

TOSHIBA

Leading Innovation >>>

NETWORK CAMERA

Model: IK-WD01A

User's Manual



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

■ <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>).



Introduction

FCC (USA)-INFORMATION

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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.

Thank you for purchasing the IK-WD01A 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® and Windows® are trademarks or registered trademarks of Microsoft® Corporation in the United States and other countries.
- 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

All the safety and operating instructions should be read before the product is operated.

2. Retain Instructions

The safety instructions and user's manual should be retained 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. Water and Moisture

Do not use this video product near water. Some examples are: near a bath tub, wash bowl, kitchen sink, or laundry tub, in a wet basement, or near a swimming pool.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. Overloading

Do not overload the power supply or extension cords as this can result in a risk of fire or electric shock.

15. 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.

16. 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.

17. Damage Requiring service

Disconnect this video product from the power supply and refer servicing to qualified service personnel under the following conditions.

- When the power-supply cord or plug is damaged.
- If liquid has been spilled, or objects have fallen into the video product.
- If the video product has been exposed to rain or water.
- 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.
- If the video product has been dropped or the cover has been damaged.
- When the video product exhibits a distinct change in performance which indicates a need for service.

18. 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.

19. 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 (OR BACK).
NO USER SERVICEABLE PARTS INSIDE.
REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.**



The lightning flash with arrow head 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 EXPOSE THIS APPLIANCE TO RAIN OR MOISTURE.

CAUTION:

CONNECT 24 VAC UL LISTED CLASS 2 POWER SUPPLY.

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

- **This camera is for indoor use.**
- **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**
Do not drop the camera or subject it to intense vibration.

- **Never touch internal parts**
Do not touch the internal parts of the camera other than the parts specified.
- **Do not splash water on the camera**
Install the camera where the camera can be kept dry. If the camera gets wet, 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.

- **Cleaning the camera**
Turn the power off and use a dry cloth to clean the camera. When the dirt is hard to remove, use a cloth with a mild detergent and wipe gently.
Do not use volatile substances (e.g. paint thinner, petroleum benzine, or household pesticide) on the camera. Otherwise, it may cause discoloration or malfunctions. Use a lens cleaning paper (used to clean camera lenses or lenses of spectacles) to clean the camera lens.

- **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 much 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 120 VAC outlet.
If inserting it into other than 120 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 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 (AH1812-B)

Power source	: 100-240 VAC 50/60 Hz 18 W
Rated output	: 12 VDC, 1.5 A
Ambient temperature guaranteed for performance	: 0° C to 40° C (32° F to 104° F)
Storage temperature	: -25° C to 85° C (-13° F to 185° F)
Maximum external dimensions	: 34.5 x 75 x 46.5 mm (1.358 x 2.953 x 1.831 inches) (width x height x depth)
Cord length	: 1800 mm (70.866 inches)



Table of Contents

Introduction

Introduction

- Introduction.....2
- IMPORTANT SAFEGUARDS.....4
- NOTES ON USE AND INSTALLATION6
- Precautions for Use.....7
- AC adapter.....8
- Table of Contents.....10
- Contents.....12

Installation

Installation

- Installation.....13
 - Hardware installation13
 - Software installation14
- Initial Access to the Network Camera.....15
 - Check Network Settings.....15
 - Add Password to prevent Unauthorized Access15

How to Use

How to Use

- How to Use16
- Authentication.....16
- Installing plug-in.....17
- User's features.....18
 - Main Screen with Camera View.....18
 - Digital Zoom.....19
 - MP4 Recording.....20
 - Snapshot.....20
 - Client settings.....21
 - Digital output.....23
 - Audio communication.....24
- Administrator's features25
 - Fine-tuning for Best Performance25
 - Opening accounts for new users.....27
 - Build a security application.....28
 - Software revision upgrade.....29

Definitions in Configuration

Appendix

Definitions in Configuration

● Definitions in Configuration	30
● System parameters	31
● Security settings	32
● Network settings	33
• Network type	34
• HTTP	35
• Two way audio	35
• FTP	35
• RTSP Streaming	36
● DDNS	37
● Access List	38
● Audio and Video	39
• Video Settings	40
• Audio Settings	41
• Image Settings	42
• Privacy Mask	43
● Motion detection	45
● Application	46
• Event	47
• Server	48
• Media	50
● Recording	51
● System log	53
● Maintenance	54

Appendix

● A. Troubleshooting	55
• Status LED	55
• Reset and restore	55
● B. Glossary (Index)	56
● C. Specifications	58
● D. Appearance Diagram	59

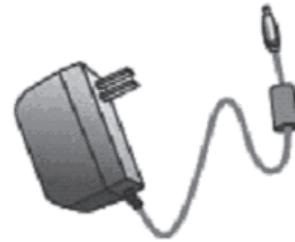
Contents

Introduction

● IK-WD01A

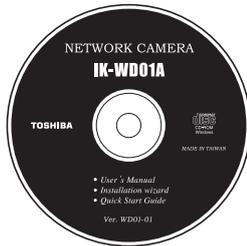


● AC Adapter

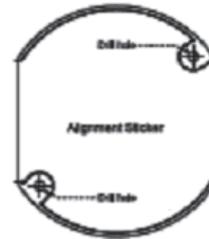


Installation

● CD-ROM



● Alignment Sticker

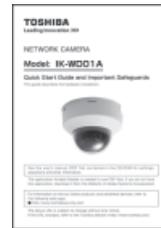


How to Use

● Warranty



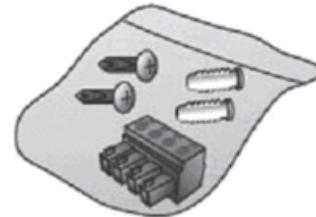
● Quick Start Guide and Important Safeguards



● Torx driver



● Screws and I/O Connector



Definitions in Configuration

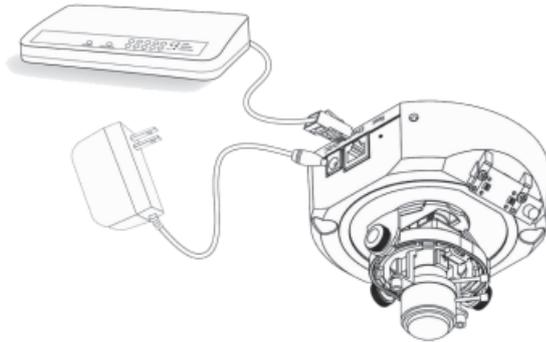
Appendix



Installation

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 foregoing Package Contents. 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.

Upon powering up, the status LED will light up and then the device will go through a booting process. The status LED will be steady orange when obtaining an IP address. After obtaining an IP address, the LED will blink orange and red indicating the camera is ready.

Please refer to the Quick Start Guide for details to the hardware installation.

To install in Ethernet

Make sure the Ethernet is firmly connected to a switch hub. After attaching the Ethernet cable plug in the power adapter. If the LED turns out to blink orange-color, go to next paragraph "Software installation".

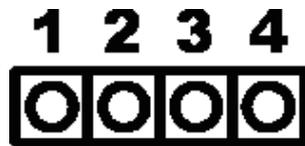
Power over Ethernet (PoE) installation

Connect the Ethernet cable to a PoE switch or hub and to the camera. The camera will go through the "power up" sequence. Proceed to "Software installation" after the camera goes into the ready state.

Installation (Cont.)

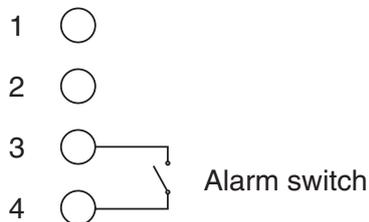
General I/O terminal block

This Network Camera provides a general I/O terminal block with one digital input and one digital output device control. The pin definition is as below.



- 1: Power
- 2: Digital output
- 3: Digital input
- 4: Ground

The connection definition is as below when "Digital input" is used for alarm input.



External/Internal MIC switch

Switch "Internal" or "Microphone" to set up the source of microphone input.

Software installation

At the end of the hardware installation, users can use Installation Wizard program included in the product CD-ROM to find the location of the Network Camera. There may be many Network Cameras in the local network. Users can differentiate the Network Cameras with the serial number. **The serial number is printed on the labels on the carton and the bottom of the Network Camera body.** Please refer to the Quick Start Guide for details to the Installation Wizard.

Once installation is complete, the Administrator should proceed to the next section "Initial Access to the Network Camera" for necessary checks and configurations.



Initial Access to the Network Camera

Check Network Settings

The Network Camera can be connected either before or immediately after software installation onto the Local Area Network. The Administrator should complete the network settings on the configuration page, including the correct subnet mask and IP address of gateway and DNS. Ask your network administrator or Internet service provider for the detail information. By default the Network Camera requires the Administrator to run installation every time it reboots. If the network settings are to remain unchanged, disable the Install option. Refer to “Network settings” on the System Configuration page for details. If any setting is entered incorrectly and cannot proceed to setting up the Network Camera, restore the factory settings following the steps in the “Troubleshooting” chapter of the Appendix.

Add Password to prevent Unauthorized Access

The default Administrator's password is blank and the Network Camera initially will not ask for any password. **The Administrator should immediately implement a new password as a matter of prudent security practice.** Once the Administrator's password is saved, the Network Camera will ask for the user's name and password before each access. The Administrator can set up a maximum of twenty (20) user accounts. Each user can access the Network Camera except to perform system configuration. Some critical functions are exclusive for the Administrator, such as system configuration, user administration, and software upgrades. The user name for the Administrator is permanently assigned as "root". **Once the password is changed, the browser will display an authentication window to ask for the new password. Once the password is set, there is no provision to recover the Administrator's password. The only option is to restore to the original factory default settings.**



How to Use

A PC with the Windows operating system can use Internet Explorer (IE) to connect to the Network Camera. A plug-in will be installed into IE when it is connected for the first time.

Authentication

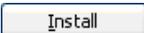
After opening the Web browser and typing in the URL of the Network Camera, a dialogue window pops up to request a username and password. Upon successful authentication, the following figure is displayed.

Note: Because this network camera is shipped without any password by factory default, this dialogue window does not pop up.

The foreground is the login window and the background shows the message if authentication fails. The user may check the option box to save the password for future convenience. This option is not available to the Administrator.



Installing plug-in

During initial access to the Network Camera in Windows, the web browser may prompt for permission to install a new plug-in for the Network Camera. Permission request depends on the Internet security settings of the user's PC or notebook. If the highest security level is set, the computer may prohibit any installation and execution attempt. This plug-in has been registered for certificate and is used to display the video in the browser. Users may click on  to proceed. If the web browser does not allow the user to continue to install, check the Internet security option and lower the security levels or contact your IT or networking supervisor for help.



User's features

Main Screen with Camera View

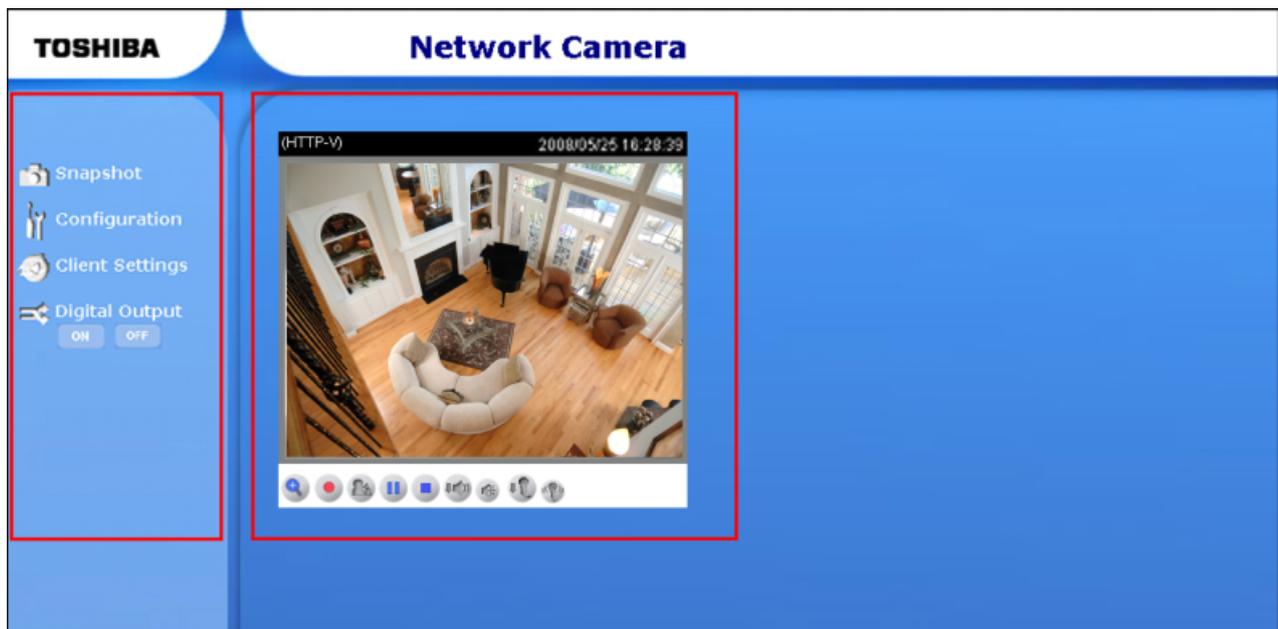
The main page layout has two sections:

Configuration functions: The camera can be configured using these user interfaces.

