

# 1-CHANNEL VIDEO TRANSMITTER

## USER'S MANUAL





**WARNING**

**RISK OF ELECTRIC SHOCK  
DO NOT OPEN**

**WARNING:** TO REDUCE THE RISK OF ELECTRIC SHOCK,  
DO NOT REMOVE COVER (OR BACK).  
NO USER-SERVICEABLE PARTS INSIDE.  
REFER SERVICING TO QUALIFIED  
SERVICE PERSONNEL.

**COMPLIANCE NOTICE OF FCC:**

THIS EQUIPMENT HAS BEEN TESTED AND FOUND TO COMPLY WITH THE LIMITS FOR A CLASS A DIGITAL DEVICE, PURSUANT TO PART 15 OF THE FCC RULES. THESE LIMITS ARE DESIGNED TO PROVIDE REASONABLE PROTECTION AGAINST HARMFUL INTERFERENCE WHEN THE EQUIPMENT IS OPERATED IN A COMMERCIAL ENVIRONMENT. THIS EQUIPMENT GENERATES, USES, AND CAN RADIATE RADIO FREQUENCY ENERGY AND IF NOT INSTALLED AND USED IN ACCORDANCE WITH THE INSTRUCTION MANUAL, MAY CAUSE HARMFUL INTERFERENCE TO RADIO COMMUNICATIONS. OPERATION OF THIS EQUIPMENT IN A RESIDENTIAL AREA IS LIKELY TO CAUSE HARMFUL INTERFERENCE, IN WHICH CASE USERS WILL BE REQUIRED TO CORRECT THE INTERFERENCE AT THEIR OWN EXPENSE.

**WARNING:** CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

THIS CLASS OF DIGITAL APPARATUS MEETS ALL REQUIREMENTS OF THE CANADIAN INTERFERENCE-CAUSING EQUIPMENT REGULATIONS.

The information in this manual is believed to be accurate as of the date of publication. We are not responsible for any problems resulting from the use thereof. The information contained herein is subject to change without notice. Revisions or new editions to this publication may be issued to incorporate such changes.

The software included in this product contains some Open Sources. You may obtain the complete corresponding source code from us. See the Open Source Guide on the software CD (OpenSourceGuide\OpenSourceGuide.pdf) or as a printed document included along with the User's Manual.

**WEEE (Waste Electrical & Electronic Equipment)****Correct Disposal of This Product**

*(Applicable in the European Union and other European countries with separate collection systems)*



This marking shown on the product or its literature, indicates that it should not be disposed with other household wastes at the end of its working life. To prevent possible harm to the environment or human health from uncontrolled waste disposal, please separate this from other types of wastes and recycle it responsibly to promote the sustainable reuse of material resources.

Household users should contact either the retailer where they purchased this product, or their local government office, for details of where and how they can take this item for environmentally safe recycling.

Business users should contact their supplier and check the terms and conditions of the purchase contract. This product should not be mixed with other commercial wastes for disposal.

## Important Safeguards

### 1. Read Instructions

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

### 2. Retain Instructions

The safety and operating instructions should be retained for future reference.

### 3. Cleaning

Unplug this equipment from the wall outlet before cleaning it. Do not use liquid aerosol cleaners. Use a damp soft cloth for cleaning.

### 4. Attachments

Never add any attachments and/or equipment without the approval of the manufacturer as such additions may result in the risk of fire, electric shock or other personal injury.

### 5. Water and/or Moisture

Do not use this equipment near water or in contact with water.

### 6. Placing and Accessories

Do not place this equipment on an unstable cart, stand or table. The equipment may fall, causing serious injury to a child or adult, and serious damage to the equipment. Wall or shelf mounting should follow the manufacturer's instructions, and should use a mounting kit approved by the manufacturer.



This equipment and cart combination should be moved with care. Quick stops, excessive force, and uneven surfaces may cause the equipment and cart combination to overturn.

### 7. Power Sources

This equipment should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power, please consult your equipment dealer or local power company.

### 8. Power Cord

Operator or installer must remove power and TNT connections before handling the equipment.

### 9. Lightning

For added protection for this equipment during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet and disconnect the antenna or cable system. This will prevent damage to the equipment due to lightning and power-line surges.

### 10. Overloading

Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.

### 11. Objects and Liquids

Never push objects of any kind through openings of this equipment as they may touch dangerous voltage points or short out parts that could result in a fire or electric shock. Never spill liquid of any kind on the equipment.

### 12. Servicing

Do not attempt to service this equipment yourself. Refer all servicing to qualified service personnel.

### 13. Damage requiring Service

Unplug this equipment from the wall outlet and refer servicing to qualified service personnel under the following conditions:

- A. When the power-supply cord or the plug has been damaged.
- B. If liquid is spilled, or objects have fallen into the equipment.
- C. If the equipment has been exposed to rain or water.
- D. If the equipment does not operate normally by following the operating instructions, adjust only those controls that are covered by the operating instructions as an improper adjustment of other controls may result in damage and will often require extensive work by a qualified technician to restore the equipment to its normal operation.
- E. If the equipment has been dropped, or the cabinet damaged.
- F. When the equipment exhibits a distinct change in performance — this indicates a need for service.

### 14. Replacement Parts

When replacement parts are required, be sure the service technician has used replacement parts specified by the manufacturer or that have the same characteristics as the original part. Unauthorized substitutions may result in fire, electric shock or other hazards.

### 15. Safety Check

Upon completion of any service or repairs to this equipment, ask the service technician to perform safety checks to determine that the equipment is in proper operating condition.

### 16. Field Installation

This installation should be made by a qualified service person and should conform to all local codes.

### 17. Correct Batteries

Warning: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

### 18. Tmra

A manufacturer's maximum recommended ambient temperature (Tmra) for the equipment must be specified so that the customer and installer may determine a suitable maximum operating environment for the equipment.

### 19. Elevated Operating Ambient Temperature

If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (Tmra).

### 20. Reduced Air Flow

Installation of the equipment in the rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.

### 21. Mechanical Loading

Mounting of the equipment in the rack should be such that a hazardous condition is not caused by uneven mechanical loading.

### 22. Circuit Overloading

Consideration should be given to connection of the equipment to supply circuit and the effect that overloading of circuits might have on over current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

### 23. Reliable Earthing (Grounding)

Reliable grounding of rack mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).

# Table of Contents

Chapter 1 — Introduction .....	1
1.1 In This Manual .....	1
1.2 Features .....	1
1.3 Typical Applications .....	2
Chapter 2 — Installation .....	5
2.1 Package Contents .....	5
2.2 Front Panel .....	5
Factory Reset .....	5
2.3 Rear Panel .....	6
Chapter 3 — Remote Setup .....	8
3.1 Quick Setup .....	8
3.2 System .....	9
General .....	9
Date/Time .....	10
User/Group .....	10
3.3 Network .....	11
IP Address .....	11
DVRNS .....	12
Port .....	12
Bandwidth Control .....	13
Security .....	13
3.4 Video .....	14
Camera .....	14
Live Monitoring .....	14
Webcasting .....	15
MAT .....	15
3.5 Audio .....	15
Input/Output .....	16
3.6 Event .....	16
Alarm In .....	16
Motion Detection .....	17
Video Loss .....	18
Video Blind .....	18
System Event .....	19
Event Action .....	19
Chapter 4 — Web Monitoring .....	20
Appendix .....	23
LED Indicators .....	23
Troubleshooting .....	23
Connector Pin Outs .....	23
Map of Screens (Remote Setup) .....	24
Specifications .....	25



# Chapter 1 — Introduction

## 1.1 In This Manual

This manual is intended for users of the one-channel network video transmitter (network video encoder) and includes instructions for using and managing the transmitter on the network.

