

4/16 CHANNEL NETWORK VIDEO ENCODER

User Manual

SPE-420
SPE-1630



4/16 Channel Network Video Encoder

User Manual

Copyright

©2022 [Hanwha Vision](#) Co., Ltd. All rights reserved.

Trademark

Each of trademarks herein is registered. The name of this product and other trademarks mentioned in this manual are the registered trademark of their respective company.

Restriction

Copyright of this document is reserved. Under no circumstances, this document shall be reproduced, distributed or changed, partially or wholly, without formal authorization.

Disclaimer

[Hanwha Vision](#) makes the best to verify the integrity and correctness of the contents in this document, but no formal guarantee shall be provided. Use of this document and the subsequent results shall be entirely on the user's own responsibility. [Hanwha Vision](#) reserves the right to change the contents of this document without prior notice.

❖ Design and specifications are subject to change without prior notice.

❖ The initial administrator ID is “admin” and the password should be set when logging in for the first time.

Please change your password every three months to safely protect personal information and to prevent the damage of the information theft.

Please, take note that it's a user's responsibility for the security and any other problems caused by mismanaging a password.

IMPORTANT SAFETY INSTRUCTIONS

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean the contaminated area on the product surface with a soft, dry cloth or a damp cloth.
(Do not use a detergent or cosmetic products that contain alcohol, solvents or surfactants or oil constituents as they may deform or cause damage to the product.)
7. Do not block any ventilation openings, Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/ accessories specified by the manufacturer.
12. Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/ apparatus combination to avoid injury from tip-over.
13. Unplug this apparatus during lighting storms or when unused for long periods of time.
14. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
15. This product is intended to be supplied by a Listed Power Supply Unit marked "Class 2" or "LPS" and rated 12 Vdc, 0.42 A or PoE, 0.11 A. (SPE-420)
16. This product is intended to be supplied by a Listed Power Supply Unit marked "Class 2" or "LPS" and rated 12 Vdc, 1.67 A. (SPE-1630)
17. If you use excessive force when installing the product, the encoder may be damaged and malfunction. If you forcibly install the product using non-compliant tools, the product may be damaged.
18. Do not install the product in a place where chemical substances or oil mist exists or may be generated. As edible oils such as soybean oil may damage or warp the product, do not install the product in the kitchen or near the kitchen table.
This may cause damage to the product.
19. When installing the product, be careful not to allow the surface of the product to be stained with chemical substance.
Some chemical solvents such as cleaner or adhesives may cause serious damage to the product's surface.
20. If you install/disassemble the product in a manner that has not been recommended, the production functions/ performance may not be guaranteed.
Install the product by referring to "Installation & connection" in the user manual.
21. Installing or using the product in water can cause serious damage to the product.



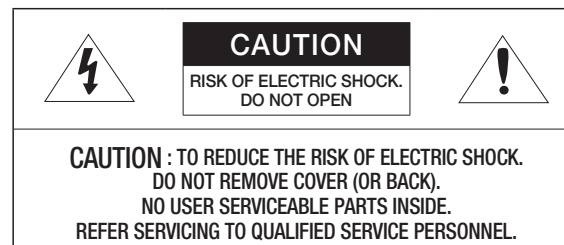
WARNING

TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. DO NOT INSERT ANY METALLIC OBJECT THROUGH THE VENTILATION GRILLS OR OTHER OPENINGS ON THE EQUIPMENT.

Apparatus shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the apparatus.

To prevent injury, this apparatus must be securely attached to the Wall/ceiling in accordance with the installation instructions.

CAUTION



EXPLANATION OF GRAPHICAL SYMBOLS



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



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

Class I construction

An apparatus with CLASS I construction shall be connected to a MAINS socket outlet with a protective earthing connection.

Battery

Batteries(battery pack or batteries installed) shall not be exposed to excessive heat such as sunshine, fire or the like.

Disconnection Device

Disconnect the main plug from the apparatus, if it's defected. And please call a repair man in your location.

When used outside of the U.S., it may be used HAR code with fittings of an approved agency is employed.

CAUTION

RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

ATTENTION

IL Y A RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UNE BATTERIE DE TYPE INCORRECT.
METTRE AU REBUT LES BATTERIES USAGÉES CONFORMÉMENT AUX INSTRUCTIONS.

These servicing instructions are for use by qualified service personnel only.

To reduce the risk of electric shock do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so.

The HDMI out terminal of the product is provided for easier installation, and is not recommended for monitoring purposes.

Please use the input power with just one encoder and other devices must not be connected.

The ITE is to be connected only to PoE networks without routing to the outside plant.

The wired LAN hub providing power over the Ethernet (PoE) in accordance with IEEE 802-3af shall be a UL Listed device with the output evaluated as a Limited Power Source as defined in UL60950-1 or PS2 as defined in UL62368-1.

Unit is intended for installation in a Network Environment 0 as defined in IEC TR 62102. As such, associated Ethernet wiring shall be limited to inside the building.

Please read the following recommended safety precautions carefully.

- Do not place this apparatus on an uneven surface.
- Do not install on a surface where it is exposed to direct sunlight, near heating equipment or heavy cold area.
- Do not place this apparatus near conductive material.
- Do not attempt to service this apparatus yourself.
- Do not place a glass of water on the product.
- Do not install near any magnetic sources.
- Do not block any ventilation openings.
- Do not place heavy items on the product.
- Please wear protective gloves when installing/removing the encoder.
The high temperature of the product surface may cause a burn.

User's Manual is a guidance book for how to use the products.

The meaning of the symbols are shown below.

- Reference : In case of providing information for helping of product's usages
 - Notice : If there's any possibility to occur any damages for the goods and human caused by not following the instruction
- ※ Please read this manual for the safety before using of goods and keep it in the safe place.

BEFORE START

This manual provides operational information necessary for using the product and contains a description about each component part and its function as well as menu or network settings.

You have to keep in mind the following notices :

- **Hanwha Vision** retains the copyright on this manual.
- This manual cannot be copied without **Hanwha Vision**'s prior written approval.
- We are not liable for any or all losses to the product incurred by your use of non-standard product or violation of instructions mentioned in this manual.
- Prior to opening the case, please consult a qualified technician first. Whenever this is needed power must be removed from the unit.

Warning

Battery

It is essential that when changing the battery in the unit, the replacement battery must be of the same type otherwise there may be a possibility of an explosion.

The following are the specifications of the battery you are using now.

- Normal voltage : 3V
- Normal capacity : 220mAh
- Discharge Current : 0.2mA
- Operating temperature : -20°C ~ 60°C (-4°F ~ 140°F)

Operating Temperature

The guaranteed operating temperature range of this product is

SPE-1630 : -10°C ~ 50°C (14°F ~ 122°F) (-10°C ~ 40°C (14°F ~ 104°F), When installing Rack)

SPE-420 : 0°C ~ 50°C (32°F ~ 122°F).

This product may not work properly if you run right after a long period of storage at a temperature below the guaranteed one.

Prior to using a device that has been stored for a long period in low temperatures, allow the product to stand at room temperature for a period.

Security Precautions

The default administrator ID is "admin", and the password must be set when the user log in at the first time.

To prevent from your personal information being exposed, please change your password every 3 months.

Note that the security and other related issues caused by careless management of password shall be in the charge of the user.

CONTENTS

OVERVIEW

3

- 3 Important Safety Instructions
- 5 Before Start
- 7 Product Features
- 7 Recommended PC Specifications
- 8 Package Contents
- 9 Part Names and Functions (Front)
- 10 Part Names and Functions (Rear)

WEB VIEWER

21

- 21 Connecting to the encoder
- 22 Password setting
- 22 Login
- 22 Using the Live Screen

INSTALLATION & CONNECTION

11

- 11 Checking the installation environment
- 11 Rack Installation
- 12 Connecting with other Device

SETUP SCREEN

25

- 25 Setup
- 25 Basic Setup
- 29 PTZ setup
- 30 Video & Audio setup
- 31 Network Setup
- 35 Event Setup
- 38 Configure analysis settings
- 39 System Setup

NETWORK CONNECTION AND
SETUP

16

- 16 Connecting the product Directly to Local Area Networking
- 16 Connecting the encoder Directly to a DHCP Based DSL/Cable Modem
- 17 Using Device Manager
- 17 Automatically searching product
- 17 Configuring IP address
- 18 Manually registering product
- 18 Automatically configuring IP
- 19 Port Range Forward (Port Mapping) Setup
- 20 Connecting to the encoder from a Shared Local PC
- 20 Connecting to the encoder from a Remote PC via the Internet

APPENDIX

41

- 41 Device Type setup guide
- 41 Troubleshooting

PRODUCT FEATURES

This product can output videos of different resolutions and quality levels to different codecs at the same time, and provides an environment that can be monitored from a remote PC through a network.

- Provides a convenient viewer
- Video input terminals for 4/16 channels
- Supports various resolutions via the network

SPE-420

- NTSC : 2560x1440, 1920x1080, 1280x720, 928x480, 704x480, 928x240, 704x240, 640x368, 352x240
- PAL : 2560x1440, 1920x1080, 1280x720, 928x576, 704x576, 928x288, 704x288, 640x368, 352x288

SPE-1630

- NTSC : 2560x1920, 2560x1440, 1920x1080, 1280x720, 928x480, 704x480, 928x240, 704x240, 640x368, 352x240
- PAL : 2560x1920, 2560x1440, 1920x1080, 1280x720, 928x576, 704x576, 928x288, 704x288, 640x368, 352x288

- Alarm Interface
- Remote Monitoring function by Network Viewer, Smart Viewer and Mobile Viewer
- Supports coaxial and RS-485 protocols
- Tampering Detection
- ONVIF Compliance



RECOMMENDED PC SPECIFICATIONS

- CPU : Intel(R) Core(TM) i7 3.4 GHz or higher
- RAM : 8G or higher
- Supported OS : Windows, Mac OS X
- Supported web browsers : Google Chrome, MS Edge, MS IE, Firefox (Windows 64bit only), Apple Safari (Mac OS X only)

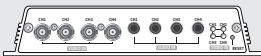
※ Please see the appendix for detailed information on verified OS and browsers
Some functions may be restricted even in supported browsers.

PACKAGE CONTENTS

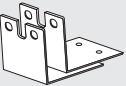
Please unwrap the product, and place the product on a flat place or in the place to be installed.
Please check the following contents are included in addition to the main unit.

- 
- The appearance of the components may differ from the image shown.
 - Accessory category and quantity may differ depending on sales region.

SPE-420

		
Network Video Encoder	Power Terminal Block	User Manual or Quick Manual
		
Tapping Screw	Terminal Block (15 pin)	

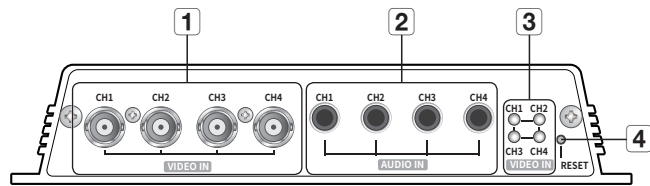
SPE-1630

		
Network Video Encoder	Power Adapter	Power Cord
		
User Manual or Quick Manual	Bracket Fixing Screw	Bracket Rack
		
Rubber foot pads		

- If the product is being installed somewhere besides the rack, assemble the provided rubber foot pads on the product.

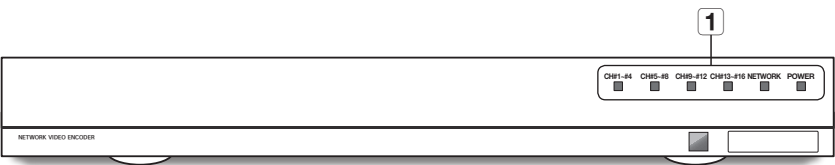
PART NAMES AND FUNCTIONS (FRONT)

SPE-420



Part Names	Functions
1 Video input	This is the video signal input terminal (BNC type).
2 Audio input	This is the audio signal input terminal (RCA jack) and the optional audio extension cable jack.
3 Video input status indicator	Displays the operation status of each video input channel.
4 Reset Button	This button is used to reset the encoder settings to their factory defaults. Press and hold for about 5 seconds to reboot. I If you reset the product, the network settings will be adjusted so that DHCP can be enabled. If there is no DHCP server in the network, you must run the Device Manager program to change the basic network settings such as IP address, Subnet mask, Gateway, etc., before you can connect to the network.

