



# Network Camera IP2112/2122

**User's Manual**

User's Manual



---

---

## Before You Use

It is important to carefully examine the contents with the Chapter [Package Contents](#) after opening the package. If there is anything missing, contact your reseller. Read the Chapter [Physical Description](#) before assembling and operating the device and peripherals. Understanding the physical description can prevent damage caused by abnormal usage and reduce most problems during installation.

Basically Network Camera is a network device and should be easy to use for those who already have basic network knowledge. If there is a system error and it does not recover easily due to erroneous configuration, read the [System recovery](#) section in Appendix [Troubleshooting](#) to restore factory default settings and perform installation again.

Network Camera has been designed for various environments and can be used to build various applications for general security or demonstration purposes. For standard applications, find the appropriate section in the Chapter [How to Use](#) for your application and follow the steps to setup the system. To make best use of Network Camera, read Chapter [Advanced Functions](#) to get creative ideas and review Chapter [System Configuration](#) for detailed explanations of system configurations. To those professional developers, the Appendix [URL Commands of Network Camera](#) will be a very helpful reference to develop a Web-based application.

Surveillance devices may be prohibited by law in your country. Though Network Camera is not only a high performance surveillance system but also a networked video server, ensure that the operations of such devices are legal before installing this unit for surveillance.

**Those paragraphs preceding with  must be fully understood and cautioned. Ignoring the warnings may result in serious hazards.**

---

---

# Table of Contents

<b>Before You Use</b> .....	<b>1</b>
<b>Table of Contents</b> .....	<b>2</b>
<b>Package Contents</b> .....	<b>4</b>
<b>Features and Benefits</b> .....	<b>5</b>
<b>Physical Description</b> .....	<b>7</b>
Front Panel .....	7
Rear Panel .....	8
<b>How to Install</b> .....	<b>10</b>
Ethernet Environment .....	11
<b>How to Use</b> .....	<b>16</b>
Authentication .....	16
Installing Plug-in .....	17
Main Page .....	18
<b>System Configuration</b> .....	<b>21</b>
Introduction .....	21
 Setup Wizard .....	22
 Application Wizard .....	22
Definitions of Configuration .....	23
<b>Advanced Functions</b> .....	<b>32</b>
Capture Up-to-date Still Images .....	32
Uploading Snapshots Periodically .....	35
Customize Graphics in Homepage .....	36
Command Script for Complex Applications .....	37
URL for External Device Control .....	40
URL of System Maintenance .....	41

---

---

Configure System via FTP .....	42
Telnet Commands .....	47

**Appendix .....49**

A. Troubleshooting .....	49
B. Frequently Asked Questions.....	49
B. Frequently Asked Questions.....	50
C. Upgrade System Firmware .....	54
D. URL Commands of Network Camera .....	55
E. Time Zone Table.....	64
G. Technical Specifications .....	67

# Package Contents

If any of the following items are missing, please contact your reseller.

- Network Camera IP2112/IP2122



- I/O Connector



- Power adapter



- Software CD



- Camera Stand



- Quick installation guide



- CS Ring and wrench



- Warranty card



# Features and Benefits

Network Camera is a high-performance networking video transmitter. With powerful VLIW DSP core and fully optimized algorithm, it can compress and transmit the high quality real-time video through standard TCP/IP inter-network. In addition to meet the basic needs of video feed, many advanced features are added to help building applications of surveillance or web attraction. The state-of-art design well compromises among stable, robust, simple-to-use and flexibility.

## Real-time motion-JPEG compression

Video input can be efficiently compressed into packets of JPEG images without delay. Optimal compression engine makes the equivalently excellent image with much smaller size. There is no more sacrifice in remote monitoring and storage. Five levels of compression ratio and three sizes of image resolutions are easy to meet your requirement.

## Robust system operation

Industrial real-time operating system prevents from malicious hackers and virus that threat Windows or Linux systems. The on-board watchdog eternally monitors the system operations for dead-proof.

## Easy Web access via standard browser

You don't have to install any software to access Network Camera. The embedded Web server makes users can access Network Camera anywhere over Internet with any popular Web browser. As long as you are connected to network, you can cast your eyes on your precious property.

## Password protection of system access

Password level protection is provided by the system to prevent from malicious intruders from network. Once the password of administrator is entered, any user will need password authentication to access Network Camera. Each user can have individual access right to view video or control external devices.

## Built-in motion detection

No more external sensors are required. The video channel can be setup to detect any motion with customized settings. By tuning the object size and sensitivity, it is more reliable to fit into your environment. With this built-in facility, you can easily setup a

---

---

security system in your home or office.

#### Weekly schedule for automatic surveillance

The user-defined time period will repeat weekly to check any security settings and accordingly sending notification or drive external devices. It is easy to install in SOHO, retail shop and home as a security system.

#### Flexible I/O control for external devices

There is one opto-isolated sensor input and one relay output to control external devices. System integrators can easily replace the current analog systems to build an advanced security system.

#### Remote system upgrade

To achieve the promise we made to support our valuable customers in life-time, the most up-to-date firmware is always put on our web site to add new functions or solve known bugs. A free upgrade wizard is included to facilitate the job.

#### Developer's technical support

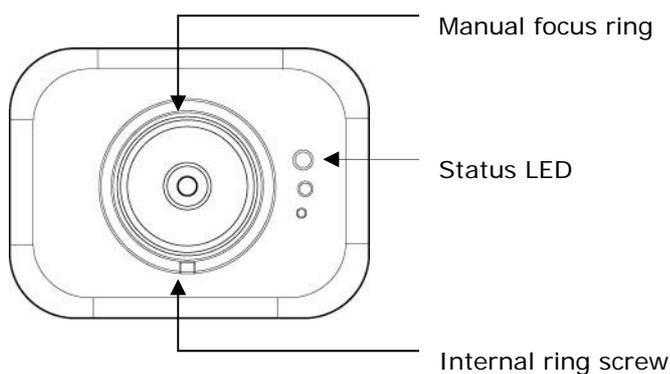
The high-performance Network Camera can be integrated into many applications under perfect control of budget. The complete programming interface and standard JPEG format can ease and speed developers' task. More creative ideas can be found on our Web site.

---

---

# Physical Description

## Front Panel



### Status LED

The dual color LED indicates system and network status including power-on-self-test and system activity. Refer to the Appendix for details.

### Manual focus ring

The ring of the lens can be rotated to fine tune the focus. The video output at the rear panel can be used to monitor.

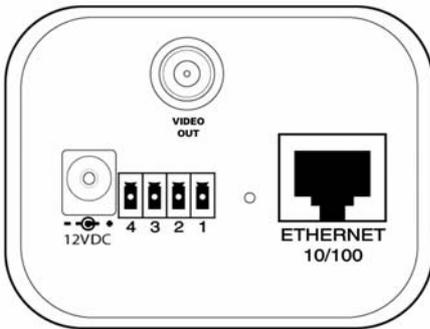
### Internal ring screw

If another special lens is needed to replace the bundled one, the image may be out of focus for new lens and not able to fine tune by the manual focus ring. Use the included wrench to loose the screw to adjust the internal ring to get the best focus. Then tighten the internal ring to fix the focus.

---

---

## Rear Panel



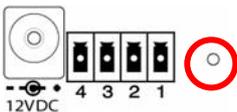
### BNC video output connector

A 75Ohms-resistance video connector can be connected to a TV for monitoring the video from the front CCD sensor.

### Ethernet 10/100 socket

Connect to an Ethernet network with a UTP category 5 cable of length shorter than 100 meters according to the standard.

### Reset and restore button



There is a button hidden in the pinhole beside the Ethernet socket. It is used to reset the system or restore the factory default settings.

### General I/O terminal block



1	←	DI-	INPUT	(Max. 50mA, 12VDC)
2	←	DI+	INPUT	
3	←	SW_COMMON	OUTPUT	(short with NC at initial state)
4	←	SW_NOPEN	OUTPUT	(Max. 1A, 24VDC or 0.5A, 125VAC)

---

---

Network Camera provides a general I/O terminal block with one digital input and one relay switch for device control. Pin 1 and pin 2 can be connected to an external sensor and the state of voltage will be monitored from the initial state 'LOW'. The relay switch of pin 3 and pin 4 can be used to turn on or off the external device.

### **Power cord socket**

Connect the power jack of the included power adapter. Connecting the power adapter should be the last operation while physically installing Network Camera.

---

---

## How to Install

To easily fit into various environments, Network Camera automatically detects the attached interfaces and configures itself to the best condition. The high performance built-in CCD and lens always give users delicate image quality.

In the following content, "**user**" refers to those who can access Network Camera and "**administrator**" means the supervisor who has the root password to configure Network Camera in addition to general access. Administrators should carefully read this manual, especially during installation.

---

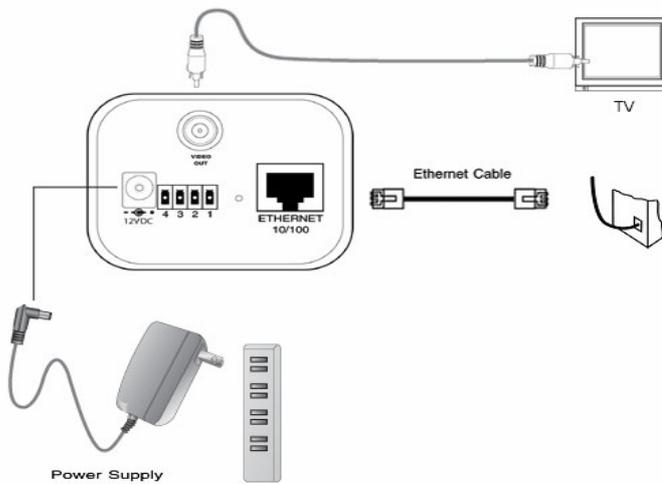
---

# Ethernet Environment

## Hardware installation

Before installing multiple Network Cameras at the well-chosen locations, the administrator should memorize the serial numbers on the packages respectively for future use.

### Cable connection



Connect the supplied cables from Network Camera to related devices according to the above diagram. Note that the power adaptor must be kept unplugged until other cables are firmly connected.

## Power on

Make sure all cables are correctly and firmly connected before turning on Network Camera. Turn on cameras, sensors, alarm devices, and then attach the power adaptor of Network Camera to the electric power socket. After the POST (power-on self test) is complete and the result is successful, Network Camera is ready for software configuration as described in this manual. At this stage, network speed and video modulation type are automatically detected. Refer to the configuration section for further information.



Connect the power jack of the power adapter to Network Camera prior to plugging the utility end into the utility power socket. It will reduce accidental electric surge shock.

