

H.264 • Privacy Button • Compact Design **IP8132/8133/8133W**

NETWORK CAMERA *User's Manual*

IP8132
Wired



IP8133W
Wireless



IP8133
Wired PoE



Rev. 1.1

Table of Contents

| | |
|---|------------|
| Overview | 3 |
| Read Before Use..... | 3 |
| Package Contents..... | 3 |
| Physical Description..... | 4 |
| Install Ferrite Core..... | 6 |
| Network Deployment..... | 8 |
| Software Installation..... | 10 |
| Ready to Use..... | 11 |
| Accessing the Network Camera | 12 |
| Using Web Browsers..... | 12 |
| Using RTSP Players..... | 15 |
| Using 3GPP-compatible Mobile Devices..... | 16 |
| Using VIVOTEK Recording Software..... | 17 |
| Main Page | 18 |
| Client Settings | 22 |
| Configuration | 24 |
| System..... | 25 |
| Security..... | 28 |
| HTTPS (Hypertext Transfer Protocol over SSL)..... | 29 |
| SNMP (Simple Network Management Protocol)..... | 34 |
| Network..... | 35 |
| Wireless (IP8133W)..... | 49 |
| Express Link..... | 58 |
| DDNS..... | 59 |
| Access List..... | 61 |
| Audio and Video..... | 64 |
| Motion Detection..... | 74 |
| Camera Tampering Detection..... | 77 |
| Homepage Layout..... | 78 |
| Application..... | 81 |
| Recording..... | 97 |
| System Log..... | 101 |
| View Parameters..... | 102 |
| Maintenance..... | 103 |
| Appendix | 107 |
| URL Commands for the Network Camera..... | 107 |
| Technical Specifications..... | 159 |
| Technology License Notice..... | 160 |
| Electromagnetic Compatibility (EMC)..... | 161 |

Overview

Read Before Use

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

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

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

Package Contents

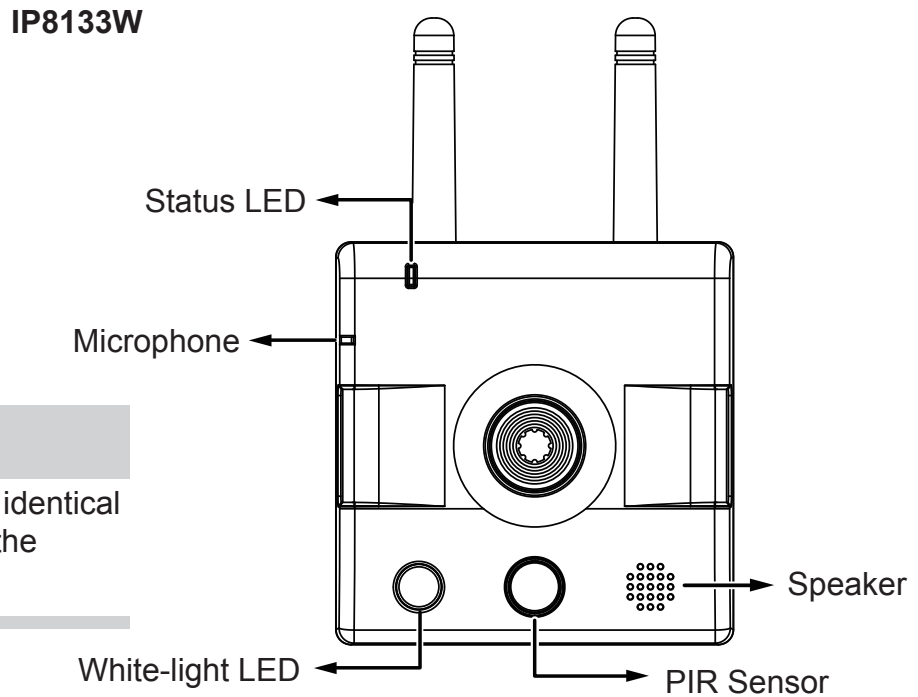
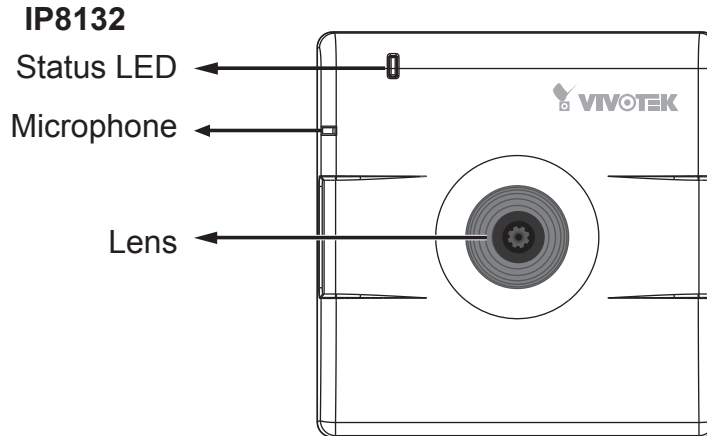
- IP8132, IP8133, or IP8133W
- Power Adapter and Ferrite Core (IP8133/33W)
- Camera Stand
- Software CD
- Warranty Card
- Quick Installation Guide
- Screws
- Antenna (IP8133W)

Revision History

- Rev. 1.0: Initial release
- Rev. 1.1: Updated RTSP audio port screen captures.
Updated available network bit rates.

Physical Description

Front Panel

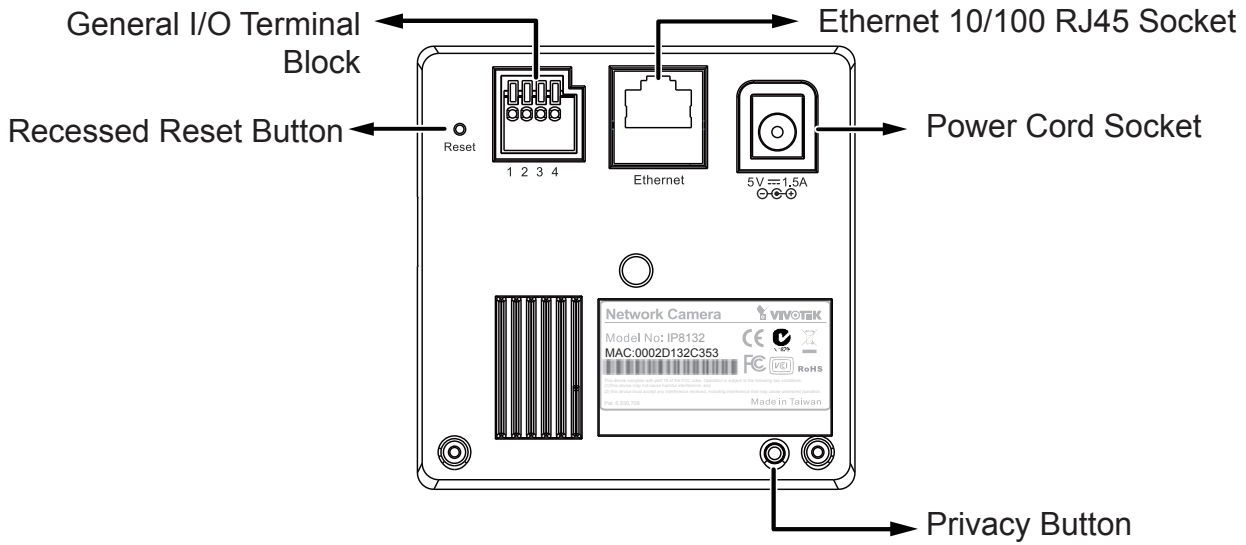


NOTE:
 The front view of IP8133 is identical to that of IP8133W except the wireless antenna.

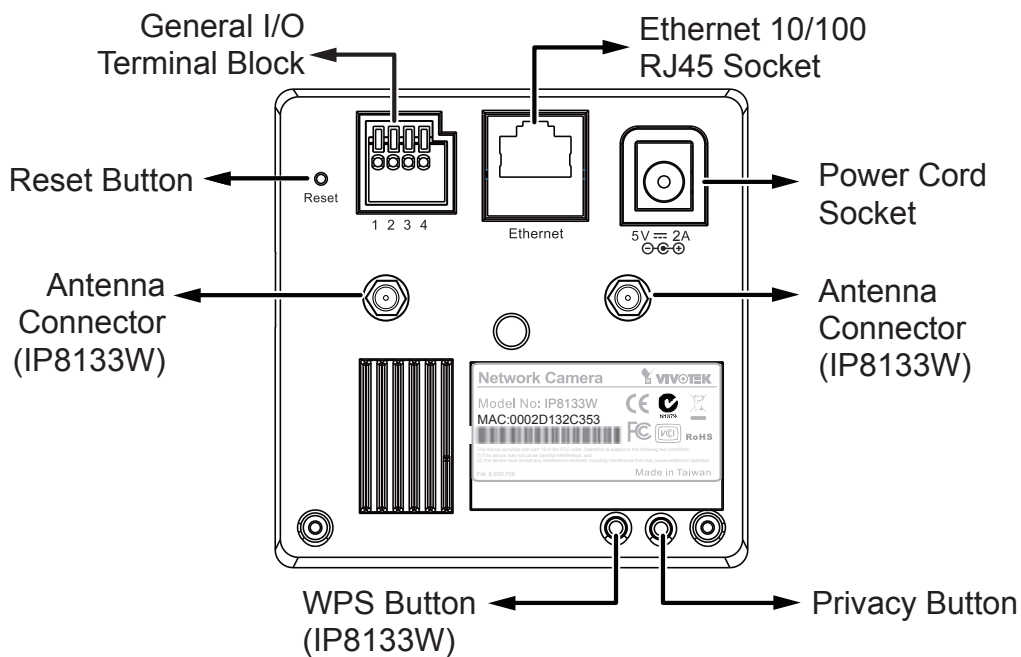
| | Item | LED status | Description |
|------------------------|---|---------------------------|--------------------------|
| LED Definitions | 1 | Steady Red | Power on and system boot |
| | | Red LED off | Power off |
| | 2 | Blink Green every 1 sec. | Network connected |
| | | Steady Red | Network failed |
| | 3 | Blink Green every 2 sec. | Audio muted |
| | 4 | Blink Orange every 2 sec. | Privacy button pressed |
| 5 | Blink Green, RED, and Orange intermittently | Upgrading firmware | |
| 6 | Blink Orange every 0.15 sec. | Restoring default | |

Back Panel

IP8132

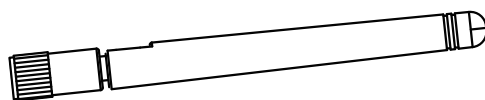


IP8133 & 8133W



NOTE:

Two antennas come with the IP8133W. They are installed by users by turning clockwise to attach to connectors.



General I/O Terminal Block

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

| Pin | Name |
|-----|------------------|
| 4 | Power |
| 3 | Digital Output + |
| 2 | Digital Input - |
| 1 | Ground |

Hardware Reset

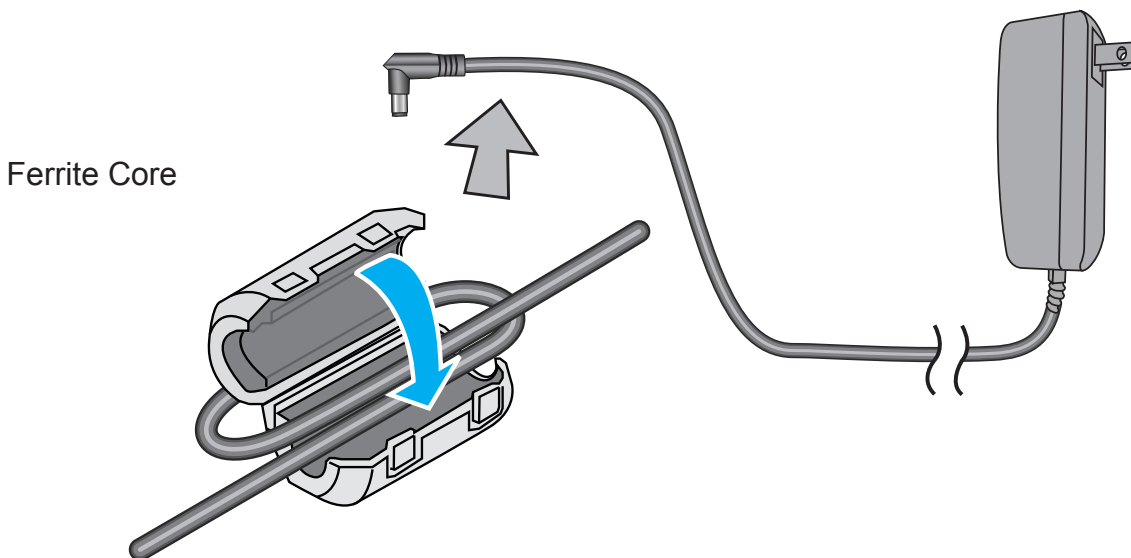
The reset button is used to reset the system or restore the factory default settings. Sometimes resetting the system can return the camera to normal operation. If the system problems remain after reset, restore the factory settings and install again.

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

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

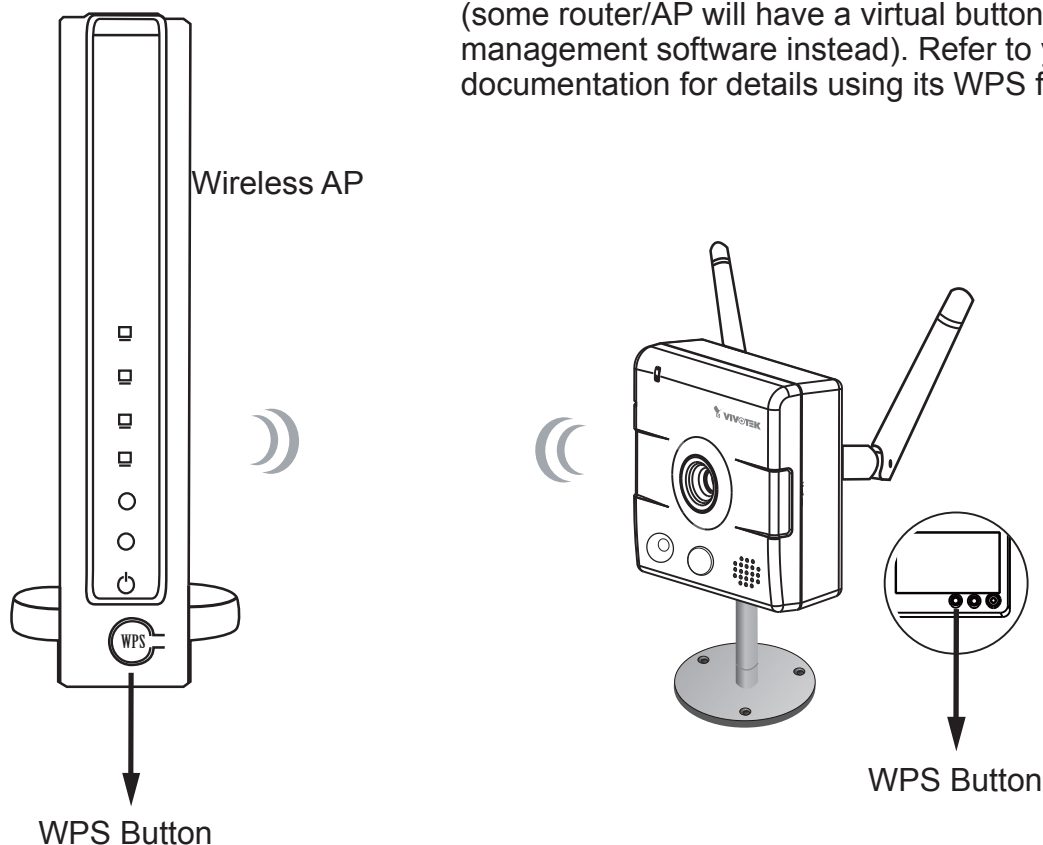
Install Ferrite Core

1. Unsnap the two halves of the ferrite core.
2. Attach the ferrite core to the power cord as close to the DC connector as possible. Fold the ferrite core over the power cord, wrap the power cord once, and snap the small latches together.



Wireless Connection: Using the WPS Button

1. Make sure your AP (Access Point) and Operating System support WPS (Wi-Fi Protected Setup) functions. WPS enables easy setup with compatible APs.
2. Disconnect your LAN cable, and wait for the LED to turn red.
3. Press the WPS button for 1 second. You can then hear vocal instructions (in English) from the camera speaker.
4. Press and hold down the WPS button on your AP (some router/AP will have a virtual button on their management software instead). Refer to your AP's documentation for details using its WPS functions.



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



NOTE:

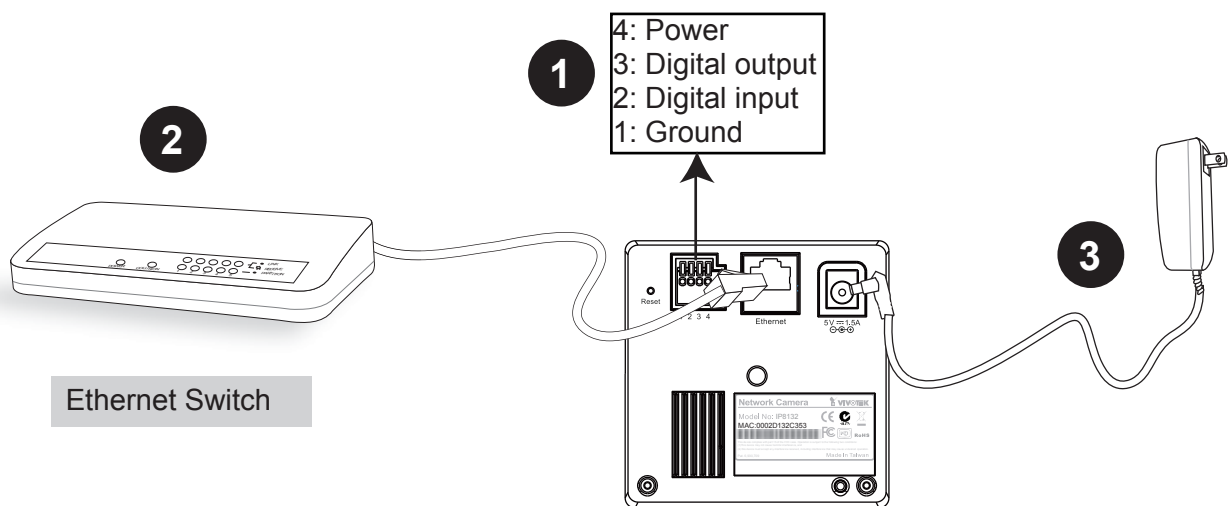
1. WPS may not work if your AP is configured with a "hidden" SSID.
2. If no WPS-enabled AP is detected, the camera will repeat vocal instructions by every 20 seconds, and if the camera still can not detect an AP after 2 minutes, the wireless setup will be cancelled.
3. If a camera is assigned with a fixed IP outside the AP's network segment, wireless setup will fail.
4. A wired connection always has a higher priority, and hence wireless setup will not take effect when the RJ45 LAN port is connected.

Network Deployment

Setting up the Network Camera over the Internet

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

1. If you have external devices such as sensors and alarms, make connections from general I/O terminal block.
2. Connect the camera to a switch via Ethernet cable. Use a Category 5 Cross Cable when Network Camera is directly connected to PC.
3. Connect the power cable from the Network Camera to a power outlet.



NOTE:

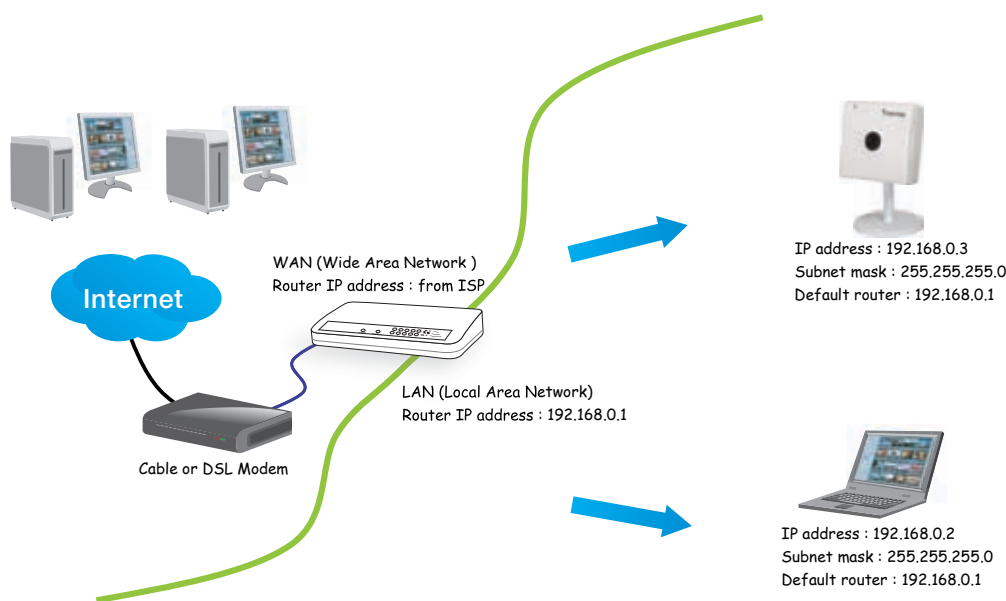
The IP8133 can acquire power through a cable connection with a PoE switch. However, when so connected, the camera is only to be connected to PoE networks without routing to outside plants.

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

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 10 for details.



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

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

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 35 for details.

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN on page 35 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 36 for details.

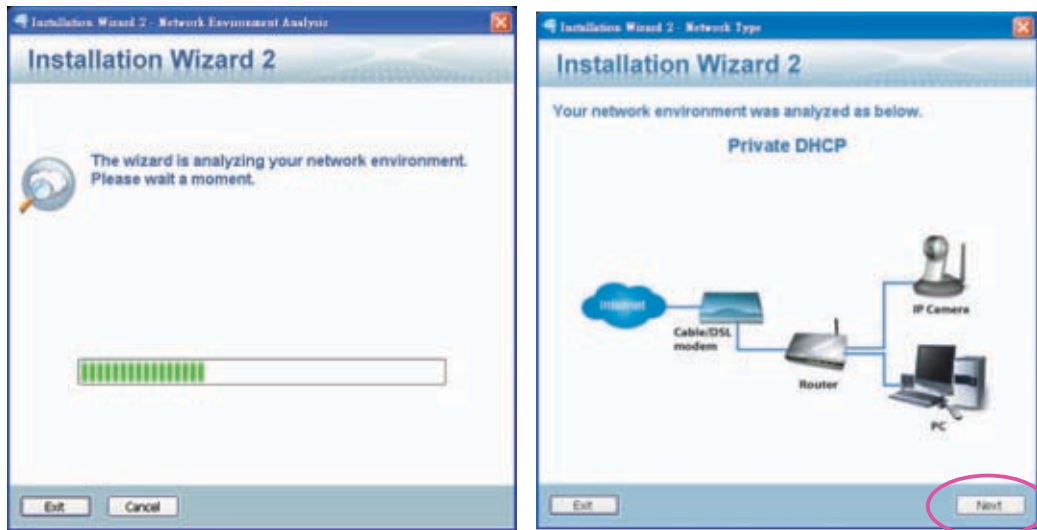
Software Installation

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

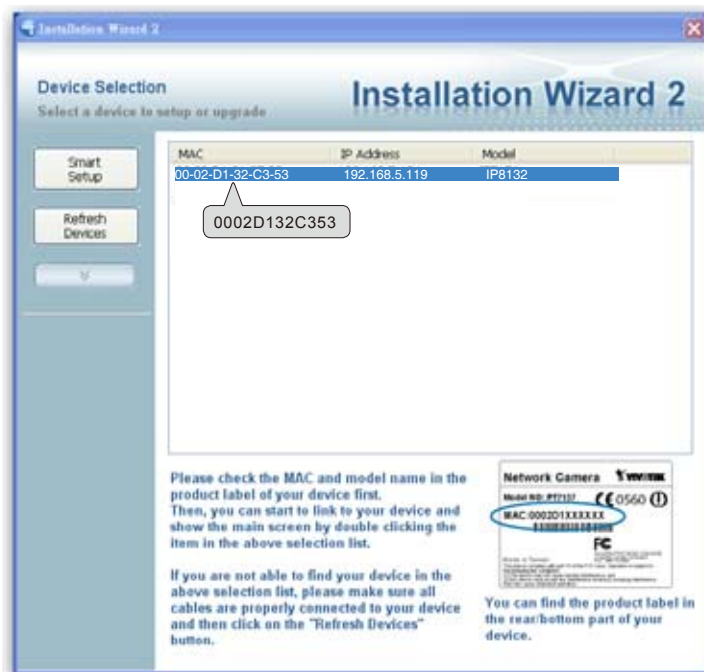
1. Install IW2 under the Software Utility directory from the software CD.
Double click the IW2 shortcut on your desktop to launch the program.



