User's Manual

IP8352

Supreme Night Visibility • 1.3MP • 60fps

Network Camera

SUPREME
A NEW DEFINITION OF HD

VIVOTEK

Table of Contents

Overview

VIVOTEK IP8352 is a best-in-class 1.3-Megapixel bullet network camera designed for diverse outdoor applications. Incorporated with a progressive scan CMOS sensor with exceptional low lux capabilities, the IP8352 captures not only razor-sharp images of fast-moving objects during the daytime, but also offers unparalleled night visibility under low light conditions.

Equipped with VIVOTEK's self-developed next-generation SoC, the IP8352 supports high-performance H.264/MPEG-4/MJPEG compression technology and offers extra smooth video quality up to 60 fps @ 720p and 30fps @ 1.3MP. Furthermore, the IP8352 boasts a number of innovative technologies, including Activity Adaptive Streaming and Gigabit Ethernet Transmission, giving a user the utmost in bandwidth flexibility and storage efficiency.

To adapt to constantly changing lighting conditions, the IP8352 comes with a removable IR-cut filter and built-in IR illuminators for both day and night applications. Its IP67-rated housing protects the camera body against rain and dust and ensures operation under extreme weather conditions. For complete installation and prevention of tampering and vandalism, the IP8352 is also packaged with a mounting bracket that conceals all cabling.

With other advanced features such as tamper detection, 802.3af compliant PoE, MicroSD/SDHC card slot for on-board storage, Gigabit Ethernet Transmission, plus Supreme Night Visibility and 60fps high definition video quality, the IP8352 is the best choice for the most demanding outdoor surveillance applications such as parking lots, entrances, housing communities, and much more.

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

- IP8352 - the Network Camera
- Alignment Sticker
- Sun Shield, Wrench/RJ45 Female/Female Coupler/Double-sided Tape/Screws
- Power Adapter
- Wall Mount Bracket & Mounting Plate
- Waterproof Connector (Optional)
- Moisture Absorber
- Quick Installation Guide / Warranty Card
- Software CD

Symbols and Statements in this Document

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

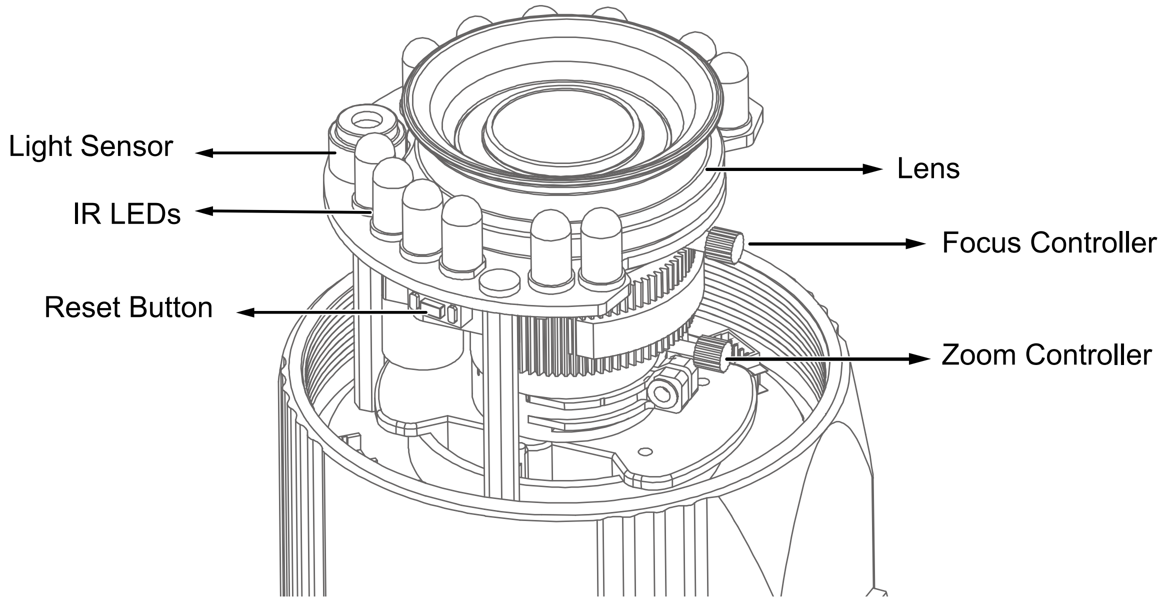
✎ **NOTE**: Notices provide guidance or advices that are related to the functional integrity of the machine.

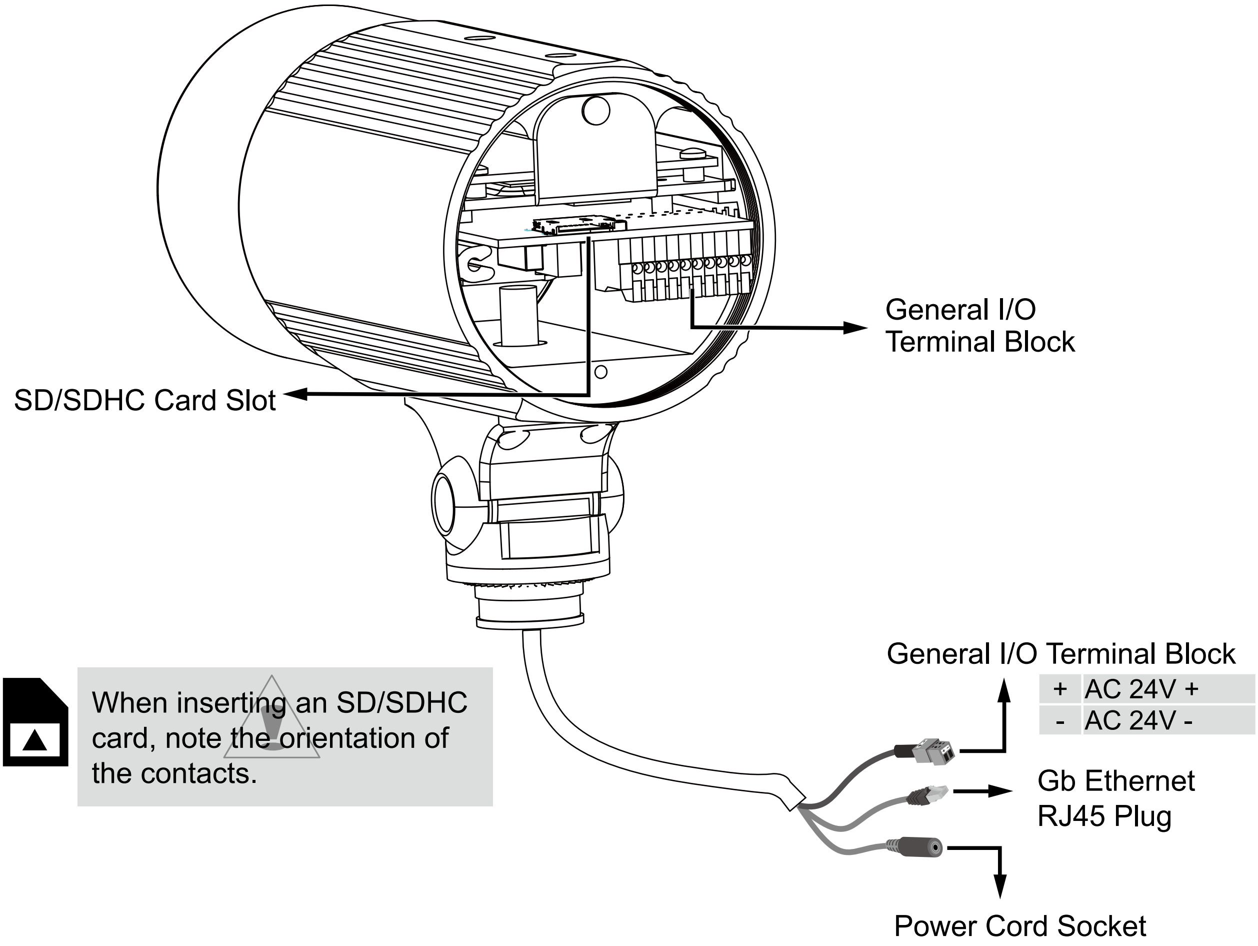
💡 **Tips**: Tips are useful information that helps enhance or facilitae an installation, function, or process.

⚠ **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



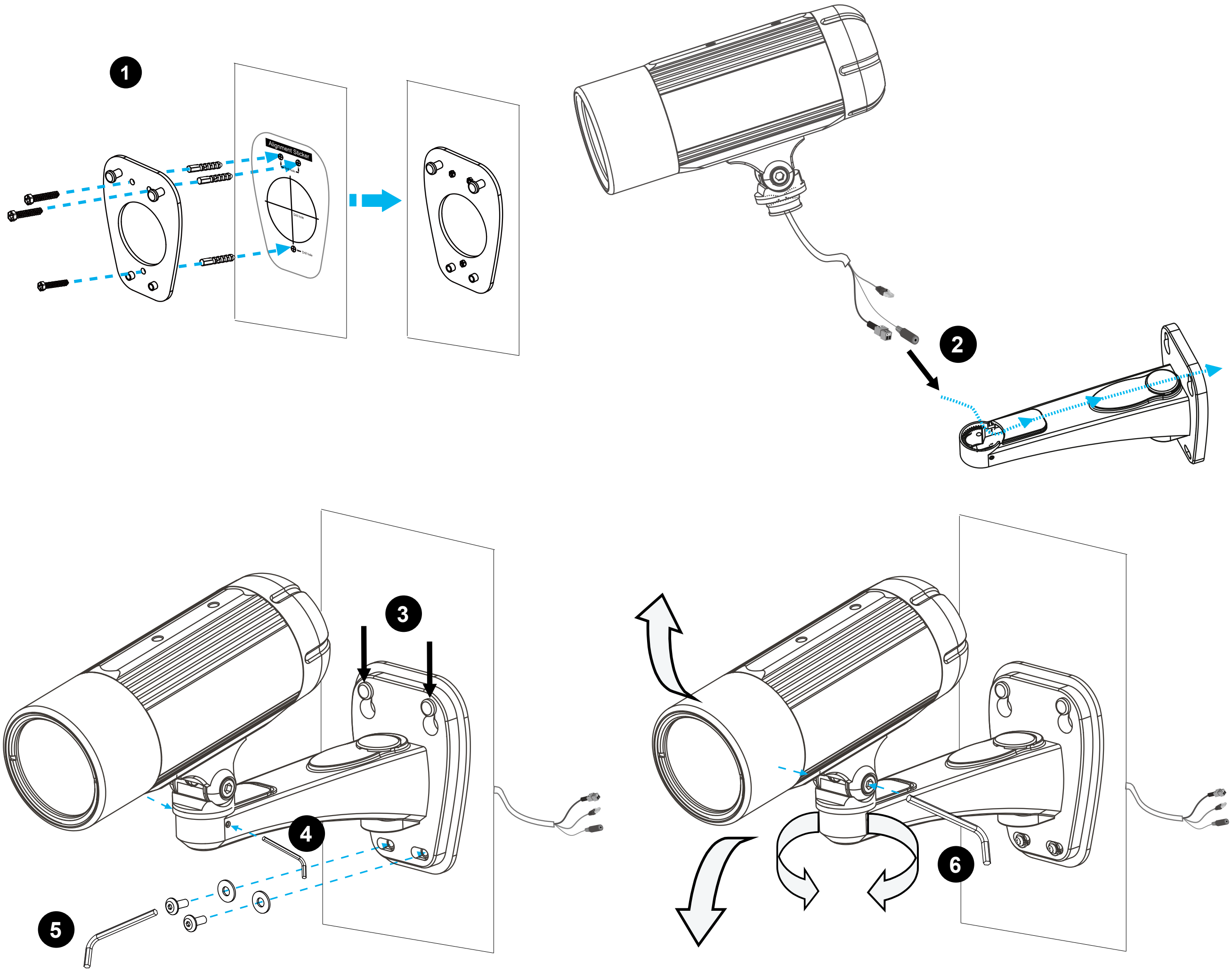


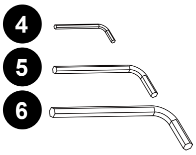
+	AC 24V +
-	AC 24V -

When inserting an SD/SDHC card, note the orientation of the contacts.

Hardware Installation

1. Attach the alignment sticker to the wall. Drill three holes into the wall. Then hammer the supplied plastic anchors into the holes and secure the plate with supplied screws.
2. Feed the cables through the front opening of the wall mount bracket. (If you want to use external devices such as sensors and alarms, please refer to the assembling steps on the next page.)
3. Hang the wall mount bracket on the plate.
4. Fix the Network Camera on the wall mount bracket with two screws on both sides.
5. Secure the wall mount bracket with the supplied screws.
6. Adjust the angle of the wall mount bracket to aim at the shooting area.

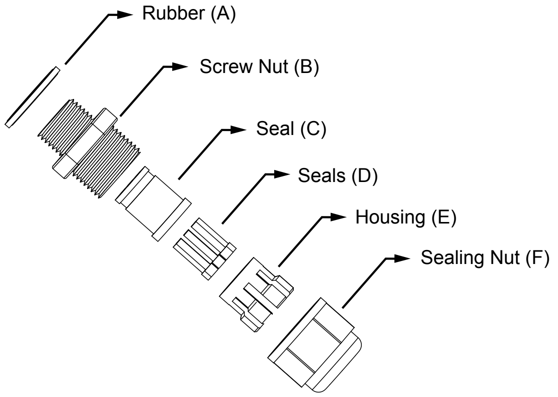




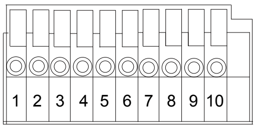
IMPORTANT!
The supplied L-type hex key wrenches are exclusively designed to match each screw. In case you will need to adjust the lens later, do not discard the wrenches.

Waterproof Connector

Components of the Waterproof Connector



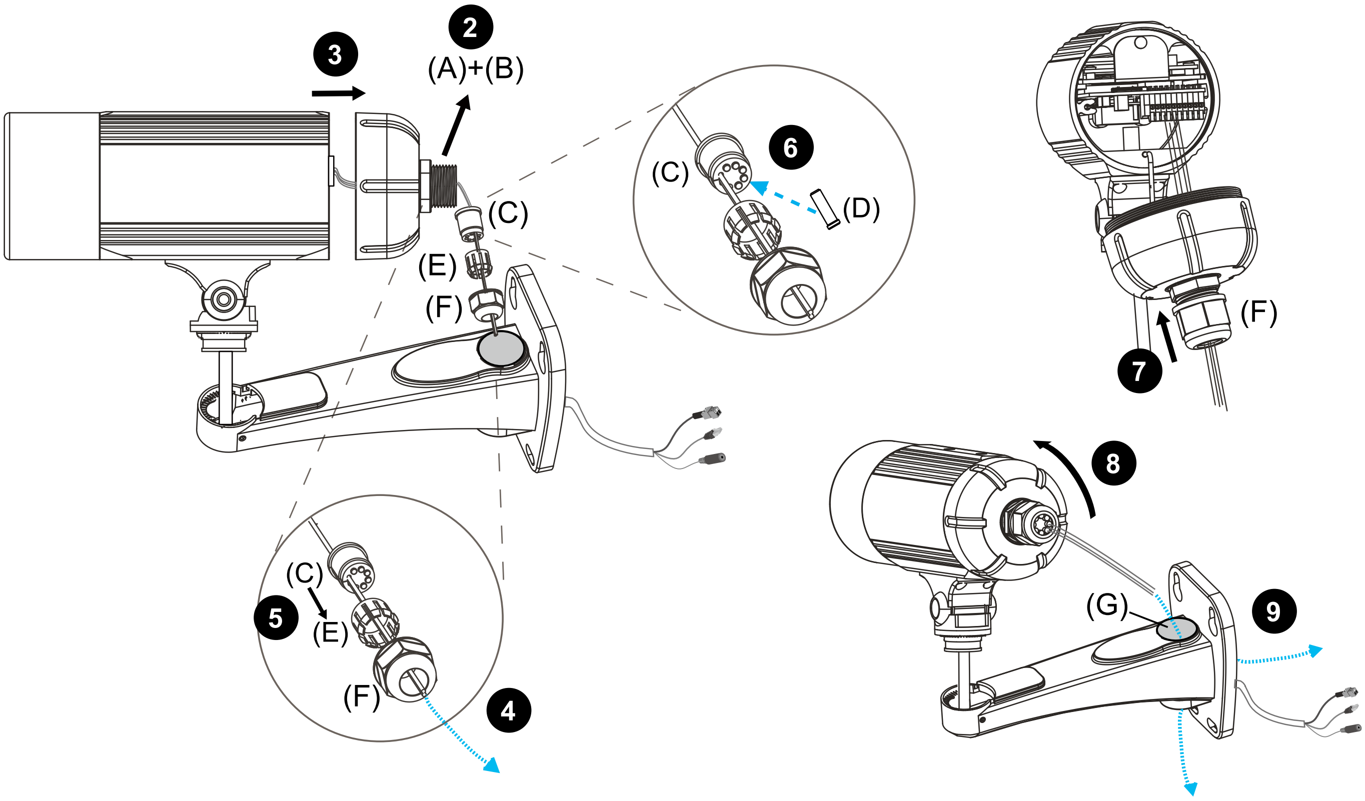
IO Block Pin Definitions



1	Power +12V
2	Digital Output
3	Digital Input
4	Ground
5	RS485 +
6	RS485 -
7	Ground
8	Audio Input
9	Ground
10	Audio Output

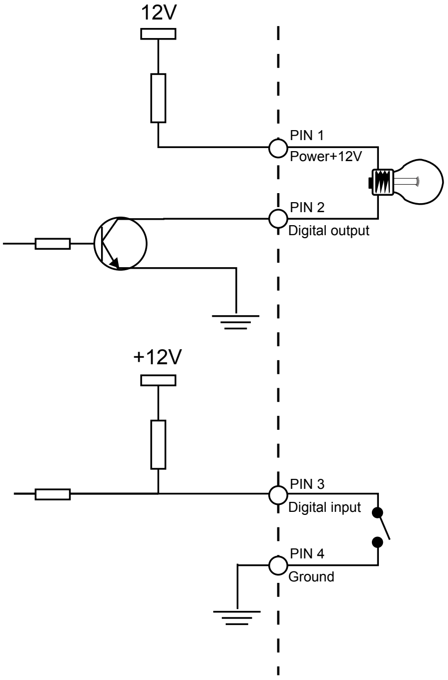
Assembling Steps

1. Disassemble the components of the waterproof connector into part (A) ~ (F) as shown above.
2. Remove the rubber stopper from the bottom of the Network Camera and secure the rubber (A) and screw nut (B) tightly.
3. Open the back cover of the Network Camera.
4. If you have external devices such as sensors and alarms, feed the cables through the waterproof connector (F --> E --> C --> A+B) as the illustration shown below. Then refer to the pin definition to connect them to the general I/O terminal block. Note: The recommended cable gauge is 2.0 ~ 2.8 mm.
5. Push the seal (C) into the housing (E).
6. Insert the seals (D) into the empty holes on the seal (C) to avoid moisture.
7. Secure the sealing nut (F) tightly.
8. Tighten the back cover.
9. Remove rubber (G) and feed the cables through the wall mount bracket.

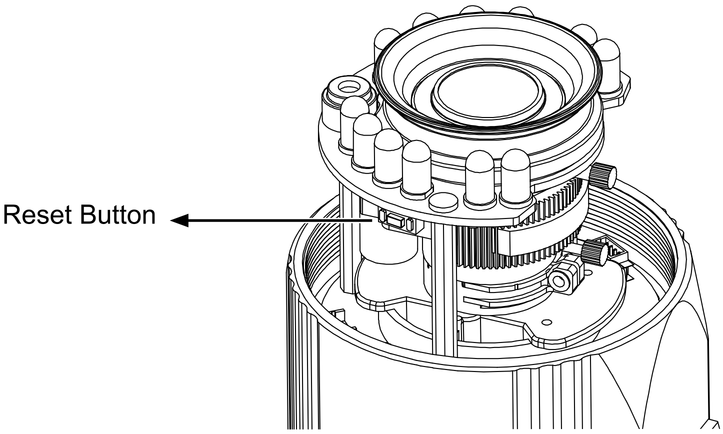


DI/DO Diagram

Please refer to the following illustration for the connection method.



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, press the reset button longer to restore the factory settings and install again.

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

Restore: Press and hold the recessed reset button for at least several seconds to restore. Note that all settings will be restored to factory defaults.

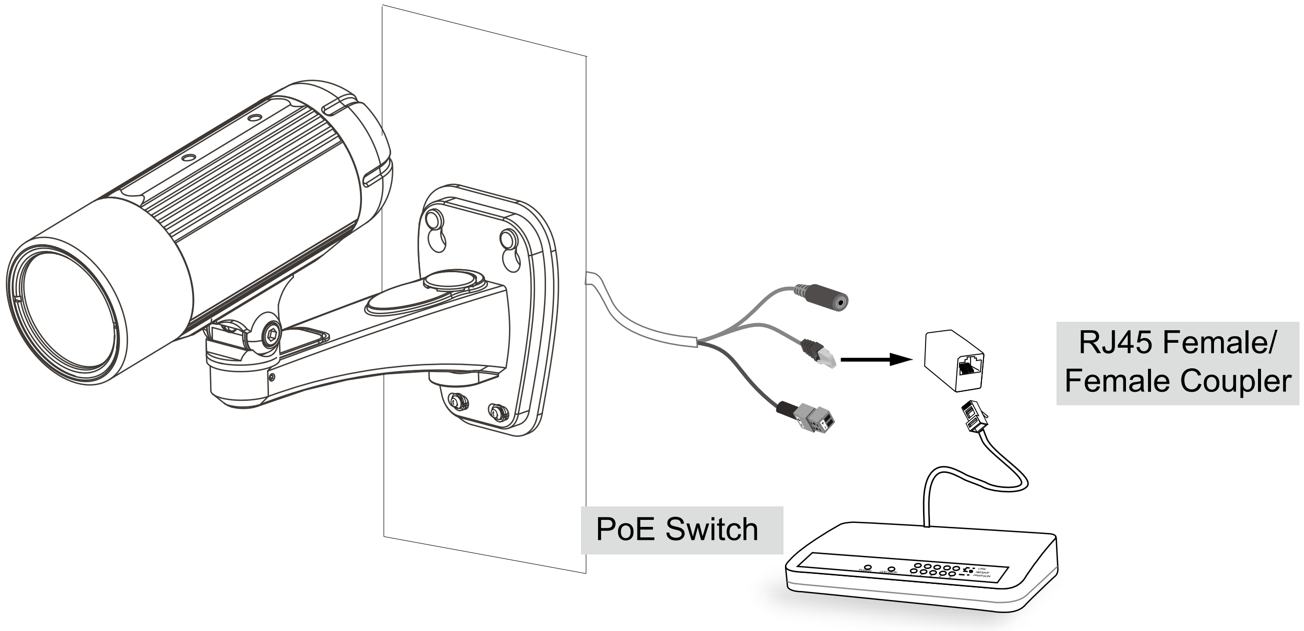
SD/SDHC Card Capacity

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

Network Deployment

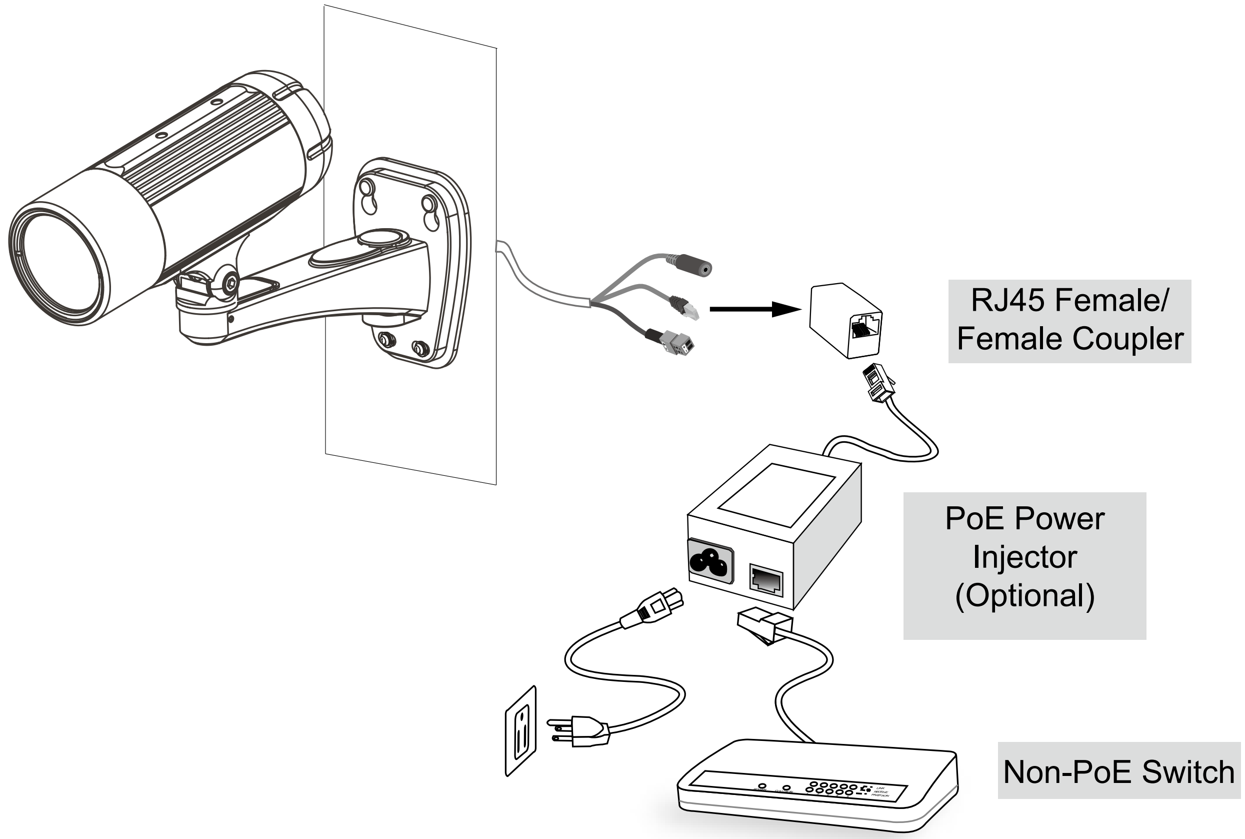
When using a PoE-enabled switch

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

Use a PoE power injector (optional) to connect between the Network Camera and a non-PoE switch.



Network Deployment

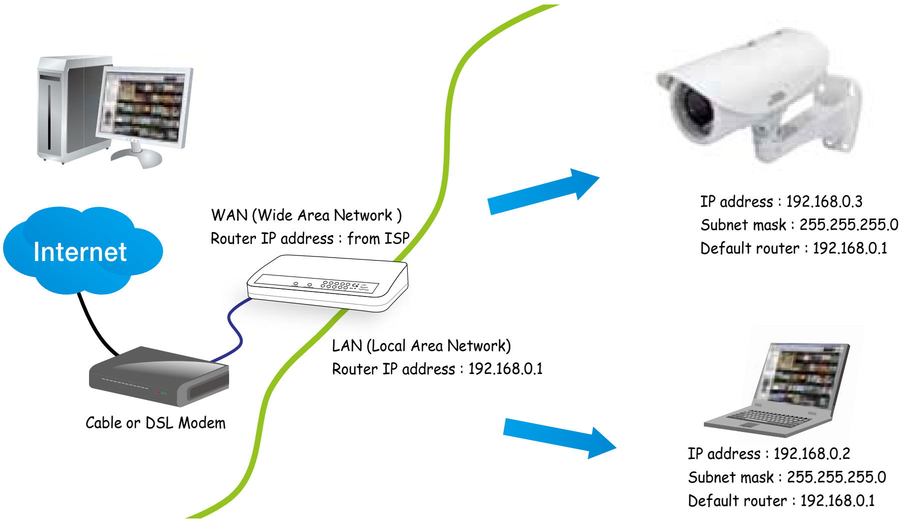
Setting up the Network Camera over the Internet

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

Internet connection via a router

Before enabling the access to 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
LAN (Local Area Network)
Router IP address : 192.168.0.1
Cable or DSL Modem
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.

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

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

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 51 for details.

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN configuration on page 51 for details.

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

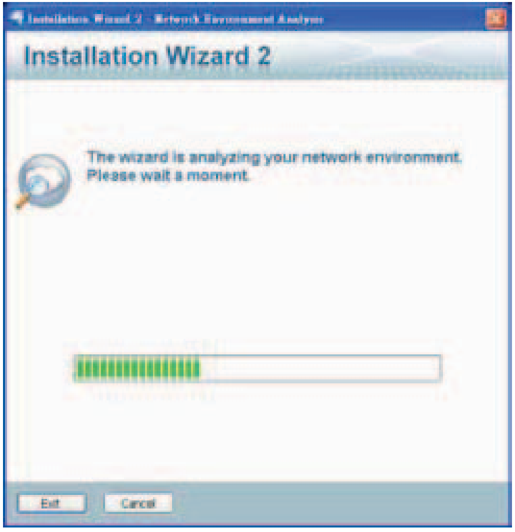
Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 49 for details.

Software Installation

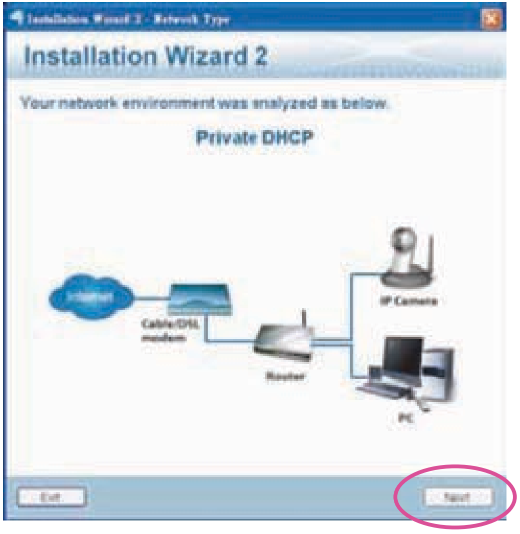
Installation Wizard 2 (IW2), free-bundled software included on the product CD, helps you set up your Network Camera on the LAN.

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

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

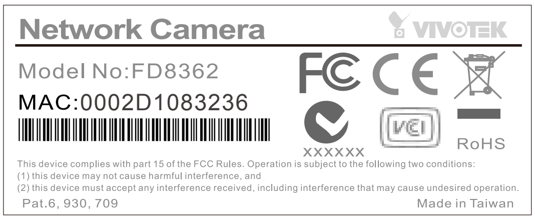

Installation Wizard 2

Your network environment was analyzed as below.

Private DHCP

3. The program will search for all VIVOTEK network devices 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

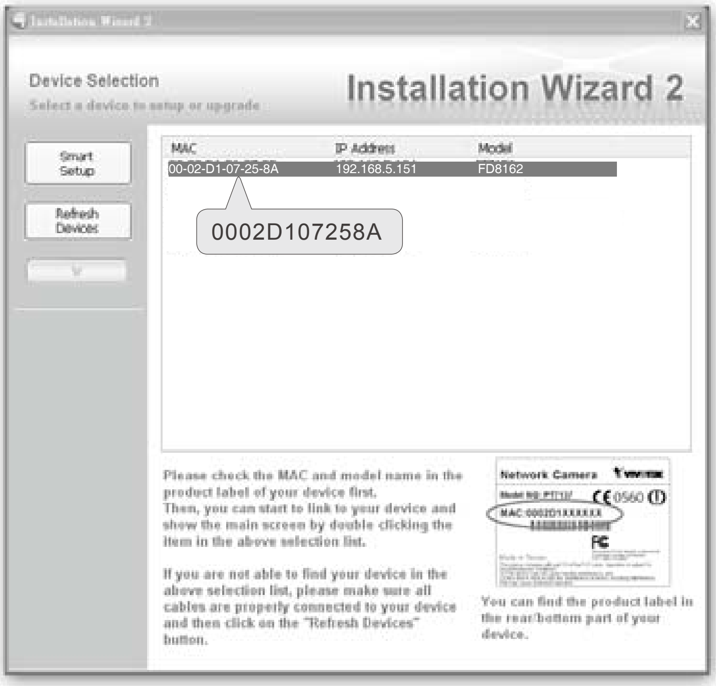
Model No:FD8362

MAC:0002D1083236

XXXXXX 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


Device Selection

Select a device to setup or upgrade

Installation Wizard 2

MAC	IP Address	Model
00-02-D1-07-25-8A	192.168.5.151	FD8162

0002D107258A

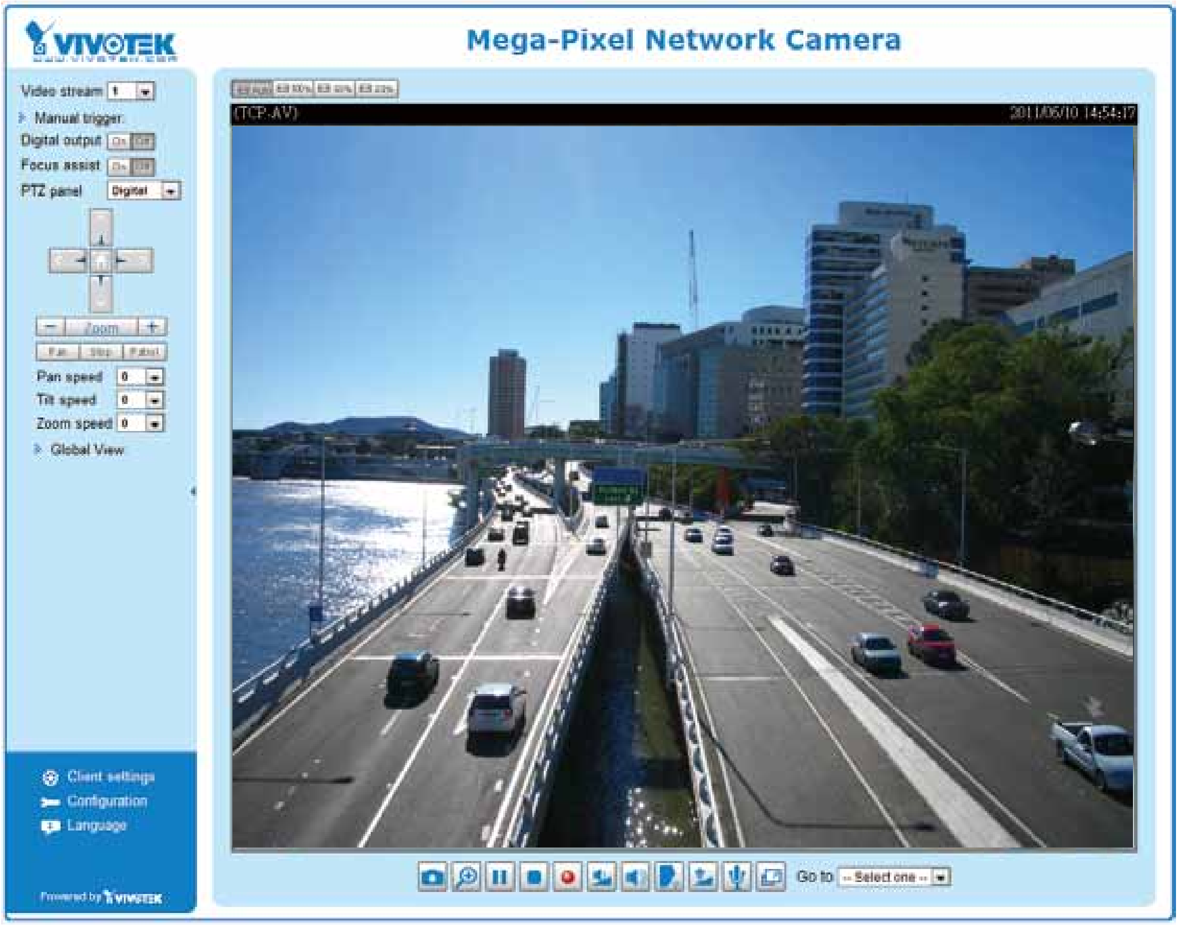
Please check the MAC and model name in the product label of your device first.
Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.

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

Digital output On Off

Focus assist On Off

PTZ panel Digital

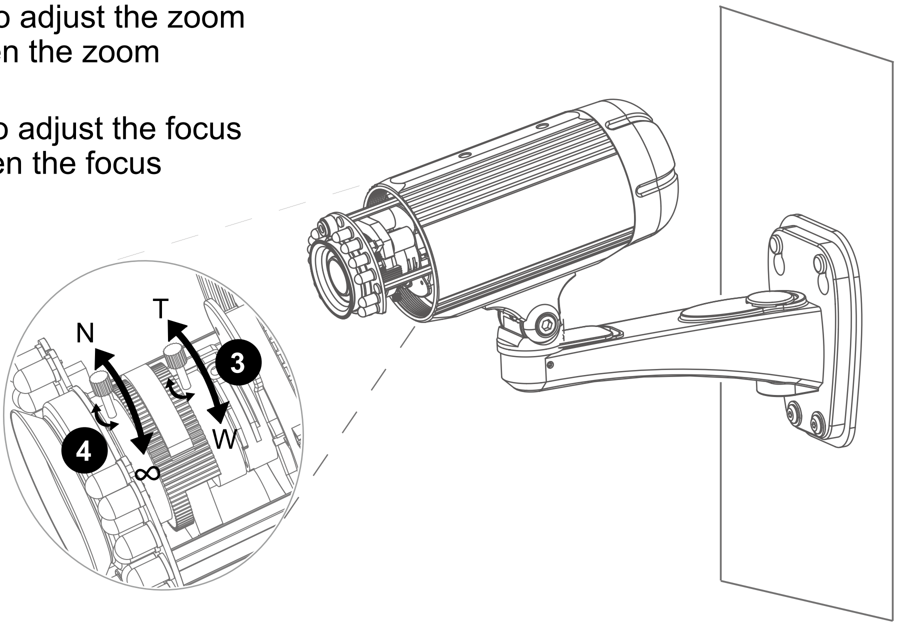
Pan speed 0

Tilt speed 0

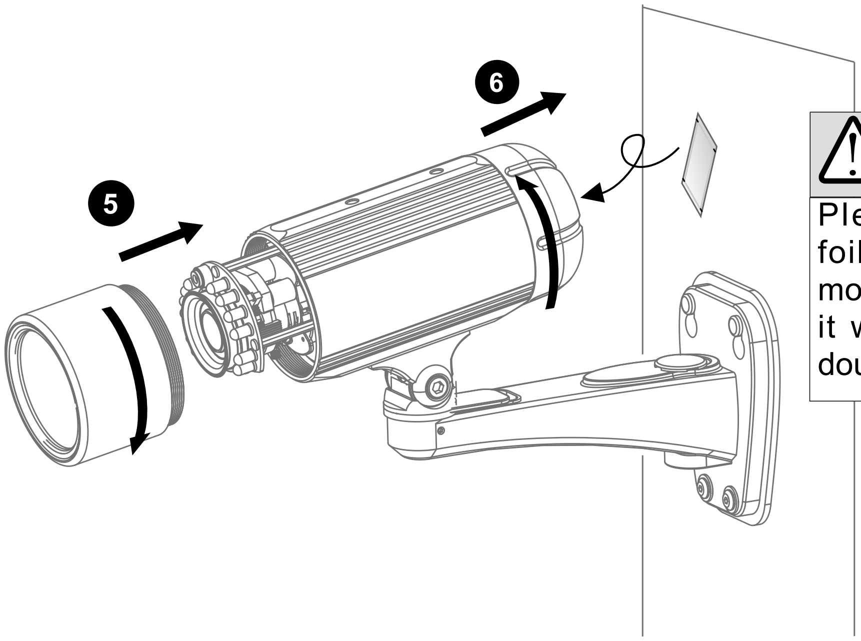
Zoom speed 0

(TCP-AV) 2011/06/10 14:54:17

3. Unscrew the zoom controller to adjust the zoom factor. Upon completion, tighten the zoom controller.
4. Unscrew the focus controller to adjust the focus range. Upon completion, tighten the focus controller.



5. Tighten the lens cover.
6. Replace the moisture absorber with a new one if you open the back cover during the installation procedure.



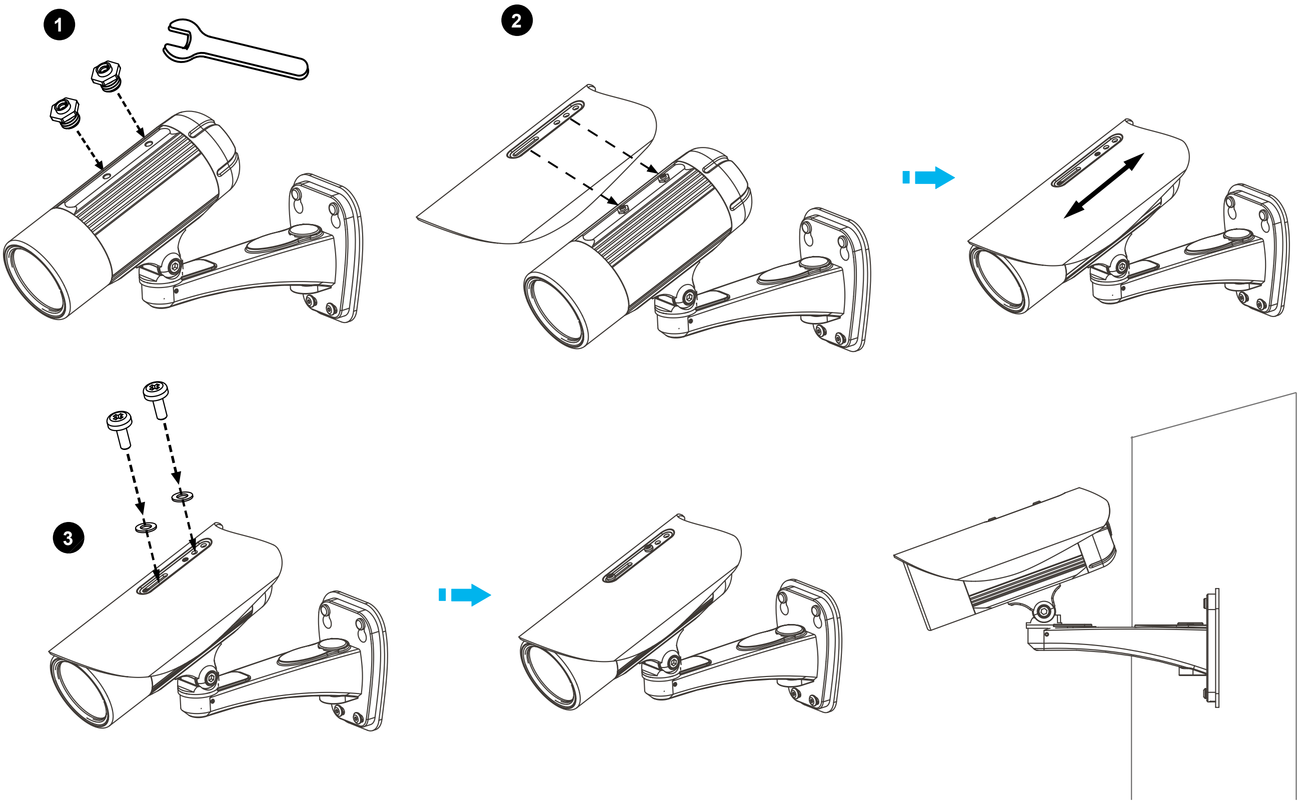
IMPORTANT!

Please tear down the aluminum foil vacuum bag and take out the moisture absorber, and then replace it with the absorber in kit using a double-sided tape.

NOTE:

If you want to use the supplied sun shield for outdoor environments, please follow the steps below to install:

1. Tighten the supplied two screws.
2. Attach the supplied sun shield to the Network Camera and slide it to the desired position.
3. Fix the sun shield with the supplied two screws.



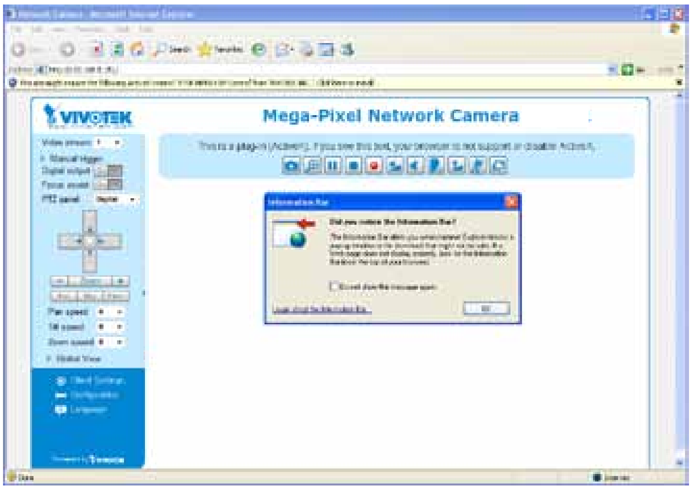
Accessing the Network Camera

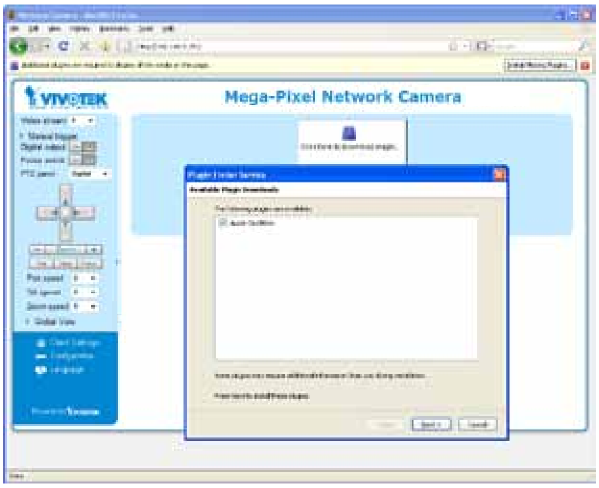
This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

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

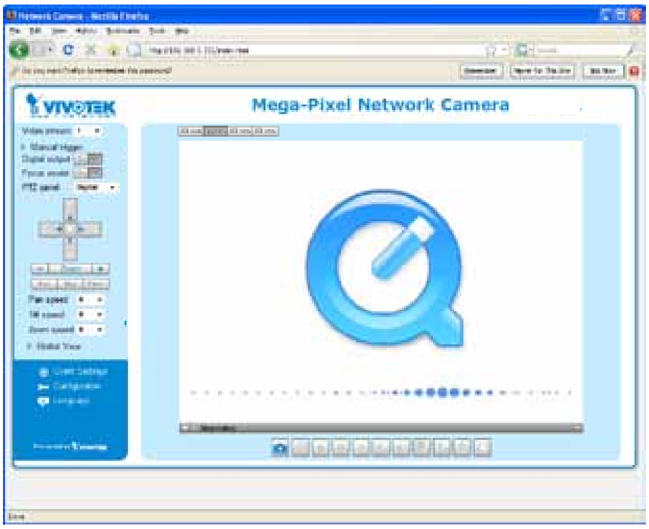
1. Launch your web browser (ex. Microsoft® Internet Explorer or Mozilla Firefox).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If it is the first time installing the VIVOTEK network camera, an information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

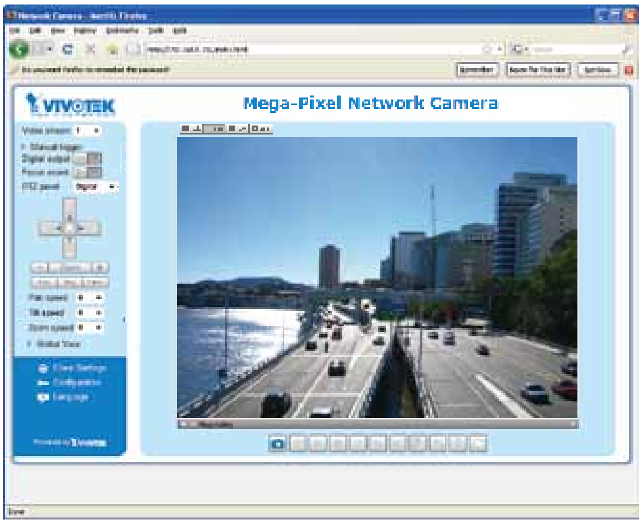




NOTE:

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



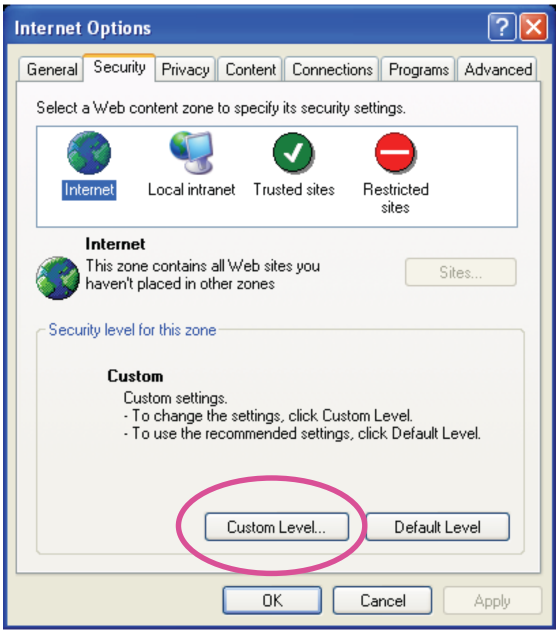


NOTE:

1. By default, your Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to configure a password for your camera later. *For more information about how to enable password protection, please refer to Security on page 40*.
2. If you see a dialogue box indicating that your security settings prohibit running ActiveX Controls®, please enable ActiveX Controls for your browser.

To enable the ActiveX® Controls for your browser:

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

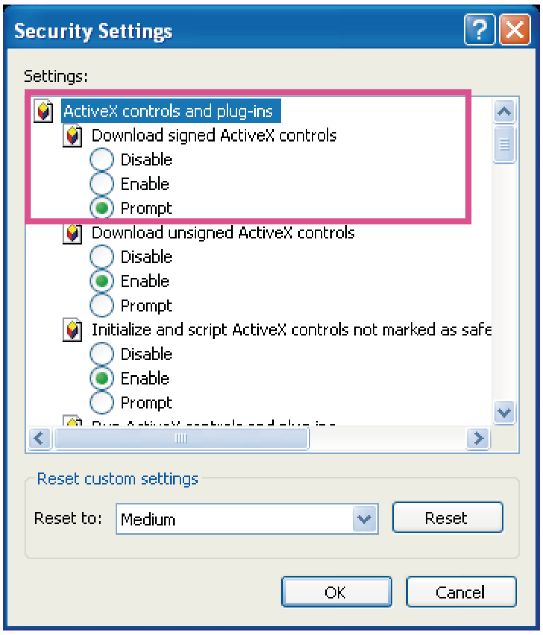


Select a Web content zone to specify its security settings.

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

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**.



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

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

Using RTSP Players

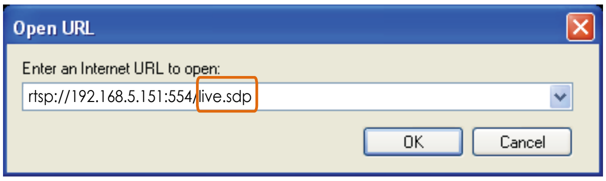
To view the H.264/MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.

- Quick Time Player
- Real Player

1. Launch the RTSP player.
2. Choose File > Open URL. A URL dialog box will prompt.
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 60.