## 1.2 Features

This network video transmitter compresses live video from analog cameras and transmits the video over Ethernet connections. The transmitter can be accessed, configured and managed by using the INIT (Integrated Network Installation Tool) program. It has a built-in web server allowing you to monitor live video remotely using a web browser. The remote programs (RASplus and iNEX Basic) provided with the transmitter also allows remote management, monitoring and recording. This transmitter offers the following features:

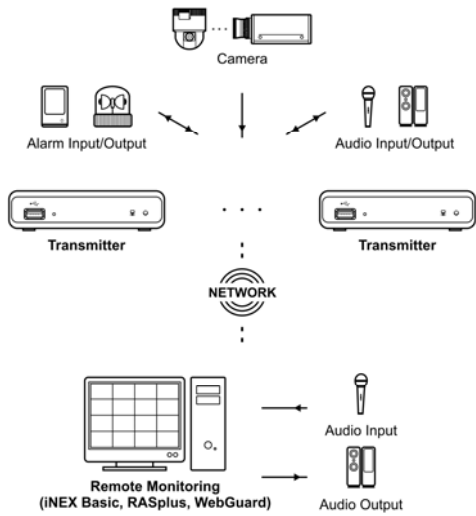
- Auto detection for NTSC and PAL
- Dual streaming for monitoring and recording
- H.264, MPEG-4 and M-JPEG compression algorithm
- Four levels of video compression and various video compression resolutions
- Two-way audio communication
- Pre- and post-event buffering and video stream buffering to enhance reliability of network recording
- Remote monitoring via web browser or remote software
- Compatibility with Genetec Omnicast software using Genetec Protocol (RTSP Port: 554)
- Automatic HTML code generation for webcasting on a user's website
- Up to 20 simultaneous connections to the transmitter
- Enhanced security using IP address filtering, HTTPS and SSL functions and password protected multiple user levels
- Network bandwidth limit and MAT functions to use network bandwidth efficiently
- ONVIF protocol supported
- Convenient firmware upgrades via either the USB port or the network
- Firmware duplication and autorecovery functions to enhance system stability
- Management of multiple transmitters via Ethernet connections
- Event detection functions: alarm-in, motion, video loss, video blind
- Power sources: 12 VDC, 24 VAC, PoE (Power over Ethernet)
- RS485 interface for controlling a PTZ camera
- 1-channel alarm in and out
- 1-channel audio in and out

### NOTES:

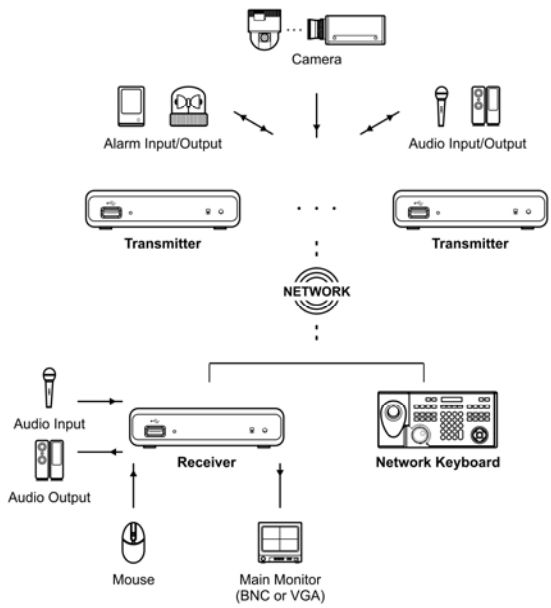
- Remote monitoring and recording through dual streaming are available by using the RASplus and iNEX Basic programs provided with the transmitter.
- In this manual, a "remote system" refers to a PC that the remote program or WebGuard program is running, or a network video receiver.

### 1.3 Typical Applications

#### Remote Monitoring (I)

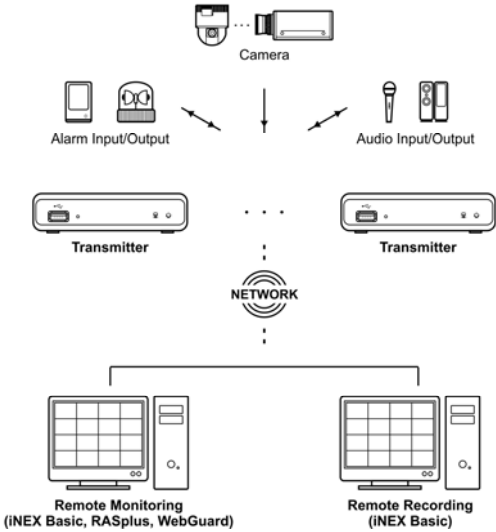


#### Remote Monitoring (II)

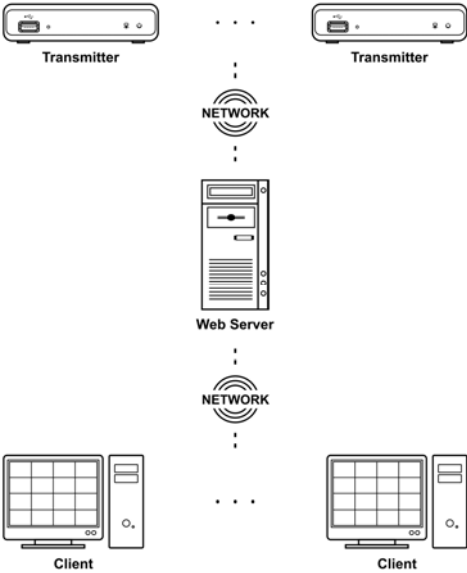




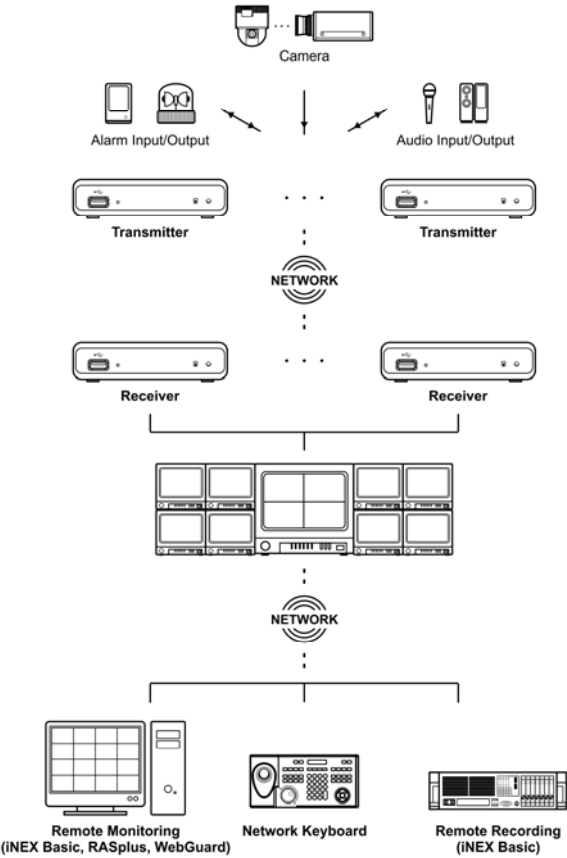
## Remote Recording



## Webcasting



Control Center

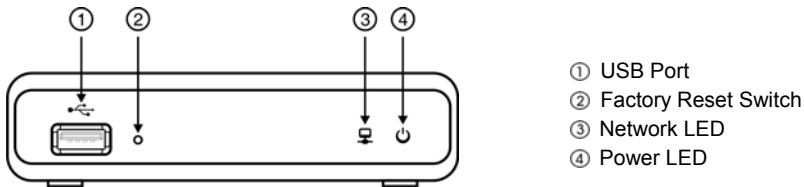


## Chapter 2 — Installation

### 2.1 Package Contents

- Network Video Transmitter
- DC Adapter (12V)
- Power Cord
- Installation CD (INIT, RASplus and iNEX Basic software, iNEX Basic User's Manual)
- User's Manuals (Transmitter, INIT, RASplus)
- Wall-mount Kits

### 2.2 Front Panel



- **USB Port:** Connect a USB flash drive to upgrade the software. Disconnect power from the transmitter and connect a USB flash drive containing the upgrade package file (.rui and autorun.txt) to the transmitter. Connect power to the transmitter, and the software will be upgraded automatically. You can upgrade the software remotely by running the INIT program. Refer to the INIT User's Manual for details on remote software upgrade.
- **Factory Reset Switch:** Use to return all settings to the original factory settings. See below for details.
- **Network LED:** Displays network connection status. Refer to *Appendix A – LED Indicators* for details.
- **Power LED:** Displays system operating status. Refer to *Appendix A – LED Indicators* for details.