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

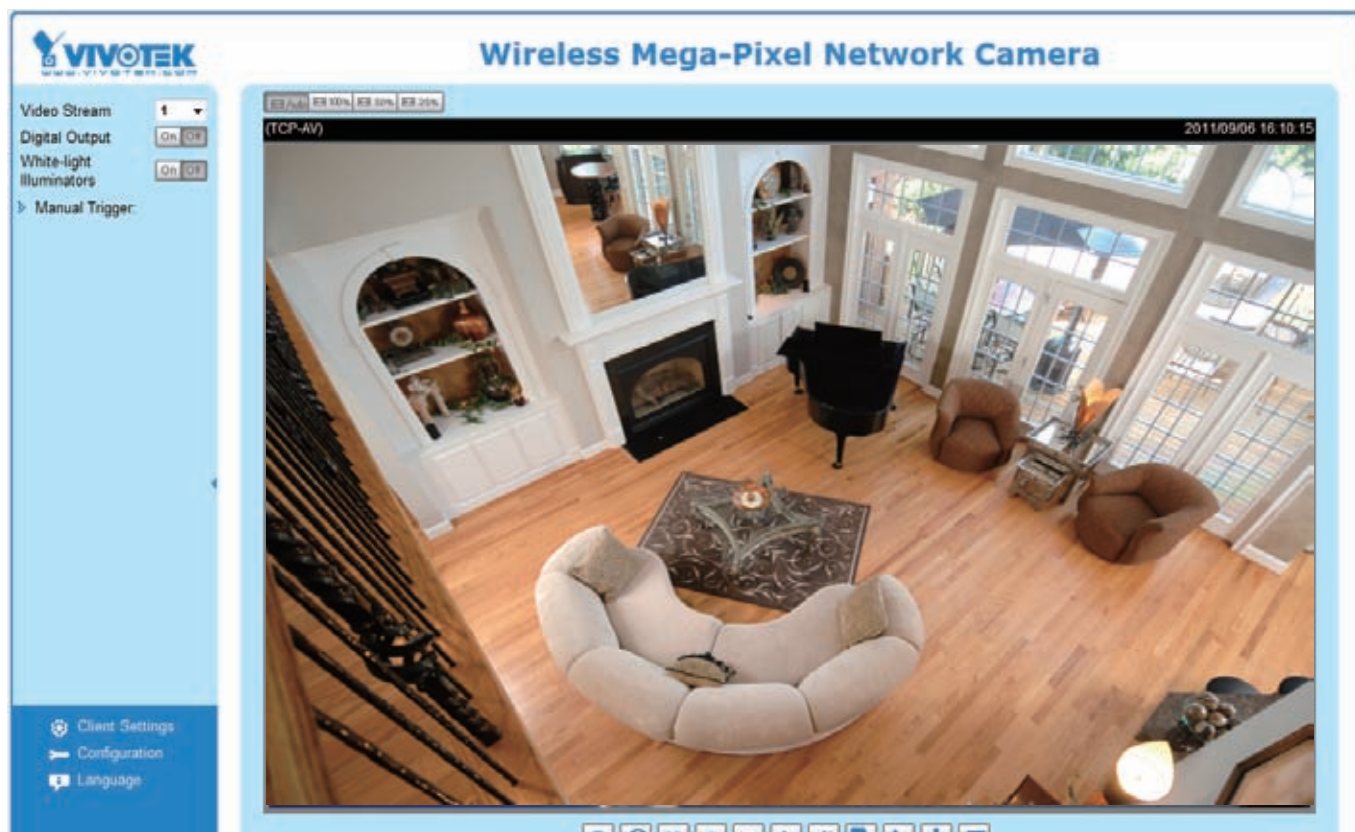


3. The program will search for all VIVOTEK network devices on the same LAN.
4. After searching, the main installer window will pop up. Click on the MAC and model name which matches the product label on your device to connect to the Network Camera via Internet Explorer.



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.



Accessing the Network Camera

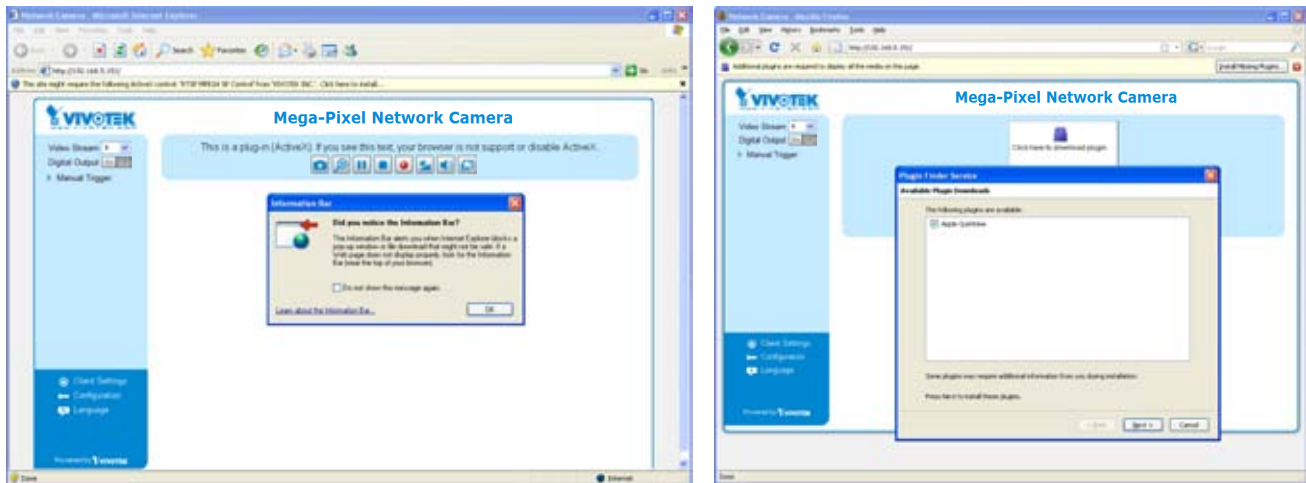
This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

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

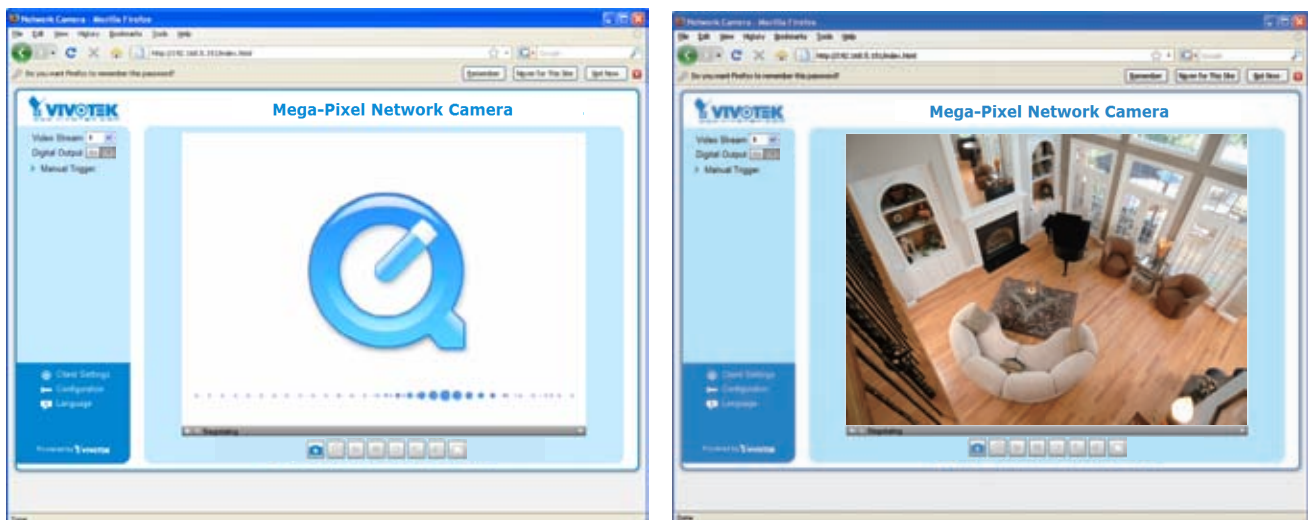
If your network environment is not a LAN, follow these steps to access the Network Camera:

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



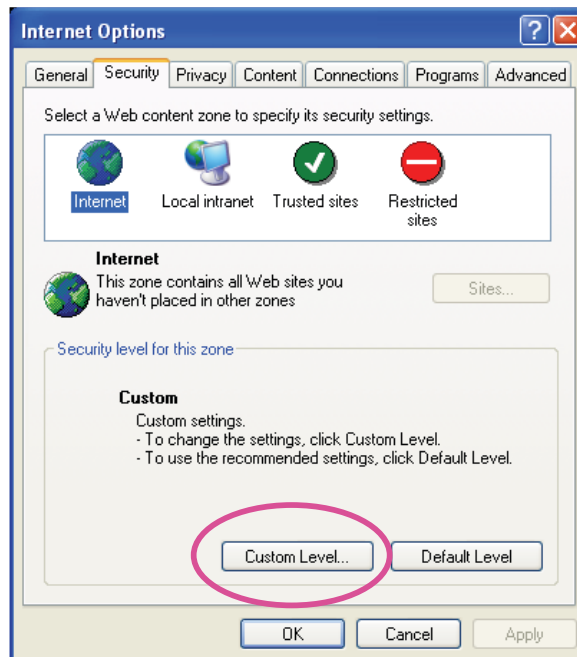
NOTE:

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

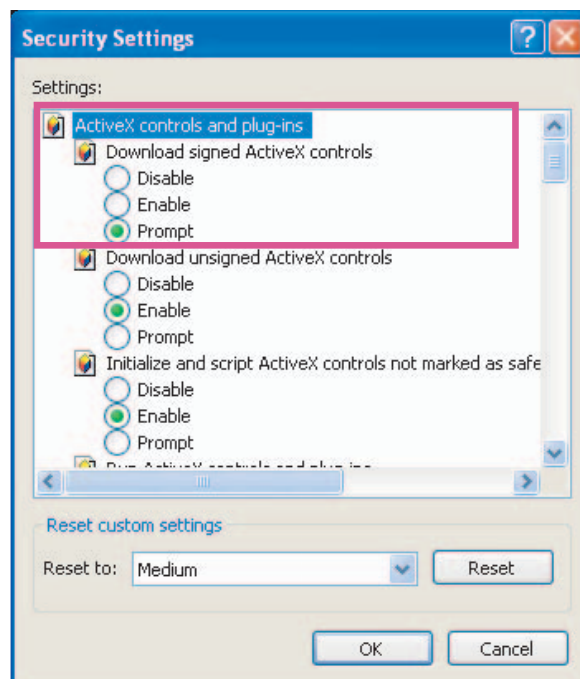


- ▶ *By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera. For more information about how to enable password protection, please refer to Security on page 28.*
- ▶ *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable the ActiveX® Controls for your browser.*

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



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



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

**IMPORTANT!**

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

Using RTSP Players

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



Quick Time Player

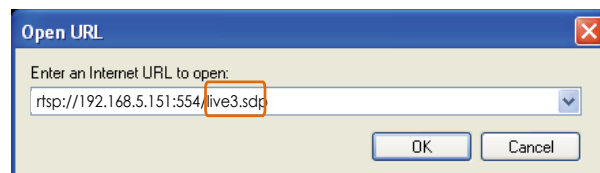


Real Player

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

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 47.

For example:



4. The live video will be displayed in your player.
For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 47 for details.



Using 3GPP-compatible Mobile Devices

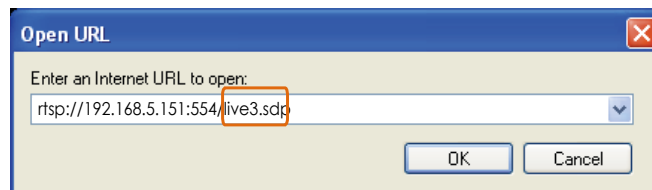
To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 8.

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 47.
2. As the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video streaming parameters as listed below.
For more information, please refer to Viewing Window on page 69.

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

3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 47.
4. Launch the player on the 3GPP-compatible mobile devices (ex. Real Player).
5. Type the following URL commands into the player.
The address format is `rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream 3>`.
For example:



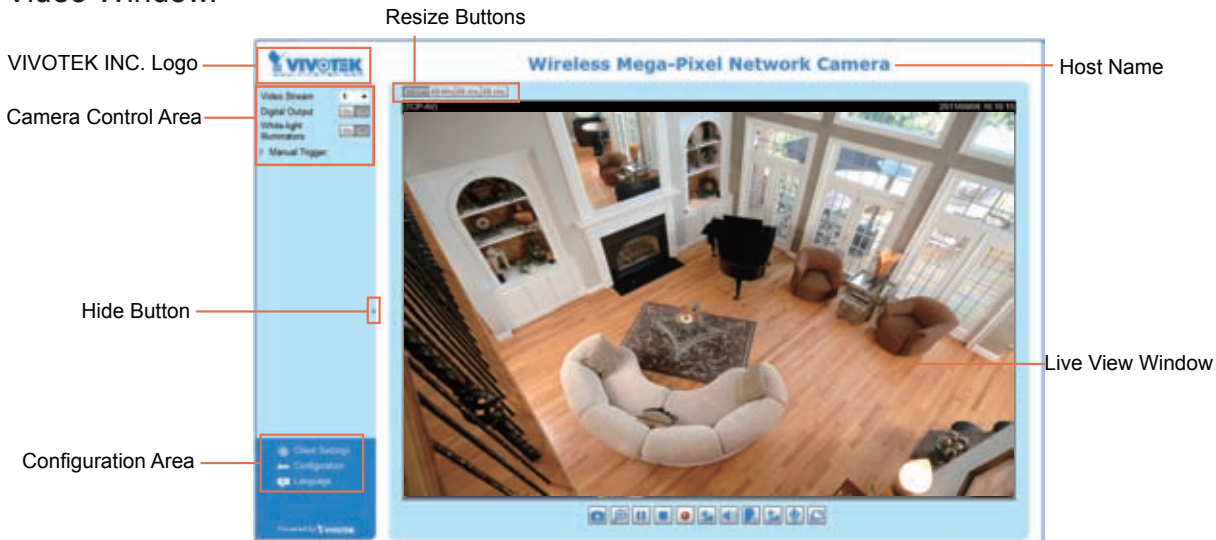
Using VIVOTEK Recording Software

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



Main Page

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



VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

Host Name

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

Camera Control Area

Video Stream: This Network Camera supports multiple streams (streams 1 to 3) simultaneously. You can select any one for live viewing. For more information about multiple streams, please refer to page 69 for detailed information.

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

White-light Illuminator: Click to turn on the white LED (available on IP8133 and IP8133W). The LED also turns on when triggered by the occurrence of an event. Please refer to page 85 for more information. Light adjustment setting is found on page 27.

Manual Trigger: Click to enable/disable an event trigger manually. Please configure an event setting on Application page before enable this function. A total of 3 event settings can be configured. For more information about event settings, please refer to page 82.
If you want to hide this item on the homepage, please go to the Homepage Layout page to uncheck "show manual trigger button". Please refer to page 78 for detailed illustration.

Configuration Area

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

Configuration: Click this button to access the configuration page of the Network Camera. It is suggested that a password be applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 24.

Language: Click this button to choose a language for the user interface. Language options are available

in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡體中文, and 繁體中文.

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.

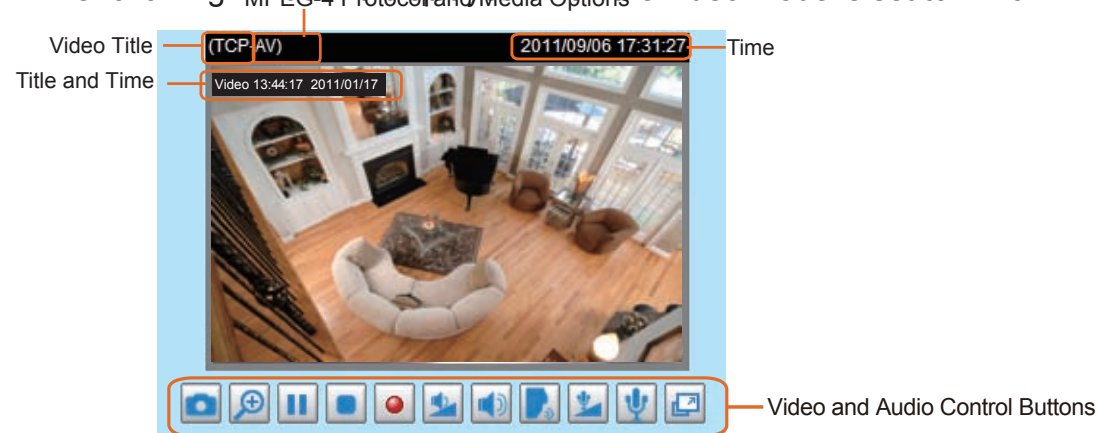
Click 100% is to display the original homepage size.

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:




Video Title: The video title can be configured. For more information, please refer to Video Settings on page 64.


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 22.

Time: Display the current time. For further configuration, please refer to Video Settings on page 64.



Title and Time: The video title and time can be stamped on the streaming video. For further configuration, please refer to Video Settings on page 64.



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







 **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 23 for details.


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

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

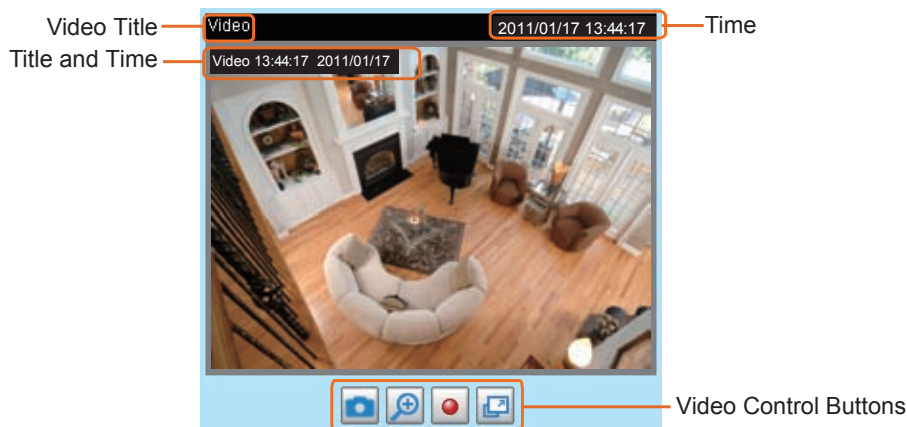
 **Talk:** Click this button to talk to people around the Network Camera. Audio will project from the embedded/external speaker connected to the Network Camera. Click this button  again to end conversation.

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

 **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 is user-configurable. For more information, please refer to Video Settings on page 64.


Time: Display the current time. For more information, please refer to Video Settings on page 64.

Title and Time: Video title and time can be stamped on the streaming video. For more information, please refer to Video Settings on page 64.



Video Control Buttons: Depending on the Network Camera model and Network Camera configuration,


some buttons may not be available.

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

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



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

 **Full Screen:** Click this button to switch to full screen mode. Press 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 transmission modes of H.264 or MPEG-4 streaming:

UDP unicast: This protocol allows for more real-time 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 47.

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

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

MP4 Saving Options

MP4 Saving Options

Folder:

File name prefix:

Add date and time suffix to file name

Users can record 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

Millisecond

Due to the unsteady bandwidth flow, the live streaming may lag and not be very smoothly. If you enable this option, the live streaming will be stored on the camera's buffer area for a few seconds before playing on the live viewing window. This will help you see the streaming more smoothly. If you enter 3000 Millisecond, the streaming will delay 3 seconds.

Configuration

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

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

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

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

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

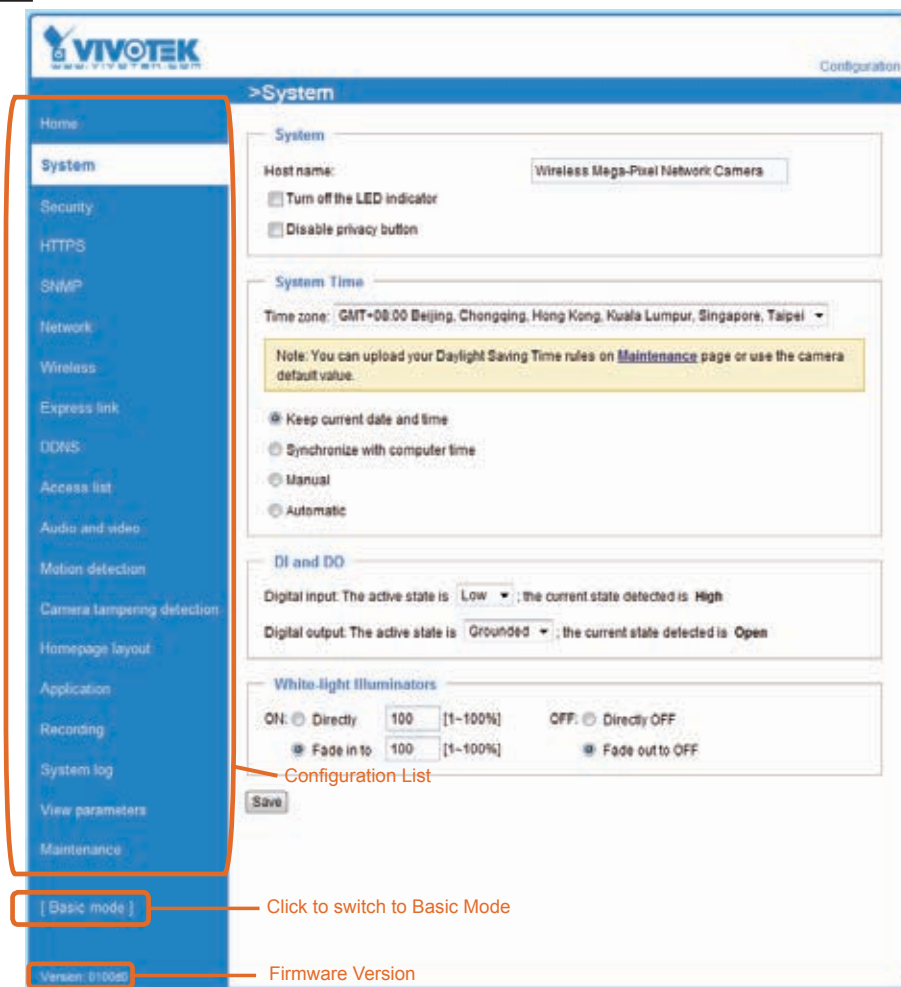
Basic Mode

The screenshot displays the VIVOTEK configuration interface in Basic Mode. The sidebar on the left contains a menu with the following items: Home, System, Security, Network, Wireless, Express link, DDNS, Audio and video, Motion detection, Camera tampering detection, and Maintenance. The 'System' menu item is selected. The main content area is titled '>System' and includes the following sections:

- System**: Host name: Wireless Mega-Pixel Network Camera; Turn off the LED indicator (checkbox); Disable privacy button (checkbox).
- Configuration List**: System Time: Keep current date and time (selected), Synchronize with computer time, Manual, Automatic.
- DI and DO**: Digital input: The active state is Low; the current state detected is High; Digital output: The active state is Grounded; the current state detected is Open.
- White-light Illuminators**: ON: Directly (radio), 100 [1~100%]; Fade in to (selected), 100 [1~100%]; OFF: Directly OFF (radio), Fade out to OFF (radio).

A '[Advanced mode]' link is located at the bottom of the sidebar. A 'Save' button is at the bottom of the main content area. The firmware version is displayed as 'Version: 0100d0' at the bottom left.

Advanced Mode



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

System

This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following three columns: System, System Time, and DI and DO. When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

System

System

Host name:

Turn off the LED indicator

Disable privacy button

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

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

Disable Privacy Button: The privacy button is on the rear panel of the camera. You are able to manually stop the operation of video monitoring for privacy concern by pushing the button. Later on, you can push the button again to resend the video. If you want to disable the function of privacy button, please select this item.

System Time

System Time

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

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

Keep current date and time

Synchronize with computer time

Manual

Automatic

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

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

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

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

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

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

Time zone Advanced Mode: Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules on the Maintenance page, please refer to Upload / Export Daylight Saving Time Configuration File on page 104 for details.

DI and DO

DI and DO

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

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

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

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.

White-light Illuminators

White-light Illuminators

ON: Directly [1~100%] OFF: Directly OFF

Fade in to [1~100%] Fade out to OFF

ON: The white-light LED allows you to illuminate the monitored area when an event occurs. You can select to turn on the LED directly to a configurable brightness level or gradually light up to that level. You can manually enter a percentage number in the text fields. The white-light LED can be manually lit using a button on the home page or passively triggered by a camera event.

OFF: Select to turn off the LED directly or let the light gradually fade out.

Security

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

Root Password

Root Password

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

Root Password:

Confirm root password:

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

1. 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: | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| White-light Illuminators: | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Allow anonymous viewing | | |

Digital Output: You can modify the manage privilege of operators or viewers. Check or uncheck the item, then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Main Page on page 24.)

