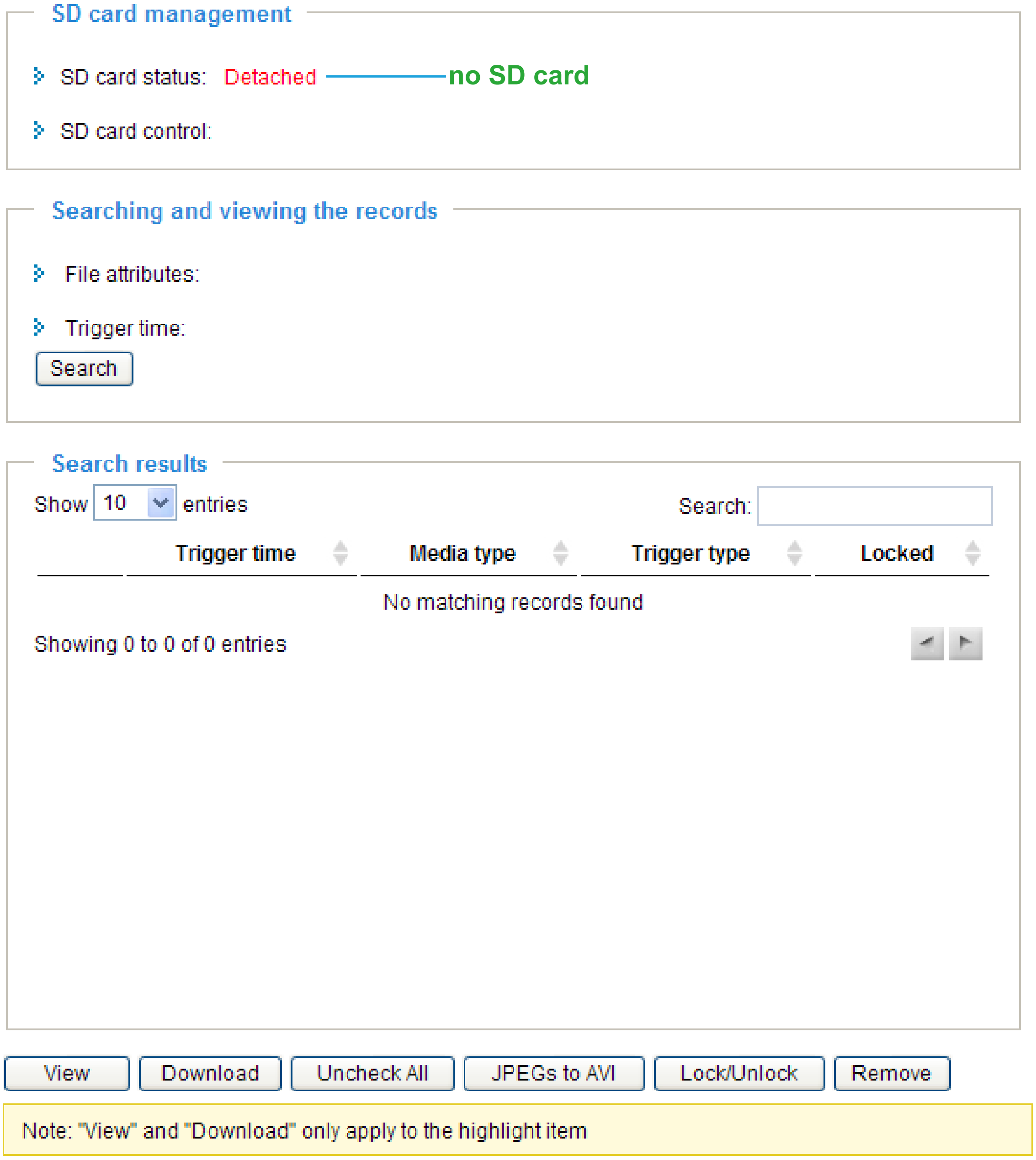
- Click **Video (Name)**: Opens the Recording Settings page to modify.
- Click **ON (Status)**: The Status will become OFF and stop recording.
- Click **NAS (Destination)**: Opens the file list of recordings as shown below. For more information about folder naming rules, please refer to page 88 for details.



□ 20100115
□ 20100115
□ 20100115

Local Storage Advanced Mode

This section explains how to manage the SD card for on board storage. Here you can view SD card status, search for recorded files to playback, download, etc.



SD card management

SD card status: Detached — no SD card

SD card control:

Searching and viewing the records

File attributes:

Trigger time:

Search results

Show 10 entries

Search:

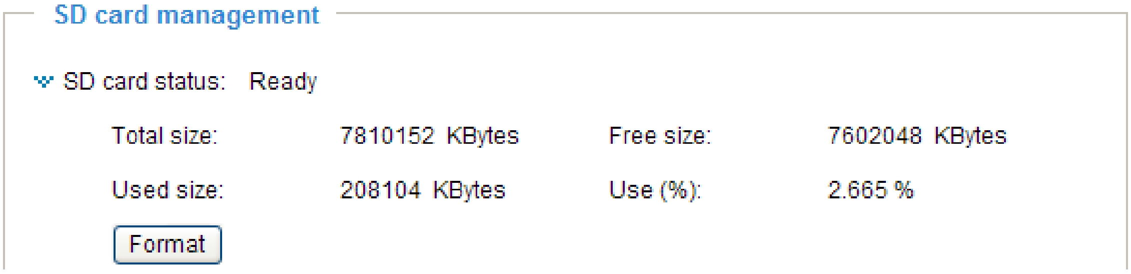
	Trigger time	Media type	Trigger type	Locked
	No matching records found			

Showing 0 to 0 of 0 entries

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

SD Card Management

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



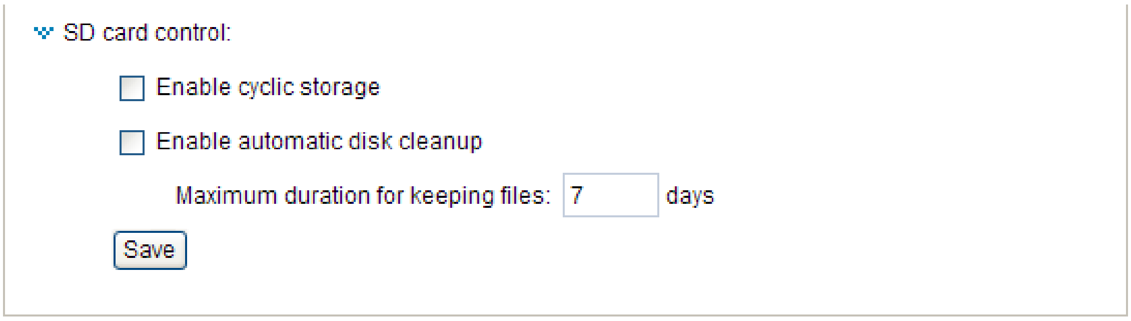
SD card management

SD card status: Ready

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

SD card control

■ Enable cyclic storage: Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.



SD card control:

□ Enable cyclic storage

□ Enable automatic disk cleanup

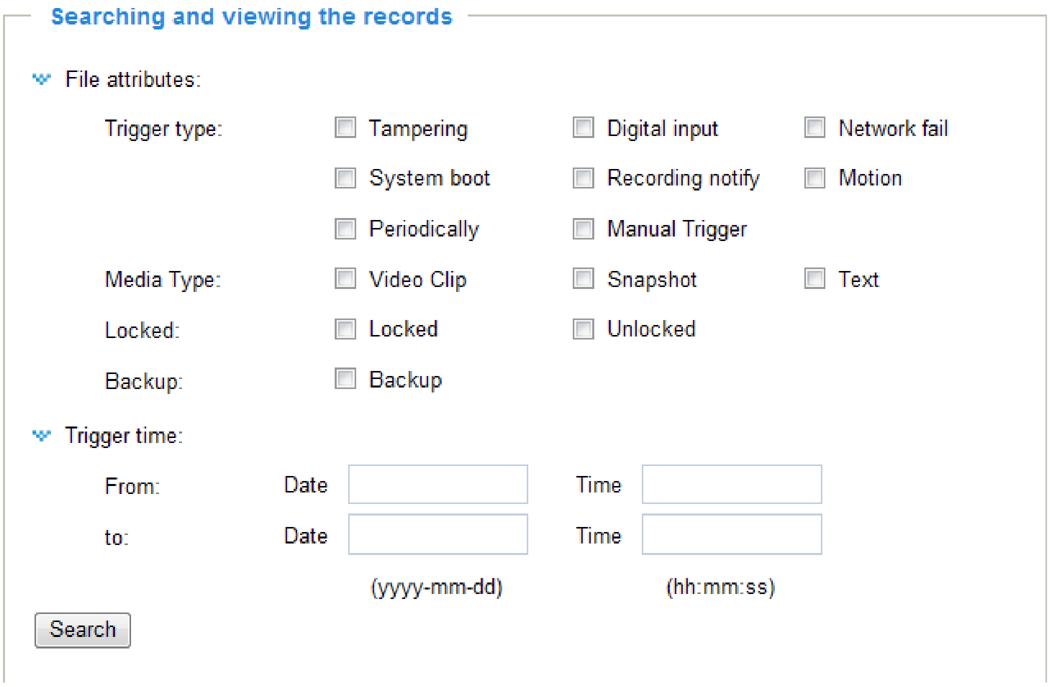
Maximum duration for keeping files: 7 days

■ Enable automatic disk cleanup: Check this item and enter the number of days you wish to retain a file. For example, if you enter “7 days”, the recorded files will be stored on the SD card for 7 days.

Click **Save** to enable your settings.

Searching and Viewing the Records

This column allows the user to set up search criteria for recorded data. If you do not select any criteria and click **Search** button, all recorded data will be listed in the **Search Results** cloumn.



Searching and viewing the records

File attributes:

Trigger type:	□ Tampering	□ Digital input	□ Network fail
	□ System boot	□ Recording notify	□ Motion
	□ Periodically	□ Manual Trigger	
Media Type:	□ Video Clip	□ Snapshot	□ Text
Locked:	□ Locked	□ Unlocked	
Backup:	□ Backup		

Trigger time:

From: Date ____ Time ____

to: Date ____ Time ____

(yyyy-mm-dd) (hh:mm:ss)

File attributes: Select one or more items as your search criteria.

Trigger time: Manually enter the time range you want to search.