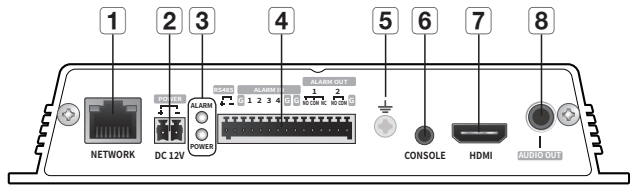
SPE-1630



Part Names	Functions
1 LED lamp	CH#1~#4 : Video input channels. The light turns off only when all four video signals are not connected.
	CH#5~#8 : Video input channels. The light turns off only when all four video signals are not connected.
	CH#9~#12 : Video input channels. The light turns off only when all four video signals are not connected.
	CH#13~#16 : Video input channels. The light turns off only when all four video signals are not connected.
	NETWORK : Displays the network connection status and the data transmission status.
	POWER : Displays the power ON/OFF status.

PART NAMES AND FUNCTIONS (REAR)

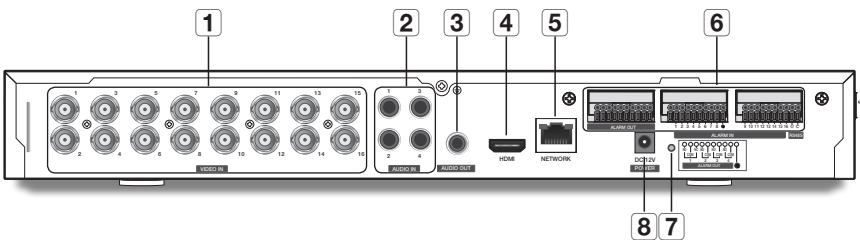
SPE-420



Part Names	Functions
1 Network connection	This is a terminal that connects to the network through PoE or Ethernet cable.
2 DC 12V	This is a network video encoder power connection terminal.
3 LED lamp	ALARM : Lights up when an event occurs.
	POWER : Displays the power ON/OFF status.
4 I/O terminal * NVR compatibility is under preparation.	RS485: Used for RS-485 communication.
	ALARM IN: Alarm input terminal. (1 - 4 channels)
	ALARM OUT: Alarm output terminal. (1 - 2 channels)
5 Ground connection	A terminal to connect a separate ground cable. ■ Make sure to add a ground cable in order to use the equipment safely.
6 CONSOLE	This is the console connection terminal.
7 HDMI video output	This is the terminal that is used to check the test video. You can check the test video by connecting to the portable display using the HDMI cable. ■ You can view the video in 4 split screens. Only FHD video is supported.
8 Audio output	This is the video signal output terminal (RCA jack).

■ [CONSOLE] is designed for the service repair purpose only.

SPE-1630



Part Names	Functions
1 Video input	This is the video signal input terminal (BNC type).
2 Audio input	This is the audio signal input terminal (RCA jack) and the optional audio extension cable jack.
3 Audio output	This is the video signal output terminal (RCA jack).
4 HDMI video output	This is the terminal that is used to check the test video. You can check the test video by connecting to the portable display using the HDMI cable. ■ You can view the video in 16 split screens. Only FHD video is supported.
5 Network connection	This is the network connection terminal.
6 I/O terminal * NVR compatibility is under preparation.	RS485: Used for RS-485 communication.
	ALARM IN: Alarm input terminal. (1 - 16 channels) ALARM OUT: Alarm output terminal. (1 - 4 channels)
7 Reset Button	This button is used to reset the encoder settings to their factory defaults. Press and hold for about 5 seconds to reboot. ■ If you reset the product, the network settings will be adjusted so that DHCP can be enabled. If there is no DHCP server in the network, you must run the Device Manager program to change the basic network settings such as IP address, Subnet mask, Gateway, etc., before you can connect to the network.
8 Power input	This is the power input terminal.

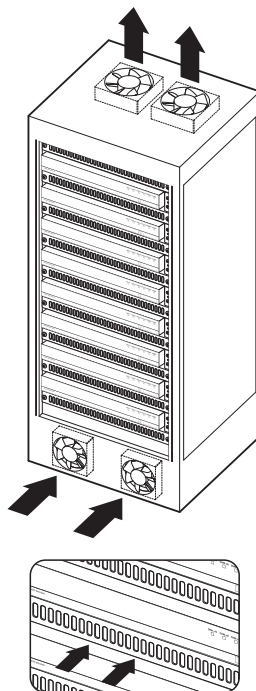
Please take note of the followings before using this product.

- Do not use the product outdoor.
- Do not spill water or liquid in the connection part of the product.
- Do not impose the system to excessive shock or force.
- Do not pull out the power plug forcefully.
- Do not disassemble the product on your own.
- Do not exceed the rated input/output range.
- Use a certified power cord only.
- For the product with an input ground, use a grounded power plug.

CHECKING THE INSTALLATION ENVIRONMENT

When mounting the SPE-1630 on a rack, comply with the following instructions.

1. Please ensure that the rack inside is not sealed.
2. Please ensure the air is circulated through the inlet/outlet as shown in the picture.
3. If you pile up the products or other rack-mount devices as shown in figure 1, secure room for ventilation or install a vent.
4. For natural air convection, place the inlet at the bottom of the rack and the outlet on top.
5. It is strongly recommended that a fan motor is installed at the inlet and the outlet for air circulation. (Please fit a filter at the inlet to screen dust or foreign substances.)
6. Please maintain the temperature inside the rack or surrounding areas between $-10^{\circ}\text{C} \sim 40^{\circ}\text{C}$ ($14^{\circ}\text{F} \sim 104^{\circ}\text{F}$) as shown in the figure.

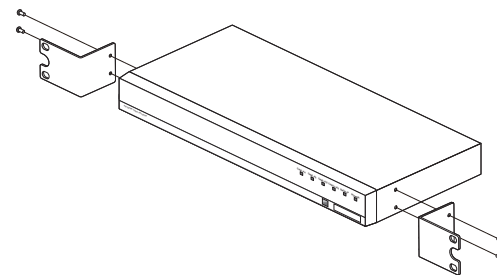


[Figure 1]

RACK INSTALLATION

Install the Bracket-Rack as shown in the figure, and then fasten the screws on both sides (2 screws on each side).

- Fix the screws not to be loosened by vibrations.

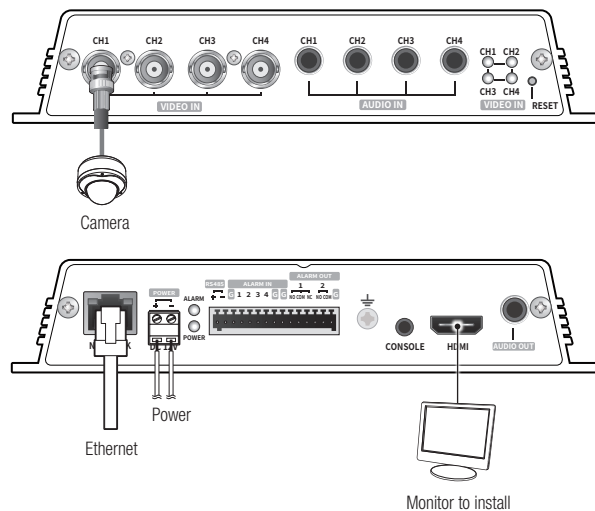


CONNECTING WITH OTHER DEVICE

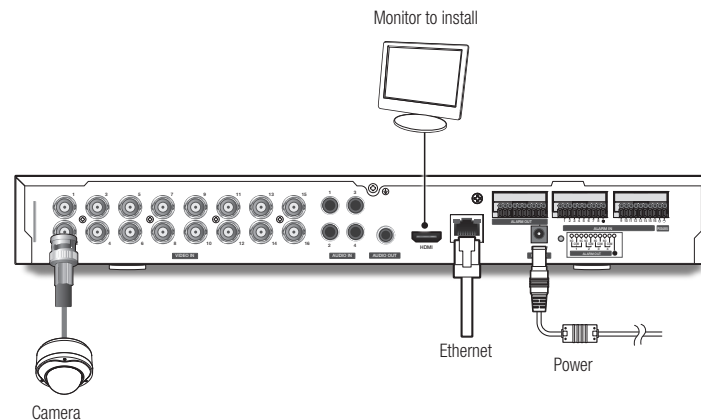
Connecting the camera

Connect the [VIDEO IN] port of the network video encoder to the video output port of the camera.

SPE-420



SPE-1630



! The HDMI out terminal of the product is provided for easier installation, and is not recommended for monitoring purposes.

Ethernet Connection

Connect the Ethernet cable to the local network or to the Internet.

Power Supply

Use the screwdriver to connect each line (+, -) of the power cable to the corresponding power port of the encoder.

- 
- If the power sources for PoE and DC 12 V are simultaneously turned on, the device power will be supplied by both of PoE and DC 12 V. (SPE-420)
 - You can also use a router featuring PoE to supply power to the encoder.
 - Use PoE that is compliant with the IEEE802.3af protocols.
 - It is recommended to use a single source for powering the equipment among PoE and DC 12V.
 - Be careful not to reverse the polarity when you connect the power cable.
 - If you want to connect an external device, you must turn off the external device before proceeding.
 - Connect the set and the adapter power line first, and then connect the power cable to the outlet on the wall.

Power Cable Specification for Each Model

When the input is DC 12V :

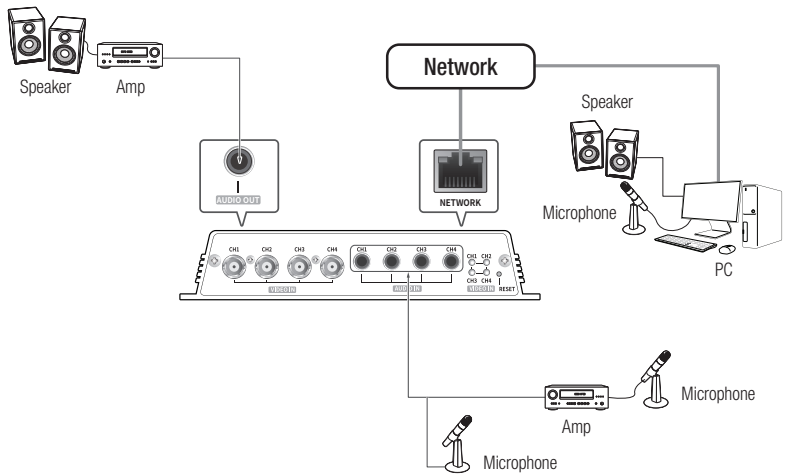
Wire Type (AWG)	#22	#20
Cable Length (Max.)	19m	30m

Network Cable Specification

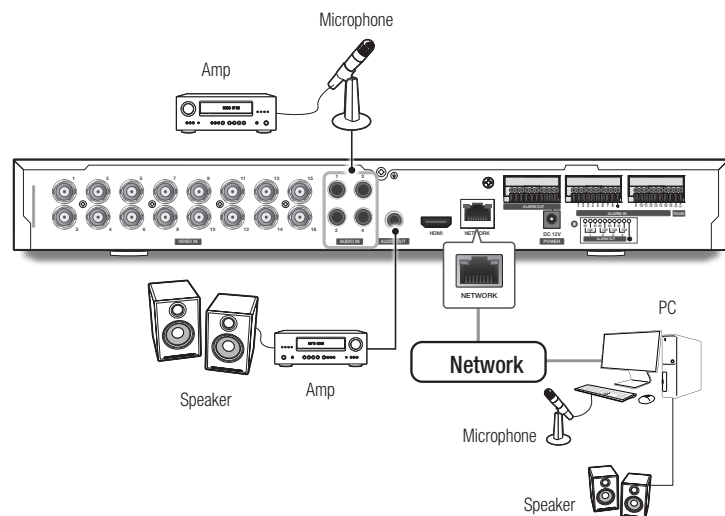
Item	Contents	Remark
Connector	RJ45 (10/100/1000BASE-T)	
Ethernet	10/100/1000Base-T	
Cable	Category 6	
Max Distance	100M	DC Resistance ≤ 0.125Ω/m
PoE Support	IEEE 802.3af	SPE-420

Connecting to Audio Input/Output

SPE-420



SPE-1630



1. Connect the AUDIO IN port of the encoder with the microphone or LINE OUT port of the amplifier that the microphone is connected to.
2. Connect the AUDIO OUT port of the encoder with the speaker or LINE IN port of the amplifier that the speaker is connected to.
3. Check the specifications for audio input.