White-light Illuminators: Determines if an operator or viewer can control the white LED.

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

Manage User

Manage User

Existing user name:

User name:

User password:

Confirm user password:

Privilege:

Administrator
 Operator
 Viewer

Administrators can add up to 20 user accounts.

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

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. 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 107. Viewers access only the main page for live viewing.

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

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

HTTPS (Hypertext Transfer Protocol over SSL) Advanced Mode

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

Enable HTTPS

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

Enable HTTPS

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

Enable HTTPS secure connection:

HTTP & HTTPS
 HTTPS only

Save

Create and install certificate method

Create self-signed certificate automatically

Create self-signed certificate manually:

Create certificate request and install:

Create and Install Certificate Method

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

Create self-signed certificate automatically

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

Enable HTTPS

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

Enable HTTPS secure connection:

HTTP & HTTPS
 HTTPS only

Save

Create and install certificate method

Create self-signed certificate automatically

Create self-signed certificate manually:

Create certificate request and install:

Certificate Information

Status: Not installed

Please wait while the certificate is being generated...

Progress bar

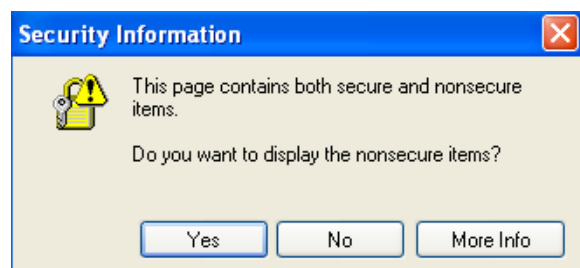
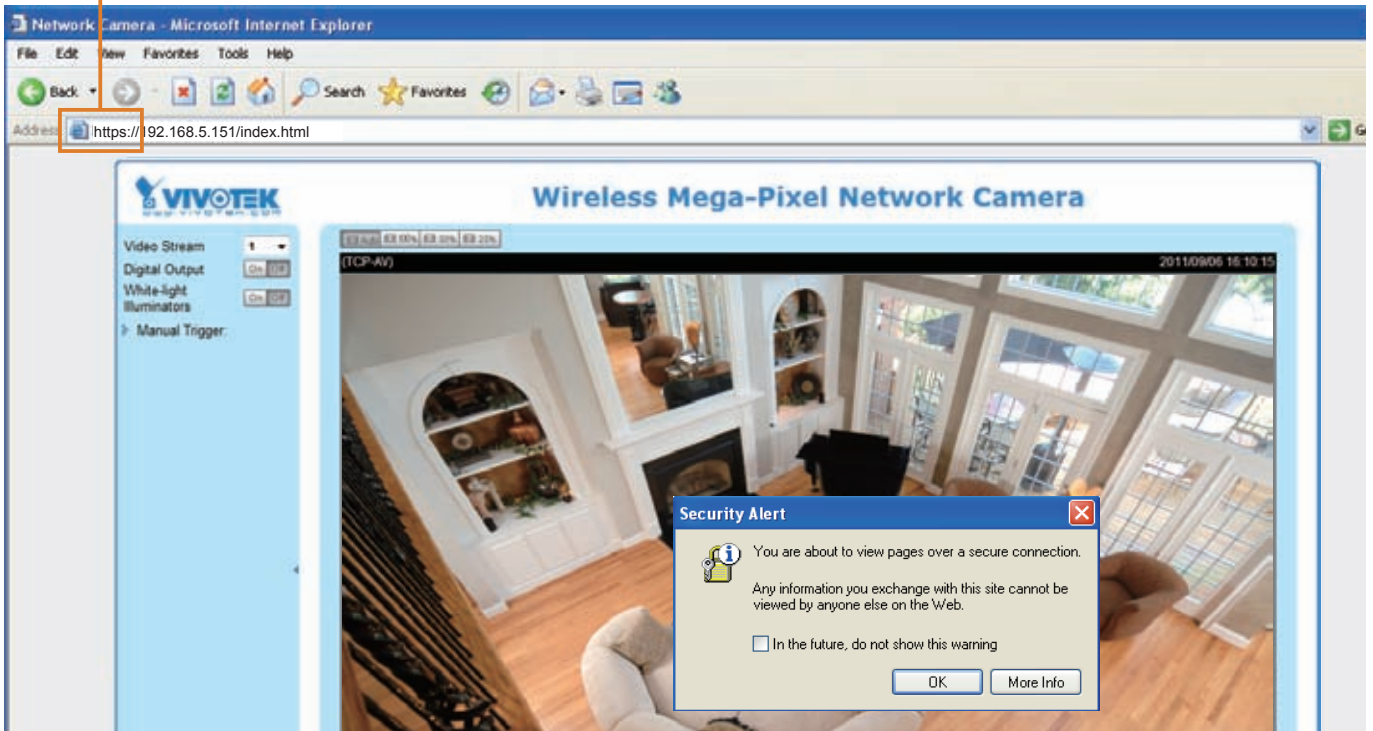
- The Certificate Information will automatically be displayed in the third column as shown below. You can click **Property** to view detailed information about the certificate.

Certificate Information

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

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

https://



Create self-signed certificate manually

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

Create Certificate

Country:

State or province:

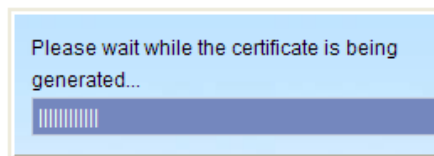
Locality:

Organization:

Organization Unit:

Common Name:

Validity: days



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

Certificate Information

Status:

Country: TW

State or province: Asia

Locality: Asia

Organization: Vivotek.Inc

Organization Unit: Vivotek.Inc

Common Name: www.vivotek.com

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

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

Create and install certificate method

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

Create Certificate

Country:

State or province:

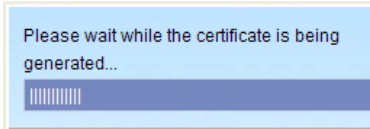
Locality:

Organization:

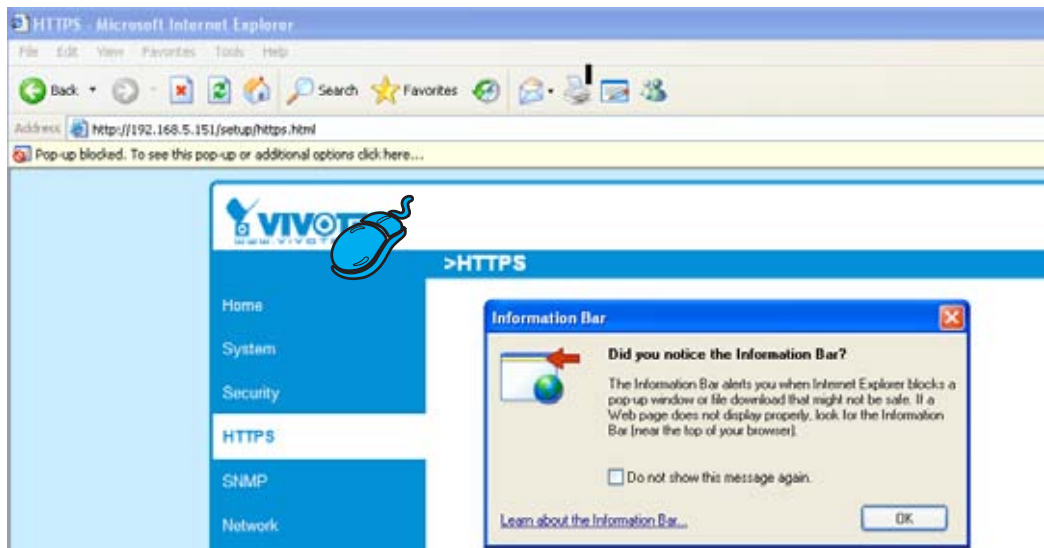
Organization Unit:

Common Name:

Validity: days



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



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

Create Certificate Request Completed

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

Certificate Request (PEM format)

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBuDCCASECADB5MQswCQYDVQQGEwJUVzERM&8GA1UECBMIUHJvdmluY2UxEjAQ
BgNVBAsTCUNpdHkgTmFtZTEaMBGGA1UEChMRMT3JnYW5pemFoaW9uIE5hbWUxEjAQ
BgNVBAsTCVVueXQgTmFtZTEaMBGGA1UEAxMKSVAgQWRkcmVzcCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwgYkCgYEAuOT75EY52gsSyPFMxZ7wHdQ1obPescsXLUx9DFw6
OMRheukFaXFDkM+5xk+K5oEPBPqj77yhH+zdUHS27fFSLG57bW9S0xrWuLhSvRZW
mCD+//AiJX864dJ/mjHn7Wc55GFaxgMvbALcxT+hCIeDCWYnRqh/fpRNj+BxvVoN
UrcCAwEAaAAAMADGCSqGSIB3DQEBBQUAA4GBAAVazWOAtftE9dyFgTxOY01D/zO
FOTkbnDQQG18e4ftJ3rROD1TvIIMjg3K8zsAS8Gd3pME1ejqLYoBrtaSqdCuqGiX
5ObLGLsubWsXr88PngaBwjYoTpG3q1zvUPJZL&VmdL3ne5urTb&BXOScCHOQGtH+
PX9dw4OJWkIC8QhV
-----END CERTIFICATE REQUEST-----
    
```

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

certificate, then click Upload in the second column.

Create and install certificate method

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

Certificate request:

Select certificate file:

Certificate Information

Status:



NOTE:

► How do I cancel the HTTPS settings?

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

Enable HTTPS

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

Enable HTTPS secure connection:

Create and install certificate method

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

Microsoft Internet Explorer

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

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

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

Certificate Information

Status:

Country:

State or province:

Locality:

Organization:

Organization Unit:

Common Name:

Microsoft Internet Explorer

? Are you sure you want to delete the certificate?

SNMP (Simple Network Management Protocol) Advanced Mode

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

■ The SNMP consists of the following three key components:

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

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

SNMP Configuration

Enable SNMPv1, SNMPv2c

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

Enable SNMPv1, SNMPv2c

SNMPv1, SNMPv2c Settings

Read/Write community:

Read only community:

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:

Authentication Type:

Authentication Password:

Encryption Password:

Read only Security name:

Authentication Type:

Authentication Password:

Encryption Password:

Network

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

Network Type

The screenshot shows the 'Network Type' configuration window. The 'LAN' option is selected with a radio button. Under 'LAN', 'Get IP address automatically' is selected with a radio button, 'Use fixed IP address:' is unselected, 'Enable UPnP presentation' is checked with a checkbox, and 'Enable UPnP port forwarding' is unselected. Below the 'LAN' section, 'PPPoE:' is unselected and 'Enable IPv6' is unselected. A 'Save' button is located at the bottom left of the window.

LAN

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

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

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

The screenshot shows the 'Network Type' configuration window with 'Use fixed IP address:' selected. The 'IP address:' field contains '192.168.5.109', 'Subnet mask:' contains '255.255.255.0', 'Default router:' contains '192.168.5.1', 'Primary DNS:' contains '192.168.0.10', and 'Secondary DNS:' contains '192.168.0.20'. The 'Primary WINS server:' and 'Secondary WINS server:' fields are empty. 'Enable UPnP presentation' is checked, and 'Enable UPnP port forwarding' is unselected. 'PPPoE:' and 'Enable IPv6' are unselected. A 'Save' button is at the bottom left.

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

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

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

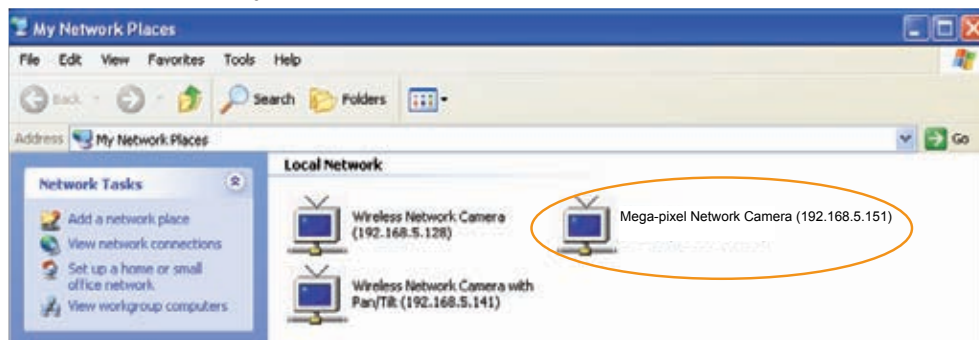
Primary DNS: The primary domain name server that translates hostnames into IP addresses.

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

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

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

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



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

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.

1. Set up the Network Camera on the LAN.
2. Go to Home > Configuration > Application > Server Settings (please refer to Server Settings on page 88) to add a new email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 91). Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > Network Type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.

Network Type

LAN:

PPPoE:

User name:

Password:

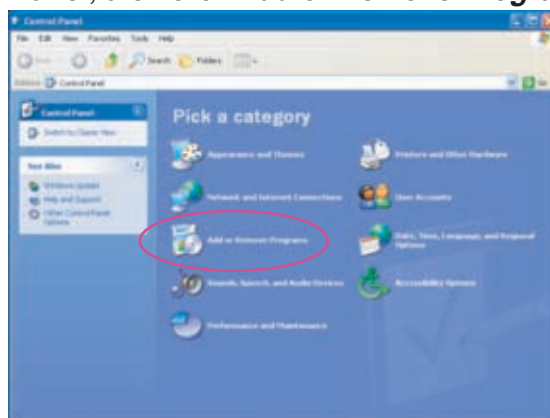
Confirm password:

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

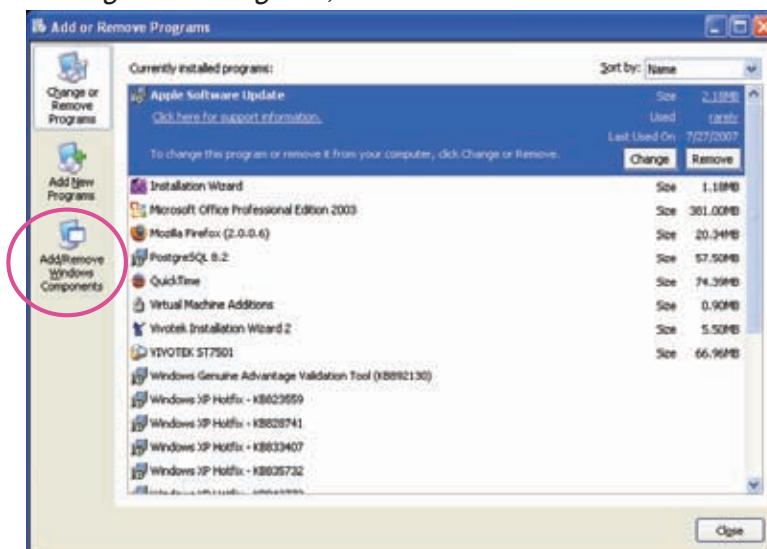
 **NOTE:**

- ▶ If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.
- ▶ If UPnP™ is not supported by your router, you will see the following message:
Error: Router does not support UPnP port forwarding.
- ▶ Steps to enable the UPnP™ user interface on your computer:
Note that you must log on to the computer as a system administrator to install the UPnP™ components.

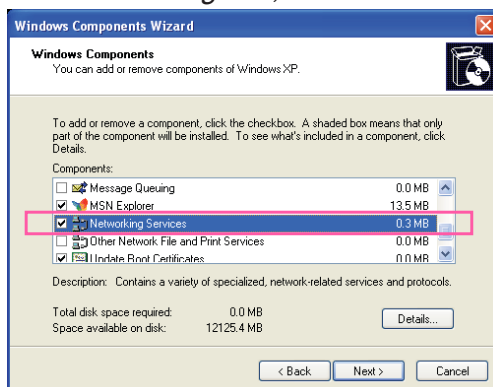
1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.



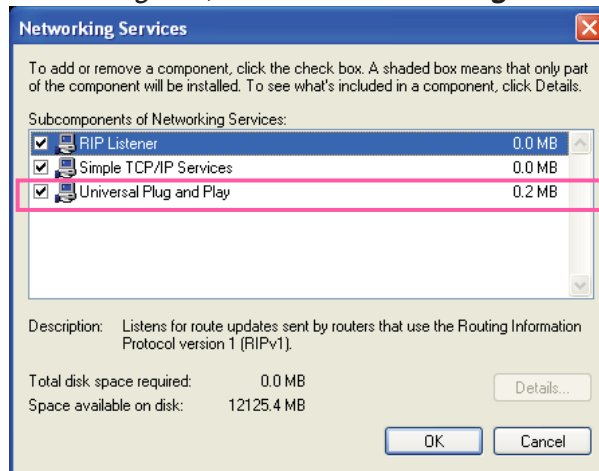
2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.



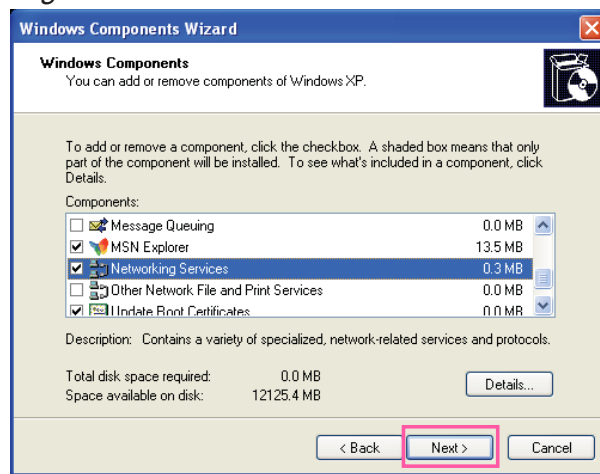
3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.



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



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



6. Click **Finish**. UPnP™ is enabled.

► **How does UPnP™ work?**

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

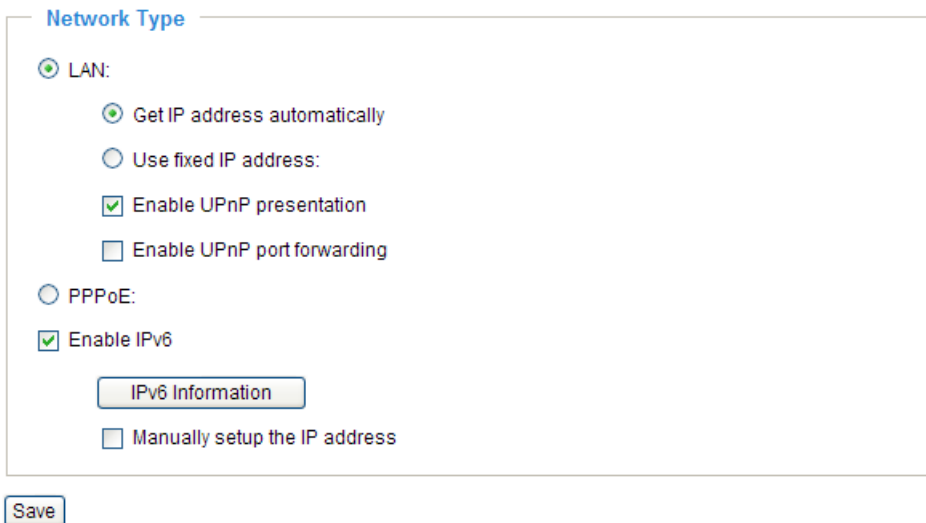
► **Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP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

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

► **If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 103 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.**

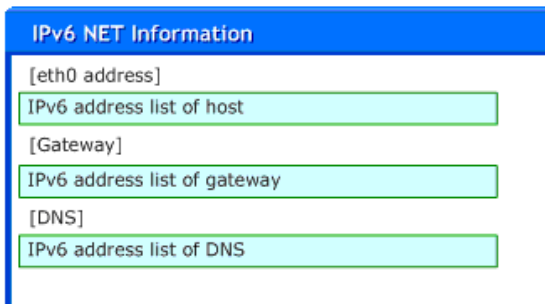
Enable IPv6

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.



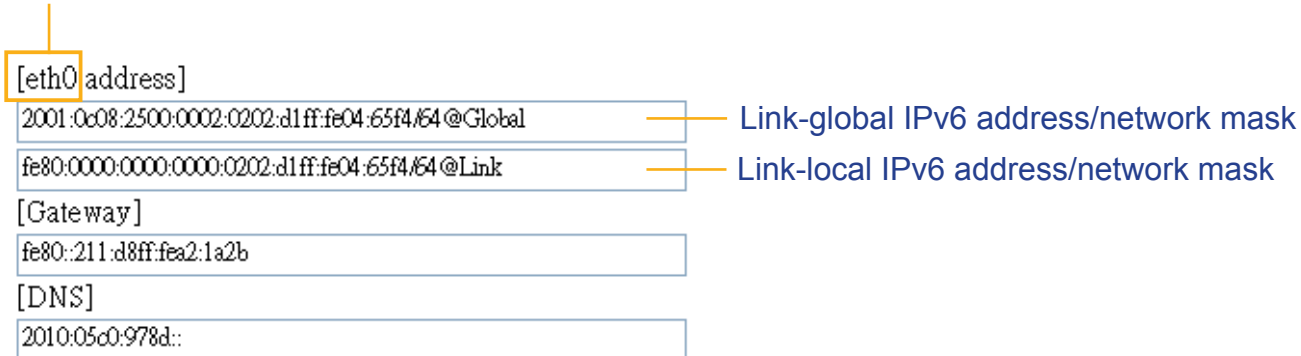
When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

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



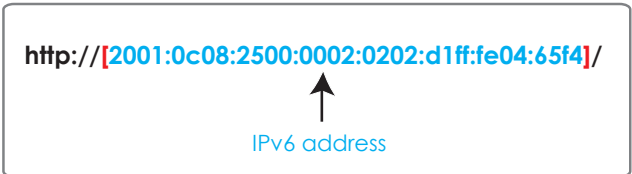
If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window. The IPv6 address will be displayed as follows:

Refers to Ethernet

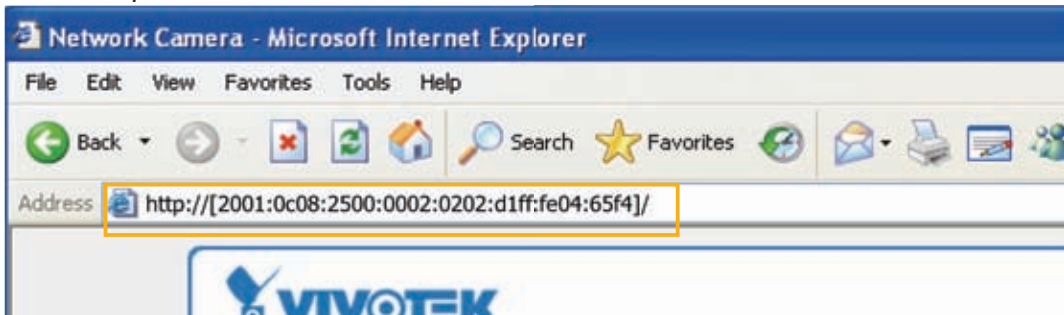


Please follow the steps below to link to an IPv6 address:

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



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



NOTE:

- ▶ If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to **HTTP** on page 45 for detailed information.)



- ▶ If you choose PPPoE as the Network Type, the [PPPoE 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 advertisements-enabled routers.

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

Enable IPv6

IPv6 Information

Manually setup the IP address

Optional IP address / Prefix length / 64

Optional default router

Optional primary DNS

IEEE 802.1x **Advanced Mode**

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

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

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



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

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

Please follow the steps below to enable 802.1x settings:

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

IEEE 802.1x

Enable IEEE 802.1x

EAP method: EAP-PEAP ▼

Identity:

Password:

CA certificate:

Status: no file

IEEE 802.1x

Enable 802.1x

EAP method: EAP-TLS ▾

Identity:

Private key password:

CA certificate: Browse... Upload

Status: no file Remove


client certificate: Browse... Upload

Status: no file Remove

Client private key: Browse... Upload

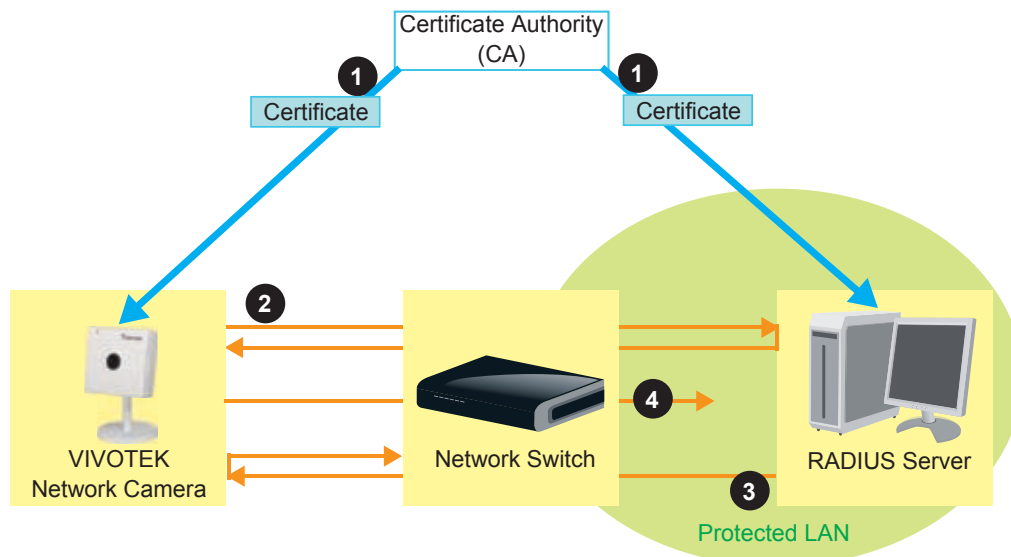
Status: no file Remove

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

 **NOTE:**

► *The authentication process for 802.1x:*

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



QoS (Quality of Service) Advanced Mode

Quality of Service refers to a resource reservation control mechanism, which guarantees a certain quality to different services (voice, data, video, etc) 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: | <input style="width: 60px;" type="text" value="1"/> |
| Live video: | <input style="width: 40px;" type="text" value="0"/> ▼ |
| Live audio: | <input style="width: 40px;" type="text" value="0"/> ▼ |
| Event/Alarm: | <input style="width: 40px;" type="text" value="0"/> ▼ |
| Management: | <input style="width: 40px;" type="text" value="0"/> ▼ |

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



NOTE:

- ▶ *The VLAN Switch (802.1p) is required. The 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.*
- ▶ *Though CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.*

QoS/DSCP (the DiffServ model)

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

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

QoS/DSCP

Enable QoS/DSCP

| | |
|--------------|--------------------------------|
| Live video: | <input type="text" value="0"/> |
| Live audio: | <input type="text" value="0"/> |
| Event/Alarm: | <input type="text" value="0"/> |
| Management: | <input type="text" value="0"/> |

HTTP **Advanced Mode**

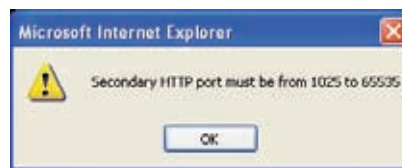
To utilize HTTP authentication, make sure that you have already set a password for the Network Camera first; please refer to Security on page 28 for details.

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

Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest.

If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. They can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages will be displayed:



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

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

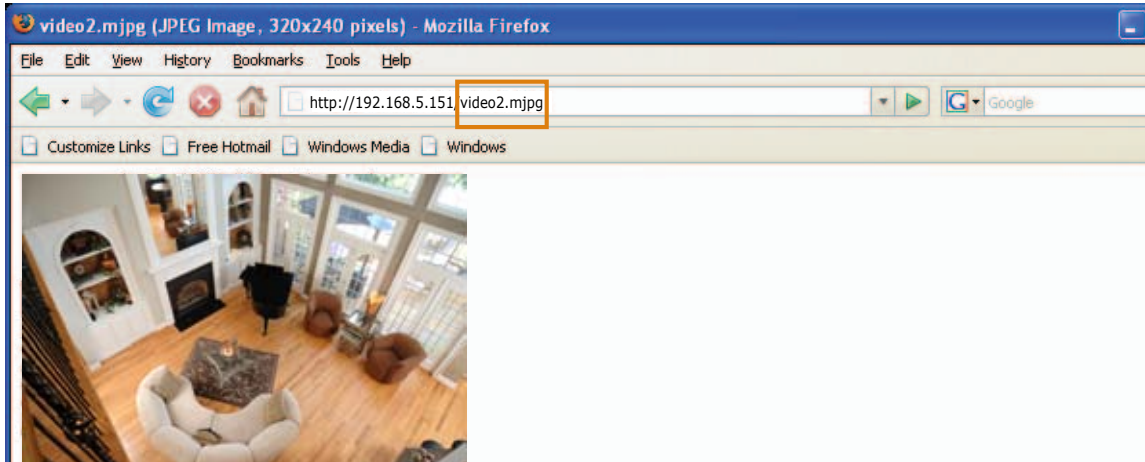
Access name for stream 1 ~ 3: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. Users can click **Configuration > Audio and video > Video Settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Viewing Windows on page 69.

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 ~ 3>>

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.



NOTE:

- ▶ Microsoft® Internet Explorer does not support server push technology; therefore, access to the camera will fail using <http://<ip address>:<http port>/<access name for stream 1 ~ 3>>.

HTTPS

HTTPS

HTTPS port:

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

FTP

FTP

FTP port:

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

RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for the Network Camera first; please refer to Security on page 28 for details.

RTSP Streaming

Authentication:

Access name for stream 1:

Access name for stream 2:

Access name for stream 3:

RTSP port:

RTP port for video:

RTCP port for video:

RTP port for audio:

RTCP port for audio:

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 |

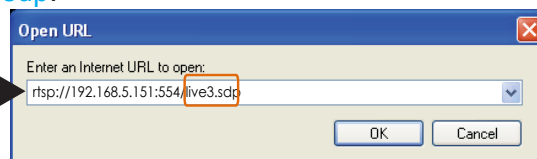
Access name for stream 1 ~ 3: This Network Camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.

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

rtsp://<ip address>:<rtsp port>/<access name for stream1 ~ 3>

For example, when the access name for **stream 3** is set to **live.sdp**:

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

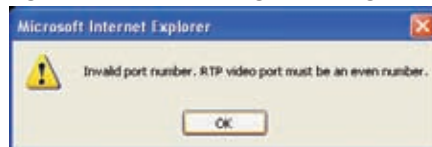


RTSP port /RTP port for video/ RTCP port for video

- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.
- The RTP (Real-time Transport Protocol) is used to deliver video data to the clients. By default, the RTP port for video is set to 5556.
- The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557.

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

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



Multicast settings for stream 1 ~ 3: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1 ~ 3.

▼ 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 3:

Always multicast

Multicast group address: 239.128.1.101

Multicast video port: 5568

Multicast RTCP video port: 5569

Multicast audio port: 5570

Multicast RTCP audio port: 5571

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 bandwidth.

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and 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:



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

Wireless (IP8133W)

Manual Configuration:

Setting up wireless cameras' connections can be tricky. The configuration process involves hardwire connection to your LAN for initial setup and wireless connection to AP. To switch between the connection types, you have to physically disconnect the 5V DC connector. For example, when you are finished with initial setup via LAN, you have to remove the RJ-45 LAN cable and disconnect the DC power jack, and then reconnect the power.

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

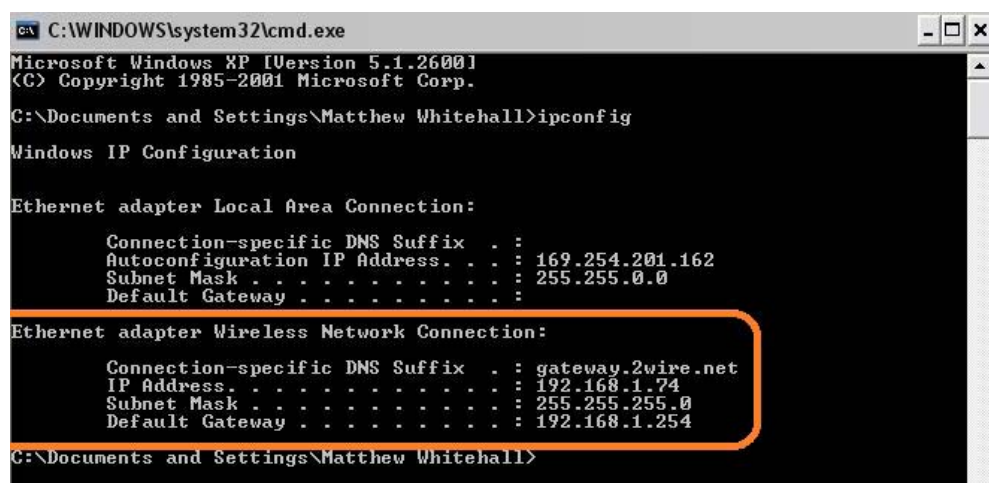
To set up a wireless connection with the camera,

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

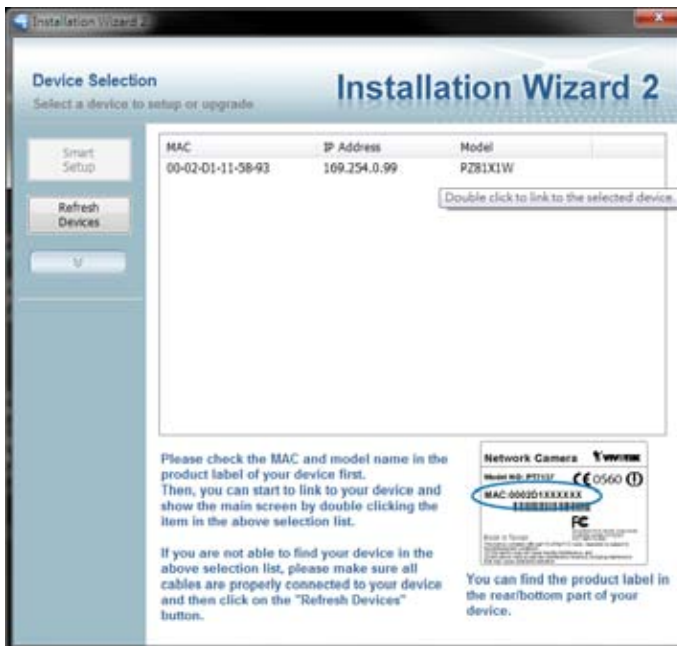


For connection using the wireless Ad-hoc mode, please refer to page 58.

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



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



- Enter the **Configuration > Wireless** menu, and enter the name (**SSID**) of the existing wireless network, channel number, and other related information. See the following pages for more details. You may enter the **Configuration > Network** page to setup a DHCP or a static IP.
- You may then use the ping command to detect if your camera is switching from “wired” connection to “wireless” connection. Open a command prompt window (or click on Windows Start menu, type “cmd” in the Run command field). Ping the camera’s LAN port IP address (use the <ping xxx.xxx.xx.xx -t> argument in the command).

Watch closely when the pinging process displays “Request timed out.” That means the wireless connection is taking over. Unplug your LAN cable immediately.