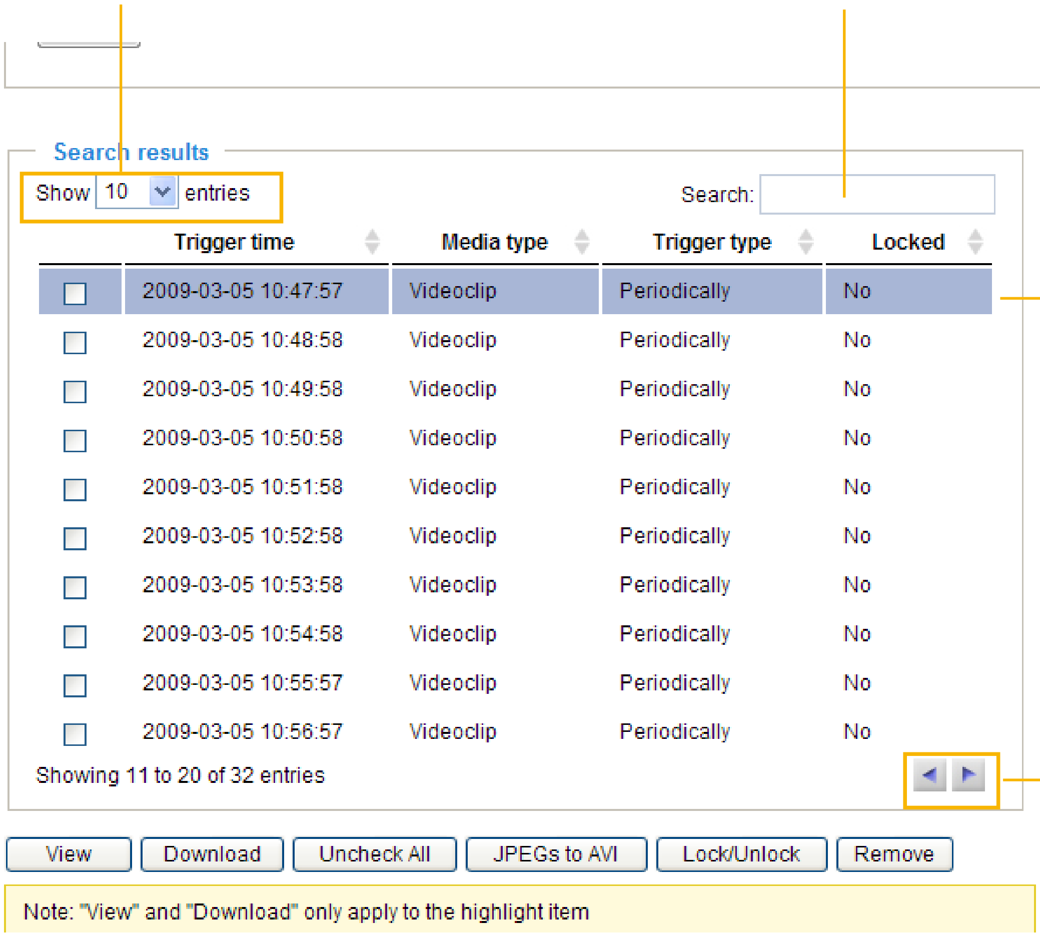
Click **Search** and the recorded data corresponding to the search criteria will be listed in **Search Results** window.

Search Results

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

Numbers of entries displayed on one page

Enter a key word to filter the search results



	Trigger time	Media type	Trigger type	Locked
□	2009-03-05 10:47:57	Videoclip	Periodically	No
□	2009-03-05 10:48:58	Videoclip	Periodically	No
□	2009-03-05 10:49:58	Videoclip	Periodically	No
□	2009-03-05 10:50:58	Videoclip	Periodically	No
□	2009-03-05 10:51:58	Videoclip	Periodically	No
□	2009-03-05 10:52:58	Videoclip	Periodically	No
□	2009-03-05 10:53:58	Videoclip	Periodically	No
□	2009-03-05 10:54:58	Videoclip	Periodically	No
□	2009-03-05 10:55:57	Videoclip	Periodically	No
□	2009-03-05 10:56:57	Videoclip	Periodically	No

Showing 11 to 20 of 32 entries

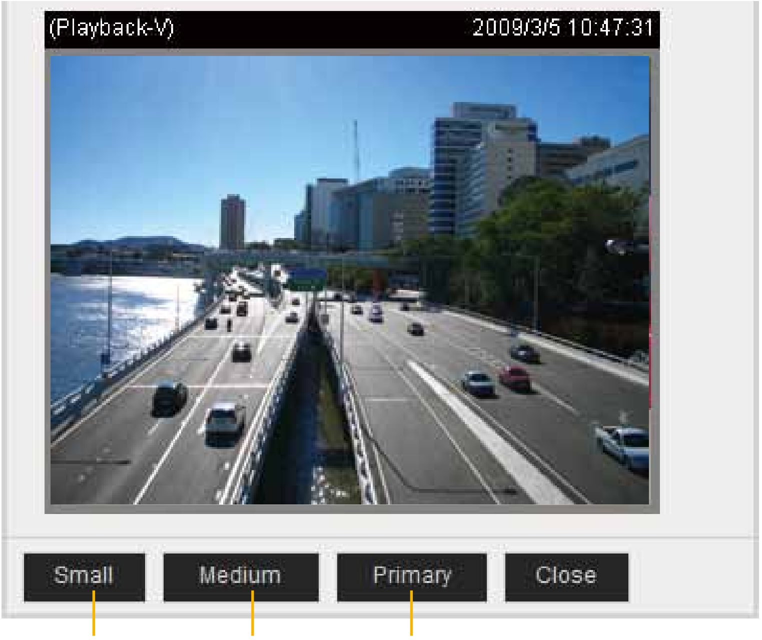
Note: "View" and "Download" only apply to the highlight item

Highlight an item

Click to switch pages

View: Click on a search result which will highlight the selected item in purple as shown above. Click the **View** button and a media window will pop up to play back the selected file.

For example:

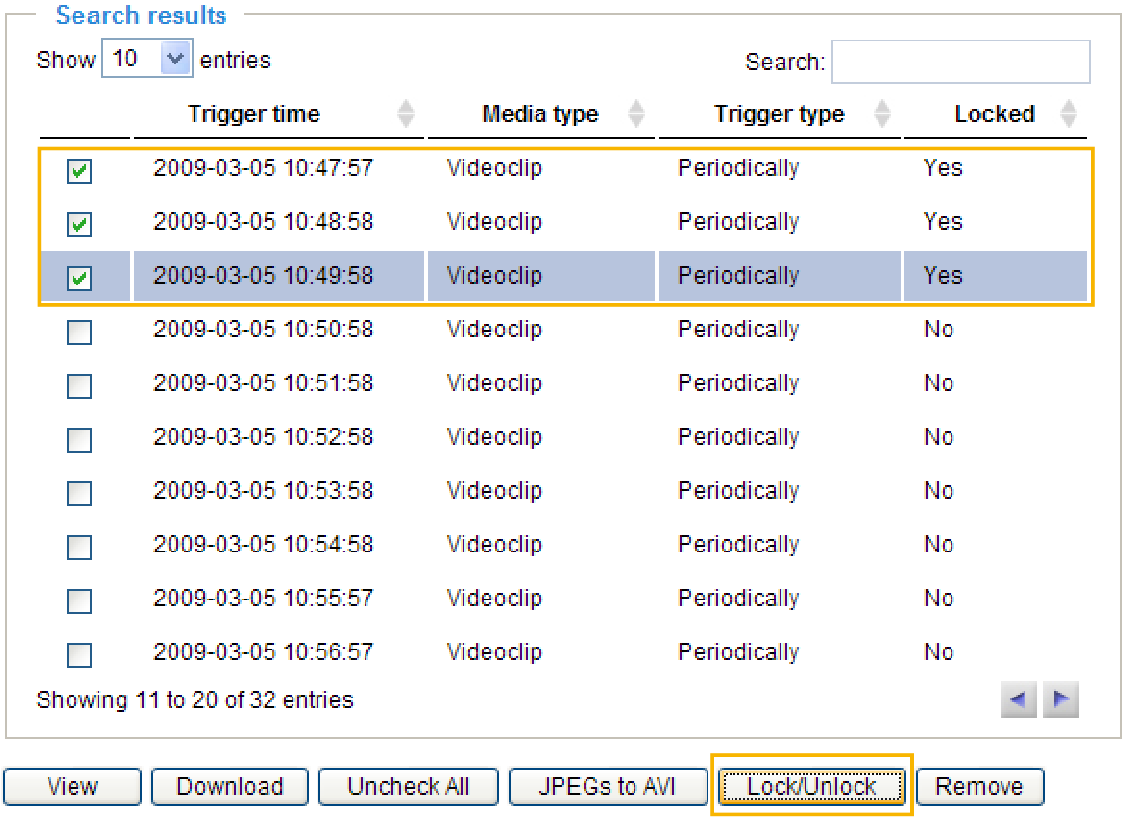


Click to adjust the image size

Download: Click on a search result to highlight the selected item in purple as shown above. Then click the **Download** button and a file download window will pop up for you to save the file.

JPEGs to AVI: This functions only applies to “JPEG“ format files such as snapshots. You can select several snapshots from the list, then click this button. Those snapshots will be converted into an AVI file.

Lock/Unlock: Select the desired search results, then click this button. The selected items will become Locked, which will not be deleted during cyclic recoroding. You can click again to unlock the selections. For example:



Search results

Show 10 entries Search:

	Trigger time	Media type	Trigger type	Locked
☑	2009-03-05 10:47:57	Videoclip	Periodically	Yes
☑	2009-03-05 10:48:58	Videoclip	Periodically	Yes
☑	2009-03-05 10:49:58	Videoclip	Periodically	Yes
□	2009-03-05 10:50:58	Videoclip	Periodically	No
□	2009-03-05 10:51:58	Videoclip	Periodically	No
□	2009-03-05 10:52:58	Videoclip	Periodically	No
□	2009-03-05 10:53:58	Videoclip	Periodically	No
□	2009-03-05 10:54:58	Videoclip	Periodically	No
□	2009-03-05 10:55:57	Videoclip	Periodically	No
□	2009-03-05 10:56:57	Videoclip	Periodically	No

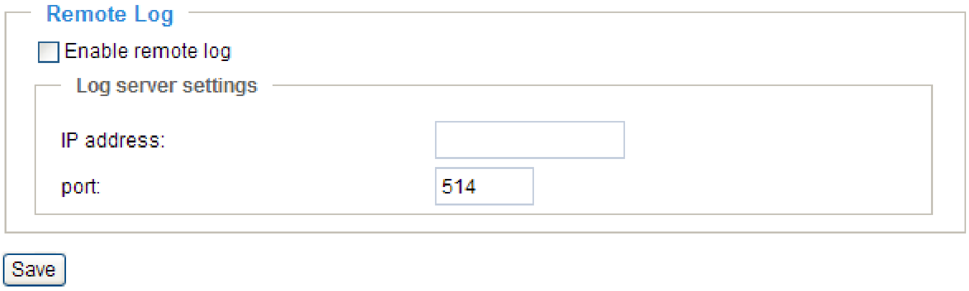
Showing 11 to 20 of 32 entries

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

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

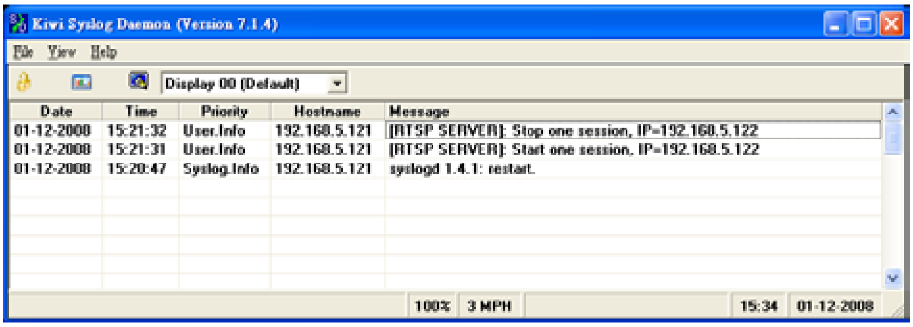
□ Enable remote log

Log server settings

IP address:

port: 514

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/.



