TOSHIBA

Leading Innovation

NETWORK CAMERA

Model: IK-WB70A

User's Manual

For information on our latest products and peripheral devices, refer to the following Website:

■ http://www.toshibasecurity.com

The above URL is subject to change without prior notice.
If the URL changes, refer to the Toshiba website (http://www.toshiba.com).

FCC (USA)-INFORMATION

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

USER-INSTALLER CAUTION: Your authority to operate this FCC verified equipment could be voided if you make changes or modifications not expressly approved by the party.

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

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme
NMB-003 du Canada

Thank you for purchasing the IK-WB70A Network Camera. Before you start using the camera, read this User's Manual carefully to ensure correct usage. Once you have finished reading this User's Manual, keep it in a convenient place for future reference.

The design, specifications, software, and User's Manual contents are subject to change without prior notice.

Terms and Trademarks

- The term "OS" is used in this User's Manual to indicate operating systems compatible with this product.
  - Windows® XP: Microsoft® Windows® XP operating system
  - Windows Vista®: Microsoft® Windows Vista® Business operating system
- The formal name of Windows® is Microsoft® Windows® Operating System.
- Microsoft®, Windows®, and Windows Vista® are trademarks or registered trademarks of Microsoft® Corporation in the United States and other countries.
- Adobe is a registered trademark and Adobe Reader is a trademark of Adobe Systems Incorporated.
- Other product names appearing in this User's Manual may be trademarks or registered trademarks of their respective holders.

NOTE

- This network camera might not operate correctly depending on the network environment.

IMPORTANT SAFEGUARDS

1. Read Instructions
   Read all the safety and operating instructions before operating the product.
2. Retain Instructions
   Retain the safety instructions and user's manual for future reference.
3. Warnings
   Comply with all warnings on the product and in the user's manual.
4. Follow Instructions
   Follow all operating and use instructions.
5. Cleaning
   Disconnect this video product from the power supply before cleaning.
6. Attachments
   Do not use attachments not recommended by the video product manufacturer as they may cause hazards.
7. Accessories
   Do not place this video product on an unstable cart, stand, tripod, bracket or table. The video product may fall, causing serious injury to a person, or serious damage to the product. Use only with stand, tripod, bracket, or table recommended by the manufacturer, or sold with the video product. Any mounting of the product should follow the manufacturer's instructions, and should use a mounting accessory recommended by the manufacturer.
8. Ventilation
   This video product should never be placed near or over a radiator or heat register. If this product is placed in a built in installation verify that there is proper ventilation so that the camera temperature operates within the recommended temperature range.
9. Power Sources
   This video product should be operated only from the type of power source indicated on the information label. If you are not sure of the type of power supply at your location, consult your product dealer.
10. Power-Cord Protection
    Power cords should be routed so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords at plugs, screws and the point where they exit the product.
11. Installation
    Install this video product on a secure part of the ceiling or wall. If installed on an unsecured location, the camera could fall causing injury and damage.
12. Lightning
    For additional protection on this video product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet and disconnect the power supply and cable system. This will prevent damage to the video product due to lightning and power-line surges. If lightning occurs, do not touch the unit or any connected cables in order to avoid electric shock.
13. Overloading
    Do not overload the power supply or extension cords as this can result in a risk of fire or electric shock.
14. Object and Liquid Entry
    Never push objects of any kind into this video product through openings as they may touch dangerous electrical points or short-out parts that could result in a fire or electrical shock. Never spill liquid of any kind on the video product.
15. Servicing
    Do not attempt to service this video product yourself as opening or removing covers may expose you to dangerous electrical or other hazards. Refer all servicing to qualified service personnel.
16. Damage Requiring service
    Disconnect this video product from the power supply and refer servicing to qualified service personnel under the following conditions.
    a. When the power-supply cord or plug is damaged.
    b. If liquid has been spilled, or objects have fallen into the video product.
    c. If the video product has been submerged in water.
    d. If the video product does not operate normally by following the operating instructions in the user's manual. Adjust only those controls that are covered by the user's manual as an improper adjustment of other controls may result in damage and will often require extensive work by a qualified technician to restore the video product to its normal operation.
    e. If the video product has been dropped or the cabinet has been damaged.
    f. When the video product exhibiting a distinct change in performance which indicates a need for service.
17. Replacement Parts
    When replacing parts be sure the service technician uses parts specified by the manufacturer or have the same characteristics as the original part. Unauthorized substitutions may result in fire, electric shock or other hazards.
18. Safety Check
    Upon completion of any service or repairs to this video product, ask the service technician to perform safety checks to determine that the video product is in proper operating condition.

CAUTION TO REDUCE THE RISK OF ELECTRIC SHOCK.
DO NOT REMOVE COVER. NO USER SERVICEABLE PARTS INSIDE.
REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.

The lightning flash with arrowhead symbol, within an equilateral triangle, is intended to alert the user to the presence of uninsulated "dangerous voltage" within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

WARNING:
TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT SUBMERGE THIS CAMERA IN WATER.

FIELD INSTALLATION MARKING:
WORDED : “THIS INSTALLATION SHOULD BE MADE BY A QUALIFIED SERVICE PERSON AND SHOULD CONFORM TO ALL LOCAL CODES.”

NOTES ON USE AND INSTALLATION

- **Do not aim the camera at the sun**
  Never aim the camera at the sun even with the camera power off.
- **Do not shoot intense light**
  Intense light such as a spotlight may cause a bloom or smear. A vertical stripe may appear on the screen. However, this is not a malfunction.
- **Treat the camera with care**
  Dropping or subjecting the camera to intense vibration may cause it to malfunction.
- **Never touch internal parts**
  Do not touch the internal parts of the camera other than the parts specified.
- **Do not submerge in water**
  The camera has some protection to water (see IP rating), and can be used indoors or outdoors.
  If the camera was submerged in water, turn off the power and contact your dealer.
- **Keep the camera installation away from video noise**
  If cables are wired near electric lighting wires or a TV set, noise may appear in images. In this event relocate cables or reinstall equipment.
- **Check the ambient temperature and humidity**
  Avoid using the camera where the temperature is hotter or colder than the specified operating range. Doing so could affect the internal parts or cause the image quality to deteriorate. Special care is required to use the camera at high temperature and humidity.
- **Should you notice any trouble**
  If any trouble occurs while you are using the camera, turn off the power and contact your dealer. If you continue to use the camera when there is something wrong with it, the trouble may get worse and an unpredictable problem may occur.

Precautions for Use

Disclaimer

We disclaim any responsibility and shall be held harmless for any damages or losses incurred by the user in any of the following cases:

1. Fire, earthquake or any other act of God; acts by third parties; misuse by the user, whether intentional or accidental; use under extreme operating conditions.
2. Malfunction or non-function resulting in indirect, additional or consequential damages, including but not limited to loss of expected income and suspension of business activities.
3. Incorrect use not in compliance with instructions in this user's manual.
4. Malfunctions resulting from misconnection to other equipment.
5. Repairs or modifications made by the user or caused to be made by the user and carried out by an unauthorized third party.
6. Notwithstanding the foregoing, Toshiba's liabilities shall not, in any circumstances, exceed the purchase price of the product.

Copyright and Right of Portrait

There may be a conflict with the Copyright Law and other laws when a customer uses, displays, distributes, or exhibits an image picked up by the camera without permission from the copyright holder. Please also note that transfer of an image or file covered by copyright is restricted to use within the scope permitted by the Copyright Law.

Protection of Personal Information

Images taken by the camera that reveal the likeness of an individual person may be considered personal information. To disclose, exhibit or transmit those images over the internet or otherwise, consent of the person may be required.

Usage Limitation

The product is not designed for any "critical applications." "Critical applications" means life support systems, exhaust or smoke extraction applications, medical applications, commercial aviation, mass transit applications, military applications, homeland security applications, nuclear facilities or systems or any other applications where product failure could lead to injury to persons or loss of life or catastrophic property damage.
Accordingly, [Toshiba/TAIS] disclaims any and all liability arising out of the use of the product in any critical applications.

AC adapter

Be sure to use only the supplied AC adapter. Using a different AC adapter may cause the camera to malfunction, heat up, or catch fire. Before using the AC adapter, carefully read and observe the Important Safety Instructions (→page 4) and the notes below.

- Plug the AC adapter into the 100-240 VAC outlet.
  If inserting it into other than 100-240 VAC outlet, it may result in electric shock or fire hazard.
- Do not repair, modify or disassemble the AC adapter. It may result in electric shock or fire hazard.
- Keep the blades of Plug free from any dust or dirt. Neglecting to do so may cause a fire due to deterioration of the insulation. Pull out the power plug from the outlet before cleaning the blades.
- Do not cover or wrap the AC adapter with a cloth or place it near heating devices. It may cause fire or malfunction of the unit.
- Protect the power cord from being:
  - damaged, modified for extension, or applied heat.
  - pulled, put heavy objects, or pinched.
  - bent, twisted extremely, or bundle.

  Neglecting to do so may cause electric shock or fire hazard.
- Do not expose this AC adapter to water.
- Install the AC adapter properly on a wall or ceiling after plugging in the AC adapter. Avoid dropping the AC adapter, failing to do so may cause serious personal injury or death.
- Do not allow the connectors on the AC adapter to come into contact with any other metal object as this may result in short circuit.
- To connect the AC adapter, firmly insert the plug end of the cable into the AC adapter jack. Do not insert the plug into other jacks as this may cause a malfunction.
- When removing the connection cable, disconnect the cable by holding its plug. Do not disconnect the cable by pulling on the cable.
- Do not drop the AC adapter or subject it to strong impact.
- Do not use the AC adapter in hot and humid places.
- Do not use the supplied AC adapter with devices other than this camera.
- Temperature increasing on the surface of the adapter is normal. Before moving the adapter to another location, unplug it from the wall outlet, and wait until its temperature decreases.
- Buzzing noises may come from inside. This does not indicate malfunction.
- Using the AC adapter near a radio, TV, or cellphone may cause interference. Use the adapter at sufficient distances from these devices.
- Be sure to use the supplied AC adapter. Using different AC adapter may cause fire hazard or the camera to malfunction.

Specifications

AC adapter (DSA-20P-10)

Power source	: 100-240 VAC 50/60 Hz
Rated output	: 12 VDC, 1.5 A
Ambient temperature guaranteed for performance	: 32°F to 104°F (0℃ to 40℃)
Storage temperature	: -4°F to 140°F (-20℃ to 60℃)
Maximum external dimensions	: 1.42 x 1.85 x 2.93 inches (36 x 47 x 74.5 mm) (width x height x depth)
Cord length	: 72 inches (1828 mm)

Table of Contents

Introduction

Installation

How to Use

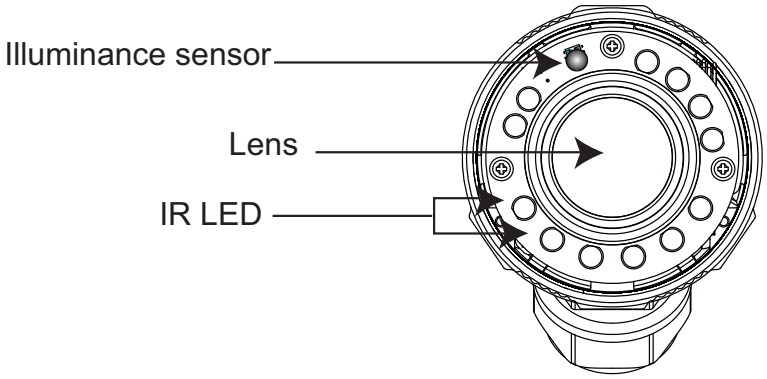
Configuration Definitions

Appendix

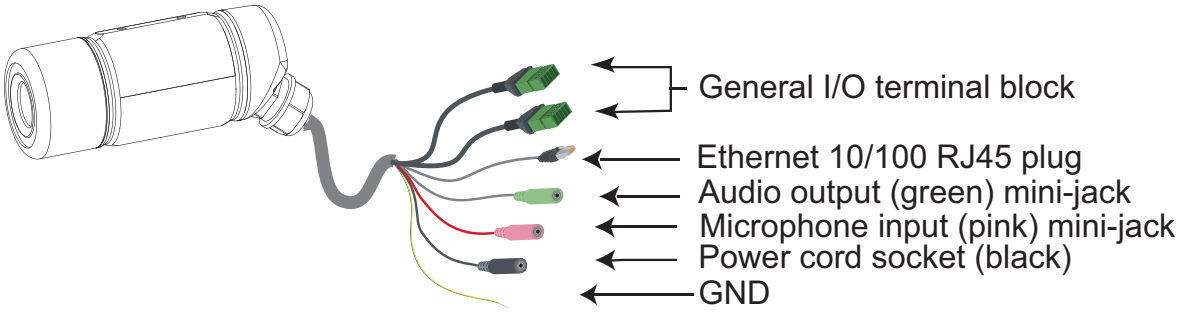
Contents

Physical description

Front panel



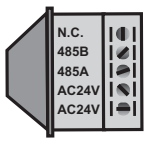
Connectors



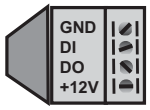
Cable length: approx. 39 inches (1000 mm)

General I/O Terminal Block

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

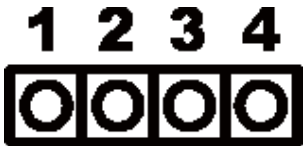


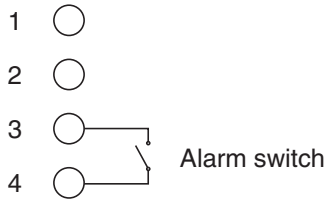
N.C.: No Connector
485B: RS485-
485A: RS485+
AC24V: 24 VAC Power Input
AC24V: 24 VAC Power Input



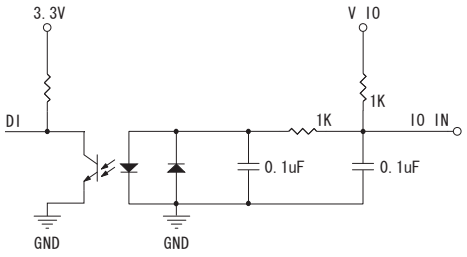
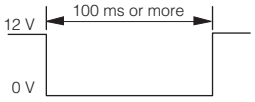
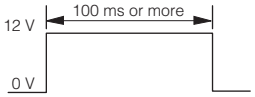
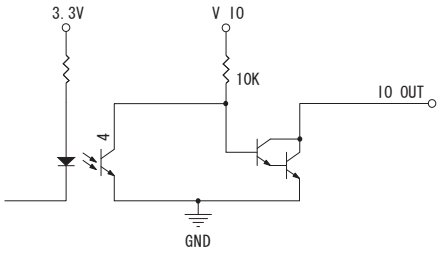
GND: Ground
DI : Digital Input
DO : Digital Output
+12V : 12 VDC Output

Pin	Name	Specification
N.C.	No Connector	
485B	RS485-	3.3 V
485A	RS485+	3.3 V
AC24V	24 VAC Power Input	24 VAC ± 10 %
AC24V	24 VAC Power Input	24 VAC ± 10 %
GND	Ground	
DI	Digital Iutput	OPEN/Short-to-GND, isolation 2 kV
DO	Digital Output	Max. 12 VDC, max. 400 mA, isolation 2 kV
+12V	12 VDC Output	12 VDC ± 10 %, max. 0.4A



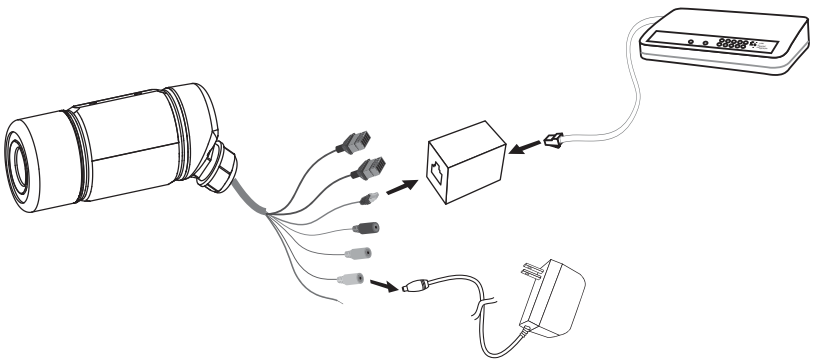


1: +12 V 12 VDC Output
2: DO Digital Output
3: DI Digital Input
4: GND Ground
The connection definition is as below when "Digital input" is used for alarm input.

	Internal Circuit	Signal Condition
Digital Input		Active state is low.  Active state is high. 
Digital Output		MAX. 12 VDC, 400 mA

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

Hardware installation



Please verify that your product package contains all the accessories listed in the Package Contents listed on page 11. Depending on the user's application, an Ethernet cable may be needed. The Ethernet cable should meet the specs of UTP Category 5.

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

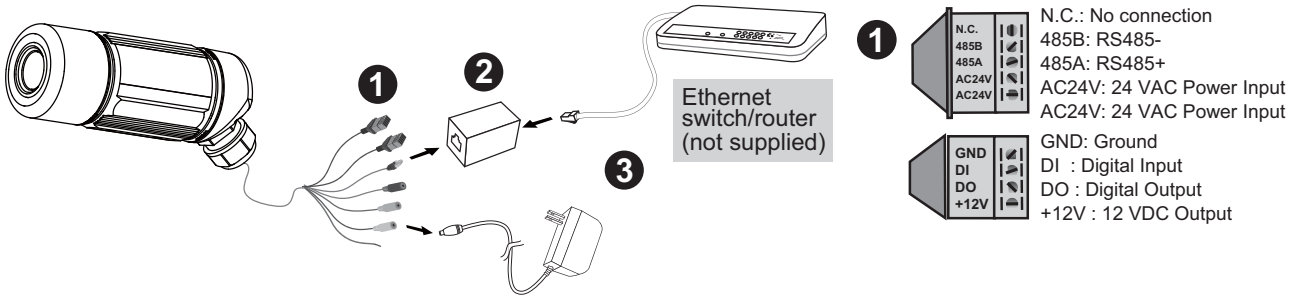
Refer to the Quick Start Guide for details for hardware installation.

Network deployment

Setup 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 connection from general I/O terminal block.
2. Use the supplied RJ45 female/female coupler to connect the Network Camera to a network port via an Ethernet cable. Use Category 5 Cross Cable when the Network Camera is directly connected to a PC.
3. Connect the power cord socket from the Network Camera to the supplied AC adapter.