For example:

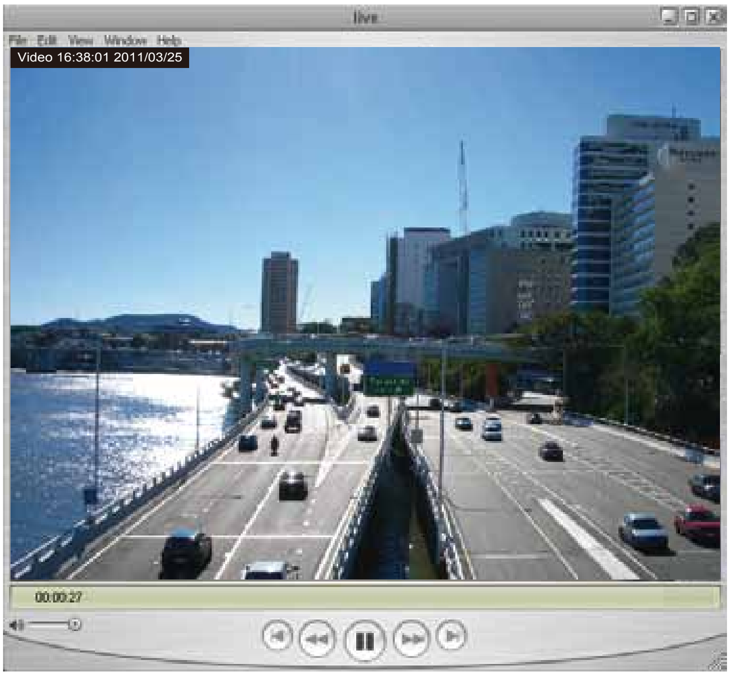


Open URL

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 60 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 11.

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 60.

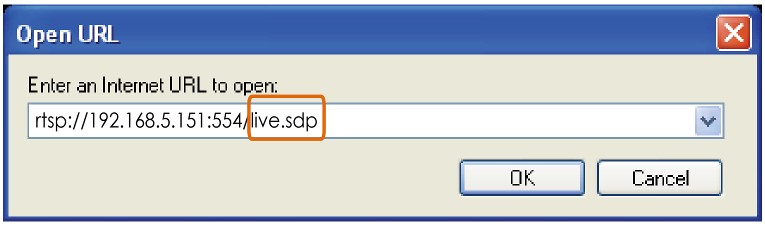
2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video and audio streaming parameters as listed below.
   For more information, please refer to Stream settings on page 77.

Video Mode	MPEG-4
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (GSM-AMR)	12.2kbps

3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 60.

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

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



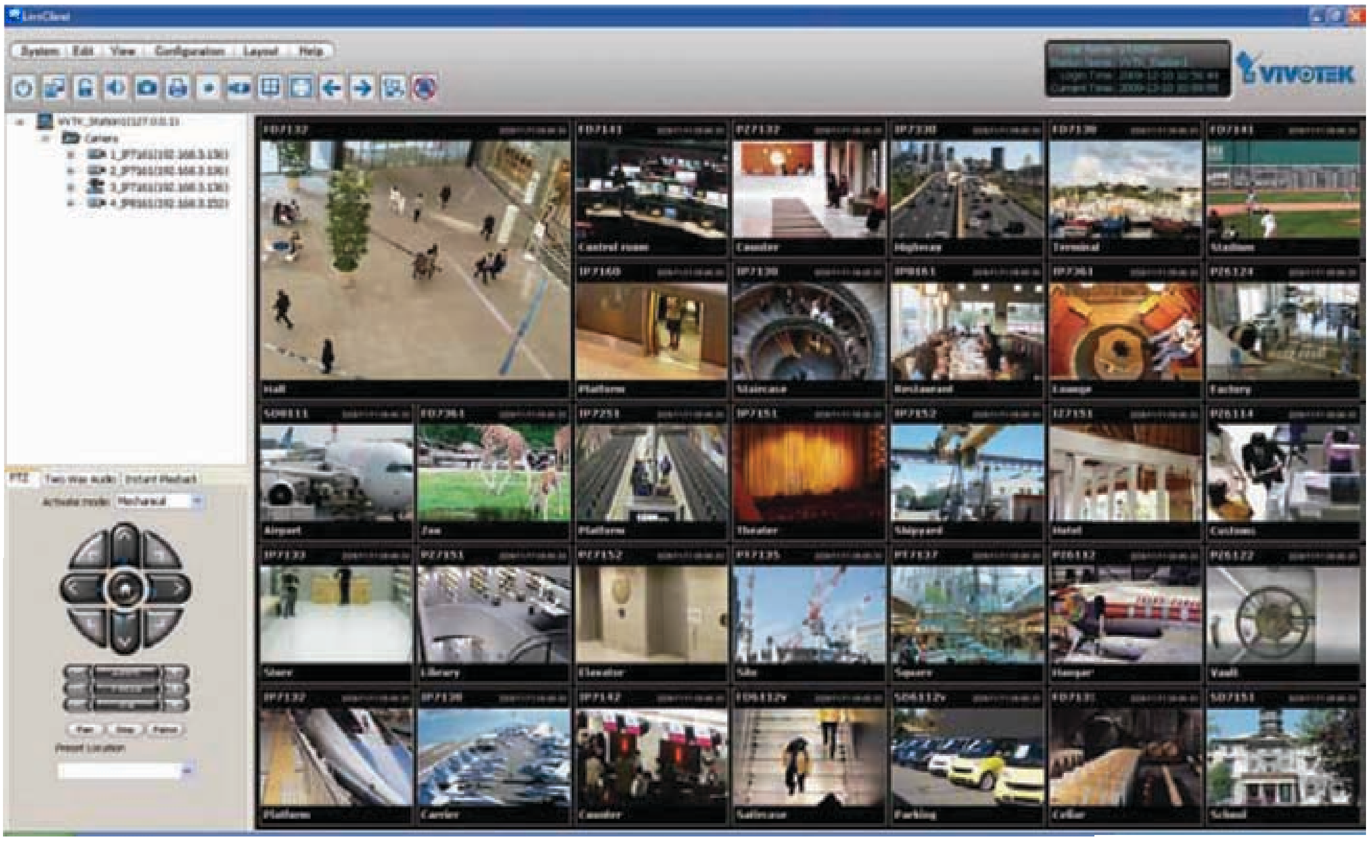
Open URL

Enter an Internet URL to open:

rtsp://192.168.5.151:554/live.sdp

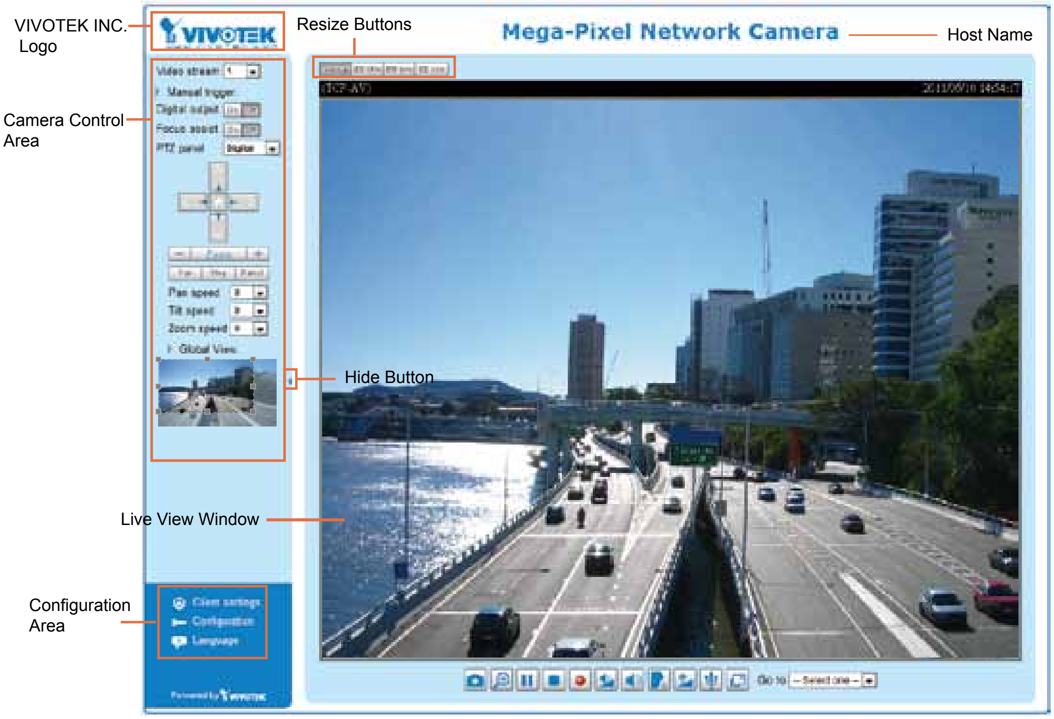
Using VIVOTEK Recording Software

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 screen elements on the main page. It is composed of the following sections: VIVOTEK INC. Logo, Host Name, Camera Control Area, Configuration Area, and Live Video Window.



VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page 29.

Camera Control Area

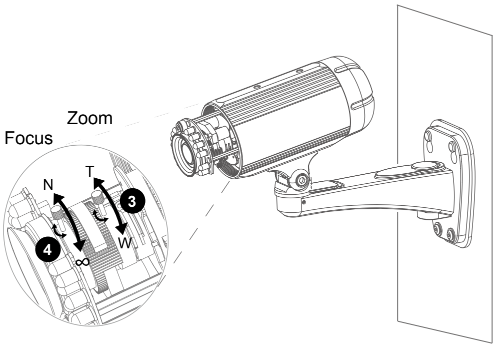
Video Stream: This Network Cmera supports multiple streams (stream 1 ~ 4) simultaneously. You can select either one for live viewing. For more information about multiple streams, please refer to page 77 for detailed information.

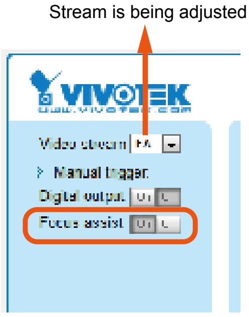
Manual Trigger: Click to enable/disable an event trigger manually. Please configure an event setting before enabling this function. A total of 3 or 4 event settings can be configured. For more information about event setting, please refer to page 85. If you want to hide this item on the homepage, please go to the **System > Homepage Layout > General settings > Customized button** to uncheck “show manual trigger button”.

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

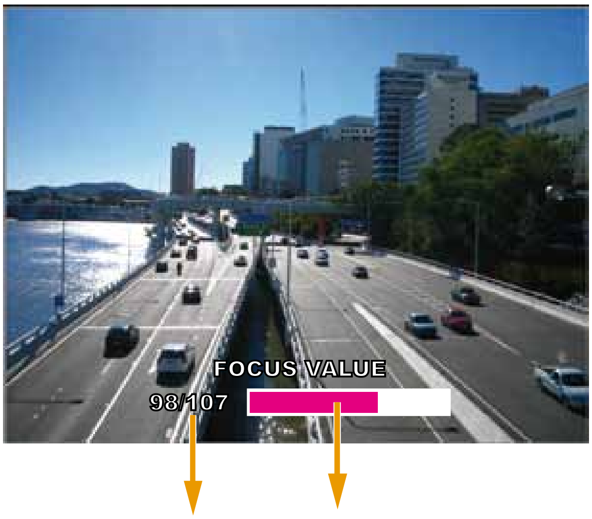
Focus Assist Button:

Follow the steps below to manually fine-tune the camera's focus.
1. Manually adjust the zoom controller of the camera lens to fix the camer's view angle.
2. Click on the "On" button of the Focus Assist function on the homepage session with the camera to start the focus assist function. The Live View window will automatically enter the full screen mode.

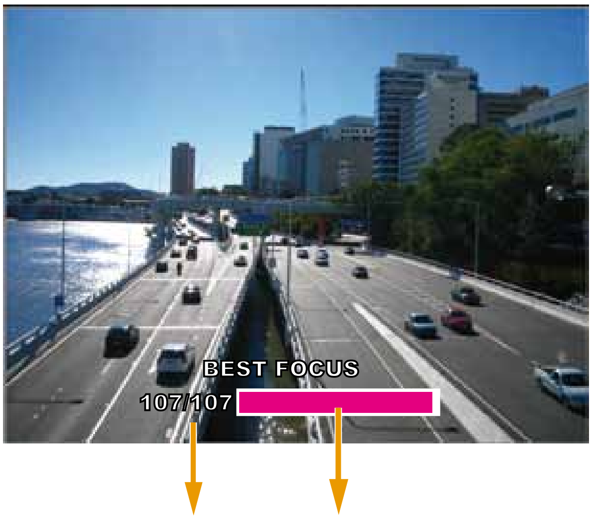




3. The floating indicator will appear at the bottom of the screen showing the calculated focus information. While you manually adjust the camera's focus, the numeric readings and the onscreen color bar should fluctuate and you should find the best results when the focus value is stated as the "BEST FOCUS."



The color bar fluctuates according to current focus value.



The color bar reaches the optimal value.

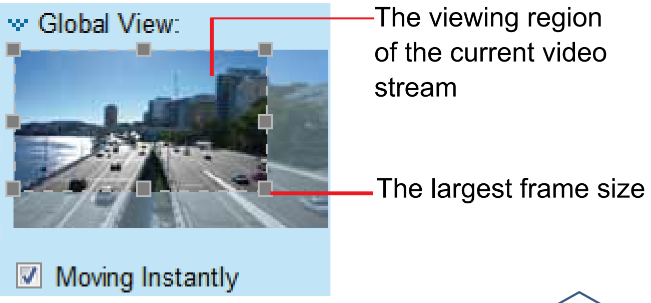
4. When done, tighten the zoom and focus controller bars, and then press the ESC key to leave the full-screen mode.
5. Turn off the focus assist function by clicking the "Off" button.

IMPORTANT!

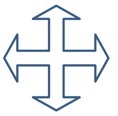
1. Before using the Focus Assist function, the camera should have been stably installed and the camera's shooting direction and view angle must be secured for a stable view. If the view is altered, you should fine-tune the camera's zoom and focus again by turning off and restarting the function.
2. Instead of a BNC connector, the camera is equipped with an AV output phone-jack that serves the same purpose for initial video adjustment. You may use the AV output to connect to a portable monitor such as a mini-DVR.

You may also refer to VIVOTEK's website for an application note on the use of this function: http://www.vivotek.com/support/appnote.php?appcon=29&appcatagory=firmware.

Global View: Click on this item to display the Global View window. The Global View window contains a full view image (the largest frame size of the captured video) and a floating frame (the viewing region of the current video stream). The floating frame allows users to control the e-PTZ function (Electronic Pan/Tilt/Zoom). For more information about e-PTZ operation, please refer to E-PTZ Operation on page 82. For more information about how to set up the viewing region of the current video stream, please refer to page 77.



To move the current view window, place your cursor on it and let the cursor change to the all-direction arrow.



all-direction arrow

Configuration Area

Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 26.

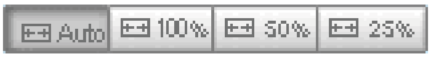
Configuration: Click this button to access more of the configuration options provided with the Network Camera. It is suggested that a password is applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to the description for the Configuration menus on page 28.

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. You can also change a language on the Configuration page; please refer to page 28.

Hide Button

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

Resize Buttons

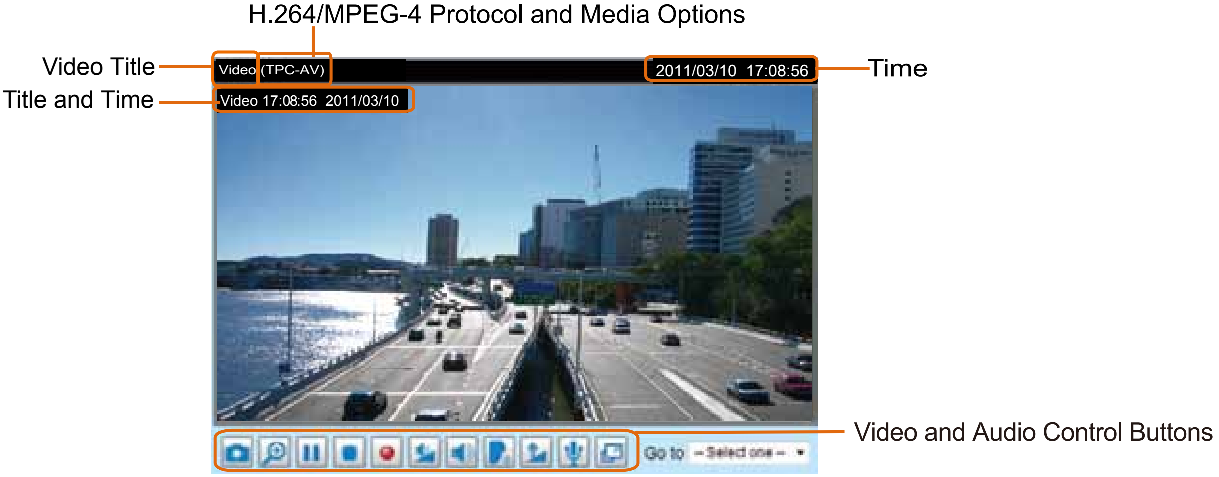


:

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

Live Video Window

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


H.264/MPEG-4 Protocol and Media Options
Video Title
Title and Time
Video (TPC-AV)
2011/03/10 17:08:56
Time
Video 17:08:56 2011/03/10
Video and Audio Control Buttons
Go to
-- Select one --

Video Title: The video title can be configured. For more information, please refer to Video settings on page 69.

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 26.

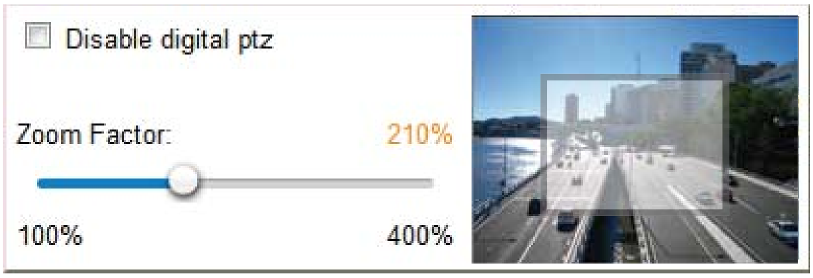
Time: Display the current time. For further configuration, please refer to Media > Image > Genral settings on page 69.

Title and Time: The video title and time can be stamped on the streaming video. For further configuration, please refer to Media > Image > Genral settings on page 69.

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

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

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



☐ Disable digital ptz

Zoom Factor: 210%

100% 400%

⏸ 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 27 for details.

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

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

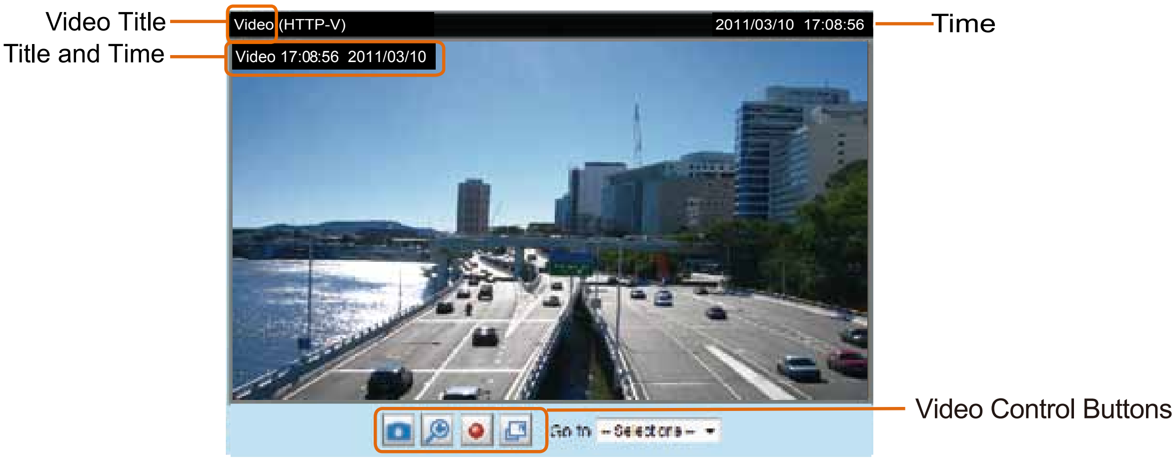
📞 Talk: Click this button to talk to people around the Network Camera. Audio will project from the external speaker connected to the Network Camera. Click this button 📞 again to end talking transmission.

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

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

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

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



Video Title: The video title can be configured. For more information, please refer to Media > Image on page 69.

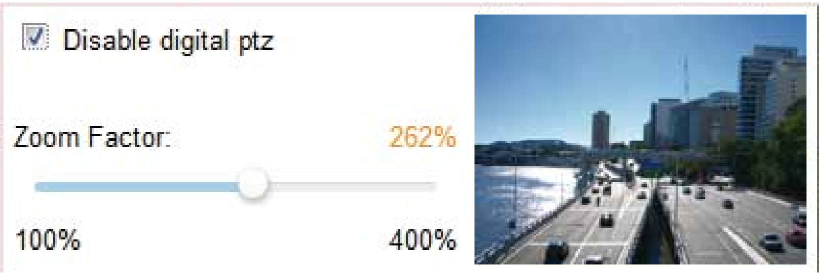
Time: Display the current time. For more information, please refer to Media > Image on page 69.

Title and Time: Video title and time can be stamped on the streaming video. For more information, please refer to Media > Image on page 69.

Video Control Buttons: Depending on the camera model and your current 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 ptz

Zoom Factor: 262%

100% 400%

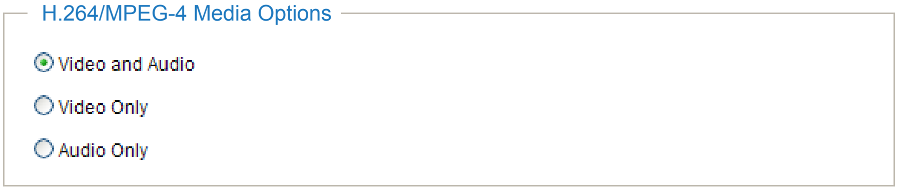
Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the ■ Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 27 for details.

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

Client Settings

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

H.264 / MPEG-4 Media Options



H.264/MPEG-4 Media Options

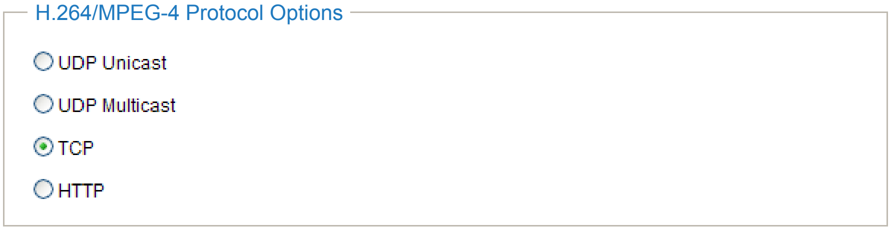
● Video and Audio

○ Video Only

○ Audio Only

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

H.264 / MPEG-4 Protocol Options



H.264/MPEG-4 Protocol Options

○ UDP Unicast

○ UDP Multicast

● TCP

○ HTTP

Depending on your network environment, there are four options with the transmission protocols with H.264 or MPEG-4 streaming:

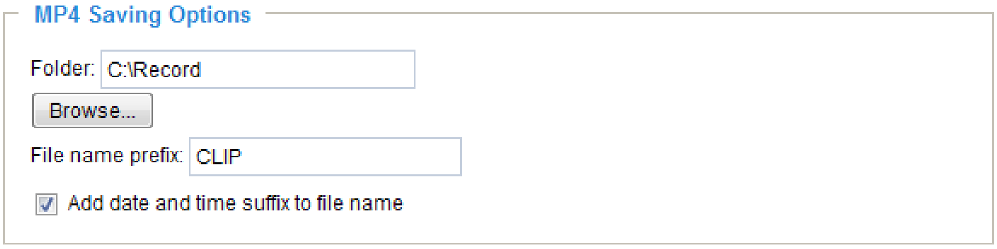
UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast 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 60.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. The downside of this protocol is that its real-time effect is not as good as that of using 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 behind a firewall can utilize this protocol to allow camera's streaming data to pass through.

MP4 Saving Options



MP4 Saving Options

Folder: C:\Record

File name prefix: CLIP

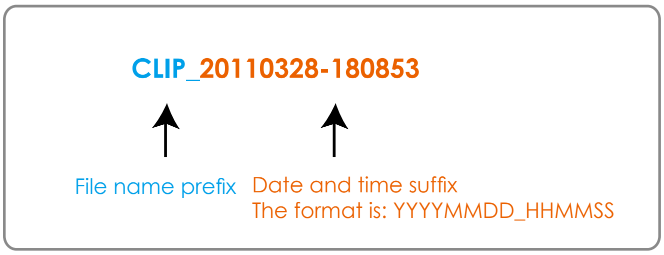
☑ Add date and time suffix to file name

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.

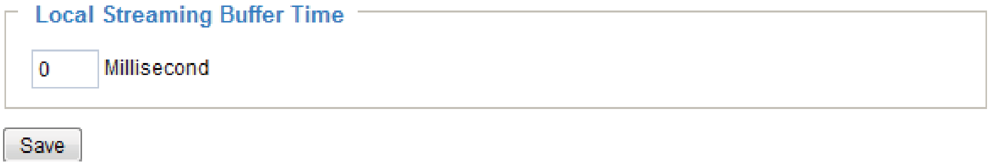
Folder: Specify a storage destination for the recorded video files.

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

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

Configuration

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

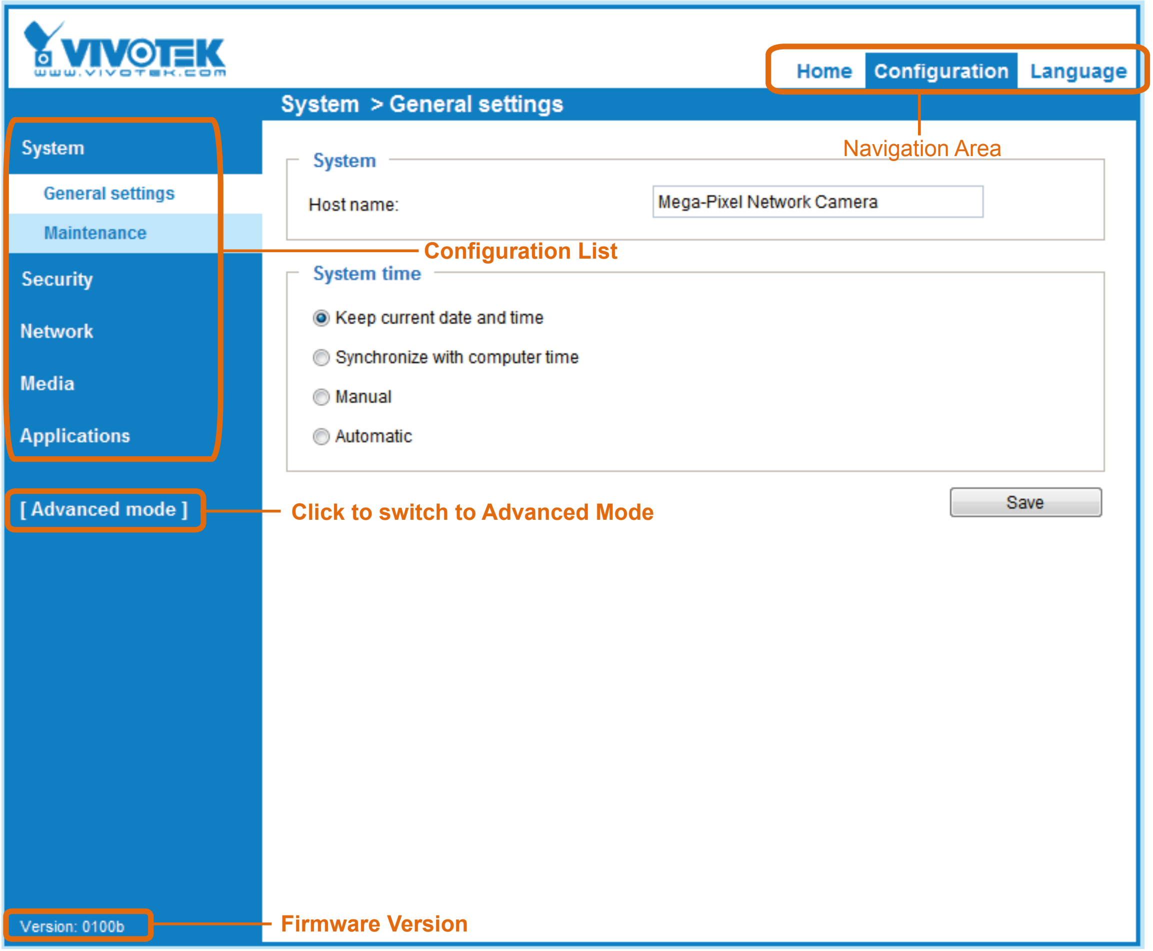
VIVOTEK offers an easy-to-use user interface that helps you set up your network camera with minimal effort. To simplify the setting procedure, two types of user interfaces are available: Advanced Mode for professional users and Basic Mode for entry-level users. Some advanced functions (PTZ/ Event/ Recording/ Local storage) are not displayed in Basic Mode.

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

In order to simplify the user interface, 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

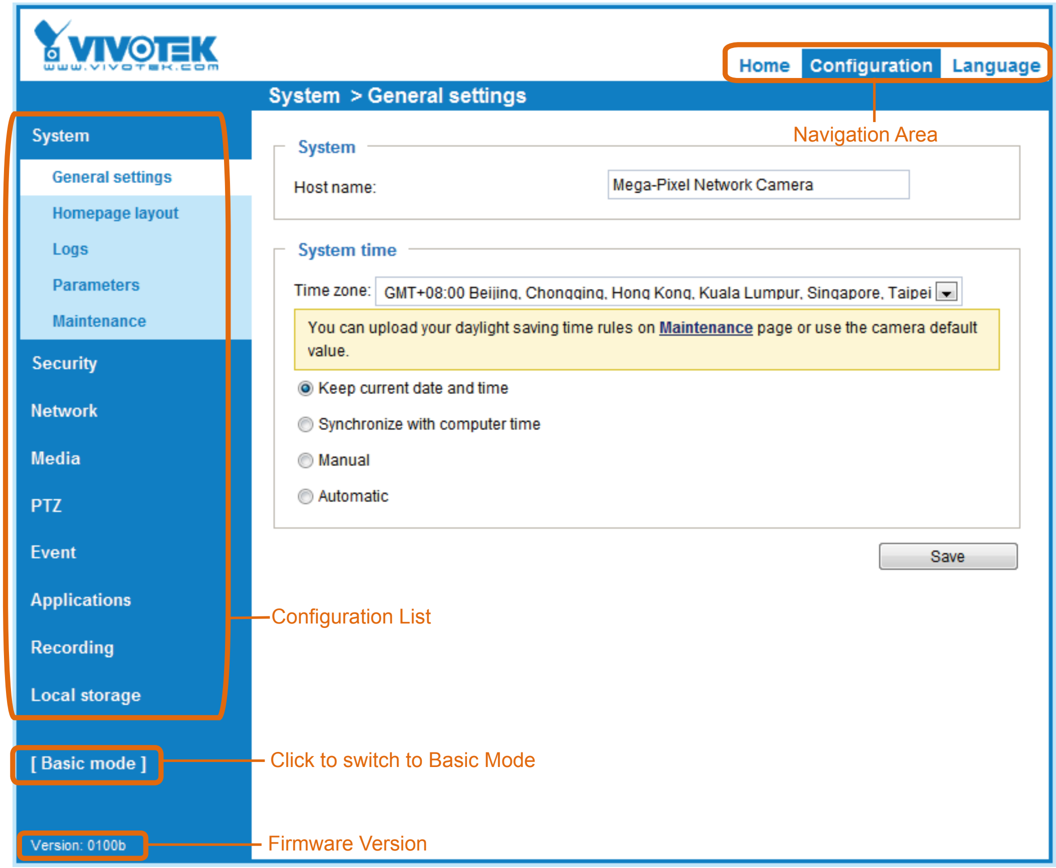
Navigation Area

Configuration List

Click to switch to Advanced Mode

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

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

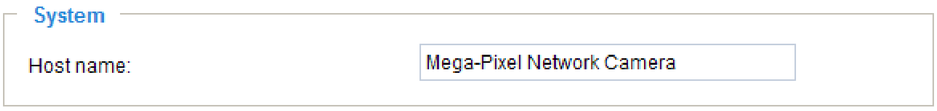
Each function on the configuration list will be explained in the following sections. Those functions that are displayed only in Advanced Mode are marked with Advanced Mode. If you want to set up advanced functions, please click on **[Advanced Mode]** at the bottom of the configuration list.

The Navigation Area provides access to all different views from the **Home** page (for live viewing), **Configuration** page, and multi-language selection.

System > General settings

This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following two columns: System and System Time.

System

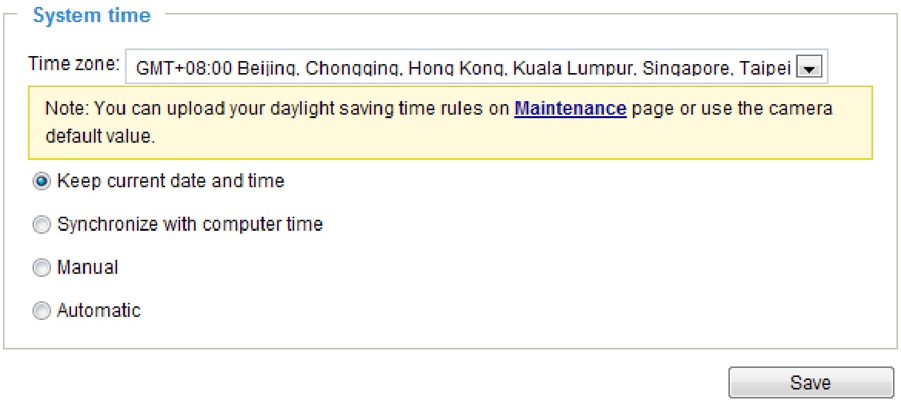


System

Host name: Mega-Pixel Network Camera

Host name: Enter a desired name for the Network Camera. The name will be displayed at the top center 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.

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

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

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

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

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

Time zone Advanced Mode: Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules, please refer to **System > Maintenance > Import/ Export files** on page 37 for details.

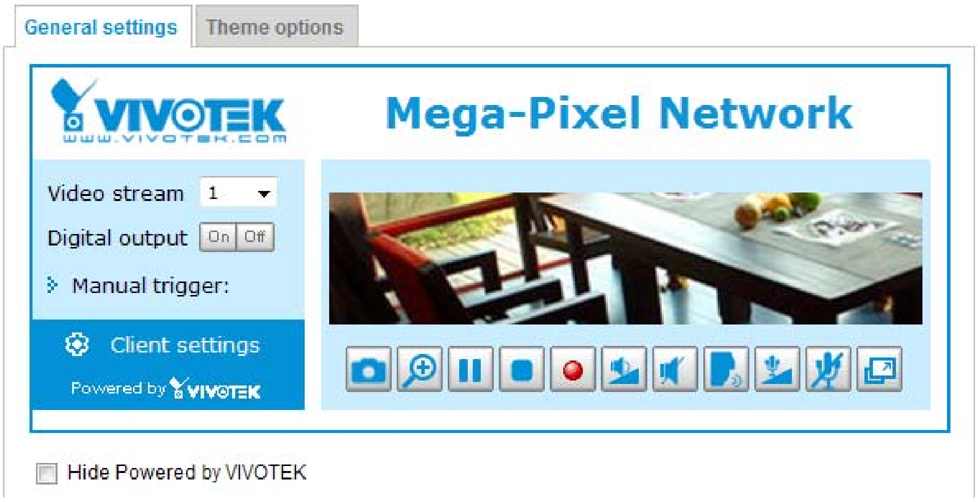
When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

System > Homepage layout Advanced Mode

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

General settings

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

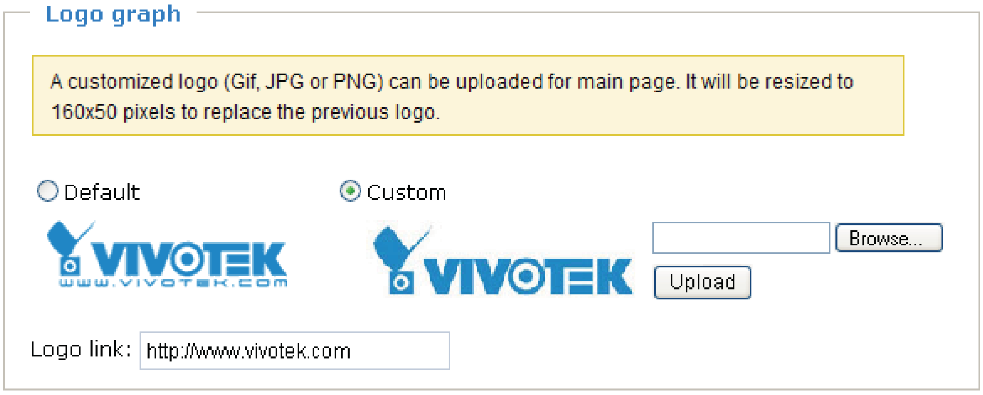


□ Hide Powered by VIVOTEK

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

Logo graph

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


Logo graph

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

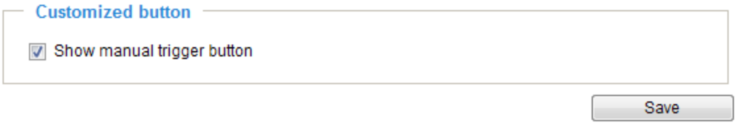
○ Default ● Custom

Logo link: 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.

Customized button

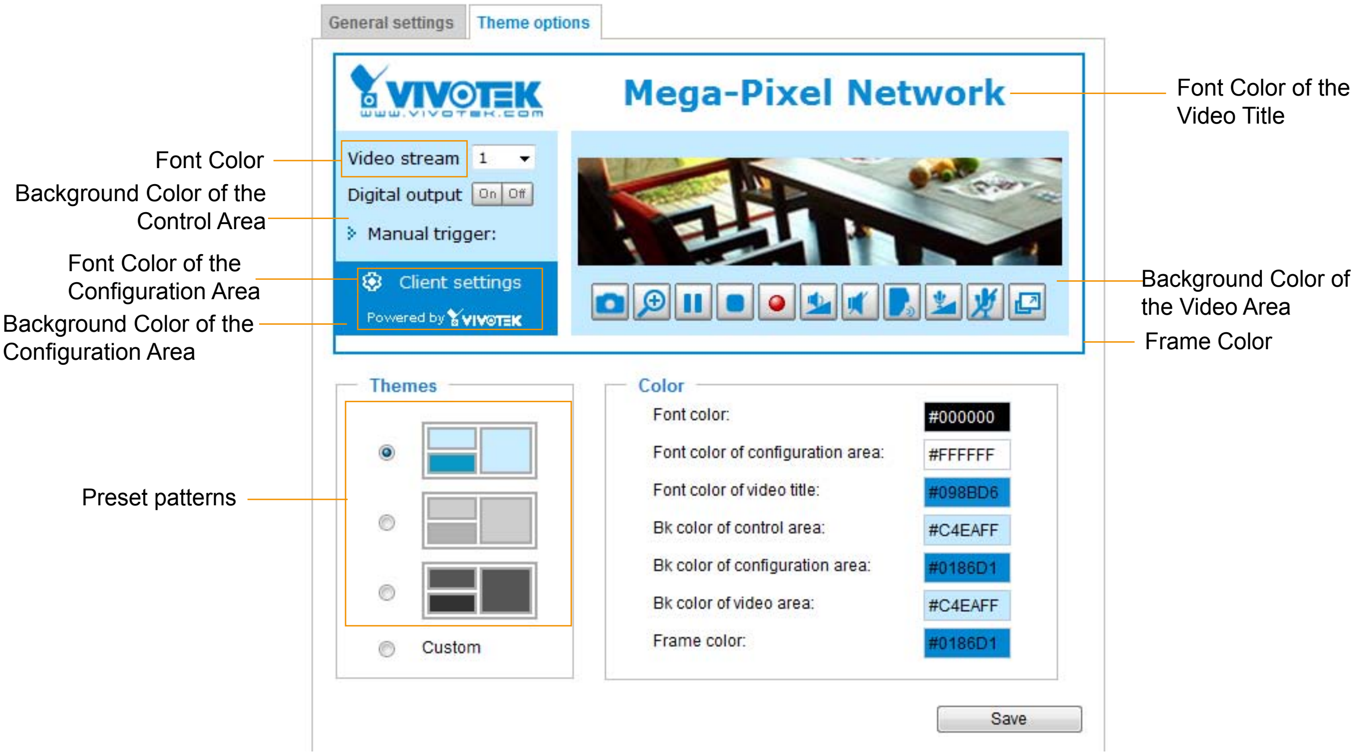
If you want to hide manual trigger buttons on the homepage, please uncheck this item. This item is checked by default.


Customized button

☑ Show manual trigger button

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.



Font color: #000000

Font color of configuration area: #FFFFFF

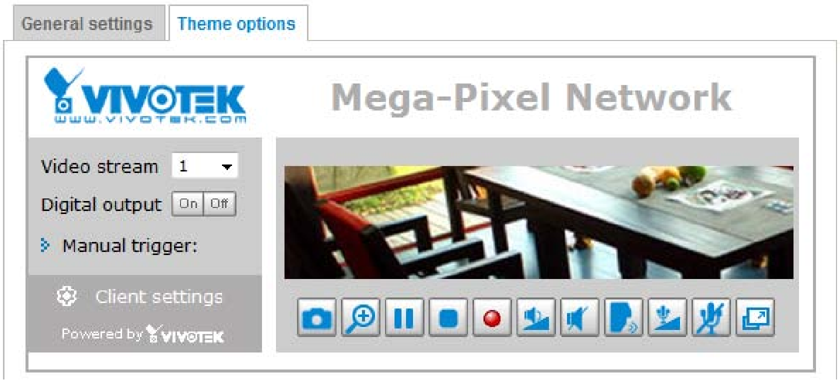
Font color of video title: #098BD6

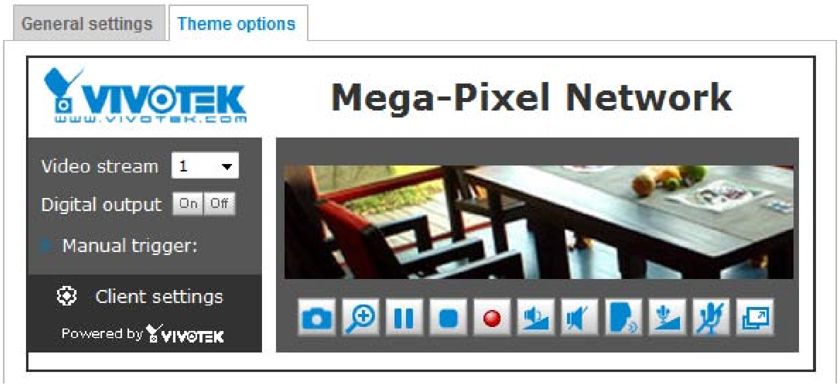
Bk color of control area: #C4EAFF

Bk color of configuration area: #0186D1

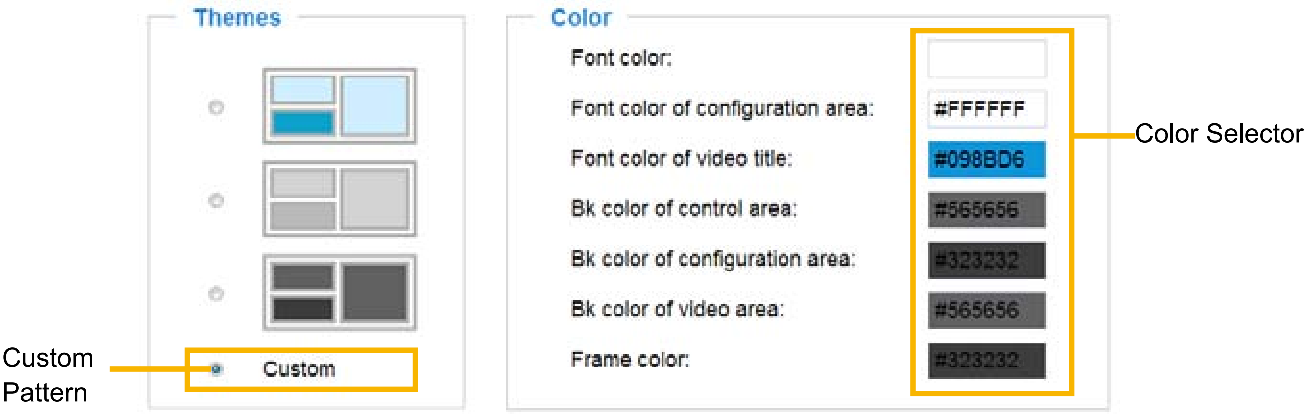
Bk color of video area: #C4EAFF

Frame color: #0186D1





■ Follow the steps below to set up a custome homepage:
1. Click **Custom** on the left column.
2. Click to select a color on on the right column.



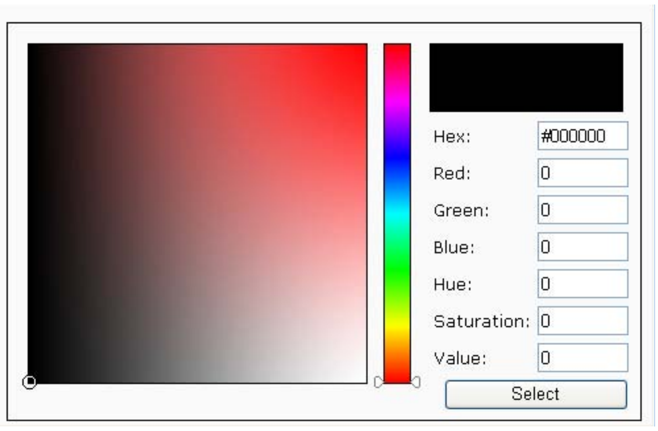
Themes

○ Custom

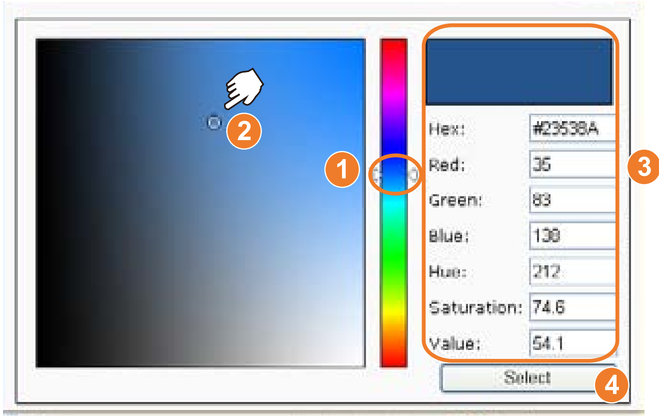
Color

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



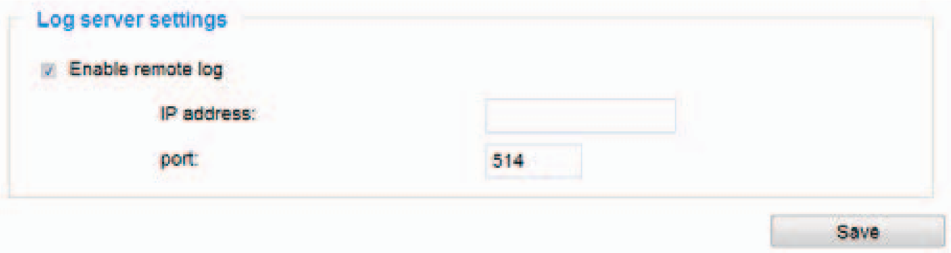
Hex:	#23538A
Red:	35
Green:	83
Blue:	138
Hue:	212
Saturation:	74.6
Value:	54.1

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.

System > Logs Advanced Mode

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

Log server settings



Log server settings

☑ Enable remote log

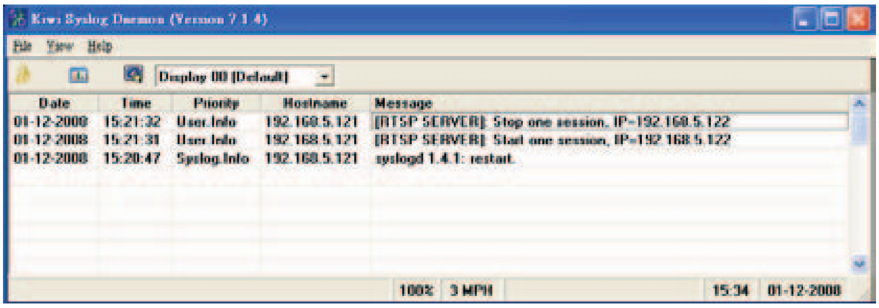
IP address:

port: 514

Follow the steps below to set up the remote log:

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

You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log messages from the Network Camera. An example is Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.

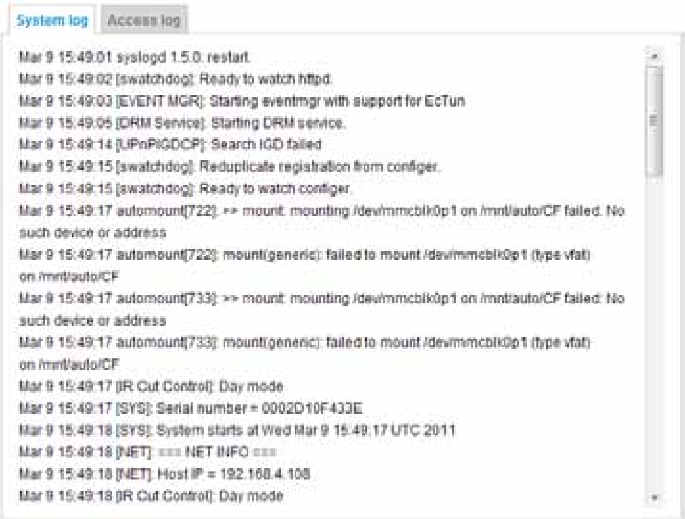


```
Date        Time      Priority     Hostname       Message
01-12-2008  15:21:32  User.Info    192.168.5.121  [RTSP SERVER]: Stop one session, IP=192.168.5.122
01-12-2008  15:21:31  User.Info    192.168.5.121  [RTSP SERVER]: Start one session, IP=192.168.5.122
01-12-2008  15:20:47  Syslog.Info  192.168.5.121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

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

System log

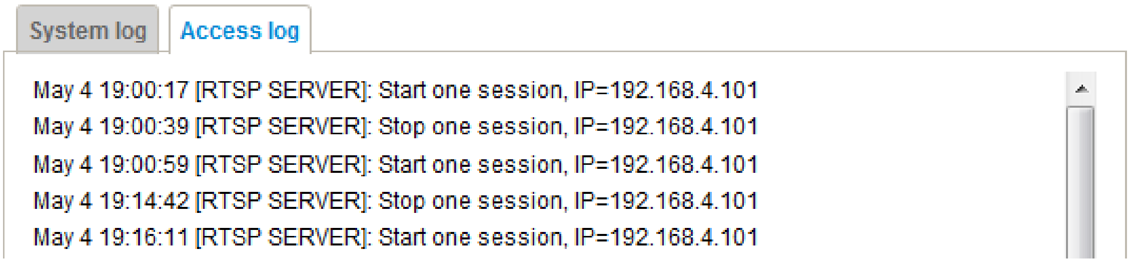
This column displays the system log in chronological order. The system log is stored in the Network Camera's buffer and dated events will be overwritten when the number of events reaches a limit.



