

Video Encoder



Operation Manual



Before reading this manual

This operation manual contains basic instructions on installing and using DirectIP Video Encoder.
Users who are using this product for the first time, as well as users with experience using comparable products, must read this operation manual carefully before use and heed to the warnings and precautions contained herein while using the product. Safety warnings and precautions contained in this operation manual are intended to promote proper use of the product and thereby prevent accidents and property damage and must be followed at all times. Once you have read this operation manual, keep it at an easily accessible location for future reference.

- ☒
- The manufacturer will not be held responsible for any product damage resulting from the use of unauthorized parts and accessories or from the user's failure to comply with the instructions contained in this operation manual.
 - It is recommended that first-time users of this video encoder and individuals who are not familiar with its use seek technical assistance from their retailer regarding product installation and use.
 - If you need to disassemble the product for functionality expansion or repair purposes, you must contact your retailer and seek professional assistance.
 - Both retailers and users should be aware that this product has been certified as being electromagnetically compatible for commercial use. If you have sold or purchased this product unintentionally, please replace with a consumer version.

Safety Precautions

	<div>CAUTION</div> <div>RISK OF ELECTRIC SHOCK DO NOT OPEN</div>	
CAUTION: TO REDUCE THE RISK OF ELECTRIC SHOCK, DO NOT REMOVE COVER (OR BACK). NO USER-SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.		

- 
- The lightning flash with arrowhead symbol, within an equilateral triangle, is intended to alert the user to the presence of uninsulated "dangerous voltage" within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock.
- 
- The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

Safety Precautions

Important Safeguards

1. Read Instructions

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

2. Retain Instructions

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

3. Cleaning

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

4. Attachments

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

5. Water and/or Moisture

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

6. Ventilation

Place this equipment only in an upright position. This equipment has an open-frame Switching Mode Power Supply (SMPS), which can cause a fire or electric shock if anything is inserted through the ventilation holes on the side of the equipment.

7. Accessories

Do not place this equipment on an wall or ceiling that is not strong enough to sustain the camera. The equipment may fall, causing serious injury to a child or adult, and serious damage to the equipment. Wall or shelf mounting should follow the manufacturer's instructions, and should use a mounting kit approved by the manufacturer.



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

8. Power Sources

This equipment should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power, please consult your equipment dealer or local power company. You may want to install a UPS (Uninterruptible Power Supply) system for safe operation in order to prevent damage caused by an unexpected power stoppage. Any questions concerning UPS, consult your UPS retailer.

9. Power Cord

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

10. Lightning

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

11. Overloading

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

12. Objects and Liquids

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

13. Servicing

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

14. Damage requiring Service

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

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

15. Replacement Parts

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

16. Safety Check

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

17. Field Installation

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

18. Correct Batteries

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

19. Tmra

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

20. Elevated Operating Ambient Temperature

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

21. Reduced Air Flow

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

22. Mechanical Loading

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



23. Circuit Overloading

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

24. Reliable Earthing (Grounding)

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

In-Text

Symbol	Type	Description
	Caution	Important information concerning a specific function.
	Note	Useful information concerning a specific function.

User's Caution Statement

Caution: Any changes or modifications to the equipment not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

FCC Compliance Statement

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

WARNING: CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT. THIS CLASS OF DIGITAL APPARATUS MEETS ALL REQUIREMENTS OF THE CANADIAN INTERFERENCE CAUSING EQUIPMENT REGULATIONS.

WEEE (Waste Electrical & Electronic Equipment)

Correct Disposal of This Product

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



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

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

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

Copyright

© 2023 Costar Video Systems

Costar Video Systems reserves all rights concerning this operation manual.

Use or duplication of this operation manual in part or whole without the prior consent of Costar Video Systems is strictly prohibited.

Contents of this operation manual are subject to change without prior notice for reasons such as functionality enhancements.

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

The software included in this product contains some Open Sources. You may obtain the corresponding source code which we have to distribute according to the license policy. For more information, refer to System > General page. This product includes software developed by the University of California, Berkeley and its contributors, and software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). Also, this product includes cryptographic software written by Eric Young (eyay@cryptsoft.com).

Covered by one or more claims of the patents listed at patentlist.accessadvance.com.