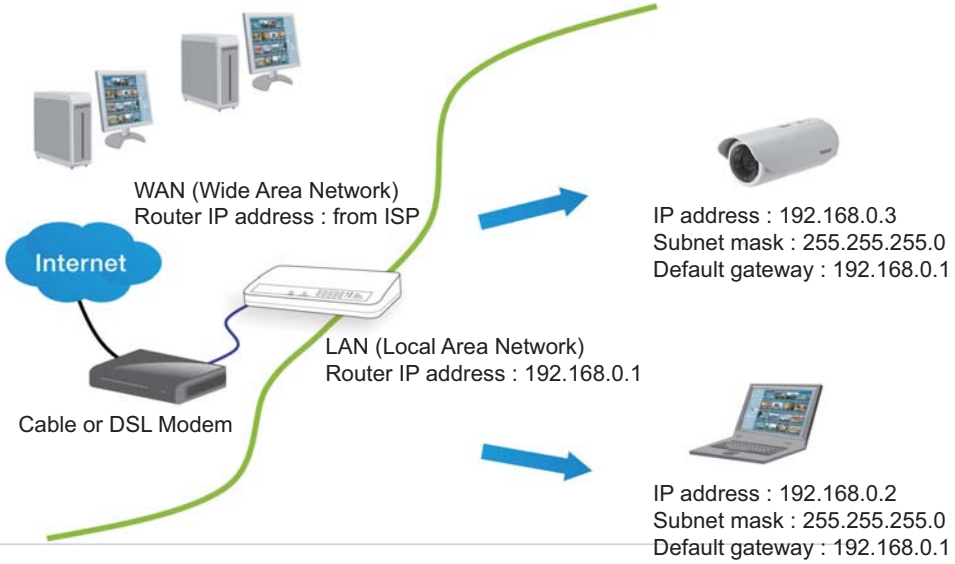


There are three ways to setup the Network Camera over the Internet. The first way is to setup the Network Camera behind a gateway. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet connection via a gateway

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

1. Connect your Network Camera behind a gateway, a network environment example is illustrated as below. Regarding how to get your IP address, refer to Software installation on page 18 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 gateway.
   - ■ HTTP port
   - ■ RTSP port
   - ■ RTP port for audio
   - ■ RTCP port for audio
   - ■ RTP port for video
   - ■ RTCP port for video

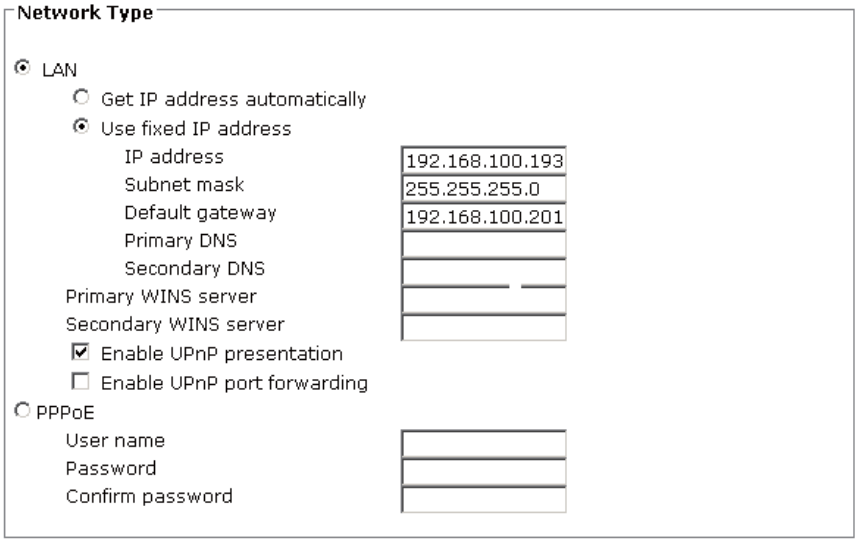
If you have changed the port numbers on the Network page, please open the ports accordingly on your gateway. For information on how to forward ports on the gateway, please refer to the gateway user's manual.

3. Find out the public IP address of your gateway 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 and follow the steps below.

1. Set up the Network Camera in a LAN. Please refer to Software installation on page 18 for details.
2. Go to Configuration > Network > Network Type. Select LAN > Use fixed IP address.
3. Enter the static IP, Subnet mask, Default gateway, Primary DNS provided by your ISP.



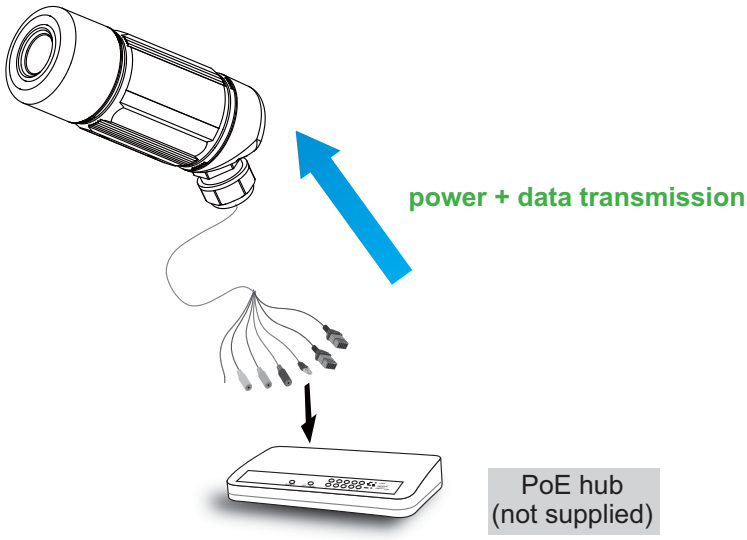
Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 36 for details.

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

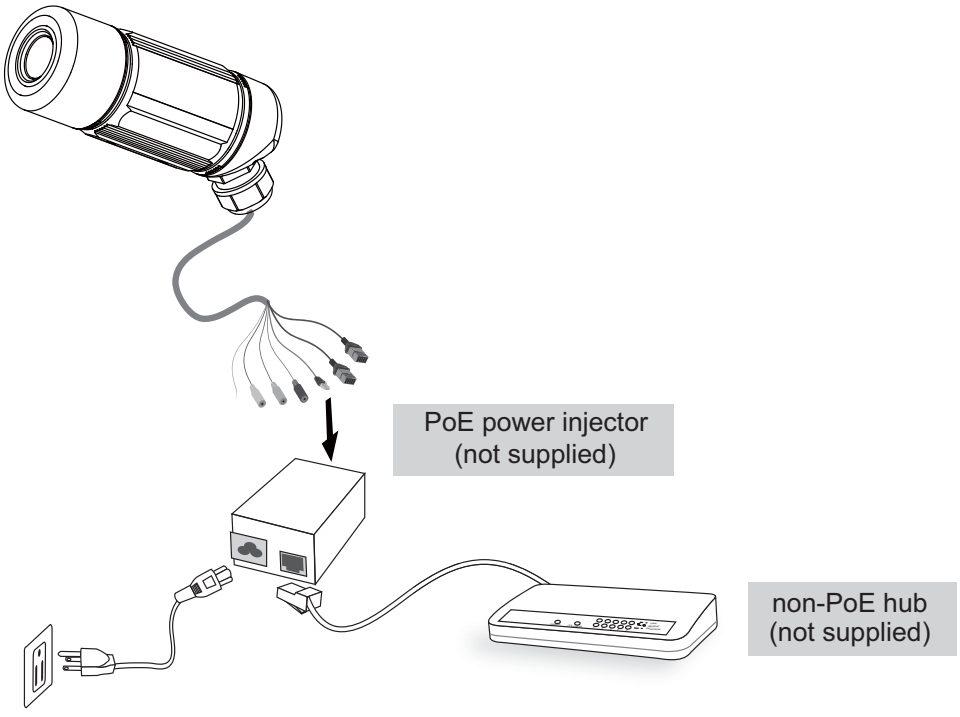
When using a PoE hub

The Network Camera is PoE-compliant, which allows it to be powered via a single Ethernet cable. If your hub or gateway supports PoE, refer to the following illustration to connect the Network Camera to a PoE hub/gateway via an Ethernet cable.



When using a non-PoE hub

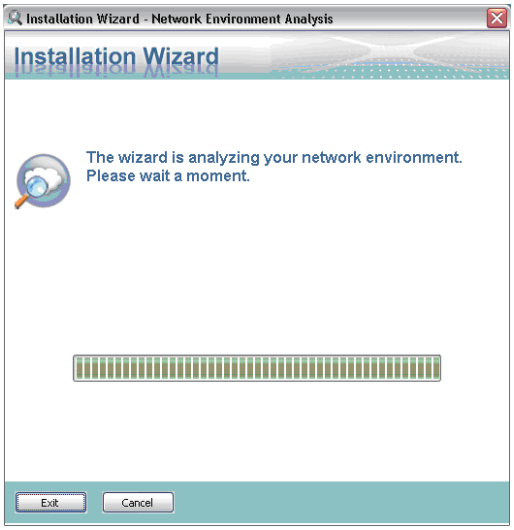
If your hub or gateway does not support PoE, use a PoE power injector (not supplied) to connect between the Network Camera and a non-PoE hub or gateway.

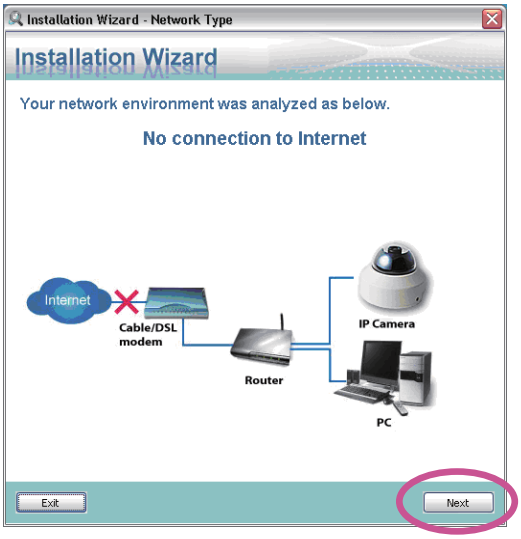


Software installation

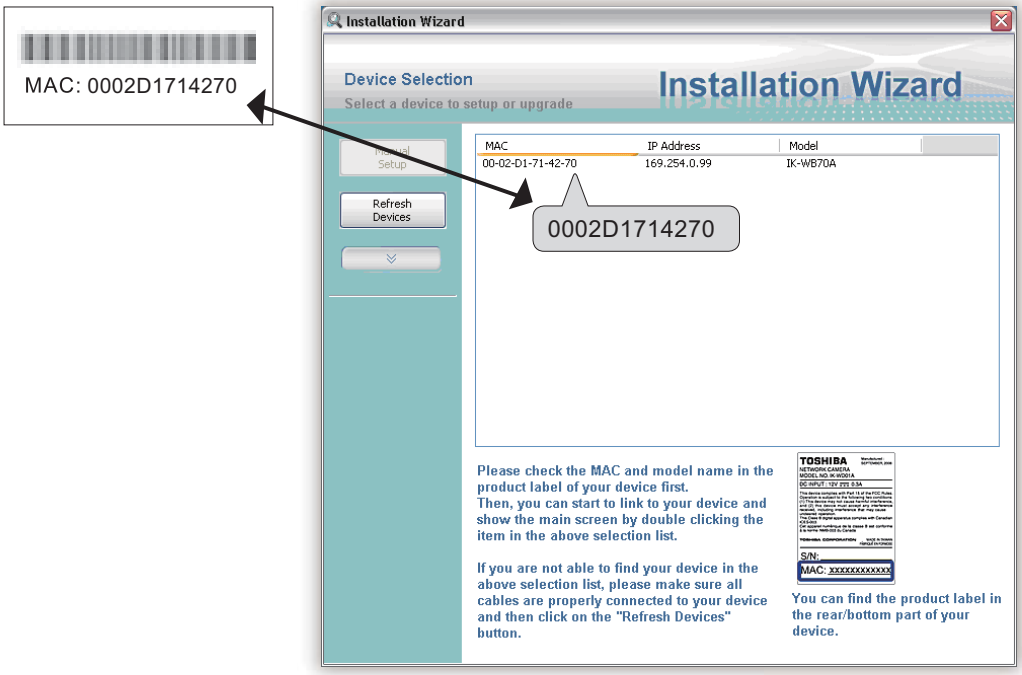
Installation Wizard (IW), a free-bundled software packaged in the product CD, helps to set up your Network Camera in a LAN.

1. Install the IW under the Software Utility directory from the software CD. Double click the IW shortcut on your desktop to launch the program.
2. The program will analyze network environment. After your network environment is analyzed, please click Next to continue the program.





3. The program will search for Network Cameras on the same LAN.
4. After searching, the main installer window will pop up. Click on the MAC and model name which match the MAC attached the camera to connect to the Network Camera.

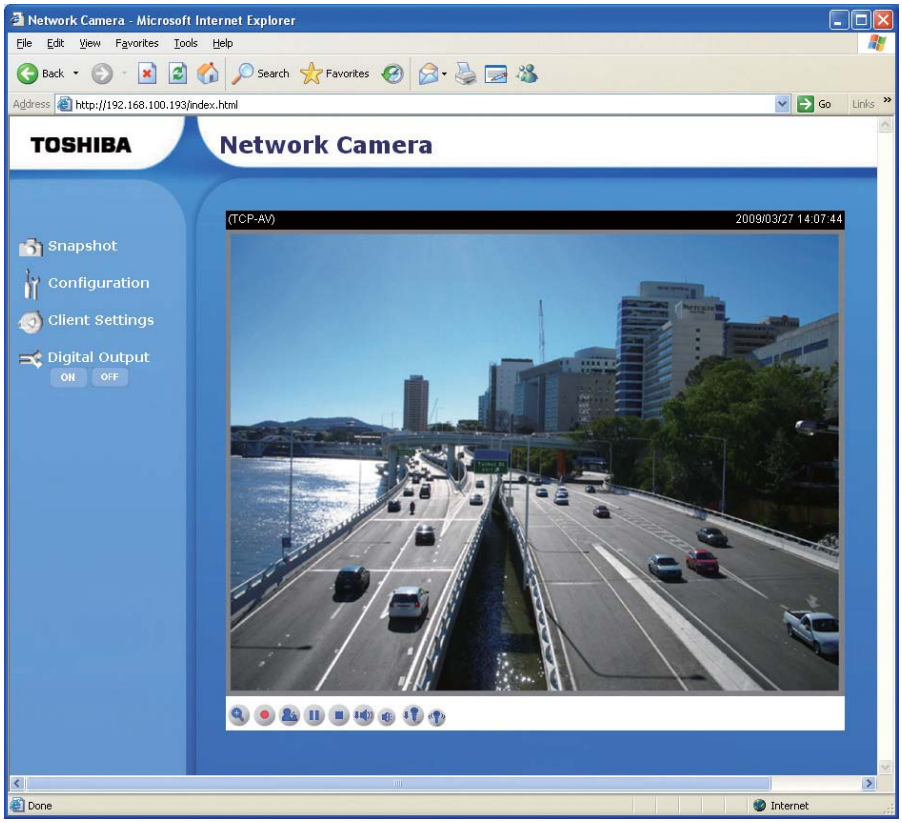


Initial Access to the Network Camera

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

Using web browsers

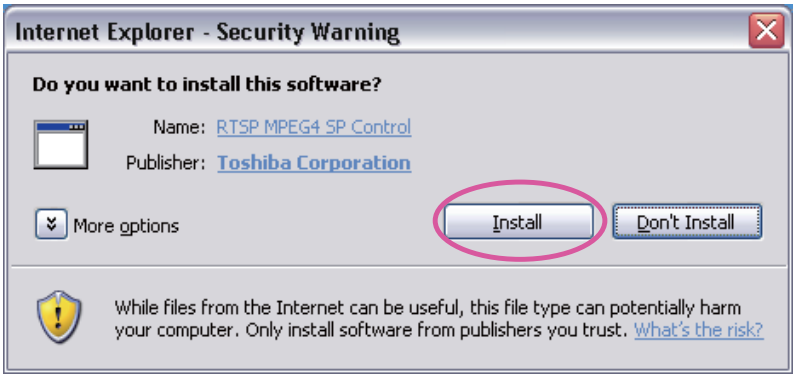
1. Launch your web browser (ex. Microsoft® Internet Explorer®).
2. Enter the IP address of the Network Camera in the address field. Press Enter.
3. The live video will be displayed in your web browser.



Initial Access to the Network Camera (Cont.)

NOTE

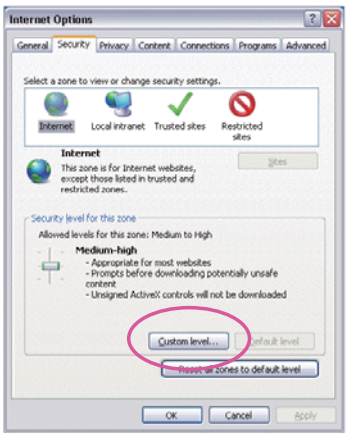
- By default, the Network Camera is not password-protected. To prevent unauthorized accesses, it is highly recommended to set a password for the Network Camera. For more information about how to enable password protection, please refer to Security Settings on page 30.
- If you see a warning message at initial access, click Install to install an ActiveX® control on your computer.



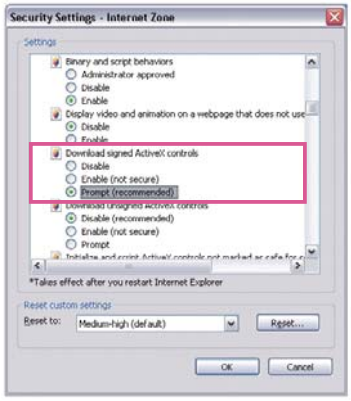
This page applies to Windows® XP. It is also applicable for Windows Vista® Business.

- If you see a dialog box indicating that your security settings prohibit running ActiveX® controls, please enable your ActiveX® controls for your browser.

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



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



Using 3GPP-compatible mobile devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed from the Internet. For more information on how to set up the Network Camera over the Internet, refer to Setup the Network Camera over the Internet on page 15.