### Factory Reset

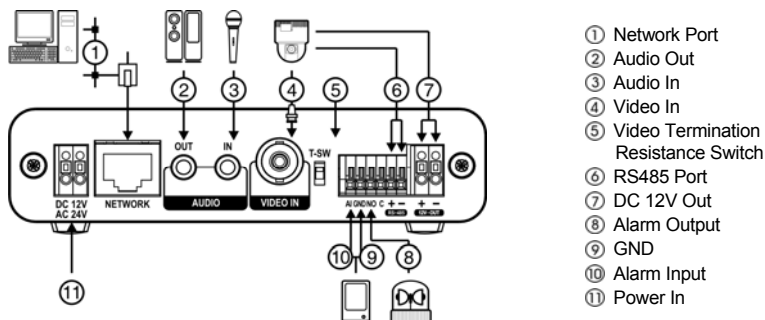
This switch will only be used on the rare occasions that you want to return all the settings to the original factory settings.

**CAUTION:** When performing a Factory Reset, you will lose any settings you have saved.

Disconnect the power adapter from the transmitter. → Poke a straightened paperclip into the factory reset switch hole. → Connect the power while holding the reset switch → Release the switch when the Network and Power LEDs blink together. → The transmitter resets to factory defaults and restarts after completing the factory reset.

You can perform a factory reset while the transmitter is turned on by poking a straightened paperclip into the factory reset switch hole and releasing the reset switch. A factory reset also can be performed remotely by running the INIT program. The transmitter restarts after completing the factory reset. Refer to the INIT User's Manual for details on remote factory resetting.

## 2.3 Rear Panel



- **Network Port:** Connect a Cat5 cable with an RJ-45 connector. Refer to the INIT User's Manual for details about network connection setup. When using a PoE switch, the transmitter can be supplied with power over Ethernet cable (Refer to the PoE switch manufacturer's manual for details).
- **Audio Out:** Connect to an amplifier (Line-out). The transmitter does not have amplified audio output, so you will need a speaker with an amplifier.
- **Audio In:** Connect to an audio source. (Line-in or Microphone)
- **Video In:** Connect coaxial cables from the video sources (NTSC or PAL).
- **Video Termination Resistance Switch:** Push down the video termination resistance switch to turn it on.
- **RS485 Port:** Connect to a PTZ camera. Connect TX+/RX+ and TX-/RX- of the PTZ camera to the + and - (respectively) of the transmitter. Refer to the PTZ camera manufacturer's manual for configuring the RS485 connection. When the transmitter receives RS485 data via a video receiver, other RS485 communication devices can be connected. Refer to the video receiver's User's Manual for details for receiving RS485 data via a video receiver.
- **DC 12V Out:** Connect the power wires from the camera (12 VDC). The camera can be supplied power from the transmitter when using 12 VDC power. Connect + and - of the camera to the + and - (respectively) of the transmitter.
- **Alarm Output:** Connect an alarm-out device to the NO (Normally Open) and C (Common) connectors. NO is a relay output which sinks 0.3A @ 125 VAC and 1A @ 30 VDC.
- **GND:** Connect to the ground side of the alarm inputs.
- **Alarm Input:** Connect alarm-in devices. Mechanical or electrical switches can be wired to the AI (Alarm-In) and GND (Ground) connectors. The voltage range is from 0V to 3.3V. When the electrical switch is wired, the threshold voltage for NC (Normally Closed) is above 2.4V and for NO (Normally Open) is below 0.3V, and it should be stable at least 0.5 seconds to be detected.
- **Power In:** Connect two wires from the power adapter (12 VDC or 24 VAC). You do not need to distinguish power polarity when connecting the wires. The transmitter starts booting as soon as power is applied.

### NOTES:


- To make connections on the Alarm Connector Strip, press and hold the button and insert the wire in the hole below the button. After releasing the button, tug gently on the wire to make certain it is connected. To disconnect a wire, press and hold the button above the wire and pull out the wire.
- Camera and audio surveillance may be prohibited by laws that vary by region. Check the laws in your area before using this product for surveillance purposes.

**CAUTIONS:**

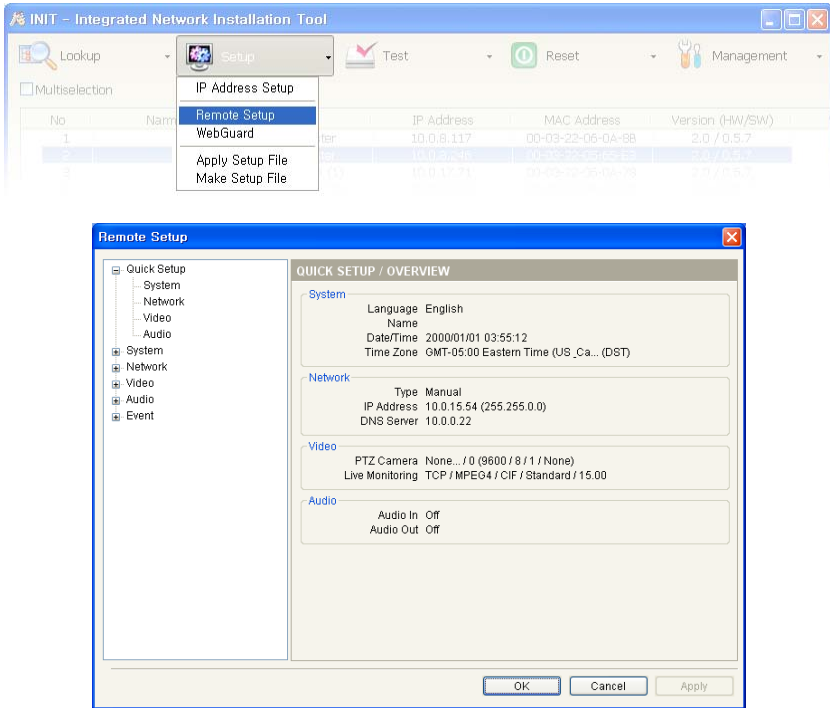
- The transmitter restarts after the power adaptor is disconnected from the transmitter when switching the power source from 12 VDC or 24 VAC to PoE.
- The network connector is not designed to be connected directly with cable or wire intended for outdoor use.

**WARNING: ROUTE POWER CORDS SO THAT THEY ARE NOT A TRIPPING HAZARD. MAKE CERTAIN THE POWER CORD WILL NOT BE PINCHED OR ABRADED BY FURNITURE. DO NOT INSTALL POWER CORDS UNDER RUGS OR CARPET. THE POWER CORD HAS A GROUNDING PIN. IF YOUR POWER OUTLET DOES NOT HAVE A GROUNDING PIN RECEPTACLE, DO NOT MODIFY THE PLUG. DO NOT OVERLOAD THE CIRCUIT BY PLUGGING TOO MANY DEVICES INTO ONE CIRCUIT.**

# Chapter 3 — Remote Setup

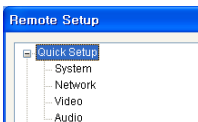
Remote Setup allows you to change all settings of the transmitter. Run the INIT program, select a transmitter and click the Setup icon  on the Main screen. Select Remote Setup from the Setup menu and the Remote Setup screen appears. You can also display the Remote Setup screen by selecting a transmitter, clicking the right mouse button and selecting Remote Setup on the Main screen.

**NOTE:** You can also change the settings by using remote programs (RASplus or iNEX Basic) or a web browser.



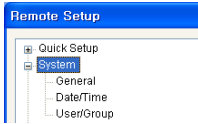
Clicking a menu in the left of the Remote Setup screen displays the current settings for that menu on the right side of the screen. Clicking submenus under each menu allows you to change the settings. Clicking the OK button closes the Remote Setup screen and applies the changes.

## 3.1 Quick Setup



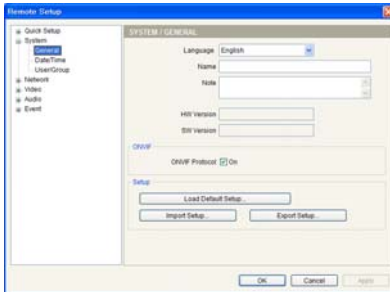
The Quick Setup allows you to change a transmitter's basic system, network, video and audio settings.