Table of Contents

1

Part 1 – Introduction..... 8

Product Features8

Accessories.....10

Overview10

 Front Panel.....10

 Rear Panel11

2

Part 2 - Remote Setup..... 13

Remote Setup13

Quick Setup14

System.....14

 General14

 Date/Time15

 User/Group16

Network16

 IP Address16

 FEN.....17

 Port/QoS.....18

 Security.....19

Video20

 Camera20

 Streaming21

 Privacy Masking.....22

Audio23

 Input23

 Email23

Event24

 Motion Detection24

 Trip-Zone25

 Tampering26

 Video Loss27

3	Part 3 - WebGuard	28
	Web Live Mode.....	30
4	Part 4 - Appendix	32
	Troubleshooting	32
	Specifications	32

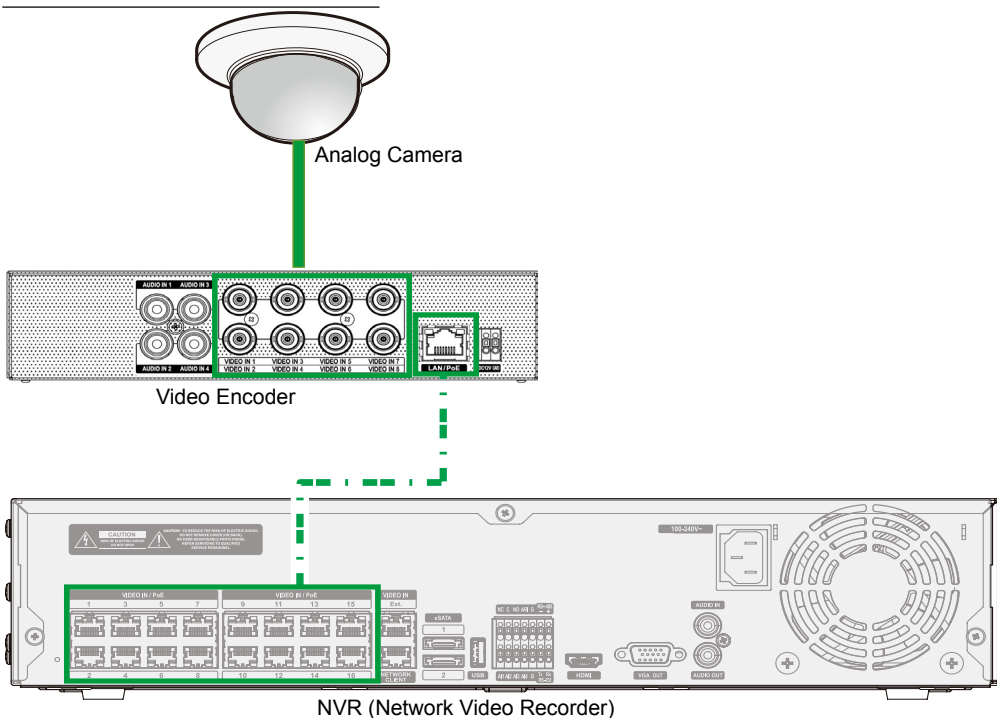
Part 1 – Introduction

Product Features

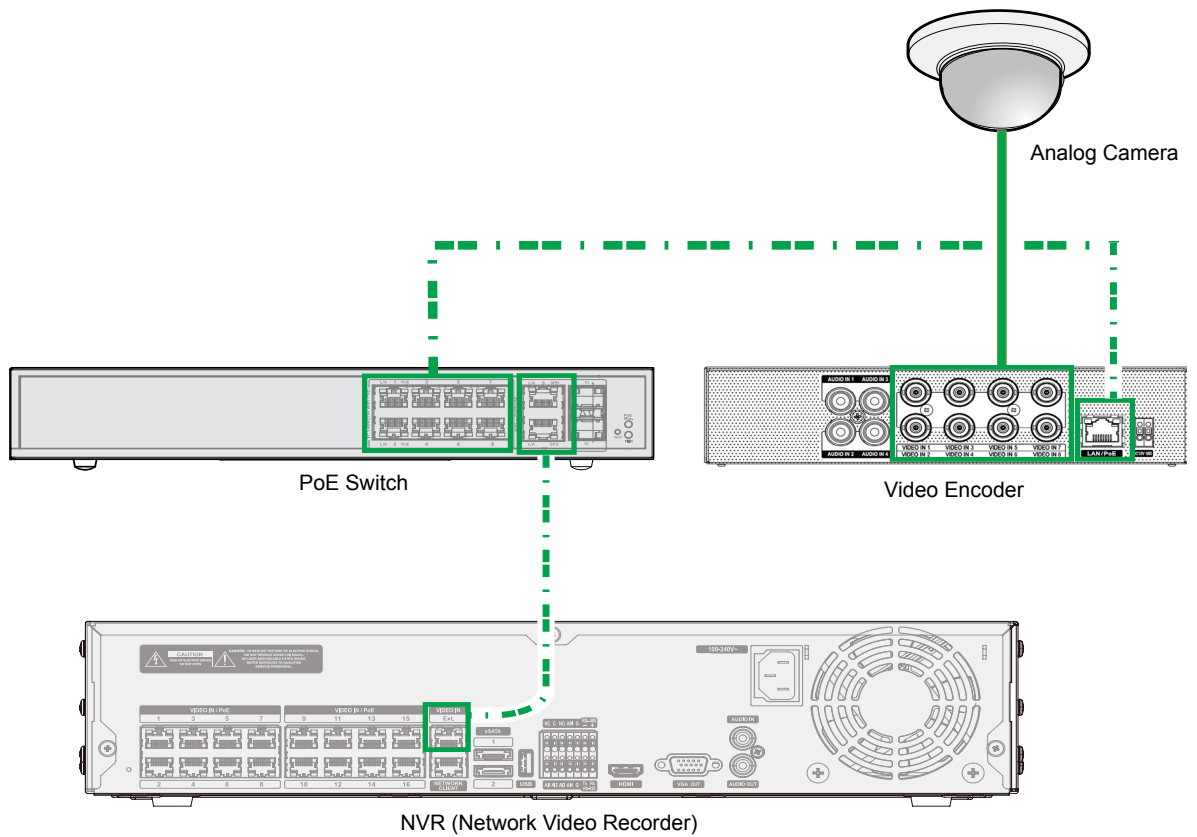
This video encoder compresses live video from analog cameras and transmits the video over Ethernet connections. This encoder offers the following features:

- 8 composite video input connectors
- Multi-streaming for monitoring and recording
- H.264 and H.265 compression algorithm
- Four levels of video compression and various video compression resolutions
- DirectIP 2.0 protocol supported
- Convenient firmware upgrades via network
- Firmware duplication and autorecovery functions to enhance system stability
- Event detection functions: Motion, Trip-Zone, Video Loss, Tampering
- 4-channel audio in
- Configuration of encoder settings and integrated management of multiple encoders on the NVR (Network Video Recorder)
- Configuration of encoder settings and integrated management of multiple encoders on the iNEX Basic software (network integration solution)



Video Encoder Connection Diagram



Video Encoder Connection Diagram Using PoE Switch



Types of Cables

	Analog BNC Cable
	LAN Cable (Data + PoE Power)

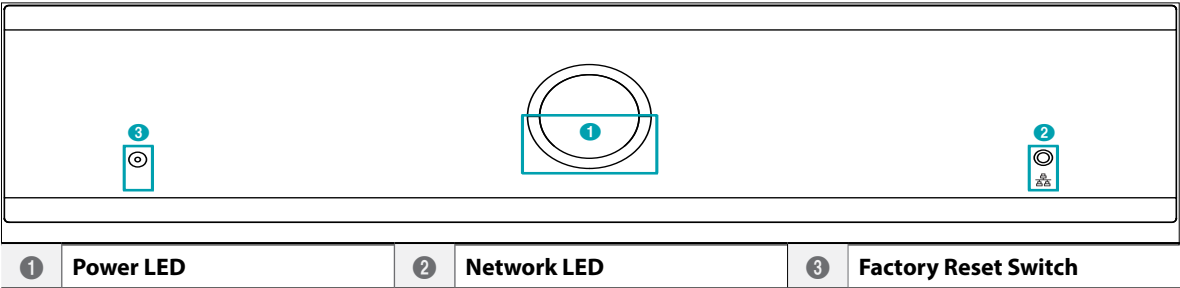
Accessories

Upon unpacking the product, check the contents inside to ensure that all the following contents are included.

- Video Encoder
- User Guide and Instruction Manual (This document)
- Rubber Foot (4ea.)

Overview

Front Panel



1 Power LED

Displays system operating status

2 Network LED

Displays network connection status

LED Status Indications

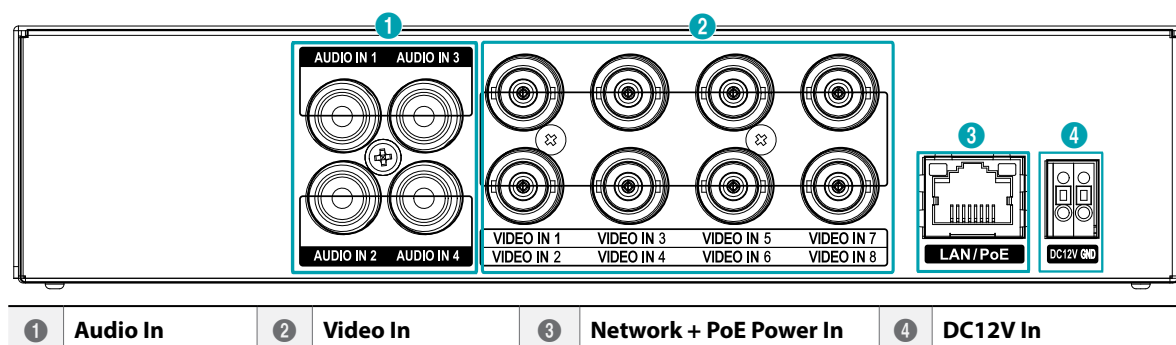
LED	Status	Description
Power LED	Off	No power connection
	Blinking	System booting or upgrading
	On	System operating
Network LED	Off	Network connection errors or no network connection
	Blinking	Data transmission in progress
	On	Normal network connection

3 Factory Reset Switch

Used to return all settings to the original factory settings. Connect the power and poke a straightened paperclip into the factory reset switch hole. Hold the reset switch until the encoder’s front power led blinks. Release the reset switch, and all of the encoder’s settings are now at the original settings it had when it left the factory.

- **Factory Reset during system booting:** All of the encoder's settings are now at the original settings it had when it left the factory.
- **Factory Reset during system operating:** The other settings except for protocol and system log are now at the original settings it had when it left the factory.
- **Factory Reset via the INIT program:** The other settings except for protocol, system log and network settings are now at the original settings it had when it left the factory.
- **Factory Reset via the INIT program(including network settings) :** The other settings except for protocol and system log are now at the original settings it had when it left the factory.

Rear Panel



① Audio In

Connect to an audio source.

② Video In

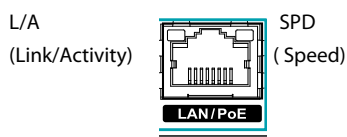
Connect coaxial cables from the video sources.

③ Network + PoE Power In

Connect a Cat5e cable with an RJ-45 jack. The video encoder is capable of connecting to networks via an Ethernet connector and also receives PoE power from the NVR. When the network link is established, the orange LED on the left blinks. When a 1000 BASE-T link is established, the green LED on the right is lit.