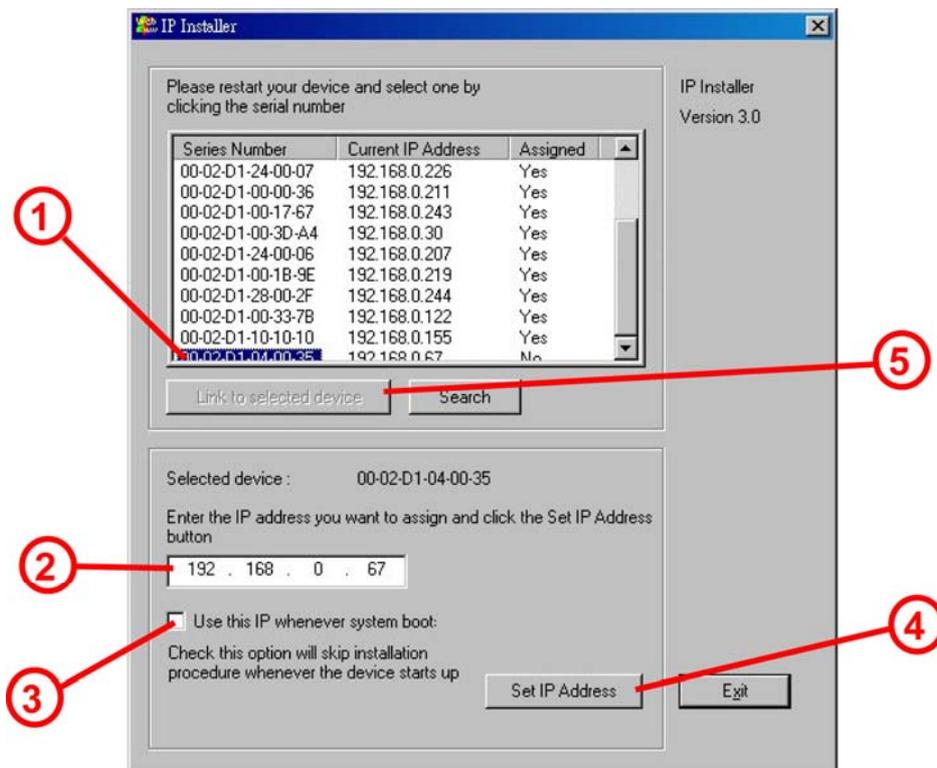
---

---

## Software installation

### Easy way with installer program

In order to configure Network Camera's remotely, administrators should keep the serial numbers of the new Network Camera's for identification and initial passwords. After successfully mounting Network Camera's in the proper position, run the Installer program on the PC in the same network to locate the newly mounted Network Camera's. Network Camera's also support manual setup procedures to non-Windows based environments. The manual procedure is described next.



After the POST is done, Network Camera will try to configure itself by detecting the network environment. If there is DHCP service over the network, the Installer program will catch the given information, then display the serial number and given IP address for each Network Camera as the figure above. To install the IP address, follow the steps.

- 1 Click on the entry with the serial number you want to install. If the "**Assigned**" field of the entry is labeled "**Yes**", that means the Network Camera has already been installed.
- 2 Type the desired IP address if it is other than the IP address given by the DHCP server.
- 3 Check the box to fix the IP address of the Network Camera. Otherwise the Network Camera will lose the network address at next system boot and you have to run this installer again.

- 4 Click  to progress the installation.

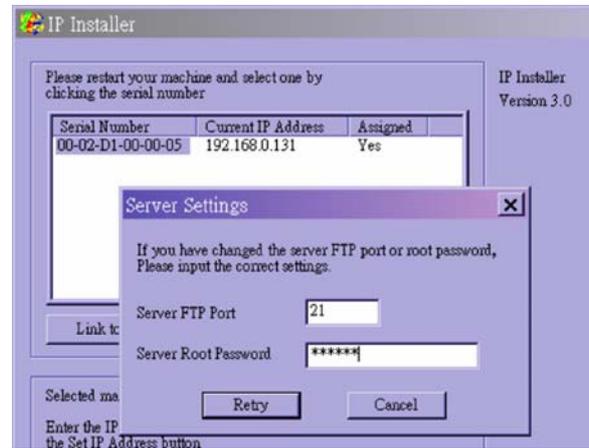
- 5 After successful notification, administrators may keep the address information and

---

---

click directly on [Link to selected server](#) to access the Network Camera in the default browser. If the IP address is taken by another network device in the network, the Installer program will pop out another message window to warn that the assigned IP conflicts. In this case, administrators should ask the network supervisor for a vacant IP address.

While "**Use this IP whenever system boots**", is checked, a dialog window may pop out to ask for "**Server FTP Port**" and "**Root Password**" because they are already changed by administrators to other than default settings. If the original settings are lost, restore default settings and run software installation again.



 Once the installation is complete, administrators should follow the [First access to Network Camera](#) section for necessary checks and configurations.

---

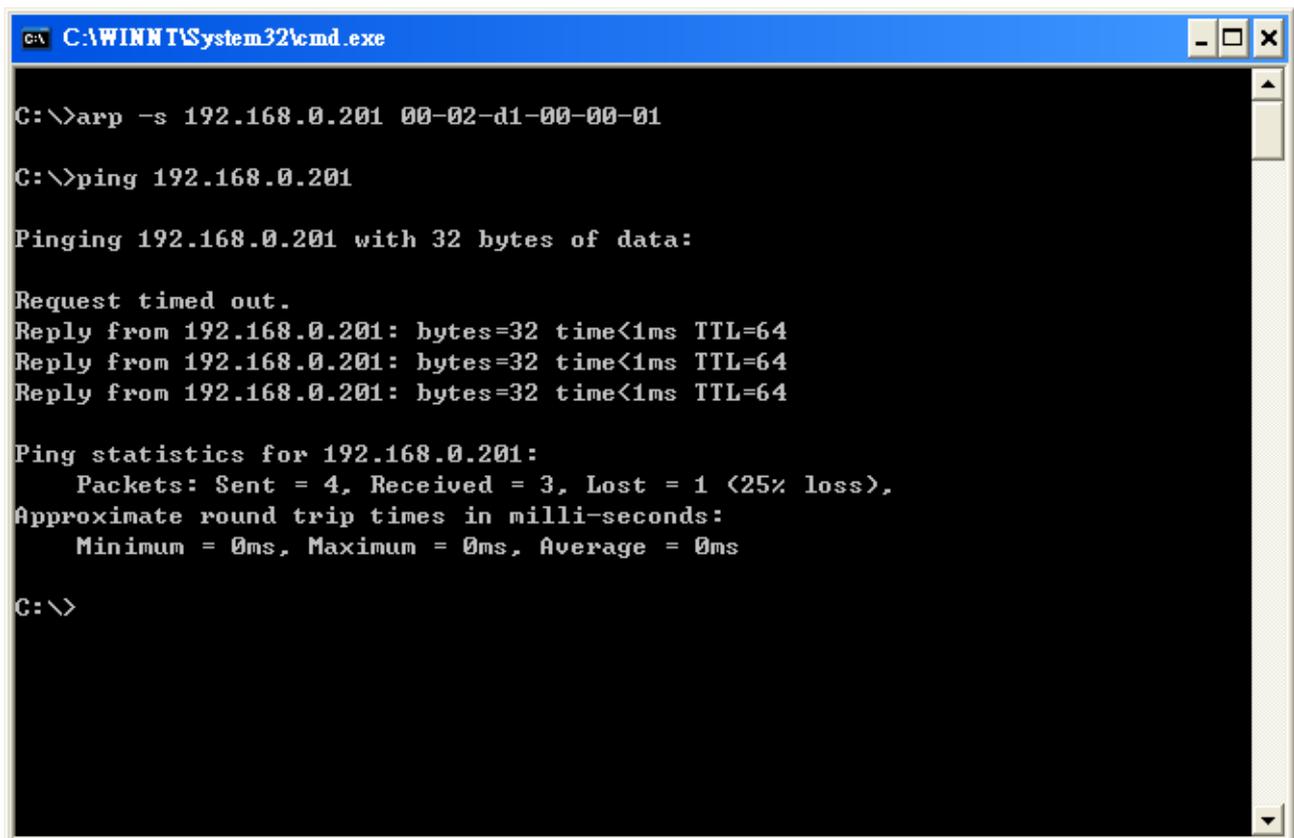
## Manual way with existing programs

For those environments such as MAC, Linux, Unix or other operating systems, whose installer is not yet available, some common network tools including ARP and PING can be used to install Network Camera. Before proceeding further, make sure ARP and PING programs exist.

First, type `arp -s "assigned IP address" "Ethernet address"` to add an entity in the system's name table. The Ethernet address is identical to the serial number of Network Camera and should be typed in the appropriate format like "uu-vv-ww-xx-yy-zz" or "uu:vv:ww:xx:yy:zz", which depends on the operating system.

Once the name entity is added, type `ping "assigned IP address"` to invite the new Network Camera. If it replies, that means Network Camera has accepted the assigned IP address and is ready for access. The first several ping requests may fail during the self-configuration period of Network Camera. Since the accurate grammar of ARP and PING depends on the operating system, refer to its related help manual.