```
Mar 9 15:49:01 syslogd 1.5.0: restart.
Mar 9 15:49:02 [swatchdog]: Ready to watch httpd.
Mar 9 15:49:03 [EVENT MGR]: Starting eventmgr with support for EcTun
Mar 9 15:49:05 [DRM Service]: Starting DRM service.
Mar 9 15:49:14 [UPnPIGDCP]: Search IGD failed
Mar 9 15:49:15 [swatchdog]: Reduplicate registration from configer.
Mar 9 15:49:15 [swatchdog]: Ready to watch configer.
Mar 9 15:49:17 automount[722]: >> mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No
such device or address
Mar 9 15:49:17 automount[722]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat)
on /mnt/auto/CF
Mar 9 15:49:17 automount[733]: >> mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No
such device or address
Mar 9 15:49:17 automount[733]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat)
on /mnt/auto/CF
Mar 9 15:49:17 [IR Cut Control]: Day mode
Mar 9 15:49:17 [SYS]: Serial number = 0002D10F433E
Mar 9 15:49:18 [SYS]: System starts at Wed Mar 9 15:49:17 UTC 2011
Mar 9 15:49:18 [NET]: === NET INFO ===
Mar 9 15:49:18 [NET]: Host IP = 192.168.4.108
Mar 9 15:49:18 [IR Cut Control]: Day mode
```

Access log

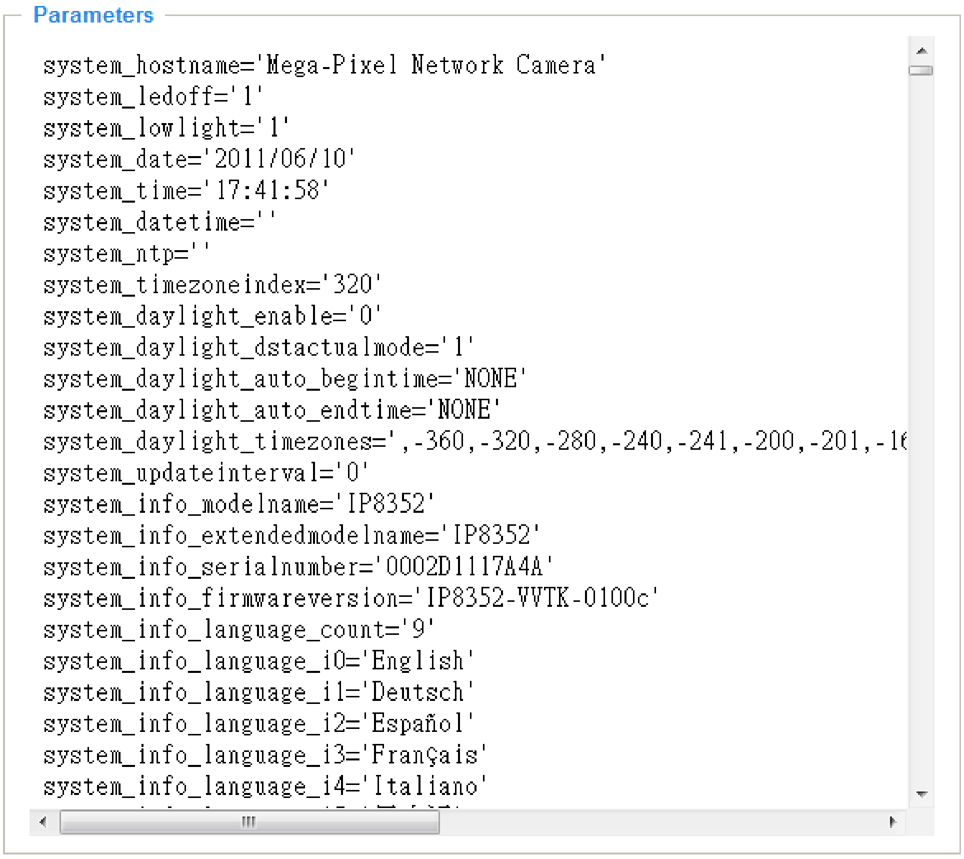
Access log displays the access time and IP address of all viewers (including operators and administrators) in a chronological order. The access log is stored in the Network Camera's buffer and older events will be overwritten when the number of events reaches a limit.



```
May 4 19:00:17 [RTSP SERVER]: Start one session, IP=192.168.4.101
May 4 19:00:39 [RTSP SERVER]: Stop one session, IP=192.168.4.101
May 4 19:00:59 [RTSP SERVER]: Start one session, IP=192.168.4.101
May 4 19:14:42 [RTSP SERVER]: Stop one session, IP=192.168.4.101
May 4 19:16:11 [RTSP SERVER]: Start one session, IP=192.168.4.101
```

System > Parameters Advanced Mode

The View Parameters page lists the entire system's parameters in an alphabetical order. If you need technical assistance, use a text-editor program to copy and save the parameters listed on this page. Send the parameter text file to VIVOTEK's technical support.

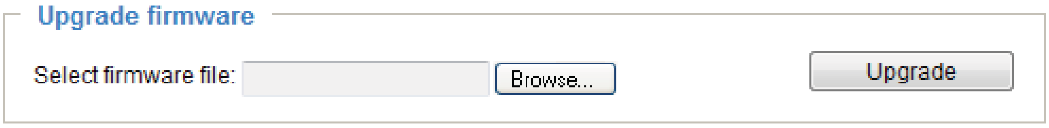


```
system_hostname='Mega-Pixel Network Camera'
system_ledoff='1'
system_lowlight='1'
system_date='2011/06/10'
system_time='17:41:58'
system_datetime=''
system_ntp=''
system_timezoneindex='320'
system_daylight_enable='0'
system_daylight_dstactualmode='1'
system_daylight_auto_begintime='NONE'
system_daylight_auto_endtime='NONE'
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-16
system_updateinterval='0'
system_info_modelname='IP8352'
system_info_extendedmodelname='IP8352'
system_info_serialnumber='0002D1117A4A'
system_info_firmwareversion='IP8352-VVTK-0100c'
system_info_language_count='9'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system_info_language_i3='Français'
system_info_language_i4='Italiano'
```

System > Maintenance

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

General settings > Upgrade firmware

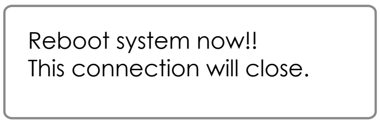


This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.
Note: Do not power off the Network Camera during the upgrade!

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

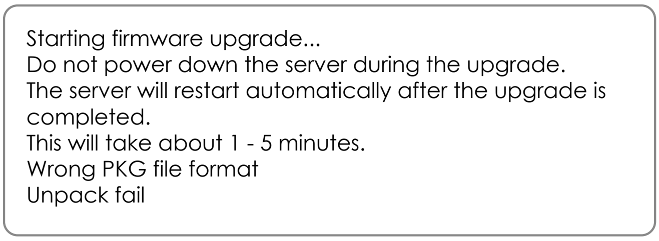
If the upgrade is successful, you will see “Reboot system now!! This connection will close”. After that, re-access the Network Camera.

The following message is displayed when the upgrade has succeeded.



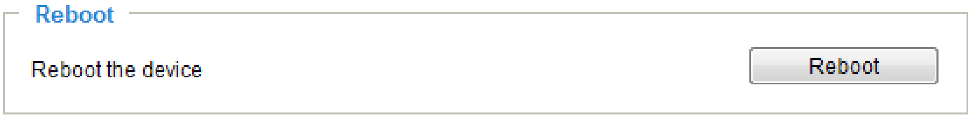
Reboot system now!!
This connection will close.

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

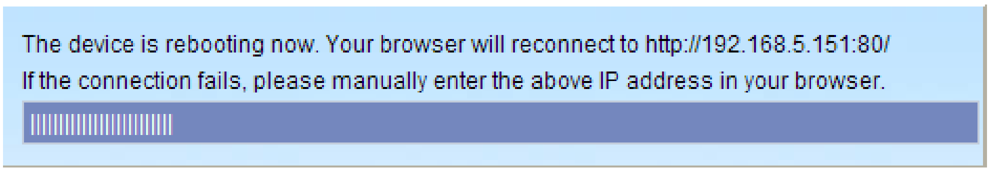


Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is completed.
This will take about 1 - 5 minutes.
Wrong PKG file format
Unpack fail

General settings > Reboot



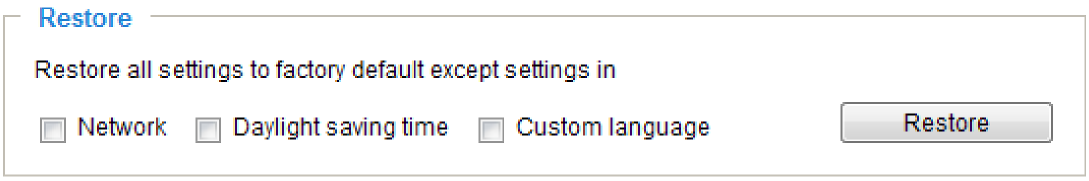
This feature allows you to reboot the Network Camera, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will be displayed during the reboot process.



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.

General settings > Restore



Restore

Restore all settings to factory default except settings in

□ Network □ Daylight saving time □ Custom language

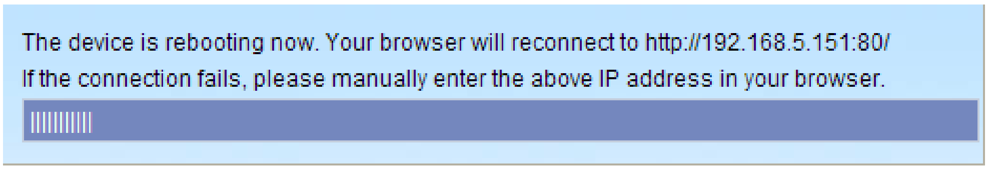
This feature allows you to restore the Network Camera to factory default settings.

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

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

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

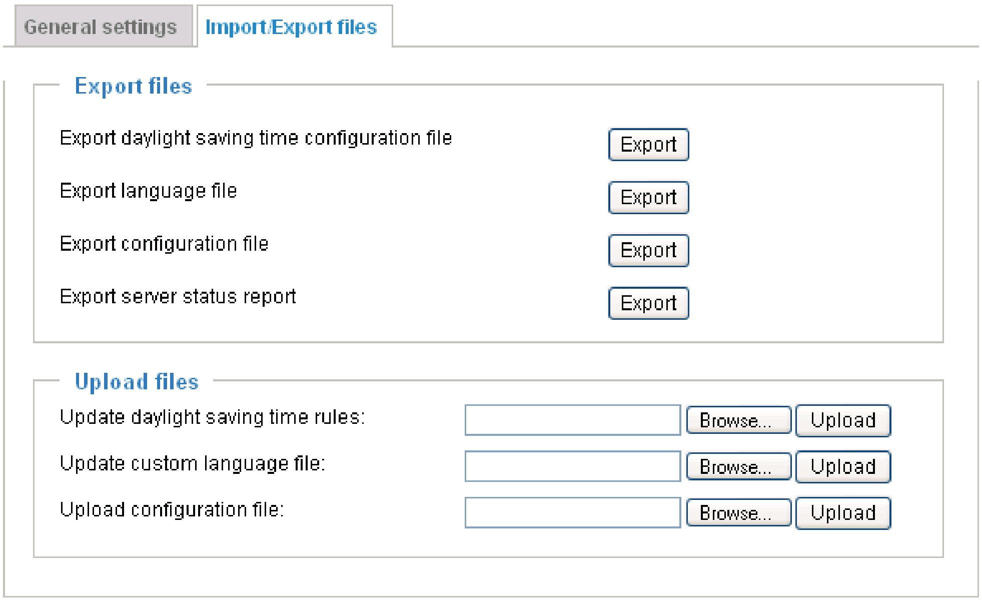
If none of the options is selected, all settings will be restored to factory default. The following message is displayed during the restoring process.



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

Import/Export files Advanced Mode

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



Export files

Export daylight saving time configuration file

Export language file

Export configuration file

Export server status report

Upload files

Update daylight saving time rules:

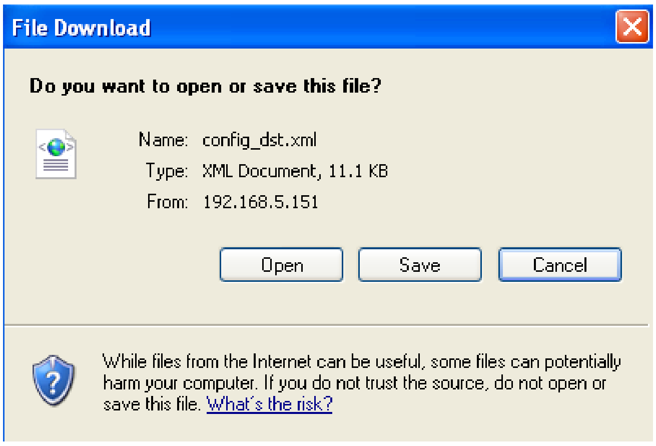
Update custom language file:

Upload configuration 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

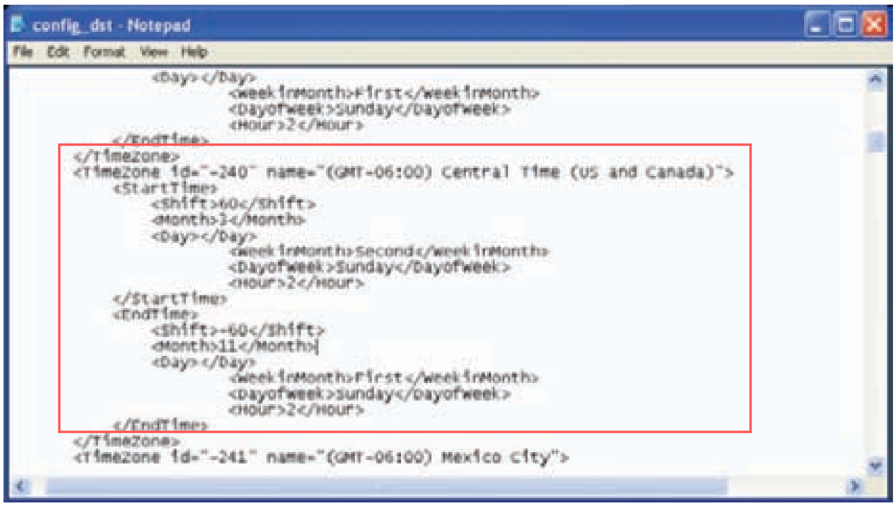
Do you want to open or save this file?

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.

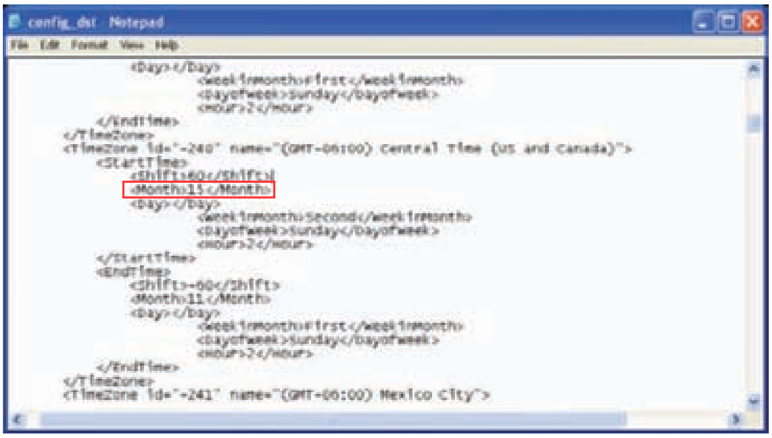
   In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.



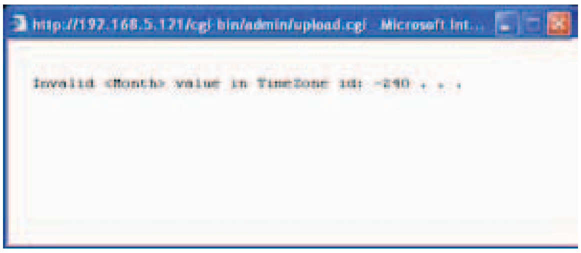
```
            <Day></Day>
                    <weekInMonth>First</weekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-240" name="(GMT-06:00) Central Time (US and Canada)">
        <StartTime>
            <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">
```

<u>Update daylight saving time rules</u>: Click **Browse…** and specify the XML file to update.

If incorrect date and time are assigned, you will see the following warning message when uploading the file to the Network Camera.



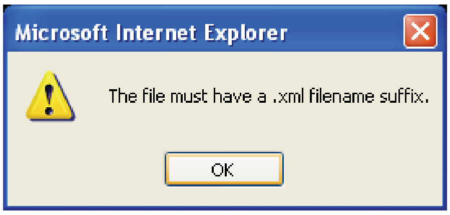
```
            <Day></Day>
                    <weekInMonth>First</weekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-240" name="(GMT-06:00) Central Time (US and Canada)">
        <StartTime>
            <Shift>60</Shift>
            <Month>13</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.



Microsoft Internet Explorer

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.

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

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

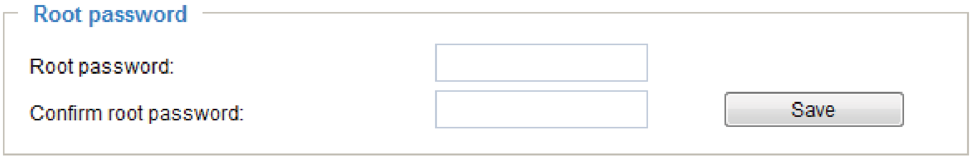
Update configuration file: Click **Browse…** to update a configuration file. Please note that the model and firmware version of the device should be the same as the configuration file. If you have set up a fixed IP or other special settings for your device, it is not suggested to update a configuration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

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

Security > User Account

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

Root Password



Root password

Root password:

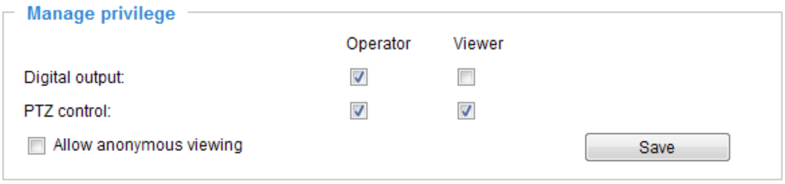
Confirm root password:

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

Manage Privilege

Advanced Mode



Manage privilege

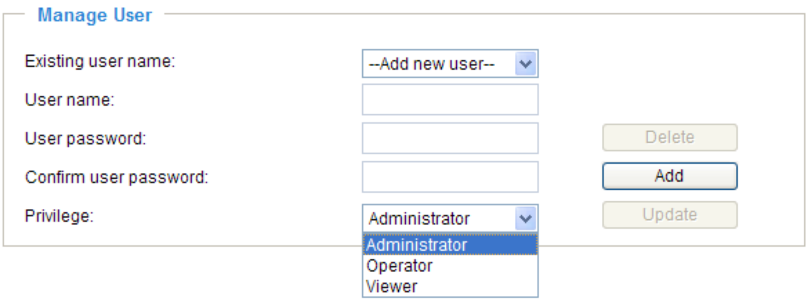
	Operator	Viewer
Digital output:	☑	□
PTZ control:	☑	☑

□ Allow anonymous viewing

Digital Output & PTZ control: You can modify the management privilege as operators or viewers. Select or de-select the checkboxes, and then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Configuration on page 28).

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

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. Though operators cannot access the Configuration page, they can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 110. 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.

Advanced Mode

Security > HTTPS (Hypertext Transfer Protocol over SSL)

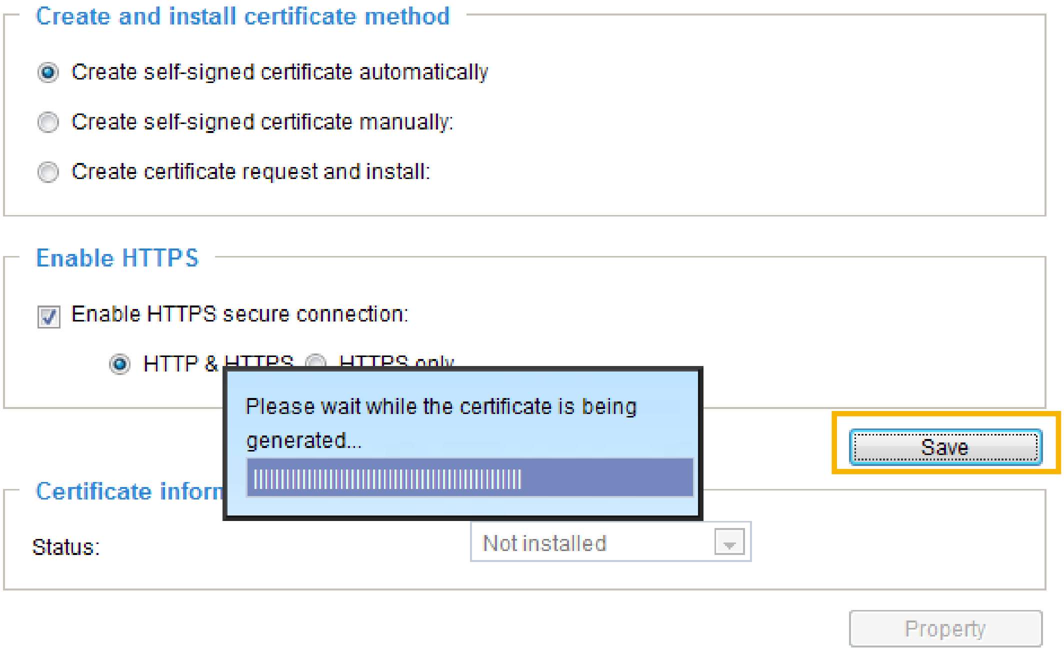
This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

Create and Install Certificate Method

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

Create self-signed certificate automatically

1. Select the first option.
2. Check **Enable HTTPS secure connection**, then select a connection option: “HTTP & HTTPS” or “HTTPS only”.
3. Click **Save** to generate a certificate.



Create and install certificate method

● Create self-signed certificate automatically

○ Create self-signed certificate manually:

○ Create certificate request and install:

Enable HTTPS

☑ Enable HTTPS secure connection:

● HTTP & HTTPS ○ HTTPS only

Please wait while the certificate is being generated...

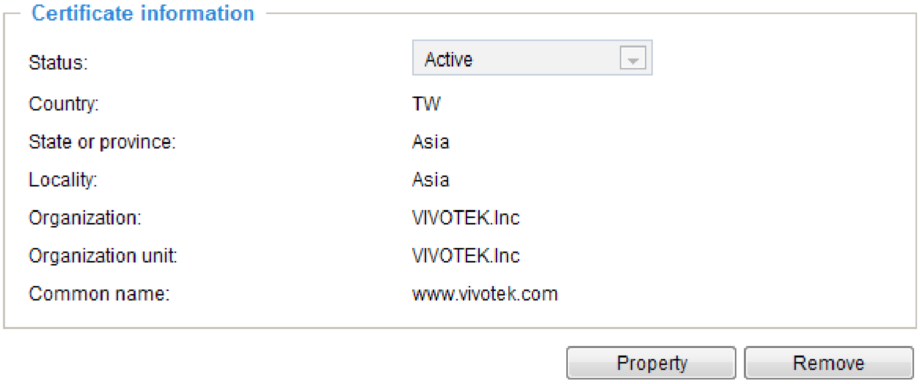
Save

Certificate inforn

Status: Not installed

Property

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.

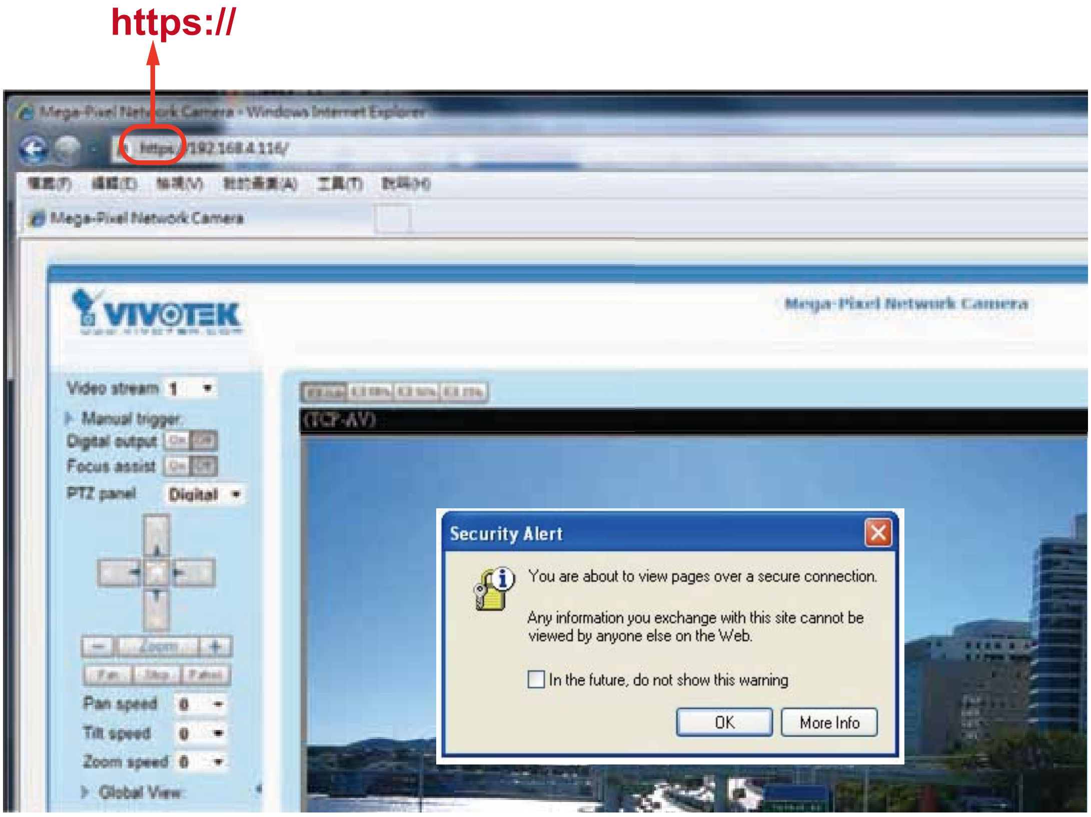


Certificate information

Status:	Active
Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	VIVOTEK.Inc
Organization unit:	VIVOTEK.Inc
Common name:	www.vivotek.com

Property Remove

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.



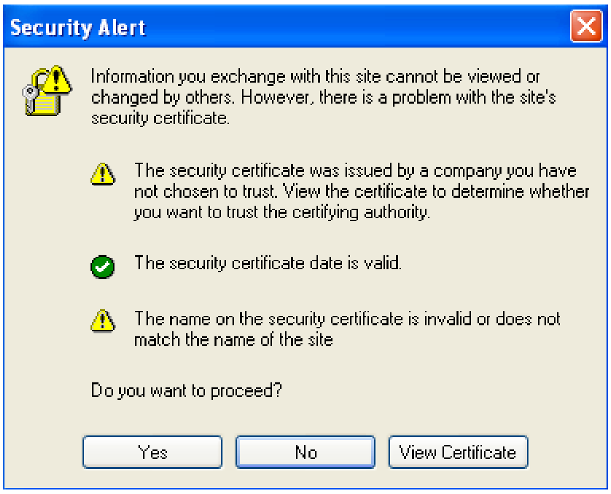
Security Alert

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

OK | More Info



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.

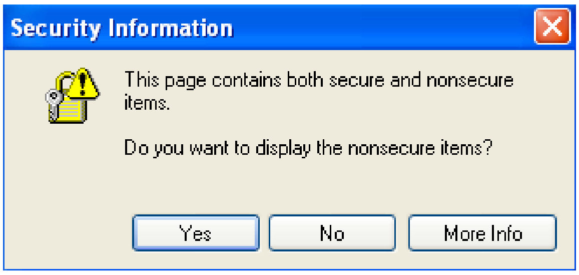
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ 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?

Yes | No | View Certificate



Security Information

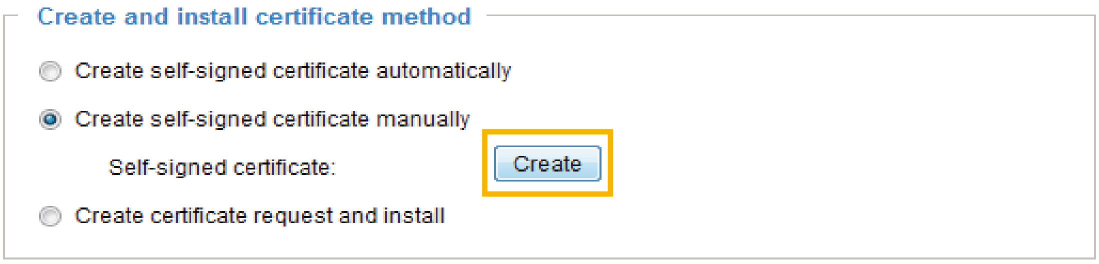
This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

Yes | No | More Info

Create self-signed certificate manually

1. Select the second option.
2. Click **Create** to open the Create Certificate page.



Create and install certificate method

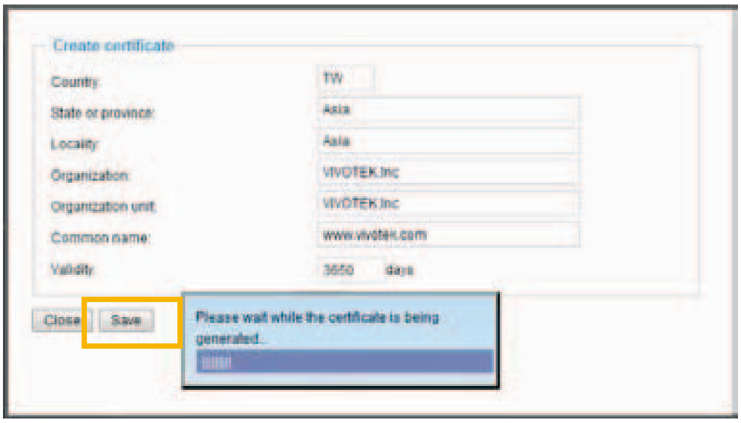
○ Create self-signed certificate automatically

● Create self-signed certificate manually

Self-signed certificate: Create

○ Create certificate request and install

3. The following information will show up in a pop-up window after clicking **Create**. Then click **Save** to generate the certificate.

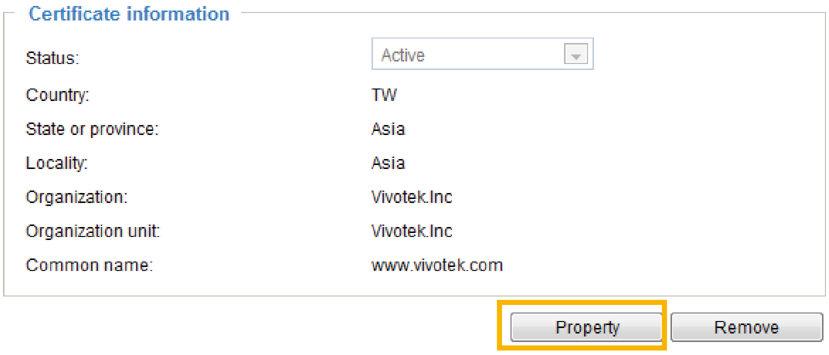


Create certificate

Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	VIVOTEK.Inc
Organization unit:	VIVOTEK.Inc
Common name:	www.vivotek.com
Validity:	3650 days

Please wait while the certificate is being generated...

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



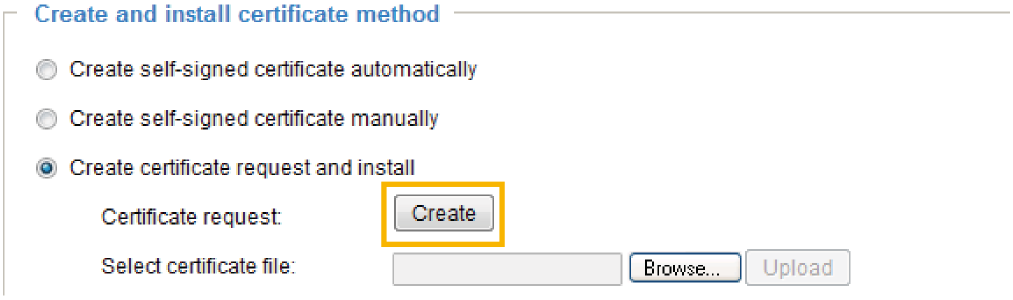
Certificate information

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

5. Check **Enable HTTPS secure connection**, then select a connection option: “HTTP & HTTPS” or “HTTPS only”. Click **Save** to enable the settings.

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

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



Create and install certificate method

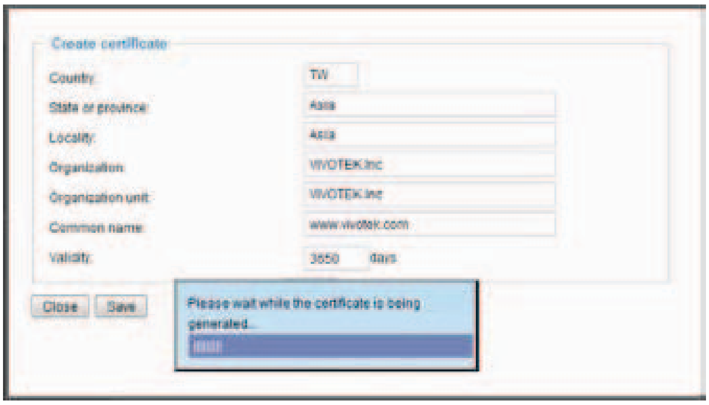
○ Create self-signed certificate automatically

○ Create self-signed certificate manually

● Create certificate request and install

Certificate request: Create

Select certificate file:

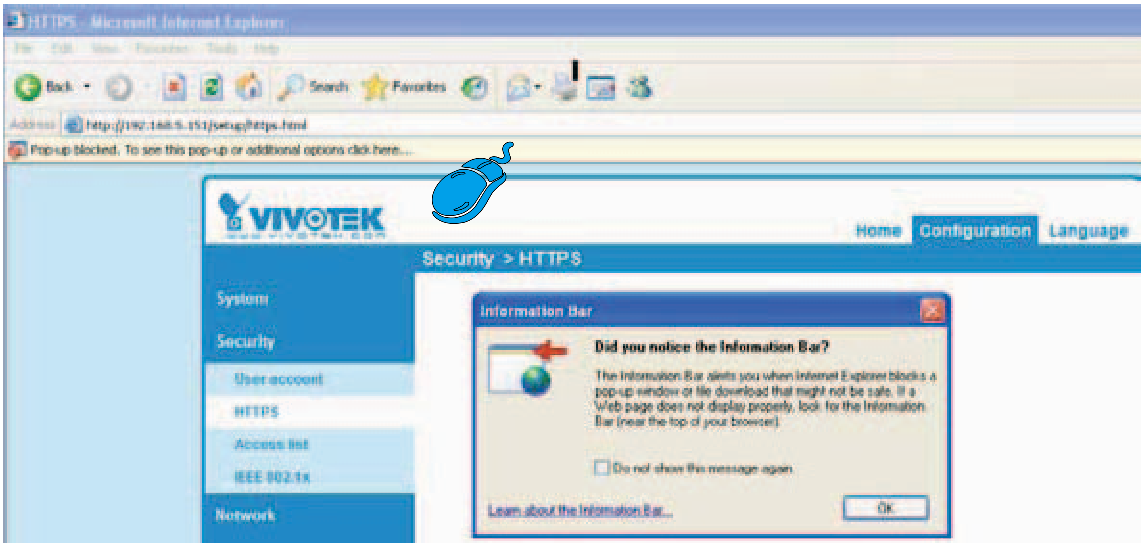


Create certificate

Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	VIVOTEK.Inc
Organization unit:	VIVOTEK.Inc
Common name:	www.vivotek.com
Validity:	3650 days

Please wait while the certificate is being generated...

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



HTTPS - Microsoft Internet Explorer

Address http://192.168.5.151/setup/https.html

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

Security > HTTPS

Information Bar

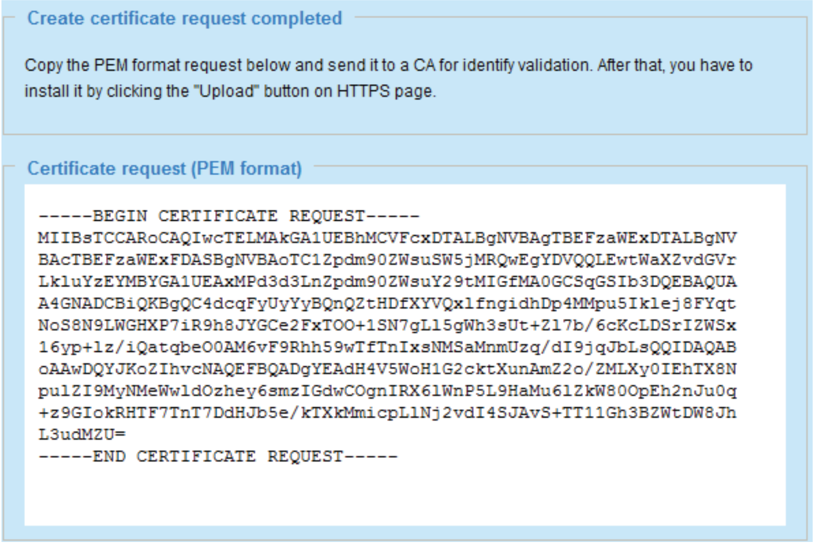
Did you notice the Information Bar?

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.