☒ Depending on the type and settings of the connected camera, video transmission problems may occur when operating at 10/100 Mbps. Therefore, it is recommended to connect at 1000 Mbps

LED Status Indications



Mode	Status	Color	Description
LA (Link/Activity)	Off	-	No network connection or a problem with the connection
	Blinking	Orange	Data transmission over the network in progress at 10/100/1000Mbps
	On	Orange	Normal network connection at 10/100/1000Mbps
SPD (Speed)	Off	-	Network connection errors or no network connection
	On	Green	Normal network connection at 1000Mbps

④ DC12V In

Connect the two wires of the power adapter to these ports. Be careful not to cross the DC12V and ground (GND) wires. Booting will commence once connected to a power supply.

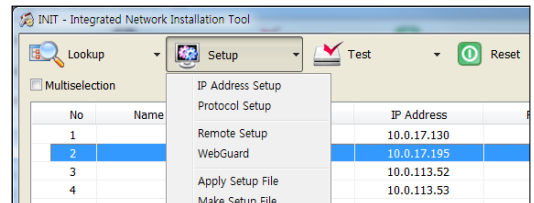
- ☒ • The network connector is not designed to be connected directly with cable or wire intended for outdoor use.
- ☒ • Press down on the button and insert the cable into the opening when you connect power connectors. Release the button and then pull on the cable slightly to ensure it is held securely in place. To disconnect the cable, press down on the button again and pull the cable out.
- ☐ • Ground the power port's ground terminal before use.
- ☐ • Organize the power cable so that it will not cause people to trip over or become damaged from chairs, cabinets, desks, and other objects in the vicinity. Do not run the power cable underneath a rug or carpet.
- ☐ • Do not connect multiple devices to a single power outlet.
- ☐ • Please wire within 3m(118") indoors for stable power supply when installing the adapter.

Part 2 - Remote Setup

Configure basic video encoder settings and all other system settings.



Screen images may vary depending on the model.

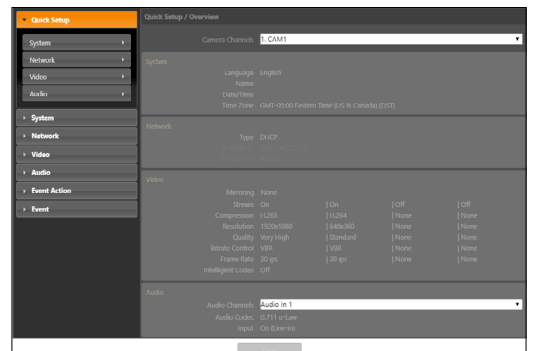


Remote Setup

- 1 Launch the INIT program and then from the main screen, select a video encoder whose settings you wish to change.
- 2 Click on the **Setup** icon.
- 3 Select **Remote Setup** from the **Setup** menu to load the **Remote Setup** screen. Alternatively, you can select **Video Encoder** from the main screen and then right-click to access the **Remote Setup** screen.

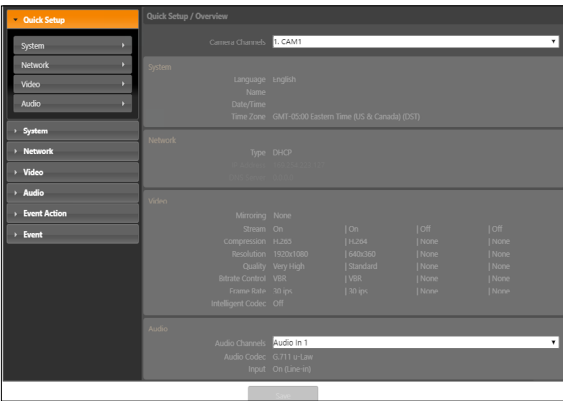


- System settings can also be changed using a remote program.
- Remote Setup works with the following web browsers when the web browsers support HTML5: Microsoft Internet Explorer version 10 or later, Google Chrome, Mozilla Firefox, or Apple Safari. It may not work properly with Microsoft Internet Explorer version 9.0 or earlier. It is recommended that you update the web browser to the latest version. When you launch Remote Setup on a Microsoft Internet Explorer version 10 or later supporting HTML5 and the Remote Setup screen does not appear, check if the web browser's document mode is set to 9 or higher or Edge. You can check the document mode as follows: Press the F12 key on the keyboard → click the Document mode icon.



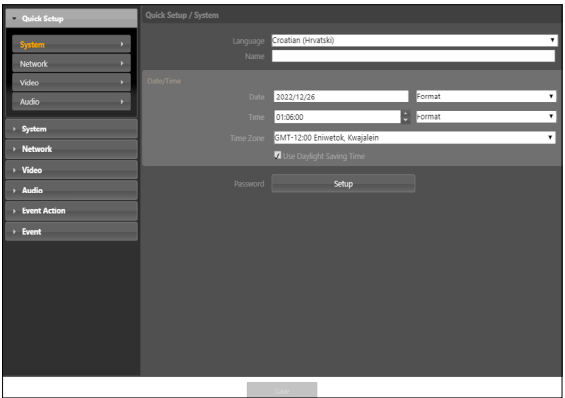
From the Remote Setup screen, select the menu on the left to display the current settings. Select an option under the menu to change the corresponding settings. Once you have changed the settings, click **OK** to apply the settings and exit from the Remote Setup screen.

Quick Setup



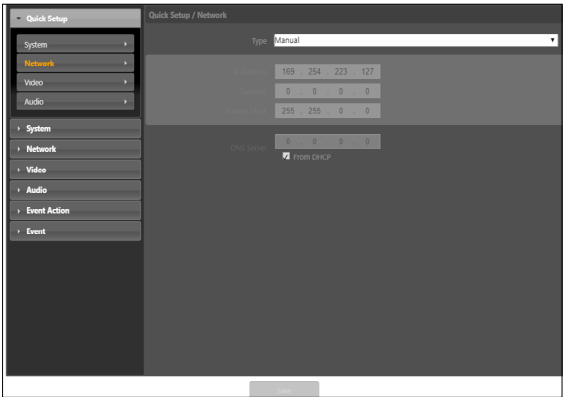
Quick Setup allows you to set up **System**, **Network**, **Video**, **Audio**, and other basic settings needed for video encoder use.

System



Change the video encoder's system information, add users/groups, and/or import/export settings.

General



- **SYSTEM/GENERAL**
 - **Language:** Select the language you wish to use for remote setup.
 - **Name:** Enter a name for the video encoder. (Up to 31 alphanumeric characters, including spaces)
 - **Note:** Enter a description for the video encoder.
 - **Product:** Enter a model name for the encoder.
 - **HW Version:** Indicates the encoder's hardware versions.
 - **SW Version:** Indicates the encoder's software versions.

- **MAC Address:** Indicates the encoder's MAC address.

- **Miscellaneous**

- **Opensource Licenses:** Click **View** to see the information of opensource licenses.

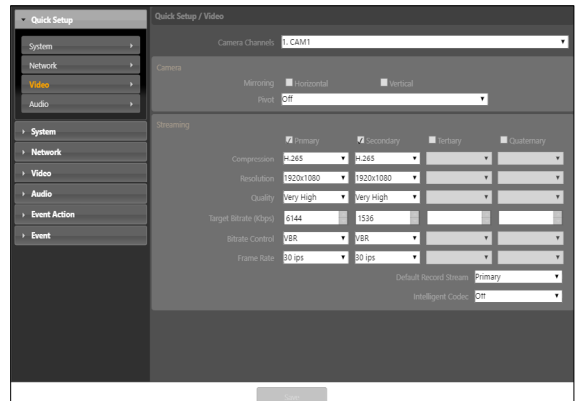
- **Setup**

- **Load Default Setup:** Restores all settings other than Date/Time to their factory defaults. Select Include Network Setup to load default network settings as well. For more information on network setup, refer to the **Network** on page 16.
- **Import Setup:** Open a setup file and apply its settings to the video encoder. Click on the button and then select a setup file. Select Include Network Setup to apply the file's network setup settings (exc. FEN). For more information on network setup, refer to the **Network** on page 16.
- **Export Setup:** Export the current settings as a .dat file. Click on the button and then enter a file name.