```

C:\WINDOWS\system32\cmd.exe - ping 192.168.14.86 -t
Microsoft Windows XP [版本 5.1.2600.1
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\liya.liu>ping 192.168.14.86 -t

Pinging 192.168.14.86 with 32 bytes of data:

Reply from 192.168.14.86: bytes=32 time<1ms TTL=64
Reply from 192.168.14.86: bytes=32 time<1ms TTL=64
Reply from 192.168.14.86: bytes=32 time<1ms TTL=64
Reply from 192.168.14.86: bytes=32 time<1ms TTL=64
Reply from 192.168.14.86: bytes=32 time<1ms TTL=64
Reply from 192.168.14.86: bytes=32 time<1ms TTL=64
Reply from 192.168.14.86: bytes=32 time<1ms TTL=64
Reply from 192.168.14.86: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Request timed out.

```

6. The camera will automatically reset itself. You can then access the camera via a wireless connection.

WLAN configuration

| | |
|---------------|----------------|
| SSID | default |
| Wireless mode | infrastructure |
| Channel | 6 |
| TX rate | Auto |
| Security | None |

Save

Below are more information about encryption and other wireless-related settings.

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

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

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

WLAN configuration

| | |
|---------------|---------|
| SSID | default |
| Wireless mode | ad-hoc |
| Channel | 6 |
| TX rate | Auto |
| Security | None |

Save

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

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

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

WLAN configuration

| | |
|---------------|----------------|
| SSID | default |
| Wireless mode | infrastructure |
| Channel | 6 |
| TX rate | Auto |
| Security | None |

Save

None
WEP
WPA-PSK
WPA2-PSK

1. None: No data encryption.

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

WLAN configuration

| | |
|---------------------|---|
| SSID | default |
| Wireless mode | infrastructure |
| Channel | 6 |
| TX rate | Auto |
| Security | WEP |
| Authentication mode | Open |
| Key length | 64 bits |
| Key format | HEX |
| Default key | <input checked="" type="radio"/> Network key <input type="radio"/> <input type="radio"/> <input type="radio"/> |
| | 0000000000 |
| | 0000000000 |
| | 0000000000 |
| | 0000000000 |

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



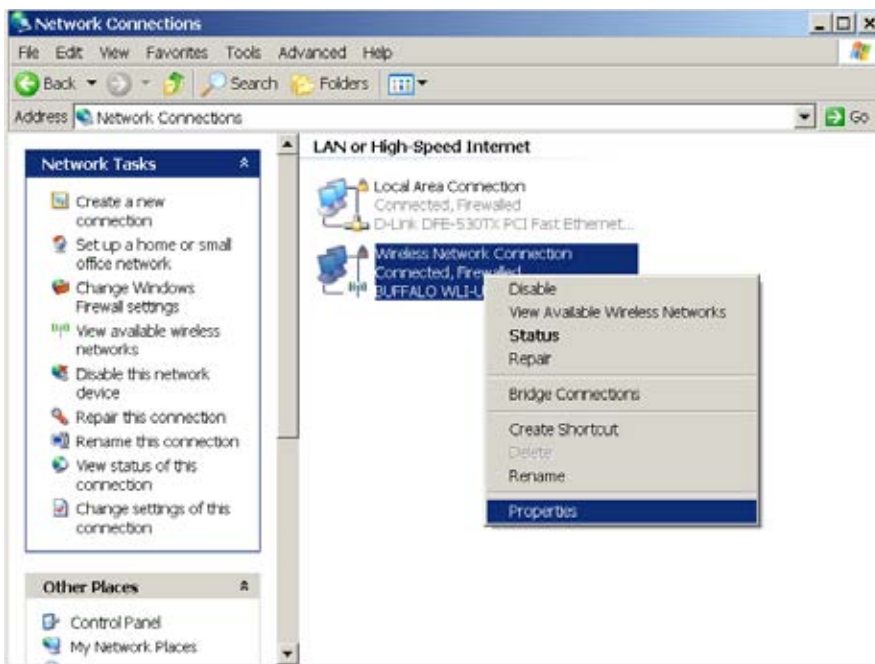
NOTE:

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

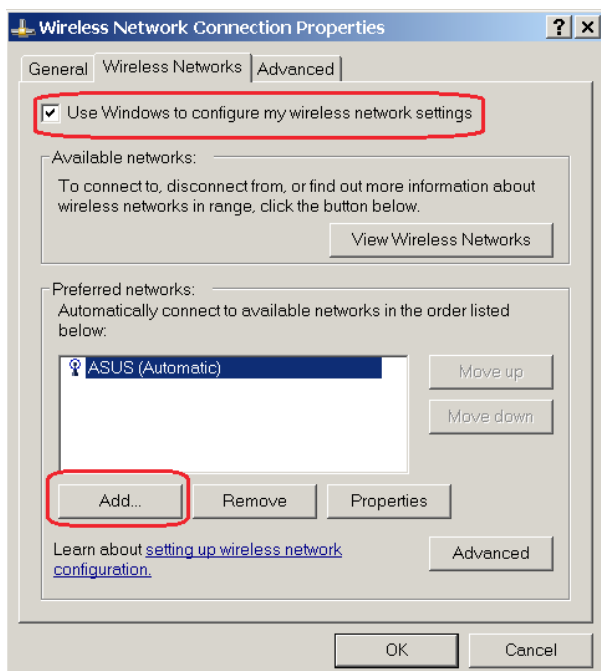
Ad-hoc Connection

To configure your wireless connection in Ad-hoc mode,

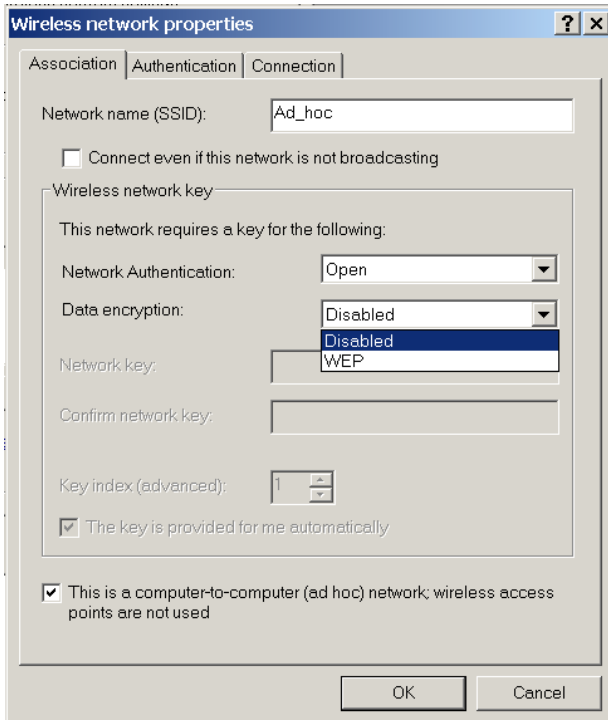
1. Configure a fixed IP for the network camera.
2. Configure wireless connection for the camera in the "Infrastructure" mode as previously described.
3. Return to the Wireless setting page, and change the Wireless mode into "Ad-hoc". Select the encryption mode and a Wireless mode channel.
4. Configure the PC or laptop that is equipped with a wireless adaptor in the following way:
 - 4-1. Enter your Windows Control Panel -> Network and Internet Connections -> Network Connections.
 - 4-2. Select a Wireless Network Connection and right-click on it to select the Properties command.



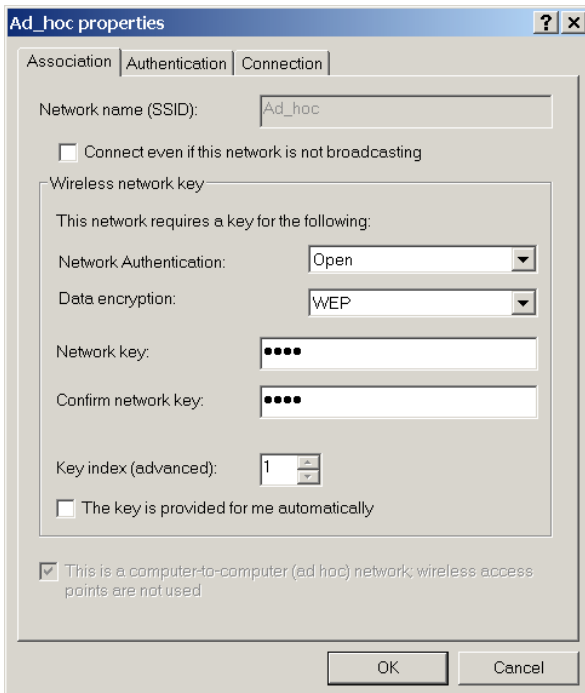
- 4-3. Select "Wireless Networks" from the tabbed menu on the top.



- 4-4. Select the first checkbox: "Use Windows to configure my wireless network settings."
- 4-5. Click Add to create a new wireless connection.
- 4-6. On the Properties window, enter a name for the network and configure the Data encryption option.

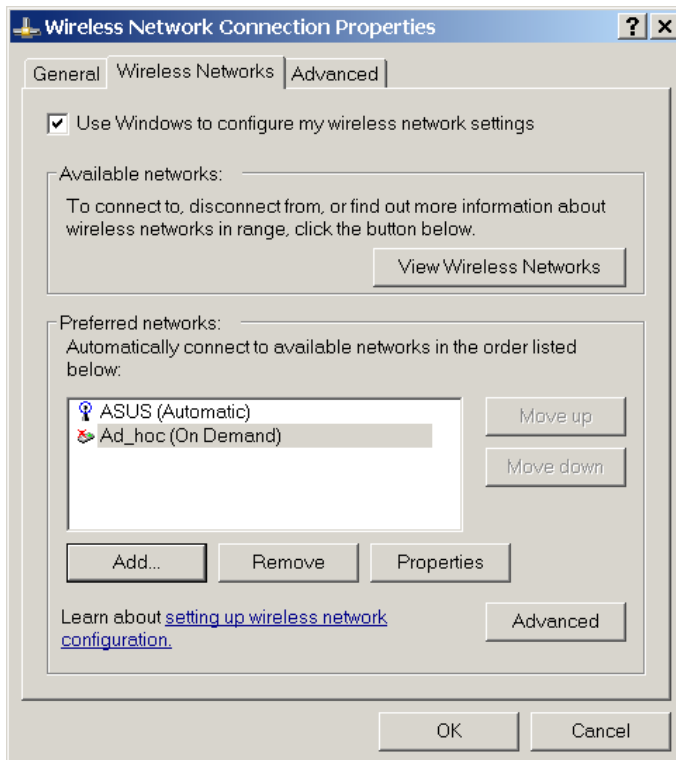


- 4-7. Click to select the ad hoc checkbox at the bottom of this window. You may also configure a WEP network key for secure connection.

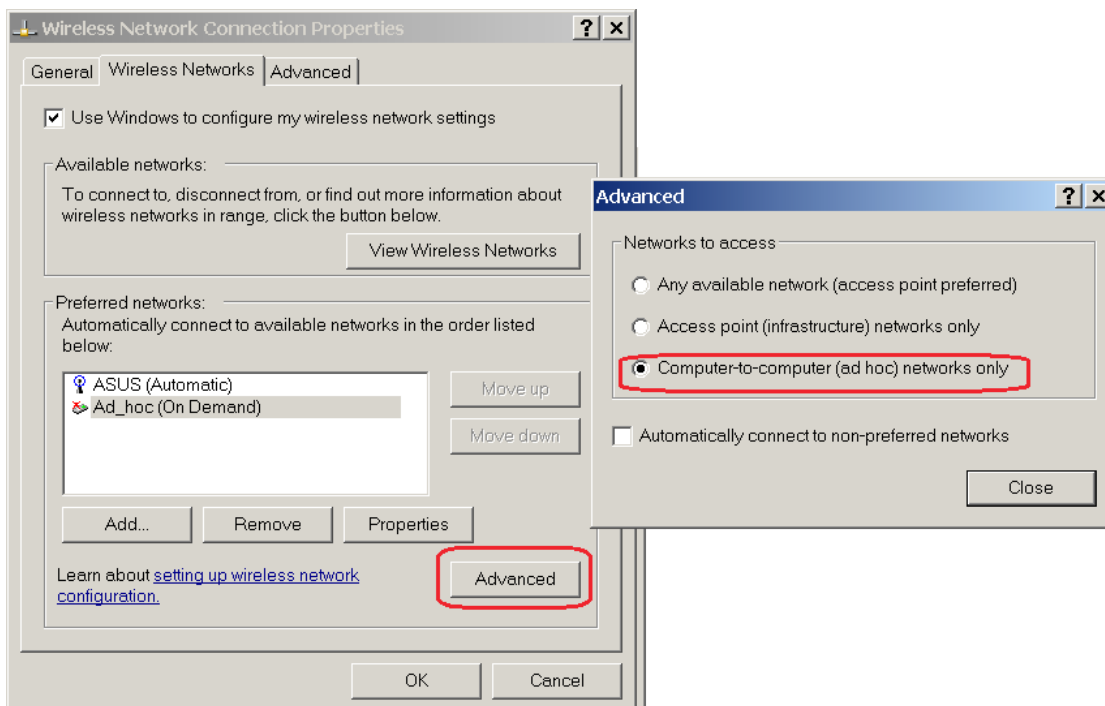


- 4-8. Click OK when the setting is done. You will return to the Properties window.

4-9. Click on the Advanced button.

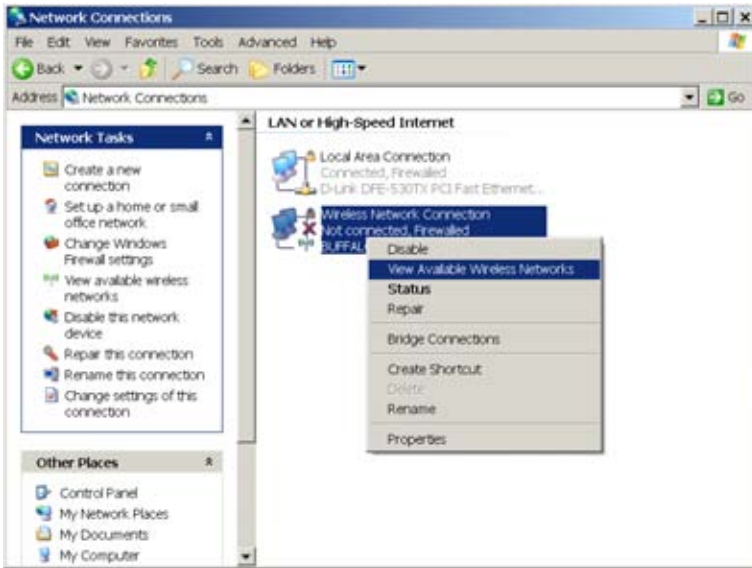


4-10. Select the “Computer-to-computer (ad hoc) networks only” checkbox.

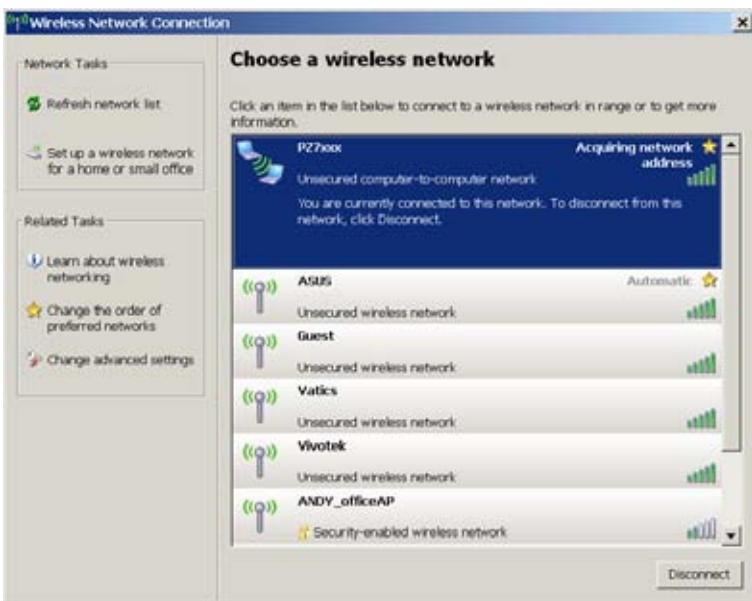


5. Return to the Wireless page and click on the Next button to proceed. Depending on the connection quality of your wireless network, the apply process may take several minutes, and the connection should be available.

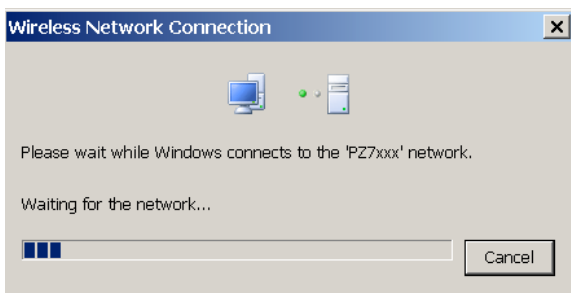
- Return to the Windows Network Connections page, right-click on the Wireless Network Connection icon and select the "View Available Wireless Networks" command.



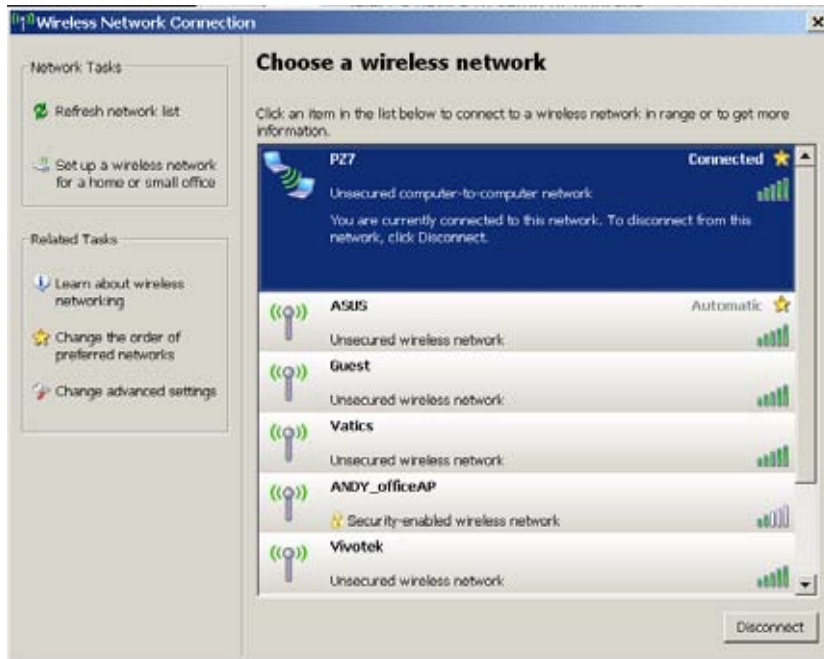
- Your wireless camera's SSID should appear on the list of Wireless Networks. Left-click to select and click on the Connect button at the lower right to proceed.



- Windows will start connecting to your network camera.



9. Wait for the connection to be established. The process can take several minutes. When done, the connection status should be stated as Connected.



10. Open a command prompt window. Ping the camera's IP to ensure the connection is up and running.