## Example of DOS prompt in Windows 2000



```
C:\WINNT\System32\cmd.exe
C:\>arp -s 192.168.0.201 00-02-d1-00-00-01
C:\>ping 192.168.0.201
Pinging 192.168.0.201 with 32 bytes of data:
Request timed out.
Reply from 192.168.0.201: bytes=32 time<1ms TTL=64
Reply from 192.168.0.201: bytes=32 time<1ms TTL=64
Reply from 192.168.0.201: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.0.201:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

---

---

## First access to Network Camera

### Change initial password of administrator

Starting the Web browser to connect to the assigned IP address of Network Camera, users will be asked for user name and password by an authentication message window. A root password, identical to the Network Camera's serial number, is needed for the initial access to a newly installed Network Camera. The administrator must change the root password immediately after the initial installation to ensure security. The new root password should be well memorized since there is no way to retrieve or recover it. After changing the password, the browser will display an authentication window again to ask for the new password. If the root password is deleted as blank, the authentication mechanism will be disabled.

### Manage user privilege

For complete protection from illegal usage, Network Camera provides three privileges and always needs user name and password before access. The lowest level is DEMO mode whose services are subject to administrator's permission. The standard level is the USER mode that consists of twenty user profiles. Each user is able to access Network Camera under the given privilege, except for system configuration. The twenty user profiles are also maintained by the administrator. The highest level is ROOT mode that only opens to administrators for initial setup, system configuration, user administration and software upgrade. The user name of the administrator is internally assigned to **"root"**.

### Complete the network settings

Although Network Camera already can be accessed after software installation in local area network, administrators should complete the network settings in the configuration page. The complete network configurations including subnet mask as well as the IP address of default gateway and DNS are provided by your network administrator or Internet service provider. Once the wrong network settings make Network Camera fail to work, refer to Appendix A to restore factory default settings.

By default Network Camera will need administrator's installation every time it reboots. If the network settings are sure to work all the time, disable the install option in network configuration Web page or Installer program.

Details about configurations are described in the relative category of the Chapter [Definitions of Configuration](#).

---

---

## How to Use

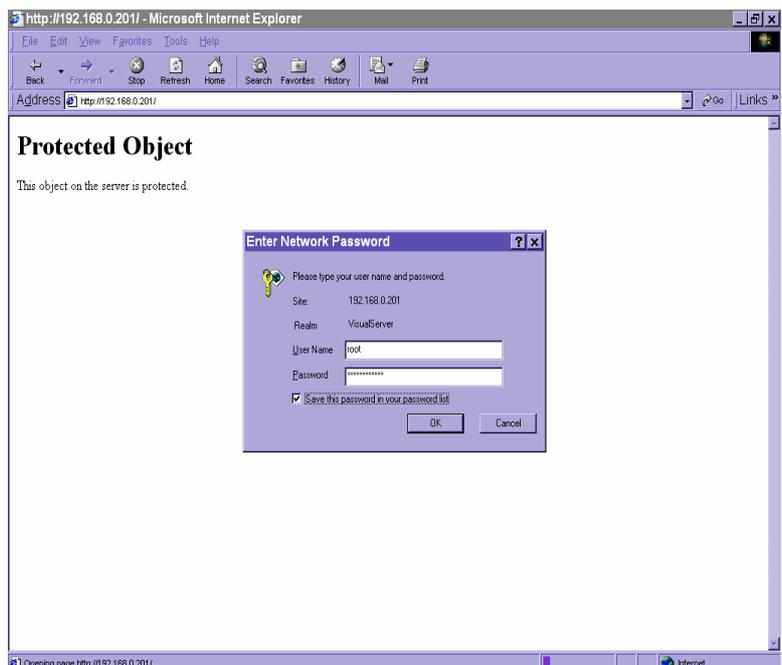
Open your familiar web browser and connect to Network Camera just like any general web site and the video will present on demand. Make sure the web address of the target Network Camera is accurate.

## Authentication

After opening the Web browser and typing in the URL of Network Camera, a dialogue window will pop out to request a username and password. For administrator's initial usage of Network Camera, enter the username as "root" and the password as the serial number in capital letters. The serial number can be found on the labels under the body of Network Camera and the top side of the carton. The primary users will be allowed to enter as soon as the administrator finishes adding user profiles. Upon successful authentication, the main page will be displayed.

For demonstration purpose, enter the Security Web page of configuration to activate the demo account and choose permitted services. Once the demo account is setup, any one may watch the video by using "**demo**" as user name while ignoring the password. Different from primary users, the demo account has certain limitations that are determined by administrators.

In the figure, the foreground is the login window and the background shows the message when authentication fails. The user may check the option to save the password for future convenience.

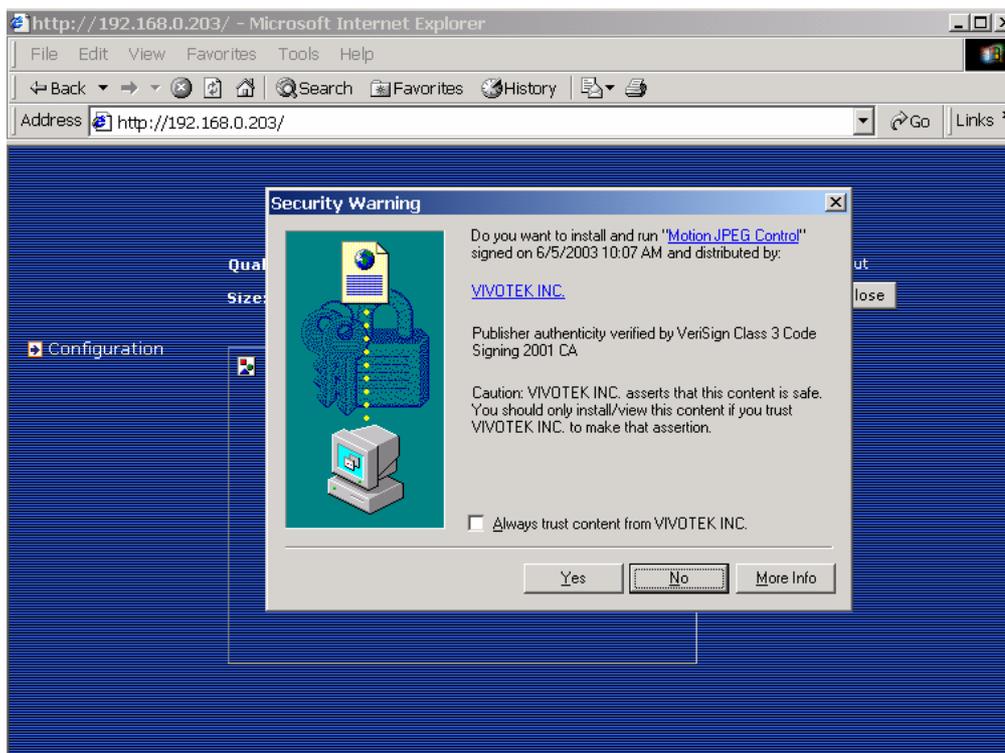


---

---

# Installing Plug-in

If it is initial access to Network Camera via the Web browser supporting server push, the motioned pictures will display directly. If the Web browser is Internet Explorer in Windows, users will be asked to install a new plug-in that is provided by Network Camera. This plug-in has been registered for certificate and is used to display motioned pictures in the Internet Explorer. Users may click on  to install the plug-in. If the web browser does not allow the user to install, check the security option to lower security levels or contact network supervisors.



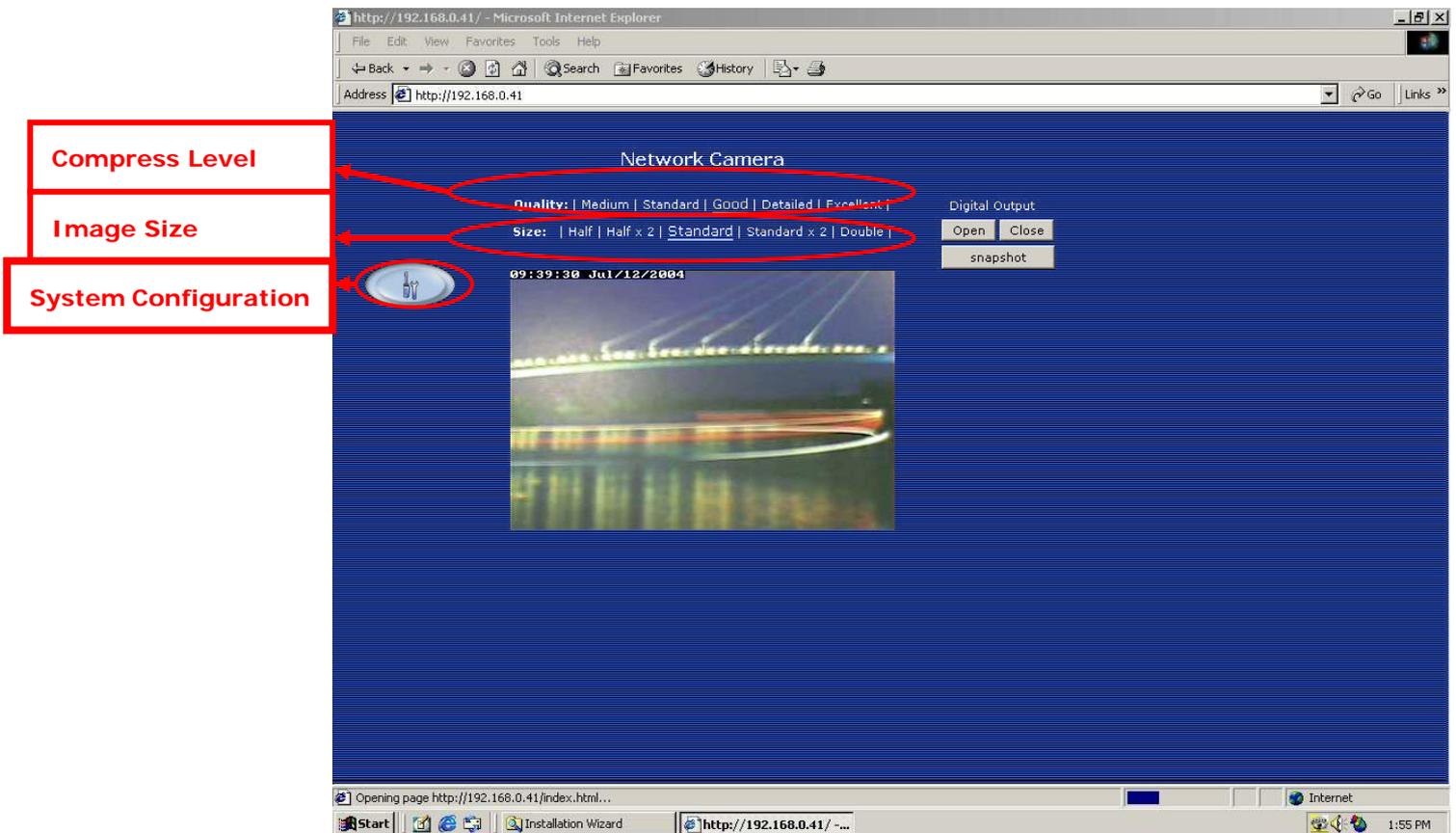
---

---

# Main Page

Basic functions are displayed in main entrance page of Network Camera. The first figure below is graphic mode that has better visual effect and the second one is text mode that will shorten download time. The main page may look different depending on the PT scanner or the privilege of the user.

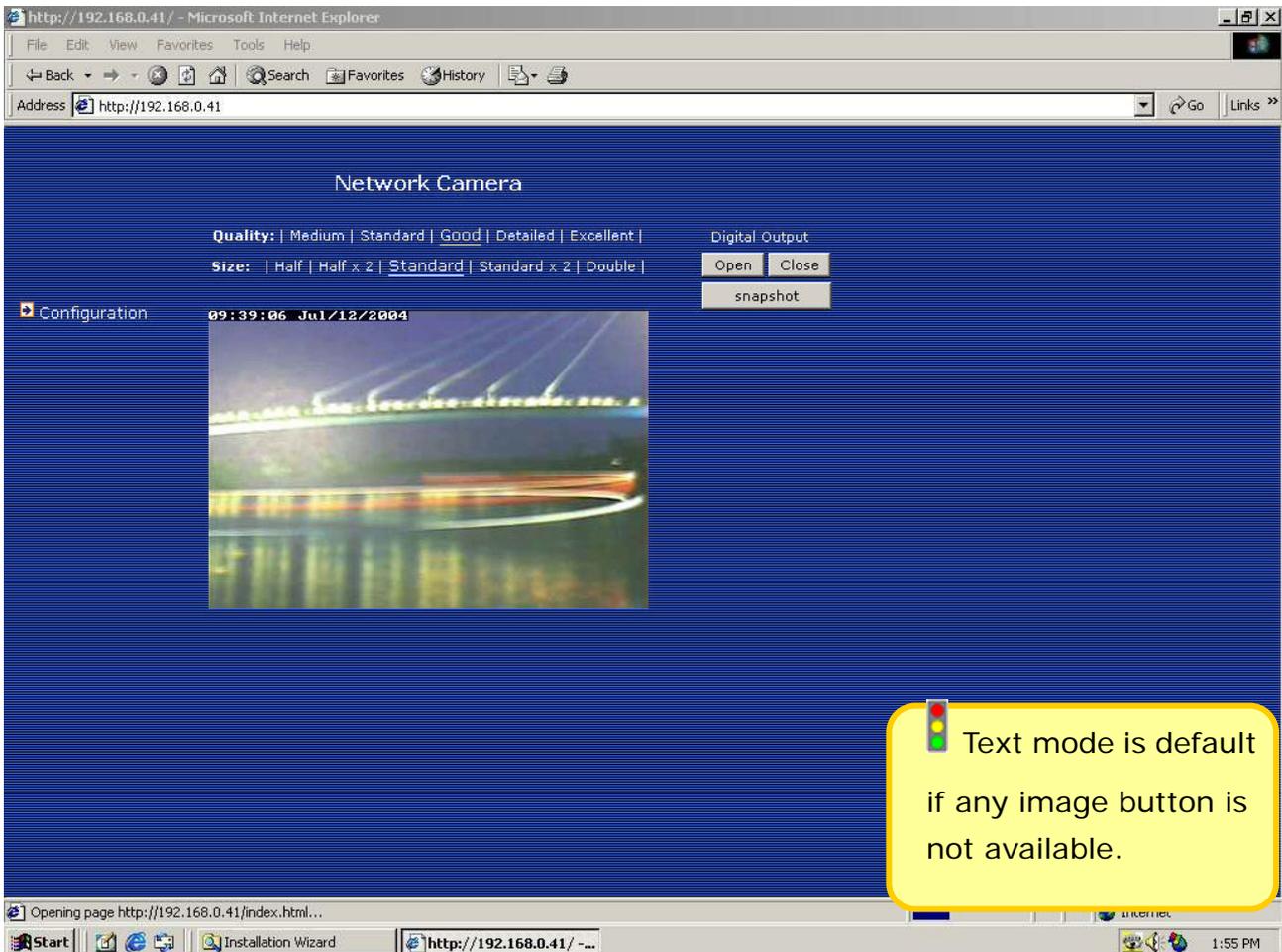
## Graphic mode



---

---

## Text mode



## Video quality selection

It allows users to adjust the video quality for speed or smoothness. The performance is also subject to the network bandwidth and the number of users. Five options are available to be chosen from "**Medium**" to "**Excellent**". "**Medium**" quality means the picture has the quickest refresh rate but the worst image quality and "**Excellent**" quality means the picture has the slowest refresh rate but the best image quality.

## Video size selection

It allows users to adjust the image size with consideration of bandwidth and image resolution. Five options are available including "**Half**", "**Half x 2**", "**Standard**",

---

---

---

---

“**Standard×2**” and “**Double**”. “**Half×2**” consumes the same bandwidth as “**Half**” but has the same size with “**Standard**”. Of course the visual effect is worse than “**Standard**”. “**Standard×2**” compared to “**Double**” is similar to the case. “**Half×2**” is especially suits in the low bandwidth environment like a dial-up network. To fit into the small image area, timestamp will be skipped in “**Half**” and “**Half×2**” modes.

## System configuration

There is a button or text link in the left side of the system configuration that only appears in administrators’ main page.

## External digital output control

There may be two remote control buttons for the each digital output on the main page. If there are external devices attached to the digital output, administrators or permitted users can click on  to short “Common” and “Normal Open” pins of the digital output or click on  to short “Common” and “Normal Close” pins of the digital output. To know more about the digital output for external devices, refer to the rear panel introduction of the Chapter [Physical Description](#).

---

---

# System Configuration

## Introduction

The system configuration can be easily done remotely on Internet Explorer through the Web interface. There are two wizards in addition to classified categories of system configurations. They can give friendly instructions and facilitate the setup job. Alternately administrators may type directly the URL of system configuration, "*http://<IP address of Network Camera>/setup/config.html*", to directly enter the configuration page. If administrators also want to set certain options through the URL, read the relative section in the Chapter [Advanced Usage](#) for reference. Network Camera also supports FTP to modify the system configuration file, CONFIG.INI, for technical usage. The details are described in the Chapter [Advanced Usage](#).

Since it is a networking video server, administrators should run "**Setup wizard**" or well configure "**Security**", "**Network**" and "**Video**" at least. To utilize the built-in features of security and web attraction, run "**Application wizard**" or configure "**Application**" and "**Demo**". Besides these features, administrators can adjust the system date and time in "**System**", or have different homepage layout by configuring "**Homepage layout**". Network Camera also provides some system maintenance like "**View log file**", "**View parameters**" and "**Factory default**".

---

---

## Setup Wizard

The setup wizard will guide administrator to enter necessary information including system name, current date and time, administrator's password, video configuration and captions, and network settings. Administrators can exit the procedures anytime to reserve the current configuration. Finally the setup wizard will ask for reboot to validate the changes and administrators can decide to reboot later.

## Application Wizard

There are two main applications including surveillance system and web attraction by means of Network Camera. The former one will utilize the built-in motion detection and external sensors to integrate with the existing e-mail or FTP server or external alarms to construct a security system. It also possesses the weekly schedule for timed monitoring. The later one will customize the main page to your personal style and setup accounts for your possible visitors. The application is perfectly constructed and performed on several clicks by your fingertip. Administrators can additionally configure the application parameters in the [Application](#) page of configuration for more advanced usage after using Application wizard.

---

---

# Definitions of Configuration

## System parameters

### Change host name

The "**host name**" is used for the homepage title of main page and displays as the title over the video window on the main page. The maximum string length is 40 characters or 20 characters in double-byte-character-systems like Chinese or Japanese.

### Adjust date and time

There are three ways to adjust system date and time. The easiest is to make Network Camera "**Sync with computer time**". The second "**Manual**" is to set the date and time manually by entering new values. Notice the format in the related field while typing. The third "**Automatic**" is to make Network Camera automatically synchronize with timeservers over the Internet every month. It may fail if the assigned **NTP server** cannot be reached or Network Camera is within a local network. Leaving the NTP server blank will let Network Camera connect to default timeservers. Domain name or IP address format is acceptable as long as DNS server is available. Do not forget setting the "**Time zone**" offset for local settings. Refer to the Appendix E for the time zone of your region. It only affects the hour in NTP method. "**Update interval**" can make the server to synchronize the system time to NTP server every hour, every day, every week or every month.

Once the settings are changed, click on  to validate changes.

---

---

## Security privilege

### Change root password

To change the administrator's password, type the new password in both text boxes identically. What is typed will be displayed as asterisks for security purposes. The maximum password is 16 characters. After pressing **Save**, the web browser will ask administrators for the new password for access.

### Add new users

To add a new user, type the new user's name and password, check respective privilege, and then press **Add** to insert the entry. There are a total of twenty user accounts. Each user can have independent access right of the video channel and external I/O access.

### Edit user's privilege

If the permitted rights of some user has to be changed, pull down the user list to find the user name and press **Edit**. A new window will pop out for administrators to change password and choose different privilege.

### Delete existing users

To delete a user, pull down the user list to find the user name to be deleted and press **Delete**. A message window will pop up for confirmation.

### Demonstration account

To setup Network Camera for demonstration to the public, administrators need to choose the service(s) to be permitted. After checking "view" in Security page, users may use "demo" as general user name and password is not required. Administrator also can assign "I/O access" option to demo account. To separate the demo account from primary users can prevent from interfering with the normal operations.

### Enable snapshot mode for more users

The maximum users that can view Network Camera at the same time are twenty. Administrators can check "**Allow more guests with snapshot mode**" to enable the snapshot mode for more users. Then the users over twenty will have the main page with snapshot mode instead of normal motion picture. It is practical for web attraction. In such case, configure the "**Snapshot interval**" to achieve better performance. The bigger interval between snapshots, the more users can have snapshot mode work.

---

---

## Network settings

### Fix the IP address

To eliminate incautious mistakes during installation, Network Camera will stay in installation mode whenever it starts unless "**Reset network at next boot**" is disabled. This option can also be disabled using the Installer program. Once the option is disabled, Network Camera will skip installation at the next boot and the Installer program will not find the installed units. That implies that Network Camera cannot be accessed if no one remembers the IP address, except for restoring factory default settings. However, with this option disabled Network Camera can automatically operate normally after restarting in case of losing power.