- **Load Default Setup** and **Import Setup** options are available only to users belonging to the **Administrator** group.
- When applying the settings of a setup file, do not select the **Include Network Setup** option if the network settings contained in the selected file is currently being used by a different video encoder. Doing so can interfere with establishing a connection with the other video encoder.
- If IP Address, Admin Port, and/or SSL settings have been changed, Remote Setup will terminate after applying the current settings.

Date/Time

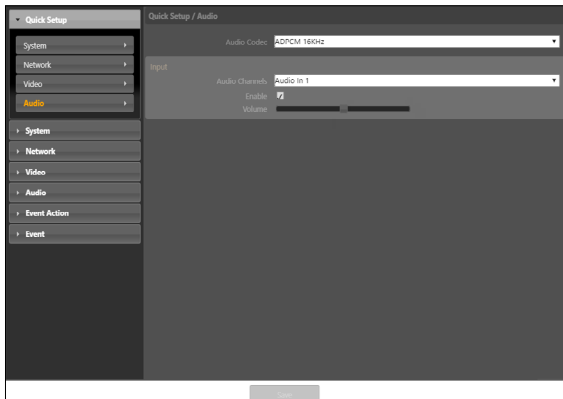


- **Date/Time:** Change the video encoder's date/time settings and display formats and configure the time zone and daylight saving time settings. Click **Apply** to apply the changes right away.
- **Time Sync**
 - **Automatic Sync:** Select to synchronize the system's time with the time server at a specified interval. Enter the time server's IP address or domain name and then specify the interval. If the time server is **FEN-enabled**, select the **Use FEN** option and then enter the time server's name instead of its IP address or domain name.
 - **Run as Server:** Select to run the camera as a time server. Other devices will then be able to synchronize its time setting with this camera's time setting.



If you wish to enter a domain name instead of an IP address for the **Time Server** setting, DNS server must be configured during **Network** setup. If you wish to enter a server name instead of an IP address or a domain name, the **Use FEN** option must be enabled during **Network** setup.

User/Group

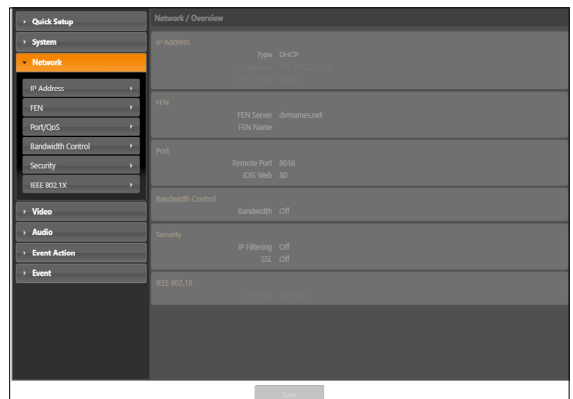


- **User/Group:** Change remote video encoder control permission settings for users and user groups.
 - **Add Group:** Add a new user group. Designate a name for the group and then specify control authorities.
 - **Add User:** Add a new user. Designate a name for the user, select which group to add the user to, and then enter a connection password.
 - **Edit:** Edit group authorities and/or user passwords. Select a group or user and then click on the button.
 - **Remove:** Delete groups or users. Select a group of user you wish to delete and then click on the button.
 - **PTZ Control:** Authority to control PTZ.



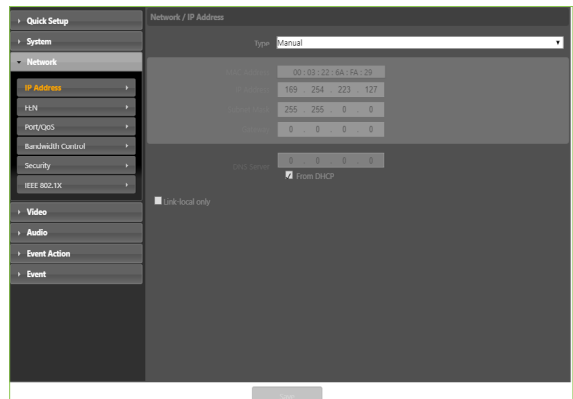
- **User/Group** settings can only be configured by users belonging to the **Administrator** group.
- There is no default password for the **Administrator** group's **admin** user.
- Group authorities that can be assigned are as follows:
 - **Upgrade:** Upgrade the system.
 - **Setup:** Configure the system's settings.
 - **Color Control:** Adjust the camera's brightness, contrast, saturation, and hue settings.
 - **PTZ Control:** Allows you to control the zoom of the lens.
 - **System Check:** View system event status.

Network



Change the network settings, enable FEN and security features.

IP Address



- **Type:** Select the type of network you are using. If this option has been changed, **Remote Setup** will terminate after applying the current settings.
 - **Manual:** Select if using a static IP. You will then be able to configure the related settings manually.
 - **DHCP:** Select if connected to the network using DHCP. Click **OK** to retrieve IP address and other network settings automatically from the DHCP server.

- **DNS Server:** Enter the DNS server's IP address. By using the DNS server, you will be able to use domain names instead of IP addresses when configuring the FEN, time, or SMTP server. If the video encoder is connected to the network via DHCP, select the **From DHCP** option to retrieve the DNS server's IP address from the DHCP server automatically. The updated address will be displayed upon the subsequent connection.
- **Link-local only:** Use only the IP addresses of the link-local IP range. (ex:169.254.x.x)



- Contact your network administrator for more information on the video encoder's network connection type, the DNS server's IP address, and other related information.
- If using DHCP, the video encoder's IP address may change from time to time. We therefore recommend that you use the **FEN** feature.

FEN

Select **Use FEN** to enable the **FEN** feature.

The screenshot shows the 'Network / FEN' configuration window. On the left is a sidebar with a tree view containing 'Quick Setup', 'System', 'Network', 'FEN', 'Port/QoS', 'Bandwidth Control', 'Security', 'IEEE 802.1X', 'Video', 'Audio', 'Event Action', and 'Event'. The 'FEN' option is selected. The main area shows the 'Use FEN' checkbox checked. Below it are three input fields: 'FEN Server' with the value 'domainname.net', 'Port' with the value '10088', and 'FEN Name' which is empty. To the right of the 'FEN Name' field is a 'Check...' button.

- **FEN Server:** Enter the FEN Server's IP address or domain name.
- **Port:** Enter the FEN Server's port number.
- **FEN Name:** Enter a video encoder name you wish to register to the FEN Server. Click **OK** to check the name's availability.

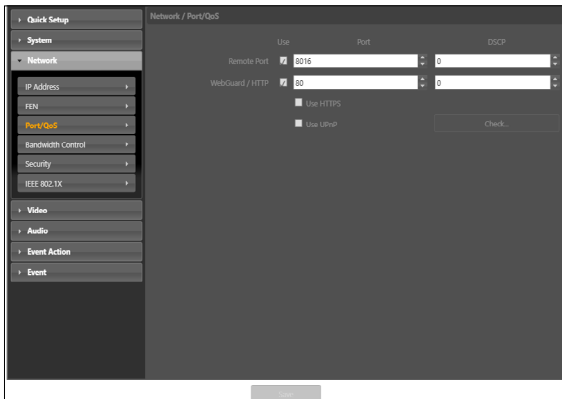


- Use **FEN** is a feature that allows you to register a unique name for a video encoder that utilizes a dynamic IP address to the FEN Server and connect to the video encoder using the registered name instead of an IP address, which can change from time to time. Moreover, you can access the video encoder without having to configure NAT (Network Address Translation) device settings even when the video encoder uses a NAT device. In order to use this feature, you must first register a FEN name to the FEN Server.
- If network settings have been changed, click **OK** at the bottom of the setup window to save the changes and then setup the **FEN**.
- Inquire with your network administrator for the **FEN Server's** IP address or domain name. If a DNS server has been configured under **Network** setup, you can enter the FEN Server's domain name instead of its IP address for the FEN Server setting.
- You will not be able to save **FEN** settings unless you click on the **OK** button next to the **FEN Name** field and check the entered name's availability. In addition, you will be prompted with an error message if you do not enter a FEN name or enter a name already registered to the FEN Server. If the FEN name contains the #, \, and/or % symbol, it might not be able to connect to the video encoder from the WebGuard program.