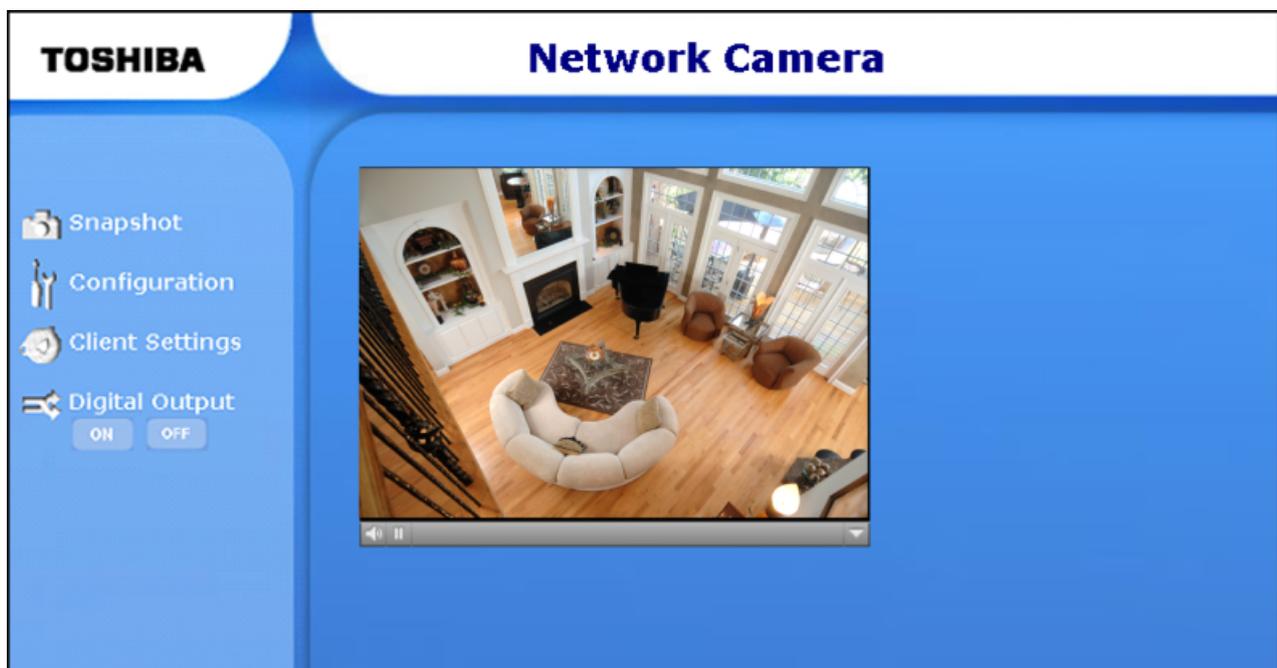
Camera View: What the camera sees.

Click on the configuration link to the left of the image window to enter the configuration page.

Internet Explorer layout when streaming MPEG-4.



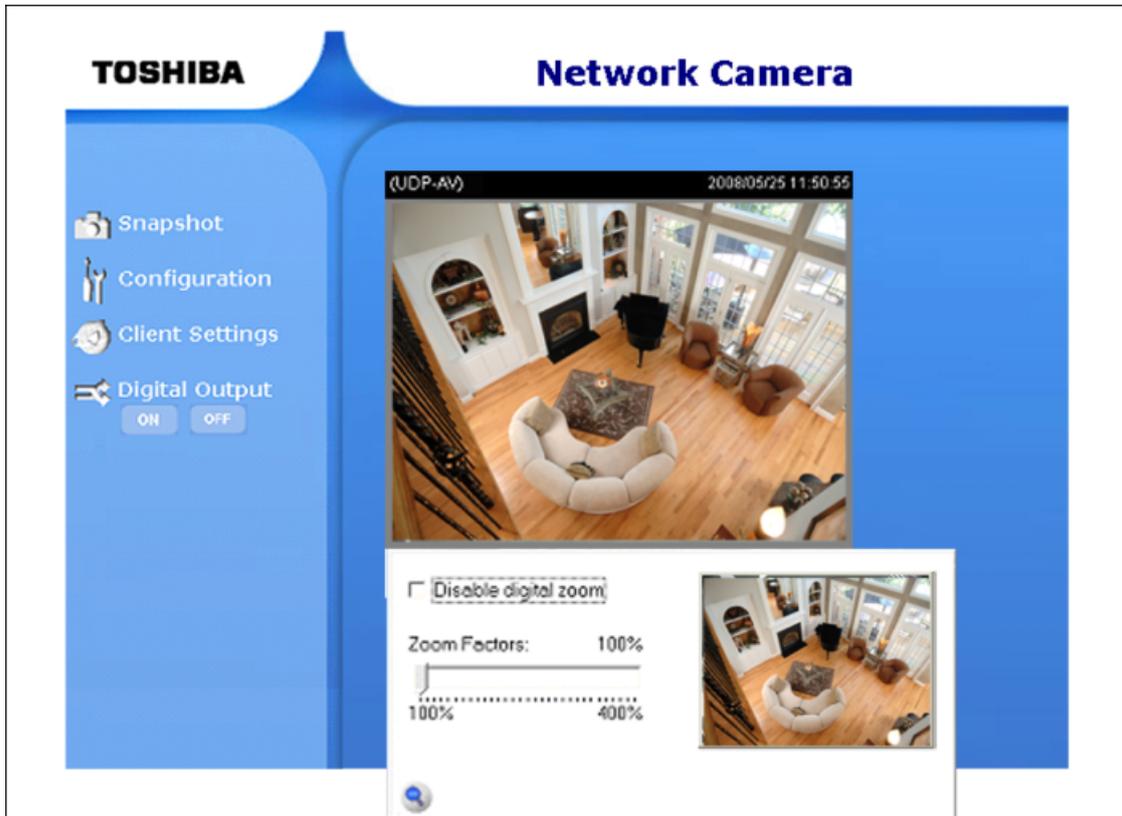
Internet Explorer layout when streaming JPEG.



Digital Zoom

Clicking on the magnifier icon, under the camera view, the digital zoom control panel will appear. Uncheck "Disable digital zoom" and use the slider control to change the zoom factors.

Use the Area Of Interest windows to zoom in on a specific area.





User's features (Cont.)

MP4 Recording

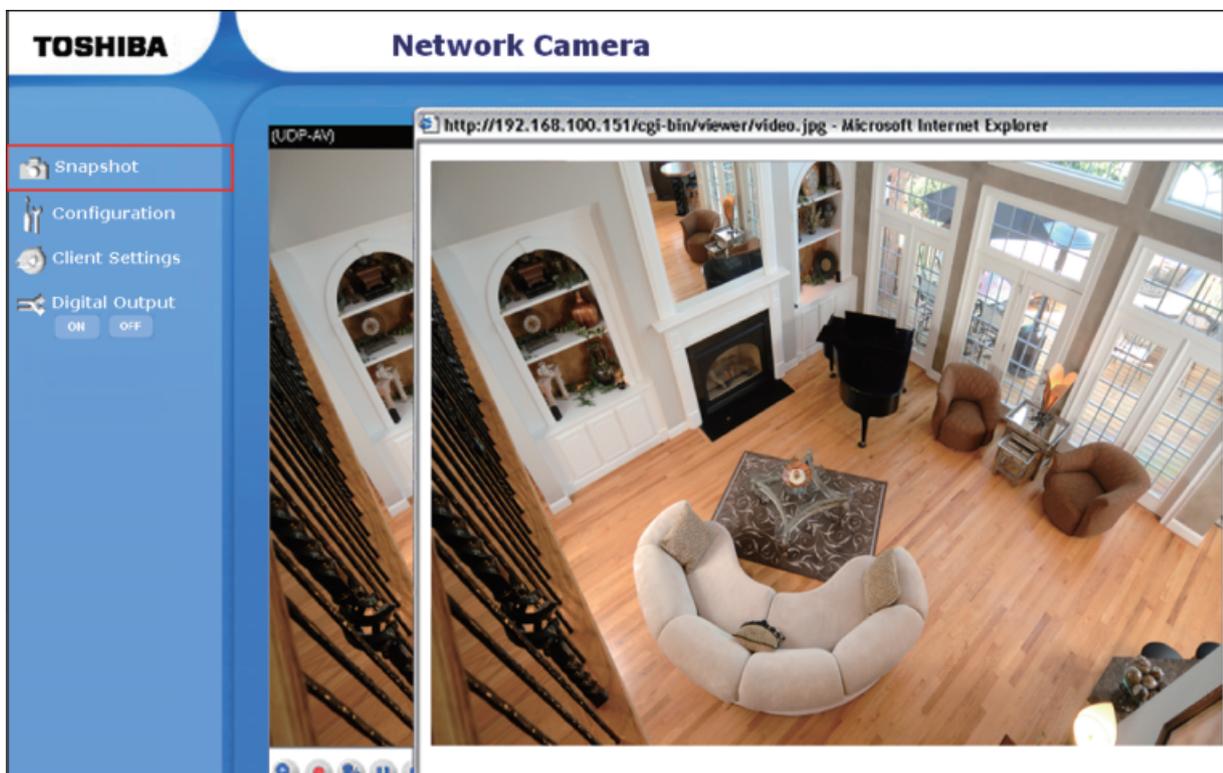
Click on the red circle button  on the plugin to start MP4 recording. You can set the related options in the client setting page.

Snapshot

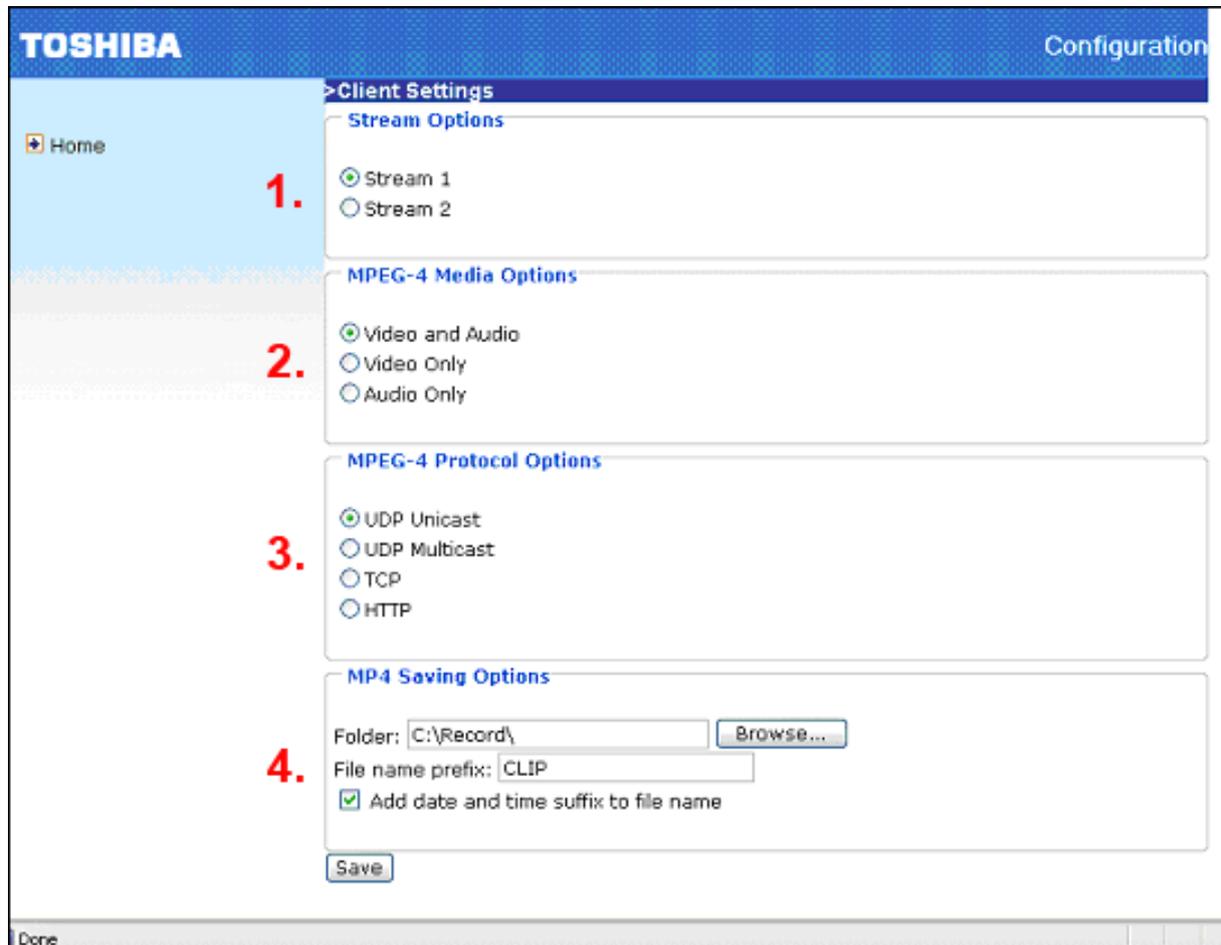
There are different frame sizes for stream 1 and stream 2.

The snapshot image will be of the larger frame size of the two.

Click on "**Snapshot**", web browser will pop up a new window to show the snapshot. Users can place the mouse pointer on the snapshot and click the right button of mouse to save it.