```
Command Prompt (2) - ping 192.168.4.131 -t
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\XPMUser>ping 192.168.4.131 -t
Pinging 192.168.4.131 with 32 bytes of data:
Reply from 192.168.4.131: bytes=32 time=1ms TTL=128
Reply from 192.168.4.131: bytes=32 time=1ms TTL=128
Reply from 192.168.4.131: bytes=32 time=1ms TTL=128
Reply from 192.168.4.131: bytes=32 time=10ms TTL=128
Reply from 192.168.4.131: bytes=32 time=2ms TTL=128
Reply from 192.168.4.131: bytes=32 time=1ms TTL=128
Reply from 192.168.4.131: bytes=32 time=1ms TTL=128
Reply from 192.168.4.131: bytes=32 time=1ms TTL=128
Reply from 192.168.4.131: bytes=32 time=8ms TTL=128
Reply from 192.168.4.131: bytes=32 time=1ms TTL=128
Reply from 192.168.4.131: bytes=32 time=7ms TTL=128
Reply from 192.168.4.131: bytes=32 time=1ms TTL=128
```

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, the user has to manually check out UPnP port forwarding, Express Link is more convenient and easy to set up.

Host Name Assignment

Host Name Assignment

Connect to the camera at http:// .2bthere.net

HINT: Input a host name and click "Register" to test and register.

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 this network environment.
2. Enter a host name for the network device and click **Register**. 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.

Host Name Assignment

Connect to the camera at http:// .2bthere.net

HINT: This is a valid host name. Click "Enable" to assign http://mycamera.2bthere.net to this camera.

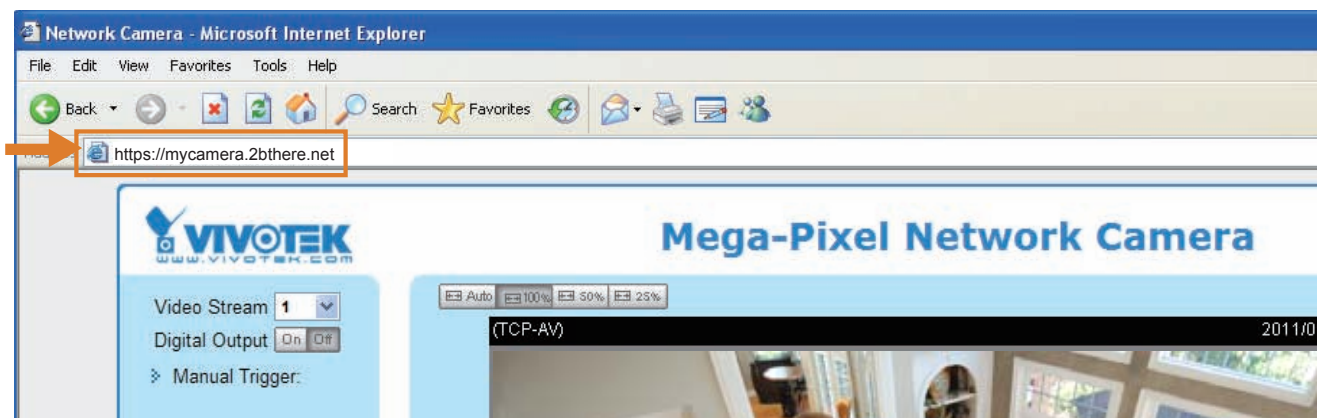
3. Click **Enable** to activate the URL.

Host Name Assignment

Connect to the camera at http:// .2bthere.net

You can now connect to this camera at http://mycamera.2bthere.net.

HINT: If you click "Disable" to suspend Express Link, you will not be able to access this camera at http://mycamera.2bthere.net.



DDNS

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

DDNS: Dynamic domain name service

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

Provider: Select a DDNS provider from the provider drop-down list.

VIVOTEK offers [Safe100.net](#), a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register [Safe100.net](#) to access VIVOTEK's Network Cameras from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it.

Note that before utilizing this function, please apply for a dynamic domain account first.

■ [Safe100.net](#)

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

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

DDNS: Dynamic domain name service

Enable DDNS:

Provider:

Host name: [*.safe100.net]

Email:

Key:

Register

Host name:

Email:

Key:

Confirm key:

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

DDNS Registration Result:

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

4. Select Enable DDNS and click **Save** to enable the setting.

■ CustomSafe100

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

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

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

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

- [Dyndns.org\(Dynamic\) / Dyndns.org\(Custom\)](http://www.dyndns.com/): visit <http://www.dyndns.com/>
- [TZO.com](http://www.tzo.com/): visit <http://www.tzo.com/>
- [DHS.org](http://www.dns.org/): visit <http://www.dns.org/>
- dyn-interfree.it: visit <http://dyn-interfree.it/>

Access List Advanced Mode

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

General Settings

General Settings

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

Enable access list filtering

Save

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

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

For example:

Connection status

| | IP address | Elapsed time | User ID |
|--------------------------|---------------|--------------|---------|
| <input type="checkbox"/> | 192.168.1.147 | 12:20:34 | root |
| <input type="checkbox"/> | 61.22.15.3 | 00:10:09 | |
| <input type="checkbox"/> | 192.168.3.25 | 45:00:34 | greg |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Refresh
Add to deny list
Disconnect

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

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

1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security on page 28.
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 47.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing**, please refer to Security on page 28.

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

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

Filter Type

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

Filter

Then you can add a rule to the following Access List. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to page 39 for detailed information.

Filter

IPv4 access list

Add
Delete

IPv6 access list

Add
Delete

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: 192.168.2.1

OK
Cancel

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

filter address

Rule: **Network** ▼

Network address / Network mask /

IP address 192.168.2.x will be blocked.

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

filter address

Rule: **Range** ▼

IP address - IP address -

Administrator IP address

Always allow the IP address to access this device: You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.

Administrator IP address

Always allow the IP address to access this device

Audio and Video

This section explains how to configure the Audio and Video settings of the Network Camera.

Video Settings

Video Settings

Video title:

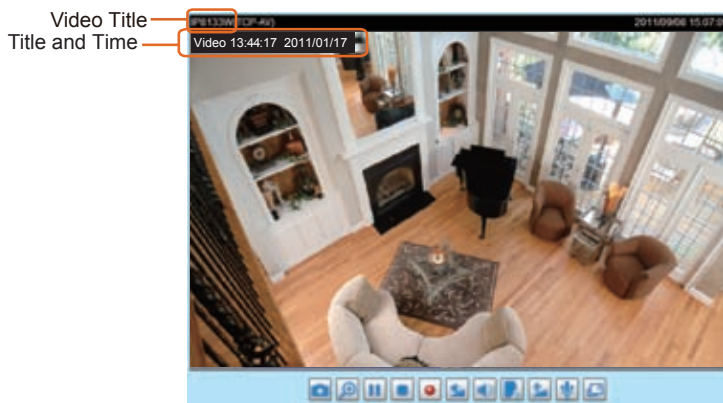
Color: Color ▾

Power line frequency: 60 Hz ▾

Video orientation: Flip Mirror

Overlay title and time stamp on video and snapshot.

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

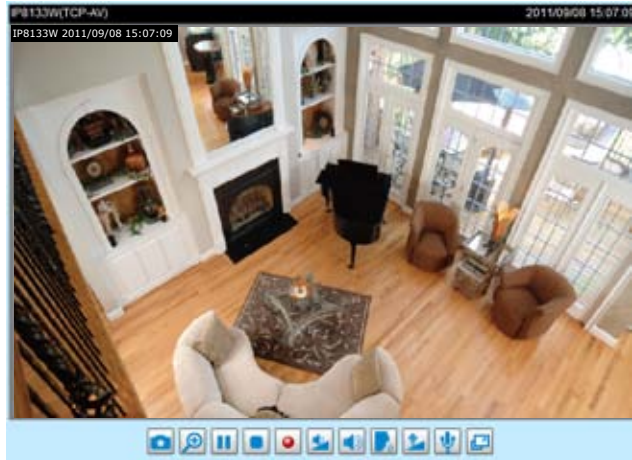


Color: Select to display color or black/white video streams.

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

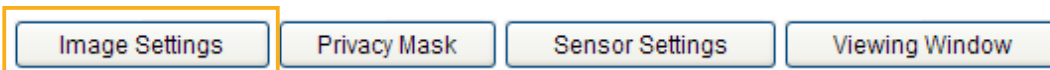
Video orientation: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (ex. on the ceiling) to correct the image orientation. Please note that the preset locations will be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

Overlay title and time stamp on video and snapshot: Select this option to place the video title and time on the video streams and snapshot.
 Note that when the frame size is set to 176 x 144 as shown in the picture below, only the time will be stamped on the video streams.



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

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



White Balance

Auto

Image Adjustment

Brightness: Saturation:

Contrast: Sharpness:

Enable Noise Reduction

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

■ **Auto**

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

■ Keep current value

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

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

Image Adjustment

- Brightness: Adjust the image brightness level, which ranges from -5 to +5.
- Saturation: Adjust the image saturation level, which ranges from -5 to +5.
- Contrast: Adjust the image contrast level, which ranges from -5 to +5.
- Sharpness: Adjust the image sharpness level, which ranges from -3 to +3.

Enable Noise Reduction

Noise reduction is the process of removing noise from a signal. Select reduction for the Gaussian (video amplifier thermal noises often occur in the the dark area of an image) or Impulse (audio clicks and pops due to electromagnetic interference). Select the type of noise to remove or select Both Faussian and Impulse and enter a value from 1 to 63 to set the degree of enhancement required.

Enable Noise Reduction

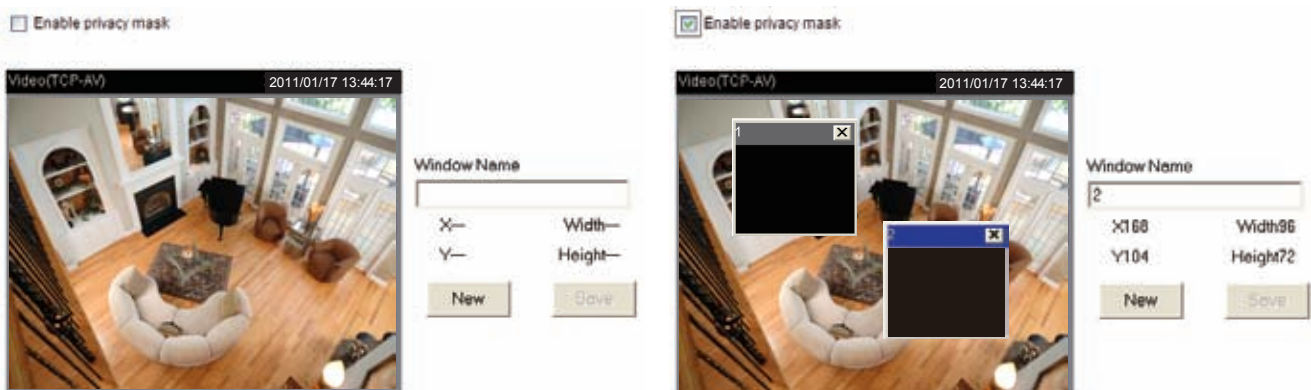
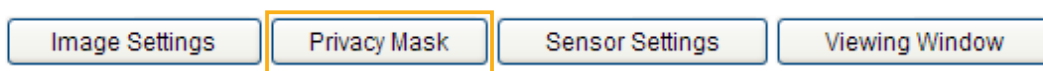
Remove Noise:

Strength: (1~63)

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

Privacy Mask **Advanced Mode**

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



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

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



NOTE:

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

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

Click **Sensor Settings** to open the Sensor Settings page. On this page, you can set the maximum exposure time, exposure level, and AGC (Auto Gain Control) settings.

You can configure two sets of sensor settings: one for normal situations, the other for special situations (schedule mode - for a different period of time with different lighting conditions).



Exposure

| | |
|-------------------------------------|--------|
| Maximum Exposure Time: | 1/30 S |
| Exposure level: | 4 |
| Max gain: | 4X |
| <input type="checkbox"/> Enable BLC | |
| Profile | |

Sensor Setting 1:
For normal situations

Sensor Setting 2:
For special situations

Preview
Restore
Save
Close

Exposure


- **Maximum Exposure Time:** Select a proper maximum exposure time according to the light source of the surroundings. Shorter exposure times result in less light. The exposure times are selectable for the following durations: 1/30 second and 1/15 second.
- **Exposure level:** You can manually set the Exposure level, which ranges from 1 to 8 (dark to bright). The default value is 4.
- **Max gain (Auto Gain Control):** You can manually set the AGC level (2X 4X, 8X, or 16X). The default value is 4X.
- **Enable BLC (Back Light Compensation):** Enable this option when the object is too dark or too bright to recognize. It allows the camera to adjust to the best light conditions in any environment and

automatically provide the necessary light compensation.

You can click **Preview** for a glimpse of expected results, or click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the settings and click **Close** to exit the page.

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

(TCP-V)
2011/01/17 13:44:17



General Settings

Enable this profile

Schedule mode:

From to [hh:mm]

Exposure

Maximum Exposure Time:

Exposure level:

Max gain:

Enable BLC

Please follow the steps below to setup a profile:

1. Check **Enable this profile**.
2. Enter a range of time for the Schedule mode.
3. Configure Exposure settings in the second column. Please refer to the previous page for detailed information.
4. Click **Save** to enable the setting and click **Close** to exit the page.


Viewing Window **Advanced Mode**

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

Users can define the "Region of Interest" (viewing region) and the "Output Frame Rate" (size of the live view window) ranging from 176 x 144 to 1280 x 800.

Image Settings Privacy Mask Sensor Settings Viewing Window

Viewing Window



Video Stream : Stream 1 ▾

Region of Interest :
(0,0) 640x480 custom ▾

Output frame size:
640x480 ▾
640x480
320x200
176x144

Save Close

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

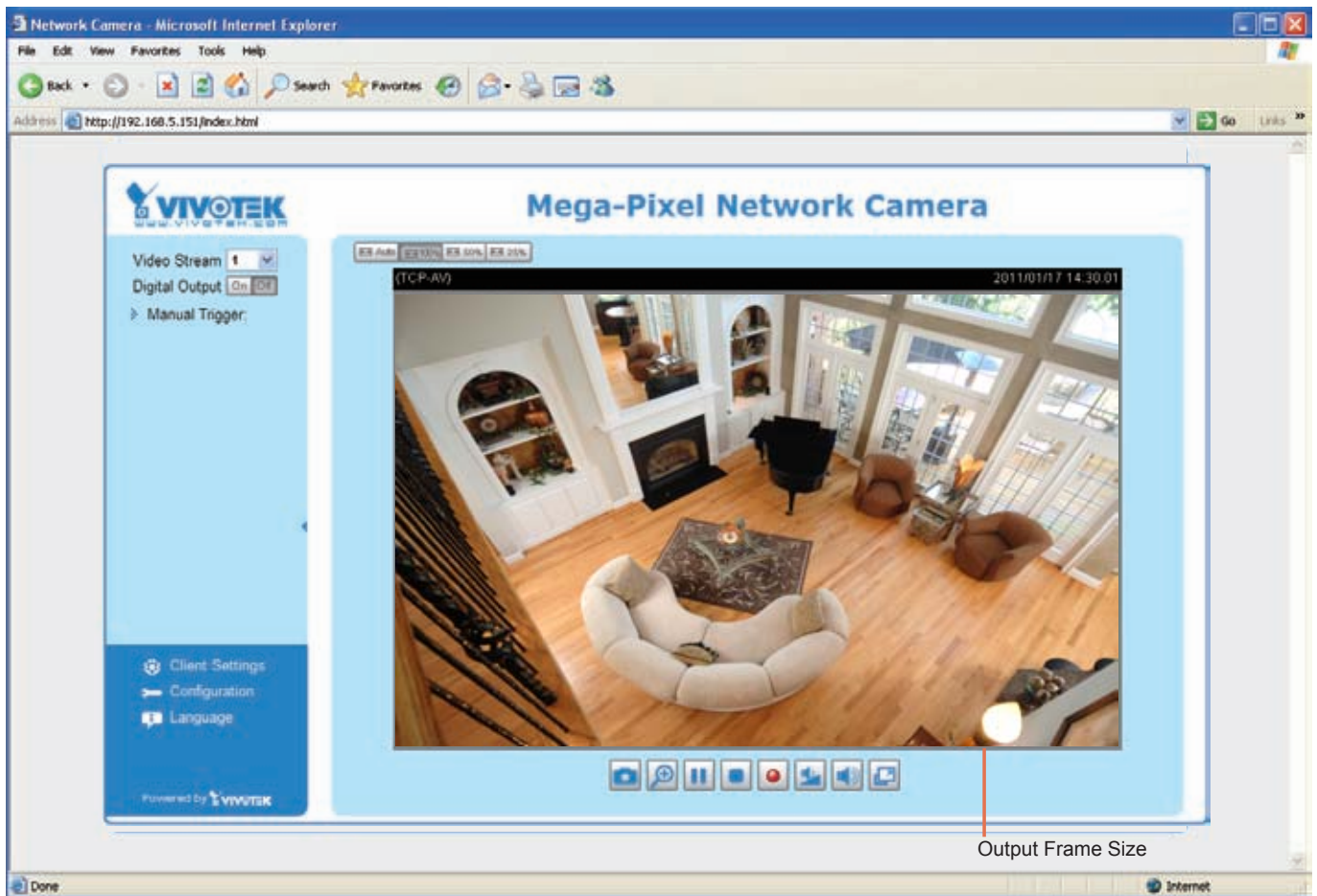
1. Select a stream which you want to set up the viewing region.
2. Select a **Region of Interest** from the drop-down list, the floating frame will resize accordingly. If you want to set up a customized viewing region, you can also resize and drag the floating frame to a desired position with your mouse.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



NOTE:

- ▶ *All the items in the "Region of Interest" should not be greater than the "Output Frame Size" (current maximum resolution).*

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



Video Quality Settings **Advanced Mode**

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

Video quality settings for stream 1:

H.264:

Frame size:

Maximum frame rate:

Intra frame period:

Video quality:

Constant bit rate:

Fixed quality:

JPEG:

Video quality settings for stream 3:

MPEG-4:

Frame size:

Maximum frame rate:

Intra frame period:

Video quality:

Constant bit rate:

Fixed quality:

H.264:

JPEG:

Video quality settings for stream 2:

MPEG-4:

H.264:

Frame size:

Maximum frame rate:

Intra frame period:

Video quality:

Constant bit rate:

Fixed quality:

JPEG:

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

H.264:

Frame size:

Maximum frame rate:

Intra frame period:

Video quality:

Constant bit rate:

Fixed quality:

■ 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.

■ Intra frame period


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

■ Video quality

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

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

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:

Maximum frame rate:

Video quality:

■ 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 load, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the event of occurrence, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

Audio Settings




NOTE:

Only IP8133 and IP8133W support two-way audio (they are equipped with an onboard speaker).

Audio Settings

Mute

Internal microphone input gain: 

Audio type:

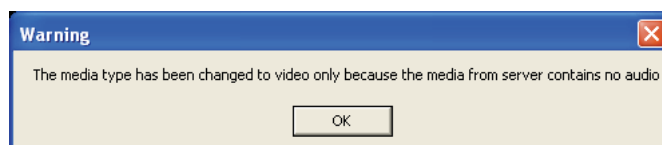
GSM-AMR:

GSM-AMR bit rate: 12.2 Kbps ▼

G.711:

Save

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



Internal microphone input gain: Manually drag the slide bar to adjust the gain of the internal audio input according to ambient conditions.

Audio type: Select audio codec and the bit rate Advanced Mode.

- 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.



NOTE:

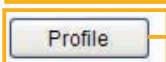
For audio recording and Event related settings (Media Settings), please refer to page 95 for more information.

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.



Motion Detection Setting 1:
For normal situations

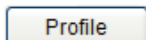


Motion Detection Setting 2:
For special situations

Follow the steps below to enable motion detection:

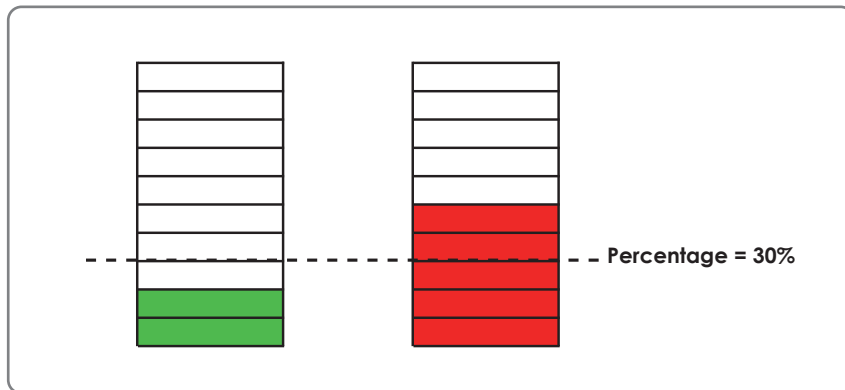
1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
 - To move and resize the window, drag and drop your mouse on the window.
 - To delete window, click X on the top right corner of the window.
3. Define the sensitivity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

For example:



The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to be sent to a remote server (Email, FTP) by utilizing this feature as a trigger source. For more information on how to set an event, please refer to Application on page 81.

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



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

The screenshot displays the Motion Detection Profile Settings interface. At the top left is a video feed labeled "Video(TCP-AV)" with a timestamp of "2011/01/17 13:44:17". To the right of the video are settings for a motion detection window: a "Window Name" text box, a "Sensitivity" slider set to 0%, and a "Percentage" slider also set to 0%. Below these are two buttons labeled "New" and "Save".

The "General Settings" section is located below the video and includes:

- An unchecked checkbox labeled "Enable this profile".
- A "Schedule mode:" section with a time range set from "18:00" to "06:00" in [hh:mm] format.
- A "Save" button at the bottom right of the settings panel.

 A "Close" button is positioned at the bottom center of the entire settings window.

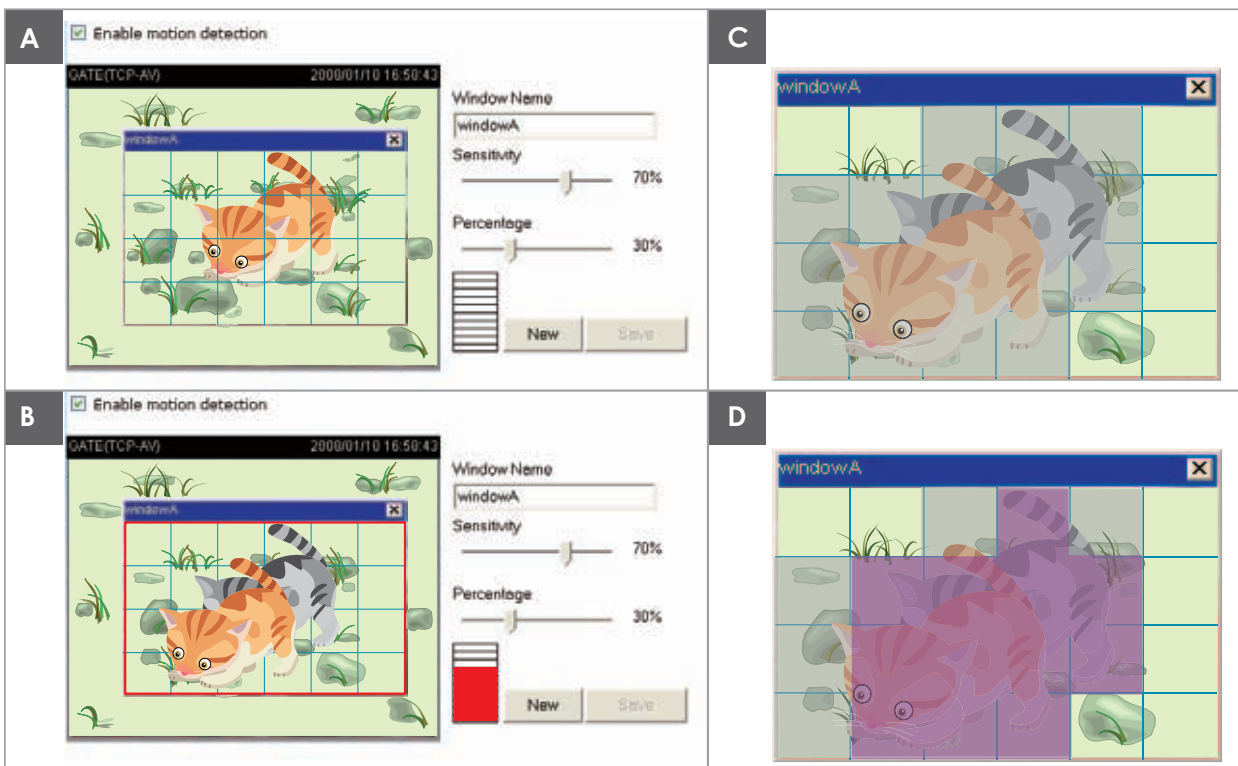
Please follow the steps below to set up a profile:

1. Create a new motion detection window.
2. Check **Enable this profile**.
3. Manually enter a time range for Schedule mode.
4. Click **Save** to enable the settings and click **Close** to exit the page.

This motion detection window will also be displayed on the Event Settings page. You can go to Application > Event Settings > Trigger to choose it as a trigger source. Please refer to page 83 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.

Camera Tampering Detection

With tamper detection, the camera is capable of detecting incidents such as **redirection**, **blocking or defocusing**, or even **spraying paint onto the camera**.

Camera tampering detection

Enable camera tampering detection

Trigger duration: seconds [10~600]

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

1. Select **Enable camera tampering detection**.
2. Enter the tamper trigger duration. (10 sec. ~ 10 min.) The tampering alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.
3. Set up the event source as Camera Tampering Detection on **Application page > Event Settings / Server Settings (how to send alarm message) / Media Settings (send what type of alarm message)**. Please refer to page 83 for detailed information.

Homepage Layout Advanced Mode

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

Preview

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



Hide Powered by VIVOTEK

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



Logo

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

Logo graph

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

Default
 Custom

Logo link:

Follow the steps below to upload a new logo:


1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.


Theme Options


Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the settings.

Theme Options

Themes







Custom

Color:

Font color:

Font color of configuration area:

Font color of video title:

Bk color of control area:

Bk color of configuration area:

Bk color of video area:

Frame color:

Preview


Font Color

Background Color of the Control Area

Font Color of the Configuration Area

Background Color of the Configuration Area

Preview



Video Stream


Digital Output









Manual Trigger:

Client Settings

Powered by VIVOTEK

Mega-Pixel Network




Font Color of the Video Title

Background Color of the Video Area

Frame Color

Preview

Preview



Video Stream


Digital Output









Manual Trigger:

Client Settings

Powered by VIVOTEK


Mega-Pixel Network



Preview

Preview



Video Stream


Digital Output









Manual Trigger:

Client Settings

Powered by VIVOTEK

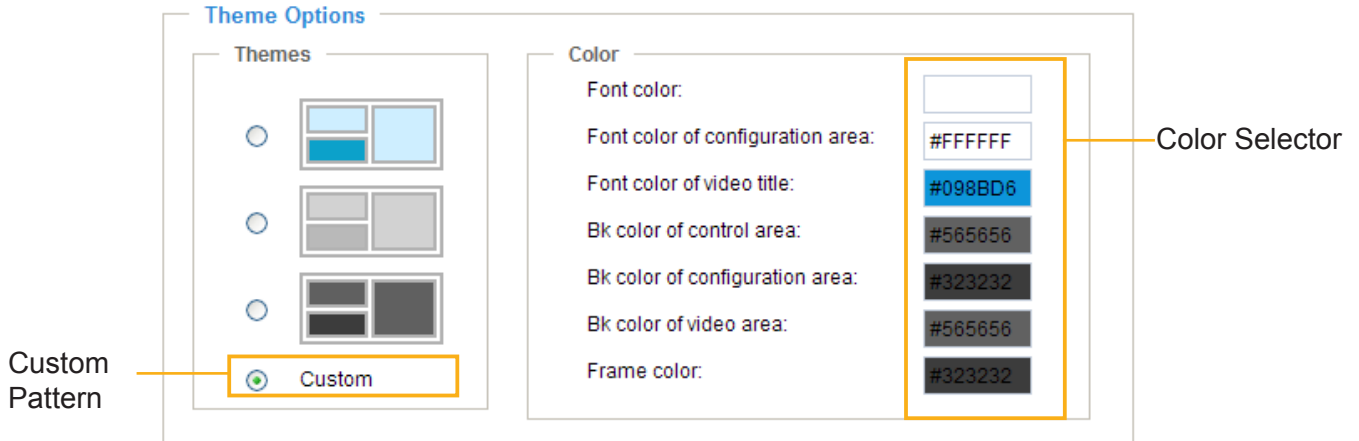
Mega-Pixel Network



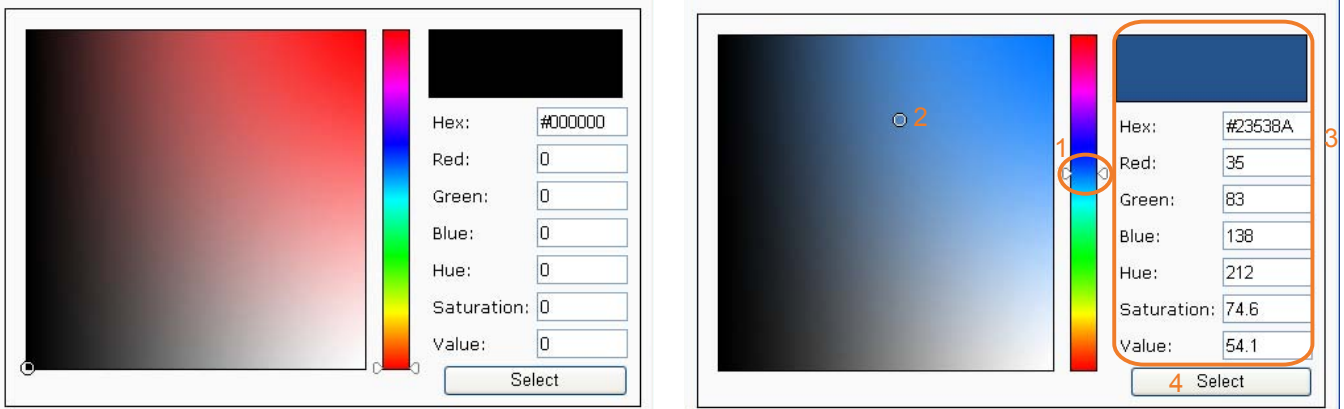









■ Follow the steps below to set up the custom homepage:

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



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

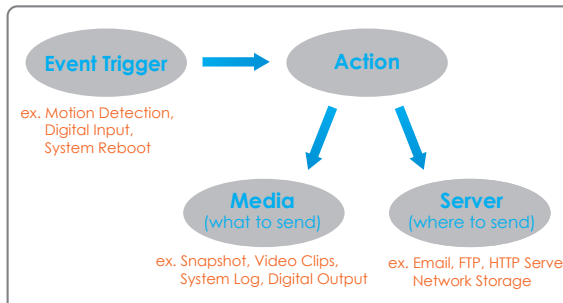


4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

Application Advanced Mode

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

As shown on the right, an event can be triggered by many sources, such as motion detection, PIR (Passive Infra Red motion detector - IP8133 & IP8133W), or external digital input devices. When an event is triggered, you can specify what type of action that will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.



>Application

Event Settings

| Name | Status | Sun | Mon | Tue | Wed | Thu | Fri | Sat | Time | Trigger |
|-----------------------|---------------------|-----|-----|-----|-----|-----|-----|-----|-------------|---------|
| vocal | OFF | V | V | V | V | V | V | V | 00:00~24:00 | pir |

Add
vocal ▼
Delete
Help

Media Settings

Available memory space for attached media: 15000KB

| Name | Type |
|--------|------|
| Add | ▼ |
| Delete | |

Available memory space for audio clips: 800KB

| Name | Size |
|------|------|
| dddd | 0 |

Add
▼
Play
Download
Delete

Customized Script

| Name | Date | Time |
|------|------|--------|
| Add | ▼ | Delete |

Event Settings

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

Event name:

Enable this event

Priority:

Detect next event after second(s).

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

Trigger

Video motion detection

Periodically

Digital input

PIR

System boot

Recording notify

Camera tampering detection

Manual Trigger

Event Schedule

Sun Mon Tue Wed Thu Fri Sat

Time

Always

From to [hh:mm]

Action

Trigger digital output for seconds

Turn on white-light illuminators for seconds

Play **Audio Clip**:

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 temporarily pause motion detection after a motion is detected. This prevents event broadcast to be too frequently delivered.

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

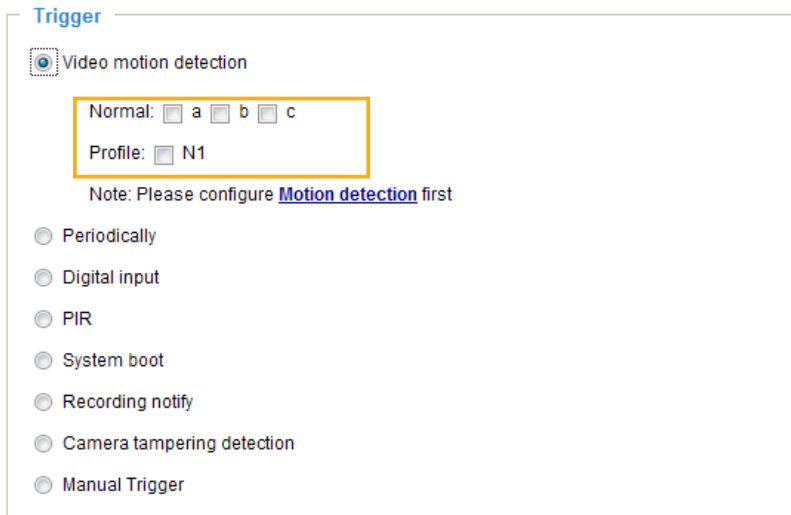
Trigger

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

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

■ Video motion detection

This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to [Motion Detection](#) on page 74 for details.



■ Periodically

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

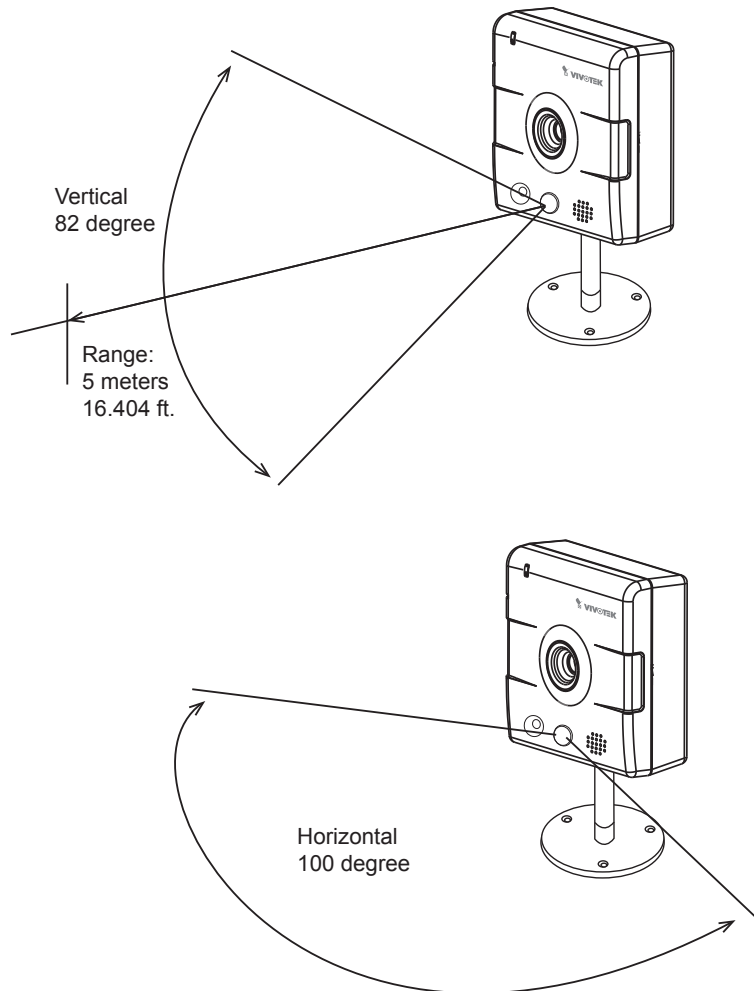


■ Digital input

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

■ PIR (Passive Infra Red motion detector)

When directed towards an anticipated area of interest, the PIR can be used to detect movements or intrusion, especially for detecting moving objects in the dark. PIR can be more effective than video motion detection. Shown below is the effective range of the PIR detector (IP8133 and IP8133W only).

**■ System boot**

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

■ Recording notify

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

■ Camera tampering detection

This option allows the Network Camera to trigger when the camera detects that it is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 77 for detailed information.

Trigger

Video motion detection:

Periodically:

Digital input

System boot

Recording notify

Camera tampering detection:

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

Manual Trigger

■ 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

Digital Output On Off

Manual Trigger:

| | | |
|---|----|-----|
| 1 | On | Off |
| 2 | On | Off |
| 3 | On | Off |

Event Schedule

Specify the period of time in which the event will take effect.

Event Schedule

Sun Mon Tue Wed Thu Fri Sat

Time

Always

From to [hh:mm]

■ Select the days of the week.

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

Action

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

Action

Trigger digital output for seconds

Turn on white-light illuminators for seconds

Play **Audio Clip:** -----None-----

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

to send the media files to) when a trigger is activated.

- **Trigger digital output for _ seconds:** You can enter a number here to turn on an external device for a duration of several seconds via the digital output connection.
- **Turn on white-light illuminators for _ seconds:** You may also turn on the white LED to light up the scene during the occurrence of a system event. Note that it is not recommended to turn on the LED for an extended period of time.
- **Play Audio Clip:** You use the onboard microphone to record a short vocal message or upload audio files from your PC. See **Add Media** in the later discussions. The camera can then playback a recorded vocal message when an event is triggered.

■ **Add Server / Add Media**

Click **Add Server** to configure [Server Settings](#). For more information, please refer to **Server Settings** on page 88.

Click **Add Media** to configure [Media Settings](#). For more information, please refer to **Media Settings** on page 91.

Here is an example of the Event Settings page:

Event name:

Enable this event

Priority:

Detect next event after second(s).

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

Trigger

Video motion detection

Periodically

Digital input

PIR

System boot

Recording notify

Camera tampering detection

Manual Trigger

Event Schedule

Sun Mon Tue Wed Thu Fri Sat

Time

Always

From to [hh:mm]

Action

Trigger digital output for seconds

Turn on white-light illuminators for seconds

Play **Audio Clip:**

| Server | Media | Extra parameter |
|--------------------------------|-----------------------------------|-----------------|
| <input type="checkbox"/> FTP | <input type="text" value="None"/> | |
| <input type="checkbox"/> Email | <input type="text" value="None"/> | |
| <input type="checkbox"/> HTTP | <input type="text" value="None"/> | |

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

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

Event Settings

| Name | Status | Sun | Mon | Tue | Wed | Thu | Fri | Sat | Time | Trigger |
|------------------------|--------------------|-----|-----|-----|-----|-----|-----|-----|-------------|---------|
| Event1 | ON | V | V | V | V | V | V | V | 00:00~24:00 | di |

Server Settings

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

Media Settings

Available memory space: 8000KB

| Name | Type |
|----------------------------|-----------|
| Snapshot | snapshot |
| Video Clip | videoclip |
| System log | systemlog |

Customized Script

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

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

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

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

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

Server Settings (Means by which to Deliver a Triggered Event)

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

Server name: Enter a name for the server setting.

Server Type

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

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

Server name:

Server Type

Email:

Sender email address:

Recipient email address:

Server address:

User name:

Password:

Server port:

This server requires a secure connection (SSL)

FTP:

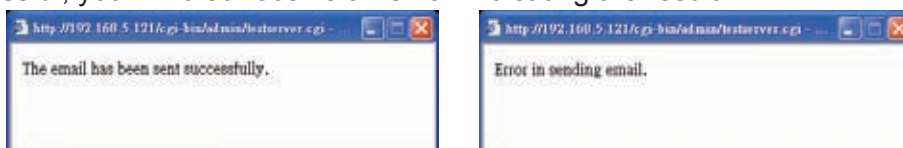
HTTP:

Network storage:

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

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

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



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

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

Server name:

Server Type

Email:

FTP:

Server address:

Server port:

User name:

Password:

FTP folder name:

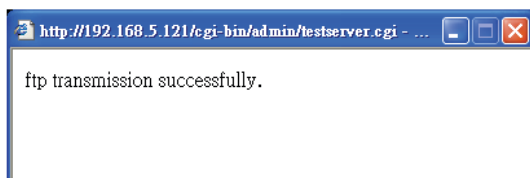
Passive mode

HTTP:

Network storage:

- **Server address:** Enter the domain name or IP address of the FTP server.
- **Server port**
By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.
- **User name:** Enter the login name of the FTP account.
- **Password:** Enter the password of the FTP account.
- **FTP folder name**
Enter the folder where the media file will be placed. If the folder name does not exist, the Network Camera will create one on the FTP server.
- **Passive mode**
Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

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



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

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

Server name:

Server Type

Email:

FTP:

HTTP:

URL:

User name:

Password:

Network storage:

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

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



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

Network storage: Select to send the media files to a network storage location when a trigger is activated. Please refer to **Network Storage Setting** on page 97 for details.

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

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

Turn on white-light illuminators for seconds

Play **Audio Clip**:

| Server | Media | Extra parameter |
|--------------------------------|---|-----------------|
| <input type="checkbox"/> FTP | <input type="text" value="----None----"/> | |
| <input type="checkbox"/> Email | <input type="text" value="----None----"/> | |
| <input type="checkbox"/> HTTP | <input type="text" value="----None----"/> | |

Media Settings (the Type of Contents that will be Preserved from a Triggered Event)

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

Media name: Enter a name for the media setting.

Media Type

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

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

Media name:

Media Type

Snapshot

Source:

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

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

File name prefix:

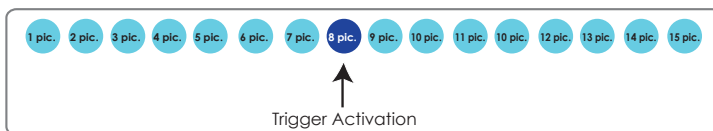
Add date and time suffix to file name

Video Clip

System log

- Source: Select any of the video streams as a source of snapshot.
- 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:

Snapshot_20110117_100341

↑
File name prefix

↑
Date and time suffix

The format is: YYYYMMDD_HHMMSS

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

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

Media name:

Media Type

Snapshot

Video Clip

Source:

Pre-event recording: seconds [0~9]

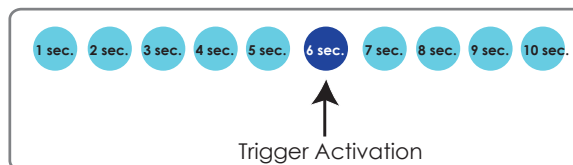
Maximum duration: seconds [1~20]

Maximum file size: Kbytes [50~800]

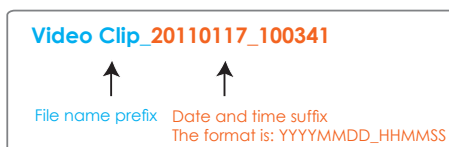
File name prefix:

System log

- **Source:** Select any of the video streams as a source of video clip.
- **Pre-event recording**
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.
- **Maximum duration**
Specify the maximum recording duration in seconds. You can record an event-triggered video for up to 20 seconds.
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** to enable the settings, then click **Close** to exit the page.

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

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

You can continue to select a server and media type for the event. Please refer to page 86 for detailed information.

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

- **Create folders by date, time, and hour automatically:** If you check this item, the system will generate folders automatically by date.
- **View:** Click this button to open a file list window. This function is only for **Network Storage (NAS)**. If you click **View** button of Network storage, a **file directory window** will prompt for you to view recorded data on Network storage. For detailed illustration, please refer to the next page.



NOTE:

The **Create folders by date/time/hour** checkbox and the **View** button may not be available until you test the connectivity using the **Test** button in each Server setting window.

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

The format is: YYYYMMDD
Click to open the directory

Click to delete selected items

Click to delete all recorded data

Click [20110118](#) to open the directory:

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

| | file name | size | date | time |
|--------------------------|-------------------|---------|------------|----------|
| <input type="checkbox"/> | Video Clip_58.mp4 | 2526004 | 2011/01/18 | 07:58:28 |
| <input type="checkbox"/> | Video Clip_59.mp4 | 2563536 | 2011/01/18 | 07:59:28 |

Click to delete selected items

Click to delete all recorded data

Click to go back to the previous level of the directory

| | file name | size | date | time |
|--------------------------|-------------------|---------|------------|----------|
| <input type="checkbox"/> | Video Clip_58.mp4 | 2526004 | 2011/01/18 | 07:58:28 |
| <input type="checkbox"/> | Video Clip_59.mp4 | 2563536 | 2011/01/18 | 07:59:28 |

The format is: File name prefix + Minute (mm)
You can set up the file name prefix on Media Settings (Video Clip) page. Please refer to page 91 for detailed information.

Media Settings

The **Media Settings** panel on the **Application** page is displayed when there are existing media settings. They are identical to those configured in the **Add Media** panel of the **Event Settings** (See page 91). Due to the limited size of the onboard memory, the media contents recorded during the occurrences of events should be delivered to the recipient side via Email, FTP, HTTP, or Network Storage. The onboard memory is primarily used as a transaction storage for capturing pre-event contents, and hopefully critical data will be preserved if the camera is maliciously disconnected.

Please note that a small amount of memory is preserved for audio recordings that will be used as a vocal message to someone on the scene or intruders. Audio clip playback is one of the event-triggered actions.

Media Settings

Available memory space for attached media: 12800KB

| Name | Type |
|----------------------------|-----------|
| snapshot | snapshot |
| Vclip | videoclip |
| video clip | videoclip |

Add

Available memory space for audio clips: 800KB

| Name | Size |
|------|------|
| ddd | 0 |

Add

NOTE:

The recorded audio will be saved as mono waves, in 8 KHz and 16-bit format.

If you prefer upload audio files to your camera, the following should be noticed:

1. Stereo will be converted to mono.
2. Higher KHz (e.g., 22.050 KHz) audio will be downgraded to 8 KHz.
3. Only **16-bit** files are supported. **8-bit** wave files are not supported.

Click **Add** to enter the recording page. You can grab the camera close to you and record a vocal message using the onboard microphone. To record a vocal message:

1. Enter a name for the recording.
2. Configure an elapse of time before the recording takes place after you click the **Record** button.
3. Click on the **Record** button. A recording progress window will prompt. Click **Stop** to end the recording.
4. Click **Replay** to ensure you have a satisfactory recording.
5. Click **Save** and click the **Close** button to end the process.

Media name:

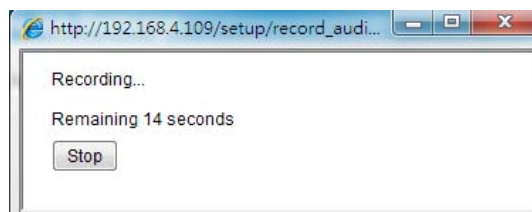
Media Type

Audio Clip

Record a sound file (*.wav) from camera:

Wait for seconds before recording [0~9]

Upload a pre-recorded sound file (*.wav):



Media Type

Audio Clip

Record a sound file (*.wav) from camera:

Upload a pre-recorded sound file (*.wav):

File: E:\Eric_desktop\music\

You can click the **Download** button to download the recorded wave file to your PC or click **Delete** to remove it from camera memory.

If you have audio wave files ready on your PC, you can upload the wave files to a camera using the corresponding **Upload** checkcircle in the Media Type window.

Customized Script

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

Customized Script

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