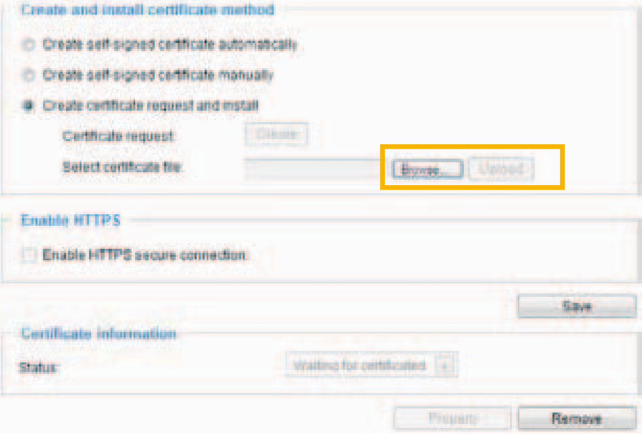
Create certificate request completed

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-----
MIIBsTCCARoCAQIwcTELMAkGA1UEBhMCVFcxDTALBgNVBAgTBEFzaWExDTALBgNV
BAcTBEFzaWExFDASBgNVBAoTC1Zpdm90ZWsuSW5jMRQwEgYDVQQLEwtWaXZvdGVr
LkluYzEYMBYGA1UEAxMPd3d3LnZpdm90ZWsuY29tMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQC4dcqFyUyYyBQnQZtHDfXYVQxlfngidhDp4MMpu5Iklej8FYqt
NoS8N9LWGHXP7iR9h8JYGCe2FxTOO+1SN7gLl5gWh3sUt+Zl7b/6cKcLDSrIZWSx
16yp+lz/iQatqbeO0AM6vF9Rhh59wTfTnIxsNMSaMnmUzq/dI9jqJbLsQQIDAQAB
oAAwDQYJKoZIhvcNAQEFBQADgYEAdH4V5WoH1G2cktXunAmZ2o/ZMLXy0IEhTX8N
pulZI9MyNMeWwldOzhey6smzIGdwCOgnIRX6lWnP5L9HaMu6lZkW80OpEh2nJu0q
+z9GIokRHTF7TnT7DdHJb5e/kTXkMmicpLlNj2vdI4SJAvS+TT11Gh3BZWtDW8Jh
L3udMZU=
-----END CERTIFICATE REQUEST-----
```

5. Look for a trusted certificate authority that issues digital certificates. Enroll the Network Camera. Wait for the certificate authority to issue an SSL certificate; click **Browse...** to search for the issued certificate, then click **Upload** in the column.
6. Check **Enable HTTPS secure connection**, then select a connection option: “HTTP & HTTPS” or “HTTPS only”. Click **Save** to enable the settings.



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

Enable HTTPS

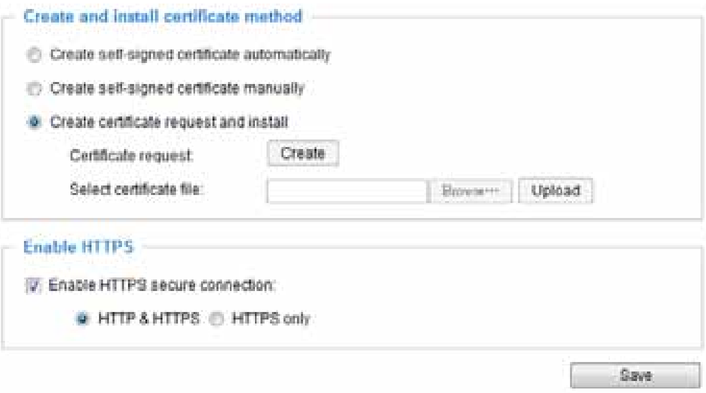
□ Enable HTTPS secure connection

Certificate information

Status: Waiting for certificated

Click this checkbox to enable HTTPS communication, and then select a connection option from below: "HTTP & HTTPS" or "HTTPS only."

Note that a certificate must have been created and installed before you can click on the "**save**" button for the configuration to take effect.



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

Enable HTTPS

☑ Enable HTTPS secure connection:

● HTTP & HTTPS ○ HTTPS only

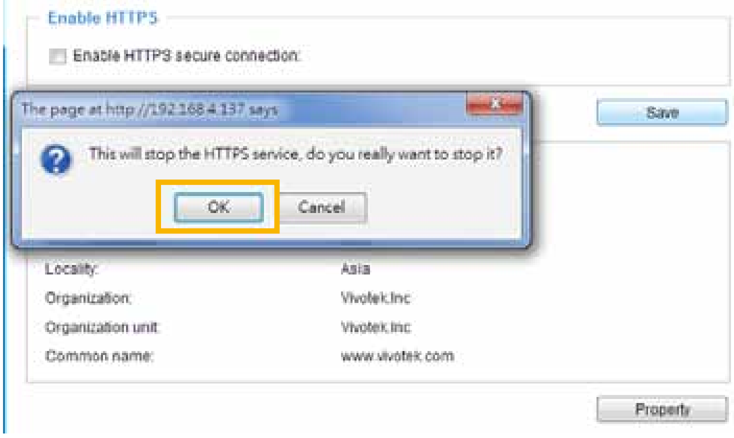
Save

Tips:

► *1. How do I cancel the HTTPS settings?*

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

*1-2. Click **OK** to disable HTTPS.*



Enable HTTPS

□ Enable HTTPS secure connection:

The page at http://192.168.4.137 says:

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

OK Cancel

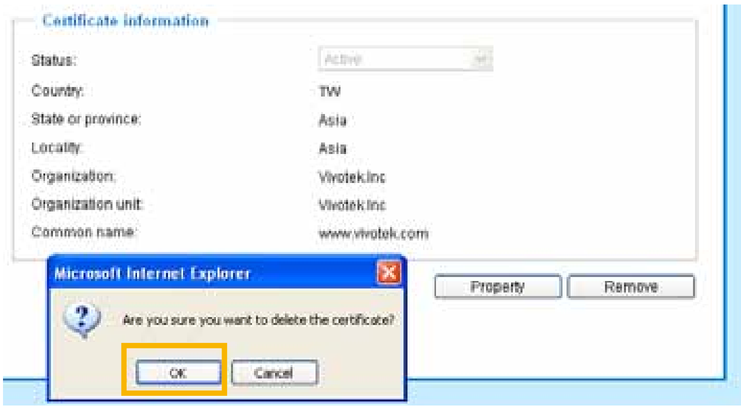
Save

Locality:	Asia
Organization:	Vivotek.Inc
Organization unit:	Vivotek.Inc
Common name:	www.vivotek.com

Property

1-3. The webpage will redirect to a non-HTTPS page automatically.

► *2. If you want to create and install other certificates, please remove the existing one.*



Certificate information

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

Microsoft Internet Explorer

Are you sure you want to delete the certificate?

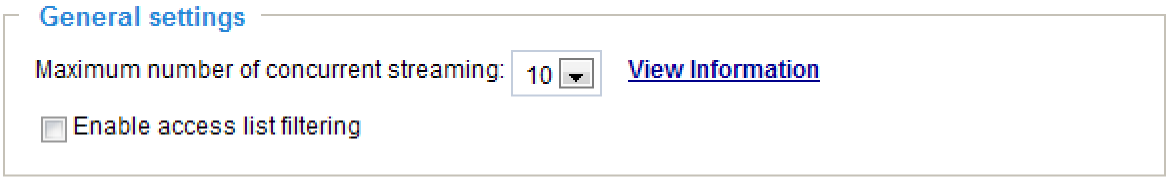
OK Cancel

Property Remove

Security > Access List Advanced Mode

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

General Settings



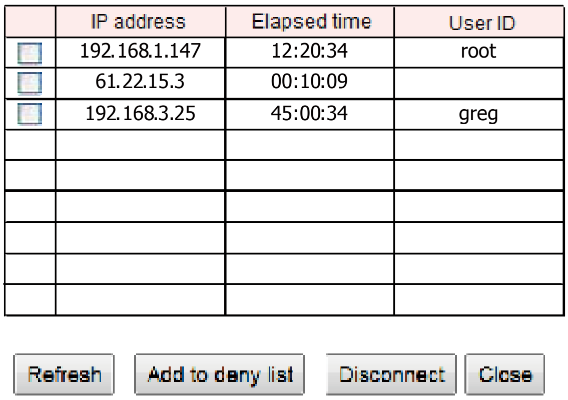
General settings

Maximum number of concurrent streaming: 10

□ Enable access list filtering

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

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



	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 > User account on page 40.
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 60.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing,** please refer to page 40.

■ Refresh: Click this button to refresh all current connections.

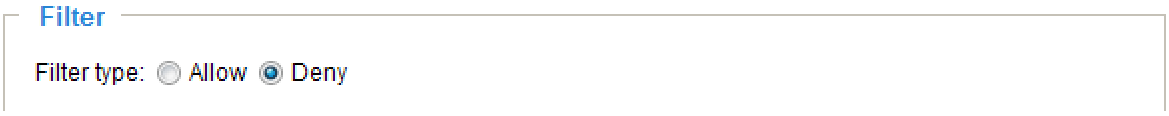
■ Add to deny list: You can select entries from the Connection Status list and add them to the Deny List to deny access. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player). If you want to enable 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 Explorer 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

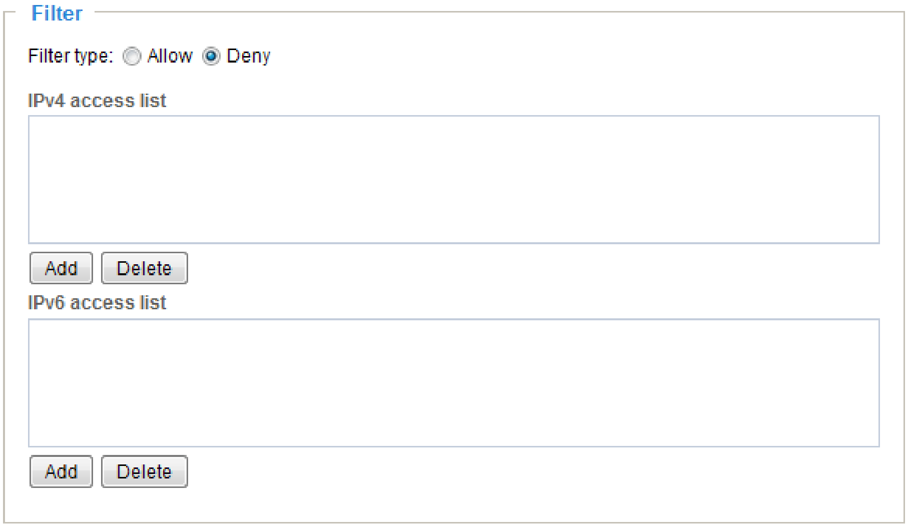
Filter type: Select **Allow** or **Deny** as the filter type. If you choose **Allow Type**, only those clients whose IP addresses are on the Access List below can access the Network Camera, and the others cannot access. On the contrary, if you choose **Deny Type**, those clients whose IP addresses are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



Filter

Filter type: ○ Allow ● Deny

Then you can **Add** a rule to the following Access List. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to Network > Enable IPv6 on page 55 for detailed information.



Filter

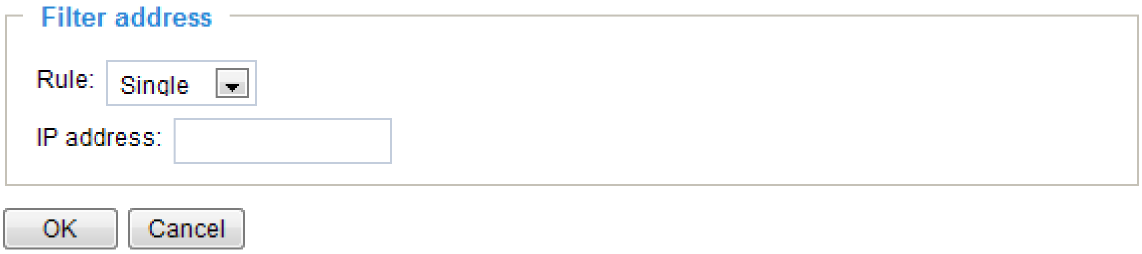
Filter type: ○ Allow ● Deny

IPv4 access list

IPv6 access list

There are three types of rules:

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

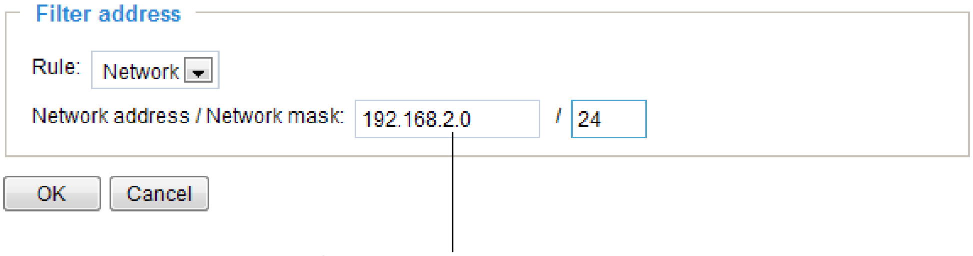


Filter address

Rule: Single

IP address:

Network: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List. The routing prefix is written in CIDR notation.
For example:



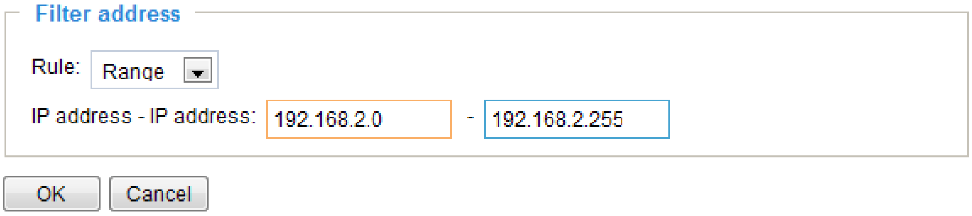
Filter address

Rule: Network

Network address / Network mask: 192.168.2.0 / 24

accesses from IP address 192.168.2.x will be bolcked.

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



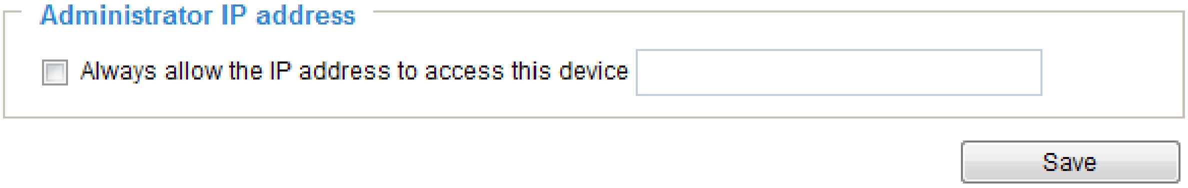
Filter address

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.



Administrator IP address

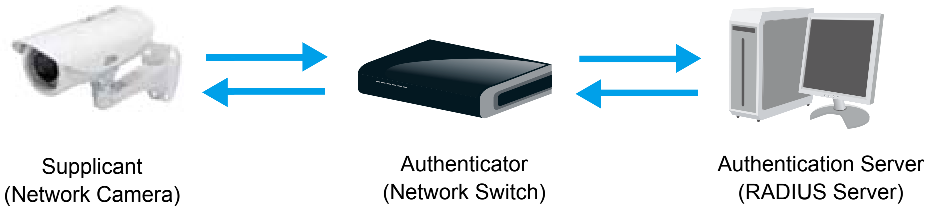
□ Always allow the IP address to access this device

Security > IEEE 802.1x Advanced Mode

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

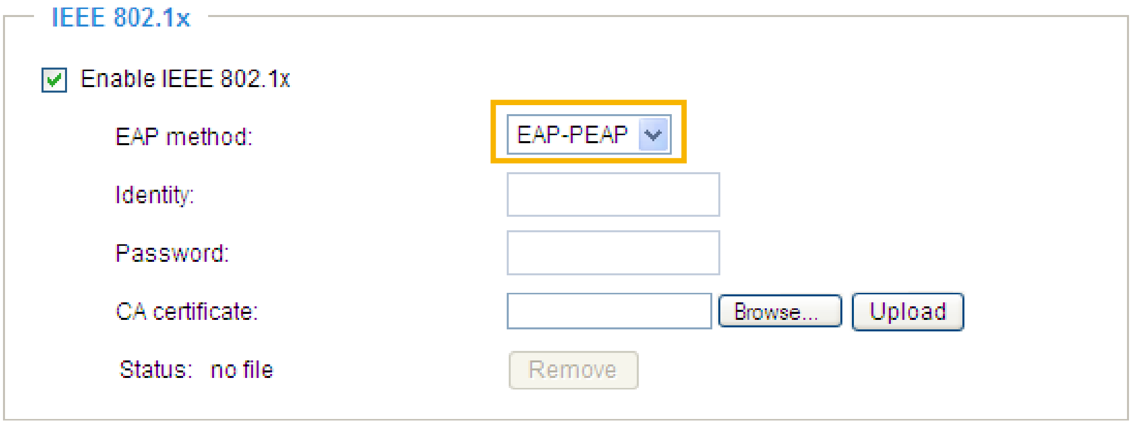
■ The components of a protected network with 802.1x authentication:



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 (i.e., 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

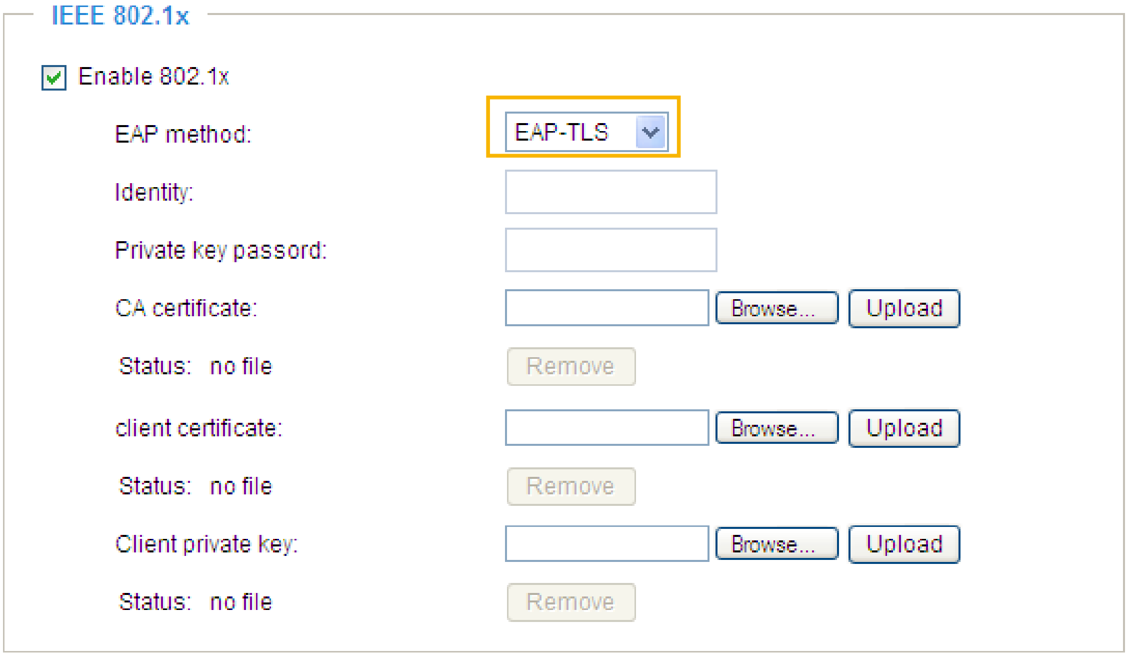
EAP method: EAP-PEAP

Identity:

Password:

CA certificate:

Status: no file



IEEE 802.1x

☑ Enable 802.1x

EAP method: EAP-TLS

Identity:

Private key pasord:

CA certificate:

Status: no file

client certificate:

Status: no file

Client private key:

Status: no file

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

NOTE:

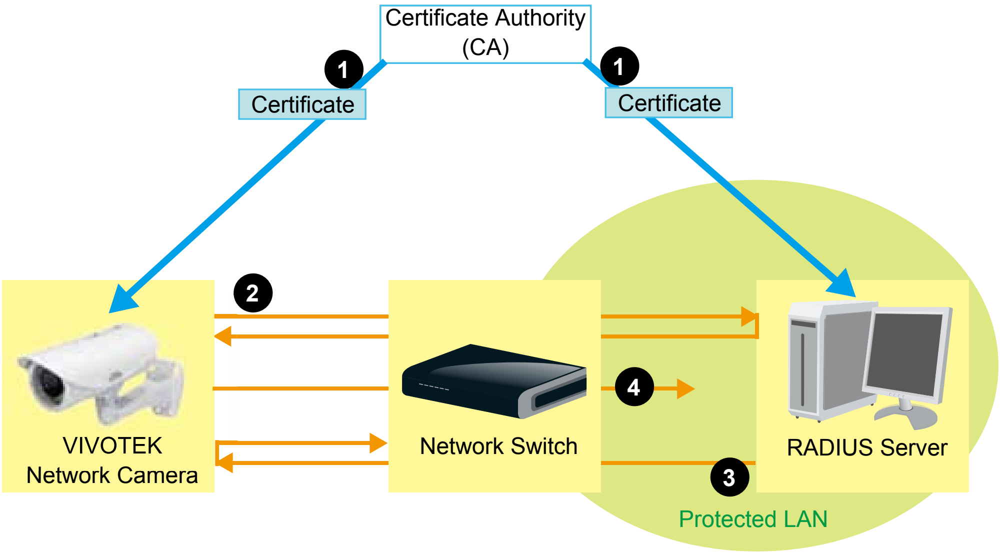
► *The authentication process for 802.1x:*

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

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

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

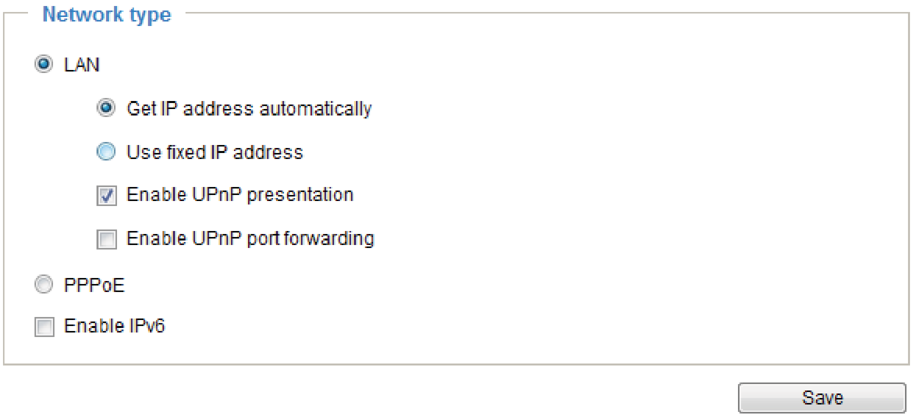
4. Assuming all certificates are validated, the switch then changes the Network Camera's state to authorized and is allowed access to the protected network via a pre-configured port.



Network > General settings

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

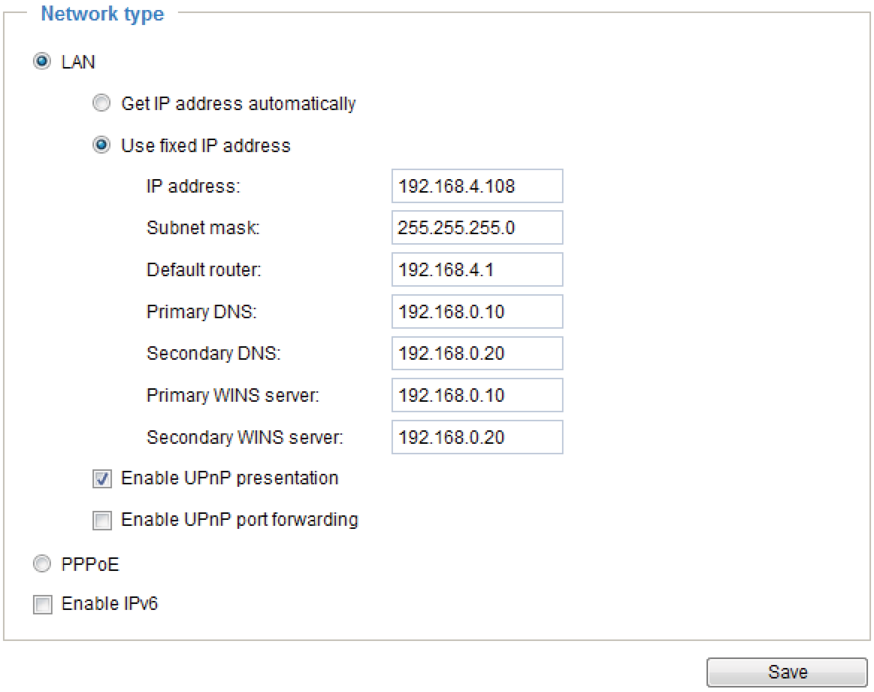
□ Enable IPv6

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.

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

<u>Use fixed IP address</u>: 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:	192.168.4.108
Subnet mask:	255.255.255.0
Default router:	192.168.4.1
Primary DNS:	192.168.0.10
Secondary DNS:	192.168.0.20
Primary WINS server:	192.168.0.10
Secondary WINS server:	192.168.0.20

☑ 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 13 for details.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP.

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

<u>Default router</u>: 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.

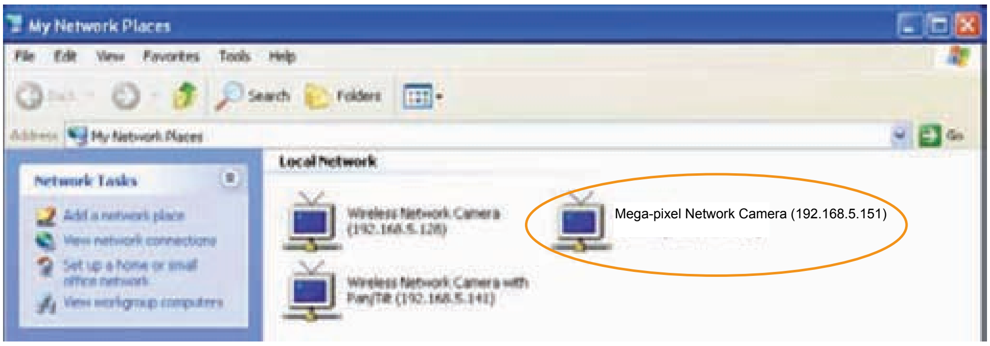
Primary DNS: The primary domain name server that translates hostnames into IP addresses.

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.

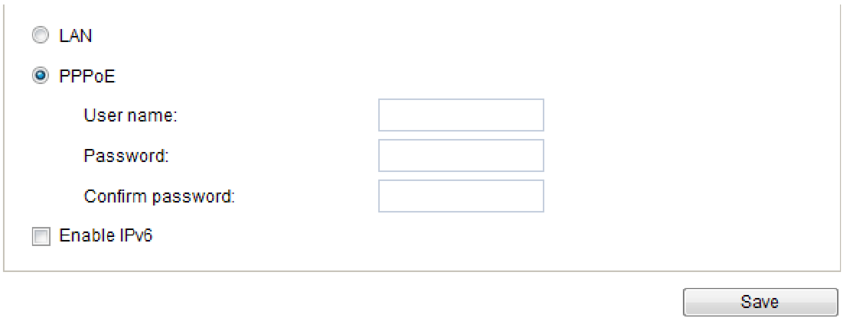

My Network Places
File Edit View Favorites Tools Help
Back
Search
Folders
Address
My Network Places
Go
Network Tasks
Add a network place
View network connections
Set up a home or small office network
View workgroup computers
Local Network
Wireless Network Camera (192.168.5.128)
Mega-pixel Network Camera (192.168.5.151)
Wireless Network Camera with Pan/Tilt (192.168.5.141)

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 Configuration > Event > Event settings > Add server (please refer to Add server on page 88) to add a new email or FTP server.
3. Go to Configuration > Event > Event settings > Add media (please refer to Add media on page 92). Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > General settings > Network type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.



○ LAN

● PPPoE

User name:

Password:

Confirm password:

□ Enable IPv6

Save

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

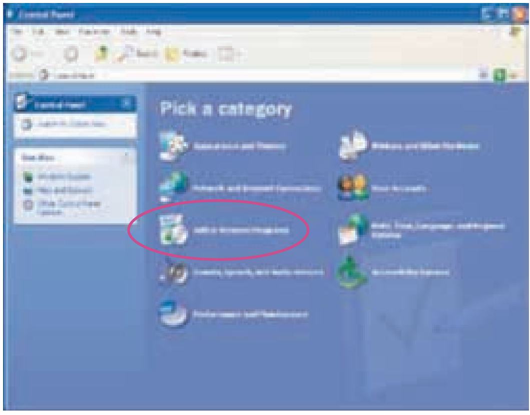
NOTE:

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

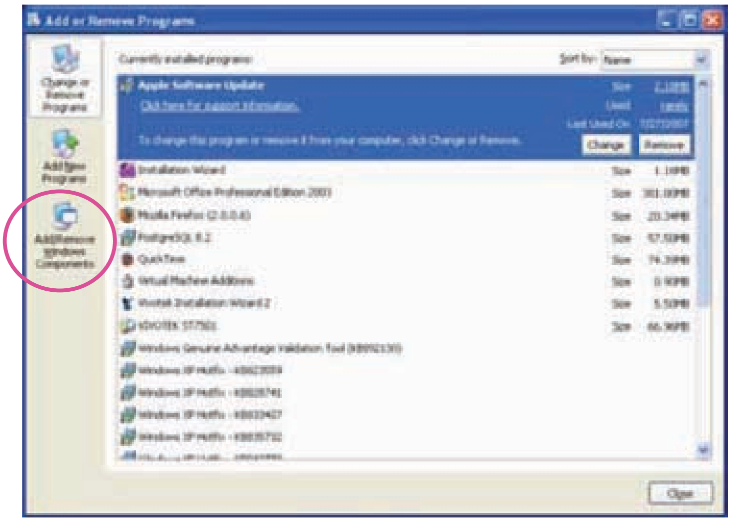
▶ *If UPnP™ is not supported by your router, you will see the following message:*
Error: Router does not support UPnP port forwarding.

▶ *Below are 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.

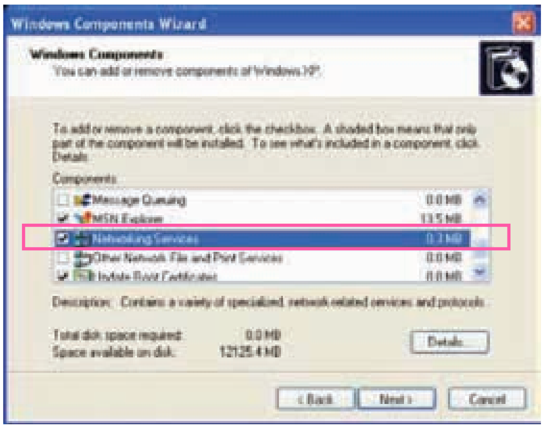
*1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.*



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


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
Sort by: Name
Apple Software Update
Change
Remove
Installation Wizard
Microsoft Office Professional Edition 2003
Mozilla Firefox (2.0.0.6)
PostgreSQL 8.2
QuickTime
Virtual Machine Additions
Vivotek Installation Wizard 2
VIVOTEK ST7501
Close

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


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.

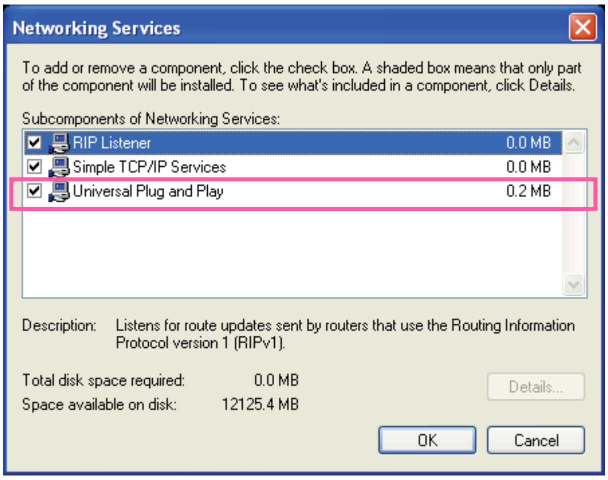
Components:

□	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

*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.

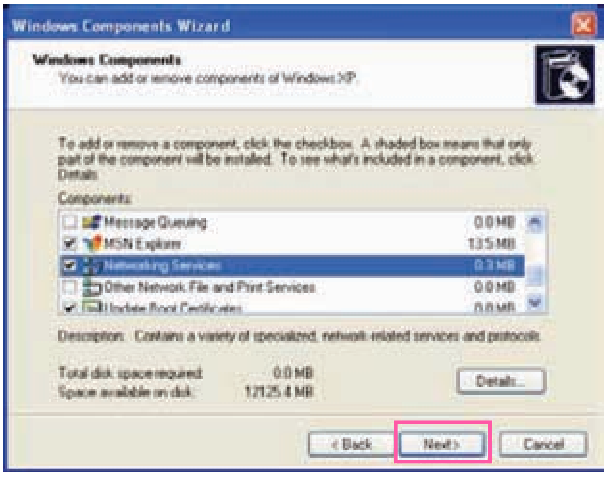
Subcomponents of Networking Services:

☑	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.

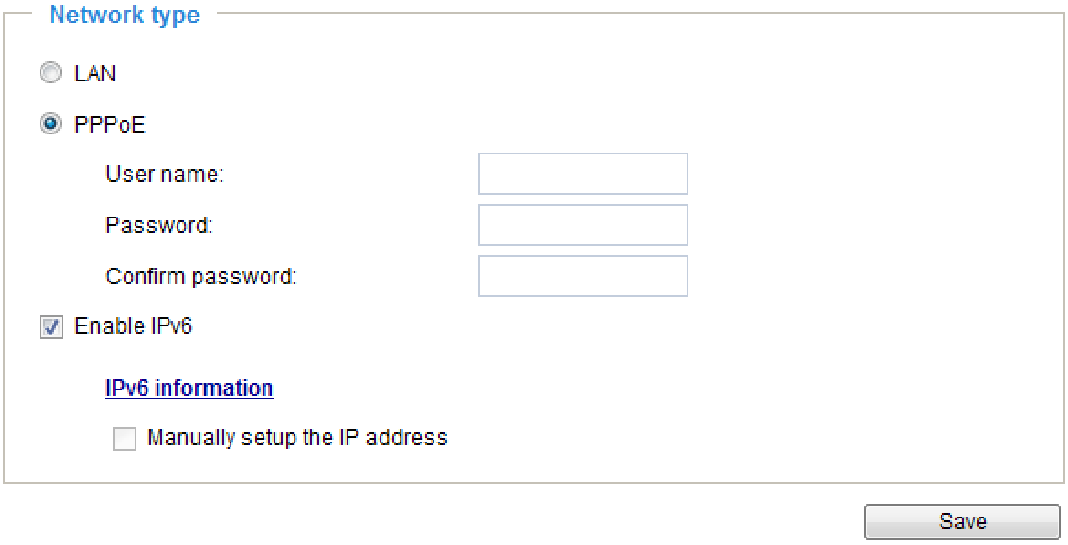
► *Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port 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 37 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.*

Enable IPv6

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



Network type

○ LAN

● PPPoE

User name:

Password:

Confirm password:

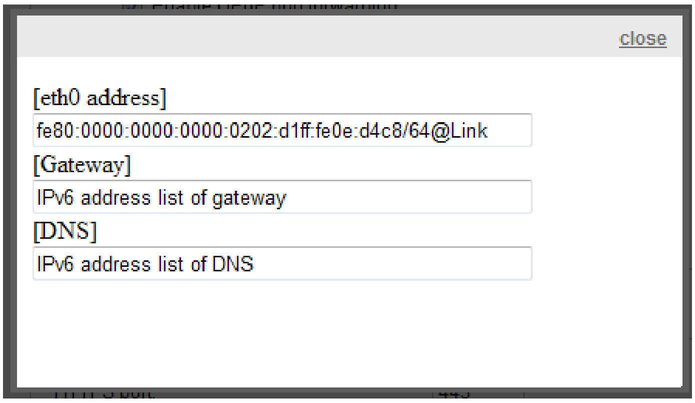
☑ Enable IPv6

IPv6 information

□ Manually setup the IP address

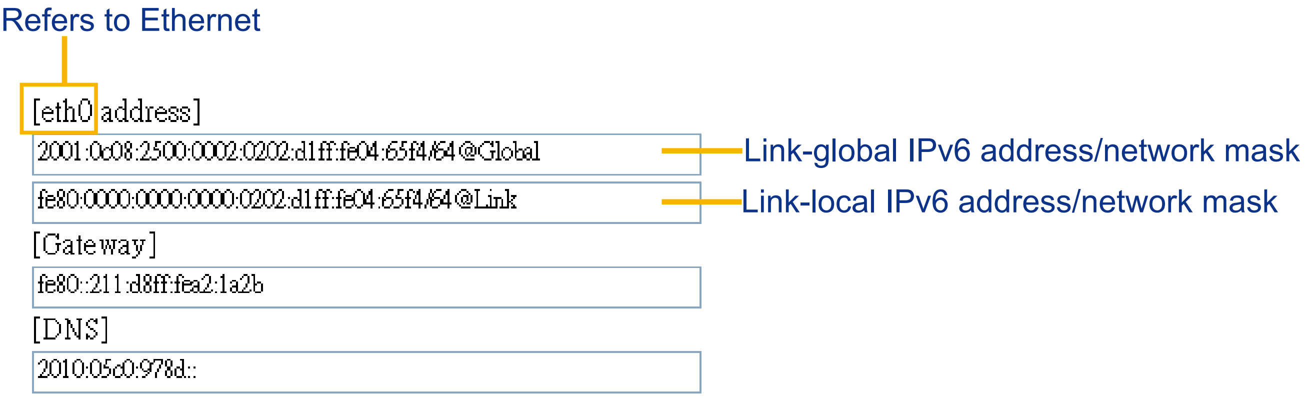
When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

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



[eth0 address]
fe80:0000:0000:0000:0202:d1ff:fe0e:d4c8/64@Link
[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:

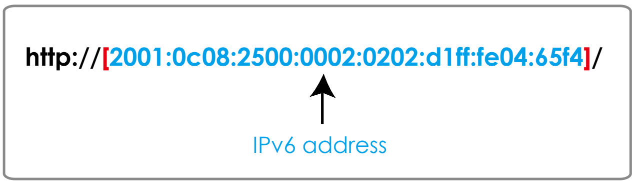


Refers to Ethernet

[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::

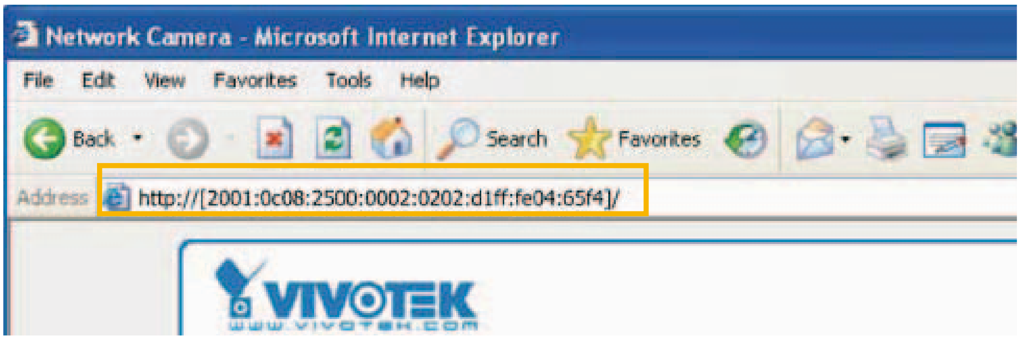
Link-global IPv6 address/network mask
Link-local IPv6 address/network mask

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:

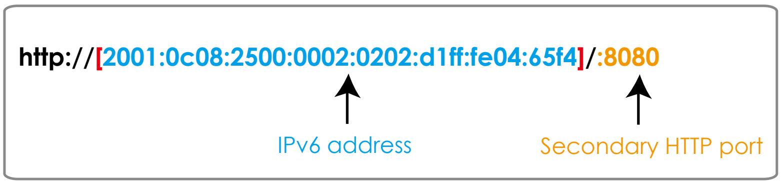


Network Camera - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address

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

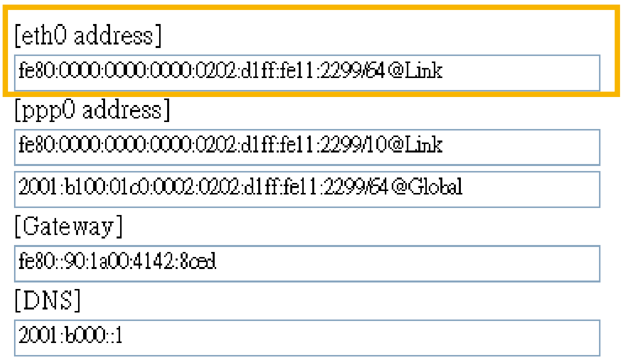
NOTE:

▶ *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** streaming on page 59 for detailed information.)*



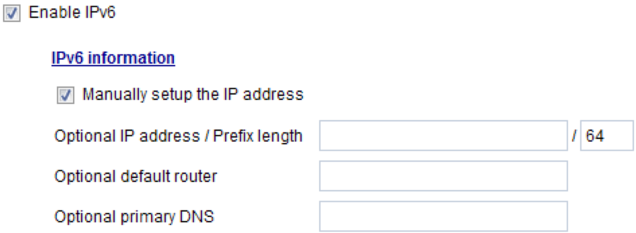
http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/:8080

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



☑ Enable IPv6

IPv6 information

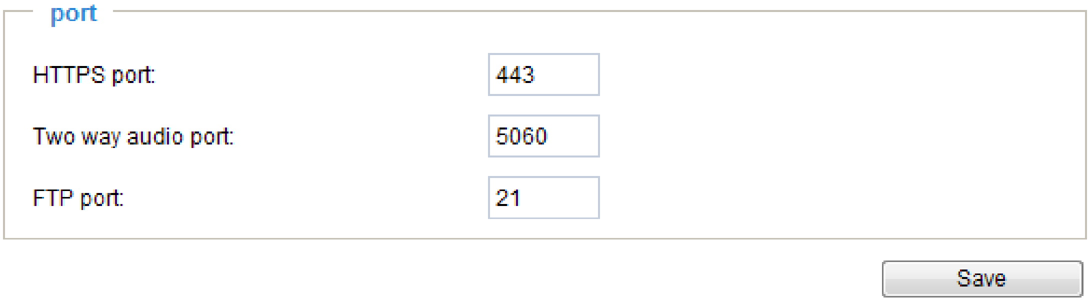
☑ Manually setup the IP address

Optional IP address / Prefix length ______ / 64

Optional default router ______

Optional primary DNS ______

Port



port

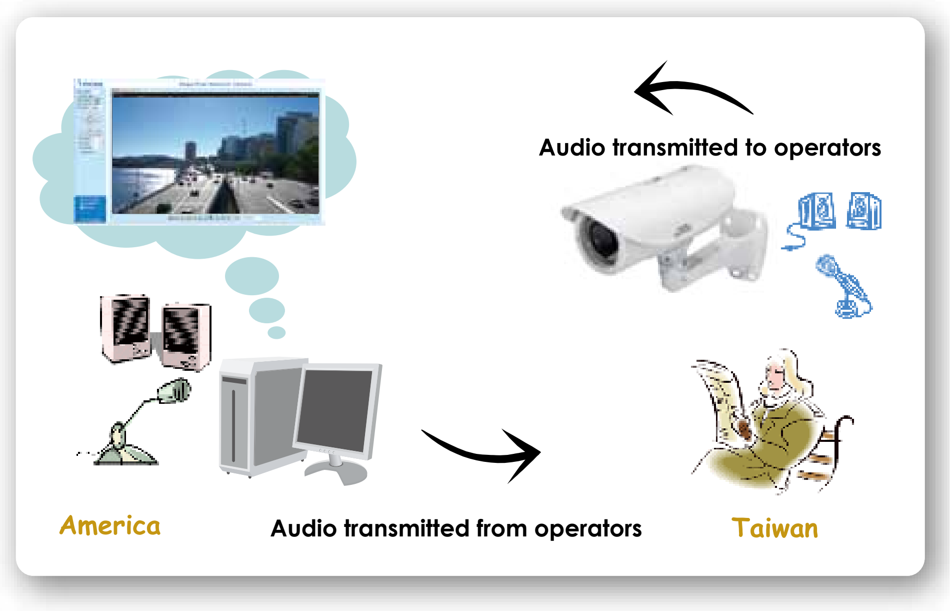
HTTPS port:	443
Two way audio port:	5060
FTP port:	21

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

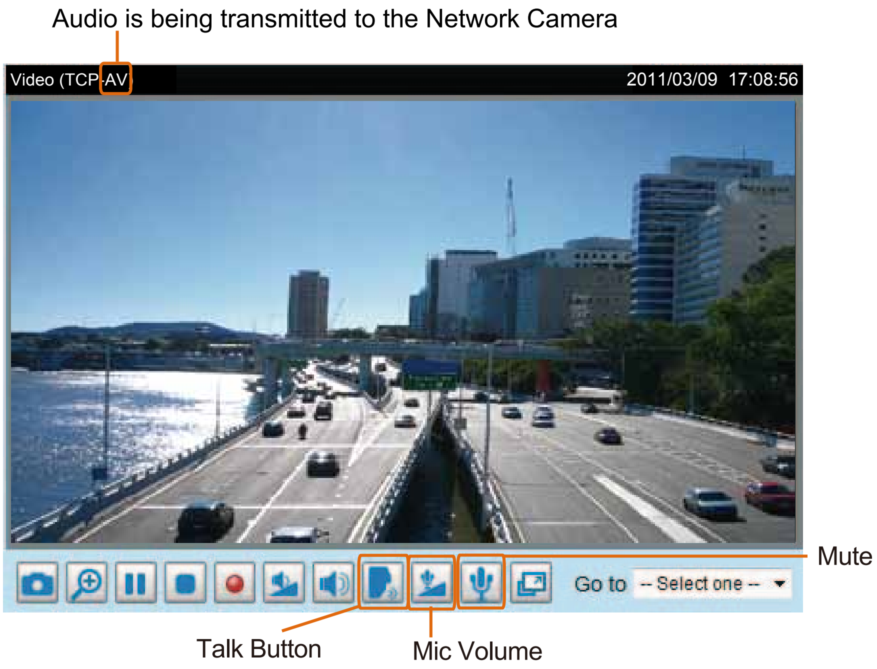
Two way audio port: By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number between 1025 and 65535.

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

Note that as JPEG only transmits a series of JPEG images to the client, to enable the two-way audio function, make sure the video mode is set to "MPEG-4" on the Media > Video > Stream settings page and the media option is set to "Media > Video > Stream settings" on the Client Settings page. Please refer to Client Settings on page 26 and Stream settings on page 77.



Audio transmitted to operators
America
Audio transmitted from operators
Taiwan



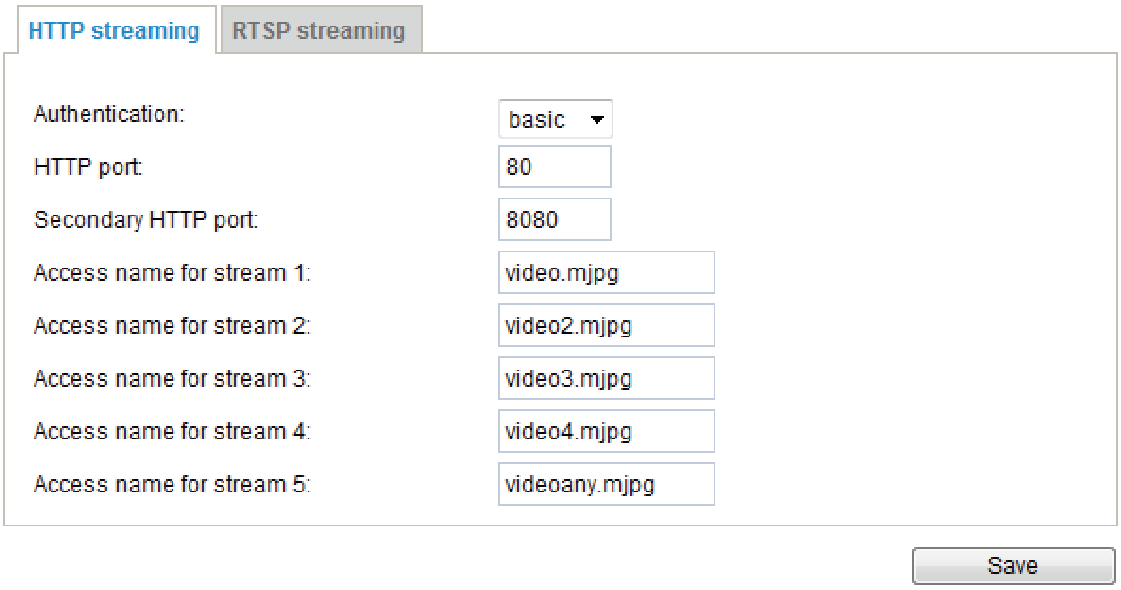
Click to enable audio transmission to the Network Camera; click to adjust the volume of microphone; click to turn off the audio. To stop talking, click again.

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

Network > Streaming protocols Advanced Mode

HTTP streaming

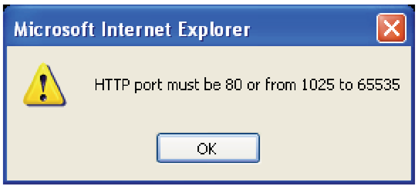
To utilize HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security > User account on page 40 for details.



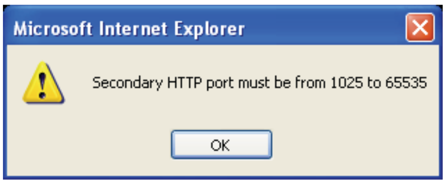
Authentication:	basic
HTTP port:	80
Secondary HTTP port:	8080
Access name for stream 1:	video.mjpg
Access name for stream 2:	video2.mjpg
Access name for stream 3:	video3.mjpg
Access name for stream 4:	video4.mjpg
Access name for stream 5:	videoany.mjpg

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:



HTTP port must be 80 or from 1025 to 65535



Secondary HTTP port must be from 1025 to 65535

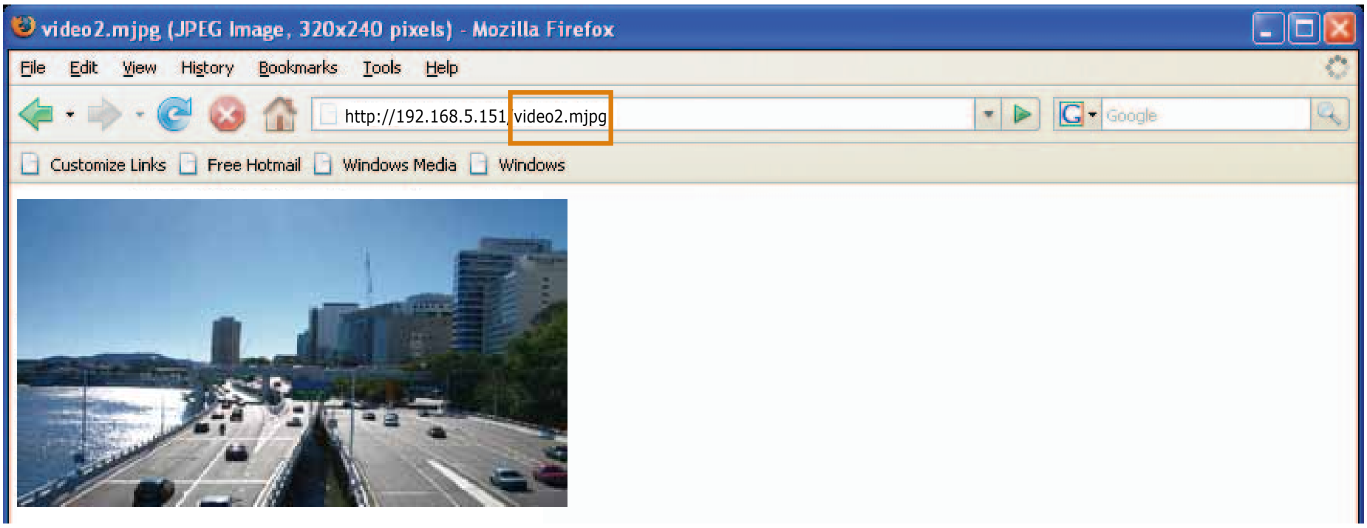
To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

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 **Media > Video > Stream settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Stream settings on page 77.

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.



http://192.168.5.151/video2.mjpg

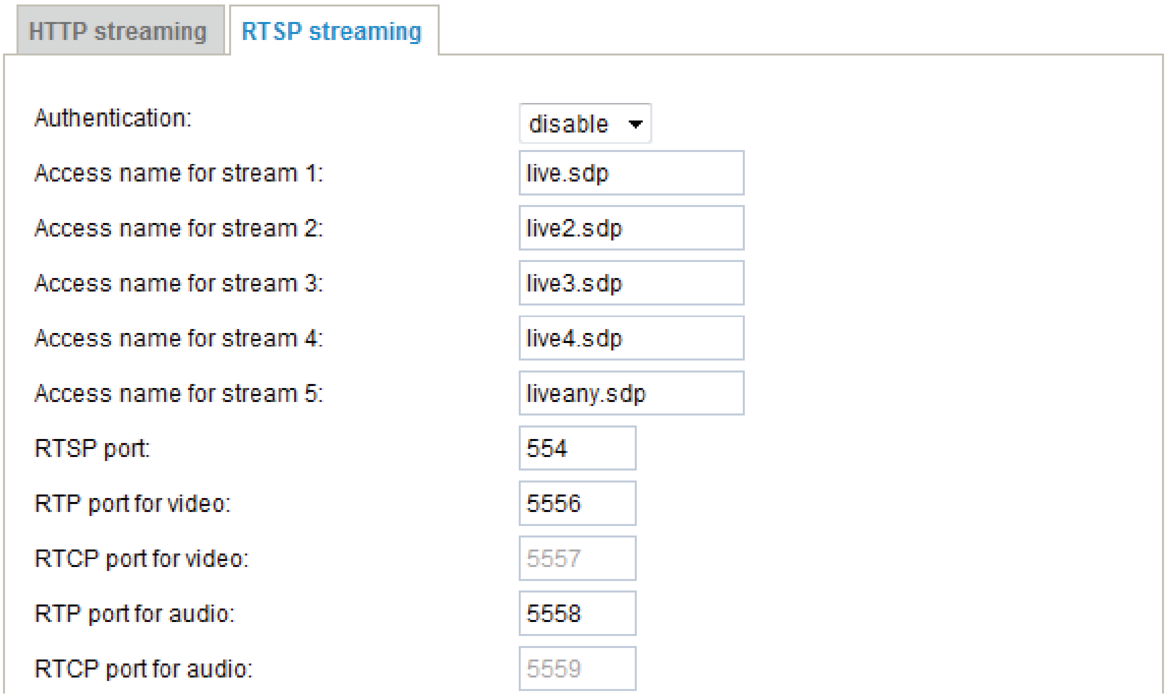
IMPORTANT:

▶ *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 110.*

RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for the Network Camera first; please refer to Security > User account on page 40 for details.



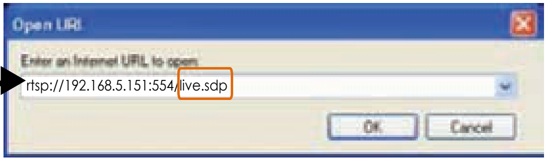
Authentication:	disable
Access name for stream 1:	live.sdp
Access name for stream 2:	live2.sdp
Access name for stream 3:	live3.sdp
Access name for stream 4:	live4.sdp
Access name for stream 5:	liveany.sdp
RTSP port:	554
RTP port for video:	5556
RTCP port for video:	5557
RTP port for audio:	5558
RTCP port for audio:	5559

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 of the corresponding stream 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:

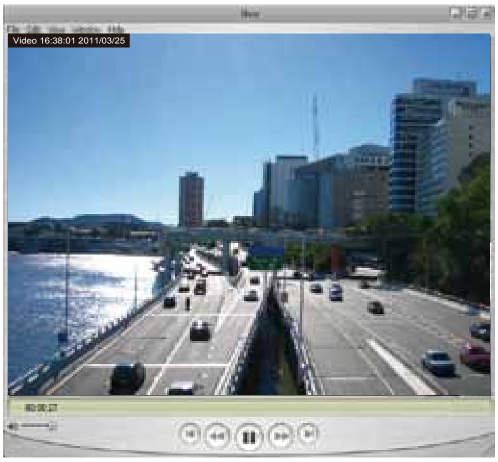
1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the above URL command in the address field.
4. The live video will be displayed in your player as shown below.



Open URL

Enter an Internet URL to open:

rtsp://192.168.5.151:554/live.sdp



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

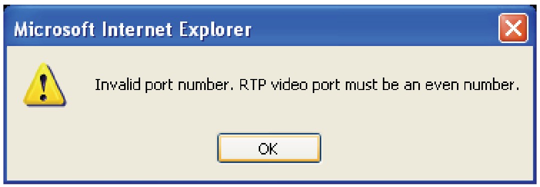
- ■ RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

- ■ The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.

- ■ The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

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

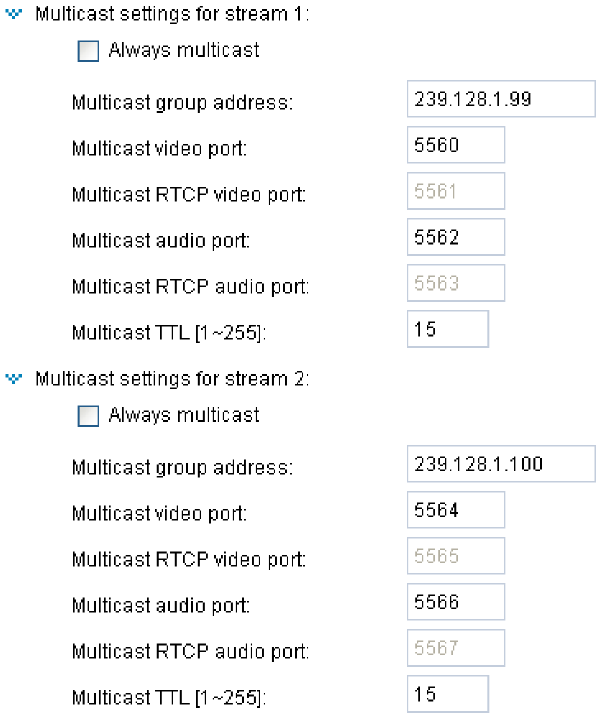
If the RTP ports are incorrectly assigned, the following warning message will be displayed:



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 audio port:	5562
Multicast RTCP audio port:	5563
Multicast TTL [1~255]:	15

Multicast settings for stream 2:

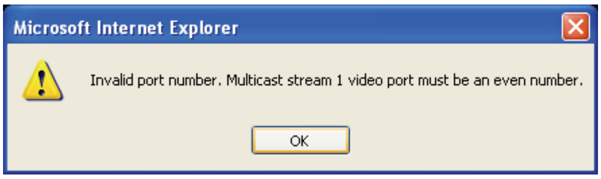
□ Always multicast

Multicast group address:	239.128.1.100
Multicast video port:	5564
Multicast RTCP video port:	5565
Multicast audio port:	5566
Multicast RTCP audio port:	5567
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.

Network > QoS (Quality of Service) Advanced Mode

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

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

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

Requirements for QoS

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

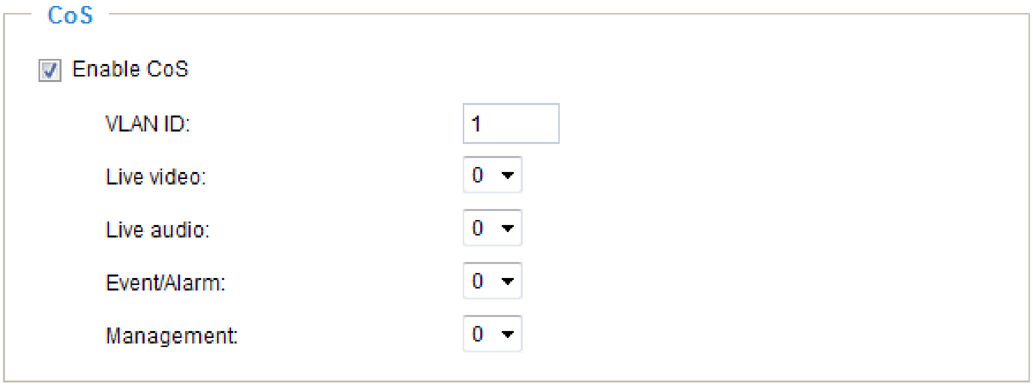
- All network switches and routers in the network must include support for QoS.
- The network video devices used in the network must be QoS-enabled.

QoS models

CoS (the VLAN 802.1p model)

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

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



CoS

☑ Enable CoS

VLAN ID:	1
Live video:	0
Live audio:	0
Event/Alarm:	0
Management:	0

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

NOTE:

▶ *A VLAN Switch (802.1p) is required. Web browsing may fail if the CoS setting is incorrect.*

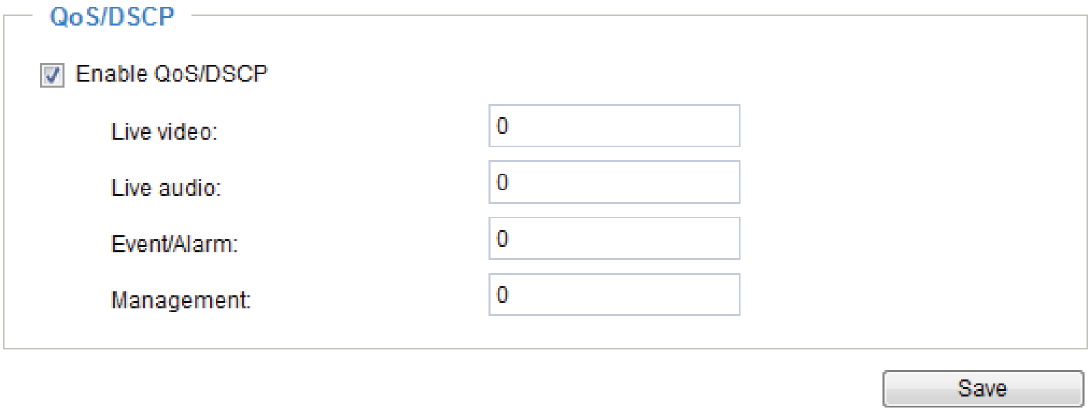
▶ *Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.*

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

QoS/DSCP (the DiffServ model)

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

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



QoS/DSCP

☑ Enable QoS/DSCP

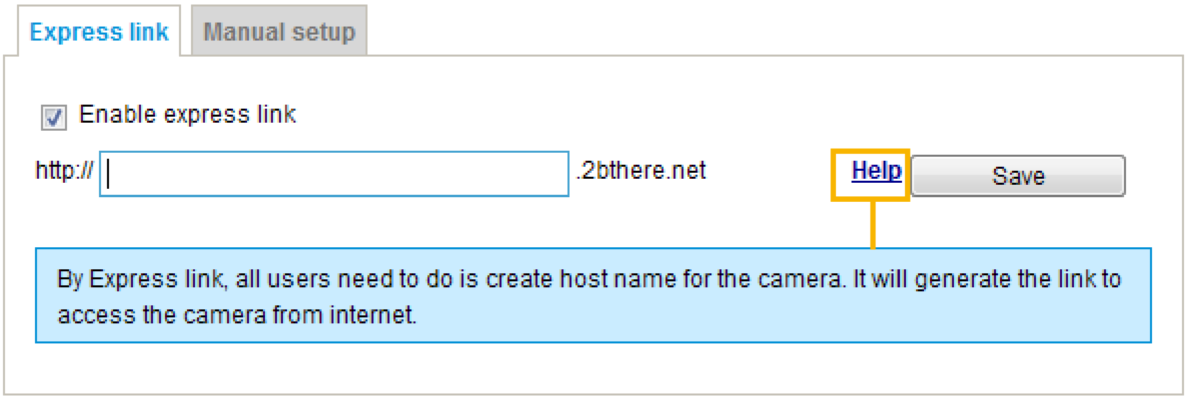