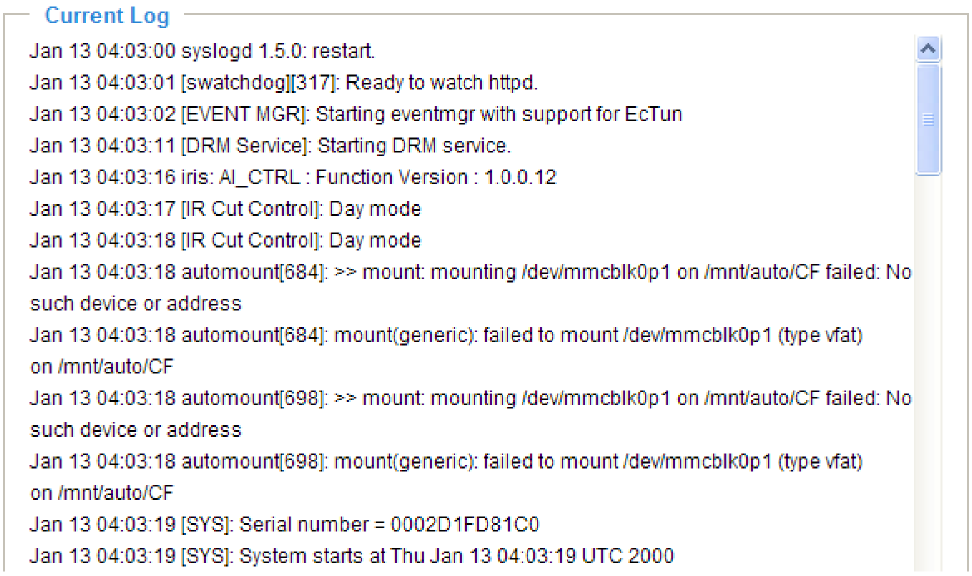
Kiwi Syslog Daemon (Version 7.1.4)
File View Help
Display 00 (Default)

Date	Time	Priority	Hostname	Message
01-12-2008	15:21:32	User.Info	192.168.5.121	[RTSP SERVER]: Stop one session, IP=192.168.5.122
01-12-2008	15:21:31	User.Info	192.168.5.121	[RTSP SERVER]: Start one session, IP=192.168.5.122
01-12-2008	15:20:47	Syslog.Info	192.168.5.121	syslogd 1.4.1: restart.

100% 3 MPH 15:34 01-12-2008

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



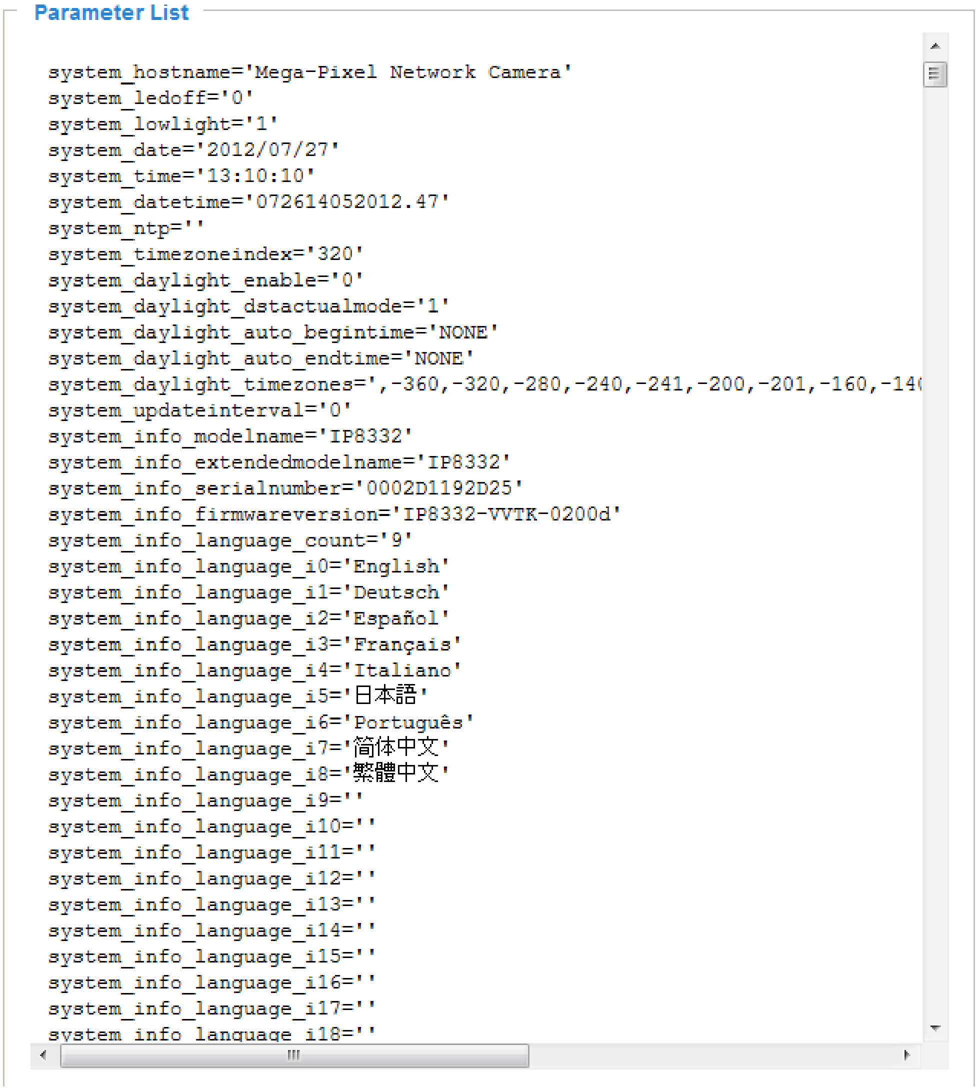
Current Log

```
Jan 13 04:03:00 syslogd 1.5.0: restart.
Jan 13 04:03:01 [swatchdog][317]: Ready to watch httpd.
Jan 13 04:03:02 [EVENT MGR]: Starting eventmgr with support for EcTun
Jan 13 04:03:11 [DRM Service]: Starting DRM service.
Jan 13 04:03:16 iris: AI_CTRL : Function Version : 1.0.0.12
Jan 13 04:03:17 [IR Cut Control]: Day mode
Jan 13 04:03:18 [IR Cut Control]: Day mode
Jan 13 04:03:18 automount[684]: >> mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No
such device or address
Jan 13 04:03:18 automount[684]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat)
on /mnt/auto/CF
Jan 13 04:03:18 automount[698]: >> mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No
such device or address
Jan 13 04:03:18 automount[698]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat)
on /mnt/auto/CF
Jan 13 04:03:19 [SYS]: Serial number = 0002D1FD81C0
Jan 13 04:03:19 [SYS]: System starts at Thu Jan 13 04:03:19 UTC 2000
```

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.

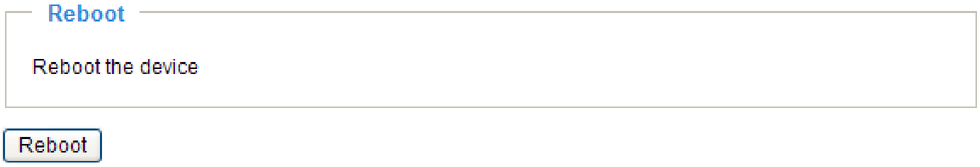


```
system_hostname='Mega-Pixel Network Camera'
system_ledoff='0'
system_lowlight='1'
system_date='2012/07/27'
system_time='13:10:10'
system_datetime='072614052012.47'
system_ntp=''
system_timezoneindex='320'
system_daylight_enable='0'
system_daylight_dstactualmode='1'
system_daylight_auto_begintime='NONE'
system_daylight_auto_endtime='NONE'
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-160,-14
system_updateinterval='0'
system_info_modelname='IP8332'
system_info_extendedmodelname='IP8332'
system_info_serialnumber='0002D1192D25'
system_info_firmwareversion='IP8332-VVTK-0200d'
system_info_language_count='9'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system_info_language_i3='Français'
system_info_language_i4='Italiano'
system_info_language_i5='日本語'
system_info_language_i6='Português'
system_info_language_i7='简体中文'
system_info_language_i8='繁體中文'
system_info_language_i9=''
system_info_language_i10=''
system_info_language_i11=''
system_info_language_i12=''
system_info_language_i13=''
system_info_language_i14=''
system_info_language_i15=''
system_info_language_i16=''
system_info_language_i17=''
system_info_language_i18=''
```

Maintenance

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

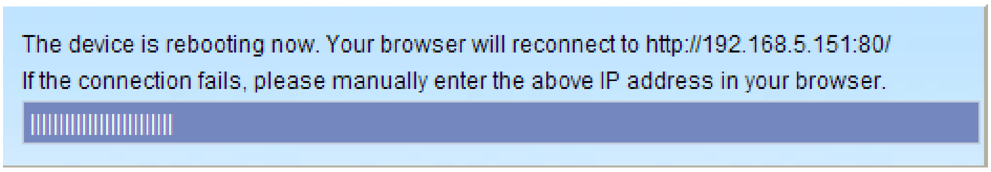
Reboot



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.

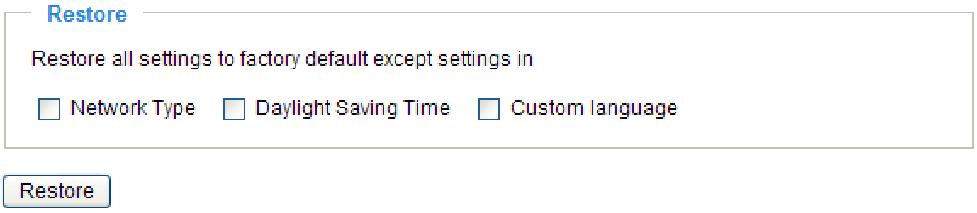


The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/

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.

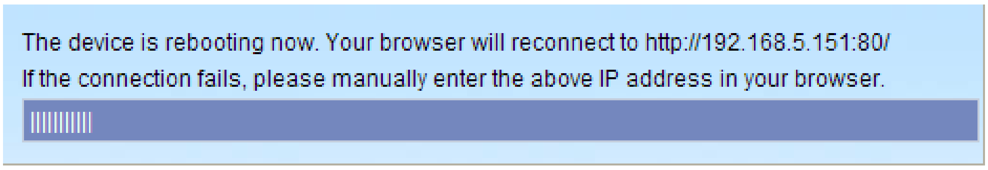
Network Type: Select this option to retain the Network Type settings (please refer to Network Type on page 37).

Daylight Saving Time: Select this option to retain the Daylight Saving Time settings (please refer to System on page 28)

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.