To utilize this feature, check the following settings on your Network Camera:

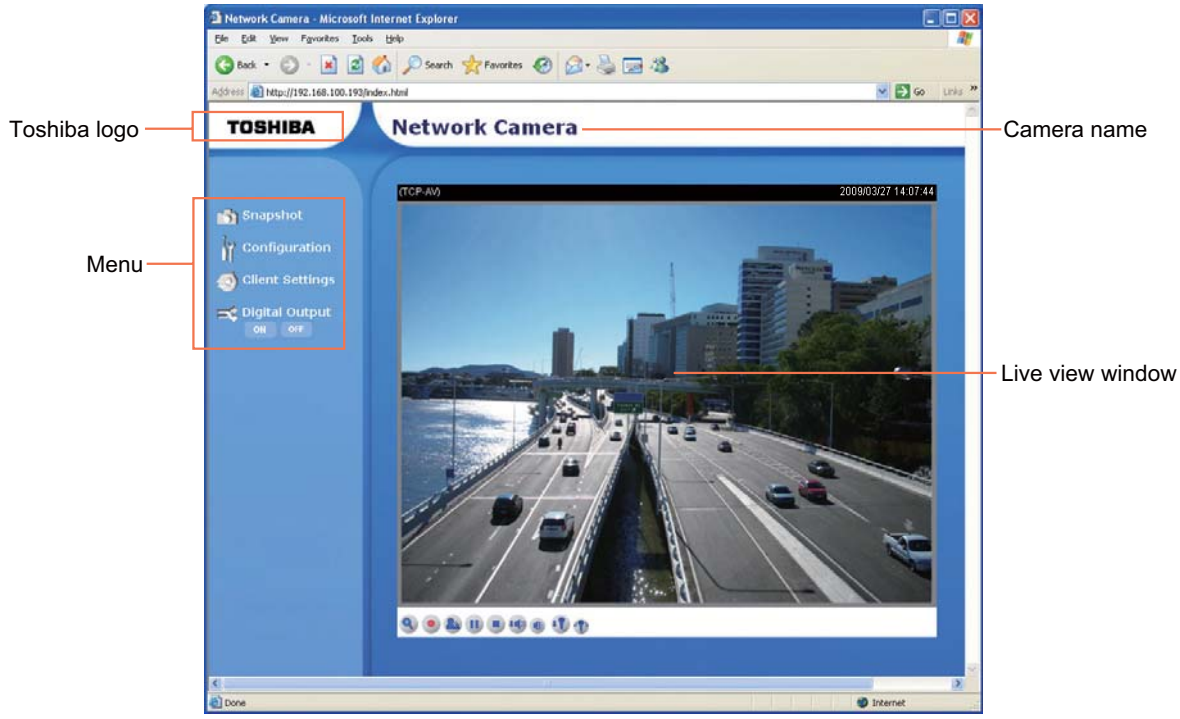
1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable. For more information, refer to RTSP Streaming on page 41.
2. As the 3G network bandwidth is limited, you can not use large video size. Set the video and audio streaming parameters as listed below.
   For more information, refer to Audio and video on page 45.

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

3. As most ISP and players only support port number 554 to allow RTSP streaming to go through, set the RTSP port to 554.For more information, refer to RTSP Streaming on page 41.
4. Launch the players on 3GPP-compatible mobile devices.
   Type the URL commands in the player.
   The format is rtsp://<public ip address of your camera>:<rtsp port>/<access name for stream1 or stream2>.

Main Screen with Camera View

This chapter explains the layout of the main page. It is composed of the following four sections:
Toshiba logo, Menu, Camera Name, and Live Video Window.



Toshiba Logo

Click this logo to visit the Toshiba website.

Menu

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.

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

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

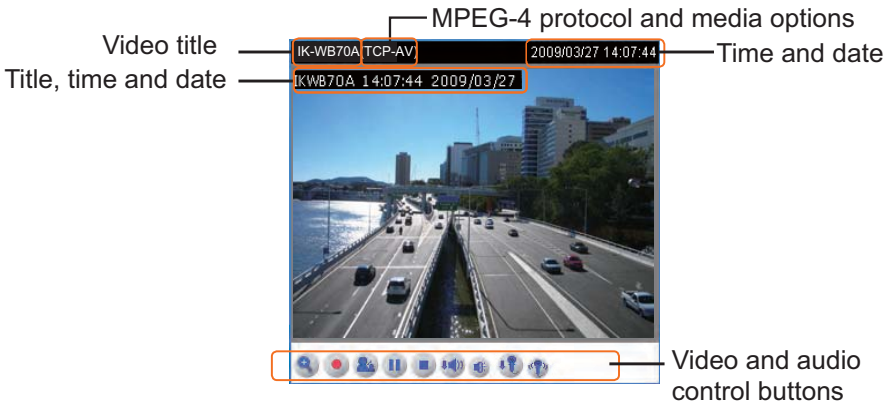
Digital Output: Click this button to turn the digital output device on or off.

Camera Name

The camera name can be customized. For more information, refer to System Parameters on page 28.

Live Video Window

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



Video title: The video title can be configured. For more information, refer to Video settings on page 45.

Time and date: Display the current time. For more information, refer to Video settings on page 45.

Title, time and date: Video title, time and date can be stamped on the streaming video. For more information, refer to Video settings on page 45.

MPEG-4 protocol and media options: The transmission protocol and media options for MPEG-4 video streaming. For more information, refer to Client Settings on page 26.

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

Digital zoom edit: Deselect Disable digital zoom to enable the zoom operation. The navigation screen indicates which part of the image is 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.

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 quit the web browser, video recording stops accordingly. To specify the storage destination and the file name, please refer to MP4 Saving Options on page 27 for details.

Talk: Click this button to talk to people around the Network Camera. Audio will come out from the external speaker connected to the Network Camera.

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

Main Screen with Camera View (Cont.)

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

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

Volume: When the mute function is not activated, move the slider bar to adjust the volume at the client computer.

Mute: Turn off the volume at the client computer.

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

Mute: Turn off the microphone volume at the client computer.

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

Video title: The video title can be configured. For more information, refer to Video settings on page 45.

Time and date: Displays the current time and date. For more information, refer to Video settings on page 45.

Title, time and date: Video title time and date can be stamped on the streaming video. For more information, refer to Video settings on page 45.

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

Digital zoom edit: Deselect Disable digital zoom to enable the zoom operation. The navigation screen indicates which part of the image is 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.

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 quit the web browser, video recording stops accordingly. To specify the storage destination and the file name, refer to MP4 Saving Options on page 27 for details.

Talk: Click this button to talk to people around the Network Camera. Audio will come out from the external speaker connected to the Network Camera.

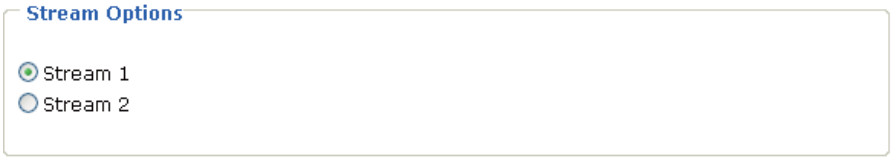
Mic Volume: When the mute function is not activated, move the slider bar to adjust the microphone volume at the client computer.

Mute: Turn off the microphone volume at the client computer.

Client Settings

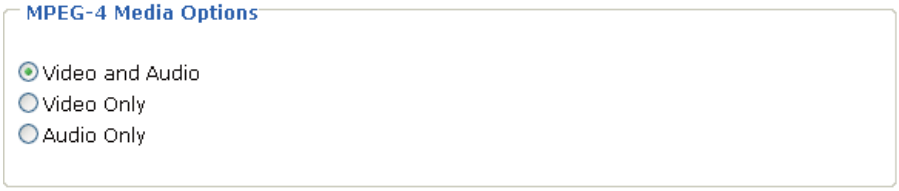
This chapter explains how to select the streaming source, transmission mode and saving options at the client computer. It is composed of the following four sections: Stream Options, MPEG-4 Media Options, MPEG-4 Protocol Options and MP4 Saving Options. When completed with the settings on this page, click Save on the bottom of the page to take effect.

Stream Options



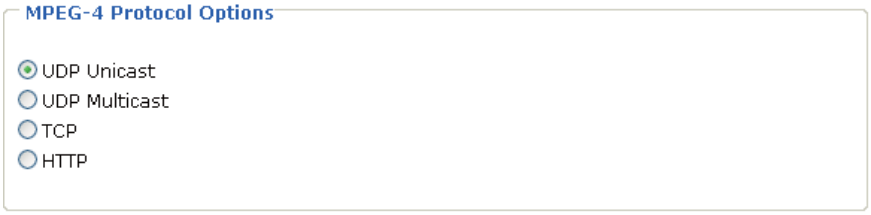
The Network Camera supports MPEG-4 and MJPEG dual streams. For more information, refer to Video settings on page 45.

MPEG-4 Media Options



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

MPEG-4 Protocol Options



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

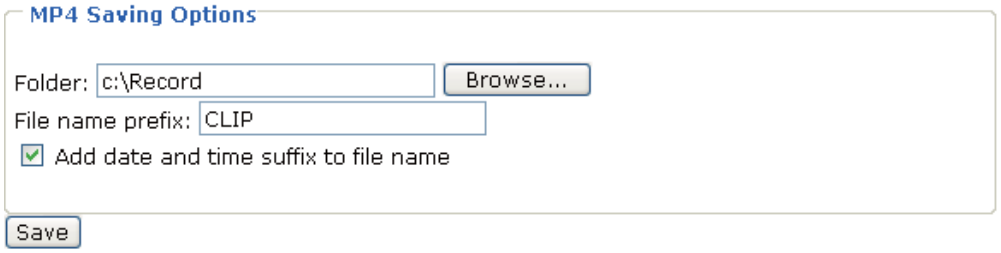
UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast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

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, see RTSP Streaming on page 41.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. The downside with 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 and you do not need to open specific port for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data to come through.

MP4 Saving Options

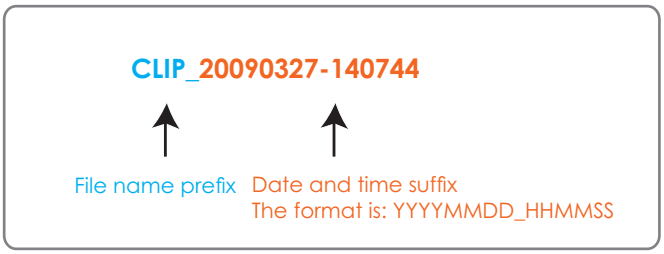


Users can record the live video as they are watching it by clicking Start MP4 Recording on the main page. Here, you can specify the storage destination and file name.

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

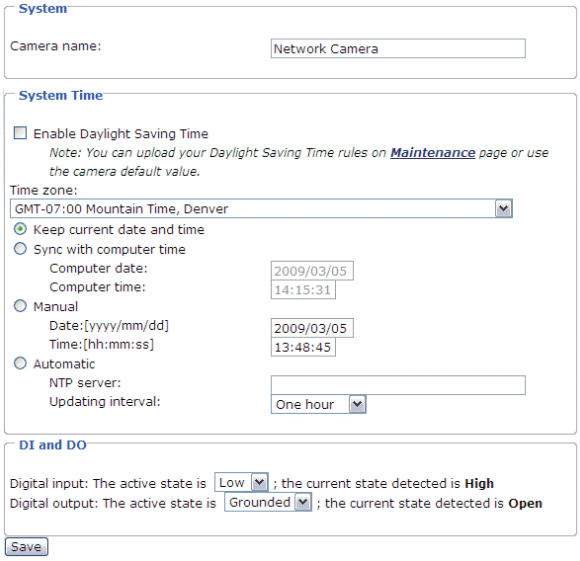
File Name Prefix: Enter the text that will be put in front of the video file name.

Add date and time suffix to the file name: Select this option to add date and time to the file name suffix.



Configuration Definitions

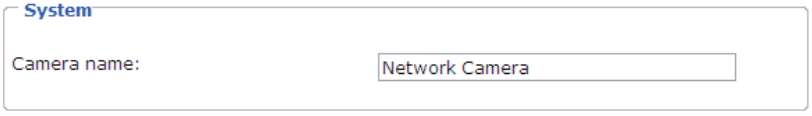
Only Administrators can access the system configuration page. Each category in the menu will be explained in the following sections.



System Parameters

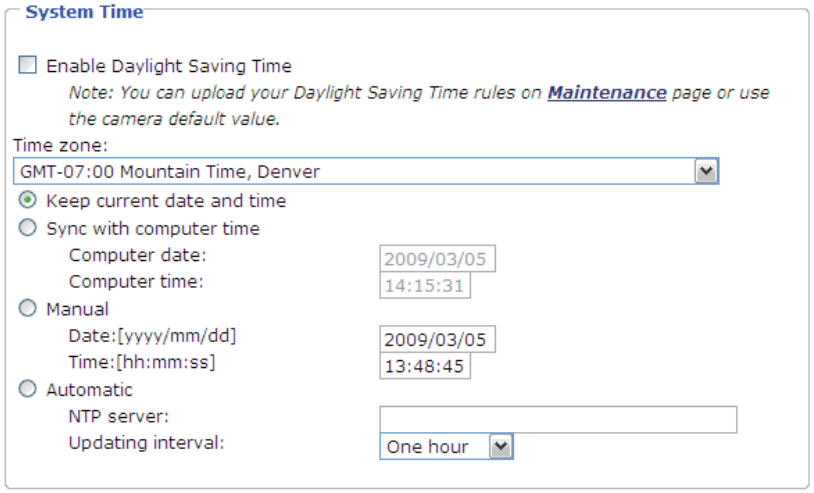
This section explains how to configure the basic settings for the Network. It contains the following three segments: System, System Time and DI/DO. After completing the settings on this page, click Save on the bottom of the page to take effect.

System

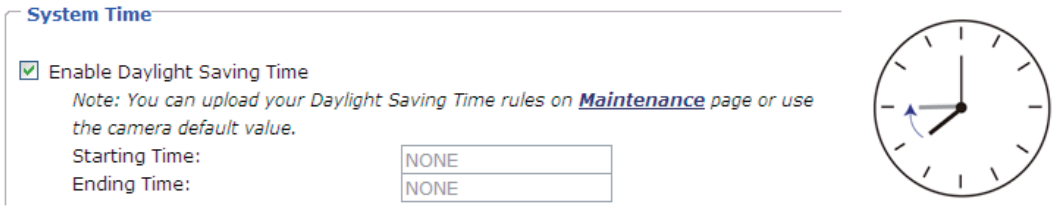


Camera name: Enter a name for the Network Camera. The camera name will be displayed at the top of the main page.

System Time



Enable Daylight Saving Time: Select this option to enable daylight savings time (DST). During DST, the system clock moves one hour ahead. Set the time zone for your Network Camera first if using this feature. The starting time and ending time of the DST is displayed upon selecting this option. To manually configure the daylight saving time rules, refer to Upload or Export Daylight Saving Time Configuration File on page 68 for details.



Time zone: Set your local time zone from the drop-down list.

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

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

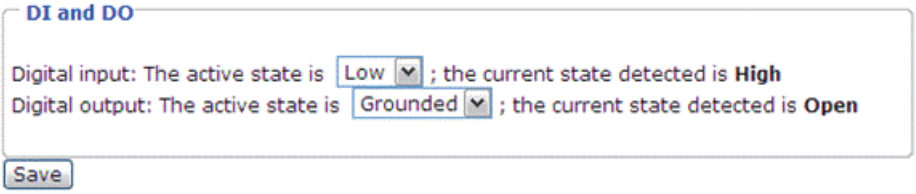
Manual: The administrator can enter the date and time manually. The date and time format are [yyyy/mm/dd] and [hh:mm:ss].

Automatic: The Network Time Protocol is a service that 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 with the NTP server on hourly, daily, weekly, or monthly basis.

DI and DO



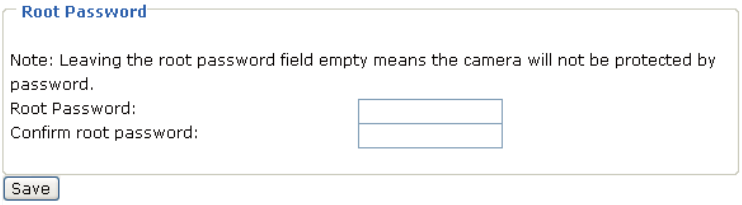
Digital input: Select High or Low to define normal status of the digital input. The Network Camera will report the current status.

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

Security Settings

This section explains how to enable password protection and create multiple accounts. It contains the following three segments: Root Password, Add User and Manage User.

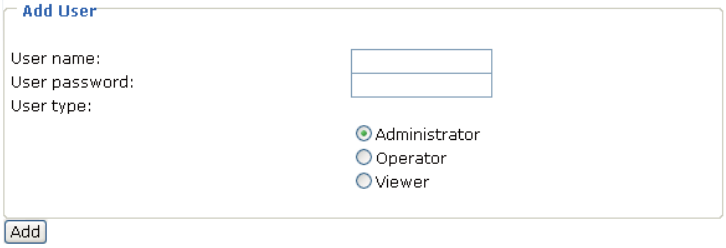
Root Password



The administrator account "root" is permanent and can not be deleted. To add more accounts, you must apply a password for the "root" account first.

1. Type the identical password in both text boxes.
2. Click Save to enable password protection.
3. A log in window is displayed for authentication; type the administrator's name and password to access the Network Camera.

Add User



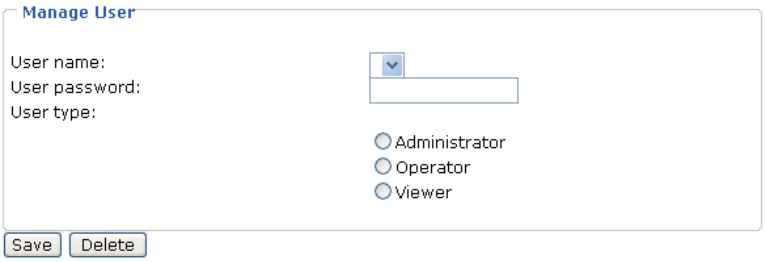
Administrators can add up to twenty user accounts.

1. Input the new user's name and password.
2. Select the desired security level. Click Add to take effect.

Access rights are sorted by account types. There are three kinds of account types.

- Administrator: can access all pages and use all URL Commands.
- Operator: can access only the main page and use some URL Commands.
- Viewer: can access only the main page and not use any URL Commands.

Manage User



Here you can change user's access rights or delete user accounts.

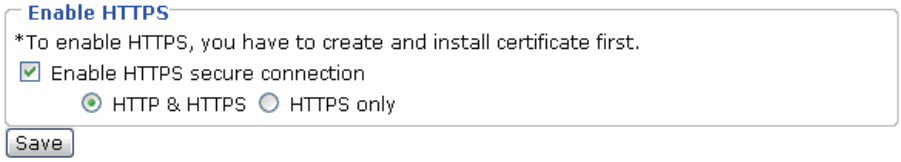
1. Pull down the user list to find an account.
2. Make necessary changes and then click Save or Delete to take effect.