Live video:	0
Live audio:	0
Event/Alarm:	0
Management:	0

Network > DDNS

This section explains how to configure the dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

Express link

Express Link is a free service provided by VIVOTEK server, which allows users to register a domain name for a network device. One URL can only be mapped to one MAC address. This service will check out if the host name is valid and automatically open a port on your router. Unlike DDNS, which requires a user to manually check out details about UPnP port forwarding, the Express Link is more convenient and easy to set up.



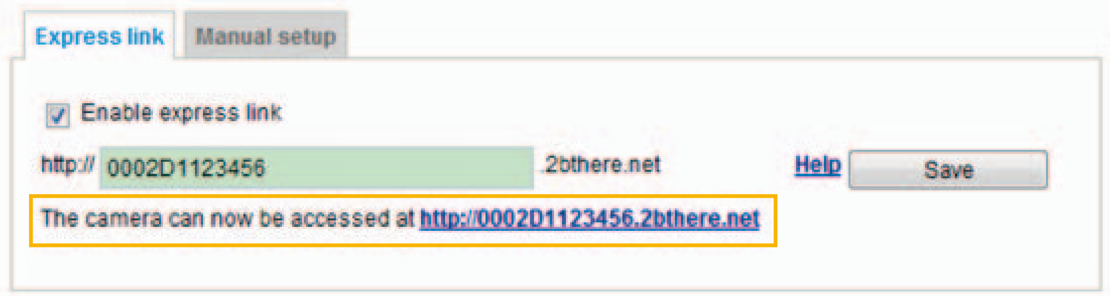
☑ Enable express link

http:// .2bthere.net

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

Please follow the steps below to enable Express Link:

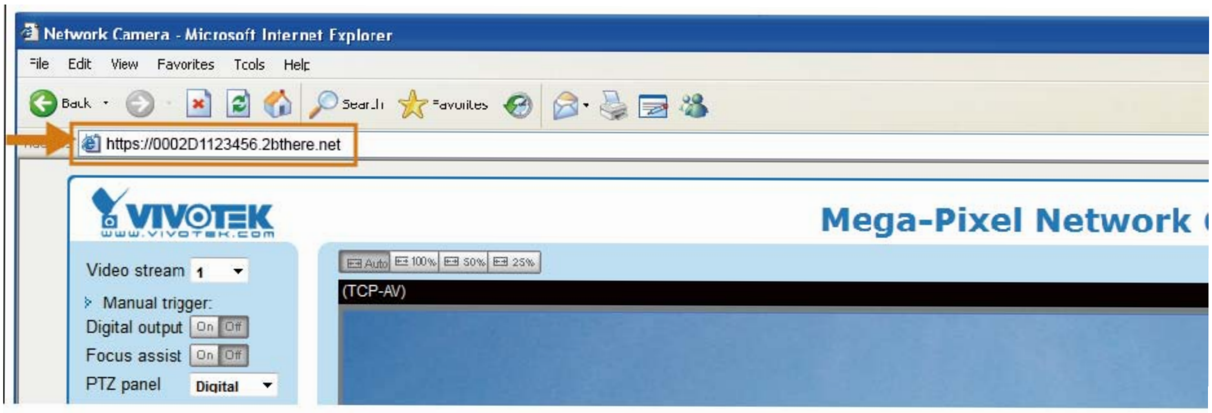
1. Make sure that your router supports UPnP port forwarding and it is activated, or you may see the following warning message: Express link is not supported under current network environment.
2. Check **Enable express link**.
3. Enter a host name for the network device and click **Save**. If the host name has been used by another device, a warning message will show up. If the host name is valid, it will show a message as shown below.



☑ Enable express link

http:// 0002D1123456 .2bthere.net

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



https://0002D1123456.2bthere.net

Video stream 1

Manual trigger:

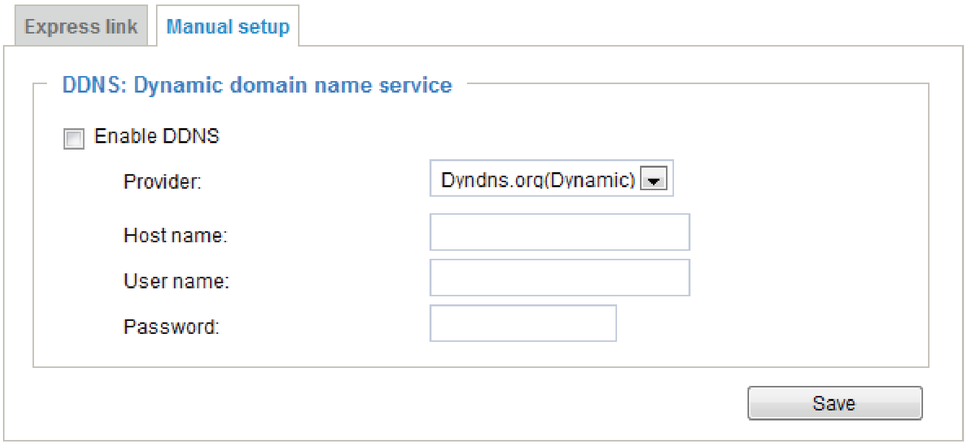
Digital output On Off

Focus assist On Off

PTZ panel Digital

Manual setup

DDNS: Dynamic domain name service



DDNS: Dynamic domain name service

□ Enable DDNS

Provider: Dyndns.org(Dynamic)

Host name:

User name:

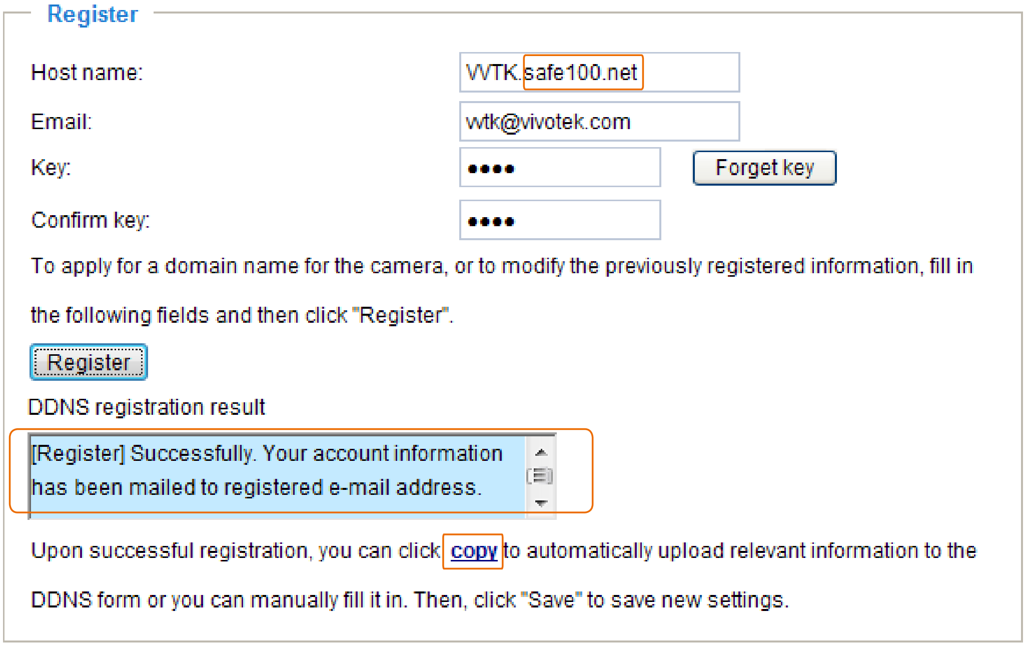
Password:

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: wtk@vivotek.com

Key: ••••

Confirm key: ••••

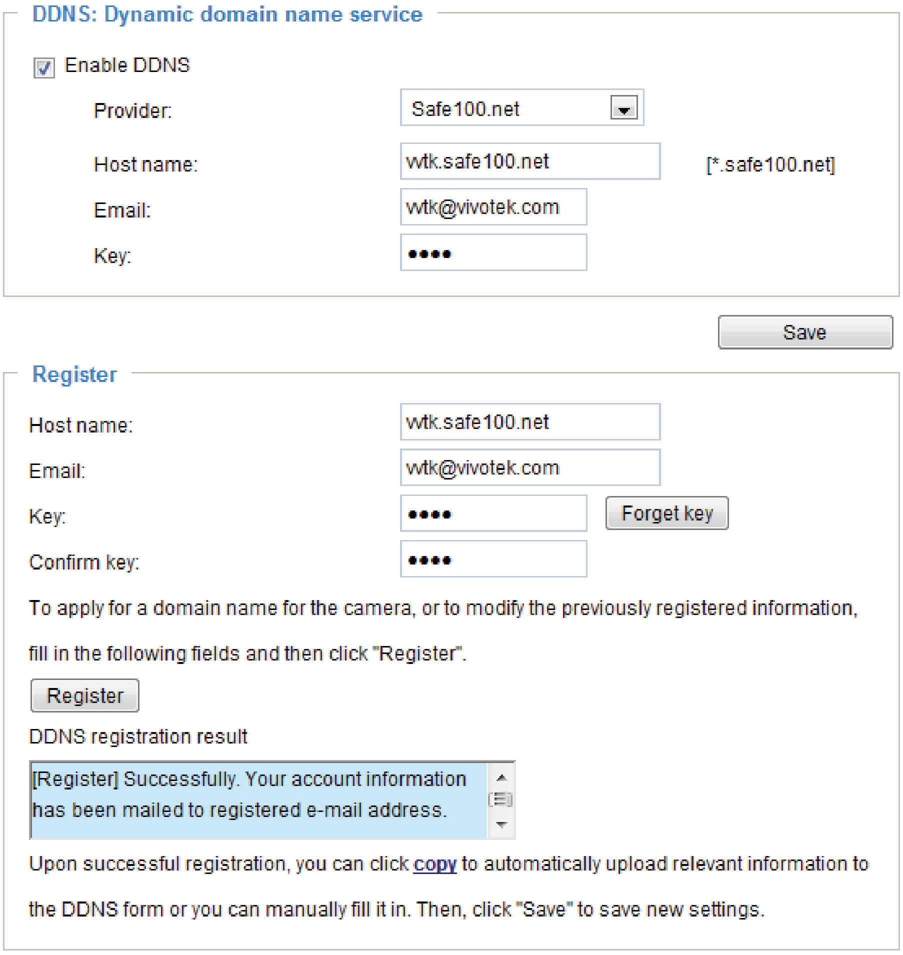
To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".

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 following screen.



DDNS: Dynamic domain name service

☑ Enable DDNS

Provider:	Safe100.net	
Host name:	wtk.safe100.net	[*.safe100.net]
Email:	wtk@vivotek.com	
Key:	••••	

Register

Host name:	wtk.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".

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/

Network > SNMP (Simple Network Management Protocol)

Advanced Mode

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

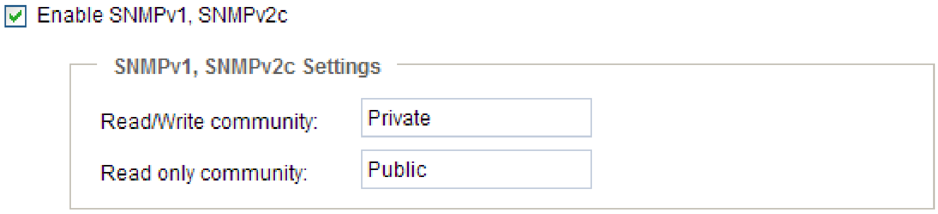
■ The SNMP consists of the following three key components:
1. Manager: Network-management station (NMS), a server which executes applications that monitor and control managed devices.
2. Agent: A network-management software module on a managed device which transfers the status of managed devices to the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

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

SNMP Configuration

Enable SNMPv1, SNMPv2c

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



☑ Enable SNMPv1, SNMPv2c

SNMPv1, SNMPv2c Settings

Read/Write community:	Private
Read only community:	Public

Enable SNMPv3

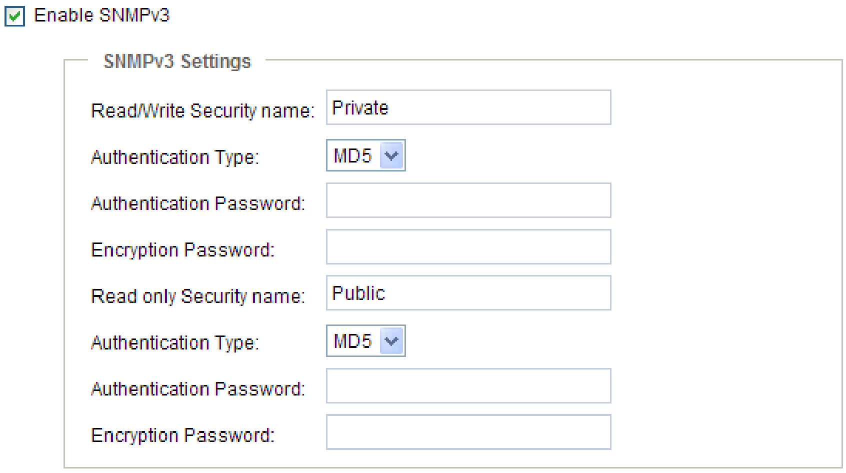
This option contains cryptographic security, a higher security level, which allows you to set the Authentication password and the Encryption password.

■ 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

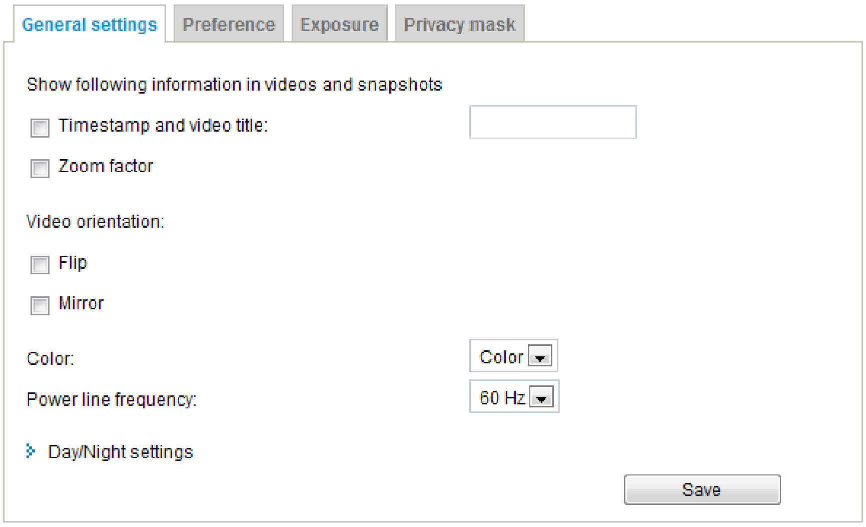
SNMPv3 Settings

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

Media > Image Advanced Mode

This section explains how to configure the image settings of the Network Camera. It is composed of the following four columns: General settings, Preference, Exposure, and Privacy mask.

General settings



Show following information in videos and snapshots

□ Timestamp and video title:

□ Zoom factor

Video orientation:

□ Flip

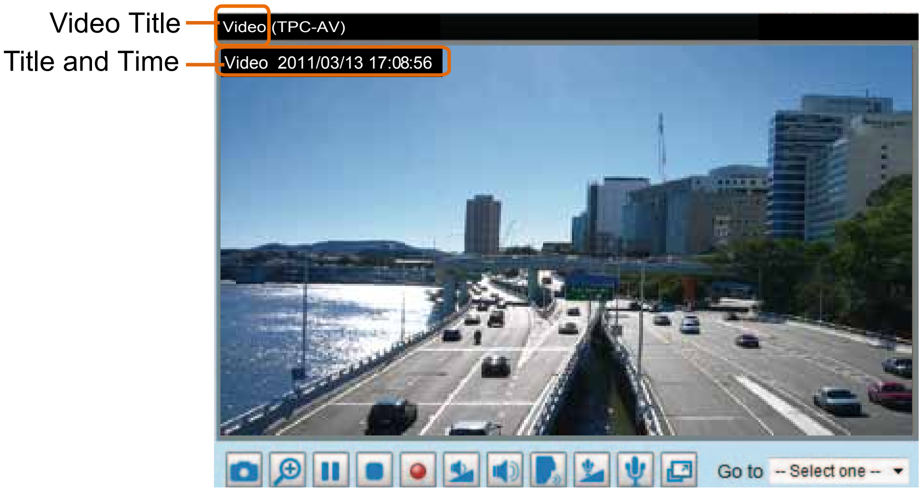
□ Mirror

Color: Color

Power line frequency: 60 Hz

Timestamp and video title: Enter a name that will be displayed on the title bar of the live video as the picture shown below.

Zoom factor: If you check this item, the zoom indicator will be displayed on the Home page when you zoom in/out the live viewing window as the picture shown below. You may zoom in/out the image by scrolling the mouse inside the live viewing window.

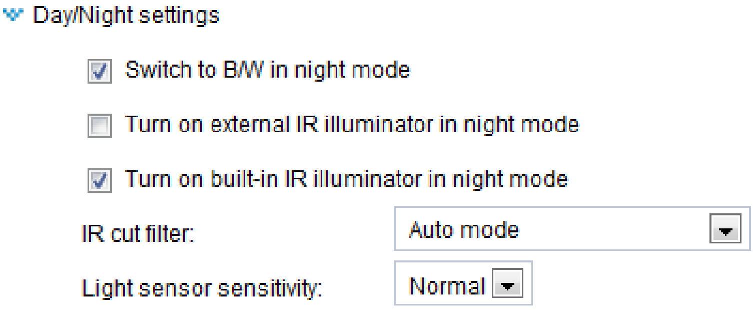


Video orientation: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (ex. on the ceiling) to correct the image orientation. Please note that the preset locations will be cleared after flip/mirror.

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

Power line frequency: Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

Day/Night Settings



Day/Night settings

☑ Switch to B/W in night mode

☐ Turn on external IR illuminator in night mode

☑ Turn on built-in IR illuminator in night mode

IR cut filter: Auto mode

Light sensor sensitivity: Normal

Switch to B/W in night mode
Select this checkbox to enable the Network Camera to automatically switch to Black & White display during the night mode.

Turn on external IR illuminator in night mode
If you install external IR illuminator along with your camera with digital input signals, you can turn on the external illuminators when the camera enters the night mode.

Turn on built-in IR illuminator in night mode
Select this checkbox for the camera to turn on its IR illuminators during the night mode situations.

IR cut filter
With a removable IR-cut filter, this Network Camera can automatically remove the filter to let Infrared light pass 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, turn on the IR illuminators, and thus helping to improve low light sensitivity.

■ Synchronize with digital input
The Network Camera automatically removes the IR cut filter when DI triggers.

■ 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.

Preference

On this page, you can tune the Image adjustment parameters. You can configure two sets of preferred settings: one for normal situations, the other for special situations, such as day/night/schedule mode.

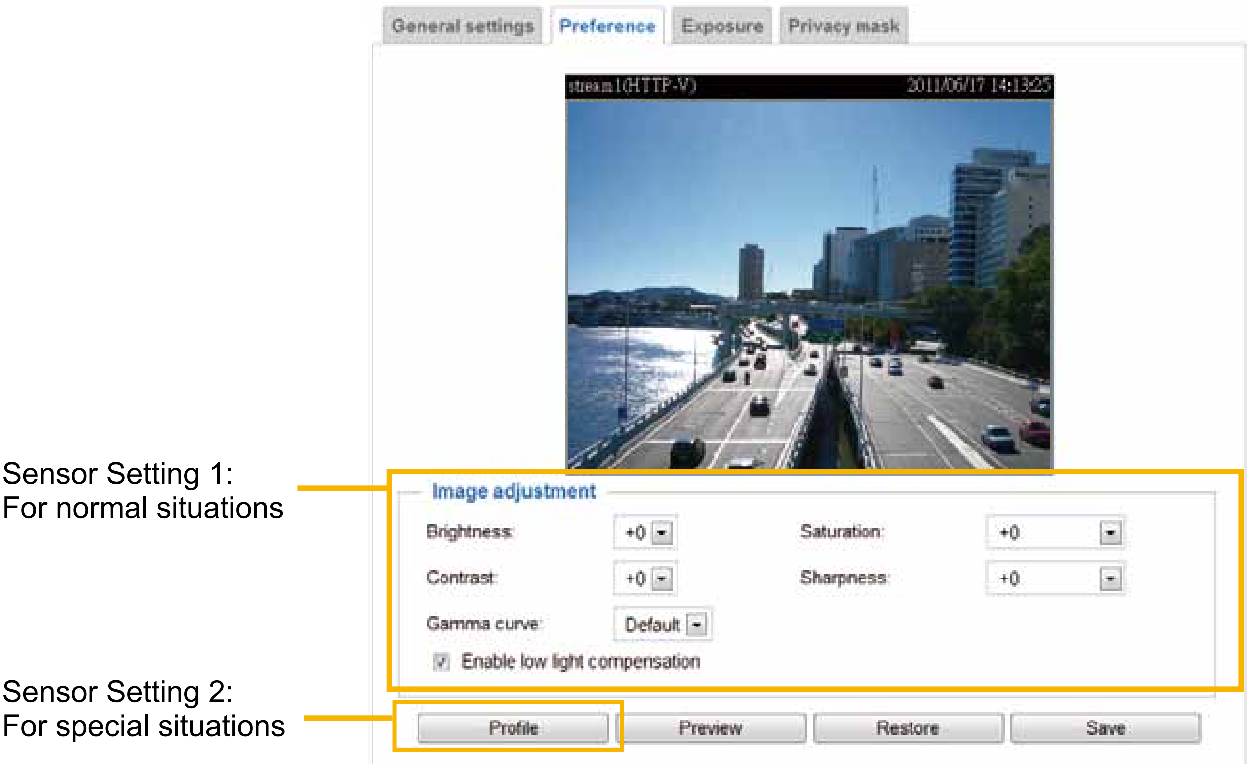


Image Adjustment

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

■ Saturation: Adjust the image saturation level, which ranges from -5 to +5. You can also select **Customize** and manually enter a value.

■ Contrast: Adjust the image contrast level, which ranges from -5 to +5. Please note that this function will be disabled if you enable WRD enhancement in the column below.

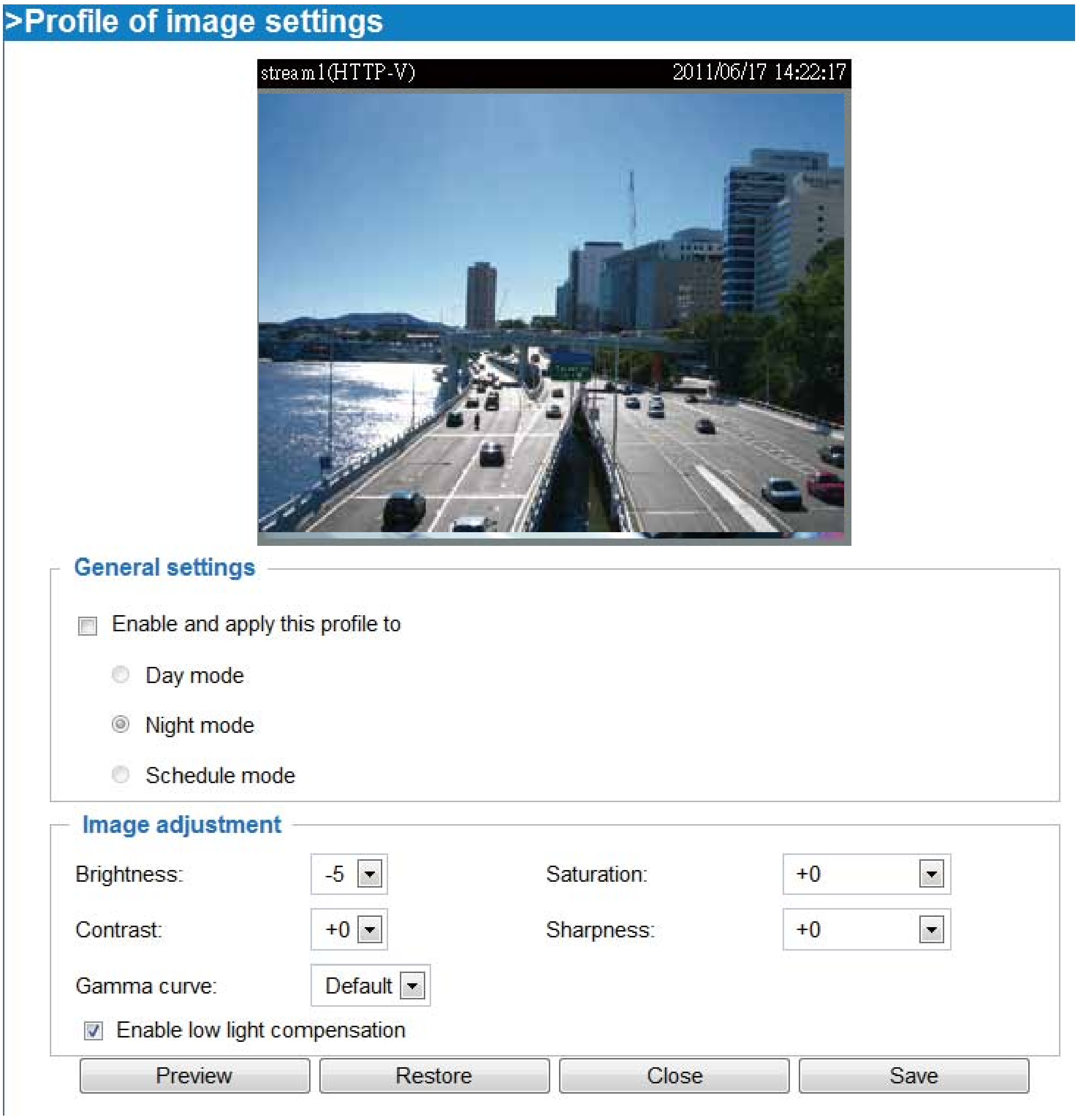
■ Sharpness: Adjust the image sharpness level, which ranges from -3 to +3. You can also select **Customize** and manually enter a value.

■ Gamma curve: This function is for user to select a proper gamma curve value to adjust the gray-scale of the monitor.

■ Enable low light compensation: Select this option in low light mode, and the values of sharpness and brightness will change automatically as the noise reduction function.

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.

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



>Profile of image settings

stream1(HTTP-V) 2011/06/17 14:22:17

General settings

□ Enable and apply this profile to

○ Day mode

● Night mode

○ Schedule mode

Image adjustment

Brightness: -5

Saturation: +0

Contrast: +0

Sharpness: +0

Gamma curve: Default

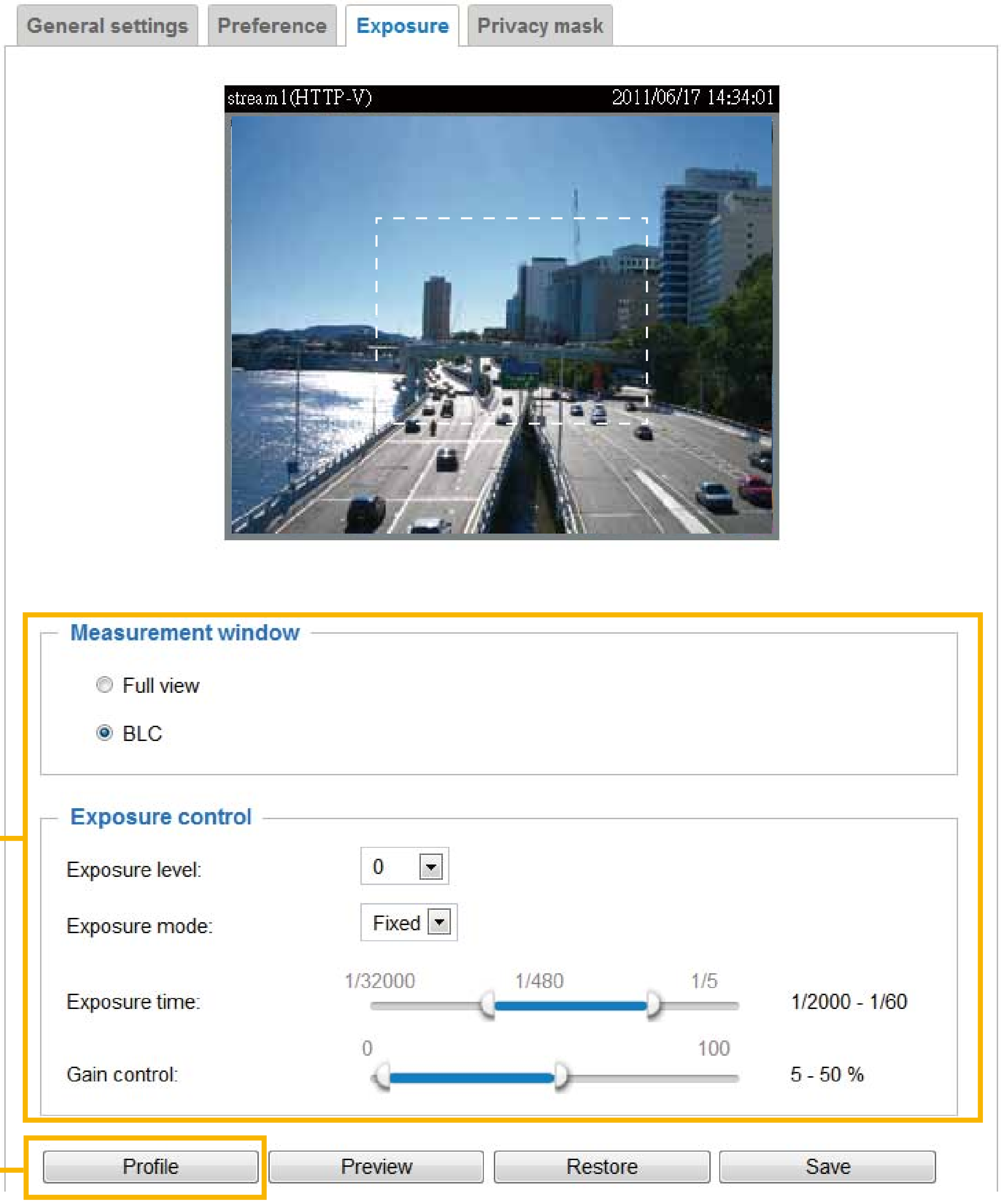
☑ Enable low light compensation

Please follow the steps below to setup a profile:

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

Exposure Advanced Mode

On this page, you can set the Exposure measurement window, Exposure level, Exposure mode, Exposure time, and Gain control settings. You can configure two sets of Exposure settings: one for normal situations, the other for special situations, such as day/night/schedule mode.



Measurement window

○ Full view

● BLC

Exposure control

Exposure level: 0

Exposure mode: Fixed

Exposure time: 1/2000 - 1/60

Gain control: 5 - 50 %

Sensor Setting 1:
For normal situations

Sensor Setting 2:
For special situations

Measurement Window: This function allows users to set measurement window(s) for low light compesation.

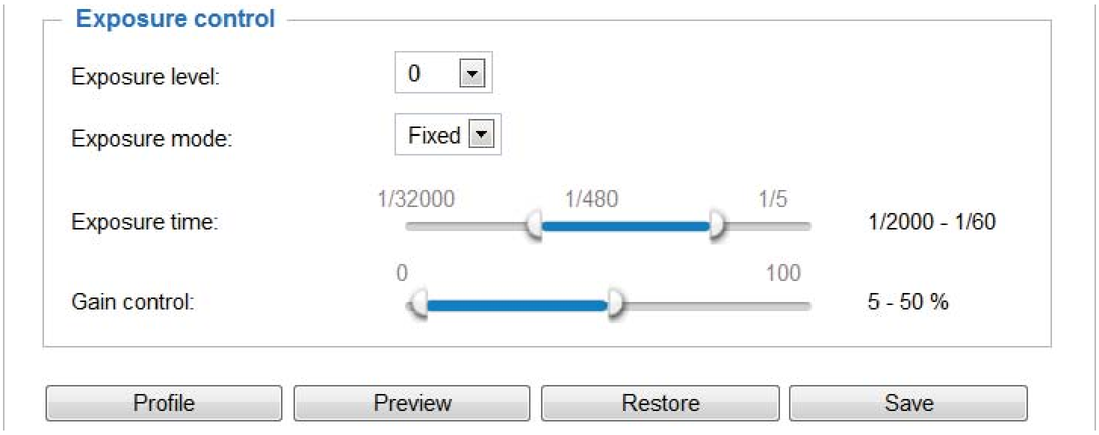
■ Full view: Calculate the full range of view and offer appropriate light compesation.

BLC (Back Light Compensation): This option will automatically add a “weighted region“ in the middle of the window and give the necessary light compensation. A white bracket will appear as the area of interest for backlight compensation.

Exposure control:

■ Exposure level: You can manually set the Exposure level, which ranges from -2.0 to +2.0 (dark to bright).

■ Exposure mode: Select **Auto** or **Fixed** mode according to your needs.
Fixed: Select **Fixed** to set a fixed exposure time and gain. Then, tune the slider bar to set the Exposure time and Gain Control to the best image quality. A shorter exposure time allows less amount of light to enter the sensor; while a higher gain control value generates certain amount of noises.



Exposure control

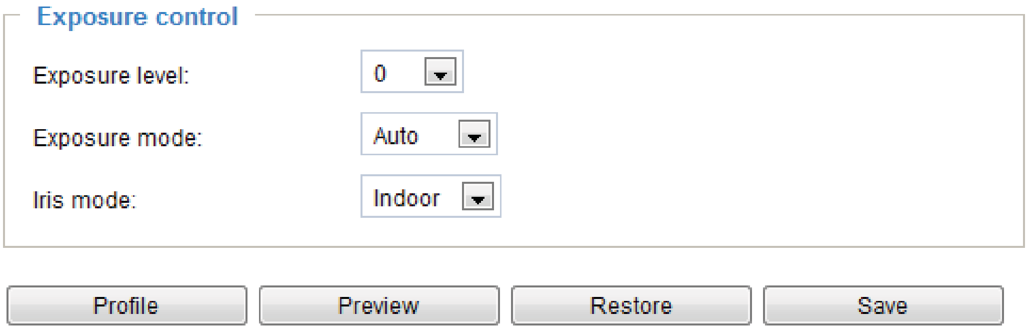
Exposure level: 0

Exposure mode: Fixed

Exposure time: 1/2000 - 1/60

Gain control: 5 - 50 %

Auto: If you set Exposure mode as **Auto**, the Exposure time and Gain control will be not configurable since the sensor library will automatically adjust the value according to the ambient light. Then you can set iris mode as “indoor” or “outdoor” to reach the best image quality.



Exposure control

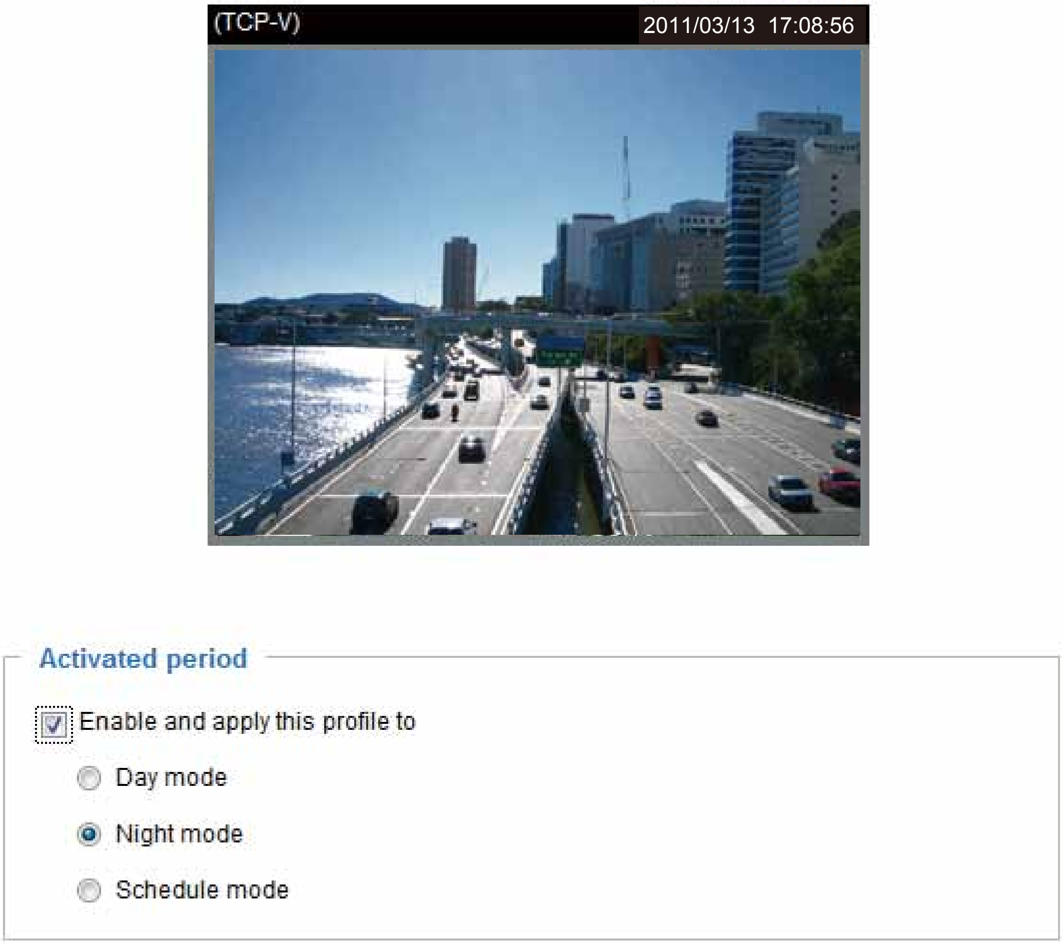
Exposure level: 0

Exposure mode: Auto

Iris mode: Indoor

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.

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



Activated period

☑ Enable and apply this profile to

○ Day mode

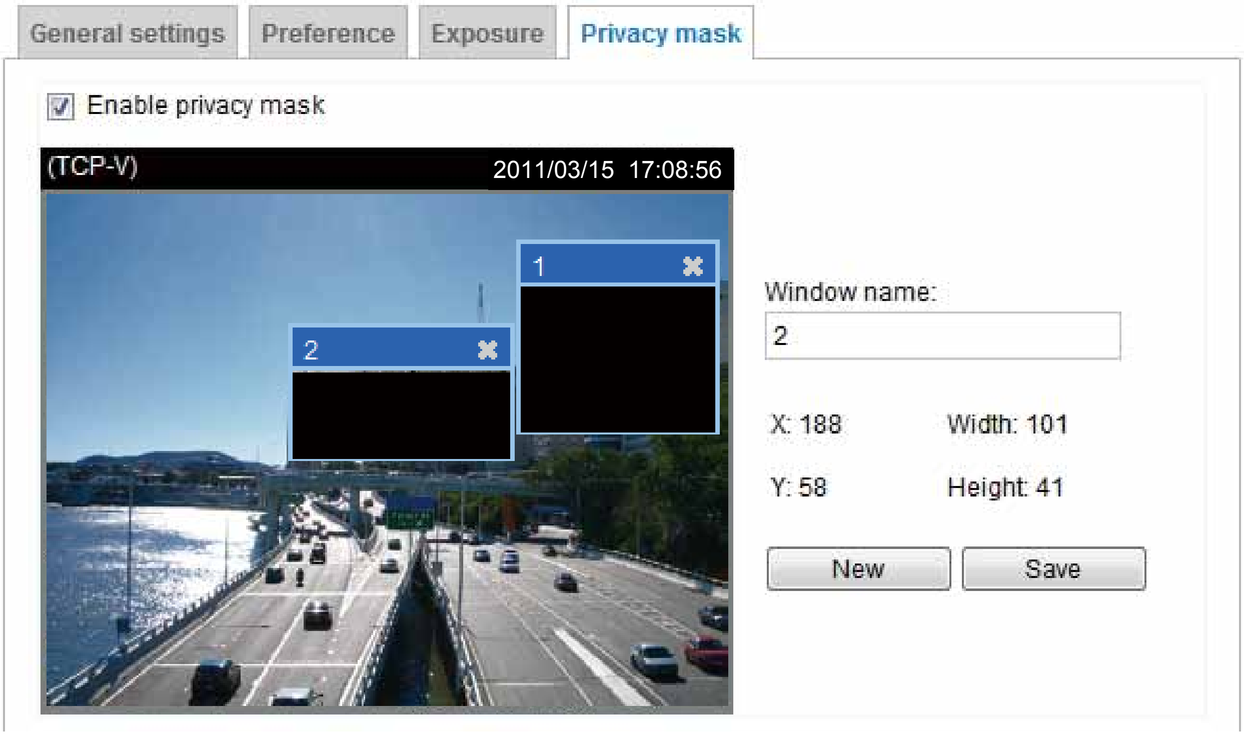
● Night mode

○ Schedule mode

Please follow the steps below to setup a profile:
1. Check **Enable and apply this profile**.
2. Select the applied mode: Day mode, Night mode, or Schedule mode. Please manually enter a range of time through which you want the Schedule mode to apply.
3. Configure **Exposure control** settings in the folowing columns. Please refer to the previous page for detailed information.
4. Click **Save** to enable the setting and click **Close** to exit the page.

Privacy mask Advanced Mode

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



☑ Enable privacy mask

Window name: 2

X: 188 Width: 101

Y: 58 Height: 41

■ 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. Check **Enable privacy mask** to enable this function.

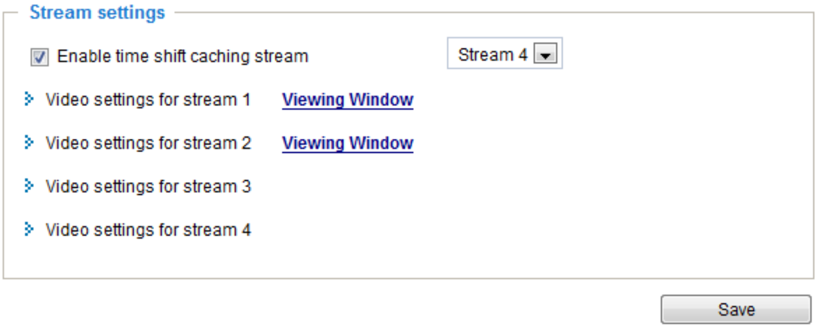
NOTE:

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

▶ *If you want to delete a configured mask window, click on the 'X' button at the upper right corner of the window.*

Media > Video

Stream settings Advanced Mode



Stream settings

☑ Enable time shift caching stream   Stream 4

Video settings for stream 1   Viewing Window

Video settings for stream 2   Viewing Window

Video settings for stream 3

Video settings for stream 4

Enable time shift caching stream: Select one stream as the time shift cache stream. This function enable the time shift cache stream on the Network Camera, which will store video in the camera's embedded memory for a period of time depending on the cache memory size on each Network Camera. This function can work seamlessly with VIVOTEK's ST7501 recording software. When an event occurs, the recording software can request time shift cache stream from the camera, which allows users to retrieve video footages taken before the occurence of an event.

This Network Camera supports multiple streams with frame size ranging from 176 x 144 to 1280 x 1024.

The definition of multiple streams:

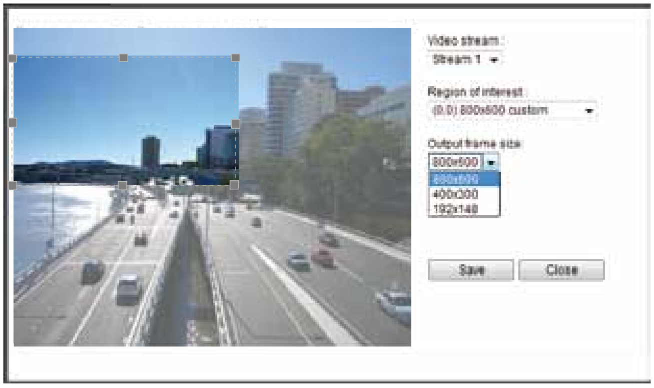
■ Stream 1: Users can define the "Region of Interest" (viewing region) and the "Output Frame Rate" (size of the live view window).

■ 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 "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 and 2.



Video stream: Stream 1

Region of interest: (0,0) 800x600 custom

Output frame size: 800x600

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

1. Select a stream to configure its viewing region.
2. Select a **Region of Interest** from the drop-down list. The floating frame, the same as the one in the Gloabl View window on the home page, will resize accordingly. To set up a customized viewing region, you can also resize and re-position 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 monitored device.

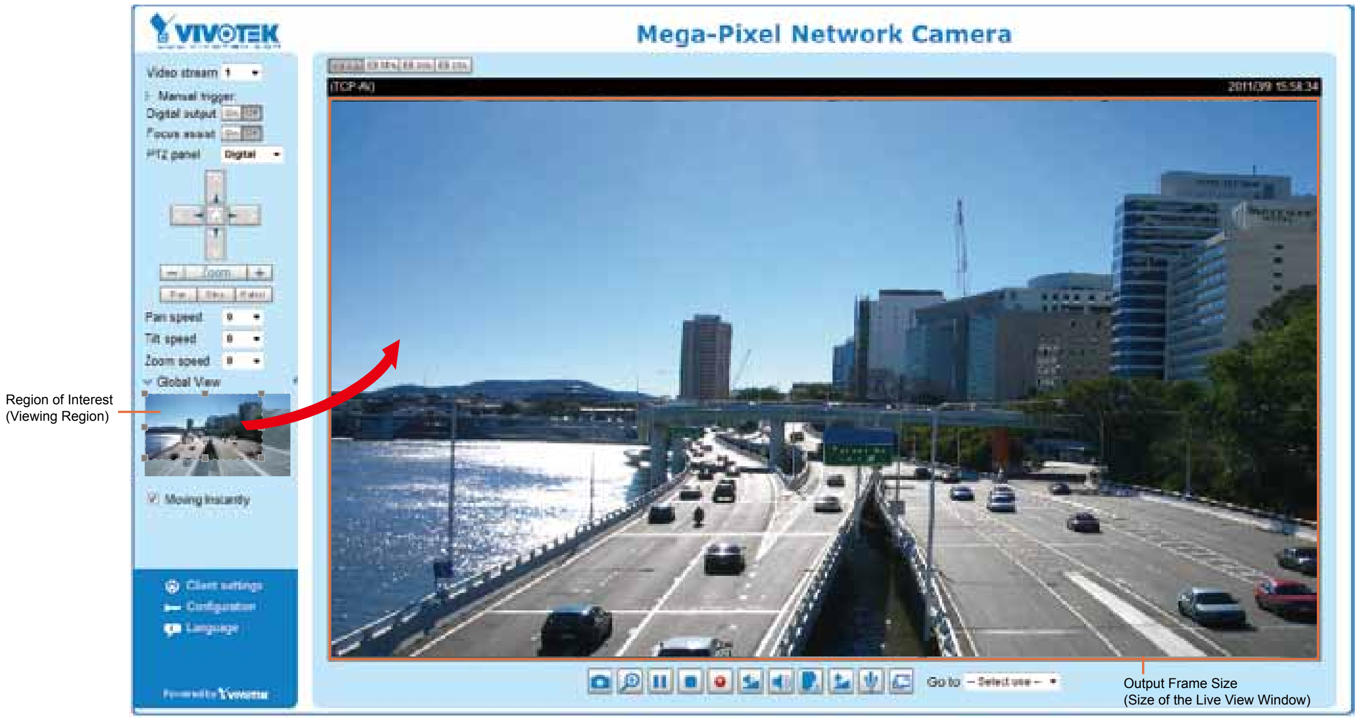
NOTE:

► *All the items in the "Region of Interest" cannot be greater than the "Output Frame Size" (current maximum resolution).*

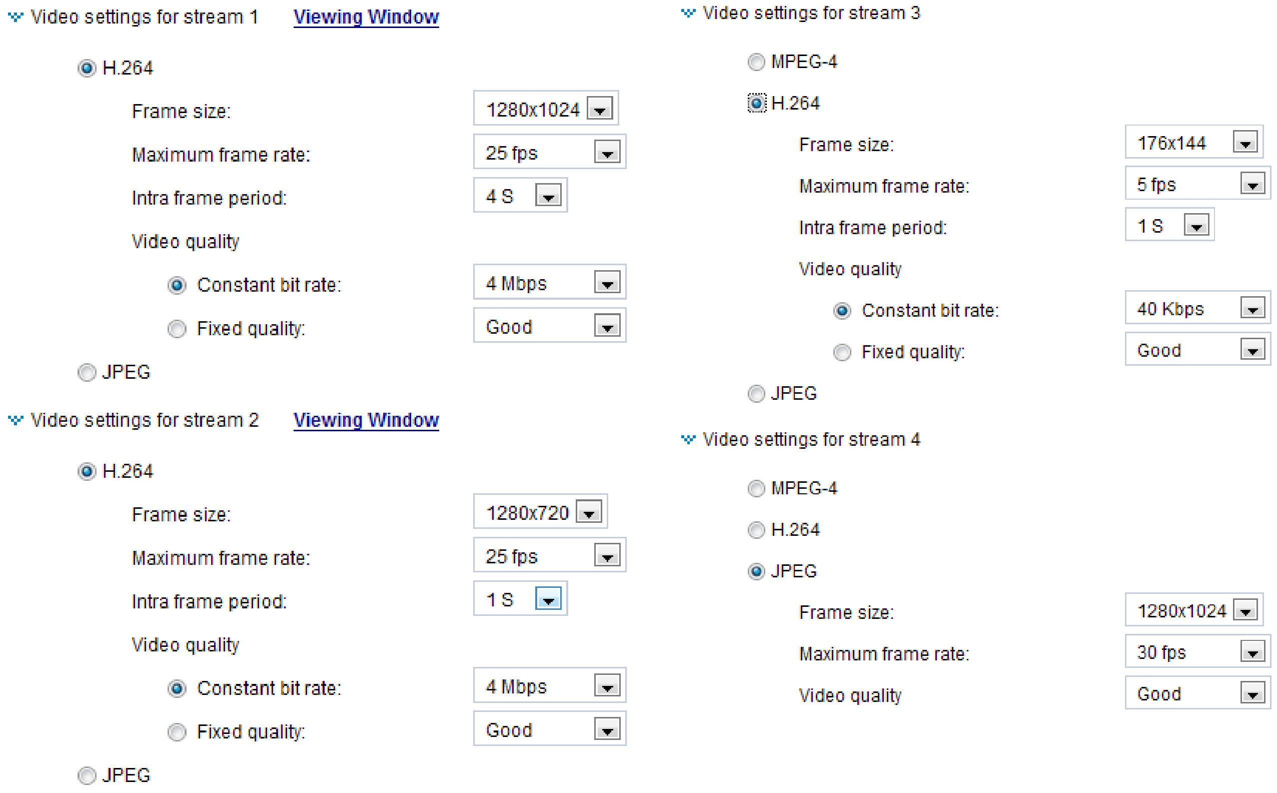
■ The parameters of the multiple streams:

	Region of Interest	Output frame size
Stream 1	1280 X 1024 ~ 176 x 144 (Selectable)	1280 X 1024 ~ 176 x 144 (Selectable)
Stream 2	1280 X 1024 ~ 176 x 144 (Selectable)	1280 X 1024 ~ 176 x 144 (Selectable)
Stream 3	non-configurable (Fixed)	1280 X 1024 ~ 176 x 144 (Selectable)
Stream 4	1280 X 1024 (Fixed)	1280 X 1024 ~ 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 each video stream. Then you can go back to the home page to test the e-PTZ function. For more information about the e-PTZ function, please refer to page 82.



Click the stream item to display the detailed information. The maximum frame size will follow your settings in the above **Viewing Window** sections.



Video settings for stream 1 Viewing Window

● H.264

Frame size: 1280x1024
Maximum frame rate: 25 fps
Intra frame period: 4 S
Video quality
● Constant bit rate: 4 Mbps
○ Fixed quality: Good

○ JPEG

Video settings for stream 2 Viewing Window

● H.264

Frame size: 1280x720
Maximum frame rate: 25 fps
Intra frame period: 1 S
Video quality
● Constant bit rate: 4 Mbps
○ Fixed quality: Good

○ JPEG

Video settings for stream 3

○ MPEG-4

● H.264

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

○ JPEG

Video settings for stream 4

○ MPEG-4

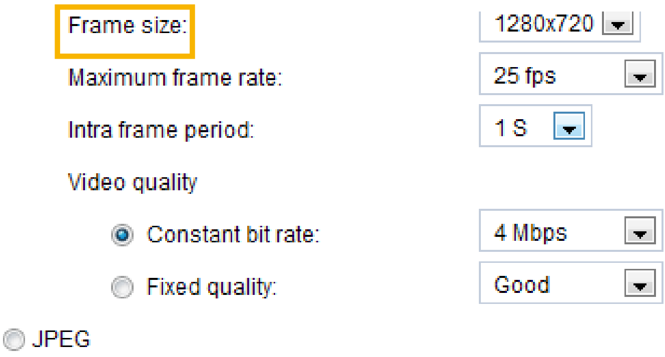
○ H.264

● JPEG

Frame size: 1280x1024
Maximum frame rate: 30 fps
Video quality Good

This Network Camera offers real-time H.264, MPEG-4 and MJPEG compression standards (Triple Codec) for real-time viewing.

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:



Frame size: 1280x720
Maximum frame rate: 25 fps
Intra frame period: 1 S
Video quality
● Constant bit rate: 4 Mbps
○ Fixed quality: Good

○ JPEG

■ Frame size

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

■ Maximum frame rate

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

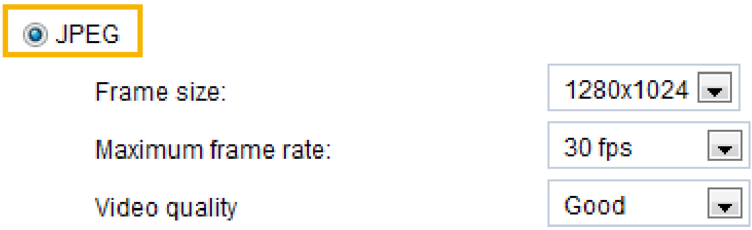
If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 50fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, 30fps, and 60fps. 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, 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: 1280x1024

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.
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.

■ 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.

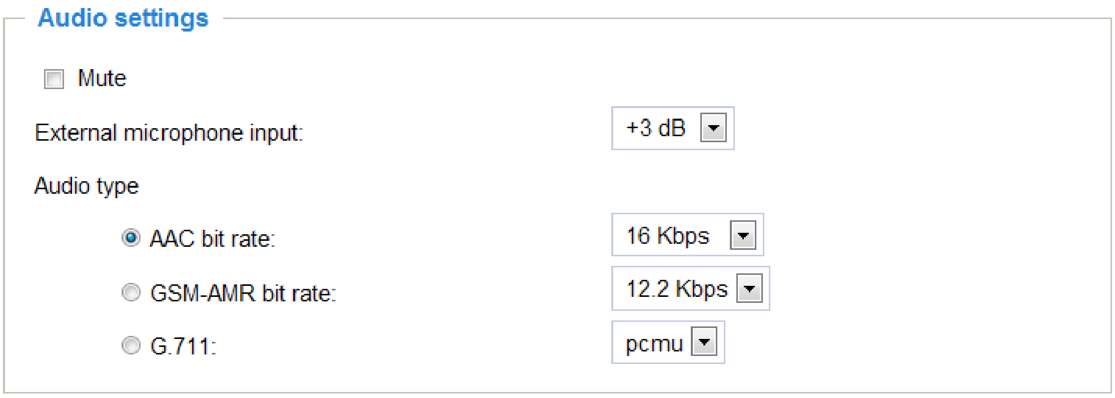
NOTE:

► *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 event of occurance, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

Media > Audio

Audio Settings



Audio settings

□ Mute

External microphone input: +3 dB

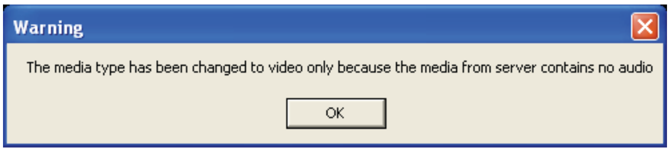
Audio type

● AAC bit rate: 16 Kbps

○ GSM-AMR bit rate: 12.2 Kbps

○ G.711: pcmu

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



Warning

The media type has been changed to video only because the media from server contains no audio

External microphone input: Select the gain of the external audio input according to ambient conditions. Adjust the gain from +33 db (most sensitive) down to -12 db (least sensitive).

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

- AAC provides good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable from: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps, and 128Kbps.
- GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable from: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps, and 12.2Kbps.
- G.711 also provides good sound quality and requires about 64Kbps. Select pcmu (μ-Law) or pcma (A-Law) mode.

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

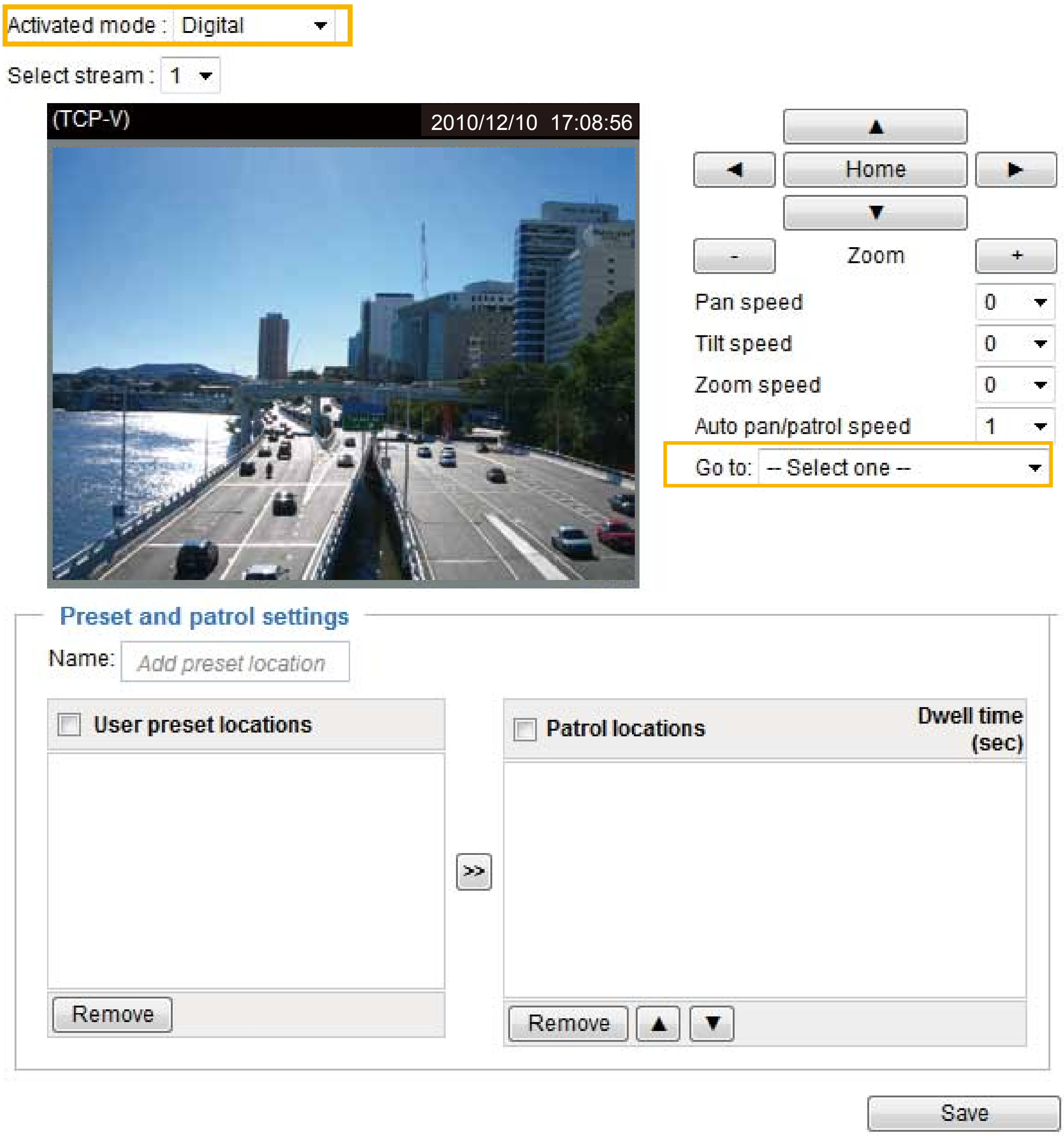
PTZ > PTZ settings Advanced Mode

This section explains how to control the Network Camera's Pan/Tilt/Zoom operation. This panel only works when a streaming view is not showing the full of the camera's largest frame size. For example, when showing a 800x600 frame out of the 1280x1024 full frame.