### Basic network settings

Administrators may need to modify the network settings to fit into existing networks. The subnet mask in some broadband service may differ from the default value 255.255.255.0 and service providers may assign more specific network settings. Administrators should change the configuration to what given by the service provider. The configuration may include "**IP address**", "**Subnet mask**", "**Default router**", "**Primary DNS server**" and "**Secondary DNS server**". After changing network settings, be sure to leave "**Reset network at next boot**" blank to skip next installation when the system restarts. Otherwise those network settings will be erased at the next start.

### Bandwidth utilization limit

Each Network Camera can be limited in bandwidth utilization by administrators according to its priority and importance of location. "**Bandwidth limit**" is most useful to balance network utilization when multiple Network Camera's are installed in the same network. It is more effective than changing image quality only and achieves better performance with adequate image size and quality.

### Changing port number of servers

For security or network integration, administrators also can hide the server from the general HTTP port by changing "**HTTP port**" to other than default 80. "**Local FTP server port**" can also be changed to other than default 21. Administrators should have enough network knowledge to change the default port.

### E-mail settings

Network Camera not only plays the role of server, it will also actively connect to servers outside to send out messages or snapshots. When Network Camera starts, it will send out a system log via e-mail as long as the settings are correct rather than upload it via

---

---

FTP. Even in modem application, Network Camera will send out a connection log whenever it dials out to an ISP or dialup server outside. If the administrator has setup some applications in either event mode or sequential mode, Network Camera will send out snapshots once conditions are met. To activate e-mail function, enter correct settings of "**SMTP (mail) server**" and "**Recipient email address**". "**Secondary SMTP (mail) server**" and "**Secondary email address**" are provided for backup connection when the primary one fails. "**Return email address**" is whom the mail will return when the SMTP server rejects upon any failure. Some ISP may reject the mail if the address is invalid.

### FTP settings

To send the log files described in the above paragraph via FTP, the SMTP server should be erased. Administrators must enter correct "**Primary FTP Server**", "**Primary FTP user name**" and "**Primary FTP password**". "**Primary FTP remote folder**" is the relative sub-folder in the remote FTP server. If the port of the remote FTP server is changed other than 21, set the real port to "**Primary FTP server port**". If the local network is protected by a firewall to prevent from initiating FTP connection from the remote FTP server, you may be able to connect to the FTP server but unable to put any file due to data channel connection failure. Check "**Primary FTP passive mode**" for passive transfer solution. Another set of "**Secondary**" server settings is also provided for backup connection.

In either e-mail or FTP, the primary server information should be entered first. If the primary server is not set, the related FTP or email will be cancelled. Note that it may take time to connect to the secondary server after the first one fails and it may affect some applications when conditions happen too often.

After everything is set, click on . A warning message will pop out for confirmation. After clicking on , Network Camera will automatically restart. If "**Reset network at next boot**" is kept checked, perform software installation again. Otherwise Network Camera will boot up according to the new configuration automatically.

 Any change made to this page will make the system restart to validate. Make sure every field is correctly typed before clicking on . If Network Camera fails to response due to erratic settings, perform the restore procedures and run software installation.

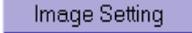
---

---

 Administrators should notice that the basic network settings including IP address, subnet mask, default router and DNS servers will be cleared when the network interface is switched to the other between Ethernet and modem.

## Video and motion detection

### Adjust image settings

"**Time stamp**" and "**Text on image**" will be enclosed in image for reference. The timestamp is captured from date and time of Network Camera that is maintained by an on-board real-time clock. "**Color**" setting is independent of the connected camera and "**B/W**" option can speed up the encoder a little. "**Default size**" option here will be the default size of video window when users first connect to Network Camera. "**Default quality**" option here will be the default quality when users first connect to Network Camera. To adjust image settings for best visual quality, press  and a motion picture window will pop up for your reference. There are four fields including "**Brightness**", "**Contrast**", "**Hue**" and "**Saturation**" for video compensation. Each field has eleven levels ranged from -5 to +5. While adjusting, administrators can click on  to check prior to  the setting in memory. If the adjustment is not good, administrators can click on  to restore the original settings without change. After configuration done, click on  to close this window. If parameters are changed without saving, they will be used until the next system startup.

### Configure motion detection

The channel can have its own settings of motion detection independently. The settings including "**Object size**" and "**Sensitivity**" allow administrators fine tune to fit into the environment. The "**Object size**" decides the space ratio of motioned objects over the monitored screen. The "**Sensitivity**" sets the measurable difference between two sequential images that would indicate motion. The larger object size and lower sensitivity will make Network Camera ignore small variations in images. While the motion amplitude of some object in the monitored screen is over the settings, a white  in red background will indicate at the upper-right corner of the window.

 Motion detection is provided as reference because it is very environment-dependent. Especially working by the very sensitive settings, some triggered events may be considered as false alarms though there is tiny difference happening indeed. It can be affected by florescent light flashing, shadow shifting, and so on.

---

---

---

---

## Application constitution

Administrators can use combinations of options on the application page to perform many useful security applications. Network Camera provides two application modes; one is performed according to the settings on the web page, the other is performed according to the external command script. Though most settings will automatically be done by the [Application Wizard](#), administrators still can adjust the settings from this page.

### Weekly schedule

A useful weekly schedule is provided for daily security application. Administrators can select weekdays from Monday to Friday with the daily schedule from 9:00 am to 6:00 pm that no one is at home to perform any event checking. If the security system needs to be installed in office that no one is there during the nights or weekend, administrators just set the time period as above, then check **"All the time except for the above schedule"** for opposite operations.

### External command script

Administrators can write a script named **SCRIPT.TXT** to perfectly match the additional software according to the [Command Script for Complex Applications](#) section in the Chapter [Advanced Functions](#). After uploading this script to Network Camera via FTP, check the option **"Enable the external script file to exclude the following settings"**. Otherwise Network Camera will operate according to the settings below.

### Event operation

Network Camera provides general options for two basic applications, **event operation** for security and **sequential operation** for web attraction. In event operation, administrators have to setup some conditions to check and some actions to happen consequently. The conditions include motion detection and the status of digital input. While checking "Detect motion" box, administrators should click "Motion Detection" button on **Video** page or click "Motion Detection" link in **Application** page to configure the appropriate parameters. In the newly opened window, percentage of **object size** over whole window and **sensitivity** can be fine tuned to fit into the environment. If any motion is over the settings, an  will appear on the upper-right corner of image for indication. The  will appear in the image to indicate some motion is detected as long as **"Show alert in image"** is checked. If there are any sensors attached to the digital input, administrators can set the state to fire alarm. There are four states of "Input is **High**", "Input is **Low**", "Input is **Rising**" and "Input is **Falling**". The edge trigger like "Rising" or "Falling" is generally used to detect the emerging signal from the external sensor. Once any event happens, administrators can select **"Delay second(s) after**

---

---

**event**” option to drive some device attached to the digital output several seconds after the event happens and/or send snapshots that are taken right at the moment. . If administrators want to receive some snapshots to check the event, please check the **“Upload snapshot while input condition match”** box to get snapshots when inputting condition is matched the setting or check the **“Upload snapshots while motion detected”** box to get snapshot when motion has been detected. Network Camera will take three snapshots of pre-event, the moment of event, and post-event for video channel. Three snapshots of the channel can also be downloaded via FTP or HTTP URL. Refer to the [Download Event-triggered Snapshots](#) section for details.

### Sequential operation

With this feature, Network Camera can upload snapshots periodically to external server as a live video source. The interval can be set from tenth second to several hours. The external server must be setup correctly in the [Network](#) configuration page.

### Sending method

Either event mode or sequential mode can select one method between **email** and **FTP**. The accompanied external server must be setup correctly in advance. If email is chosen, the snapshots of the video channel will be attached in the emails. If FTP is chosen, administrators can choose to add date and time in the file name of snapshots. If the snapshots are used as the live video source, the date and time suffix can be eliminated to update the same source file.

 The option “Show alert in image” may be set when running application wizard or configuring motion detection. Administrators should manually uncheck it if no indication of motion detection is needed in the image.

---

---

## Homepage layout

There are two homepage display modes. One is "**Image mode**" that uses graphics for links; the other is "**Text mode**" that mostly uses text for links.

Administrators may easily give Network Camera a different presence of homepage. The "**logo graph**" for the system logo at the upper-left corner can be hidden; or the default image from the system memory can be used; or an external resource can be used by assigning a URL. The "**Background graph**" is similar. Default images of the system can be customized but limited by memory size. Images from external resources can be larger and more beautiful but will need more time to load. If the background is skipped, the background color will fill the browser window. Administrators also can give the system logo a "**Logo link**" to connect to another web site while clicked. The "**Font color**" and "**Background color**" can be chosen from sixteen colors as you like. See the [Customize graphics in homepage](#) section in the Chapter [Advanced Functions](#) for how to replace the default images of log, background and buttons of video switch.



If any necessary image is lost while homepage layout is image mode, Network Camera will switch to text mode automatically.

---

---

## **View log file**

There is some useful information in the system log including current system configuration and activity history with timestamp for tracking.

## **View parameters**

The whole system parameters will be categorized listed for administrators to check. The content is the same as CONFIG.INI.

## **Factory default**

It is used to restore the factory default settings. This means any changes made before will be lost and the system will be reset to the initial status as shipping out of the factory. After confirmation, the system will restart and require the software installation to setup the network.

---

---

## Advanced Functions

### Capture Up-to-date Still Images

#### Get snapshot via URL

Administrator and users can use the specific URL to capture the current still image.

##### URL