## 3.2 System



You can change a transmitter's system information, import or export all settings, and add users or groups.

### General



- **Language:** Choose the language to be used during remote setup.
- **Name:** Enter the transmitter's name (up to 31 characters including spaces).
- **Note:** Enter additional information about the transmitter.
- **HW Version, SW Version:** These fields display the transmitter's hardware and software versions.
- **ONVIF Protocol:** Check the box to enable the ONVIF protocol.

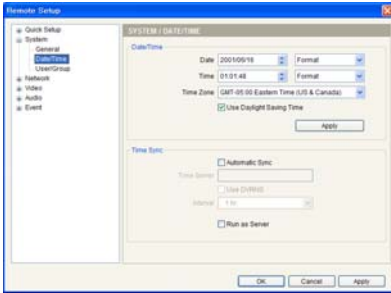
### • Setup

- **Load Default Setup...**: Click to return all to the original factory settings. You can select whether or not network settings will be included when the default setup is applied. Refer to the Network menu for details of the network settings.
- **Import Setup...**: Click to apply the settings saved as a .dat file format to the transmitter. A setup screen appears allowing you to select the setup file. You can select whether or not network settings (except the DVRNS setting) will be included when the setup is applied. Refer to the Network menu for details of the network settings.
- **Export Setup...**: Click to save the current transmitter settings as a .dat file format. A setup screen appears allowing you to name the setup file.

### NOTES:

- The *Load Default Setup* and *Import Setup* functions are permitted only to the users in the *Administrator* group.
- Do NOT check the *Include Network Setup* box when the network settings of the setup file are used in another transmitter. Otherwise, the connection to the transmitter might not be made properly.
- If the IP address, admin port number or SSL settings are changed during *Setup*, Remote Setup closes after saving the changes.

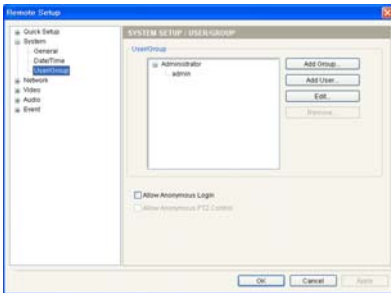
## Date/Time



- **Date/Time:** Change the system date/time, date/time format and time zone and turn daylight saving time on or off by checking the box. Clicking the **Apply** button applies the changes immediately.
- **Time Sync**
  - **Automatic Sync:** Check the box to automatically synchronize the time with a time server. Enter the IP address or the domain name of the time server and set the time interval for synchronization. If the time server uses the DVRNS function, selecting the **Use DVRNS** box allows you to enter the name instead of the IP address or the domain name of the time server.
  - **Run as Server:** Check the box to run the transmitter as a time server.

**NOTE:** If you want to use a domain name instead of the IP address of the time server, the DNS server must be set up properly during the *Network – IP Address* setup. If you want to use a name instead of the IP address or the domain name of the time server, the DVRNS function must be set up properly during the *Network – DVRNS* setup.

## User/Group



- **User/Group:** Click the buttons to change the settings for a group or a user allowed controlling the transmitter remotely.
  - **Add Group:** Click to add a group. Enter the desired group name and set authority levels for the group to control the transmitter remotely.
  - **Add User:** Click to add a user. Enter the desired user name and select the group that the user will belong to. Enter a password to be assigned to the user.
  - **Change:** Select a group and click the button to change authority levels assigned to the group, or select a user and click the button to change the user's password.
  - **Delete:** Select a group or user and click the button to delete the group or user.
- **Allow Anonymous Login:** Check the box to use the webcasting feature. Refer to *3.4 Video – Webcasting* for details.
- **Allow Anonymous PTZ Control:** Check the box to allow remote control of a PTZ camera on a website by using the webcasting feature.

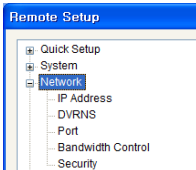
### NOTES:

- The *User/Group* changes are permitted only to the users in the *Administrator* group.
- There is no default password for the *admin* user in the *Administrator* group.
- The authority levels that can be assigned are:
  - **Upgrade:** The user can upgrade the software.
  - **Setup:** The user can set up the system.
  - **Color Control:** The user can control brightness, contrast, hue and saturation for cameras.
  - **PTZ Control:** The user can control a PTZ camera.



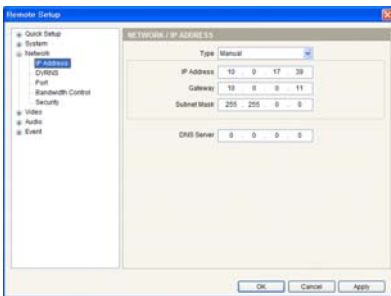
- Alarm-Out Control: The user can reset the output during an alarm.
- System Check: The user can view and check the remote system status.

### 3.3 Network



You can change the network settings, set up DVRNS and security functions and control the network bandwidth.

#### IP Address



- **Type:** Select the type of network configuration. Remote Setup closes after saving the changes.
  - **Manual:** Select when the transmitter is using a static IP address for network connection, and set up LAN parameters manually.
  - **DHCP:** Select when the transmitter is networked via DHCP (Dynamic Host Configuration Protocol). Click the OK button, and a temporary IP address is automatically assigned to the transmitter. The transmitter periodically will be issued a new IP address automatically.
  - **ADSL:** Select when the transmitter is networked via ADSL. Enter the ID and password for ADSL connection, and click the OK button. A temporary IP address is automatically assigned to the transmitter. The transmitter periodically will be issued a new IP address automatically.

- **DNS Server:** Enter the IP address of the DNS server. If you set up the DNS server, the domain name of the server can be used instead of the IP address during the DVRNS, time or SMTP server setup. Ask your Internet service provider for the IP Address of the DNS Server.

#### NOTES:

- Ask your network provider for details about the network connection type and connection information for the transmitter.
- If the transmitter is configured for a DHCP or ADSL network, it is best to use the DVRNS function because the transmitter's IP address might change frequently. Ask your Internet service provider for information about the IP Address of the DNS Server.

## DVRNS



Check the DVR Name Service box to use the DVRNS function.

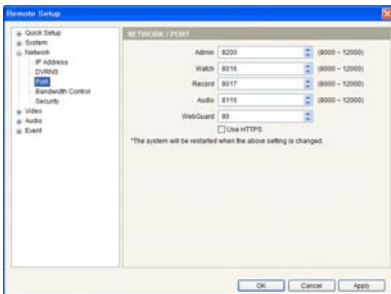
- **DVRNS Server:** Enter the IP address or domain name of the DVRNS server.
- **Port:** Set up the port number of the DVRNS server.
- **Use NAT:** Check the box when using NAT (Network Address Translation).
- **DVR Name:** Enter the transmitter's name to be registered on the DVRNS server. Check whether or not the name is available by clicking the **Check** button.

- **Help Desk:** Choosing the OK button registers the transmitter on the DVRNS server. Proper DVRNS settings will display the help desk information of the DVRNS server.

### NOTES:

- The DVRNS (DVR Name Service) function allows the transmitter to use dynamic IP addresses for remote connection. When using this function, you can access the transmitter remotely by using the transmitter's name instead of its IP address. For the DVRNS function to work properly, the transmitter should be registered on the DVRNS server, and the DVRNS server settings in the INIT program for the transmitter should match the settings registered on the DVRNS server. Any changes on the DVRNS server might cause improper operation.
- When LAN settings have been changed, set up the DVRNS settings after saving your LAN changes by clicking the **OK** button.
- You will need to get the IP address or domain name of the DVRNS server from your network administrator. You can use the domain name instead of IP address if you set up the DNS server during the IP Address setup.
- When using a NAT (Network Address Translation) device, refer to the NAT manufacturer's instructions for the proper network settings.
- The transmitter's name you entered in the *DVR Name* field should be checked by clicking the **Check** button, otherwise the DVRNS changes will not be saved. When entering no name or a name already registered on the DVRNS server, an error message displays. If a transmitter's name includes the #, \, or % characters, connections to the transmitter using a web browser might fail.