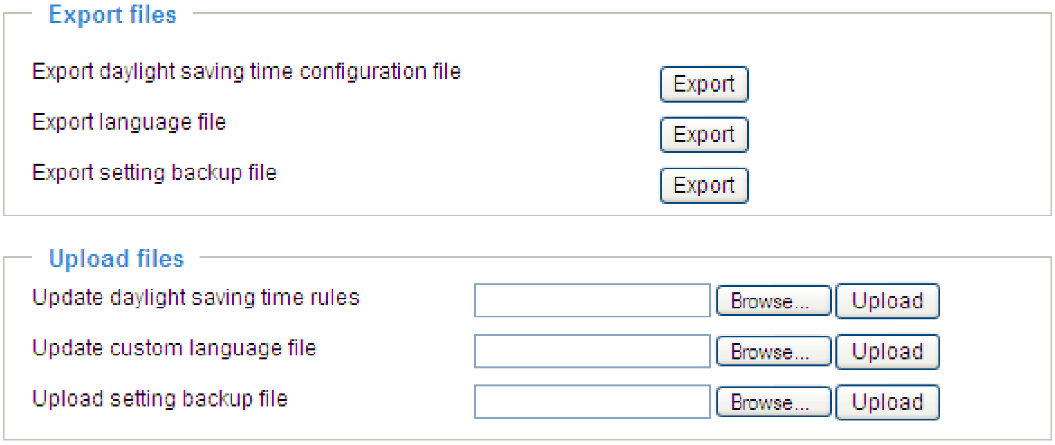


The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/

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

Export language file

Export setting backup file

Upload files

Update daylight saving time rules

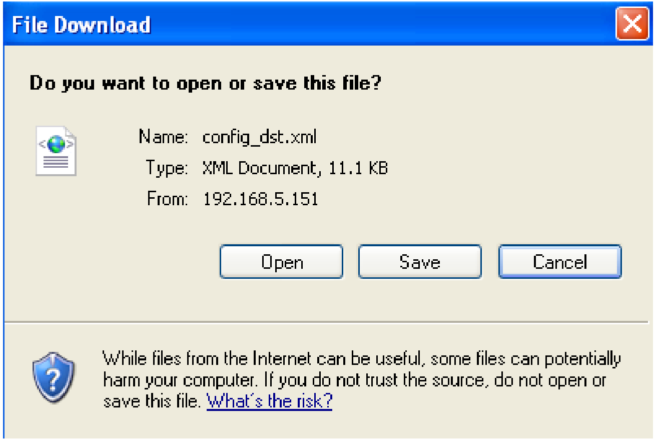
Update custom language file

Upload setting backup file

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.



File Download

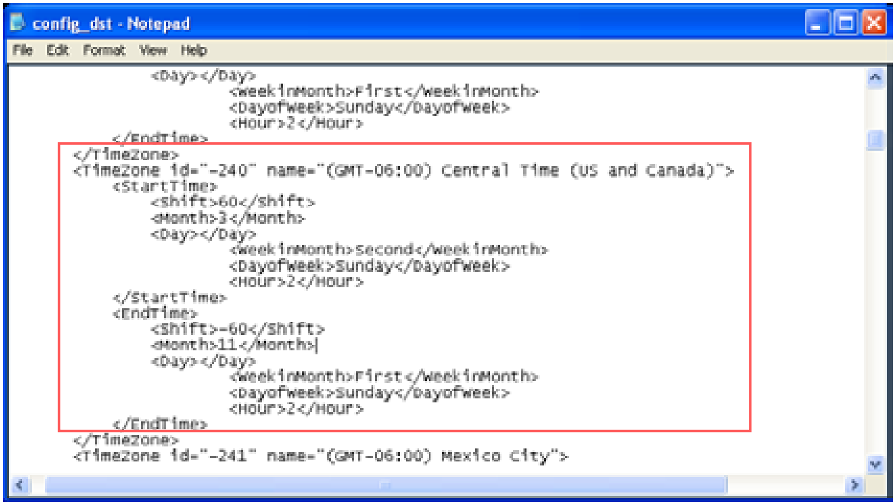
Do you want to open or save this file?

Name: config_dst.xml
Type: XML Document, 11.1 KB
From: 192.168.5.151

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

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.

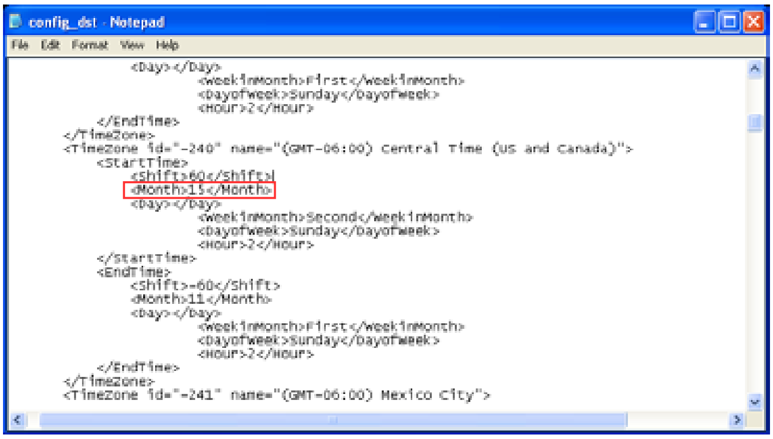
In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.



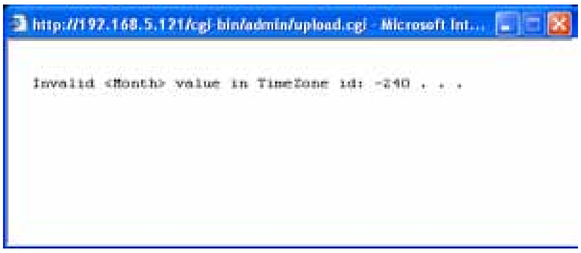
```
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-240" name="(GMT-06:00) Central Time (US and Canada)">
        <StartTime>
            <Shift>60</Shift>
            <Month>3</Month>
            <Day></Day>
                    <WeekInMonth>Second</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </StartTime>
        <EndTime>
            <Shift>-60</Shift>
            <Month>11</Month>
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-241" name="(GMT-06:00) Mexico City">
```

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.



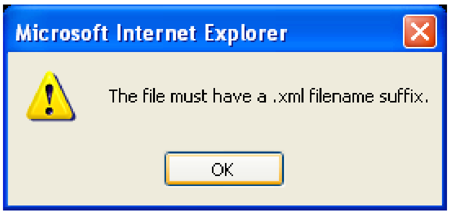
```
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayOfWeek>Sunday</DayOfWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-240" name="(GMT-06:00) Central Time (US and Canada)">
        <StartTime>
            <Shift>60</Shift>
            <Month>15</Month>
            <Day></Day>
                    <WeekInMonth>Second</WeekInMonth>
                    <DayOfWeek>Sunday</DayOfWeek>
                    <Hour>2</Hour>
        </StartTime>
        <EndTime>
            <Shift>-60</Shift>
            <Month>11</Month>
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayOfWeek>Sunday</DayOfWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-241" name="(GMT-06:00) Mexico City">
```



http://192.168.5.121/cgi-bin/admin/upload.cgi - Microsoft Int...

```
Invalid <Month> value in TimeZone id: -240 . . .
```

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



The file must have a .xml filename suffix.

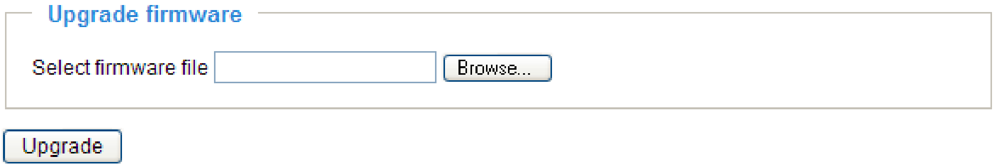
Export language file: Click to export language strings. VIVOTEK provides nine languages: English, Deutsch, Español, Français, Italiano, 日本語 , Português, 簡体中文 , and 繁體中文 .

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



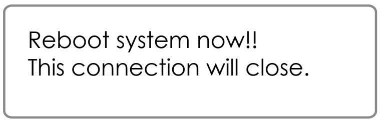
This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.
Note: Do not power off the Network Camera during the upgrade!

Follow the steps below to upgrade the firmware:

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

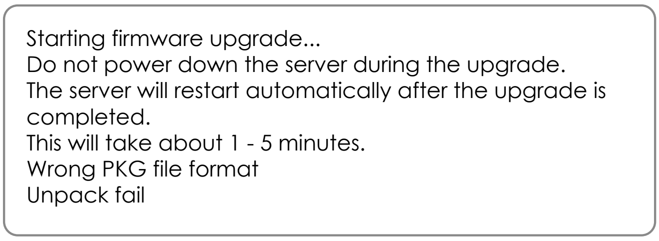
If the upgrade is successful, you will see “Reboot system now!! This connection will close”. After that, re-access the Network Camera.

The following message is displayed when the upgrade has succeeded.



```
Reboot system now!!
This connection will close.
```

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



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

Appendix

URL Commands for the Network Camera

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
```

2. Style Convention

In URL syntax and in descriptions of CGI parameters, a text within angle brackets denotes a content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets shall 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, which is replaced with the string myserver in the URL syntax example, also below.

URL syntax is written with the word "**Syntax:**" written in bold face followed by a box with the reference syntax as seen below. The name of the server is written as <servername>. This 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.

Special notes will be marked in RED.

Syntax:

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

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

Return:

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

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

Example: Request a single snapshot image

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

3. General CGI URL Syntax and Parameters

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

Syntax:

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

Example: Set digital output #1 to active

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

4. Security Level

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

5. Get Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

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

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

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

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

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

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

A successful control request returns parameter pairs as follows:

Return:

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

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

<length> is the actual length of content.

Example: Request IP address and its response

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

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

6. Set Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

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

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

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

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

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

Return:

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

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

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

Example: Set the IP address of server to 192.168.0.123:

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

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
```

7. Available parameters on the server

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

Valid values:

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

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

7.1 system

Group: **system**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	Mega-Pixel Network Camera	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
date	<yyyy/mm/dd>, keep, auto	<current date>	6/6	Current date of system. Set to 'keep' to keep date unchanged. Set to 'auto' to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	<current time>	6/6	Current time of the system. Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	<MMDDhhmmYYYY.ss>	<current time>	6/6	Another current time format of the system.
ntp	<domain name>, <ip address>, <blank>	<blank>	6/6	NTP server. *Do not use "skip to invoke default server" for default value.
timezoneindex	-489 ~ 529	320	6/6	Indicate timezone and area. -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona

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

				200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'Alofa
daylight_enable	<boolean>	0	6/6	Enable automatic daylight saving time in time zone.
daylight_dstactualmode	<boolean>	1	6/7	Check if current time is under daylight saving time. (Used internally)
daylight_auto_begintime	string[19]	NONE	6/7	Display the current daylight saving start time. (product dependent)
daylight_auto_endtime	string[19]	NONE	6/7	Display the current daylight saving end time. (product dependent)

daylight_timezones	string	,-360,-320,-280,-240,-241,-200,-201,-160,-140,-120,-80,-40,0,40,41,80,81,82,83,120,140,380,400,480	6/6	List time zone index which support daylight saving time.
updateinterval	0, 3600, 86400, 604800, 2592000	0	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.
restore	0, <positive integer>	N/A	7/6	Restore the system parameters to default values after <value> seconds.
reset	0, <positive integer>	N/A	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	<Any value>	N/A	7/6	Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
restoreexceptdst	<Any value>	N/A	7/6	Restore the system parameters to default values except all daylight saving time settings. This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system

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

7.1.1 system.info

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	IP8332	0/7	Internal model name of the server (eg. IP7139)
extendedmodelname	string[40]	IP8332	0/7	ODM specific model name of server (eg. DCS-5610). If it is not an ODM model, this field will be equal to "modelname"
serialnumber	<mac address>	<product mac address>	0/7	12 characters MAC address (without hyphens).
firmwareversion	string[40]	<firmware version>	0/7	Firmware version, including model, company, and version number in the format: <MODEL-BRAND-VERSION>
language_count	<integer>	9	0/7	Number of webpage languages available on the server.
language_i<0~(count-1)>	string[16]	English Deutsch Espanol Francais	0/7	Available language lists.