HTTPS

This section explains how to enable authentication and encrypted communication over SSL.

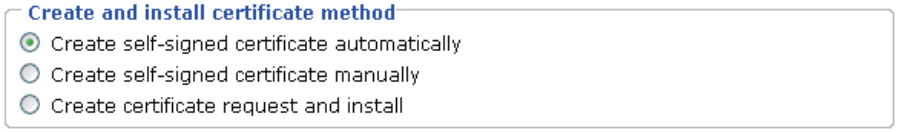
Enable HTTPS

Select this options to turn on the HTTPS communications.
Select either “HTTP & HTTPS” or “HTTPS only.”
Select the method to create a certificate before clicking Save.



Create and Install Certificate

Select either to create a self-signed certificate or a signed certificate.



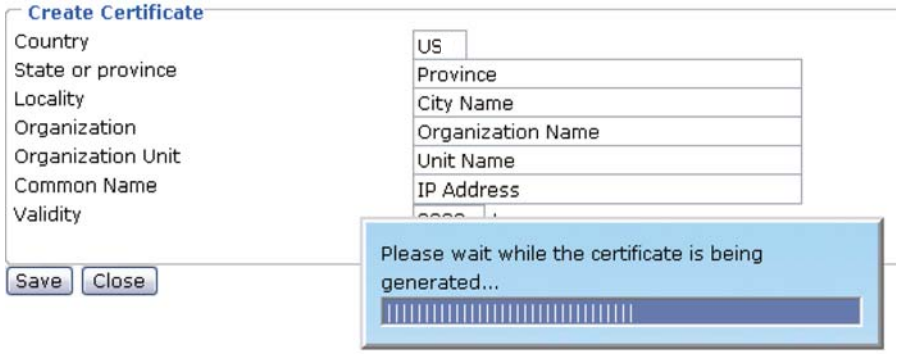
To create a self-signed certificate automatically.

1. Click "Create self-signed certificate automatically."
2. Click Save.

To create a self-signed certificate manually.

1. Click "Create self-signed certificate manually". The Create Certificate window will pop up.

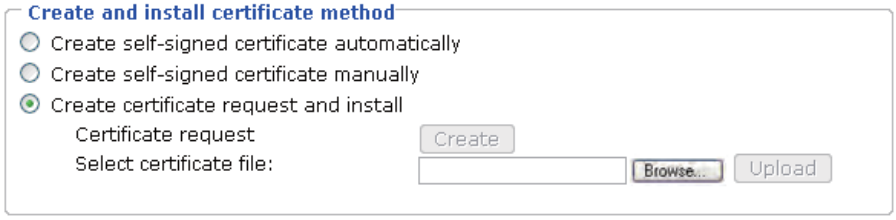
2. Fill in the information required for generating a Certificate Signed Request (CSR) and click Save.



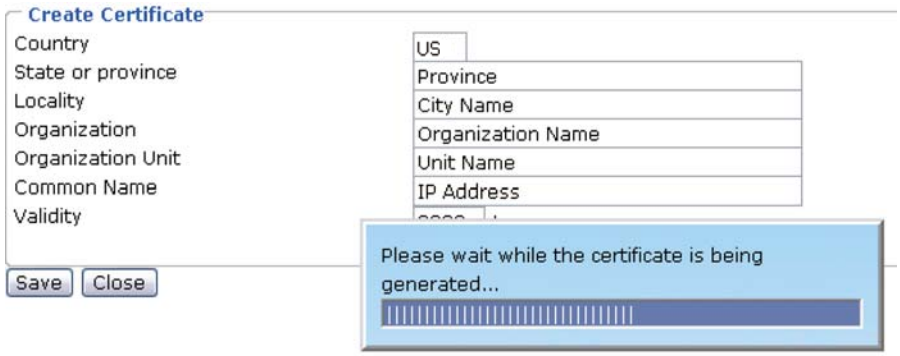
3. Click Save.

To install a trusted create certificate.

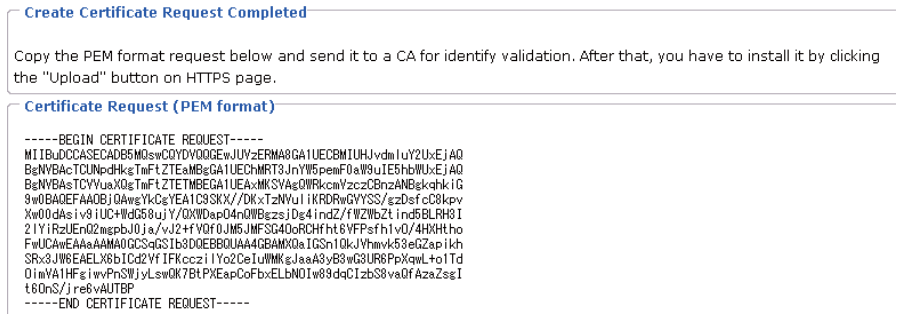
1. Click "Create certificate request and install". The Create Certificate window will pop up.



2. Fill in the information required for generating a Certificate Signed Request (CSR) and click Save.



3. Here is an example of a CSR:



4. Click Save.

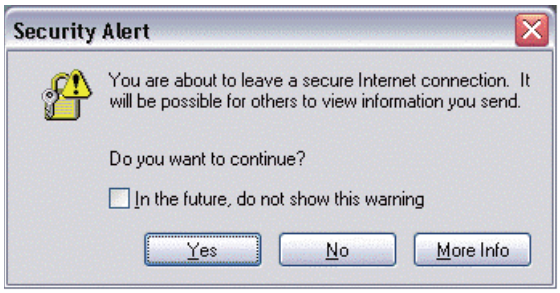
Certificate Information

Display the certificate information. Users may click Property for details. To remove the signed certificated, uncheck the Enable HTTPS secure connection and click Remove.

Security Alert

Fig.1

Fig.2



Above security alert may be shown when switch between HTTP and HTTPS connection. Click OK or Yes to continue the operation.

Fig.3

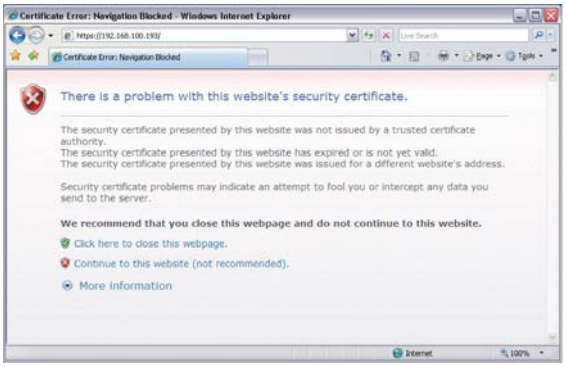


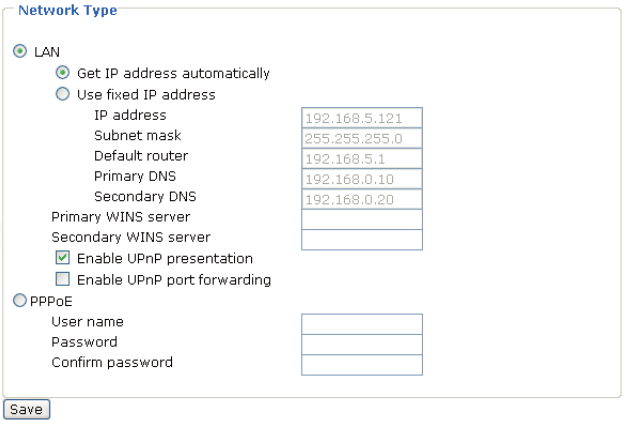
Fig.4

Above security alert may be shown when accessing the camera by HTTPS using "Self-Signed Certificate",
IE7: Click "Continue to this website (not recommended)" on Fig.3 to continue the operation.
IE6: Click Yes on Fig.4 to continue the operation.

Network

This section explains how to configure wired network connection for the Network Camera. It consists the following five segments: Network Type, HTTP, Two way audio, FTP and RTSP Streaming. After completing the settings on this page, click Save to take effect.

Network Type



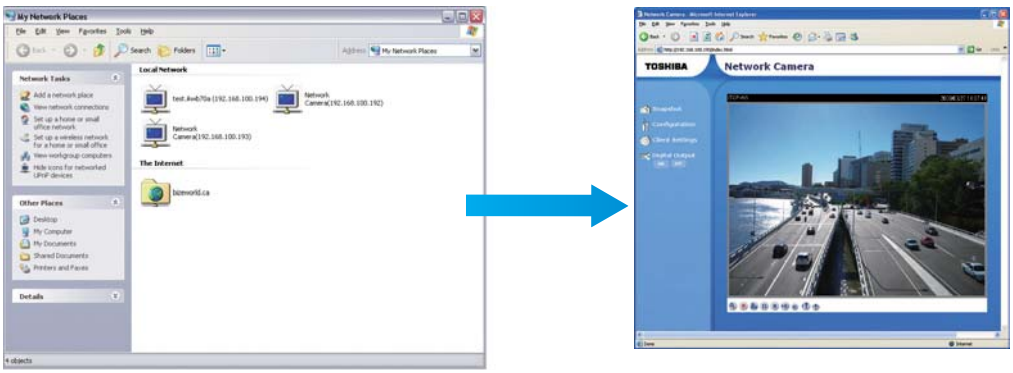
LAN

Select this option when the Network Camera is deployed in a local area network (LAN) and is intended to be accessed by local computers.

Get IP address automatically: Select this option to obtain a dynamic IP address assigned by a 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. Please refer to Internet connection with static IP on page 16 for details.

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. Currently, UPnP™ is supported by Windows XP or later. To use this feature, verify that 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 gateway automatically so that video streams can be sent out from a LAN. To utilize of this feature, verify that your gateway supports UPnP™ and activated.

PPPoE (Point-to-point over Ethernet)

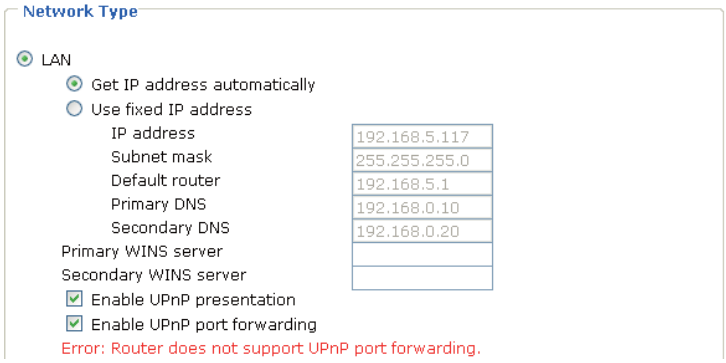
Select this option to configure your Network Camera to make it accessible from a DSL Internet connection. To use this feature, requires an account provided by your ISP.

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

1. Set up the Network Camera in a LAN.
2. Go to Configuration > Application > Server Settings (refer to Server Settings on page 59) to add a new server -- email or FTP server.
3. Go to Configuration > Application > Media Settings (refer to Media Settings on page 57). Select System log so that you will receive a list of 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 take effect.
5. The Network Camera will to reboot.
6. After the camera reboots, disconnect power from the Network Camera. Move the ethernet connection from the LAN to the DSL modem.

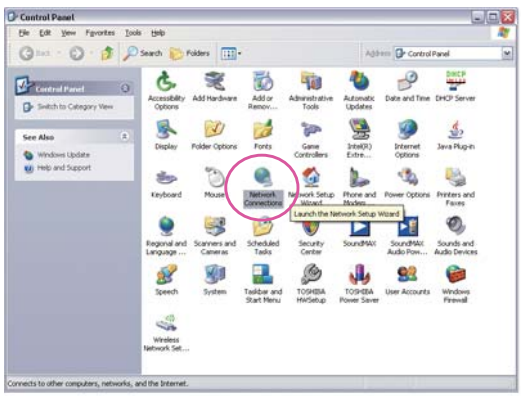
NOTE

- If the default ports are already used by other device connecting to the same gateway, the Network Camera will select other ports for the Network Camera.
- If UPnP™ is not supported by your gateway, you will see the following message.

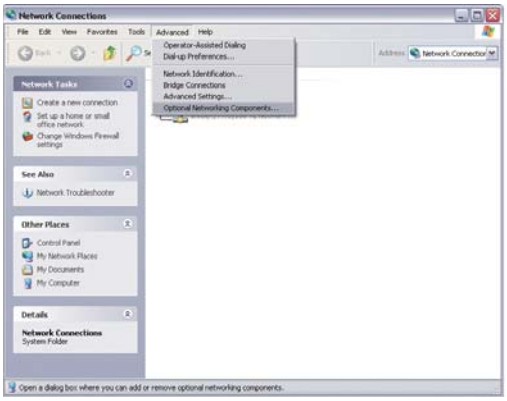


- Steps to enable UPnP™ user interface on your computer:
  Note that you must log on to the computer as a system administrator to install the UPnP™ components.

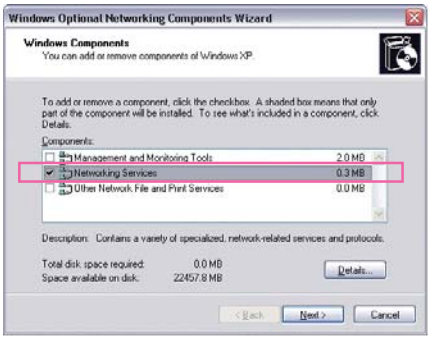
1. Go to Start, click Control Panel, and then click Network Connections.



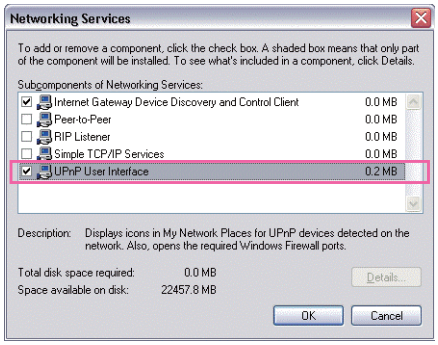
2. Click the Optional Network Components in the menu bar's Advanced.



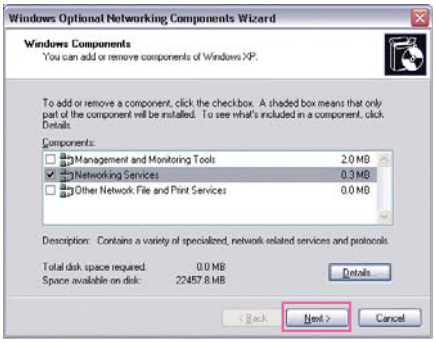
3. In the Windows Components Wizard dialog box, select Networking Services and then click Details.



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



5. Click Next in the following window.



6. UPnP™ is enabled.

Configuration Definitions (Cont.)

- How does UPnP™ work?

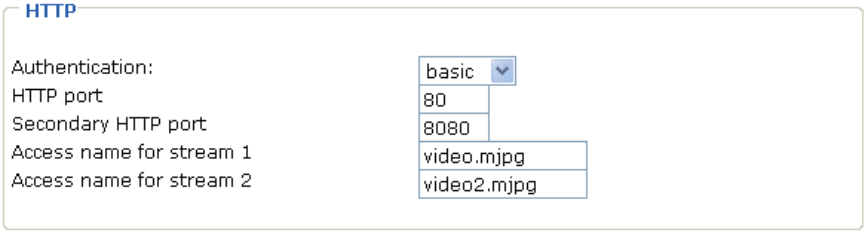
  UPnP™ networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without bothersome network configuration. In the case of Network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

- Enabling UPnP port forwarding allows the Network Camera to open secondary HTTP port on the gateway, not HTTP port 80, meaning that you have to add the secondary HTTP port number behind 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 a 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; refer to Restore on page 67 for details. After the Network Camera is reset to factory default, it is accessible in a LAN.

HTTP



Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for a HTTP transaction: basic and digest. If basic authentication is selected, the password is sent in plain text format; there can be potential risks of being intercepted. If digest authentication is selected, user credentials are encrypted in MD5 algorithm and thus provide better protection against unauthorized accesses.

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

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

In a LAN
http://192.168.4.160 or http://192.168.4.160 : 8080

NOTE

- To use HTTP authentication, make sure that there is set a password for the Network Camera first; refer to Security Settings on page 30 for details.

HTTPS

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

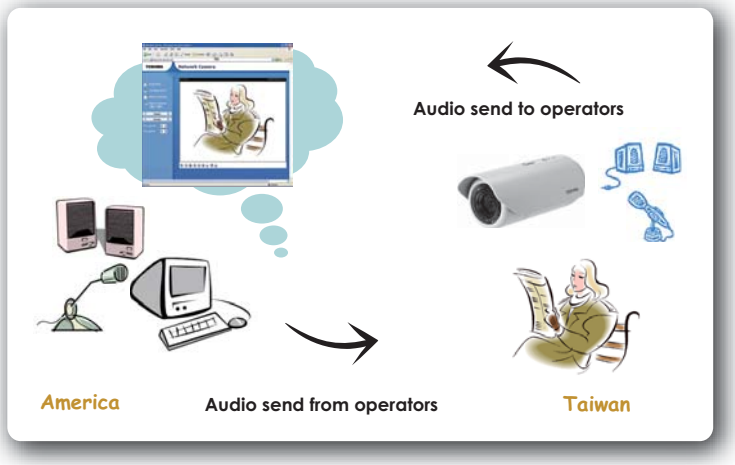
Two way audio

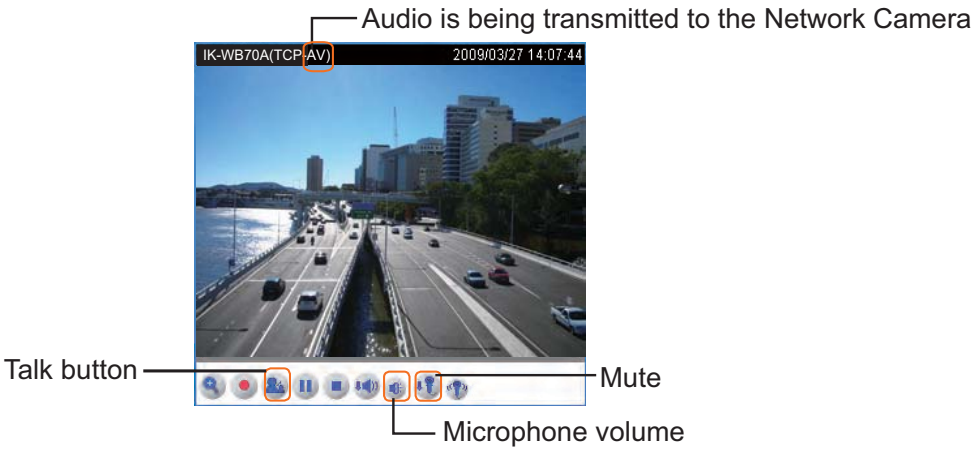
By default, the two way audio port is set to 5060. It can be assigned with another port number between 1025 and 65535.