```
http://<IP of Network Camera>/cgi-bin/video1.jpg[?<param>=<value>]
```

param	value	Description
quality	1	Medium
	2	Standard
	3	Good
	4	Detailed
	5	Excellent
size	1	Half
	2	Standard
	3	Double

#### Get snapshot via FTP

Administrator and users can log-in the FTP daemon of Network Camera to download the refreshed JPEG image named **video.jpg**. The user name and password are as same as what in web access. The zero file size in file directory means it is captured by request.

---

---

## Video Embedded in Customers' Homepage

In addition to the URL, some scripts should be added to download a plug-in for motion pictures. The following example simply displays title text and a real-time video window in Internet Explorer or Netscape. The user name and password should be configured in advance. Those who are familiar with HTML can easily add more components or rewrite a more vivid and useful homepage.

```
<html>
<head><title>Network Camera Sample Page</title></head>
<body>
<h2>Network Camera Sample Page</h2>
<script language="JavaScript">
<!--
if ((navigator.appName == "Microsoft Internet Explorer")&&(navigator.platform != "MacPPC"))
{
document.write("<OBJECT ID=\"MjpegControl\" WIDTH=352 HEIGHT=288");
document.write("CLASSID=\"CLSID:EAA105FE-7BBD-4196-8B96-D46743894195\" ");
document.write("CODEBASE=\"http://root: <root_spassword>@<IP_Address>/plugin/mjpegcontro
l.cab#version=2,0,0,0\">");
document.write("<PARAM NAME=\"VSize\" VALUE=\"2\">");
document.write("<PARAM                               NAME=\"UrI\"
VALUE=\"http://root: <root's_password>@<IP_Address>/cgi-bin/video.jpg");
document.write("?cam=1&quality=3&size=2\">");
document.write("</OBJECT>");
} else {
    document.write("<img width=352 height=240");
    document.write("src=\"http://root: <root_password>@<IP_Address>/cgi-bin/video.jpg?ca
m=1&quality=3&size=2\">");
}
//-->
</script>
</body>
</html>
```

---

---

## Download Event-triggered Snapshots

There are three video image files for the video channel of three stages: pre-alarm, the moment when triggered and post-alarm. Only the snapshots captured by the last event are preserved. Administrator and users can use FTP or URL to get the saved snapshots. They can also be browsed from the application page in system configuration.

### Get triggered snapshots via URL

/cgi-bin/snapshot.jpg?file= <value>

<b>Video channel</b>	<b>Video</b>
<b>Snapshot stage</b>	
snapshot before event	Pre1
snapshot upon event	Trg1
snapshot after event	Pos1

### Get triggered snapshots via FTP

<b>File name</b>	<b>Pre-alarm</b>	<b>Upon alarm</b>	<b>Post-alarm</b>
Video	vpre.jpg	vtrg.jpg	vpos.jpg

---

---

## Uploading Snapshots Periodically

### **Upload snapshots to external FTP server**

In sequential mode, Network Camera will send out snapshots according to interval and period settings. If snapshot files are intended for quick updates, it is better to skip date and time suffix. The file name will then be video.jpg. If the snapshots are used for occasional monitoring, suffix with date and time can help administrators classify them easily.

### **Send snapshots to external SMTP (email) server**

Comparing to the FTP method, email will induce more delay. But the email can notify users for prompt action.

---

---

## Customize Graphics in Homepage

While in text mode, there is a small icon named BTN\_TEXT.GIF preceding with each link that can be changed by administrators. While in image mode, the default method will use the image stored in Flash memory. The followings are the referenced file name and size limitation of each stored images. Administrators may customize preferred image under the size limit and put to the specific name via FTP. Administrators can download the original images before upload for backup.

Object	File name	Maximal size
Logo	logo.gif	Logo and background share 8000 bytes
Background	back.gif	Logo and background share 8000 bytes
Link icon	btn_text.gif	2000 bytes
Configuration	btn_conf.gif	5000 bytes

Usage via FTP is illustrated as below.

```
F:\>ftp 192.168.0.62
Connected to 192.168.0.62.
220 Networ Camera FTP server ready.
User (192.168.0.62:(none)): root
331 Password required.
Password:
230 User name accepted.
ftp> put logo.gif logo.gif
200 PORT command OK.
150 ready to take file.
226 closing.
ftp: 2533 bytes sent in 0.00Seconds 2533000.00kbytes/sec.
ftp> bye
221 Goodbye.