Client settings



There are four settings for the client side in IE.

1. The "**Stream Options**" is to select which one of the dual-streaming channels to monitor.
2. The "**MPEG-4 Media Options**" determines which media type to stream using the MPEG-4 mode.



User's features (Cont.)

3. The "**MPEG-4 Protocol Options**" allows choices of the connection protocol between client and server. The four protocol choices to optimize your usage are UDP unicast, UDP multicast, TCP and HTTP.
 - The **UDP Unicast** protocol allows for more real-time audio and video streams. However, some packets may be lost due to network burst traffic and images may be obscured.
 - The **UDP Multicast** protocol saves server bandwidth while serving multiple clients at the same time.
 - The **TCP** protocol allows for less packet loss and produces a more accurate video display. The downside with this protocol is that the real-time effect is worse than that with the UDP protocol.
 - The **HTTP** protocol allows the same quality as TCP protocol and the user don't need to open specific port to streaming under some network environment.

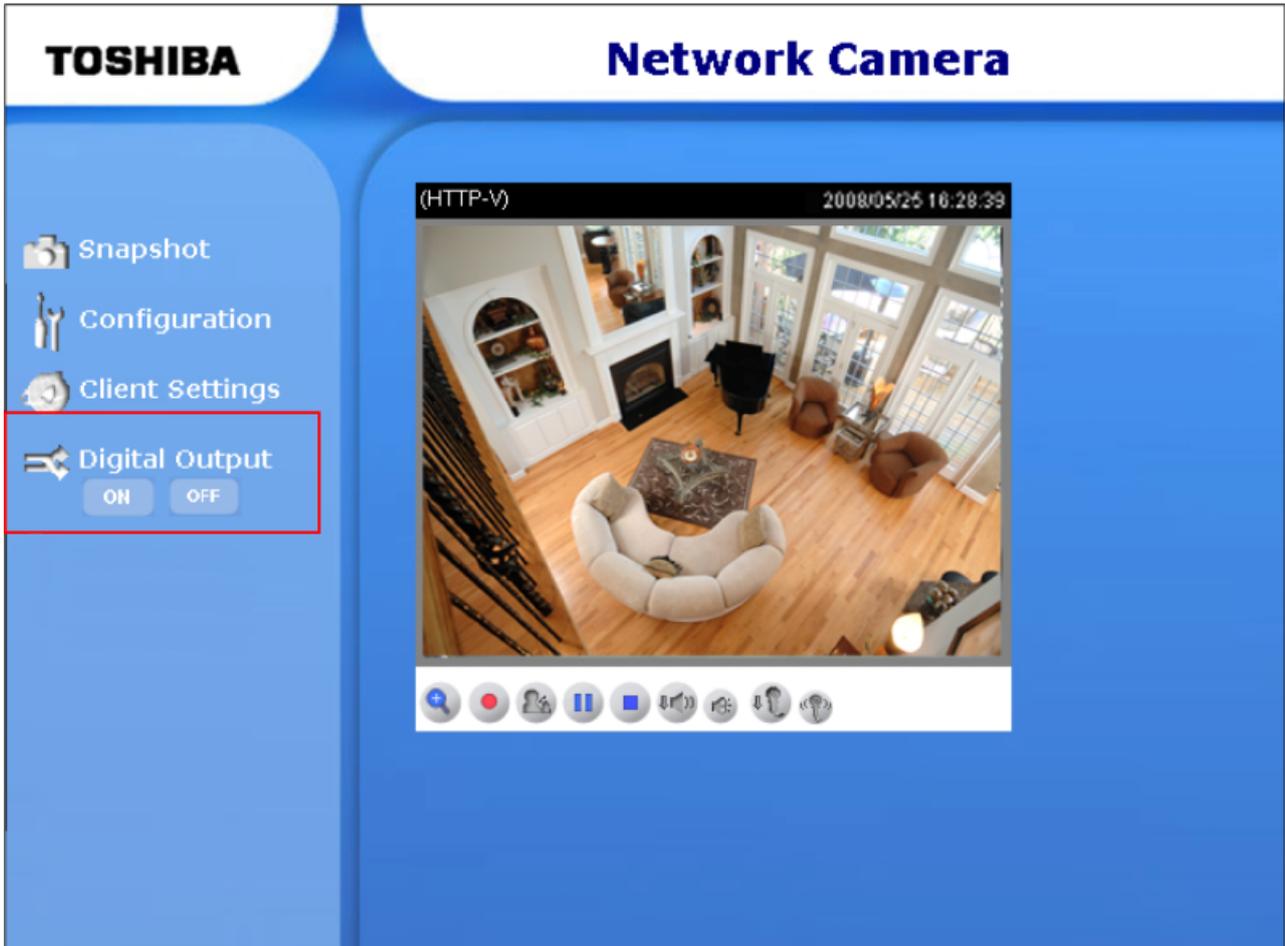
If no special need is required, UDP unicast protocol is recommended.

Generally speaking, the client's choice will be in the order of UDP multicast → UDP unicast → TCP → HTTP. After the Network Camera is connected successfully, "Protocol Option" will indicate the selected protocol. The selected protocol will be recorded in the user's PC and will be used for the next connection. If the network environment has changed, or the user wants to let the web browser again detect, manually select the UDP protocol, save, and return HOME to re-connect.

4. The "**MP4 Saving Options**" save the selections and can specify the recording folder, filename prefix and suffix.

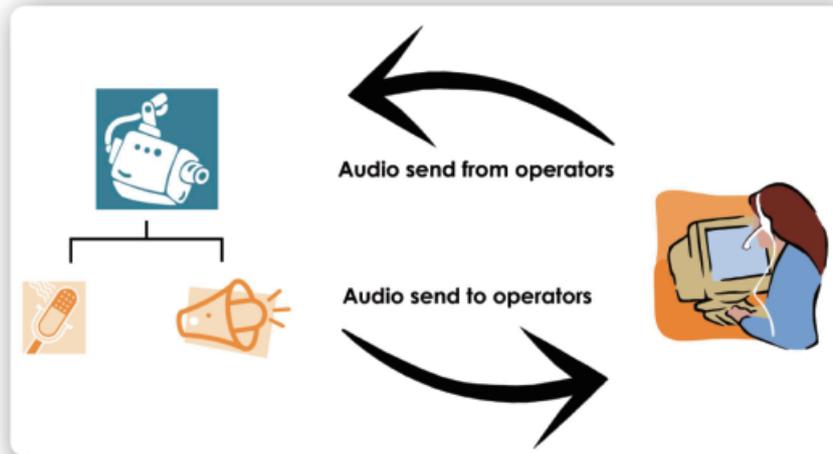
Digital output

Select "ON" to activate triggering of the digital output or "OFF" to return the digital output to the normal state.



User's features (Cont.)

Audio communication



The camera supports two-way audio communication in the MPEG-4 mode so that operators can transmit and receive audio simultaneously. By using the camera's microphone input and an external speaker, you can communicate and give instructions to people at the camera's location.

Note: Audio communication does not work with JPEG because JPEG only transmits a series of images to the client.

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

TOSHIBA Network Camera

Snapshot
Configuration
Client Settings
Digital Output
ON OFF

(UDP-AV/T) 20080526 13:24:07

Audio is being transmitted to the camera.

Administrator's features

Fine-tuning for Best Performance

Best performance generally equates to the fastest image refresh rate with the best video quality, and at the lowest network bandwidth as possible. The three factors, "Maximum frame rate", "Constant bit rate", and "Fixed quality" for MPEG-4 mode and "Maximum frame rate" and "Fixed quality" for JPEG mode on the Audio and Video Configuration page, are correlative to allow for achieving the best performance possible.

TOSHIBA Configuration

Audio and video

Video settings

Video title:

Color: Color

Power line frequency: 60 Hz

Video orientation: Flip Mirror

Maximum Exposure Time: Auto

Overlay title and time stamp on video and snapshot.

Video quality settings for stream 1

Mode: MPEG-4

Frame size: 640x480

Maximum frame rate: 30 fps

Intra frame period: 1 s

Video quality

Constant bit rate: 512 Kbps

Fixed quality: Good

Video quality settings for stream 2

Mode: MPEG-4

Frame size: 176x144

Maximum frame rate: 5 fps

Intra frame period: 1 s

Video quality

Constant bit rate: 40 Kbps

Fixed quality: Good

Audio Settings

Mute

Internal microphone input gain: -10.5 dB

External microphone input: 0db 20db

Audio type: AAC GSM-AMR

AAC bit rate: 128 Kbps

GSM-AMR bit rate: 12.2 Kbps

Version: 0100d

Administrator's features (Cont.)

For Best Real-time Video Images

To achieve good real-time visual effect, the network bandwidth should be large enough to allow a transmission rate of greater than 20 image frames per second. If the broadband network is over 1 Mbps, set the "Constant bit rate" to 1000Kbps or 1200Kbps, or set "Fixed quality" at the highest quality. The maximum frame rate is 30. If your network bandwidth is more than 512 Kbps, you can adjust the bit rate according to your bandwidth and set the maximum frame rate to 30 fps. If the images vary dramatically in your environment, you may want to slow the maximum frame rate down to 20 fps in order to lower the rate of data transmission. This allows for better video quality and the human eyes cannot readily detect the differences between those of 20, 25, or 30 frames per second. If your network bandwidth is below 512 Kbps, set the "Constant bit rate" according to your bandwidth and try to get the best performance by fine-tuning with the "Maximum frame rate". In a slow network, greater frame rate results in blur images. Video quality performance will vary somewhat due to the number of users viewing on the network; even when the parameters have initially been finely tuned. Performance will also suffer due to poor connectivity because of the network's burst constraint.

Only Quality Images Will Do

To have the best video quality, you should set "Fixed quality" at "Detailed" or "Excellent" and adjust the "Maximum frame rate" to match your network's bandwidth. If your network is slow and you receive "broken" pictures, go to the TCP or HTTP protocol in "MPEG-4 Protocol Options" and choose a more appropriate mode of transmission. The images may suffer a time delay due to a slower connection. The delay will also increase with added number of users.

Somewhere Between Real-time and Clear Images

If you have a broadband network, set "Fixed quality" at "Good" or better, rather than setting "Constant bit rate". You can also fix the bandwidth according to your actual network speed and adjust the frame rate. Start from 30 fps down for best results but not below 15 fps. If the image qualities are not improved, select a lower bandwidth setting.

Opening accounts for new users

TOSHIBA Configuration

>Security

Home
System
Security
Network
DDNS
Access list
Audio and video
Motion detection
Application
Recording
System log
View parameters
Maintenance

Version: 0100d

1

Root Password

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

Root Password:

Confirm root password:

Save

2

Add User

User name:

User password:

Account type:

Administrator
 Operator
 Viewer

Add

3

Manage User

User name:

User password:

Account type:

Administrator
 Operator
 Viewer

Save Delete

Protect Network Camera by passwords

The Network Camera is shipped without any password by default. That means everyone can access the Network Camera including the configuration as long as the IP address is known. It is necessary to assign a password if the Network Camera is intended not to be accessed by others. Type a new word twice in [1] to enable protection. This password is used to identify the administrator. Then add an account with user name, password and authentication for your friends in [2]. You can edit or delete users from [3].

Administrator's features (Cont.)

Build a security application

The Administrator can use the built-in motion detection to monitor any movement to perform many useful security applications. To upload the snapshots, users can choose either email, FTP, HTTP or Network storage according to user's needs. All server settings are in the Server section on the Application page. Refer to the definition section for detail configuration.

1. Click on "**Configuration**" on the home page.
2. Click on "**Motion detection**" in the left column.
3. Check "Enable motion detection".
4. Click on "**New**" to have a new window to monitor video.
5. Type in a name to identify the new window.
6. Use the mouse to click, hold, and drag the window corner to resize or the title bar to move the window.
7. Fine-tune using the "Sensitivity" and "Percentage" fields to best suit the camera's environment. Higher "Sensitivity" detects the slighter motion. Higher "Percentage" discriminates smaller objects.
8. Clicking on "Save" enables the activity display. Green means the motion in the window is below the threshold and red means it is over the threshold.
9. Click on "**Application**" in the left column.
10. Add a server in the server section.
11. Add a media with snapshot type in media section. Set the number of pre-event and post-event images to be uploaded.
12. Add a event in event section.
 - Enter one event name and enable this event.
 - Check the weekdays as you need and give the time interval to monitor the motion detection every day.
 - Select the Trigger on Motion detection and Check the window name set in step 5.
 - Set the appropriate delay time to avoid continuous false alarms following the original event.
 - Check the server name set in Step 10 and select the media name set in Step 11.
13. Click on "Save" to save the settings.

Software revision upgrade

Obtain up-to-date software from the Toshiba web site (<http://www.toshibasecurity.com>). An easy-to-use Upgrade Wizard is provided to upgrade the Network Camera with just a few clicks. The upgrade function is available to only the Administrator. To upgrade the system, follow the procedures below.