The FEN Server may go offline without notice for server update purposes or due to an unexpected failure.

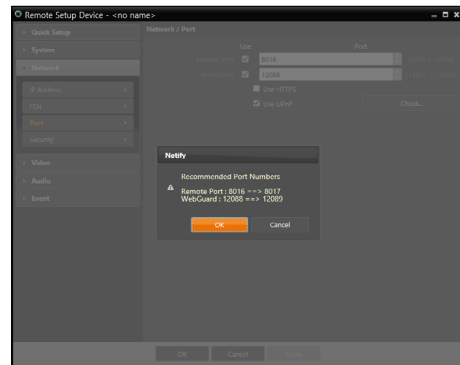
Port/QoS



- **Use/Port:** Enable/disable ports and designate corresponding port numbers. **Remote Port** and **WebGuard / HTTP** ports are enabled by default and cannot be disabled. By enabling WebGuard, you will be able to use the WebGuard program to connect to the encoder. When the HTTP port is enabled, you can run the encoder's Remote Setup. If this option has been changed, click **Save** to apply the current settings, and then restart Remote Setup. If you do not restart Remote Setup, the changes afterwards will not be applied.
- **DSCP:** Designate each port's QoS (Quality of Service) level using DSCP values. Assigning QoS levels prioritizes the ports for network bandwidth use. Higher the DSCP value, higher the QoS level and thus higher on the network bandwidth allocation priority list. Use **0** if you do not want to assign a QoS level. The network environment must support DSCP in order for this feature to function properly. Contact your network administrator for more details.
- **Use HTTPS:** Select this option to apply https protocol-based security on IDIS Web.

- Use **UPnP:** If the video encoder is connected to the network via an IP router (or NAT), select this option to connect to the video encoder without setting up port forwarding. The IP router (or NAT) must be enabled with UPnP in order for this feature to function properly. For more information enabling UPnP on your IP router (or NAT), refer to the **IP router or NAT's operation manual**.

Click **Check** to test the current port settings. A confirmation message will appear if all the selected ports are available for use. If not, a list of recommended port numbers will be shown.



Click **OK** to use the recommended port numbers.



In a WAN environment, it is recommended that you use the UPnP function if you record video by using the FEN function or FEN connection is not smooth. Otherwise, monitoring or recording might not be smooth depending on the network environment.



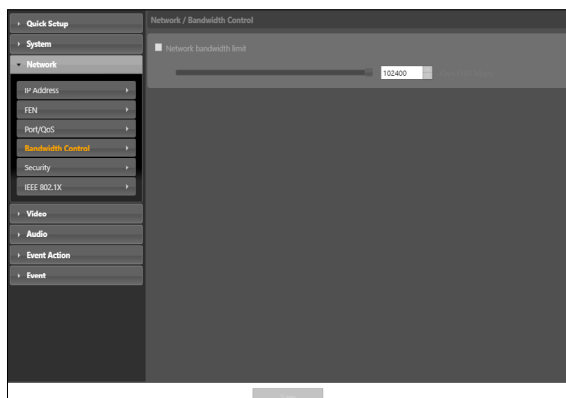
Each port number must be unique.



Port numbers of the remote program must be updated whenever the video encoder's port numbers are changed.

Bandwidth Control

Regulates the network bandwidth use based on network traffic fluctuations.



Select **Network Bandwidth limit** and then specify the maximum bandwidth. The device will not be able to use more than the specified limit in the event of network traffic.

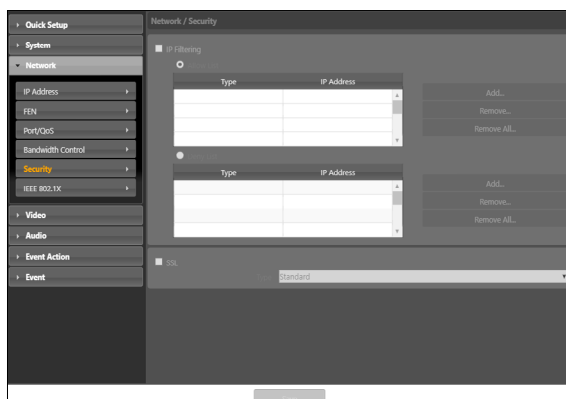


It may not be possible to produce the frame rate specified under **Video > Streaming** if a network bandwidth limit has been set.

a time. Select the **Group** option to define a range of IP addresses you wish to add.

- **Remove/Remove All:** Remove individual or all IP addresses from Allow List or Deny List.
- **SSL:** Select this option to enable SSL (Secure Sockets Layer). Enabling this option applies SSL protocol protection on data transmitted out. However, programs and systems that do not support SSL will not be able to connect to the camera. If this option has been changed, Remote Setup will terminate after applying the current settings.
- Time server, FEN Server, and SMTP server's IP addresses must be added to Allow List under **IP Filtering** in order to use Time Sync, FEN, and Send Email features. No connection to the encoder will be permitted whatsoever from IP addresses added to **Deny List**.
- Enabling the **SSL** option may place a greater load on the external system, depending on the level of security being used.
- This product contains software developed by Open SSL Project for use in Open SSL Toolkit. (<http://www.openssl.org/>)

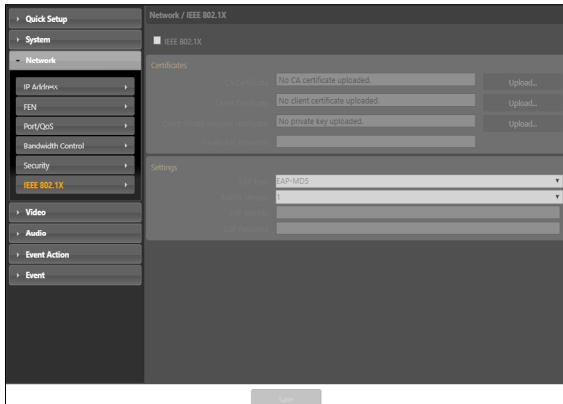
Security



- **IP Filtering:** Select this option to enable IP Filtering. IP Filtering allows encoder access from certain IP addresses and blocks access from others.
 - **Add:** Add new IP addresses to Allow List or Deny List. Select the **Host** option to add one IP address at

IEEE 802.1X

Select the **IEEE 802.1X** option to enable IEEE 802.1X network connection authentication.

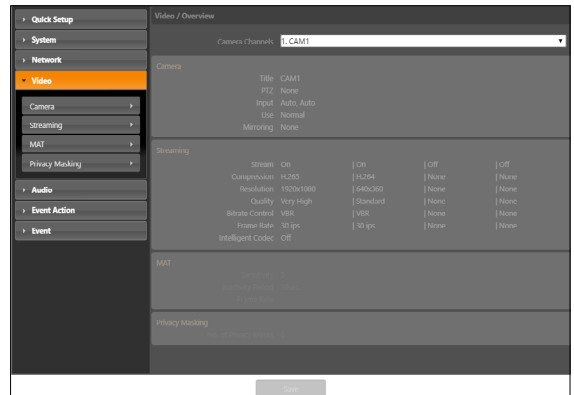


- **Certificates:** Upload a certificate or a private key. You may be prompted to enter a password for the private key.
- **Settings:** Configure EAP (Extensible Authentication Protocol) settings.
 - **EAP Type:** Choose a network connection authentication method. Selected method must be identical to the authentication method used on the authentication server.
 - **EAPOL Version:** Choose EAP authentication's version.
 - **EAP Identity/EAP Password:** Enter authentication ID and password.