■ Audio input is possible on CH1 to CH4, while audio output is only possible on CH1.

• Audio Codec

- Audio In : G.711 PCM (Bit Rate: 64kbps / Sampling Frequency: 8kHz)
- Audio Out : G.711 PCM (Bit Rate: 64kbps / Sampling Frequency: 8kHz)

• Full duplex Audio

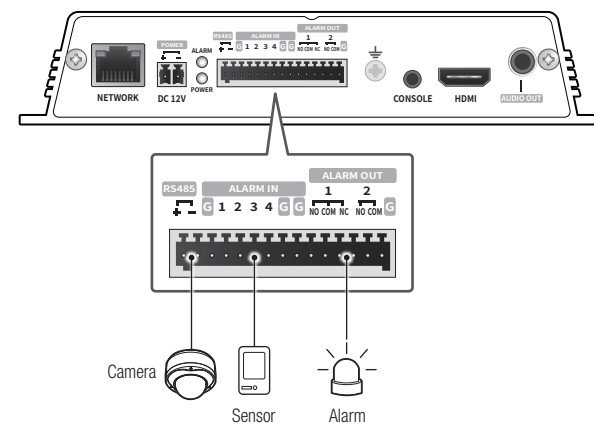
- **Audio in** : Mono signal line input (Max.1.0Vpp)
- **Audio out** : Mono signal line output (Max.1.0Vpp)
- **Line out impedance** : 600Ω

Connecting to the I/O port box

Connect the Alarm I/O signal to the corresponding port of the rear port box.

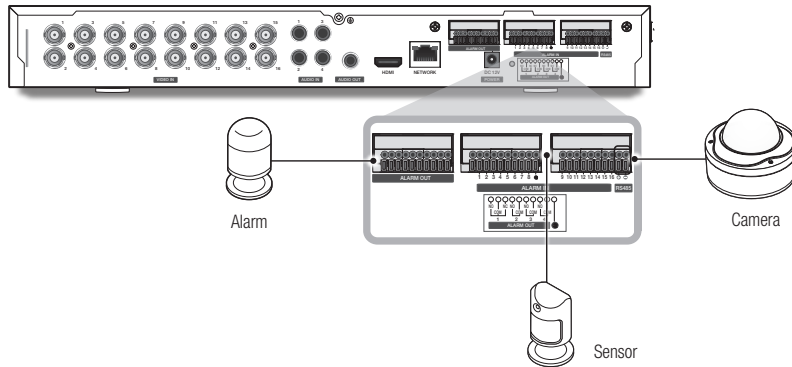
■ We are preparing to provide the alarm input and output functions by connecting the encoder to the NVR. (You can check it on the homepage.)

SPE-420



The alarm input and output ports are configured as shown below.

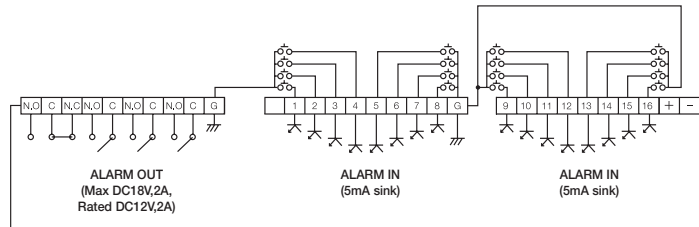
- G : Terminal for alarm ground
- ALARM OUT 1 : NO(Normal Open), COM(Common), NC(Normal Closed)
- ALARM OUT 2 : NO(Normal Open), COM(Common)
- ALARM IN 1 - 4 : Alarm input terminals



The alarm input and output ports are configured as shown below.

- G : Terminal for alarm ground
- ALARM OUT 1 : NO(Normal Open), COM(Common), NC(Normal Closed)
- ALARM OUT 2 ~ 4 : NO(Normal Open), COM(Common)
- ALARM IN 1 ~ 16 : Alarm input terminals

! ■ Do not connect the Ground signal of the encoder to the power of Alarm (DC-).



Connecting to the Alarm Input

Connect one signal cable (out of 2) of applicable sensor to the [ALARM IN] port, and the other to the [G] port.

Connecting the Alarm Output

Connect one signal cable (out of 2) of applicable external device to the [ALARM OUT], and the other to the [COM] port.

! ■ You must use the specific RS-485 alarm I/O ports for each channel.

Connecting to the RS-485 device

Connect the external device to the [RS-485 +, -] ports. You can connect and control PTZ camera that supports RS-485 communication.

- ! ■ You can connect and control the PTZ camera which supports the RS-485 communication.
- You can control these by connecting the AUX function that supports RS-485 communication.
- Check if the RS-485 device is compatible with the product first.
- Pay attention not to change the polarity (+/-) of the RS-485 device when connecting it.
- For further information, refer to the respective Camera's documentation.

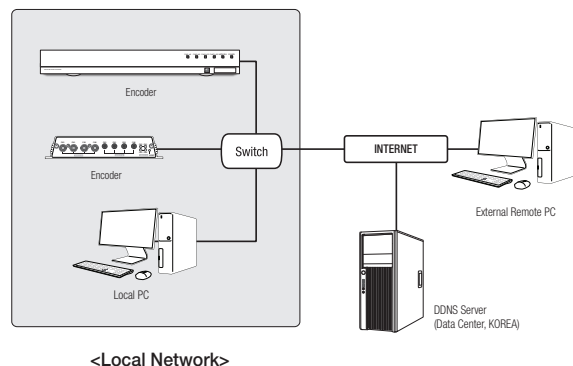
network connection and setup

You can set up the network settings according to your network configurations.

CONNECTING THE PRODUCT DIRECTLY TO LOCAL AREA NETWORKING

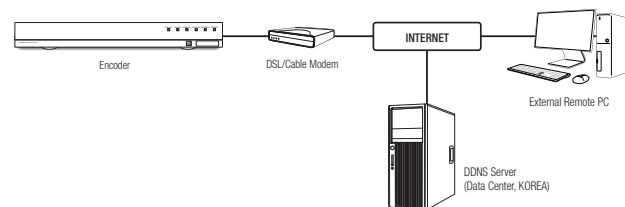
Connecting to the product from a local PC in the LAN

1. Launch an Internet browser on the local PC.
2. Enter the IP address of the encoder in the address bar of the browser.



- A remote PC in an external Internet out of the LAN network may not be able to connect to the encoder installed in the intranet if the port-forwarding is not properly set or a firewall is set. In this case, to resolve the problem, contact your network administrator.
- By factory default, the IP address will be assigned from the DHCP server automatically. If there is no DHCP server available, the IP address will be set to 192.168.1.100. To change the IP address, use the Device Manager. For further details on Device Manager use, refer to "Using Device Manager". (page 17)

CONNECTING THE ENCODER DIRECTLY TO A DHCP BASED DSL/CABLE MODEM



1. Connect the user PC directly with the network encoder.
 2. Run the Device Manager and change the IP address of the encoder so that you can use the web browser on your desktop to connect to the Internet.
 3. Use the Internet browser to connect to the web viewer.
 4. Move to [Setup] page.
 5. Move to [Network] – [DDNS] and configure the DDNS settings.
 6. Move to [Basic] – [IP & Port], and set the IP type to [DHCP].
 7. Connect the encoder, which was removed from your PC, directly to the modem.
 8. Restart the encoder.
- For configuring the DDNS settings, refer to "DDNS". (page 31)
 - For registering the DDNS settings, refer to "Registering with DDNS". (page 31)
 - Refer to "IP & Port" for how to setup IP. (page 28)

USING DEVICE MANAGER



- Device manager program can be downloaded from <Support>-<Online Tool> menu at [Hanwha Vision](https://www.HanwhaVision.com) website (<https://www.HanwhaVision.com>).
- More instructions of Device Manager can be found at <Help> menu of the main page.

AUTOMATICALLY SEARCHING PRODUCT

If a product is connected to the same network of the PC where device manager is installed, you can find network product by using search function.

1. Click <Search> at the main page of device manager.
2. Check the product from the list.
 - Check MAC address at the sticker attached to the product.

CONFIGURING IP ADDRESS

If you want to change product network setting, <Login OK> sign must be displayed at <Status>. Click <Authentication> at the main page to log in.

Configuring Static IP

Manually insert and configure IP address & port information.

1. Click the product from the list that you want the change the IP setting.
2. Click <IP Assign> at the main page of device manager.
3. Select <Assign the following IP address>.
 - IP information of the product will be displayed as previously set.
4. Fill in IP & Port related categories.

If not using a Broadband Router

For setting <IP Address>, <Subnet Mask>, and <Gateway>, contact your network administrator.

- HTTP Port : Used to access the product using the Internet browser, defaulted to 80.
- RTSP Port : A port that controls real-time streaming. The initial value is 554.

If using a Broadband Router

- IP Address : Enter an address falling in the IP range provided by the Broadband Router.
ex) 192.168.1.2~254, 192.168.0.2~254, 192.168.XXX.2~254
- Subnet Mask : The <Subnet Mask> of the Broadband Router will be the <Subnet Mask> of the product.
- Gateway : The <Local IP Address> of the Broadband Router will be the <Gateway> of the product.



- The settings may differ depending on the connected Broadband Router model.
For more information, refer to the user manual of the applicable router.
- For more information about port forwarding of the broadband router, refer to "Port Range Forward (Port Mapping) Setup". (page 19)

If the Broadband Router has more than one product connected

Configure the IP related settings and the Port related settings distinctly with each other.

ex)

	Category	Product #1	Product #2
IP related settings	IP Address	192.168.1.100	192.168.1.101
	Subnet Mask	255.255.255.0	255.255.255.0
	Gateway	192.168.1.1	192.168.1.1
Port related settings	HTTP Port	8080	8081
	RTSP Port	554	555



- If the <HTTP Port> is set other than 80, you must provide the <Port> number in the address bar of the Internet browser before you can access the product.
ex) http://IP address : HTTP Port
http://192.168.1.100:8080

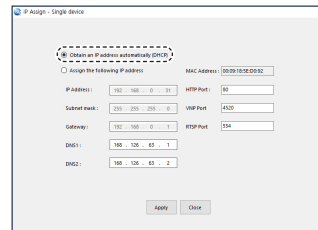
5. Click [Apply] Button.
6. If the success message is displayed, click [OK].

Configuring Dynamic IP

Receive IP address from DHCP

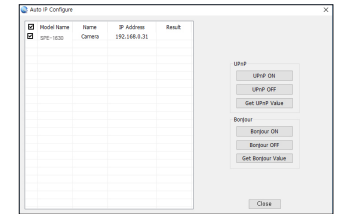
- Example of the Dynamic IP environment
 - If a Broadband Router, with products connected, is assigned an IP address by the DHCP server
 - If connecting the product directly to modem using the DHCP protocols
 - If IPs are assigned by the internal DHCP server via the LAN

1. Click the product from the list that you want to change the IP setting.
2. Click **<IP Assign>** at the main page of device manager.
3. Select **<Obtain an IP address automatically (DHCP)>**.
4. Click **[Apply]** button.
5. If the success message is displayed, click **[OK]**.



AUTOMATICALLY CONFIGURING IP

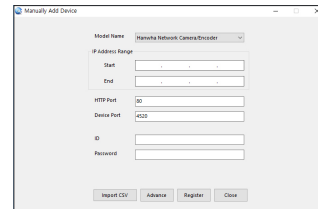
1. Click the product from the list that you want to automatically configure the IP.
2. Click **<+>** at the main page of device manager.
 - Equipment Setting menu appears.
3. At the menu, click **<Auto IP Configure>**.
4. Click **[Close]** button.



MANUALLY REGISTERING PRODUCT

If the product cannot be found using search function, the product can be registered remotely by manually inserting IP information, if the product is connected to external network.

1. Click **<Add Devices>** - **<Manually Add Device>** at the main page of device manager.
2. Insert the range of IP address that you search.
3. Select the **<Model Name>** of the product that you register, and insert HTTP port, ID, and password.
4. Click **[Register]** button.
5. Check if product is registered.
 - Check MAC address at the sticker attached to the product.