Digital: Control the e-PTZ operation. It allows users to quickly move the focus to a pre-configured target area for close-up viewing without physically zooming the camera.

Digital PTZ Operation (E-PTZ Operation)

If you select "Digital", the e-PTZ control settings section will be displayed as shown below:



Activated mode : Digital

Select stream : 1

Pan speed: 0

Tilt speed: 0

Zoom speed: 0

Auto pan/patrol speed: 1

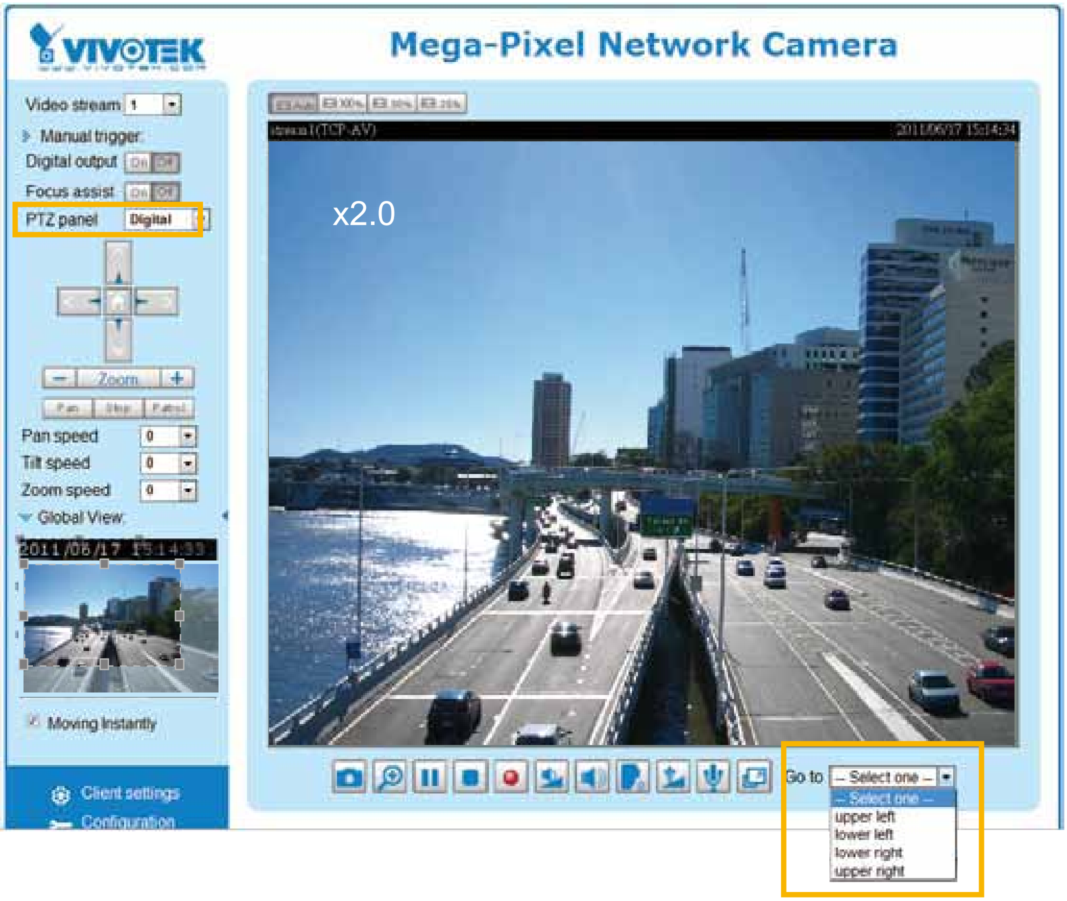
Go to: -- Select one --

Name: Add preset location

Select stream: Select one of the streams from 1 and 2 to set up the e-PTZ control. Please note that each stream can be set up with its own preset and patrol settings. 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 (slow/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.

Home page in E-PTZ Mode



Video stream 1

PTZ panel Digital

Pan speed 0

Tilt speed 0

Zoom speed 0

Go to -- Select one --

- ■ The e-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 e-preset positions for streams 1 and 2, you can select one of the video streams to display its separate e-preset positions.

Global View

In addition to using the e-PTZ 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.

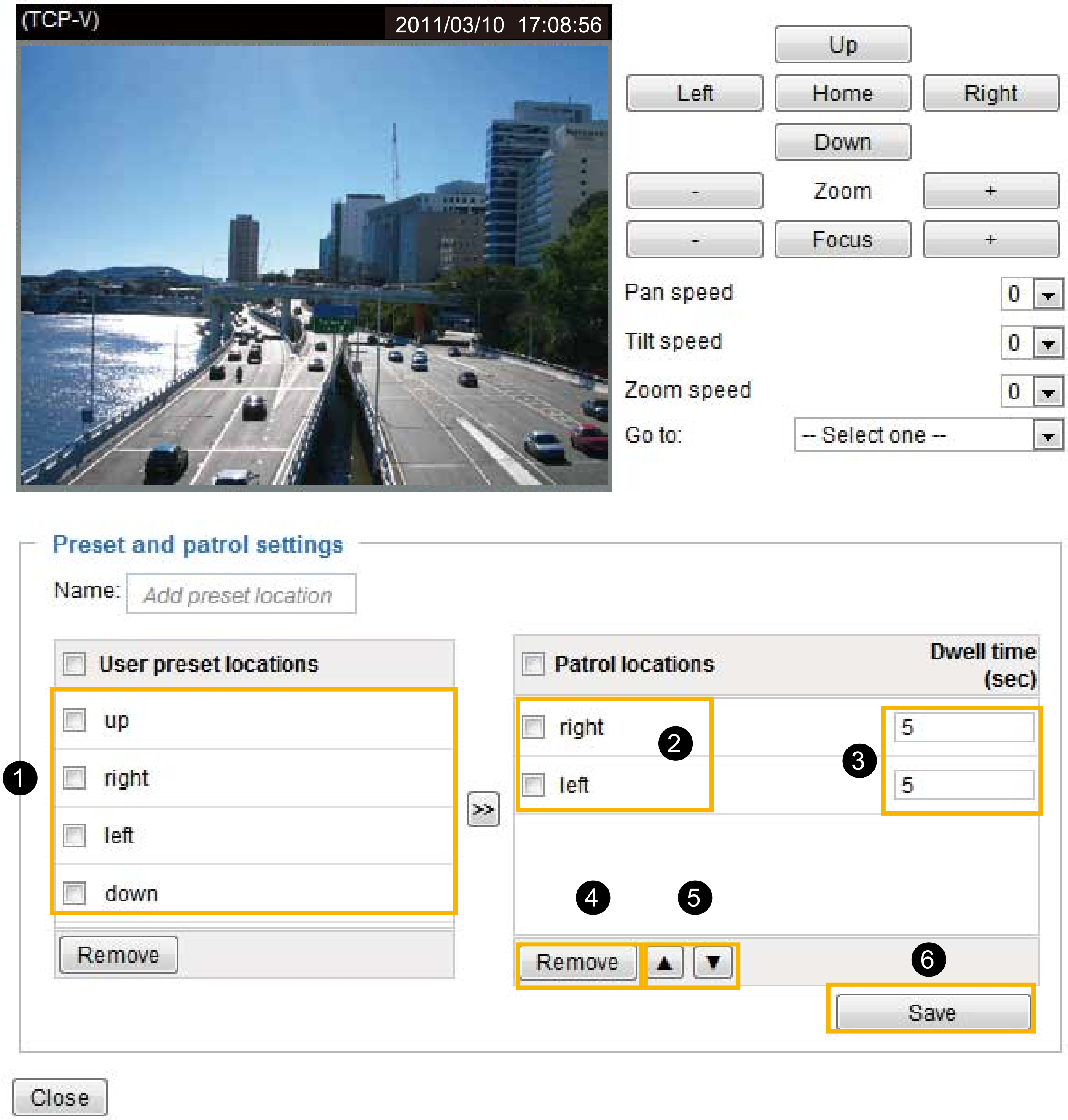
Click on Image

The e-PTZ 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. Select the preset locations on the list, and click >> .
2. The selected preset locations will be displayed on the **Patrol locations** list.
3. Set the **Dwelling time** for the streaming view to stay at the preset location during auto patrol.
4. If you want to delete a preset location from the Patrol locations list, select it and click **Remove**.
5. Select a location and click ▲ ▼ to rearrange the patrol order.
6. Select patrol locations you want to save in the list and click **Save** to enable the patrol settings.
7. To perform a pre-configured patrol, return to homepage and click on the **Patrol** button.



Pan speed: 0

Tilt speed: 0

Zoom speed: 0

Go to: -- Select one --

Preset and patrol settings

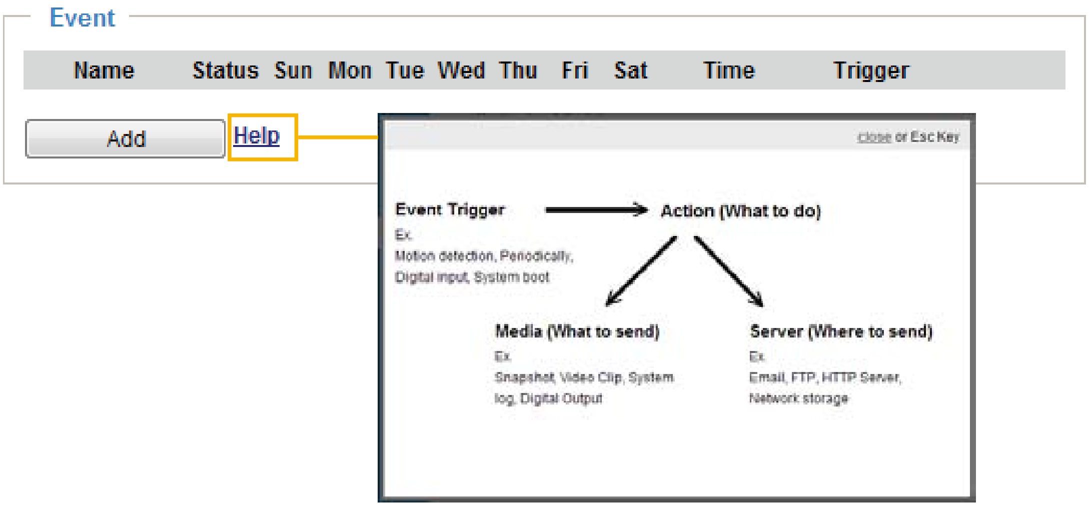
Name: Add preset location

□ User preset locations
□ up
□ right
□ left
□ down

□ Patrol locations	Dwell time (sec)
□ right	5
□ left	5

Event > Event settings Advanced Mode

This section explains how to configure the Network Camera to respond to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or e-mail address as notifications. Click on **Help**, there is an illustration shown in the pop-up window explaining that an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action that will be performed.



Event

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger

Add Help

close or Esc Key

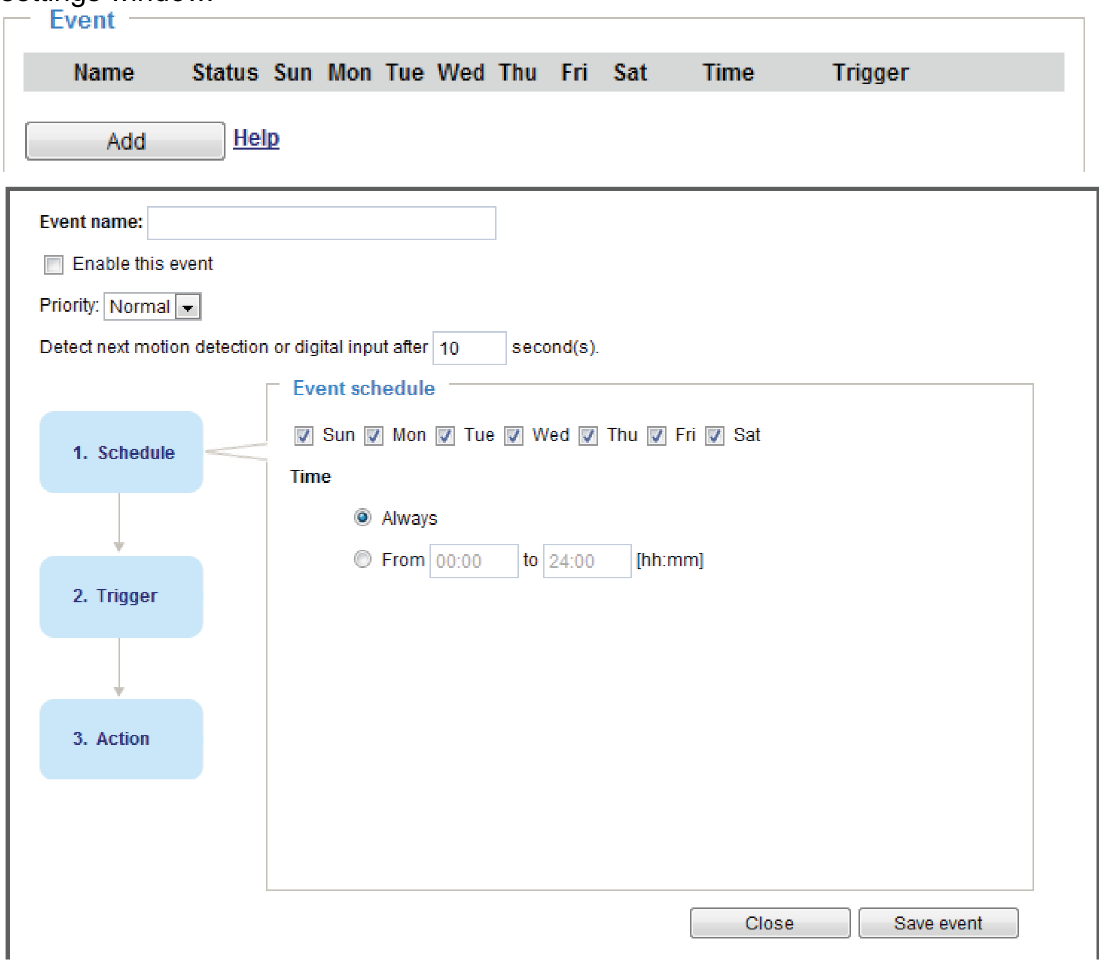
Event Trigger → Action (What to do)
Ex.
Motion detection, Periodically,
Digital input, System boot

Media (What to send)
Ex.
Snapshot, Video Clip, System log, Digital Output

Server (Where to send)
Ex.
Email, FTP, HTTP Server, Network storage

Event

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



Event

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger

Add Help

Event name:

□ Enable this event

Priority: Normal

Detect next motion detection or digital input after 10 second(s).

1. Schedule
2. Trigger
3. Action

Event schedule

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

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

Close Save event

■ 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.

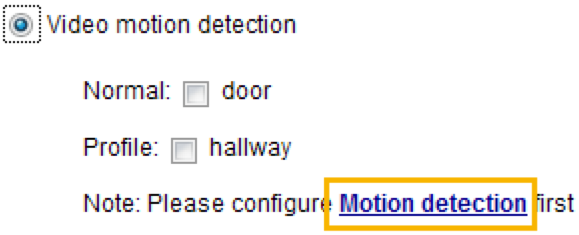
Follow the steps 1~3 to arrange the three elements each by a mouse click on its blue text -- Schedule, Trigger, and Action to set an event. A total of 3 event settings can be configured.

1. Schedule
Specify the period for the event to apply. Please select the days of the week and the time in a day (in 24-hr time format) to specify when will the event-triggering conditions take effect.

2. Trigger
This is the cause or stimulus which defines what will trigger the event. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital inputs.

There are several choices of trigger sources as shown on next page. Select each item to display its related options.

■ Video motion detection
This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to Motion Detection on page 98 for details.



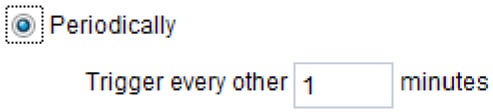
● Video motion detection

Normal: □ door

Profile: □ hallway

Note: Please configure Motion detection first

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



● Periodically

Trigger every other 1 minutes

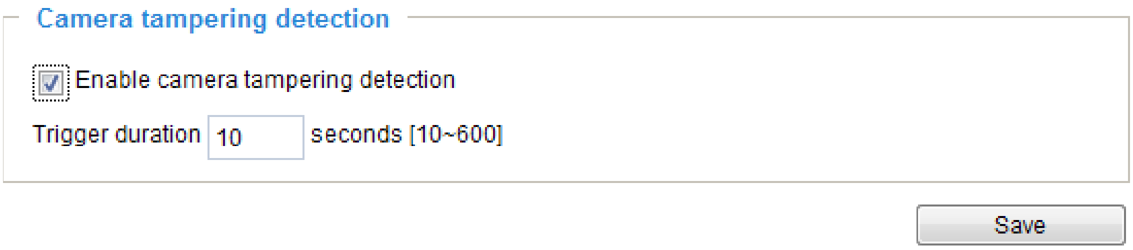
■ Digital input
This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices with digital input devices on the market which help detect changes in temperature, vibration, sound, light, etc.

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

■ Recording notify
This option allows the Network Camera to trigger when the recording disk is full or when recording starts to overwrite 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 101 for detailed information.



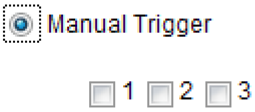
Camera tampering detection

☑ Enable camera tampering detection

Trigger duration 10 seconds [10~600]

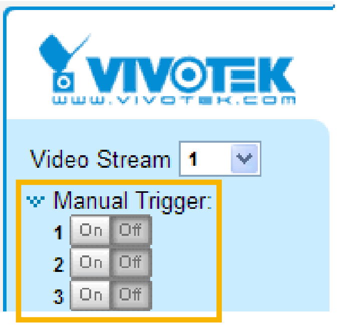
■ Manual Trigger

This option allows user to enable event triggers manually by clicking the on/off button on the homepage. Please configure 1 to 3 events before using this function.



● Manual Trigger

□ 1 □ 2 □ 3

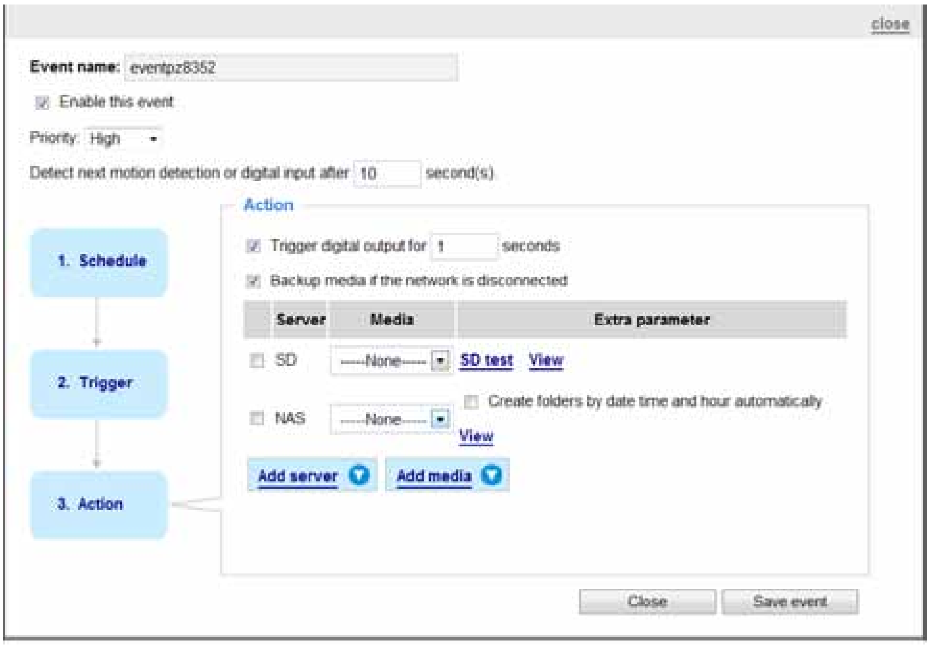


Video Stream 1

Manual Trigger:

3. Action

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



Event name: eventpz8352

☑ Enable this event

Priority: High

Detect next motion detection or digital input after 10 second(s)

Action

☑ Trigger digital output for 1 seconds

☑ Backup media if the network is disconnected

Server	Media	Extra parameter
□ SD	----None----	SD test View
□ NAS	----None----	□ Create folders by date time and hour automatically View

■ Trigger digital output for □ seconds

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

■ Backup media if the network is disconnected

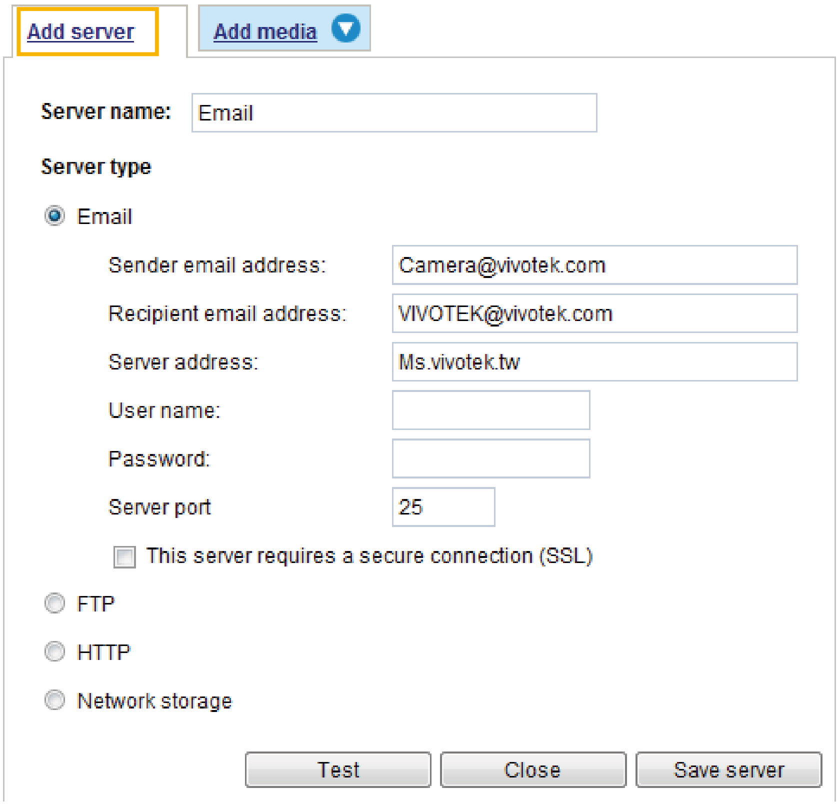
Select this option to backup media file on SD card if the network is disconnected. Please note that this function will only apply after you set up the network storage (NAS). For more information about how to set up network storage, please refer to page 104.

To configure an event with video recording or snapshots, it is necessary to configure/provide servers and storage media settings so that the Network Camera will know where to send the media files to when a trigger is activated.

Add server

Click **Add server** to unfold the server setting window. You can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

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



Server 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

Server type - Email
Select to send the media files via email when a trigger is activated.

■ Server name: Enter a name for the server setting.

■ Sender email address: Enter a valid email address as the sender address.

■ Recipient email address: Enter a valid email address as the recipient address.

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

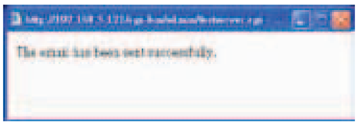
■ User name: Enter the user name of the email account if necessary.

■ Password: Enter the password of the email account if necessary.

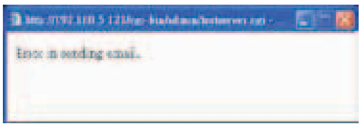
■ Server port: The default mail server port is set to 25. You can also manually set another port.

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.



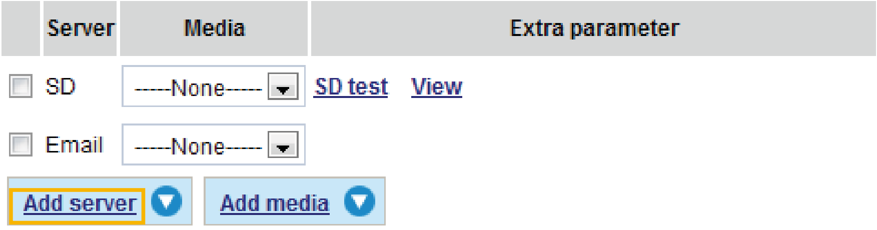
The email has been sent successfully.



Error in sending email.

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

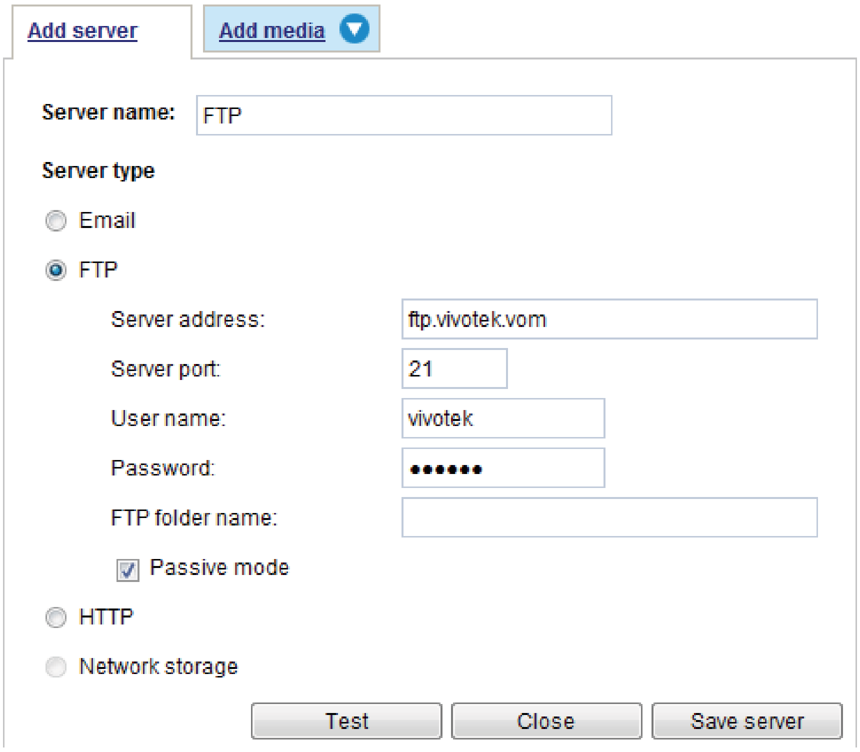
After you set up the first event server, a new item for event server will automatically appear on the Server list. If you wish to add more server options, click **Add server**.



	Server	Media	Extra parameter
□	SD	-----None-----	SD test View
□	Email	-----None-----	

Server type - 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.vom

Server port: 21

User name: vivotek

Password: ●●●●●●

FTP folder name:

☑ Passive mode

○ HTTP

○ Network storage

- Server name: Enter a name for the server setting.

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

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

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

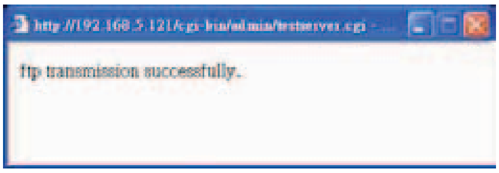
- Password: Enter the password of the FTP account.

- FTP folder name

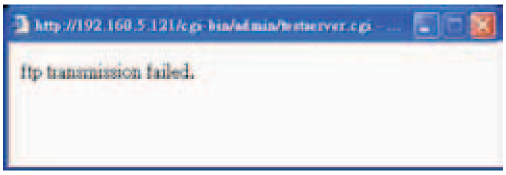
  Enter the folder where the media file will be placed. If the folder name does not exist, the Network Camera will create one on the FTP server.

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

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



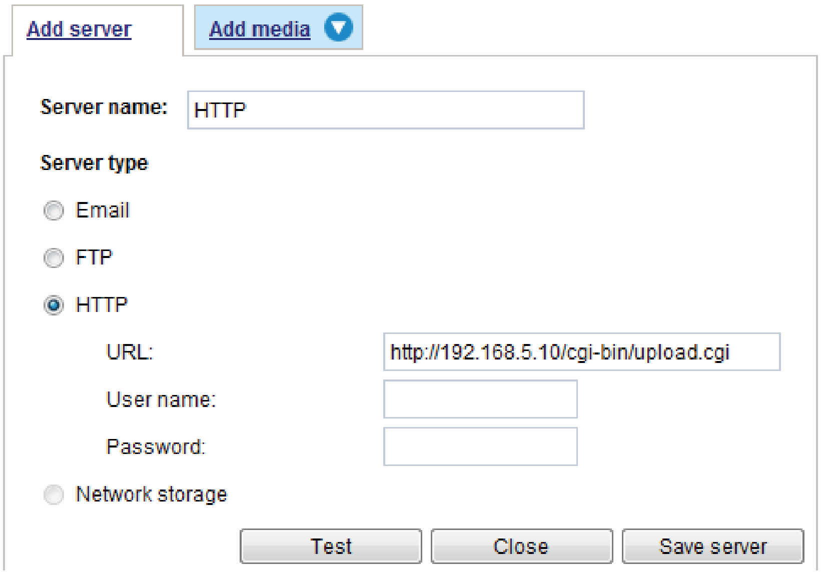
ftp transmission successfully.



ftp transmission failed.

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

Server type - HTTP
Select to send the media files to an HTTP server when a trigger is activated.



Server name: HTTP

Server type

○ Email

○ FTP

● HTTP

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

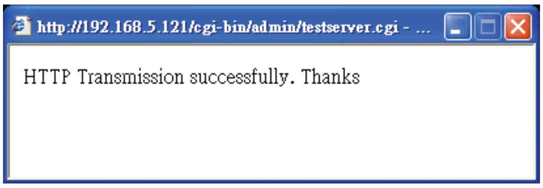
User name:

Password:

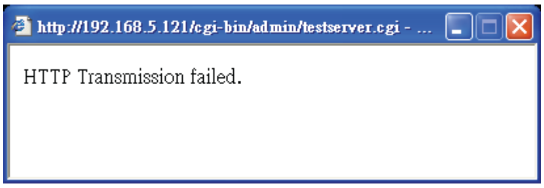
○ Network storage

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

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



HTTP Transmission successfully. Thanks

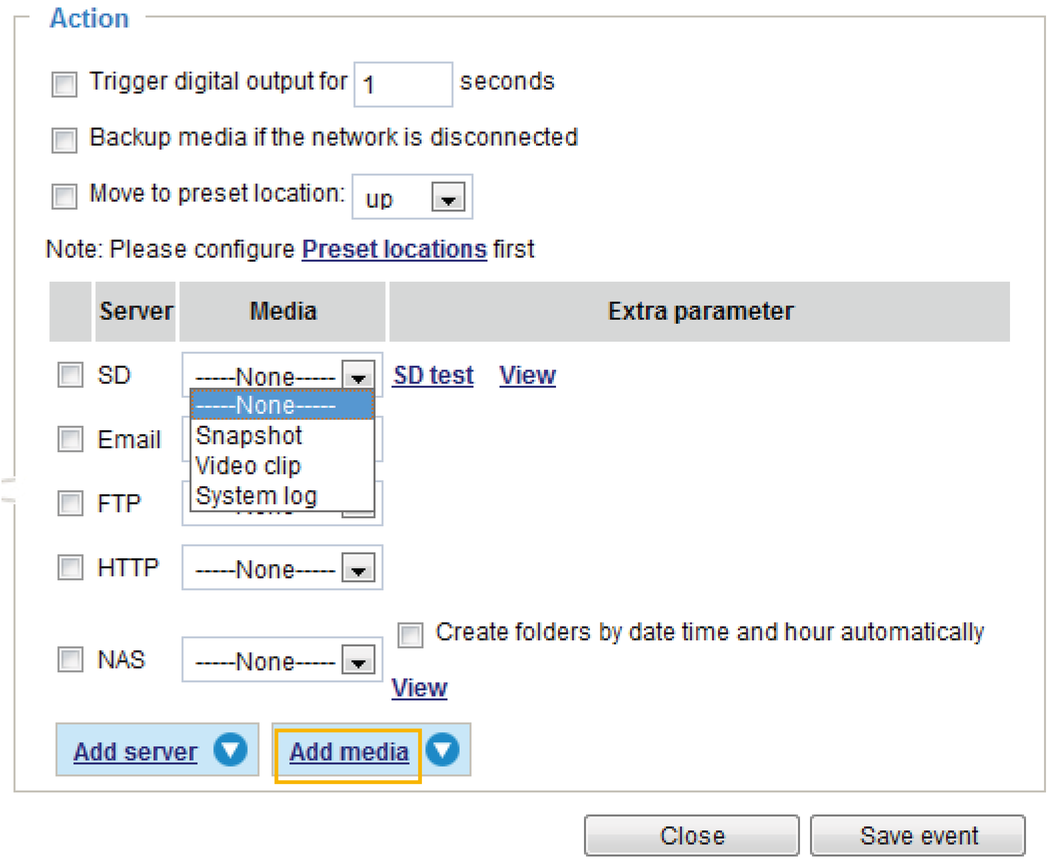


HTTP Transmission failed.

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

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

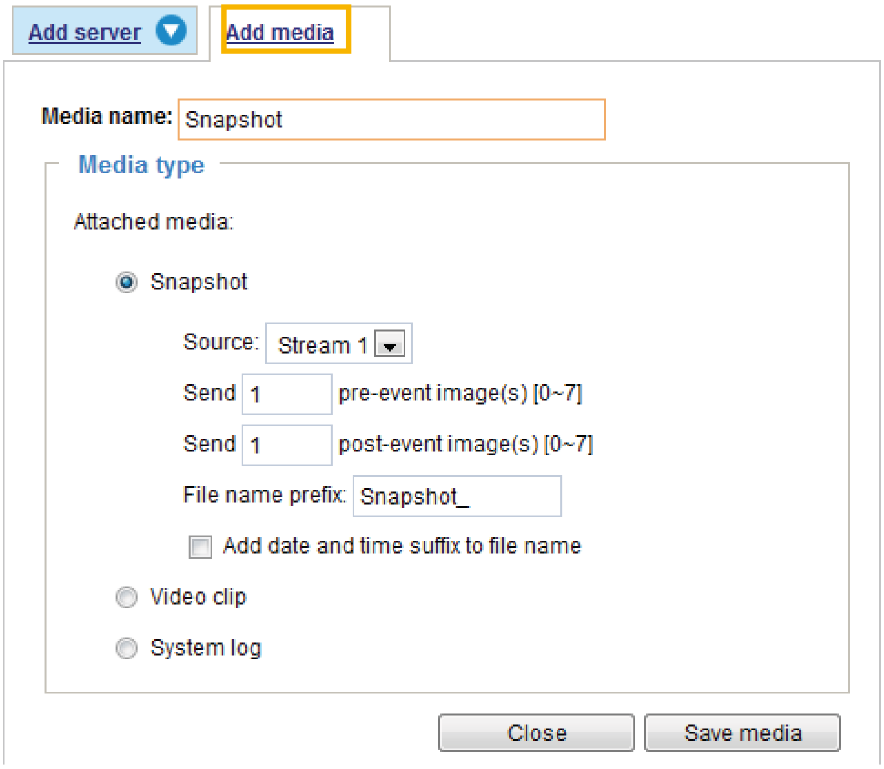
Click **Save server** to enable the settings, then click **Close** to exit the Add server page.


Action
□ Trigger digital output for 1 seconds
□ Backup media if the network is disconnected
□ Move to preset location: up
Note: Please configure Preset locations first
Server
Media
Extra parameter
□ SD
-----None-----
-----None-----
Snapshot
Video clip
System log
SD test
View
□ Email
□ FTP
□ HTTP
-----None-----
□ NAS
-----None-----
□ Create folders by date time and hour automatically
View
Add server
Add media
Close
Save event

■ SD Test: Click to test your SD card. The system will display a message indicating success or failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 107 for detailed information.

Add media

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



Media name: Snapshot

Media type

Attached media:

● Snapshot

Source: Stream 1

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

Media type - Snapshot
Select to send snapshots when a trigger is activated.

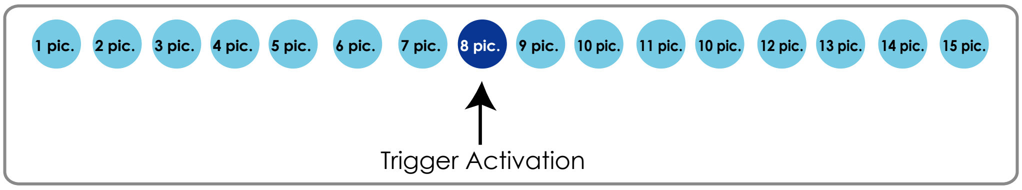
■ Media name: Enter a name for the media setting.

■ Source: Select to take snapshots from streams 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.

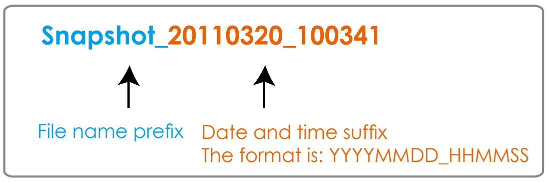
■ Send □ post-event images
Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

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.



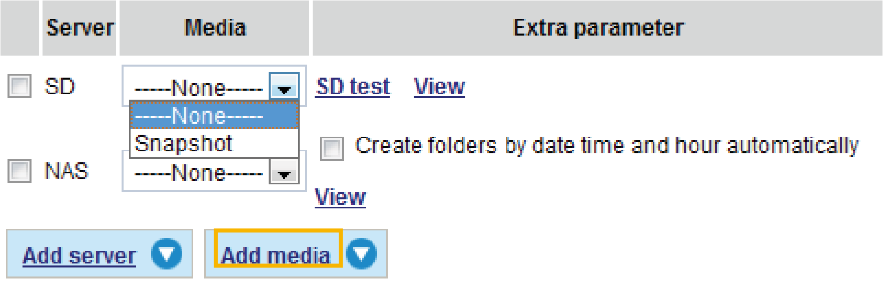
■ File name prefix
Enter the text that will be appended to the front of the file name.

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



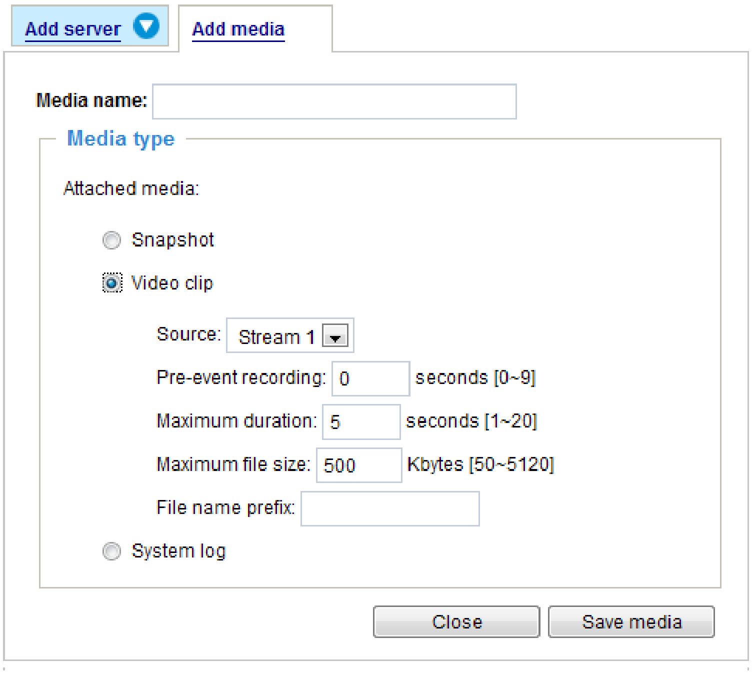
Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

After you set up the first media server, a new column for media server will automatically display on the Media list. If you wish to add more media options, click **Add media**.



	Server	Media	Extra parameter
□	SD	-----None-----	SD test View
□	NAS	-----None-----	□ Create folders by date time and hour automatically View

Media type - Video clip
Select to send video clips when a trigger is activated.



Media name:

Media type

Attached media:

○ Snapshot

● Video clip

Source: Stream 1

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

Maximum duration: 5 seconds [1~20]

Maximum file size: 500 Kbytes [50~5120]

File name prefix:

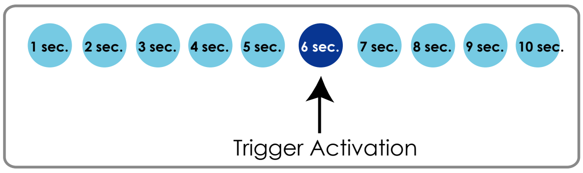
○ System log

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

■ Source: Select the source of video clip.

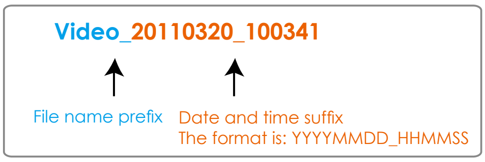
■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds of video can be recorded.

- Maximum duration
  Specify the maximum recording duration in seconds. Up to 10 seconds of video can be recorded. For example, if pre-event recording is set to 5 seconds and the maximum duration is set to 10 seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.



- Maximum file size
  Specify the maximum file size allowed.

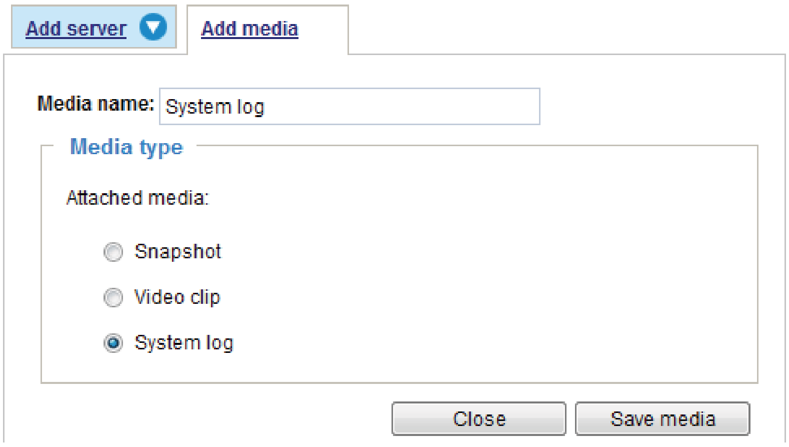
- File name prefix
  Enter the text that will be appended to the front of the file name.
  For example:



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

Media type - System log

Select to send a system log when a trigger is activated.



Media name: System log

Media type

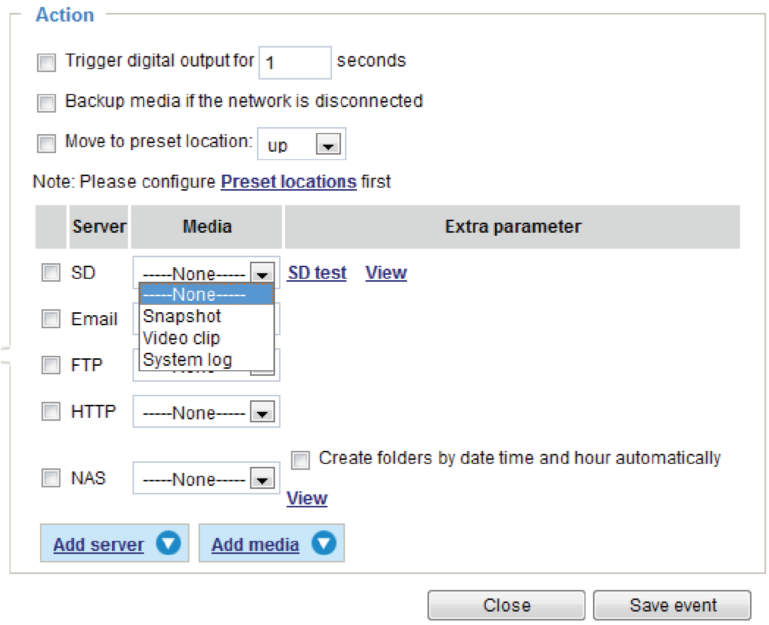
Attached media:

○ Snapshot

○ Video clip

● System log

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



Action

□ Trigger digital output for 1 seconds

□ Backup media if the network is disconnected

□ Move to preset location: up

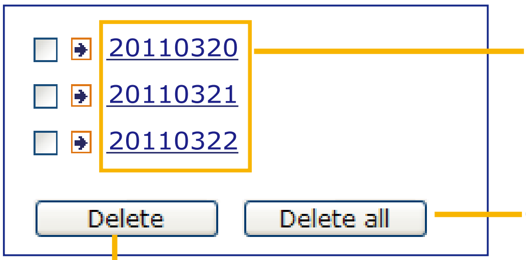
Note: Please configure Preset locations first

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

- View: A View button will appear on the Event setting window. 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 pop up for you to manage recorded files on SD card. For more information about Local storage, please refer to page 107. If you click **View** button of Network storage, a file directory window will pop up for you to view recorded data on Network storage.

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

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


□ 20110320
□ 20110321
□ 20110322

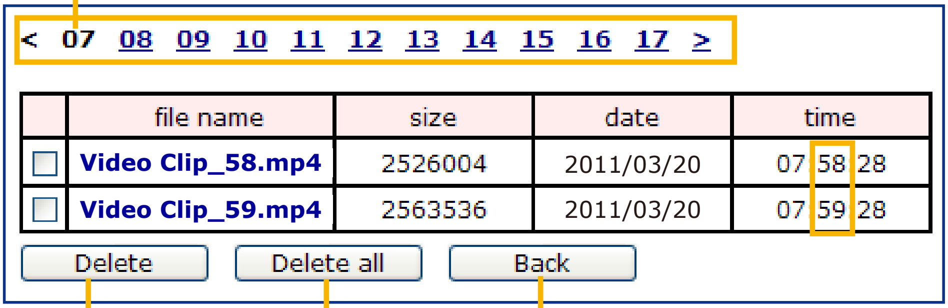
The format is: YYYYMMDD
Click to open the directory

Click to delete all recorded data

Click to delete selected items

Click **20110320** to open the directory:

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

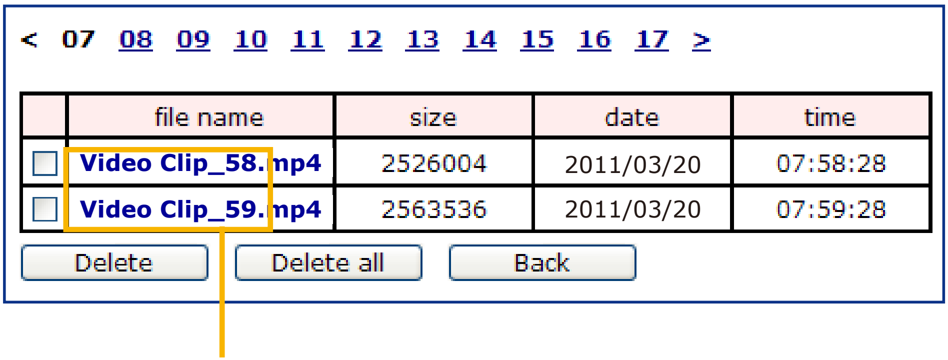

< 07 08 09 10 11 12 13 14 15 16 17 >

	file name	size	date	time
□	**Video Clip_58.mp4**	2526004	2011/03/20	07:58:28
□	**Video Clip_59.mp4**	2563536	2011/03/20	07:59:28

Click to delete selected items

Click to go back to the previous level of the directory

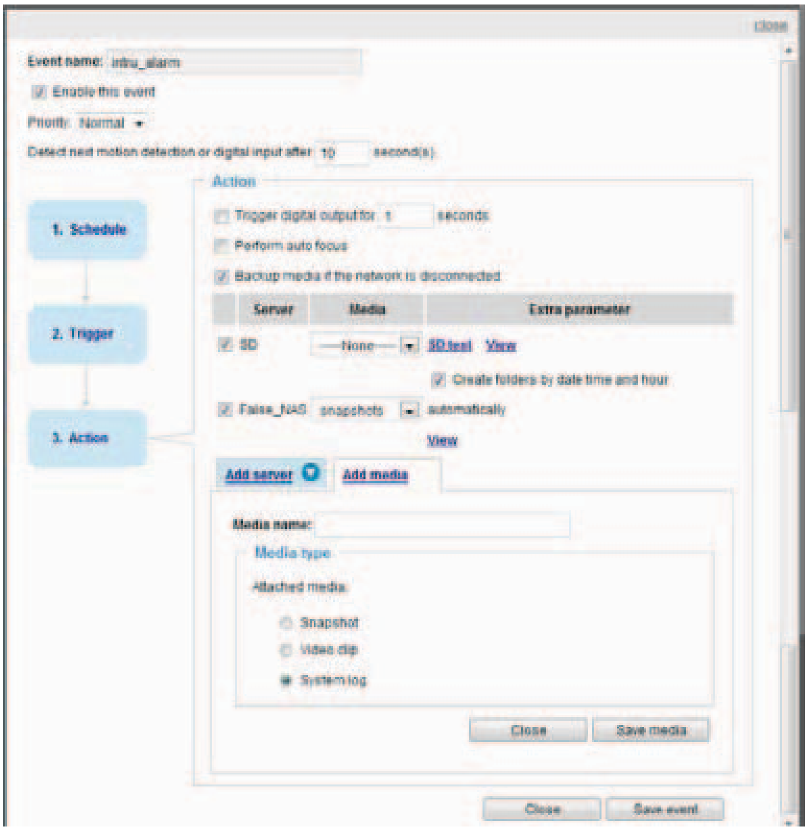
Click to delete all recorded data


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

	file name	size	date	time
□	**Video Clip_58.mp4**	2526004	2011/03/20	07:58:28
□	**Video Clip_59.mp4**	2563536	2011/03/20	07:59:28

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

Here is an example of the Event setting:



Event name: intru_alarm

☑ Enable this event

Priority: Normal

Detect next motion detection or digital input after 10 second(s)

Action

□ Trigger digital output for 1 seconds

□ Perform auto focus

☑ Backup media if the network is disconnected

	Server	Media	Extra parameter
☑	SD	---None---	SD test View ☑ Create folders by date time and hour
☑	False_NAS	snapshots	automatically View

Media name:

Media type

Attached media

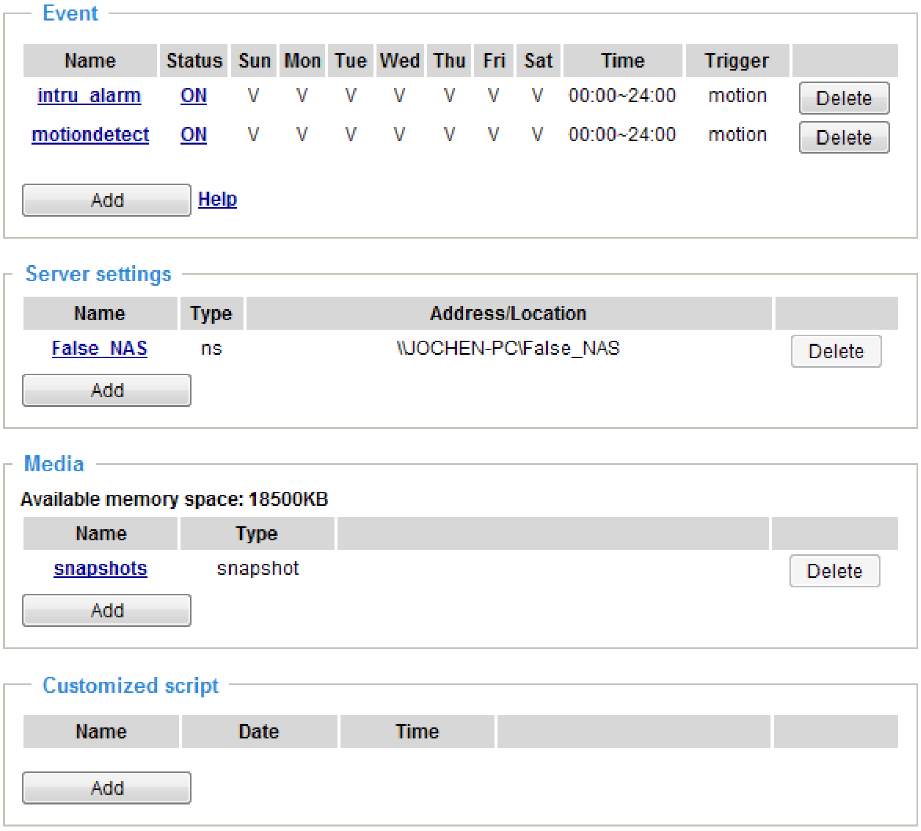
○ Snapshot

○ Video clip

● System log

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

The following is an example of the Event setting page:



Event

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger	
intru_alarm	ON	V	V	V	V	V	V	V	00:00~24:00	motion	Delete
motiondetect	ON	V	V	V	V	V	V	V	00:00~24:00	motion	Delete

Server settings

Name	Type	Address/Location	
False_NAS	ns	\\JOCHEN-PC\False_NAS	Delete

Media

Available memory space: 18500KB

Name	Type		
snapshots	snapshot		Delete

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.

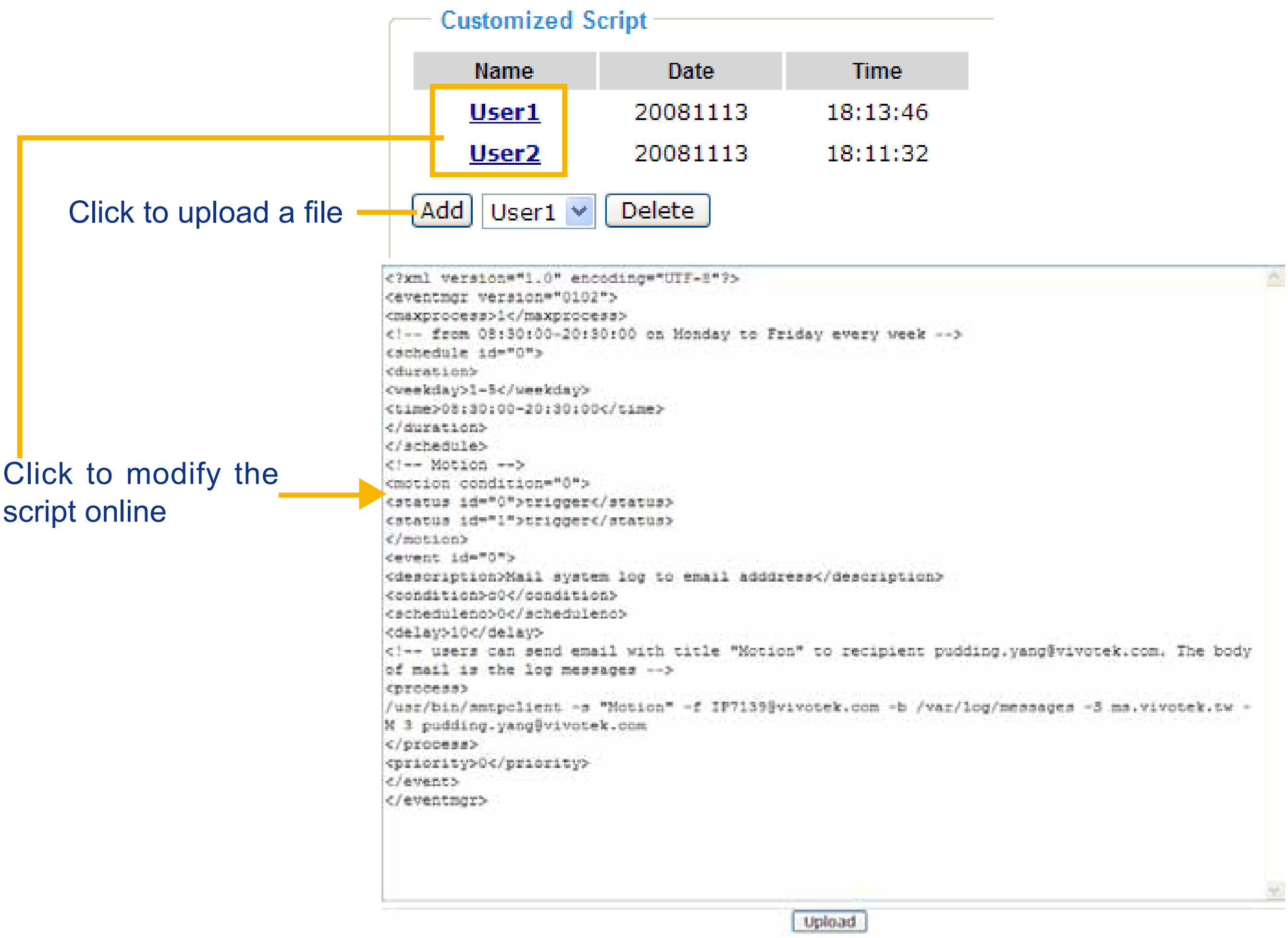
If you want to stop the event trigger, you can click **ON** to turn it to **OFF** status or click **Delete** to remove a previously-configured event setting.

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

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

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 prompt. If you need more information, please contact VIVOTEK's technical support.



Customized Script

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

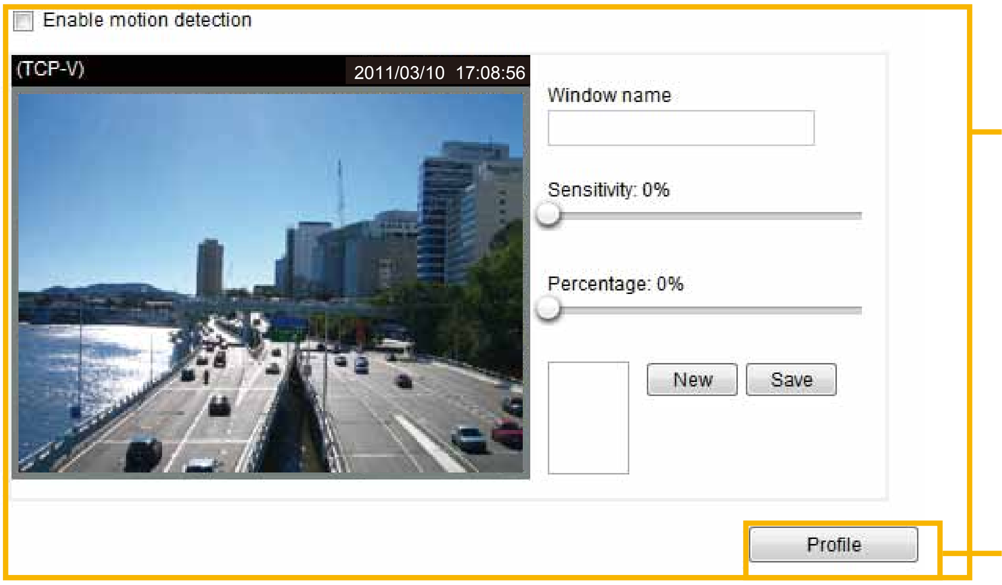
Click to upload a file

Click to modify the script online