		Italiano 日本語 Portugues 簡体中文 繁體中文		
customlanguage_maxcount	<integer>	1	0/6	Maximum number of custom languages supported on the server.
customlanguage_count	<integer>	0	0/6	Number of custom languages which have been uploaded to the server.
customlanguage_i<0~(maxcount-1)>	string	N/A	0/6	Custom language name.

7.2 status

Group: **status**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
di_i<0~(ndi-1)>	<boolean>	0	1/7	0 => Inactive, normal 1 => Active, triggered
onlinenum_rtsp	integer	0	6/7	Current number of RTSP connections.
onlinenum_httppush	integer	0	6/7	Current number of HTTP push server connections.
eth_i0	<string>	<product dependent>	1/99	Get network information from mii-tool.
vi_i<0~(nvi-1)> <product dependent>	<boolean>	0	1/7	Virtual input 0 => Inactive 1 => Active (capability.nvi > 0)

7.3 digital input behavior define

Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	high	1/1	Indicates open circuit or closed circuit (inactive status)

7.4 digital output behavior define

Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)

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

7.5 security

Group: **security**

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

user_i<1~20>_ privilege	viewer, operator, admin	<blank>	6/6	User privilege

7.6 network

Group: **network**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
type	lan, pppoe	lan	6/6	Network connection type.
resetip	<boolean>	1	6/6	1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot. 0 => Use preset ipaddress, subnet, rounter, dns1, and dns2.
ipaddress	<ip address>	<product dependent>	6/6	IP address of server.
subnet	<ip address>	<blank>	6/6	Subnet mask.
router	<ip address>	<blank>	6/6	Default gateway.
dns1	<ip address>	<blank>	6/6	Primary DNS server.
dns2	<ip address>	<blank>	6/6	Secondary DNS server.
wins1	<ip address>	<blank>	6/6	Primary WINS server.
wins2	<ip address>	<blank>	6/6	Secondary WINS server.

7.6.1 802.1x

Subgroup of **network: ieee8021x**

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

7.6.2 QoS

Subgroup of **network: qos**

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

dscp_eventalarm	0~63	0	6/6	Event/alarm channel for DSCP
dscp_management	0~63	0	6/6	Management channel for DSCP
dscp_eventtunnel	0~63	0	6/6	Event/Control channel for DSCP

7.6.3 IPv6

Subgroup of **network**: **ipv6**

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

7.6.4 FTP

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

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

7.6.5 HTTP

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	80	6/6	HTTP port.
alternateport	1025~65535	8080	6/6	Alternate HTTP port.
authmode	basic, digest	basic	1/6	HTTP authentication mode.
s0_accessname	string[32]	video.mjpg	1/6	HTTP server push access name for stream 1. (capability.protocol.spush_mjpeg =1 and video.stream.count>0)
s1_accessname	string[32]	video2.mjpg	1/6	HTTP server push access name for

				stream 2. (capability.protocol.spush_mjpeg =1 and video.stream.count>1)
s2_accessname	string[32]	video3.mjpg	1/6	Http server push access name for stream 3 (capability.protocol.spush_mjpeg =1 and video.stream.count>2)
s3_accessname	string[32]	video4.mjpg	1/6	Http server push access name for stream 4 (capability.protocol.spush_mjpeg =1 and video.stream.count>3)
s4_accessname	string[32]	videoany.mjpg	1/6	Http server push access name for stream 5 (capability.protocol.spush_mjpeg =1 and video.stream.count>4) **IP8332 ONLY**
anonymousviewing	<boolean>	0	1/6	Enable anoymous streaming viewing.

7.6.6 HTTPS port

Subgroup of **network**: **https_port**

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

7.6.7 RTSP

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	554	1/6	RTSP port. (capability.protocol.rtsp=1)
anonymousviewing	<boolean>	0	1/6	Enable anoymous streaming viewing.
authmode	disable, basic, digest	disable	1/6	RTSP authentication mode. (capability.protocol.rtsp=1)

s0_accessname	string[32]	live.sdp	1/6	RTSP access name for stream1. (capability.protocol.rtsp=1 and video.stream.count>0)
s1_accessname	string[32]	live2.sdp	1/6	RTSP access name for stream2. (capability.protocol.rtsp=1 and video.stream.count>1)
s2_accessname	string[32]	live3.sdp	1/6	RTSP access name for stream3 (capability.protocol.rtsp=1 and video.stream.count>2)
s3_accessname	string[32]	Live4.sdp	1/6	RTSP access name for stream4 (capability.protocol.rtsp=1 and video.stream.count>3)
S4_accessname	string[32]	liveany.sdp	1/6	RTSP access name for stream5 (capability.protocol.rtsp=1 and video.stream.count>4) **IP8332 ONLY**

7.6.7.1 RTSP multicast

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

(capability.protocol.rtp.multicast=1)

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

7.6.8 SIP port

Subgroup of **network**: **sip**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
Port	1025 ~ 65535	5060	1/6	SIP port. (capability.protocol.sip=1)

7.6.9 RTP port

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

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

7.6.10 PPPoE

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

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

7.7 IP Filter

Group: **ipfilter**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable access list filtering.
admin_enable	<boolean>	0	6/6	Enable administrator IP address.
admin_ip	String[44]	<blank>	6/6	Administrator IP address.
maxconnection	1~10	10	6/6	Maximum number of concurrent streaming

				connection(s).
type	0, 1	1	6/6	Ipfilter policy : 0 => allow 1 => deny
ipv4list_i<0~9>	Single address: <ip address> Network address: <ip address / network mask> Range address:<start ip address - end ip address>	<blank>	6/6	IPv4 address list.
ipv6list_i<0~9>	String[44]	<blank>	6/6	IPv6 address list.

7.8 video input

Group: **videoin**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	60	4/4	CMOS frequency. (capability.videoin.type=2)
whitebalance	auto, manual	auto	4/4	“auto” indicates auto white balance. “manual” indicates keep current value.
exposurelevel	0~12	4	4/4	Exposure level
enablewdr	<boolean>	0	4/4	Enable/disable wield dynamic range.
enableblc	<boolean>	0	4/4	Enable backlight compensation.
agc	0,1,2	1	4/4	Set auto gain control to normal level or MAX level. 0->2x, 1->4x, 2->8x
color	0, 1	1	4/4	0 =>monochrome 1 => color

flip	<boolean>	1	4/4	Flip the image.
mirror	<boolean>	1	4/4	Mirror the image.
ptzstatus	<integer>	2	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support) Bit 3 => Support **tilt** operation; 0(not support), 1(support) Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)
text	string[16]	<blank>	1/4	Enclose caption.
imprinttimestamp	<boolean>	0	4/4	Overlay time stamp on video.
maxexposure	1, 15, 30, 60, 120, 240, 480 <product dependent>	30	4/4	Maximum exposure time.
options	quality, framerate, crop	quality	4/4	Video input option: (1) video quality first mode (2) video frame rate first mode (3) cropping mode (not used in FD8372)
enablepreview	<boolean>	0	1/4	Usage for UI of exposure settings. Preview settings of video profile.

7.8.1 video input setting per channel

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

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	60	4/4	CMOS frequency. (videoin.type=2) (product dependent)
whitebalance	auto, manual	auto	4/4	"auto" indicates auto white balance. "manual" indicates keep current value.
exposurelevel	1~8	4	4/4	Exposure level (product dependent)
enableblc	<boolean>	0	4/4	Enable backlight compensation.
agc	0~2	1	4/4	Set auto gain control to normal level or MAX level.
color	0, 1	1	4/4	0 =>monochrome 1 => color
flip	<boolean>	1	4/4	Flip the image.
mirror	<boolean>	1	4/4	Mirror the image.
ptzstatus	<integer>	2	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support) Bit 3 => Support **tilt** operation; 0(not support), 1(support)

				Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)
text	string[16]	<blank>	1/4	Enclose caption.
imprinttimestamp	<boolean>	0	4/4	Overlay time stamp on video.
maxexposure	1~30 (IP8332) 1~480 (IP8330)	30	4/4	Maximum exposure time.
whitebalance <product dependent>	0~1	0	4/4	0: auto tracking white balance 1: white balance control
enableblc <product dependent>	0~1	0	4/4	Enable backlight compensation
enablepreview	<boolean>	0	1/4	Usage for UI of exposure settings. Preview settings of video profile.
crop_position	<coordinate> (x,y)	0,0	1/4	Crop left-top corner coordinate.
crop_size	<window size> (WxH)	1280x720	1/4	Crop width and height. (width must be 16x or 32x and height must be 8x)
crop_preview	< boolean >	0	1/4	Usage for UI of crop setting
s<0~(m-1)>_codectype	mpeg4, mjpeg, h264 <product dependent>	H264	1/4	Video codec type.
s<0~(m-1)>_mpeg4_intraperiod	250, 500,	1000	4/4	Intra frame period in

	1000, 2000, 3000, 4000			milliseconds.
s<0~(m-1)>_mpeg4_ratecontrolmode	cbr, vbr	vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_quant	0, 1~5	3	4/4	Quality of video when choosing vbr in “ratecontrolmode”. 0 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_mpeg4_bitrate	1000~8000000	51200	4/4	Set bit rate in bps when choosing cbr in “ratecontrolmode”.
s<0~(m-1)>_h264_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_h264_ratecontrolmode	cbr, vbr	cbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_h264_quant	1~5,99	3	4/4	Quality of video when choosing vbr in “ratecontrolmode”. 0 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_h264_qvalue	0~51	30	4/4	Manual video quality level input - choose customize input “h264_quant = 0” (for MPEG-4).
s<0~(m-1)>_h264_bitrate	1000~8000000	3000000	4/4	Set bit rate in bps when choosing cbr in “ratecontrolmode”.
s<0~(m-1)>_h264_maxframe	1~25, 26~30 (only for NTSC or 60Hz	30	1/4	Set maximum frame rate in fps (for MPEG-4).