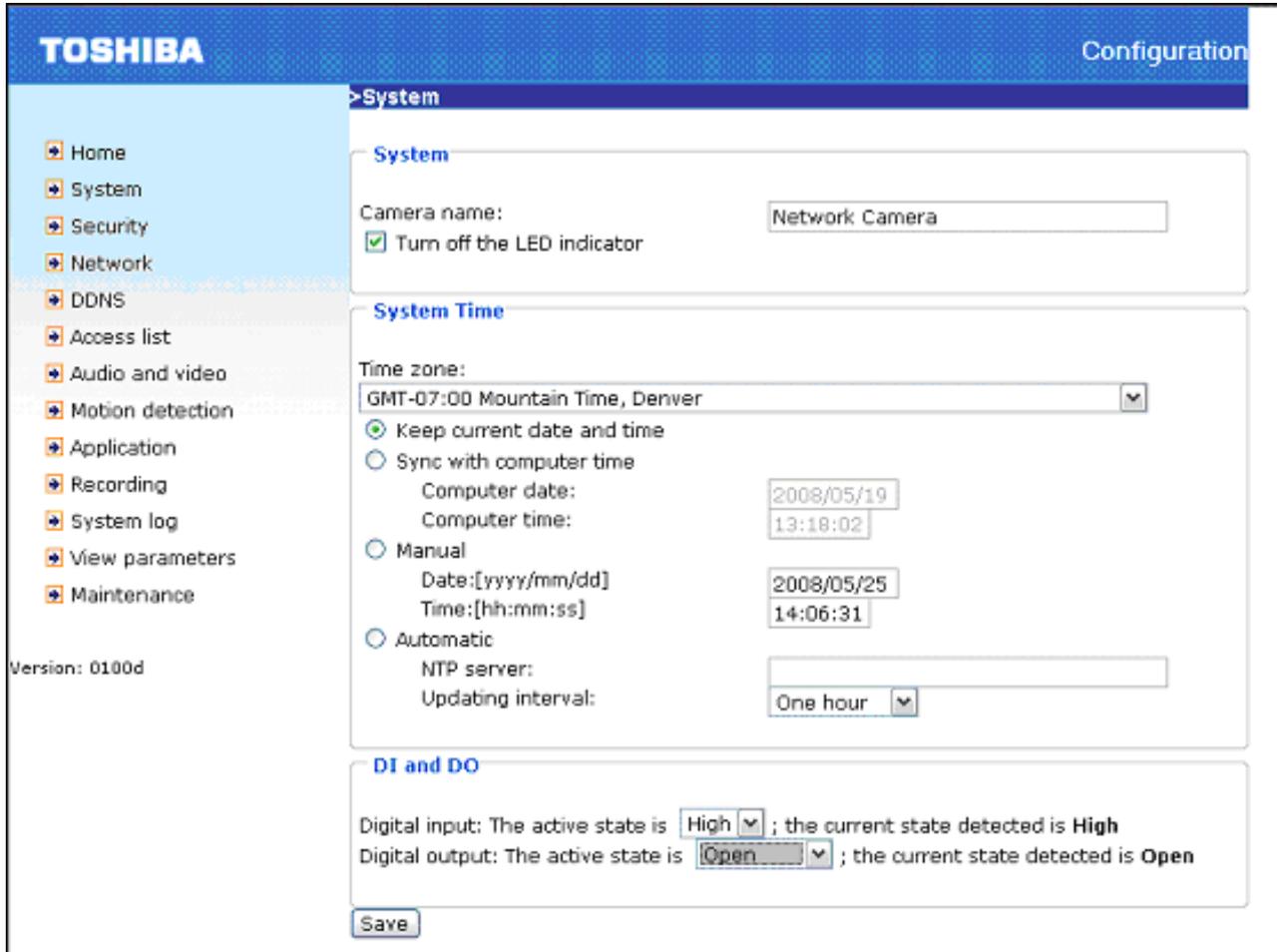
1. Download the firmware file named "xxx.pkg" from the appropriate product folder.
2. Run the Installation Wizard and proceed by following the prompts. Refer to the instructions of the Installation Wizard on CD-ROM for details.
3. Or upgrade firmware from Maintenance settings directly.
4. The entire process will finish in a few minutes and then automatically restart the system.



If power fails during the writing process to the Flash memory, the program in the memory of the Network Camera could be permanently destroyed. If the Network Camera does not restart properly, ask your dealer for technical service.

Definitions in Configuration

Only the Administrator can access system configuration. Each category in the left column will be explained in the following pages. The bold texts are the feature sets on the Option pages. The Administrator may type the URL below the figure to directly enter the configuration frame page.



<url> http://<Network Camera>/setup/system.html

<Network Camera> is the domain name or original IP address of the Network Camera.



System parameters

"Camera name" The text displays the title at the top of the main page.

"Turn off the LED indicator" Select this option to shut off the LED.

"Time zone" Adjust the time with that of the time-servers for local settings.

"Keep current date and time" Click on this to reserve the current date and time of the Network Camera. An internal real-time clock maintains the date and time even when the power of the system is turned off.

"Sync with computer time" Synchronize the date and time of the Network Camera with the local computer.

"Manual" Adjust the date and time according to what is entered by the Administrator. Notice the format in the related fields while doing the entry. Network Camera starts up. It will fail if the assigned time-server cannot be reached.

"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 hourly, daily, weekly, or monthly to update the time on the NTP server.

"Digital input" Select High or Low to define normal status of the digital input. The current status is shown, too.

"Digital output" Select Grounded or Open to define normal status of the digital output. The current status is shown, too.

Click on the button to save all the changes. Otherwise, the correct time will not be synchronized.

Security settings

Introduction

Installation

How to Use

Definitions in Configuration

Appendix

The screenshot shows the Toshiba Configuration page for Security settings. The page has a blue header with 'TOSHIBA' on the left and 'Configuration' on the right. A navigation menu on the left lists: Home, System, Security (selected), Network, DDNS, Access list, Audio and video, Motion detection, Application, Recording, System log, View parameters, and Maintenance. The main content area is titled '> Security' and contains three sections: 1. 'Root Password' section with a note: 'Note: Leaving the root password field empty leaves the camera unprotected.' It has two text boxes for 'Root Password:' and 'Confirm root password:', and a 'Save' button. 2. 'Add User' section with text boxes for 'User name:', 'User password:', and 'Account type:'. The 'Account type' has three radio buttons: 'Administrator' (selected), 'Operator', and 'Viewer'. There is an 'Add' button below. 3. 'Manage User' section with a dropdown menu for 'User name:', text boxes for 'User password:' and 'Account type:', and the same three radio buttons for 'Account type'. There are 'Save' and 'Delete' buttons at the bottom. The version '0100d' is noted at the bottom left of the configuration area.

<url> <http://<Network Camera>/setup/security.html>

<Network Camera> is the domain name or original IP address of the Network Camera.

“Root password” Change the Administrator's password by typing in the new password identically in both text boxes. The typed entries will be displayed as asterisks for security purposes. After pressing **Save**, the Administrator will have to enter the new password to access the menu.

“Add user” Type the new user's name and password and press **Add** to insert the new entry. The new user will be displayed in the user name list. There is a maximum of twenty user accounts. There are three kinds of authentication: Administrator, Operator and Viewer. Administrator can fully control the camera operation. Operator can modify most of the camera's parameters except some privilege and network options. Viewer can view, listen and control Digital Input/Digital Output of camera. Network Camera can provide twenty accounts for your valuable customers or friends.

“Manage user” Pull down the user list to find the user's name and press **Delete** to delete the selected user. Or edit the password or authentication of the selected user and press **Save** to take effect.

Network settings

TOSHIBA Configuration

> Network

Network Type

LAN

Get IP address automatically

Use fixed IP address

IP address: 192.168.100.151

Subnet mask: 255.255.255.0

Default gateway: 192.168.100.1

Primary DNS: []

Secondary DNS: []

Primary WINS server: []

Secondary WINS server: []

Enable UPnP presentation

Enable UPnP port forwarding

PPPoE

User name: []

Password: []

Confirm password: []

Save

HTTP

Authentication: basic

HTTP port: 80

Secondary HTTP port: 8080

Access name for stream 1: video.mjpg

Access name for stream 2: video2.mjpg

Two way audio

Two way audio port: 5060

FTP

FTP port: 21

RTSP Streaming

Authentication: disable

Access name for stream 1: live.sdp

Access name for stream 2: live2.sdp

RTSP port: 554

RTP port for video: 5556

RTCP port for video: 5557

RTP port for audio: 5558

RTCP port for audio: 5559

Multicast settings for stream 1

Always multicast

Multicast group address: 239.128.1.99

Multicast video port: 5560

Multicast RTCP video port: 5561

Multicast audio port: 5562

Multicast RTCP audio port: 5563

Multicast TTL [1~255]: 15

Multicast settings for stream 2

Always multicast

Multicast group address: 239.128.1.100

Multicast video port: 5564

Multicast RTCP video port: 5565

Multicast audio port: 5566

Multicast RTCP audio port: 5567

Multicast TTL [1~255]: 15

Save

<http://<Network Camera>/setup/network.html>

<Network Camera> is the domain name or original IP address of the Network Camera.

Any changes made on the Network Type section will restart the system in order to save the changes. Make sure every field is entered correctly before clicking on **Save**.

Network settings (Cont.)

Network type

“LAN” & “PPPoE”

The default type is LAN. Select PPPoE if using ADSL.

“Get IP address automatically” & “Use fixed IP address”

The default status is **“Get IP address automatically”**. This can be tedious having to perform software installation whenever the Network Camera starts. Therefore, once the network settings, especially the IP address, have been entered correctly, select **“Use fixed IP address”** then the Network Camera will skip installation at the next boot. The Network Camera can automatically restart and operate normally after a power outage.

Note: Users can run IP installer to check the IP address assigned to the Network Camera if the IP address is forgotten or using the UPnP function provided by the Network Camera (MS Windows XP provides UPnP function at My Network Place).

“IP address” By selecting "Use fixed IP address", the administrator can modify this address. This address is required for network identification.

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

“Default gateway” The gateway used to forward frames to destinations in a different subnet. Invalid router setting will fail the transmission to destinations in a different subnet.

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

“Secondary DNS” Secondary domain name server that backups the Primary DNS.

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

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

“Enable UPnP presentation” Enable the UPnP camera short cut.

“Enable UPnP port forwarding” Enable the UPnP port forwarding.

“PPPoE” If using the PPPoE interface, fill the following settings from ISP.

“User name” The login name of PPPoE account.

“Password” The password of PPPoE account.

“Confirm password” Input password again for confirmation.

HTTP

“Authentication” Supports basic and digest modes.

“HTTP port” This can be other than the default Port 80. Once the port is changed, the users must be notified the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the Network Camera whose IP address is 192.168.0.100 from 80 to 8888, the users must type in the web browser "http://192.168.0.100:8888" instead of "http://192.168.0.100".

“Secondary HTTP port” Supports for an alternate port to access the HTTP server.

“Access name for stream 1” Access URL of stream 1 for making connection from the client software when using the JPEG codec.

“Access name for stream 2” Access URL of stream 2 for making connection from the client software when using the JPEG codec.

Using http://<ip address>:<http port>/<access name> to make connection.

Two way audio

“Two way audio port” This is the port for using two way audio communication.

FTP

“FTP port” This port can change from the default value of 21 to between 1025 to 65535. The external FTP server port must match the chosen number.

Network settings (Cont.)

RTSP Streaming

“Authentication” It supports disable, basic and digest modes.

“Access name for stream 1” Access URL of stream 1 for making connection from the client software when using the MPEG-4 codec.

“Access name for stream 2” Access URL of stream 2 for making connection from the client software when using the MPEG-4 codec.

Using `rtsp://<ip address>/<access name>` to make connection.

“RTSP port” The port can be changed to another number other than the default Port 554.

“RTP port for video” The video channel port for RTP must be an even number.

“RTCP port for video” The video channel port for RTCP must be the port number of video RTP plus 1.

“RTP port for audio” The audio channel port for RTP must be an even number.

“RTCP port for audio” The audio channel port for RTCP must be the port number of audio RTP plus 1.

User can modify Multicast setting for stream1 and stream2.

“Always multicast” Select it to enable when connecting over 10 multicast clients.

“Multicast group address” Used by sources and the receivers to send and receive content.

“Multicast video port” The video channel port for multicast must be an even number.

“Multicast RTCP video port” The video channel port for multicast RTCP must be the port number of multicast video port plus 1.

“Multicast audio port” The audio channel port for multicast must be an even number.

“Multicast RTCP audio port” The audio channel port for multicast RTCP must be the port number of multicast audio port plus 1.

“Multicast TTL” Specifies the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network.

“Enable DDNS” Turns on the DDNS function.

“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.

ChangelP.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 field is necessary for logging into the DDNS server or to notify the User of the new IP address.

Note: When this field is input as "User Name", the following field 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.