```
<?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 adddress</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>
```

Applications > Motion detection

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



□ Enable motion detection

(TCP-V) 2011/03/10 17:08:56

Window name:

Sensitivity: 0%

Percentage: 0%

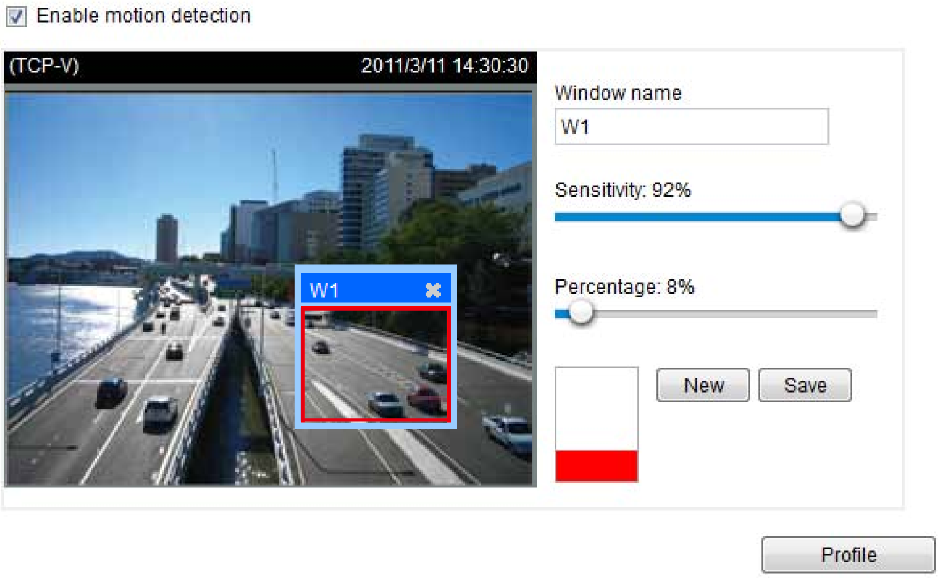
Motion Detection Setting 1: For normal situations

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 a window, click X on the upper right corner of the window.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slide bar.
4. Click **Save** to enable the settings.
5. Select **Enable motion detection** to enable this function.

For example:



☑ Enable motion detection

(TCP-V) 2011/3/11 14:30:30

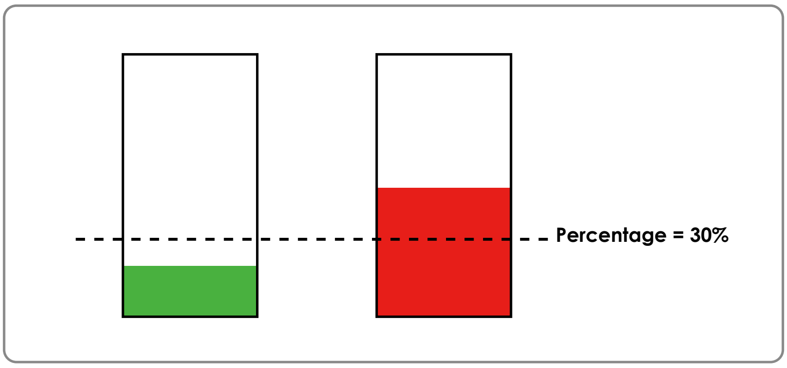
Window name: W1

Sensitivity: 92%

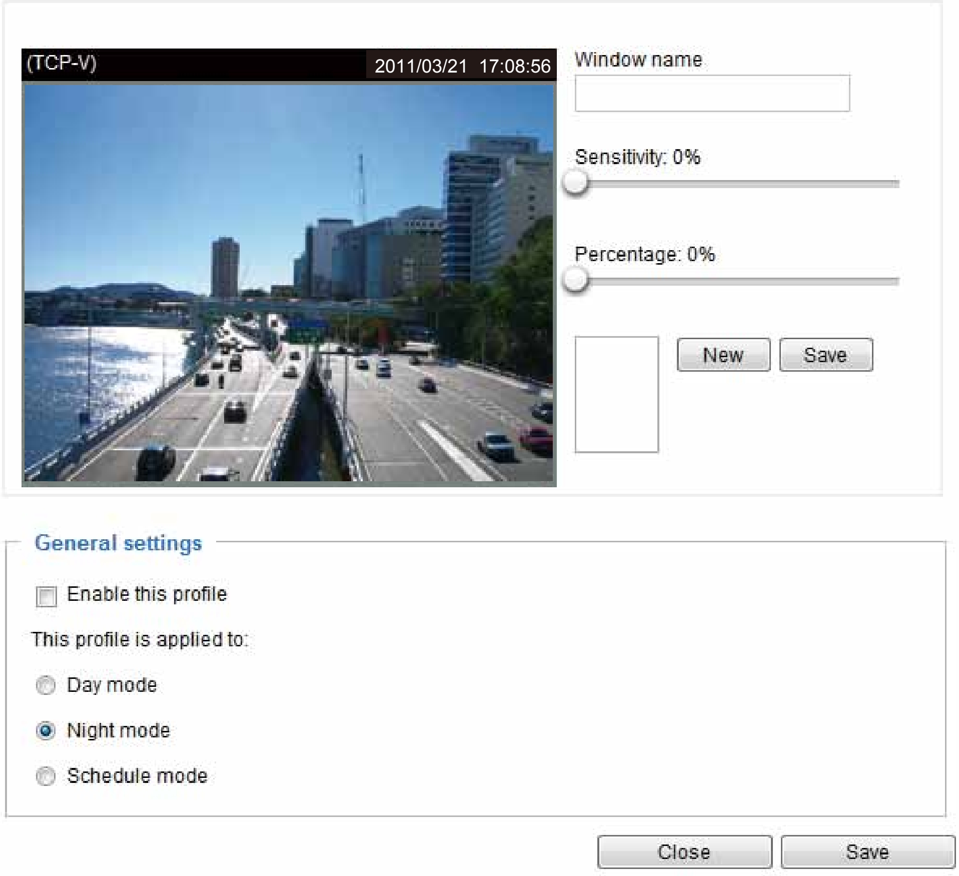
Percentage: 8%

The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are considered to have exceeded 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) using this feature as a trigger source. For more information on how to set an event, please refer to Event settings on page 85.

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 specific motion detection settings individually for day/night/schedule operations, 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.



Window name

Sensitivity: 0%

Percentage: 0%

General settings

□ Enable this profile

This profile is applied to:

○ Day mode

● Night mode

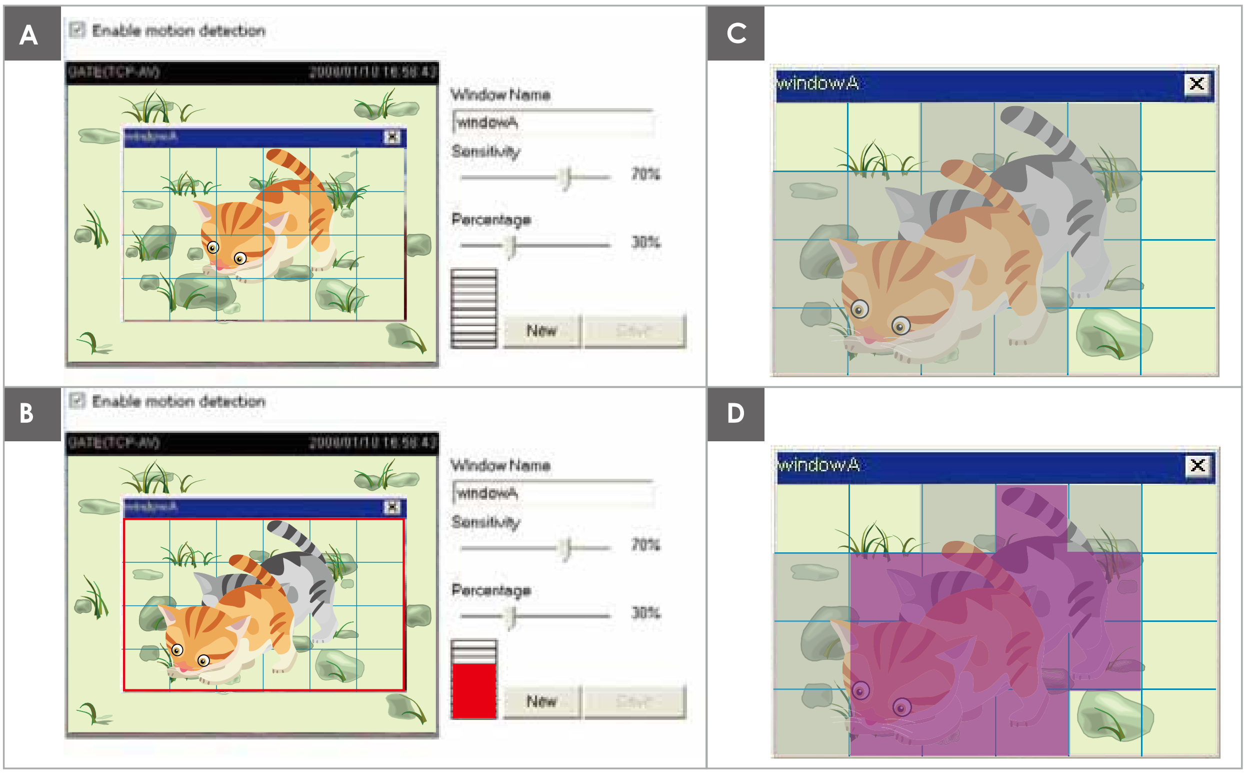
○ Schedule mode

Please follow the steps beolw 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 prefer 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 Event > Event settings > Trigger to choose it as a trigger source. Please refer to page 86 for detailed information.

NOTE:

▶ *How does motion detection work?*

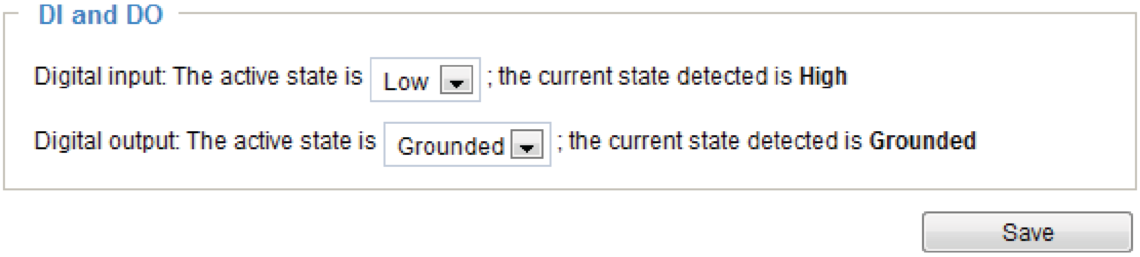


There are two motion detection parameters: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to detect slight movements while smaller sensitivity settings will neglect them. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).

Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.

*For applications that require a high level of security management, it is suggested to use **higher** sensitivity settings and **smaller** percentage values.*

Applications > DI and DO Advanced Mode



DI and DO

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

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

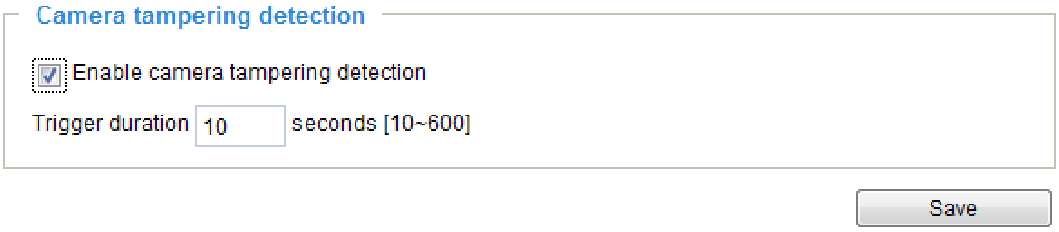
Digital input: Select High or Low to define the activate status for the digital input. The Network Camera's current status is shown on the right.

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

Set up the event source as DI on **Event > Event settings > Trigger.** Please refer to page 86 for detailed information.

Applications > Tampering detection

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



Camera tampering detection

☑ Enable camera tampering detection

Trigger duration 10 seconds [10~600]

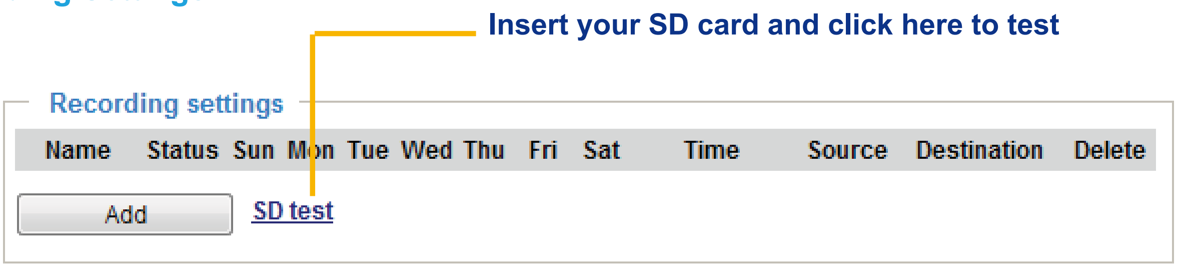
Please follow the steps below to set up the camera tamper detection function:

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 **Event > Event settings > Trigger.** Please refer to page 86 for detailed information.

Recording > Recording settings Advanced Mode

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

Recording Settings



Insert your SD card and click here to test

Recording settings

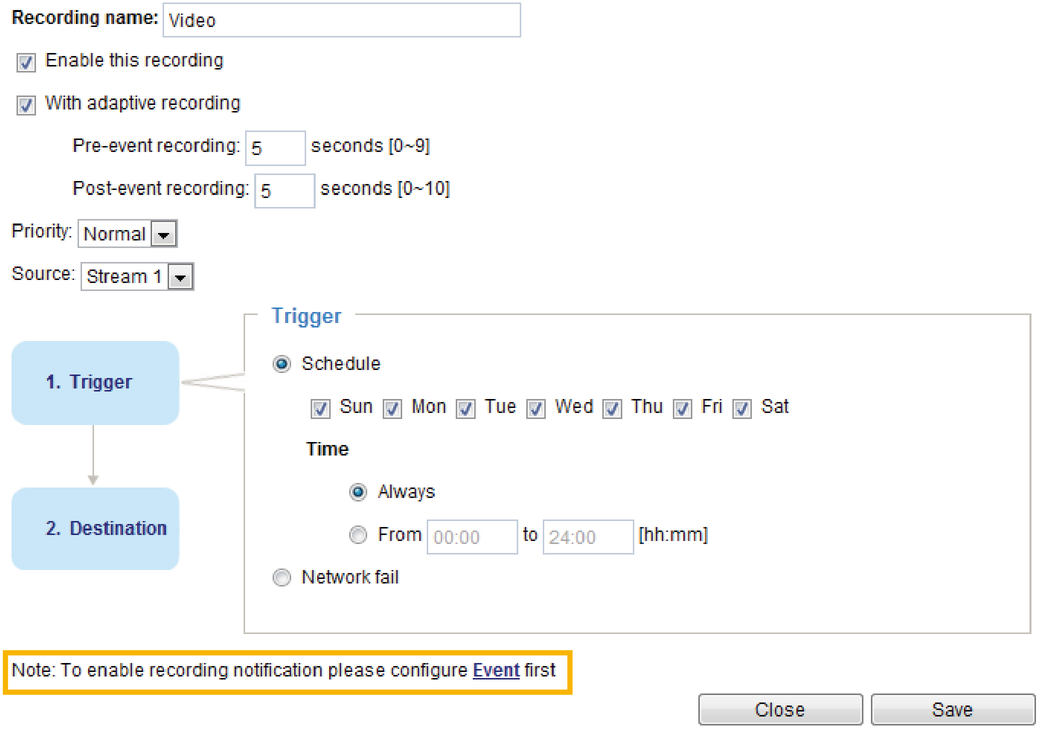
Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination	Delete

NOTE:

Please remember to format your SD card when used for the first time. Please refer to page 107 for detailed information.

Recording Settings

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



Recording name: Video

☑ 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

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

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

○ Network fail

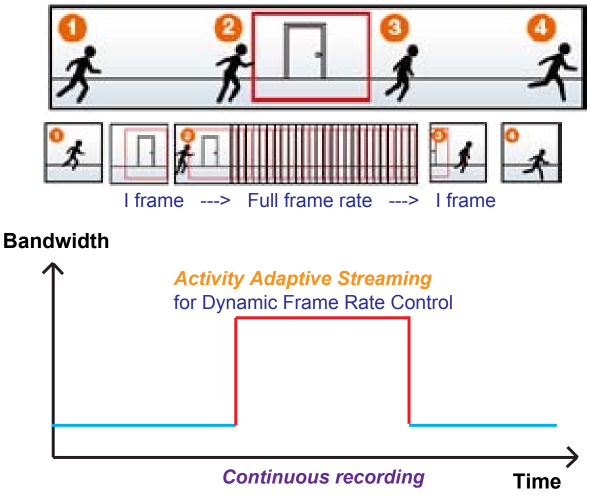
Note: To enable recording notification please configure Event first

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

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

- With adaptive recording:
  Select this option will activate the frame rate control according to alarm trigger. The frame control means that when there is a triggered alarm/event, the frame rate will raise up to the value you've set on the Stream setting page. Please refer to page 77 for more information.

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



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 into 1s when the adaptive recording is activated.*

The alarm trigger includes: motion detection and DI detection. Please refer to Event settings on page 85.

■ Pre-event recording and post-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before and after a trigger is activated.

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

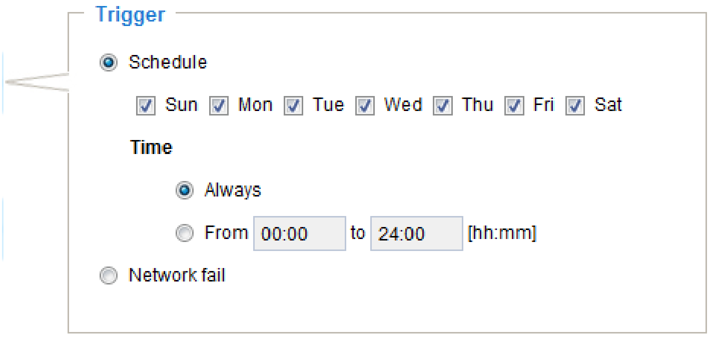
■ Source: Select a stream for the recording source.

NOTE:

- ▶ *To enable adaptive recording, please also **enable time shift caching stream** and **select a caching stream** on Media > Video > Stream settings. Please refer to page 77 for detailed instruction.*
- ▶ *To enable recording notification please configure **Event settings** first. Please refer to page 85.*

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

1. Trigger
Select a trigger source.



Trigger

● Schedule

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

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

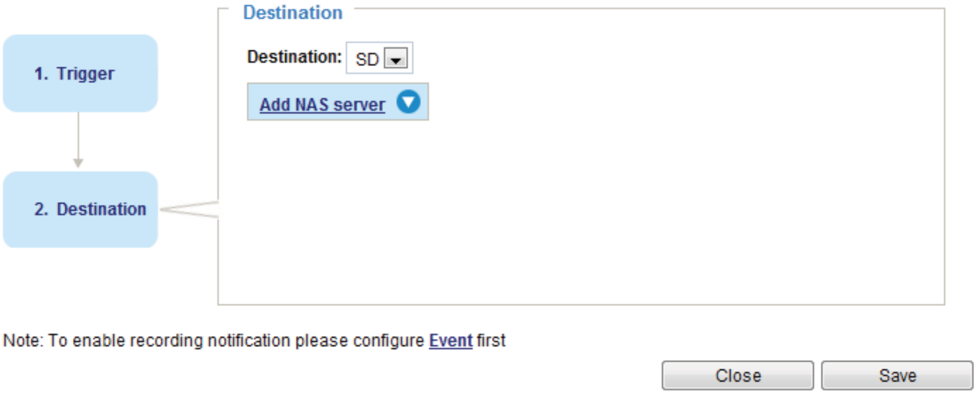
○ Network fail

■ Schedule: The server will start to record files on the local storage or network attached storage (NAS).

■ Network fail: Since network fail, the server will start to record files onto the local storage (SD card).

2. Destination

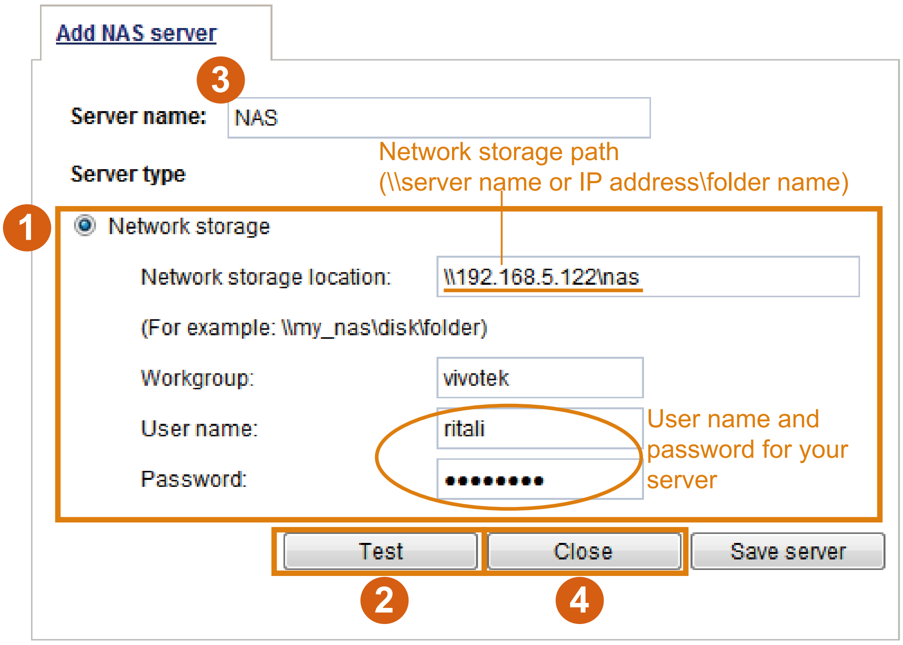
You can select the SD card or network storage (NAS) for the recorded video files.



NAS server

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

1. Fill in the information for the access to the shared networked storage.
   For example:



Add NAS server

Server name: NAS

Server type

● Network storage

Network storage location: \\192.168.5.122\nas

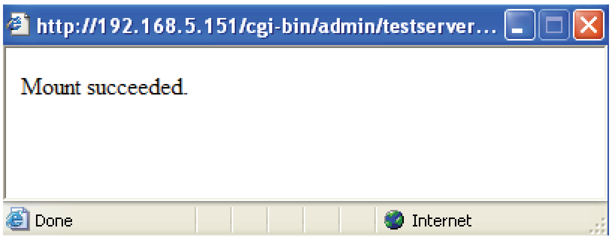
(For example: \\my_nas\disk\folder)

Workgroup: vivotek

User name: ritali

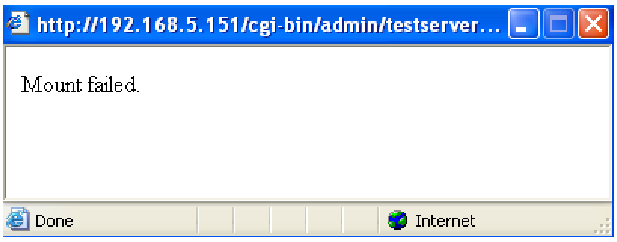
Password: ••••••••

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...

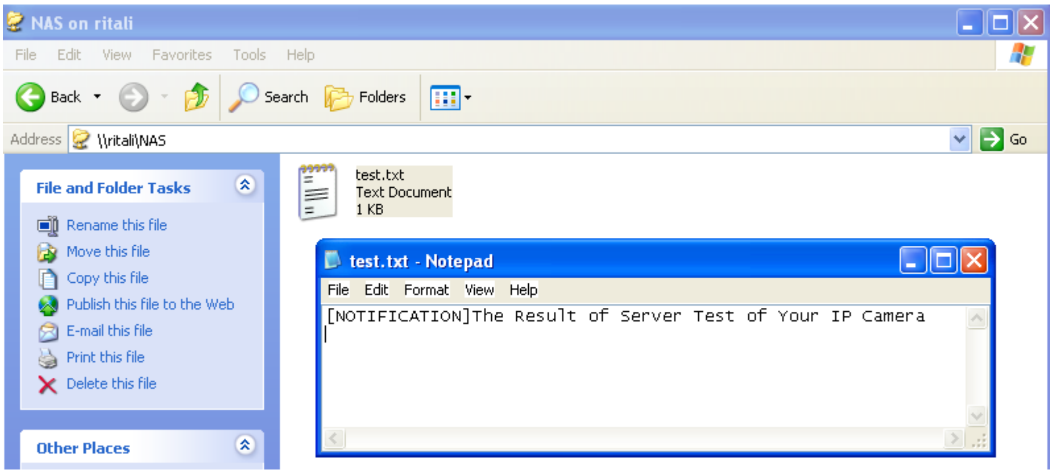
Mount succeeded.



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

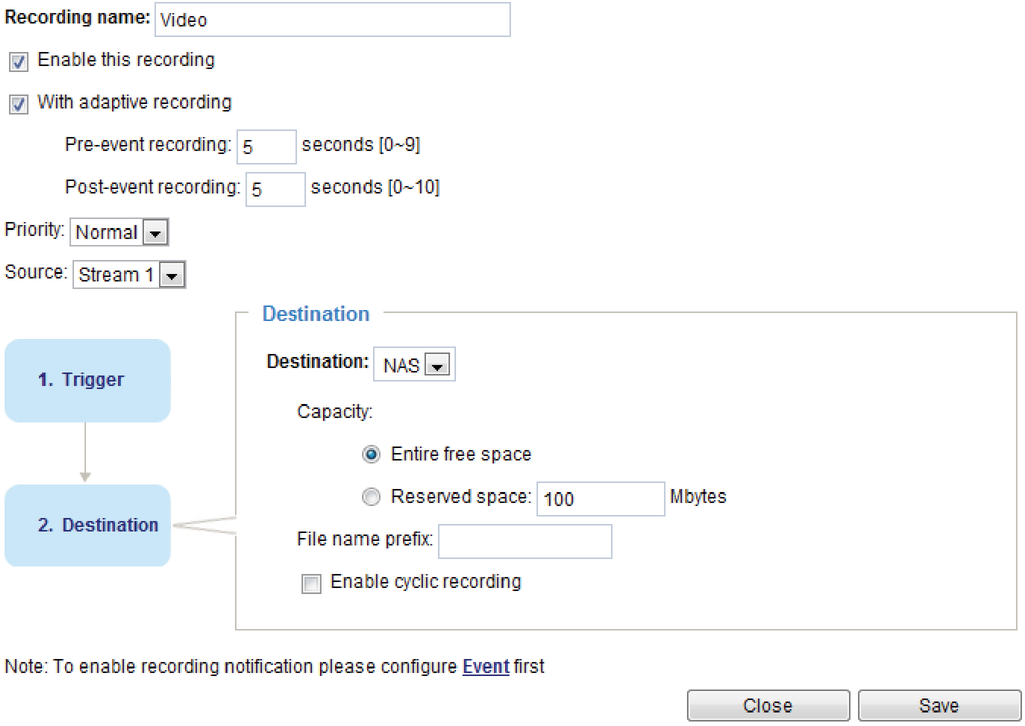
Mount failed.

If successful, you will receive a test.txt file on the networked 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 name: Video

☑ 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

Destination

Destination: NAS

Capacity:

● Entire free space

○ Reserved space: 100 Mbytes

File name prefix:

□ Enable cyclic recording

Note: To enable recording notification please configure Event first

■ Capacity: You can either choose the entire available space or impose a reserved space. The **Reserved space** should be of the size of at least **15MBytes**. The reserved space can be used as a safe buffer especially when the cyclic recording function is enabled, during the transaction stage when a storage space is full and the incoming streaming data is about to overwrite the previously saved videos.

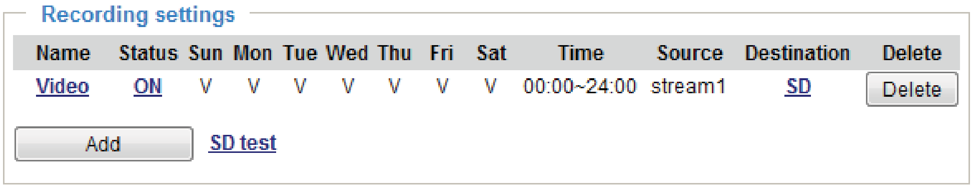
■ File name prefix: Enter the text that will be appended to the front of the file name.

■ Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one.

If you want to enable recording notification, please click **Event** to set up. Please refer to **Event > Event settings** on page 85 for more details.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the network storage or SD card. The new recording name will appear on the recording page as shown below.

To remove an existing recording setting from the list, single-click to select it and click **Delete**.



Recording settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination	Delete
Video	ON	V	V	V	V	V	V	V	00:00~24:00	stream1	SD	Delete

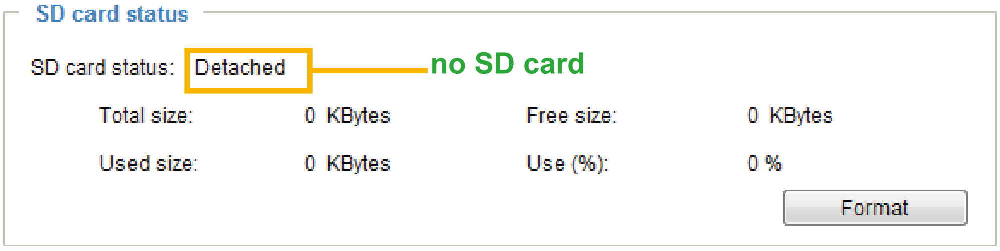
- **Video (Name)**: Click to open the Recording settings page to modify.
- **ON (Status)**: Click to manually adjust the Status. (**ON**: start recording; **OFF**: stop recording)
- **NAS or SD (Destination)**: Click to open the file list of recordings as shown below. For more information about folder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

Local storage > SD card management Advanced Mode

This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, and implement SD card control.

SD card staus

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

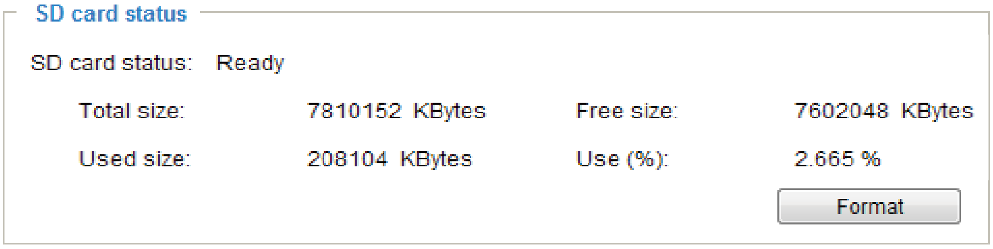


SD card status

SD card status: Detached

no SD card

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

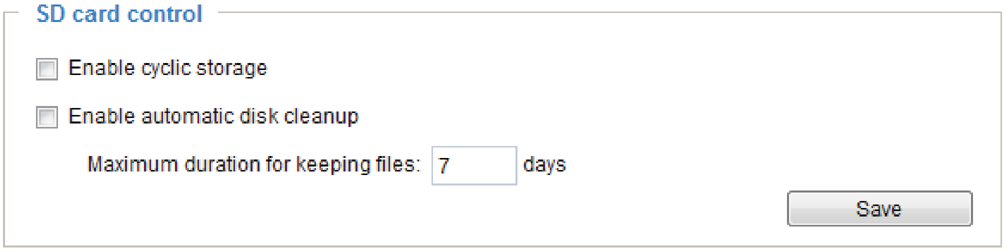


SD card status

SD card status: Ready

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

SD card control



SD card control

☐ Enable cyclic storage

☐ Enable automatic disk cleanup

Maximum duration for keeping files: 7 days

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

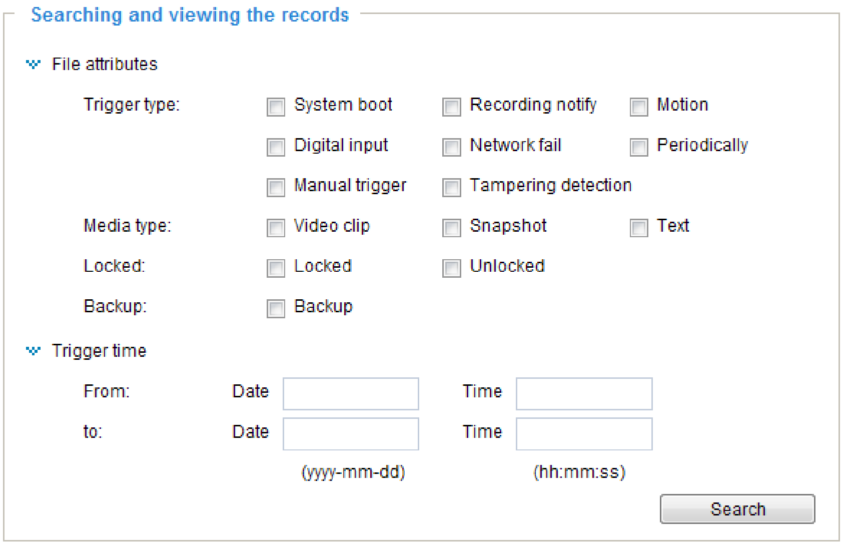
When all settings are completed, click **Save** to enable your settings.

Local storage > Content management Advanced Mode

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

Searching and Viewing the Records

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



Searching and viewing the records

File attributes

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

Trigger time

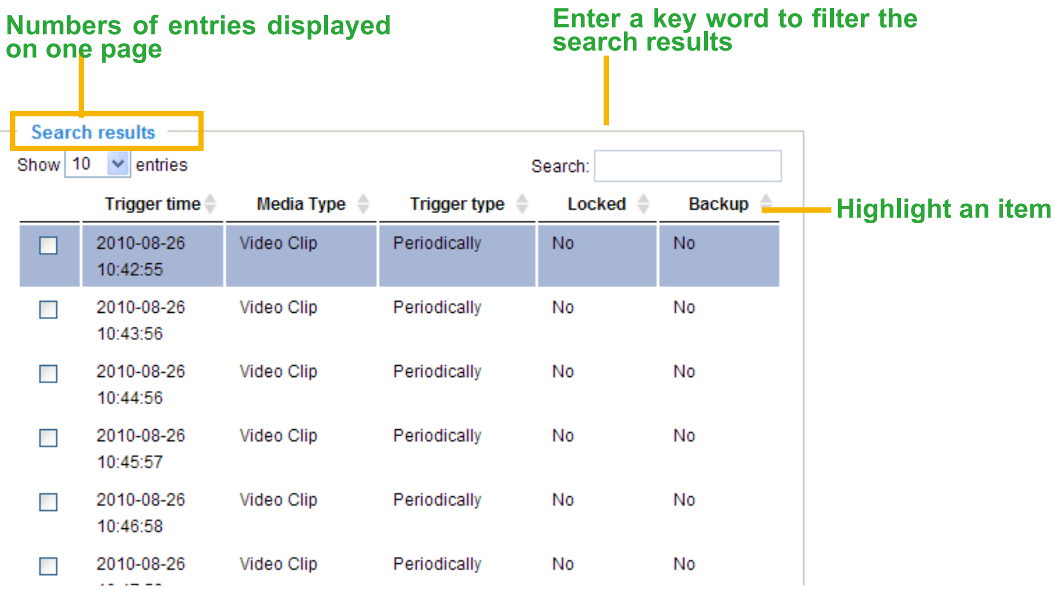
From:	Date		Time	
to:	Date		Time	
		(yyyy-mm-dd)		(hh:mm:ss)

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

Click **Search** and the recorded data 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

Highlight an item

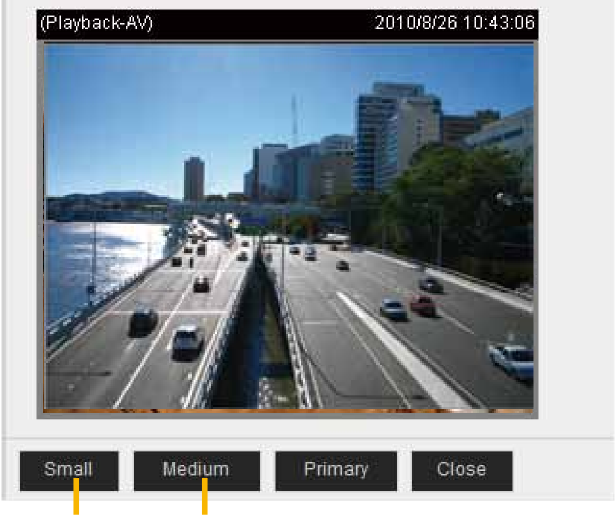
Search results

Show 10 entries

Search:

	Trigger time	Media Type	Trigger type	Locked	Backup
□	2010-08-26 10:42:55	Video Clip	Periodically	No	No
□	2010-08-26 10:43:56	Video Clip	Periodically	No	No
□	2010-08-26 10:44:56	Video Clip	Periodically	No	No
□	2010-08-26 10:45:57	Video Clip	Periodically	No	No
□	2010-08-26 10:46:58	Video Clip	Periodically	No	No
□	2010-08-26	Video Clip	Periodically	No	No

- 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:

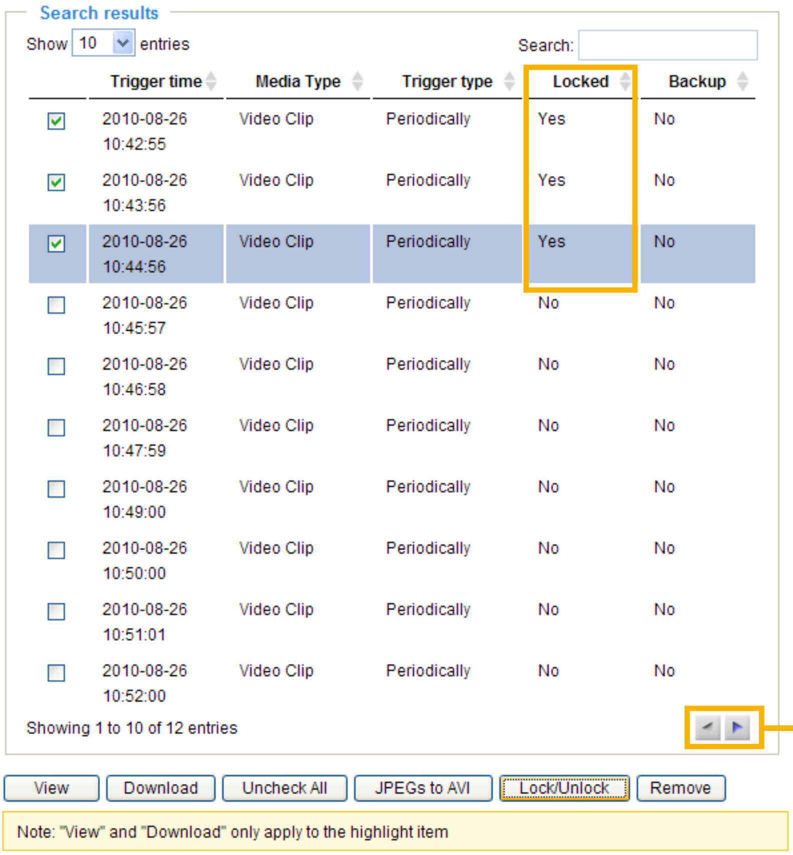


Click to adjust the image size

- 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 function 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	Backup
☑	2010-08-26 10:42:55	Video Clip	Periodically	Yes	No
☑	2010-08-26 10:43:56	Video Clip	Periodically	Yes	No
☑	2010-08-26 10:44:56	Video Clip	Periodically	Yes	No
□	2010-08-26 10:45:57	Video Clip	Periodically	No	No
□	2010-08-26 10:46:58	Video Clip	Periodically	No	No
□	2010-08-26 10:47:59	Video Clip	Periodically	No	No
□	2010-08-26 10:49:00	Video Clip	Periodically	No	No
□	2010-08-26 10:50:00	Video Clip	Periodically	No	No
□	2010-08-26 10:51:01	Video Clip	Periodically	No	No
□	2010-08-26 10:52:00	Video Clip	Periodically	No	No

Showing 1 to 10 of 12 entries

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

Click to browse pages

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

Appendix

URL Commands for the Network Camera

1. Overview

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. The HTTP-based camera interface provides the functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set internal parameter values. The image and CGI-requests are handled by the built-in Web server.

2. Style Convention

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

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

Syntax:

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

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

Return:

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

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

Example: request a single snapshot image

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

3. General CGI URL Syntax and Parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, these parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in functionally-related directories under the cgi-bin directory. The file extension .cgi is required.

Syntax:

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

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

When querying parameter values, the current parameter values are returned.
A successful control request returns parameter pairs as follows:
Return:

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

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

<length> is the actual length of content.

Example: Request IP address and its response

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

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
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>…][&update=<value>][&return=<return page>]

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

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

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

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign *<value>* to the parameter *<group>_<name>.*
update	<boolean>	Set to 1 to update all fields (no need to update parameter in each group).
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) or a VIVOTEK server script executable (.vspx) file. It cannot be a CGI command or have any extra parameters. This parameter must be placed at the end of the parameter list

Return:

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

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	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
date	<YYYY/MM/DD>, keep, auto	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	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>	6/6	Another current time format of the system.
ntp	<domain name>, <ip address>, <blank>	6/6	NTP server. *Do not use "skip to invoke default server" for default value.
timezoneindex	-489 ~ 529	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>	6/6	Enable automatic daylight saving time in time zone.
daylight_dstactualmode	<boolean>	6/7	Check if current time is under daylight saving time. (Used internally)
daylight_auto_begintime	string[19]	6/7	Display the current daylight saving start time.
daylight_auto_endtime	string[19]	6/7	Display the current daylight saving end time.
daylight_timezones	string	6/6	List time zone index which support daylight saving time.
updateinterval	0, 3600, 86400, 604800, 2592000	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.
restore	0, <positive integer>	7/6	Restore the system parameters to default values after <value> seconds.
reset	0, <positive	7/6	Restart the server after <value> seconds if <value> is non-negative.

	integer>		
restoreexceptnet	<Any value>	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>	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>	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	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	0/7	Internal model name of the server (eg. IP7139)
extendedmodelname	string[40]	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>	0/7	12 characters MAC address (without hyphens).

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

7.2 status

Group: **status**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
di_i<0~(ndi-1)> <product dependent>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered (capability.ndi > 0)
do_i<0~(ndo-1)> <product dependent>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered (capability.ndo > 0)
daynight <product dependent>	day, night	7/7	Current status of day, night.
onlinenum_rtsp	integer	6/7	Current number of RTSP connections.
onlinenum_httppush	integer	6/7	Current number of HTTP push server connections.
eth_i0	<string>	1/7	Get network information from mii-tool.
vi_i<0~(nvi-1)> <product dependent>	<boolean>	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	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	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	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	1/1	Indicate open circuit or closed circuit (inactive status)

7.5 security

Group: security

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

7.6 network

Group: **network**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
preprocess	<positive integer>	7/6	An 32-bit integer, each bit can be set separately as follows: Bit 0 => HTTP service; Bit 1=> HTTPS service; Bit 2=> FTP service; Bit 3 => Two way audio and RTSP Streaming service; To stop service before changing its port settings. It's **recommended** to set this parameter when change a service port to the port occupied by another service currently. Otherwise, the service may fail. Stopped service will auto-start after changing port settings. Ex: Change HTTP port from 80 to 5556, and change RTP port for video from 5556 to 20480. Then, set preprocess=9 to stop both service first. "/cgi-bin/admin/setparam.cgi? network_preprocess=9&network_http_port=5556& network_rtp_videoport=20480"
type	lan, pppoe <product dependent>	6/6	Network connection type.
resetip	<boolean>	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>	6/6	IP address of server.
subnet	<ip address>	6/6	Subnet mask.
router	<ip address>	6/6	Default gateway.
dns1	<ip address>	6/6	Primary DNS server.
dns2	<ip address>	6/6	Secondary DNS server.

wins1	<ip address>	6/6	Primary WINS server.
wins2	<ip address>	6/6	Secondary WINS server.

7.6.1 802.1x

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

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

7.6.2 QOS

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

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

dependent>			
eventalarm	0~7	6/6	Event/alarm channel for CoS
management	0~7	6/6	Management channel for CoS
eventtunnel	0~7	6/6	Event/Control channel for CoS

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

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

7.6.3 IPV6

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

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

7.6.4 FTP

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

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

7.6.5 HTTP

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	1/6	HTTP port.
alternateport	1025~65535	6/6	Alternate HTTP port.
authmode	basic, digest	1/6	HTTP authentication mode.
s0_accessname	string[32]	1/6	HTTP server push access name for stream 1. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 0)
s1_accessname <product dependent>	string[32]	1/6	HTTP server push access name for stream 2. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 1)
s2_accessname <product dependent>	string[32]	1/6	Http server push access name for stream 3 (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 2)
s3_accessname <product dependent>	string[32]	1/6	Http server push access name for stream 4 (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 3)
s4_accessname <product dependent>	string[32]	1/6	Http server push access name for stream 5 (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 4) For some models, it is used for anystream. (capability.protocol.spush.mjpeg = 1 and capability.nanystream = 1)
anonymousviewing	<boolean>	1/6	Enable anoymous streaming viewing.

7.6.6 HTTPS port

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	443, 1025 ~ 65535	1/6	HTTPS port.

7.6.7 RTSP

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	1/6	RTSP port. (capability.protocol.rtsp=1)
anonymousviewing	<boolean>	1/6	Enable anoymous streaming viewing.
authmode	disable, basic, digest	1/6	RTSP authentication mode. (capability.protocol.rtsp=1)
s0_accessname	<boolean>	1/6	RTSP access name for stream1. (capability.protocol.rtsp=1 and capability.nmediastream > 0)
s1_accessname	<boolean>	1/6	RTSP access name for stream2. (capability.protocol.rtsp=1 and capability.nmediastream > 1)
s2_accessname	<boolean>	1/6	RTSP access name for stream3 (capability.protocol.rtsp=1 and capability.nmediastream > 2)
s3_accessname	<boolean>	1/6	RTSP access name for stream4 (capability.protocol.rtsp=1 and capability.nmediastream > 3)
S4_accessname	<boolean>	1/6	RTSP access name for stream5 (capability.protocol.rtsp=1 and capability.nmediastream > 4) For some models, it is used for anystream. (capability.protocol.rtsp=1 and capability.nanystream = 1)
s0_audiotrack	<boolean>	1/6	Enable audio for stream1.
s1_audiotrack	<boolean>	1/6	Enable audio for stream2.
s2_audiotrack	<boolean>	1/6	Enable audio for stream3.
s3_audiotrack	<boolean>	1/6	Enable audio for stream4.
S4_audiotrack	<boolean>	1/6	Enable audio for stream5.

7.6.7.1 RTSP multicast

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	4/4	Enable always multicast.
ipaddress	<ip address>	4/4	Multicast IP address.
videoport	1025 ~ 65535	4/4	Multicast video port.
audioport <product dependent>	1025 ~ 65535	4/4	Multicast audio port. (capability.naudio > 0)
ttl	1 ~ 255	4/4	Mutlicast time to live value.

7.6.8 SIP port

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	1025 ~ 65535	1/6	SIP port.

7.6.9 RTP port

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

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

7.6.10 PPPoE

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

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

7.7 IP Filter

Group: ipfilter

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable access list filtering.
admin_enable	<boolean>	6/6	Enable administrator IP address.
admin_ip	String[44]	6/6	Administrator IP address.
maxconnection	1~10	6/6	Maximum number of concurrent streaming connection(s).
type	0, 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>	6/6	IPv4 address list.
ipv6list_i<0~9>	String[44]	6/6	IPv6 address list.

7.8 Video input

Group: **videoin**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	4/4	CMOS frequency. (capability.videoin.type=2)
exposurelevel	0~12	4/4	Exposure level
irismode	fixed, indoor, outdoor	4/4	Video Iris mode for DC Iris.
enableblc	<boolean>	4/4	Enable backlight compensation.
color	0, 1	4/4	0 =>monochrome 1 => color
flip	<boolean>	4/4	Flip the image.
mirror	<boolean>	4/4	Mirror the image.
ptzstatus	<integer>	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]	1/4	Enclose caption.
imprinttimestamp	<boolean>	4/4	Overlay time stamp on video.
maxexposure	5 ~ 32000	4/4	Maximum exposure time.
enablepreview	<boolean>	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	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	4/4	CMOS frequency.
exposurelevel	0~12	4/4	Exposure level
irismode	fixed, indoor, outdoor	4/4	Video Iris mode for DC Iris.
enableblc	0~1	4/4	Enable backlight compensation
maxgain	0~100	4/4	Manual set maximum gain value.
mingain	0~100	4/4	Manual set minimum gain value.
color	0, 1	4/4	0 =>monochrome 1 => color
flip	<boolean>	4/4	Flip the image.
mirror	<boolean>	4/4	Mirror the image.
ptzstatus	<integer>	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]	1/4	Enclose caption.
imprinttimestamp	<boolean>	4/4	Overlay time stamp on video.
minexposure	5~32000	4/4	Minimum exposure time.
maxexposure	5~32000	4/4	Maximum exposure time.

enablepreview	<boolean>	1/4	Usage for UI of exposure settings. Preview settings of video profile.
s<0~(m-1)>_codectype	mpeg4, mjpeg, h264	1/4	Video codec type.
s<0~(m-1)>_resolution	Reference capability_videoin_resolution	1/4	Video resolution in pixels.
s<0~(m-1)>_enableeptz	<boolean>	1/4	Support ePTZ or not.
s<0~(m-1)>_mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_mpeg4_ratecontrolmode	cbr, vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_quant	1~5 99, 100	4/4	Quality of video when choosing vbr in "ratecontrolmode". 99 is the customized manual input setting. 1 = worst quality, 5 = best quality. 100 is percentage mode.
s<0~(m-1)>_mpeg4_qvalue	2~31	4/4	Manual video quality level input. (s<0~(m-1)>_mpeg4_quant = 99)
s<0~(m-1)>_mpeg4_qpercent	1~100	4/4	Manual video quality level input. (s<0~(m-1)>_mpeg4_quant = 100)
s<0~(m-1)>_mpeg4_bitrate	1000~16000000 <product dependent>	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_mpeg4_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	1/4	Set maximum frame rate in fps (for MPEG-4).
s<0~(m-1)>_h264_intraperiod	250, 500, 1000, 2000, 3000, 4000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_h264_ratecontrolmode	cbr, vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_h264_quant	1~5 99, 100	4/4	Quality of video when choosing vbr in "ratecontrolmode". 99 is the customized manual input

			setting. 1 = worst quality, 5 = best quality. 100 is percentage mode.
s<0~(m-1)>_h264_qvalue	0~51	4/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 99)
s<0~(m-1)>_h264_qpercent	1~100	4/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 100)
s<0~(m-1)>_h264_bitrate	1000~16000000	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_h264_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	1/4	Set maximum frame rate in fps (for h264).
s<0~(m-1)>_h264_profile <product dependent>	0~2	1/4	Indicate H264 profiles 0: baseline 1: main profile 2: high profile
s<0~(m-1)>_mjpeg_quant	1~5 99, 100	4/4	Quality of JPEG video. 99 is the customized manual input setting. 1 = worst quality, 5 = best quality. 100 is percentage mode.
s<0~(m-1)>_mjpeg_qvalue	10~200	4/4	Manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 99)
s<0~(m-1)>_mjpeg_qpercent	1~100	4/4	Manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 100)
s<0~(m-1)>_mjpeg_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	1/4	Set maximum frame rate in fps (for JPEG).

7.8.1.1 Alternative video input profiles per channel

In addition to the primary setting of video input, there can be alternative profile video input setting for each channel which might be for different scene of light (daytime or nighttime).

Group: **videoin_c0_profile_i<0~(m-1)>** (capability. nvideoinprofile > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable/disable this profile setting
policy	day,	4/4	The mode which the profile is applied to.

	night, schedule		
begintime	hh:mm	4/4	Begin time of schedule mode.
endtime	hh:mm	4/4	End time of schedule mode.
minexposure	5~32000	4/4	Minimum exposure time.
maxexposure	5~32000	4/4	Maximum exposure time.
enableblc	<boolean>	4/4	Enable backlight compensation.
exposurelevel	0~12	4/4	Exposure level
maxgain	0~100	4/4	Manual set maximum gain value.
mingain	0~100	4/4	Manual set minimum gain value.
irismode	fixed, indoor, outdoor	4/4	Video Iris mode for DC Iris.

7.9 Video input preview

The temporary settings for video preview

Group: videoinpreview

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
minexposure	5~32000	4/4	Minimum exposure time.
maxexposure	5~32000	4/4	Maximum exposure time.
exposurelevel	0~12	4/4	Exposure level
enableblc	<boolean>	4/4	Enable backlight compensation.
irismode	fixed, indoor, outdoor	4/4	Video Iris mode for DC Iris.
maxgain	0~100	4/4	Manual set maximum gain value.
mingain	0~100	4/4	Manual set minimum gain value.

7.10 IR cut control

Group: **ircutcontrol** (capability.nvideoinprofile > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
mode	auto, day, night, di,	6/6	Set IR cut control mode

	schedule		
daymodebegintime	00:00~23:59	6/6	Day mode begin time
daymodeendtime	00:00~23:59	6/6	Day mod end time
disableirled	<boolean>	6/6	Enable/disable built-in IR LED.
enableextled	<boolean>	6/6	Enable/disable External IR LED.
bwmode	<boolean>	6/6	Switch to B/W in night mode if enabled
sensitivity	low, normal, high	6/6	Sensitivity of light sensor

7.11 Image setting per channel

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	-5~5	4/4	Adjust brightness of image according to mode settings.
saturation	-5~5,100	4/4	Adjust saturation of image according to mode settings. 100 for saturation percentage mode.
saturationpercent	0~100	4/4	Adjust saturation value of percentage when saturation=100
contrast	-5 ~ 5	4/4	Adjust contrast of image according to mode settings.
sharpness	-3~3,100	4/4	Adjust sharpness of image according to mode settings. 100 for sharpness percentage mode.
sharpnesspercent	0~100	4/4	Adjust sharpness value of percentage when sharpness=100
gammacurve	0,45,50,60,70, 80,90,100	4/4	Gamma curve.
lowlightmode	<boolean>	4/4	Enable/disable low light mode.
profile_i0_enable	<boolean>	4/4	Enable/disable this profile setting
profile_i0_policy	day, night, schedule	4/4	The mode which the profile is applied to.
profile_i0_begintime	hh:mm	4/4	Begin time of schedule mode.

profile_i0_endtime	hh:mm	4/4	End time of schedule mode.
profile_i0_brightness	-5~5	4/4	Adjust brightness of image according to mode settings.
profile_i0_saturation	-5~5,100	4/4	Adjust saturation of image according to mode settings. 100 for saturation percentage mode.
profile_i0_saturationpercent	0~100	4/4	Adjust saturation value of percentage when saturation=100
profile_i0_contrast	-5 ~ 5	4/4	Adjust contrast of image according to mode settings.
profile_i0_sharpness	-3~3,100	4/4	Adjust sharpness of image according to mode settings. 100 for sharpness percentage mode.
profile_i0_sharpnesspercent	0~100	4/4	Adjust sharpness value of percentage when sharpness=100
profile_i0_gammacurve	0,45,50,60,70, 80,90,100	4/4	Gamma curve
profile_i0_lowlightmode	<boolean>	4/4	Enable/disable low light mode.

7.12 Image setting for preview

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	-5~5	4/4	Adjust brightness of image according to mode settings.
saturation	-5~5,100	4/4	Adjust saturation of image according to mode settings. 100 for saturation percentage mode.
saturationpercent	0~100	4/4	Adjust saturation value of percentage when saturation=100
contrast	-5 ~ 5	4/4	Adjust contrast of image according to mode settings.
sharpness	-3~3,100	4/4	Adjust sharpness of image according to mode settings. 100 for sharpness percentage mode.
sharpnesspercent	0~100	4/4	Adjust sharpness value of percentage when sharpness=100
gammacurve	0,45,50,60,70,	4/4	Gamma curve

	80,90,100		
lowlightmode	<boolean>	4/4	Enable/disable low light mode.

7.14 Audio input per channel

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
mute	0, 1	4/4	Enable audio mute.
gain	1,5,9,13,17,21,25,29,33, 37,41,45,49,53,57,61	4/4	Gain of input. (-12dB, -9dB, …, +30dB, +33dB)
s<0~(m-1)>_codectype	aac4, gamr, g711	4/4	Set audio codec type for input.
s<0~(m-1)>_aac4_bitrate <product dependent>	16000, 32000, 48000, 64000, 96000, 128000	4/4	Set AAC4 bitrate in bps.
s<0~(m-1)>_gamr_bitrate <product dependent>	4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200	4/4	Set AMR bitrate in bps.
s<0~(m-1)>_g711_mode <product dependent>	pcmu, pcma	4/4	Set G.711 mode.

7.15 Time Shift settings

Group: **timeshift**, c for n channel products, m is stream number (capability.timeshift > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable time shift streaming.
c<0~(n-1)>_s<0~(m-1)>_allow	<boolean>	4/4	Enable time shift streaming for specific stream.

7.16 Motion detection settings

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

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

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

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

			detection window.

7.17 Tempering detection settings

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

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

7.18 DDNS

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

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

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

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

7.19 Express link

Group: expresslink

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable express link.
state	onlycheck, onlyoffline, checkonline, badnetwork	6/6	Camera will check the status of network environment and express link URL
url	string[64]	6/6	The url user define to link to camera

7.20 UPnP presentation

Group: upnppresentation

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

7.21 UPnP port forwarding

Group: upnpportforwarding

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

7.22 System log

Group: **syslog**

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

7.23 camera PTZ control

Group: **camctrl** (capability.camctrl.httptunnel > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enablehttptunnel	<boolean>	4/4	Enable HTTP tunnel for camera control.

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
panspeed	-5 ~ 5	1/4	Pan speed
tiltspeed	-5 ~ 5	1/4	Tilt speed
zoomspeed	-5 ~ 5	1/4	Zoom speed

focusspeed	-5 ~ 5	1/4	Auto focus speed
patrolseq	string[64]	1/4	(For external device) The indexes of patrol points, separated by “,”
patroldwelling	string[128]	1/4	(For external device) The dwelling time of each patrol point, separated by “,”
preset_i<0~(npreset-1)>_name	string[40]	1/4	Name of the preset location.
preset_i<0~(npreset-1)>_ dwelling	0 ~ 999	1/4	The dwelling time of each preset location
uart	0 ~ (m-1), m is UART count	1/4	Select corresponding uart (capability.nuart>0).
cameraid	0~255	1/4	Camera ID controlling external PTZ camera.
isptz	0 ~ 2	1/4	0: disable PTZ commands. 1: enable PTZ commands with PTZ driver. 2: enable PTZ commands with UART tunnel.
disablemdonptz	<boolean>	1/4	Disable motion detection on PTZ operation.

7.24 UART control

Group: **uart** (capability.nuart > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
ptzdrivers_i<0~19, 127>_name	string[40]	1/4	Name of the PTZ driver.
ptzdrivers_i<0~19, 127>_location	string[128]	1/4	Full path of the PTZ driver.
enablehttptunnel	<boolean>	4/4	Enable HTTP tunnel channel to control UART.

Group: **uart_i<0~(n-1)>** n is uart port count (capability.nuart > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
baudrate	110,300,600,1200,2400,3600,4800,7200,9600,19200,38400,57600,115200	4/4	Set baud rate of COM port.
databit	5,6,7,8 6,7,8	4/4	Data bits in a character frame.

	<product dependent>		
paritybit	none, odd, even	4/4	For error checking.
stopbit	1,2	4/4	1 2-1.5 , data bit is 5 2-2
uartmode	rs485, rs232	4/4	RS485 or RS232.
customdrvcmd_i<0~9>	string[128]	1/4	PTZ command for custom camera.
speedlink_i<0~4>_name	string[40]	1/4	Additional PTZ command name.
speedlink_i<0~4>_cmd	string[128]	1/4	Additional PTZ command list.
ptzdriver	0~19, 127 (custom), 128 (no driver)	4/4	The PTZ driver is used by this COM port.

7.25 SNMP

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

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

encrypttypero	DES	6/6	Read only encryption type
rwcommunity	string[31]	6/6	Read/write community
rocommunity	string[31]	6/6	Read only community
syslocation	0~128	6/6	System location
syscontact	0~128	6/6	System contact

7.26 Layout configuration

Group: **layout** (New version)

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

7.27 Privacy mask

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

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

7.28 Capability

Group: capability

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
api_httpversion	<string>	0/7	The HTTP API version.
bootuptime	<positive integer>	0/7	Server bootup time.
nir	0, <positive integer>	0/7	Number of IR interfaces. (Recommand to use ir for built-in IR and extir for external IR)
npir	0, <positive integer>	0/7	Number of PIRs.
ndi	0, <positive integer>	0/7	Number of digital inputs.
nvi	0, <positive integer>	0/7	Number of virtual inputs (manual trigger)
ndo	0, <positive integer>	0/7	Number of digital outputs.
naudioin	0, <positive integer>	0/7	Number of audio inputs.
naudioout	0, <positive integer>	0/7	Number of audio outputs.
nvideoin	<positive integer>	0/7	Number of video inputs.
nmediastream	<positive integer>	0/7	Number of media stream per channels.
nvideosetting	<positive integer>	0/7	Number of video settings per channel.
naudiosetting	<positive integer>	0/7	Number of audio settings per channel.
nuart	0, <positive integer>	0/7	Number of UART interfaces.
nvideoinprofile	<positive integer>	0/7	Number of video input profiles.
nmotionprofile	0, <positive integer>	0/7	Number of motion profiles.
ptzenabled	0, <positive integer>	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>	0/7	Indicate whether to support HTTP tunnel for event/control transfer.
joystick	<boolean>	0/7	Indicate whether to support joystick control.
storage_dbenabled	<boolean>	0/7	Media files are indexed in database.

ptzenabledclient	<boolean>	0/7	Indicate whether to support ptz client
protocol_https	< boolean >	0/7	Indicate whether to support HTTP over SSL.
protocol_rtsp	< boolean >	0/7	Indicate whether to support RTSP.
protocol_sip	<boolean>	0/7	Indicate whether to support SIP.
protocol_maxconnection	<positive integer>	0/7	The maximum allowed simultaneous connections.
protocol_maxgenconnection	<positive integer>	0/7	The maximum general streaming connections .
protocol_maxmegaconnection	<positive integer>	0/7	The maximum megapixel streaming connections.
protocol_rtp_multicast_ scalable	<boolean>	0/7	Indicate whether to support scalable multicast.
protocol_rtp_multicast_ backchannel	<boolean>	0/7	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	0/7	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	0/7	Indicate whether to support RTP over HTTP.
protocol_spush_mjpeg	<boolean>	0/7	Indicate whether to support server push MJPEG.
protocol_snmp	<boolean>	0/7	Indicate whether to support SNMP.
protocol_ipv6	<boolean>	0/7	Indicate whether to support IPv6.
videoin_type	0, 1, 2	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_resolution	176x144,320x256,640x512 ,960x768,1280x1024	0/7	Available resolutions list.
videoin_maxframerate	<a list of available maximum frame rate separated by commas> <product dependent>	0/7	Available maximum frame list.
videoin_codec	mpeg4. mjpeg, h264 <product dependent>	0/7	Available codec list.

videoout_codec	<a list of the available codec types separated by commas) <product dependent>	0/7	Available codec list.
audio_aec	<boolean>	0/7	Indicate whether to support acoustic echo cancellation.
audio_extmic	<boolean>	0/7	Indicate whether to support external microphone input.
audio_linein	<boolean>	0/7	Indicate whether to support external line input. (It will be replaced by audio_mic and audio_extmic.)
audio_lineout	<boolean>	0/7	Indicate whether to support line output.
audio_headphoneout	<boolean>	0/7	Indicate whether to support headphone output.
audioin_codec	aac4, gamr, g711 <product dependent>	0/7	Available codec list for audio input.
audioout_codec	g711 <product dependent>	0/7	Available codec list for SIP.
camctrl_httptunnel	<boolean>	0/7	Indicate whether to support httptunnel.
camctrl_httptunnelclient	<boolean>	0/7	Indicate whether to support httptunnel client.
camctrl_privilege	<boolean>	0/7	Indicate whether to support “Manage Privilege” of PTZ control in the Security page. 1: support both /cgi-bin/camctrl/camctrl.cgi and /cgi-bin/viewer/camctrl.cgi 0: support only /cgi-bin/viewer/camctrl.cgi
uart_httptunnel	<boolean>	0/7	Indicate whether to support HTTP tunnel for UART transfer.
transmission_mode	Tx, Rx, Both	0/7	Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both =

			DVR.
network_wire	<boolean>	0/7	Indicate whether to support Ethernet.
network_wireless	<boolean>	0/7	Indicate whether to support wireless.
wireless_s802dot11b	<boolean>	0/7	Indicate whether to support wireless 802.11b+.
wireless_s802dot11g	<boolean>	0/7	Indicate whether to support wireless 802.11g.
wireless_encrypt_wep	<boolean>	0/7	Indicate whether to support wireless WEP.
wireless_encrypt_wpa	<boolean>	0/7	Indicate whether to support wireless WPA.
wireless_encrypt_wpa2	<boolean>	0/7	Indicate whether to support wireless WPA2.
wireless_beginchannel	1 ~ 14	0/7	Indicate the begin channel of wireless network
wireless_endchannel	1 ~ 14	0/7	Indicate the end channel of wireless network
derivative_brand	<boolean>	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)
npreset	0, <positive integer>	0/7	Number of preset locations
eptz	0, <positive integer>	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
nanystream	0, <positive integer>	0/7	number of any media stream per channel
iva	<boolean>	0/7	Indicate whether to support Intelligent Video analysis

tampering	<boolean>	0/7	Indicate whether to support tampering detection.
test_ac	<boolean>	0/7	Indicate whether to support test ac key.
version_onvifdaemon	<string>	0/7	Indicate ONVIF daemon version
image_wdrc	<Boolean>	0/7	Indicate whether to support WDR enhanced.
image_ iristype	<string>	0/7	Indicate iris type.
image_ focusassist	<Boolean>	0/7	Indicate whether to support focus assist.

7.29 Customized event script

Group: event_customtaskfile_i<0~2>

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

7.30 Event setting

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

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry.
enable	0, 1	6/6	Enable or disable this event.
priority	0, 1, 2	6/6	Indicate the priority of this event: “0” = low priority “1” = normal priority “2” = high priority
delay	1~999	6/6	Delay in seconds before detecting the next event.

trigger	boot, di, motion, seq, recnotify, tampering, vi	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. “vi”= Virtual input (Manual trigger)
triggerstatus	String[40]	6/6	The status for event trigger
di	<integer>	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>	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>	6/6	Similar to mdwin. The parameter takes effect when profile 1 of motion detection is enabled.
vi	<integer>	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	6/6	Interval of snapshots in minutes. This field is used when trigger condition is “seq”.

weekday	0~127	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	6/6	Begin time of the weekly schedule.
endtime	hh:mm	6/6	End time of the weekly schedule. (00:00 ~ 24:00 sets schedule as always on)
action_do_i<0~(ndo-1)>_enable	0, 1	6/6	Enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	6/6	Duration of the digital output trigger in seconds.
action_goto_enable <product dependent>	<Boolean>	6/6	Enable/disable ptz goto preset position on event triggered.
action_goto_name <product dependent>	string[40]	6/6	Specify the preset name that ptz goto on event triggered.
action_cf_enable	<Boolean>	6/6	Enable or disable sending media to SD card.
action_cf_folder	string[128]	6/6	Path to store media.
action_cf_media	NULL, 0~4	6/6	Index of the attached media.
action_cf_datefolder	<boolean>	6/6	Enable this to create folders by date, time, and hour automatically.
action_cf_backup	<Boolean>	6/6	Enable or disable the function that send media to SD card for backup if network is disconnected.
action_server_i<0~4>_enable	0, 1	6/6	Enable or disable this server action.
action_server_i<0~4>_media	NULL, 0~4	6/6	Index of the attached media.
action_server_i<0~4>_datefolder	<boolean>	6/6	Enable this to create folders by date, time, and hour automatically.

7.31 Server setting for event action

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

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry
type	email, ftp, http, ns	6/6	Indicate the server type: "email" = email server "ftp" = FTP server "http" = HTTP server "ns" = network storage
http_url	string[128]	6/6	URL of the HTTP server to upload.

http_username	string[64]	6/6	Username to log in to the server.
http_passwd	string[64]	6/6	Password of the user.
ftp_address	string[128]	6/6	FTP server address.
ftp_username	string[64]	6/6	Username to log in to the server.
ftp_passwd	string[64]	6/6	Password of the user.
ftp_port	0~65535	6/6	Port to connect to the server.
ftp_location	string[128]	6/6	Location to upload or store the media.
ftp_passive	0, 1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode
email_address	string[128]	6/6	Email server address.
email_sslmode	0, 1	6/6	Enable support SSL.
email_port	0~65535	6/6	Port to connect to the server.
email_username	string[64]	6/6	Username to log in to the server.
email_passwd	string[64]	6/6	Password of the user.
email_senderemail	string[128]	6/6	Email address of the sender.
email_recipientemail	string[128]	6/6	Email address of the recipient.
ns_location	string[128]	6/6	Location to upload or store the media.
ns_username	string[64]	6/6	Username to log in to the server.
ns_passwd	string[64]	6/6	Password of the user.
ns_workgroup	string[64]	6/6	Workgroup for network storage.

7.32 Media setting for event action

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

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry
type	snapshot, systemlog, videoclip, recordmsg	6/6	Media type to send to the server or store on the server.

snapshot_source	<integer>	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]	6/6	Indicate the prefix of the filename.
			media_i0=> Snapshot1_
			media_i1=> Snapshot2_
			media_i2=> Snapshot3_
			media_i3=> Snapshot4_
			media_i4=> Snapshot5_

snapshot_datesuffix	0, 1	6/6	Add date and time suffix to filename: 1 = Add date and time suffix. 0 = Do not add.
snapshot_preevent	0 ~ 7	6/6	Indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	6/6	The number of post-event images.
videoclip_source	<integer>	6/6	Indicate the source of media stream. 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]	6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	6/6	Indicates the time for pre-event recording in seconds.
videoclip_maxduration	1 ~ 20	6/6	Maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 8192	6/6	Maximum size of one video clip file in Kbytes.

7.33 Recording

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

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry.
trigger	schedule, networkfail	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	6/6	Enable or disable this recording.

priority	0, 1, 2	6/6	Indicate the priority of this recording: “0” indicates low priority. “1” indicates normal priority. “2” indicates high priority.
source	0~3	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and so on.
limitsize	0,1	6/6	0: Entire free space mechanism 1: Limit recording size mechanism
cyclic	0,1	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	0,1	6/6	0: Disable recording notification 1: Enable recording notification

notifyserver	0~31	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	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	6/6	Start time of the weekly schedule.
endtime	hh:mm	6/6	End time of the weekly schedule. (00:00~24:00 indicates schedule always on)
prefix	string[16]	6/6	Indicate the prefix of the filename.

cyclesize	200~	6/6	The maximum size for cycle recording in Kbytes when choosing to limit recording size. (not used in IP8362)
reserveamount	0~	6/6	The reserved amount in Mbytes when choosing cyclic recording mechanism.
dest	cf, 0~4	6/6	The destination to store the recorded data. “cf” means local storage (CF or SD card). “0” means the index of the network storage.
cffolder	string[128]	6/6	Folder name.
adaptive_enable <product dependent>	0,1	6/6	Indicate whether the adaptive recording is enabled
adaptive_preevent <product dependent>	0~9	6/6	Indicate when is the adaptive recording started before the event trigger point (seconds)
adaptive_postevent <product dependent>	0~10	6/6	Indicate when is the adaptive recording stopped after the event trigger point (seconds)

7.34 HTTPS

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

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

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

status	-3 ~ 1	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]	6/6	Country name in the certificate information.
stateorprovincename	string[128]	6/6	State or province name in the certificate information.

localityname	string[128]	6/6	The locality name in the certificate information.
organizationname	string[64]	6/6	Organization name in the certificate information.
unit	string[32]	6/6	Organizational unit name in the certificate information.
commonname	string[64]	6/6	Common name in the certificate information.
validdays	0 ~ 3650	6/6	Valid period for the certification.

7.35 Storage management setting

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

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

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

7.36 Region of interest

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

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

7.37 ePTZ setting

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

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
osdzoom	<boolean>	1/4	Indicates multiple of zoom in is "on-screen display" or not
smooth	<boolean>	1/4	Enable the ePTZ "move smoothly" feature
tiltspeed	-5 ~ 5	1/7	Tilt speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
panspeed	-5 ~ 5	1/7	Pan speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
zoomspeed	-5 ~ 5	1/7	Zoom speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
autospeed	1 ~ 5	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	SECURITY (get/set)	DESCRIPTION
patrolseq	string[120]	1/4	The patrol sequence of ePTZ. All the patrol position indexes will be separated by ","
patroldwelling	string[160]	1/4	The dwelling time (unit: second) of each patrol point, separated by ",".
preset_i<0~19>_name	string[40]	1/7	Name of ePTZ preset. (It should be set by ePreset.cgi rather than by setparam.cgi.)
preset_i<0~19>_pos	<coordinate>	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>	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 Drive the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

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

Where state is 0 or 1; “0” means inactive or normal state, while “1” means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – Inactive, normal state
		1 – Active, triggered state

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

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

8.2 Query Status of the Digital Input (capability.ndi > 0)

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
```