F:\>
```

---

---

## Command Script for Complex Applications

Besides the application wizard, Network Camera provides a more professional command script for advanced applications. The command script will be executed exclusively with the settings in Application page of system configuration except for the weekly schedule. To build the advanced application, follow the steps below.

1. Use any text editor to edit the appropriate command script according to the command format. The script size cannot exceed 500 bytes.
2. Save the script as a file named "SCRIPT.TXT".
3. Use FTP with administrator's privilege to upload the script file.
4. Enter the Application page in system configuration to define the time period in weekly schedule. If it is supposed to run any time, keep the original settings but check the option "All the time except for the above schedule".
5. Check the option "Enable the external script file to exclude the following settings" to activate the command script.

### Command format

[Event][OperatorEvent].....=[Action][+Action].....;

Event

["Digital Input Number""Digital Input State"]

["M" "Channel Number..."]

["Channel Number""Video Input State"]

Operator

"+": (OR)

"\*": (AND)

Action

[("Delay Time")"Digital Output Number""Digital Output State"]

["V""Channel Number""P""Preset Location Number"]

["W"{ "IP": "Port" } { "Message" }]

["U""Method"]

["S""Channel Number..."]

["N"{ "filename" }];

### Parameter explanation

Item between brackets means optional but at least one item should exist.

"Digital input number": always 1

---



---

"Digital input state":	H (high), L (low), / (low to high), \ (high to low)
"M":	motion detection event.
"Channel Number":	always A
"Video input state":	/ (signal from loss to presence), \ (signal from presence to loss), X (as long as signal loss)
"Delay time":	seconds of delay for the following actions after events happen
"Digital output number":	always 1
"Digital output state":	C (NC), O (NO)
"V":	set video channel to go to preset location
"P":	set preset location number to go to preset location
"W":	send warning to server
"IP":	server IP
"Port":	server port
"Message":	texts to be sent to the server
"U":	upload snapshots
"Method":	'F' is by FTP, 'M' is by e-mail
"S":	take snapshot
"N":	define the format of the filename
";":	end of line

The filename format is,

%a	image characterization (pre, trg, pos)
%y	year
%M	month
%d	day
%h	hour
%m	minute
%s	second
%t	tenth second

---

---

## Practical examples

Command line	Description
M1=1C;	When any motion is detected, "Normal Close" of relay output will short with "Common".
1\=(5)1O;	When DI transients from high to low, "Normal Open" of relay output will short with COMMON in 5 seconds.
A=W{192.168.0.1:6000}{no signal!};	If there is no video signal, a message "no signal!" will be sent to port 6000 of 192.168.0.1 once.
1H=V1P15;	When sensor input 2 is high, drive the camera mapped to video 1 to go to preset location 16.
M1=UF+S1+N{video%c%a@%y%M%d%h%m%s};	If any motion is detected, upload snapshots. If an event triggered at 19:05:30 2002/10/15, the snapshot files will be named as, videopre@20021015190530.jpg, videotrg@20021015190530.jpg, videopos@20021015190531.jpg

 The script file is limited to maximum 500 characters. The actual performance will depend on the complexity of the command script. Administrators should reduce the redundant check as possible. Overload conditional check and heavy actions may retard the system operation.

---

---

## URL for External Device Control

### Query status of digital input

[/cgi-bin/getdi.cgi](#)

Network Camera will return the status of digital input.

### Drive digital output

[/cgi-bin/setdo.cgi?do1=<state>](#)

<state>:            *C*, *O* denoting Normal Close or Normal Open respectively.

---

---

## URL of System Maintenance

### Download System Log via FTP

Besides viewing the system log from the web page, administrators can download the system log file, SYSTEM.LOG, via FTP. To log into the FTP daemon, enter "root" as the user name and the same administrator's password used in Web access.

### Restart System via URL

/cgi-bin/reset.cgi

Restart Network Camera without warning.

### Restore Factory Default Settings via URL

/cgi-bin/restore.cgi

Network Camera will automatically restart after restoring factory default configurations.

---

---

## Configure System via FTP

Administrators can use FTP to configure Network Camera much quicker than Web page especially for multiple targets. To configure system via FTP, first download the parameter file, CONFIG.INI, to customize each field according to the environment and then upload back to validate the new settings. To log into the FTP daemon, enter "root" as the user name and the same password used when connecting to the Web server. The serial number of Network Camera is the password for the initial access.

The file is composed of eight categories: [SYSTEM], [LAYOUT], [NETWORK], [VIDEO], [ALERT], and [DEMO]. The category name in brackets should be in upper case. The item name in angle braces should be in lower case. Some items related to disable/enable should use the keywords "YES"/"NO". The number zero entry in <user name> and <user password> is for administrators, i.e. "root". Basically Network Camera will restart automatically as soon as the file is accepted. If administrators want to cancel the reboot procedure, set the first item, <reset system> to NO. It will take effect once only and always show YES in the download file.

A sample CONFIG.INI is attached below. *The italic text* following each line describes the characteristic of the field and *the bold italic characters* are the options of the field.

### Network Camera Initial Configuration File

[SYSTEM]	
<reset system>	
YES	<i>or NO</i>
<host name>	
Network Camera	<i>string of maximum 40 characters</i>
<serial number>	
0002D1040011	<i>read-only</i>
<software version>	
IP21x2-VVTK-0101c	<i>read-only</i>
<current date>	
2004/06/08	<i>read-only</i>
<current time>	
12:34:56	<i>read-only</i>
<time zone>	
0	<i>from 12 to -12</i>
<user name>	
(0)root	<i>read-only</i>
(1)	<i>string of maximum 16 characters</i>
(2)	<i>the followings are as same as the above</i>
(3)	
(4)	
(5)	
(6)	

(7)  
(8)  
(9)  
(10)  
(11)  
(12)  
(13)  
(14)  
(15)  
(16)  
(17)  
(18)  
(19)  
(20)

<user password>  
(0)0002D1040011

(1)  
(2)  
(3)  
(4)  
(5)  
(6)  
(7)  
(8)  
(9)  
(10)  
(11)  
(12)  
(13)  
(14)  
(15)  
(16)  
(17)  
(18)  
(19)  
(20)

<more guests enabled>  
NO  
<more guests interval>  
0

[LAYOUT]

<layout type>

1

<font color>

1

<background color>

0

<logo type>

1

<background type>

1

<logo source>

http://

<background source>

http://

<logo link>

http://

*string of maximum 16 characters  
the followings are as same as the above*

*or YES to enable snapshot mode*

*seconds of snapshot interval*

*image mode or 0 for text mode*

*0-black, 1-white, 2-green, 3-maroon, 4-olive, 5-navy, 6-purple, 7-gray, 8-yellow, 9-lime, 10-aqua, 11-fuchsia, 12-silver, 13-red, 14-blue, 15-teal,*

*default image, or 0 for blank, or 2 from URL*

*default image, or 0 for blank, or 2 from URL*

*URL of logo type 2, maximum 80 characters*

*URL of logo type 2, maximum 80 characters*

*reference link of logo, max. 80 characters*

[NETWORK]

<install enabled>

YES

*string of maximum 8 characters*

<ppp enabled>

NO

*reset IP whenever system boots or **NO***

<ethernet address>

00-02-D1-04-00-11

*obsolete*

<host ip>

192.168.0.207

*read-only*

<subnet mask>

255.255.255.0

*standard IP format*

<gateway ip>

0.0.0.0

*standard IP format*

<primary name server>

0.0.0.0

*standard IP format*

<secondary name server>

0.0.0.0

*standard IP format*

<ntp enabled>

NO

*standard IP format*

<network timing server>

*or **YES***

<smtp mail server>

*IP address or domain name*

<mail recipient address>

*IP address or domain name*

<mail return address>

Network Camera

*string of maximum 80 characters*

<backup smtp mail server>

*string of maximum 80 characters*

<backup mail recipient address>

*IP address or domain name*

<local ftp port>

21

*string of maximum 80 characters*

<ftp server>

*or 1024 ~ 65535*

<ftp port>

21

*IP address or domain name*

<ftp username>

*or 1024 ~ 65535*

<ftp password>

*string of maximum 16 characters*

<ftp init path>

*string of maximum 16 characters*

<ftp passive>

NO

*string of maximum 40 characters*

<backup ftp server>

*or **YES***

<backup ftp port>

21

*IP address or domain name*

<backup ftp username>

*or 1024 ~ 65535*

<backup ftp password>

*string of maximum 16 characters*

<backup ftp init path>

*string of maximum 16 characters*

<backup ftp passive>

NO

<http server port>

80

<bandwidth limit>

0

[VIDEO]

<overlay timestamp>

NO

<caption text>

<colored video>

YES

<video quality>

4

<default size>

1

<brightness>

0

<contrast>

0

<hue>

0

<saturation>

0

[ALERT]

<script file enabled>

NO

<motion detection channel enabled>

NO

<snapshot channel enabled>

NO

<series snapshot channel enabled>

NO

<application mode>

0

<visual alert>

NO

<upload method>

0

<file with time suffix>

YES

<percentage of object size over screen>

10

*string of maximum 40 characters*

*or YES*

*or 1024 ~ 65535*

*or 64000, 128000, 256000, 512000,  
768000, 1000000, 1500000, 2000000*

*or YES*

*or NO*

*8,6,4,3,2 representing Medium, Standard,  
GOOD, DETAILED, EXCELLENT*

*0,1,2,3,4, representing Double, Standard,  
Half, Standard x2, Half X2*

*among 5 and -5*

*among 5 and -5*

*among 5 and -5*

*among 5 and -5*

*or YES to activate external script*

*or YES*

*or YES*

*or YES*

*disabled, 1 for Sequential, 10 for motion  
detection event, 12 for DI event*

*or YES*

*FTP, 1 for email*

*or NO*

*1~99*

---

---

<percentage of sensitivity>

**90**

*1~99*

<tenth seconds to snapshot after event>

5

<snapshots taken after event>

1

<time to start snapshot>

00:00:00

24 hours format

<time to stop snapshot>

00:00:00

24 hours format

[DEMO]

<demo enabled>

NO

*or YES*

<video is open>

NO

*or YES*

---

---

## Telnet Commands

Network Camera has a Telnet daemon for only administrators to access some seldom used functions. Using any general terminal program to connect to Network Camera will prompt the user for a password. Username is not requested here since only administrators can access the Telnet daemon. The password is as same as that used in web access. After logging in, type "*help*" for the command list. If "*debug*" or "*dinote*" is not executed, Telnet will disconnect automatically after being idle for 1 minute.

### System core debugging

General activities are recorded into SYSTEM.LOG continuously, but information about abnormal status is not. To look deep into the core debugging information, administrators may type the "*debug*" command. This will cause Network Camera to start dumping the detailed debugging information while the system is running. This is useful to examine if any error has occurred when the system operates abnormally. The stored information will be cleared automatically after the dump. Network Camera will continue to dump new messages unless the connection is broken. If Telnet is not connected, any messages will be stored until administrators re-login.

### Monitor changed status of digital input

Typing "*dinote*" will make Network Camera send the current status of digital input. After that Network Camera will continuously monitor DI status and send messages only when the state has changed. For example, after typing "*dinote*" the terminal will display  
DI1=L  
and after DI1 changes to H, terminal will display  
DI1=H

### Stop information dumping

Typing "*stop*" will cease dumping debug information and the digital input status.

### Query status of digital input

Typing "*diquery*" will display the status of all digital input once.

### Set digital output

To set digital output to connect NO with COMMON, type "DO1=L".

To set digital output to connect NC with COMMON, type "DO1=H".

---

---

## Erase snapshots stored in Flash memory

Typing "*erase image*" will clear all snapshots saved in Flash memory.

## Erase logo and graphic buttons

Typing "*erase graph*" will clear all images used on the homepage. If no new images are uploaded, the system will switch to text mode and use default images instead.

## Skip installation at next boot

Typing "*lock*" will inform Network Camera to fix current network settings. It need not wait for installation during the next boot.

## Reset network for new settings

Typing "*unlock*" will make Network Camera give up current settings and wait for installation.

## Restore factory default settings

Typing "*clear*" will make Network Camera restore factory settings but not restart. To validate new settings, type "*reset*" to make the system restart.

## Reset system

Typing "*reset*" will make Network Camera perform a software reset.

---

---

# Appendix

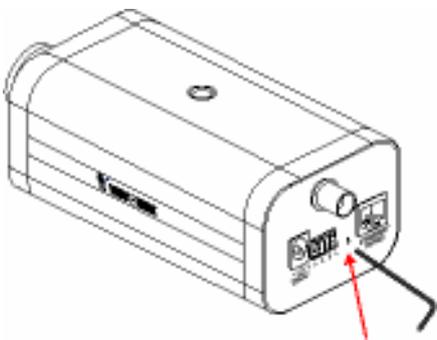
## A. Troubleshooting

### Status LED

After the power has been turned on, Network Camera will perform a self-diagnostic to detect any hardware defects. The following table lists the LED patterns in general conditions. In case of any fatal error, the LED will blink in another pattern.

| Condition                             | LED color                             |
|---------------------------------------|---------------------------------------|
| During self-diagnostic after power on | Blink in interchanged green and red   |
| Ethernet signal is lost               | Steady red till Ethernet is detected  |
| Before network is setup               | No LED of sign till IP address is set |
| After network is setup                | Blink green once per second           |
| Any hardware failure                  | Other patterns                        |

### Reset and restore



Sometimes resetting the system can make the system back to normal state. If the system still has problems after reset, restore the factory settings and install again.

RESET: Poke the wrench to click on the button.

RESTORE:

1. Poke the wrench to press on the button continuously.
2. Wait for self-diagnostic to run twice.
3. Withdraw the wrench as soon as the second

### self-diagnostic starts.



Restore the factory defaults will lose any previous settings. Reset or restore the system after power on.

---

---