	CMOS)			
s<0~(m-1)>_h264_profile	0~2	1	1/4	Indicate H264 profiles 0: baseline 1: main profile 2: high profile
s<0~(m-1)>_mpeg4_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	25 => PAL CCD or 50Hz CMOS 30 => NTSC CCD or 60Hz CMOS	1/4	Set maximum frame rate in fps (for MPEG-4).
s<0~(m-1)>_mpeg4_qvalue	1~31	7	4/4	Manual video quality level input - choose customize input “mpeg4_quant = 0” (for MPEG-4).
s<0~(m-1)>_mjpeg_quant	0 ~ 5	3	4/4	Quality of JPEG video. 0 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_mjpeg_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	25 => PAL CCD or 50Hz CMOS 30 => NTSC CCD or 60Hz CMOS	1/4	Set maximum frame rate in fps (for JPEG).
s<0~(m-1)>_mjpeg_qvalue	10~200	50	4/4	Manual video quality level input - choose customize input “mjpeg_quant = 0” (for MJPEG).
s<0~(m-1)>_forcei	1	N/A	7/6	Force I frame.

7.9 video input preview

The temporary settings for video preview

Group: **videoinpreview**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
maxexposure	1~32000	30	4/4	Maximum exposure time.
enableblc	<boolean>	0	4/4	Preview of enable backlight compensation.
enablewdr	<boolean>	0	4/4	Enable/disable wield dynamic range.
agc	0~2	1	4/4	Preview of set auto gain control to normal level or MAX level. 0->normal, 1->max
exposurelevel	1~8	4	4/4	Preview of exposure level (product dependent)
enableblc	0~1	0	4/4	Enable backlight compensation
autoiris	<boolean>	0	4/4	Enable auto Iris.

7.10 IR cut control

Group: **ircutcontrol**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
mode	auto, day, night, di, schedule	auto	6/6	Set IR cut control mode
daymodebegintime	00:00~23:59	07:00	6/6	Day mode begin time
daymodeendtime	00:00~23:59	18:00	6/6	Day mod end time
disableirled	<boolean>	0	6/6	Enable/disable IR led
bwmode	<boolean>	1	6/6	Switch to B/W in night mode if enabled
sensitivity	low, normal,	normal	6/6	Sensitivity of light sensor

	high			

7.11 image setting per channel

Group: **image_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5 ~ 5	-5	4/4	Adjust brightness of image according to mode settings.
saturation	-5 ~ 5	0	4/4	Adjust saturation of image according to mode settings.
contrast	-5 ~ 5	0	4/4	Adjust contrast of image according to mode settings.
sharpness	-3~3	0	4/4	Adjust sharpness of image according to mode settings.

7.12 image setting for preview

Group: **imagepreview_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5 ~ 5	-5	4/4	Preview of brightness adjustment of image according to mode settings.
saturation	-5 ~ 5	0	4/4	Preview of saturation adjustment of image according to mode settings.
contrast	-5 ~ 5	0	4/4	Preview of contrast adjustment of image according to mode settings.
sharpness	-3~ 3	0	4/4	Preview of sharpness adjustment of image according to mode settings.

Group: **imagepreview**

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

7.13 Time Shift settings

Group: **timeshift**, c for n channel products, m is stream number (product dependent)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable time shift streaming.
c<0~(n-1)>_s<0~(m-1)>_allow	<boolean>	c0_s<0~2>_allow=0 c0_s3_allow=1 (IP8332)	4/4	Enable time shift streaming for specific stream. (product dependent)

7.14 Motion detection settings

Group: **motion_c<0~(n-1)>** for m profile and n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable motion detection.
win_i<0~2>_enable	<boolean>	0	4/4	Enable motion window 1~3.
win_i<0~2>_name	string[14]	<blank>	4/4	Name of motion window 1~3.
win_i<0~2>_left	0 ~ 320	0	4/4	Left coordinate of window position.
win_i<0~2>_top	0 ~ 240	0	4/4	Top coordinate of window position.
win_i<0~2>_width	0 ~ 320	0	4/4	Width of motion

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

profile_i<0~(m-1)>_win_i<0~2>_objsize	0 ~ 100	0	4/4	Percent of motion detection window.
profile_i<0~(m-1)>_win_i<0~2>_sensitivity <product dependent>	0 ~ 100	0	4/4	Sensitivity of motion detection window.

7.15 Tampering detection settings

Group: **tampering_c<0~(n-1)>** for n channel product (product dependent)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable or disable tamper detection.
threshold	0 ~ 255	32	4/4	Threshold of tamper detection.
duration	10 ~ 600	10	4/4	If tampering value exceeds the 'threshold' for more than 'duration' second(s), then tamper detection is triggered.

7.16 DDNS

Group: **ddns**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the dynamic DNS.

provider	Safe100,
	DyndnsDynamic,
	DyndnsCustom,
	TZO,
	DHS,
	DynInterfree,
	CustomSafe100
		DyndnsDynamic	6/6	Safe100 => safe100.net
				DyndnsDynamic => dyndns.org (dynamic)
				DyndnsCustom => dyndns.org (custom)
				TZO => tzo.com
				DHS => dhs.org
				DynInterfree =>dyn-interfree.it
				CustomSafe100 =>
				Custom server using safe100 method

<provider>_hostname	string[128]	<blank>	6/6	Your DDNS hostname.

<provider>_usernameemail	string[64]	<blank>	6/6	Your user name or email to login to the DDNS service provider
<provider>_passwordkey	string[64]	<blank>	6/6	Your password or key to login to the DDNS service provider.
<provider>_servername	string[128]	<blank>	6/6	The server name for safe100. (This field only exists if the provider is customsafe100)

7.17 UPnP presentation

Group: **upnppresentation**

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

7.18 UPnP port forwarding

Group: **upnpportforwarding**

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

7.19 System log

Group: **syslog**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	0	6/6	Enable remote log.
serverip	<IP address>	<blank>	6/6	Log server IP address.
serverport	514, 1025~65535	514	6/6	Server port used for log.
level	0~7	6	6/6	Levels used to distinguish the importance of the

				information: 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG

7.20 SNMP

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

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

7.21 Layout configuration

Group: **layout** (New version)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
logo_default	<boolean>	1	1/6	0 => Custom logo 1 => Default logo
logo_link	string[40]	http://www.vivotek.com	1/6	Hyperlink of the logo
logo_powerbyvvtk_hidden	<boolean>	0	1/6	0 => display the power by vivotek logo 1 => hide the power by vivotek logo
theme_option	1~4	1	1/6	1~3: One of the default themes. 4: Custom definition.
theme_color_font	string[7]	#ffffff	1/6	Font color
theme_color_configfont	string[7]	#ffffff	1/6	Font color of configuration area.
theme_color_titlefont	string[7]	#098bd6	1/6	Font color of video title.
theme_color_controlbackground	string[7]	#565656	1/6	Background color of control area.
theme_color_configbackground	string[7]	#323232	1/6	Background color of configuration area.
theme_color_videobackground	string[7]	#565656	1/6	Background color of video area.
theme_color_case	string[7]	#323232	1/6	Frame color
custombutton_manualtrigger_show	<boolean>	1	1/6	Show or hide manual trigger (VI) button in homepage 0 -> Hidden 1 -> Visible

7.22 Privacy mask

Group: **privacymask_c<0~(n-1)>** for n channel product

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

7.23 Capability

Group: **capability**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
api_httpversion	0200a	0100a	0/7	The HTTP API version.
bootuptime	<positive integer>	60	0/7	Server bootup time.
nir	0, <positive integer>	1	0/7	Number of IR interfaces.
npir	0, <positive integer>	0	0/7	Number of PIRs.
ndi	0, <positive integer>	1	0/7	Number of digital inputs.
nvi	0, <positive integer>	3	0/7	Number of virtual inputs (manual trigger)
ndo	0, <positive integer>	0	0/7	Number of digital outputs.
naudioin	0,	0	0/7	Number of audio inputs.

	<positive integer>			
naudioout	0, <positive integer>	0	0/7	Number of audio outputs.
nvideoin	<positive integer>	1	0/7	Number of video inputs.
nmediastream	<positive integer>	4	0/7	Number of media stream per channels.
nvideosetting	<positive integer>	2	0/7	Number of video settings per channel.
naudiosetting	<positive integer>	0	0/7	Number of audio settings per channel.
nuart	0, <positive integer>	0	0/7	Number of UART interfaces.
nvideoinprofile	<positive integer>	1	0/7	Number of video input profiles.
nmotionprofile	<positive integer>	1	0/7	Number of motion profiles.

ptzenabled	<positive integer>	0	0/7	An 32-bit integer, each bit can be set separately as follows:
				Bit 0 => Support camera control function;
				0(not support), 1(support)
				Bit 1 => Built-in or external camera;
				0(external), 1(built-in)
				Bit 2 => Support pan operation, 0(not support), 1(support)
				Bit 3 => Support tilt operation; 0(not support), 1(support)
				Bit 4 => Support zoom operation;
				0(not support), 1(support)
				Bit 5 => Support focus operation;
				0(not support), 1(support)
				Bit 6 => Support iris operation;
				0(not support), 1(support)
				Bit 7 => External or built-in PT; 0(built-in), 1(external)
				Bit 8 => Invalidate bit 1 ~ 7;
				0(bit 1 ~ 7 are valid),
				1(bit 1 ~ 7 are invalid)
				Bit 9 => Reserved bit; Invalidate

				lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris. 0(fields are valid), 1(fields are invalid)
evctrlchannel	<boolean>	1	0/7	Indicate whether to support HTTP tunnel for event/control transfer.
eptz	<positive integer>	7	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => stream 1 supports ePTZ or not. Bit 1 => stream 2 supports ePTZ or not. The rest may be deduced by analogy
npreset	<positive integer>	0	0/7	Number of preset locations.
ptzenabledclient	<boolean>	0	0/7	Indicate whether to support ptz client
protocol_https	< boolean >	1	0/7	Indicate whether to support HTTP over SSL.
protocol_rtsp	< boolean >	1	0/7	Indicate whether to support RTSP.
protocol_sip	<boolean>	0	0/7	Indicate whether to support SIP.
protocol_maxconnection	<positive integer>	10	0/7	The maximum allowed simultaneous connections.
protocol_maxgenconnection	<positive integer>	10	0/7	The maximum general streaming connections .
protocol_maxmegaconnection	<positive integer>	0	0/7	The maximum megapixel streaming connections.
protocol_rtp_multicast_ scalable	<boolean>	1	0/7	Indicate whether to support scalable multicast.
protocol_rtp_multicast_ backchannel	<boolean>	0	0/7	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	1	0/7	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	1	0/7	Indicate whether to support RTP over HTTP.
protocol_spush_mjp	<boolean>	1	0/7	Indicate whether to support server

eg				push MJPEG.
protocol_snmp	<boolean>	1	0/7	Indicate whether to support SNMP.
protocol_ipv6	<boolean>	1	0/7	Indicate whether to support IPv6.
videoin_type	0, 1, 2	2	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_resolution	<a list of available resolution separated by commas>	176x144,320x200 640x400,1280x800	0/7	Available resolutions list.
videoin_maxframerate	<a list of available maximum frame rate separated by commas>	30,30,30,30	0/7	Available maximum frame list.
videoin_codec	<a list of available codec types separated by commas>	mpeg4,mjpeg,h264	0/7	Available codec list.
derivative_brand	<boolean>	1	0/7	Indicate whether to support the upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)
joystick	<boolean>	0	0/7	Indicate whether to support joystick control.
storage_dbenabled	<boolean>	1	0/7	Media files are indexed in database.
nanystream	<positive integer>	1	0/7	number of any media stream per channel
iva	<boolean>	0	0/7	Indicate whether to support Intelligent Video analysis
whitelight	<boolean>	0	0/7	Indicate whether to support white light led.
tampering	<boolean>	1	0/7	Indicate whether to support

				tampering detection.
temperature	<boolean>	0	0/7	Indicate whether to support temperature detection.
version_onvifdaemon	<string>	1.6.0.17	0/7	Indicate ONVIF daemon version

7.24 Customized event script

Group: **event_customtaskfile_i**<0~2>

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

Group: **custom_i**<0~2>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of customized event script file.