## Port

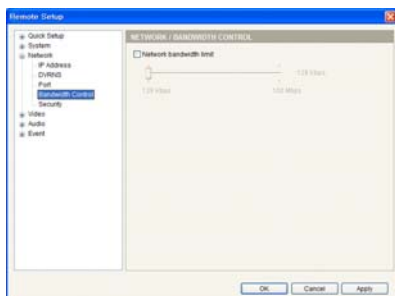


- **Admin, Watch, Record, Audio, WebGuard:** Set up port numbers for connections to the transmitter by using the remote programs or web browser. Remote Setup closes after saving the changes (Admin port number only).
- **Use HTTPS:** Check the box to enhance the security of WebGuard pages by using the HTTPS protocol when running the WebGuard program.

**NOTE:** Do NOT use the same port number for more than one function, or else, the transmitter cannot be connected with the remote programs.

**CAUTIONS:**

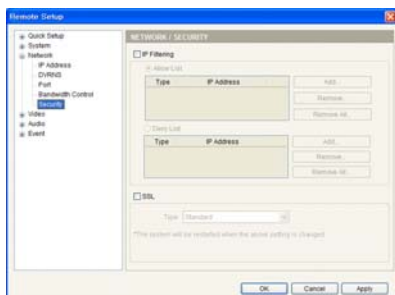
- When changing the port settings, you must change the port settings on remote programs too.
- When using the HTTPS protocol, the ONVIF protocol might not work.

**Bandwidth Control**

You can control the network bandwidth by limiting the network bandwidth depending on the network traffic.

Check the **Network bandwidth limit** box and set the desired maximum bandwidth.

**NOTE:** When limiting the network bandwidth, the frame rate might decrease to lower than the frame rate set during the *3.4 Video – Live Monitoring* setup.

**Security**

- **IP Filtering:** Check the box to use the IP filtering function. You can allow or block connections to the transmitter by designating IP addresses.

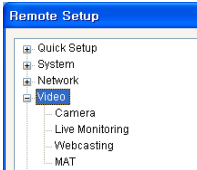
- **Add:** Click the button to add IP addresses to the **Allow List** or **Deny List** to allow or block connection to the transmitter. Selecting the **Host** option allows you to add one IP address at a time. Selecting the **Group** option allows you to add continuous IP address numbers in one action by designating a range of IP addresses to add.
- **Remove, Remove All:** Click the button to remove the selected IP address or all IP addresses from **Allow List** or **Deny List**.

- **SSL:** Check the box to use the SSL function. You can enhance the security of outgoing data from the transmitter by using the SSL (Secure Sockets Layer) protocol. When using the SSL function, the transmitter cannot be connected with a program or a system that does not support the SSL function. Remote Setup closes after saving the changes.

**NOTES:**

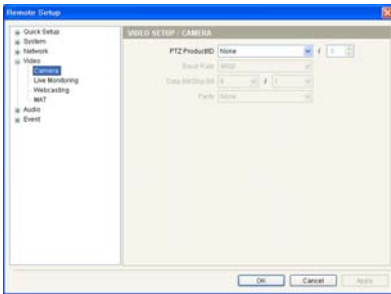
- If you want to use the time synchronization, DVRNS and Email sending functions, the connection of the IP addresses of the time server, DVRNS server and the SMTP server must be allowed when you set up the IP filtering function. Any connection to the transmitter from the IP address in *Deny List* will NOT be allowed.
- Using the SSL function might cause congestion in the system receiving data from the transmitter depending on the security level.
- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)

### 3.4 Video



You can set camera features and image transmission parameters for both remote monitoring and webcasting.

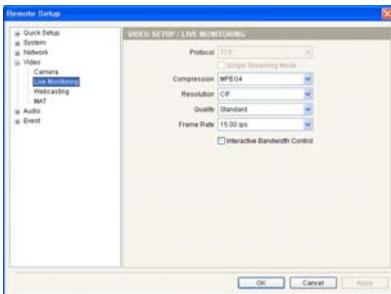
#### Camera



- **PTZ Product / ID:** Select a PTZ camera connected to the transmitter and assign an ID to the PTZ camera.
- **Baud Rate, Data Bit, Stop Bit, Parity:** Set up baud rate, data bit, stop bit and parity by referring to the PTZ camera manufacturer's instructions.

**NOTE:** You will not be able to control a PTZ camera if it is not connected to the RS485 port properly. See Chapter 2 – Installation; 2.3 Rear Panel Connectors, RS485 Port and the PTZ camera manufacturer's manual for configuring the RS485 connection.

#### Live Monitoring



- **Compression, Resolution, Quality, Frame Rate:** Select the image parameters to transmit images to remote systems for live monitoring. The setting might be changed when the Interactive Bandwidth Control function is set up.
- **Single Streaming Mode:** Check the box to set up the Single Streaming mode (H.264 compression algorithm only). When in the Single Streaming mode, the maximum frame rate you can set for H.264 compression algorithm increases, but instead remote recording is not available.

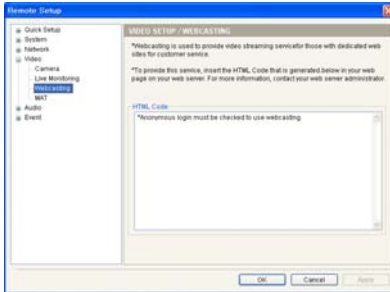
- **Interactive Bandwidth Control:** Check the box to control the network bandwidth by allowing the Resolution or Frame Rate set above to be changed flexibly depending on the screen format. The resolution or frame rate will be changed automatically to the value adjusted to the screen format of the system that the screen format is changed the most recently among systems which receive images from the transmitter.

#### NOTES:

- Simultaneous connections to the transmitter might cause the frame rate to decrease.
- The maximum frame rate you can set for H.264 compression algorithm is half of that for other compression algorithms in the dual streaming mode. When setting up the Single Streaming mode, the maximum frame rate you can set for H.264 compression algorithm increases.
- For the *Interactive Bandwidth Control* function to work, the system which receives images from the transmitter also should be set up to use the function.

**CAUTION:** Remote recording is not available when in the single streaming mode.

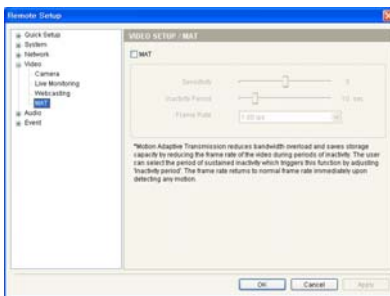
## Webcasting



You can stream live video from the transmitter to a website. Copy the HTML Code displayed on the screen and paste it in your web page code.

**NOTE:** To use the webcasting service, you must check the *Allow Anonymous Login* option during 3.2 System – User/Group setup.

## MAT

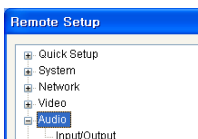


Check the MAT box to use the MAT (Motion Adaptive Transmission) function for live monitoring images.

- **Sensitivity:** Set the motion sensitivity. The higher the number is, the more sensitive it is.
- **Inactivity Period:** Set the inactivity period. The transmitter will transmit images in Frame Rate set below until any change is detected after the inactivity period when no motion is detected during the preset inactivity period.
- **Frame Rate:** Select the frame rate of video to transmit images to remote systems when no motion is detected. The selected frame rate will be applied until any motion is detected after the inactivity period and will return to the normal frame rate set during the Live Monitoring setup immediately upon detecting any motion. This frame rate cannot be set up to higher than the normal frame rate set during the Live Monitoring setup.

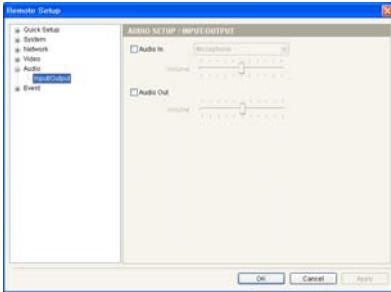
**NOTE:** The MAT (Motion Adaptive Transmission) function allows you to reduce bandwidth overload by reducing the frame rate when no motion is detected. The transmitter considers that no motion is detected when no change is detected between two consecutive images based on the sensitivity setting. This function is not supported for remote recording.