```

<?xml version="1.0" encoding="UTF-8"?>
<eventmgr version="0101">
<maxprocess>0</maxprocess>
<!-- From 08:30:00-20:30:00 on Monday to Friday every week -->
<schedule id="0">
<duration>
<weekday>1-5</weekday>
<time>08:30:00-20:30:00</time>
</duration>
</schedule>
<!-- Motion -->
<motion condition="0">
<status id="0">trigger</status>
<status id="1">trigger</status>
</motion>
<event id="0">
<description>Mail system log to email address</description>
<condition>0</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/sendmail -s "Motion" -f IPT139@vivotek.com -b /var/log/messages -S ms.vivotek.tw -
M 3 pudding.yang@vivotek.com
</process>
<priority>0</priority>
</event>
</eventmgr>
    
```


Recording Advanced Mode

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

Recording Settings

Recording Settings

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

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



NOTE:

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

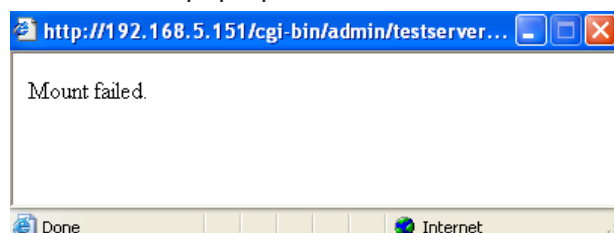
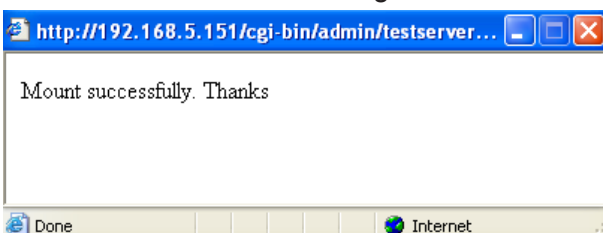
Network Storage Setting

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

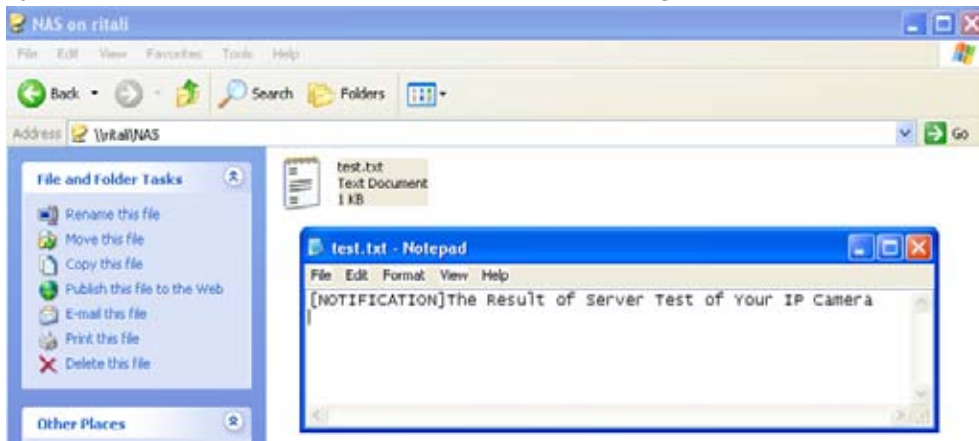
1. Fill in the information for your server.

For example:

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



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



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

Recording Settings

Click **Add** to open the recording setting page. 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

Recording name:

Enable this recording

With adaptive recording

Pre-event recording: seconds [0~9]

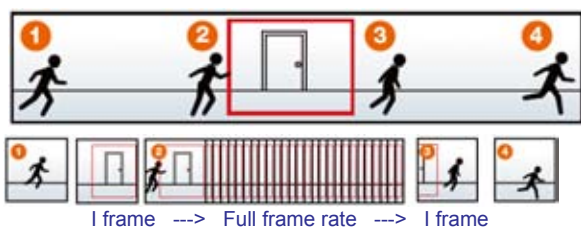
Post-event recording: seconds [0~10]

Recording name: Enter a name for the recording setting.

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

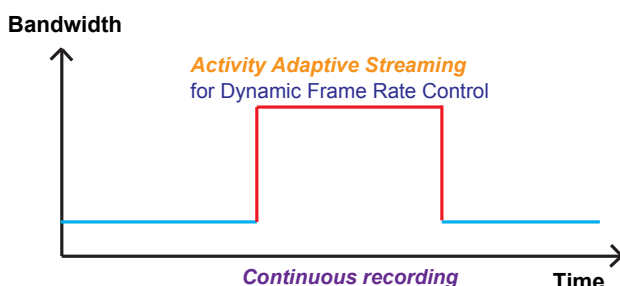
With adaptive recording: Select this option will activate the frame rate control according to alarm trigger. The frame control means that when there is alarm trigger, the frame rate will raise up to the value you've set on Video page. Please refer to page 64 for more information.

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



- 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 I frame period is >1s on Video settings page, the I frame period will be forced down to 1s when the adaptive recording feature is activated.



The alarm trigger includes: motion detection, DI detection, and manual trigger, etc. Please refer to Event Settings on page 82.

■ **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:

Source:

Trigger

Schedule

Recording Schedule

Sun Mon Tue Wed Thu Fri Sat

Time

Always

From to [hh:mm]

Destination:

Capacity:

Entire free space

Reserved space: Mbytes

File name prefix:

Enable cyclic recording

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

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

Source: Select the recording source (stream 1 ~ 3).

Trigger

- **Schedule:** The server will start to record files on the local storage or network storage (NAS) according to the following recording schedule.

Recording Schedule: Specify the recording duration.

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

Destination: Select the network storage that was set up for the recorded video files.

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

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

Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for cyclic recording during the transaction stage when the storage space is about to be fully filled. This value must be larger than 15 MBytes.

If you want to enable recording notification, please click [Application](#) to set up. Please refer to **Trigger > Recording notify** on page 85 for detailed information.

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

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

Recording Settings

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

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

Add SD Test Video ▼ Delete

- Click [Video \(Name\)](#): Opens the Recording Settings page to modify.
- Click [ON \(Status\)](#): The Status will become [OFF](#) and stop recording.
- Click [NAS \(Destination\)](#): Opens the file list of recordings as shown below. For more information about folder naming rules, please refer to page 94 for details.

| | | |
|--------------------------|--|--------------------------|
| <input type="checkbox"/> | | 20110118 |
| <input type="checkbox"/> | | 20110118 |
| <input type="checkbox"/> | | 20110118 |

Delete Delete all

System Log Advanced Mode

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

Remote Log

Remote Log

Enable remote log

Log server settings

IP address:

port:

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

| 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. |

Follow the steps below to set up the remote log:

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

Current Log

Current Log

```

Jan 8 13:26:53 syslogd 1.5.0: restart.
Jan 8 13:26:53 [swatdog]: Ready to watch httpd.
Jan 8 13:26:53 [swatdog]: Ready to watch recorder.
Jan 8 13:26:54 [EVENT MGR]: Starting eventmgr with support for EcTun
Jan 8 13:26:54 [EVENT MGR]: Task conf file: there is no valid event in recording_task.xml, skip it
Jan 8 13:26:54 [EVENT MGR]: Task conf file: there is no valid event in event_task.xml, skip it
Jan 8 13:26:54 [DRM Service]: Starting DRM service.
Jan 8 13:26:56 [UPnPIGDCP]: Search IGD failed
Jan 8 13:26:56 [swatdog]: Reduplicate registration from configer.
Jan 8 13:26:56 [swatdog]: Ready to watch configer.
Jan 8 13:26:57 [swatdog]: Ready to watch vencslave1.
Jan 8 13:26:57 [swatdog]: Ready to watch vencslave2.
Jan 8 13:26:57 [swatdog]: Ready to watch vencslave3.
Jan 8 13:26:58 automount[786]: >> mount: mounting /dev/localstorage1 on /mnt/auto/CF failed:
No such file or directory
Jan 8 13:26:58 automount[786]: mount(generic): failed to mount /dev/localstorage1 (type vfat)
on /mnt/auto/CF

```

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

View Parameters Advanced Mode

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

Parameter List