7.25 Event setting

Group: **event_i**<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry.
enable	0, 1	0	6/6	Enable or disable this event.
priority	0, 1, 2	1	6/6	Indicate the priority of this event: "0" = low priority "1" = normal priority "2" = high priority
delay	1~999	10	6/6	Delay in seconds before detecting the next event.
trigger	boot, vi, di, motion, seq, recnotify, tampering, visignal	boot	6/6	Indicate the trigger condition: "boot" = System boot "di"= Digital input "motion" = Video motion detection "seq" = Periodic condition "recnotify" = Recording notification. "tampering" = Tamper detection.
triggerstatus	String[40]	trigger	6/6	The status for event trigger
lowlightcondition <product dependent>	0, 1	1	6/6	Switch on white light LED in low light condition 0 => Do action at all times 1 => Do action in low-light conditions
di	<integer>	1	6/6	Indicate the source id of di trigger. This field is required when trigger condition is "di". One bit represents one digital input. The LSB indicates DI 0.

mdwin	<integer>	0	6/6	Indicate the source window id of motion detection. This field is required when trigger condition is “md”. One bit represents one window. The LSB indicates the 1st window. For example, to detect the 1st and 3rd windows, set mdwin as 5.
mdwin0	<integer>	0	6/6	Similar to mdwin. The parameter takes effect when profile 1 of motion detection is enabled.
vi	<integer>	0	6/6	Indicate the source id of vi trigger. This field is required when trigger condition is “vi”. One bit represents one digital input. The LSB indicates VI 0.
inter	1~999	1	6/6	Interval of snapshots in minutes. This field is used when trigger condition is “seq”.

weekday	0~127	127	6/6	Indicate which weekday is scheduled.
				One bit represents one weekday.
				bit0 (LSB) = Saturday
				bit1 = Friday
				bit2 = Thursday
				bit3 = Wednesday
				bit4 = Tuesday
				bit5 = Monday
				bit6 = Sunday
				For example, to detect events on Friday and Sunday, set weekday as 66.

begintime	hh:mm	00:00	6/6	Begin time of the weekly schedule.
endtime	hh:mm	24:00	6/6	End time of the weekly schedule. (00:00 ~ 24:00 sets schedule as always on)
action_cf_enable	0. 1	0	6/6	Enable media write on CF or other local storage media
action_cf_folder	string[128]	NULL	6/6	Path to store media.

action_cf_media	NULL, 0~4	NULL	6/6	Index of the attached media.
action_cf_datefolder	<boolean>	1	6/6	Enable this to create folders by date, time, and hour automatically.
action_server_i<0~4>_enable	0, 1	0	6/6	Enable or disable this server action.
action_server_i<0~4>_media	NULL, 0~4	NULL	6/6	Index of the attached media.
action_server_i<0~4>_datefolder	<boolean>	0	6/6	Enable this to create folders by date, time, and hour automatically.
action_cf_backup	<Boolean>	0	6/6	Enable or disable the function that send media to SD card for backup if network is disconnected.
action_do_i<0~(ndo-1)>_enable	0, 1	0	6/6	Enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	1	6/6	Duration of the digital output trigger in seconds.
action_goto_enable <product dependent>	<Boolean>	0	6/6	Enable/disable ptz goto preset position on event triggered.
action_goto_name <product dependent>	string[40]	<blank>	6/6	Specify the preset name that ptz goto on event triggered.
action_patrol_enable (only for VS series) <product dependent>	<Boolean>	0	6/6	Enable/disable ptz patrol when event triggered.

action_ patrol _server
(only for VS series)
<product dependent>
	0~255	0	6/6	Indicate the target servers to which the snapshots taken during patrol dwelling time should be sent.
				One bit represents one application server (server_i0~i4).
				bit0 (LSB) = server_i0.
				bit1 = server_i1.
				bit2 = server_i2.
				bit3 = server_i3.
				bit4 = server_i4.
				For example, enable server_i0, server_i2, and server_i4 as notification servers; the notifyserver value is 21.

7.26 Server setting for event action

Group: **server_i**<0~4>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	email, ftp, http, ns	email	6/6	Indicate the server type: "email" = email server "ftp" = FTP server "http" = HTTP server "ns" = network storage
http_url	string[128]	http://	6/6	URL of the HTTP server to upload.
http_username	string[64]	NULL	6/6	Username to log in to the server.
http_passwd	string[64]	NULL	6/6	Password of the user.
ftp_address	string[128]	NULL	6/6	FTP server address.
ftp_username	string[64]	NULL	6/6	Username to log in to the server.
ftp_passwd	string[64]	NULL	6/6	Password of the user.
ftp_port	0~65535	21	6/6	Port to connect to the server.
ftp_location	string[128]	NULL	6/6	Location to upload or store the media.
ftp_passive	0, 1	1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode
email_address	string[128]	NULL	6/6	Email server address.
email_sslmode	0, 1	0	6/6	Enable support SSL.
email_port	0~65535	25	6/6	Port to connect to the server.
email_username	string[64]	NULL	6/6	Username to log in to the server.
email_passwd	string[64]	NULL	6/6	Password of the user.
email_senderemail	string[128]	NULL	6/6	Email address of the sender.
email_recipientemail	string[128]	NULL	6/6	Email address of the recipient.
ns_location	string[128]	NULL	6/6	Location to upload or store the media.
ns_username	string[64]	NULL	6/6	Username to log in to the server.
ns_passwd	string[64]	NULL	6/6	Password of the user.

ns_workgroup	string[64]	NULL	6/6	Workgroup for network storage.

7.27 Media setting for event action

Group: **media_i<0~4>** (media_freespace is used internally.)

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	snapshot, systemlog, videoclip, recordmsg	snapshot	6/6	Media type to send to the server or store on the server.
snapshot_source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
snapshot_prefix	string[16]	Snapshot i<0~4>_	6/6	Indicate the prefix of the filename.
snapshot_datesuffix	0, 1	0	6/6	Add date and time suffix to filename: 1 = Add date and time suffix. 0 = Do not add.
snapshot_preevent	0 ~ 7	1	6/6	Indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	1	6/6	The number of post-event images.
videoclip_source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
videoclip_prefix	string[16]	VideoClip i<0~4>_	6/6	Indicate the prefix of the filename.

videoclip_preevent	0 ~ 9	0	6/6	Indicates the time for pre-event recording in seconds.
videoclip_maxduration	1 ~ 10	5	6/6	Maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 4096	500	6/6	Maximum size of one video clip file in Kbytes.

7.28 Recording

Group: **recording_i**<0~1>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry.
trigger	schedule, networkfail	schedule	6/6	The event trigger type schedule: The event is triggered by schedule networkfail: The event is triggered by the failure of network connection.
enable	0, 1	0	6/6	Enable or disable this recording.
priority	0, 1, 2	1	6/6	Indicate the priority of this recording: “0” indicates low priority. “1” indicates normal priority. “2” indicates high priority.
source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
limitsize	0,1	0	6/6	0: Entire free space mechanism 1: Limit recording size mechanism
cyclic	0,1	0	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	0,1	1	6/6	0: Disable recording notification 1: Enable recording notification

notifyserver	0~31	0	6/6	Indicate which notification server is scheduled.
				One bit represents one application server (server_i0~i4).
				bit0 (LSB) = server_i0.
				bit1 = server_i1.
				bit2 = server_i2.
				bit3 = server_i3.
				bit4 = server_i4.
				For example, enable server_i0, server_i2, and server_i4 as notification servers; the notifyserver value is 21.

weekday	0~127	127	6/6	Indicate which weekday is scheduled.
				One bit represents one weekday.
				bit0 (LSB) = Saturday
				bit1 = Friday
				bit2 = Thursday
				bit3 = Wednesday
				bit4 = Tuesday
				bit5 = Monday
				bit6 = Sunday
				For example, to detect events on Friday and Sunday, set weekday as 66.

begintime	hh:mm	00:00	6/6	Start time of the weekly schedule.
endtime	hh:mm	24:00	6/6	End time of the weekly schedule. (00:00~24:00 indicates schedule always on)
prefix	string[16]	NULL	6/6	Indicate the prefix of the filename.
cyclesize	20~	100	6/6	The maximum size for cycle recording in Kbytes when choosing to limit recording size.
reserveamount	15~	100	6/6	The reserved amount in Mbytes when choosing cyclic recording mechanism.

dest	cf, 0~4	cf	6/6	The destination to store the recorded data. "cf" means CF card. "0~4" means the index of the network storage.
cffolder	string[128]	NULL	6/6	Folder name.
filesize <product dependent>	1024~307200 <product dependent>	102400 <product dependent>	6/6	Unit: Kilo bytes. When this condition is reached, recording file is truncated.
duration <product dependent>	60~600 <product dependent>	60 <product dependent>	6/6	Uuit: Second When this condition is reached, recording file is truncated.
adaptive_enable <product dependent>	0,1	0	6/6	Indicate whether the adaptive recording is enabled
adaptive_preevent <product dependent>	0~9	1	6/6	Indicate when is the adaptive recording started before the event trigger point (seconds)
adaptive_postevent <product dependent>	0~10	1	6/6	Indicate when is the adaptive recording stopped after the event trigger point (seconds)

7.29 HTTPS

Group: **https** (product dependent)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	To enable or disable secure HTTP.
policy	<Boolean>	0	6/6	If the value is 1, it will force HTTP connection redirect to HTTPS connection

method	auto,
	manual,
	install
		auto	6/6	auto => Create self-signed certificate automatically.
				manual => Create self-signed certificate manually.
				install => Create certificate request and install.

status	-3 ~ 1	0	6/7	Specify the https status. -3 = Certificate not installed -2 = Invalid public key -1 = Waiting for certificate 0 = Not installed 1 = Active
countryname	string[2]	TW	6/6	Country name in the certificate information.
stateorprovincename	string[128]	Asia	6/6	State or province name in the certificate information.
localityname	string[128]	Asia	6/6	The locality name in the certificate information.
organizationname	string[64]	Vivotek.Inc	6/6	Organization name in the certificate information.
unit	string[32]	Vivotek.Inc	6/6	Organizational unit name in the certificate information.
commonname	string[64]	www.vivotek.com	6/6	Common name in the certificate information.
validdays	0 ~ 3650	3650	6/6	Valid period for the certification.

7.30 Storage management setting

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

Group: **disk_i<0~(n-1)>** n is the total number of storage devices.