TOSHIBA Configuration

>DDNS

DDNS: Dynamic domain name service

Enable DDNS

Provider

Camera name

User name

Password

Save

ersion: 0100d

- Home
- System
- Security
- Network
- DDNS
- Access list
- Audio and video
- Motion detection
- Application
- Recording
- System log
- View parameters
- Maintenance

Access List

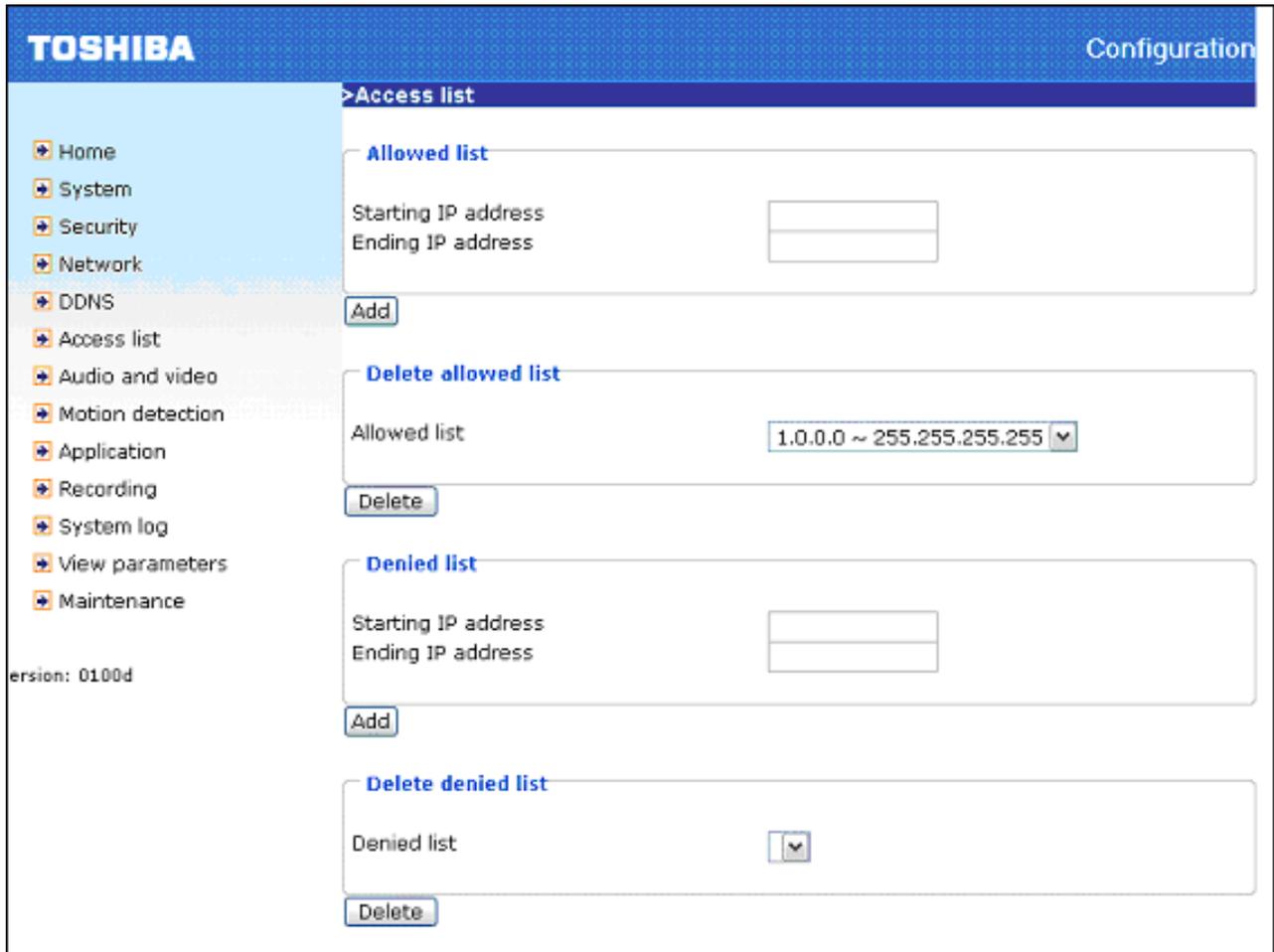
Introduction

Installation

How to Use

Definitions in Configuration

Appendix



<url> <http://<Network Camera>/setup/accesslist.html>

<Network Camera> is the domain name or original IP address of the Network Camera.

The access lists are to control the client's status by checking the client's IP address.

The two lists for permission control are the **Allowed list** and **Denied list**.

The two lists for permission control are the **Allowed list** and **Denied list**. The clients whose IP address is in the **Allowed list** can connect to the Network Camera for receiving the audio/video streaming. To add a new IP address range, type the **Starting IP address** and **Ending IP address** in the text boxes and click on the **Add** button. To remove an existing IP address range, select the address from the pull-down menu and click on the **Delete** button. Both the **Allowed list** and **Denied list** can each have 10 entries.

Audio and Video

TOSHIBA Configuration

>Audio and video

Video settings

Video title:

Color:

Power line frequency:

Video orientation: Flip Mirror

Maximum Exposure Time:

Overlay title and time stamp on video and snapshot.

Video quality settings for stream 1

Mode:

Frame size:

Maximum frame rate:

Intra frame period:

Video quality

Constant bit rate:

Fixed quality:

Video quality settings for stream 2

Mode:

Frame size:

Maximum frame rate:

Intra frame period:

Video quality

Constant bit rate:

Fixed quality:

Audio Settings

Mute

Internal microphone input gain:

External microphone input: 0db 20db

Audio type: AAC GSM-AMR

AAC bit rate:

GSM-AMR bit rate:

<http://<Network Camera>/setup/audiovideo.htm>

<Network Camera> is the domain name or original IP address of the Network Camera.

This product supports dual-stream. It provides two setting for video streams, but only one setting for audio.

Audio and Video (Cont.)

Video Settings

Introduction

“Video title” The text string can be displayed on video.

“Color” Selects either color or monochrome video display.

“Power line frequency” Fluorescent lights flash according to the power line frequency. Change the frequency setting to eliminate uncomfortable flash images when the light source is only fluorescent lighting.

“Video orientation”

- **Flip:** Vertically rotate the video.
- **Mirror:** Horizontally rotate the video.

Note: Check both options if the Network Camera is installed upside down.

Installation

“Maximum Exposure Time” Adjust the maximum exposure time in different environment.

- **Overlay title and time stamp on video and snapshot:** Check if the title is to be shown on video.

How to Use

There are different video quality settings for stream1 and stream2.

- **Mode:** If MPEG-4 is selected, streaming is in RTSP protocol. If JPEG is selected, streaming is in server push mode.
- **Frame size:** In either the MPEG-4 mode or the JPEG mode, the three options are **"176x144"**, **"320x240"** and **"640x480"**.

MPEG-4 mode has three dependent parameters for video performance adjustment.

“Maximum frame rate” Limits the maximum refresh frame rate which can be combined with the **“Video quality”** to optimize bandwidth utilization and video quality.

“Intra frame period” The interval of intra frame.

“Video quality” settings are:

“Constant bit rate” Fixes the bandwidth utilization regardless of the video quality.

“Fixed quality” Select the desired video quality.

Note: The video quality may be poor due to the sending of the maximum frame rate within the limited bandwidth when images are moving rapidly. Consequently, to ensure detailed video quality (quantization rate) regardless of the network, it will utilize more bandwidth to send the maximum frames when images change drastically.

JPEG mode is limited to two parameters **“Maximum frame rate”** and **“Video quality”** to adjust the video performance.

Definitions in Configuration

Appendix

Audio Settings

“Mute” Turn off audio.

“Internal microphone input gain” Modify the gain of the internal microphone input.

“External microphone input” There are two gain options, 0db and 20db.

“Audio type” Select audio codec **“AAC”** or **“GSM-AMR”** and the bit rate.

Audio and Video (Cont.)

Image Settings

Introduction

Installation

How to Use

Definitions in Configuration

Appendix

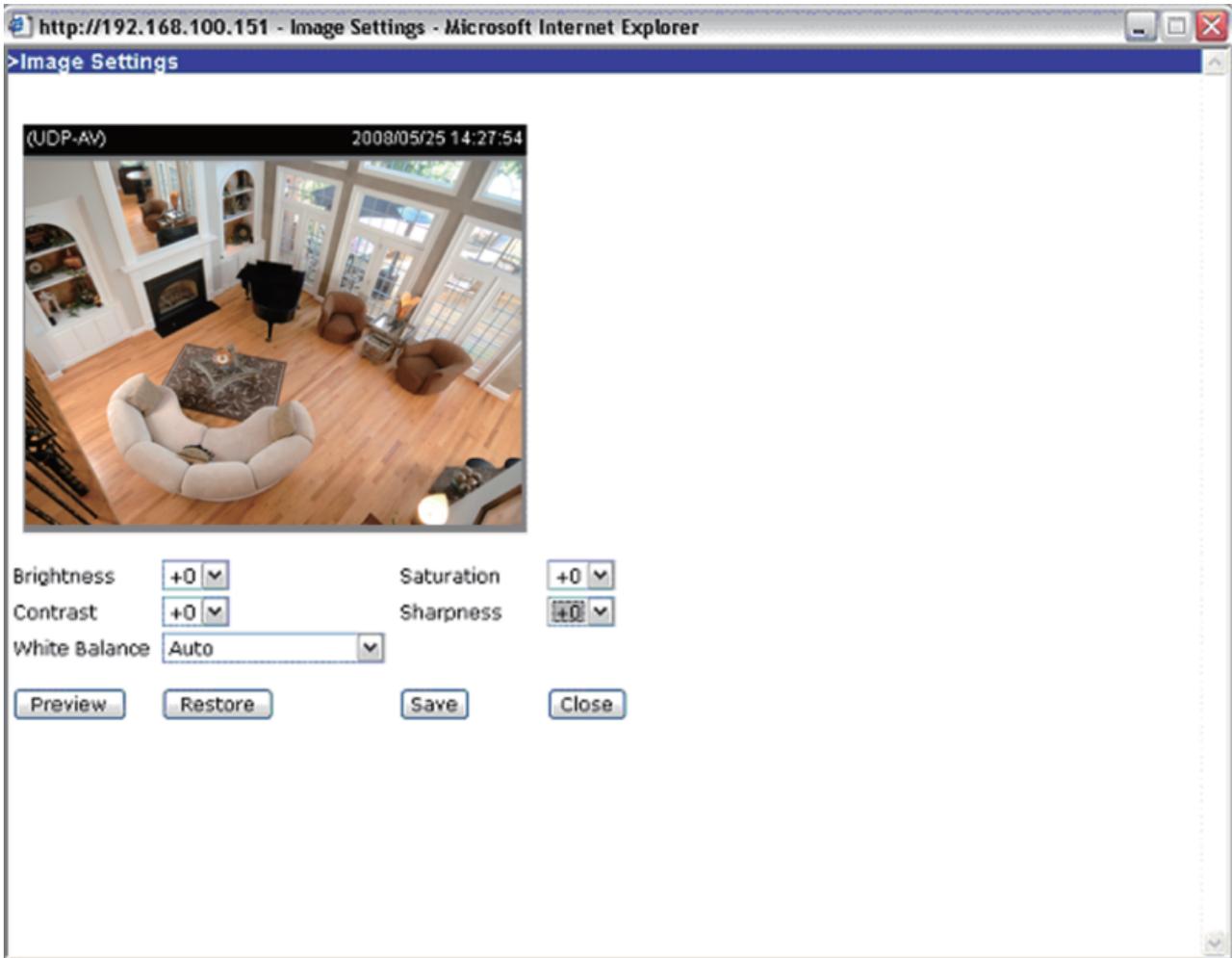
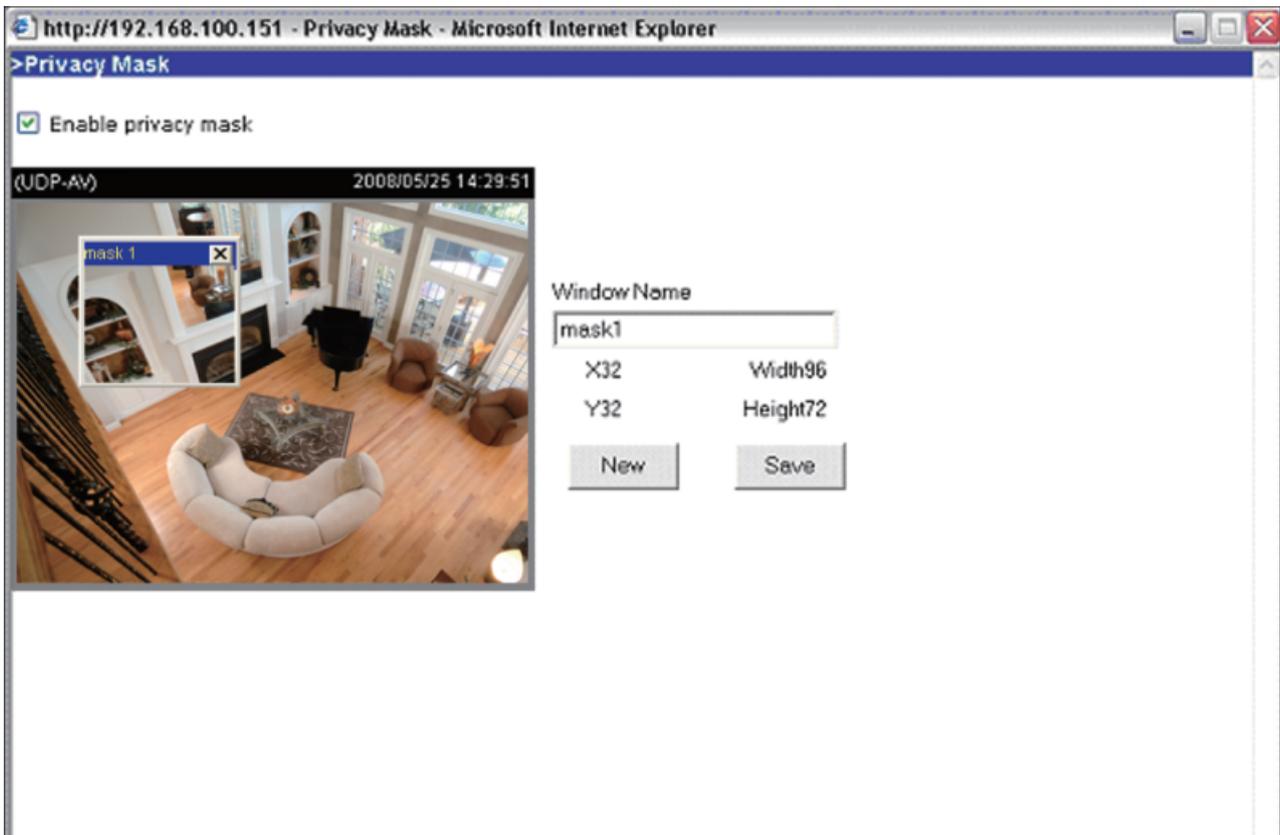


Image Settings Click on this button to pop up another window to tune "**Brightness**", "**Contrast**", "**White Balance**", "**Saturation**" and "**Sharpness**" for video compensation. Each field has eleven levels ranging from -5 to +5 except "**White Balance**" which has "**Auto**" or "**Keep current value.**" In "**Brightness**" and "**Contrast**" fields the value 0 indicates auto tuning. The user may press **Preview** to fine-tune the image. When the image is O.K., press **Save** to set the image settings. Click on **Restore** to recall the original settings without incorporating the changes.