## 3.5 Audio



You can set up audio in and out.

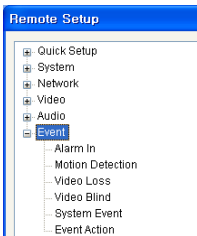
## Input/Output



- **Audio In:** Check the box to enable audio in and select the proper audio-in device. You can also adjust the volume.
- **Audio Out:** Check the box to enable audio out. You can also adjust the volume.

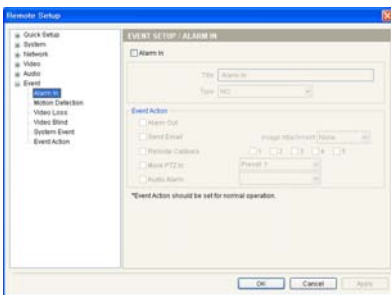
**NOTE:** The transmitter does not have amplified audio output, so you need to use a speaker with an amplifier.

## 3.6 Event



You can set up event detection and actions to be taken.

### Alarm In



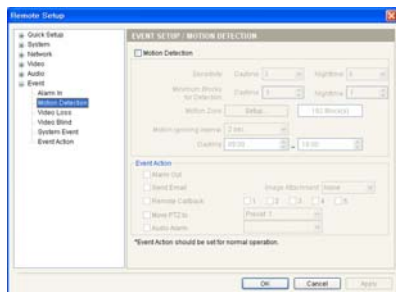
Check the **Alarm In** box to set up an alarm-in event. When the transmitter senses an input on the alarm input connector, it considers it as an event.

- **Title:** Enter the alarm-in device's name.
- **Type:** Select the alarm-in type.
- **Event Action:** Check the box for each action the transmitter will take whenever it detects an alarm-in event.
  - **Alarm Out:** Check the box to trigger an alarm-output signal.

- **Send Email:** Check the box to send an email. Selecting a camera in the **Image Attachment** field attaches an event detected image file (.JPG) to the email.
- **Remote Callback:** Check the box and select the remote systems to send a message (Not supported for the WebGuard program).
- **Move PTZ to:** Select the desired preset number that you want the PTZ camera to move to. You must set up preset locations of a PTZ camera using remote programs or a web browser.
- **Audio Alarm:** Check the box and select the audio file (.wav) to sound.

**NOTE:** You must properly configure the settings related to each event action during 3.6 Event – Event Action setup to enable event actions.

## Motion Detection



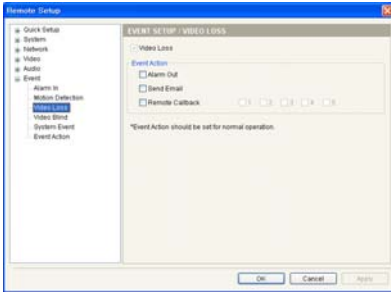
Check the Motion Detection box to set up a motion detection event. When the transmitter detects a motion in a configured motion detection zone, it considers the motion as an event.

- **Sensitivity:** Set the motion sensitivity for daytime and nighttime independently.
- **Minimum Blocks for Detection:** Adjust the minimum number of detection blocks (1 to 192) that must be activated to be considered as a motion event for daytime and nighttime independently.

- **Motion Zone:** Click the Setup... button and a motion detection zone setup screen appears. Define the area of the image that you want to set up a motion detection zone by using the motion detection zone icons.
  - (Select) or (Clear): Click to select or clear blocks for motion detection.
  - or (One or All block): Click to select or clear one or all blocks at a time.
  - (Area): Click to select or clear several blocks of an area.
- **Motion Ignoring Interval:** Select the motion ignoring dwell time from the drop-down list. The transmitter will not log or send notifications of motion events occurring during the preset interval after other motion is detected. You can control excessive event logging and remote notifications of motion detection events by adjusting the motion ignoring dwell intervals.
- **Daytime:** Set up the daytime range. The transmitter will consider the remaining time range as the nighttime.
- **Event Action:** Check the box for each action the transmitter is to take when it detects a motion detection event.
  - **Alarm Out:** Check the box to trigger an alarm-output signal.
  - **Send Email:** Check the box to send an email. Selecting a camera in the Image Attachment field attaches an event detected image file (.JPG) to the email.
  - **Remote Callback:** Check the box and select the remote systems to send a message (Not supported for the WebGuard program).
  - **Move PTZ to:** Click the Setup... button to move a PTZ camera to the previously saved preset location and select the desired preset number. You must set up preset locations of a PTZ camera using remote programs or a web browser.
  - **Audio Alarm:** Check the box and select the audio file (.wav) to sound.

**NOTE:** You must properly configure the settings related to each event action during 3.6 Event – Event Action setup to enable event actions.

## Video Loss

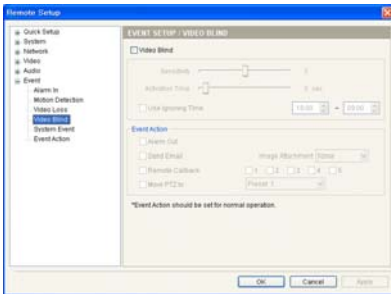


When the transmitter has lost video, it considers the video loss as a video loss event.

- **Event Action:** Check the box for each action the transmitter will take whenever it detects a video loss event.
  - **Alarm Out:** Check the box to trigger an alarm-output signal.
  - **Send Email:** Check the box to send an email.
  - **Remote Callback:** Check the box and select the remote systems to send a message (Not supported for the WebGuard program).

**NOTE:** You must properly configure the settings related to each event action during 3.6 *Event – Event Action* setup to enable event actions.

## Video Blind



Check the Video Blind box to set up a video blind event. When the transmitter detects that more than 70% of a camera is blinded by anything, it considers the video blind as an event.

- **Sensitivity:** Adjust the sensitivity for the video blind.
- **Activation Time:** Adjust the duration that a video blind should last to be considered a video blind event. The transmitter will not consider any video blind as a video blind event if it is shorter than the preset time.

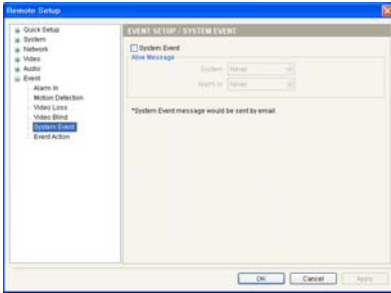
- **Use Ignoring Time:** Set up the event ignoring time. The transmitter will not consider video blind that occurs during the preset time span as an event.
- **Event Action:** Check the box for each action the transmitter will take whenever it detects a video blind event.
  - **Alarm Out:** Check the box to trigger an alarm-output signal.
  - **Send Email:** Check the box to send an email. Selecting a camera in the Image Attachment field attaches an event detected image file (.JPG) to the email.
  - **Remote Callback:** Check the box and select the remote systems to send a message (Not supported for the WebGuard program).
  - **Move PTZ to:** Click the Setup... button to move a PTZ camera to the previously saved preset location and select the desired preset number. You must set up preset locations of a PTZ camera using remote programs or a web browser.

### NOTES:

- Video blind events might NOT be detected for a camera with a very noisy image especially when set for low Sensitivity values.
- You must properly configure the settings related to each event action during 3.6 *Event – Event Action* setup to enable event actions.



## System Event



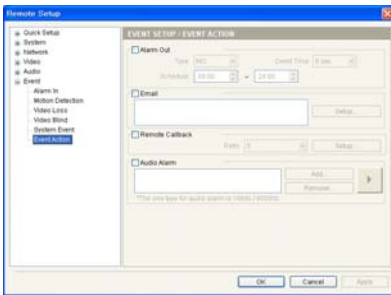
Check the **System Event** box to set up a system event. The transmitter checks and reports the system and alarm-in status.

- **System:** Select the check interval. The transmitter sends an email when the system is operating.
- **Alarm In:** Select the check interval. The transmitter sends an email when there is no alarm-in event status change.