8.3 Query Status of the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

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

If no parameter is specified, all the digital output 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
[do0=<state>]\r\n
[do1=<state>]\r\n
[do2=<state>]\r\n
[do3=<state>]\r\n
```

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

Example: Query the status of digital output 1.

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

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

```
\r\n
do1=1\r\n
```

8.5 Capture Single Snapshot

Note: This request requires Normal User privileges.

Method: GET/POST

Syntax:

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

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

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

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

Return:

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

<binary JPEG image data>
```

8.6 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.

8.7 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
```

8.8 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.

8.9 Camera Control (capability.ptzenabled)

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/camctrl.cgi?[channel=<value>][&camid=<value>]
[&move=<value>] – Move home, up, down, left, right
[&focus=<value>] – Focus operation
[&iris=<value>] – Iris operation
[&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>][&speedlink
=<value>] ] – Set speeds
[&return=<return page>]
```

Example:

```
http://myserver/cgi-bin/viewer/camctrl.cgi?channel=0&camid=1&move=right
http://myserver/cgi-bin/viewer/camctrl.cgi?channel=0&camid=1&zoom=tele
```

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

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
camid	0,<positive integer>	Camera ID.
move	home	Move to camera to home position.
	up	Move camera up.
	down	Move camera down.
	left	Move camera left.
	right	Move camera right.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.
speedfocus	-5 ~ 5	Set the focus speed.
speedapp	-5 ~ 5	Set the auto pan/patrol speed.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop camera.
zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.
	stop	Stop zoom.
zooming	wide or tele	Zoom without stopping for larger view or further view with zs speed, used for joystick control.
zs	0 ~ 6 0 ~ 15 <SD81X1>	Set the speed of zooming, "0" means stop.
vx	<integer , excluding 0>	The slope of movement = vy/vx, used for joystick control.
vy	<integer>	
vs	0 ~ 7 0 ~ 15 <SD81X1>	Set the speed of movement, "0" means stop.
x	<integer>	x-coordinate clicked by user. It will be the x-coordinate of center after movement.
y	<integer>	y-coordinate clicked by user. It will be the y-coordinate of center after movement.

videosize	<window size>	The size of plug-in (ActiveX) window in web page
resolution	<window size>	The resolution of streaming.
stretch	<boolean>	0 indicates that it uses **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.
focus	auto	Auto focus.
	far	Focus on further distance.
	near	Focus on closer distance.
iris	auto	Let the Network Camera control iris size.
	open	Manually control the iris for bigger size.
	close	Manually control the iris for smaller size.
speedlink	0 ~ 4	Issue speed link command.
gaptime	0~32768	The gaptime between two consecutive ptz commands for device. (unit: ms)
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned*.* The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.10 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.

8.11 Recall (capability.ptzenabled)

Note: This request requires Viewer privileges.

Method: GET

Syntax:

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

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

8.12 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.

8.13 Preset Locations (capability.ptzenabled)

Note: This request requires Operator privileges.

Method: GET/POST

Syntax:

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

PARAMETER	VALUE	DESCRIPTION
addpos	<Text string less than 30 characters>	Add one preset location to the preset list.
channel	<0~(n-1)>	Channel of the video source.
delpos	<Text string less than 30 characters>	Delete preset location from preset list.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned*.* The <*return page*> can be a full URL path or relative

		path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.14 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.

8.15 IP Filtering

Note: This request requires Administrator access privileges.

Method: GET/POST

Syntax: <product dependent>

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

PARAMETER	VALUE	DESCRIPTION
type	NULL	Get IP filter type
	allow, deny	Set IP filter type
method	addv4	Add IPv4 address into access list.

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

8.16 UART HTTP Tunnel Channel (capability.nuart > 0)

Note: This request requires Operator privileges.

Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/operator/uartchannel.cgi?[channel=<value>]
-----------------------------------------------------------------------
GET /cgi-bin/operator/uartchannel.cgi?[channel=<value>]
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache

-----------------------------------------------------------------------
POST /cgi-bin/operator/uartchannel.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 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 a proxy server.

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

Please see UART tunnel spec for detail information

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

8.17 Event/Control HTTP Tunnel Channel (capability. evctrlchannel > 0)

Note: This request requires Administrator privileges.

Method: GET and POST

Syntax:

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

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

8.18 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.

8.19 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.

8.20 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.

8.21 Storage managements (capability.storage.dbenabled > 0)

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
```

8.22 Virtual input (capability.nvi > 0)

Note: Change virtual input (manual trigger) status.

Method: GET

Syntax:

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

PARAMETER	VALUE	DESCRIPTION
vi<num>	state[(duration)nstate] Where "state" is 0, 1. “0” means inactive or normal state while “1” means active or triggered state. Where "nstate" is next	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. Note that when the virtual input is waiting for next state,

	state after duration.	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).

8.23 Open Timeshift Stream (capability.timeshift > 0, timeshift_enable=1, timeshift_c<n>_s<m>_allow=1)

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

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

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

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

"n" is the channel index.

"m" is the timeshift stream index.

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

PARAMETER	VALUE	DEFAULT	DESCRIPTION
maxsft	<positive interger>	0	Request cached stream at most how many seconds ago.
tsmode	normal, adaptive	normal	Streaming mode: normal => Full FPS all the time. adaptive => Default send only I-frame for MP4 and H.264, and send 1 FPS for MJPEG. If DI or motion window are triggered, the streaming is changed to send full FPS for 10 seconds. (*Note: this parameter also works on non-timeshift streams.)
reftime	mm:ss	The time camera receives the request.	Reference time for maxsft and minsft. (This provides more precise time control to eliminate the inaccuracy due to network latency.) Ex: Request the streaming from 12:20 rtsp://10.0.0.1/live.sdp?maxsft=10&reftime=12:30
forcechk	N/A	N/A	Check if the requested stream enables timeshift, feature and if minsft is achievable. If false, return "415 Unsupported Media Type".
minsft	<positive interger>	0	How many seconds of cached stream client can accept at least. (Used by forcechk)

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

8. 24 Open Anystream (capability.nanystream > 0)

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

```
http://<servername>/videoany.mjpg?codectype=mjpeg[&resolution=<value>&mjpeg_quant=<value>&
mjpeg_qvalue=<value>&mjpeg_maxframe=<value>]
```

For RTSP (MPEG4), the user needs to input the URL below into an RTSP compatible player.

```
rtsp://<servername>/liveany.sdp?codectype=mpeg4[&resolution=<value>&mpeg4_intraperiod=<value>
&mpeg4_ratecontrolmode=<value>&mpeg4_quant=<value>&mpeg4_qvalue=<value>&mpeg4_bitrate=
<value>&mpeg4_maxframe=<value>]
```

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

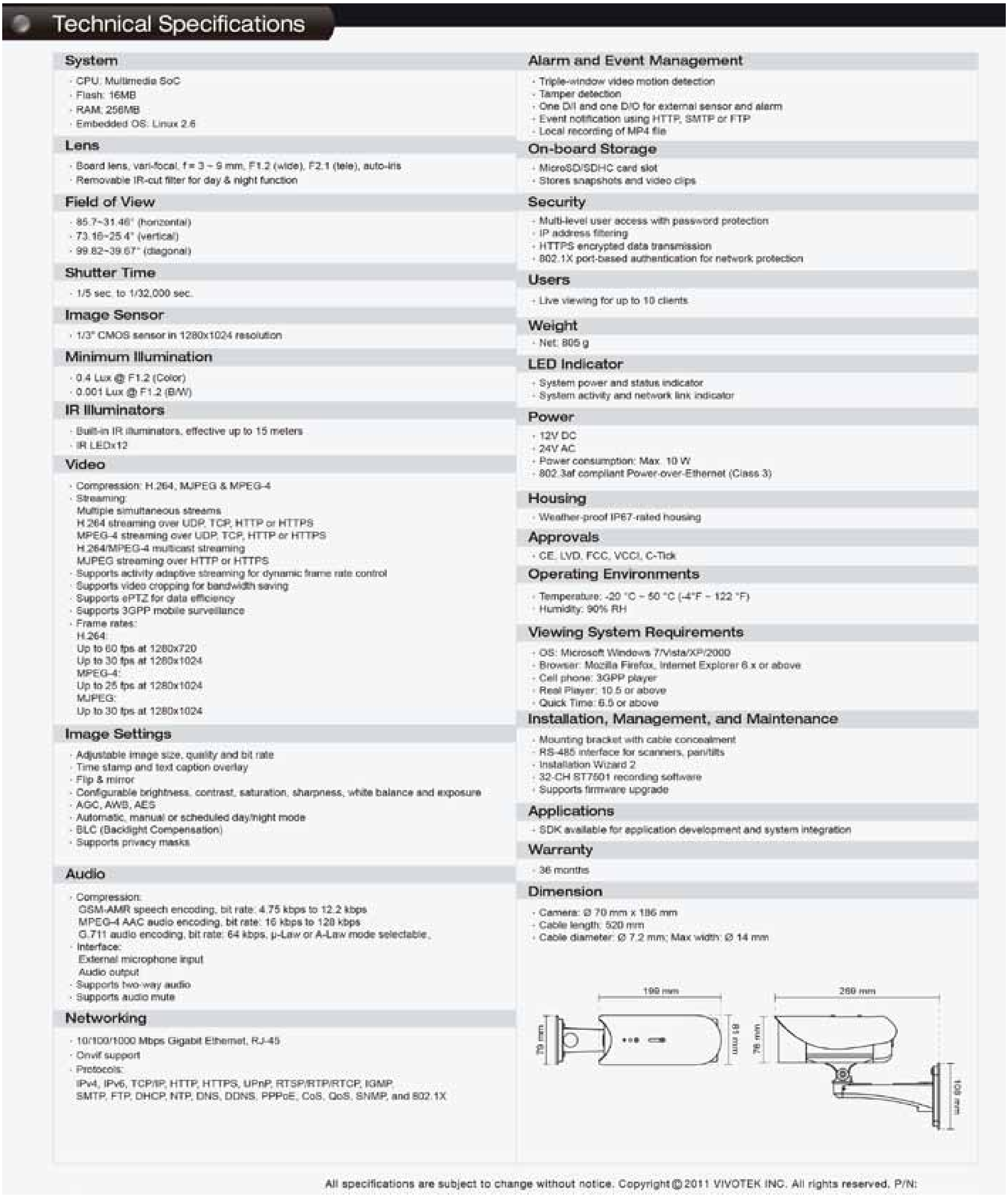
```
rtsp://<servername>/liveany.sdp?codectype=h264[&resolution=<value>&h264_intraperiod=<value>&
h264_ratecontrolmode=<value>& h264_quant=<value>& h264_qvalue=<value>&
h264_bitrate=<value>& h264_maxframe=<value>]
```

<product dependent>

PARAMETER	VALUE	DEFAULT	DESCRIPTION
codectype	mjpeg, mpeg4, h264 <product dependent>	N/A	Set codec type for Anystream.
solution	capability_videoin_resolution	<product dependent>	Video resolution in pixels.
mjpeg_quant	1~5, 100, 99 <product dependent>	3	Quality of JPEG video. 100,99 is the customized manual input setting. 1 = worst quality, 5 = best quality. <product dependent>
mjpeg_qvalue	10~200	50 <product dependent>	Manual video quality level input. (This must be present if mjpeg_quant is equal to 99) <product dependent>
mjpeg_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	15	Set maximum frame rate in fps (for JPEG).
mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	Intra frame period in milliseconds.
mpeg4_ratecontrolmode	cbr, vbr	vbr	cbr: constant bitrate vbr: fix quality
mpeg4_quant	1~5, 100, 99 <product dependent>	3	Quality of video when choosing vbr in “mpeg4_ratecontrolmode”. 100,99 is the customized manual input setting. 1 = worst quality, 5 = best quality. <product dependent>
mpeg4_qvalue	2~31 <product dependent>	7 <product	Manual video quality level input. (This must be present if mpeg4_quant

		dependent>	is equal to 99)
mpeg4_bitrate	1000~16000000	512000 <product dependent>	Set bit rate in bps when choosing cbr in “mpeg4_ratecontrolmode”.
mpeg4_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	10 15 <product dependent>	Set maximum frame rate in fps (for MPEG-4).
h264_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	Intra frame period in milliseconds.
h264_ratecontrolmode	cbr, vbr	vbr	cbr: constant bitrate vbr: fix quality
h264_quant	1~5, 100, 99 <product dependent>	3	Quality of video when choosing vbr in “h264_ratecontrolmode”. 100,99 is the customized manual input setting. 1 = worst quality, 5 = best quality. <product dependent>
h264_qvalue	0~51 <product dependent>	30 <product dependent>	Manual video quality level input. (This must be present if h264_quant is equal to 99) <product dependent>
h264_bitrate	1000~16000000	512000 <product dependent>	Set bit rate in bps when choosing cbr in “h264_ratecontrolmode”.
h264_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	10 15 <product dependent>	Set maximum frame rate in fps (for H264).

Technical Specifications



Technical Specifications

System
- CPU: Multimedia SoC
- Flash: 16MB
- RAM: 256MB
- Embedded OS: Linux 2.6

Lens
- Board lens, vari-focal, f = 3 ~ 9 mm, F1.2 (wide), F2.1 (tele), auto-iris
- Removable IR-cut filter for day & night function

Field of View
- 85.7~31.46° (horizontal)
- 73.16~25.4° (vertical)
- 99.82~39.67° (diagonal)

Shutter Time
- 1/5 sec. to 1/32,000 sec.

Image Sensor
- 1/3" CMOS sensor in 1280x1024 resolution

Minimum Illumination
- 0.4 Lux @ F1.2 (Color)
- 0.001 Lux @ F1.2 (B/W)

IR Illuminators
- Built-in IR illuminators, effective up to 15 meters
- IR LEDx12

Video
- Compression: H.264, MJPEG & MPEG-4
- Streaming:
  Multiple simultaneous streams
  H.264 streaming over UDP, TCP, HTTP or HTTPS
  MPEG-4 streaming over UDP, TCP, HTTP or HTTPS
  H.264/MPEG-4 multicast streaming
  MJPEG streaming over HTTP or HTTPS
- Supports activity adaptive streaming for dynamic frame rate control
- Supports video cropping for bandwidth saving
- Supports ePTZ for data efficiency
- Supports 3GPP mobile surveillance
- Frame rates:
  H.264:
  Up to 60 fps at 1280x720
  Up to 30 fps at 1280x1024
  MPEG-4:
  Up to 25 fps at 1280x1024
  MJPEG:
  Up to 30 fps at 1280x1024

Image Settings
- Adjustable image size, quality and bit rate
- Time stamp and text caption overlay
- Flip & mirror
- Configurable brightness, contrast, saturation, sharpness, white balance and exposure
- AGC, AWB, AES
- Automatic, manual or scheduled day/night mode
- BLC (Backlight Compensation)
- Supports privacy masks

Audio
- Compression:
  GSM-AMR speech encoding, bit rate: 4.75 kbps to 12.2 kbps
  MPEG-4 AAC audio encoding, bit rate: 16 kbps to 128 kbps
  G.711 audio encoding, bit rate: 64 kbps, μ-Law or A-Law mode selectable.
- Interface:
  External microphone input
  Audio output
- Supports two-way audio
- Supports audio mute

Networking
- 10/100/1000 Mbps Gigabit Ethernet, RJ-45
- Onvif support
- Protocols:
  IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP,
  SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP, and 802.1X

Alarm and Event Management
- Triple-window video motion detection
- Tamper detection
- One D/I and one D/O for external sensor and alarm
- Event notification using HTTP, SMTP or FTP
- Local recording of MP4 file

On-board Storage
- MicroSD/SDHC card slot
- Stores snapshots and video clips

Security
- Multi-level user access with password protection
- IP address filtering
- HTTPS encrypted data transmission
- 802.1X port-based authentication for network protection

Users
- Live viewing for up to 10 clients

Weight
- Net: 805 g

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

Power
- 12V DC
- 24V AC
- Power consumption: Max. 10 W
- 802.3af compliant Power-over-Ethernet (Class 3)

Housing
- Weather-proof IP67-rated housing

Approvals
- CE, LVD, FCC, VCCI, C-Tick

Operating Environments
- Temperature: -20 °C ~ 50 °C (-4°F ~ 122 °F)
- Humidity: 90% RH

Viewing System Requirements
- OS: Microsoft Windows 7/Vista/XP/2000
- Browser: Mozilla Firefox, Internet Explorer 6.x or above
- Cell phone: 3GPP player
- Real Player: 10.5 or above
- Quick Time: 6.5 or above

Installation, Management, and Maintenance
- Mounting bracket with cable concealment
- RS-485 interface for scanners, pan/tilts
- Installation Wizard 2
- 32-CH ST7501 recording software
- Supports firmware upgrade

Applications
- SDK available for application development and system integration

Warranty
- 36 months

Dimension
- Camera: Ø 70 mm x 186 mm
- Cable length: 520 mm
- Cable diameter: Ø 7.2 mm; Max width: Ø 14 mm

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.

VCCI Warning

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準にづくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.