Privacy Mask



Click on the button to pop open another window to set the privacy mask window. Users can not view the blocked area or areas as set in privacy mask window.

“Enable privacy mask” Check this option to turn on privacy mask.

New Click on this button to add a new window. At most five windows can exist simultaneously. Use the mouse to click, hold, and drag the window frame to resize or the title bar to move. Clicking on the 'x' at the upper right-hand corner of the window deletes the window. The base of window axis is eight. You can see the X, Y, width and height of the window.

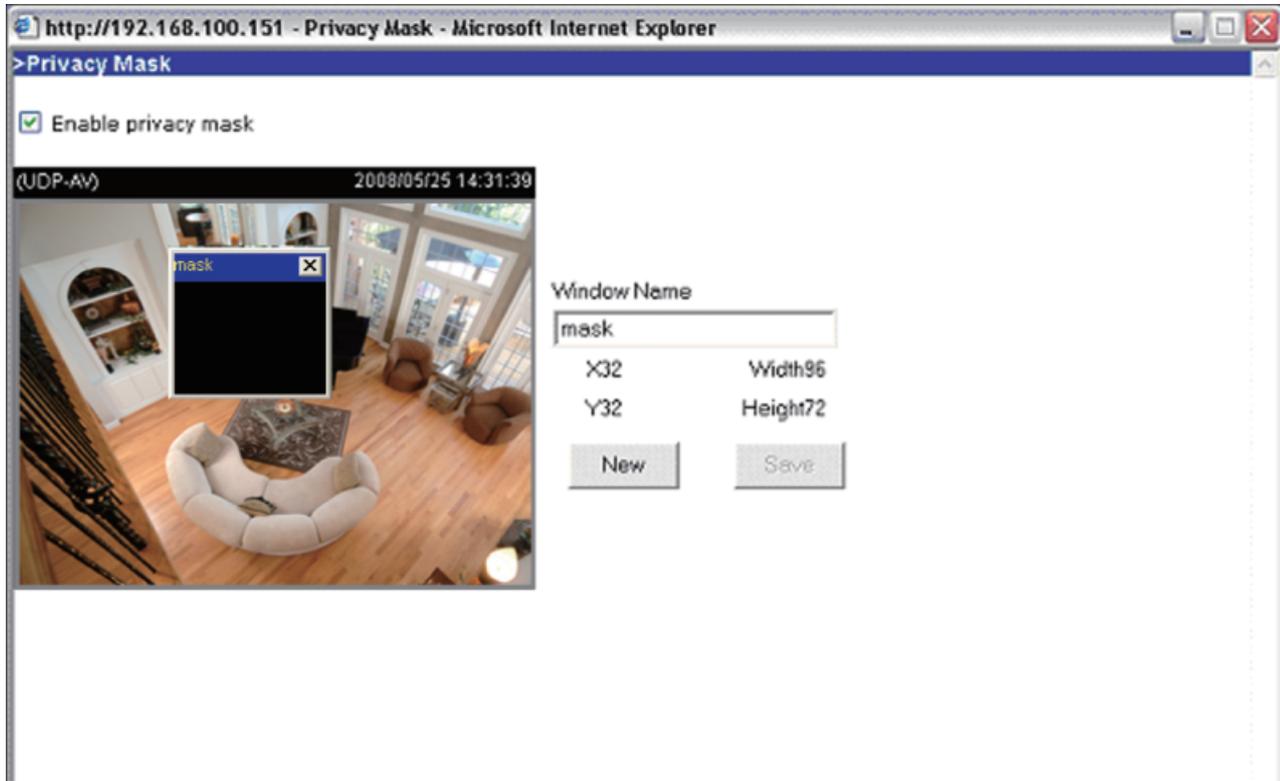
Save Click on this button to save the settings.



Audio and Video (Cont.)

"Window Name" The text will show at the top of the window.

The following figure shows the screen when is clicked and the privacy mask is enabled.



Motion detection

“Enable motion detection” Check this option to turn on motion detection.

New Click on this button to add a new window. At most three windows can exist simultaneously. Use the mouse to click, hold, and drag the window frame to resize or to move the title bar. Clicking on the 'x' at the upper right-hand corner of the window deletes the window.

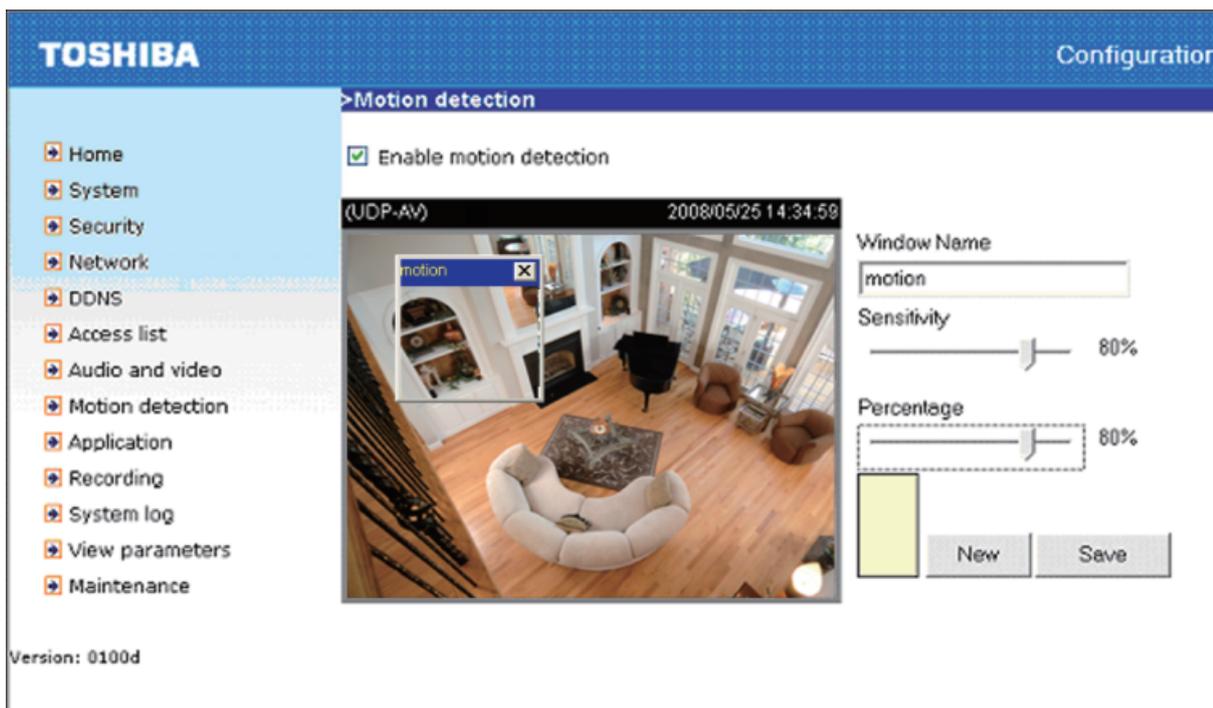
Save Click on this button to save the settings. A graphic bar will rise or fall depending on the image variation. A green bar means the image variation is under monitoring level and a red bar means the image variation is over monitoring level. When the bar goes red, the detected window will also be outlined in red. Going back to the homepage, the monitored window is hidden but the red frame shows when motion is detected.

"Window Name" The text will show at the top of the window.

“Sensitivity” This sets the endurable difference between two sequential images.

“Percentage” This sets the space ratio of moving objects in the monitoring window. Higher sensitivity and small percentage will allow easier motion detection.

The following figure shows the screen when **Save** is clicked.



<url> <http://<Network Camera>/setup/motion.htm>

<Network Camera> is the domain name or original IP address of the Network Camera.



Application

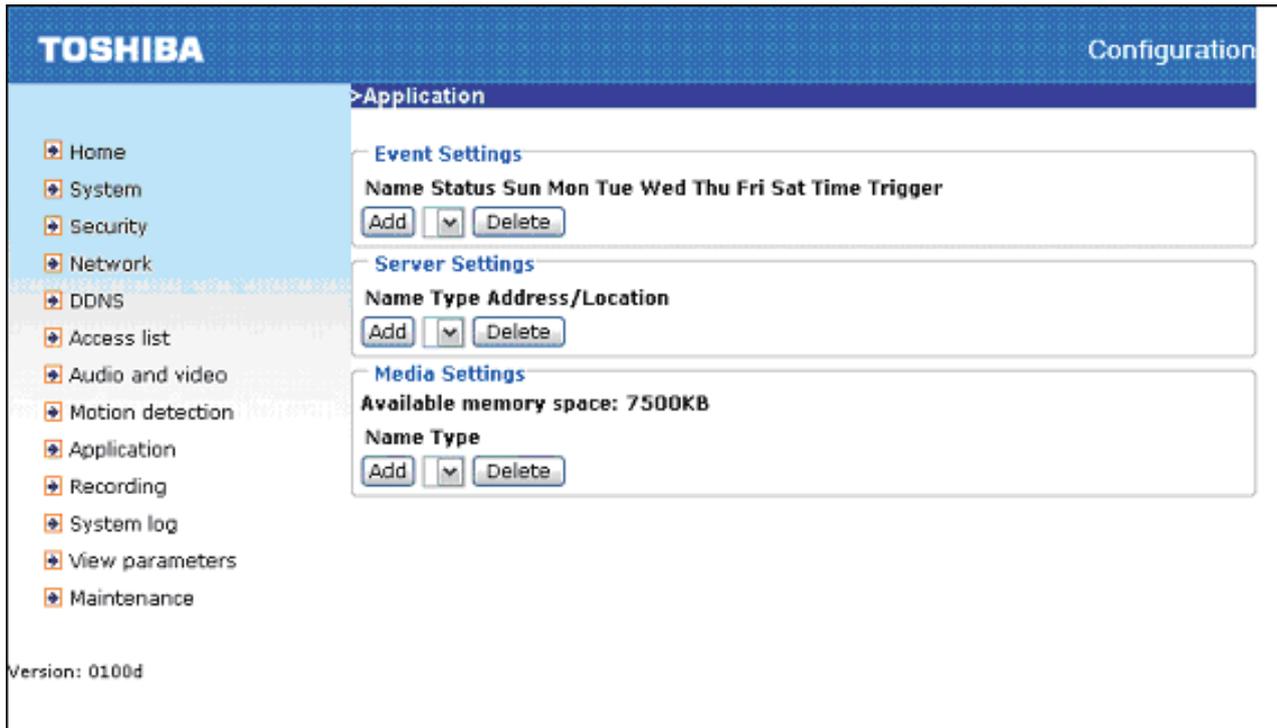
Introduction

Installation

How to Use

Definitions in Configuration

Appendix



`<url> http://<Network Camera>/setup/application.htm`

`<Network Camera>` is the domain name or original IP address of the Network Camera.

There are three sections in application page. They are event, server and media. Click **Add** to pop a window to add a new item of event, server or media. Click **Delete** to delete the selected item from event, server or media. Click on the item name to pop a window to edit it.

There can be at most three events. There can be at most five server and five media configurations.

User can know the event name, status, weekly and time schedule and trigger type in event section. The server name, type and address/location are shown in server section.

The current media free space, media name and type are shown in media section. After adding a new media, the value of free space will be updated. User cannot add media which size is larger than media free space.

It is suggested to set server and media first before setting event. The servers and media selected in event list are not modified or deleted. Please remove them first from the event if you want to delete or modify them. Recommend that using different media in different event to make use all media be produced and received correctly. If using the same media in different events and the events trigger almost simultaneously, the servers in the second triggered event will not receive any media; there would be only notifications.

Event

A maximum of three events can be registered.

“Event name” Unique name for the event.

“Enable this event” Check to enable this event.