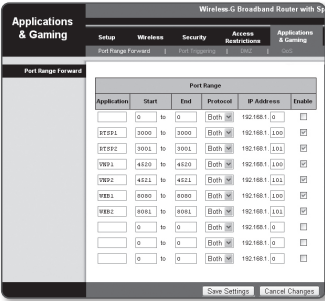


PORT RANGE FORWARD (PORT MAPPING) SETUP

If you have installed a Broadband Router with a product connected, you must set the port range forwarding on the Broadband Router so that a remote PC can access the product in it.

Manual Port Range Forwarding

1. From the Setup menu of the Broadband Router, select <Applications & Gaming> - <Port Range Forward>. For setting the port range forward for a third-party Broadband Router, refer to the user guide of that Broadband Router.
2. Select <TCP> and <UDP Port> for each connected product to the Broadband Router.
The number of each port to be configured to the IP router should be set according to the port number designated in <Setup> - <Basic> - <IP & Port> on the product web viewer.
3. When done, click [Save Settings].
Your settings will be saved.

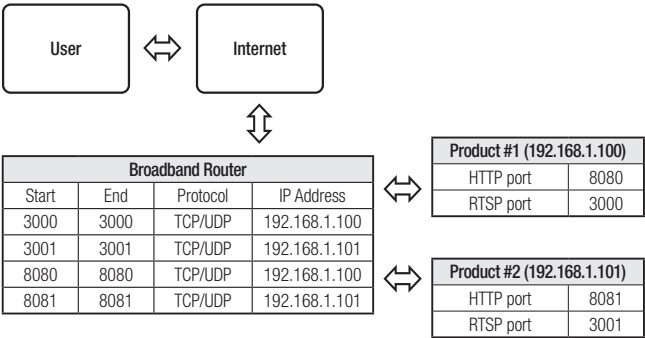


- Port forwarding setting is an example of setting CISCO IP router.
- The settings may differ depending on the connected Broadband Router model.
For more information, refer to the user manual of the applicable router.

Setting up Port Range Forward for several network products

- You can set a rule of Port Forwarding on the Broadband Router device through its configuration web page.
- A user can change each port using the product setting screen.

When Product#1 and Product#2 are connected to a router :



CONNECTING TO THE ENCODER FROM A SHARED LOCAL PC

1. Run device manager.
It will scan for connected encoders and display them as a list.
2. Double-click an encoder to access.
The Internet browser starts and connects to the encoder.



- Access to the encoder can also be gained by typing the encoder's IP address in the address bar of the Internet browser.

CONNECTING TO THE ENCODER FROM A REMOTE PC VIA THE INTERNET

Since using the Device manager on a remote computer that is not in the Broadband Router's network cluster is not allowed, users can access encoders within a Broadband Router's network by using the encoder's DDNS URL.

1. Before you can access an encoder in the Broadband Router network, you should have set the port range forward for the Broadband Router.
2. From the remote PC, launch the Internet browser and type the DDNS URL address of the encoder, or the IP address of the Broadband Router in the address bar.
ex) `http://ddns.hanwha-security.com/ID`

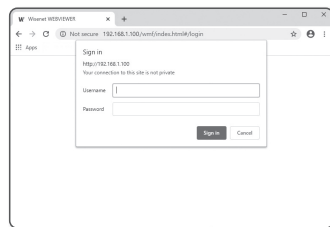


- For registering the DDNS settings, refer to **"Registering with DDNS"**. (page 31)

CONNECTING TO THE ENCODER

Normally, you would

1. Launch the Internet browser.
2. Type the IP address of the encoder in the address bar.
ex) • IP address (IPv4) : 192.168.1.100
→ http://192.168.1.100
- the Login dialog should appear.
• IP address (IPv6) : 2001:230:abcd:ffff:0000:0000:ffff:1111
→ http://[2001:230:abcd:ffff:0000:0000:ffff:1111]
- the Login dialog should appear.



If the HTTP port is other than 80

1. Launch the Internet browser.
2. Type the IP address and HTTP port number of the encoder in the address bar.
ex) IP address : 192.168.1.100:HTTP Port number(8080)
→ http://192.168.1.100:8080 - the Login dialog should appear.

Using URL

1. Launch the Internet browser.
2. Type the DDNS URL of the encoder in the address bar.
ex) URL address : http://ddns.hanwha-security.com/ID
- the Login dialog should appear.



■ Network connection is disabled in the LAN only environment.

Connecting via UPnP

1. Run the client or operating system in support of the UPnP protocol.
2. Click the encoder name for search.
In the Windows operating system, click the encoder name searched from the network menu.
- The login window is displayed.

Connecting via Bonjour

1. Run the client or operating system in support of the Bonjour protocol.
2. Click the encoder name for search.
In the Mac operating system, click the encoder name searched from the Bonjour tab of Safari.
- The login window is displayed.

To check the DDNS address

If the encoder is connected directly to the DHCP cable modem or DSL modem, the IP address of your network will be changed each time you try to connect to the ISP (Internet Service Provider) server. If this is the case, you will not be informed of the IP address changed by DDNS.

Once you register a dynamic IP-based device with the DDNS server, you can easily check the changed IP when you try to access the device.

To register your device to the <DDNS> server, visit <http://ddns.hanwha-security.com> and register your device first, and then set the Web Viewer's <Network> - <DDNS> to <Wisenet DDNS>, as well as providing <Product ID> that had been used for DDNS registration.

PASSWORD SETTING

When you access the product for the first time, you must register the login password.

- !

- For a new password with 8 to 9 digits, you must use at least 3 of the following: uppercase/lowercase letters, numbers and special characters. For a password with 10 to 15 digits, you must use at least 2 types of those mentioned.
 - Special characters that are allowed: ~!@#\$%^&*()_-=[]\|;:'<>.,/?
 - Space is not allowed for password.
 - For higher security, you are not recommended to repeat the same characters or consecutive keyboard inputs for your passwords.
 - If you lost your password, you can press the **[RESET]** button to initialize the product. So, don't lose your password by using a memo pad or memorizing it.
- Administrator password change

New password

Confirm new password

- If the password is 8 to 9 characters long, it must include at least 3 of the following character types: English uppercase letters, English lowercase letters, numbers, and special characters.
 - If the password is 10 characters or longer, it must include at least 2 of the following character types: English uppercase letters, English lowercase letters, numbers, and special characters.
 - It may not be used as password. The password and ID cannot be identical.
 - The following special characters can be used: ~!@#\$%^&*()_-=[]\|;:'<>.,/?
 - You may not use more than 4 consecutive characters. (example: 1234abcd, etc.)
 - You may not use the same character 4 or more times consecutively. (example: 1111, aaaa, etc.)

Apply

LOGIN

Whenever you access the encoder, the login window appears. Enter the User ID and password to access the encoder.

1. Enter "admin" in the <User name> input box.
The administrator's ID, "admin," can be changed in the Web Viewer.

2. Enter the password in the <Password> input field.

3. Click **[Sign in]**.
If you have logged in successfully, you will the Live Viewer screen.
- Sign in

http://192.168.1.100

Your connection to this site is not private

Username

Password

Sign in

Cancel
- !

- When you access the encoder web viewer, pay special attention to the security by checking whether the image data is encrypted.
- 🔒

- You will experience the best video quality if the screen size is 100%. Reducing the ratio may cut the image on the borders.

USING THE LIVE SCREEN



Item	Description
1 Live	Moves to the Live screen.
2 Setup	Move to the Setup screen.
3 Viewer Screen	Displays the Live video on the screen. You can use the mouse wheel to activate the digital zooming in Viewer screen.
4 Online help	The Online help provides detailed descriptions for each function.
5 Channel change	Sets the camera channel to be displayed on the live screen. (Single screen / 4-split screen)

Item	Description	
6 PTZ	PTZ	Controls the PAN/TILT/ZOOM motion.
	Manual focus ()	Adjusts the focus of the screen to near distance or far distance.
	Zoom In ()	Drag the bar on the right side of the UI up, or click the [] button to zoom in the screen. The farther the bar position is from the center, the faster the screen will be zoomed in.
	Zoom Out ()	Drag the bar on the right side of the UI down or click the [] button to zoom out the screen. The farther the bar position is from the center, the faster the screen will be zoomed out.
	Move screen ()	Moves in the direction where the cursor is located.
	OSD menu	You can control the functions of the connected camera.
7 Capture	Saves the current image as an image file.	
8 Alarm output	Activate the Alarm Out port.	
9 Audio control	Activates audio and adjusts the volume.	
10 Microphone control	Activates the microphone.	
11 Profile access information	You can read the profile information.	
12 Profile type	You can select a profile type in <Video profile> under the <Basic> setup menu. - Click the icon to display the name of the current profile. - Afterimages can be displayed on the screen under the following conditions if the video is played in the monitoring page: - The resolution is changed due to a profile change. - Incoming data is being slowed due to a network delay when the profile is changed. - The web browser window size and location is changed.	
13 Pixel Counter	Checks the number of pixels in the selected area on the video screen.	

Item	Description	
14 Switch View Mode	Full Screen ()	Double click on the video screen, and the current video will be played in the full screen of the monitor.
	Fit to screen ()	A view mode in which the size of the camera video automatically fits to the web browser size.
	Size of the original file ()	View mode in which the video is played in the actual resolution.
	Maintain Aspect Ratio ()	View mode that adjusts the aspect ratio to best fit the resolution.



- Some functions may not work on a specific browser or codec.

To change channels

- Select the desired channel number.
 - Click the [, ,] icons to select a channel for SPE-1630 models.
- The viewer screen shows the corresponding channel.
- To view the 4-split screen, click the [] icon.
- To return to single screen, click the [] icon.

To capture the snapshot

- Click [Capture ()] on the scene to capture.
- When a captured video is saved, a notification message appears.
The captured image is saved in the designated folder for each browser.



- If the screen is not captured by IE browser in Windows 7 or higher, run the IE Browser with the Admin privilege.

To fit the full screen

- Click the [Full Screen ()] icon.
- This will fit the Viewer to the full screen.
- To leave full screen mode, click the [Full Screen ()] button again or press the [Esc] key on the keyboard.

To Use Audio

1. Click [Audio ()] icon to activate audio communication.
2. Use [Audio control] bar to control the volume.



- If there is no sound from pulling in and out the audio jack while it is in operation, click the [Audio ()] icon to enable it again.
- To use audio, you need to set <Audio in> in "Video Profile" to <Enable> (page 25).



To Use Microphone

Click [Mic ()] icon to activate the microphone.

To count the number of pixels

1. Click the [Pixel count ()] icon to activate it.
2. Drag the mouse on the video to select an area.
3. The number of pixels in the selected area is displayed on the screen.

To control PTZ

1. Click the [PTZ ()] icon.
2. Move the jog dial [] on the Move Screen pad to move the camera direction, or zoom in or out by moving the bar on the right side of the UI up or down.
3. Select [ ] of the screen focus to adjust the focus.

To apply the preset

- Preset : Applies the saved preset.
Refer to "External PTZ" for detailed preset settings. (page 29)
 - Move : Applies the saved preset.
 - Setup : Specifies the preset.

To check the profile status

You can check the profile information.

1. Click the [Status ()] icon.
2. The profile access information screen is updated whenever the screen is enabled.
 - Profile access : Show the information of the newly added profile.
 - Profile : Show the information of the newly added codec.
 - Bitrate(kbps) : Show both the actual bit rate and the set bit rate.
 - Framerate(fps) : Show both the actual frame rate and the set frame rate.
 - Concurrent users count : Show the number of concurrent users who access the profile.
 - Current users : Shows information on users accessing web viewer and displaying monitoring video.
 - Profile : Show the name of the profile accessed by the user.
 - Bitrate(kbps) : Show the current bit rate.
 - Network connection status : It shows whether the network is working fine.
 - IP address : Show the IP address of the current user.

SETUP

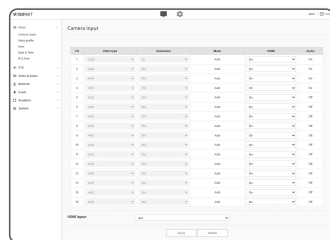
You can configure the basic encoder information, PTZ, video and audio, network, event, analyze and system settings.