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

Configuration Definitions (Cont.)

Note that as JPEG only transmits a series of JPEG images to the client, to use this feature, make sure the video mode is set to "MPEG-4" and the media option is set to "Video and Audio".



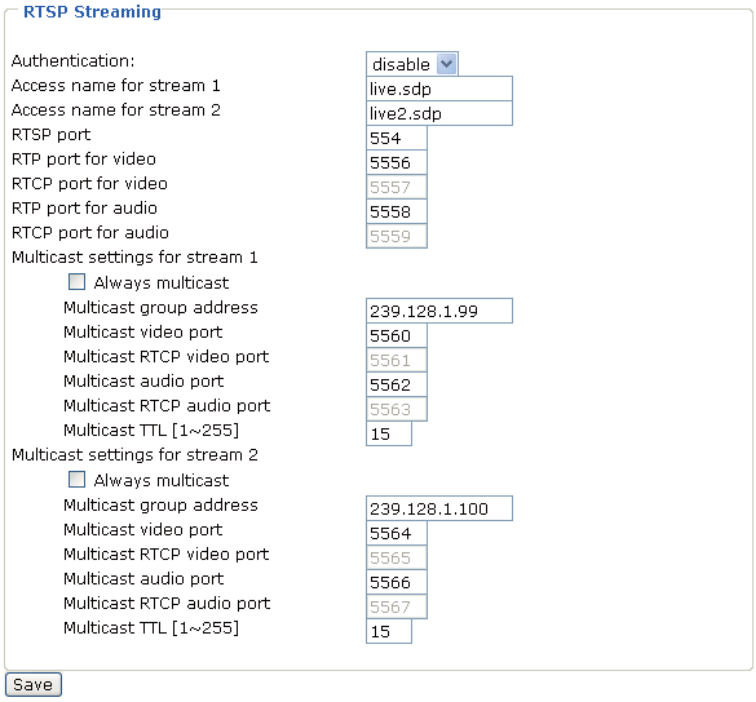


Click to enable audio transmission to the Network Camera; click to adjust the volume of microphone; click to turn off the audio. To stop talking, click again.

FTP

The FTP server allows the Network Camera to use the Toshiba Installation Wizard to upgrade firmware. By default, the FTP port is set to 21. It can be assigned with another port number between 1025 and 65535.

RTSP Streaming



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; there can be potential risks of being intercepted. If digest authentication is selected, user credentials are encrypted in MD5 algorithm and thus provide better protection against unauthorized accesses.

Access name for stream 1 or Access name for stream 2: The access name is used to differentiate the streaming source. When using an RTSP player (e.g. Quick time) to access the Network Camera, and the video mode is set to MPEG-4, use the following RTSP URL command to request a transmission of streaming data.
rtsp://<ip address>:<rtsp port>/<access name for stream1 or stream2>
For example, when the access name for stream 1 is set to live sdp:

1. Launch a RTSP player
2. Choose File > Open URL. An URL dialog box will pop up.
3. Type the URL command in the text box.

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

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

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

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

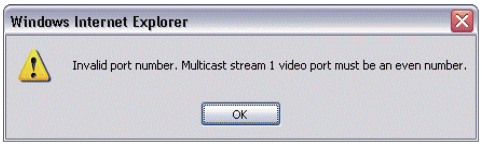
Configuration Definitions (Cont.)

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

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

Multicast settings for stream 1 or Multicast settings for stream 2: Selecting the Always multicast enables Network Camera to transmit the multicast packets. 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 by requesting a copy from the Multicast group address.

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 it is always be odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly. These ports can be changed between 1025 and 65535.
If the multicast RTP video ports are incorrectly assigned, the following warning message is displayed:



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

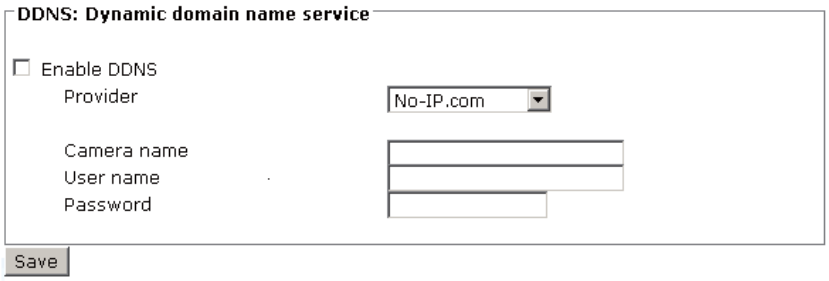
NOTE

- To use the RTSP streaming authentication, make sure that your have set a password for the Network Camera first; refer to Security Settings on page 30 for details.

DDNS

This section explains how to configure 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" The provider list contains seven hosts that provide DDNS services. Please connect to the service provider's web site to review the service charges and sign-up for the service if you want to use DDNS.
ChangeIP.com
http://www.changeip.com/toshiba/
No-IP.com
http://www.no-ip.com/ext/toshiba.php

"Camera Name" If the User wants to use a DDNS service, enter the camera name that is registered at the DDNS server.

"User name" The User Name fi eld is necessary for logging into the DDNS server or to notify the User of the new IP address.
Note: When this fi eld is input as "User Name", the following fi eld must be input as "Password".

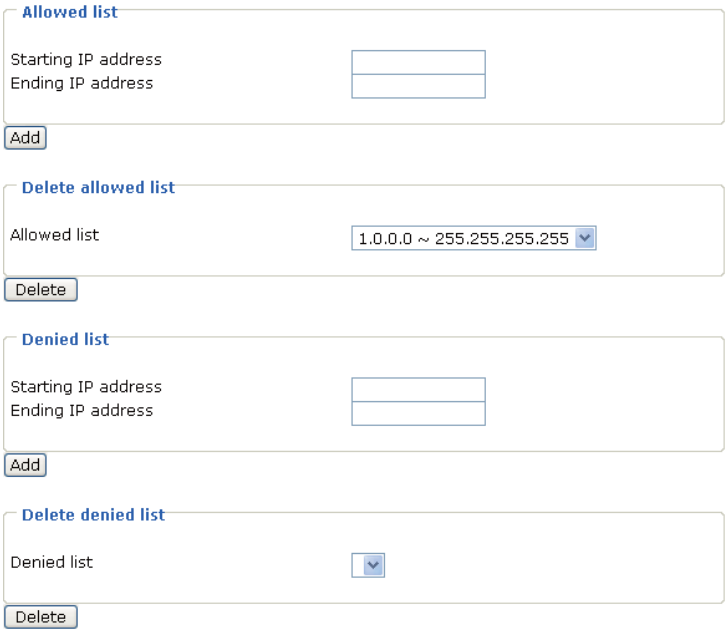
"Password" Input the password to access the DDNS service.

"Save" Click on this button to save current settings for the DDNS service.

Access list

This section explains how to control the access permission by checking the client PC's IP addresses. It contains of the following four segments: Allowed list, Denied list, Delete allowed list, and Delete denied list.

Allowed list or Denied list

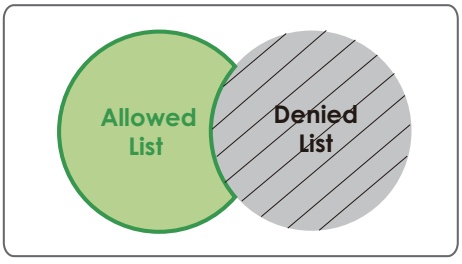


There are two lists for permission control: Allowed list and Denied list. Only those clients whose IP addresses are in the Allowed list and not in the Denied list can access the Network Camera.

1. In the Allowed list or Denied list column, type the starting IP address and ending IP address in the text boxes. A total of ten lists can be configured for both columns.
2. Click Add to take effect.

NOTE

- For example, when the range of the allowed list is set from 1.1.1.0 to 192. 255. 255. 255 and the range of the denied list is set from 1.1.1.0 to 170. 255. 255. 255, Only users' IP located between 171.0.0.0 and 192. 255. 255. 255 can access the Network Camera.



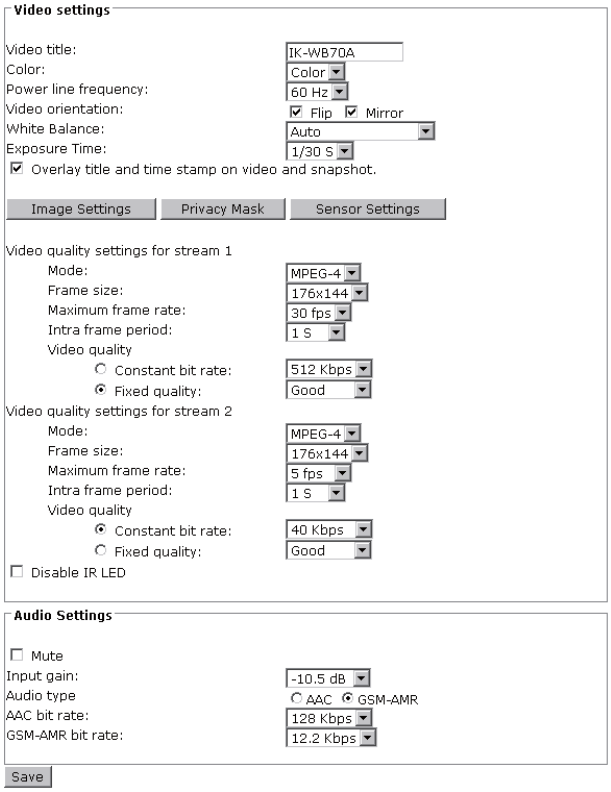
Delete allowed list / Delete denied list

1. In the Delete allowed list or Delete denied list, select a list from the drop-down list.
2. Click Delete to take effect.

Audio and video

This section explains how to cofigure audio and video performances of the Network Camera. It contains the following two segments: Video settings and Audio settings.

Video settings



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 to match the local electricity settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, it is required to disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

Configuration Definitions (Cont.)

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 to correct the image orientation.

White balance: Adjust the value for best color temperature.

■ **Auto**

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

■ **Keep current value**

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

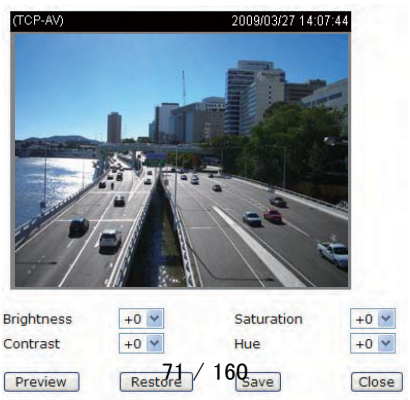
1. Set the White balance to Manual.
2. Place a sheet of white paper in front of the lens; then allow the Network Camera to adjust the color temperature automatically.

Exposure Time: 1/30 S, 1/15 S, and 1/5 S.

Overlay title and time stamp on video: Select this option to place the video title and time on video streams. When the frame size is set to 176 x 144 as the right picture below, only time will be stamped on video streams.

Image Settings

Click Image Settings to open the Image Settings page. In this page, you can tune Brightness, Saturation, Contrast, and Hue for video compensation. Each field has eleven levels ranged from -5 to +5. The value 0 indicates default auto tuning. You can click Preview to fine-tune the image, or click Restore to recall the original settings without incorporating the changes. When completed with the settings on this page, click Save to take effect and click Close to quit the page.



Privacy mask

Click Privacy Mask to open the Privacy Mask page. In this page, you can block out some sensitive zones for privacy concerns.

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

1. Click New to add a new window.
2. To resize 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 descriptive Window Name and click Save to take effect.
4. Select Enable privacy mask to enable this function.

NOTE

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

Sensor Settings

Click Sensor Settings to open the Sensor Settings page. In this page, you can set the exposure level, AGC, WDR (Wide Dynamic Range), night mode, and IR cut filter.

Configuration Definitions (Cont.)

Exposure level: You can manually set the Exposure level from 1 to 8. The default value is 4.

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

Enable WDR (Wide Dynamic Range):
Select to enable the WDR function. This Network Camera with WDR feature can cope with very challenging lighting conditions. It is capable of capturing both of the dark part and bright part of a target and combining the differences into a scene to generate a highly realistic image as the human eyes can see.
If this function is selected the exposure level and AGC function will be disabled.

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

IR cut filter:
The Network Camera has the ability to automatically remove the IR cut filter and turn on the IR illuminators during night or low light conditions.

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

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

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

■ Night mode
In night mode, the Network Camera switches off (remove) the IR cut filter to allow the infrared light to pass through. This improves the sensitivity of the Network Camera in low-light conditions.

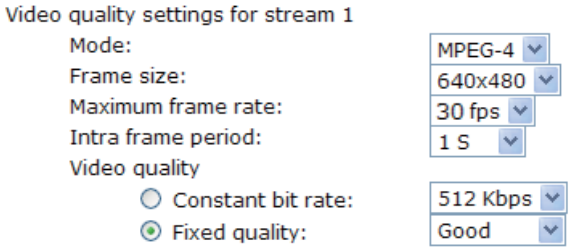
You can click Preview to fine-tune the image, or click Restore to recall the original settings without incorporating the changes. After completing the settings on this page, click Save to take effect and click Close to quit the page.

Video quality settings for stream 1 or stream 2: You can set up two separate streams for the Network Camera for different viewing devices. For example, set the Network Camera to a smaller frame size and a lower bit rate for remote viewing on mobile phones. Or, set the Network Camera to a larger video size and a higher bit rate for live viewing on web browsers.

■ Mode

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

If **MPEG-4** is selected, it is streamed in RTSP or HTTP. There are four dependent parameters provided in MPEG-4 mode for video performance adjustment.



■ Frame size

Select the video size. A larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions: 176 x 144, 352 x 240 and 640 x 480.

■ Maximum frame rate

This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video update.

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

■ Intra frame period

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

■ Video quality

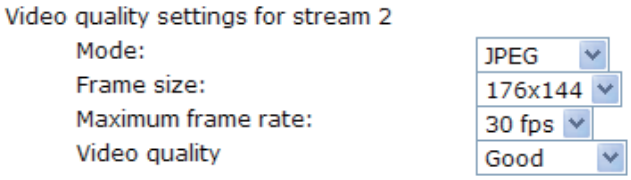
A complex scene generally produces larger file size, meaning that higher bandwidth will be needed for data transmission. Therefore, if Constant bit rate is selected, the bandwidth utilization is fixed at a selected level, resulting in mutable video quality performances. The bit rates are selectable at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

On the other hand, if Fixed quality is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video qualities are selectable at the following settings:

Medium, Standard, Good, Detailed and Excellent.

Configuration Definitions (Cont.)

If **JPEG** mode is selected, the Network Camera continuously sends JPEG images to the clients, producing dynamic effects similar to movies. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. And because the media contents are a combination of JPEG images, no audio data is transmitted to the clients.



■ Frame size

Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions: 176 x 144, 352 x 240 and 640 x 480.

■ Maximum frame rate

This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video update.

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

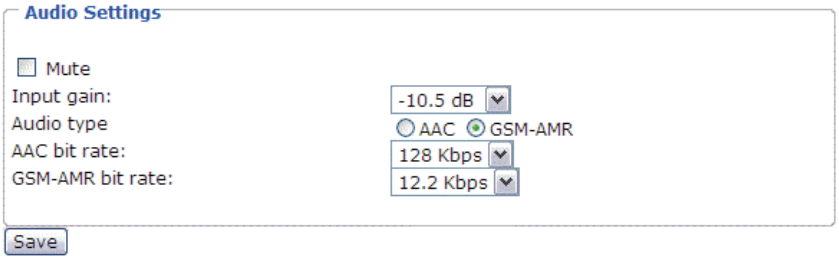
■ Video quality

The video qualities are selectable at the following settings: Medium, Standard, Good, Detailed and Excellent.

Disable IR LED:

If you don't want to let others know that the network camera is on, you can select this option to turn off the LED illuminators. This will prevent the Network Camera's operation from being noticed.

Audio settings



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 to all clients even though the audio transmission is enabled in the Client Settings page. In that case, the following message is displayed.

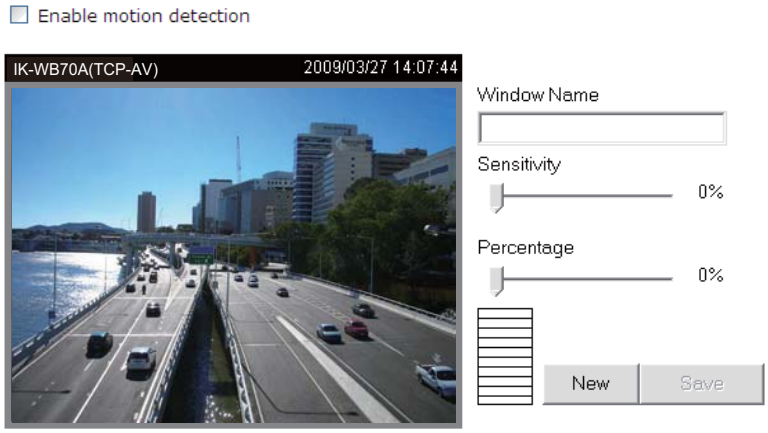
Input gain: The input gain are selectable at the folowing settings:
-34.5 dB, -33 dB, -31.5 dB, -30 dB, -28.5 dB, -27 dB, -25.5 dB, -24 dB, -22.5 dB, -21 dB, -19.5 dB, -18 dB, -16.5 dB, -15 dB, -13.5 dB, -12 dB, -10.5 dB, -9 dB, -7.5 dB, -6 dB, -4.5 dB, -3 dB, -1.5 dB, 0 dB, +1.5 dB, +3 dB, +4.5 dB, +6 dB, +7.5 dB, +9 dB, +10.5 dB, +12 dB.

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

- AAC targets at performing good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable at the following rates: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps and128Kbps
- GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable at the following rates: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps and 12.2Kbps.
  When completed with the settings on this page, click Save to take effect.