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

7.31 Region of interest (IP8332 ONLY)

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

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
s<0~(m-1)>_home	<coordinate>	0,0 320,200 0,0	6/6	ROI left-top corner coordinate.
s<0~(m-1)>_size	<window size>	1280x800 640x400 1280x800	6/6	ROI width and height. The width value must be multiples of 16 and the height value must be multiples of 8

7.32 ePTZ setting

Group: **eptz_c<0~(n-1)>** for n channel product. (capability.eptz > 0)

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

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

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

8. Useful Functions

8.1 Query Status of the Digital Input

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

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

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

Return:

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

where <*state*> can be 0 or 1.

Example: Query the status of digital input 1 .

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

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
Di1=1\r\n
```

8.2 Capture Single Snapshot

Note: This request requires Normal User privileges.

Method: GET/POST

Syntax:

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

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

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

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

Return:

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

<binary JPEG image data>
```

8.3 Account Management

Note: This request requires Administrator privileges.

Method: GET/POST

Syntax:

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

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

8.4 System Logs

Note: This request require Administrator privileges.

Method: GET/POST

Syntax:

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

Server will return the most up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n
```

8.5 Upgrade Firmware

Note: This request requires Administrator privileges.

Method: POST

Syntax:

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

Post data:

```
fimage=<file name>[&return=<return page>]\r\n
\r\n
<multipart encoded form data>
```

Server will accept the file named <file name> to upgrade the firmware and return with <return page> if indicated.

8.6 ePTZ Camera Control (capability.eptz > 0)

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/camctrl/eCamCtrl.cgi?channel=<value>&stream=<value>
[&move=<value>] – Move home, up, down, left, right
[&auto=<value>] – Auto pan, patrol
[&zoom=<value>] – Zoom in, out
[&zooming=<value>&zs=<value>] – Zoom without stopping, used for joystick
[&vx=<value>&vy=<value>&vs=<value>] – Shift without stopping, used for joystick
[&x=<value>&y=<value>&videosize=<value>&resolution=<value>&stretch=<value>] – Click on image
(Move the center of image to the coordination (x,y) based on resolution or videosize.)
[ [&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>] ] – Set
  speeds
[&return=<return page>]
```

Example:

http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=0&move=right

http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&vx=2&vy=2&vz=2

http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&x=100&y=100&videosize=640x480&resolution=640x480&stretch=0

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

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

8.7 ePTZ Recall (capability.eptz > 0)

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

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

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

8.8 ePTZ Preset Locations (capability.eptz > 0)

Note: This request requires Operator privileges.

Method: GET/POST

Syntax:

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

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

		path according to the current path.

8.9 IP Filtering

Note: This request requires Administrator access privileges.

Method: GET/POST

Syntax:

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

PARAMETER	VALUE	DESCRIPTION
Method	addallow	Add allowed IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	adddeny	Add denied IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	deleteallow	Remove allowed IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
	deletedeny	Remove denied IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start	<ip address>	The starting IP address to add or to delete.
end	<ip address>	The ending IP address to add or to delete.
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.10 Event/Control HTTP Tunnel Channel

Note: This request requires Administrator privileges.

Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/admin/ctrlevent.cgi
------------------------------------------------------------------------
GET /cgi-bin/admin/ctrlevent.cgi
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache

------------------------------------------------------------------------
POST /cgi-bin/admin/ ctrlevent.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
```

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through the proxy server.

This channel will help perform real-time event subscription and notification as well as camera control more efficiently. The event and control formats are described in another document.

See Event/control tunnel spec for detail information

8.11 Get SDP of Streams

Note: This request requires Viewer access privileges.

Method: GET/POST

Syntax:

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

“m” is the stream number.

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

You can get the SDP by HTTP GET.

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

8.12 Open the Network Stream

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

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

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

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

“m” is the stream number.

For details on streaming protocol, please refer to the “control signaling” and “data format” documents.

8.13 Senddata (capability.nuart>0)

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/senddata.cgi?
[com=<value>][&data=<value>][&flush=<value>] [&wait=<value>] [&read=<value>]
```

PARAMETER	VALUE	DESCRIPTION
com	1 ~ <max. com port number>	The target COM/RS485 port number.
data	<hex decimal data>[,<hex decimal data>]	The <hex decimal data> is a series of digits from 0 ~ 9, A ~ F. Each comma separates the commands by 200 milliseconds.
flush	yes,no	yes: Receive data buffer of the COM port will be cleared before read. no: Do not clear the receive data buffer.
wait	*1 ~ 65535*	Wait time in milliseconds before read data.
read	*1 ~ 128*	The data length in bytes to read. The read data will be in the return page.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
<hex decimal data>\r\n
```

Where hexadecimal data is digits from 0 ~ 9, A ~ F.

8.14 Storage managements (capability.storage.dbenabled=1)

Note: This request requires administrator privileges.

Method: GET and POST

Syntax:

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

The commands usage and their input arguments are as follows.

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

Command: **search**

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

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

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

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

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

Command: **delete**

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

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

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

Command: **update**

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

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

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=1&label=1&label=5
```

Ex. Update records whose key numbers are 2 and 3 to be unlocked status.

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

Command: queryStatus

PARAMETER	VALUE	DESCRIPTION
retType	xml or javascript	Optional. Ex. retype=javascript The default return message is in XML format.

Ex. Query local storage status and call for javascript format return message.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=queryStatus&retType=javascript
```

8.15 Virtual input (capability.nvi > 0)

Note: Change virtual input (manual trigger) status.

Method: GET

Syntax:

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

PARAMETER	VALUE	DESCRIPTION
vi<num>	state[(duration)nstate] Where "state" is 0, 1. “0” means inactive or normal state while “1” means active or triggered state.	Ex: vi0=1 Setting virtual input 0 to trigger state
		Ex: vi0=0(200)1 Setting virtual input 0 to normal state, waiting 200 **milliseconds**, setting it to trigger state.

	Where "nstate" is next state after duration.	Note that when the virtual input is waiting for next state, it cannot accept new requests.
return	<return page>	Redirect to the page *<return page>* after the request is completely assigned. The *<return page>* can be a full URL path or relative path according the current path. If you omit this parameter, it will redirect to an empty page.

Return Code	Description
200	The request is successfully executed.
400	The request cannot be assigned, ex. incorrect parameters. Examples: setvi.cgi?vi0=0(10000)1(15000)0(20000)1 No multiple duration. setvi.cgi?vi3=0 VI index is out of range. setvi.cgi?vi=1 No VI index is specified.
503	The resource is unavailable, ex. Virtual input is waiting for next state. Examples: setvi.cgi?vi0=0(15000)1 setvi.cgi?vi0=1 Request 2 will not be accepted during the execution time(15 seconds).

Technical Specifications

Technical Specifications

Models	IP8332 IP8332-C

System Information

CPU	Multimedia SoC (System-on-Chip)
Flash	128 MB
RAM	256 MB

Camera Features

Image Sensor	1/4" Progressive CMOS
Maximum Resolution	1280x800
Lens Type	Fixed-focal
Focal Length	f = 3.6 mm
Aperture	F1.8
Field of View	56° (horizontal) 41° (vertical) 71° (diagonal)
Shutter Time	1/5 sec. to 1/25,000 sec.
Minimum Illumination	0.3 Lux, 50 IRE (Color) 0.001 Lux, 50 IRE (B/W)
Pan/tilt/zoom Functionalities	ePTZ: 16x digital zoom (4x on IE plug-in, 4x built-in)
IR Illuminators	Built-in IR illuminators, effective up to 15 meters IR LED*12
On-board Storage	MicroSD/SDHC card slot

Video

Compression	H.264, MJPEG & MPEG-4
Maximum Frame Rate	H.264: 30 fps at 1280x800 MPEG-4: 30 fps at 1280x800 MJPEG: 30 fps at 1280x800
Maximum Streams	4 simultaneous streams
S/N Ratio	Above 50 dB
Video Streaming	Adjustable resolution, quality and bitrate Configurable video cropping for bandwidth saving
Image Settings	Adjustable image size, quality and bit rate Time stamp, text overlay, flip & mirror Configurable brightness, contrast, saturation, sharpness, white balance, exposure control, gain, backlight compensation, privacy masks Scheduled profile settings

Network

Users	Live viewing for up to 10 clients
Protocols	IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP, 802.1X
Interface	10Base-T/100 BaseTX Ethernet (RJ-45)
ONVIF	Ver. 1.02

Intelligent Video

Video Motion Detection	Triple-window video motion detection

Alarm and Event

Alarm Triggers	Video motion detection, manual trigger, digital input, periodical trigger, system boot, recording notification, camera tampering detection
Alarm Events	Event notification using digital output, HTTP, SMTP, FTP and NAS server File upload via HTTP, SMTP, FTP and NAS server

General

Connectors	RJ-45 for Network/PoE connection DC 12V power input AC 24V power input Digital input*1
LED Indicator	System power and status indicator
Power Input	24V AC 12V DC IEEE 802.3af PoE Class 2
Power Consumption	Max. 4.0 W
Dimensions	Ø: 60 mm x 170 mm (IP8332) Ø: 60 mm x 294 mm (IP8332-C)
Weight	Net: 702 g (IP8332) Net: 1,282 g (IP8332-C)
Safety Certifications	CE, LVD, FCC Class A, VCCI, C-Tick
Operating Temperature	-20°C ~ 50°C (-4°F ~ 122°F)
Warranty	24 months

System Requirements

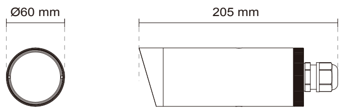
Operating System	Microsoft Windows 7/Vista/XP/2000
Web Browser	Mozilla Firefox 7~10 (streaming only) Internet Explorer 7.x or 8.x
Other Players	VLC: 1.1.11 or above QuickTime: 7 or above

Included Accessories

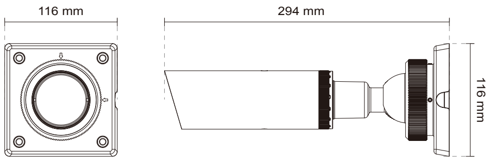
CD	User's manual, quick installation guide, Installation Wizard 2, ST7501 32-channel recording software
Others	Quick installation guide, warranty card, alignment sticker, waterproof connector, desiccant bag, RJ45 coupler, software CD Camera stand (IP8332) Cable management bracket (IP8332-C)

Dimensions

- IP8332



- IP8332-C



Compatible Accessories

Power Adapter

AA-221
DC 12V Power Adapter

PoE Kits

MS-POE-IJAF
PoE injector, 802.3af compliant

All specifications are subject to change without notice.

Distributed by:

VIVOTEK
www.vivotek.com

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

VIVOTEK USA, INC.
2050 Ringwood Avenue, San Jose, CA 95131
| **T**: 408-773-8686 | **F**: 408-773-8298 | **E**: salesusa@vivotek.com

Ver 1.0

Technology License Notice

MPEG-4 AAC Technology

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

MPEG-4 Visual Technology

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

AMR-NB Standard

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

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

Electromagnetic Compatibility (EMC)

FCC Statement

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

■ This device may not cause harmful interference, and

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

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

CE Mark Warning

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

C-Tick Warning

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

VCCI Warning

この装置は、クラスA情報装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあいます。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

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.