The authentication server and AP must support IEEE 802.1X authentication in order for the IEEE 802.1X network connection authentication feature to function properly.

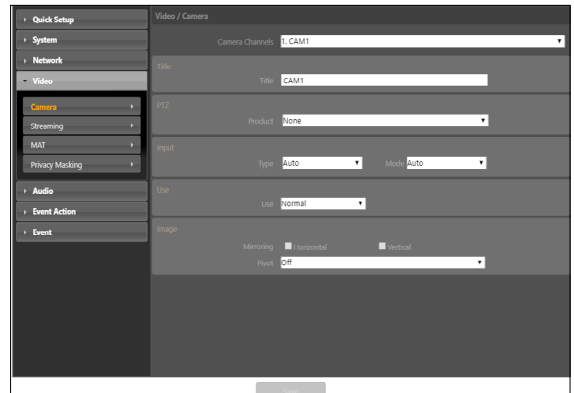
Video



Configure **Encoder**, **Streaming** and **Privacy Masking** options.

Camera

Configure **Camera Title**, **Image**, **Camera Mode** and **Use Setup** settings.



- **Camera Title:** Edit the camera's name.
- **PTZ:** Move the PTZ camera left/right/up/down (Pan and Tilt).
 - **Product:** Select the PTZ camera.
- **Image :** Configure Image Sensor settings.
 - **Mirroring:** Select Horizontal Reverse or Vertical



PTZ works only with HD, Full HD, 3M, 4M, and 5M cameras supporting the UTC PTZ function and UTC may not work properly depending on the type of camera.

Reverse to flip the image horizontally or vertically.

- **Pivot:** Select a direction to rotate images 90 degrees clockwise or counterclockwise. If both Mirroring and Pivot functions are enabled, Mirroring functions first, then Pivot.
- **Input:** Configure the input method and resolution setting of the camera connected to the video encoder.
- **Type:** Choose the camera input method.
- **Mode:** Choose the camera resolution.
- **Use:** Use this feature to assign **Covert Camera View** permissions.

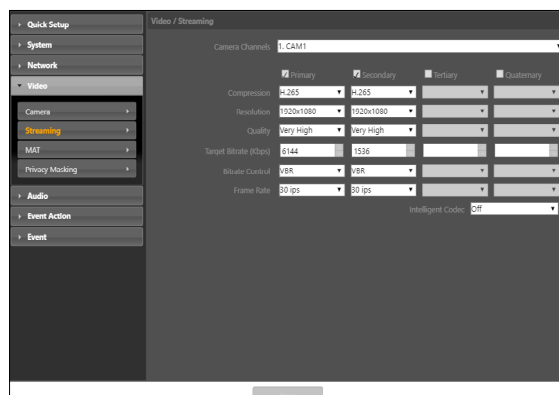
Navigate to **Camera Setup > General** and designate cameras as **Covert 1** or **Covert 2**.

- **Covert 1:** Hides images from the camera in Live mode but does indicate the camera's title and status via icons.
- **Covert 2:** The camera is indicated as being inactive. Images from the camera are not shown. Camera title and status icons are not shown.



Users that have a cover **Covert Camera View** are able to view both images from and status icons for all **Covert 1** and **Covert 2** cameras.

Streaming



- **Camera Channels:** Select which cameras to apply the streaming to.
- **Primary, Secondary, Tertiary, Quaternary:** Multistreaming is supported. (priority: Primary > Secondary > Tertiary > Quaternary). Enable/disable streaming use. The lower stream settings may change depending on higher stream settings. The tertiary stream and the quaternary stream may not be able to use a resolution and frame rate settings depending on higher stream settings (refer to the table below).

Primary		Secondary		Tertiary		Quaternary	
Resolution	ips	Resolution	ips	Resolution	ips	Resolution	ips
720x480 (NTSC)	30	720x480 (NTSC)	30	640x360 (NTSC)	1	360x240 (NTSC)	1
720x576 (PAL)	25	720x576 (PAL)	25				

- **Compression:** Choose the streaming compression method.
- **Resolution:** Choose a resolution setting for video streaming.
- **Quality:** Choose a quality setting for video streaming.
- **Bitrate Control:** Choose a bitrate control mode for H.264 compression.
 - **VBR (Variable Bitrate):** Bitrate varies depending on motion changes in the video. Less movement places less load on the network and takes up less storage space.

Frame Rate: Choose a frame rate setting for video streaming.

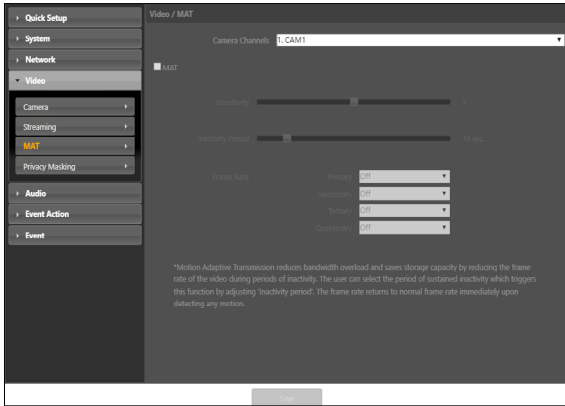


If multiple users are connected to the encoder, the increase in bandwidth use can lower the frame rate.

- **Intelligent Codec:** Lower bitrate by using the intelligent codec

MAT

Select the **MAT** option to use the MAT (Motion Adaptive Transmission) feature during video transmission and recording.

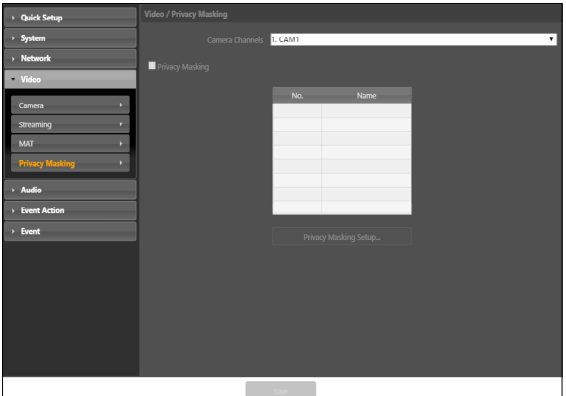


- **Sensitivity:** Set the motion detection sensitivity. Higher values will result in more sensitive motion detection.
- **Inactivity Period:** Set the Inactivity Period. If motion is not detected for the duration of time specified, video is transmitted and recorded using the frame rate designated below until movement is detected again.
- **Frame Rate:** Designate the frame rate to be used between the end of the Inactivity Period and the next motion detection. Video is transmitted and recorded at the designated frame rate between then end of the Inactivity Period and the next motion detection. Once motion is detected again, the frame rate designated under **Streaming** is restored immediately.

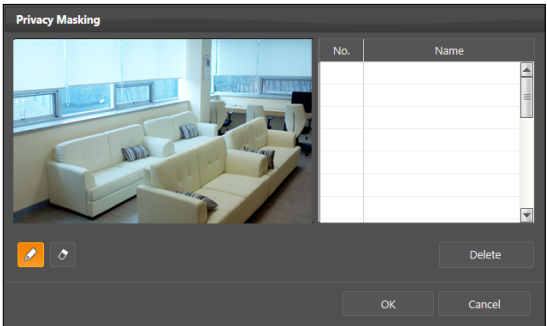
☒ **MAT (Motion Adaptive Transmission)** is a feature that lowers the frame rate when motion is not detected to reduce the load on the network and save on storage space. Based on the specified sensitivity setting, no movement will be assumed if there is no change between two consecutive images.

Privacy Masking

Select **Privacy Masking** to set up a privacy mask over a specific area. The section on which a privacy mask is applied will appear as black when monitoring video.