## B. Frequently Asked Questions

**Q** Why can't I see the Network Camera in the installer after reboot?

**A** The installer is only used to install the IP address of Network Camera. If the IP address is fixed by checking the option in the installer, the Network Camera will no longer appear in the installer.

**Q** Why can't I connect the Network Camera after reboot?

**A** If the IP address is not fixed, Network Camera will always wait for installing command for a valid IP address. That means the previous IP address will not be used if the option in the installer is not checked; or the option in the network configuration is not cleared. The benefit of waiting for a valid IP address by default is that administrators can find the Network Camera in the installer to prevent IP conflict. As long as the IP address is confirmed, it is suggested to fix the IP address to make Network Camera automatically start up whenever regaining power.

**Q** What if I forget my password?

**A** Every access to Network Camera needs authentication. If you are not a permitted user, you may view the images or control the camera as long as the demo account is opened. The demo account user may use username as "demo" without any password to access limited features. If you are one of the managed users, you have to ask the administrators for the password. If you are the administrator, there is no way to recover the root password. The only way to regain access to Network Camera is to restore the factory settings and reinstall it.

**Q** Why can't I watch video from Network Camera after it is authenticated?

**A** There are many possible scenarios regarding this problem,

1. If you have just installed Network Camera and are unable to watch the video, check if the video input is enabled and the video modulation in Configuration page.
  2. If Network Camera is well installed and you are accessing Network Camera for the first time using Internet Explorer, adjust the security level of Internet Explorer to allow installation of the plug-in.
  3. If the problem still exists after adjusting, the current users may be over the system allows.
  4. In case that you use demo account, the administrator may protect the video from the public.
- 
-

---

---

Q How can I use a name instead of the IP address to connect Network Camera?

A To allow users to connect to Network Camera through an easily memorized name, the administrators must first configure the name server in his network. Here is an example: the administrator installs the Network Camera with a reserved IP address and assigns it with a name in the domain name service, then users can connect to Network Camera by typing a name instead of IP address. If there is DHCP service in the network, the IP address must be excluded in the DHCP service to prevent from IP conflict.

Q What is the plug-in for?

A The plug-in provided by Network Camera is used to display motion pictures on Internet Explorer that does not support server push technology. If your system does not allow installation of any plug-in software, the security level of web browser may need to be lowered. It is recommended that you consult your network supervisor in your office regarding the adjustment of the security level.

Q Why is the timestamp different from the system time of my PC or notebook?

A The timestamp is based on the system time of Network Camera. It is maintained by a real-time clock inside and automatically synchronizes with the time server if Network Camera is connected to the Internet and the function is enabled. Differences of several hours may result from the time zone setting.

Q Why does the image not refresh regularly?

A In a modem environment, it is because the bandwidth of PPP connection is far less than Ethernet. If the difference of the timestamp is not stable, adjust the UART FIFO lower in both receiving and transmitting from modem property in the control panel. While in Ethernet, it may be due to time taken in storing snapshots into memory upon events occurring.

Q How many users are allowed to watch Network Camera at the same time?

A To achieve the best effect, Network Camera will allow twenty users to connect at the same time. Excess users can get an auto-refreshed still image in homepage instead. It is recommended to build another web server to host a large quantity of users by retrieving images from Network Camera periodically.

Q How fast is the video rate of Network Camera?

A The JPEG codec can process 30 frames per second internally. However the total performance is subject to many coefficients as follows,

1. network throughput,

2. bandwidth share,
  3. number of users,
  4. number of video input is accessed at one time,
  5. the complicated objects in view results in larger image file,
  6. the level of your PC or notebook which is responsible of displaying images.
- In general, the transfer rate in general local network environment can achieve over 200 kilobytes per second and approximately 10 to 20 pictures of normal environment per second. The general frame size is illustrated in the follow table for reference.

| Quality setting | Size of each frame | Bandwidth demand for 30fps |
|-----------------|--------------------|----------------------------|
| Medium          | 9.3 kbyte          | 2246 kbps                  |
| Standard        | 11.15 kbyte        | 2676 kbps                  |
| Good            | 13.76 kbyte        | 3303 kbps                  |
| Detailed        | 16.35 kbyte        | 3925 kbps                  |
| Excellent       | 20.3 kbyte         | 4886 kbps                  |

**Q** How can I keep Network Camera as private as possible?

**A** Network Camera is designed for surveillance purpose and has many flexible interfaces. The user authentication and special confirmation in installation can keep Network Camera from unauthorized access. You may also change the HTTP port to non-public number. You can check system log to examine any abnormal activities and trace the origins.

**Q** Why can I see image files when I use dir in FTP even if the alarm is not triggered?

**A** Every time Network Camera starts, it will capture the images as vpre.jpg. If there are previously saved image files that are not retrieved, Network Camera will keep them until they are accessed.

**Q** How will the stored images be processed if Network Camera loses power?

**A** If user has defined the snapshot interval, Network Camera will capture images periodically. Once the pre-defined condition is match, the pre-alarm images will be kept and the current images will be saved. The subsequent images will be stored as post-alarm stage. User may retrieve these files either by downloading via FTP or direct Network Camera send them in e-mails. That means after monitoring conditions are met, Network Camera will keep these image files until user retrieval even if power is lost.

**Q** If I set Network Camera to send e-mails of images whenever the conditions are met, will my e-mail account overflow?

**A** It is recommended to use transient state rather than steady state. For instance, use

---

---

'Input is Rising' and 'Input is Falling' rather than 'Input is High' and 'Input is Low' to let the condition be triggered only when state is changed.

**Q** The image is not clear enough. Is anything broken?

**A** The lens can be fine adjusted by rotating the outer ring. Please rotate it clockwise or counter-clockwise to focus near or far.

---

---

## C. Upgrade System Firmware

Customers can frequently check the appropriate product folder on our web site to download the latest firmware. Only administrators can upgrade the system firmware of Network Camera.

### Easy way via Upgrade Wizard

Run the Upgrade Wizard included in the product CDROM and proceed by the prompts. Refer to the user's guide of Upgrade Wizard for details.

### Alternative via FTP

1. Decompress the compressed file in a local folder. A file named FLASH.BIN should appear.
2. Use the FTP program and change the working directory to the local folder where FLASH.BIN exists.
3. Connect to Network Camera with user name as "root" and password.
4. Use the PUT command to upload FLASH.BIN to Network Camera. The file size is near 1.5 mega bytes. It will take approximately 2 seconds in a local network, 2 minutes by null modem connection or 6 minutes by modem, but still subject to user's network.
5. After upload is complete, close the connection.
6. If the received FLASH.BIN is checked without error, Network Camera will update the software in Flash memory and restart automatically. When Network Camera starts writing firmware, both status LED indicators will stay on until system restarts. It takes about 30 to 40 seconds. User must keep the power stable during the update process. After the system restarts, Network Camera may need installation depending on whether the "Reset network at next boot" option is enabled or not. After Network Camera boots up, reload the web page in the browser.



If power fails during the software upgrade, the program in the memory of Network Camera may be destroyed permanently. If Network Camera cannot restart properly, ask the dealer for technical service.

---

---

## D. URL Commands of Network Camera

For some customers who already have their own web site or web control application, Network Camera can be easily integrated through convenient URL. This section lists the commands in URL format corresponding to the basic functions of Network Camera. Some RFC standards related to HTML may be a good reference for implementation of the customized homepage.

### Page URL

The configuration page has a frame layout including option list frame and an option page frame. Referenced URL except for the configuration page directs to option page frame only. Some pages, like image quality setting and preset setting, are opened in new windows for preview.

These URLs can be accessed only by administrators.

| Homepage name            | Referenced URL       |
|--------------------------|----------------------|
| configuration page       | /setup/config.html   |
| system option            | /setup/system.html   |
| security option          | /setup/security.html |
| network option           | /setup/network.html  |
| video option             | /setup/video.html    |
| image quality option     | /setup/image.html    |
| application option       | /setup/app.html      |
| motion detection setting | /setup/motion.html   |
| view snapshots           | /setup/snap.html     |
| demo option              | /setup/demo.html     |
| homepage layout option   | /setup/layout.html   |
| system log               | /setup/logfile.html  |
| system parameters        | /setup/parafile.html |
| set factory default      | /setup/factory.html  |

### System resource URL

There are some images used on the homepage when the homepage layout is in image mode. Administrators may use the following links to show the images saved in Network Camera on another page. To change the logo or the background images referenced by the URL, refer to the [homepage layout](#) section in configuration.

---

---

---

---

| <b>Resource name</b>           | <b>Referenced URL</b> |
|--------------------------------|-----------------------|
| system logo image              | /logo.gif             |
| background image               | /back.gif             |
| button image for configuration | /btn_conf.gif         |
| icon image for link indicator  | /btn_text.gif         |

---

---

## General format of command URL

Every configuration can be set through URL with POST method by administrators only.

<general format>

URL[?[name=value][&name=value].....]

<method>

POST

<authorized user>

root

## System configuration URL

URL: [/cgi-bin/system.cgi](#)

| NAME   | VALUE                                    | DESCRIPTION                                |
|--------|--|--|
| host   | <text string shorter than 15 characters> | system name                                |
| method | keep                                     | keep date and time unchanged               |
|        | auto                                     | use NTP server to synchronize              |
|        | manu                                     | directly adjust date and time              |
| date   | <yy/mm/dd>                               | year, month and date separated by slash    |
| time   | <hh:mm:ss>                               | hour, minute and second separated by colon |
| ntp    | <domain name or IP address>              | NTP server                                 |
| zone   | GMT±<n>:00                               | time zone, n ranged from 0 to 12           |

## Security configuration URL

URL: [/cgi-bin/security.cgi](#)

| NAME       | VALUE                                    | DESCRIPTION                         |
|------------|--|-------------------------------------|
| rootpass   | <text string shorter than 15 characters> | change root password                |
| username   | <text string shorter than 15 characters> | add new user                        |
| userpass   | <text string shorter than 15 characters> | new user's password                 |
| ioallowed  | <not required>                           | allow user to control DO            |
| ptzallowed | <not required>                           | allow user to view PT scanner panel |
| deluser    | <text string shorter than 15 characters> | Existing user name                  |

---

---

|               |                |   |
|---------------|----------------|---|
|               | characters>    |   |
| slow          | <not required> | Snapshot mode                             |
| open          | <not required> | enable demo account                       |
| demoioallowed | <not required> | allow demo user to control the I/O access |
| slow          | <not required> | snapshot mode                             |
| delay         | <integer>      | refresh time in snapshot mode             |

## Network configuration URL

URL: </cgi-bin/network.cgi>

| NAME          | VALUE                                    | DESCRIPTION                       |
|---------------|--|-----------------------------------|
| reset         | yes                                      | enable installation at next boot  |
|               | <other than yes>                         | disable installation at next boot |
| ip            | <IP address>                             | Network Camera's IP address       |
| subnet        | <IP address>                             | subnet mask                       |
| router        | <IP address>                             | default gateway                   |
| domain        | <text string shorter than 40 characters> | domain name of Network Camera     |
| dns1          | <IP address>                             | primary DNS server                |
| dns2          | <IP address>                             | secondary DNS server              |
| limit         | Not limited                              | use full network bandwidth        |
|               | 64Kbits/second                           | use only 64Kbps of bandwidth      |
|               | 128Kbits/second                          | use only 128Kbps of bandwidth     |
|               | 256Kbits/second                          | use only 256Kbps of bandwidth     |