Motion detection

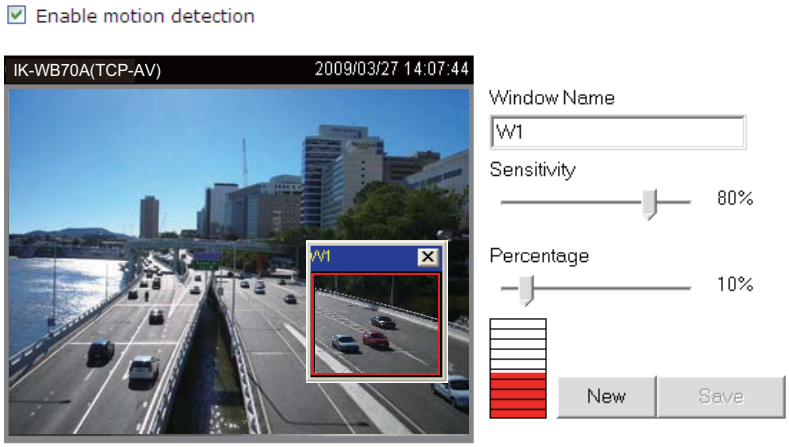
This section explains how to configure the Network Camera to enable motion detection. A total of three motion detection windows can be configured.



To enable motion detection, follow the steps below:

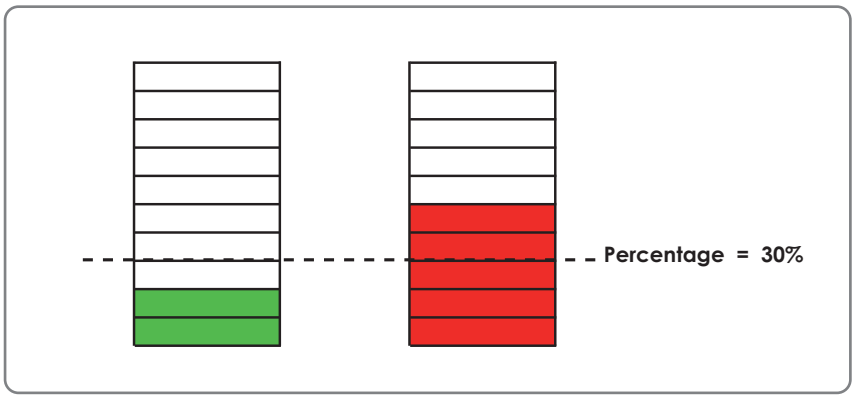
1. Click New to add a new motion detection window.
2. In the Window Name text box, enter a descriptive name for the motion detection window.
   - ■ To move and resize the window, drag-drop the window.
   - ■ To delete window, click X at top right of the window.
3. Define the sensitivity to moving objects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

For example:



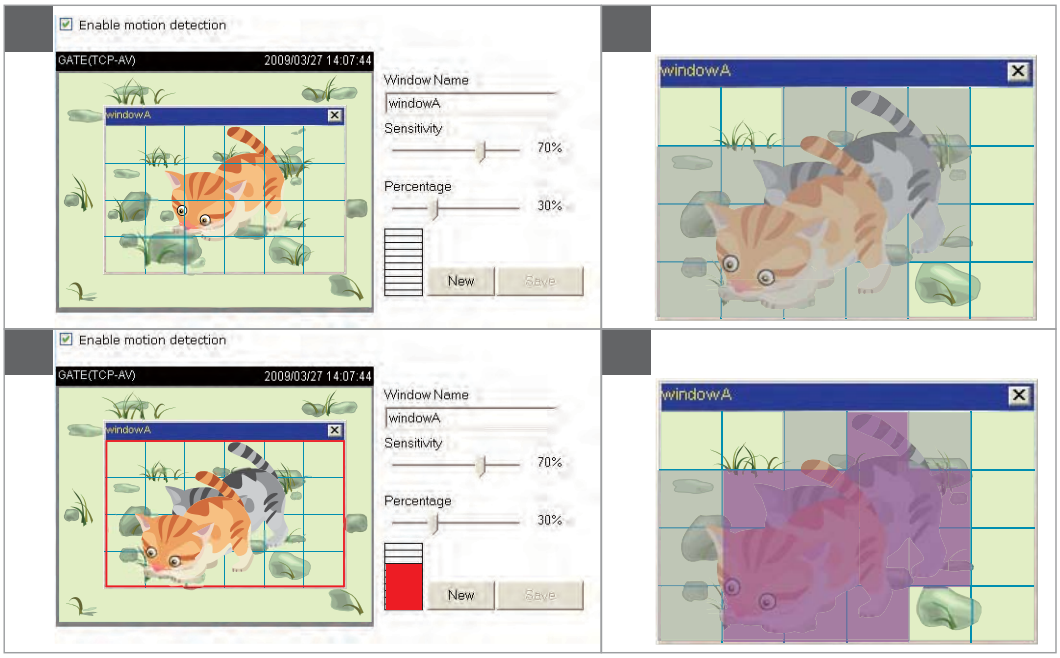
The Percentage Indicator will rise or fall depending on the image variation. When motions are detected by the Network Camera and are judged to exceed the defined threshold, a red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to send to the remote server (Email, FTP) by using this feature as a trigger source. For more information on how to plot an event, refer to Application on page 57.

A green bar indicates that even though motions are detected, the event will not be triggered because the image variations are still falling under the defined threshold.



NOTE

● How does motion detection work?



There are two parameters for setting the motion detection: 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 sense a slight movement while smaller sensitivity settings tend to neglect it. 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 higher security management, it is suggested to set higher sensitivity settings and smaller percentage values.

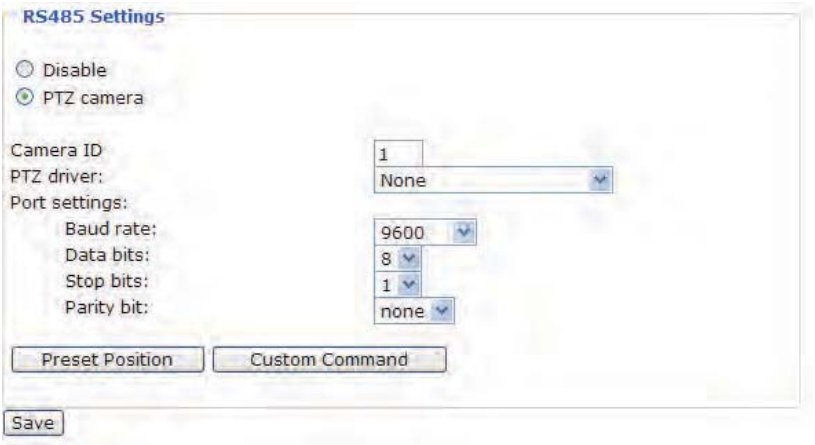
Camera control

This section explains how to control the Network Camera's digital zoom and optional pan/tilt unit or scanner using RS485 interface.

RS485 Settings

Disable: Select this option to disable this function.

PTZ camera: Select this option to enable PTZ operation.
To use this feature, first connect the Network Camera with a PTZ Unit or scanner via RS485 interface. Then configure the PTZ driver and RS485 port settings in the following diagram.



Toshiba offers Pelco D protocol and others. If none of the above PTZ drivers is supported by your PTZ scanner, select Custom camera (scanner). Refer to the user's manual of your PTZ scanner to set the Camera ID, PTZ driver, and Port settings. The Camera ID is necessary for multiple cameras control. If you select PTZ camera and click Save to enable this function, the camera control panel will be displayed in the main page as the following diagram:

Preset Position

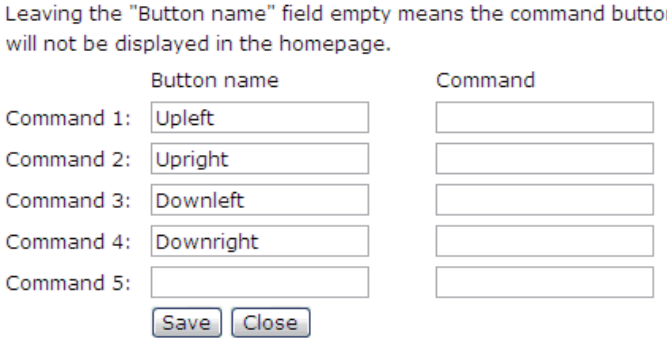
Click Preset Position to open the Preset Position page. In this page, you can set the preset position for the Network Camera. A total of 20 preset positions can be configured.

Follow the steps below to set preset positions:

1. Adjust the Network Camera to a desired position with the buttons on the right side of the window.
2. In the Preset position name text box, enter a descriptive name for the preset position. The preset position name allows up to forty characters. Click Add to take effect. The preset position name will appear in the Preset Positions drop-down list. To remove a preset position from the list, select a preset position name from the Preset Positions drop-down list and then click Delete.
3. You can click "Go to" to aim at preset positions, which will also displayed in the main page.
4. Click Save to take effect.

Custom Command

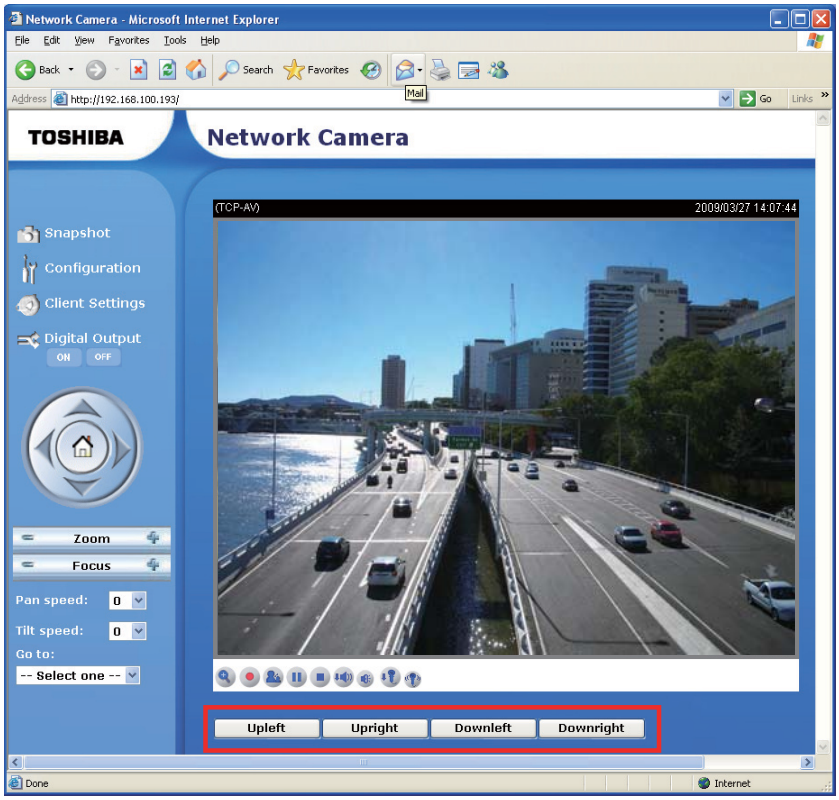
If the Custom camera (scanner) is selected as the PTZ driver, the PTZ control panel on the main page will not take effect. You need to **configure command buttons to control the PTZ scanner. Click Custom Command to open the Custom Command page. A total of five command buttons can be configured. Refer to the user's manual of your PTZ scanner to enter the command in the following blanks.**



Click Save to enable the settings and click Close to quit the page.

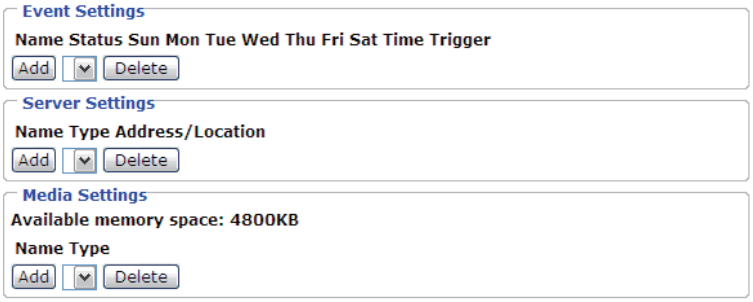
Configuration Definitions (Cont.)

The command button will appear in the main page as the following diagram.

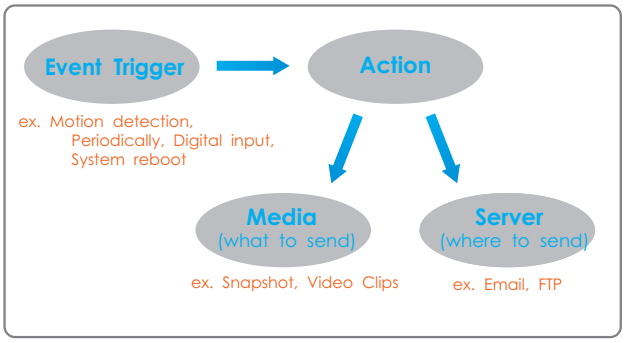


Application

This section explains how to configure the Network Camera to react in response to particular situations. A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or via Email as notifications.



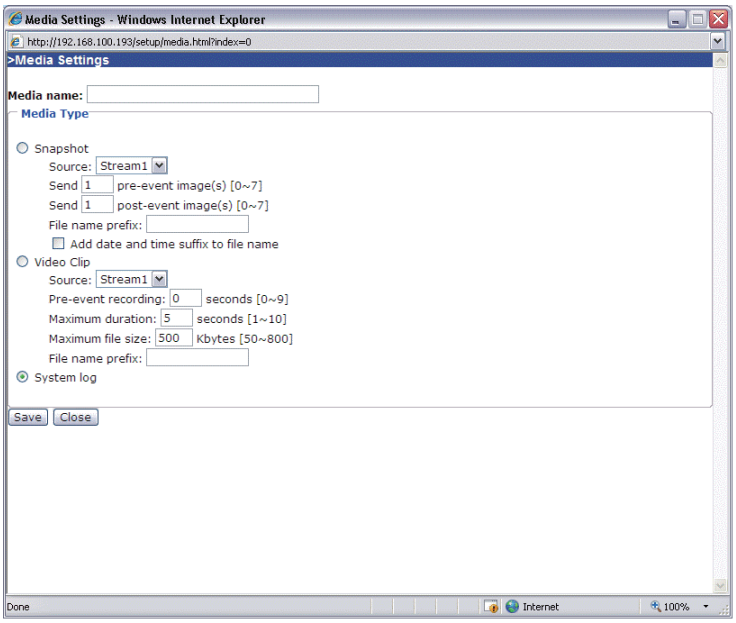
In the illustation on the right side, an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what kind of action will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.



To start plotting an event, it is suggested to configure server and media segments first so that the Network Camera will know what action to perform when a trigger is activated.

Media Settings

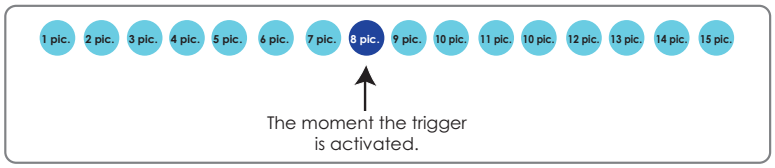
In Media Settings column, click Add to open the media setting page. In this page, you can specify what kind of media to send when a trigger is activated. A total of five media settings can be configured.



Configuration Definitions (Cont.)

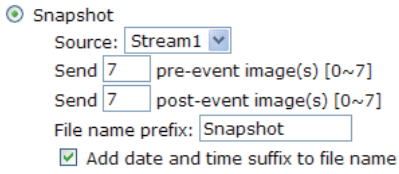
Media name: Enter a descriptive name for the media setting.
Media Type: There are three choices of media types available: Snapshot, Video Clip, and System log.
Snapshot: Select to send snapshots when a trigger is activated.

■ Source: Select to take snapshots from stream 1 or stream 2.
■ Send [#] pre-event images
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Specify to capture how many images before a trigger is activated. Up to seven images can be generated.
■ Send [#] post-event images
Specify to capture how many images after a trigger is activated. Up to seven images can be generated. For example, if both the Send pre-event images and Send post-event images are set to seven, a total of fifteen images are generated after a trigger is activated.



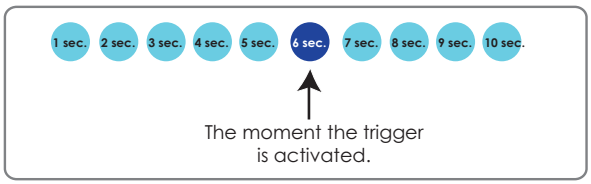
■ File Name Prefix
Enter the text for the file name.
■ Add date and time suffix to the file name
Select this option to add date and time to the file name suffix.

For example:



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

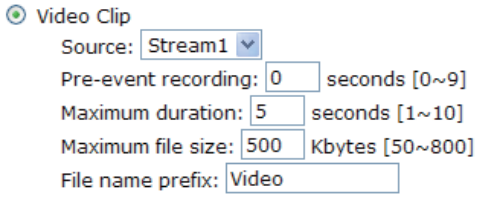
■ Source: Select to record video clips from stream 1 or stream 2.
■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Specify to record video clips for how many seconds before a trigger is activated. Up to nine seconds can be set.
■ Maximum duration
Specify the maximal recording duration in seconds. Up to ten seconds can be set. For example, if the Pre-event recording is set to five seconds and the Maximum duration is set to ten seconds, the Network Camera continues to record for another four seconds after a trigger is activated.



■ Maximum file size
Specify the maximal file size allowed.

■ File Name Prefix
Enter the text for the file name.

For example:

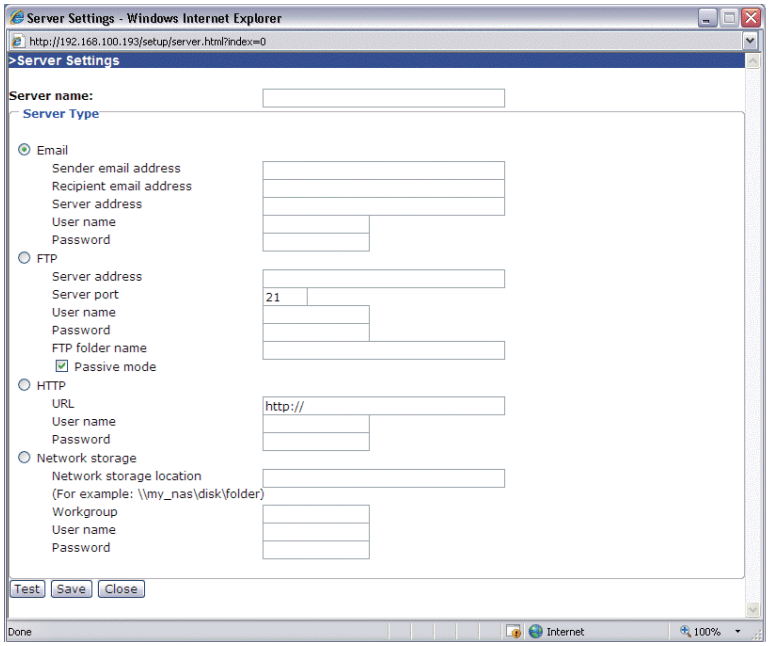


System log: Select to send a system log when a trigger is activated.