**NOTE:** You must properly configure the *Email* settings during 3.6 Event – Event Action setup to send an email.

## Event Action

You can set up event actions to notify the event detection when the transmitter detects events.



- **Alarm Out:** Check the box to activate alarm out.
  - **Type:** Select the type of alarm-out device.
  - **Dwell Time:** Select the alarm-out dwell time. An alarm out is activated for the preset dwell time after detecting an event.
  - **Schedule:** Set up the period to enable alarm out. An alarm out can be activated only during this period.
- **Email:** Check the box and click the **Setup** button to send an email.
  - **SMTP Server, Port:** Enter the IP address or domain name and port number of the SMTP server. Select **Use SSL/TLS** if the SMTP server requires SSL (Secure Sockets Layer) authentication.

- **Authentication ID, Password:** Enter the ID and password if the SMTP server requires user authentication.
- **Sender, Recipient:** Enter the sender's and recipients' email address. Up to 10 recipients can be added.
- **Image Attachment:** Select the resolution of the image to be attached when sending an Email.
- **Remote Callback:** Check the box to send a callback message to remote systems (Not supported for the WebGuard program).
  - **Retry:** Select the number of times to try sending a message if it fails to send.
  - **Setup:** Enter the IP addresses and port numbers of the remote systems to send a message.
- **Audio Alarm:** Check the box to sound by playing back an audio file. You can add or delete an audio file (.wav) (Mono encoded file in 16 bits/8 KHz only) by clicking the **Add** or **Remove** button. Selecting an audio file in the list and clicking the ► button allows you to test the sound by playing back the selected audio file.

### NOTES:

- You will need to get the IP address or domain name of the SMTP server from your network administrator. You can use the domain name instead of the IP address if you set up the DNS server when setting up the network.
- An email address must include the "@" character to be a valid address.

## Chapter 4 — Web Monitoring

You can monitor live video images from the transmitter on the web browser by using the WebGuard program.

Computer system requirements for using WebGuard are:

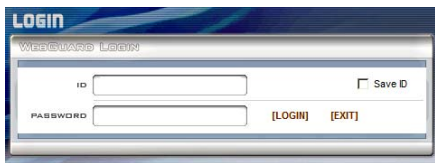
- Operating System: Microsoft® Windows® XP x86 (32 Bit) (Service Pack 3) or Microsoft® Windows® Vista x86 (32 Bit) (Service Pack 1)
- CPU: Intel Pentium III (Celeron) 600MHz or faster
- RAM: 128MB or more
- VGA: 8MB or more (1024x768, 24bpp or higher)
- Internet Explorer: Version 6.0 or later

Start Internet Explorer on your local PC. You can run the WebGuard program by entering the following information in the address field.

- “http://IP address:port number” (The transmitter’s IP address and the WebGuard port number set during the port setup)
- Or, “http://DVRNS server address/transmitter’s name” (The DVRNS server address and the transmitter’s name registered on the DVRNS server)

### NOTES:

- Enter *https* instead of *http* if you have checked the *Use HTTPS* box during the WebGuard port number setup. Click *Continue to this website (not recommended)* when the security certificate warning page is displayed. When the WebGuard login page is not displayed, check Internet option settings as follows:
  - Go to *Tools*, then *Internet Options*, and then the *Security* tab → Click the *Custom level...* button → Set the setting of *Reset custom settings* to *Medium-high (default)* or *Medium*.
  - Go to *Tools*, then *Internet Options*, and then the *Advanced* tab → Check the *Use TLS 1.0* box under the *Security* option.
- You do not need to enter the WebGuard port number if the WebGuard port number is set to 80 (443 when entering *https*) when running the WebGuard program by entering the IP address and port number.



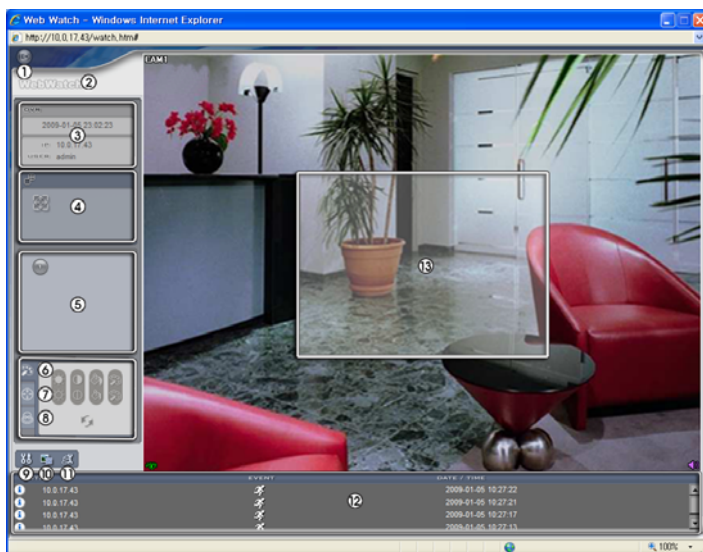
Enter your ID and PASSWORD and click the [LOGIN] button. Selecting Save ID saves the ID you entered.

### NOTES:

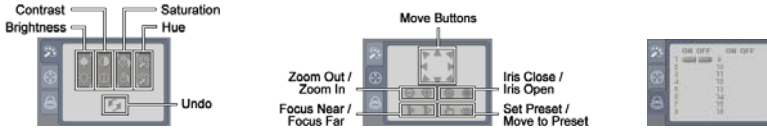
- WebGuard only works with Microsoft Internet Explorer and will NOT work with other web browsers.
- There might be a problem with the bottom of the WebGuard page being cropped caused by the address or status bars in Microsoft Internet Explorer 7.0. In this situation, it is recommended that websites open windows without address or status bars by changing Internet setting. (Go to *Tools*, and *Internet Options*, and then the *Security* tab → Click the *Custom level...* button → Select *Enable* for the *Allow websites to open windows without address or status bars* option.)
- When running WebGuard in the Microsoft® Windows® Vista operating system, it is recommended that you start Internet Explorer with elevated administrator permissions. Click the right mouse button on the Internet Explorer icon and select the *Run as administrator* option from the context menu. Otherwise, some functions of WebGuard might be limited.

**NOTES:**

- There might be a problem with screen display or screen update caused by low image transmission speed when using the Microsoft® Windows® Vista operating system. In this situation, it is recommended that you disable the Auto Tuning capability of your computer. Run the *Command Prompt* with elevated administrator permissions (Go to the *Start Menu*, and *Accessories*, and then *Command Prompt* → Click the right mouse button and select the *Run as administrator* option). Then enter "netsh int tcp set global autotuninglevel=disable" and press the enter key. Restart your computer to apply the changes. If you want to enable the Auto Tuning capability again, enter "netsh int tcp set global autotuninglevel=normal" after running the Command Prompt with elevated administrator permissions. Restart your computer to apply the changes.
- When running the updated WebGuard for the first time, Internet Explorer might occasionally load the information from the previous version. In this case, delete the temporary Internet files by selecting *Tools* → *Internet Options* → *General* tab, and then run WebGuard again.
- You will need to get the appropriate IP address for the transmitter you want to connect to and the WebGuard port number from your network administrator.



- ① **Log Out:** Click to log out of the WebGuard program.
- ② **Version:** Position the mouse pointer on the WebWatch logo to see the WebGuard program version.
- ③ **Information:** The Information window displays the login information of WebGuard.
- ④ **Full Display:** Clicking the button displays the video in full screen. Pressing the *Esc* button on a keyboard returns to the previous screen.
- ⑤ **Camera Button:** The button displays the camera number.
- ⑥ **Image Adjustment:** Click to adjust the brightness, contrast, saturation and hue of monitored image.
- ⑦ **PTZ Control:** Click to control pan, tilt and zoom of the camera remotely.
- ⑧ **Alarm-Out Control:** Click to control an alarm out device remotely.



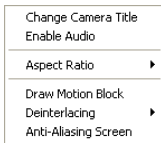
- ⑨ **Setup:** Click to set up the image drawing mode and OSD display. You can adjust the display speed by changing the image drawing mode, and select OSD information to be displayed on the screen.
- ⑩ **Save Image:** Click to save the current image as a bitmap or JPEG file format.
- ⑪ **Remote Setup:** Click to change the settings of the transmitter by using the Remote Setup screen.
- ⑫ **Event Status Window:** The event status window at the bottom displays a list of events that were detected in the transmitter.