```

system_hostname='Mega-Pixel Network Camera'
system_ledoff='0'
system_lowlight='1'
system_date='2011/01/18'
system_time='14:33:58'
system_datetime='011814332011.54'
system_ntp=''
system_timezoneindex='320'
system_daylight_enable='0'
system_daylight_dstactualmode='1'
system_daylight_auto_begintime='NONE'
system_daylight_auto_endtime='NONE'
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-1
system_privacy='0'
system_privacybuttonoff='0'
system_updateinterval='0'
system_info_modelname='IP8132'
system_info_extendedmodelname='IP8132'
system_info_serialnumber='0002D1125566'
system_info_firmwareversion='IP8132-VVTK-0100f'
system_info_language_count='9'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system_info_language_i3='Français'
system_info_language_i4='Italiano'
system_info_language_i5='日本語'
system_info_language_i6='Português'
system_info_language_i7='简体中文'
system_info_language_i8='繁體中文'
system_info_language_i9=''
system_info_language_i10=''
system_info_language_i11=''
system_info_language_i12=''
system_info_language_i13=''
system_info_language_i14=''

```

Maintenance

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

Reboot

Reboot

Reboot the device

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

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

|||||

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

Restore

Restore

Restore all settings to factory default except settings in

Network
 Daylight Saving Time
 Custom language
 Wireless

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

Network Type: Select this option to retain the Network Type settings (please refer to Network Type on page 35).

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

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

Wireless: Select this option to retain the settings related to wireless connection.

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

The following message is displayed during the restoring process.

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

|||||

Export / Upload Files Advanced Mode

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

Export files

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

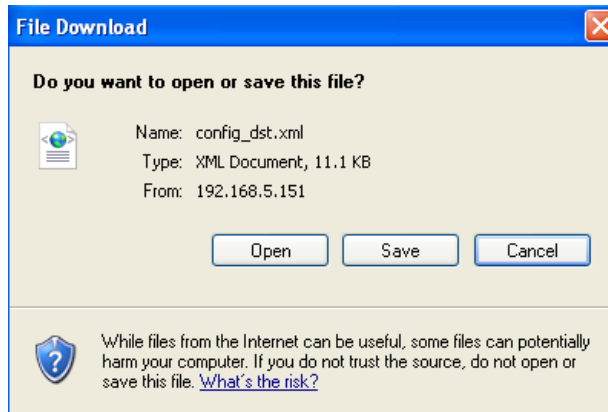
Upload files

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

Export daylight saving time configuration file: Click to set the start and end time of DST.

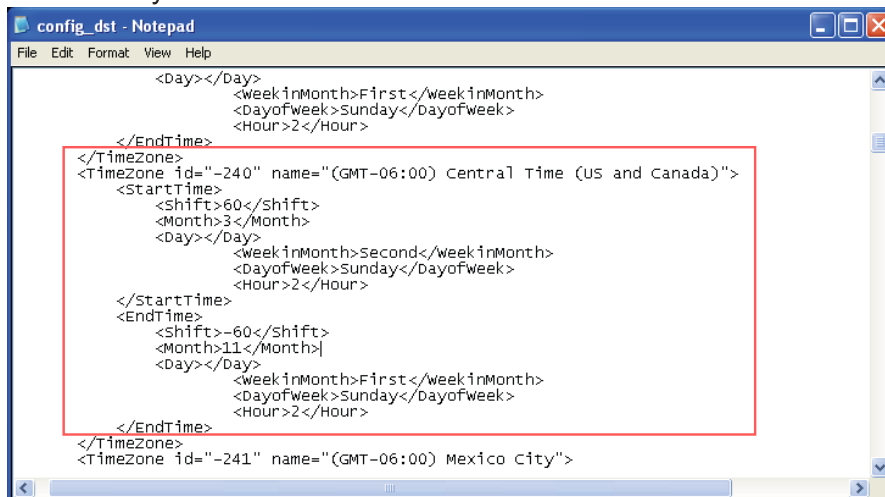
Follow the steps below to export:

1. In the Export files column, click **Export** to export the daylight saving time configuration file from the Network Camera.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.



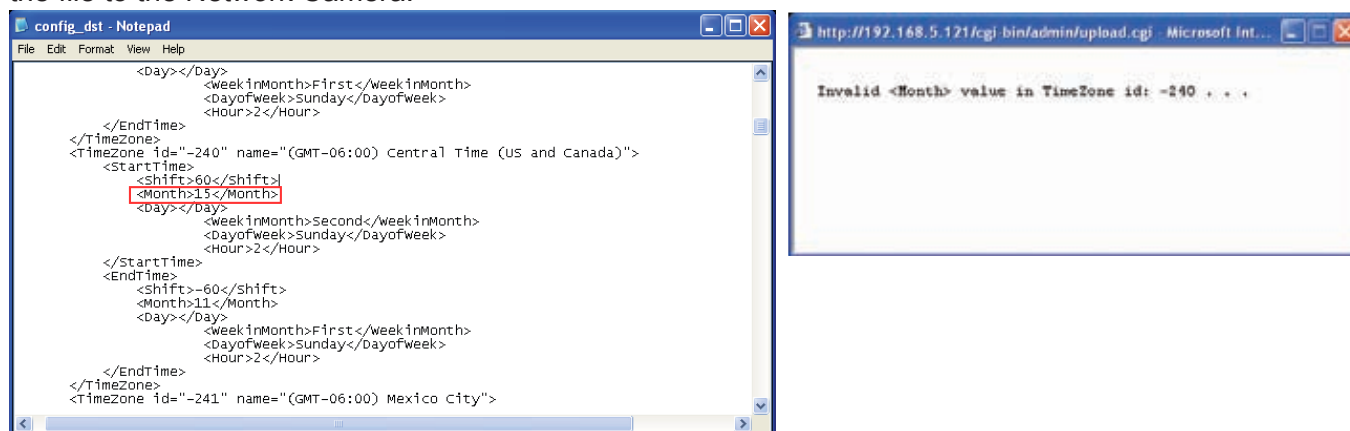
3. Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST. When completed, save the file.

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

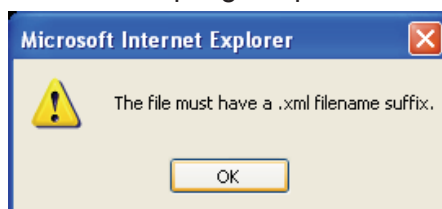


Upload daylight saving time rule: Click **Browse...** and specify the XML file to upload.

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



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



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

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

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

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

Upgrade Firmware

Upgrade firmware

Select firmware file

This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.

Note: Do not power off the Network Camera during the upgrade!

Follow the steps below to upgrade the firmware:

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

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

The following message is displayed when the upgrade has succeeded.

Reboot system now!!
This connection will close.

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

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

Appendix

URL Commands for the Network Camera

1. Overview

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

2. Style Convention

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

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

Syntax:

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

Description of returned data is written with "Return:" in bold face followed by the returned data in a box. All data 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

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 #0 to active

<http://mywebserver/cgi-bin/dido/setdo.cgi?do0=1>

4. Security Level

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

5. Get Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

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

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

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

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

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

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

A successful control request returns parameter pairs as follows:

Return:

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

where *<parameter pair>* is

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

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

<length> is the actual length of content.

Example: Request IP address and its response

Request:

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

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

6. Set Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

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

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

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

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

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

Return:

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

where <parameter pair> is

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

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

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

Example: Set the IP address of server to 192.168.0.123:

Request:

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

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Content-Length: 33\r\n

\r\n

network_ipaddress=192.168.0.123\r\n

7. Available parameters on the server

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

Valid values:

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

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

7.1 System

Group: system

| NAME | VALUE | SECURITY (get/set) | DESCRIPTION |
|---------------|--|-----------------------|---|
| hostname | string[40] | 1/6 | Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server). |
| ledoff | <boolean> | 6/6 | Turn on (0) or turn off (1) all led indicators. |
| 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, |

| | | | | |
|--|--|--|--|---|
| | | | | <p>La Paz, Santiago</p> <p>-140: GMT-03:30 Newfoundland</p> <p>-120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland</p> <p>-80: GMT-02:00 Mid-Atlantic</p> <p>-40: GMT-01:00 Azores, Cape_Verde_IS.</p> <p>0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London</p> <p>40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris</p> <p>41: GMT 01:00 Warsaw, Budapest, Bern</p> <p>80: GMT 02:00 Athens, Helsinki, Istanbul, Riga</p> <p>81: GMT 02:00 Cairo</p> <p>82: GMT 02:00 Lebanon, Minsk</p> <p>83: GMT 02:00 Israel</p> <p>120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi</p> <p>121: GMT 03:00 Iraq</p> <p>140: GMT 03:30 Tehran</p> <p>160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan</p> <p>180: GMT 04:30 Kabul</p> <p>200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent</p> <p>220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi</p> <p>230: GMT 05:45 Kathmandu</p> <p>240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura</p> <p>260: GMT 06:30 Rangoon</p> <p>280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk</p> <p>320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei</p> <p>360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk</p> <p>380: GMT 09:30 Adelaide, Darwin</p> <p>400: GMT 10:00 Brisbane, Canberra,</p> |
|--|--|--|--|---|

| | | | |
|-----------------------------|---|-----|--|
| | | | 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_beginningtime | string[19] | 6/7 | Display the current daylight saving start time. |
| daylight_auto_endingtime | 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. |
| privacy | <boolean> | 6/6 | Represent privacy button status |
| privacybuttonoff | <boolean> | 6/6 | 0: enable privacy button function 1: disable privacy button function |
| 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 integer> | 7/6 | Restart the server after <value> seconds if <value> is non-negative. |
| 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 |

| | | | |
|-----------------------|-------------|-----|--|
| | | | <p>settings.</p> <p>This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to default values except for a union of combined results.</p> |
| restoreexceptlang | <Any Value> | 7/6 | <p>Restore the system parameters to default values except the custom language file the user has uploaded.</p> <p>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.</p> |
| restoreexceptwireless | <Any Value> | 7/6 | <p>Restore the system parameters to default values except wireless settings.</p> <p>This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to default values except for a union of combined results.</p> <p>(capability_network_wireless=1)</p> |

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) |
| wled_i<0~(nwled-1)> <product dependent> | <boolean> | 1/7 | 0 => Inactive, normal 1 => Active, triggered (capability.nwled > 0) |
| vi_i<0~(nvi-1)> <product dependent> | <boolean> | 1/7 | Virtual input 0 => Inactive 1 => Active (capability.nvi > 0) |
| onlinenum_rtsp | <integer> | 6/7 | Current number of RTSP connections. |
| onlinenum_httppush | <integer> | 6/7 | Current number of HTTP push server connections. |
| onlinenum_sip | <integer> | 6/7 | Current number of SIP connections. |
| eth_i0 | <string> | 1/7 | Get network information from mii-tool. |

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_wled <product dependent> | view, operator, admin | 6/6 | Indicate which privileges and above can control white light LED (capability.nwled > 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 | view, operator, admin | 6/7 | Root privilege |
| user_i<1~20>_ privilege | view, operator, admin | 6/6 | User privilege |

7.6 Network

Group: **network**

| NAME | VALUE | SECURITY (get/set) | DESCRIPTION |
|------------|---|-----------------------|--|
| preprocess | <positive integer> | 7/6 | <p>An 32-bit integer, each bit can be set separately as follows:</p> <p>Bit 0 => HTTP service; Bit 1=> HTTPS service; Bit 2=> FTP service; Bit 3 => Two way audio and RTSP Streaming service;</p> <p>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.</p> <p>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”</p> |
| type | lan, pppoe <product dependent> | 6/6 | Network connection type. |
| resetip | <boolean> | 6/6 | <p>1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot. 0 => Use preset ipaddress, subnet, rounter, dns1, and dns2.</p> |
| 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 dependent> | 0~7 | 6/6 | Audio channel for CoS (capability.naudio > 0) |
| 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 <product dependent> | 0~63 | 6/6 | Audio channel for DSCP (capability.audio > 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 | 6/6 | 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 | string[32] | 1/6 | Http server push access name for stream 3 |

| | | | |
|---------------------|-----------|-----|--|
| <product dependent> | | | (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 2) |
| anonymousviewing | <boolean> | 1/6 | Enable anonymous streaming viewing. |

7.6.6 HTTPS port

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

| NAME | VALUE | SECURITY (get/set) | DESCRIPTION |
|------|-------------------|-----------------------|-------------|
| port | 443, 1025 ~ 65535 | 6/6 | 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 anonymous streaming viewing. |
| authmode | disable, basic, digest | 1/6 | RTSP authentication mode. (capability.protocol.rtsp=1) |
| s0_accessname | string[32] | 1/6 | RTSP access name for stream1. (capability.protocol.rtsp=1 and capability.nmediastream > 0) |
| s1_accessname <product dependent> | string[32] | 1/6 | RTSP access name for stream2. (capability.protocol.rtsp=1 and capability.nmediastream > 1) |
| s2_accessname <product dependent> | string[32] | 1/6 | RTSP access name for stream3 (capability.protocol.rtsp=1 and capability.nmediastream > 2) |

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. |
| audiotrack | -1, 0 | 6/6 | Select the audio stream for streaming. -1: no audio 0: audio stream 0 |

| | | | |
|-----------|--------------|-----|---|
| ipaddress | <ip address> | 4/4 | Multicast IP address. |
| videoport | 1025 ~ 65535 | 4/4 | Multicast video port. |
| audioport | 1025 ~ 65535 | 4/4 | Multicast audio port. (capability.audio > 0) |
| ttl | 1 ~ 255 | 4/4 | Multicast time to live value. |

7.6.8 SIP port

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

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|------|--------------|---------|-----------------------|-------------|
| port | 1025 ~ 65535 | 5060 | 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 Wireless

Group: **wireless** (capability.network.wireless > 0)

| NAME | VALUE | SECURITY (get/set) | DESCRIPTION |
|---------|-----------------|-----------------------|--|
| ssid | string[32] | 6/6 | SSID for wireless lan settings. The valid characters are [A-Z] [a-z] [0-9] [/] [.] [] [=] [] [-] [+]. |
| wlmode | Infra, Adhoc | 6/6 | Wireless mode. Infra: Infrastructure Adhoc: Ad hoc |
| channel | 1~11 or | 6/6 | USA and Canada |

| | | | |
|-------------|--|-----|--|
| | 1 ~ 13 or 10~11 or 10~13 or 1~14 | | Europe Spain France All |
| txrate | NONE, 1M, 2M, 5.5M, 11M, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M, Auto | 6/6 | Maximum transmit rate in Mbps. |
| encrypt | 0~3 | 6/6 | Encryption method: 0=> NONE, 1 => WEP, 2 => WPA, 3 => WPA2PSK <product dependent> |
| authmode | OPEN, SHARED | 6/6 | Authentication mode. |
| keylength | 64, 128 | 6/6 | Key length in bits. |
| keyformat | HEX, ASCII | 6/6 | Key1 ~ key4 presentation format. |
| keyselect | 1 ~ 4 | 6/6 | Default key number. |
| key1 | password [32] | 6/6 | WEP key1 for encryption. The valid characters are [A-Z] [a-z] [0-9]. |
| key2 | password [32] | 6/6 | WEP key2 for encryption. The valid characters are [A-Z] [a-z] [0-9]. |
| key3 | password [32] | 6/6 | WEP key3 for encryption. The valid characters are [A-Z] [a-z] [0-9]. |
| key4 | password [32] | 6/6 | WEP key4 for encryption. The valid characters are [A-Z] [a-z] [0-9]. |
| Domain | 'U' for USA 'C' for Canada 'E' for Euro 'S' for Spain 'F' for France 'I' for Isrel 'A' for All | 6/7 | Wireless domain. |
| algorithm | AES, TKIP | 6/6 | Algorithm |
| presaredkey | password [63] | 6/6 | WPA mode pre-shared key. The valid characters are [A-Z] [a-z] [0-9]. |

7.8 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[39] | 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. |

7.9 Video input

Group: **videoin**

| NAME | VALUE | SECURITY (get/set) | DESCRIPTION |
|---------------|--------------|-----------------------|---|
| cmosfreq | 50, 60 | 4/4 | CMOS frequency. (capability.videoin.type=2) |
| whitebalance | auto, manual | 4/4 | “auto” indicates auto white balance. “manual” indicates keep current value. |
| atwbvalue1 | 0~999999999 | 4/4 | Auto white balance value |
| atwbvalue2 | 0~999999999 | 4/4 | Auto white balance value |
| exposurelevel | 1~8 | 4/4 | Exposure level |
| enableblec | <boolean> | 4/4 | Enable backlight compensation. |
| privacystatus | <boolean> | 4/4 | Same as privacy button status 0: normal streaming 1: blue frame streaming |
| agc | 0,1,2,3 | 4/4 | Set auto gain control to normal level, middle or MAX level. 0->2X 1->4X |

| | | | |
|--|--|--|-----------------|
| | | | 2->8X 3->16X |
|--|--|--|-----------------|

7.9.1 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. (capability.videoin.type=2) |
| whitebalance | auto, manual | 4/4 | “auto” indicates auto white balance. “manual” indicates keep current value. |
| atwbvalue1 | 0~999999999 | 4/4 | Auto white balance value |
| atwbvalue2 | 0~999999999 | 4/4 | Auto white balance value |
| exposurelevel | 1~8 | 4/4 | Exposure level |
| enableblc | <boolean> | 4/4 | Enable backlight compensation. |
| agc | 0,1,2,3 | 4/4 | Set auto gain control to normal level, middle or MAX level. 0->2X 1->4X 2->8X 3->16X |
| 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. |

| | | | |
|--------------------------------------|---|-----|--|
| imprnttimestamp | <boolean> | 4/4 | Overlay time stamp on video. |
| maxexposure | 15~30 | 4/4 | Maximum exposure time. |
| privacystatus | <boolean> | 4/4 | Same as privacy button status 0: normal streaming 1: blue frame streaming |
| enablepreview | <boolean> | 1/4 | Enable preview |
| s<0~(m-1)>_codectype | mpeg4, mjpeg, h264 | 1/4 | Video codec type. Stream0 does not support mpeg4 |
| s<0~(m-1)>_resolution | 176x144 ~ 1280x800 | 1/4 | Video resolution in pixels. |
| s<0~(m-1)>_mpeg4_intra period | 250, 500, 1000, 2000, 3000, 4000 | 4/4 | Intra frame period in milliseconds. |
| s<0~(m-1)>_mpeg4_rate controlmode | cbr, vbr | 4/4 | cbr, constant bitrate vbr, fix quality |
| s<0~(m-1)>_mpeg4_qua nt | 0, 1~5 99, 100 | 4/4 | Quality of video when choosing vbr in “ratecontrolmode”. 0,99,100 is the customized manual input setting. 1 = worst quality, 5 = best quality. |
| s<0~(m-1)>_mpeg4 _qvalue | 1~31 | 4/4 | Manual video quality level input. (s<0~(m-1)>_mpeg4_quant = 0 or 99) |
| s<0~(m-1)>_mpeg4 _qpercent | 1~100 | 4/4 | Using percentage to represent manual video quality level input. (s<0~(m-1)>_mpeg4_quant = 100) |
| s<0~(m-1)>_mpeg4_bitra te | 1000~8000000 | 4/4 | Set bit rate in bps when choosing cbr in “ratecontrolmode”. |
| s<0~(m-1)>_mpeg4_max frame | 1~25, 26~30 (only for NTSC or 60Hz CMOS) | 1/4 | Set maximum frame rate in fps (for mpeg4). |
| s<0~(m-1)>_h264_intra period | 250, 500, 1000, 2000, 3000, 4000 | 4/4 | Intra frame period in milliseconds. |
| s<0~(m-1)>_h264_rateco ntrolmode | cbr, vbr | 4/4 | cbr, constant bitrate vbr, fix quality |
| s<0~(m-1)>_h264_quant | 0,1~5,99,100 | 4/4 | Quality of video when choosing vbr in “ratecontrolmode”. 0, 99, 100 is the customized manual input |

| | | | |
|---------------------------|---|-----|--|
| | | | setting. 1 = worst quality, 5 = best quality. |
| s<0~(m-1)>_h264_qvalue | 0~51 | 4/4 | Manual video quality level input. (s<0~(m-1)>_h264_quant = 0 or 99) |
| s<0~(m-1)>_h264_qpercent | 1~100 | 4/4 | Using percentage to represent manual video quality level input. (s<0~(m-1)>_h264_quant = 100) |
| s<0~(m-1)>_h264_bitrate | 1000~8000000 | 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 | 0~2 | 1/4 | Indicate H264 profiles 0: baseline 1: main profile 2: high profile |
| s<0~(m-1)>_mjpeg_quant | 0, 1 ~ 5 99, 100 | 4/4 | Quality of JPEG video. 0, 99, 100 is the customized manual input setting. 1 = worst quality, 5 = best quality. |
| s<0~(m-1)>_mjpeg_qvalue | 0~200 | 4/4 | Manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 0 or 99 or 100) |
| s<0~(m-1)>_mjpeg_qpercent | 1~100 | 4/4 | Using percentage to represent manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 0 or 99 or 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). |
| s<0~(m-1)>_forcei | 1 | 7/6 | Force I frame. |

7.9.1.1 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_c<0~(n-1)>_profile_i<0~(m-1)>** (**capability.nvideoinprofile > 0**)

| NAME | VALUE | SECURITY (get/set) | DESCRIPTION |
|---------------|-----------|-----------------------|--|
| Enable | <boolean> | 4/4 | Enable/disable this profile setting |
| Policy | schedule | 4/4 | The mode which the profile is applied to. |
| begintime | hh:mm | 4/4 | Begin time of schedule mode. |
| endtime | hh:mm | 4/4 | End time of schedule mode. |
| maxexposure | 15~30 | 4/4 | Maximum exposure time. |
| enableblec | <boolean> | 4/4 | Enable backlight compensation. |
| exposurelevel | 1~8 | 4/4 | Exposure level |
| agc | 0,1,2,3 | 4/4 | Set auto gain control to normal level, middle or MAX level. 0->2X 1->4X 2->8X 3->16X |

7.10 Video input preview

The temporary settings for video preview

Group: **videoinpreview**

| NAME | VALUE | SECURITY (get/set) | DESCRIPTION |
|---------------|-----------|-----------------------|---|
| maxexposure | 15~30 | 4/4 | Maximum exposure time |
| exposurelevel | 1~8 | 4/4 | Preview of exposure level |
| enableblec | <boolean> | 4/4 | Preview of enable backlight compensation. |
| agc | 0,1,2,3 | 4/4 | Preview of set auto gain control to normal level or MAX level. 0->2X 1->4X 2->8X 3->16X |

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 | 4/4 | Adjust saturation of image according to mode settings. |
| Contrast | -5 ~ 5 | 4/4 | Adjust contrast of image according to mode settings. |
| sharpness | -3 ~ 3 | 4/4 | Adjust sharpness of image according to mode settings. |
| IBPE_nrenable | <boolean> | 4/4 | Enable noise reduction. |
| IBPE_nrmode | 1 ~ 3 | 4/4 | Adjust noise reduction mode. 1 => DeGaussian 2 => DeImpulse 3 => DeGaussian + DeImpulse |
| IBPE_nrstrength | 1 ~ 63 | 4/4 | Adjust noise reduction strength. 1 is minimum and 63 is maximum. |

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 | Preview of brightness adjustment of image according to mode settings. |
| saturation | -5 ~ 5 | 4/4 | Preview of saturation adjustment of image according to mode settings. |
| Contrast | -5 ~ 5 | 4/4 | Preview of contrast adjustment of image according to mode settings. |
| sharpness | -3 ~ 3 | 4/4 | Preview of sharpness adjustment of image according to mode settings. |
| IBPE_nrenable | <boolean> | 4/4 | Preview of adjusting enabling noise reduction. |
| IBPE_nrmode | 1 ~ 3 | 4/4 | Preview of adjusting noise reduction mode. 1 => DeGaussian 2 => DeImpulse 3 => DeGaussian + DeImpulse |
| IBPE_nrstrength | 1 ~ 63 | 4/4 | Preview of adjusting noise reduction strength. 1 is minimum and 63 is maximum. |

Group: **imagepreview**

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

7.13 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 | 1/4 | Enable audio mute. |
| gain | 1~100 | 4/4 | Gain of input. |
| s<0~(m-1)>_codectype | gamr, g711 | 4/4 | Set audio codec type for input. |
| s<0~(m-1)>_gamr_bitrate | 4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200 | 4/4 | Set AMR bitrate in bps. |
| s<0~(m-1)>_g711_mode | pcmu, pcma | 4/4 | Set G.711 mode. |

7.14 Audio output per channel

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

| NAME | VALUE | SECURITY (get/set) | DESCRIPTION |
|----------------|-------|-----------------------|-----------------|
| gainpercentage | 1~100 | 4/4 | Gain of output. |

7.15 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 | 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. |

7.16 Tampering 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. |

7.17 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 | 6/6 | Safe100 => safe100.net DyndnsDynamic => dyndns.org (dynamic) DyndnsCustom => dyndns.org (custom) TZO => tzo.com DHS => dhs.org DynInterfree => dyn-interfree.it CustomSafe100 => Custom server using safe100 method |
| <provider>_hostname | string[128] | 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 customsaf100) |

7.18 UPnP presentation

Group: **upnppresentation**

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

7.19 UPnP port forwarding

Group: **upnpportforwarding**

| NAME | VALUE | SECURITY (get/set) | DESCRIPTION |
|----------------|-----------|-----------------------|--|
| enable | <boolean> | 6/6 | Enable or disable the UPnP port forwarding service. |
| upnppnatstatus | 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

7.20 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 |

7.21 SNMP

Group: **snmp** (**capability.protocol.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 |
| authyperw | MD5,SHA | 6/6 | Read/write authentication type |
| authypero | MD5,SHA | 6/6 | Read only authentication type |
| encryptpwrw | string[8~128] | 6/6 | Read/write password |
| encryptpwro | string[8~128] | 6/6 | Read only password |
| encryptyperw | DES | 6/6 | Read/write encryption type |
| encryptypero | DES | 6/6 | Read only encryption type |
| rwcommunity | string[31] | 6/6 | Read/write community |
| rocommunity | string[31] | 6/6 | Ready only community |

7.22 Layout configuration

Group: **layout**

| 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 | <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 |

7.23 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. |

7.24 Capability

Group: **capability**

| NAME | VALUE | SECURITY (get/set) | DESCRIPTION |
|-----------------|--------------------------|-----------------------|--|
| api_httpversion | 0100a | 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 |

| | | | |
|------------------------------------|-----------------------|-----|--|
| | | | <p>support), 1(support)</p> <p>Bit 3 => Support tilt operation; 0(not support), 1(support)</p> <p>Bit 4 => Support zoom operation; 0(not support), 1(support)</p> <p>Bit 5 => Support focus operation; 0(not support), 1(support)</p> <p>Bit 6 => Support iris operation; 0(not support), 1(support)</p> <p>Bit 7 => External or built-in PT; 0(built-in), 1(external)</p> <p>Bit 8 => Invalidate bit 1 ~ 7; 0(bit 1 ~ 7 are valid), 1(bit 1 ~ 7 are invalid)</p> <p>Bit 9 => Reserved bit; Invalidate lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris. 0(fields are valid), 1(fields are invalid)</p> |
| eptz | 0, <positive integer> | 0/7 | <p>A 32-bit integer, each bit can be set separately as follows:</p> <p>Bit 0 => stream 1 supports ePTZ or not.</p> <p>Bit 1 => stream 2 supports ePTZ or not.</p> <p>The rest may be deduced by analogy</p> |
| npreset | 0, <positive integer> | 0/7 | Number of preset locations. |
| 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 | <a list of available resolution separated by commas> | 0/7 | Available resolutions list. |
| videoin_maxframerate | <a list of available maximum frame rate separated by commas> | 0/7 | Available maximum frame list. |
| videoin_codec | mpeg4, mjpeg, h264 | 0/7 | Available codec list. |
| videoin_streamcodec | <integer> | 0/7 | Each stream has its own support codec type. It is bitwise depends on videoin_codec. bit0: mpeg4 bit1: mjpeg bit2: h264 First stream support mjpeg and h264 (bit0:0, bit1:1, bit2:1) |
| videoout_codec | <a list of the available codec types separated by commas> | 0/7 | Available codec list. |
| audio_aec | <boolean> | 0/7 | Indicate whether to support acoustic echo cancellation. |
| audio_mic | <boolean> | 0/7 | Indicate whether to support built-in microphone input. |
| 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 | gamr, g711 | 0/7 | Available codec list for audio input. |
| uart_httptunnel | <boolean> | 0/7 | Indicate whether to support HTTP tunnel for UART transfer. |
| 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 |
| 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_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 |
| 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. |
| 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) |
| 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. |
| nanystream | 0, <positive | 0/7 | number of any media stream per channel |

| | | | |
|---------------------|-----------|-----|--|
| | integer> | | |
| iva | <boolean> | 0/7 | Indicate whether to support Intelligent Video analysis |
| version_onvifdaemon | <string> | 0/7 | Indicate ONVIF daemon version |

7.25 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. |

7.26 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, pir, motion, seq, renotify, tampering, vi | 6/6 | Indicate the trigger condition: “boot” = System boot “di” = Digital input “pir” = PIR “motion” = Video motion detection “seq” = Periodic condition “renotify” = 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. |

| | | | |
|-------------------------------------|------------------|-----|--|
| 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. |
| 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 1 st window. For example, to detect the 1 st and 3 rd windows, set mdwin as 5. |
| mdwin0 | <integer> | 6/6 | Similar to mdwin. The parameter takes effect when profile 1 of motion detection is enabled. |
| 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_wled_i<0~(nwled-1)>_enable | 0, 1 | 6/6 | Enable or disable trigger white light LED. |
| action_wled_i<0~(nwled-1)>_duration | 1~999 | 6/6 | Duration of the white light LED trigger in seconds. |
| action_server_i<0~4>_enable | 0, 1 | 6/6 | Enable or disable this server action. |
| action_server_i<0~4>_media | NULL, 0~4,101 | 6/6 | Index of the attached media. 101: recording notify |

| | | | |
|---------------------------------|-----------|-----|--|
| action_server_i<0~4>_datefolder | <boolean> | 6/6 | Enable this to create folders by date, time, and hour automatically. |
|---------------------------------|-----------|-----|--|

7.27 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. |

7.28 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. |
| 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 ~ 5000 | 6/6 | Maximum size of one video clip file in Kbytes. |

Group: **media_i101** (can't be modified by user)

| PARAMETER | VALUE | SECURITY (get/set) | DESCRIPTION |
|-----------|------------|-----------------------|--|
| name | string[40] | 6/7 | Identification of this entry |
| type | recordmsg | 6/7 | Media type to send to the server or store on the server. |

7.29 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 | 0~2 | 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 | 16~ | 6/6 | The maximum size for cycle recording in Kbytes when choosing to limit recording size. |
| reserveamount | 0~15000000 | 6/6 | The reserved amount in Mbytes when choosing cyclic recording mechanism. |
| dest | 0 | 6/6 | The destination to store the recorded data. “0” means the index of the network storage. |
| adaptive_enable | 0,1 | 6/6 | Indicate whether the adaptive recording is enabled |
| adaptive_preevent | 0~9 | 6/6 | Indicate when is the adaptive recording started before the event trigger point (seconds) |
| adaptive_postevent | 0~10 | 6/6 | Indicate when is the adaptive recording stopped after the event trigger point (seconds) |

7.30 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 | 6/6 | Specify the https status. -3 = Certificate not installed -2 = Invalid public key -1 = Waiting for certificate 0 = Not installed 1 = Active |
| countryname | string[2] | 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 ~ 9999 | 6/6 | Valid period for the certification. |

7.31 Region of interest

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

In this model only stream0 support ROI

| PARAMETER | VALUE | SECURITY (get/set) | DESCRIPTION |
|-----------------|--------------|-----------------------|---|
| s<0~(m-1)>_home | 0,0~1104~656 | 1/6 | ROI left-top corner coordinate. |
| s<0~(m-1)>_size | 176x144~ | 1/6 | ROI width and height. The width value must be multiples of 16 and the height value must be multiples of 8 |

7.32 Express link

Group: **expresslink**

| PARAMETER | VALUE | SECURITY (get/set) | DESCRIPTION |
|-----------|--|-----------------------|--|
| 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 |

7.33 White light LED

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

| PARAMETER | VALUE | SECURITY (get/set) | DESCRIPTION |
|-------------------|-------|-----------------------|--|
| on_mode | 0,1 | 1/6 | The style to turn on white light LED. 0: Directly. 1: Fade in. |
| off_mode | 0,1 | 1/6 | The style to turn off white light LED. 0: Directly. 1: Fade out. |
| direct_brightness | 1~100 | 1/6 | Brightness percentage of white light LED to reach as on_mode is 0. |
| fade_brightness | 1~100 | 1/6 | Brightness percentage of white light LED to reach as on_mode is 1. |

7.34 Audio clip

Group: **audioclip_i<0~19>**

| PARAMETER | VALUE | SECURITY (get/set) | DESCRIPTION |
|-----------|------------|-----------------------|------------------------------------|
| name | string[40] | 1/6 | Identification of this audio clip. |
| location | <string> | 1/6 | Saved location of this audio clip. |
| size | <integer> | 1/6 | Size of this audio clip. |

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
do l=1\r\n
```

8.4 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) | 1 | 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>
```

8.5 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 for 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. |

8.6 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
```

8.7 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.

8.8 IP Filtering

Note: This request requires Administrator access privileges.

Method: GET/POST

Syntax:

```
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 <i><return page></i> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. |
|--|--|--|

8.9 Event/Control HTTP Tunnel Channel (**capability.**

evctrlchannel > 0)

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

Method: GET and POST

Syntax:

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

```
-----
```

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

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

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

```
pragma: no-cache
```

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

```
-----
```

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

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

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

```
pragma : no-cache
```

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

```
content-length: 32767
```

```
expires: Sun, 9 Jan 1972 00:00:00 GMT
```

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

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

See Event/control tunnel spec for detail information

8.10 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.

8.11 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.

8.12 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] | Ex: vi0=1 Setting virtual input 0 to trigger state |
| | Where "state" is 0, 1. "0" means inactive or normal state while "1" means active or triggered state. Where "nstate" is next state after duration. | Ex: vi0=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, 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: 1. setvi.cgi?vi0=0(10000)1(15000)0(20000)1 No multiple duration. 2. setvi.cgi?vi3=0 VI index is out of range. 3. setvi.cgi?vi=1 No VI index is specified. |
| 503 | The resource is unavailable, ex. Virtual input is waiting for next state. |

Examples:

1. setvi.cgi?vi0=0(15000)1

2. setvi.cgi?vi0=1

Request 2 will not be accepted during the execution time(15 seconds).

Technical Specifications

| | | | |
|----------------------|--|---|--|
| Models | <ul style="list-style-type: none"> · IP8132 (Wired) · IP8133 (PoE) · IP8133W (WLAN) | Alarm and Event Management | <ul style="list-style-type: none"> · Triple-window video motion detection · Tamper detection · One D/I and one D/O for external sensor and alarm · PIR (Passive Infrared Sensor) for human detection (IP8133/33W) · White-light illuminators when event triggered (IP8133/33W) · Event notification using HTTP, SMTP or FTP · Local recording of MP4 file |
| System | <ul style="list-style-type: none"> · CPU: Mozart 365 SoC · Flash: 16MB · RAM: 128MB · Embedded OS: Linux 2.6 | On-board Storage (IP8133/33W) | <ul style="list-style-type: none"> · MicroSD/SDHC card slot · Stores snapshots and video clips |
| Lens | <ul style="list-style-type: none"> · Board lens, Fixed, f = 3.45 mm, F2.4 | Security | <ul style="list-style-type: none"> · Multi-level user access with password protection · IP address filtering · Wireless: WEP, WPA-PSK, WPA2 (IP8133W) · WPS - Wi-Fi Protected Setup (IP8133W) · HTTPS encrypted data transmission |
| Angle of View | <ul style="list-style-type: none"> · 47.4° (horizontal) · 30.6° (vertical) · 54.7° (diagonal) | Users | <ul style="list-style-type: none"> · Live viewing for up to 10 clients |
| Shutter Time | <ul style="list-style-type: none"> · 1/5 sec. to 1/25,000 sec. | Dimension | <ul style="list-style-type: none"> · 32 mm (D) x 79 mm (W) x 80 mm (H) |
| Image Sensor | <ul style="list-style-type: none"> · 1/4" CMOS sensor in 1280x800 resolution | Weight | <ul style="list-style-type: none"> · Net: 180 g (IP8132) · Net: 200 g (IP8133) · Net: 195 g (IP8133W) |
| Minimum Illumination | <ul style="list-style-type: none"> · 3.0 Lux / F2.4 | LED Indicator | <ul style="list-style-type: none"> · System power and status indicator · System activity and network link indicator · Privacy button on |
| Video | <ul style="list-style-type: none"> · Compression: H.264, MJPEG & MPEG-4 · Streaming: <ul style="list-style-type: none"> Multiple simultaneous streams H.264 streaming over UDP, TCP, HTTP or HTTPS MPEG-4 streaming over UDP, TCP, HTTP or HTTPS MPEG-4 multicast streaming MJPEG streaming over HTTP or HTTPS · Supports activity adaptive streaming for dynamic frame rate control · Supports 3GPP mobile surveillance · Frame rates: <ul style="list-style-type: none"> H.264: Up to 30 fps at 1280x800 MPEG-4: Up to 23 fps at 1280x800 MJPEG: Up to 30 fps at 1280x800 | Power | <ul style="list-style-type: none"> · 5V DC · Power consumption: Max. 3.4 W (IP8132) · Power consumption: Max. 4.3 W (IP8133) · Power consumption: Max. 4.7 W (IP8133W) · 802.3af compliant Power-over-Ethernet (Class 3) (IP8133) |
| Image Settings | <ul style="list-style-type: none"> · 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 · BLC (Backlight Compensation) · Supports privacy masks | Approvals | <ul style="list-style-type: none"> · CE, LVD, FCC, VCCI, C-Tick |
| Audio | <ul style="list-style-type: none"> · Compression: <ul style="list-style-type: none"> GSM-AMR speech encoding, bit rate: 4.75 kbps to 12.2 kbps G.711 audio encoding, bit rate: 64 kbps, μ-Law or A-Law mode selectable · Interface: <ul style="list-style-type: none"> Built-in microphone (IP8132/33/33W) Built-in speaker (IP8133/33W) · Supports two-way audio via SIP protocol (IP8133/33W) · Supports audio mute | Operating Environments | <ul style="list-style-type: none"> · Temperature: 0 ~ 40C (32 ~ 104°F) · Humidity: 90% RH |
| Networking | <ul style="list-style-type: none"> · 10/100 Mbps Ethernet, RJ-45 · Built-in 802.11b/g/n WLAN (IP8133W) · Onvif support · Protocols: IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, and SNMP | Viewing System Requirements | <ul style="list-style-type: none"> · 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 | <ul style="list-style-type: none"> · Installation Wizard 2 · 32-CH ST7501 recording software · Supports firmware upgrade |
| | | Applications | <ul style="list-style-type: none"> · SDK available for application development and system integration |
| | | Warranty | <ul style="list-style-type: none"> · 24 months |

Technology License Notice

MPEG-4 Visual Technology

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

AMR-NB Standard

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

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

Electromagnetic Compatibility (EMC)

FCC Statement

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

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

CE Mark Warning

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

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）の基準に基づくクラス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.

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

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

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

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

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>