When completed, click Save to take effect and then click Close to quit this page. The new media name will appear in the media drop-down list on the Application page as below. To remove a media setting from the list, select a media name from the drop-down list and then click Delete. Only when the media setting is not being applied to an event setting, can it be deleted.

Server Settings

In the Server column, click Add to open the server setting page. In this page, you can specify where the notification messages will be sent when a trigger is activated. A total of five server settings can be configured.



Configuration Definitions (Cont.)

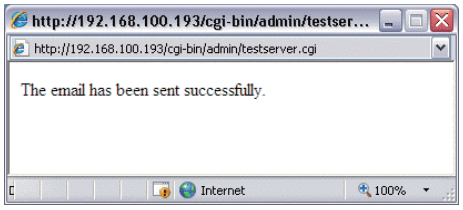
Server name: Enter a descriptive name for the server setting.

Server Type: There are four choices of server types available: Email, FTP, HTTP, and Network storage.

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

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

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



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

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

■ Server port
By default, the FTP port server is set to 21. Also, it can be assigned with another port number between 1025 and 65535.

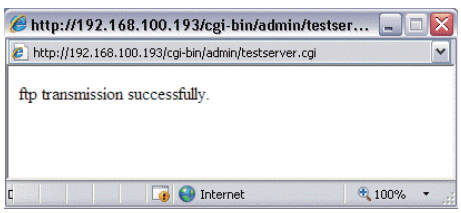
■ User name: Enter the login name of the FTP account.

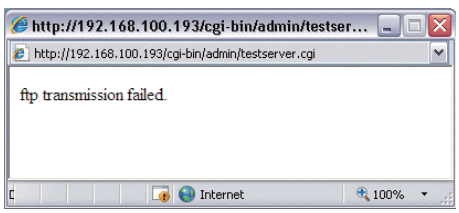
■ Password: Enter the password of the FTP account.

■ Remote folder name
Enter a folder to place the media file. 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. If it works, you will also receive a test.txt file on the FTP server.

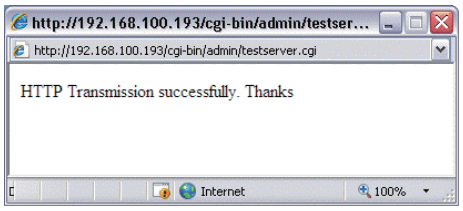


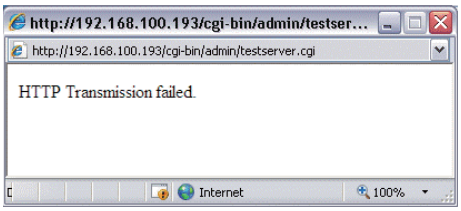


HTTP: Select to send the media to an HTTP server when a trigger is activated.

■ URL: Enter the URL of the HTTP server.
■ User name: Enter the user name.
■ Password: Enter the password.

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

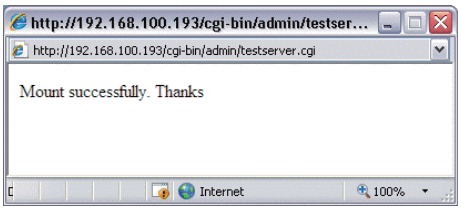




Network storage: Select to send the media to a network storage when a trigger is activated.

■ Network storage location: Enter the path of the network storage.
■ Workgroup: Enter the workgroup for network storage.
■ User name: Enter the user name.
■ Password: Enter the password.

To verify if the network storage settings are correctly configured, click Test. The result will be shown in a pop-up window. If it works, you will also receive a test.txt file on the network storage server.



When completed, click Save to take effect and then click Close to quit this page. The new server name will appear in the server drop-down list on the application page as below. To remove a server setting from the list, select a server name from the drop-down list and then click Delete. Only when the server setting is not being applied to an event setting can it be deleted.

Event

In the Event section, click Add to open the event setting page. In this page, you can arrange the three elements -- Trigger, Schedule and Action to plot an event. A total of three event settings can be configured.

Event name: Enter a descriptive name for the event setting.

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

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

Detect next event after [#] seconds: Enter the duration in seconds to pause continuous motion detection after a motion is detected and a continuous DI after a DI.

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

Trigger: Defines the source by which an event is caused. The trigger source can be configured to use the Network Camera's built-in motion detection system or external digital input devices.There are four choices of trigger sources:

■ Video motion detection
Select this option to allow the Network Camera to use the built-in motion detection system as a trigger source. To enable this function, you need to configure Motion detection first. For more information, refer to Motion detection on page 52 for details.

■ Periodically
Select this option to allow the Network Camera to trigger periodically for every other defined minute. At most 999 minutes can be set.

■ Digital input
Select one of the Digital inputs to allow the Network Camera to use external digital input device as a trigger source.

■ System boot
Select this option to allow the Network Camera to trigger when the power of Network Camera is disconnected.

Event Schedule: The effective period in which the event stays active. Specify the effective period for the event.

■ Select the days on weekly basis.

■ Select the time for recording in 24-hour time format.

Action: Also referred as the effect, defines the action to be performed by the Network Camera when the trigger is activated. Select the action to perform when a trigger is activated.

■ Trigger digital output for [#] seconds
Select this option to turn on external digital output device when a trigger is activated. Specify the length of trigger interval in the text box.

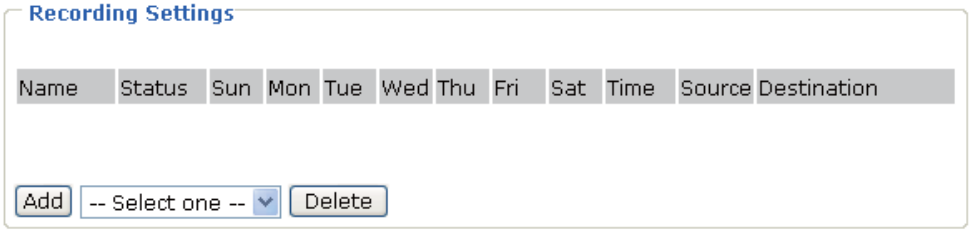
■ Server name and Media name
Select the server and media name to allow the Network Camera to send the media files to the server when a trigger is activated. The server name is a name specified on the server setting page.
The media name is a name specified on the media setting page and listed in the drop-down list.

When completed, select Enable this event. Click Save to take effect and then click Close to quit this page. The new event name will appear in the event drop-down list on the application page. To remove an event setting from the list, select an event name from the drop-down list and then click Delete.

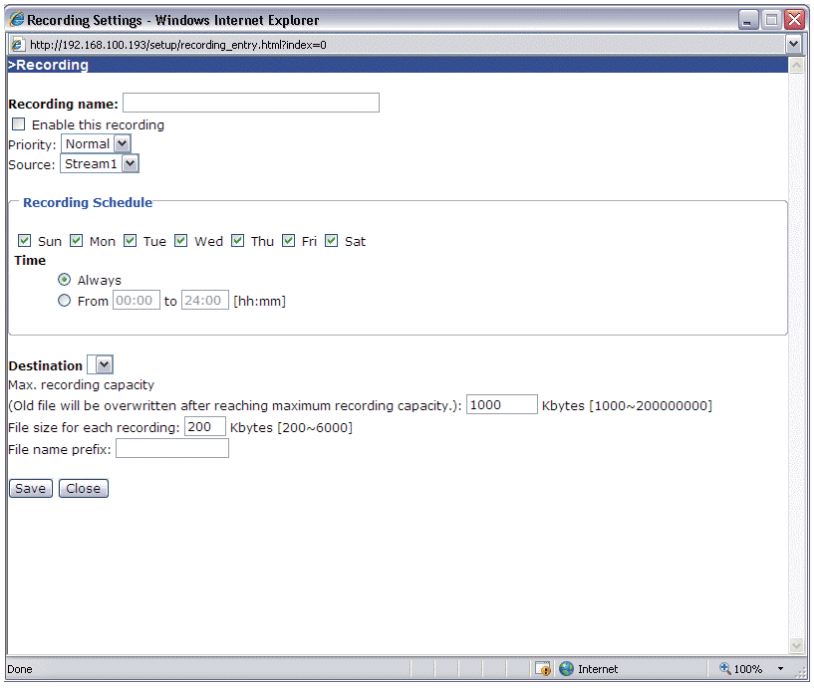
Recording

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

Recording Settings



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



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

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

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

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

Recording Schedule: Specify the recording duration.

■ Select the days on weekly basis.
■ Select the time for recording in 24-hour time format.

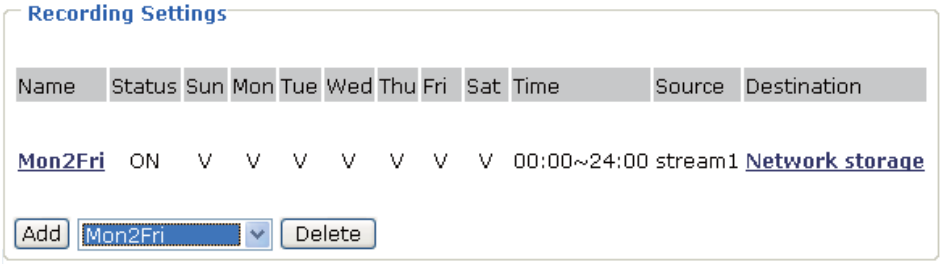
Destination: Specify a storage destination for the recorded video files. Note that the destination field is empty by default. Go to Configuration > Application > Server Settings to set a Network storage server; refer to Server Settings on page 59.

Max. recording capacity: When the maximum capacity is reached, the oldest file will be overwritten by the latest one.

File size for each recording: Specify the file size for each recording media.

File name prefix: Enter the text that will be put in front of the file name.

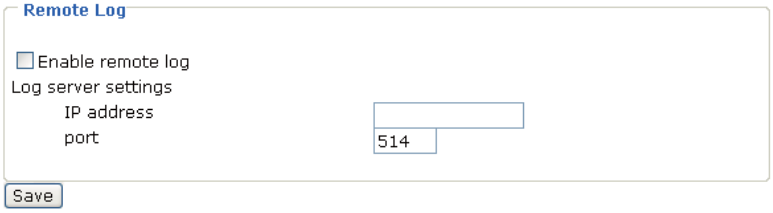
When completed, select Enable this recording. Click Save to take effect and then click Close to quit this page. The new recording name will appear in the recording drop-down list on the recording page. To remove a recording setting from the list, select a recording name from the drop-down list then and click Delete.



System log

This section explains how to configure the Network Camera to send the system log message to a remote server and how to refer the current log message of the Network Camera.
It is composed of the following two Segments: Remote Log and Current Log.

Remote Log



You can configure the Network Camera to send the system log file to a remote server as a log message.

When using this feature, the appropriate syslog server is required for receiving the system log message from the Network Camera.
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 take effect.

Current Log

This column displays the system's log in chronological order. The system log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain amount.
The system log messages stored in the Network Camera will be all cleared after reboot or power down the Network Camera.

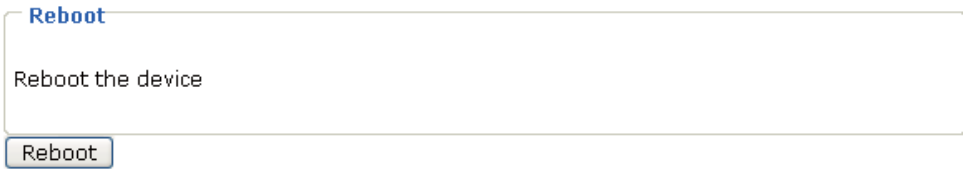
View parameters

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

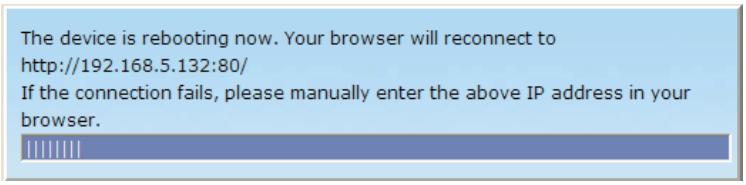
Maintenance

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

Reboot

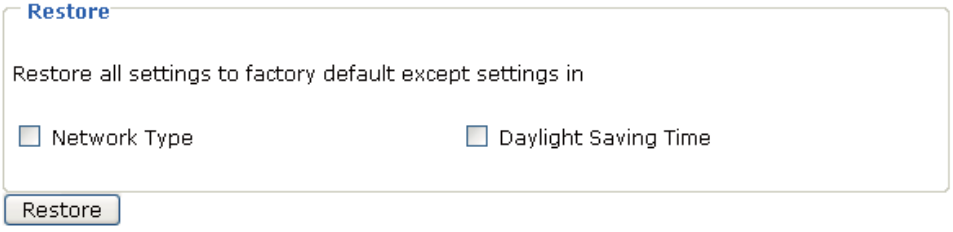


This feature allows you to turn off and then turn on the Network Camera. It takes about one ~ two minutes to complete the process. When completed, the live video will be displayed in your browser. The following message is displayed during the rebooting process.



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

Restore



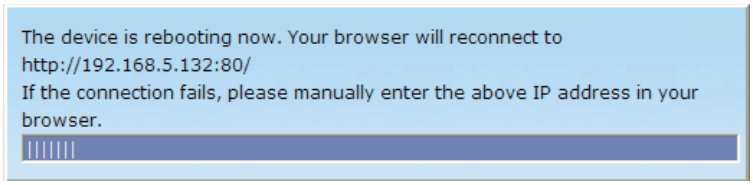
This feature allows you to restore the Network Camera to factory default. Two settings can be excluded:

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 (refer to System Parameters on page 28)

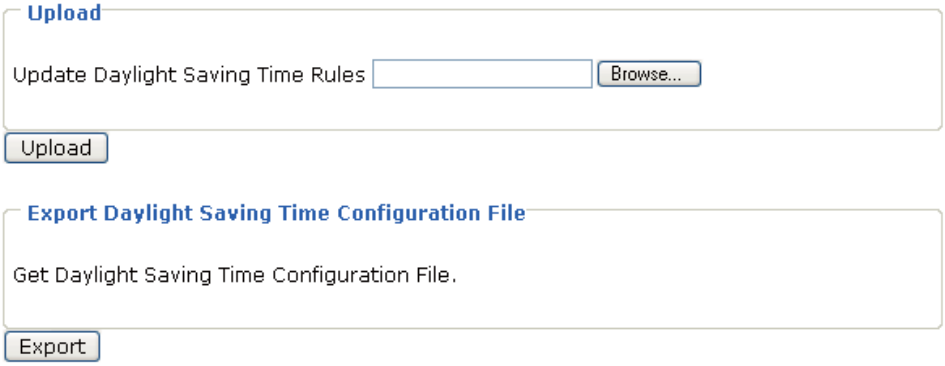
If none of the options is selected, all settings will be restored to factory default.

The following message is displayed during the restoring process.



Configuration Definitions (Cont.)

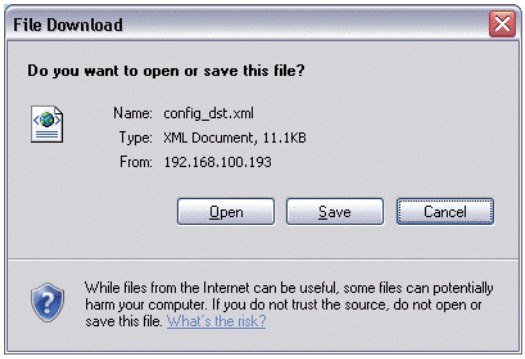
Upload or Export Daylight Saving Time Configuration File



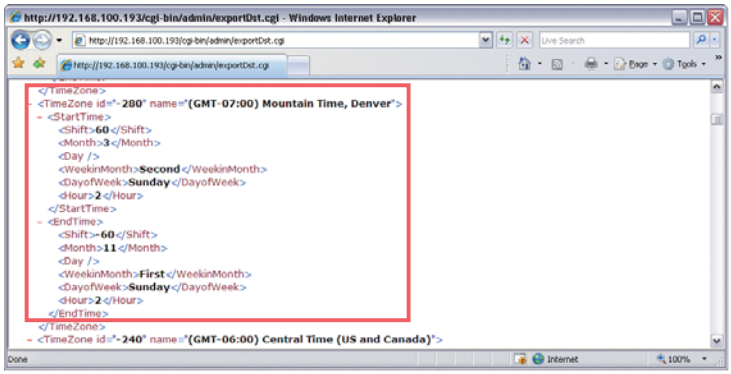
This feature allows you to set the starting time and ending time of DST.

Follow the steps below to set up:

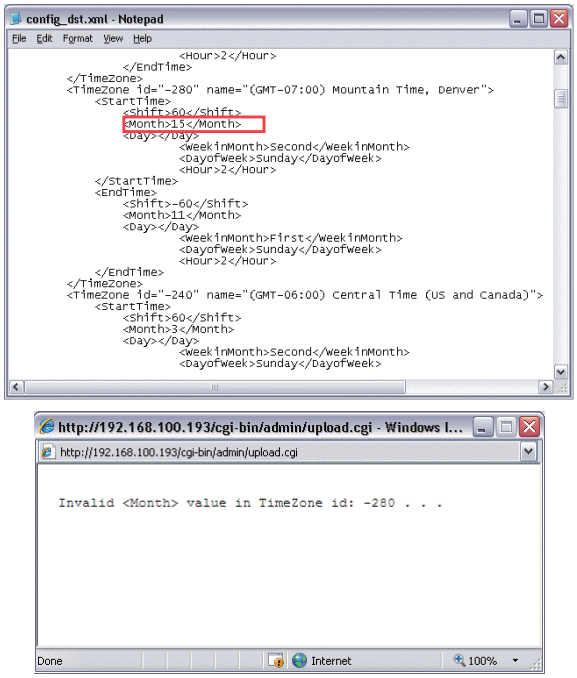
1. In the Export Daylight Saving Time Configuration File column, click Export to export an Extensible Markup Language (*.xml) file from the Network Camera.
2. Edit the XML file and locate your time zone; set the starting time and ending time of the DST. When completed, save the file.



In the example below, the 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.