“Priority” The event with highest priority will be executed first.

“Delay second(s) before detecting next event” Delay, in seconds, to check the next event setting. This setting is used in motion detection and digital input trigger type.

And the four kinds of trigger are supported.

“Video motion detection” Select the windows which need to be monitored.

“Periodically” The event is triggered in minutes at specified intervals.

“Digital input” To monitor digital input.

“System boot” The event is triggered when the system boots up. The weekly and time schedules are provided.

“Sun” ~ “Sat” Select the days of the week to perform the event.

“Time” show **“Always”** or input the time interval.

The default action is triggered digital output. If there are servers configured, the user can select them from **“Server name”**, too.

“Trigger digital output” Check it to trigger digital output for specific seconds when event is triggered.

The screenshot shows the 'Event Settings' window with the following configuration:

- Event name:** [Empty text box]
- Enable this event:**
- Priority:** Normal (dropdown menu)
- Detect next event after:** 10 second(s)
- Trigger:**
 - Video motion detection
Detect motion in window
Note: Please configure [Motion detection](#) first
 - Periodically
Trigger every other 1 minutes
 - Digital input
 - System boot
- Event Schedule:**
 - Sun Mon Tue Wed Thu Fri Sat
 - Time:**
 - Always
 - From 00:00 to 24:00 [hh:mm]
- Action:**
 - Trigger digital output for 1 seconds

Buttons: Save, Close

Application (Cont.)

Server

A maximum of five servers can be registered.

“Server name” The unique server name.

The four kinds of servers supported are email server, FTP server, HTTP server and network storage.

Email Server Settings.

“Sender email address” Email address of the sender.

“Recipient email address” Email address of the recipient.

“Server address” Domain name or IP address of the external email server.

“User name” User name on the external email server.

“Password” Password on the external email server.

FTP Server Settings.

“Server address” Domain name or IP address of the external FTP server.

“Server port” The default port is port 21 but this number can be changed to any value from 1025 to 65535.

“User name” User name on the external FTP server.

“Password” Password on the external FTP server.

“FTP folder name” Name of folder on the external FTP server. The string must conform to that of the external FTP server. Some FTP servers cannot accept preceding slash symbol before the path without virtual path mapping. Refer to the instructions for the external FTP server for details. The folder privilege must be open for upload.

“Passive Mode” Check to enable transmission passive mode.

HTTP Server Settings.

“URL” URL to upload the media.

“User name” User name on the external HTTP server.

“Password” Password on the external HTTP server.

Network Storage Settings. Only one network storage is supported.

“Network storage location” Path to upload the media.

“Workgroup” Workgroup for network storage.

“User name” User name on the network storage.

“Password” Password on the network storage.

After entering the server settings, the user can click on to test whether the settings are correct. The testing result will be shown in a pop-up window.

Server Settings

Server name:

Server Type

Email

Sender email address:

Recipient email address:

Server address:

User name:

Password:

FTP

Server address:

Server port:

User name:

Password:

FTP folder name:

Passive mode

HTTP

URL:

User name:

Password:

Network storage

Network storage location:

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

Workgroup:

User name:

Password:

Application (Cont.)

Media

A maximum of five medias can be registered.

“Media name” The unique name for media.

There are three kinds of media. They are snapshot, video clip and system log.

Snapshot Settings.

“Source” Select the source of the stream; stream1 or stream2.

“Send pre-event images” Number of pre-event images.

“Send post-event images” Number of post-event images.

“File Name Prefix” The prefix name will be added on the file name of the snapshot images.

“Add date and time suffix to file name” Check to add timing information as file name suffix.

Video Clip Settings.

“Source” Select the source of the stream; stream1 or stream2.

“Pre-event recording” Interval of pre-event recording in seconds.

Note: The two limitations for video clip file are **“Maximum duration”** and **“Maximum file size”**.

“Maximum duration” Maximum recording file duration in seconds.

“Maximum file size” Maximal file size that would be generated.

“File name prefix” The prefix name will be added on the file name of the video clip.

The screenshot shows a configuration window titled ">Media". The "Media name" field contains "Snapshot". Under "Media type", three options are listed: "Snapshot" (selected), "Video Clip", and "System log".

Snapshot settings:

- Source: Stream1 (dropdown)
- Send 1 pre-event image(s) [0~7]
- Send 1 post-event image(s) [0~7]
- File Name Prefix: Snapshot
- Add date and time suffix to file name

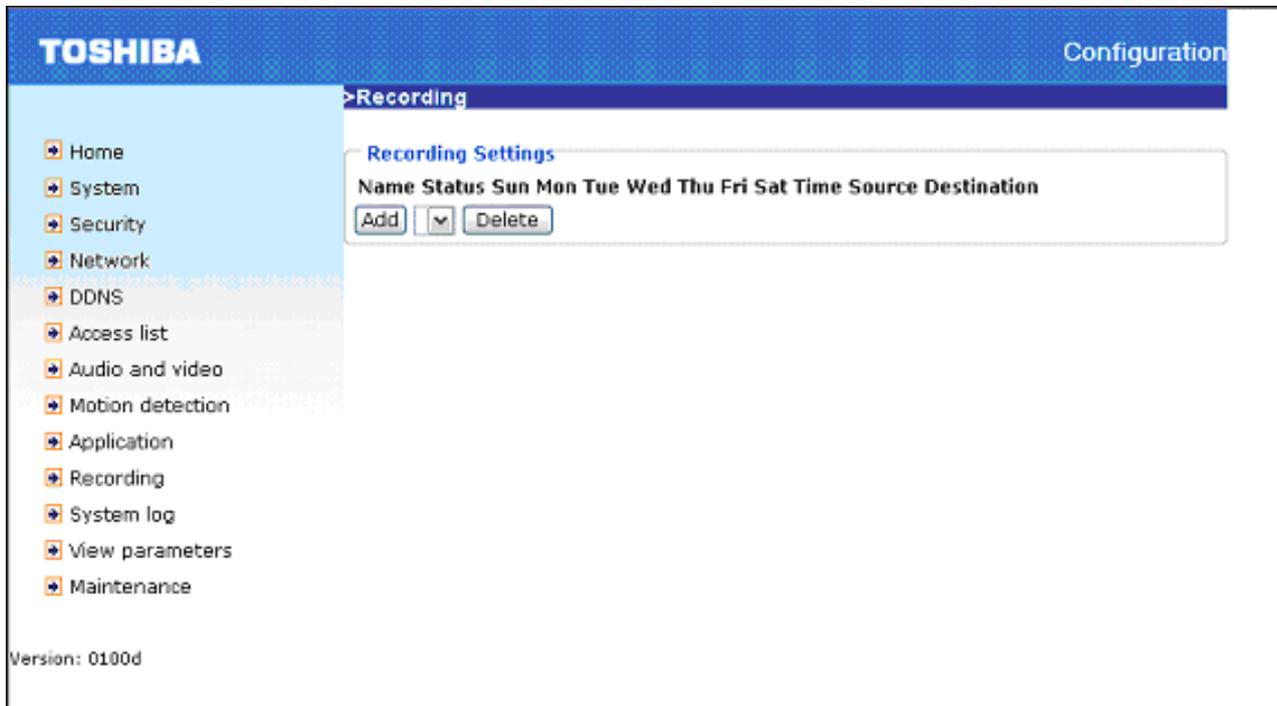
Video Clip settings:

- Source: Stream1 (dropdown)
- Pre-event recording: 0 seconds [0~9]
- Maximum duration: 5 seconds [1~10]
- Maximum file size: 500 Kbytes [50~800]
- File Name Prefix: (empty field)

Buttons: Save, Close

Recording

The Network camera supports recording on network storage. Setting up editing recording is the same as in application page. Recording name, status, weekly and time schedule, stream source and destination of recording must be entered. There can be at most two recording entries. To record on network storage, add the network storage server in application page first.



`<url> http://<Network Camera>/setup/recording.htm`

`<Network Camera>` is the domain name or original IP address of the Network Camera.

“Recording name” Unique name for recording entry.

“Enable this recording” Check to enable this event.

“Priority” The recording with higher priority will be executed first.

“Source” Select the source of the stream: stream 1 or stream 2.

Weekly and Time Schedule Settings.

“Sun” ~ “Sat” Select the days of the week.

“Time” Select **“Always”** or input the time interval.

“Destination” Select the network storage server.

“Max. recording capacity” Total size for cycle recording in Kbytes.

“File size for each recording” Single file size in Kbytes.

“File Name Prefix” The prefix name will be added on the file name of the recording.



Recording (Cont.)

Introduction

Installation

How to Use

Definitions in Configuration

Appendix

>Recording

Recording name:

Enable this recording

Priority: Normal

Source: Stream1

Recording Schedule

Sun Mon Tue Wed Thu Fri Sat

Time

Always

From to [hh:mm]

Destination

Max. recording capacity
(Old file will be overwritten after reaching maximum recording capacity.): Kbytes [1000~200000000]

File size for each recording: Kbytes [200~6000]

File name prefix:

System log

The Network camera support logs the system messages on a remote server. The protocol is compliant to RFC 3164. If using an external Linux server with syslogd service, use "-r" option to turn on the facility for receiving the log from remote machine. Or you can use some software on Windows which is compliant to RFC 3164.

Check **"Enable remote log"** and input the **"IP address"** and **"port"** number of the log server to enable the remote log facility.

In the **"Current log"**, it displays the current system log file. The content of the log provides useful information about configuration and connection after system boot-up.

The screenshot shows the Toshiba Network Camera Configuration interface. The left sidebar contains a navigation menu with options: Home, System, Security, Network, DDNS, Access list, Audio and video, Motion detection, Application, Recording, System log, View parameters, and Maintenance. The main content area is titled 'System log' and is divided into two sections: 'Remote Log' and 'Current Log'. In the 'Remote Log' section, there is a checkbox for 'Enable remote log' which is currently unchecked. Below it, there are input fields for 'Log server settings', 'IP address', and 'port'. The 'port' field contains the value '514'. A 'Save' button is located below these fields. The 'Current Log' section displays a scrollable list of system messages, including timestamps, log levels, and service names. The messages include: 'May 25 11:44:01 2008 syslogd 1.4.1: restart.', 'May 25 11:44:04 2008 [DRM Service]: Starting DRM service.', 'May 25 11:44:15 2008 [VIDEO SLAVE][567]: [304] connect to socket [/var/run/venc/s0/mediasck_2] error!, ERRNO :No such file or directory', 'May 25 11:44:15 2008 [VIDEO SLAVE][584]: [304] connect to socket [/var/run/venc/s1/mediasck_2] error!, ERRNO :No such file or directory', 'May 25 11:44:15 2008 [RTSP SERVER]: Start one session, IP=192.168.100.102', 'May 25 11:44:17 2008 [SYS]: Serial number = 0002D1066F1C', 'May 25 11:44:17 2008 [SYS]: System starts at Sun May 25 11:44:17 UTC 2008', 'May 25 11:44:17 2008 [NET]: --- NET INFO ---', 'May 25 11:44:17 2008 [NET]: Host IP = 192.168.100.151', 'May 25 11:44:17 2008 [NET]: Subnet Mask = 255.255.255.0', 'May 25 11:44:17 2008 [NET]: Gateway = 192.168.100.1', 'May 25 11:44:17 2008 [NET]: Primary DNS =', 'May 25 11:44:17 2008 [NET]: Secondary DNS =', 'May 25 11:44:18 2008 [SYS]: Recording entry 0 stop', 'May 25 11:44:19 2008 [SYS]: Recording entry 1 stop', 'May 25 11:44:20 2008 [EVENT MGR]: reload config file', 'May 25 11:44:23 2008 init: ^MStarting pid 730, console /dev/ttyS0: '/sbin/getty'', 'May 25 11:44:25 2008 [RTSP SERVER]: Stop one session, IP=192.168.100.102', and 'May 25 11:44:46 2008 [RTSP SERVER]: Start one session, IP=192.168.100.102'. The bottom left corner of the page shows 'Version: 0100d'.

<http://<Network Camera>/setup/syslog.htm>

<Network Camera> is the domain name or original IP address of the Network Camera.