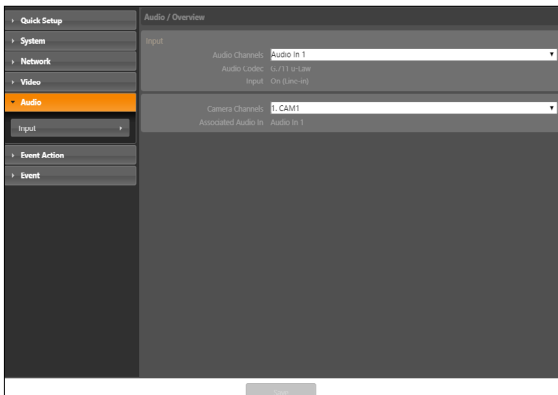
- **Camera Channels:** Select which cameras to apply the privacy masking to.
- **Privacy Masking Setup:** Set up privacy masks. (Up to 16)



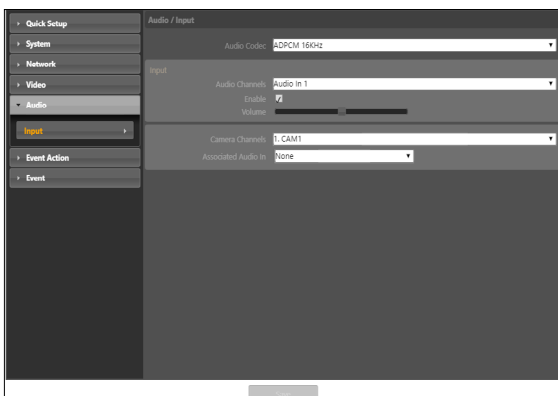
- **(Select)/(Unselect):** Set or remove a privacy mask. Click on the button and drag & drop using the mouse to set up a privacy mask.
- **No./Name:** Displays a list of active privacy masks. The numbers indicate privacy mask numbers. Select the empty space next to a number to assign a name to the corresponding privacy mask. Click **Delete** to remove the selected privacy mask.

Audio

Configure audio in settings.



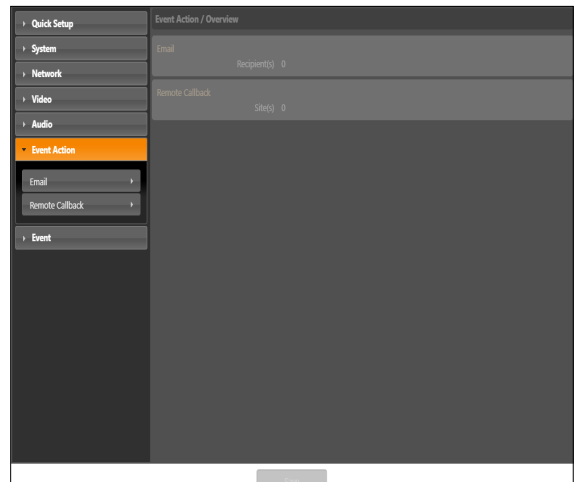
Input



- **Audio Codec:** Select an audio codec.
- **Input:** Click **Enable** option and control the volume.
- **Camera Channels:** Select which cameras to apply the the input to.
- **Associated Audio In:** Select an associated audio in.

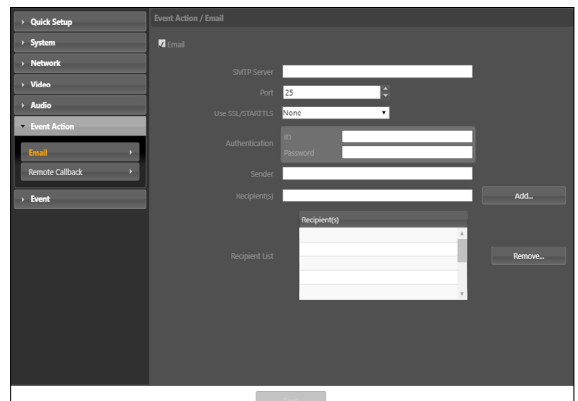
Event Action

Designate event detection alert actions.



Email

Select **Email** to send out emails.



- **SMTP Server/Port:** Enter the SMTP server's IP address (or domain name) and port number you received from the network administrator. If a DNS server has been set up during network configuration, you can enter a domain name instead of an IP address.
- **Use SSL/STARTTLS:** If using an SMTP server requiring an SSL or STARTTLS connection, select **SSL** or **STARTTLS** option.
- **Authentication:** Enter a user ID and password if user authentication is required by the SMTP server.
- **Sender/Recipient(s):** Enter the sender and recipients' addresses. (Up to 10) The addresses must be properly formatted and include the @ symbol.

Remote Callback

Select **Remote Callback** to send callback messages to a remote system.



- Not supported from the IDIS Web program.
- The encoder must be registered to the remote system in order to use the **Remote Callback** feature.

- **IP Address:** Enter the IP address and port number of the remote system that will receive the messages.
- **Retry:** Designate how many reattempts to make if message delivery fails.

Event

Configure event detection settings.

Motion Detection

Select **Motion Detection** to configure motion detection event settings. With motion detection event enabled, motion detections within the designated area will be assumed as events.

- **Camera Channels:** Select which cameras to apply the motion detection to.
- **Sensitivity:** Select daytime and nighttime motion detection sensitivity levels. Higher values will result in more sensitive motion detection.
- **Minimum Blocks for Detection:** Select minimum blocks for daytime and nighttime motion detection. Motion must take place over the selected number of blocks in order for it to be considered as a motion detection event.
- **Motion Zone:** Click **Setup** and define the motion zone using blocks.
 - **(Select)** / **(Unselect):** Enable/disable motion detection.
 - **(Single Block):** Select/unselect motion detection blocks individually.
 - **(Zone):** Select/unselect multiple motion detection blocks.
 - **(All):** Select/unselect all motion detection blocks.
- **Motion Ignoring Interval:** With Motion Ignoring Interval configured, no event log or notification is generated for motions detected during a period of time following a motion detection event.
- **Daytime:** Specify when daytime starts and ends. All other times will be assumed as nighttime.
- **Event Action:** Select a motion detection event alert action.
 - **Send Email:** Select if you wish to send an email.

Select the **Image Attachment** option to attach a .jpg image of the event detected to the email.

- **Remote Callback:** Select this option to send a message to a remote system and then select which system to send the message to.



- The encoder must be registered to the remote system in order to use the **Remote Callback** feature.

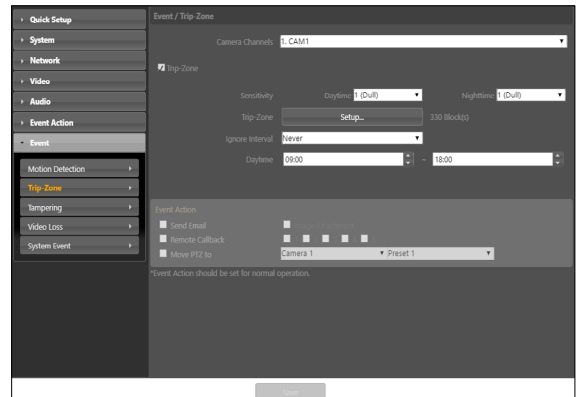
- **Move PTZ to:** Select a preset position to move the pan/tilt/zoom driver to that position. Preset positions can be set from the remote program.



- **Event Action** settings must be configured correctly in order to perform event actions.

Trip-Zone

Select **Trip-Zone** to configure trip zone event settings. With trip zone event enabled, motion detected inside/outside the selected area will be assumed as an event.