|               | 512Kbits/second                          | use only 512Kbps of bandwidth     |
|               | 768Kbits/second                          | use only 768Kbps of bandwidth     |
|               | 1Mbits/second                            | use only 1Mbps of bandwidth       |
|               | 1.5Mbits/second                          | use only 1.5Mbps of bandwidth     |
| 2Mbits/second | use only 2Mbps of bandwidth              |                                   |
| http          | <number less than 65535>                 | HTTP port                         |
| smtp1         | <domain name or IP address>              | primary SMTP server               |
| mailto1       | <text string shorter than 80 characters> | mail recipient address            |
| smtp2         | <domain name or IP address>              | secondary SMTP server             |
| mailto2       | <text string shorter than 80 characters> | mail recipient address            |

|            |  |                                       |
|------------|--|---------------------------------------|
| returnmail | <text string shorter than 80 characters> | return address                        |
| ftp1       | <domain name or IP address>              | primary FTP server                    |
| ftprp1     | <number less than 65535>                 | FTP server port                       |
| ftpuser1   | <text string shorter than 15 characters> | user name for primary FTP server      |
| ftppass1   | <text string shorter than 15 characters> | password for primary FTP server       |
| ftpfolder1 | <text string shorter than 40 characters> | upload folder in primary FTP server   |
| ftp2       | <domain name or IP address>              | secondary FTP server                  |
| ftprp2     | <number less than 65535>                 | secondary FTP server port             |
| ftpuser2   | <text string shorter than 15 characters> | user name for secondary FTP server    |
| ftppass2   | <text string shorter than 15 characters> | password for secondary FTP server     |
| ftpfolder2 | <text string shorter than 40 characters> | upload folder in secondary FTP server |

## Video configuration URL

URL: </cgi-bin/video.cgi>

| NAME    | VALUE                                    | DESCRIPTION               |
|---------|--|---------------------------|
| time    | <not required>                           | enclose timestamp         |
| text    | <text string shorter than 15 characters> | enclose caption           |
| color   | B/W                                      | set encoder to monochrome |
|         | <other than B/W>                         | set encoder to color      |
| size    | Half                                     | set size to half          |
|         | Standard                                 | set size to standard      |
|         | Double                                   | set size to double        |
|         | Half x 2                                 | set size to half x 2      |
|         | Standard x 2                             | set size to standard x 2  |
| quality | Medium                                   | lowest resolution         |
|         | Standard                                 | lower resolution          |
|         | Good                                     | normal setting            |
|         | Detailed                                 | higher resolution         |

---

---

Excellent

highest resolution

---

---

## Image quality configuration URL

URL: </cgi-bin/imagesetting.cgi>

| NAME       | VALUE          | DESCRIPTION                  |
|------------|----------------|------------------------------|
| brightness | <-5 ~ 5>       | adjust brightness of image   |
| contrast   | <-5 ~ 5>       | adjust contrast of image     |
| hue        | <-5 ~ 5>       | adjust hue of image          |
| saturation | <-5 ~ 5>       | adjust saturation of image   |
| preview    | <not required> | not save the parameters      |
| restore    | <not required> | recall the original settings |
| save       | <not required> | save the parameters          |

## Motion detection configuration URL

URL: </cgi-bin/motion.cgi>

| NAME | VALUE     | DESCRIPTION            |
|------|-----------|------------------------|
| per  | <integer> | object size percentage |
| sen  | <integer> | sensitivity percentage |

## Application configuration URL

URL: </cgi-bin/app.cgi>

| NAME      | VALUE          | DESCRIPTION                         |
|-----------|----------------|-------------------------------------|
| sun       | <not required> | set Sunday in weekly schedule       |
| mon       | <not required> | set Monday in weekly schedule       |
| tue       | <not required> | set Tuesday in weekly schedule      |
| wed       | <not required> | set Wednesday in weekly schedule    |
| thu       | <not required> | set Thursday in weekly schedule     |
| fri       | <not required> | set Friday in weekly schedule       |
| sat       | <not required> | set Saturday in weekly schedule     |
| sbegin    | <hh:mm:ss>     | time to start in weekly schedule    |
| send      | <hh:mm:ss>     | time to stop in weekly schedule     |
| inv       | <not required> | set inverse mode in weekly schedule |
| enfile    | <not required> | enable script file                  |
| emode     | <not required> | event operation                     |
| showalert | <not required> | show alert in image                 |
| mdmode    | <not required> | Enable motion detection             |
| dihigh    | <not required> | Enable DI is high                   |
| dilow     | <not required> | Enable DI is low                    |

---

---

---



---

|          |                |  |
|----------|----------------|--|
| dirise   | <not required> | Enable DI is rising                        |
| difall   | <not required> | Enable DI is falling                       |
| delay    | <integer>      | delay time of DO after event               |
| ioalarm  | <not required> | trigger DO when DI condition matched       |
| mdalarm  | <not required> | trigger DO when motion detected            |
| ioupload | <not required> | upload snapshot when DI condition matched  |
| mdupload | <not required> | upload snapshot when motion detected       |
| resetdo  | <not required> | Clear the DO status                        |
| smode    | <not required> | sequential mode application                |
| sinter   | <integer>      | tenth seconds interval for sequential mode |
| smethod  | mail           | upload snapshots by email                  |
|          | ftp            | upload snapshots by FTP                    |
| suffix   | <not required> | FTP file with date and time suffix         |

---



---

---

---

## Homepage layout configuration URL

URL: </cgi-bin/layout.cgi>

| NAME    | VALUE                                    | DESCRIPTION                       |
|---------|--|-----------------------------------|
| cuslogo | blank                                    | hide logo                         |
|         | def                                      | use default logo                  |
|         | url                                      | use image from URL                |
| logourl | <text string shorter than 80 characters> | URL of image for logo             |
| linkurl | <text string shorter than 80 characters> | URL to link when clicking on logo |
| cusback | blank                                    | hide background image             |
|         | def                                      | use default background            |
|         | url                                      | use image from URL                |
| backurl | <text string shorter than 80 characters> | URL of image for background       |
| fcolor  | <0 ~ 15>                                 | color index for font              |
| bcolor  | <0 ~ 15>                                 | color index for background        |
| dismode | image                                    | display homepage in image mode    |
|         | text                                     | display homepage in text mode     |

---

---

## E. Time Zone Table

While setting the time zone in automatic date/time synchronization, find the hour offset in the followings for your region. GMT stands for Greenwich Mean Time, which is the global time that all time zones are measured from.

|             |  |
|-------------|--|
| (GMT-12:00) | International Date Line West                           |
| (GMT-11:00) | Midway Island, Samoa                                   |
| (GMT-10:00) | Hawaii   |
| (GMT-09:00) | Alaska   |
| (GMT-08:00) | Pacific Time (US & Canada), Tijuana                    |
| (GMT-07:00) | Arizona  |
| (GMT-07:00) | Chihuahua, La Paz, Mazatlan                            |
| (GMT-07:00) | Mountain Time (US & Canada)                            |
| (GMT-06:00) | Central America  |
| (GMT-06:00) | Central Time (US & Canada)                             |
| (GMT-06:00) | Guadalajara, Mexico City, Monterrey                    |
| (GMT-06:00) | Saskatchewan   |
| (GMT-05:00) | Bogota, Lima, Quito                                    |
| (GMT-05:00) | Eastern Time (US & Canada)                             |
| (GMT-05:00) | Indiana (East)   |
| (GMT-04:00) | Atlantic Time (Canada)                                 |
| (GMT-04:00) | Caracas, La Paz  |
| (GMT-04:00) | Santiago   |
| (GMT-03:30) | Newfoundland   |
| (GMT-03:00) | Brasilia   |
| (GMT-03:00) | Buenos Aires, Georgetown                               |
| (GMT-03:00) | Greenland  |
| (GMT-02:00) | Mid-Atlantic   |
| (GMT-01:00) | Azores   |
| (GMT-01:00) | Cape Verde Is.   |
| (GMT)       | Casablanca, Monrovia                                   |
| (GMT)       | Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London |
| (GMT+01:00) | Amsterdam, Berlin, Bern, Stockholm, Vienna             |
| (GMT+01:00) | Belgrade, Bratislava, Budapest, Ljubljana, Prague      |
| (GMT+01:00) | Brussels, Copenhagen, Madrid, Paris                    |
| (GMT+01:00) | Sarajevo, Skopje, Warsaw, Zagreb                       |

---

---

|             |   |
|-------------|---|
| (GMT+01:00) | West Central Africa                           |
| (GMT+02:00) | Athens, Istanbul, Minsk                       |
| (GMT+02:00) | Bucharest                                     |
| (GMT+02:00) | Cairo   |
| (GMT+02:00) | Harare, Pretoria                              |
| (GMT+02:00) | Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius |
| (GMT+02:00) | Jerusalem                                     |
| (GMT+03:00) | Baghdad                                       |
| (GMT+03:00) | Kuwait, Riyadh                                |
| (GMT+03:00) | Moscow, St. Petersburg, Volgograd             |
| (GMT+03:00) | Nairobi                                       |
| (GMT+03:30) | Tehran  |
| (GMT+04:00) | Abu Dhabi, Muscat                             |
| (GMT+04:00) | Baku, Tbilisi, Yerevan                        |
| (GMT+04:30) | Kabul   |
| (GMT+05:00) | Ekaterinburg                                  |
| (GMT+05:00) | Islamabad, Karachi, Tashkent                  |
| (GMT+05:30) | Chennai, Kolkata, Mumbai, New Delhi           |
| (GMT+05:45) | Kathmandu                                     |
| (GMT+06:00) | Almaty, Novosibirsk                           |
| (GMT+06:00) | Astana, Dhaka                                 |
| (GMT+06:00) | Sri Jayawardenepura                           |
| (GMT+06:30) | Rangoon                                       |
| (GMT+07:00) | Bangkok, Hanoi, Jakarta                       |
| (GMT+07:00) | Krasnoyarsk                                   |
| (GMT+08:00) | Beijing, Chongqing, Hongkong, Urumqi          |
| (GMT+08:00) | Taipei  |
| (GMT+08:00) | Irkutsk, Ulaan Bataar                         |
| (GMT+08:00) | Kuala Lumpur, Singapore                       |
| (GMT+08:00) | Perth   |
| (GMT+09:00) | Osaka, Sapporo, Tokyo                         |
| (GMT+09:00) | Seoul   |
| (GMT+09:00) | Yakutsk                                       |
| (GMT+09:30) | Adelaide                                      |
| (GMT+09:30) | Darwin  |
| (GMT+10:00) | Brisbane                                      |
| (GMT+10:00) | Canberra, Melbourne, Sydney                   |
| (GMT+10:00) | Guam, Port Moresby                            |

---

---

---

---

|             |                                     |
|-------------|-------------------------------------|
| (GMT+10:00) | Hobart                              |
| (GMT+10:00) | Vladivostok                         |
| (GMT+11:00) | Magadan, Solomon Is., New Caledonia |
| (GMT+12:00) | Auckland, Wellington                |
| (GMT+12:00) | Fiji, Kamchatka, Marshall Is..      |
| (GMT+13:00) | Nuku'alofa                          |

---

---

## G. Technical Specifications

### System

CPU: Trimedia PNX1300

RAM: 16MB SDRAM

ROM: 2MB FLASH ROM

### Networking

Adjustable bandwidth limit

#### Protocol

TCP/IP, HTTP, SMTP, FTP, Telnet, NTP, DNS and DHCP

#### Modem

PPP (dial-up, direct cable connection)

#### Physical

10BaseT Ethernet or 100BaseT Fast Ethernet

### Video

#### Algorithm Supported

MJPEG

#### Features

Adjustable image size and quality

B/W or color control

Timestamp and text overlay

#### Resolution

##### IP2112

Up to 30 frames at 176x112

Up to 30 frames at 352x240

Up to 9 frames at 704x480

##### IP2122

Up to 25 frames at 176x144

Up to 25 frames at 352x288

Up to 8 frames at 704x576

### Camera Specification

1/4 inch color CCD image sensor

1 Lux/F2.0

AGC, AWB, AES

#### IP2112

- Resolution: 512(H)x492(V)

- Electroic shutter. 1/60 ~ 1/100.000sec

#### IP2122

- Resolution: 512(H)x492(V)

- Electroic shutter. 1/50 ~ 1/100.000sec

### General I/O

1 sensor inputs (max. 12VDC 50mA)

1 relay outputs (max. 24VDC 1A, 125VAC 0.5A)

### LED Indicator

System status indicator

### Dimension

168.5mm(L) \* 73.6mm(W) \* 57.3mm(H)

### Weight

Net. 376 g.

### Power

Consumption: near 5.4W

Input: 100-240VAC, 50/60Hz, 0.4A

Output: 12VDC, 1.5A

### Operating Environment

Temperature: 0-50°C/32-122°F

Humidity: 95%RH

### EMI & Safety

CE, FCC

### Viewing System Requirement

Internet Explorer 4.x or above,

Netscape Navigator 4.x or above

---

---

## Electromagnetic Compatibility (EMC)

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

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

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

**Europe** **CE** - This digital equipment fulfills the requirement for radiated emission according to limit B of EN55022/1998, and the requirement for immunity according to EN50082-1/1992.

## Liability

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

### Vivotek Inc.

web site: [www.vivotek.com](http://www.vivotek.com)

email: [sales@vivotek.com](mailto:sales@vivotek.com)

Rev. 1.0

Made in Taiwan.

©Copyright 2003. All rights reserved.