Maintenance

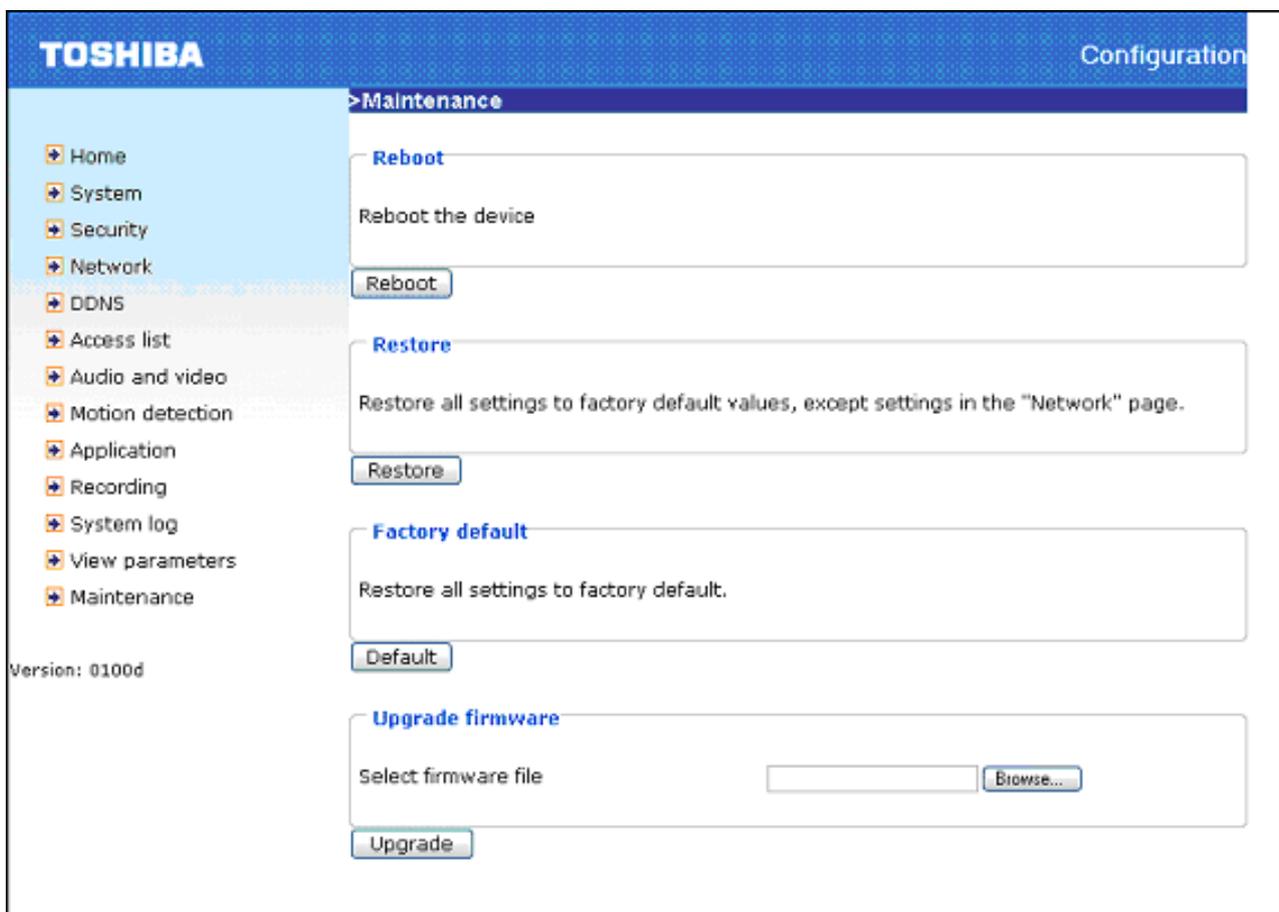
Five actions can be selected.

“Reboot” Click the reboot button to restart the device.

“Restore” Click it to restore all setting to factory default except setting in "Network type" in network page.

“Factory default” Click on Factory default button on the configuration page to restore the factory default settings. Any changes made so far will be lost and the system will be reset to the initial factory settings. The system will restart and require the installer program to set up the network again.

“Upgrade firmware” Select the firmware file and click upgrade button.



<url> <http://<Network Camera>/setup/maintain.htm>

<Network Camera> is the domain name or original IP address of the Network Camera.

A. Troubleshooting

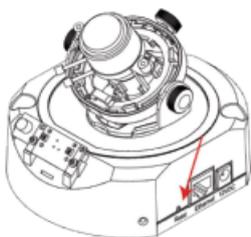
Status LED

The following table lists the LED patterns in general.

Condition	LED color
Loading system after power on	Blink green and orange (twice)
During booting procedure	No LEDs illuminated
Detecting and setting network	Steady orange till IP address is confirmed
After network is setup (system up)	Blink orange and red
During the upgrade firmware process	Rapidly blink orange till firmware is upgraded

Reset and restore

The reset button is located on the back of the Network Camera. Use this button to reset the system or restore the factory default settings. Sometimes just resetting the system sets the system back to a normal state. If the system problems remain after reset, restore to the factory settings and perform the installation again.



RESET: Click on the button.

RESTORE:

1. Continuously press on the reset button until the status LED rapidly blinks orange. It takes about 30 seconds.
2. Upon successful restore, the status LED will blink orange and red.



Restoring the factory defaults will erase any previous settings. Reset or restore the system after power on.

B. Glossary (Index)

Introduction

Installation

How to Use

Definitions in Configuration

Appendix

A

Accessories	12
Access list	38
Administrator	32
Alarm setting	45, 46
Audio output	41, Quick Start Guide: 12
Audio setting	41

B

Browser	3
Software to browse Web screens.	
Microsoft® Corporation Internet Explorer™ only.	

C

Camera name	31
Configuration	30
Contents	12

D

DDNS	37
(Dynamic Domain Name System)	
This is the technique to overwrite the information of DNS (Domain Name System) server dynamically and forward only different informations between DNS servers.	
Because of this, it enables to reduce forwarding data which are needed to renew information of DNS server, and reduce overhead of the network. When combined with DHCP (Dynamic Host Configuration Protocol), it is possible to assign IP address and host name right away as the host on the LAN changes.	
Default gateway	34
Network devices cannot communicate directly with devices in other networks. In this case, communication becomes possible by using devices like a router.	
Default gateway is the IP address of the router.	
DHCP	34
(Dynamic Host Configuration Protocol)	
This is the protocol to assign IP address dynamically to each client on TCP/IP network. DHCP server controls information of IP address, gateway address, domain name and subnet mask and can assign these to client.	

Digital In/Out	31
(Digital input/output)	
Digital zoom	19
DNS	34
(Domain Name System)	
Domain Name Systems translates IP addresses into names making it easier to manage hosts.	

E

Ethernet cable	13
E-mail	48

F

Firmware	29
Program to run this product. It is installed in the flash memory, and can be updated from PC by using PC upload function of the WEB.	
Frame rate	26
The rate of number of pictures that are translated in a second.	
Frame size	40
FTP	35
(File Transfer Protocol)	
A protocol to transfer file(s) to and from other network devices. The network camera supports both active.	

H

HTTP port number	35
------------------------	----

I

Image settings	42
Installation Wizard	Quick Start Guide: 16
I/O terminal block	14
IP address	34
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

- JPEG 40
(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

- LAN 34
(Local Area Network)
Computer networking in local area.
- Log 53
- Log-in 16

M

- Main Screen 18
- Mic. In Quick Start Guide: 12
(Microphone input)
- Motion Detection 45

N

- Network settings 33
- NTP server 31
(Network Time Protocol)
Server which provides accurate date and time from network.

O

- OS 61

P

- Protocol 58

R

- Recording 51
- Reset button Quick Start Guide: 12
- Resolution 40

S

- Security settings 32
- SMTP 48
(Simple Mail Transfer Protocol)
Protocol for sending e-mail on the Internet and Intranet.
- Specifications 58
- Subnet mask 34
Method for splitting 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.
- System Time 31

T

- TCP/IP 58
(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

- Upgrade firmware 54
- User 32

W

- White balance 42

C. Specifications

Introduction

Installation

How to Use

Definitions in Configuration

Appendix

Power supply	12 VDC \pm 10 %, PoE
Power consumption	3.6 W
Image pickup device	1/4 inch, CMOS
Effective picture element	Horizontal 640, vertical 480 pixels
Scanning system	Progressive
Minimum object illuminance	0.1 lux (Auto), 0.2 lux (1/15 s), 0.4 lux (1/30 s), 0.8 lux (1/60 s), 1.6 lux (1/120 s)
White balance	Auto
Pan	\pm 175°
Tilt	+85°, -35°
Horizontal adjustment	\pm 175°
Picture angle	Wide end: horizontal 105° vertical 78° Tele end: horizontal 53° vertical 39°
Brightness adjustment	Available (5 to -5, target value adjusted)
I/O terminal	Input 1, output 1
Image size	640 \times 480, 320 \times 240, 176 \times 144
Image compression system	JPEG, MPEG4
Image quality setting	5 levels
Maximum frame rate at M-JPEG*1	30 fps at VGA
Maximum frame rate at MPEG 4	30 fps at VGA
Number of simultaneous deliveries for image or audio	10 clients
Audio*2	Mic. in / Audio out
Motion alarm function	Available
Image recording function	Available (External storage only)
E-mail notification function	Available
Network interface	Standard: IEEE 802.3af, type 10Base-T, 100Base-TX, connector RJ-45
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
Guaranteed operating temperature	0°C to 50°C (32°F to 122°F)
Guaranteed operating humidity	20 % to 80 %
Storage temperature	-20°C to 60°C (-4°F to 140°F)
Storage humidity	90 % or less
Weight	575 g
External dimensions	143 (W) \times 106 (H) mm (5.63 (W) \times 4.17 (H) inches)
Accessories	User's manual and install software (CD-ROM) (x1), Quick start guide and important safeguards (x1), AC adapter (x1) Warranty (x1), Alignment sticker (x1), Anchor (x2), Screws (x2), I/O connector (x1), Torx driver (x1)

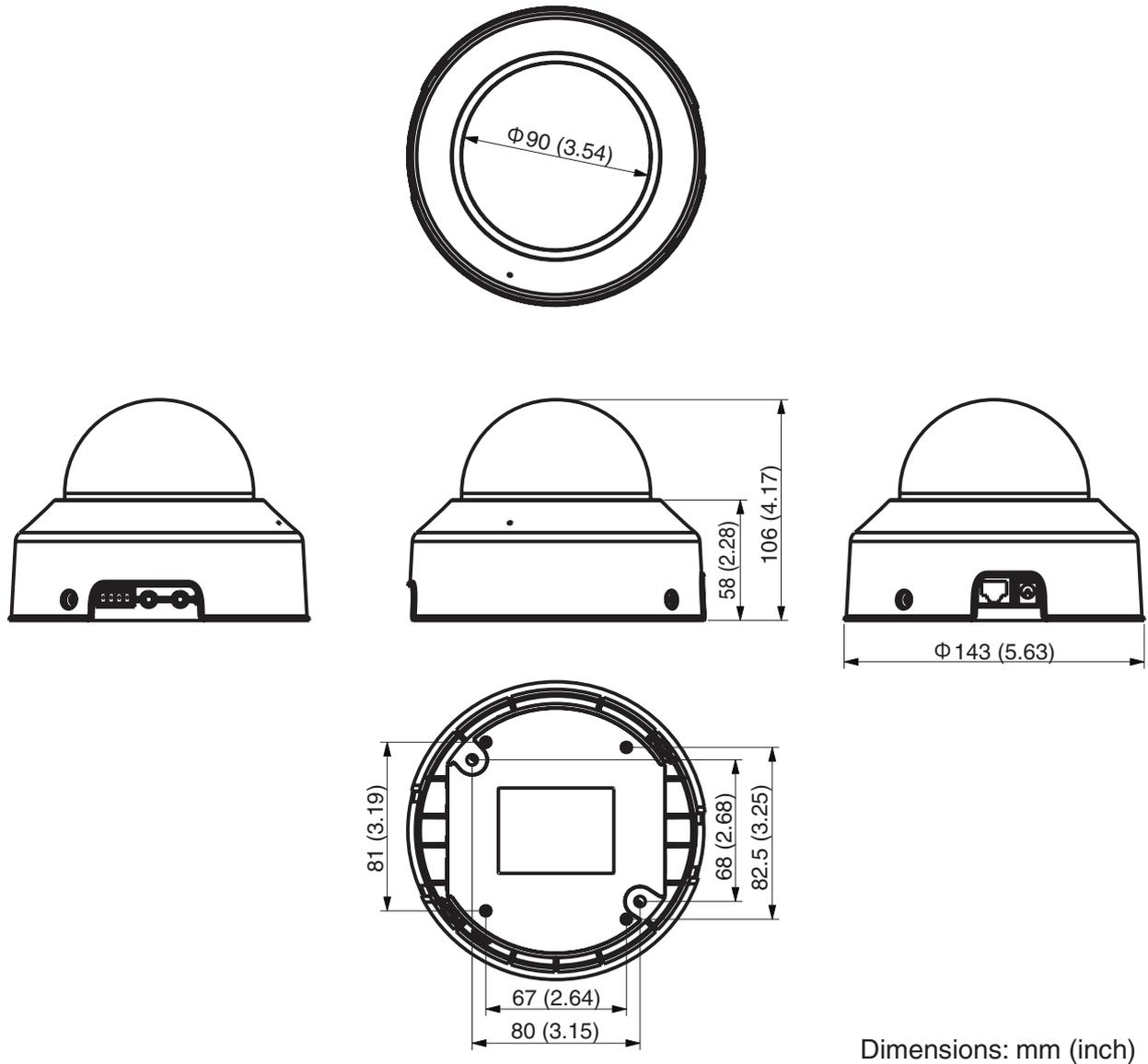
*1: Varies in accordance with the object, image quality, network environment and performance of the personal computer used.

*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.



D. Appearance Diagram



Dimensions: mm (inch)

Technology License Notice

Introduction

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](http://www.vialicensing.com).

Installation

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](http://www.mpegla.com).

How to Use

AMR-NB Standard

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

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

Definitions in Configuration

Appendix



The original text (English) of end-user license agreement on free software components used in the TOSHIBA Network Camera

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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.

Introduction

Installation

How to Use

Definitions in Configuration

Appendix

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.

Security & Network Video Products

9740 Irvine Boulevard,

Irvine California 92618-1697

Phone Number: (877) 855-1349