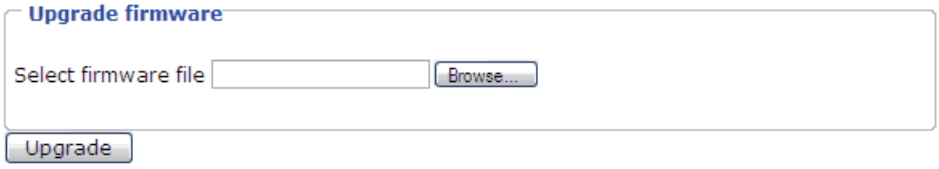


3. In the Upload Column, click Browse... and specify the XML file.
   If the incorrect date and time is assigned, you will see the following warning message when uploading the file to the Network Camera.



4. Click Upload. To enable the DST, see System Time on page 28.
   The following message is displayed when attempting to upload an incorrect file format.

Upgrade Firmware



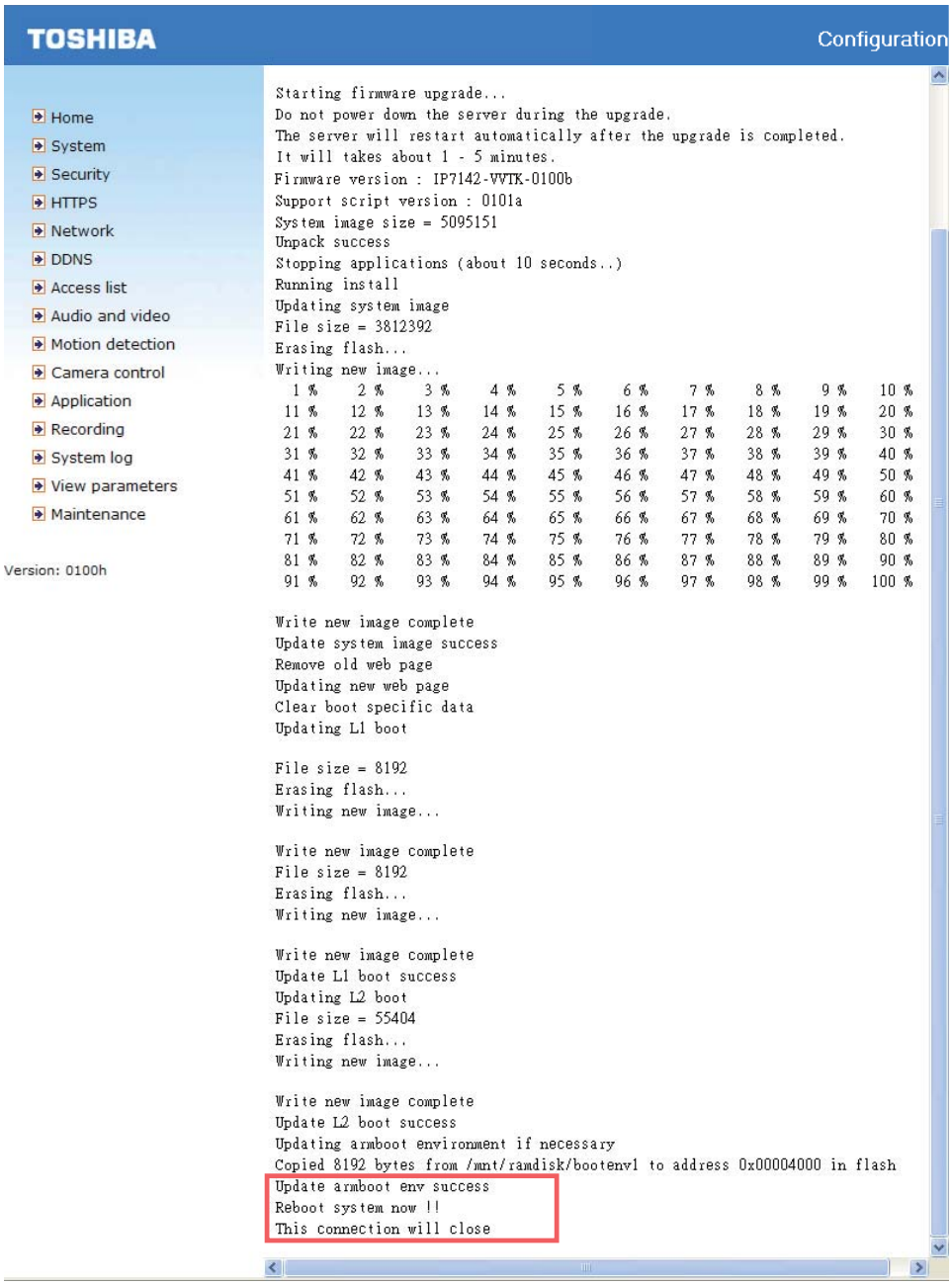
This feature allows you to upgrade the firmware on your Network Camera. It takes about five minutes to complete the process.
Do not power off the Network Camera during the upgrade.

Follow the steps below to upgrade firmware:

1. Download a new firmware file from Toshiba 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.

Configuration Definitions (Cont.)

The upgrade is successful as you see "Reboot system now!! This connection will close". After that, re-access the Network Camera.
The following message is displayed when the upgrade is succeeded.



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

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

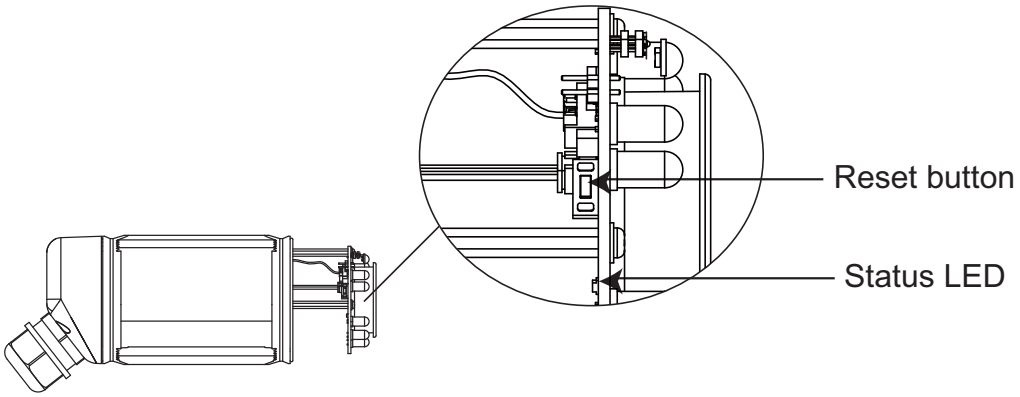
Troubleshooting

Status LED

The LED indicates the status of the Network Camera.

Status LED	Description
Blinking red (two short, one long)	1. Power is being supplied to the Network Camera. 2. Restore, or reboot the Network Camera.

Reboot and restore



There is a reset button on the inner side of the Network Camera. It is used to reboot the Network Camera or restore the Network Camera to factory default. Sometimes rebooting the Network Camera could set the Network Camera back to normal state. If the problems remain after rebooting, restore the Network Camera to factory default and install again.

Reboot: Press and release the reset button. The status LED will blink two short one long in red.

Restore: Press the reset button continuously for over 5 seconds until the status LED blinks two short one long in red. Note that all settings will be restored to factory default.

⚠ **Restoring the factory defaults will erase any previous settings.**

Audio

When using multiple network cameras, restart Internet Explorer each time you switch the camera. Using the same Internet Explorer for the multiple cameras may transmit multiple camera's audio.

Wrong date and time

If this Network Camera is left in the low-temperature environment, the date and time of camera may be delayed when turning on the power. To prevent this trouble, it is highly recommended to leave the power ON of Network Camera in the low-temperature environment.

Glossary (Index)

Glossary (Index) (Cont.)

I

Unique string of numbers that identifies network devices. All devices communicate with IP must have IP addresses. IP address can be divided into network ID and host ID.

J

(Joint Photographic Experts Group)

Standard gauge for compression of colored still image by ITU-TS (International Telecommunication Union: ex-CCITT) and ISO (International Organization for Standardization). It can compress a still image between 1/10 to 1/100 of size.

L

(Local Area Network)

Computer networking in local area.

M

N

(Network Time Protocol)

Server which provides accurate date and time from network.

O

P

Refer to Camera Control on page 54 for details.

R

Refer to Camera Control on page 54 for details.

S

(Simple Mail Transfer Protocol)

Protocol for sending e-mail on the Internet and Intranet.

Method for spliting IP network into a series of sub groups or subnets. By using this system, it estimates whether IP address of the addressed host is in local network or remote network.

T

(Transmission Control Protocol/Internet Protocol)

Protocol for communications between computers are used as standard for transmitting data over networks. This is the standard protocol of the Internet and at the same time, it is the most popularized protocol. Network layer protocol is IP, and transport layer protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). FTP, SMTP and other applications use TCP/IP.

U

W

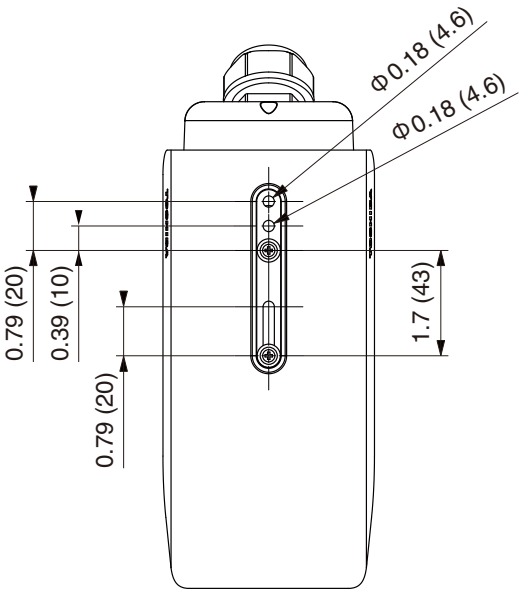
Specifications

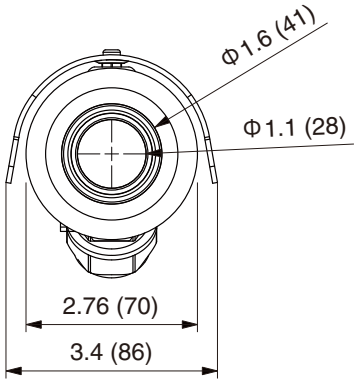
Power supply	12 VDC ± 10 %, 24 VAC ± 10 %, PoE
Power consumption	12 VDC / 0.4 A, 24 VAC / 0.4 A
Image pickup device	1/3.3 inch, CMOS
Effective pixels	Horizontal 640, vertical 480 pixels
Scanning system	Progressive
Minimum object illuminance	0 lux with IR illuminators
White balance	AWB
Viewing angle	Wide end: horizontal 85.2° vertical 51.6° Tele end: horizontal 23° vertical 14.8°
I/O terminal	Input 1, output 1
Image size	640 × 480, 352 × 240, 176 × 144
Image compression system	JPEG, MPEG4
Image quality setting	5 levels
Maximum frame rate at M-JPEG*1	30 fps at 640 × 480
Maximum frame rate at MPEG 4*1	30 fps at 640 × 480
Audio in/out terminal*2	Mic in/Line out
Network interface	10Base-T / 100Base-TX, RJ45 connector, IEEE 802.3af (PoE compatible)
Protocols	TCP/IP, HTTP, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE
OS	Windows® XP, Windows Vista® Business
Browser	Internet Explorer® Ver. 6.0 or 7.0
Operating temperature	14°F to 122°F (-10°C to 50°C)
Operating humidity	20 % to 80 %
Storage temperature	14°F to 140°F (-10°C to 60°C)
Storage humidity	90 % or less
Weight	969 g (2.14 lbs)
Dimensions	without Shade : 7.09 (L) × 2.76 (W) × 2.76 (H) inches (180 (L) × 70 (W) × 70 (H) mm) (excluding protrusion)
Accessories	User's manual and install software (CD-ROM) (×1), Quick start guide and important safeguards (×1), AC adapter (×1), Warranty (×1), Screw kit (x1), RJ45 coupler (x1), Wrench (x1), I/O connector (×2), Shade (x1), Mounting bracket and screw kit (x1), Silica gel (x1)

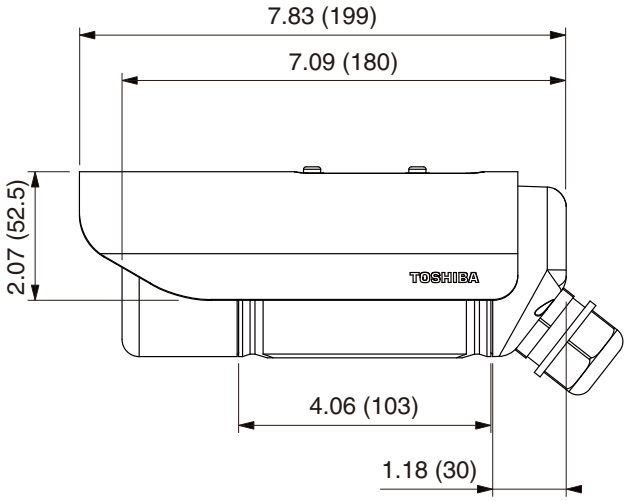
*1: Varies in accordance with the object, image quality, network environment and performance of the personal computer used.
*2: The sound may not be clear depending on the conditions of the lines.

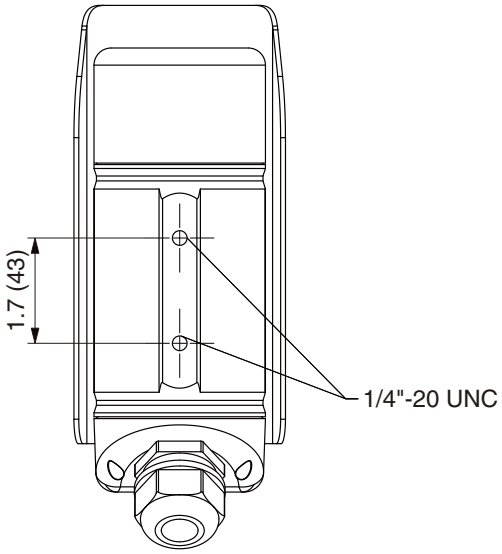
- Designs and specifications may change without prior notice for better improvement.
- Screens, photos, illustrations and other diagrams contained in this user's manual may slightly change from actual ones.

Appearance Diagram

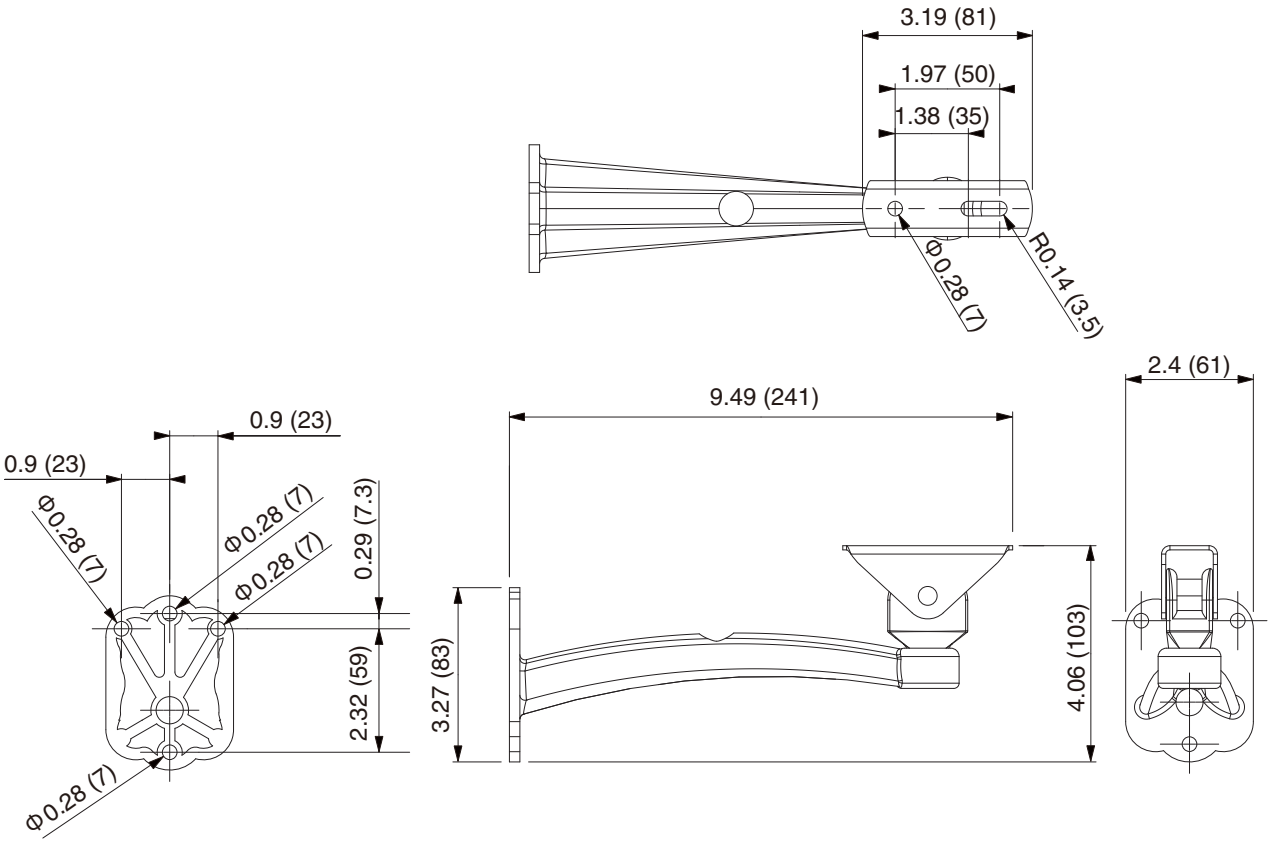








Dimensions: inch (mm)



Dimensions: inch (mm)

Technology License Notice

MPEG-4 AAC Technology

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

MPEG-4 Visual Technology

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

AMR-NB Standard

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

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

About the software

This product contains a piece of software licensed to TOSHIBA CORPORATION (hereafter TOSHIBA) by a third party. The copyright and other intellectual property rights of the software are held by this third party or the licensor. The software is protected by the Copyright Law, Universal Copyright Convention, and other intellectual property laws and agreements. The permission of Toshiba and the third party must therefore be obtained before the software can be reproduced. Contact Toshiba if you need it for more information at http://www.toshibasecurity.com/support/firmware.jsp.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void,

and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

TOSHIBA AMERICA INFORMATION SYSTEMS, INC.

Surveillance & IP Video Products

9740 Irvine Boulevard,

Irvine, CA 92618-1697

Phone Number: (877) 855-1349