1. On the live screen, click the [Setup (⚙)] button.
2. The Setup screen appears.

BASIC SETUP

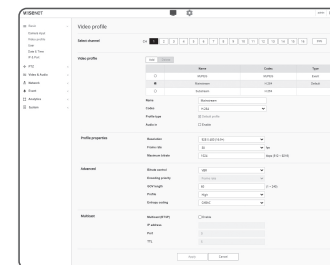
Camera input

1. From the Setup menu, select the <Basic (🏠)> tab.
2. Click <Camera input>.
 - Video type : CVBS/AHD/CVI/TVI
 - Resolution : SD/1M/2M/4M/5M
 - Mode : Auto
 - HDMI : On/Off
 - The layout outputs in a 4x4 layout, and you can select on/off for each channel.
 - Audio: Only channels 1 - 4 are available.
 - HDMI layout: 4x4/3x3/2x2/1x1



Video profile

1. From the Setup menu, select the <Basic (🏠)> tab.
2. Click <Video profile>.
3. Select the channel to set.
4. Set each item in the video profile.
Even if the setting of the profile currently accessed is changed, the previous setting will be used for output.
5. Select each profile properties.
For more details, refer to "To Add/Change the Video Profile". (page 26)
6. Select a type of profile.
 - The context menu may differ depending on the selected codec type.
7. Select whether or not to input audio in the video.
Select the <Audio In> check box and you can input audio in the video.
8. When done, click [Apply].



To Add/Change the Video Profile

The profile setup can be added or modified to accommodate various profiles depending on the recording conditions.

1. In <Video profile>, click the <Add> button.
2. Provide the name and select a codec.
3. Specify the conditions under which the codec will be applied.
4. Specify the details of the selected codec including resolution and frame rate.
 - Resolution : Set the video size of the H.264 and MJPEG files.
 - Framerate : Set the max number of video frames per sec.
 - Maximum bitrate : Set the max bit rate of video when the bit rate control is set to VBR.

 ■ As the bit rate can be adjusted limitedly according to the resolution, frame rate and screen complexity, the actual bit rate can be greater than the maximum bit rate. So you must consider the use conditions when setting the value.

 - Target bitrate : Set the target bit rate when the bit rate control is set to CBR.
 - Bitrate control : You can select one from constant bit rate and variable bit rate for compression. Fixed bitrate means that the network transmission bitrate is fixed while varying the video quality or frame rate, variable bitrate means that a higher priority is placed on the video quality while varying the bitrate.

 ■ After setting the fixed bit rate for bit control, if you select the video quality priority mode, depending on the complexity of the screen, the actual transmitted frame rate may differ from the frame rate setup in order to guarantee the optimal video quality for the given bit rate.

 - Encoding priority : You can set the priority of video transmission to frame rate or compression.
 - GOV length : It specifies the distance (in terms of number of frames) between two consecutive I-Frames in a video sequence when H.264 codec was selected. (One I-Frame + 0~Several P-Frames)
 - Profile : You can select the profile of H.264 codec.
 - Entropy coding : This is variable length coding using syntax statistics. It uses lossless compression techniques. You can set the entropy coding method. The compression rate of CABAC is better than CAVLC.

- Multicast(RTSP) : Specify the use of the RTSP protocol.
 - IP address : Enter an IPv4 address with which you can connect to the IPv4 network.
 - Port : Specify the video communication port.
 - TTL : You can set the TTL for the RTP packet.



- If you set the Multicast address to 224.0.0.0~224.0.0.255, multicast may not work properly in all environments. In that case, we recommend you change the multicast address.

What is GOV length?

GOV(Group of Video object planes) is a set of video frames for H.264 compression, indicating a collection of frames from the initial I-Frame to the next I-Frame. GOV consists of 2 kinds of frames: I-Frame and P-Frame. I-Frame is the basis frame of compression, and contains data for a completed single image. P-Frame contains only the data that has changed from the preceding I-Frame.

For H.264 codec, you can determine the GOV length.

If you set a recording profile with H.264 codec, the GOV length will be framerate/2.

User

1. From the Setup menu, select the **<Basic (Basic icon)>** tab.

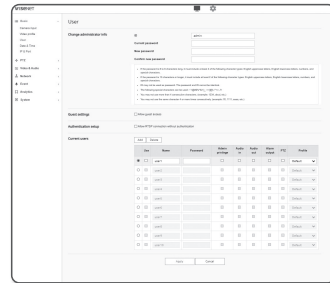
2. Click **<User>**.

3. Provide the necessary user information.

- Administrator password change : Change the password for the administrator.



- For the security purposes, you are recommended to use a combination of numbers, alphabets uppercase and lowercase and special characters for your password.
- It is recommended to change your password once every three months.
- The password length and limits are shown as follows.
 - A combination of at least three types of upper case, lower case, numeric, and special characters: 8 to 9 characters.
 - A combination of at least two types of upper case, lower case, numeric, and special characters: 10 to 15 characters.
 - Should be different from the ID.
 - Don't use 4 or more characters consecutive together. (examples : 1234, abcd)
 - Don't use 4 or more characters repeated. (examples : !!!!, 1111, aaaa)
 - Special characters that are allowed. : ~!@#%&^*()_+=[\|;:'<>.,?/
 - After the factory setting, the admin and user passwords are initialized. You need to reset the password.
 - When you access the encoder web page for the first time or access it after the initialization, you will be moved to the admin password setting menu.
 - In this menu, you need to login again with the new password before using the encoder web page menus.
 - If the existing password is not matched, when you change the admin password, you cannot change the password.
 - After changing your password, if there is an encoder connected to a CMS or NVR client, then you need to re-register it with the newly changed password. If the encoder is still connected with the same password, then the account may be locked because a client uses the previous password.
- If you try to login with the registered account, 5 or more consecutive password authentication has failed, and then the account may be locked for thirty seconds.
- When the password is changed while multiple connections are active from a PC, the browser may malfunction. In that case, reconnect to the server.



- Guest setup : If you select **<Enable guest access>**, the guest account can access the Web viewer screen but can only view the live Viewer screen.
 - The ID/password for the guest account is **<guest/guest>**, which cannot be changed.
- Authentication setup : If you select **<Enable RTSP connection without authentication>**, you can access RTSP without logging in and view the video.
- Current users : If you select **<Use>**, you can set or change the user permissions.
 - The administrator can set the audio input, audio output, alarm output, PTZ control permissions.
 - Audio input/Audio output/Alarm output : You can enable/disable Audio input/Audio output/Alarm output in the live mode on the current user account.
 - PTZ Control : Select the **<PTZ>**.
 - Profile : If you select **<Default>**, you can only see the default profile video; if selecting **<All>**, you can see the full profile videos.



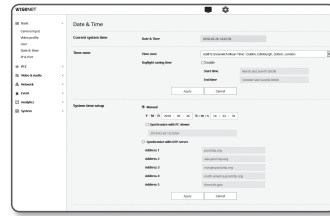
- ONVIF functions available to a registered user allowed to use ONVIF functions are limited to those of granted with permission.

4. When done, click **[Apply]**.

Date & Time

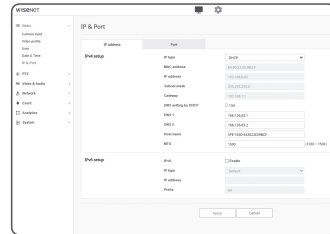
1. From the Setup menu, select the **<Basic (Basic icon)>** tab.
2. Click **<Date & Time>**.
3. Specify the time and date that will be applied to the encoder.
 - Current system time : Displays the current time settings of your system.
 - Timezone : Specify the local time zone based on the GMT.
 - Daylight saving time : If checked, the time will be set one hour before the local time zone for the specified time period.
This option will be displayed only in areas where DST is applied.
 - System time setup : Specify the time and date that will be applied to your system.
 - Manual : Sets the current time of the encoder manually.
When you select the **<Synchronize with PC viewer>** check box, the time of the webviewer is set to the time displayed on the PC that runs the webviewer.
 - Synchronize with NTP server : Sync with the time of the specified server address.
4. When done, click **[Apply]**.

! ■ If you select the **<Synchronize with PC viewer>**, the standard timezone should be set the same as the current timezone in PC.



IP & Port

1. From the Setup menu, select the **<Basic (Basic icon)>** tab.
2. Click **<IP & Port>**.
3. Click **<IP address>**.
4. Set the **<IPv4 setup>**.
 - IP type : Select an IP connection type.
 - Manual : Sets the IP address, subnet mask, gateway, DNS1, DNS2 and host name.
 - DHCP : Sets DNS1, DNS2, and host name.
 - PPPoE : Sets DNS1, DNS2, host name, ID and password.
 - If you set it to **<Manual>**, you should specify the IP, Subnet mask, Gateway, DNS 1 & 2 manually.
 - MAC address : Shows the MAC address.
 - IP address : Displays the current IP address.
 - Subnet mask : Displays the **<Subnet mask>** for the set IP.
 - Gateway : Displays the **<Gateway>** for the set IP.
 - DNS1/DNS2 : Displays the DNS(Domain Name Service) server address.
 - Host name : Displays the host name.
 - MTU : Sets the maximum data transfer size that can be sent from the network interface.
The possible value range is from 1280 to 1500. Video playback may be delayed, so make sure to set the MTU value that is appropriate for your network environment.



5. Set the **<IPv6 setup>**.

- Set to **<Use>** to use IPv6 address.
- Default : Use the default IPv6 address.
- DHCP : Display and use the IPv6 address obtained from the DHCP server.
- Manual : Enter IP address and gateway manually and use it.

! ■ The IP addressing system will be defaulted to DHCP. If no DHCP server is found, the previous settings will be restored automatically.

■ Once completed with editing, click **[Apply]** to apply changes and the browser exits. After a while, connect again with the changed IP.

6. Click **<Port>**.

7. Type in each item in the Port menu as necessary.

- Neither the port range between 0 and 1023 nor port 3702 is available.
- HTTP : HTTP port used to access the encoder via the web browser.
The default is 80(TCP).
 - Setting the HTTP port for Safari and Google Chrome browsers to 65535 is not allowed by security policy.
- HTTPS : In this version, the security of the web communication protocol HTTP is strengthened. It can be used when you set HTTPS mode in SSL.
The initial value is set to 443(TCP).
 - The available setting range is 1024~65535. (For security reasons, in your Safari or Google Chrome browser, you may not use 65535 as your HTTPS port.)
- RTSP : Used to transfer videos in the RTSP mode; the default is 554.
- Timeout : When connecting to RTSP, this function resets the connection if there's no response for a certain time.



- If changed the HTTP port, the browser exits.
Afterwards, address should contain the newly assigned HTTP port trailing the IP.
ex) IP address: 192.168.1.100, HTTP port : Assigned 8080 → http://192.168.1.100:8080
(If HTTP port is set to 80, no need to specify the port number)
- Using RTSP and HTTPS is recommended in order to prevent the image information from being restored.

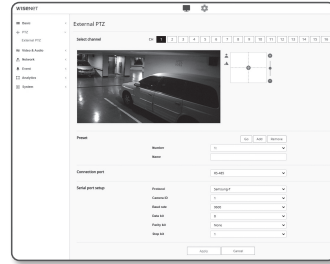
8. When done, click **[Apply]**.

PTZ SETUP

External PTZ

Sets the connection value of the external PTZ camera so that the PTZ can be controlled through the camera connected to the RS-485 terminal of the encoder.

1. From the Setup menu, select the <PTZ (+)> tab.
2. Click <External PTZ>.
3. Select the channel to set.
4. Please set the connection port.
 - RS-485 : Select this if you want to control the camera and remote AUX via the RS-485 terminal.
 - Coaxial : Set for camera control. PTZ and OSD can be controlled.
5. Please set the serial port. If you select <RS-485> as the connection port, you can set the RS-485 communication mode of the connected PTZ camera.
 - Protocol : Selects the same protocol as the camera, from among Samsung-T / Pelco-D / Pelco-P.
 - Camera ID : Displays the fixed camera ID.
 - Baudrate : Transfer rate for RS-485 communications.
 - Data bit : Specify the data bit.
 - Parity bit : Specify the parity bit.
 - Stop bit : Specify the stop bit.
6. When done, click [Apply].



■ For this operation, the encoder and the PTZ camera should be connected normally. In addition, the serial port must be set to operate the PTZ camera.

■ Check the functions supported by the camera when it is connected.
Some functions may be disabled depending on the camera or protocol specification. Refer to the following table for more details.