Alarm In On  
 Motion Detection

Alarm In Off  
 Video Loss

Alarm In Bad  
 Video Blind

- ⑬ **Screen Popup Menu:** Clicking the right mouse button on the screen displays the screen popup menu.



- **Change Camera Title:** Select to change the camera title.
- **Enable Audio:** Select to enable audio communication with the site which the transmitter is installed and the audio control panel appears. Click the button to send audio to the site which the transmitter is installed and speak into the microphone. Click the button to monitor live audio from the site which the transmitter is installed through the attached speaker. Clicking both the and buttons allows two-way communication. Clicking the button disables audio communication.
- **Aspect Ratio:** Select to change the image aspect ratio displayed on the screen and the option menu appears. Selecting **Fit to Screen** displays images by fitting them to the screen size. Selecting **Original Ratio** displays images by fitting them to the screen size while maintaining their original ratio. Selecting **Half Size (x0.5)** to **Quadruple Size (x4)** displays the images at the selected image size.
- **Draw Motion Block:** Select to display the area that detects motions on the screen in red blocks.
- **Deinterlacing:** Select to enhance image display quality of interlaced video on the screen by eliminating horizontal scan lines or noise in areas with motion.
- **Anti-Aliasing Screen:** Select to enhance image display quality by eliminating stair stepping (aliasing) effects in the enlarged image.

#### NOTES:

- The image adjustment for the monitoring screen works only in the pause mode.
- *Aspect Ratio – Half Size (x0.5) to Aspect Ratio to Quadruple Size (x4)* in the Screen Popup Menu will be enabled when the selected camera screen can display images in those sizes.
- *Draw Motion Block* option in the Screen Popup menu is available only when a Motion Detection event is set up during the 3.6 *Event, Motion Detection* setup.

# Appendix

## LED Indicators

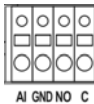
LED Status		Description
Power LED	Unlit	No power connected to the unit.
	Flicker	The unit is booting.
	Lit	The unit is operating.
Network LED	Lit	The unit is connected to a network.
Power LED & Network LED	Flicker sequentially	The unit is upgrading the software.
	Flicker simultaneously	The unit is recovering NAND flash memory.

## Troubleshooting

Problem	Possible Solution
No Power	<ul style="list-style-type: none"> <li>Check power cord connections.</li> <li>Confirm that there is power at the outlet.</li> </ul>
No Live Video	<ul style="list-style-type: none"> <li>Check camera video cable and connections.</li> <li>Confirm that the camera has power.</li> <li>Check camera lens settings.</li> <li>Check network connections on your PC and a transmitter.</li> </ul>
Live Video Very Bright	Check if a video termination resistance switch is set to ON (downward).
Connection to the INIT program is not available because of wrong ID and password.	If you lost the administrator ID and password, do a factory reset and customize all settings all over again. The factory reset returns all the settings including network settings to the original factory settings. Write down the password just in case.
The WebGuard program is not available.	If you cannot launch the login page of the WebGuard program, check Microsoft Internet Explorer's version. WebGuard might not run properly in versions earlier than 6.0.

## Connector Pin Outs

### I/O Connector



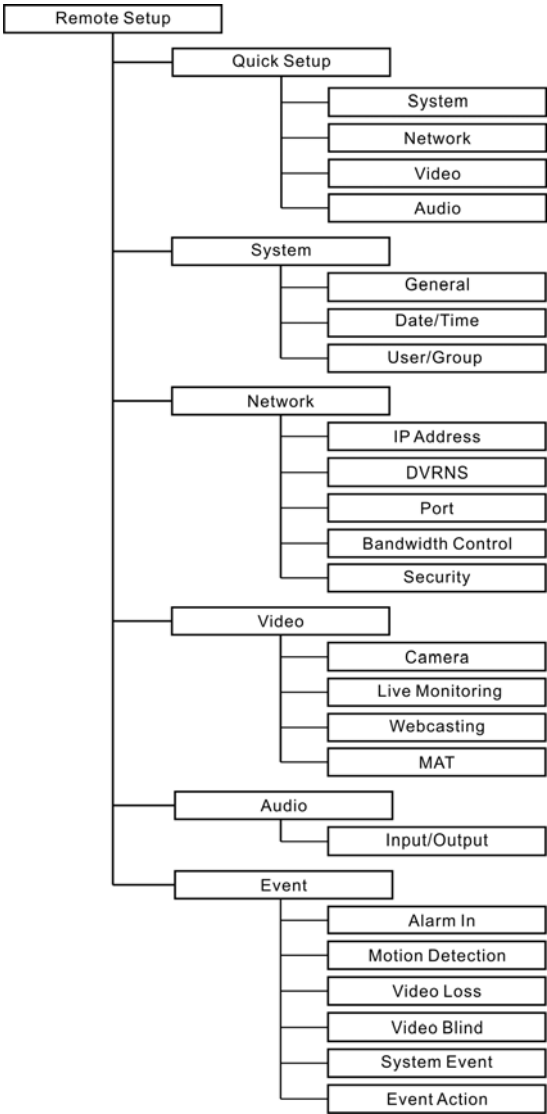
AI	Alarm Inputs
GND	GND (Chassis Ground)
NO	Alarm Out (Normally Open)
C	Common

RS485 Connector



Master Unit		Slave Unit	
+	→ To →	TX+/RX+	
-	→ To →	TX-/RX-	

Map of Screens (Remote Setup)



## Specifications

VIDEO	
Signal Format	NTSC or PAL (auto detect)
Input	Composite: 1 input, 1 Vp-p, switch-terminating, 75 Ohms
Input Resolution	Composite: 720x480 (NTSC), 720x576 (PAL)
Compression Algorithm	H.264, MPEG-4, M-JPEG (Four levels)
Compression Resolution	NTSC: 704x480, 704x240, 352x240 PAL: 704x576, 704x288, 352x288
Frame Rate (Live/Recording) (images per second)	NTSC: 30 ips/30 ips @ 4CIF (MPEG-4, M-JPEG) 15 ips/15 ips @ 4CIF or 30 ips/0 ips @ 4CIF (H.264) PAL: 25 ips/25 ips @ 4CIF (MPEG-4, M-JPEG) 12.5 ips/12.5 ips @ 4CIF or 25 ips/0 ips @ 4CIF (H.264)

INPUTS/OUTPUTS	
DC 12V Output	12 VDC, Max. 6W
Alarm Input	1 TTL, NC/NO programmable, 2.4V (NC) or 0.3V (NO) threshold, 3.3 VDC
Alarm Output	1 relay out, NO only, 0.3A @ 125 VAC, 1A @ 30 VDC
Network Connectivity	10/100 Mbps Ethernet
Audio Input	1 line in or Microphone
Audio Output	1 line out

CONNECTORS	
Video Input	BNC
Audio In/Out	Stereo
Alarm In/Out	Terminal block
Ethernet Port	RJ-45
RS-485 Serial Port	Terminal block
DC 12V Out	Terminal block
USB Port	1 on front panel (2.0)

GENERAL	
Dimensions (W x H x D)	4.7" x 1.1" x 4.3" (119mm x 29mm x 108mm)
Shipping Dimensions (W x H x D)	10.4" x 4.1" x 7.5" (265mm x 105mm x 190mm)
Unit Weight	0.64 lbs. (0.29Kg)
Shipping Weight	2.78 lbs. (1.26Kg)
Operating Temperature	32°F to 122°F (0°C to 50°C) (32°F to 104°F (0°C to 40°C) when installing by using a specialized rack mount kit*)
Operating Humidity	0% to 90%
Power Supply	12 VDC, 24 VAC, PoE (Power over Ethernet) (IEEE 802.3af, class0)
Power Consumption	Max. 13W
Approval	FCC, CE

\* The specialized rack mount kit is not supplied with the transmitter. Ask your dealer or distributor about purchasing the rack mount kit.

Specifications are subject to change without notice.