Functions Supported for Each Protocol

Protocol	P control	P movement speed	T control	T movement speed	Zoom control	Zoom movement speed	Focus control	Focus control speed	Preset save	Preset movement	Remarks
SAMSUNG-T	0	0	0	0	0	0	0	X	0	0	
PELCO-D	0	0	0	0	0	0	0	X	0	0	
PELCO-P	0	0	0	0	0	0	0	X	0	0	

7. Click the cursor [+] on the screen moving pad to control movement of the screen.
 - Move screen: Scroll the cursor in the direction desired.
 - Control screen movement rate: The further away the cursor is from the center, the faster it moves on the screen.
8. Control zoom movement.
 - Zoom In: Move up the bar in the right of the UI, or press the [+] button. The farther the bar is from the center, the faster the screen expands.
 - Zoom Out: Move down the bar in the right of the UI, or press the [-] button. The farther the bar is from the center, the faster the screen reduces in size.
9. Adjust the focus.
 - Manual focus (/) : Adjusts the focus of the screen for short distance or long distance.

■ Pan/tilt/zoom control is only possible when the encoder is connected to the PTZ camera and <Serial port setup> is set normally.

To add a preset

1. Select the preset number to add.
2. Set the name for the preset.
3. Press the [Add] button.

To delete a preset

1. Select the preset number to delete.
2. Press the [Remove] button.

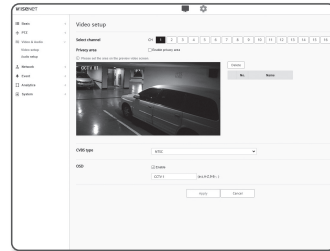
To move a preset

1. Select a preset number that you want to move.
2. Press the [Go] button.

VIDEO & AUDIO SETUP

Video setup

1. From the Setup menu, select the <Video & Audio (≡)> tab.
2. Click <Video setup>.
3. Select the channel to set.
4. Specify the privacy zone.
5. When done, click [Apply].
 - CVBS type: Select NTSC or PAL.
 - OSD: You can enter and display a camera name on the video that is up to 17 characters. (a-z, A-Z, 0-9, -, ,).



To set the privacy zone

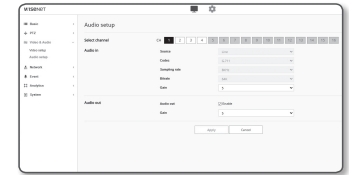
You can specify a certain area of the camera video to be protected for your privacy.

1. Select the <Enable Privacy area> checkbox.
2. Click [OK].
3. Click and drag over the video to select an area.
4. Enter the name and select the color, and then click [OK].
5. If you want to delete a name in the list, select it and click [Delete].

Audio setup

You can set the input/output value of the audio connected to the encoder.

1. From the Setup menu, select the <Video & Audio (≡)> tab.
2. Click <Audio setup>.
3. Select the channel to set.
4. Set the audio input value.



- Source : Input audio.
 - Line : Connect the cable to the audio device.
- Codec : Audio codec to use.
 - G.711 : A audio codec standard, it uses 64 Kbps PCM (Pulse Code Modulation) encoding. ITU standard audio codec that is adequate for digital voice transfer in PSTN network or through a PBX.
- Sampling rate : Refers to the number of times of sampling when digitalizing an analog soundtrack. The higher this value is, the better the sound quality is.
- Bitrate : Set the compression ratio based on the bit rate.
- Gain : Specify the audio input amplification.



■ Sound quality deterioration or howling may occur if the loudness of the sound source or gain value were set excessively.

5. Set the audio output level.
 - Enable : Sets whether to use audio output.
 - Gain : Specify the audio output amplification.
6. When done, click [Apply].

NETWORK SETUP

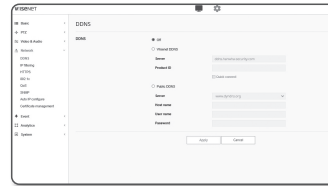
DDNS

DDNS is an abbreviation of Dynamic Domain Name Service that converts the IP address of an encoder into a general Host Name so that the user can easily remember it.

■ You can use the DDNS service only if the internet is connected.

1. From the Setup menu, select the **<Network ()>** tab.
2. Click **<DDNS>**.
3. Select the **<DDNS>** connection type.
4. Type in the DDNS items according to the selected type.
 - Wisenet DDNS : Select this if you use the DDNS server provided by [Hanwha Vision](http://ddns.hanwha-vision.com).
 - Product ID : Enter the product ID that is registered with the Wisenet DDNS service.
 - Quick connect : It sets port forwarding automatically when used with a UPnP (Universal Plug and Play) supporting router.
 - Public DDNS : Select one of provided public DDNS servers when you use a public DDNS server.
 - Server : Select desired public DDNS service server.
 - Host name : Enter the name of the host that is registered with the DDNS server.
 - User name : Enter the user name for the DDNS service.
 - Password : Enter the password for the DDNS service.
5. When done, click **[Apply]**.

■ If selected **<Quick connect>**, be sure to select Wisenet DDNS service.



Registering with DDNS

To register your product with the Wisenet DDNS

1. Visit the Wisenet DDNS web site (<http://ddns.hanwha-security.com>) and sign in with a registered account.

2. From the top menu bar, select **<MY DDNS>**.



3. Click the **[Register Product]** tab.

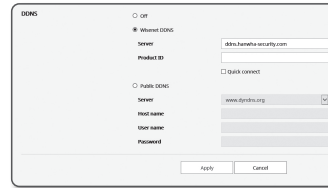
4. Enter the product ID.

5. Select a **<Type>** and specify the **<Model>**.
6. Specify the product location with a description if necessary.
7. Click **[Product Registration]**.
The product will be added to the product list that you can check.

No.	Product ID	Model	Connection Status	Product Location	View	Video Logging
1	xxxx1234	xxx	LAN DDNS		View	
2	xxxx1234	xxx	LAN DDNS		View	

To connect to the Wisenet DDNS in encoder setup

1. From the DDNS setup page, set <DDNS> to <Wisenet DDNS>.
2. Provide the <Product ID> that you registered product ID with the DDNS site.
3. Click [Apply].
When the connection is successfully made, you will see the message of <(Success)> on the screen.



Configuring public DDNS in encoder Settings

1. Open the DDNS settings page and select <Public DDNS> for <DDNS>.
2. Enter the corresponding site's host name, user name and password.
3. Click [Apply] button.
If the connection properly establishes, <(Success)> appears.
4. When done, click [Apply].

- To use DDNS service properly, both DDNS setup and the router's port forwarding setup are required.
For port forwarding setup, refer to "Port Range Forward (Port Mapping) Setup". (page 19)

IP filtering

You can create a list of IPs that you want to grant or deny access to them.

1. From the Setup menu, select the <Network ()> tab.
2. Click <IP filtering>.
3. Select <Filtering type>.
 - Deny registered IP : If selecting this, access from those IPs that are added to the filtering will be restricted.
 - Allow registered IP : If selecting this, access from only those IPs that are added to the filtering will be accepted.
4. Click the [Add] button.
The IP list will be created.
5. Provide the IP that you want to grant or deny access from.
When you enter an IP address and a Prefix, the list of IP addresses available will appear in the right-side filter range column.



- If selected <Allow registered IP> for IP Filtering and <IPv6 setup> of <IP & Port> is set to <Use>, both IPv4 and IPv6 addresses of the computer currently configuring should be assigned.
 - The IP address of the computer used for the current setup cannot be added to <Deny registered IP>, it should be added to <Allow registered IP>.
 - Only the IP addresses that are set to <Use> will be displayed in the filter column.
6. Select an IP to delete from the list.
Click the [Delete] button.
 7. When done, click [Apply].

HTTPS

You can select a secure connection system or install the public certificate for this purpose.

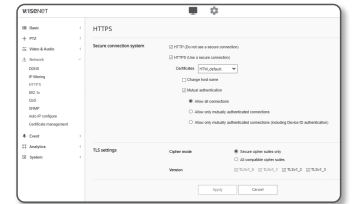
1. From the Setup menu, select the <Network ()> tab.
2. Click <HTTPS>.
3. Select a secure connection system.
 - HTTP (Do not use a secure connection): Select when you want to transmit data over HTTP without encryption.
 - HTTPS (Use a secure connection): Select when you want to connect by using a proprietary certificate.
 - Certificates: A list of registered certificates is displayed. You can register certificates in <Network> → <Certificate management>.
 - Change host name: Change the host name to be the same as the name of the certificate.
 - Mutual authentication: Select when you want to proceed with the mutual authentication to enhance the security.

The following options about allowing access are available.

 - Allow all connections: Allow all connections regardless of the mutual authentication success status.
 - Allow only mutually authenticated connections: Allow access only if mutually authenticated.
 - Allow only mutually authenticated connections (including Device ID authentication): Allow access only if has been verified and authenticated up to the device ID information.
4. Register the TLS settings.

You can select the Cipher mode or TLS version to use for encrypted communication.

 - Cipher mode: Provides cipher suites in several algorithm combinations used for encrypted communication.
 - Secure cipher suites only: Use only highly secured cipher suites.
 - All compatible cipher suites: Use all cipher suites (security vulnerability).
 - Version: You can select the TLS protocol version to use for encrypted communication.
5. When done, click [Apply].

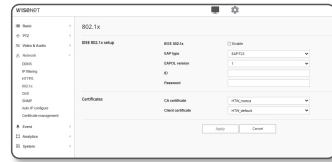


802.1x

When connecting network, you can choose whether using 802.1x protocol, and then install the certification.

1. From the Setup menu, select the **<Network (🏠)>** tab.
2. Click **<802.1x>**.
3. Set the **<IEEE 802.1x setting>**.

- IEEE 802.1x : Specify the use of the 802.1x protocol.
- EAP type : Select EAP-TLS or LEAP.
- EAPOL version : Select version 1 or 2.
- ID : Enter the client certificate ID in EAP-TLS and the user ID in LEAP.
- Password : Enter the client private key password in EAP-TLS and the user password in LEAP. You do not have to enter the password in EAP-TLS if it uses a key file that is not encrypted.



- If the connected network device does not support the 802.1x protocol, the protocol will not operate properly even if you set it.
- LEAP is an authentication method with poor security. Use it only in an environment where EAP-TLS is not available.

4. You can select the type of certificate from **<CA certificate>** or **<Client certificate>**.
 - CA certificate: Select the desired CA certificate from the list of certificates.
 - The CA certificate registered in **<Network>** → **<Certificate management>** → **<CA certificate>** is displayed.
 - Client certificate: Select the desired client certificate from the list of certificates.
 - The client certificate registered in **<Network>** → **<Certificate management>** → **<Client certificate>** is displayed.
5. When done, click **[Apply]**.

QoS

You can specify the priority to secure a stable transfer rate for a specific IP.

1. From the Setup menu, select the **<Network (🏠)>** tab.
2. Click **<QoS>**.
3. Click the **[Add]** button.
The IP list will be created.
4. Enter an IP address to which you will apply QoS.



- The default prefix for IPv4 is 32;
For DSCP, the default is set to 63.
- Only the IP addresses that are set to **<Use>** can be prioritized.

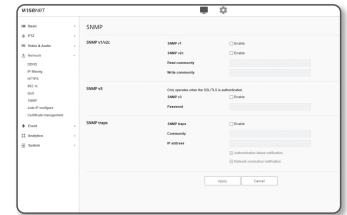
5. Select an IP to delete from the list.
Click the **[Delete]** button.
6. When done, click **[Apply]**.

SNMP

With the SNMP protocols, the system or network admin can monitor the network devices on a remote site, and configure the environment settings.

1. From the Setup menu, select the **<Network (🏠)>** tab.
2. Click **<SNMP>**.
3. Specify the **<SNMP>**.

- Enable SNMP v1 : SNMP version 1 will be active.
- Enable SNMP v2c : SNMP version 2 will be active.
 - Read community : Provide the name of the read community where you can access to the SNMP information. The default name is **<public>**.
 - Write community : Provide the name of the write community where you can access to the SNMP information. The default name is **<write>**.
- Enable SNMP v3 : SNMP version 3 will be active.
 - Password : Specify the default password for SNMP version 3.
 - The default password can be exposed to a hacking thread so it is recommended to change the password after installing the product.
Note that the security and other related issues caused by the unchanged password shall be responsible for the user.
 - Password should be longer than 8 characters, no more than 16 characters.
- Enable SNMP Trap : SNMP trap is used to send important events and conditions to the Admin.
 - Community : Enter the trap community name to receive messages.
 - IP address : Enter the IP address to which messages will be sent.
 - Authentication failure notification : It specifies whether an event shall be generated when the community information is invalid.
 - Network connection notification : It specifies whether an event shall be generated when the network disconnection is restored.



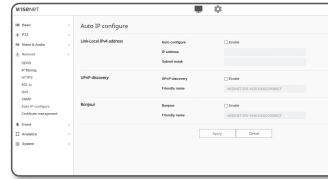
4. When done, click **[Apply]**.

- SNMP v3 is only able to be set when the secure connection mode is HTTPS.
Refer to "HTTPS". (page 32)
- If you don't use SNMP v3, there may be a security issue.

Auto IP configure

You can set the IP available for access and encoder searching automatically.

1. From the Setup menu, select the **<Network ()>** tab.
2. Click **<Auto IP configure>**.
3. Set the **<Link-Local IPv4 address>**.
An additional IP address may be assigned to access the encoder from the Link-Local network.
 - Auto configure : It specifies Able or Disable for the Link-Local IPv4 address.
 - IP address : Display the assigned IP address.
 - Subnet mask : Display the subnet mask of the assigned IP.



4. Set the **<UPnP discovery>**.
Encoders can be automatically searched in the client and operating system in support of the UPnP protocol.
 - UPnP discovery : It specifies Able or Disable for UPnP Discovery.
 - Friendly name : Display the encoder name.
Friendly name is displayed in the format of WISENET-<Model Name>-<MAC Address>.

 ■ In the Windows operating system which basically supports UPnP, the encoders connected to the network are displayed.

5. Set the **<Bonjour>**.
Encoders can be automatically searched in the client and operating system in support of the Bonjour protocol.
 - Bonjour : It specifies Able or Disable for Bonjour.
 - Friendly name : Display the encoder name.
Friendly name is displayed in the format of WISENET-<Model Name>-<MAC Address>.

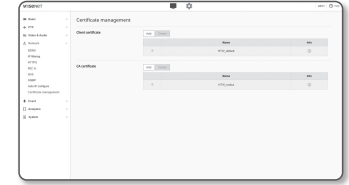
 ■ In the Mac operating system, which support Bonjour by default, the connected encoders are automatically displayed in the Bonjour bookmark of the Safari web browser.
If the Bonjour bookmark is not displayed, check Bookmarks Setup in the "Preference" menu.

6. When done, click **[Apply]**.

Certificate management

You can add or delete the CA certificate and client certificate.

1. From the Setup menu, select the **<Network ()>** tab.
2. Click **<Certificate management>**.
3. Click the **<Add>** button on the certificate you want to add.



Install/uninstall the client certificate

1. Click the **<Add>** button in the client certificate.
2. Select the **<Type>** option.
 - If you have a certificate file, select the **<Client>** and set it as follows.
 - Name for the certificate: Enter the certificate name.
 - Certificate file: Click the **[Search ()]** button to select a certificate file.
 - Key file: Click the **[Search ()]** button to select the authentication key file.
 - To create your own certificate, select **<Self-Signed>** and set up the following.
 - Name for the certificate: Enter the certificate name.
 - Common Name (CN): Enter the common name of the certificate.
 - SAN: Enter the certificate SAN (Subject Alternative Name).
 - Valid thru: Select the expiration date of the certificate.
 - Country (C): Enter the country. Up to two letters are allowed.
 - State/province (ST): Enter the state or province.
 - Organization (O): Enter the name of the organization.
 - City/locality (L): Enter the locality information.
 - Organization unit (OU): Enter the organization unit.
 - E-mail: Enter the e-mail address.
3. If the setting is complete, click the **[OK]** button.
4. To delete a certificate, select a client certificate and click the **[Delete]** button.

Install/uninstall the CA certificate

1. Click the **<Add>** button in the CA certificate.
2. Set up the items below.
 - Name for the certificate: Enter the certificate name.
 - Certificate file: Click the **[Search ()]** button to select a certificate file.
3. If the setup is complete, click the **[OK]** button.
4. To delete a certificate, select the CA certificate and click the **[Delete]** button.

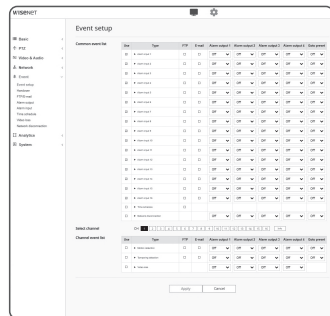
EVENT SETUP

Event setup

You can easily set the event detection items, and move to the detailed setting.

1. From the Setup menu, select the <Event (🏠)> tab.
2. Click <Event setup>.
3. Activate desired items on the Event list.
4. When done, click [Apply].

■ To configure detailed event settings, click a desired type. You will be redirected to the detailed settings.



Handover

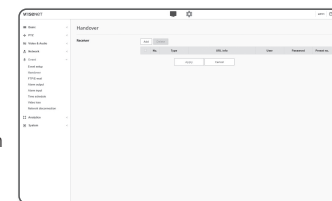
Event detection can be used in conjunction with an additional camera with a PTZ preset function. When an event is detected, the interworking PTZ camera moves to the preset position and can perform monitoring.

1. From the Setup menu, select the <Event (🏠)> tab.

2. Click <Handover>.

- Receiver camera : Register the camera that is to be interworking with event detection. Click [Add] at the top of the menu to enter the IP, port, ID, password of the camera to be interworked, and the preset number to move to when detecting an event.
 - You can use handover for motion detection, tampering detection, and/or event detection.
 - Only operates normally if the preset set in the receiver camera is specified.
 - Handover supports only one preset per area.

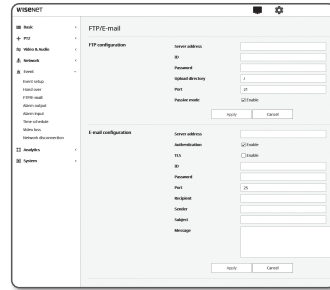
3. When done, click [Apply].



FTP / E-mail

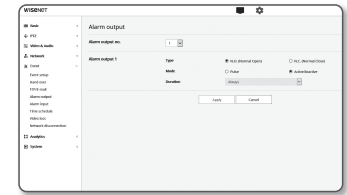
You can configure the FTP/E-mail server settings so that you can transfer the images taken with camera to your PC if an event occurs.

1. From the Setup menu, select the <Event ()> tab.
2. Click <FTP / E-mail>.
3. Select <FTP configuration> or <E-mail configuration> and enter / select a desired value.
 - FTP configuration
 - Server address : Enter the IP address of the FTP server that you transfer the alarm or event images to.
 - ID : Enter the user ID with which you will log in to the FTP server.
 - Password : Enter the user account password for logging into the FTP server.
 - Upload directory : Specify the FTP path where you will transfer the alarm or event images.
 - Port : The default port of the FTP server is 21; however, you can use a different port number according to the FTP server settings.
 - Passive mode : Select <On> if you need to connect in passive mode due to the firewall or the FTP server settings.
 - E-mail configuration
 - Server address : Enter the SMTP address of the email server that you transfer the alarm or event images to.
 - Authentication : Select whether to use authorization.
 - TLS : Specify the use of TLS.
 - ID : Enter the user ID for logging into the email server.
 - Password : Enter the user account password for logging into the email server.
 - Port : The default port of the email server is 25; however, you can use a different port number according to the email server settings.
 - Recipient : Enter the address of the email recipient.
 - Sender : Enter the address of the email sender. If the sender address is incorrect, the email from the sender may be classified as SPAM by the email server and thus may not be sent.
 - Subject : Enter a subject for your email.
 - Message : Provide the text for the message. Attach the alarm or event images to the email that you are preparing.
4. When done, click [Apply].



Alarm output

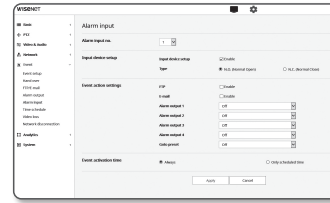
1. From the Setup menu, select the <Event ()> tab.
2. Click <Alarm output>.
3. Set the alarm output of the encoder.
 - If you change the alarm output type, the alarm out button on the monitoring page and alarm output type displayed on Event Setup page will be changed accordingly.
 - Type
 - N.O. (Normal Open) : Considers "Open circuit" status of the sensor or alarm input device as normal, and triggers alarm event if becomes "Closed circuit" status.
 - N.C. (Normal Close) : Considers "Closed circuit" status of the sensor or alarm input device as normal, and triggers alarm event if becomes "Open circuit" status.
 - Mode : Sets the alarm output method.
 - There is difference between operations when clicked alarm output button while disabled.
 - Pulse : It is activated during the time period specified by the duration (switching interval) and then becomes inactive automatically.
 - Active/Inactive : It maintains as activated until the user clicks the button again to make it inactive.
 - Duration : Set the alarm duration that maintains activated if the mode is set to pulse, from 1 to 15 seconds.
4. When done, click [Apply].



Alarm input

You can set the alarm input type, activation time, and operation mode.

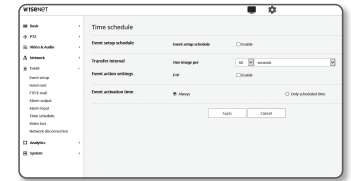
1. From the Setup menu, select the <Event (🔔)> tab.
2. Click <Alarm input>.
3. Set whether or not to <Enable>.
4. Select the type.
 - N.O. (Normal Open) : It is normally open, but if it is closed, an alarm will be triggered.
 - N.C. (Normal Close) : It is normally closed, but if it is open, an alarm will be triggered.
5. Specify the <Event activation time>.
 - Always : Always check if an alarm occurs. It activates in operated mode when the alarm occurs.
 - If set to <Always>, the activation time cannot be changed.
 - Only scheduled time : Check if an alarm occurs at a specified day of the week for a specified time period. It activates in operated mode when the alarm occurs.
 - [1 min 30 min 1 h] : Sets the time display format on the vertical axis.
 - [Reset] : Reset all settings.
6. Specify an operation that will perform if an alarm occurs.
 - FTP : Specify the use of FTP transfer in the alarm input setup.
 - Refer to "FTP / E-mail" for more details. (page 36)
 - E-mail : Specify the use of email transfer in the alarm input setup.
 - Refer to "FTP / E-mail" for more details. (page 36)
 - Alarm output : Select whether to set the alarm output if an alarm is incoming, and specify the alarm output time.
 - Goto preset : Moves to the specified preset location when setting the alarm input.
 - Preset Move is possible only when the encoder and PTZ camera are connected.
 - Only the preset of the same channel as the alarm input number can be set. (e.g., Alarm 2 → Channel 2 → Preset of Channel 2)
7. When done, click [Apply].



Time schedule

You can configure settings to transmit images at regular intervals at a scheduled operation time regardless of the occurrence of an event.

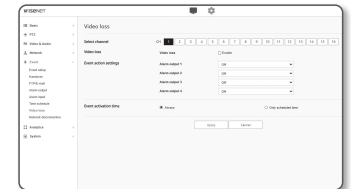
1. From the Setup menu, select the <Event (🔔)> tab.
2. Click <Time schedule>.
3. Set whether or not to <Enable>.
4. Specify the <Transfer interval>.
5. Specify the <Event activation time>.
 - Always : Always activates in operated mode at the set interval.
 - Only scheduled time : Periodically activates in operated mode at a specified time and date.
 - The transfer interval setting value must be smaller than the preset activation interval to succeed in image transmission.
6. Specify the activation conditions.
 - FTP : Specify the use of the FTP transfer if an event occurs.
 - Refer to "FTP / E-mail" for more details. (page 36)
7. When done, click [Apply].



Video loss

You can set the camera so that the camera can trigger an alarm to notify the user if the video has been lost due to disconnection with the camera.

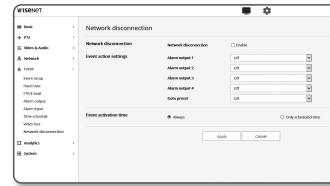
1. From the Setup menu, select the <Event (🔔)> tab.
2. Click <Video loss>.
3. Select the channel to set.
4. Set whether or not to <Enable>.
5. Configure the event motion schedule and event motion conditions.
 - For more information about <Event activation time> and <Event action settings>, refer to "Alarm input". (page 37)
6. When done, click [Apply].



Network disconnection

When the network is physically disconnected, it is considered as an event to be saved.

1. From the Setup menu, select the <Event (🔌)> tab.
2. Click <Network disconnection>.
3. Set whether or not to <Enable>.
4. Configure the event motion schedule and event motion conditions.
 - For more information about <Event activation time> and <Event action settings>, refer to "Alarm input". (page 37)
5. When done, click [Apply].

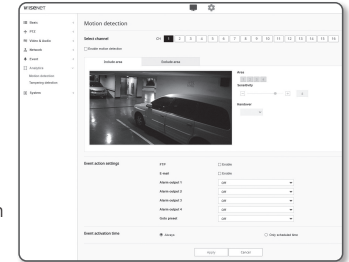


CONFIGURE ANALYSIS SETTINGS

Motion detection

You can configure settings to generate an event signal when a motion is detected.

1. From the Setup menu, select the <Analytics (🔍)> tab.
2. Click <Motion detection>.
3. Select the channel to set.
4. Set whether or not to <Enable Motion detection>.
5. Set an <Include area> and <Exclude area>.
 - You can set up to 4 areas.
6. Configure settings for each item.
 - Sensitivity : Sets the sensitivity of motion detection for each area. Decrease the sensitivity in an environment where the background and the object are clearly distinguished, and increase the sensitivity in a dark environment where the background and the object cannot be clearly distinguished.
7. Select whether or not to use the handover.
 - When a motion is detected in the set detection area, a specific camera moves to a specific PTZ preset position.
 - You can specify cameras by detection area.
8. Configure the event motion schedule and event motion conditions.
 - For more information about <Event activation time> and <Event action settings>, refer to "Alarm input". (page 37)
9. When done, click [Apply].

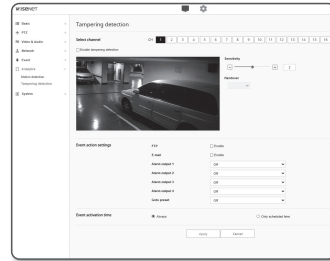


- Use continuous recording rather than motion detection event recording in areas where motion detection is frequent.
- Since the log is recorded once every 5 minutes, the buffered motion detection log data may be damaged when the power is turned off.
- Detected size of an object may have difference with the actual size according to its shape.
- In the following cases, motion detection performance may be impaired or a malfunction may occur.
 - The object color or brightness is similar to the background.
 - Small activities around the border area of the camera's field of view.
 - Multiple movements continue occurring at random due to a scene change, rapid lighting changes or other reasons.
 - A fixed object continues moving in the same position.
 - Motions of less position changing such as approaching to the camera or fading away from the camera.
 - Moving object approaches to the camera too close
 - An object hides other objects behind.
 - Too fast object (for a proper detection, one object should be found overlapping between contiguous frames).
 - Reflection / blur / shadow due to a strong light such as direct sunlight, illumination, or headlamp.
 - In severe snow, rain, wind or in dawn / dusk.

Tampering detection

You can set to detect tampering attempts and trigger events, such as sudden change of camera's framing direction, blocked lens and other overall change of scenes from the video.

1. From the Setup menu, select the **<Analytics (📊)>** tab.
2. Click **<Tampering detection>**.
3. Select the channel to set.
4. Set whether or not to **<Enable Tampering detection>**.
5. Set the sensitivity.
The higher the set value, the more sensitive the camera reaction (range: 1 to 3).
6. Select whether or not to use the handover.
7. Configure the event motion schedule and event motion conditions.
 - For more information about **<Event activation time>** and **<Event action settings>**, refer to "Alarm input". (page 37)
8. When done, click **[Apply]**.

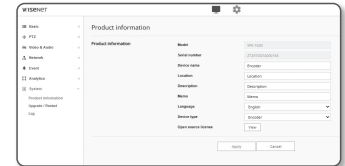


- ! ■ The detection will be restarted after stabilization for a certain period of time (about 5 seconds). During stabilization, detection is not available.
- If false alarms are frequently generated, you should gradually decrease the sensitivity to minimize false alarms.
- If you use a low sensitivity, alarms may be generated even by very small changes on the screen, but false detection may occur in response to changes in moving objects or brightness.
- In the following cases, the tampering detection function may malfunction.
 - Monitoring environment with simple background, night and low light level environment.
 - Severe camera vibration or sudden lighting changes

SYSTEM SETUP

Product information

1. From the Setup menu, select the **<System (⚙️)>** tab.
2. Click **<Product information>**.
3. Check the encoder information or enter the appropriate details for the installation environment.
 - Model : Model name of the product.
 - Serial number : Product serial number.
 - Device name : Provide a device name that will be displayed on the Live screen.
 - Location : Specify the location where the encoder is installed.
 - Description : Provide detailed information about the encoder location.
 - Memo : Provide an explanation about the encoder for better understanding.
 - Language : Select a preferred language for the Web Viewer OSD.



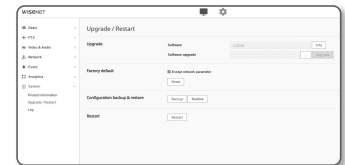
- The default language is set to **<English>**.

- Device Type : Set the type of product.
For more details, see "Device Type setup guide". (page 41)
- Open source license: click the **[View]** button to check the details of the open source license used in this product.

4. When done, click **[Apply]**.

Upgrade / Restart

1. From the Setup menu, select the **<System (⚙️)>** tab.
2. Click **<Upgrade / Restart>**.
3. Select a desired item and set it appropriately.
 - Upgrade : Performs upgrading the system.
When reconnecting, the web viewer will not run normally if the browser cache is not completely clear.
 - Factory default : Initializes all setting information including the encoder settings to the factory reset state. (however, logs are not initialized)
 - If you select the **<Except network parameter>** check box, the network settings will be excluded and reset.
 - The IP addressing system will be defaulted to DHCP if you reset the encoder. If no DHCP server is found, the previous settings will be restored automatically.
 - Configuration backup & Restore : Backs up the current system settings before performing the restoration process. The system is automatically restarts after backup or restoration.
 - Restart : Restarts the system.



To perform the upgrade

1. Click **[Browse ()]** and specify a file to upgrade.
2. Click **[Upgrade]**.
3. An **"Upgrade"** progress bar is prompted to show the upgrading status.
4. Once completed upgrading, the browser exits and the encoder restarts.



- It may take a max of 10 minutes for the upgrade process.
If you forcibly terminate the upgrade process, upgrade will not be completed properly.
- During restarting the system, accessing with web viewer will not be made.
- You can download the latest version from the [Hanwha Vision](#) web site.

To back up the current settings

1. Click **[Backup]**.
2. A file in a **".bin"** file format is saved in **"Library" -> "Document" -> "Downloads"**.

To restore the backup settings

1. To restore the backup settings, click **[Restore]**.
2. Select a desired backup file.



- If you perform the backup or restoration, the web browser will be closed and the encoder will reboot.
- If you try to recover the config file backed up in other model, some functions may malfunction and you need to change the setting manually.

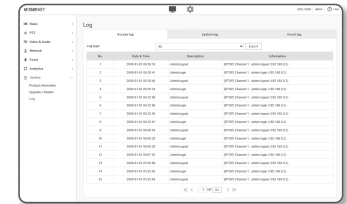
Log

You can check the system log or event log.

1. From the Setup menu, select the **<System ()>** tab.
2. Click **<Log>**.
3. Select a log type.
 - Access Log : You can check the log information that contains the user's access and the access time.
 - System log : You can check the system logs where any system changes are recorded including the time information.
 - Event log : You can check the event logs including the time information.
4. From the right log list, select an item to search for.
 - If you select **<All>** in the top left dropdown list, all logs for the applicable log type will be displayed.
5. If one page can not display all the logs available, use the bottom buttons to move to the previous, next, or the last item.
6. Click on the **<Export>** button to save all the log data for the currently selected mode in the "time stamp value create by encoder in modelname-mode-encoder.txt file" in the download folder for the browser.



- Each page displays 15 logs with the latest one displayed at the top.
- Each log contains up to 1,000 records and after 1,000 records are saved, the oldest log is deleted when a new record is generated.



DEVICE TYPE SETUP GUIDE

See the table below to connect your encoder to SSM.

For more details, see "Setting up the system" in the manual.

	SSM 2.0 lower	SSM 2.1 higher
Device type	NWC	Encoder

TROUBLESHOOTING

PROBLEM	SOLUTION
When an Windows 10 user accesses the web viewer through Chrome or Firefox, the sound volume of microphone changes periodically.	This is what happens when microphone driver has been set to Realtek driver. Install the High Definition Audio device (Windows Default Driver) or the third party driver as the microphone driver.
No video is displayed when accessing the plug-in free webviewer on Safari via HTTPS.	- On the authentication popup window prompted when initially accessing https, click "View Authentication Certificate" and select the "Always trust when connecting to the designated webviewer IP" check box. - If the webviewer continues failing to display a video after you select "Next" on the message window below, press the command key + Q to exit the Safari browser, access again and follow the procedures stated above.
I can't access the encoder from a web browser.	- Check to make sure that the encoder's Network settings are appropriate. - Check to make sure that all network cables have been connected properly. - If connected using DHCP, verify that the encoder is able to acquire dynamic IP addresses without any problem. - If the encoder is connected to a Broadband Router, verify that port forwarding is properly configured.
Viewer got disconnected during monitoring.	- Connected Viewers become disconnected upon any change to encoder or network configurations. - Check all network connections.
The product connected to the network is not detected in the Device Manager program.	Turn off the firewall settings on your PC and then search the encoder again.

PROBLEM	SOLUTION
Images overlap.	Check whether two or more encoders are set to a single multicast address instead of different addresses. If a single address is used for multiple encoders, the images may overlap.
No image appears.	If the transmission method is set to multicast, check whether there is a router that supports multicast in the LAN the encoder is connected to.
Voice is not recorded even though audio input settings are configured.	You must select the <Audio-In> check box in <Basic>-<Video Profile>.
<Motion detection> of <Analytics> is set to <Enable>, but no notification e-mail reaches me even when an analysis event had occurred.	- Verify the settings in the following sequence: A. Check <Data & Time> settings. B. The <Motion detection> should be set to <Enable>. C. Check if the <E-mail> option of <Event setup> menu is checked to use.
The system does not turn on and the indicator on the front panel does not work at all.	- Check if the power supply system is properly connected. - Check the system for the input voltage from the power source. - If the problem persists even after you have taken the above actions, check the power supplier and replace it with a new one if neccessary.
Video is being input, but some channels do not output video and instead output a video loss screen.	- Check if the camera connected to the encoder properly displays the image. Sometimes, this problem may occur on a camera that is not properly connected to the video source. - Check if the camera is properly supplied with power. - Sometimes, this problem may occur on a channel with weak video signal from a video distributor that is connected to multiple systems. In this case, input the video source of the camera directly into the encoder. This may find the cause and solve the problem.
No response is made even if I click the [PTZ] menu on the Live screen.	Setup → PTZ → External PTZ → Check if the current protocols and other settings in the PTZ device are properly configured according to the PTZ camera.
I forgot the password.	- Contact the encoder administrator for help. - Perform a factory reset by pressing the [RESET] button. Please note that this will also initialize the setting values.



Any changes or modifications in construction of this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

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



[Hanwha Vision](#) cares for the environment at all product manufacturing stages, and is taking measures to provide customers with more environmentally friendly products.

The Eco mark represents [Hanwha Vision](#)'s devotion to creating environmentally friendly products, and indicates that the product satisfies the EU RoHS Directive.



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

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

This marking on the product, accessories or literature indicates that the product and its electronic accessories (e.g. charger, headset, USB cable) should not be disposed of with other household waste at the end of their working life. To prevent possible harm to the environment or human health from uncontrolled waste disposal, please separate these items from other types of waste and recycle them 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 these items for environmentally safe recycling.

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



Correct disposal of batteries in this product

(Applicable in the European Union and other European countries with separate battery return systems.)

This marking on the battery, manual or packaging indicates that the batteries in this product should not be disposed of with other household waste at the end of their working life. Where marked, the chemical symbols Hg, Cd or Pb indicate that the battery contains mercury, cadmium or lead above the reference levels in EC Directive 2006/66. If batteries are not properly disposed of, these substances can cause harm to human health or the environment.

To protect natural resources and to promote material reuse, please separate batteries from other types of waste and recycle them through your local, free battery return system.