- **Sensitivity:** Select daytime and nighttime motion detection sensitivity levels. Higher values will result in more sensitive motion detection.
- **Trip-Zone:** Click **Setup** and define the trip zone using blocks.
 - **(Select)** / **(Unselect):** Enable/disable motion detection.
 - **(Single Block):** Select/unselect motion detection blocks individually.
 - **(Zone):** Select/unselect multiple motion detection blocks.
 - **(All):** Select/unselect all motion detection blocks.
- **Trip Direction:** Define in which direction the motion has to occur in order for it to be considered as an event. Select **In** for movement occurring from outside the trip zone in and **Out** for movement occurring from inside the trip zone out.
- **Motion Ignoring Interval:** With Motion Ignoring Interval configured, no event log or notification is generated for motions detected during a period of time following a motion detection event.
- **Daytime:** Specify when daytime starts and ends. All other times will be assumed as nighttime.
- **Event Action:** Select a trip zone event alert action.
 - **Send Email:** Select if you wish to send an email. Select the **Image Attachment** option to attach a .jpg image of the event detected to the email.
 - **Remote Callback:** Select this option to send a message to a remote system and then select which system to send the message to.



- The encoder must be registered to the remote system in order to use the **Remote Callback** feature.

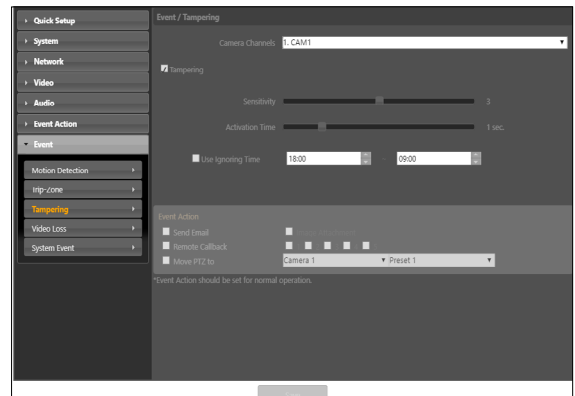
- **Move PTZ to:** Select a preset position to move the pan/tilt/zoom driver to that position. Preset positions can be set from the remote program.



- **Event Action** settings must be configured correctly in order to perform event actions.

Tampering

Select **Tampering** to configure tampering detection event settings. With tampering detection event enabled, a sudden change in the video, such as due to movement of the camera or covering up of the lens, will be assumed as an event.



- **Camera Channels:** Select which cameras to apply the tampering to.
- **Sensitivity:** Define the tampering detection sensitivity. Higher values will result in more sensitive detection.
- **Activation time:** Specify how long tampering has to be detected for it to be considered as an event. Tampering detections that do not last for the specified duration of time will not be considered as events.
- **Event Action:** Select a tampering detection event alert action.
 - **Send Email:** Select if you wish to send an email. Select the **Image Attachment** option to attach a .jpg image of the event detected to the email.
 - **Remote Callback:** Select this option to send a message to a remote system and then select which system to send the message to.



- The encoder must be registered to the remote system in order to use the **Remote Callback** feature.

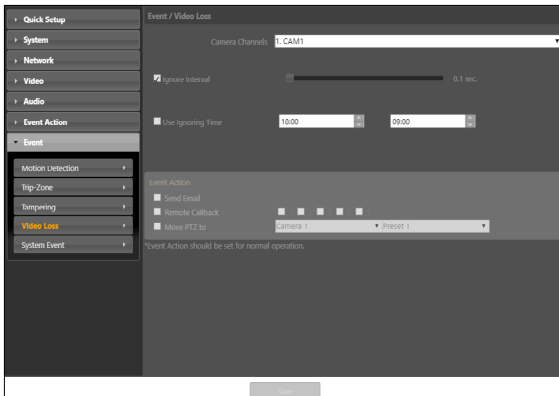
- **Move PTZ to:** Select a preset position to move the pan/tilt/zoom driver to that position. Preset positions can be set from the remote program.



- **Event Action** settings must be configured correctly in order to perform event actions.

Video Loss

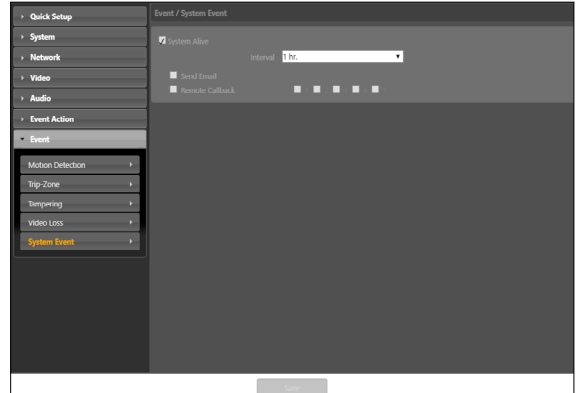
Select **Video Loss** to configure video loss event settings. With video loss event enabled, video loss will be assumed as an event.



- **Camera Channels:** Select which cameras to apply the video loss to.
- **Ignore interval:** With Ignore interval configured, no event log or notification is generated for video loss taking place during a period of time following a video loss event.
- **Use Ignoring Time:** Define the event ignoring time. Video loss taking place during the defined time range will not be assumed as events.
- **Event Action:** Select a video loss event alert action.
 - **Send Email:** Select to send an email.
 - **Remote Callback:** Select this option to send a message to a remote system and then select which system to send the message to.
 - ✓ • The encoder must be registered to the remote system in order to use the **Remote Callback** feature.
 - **Move PTZ to:** Select a preset position to move the pan/tilt/zoom driver to that position. Preset positions can be set from the remote program.
- ✓ **Event Action** settings must be configured correctly in order to perform event actions.

System Event

Select **System Event** and configure system event settings. With system event enabled, system status will be checked periodically and corresponding alerts will be generated.



- **System Alive:** Select to check the system status and then set up a schedule.
 - **Send Email:** Select to send out an email when the system comes on line.
 - **Remote Callback:** Select this option to send a message to a remote system when the system comes on line and then select which system to send the message to.
- ✓ • **Email** and **Remote Callback** settings under **Event Action** must be configured correctly in order to send out emails and messages.
- The encoder must be registered to the remote system in order to use the **Remote Callback** feature.

Part 3 - WebGuard

WebGuard is a program that allows you to view and search video from remote locations over the Internet and can be accessed on a Microsoft Internet Explorer.

System requirements for running WebGuard are as follows:

- OS: Microsoft® Windows® 7 (Home Premium, Professional, Ultimate), Microsoft® Windows® 8 (Pro, Enterprise), Microsoft® Windows® 10 (Pro, Home), Microsoft® Windows® 11
- CPU: Intel Pentium IV 2.4GHz or above (Core 2 Duo E4600 recommended)
- RAM: 1GB or more
- VGA: 128MB or more (1280x1024, 24bpp or above)
- Internet Explorer: Version 10 or later 32-bit
- Chrome: Google Chrome 22.0.1229.0 or above (59.xxx or above recommended)
- Edge: 98.0.1108.43 or above

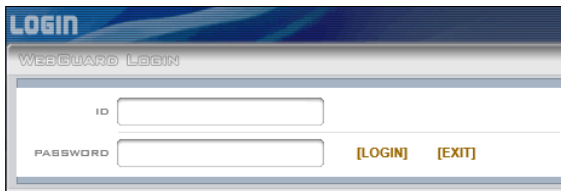
1 Launch the web browser and then enter the following information in the address bar.

- http://IP Address:Port Number (WebGuard connection port number selected during video encoder IP address and port number setup)
- Or http://FEN Server Address/FEN name (FEN Server address and FEN name registered to the FEN Server)



- If the Use HTTPS option has been selected during WebGuard port number setup, enter https instead of http. If prompted with a security certificate warning, select "Continue to this website (not recommended)." If the WebGuard login page fails to load, configure Internet Explorer's settings as follows:
 - Tools → Internet Options → Security → Custom Level... → Medium-high (default) or Medium.
 - Tools → Internet Options → Advanced → Security → Use TLS 1.0 (select)
- If connecting by entering an IP address and a port number, you can connect by entering just the IP address if WebGuard connection port number has been set to 80 (443 when entering https).
- Contact your network administrator for the IP address of the video encoder you wish to connect to the the WebGuard port number.

2 When prompted with the WebGuard login window, enter the ID and password and click **LOGIN**.

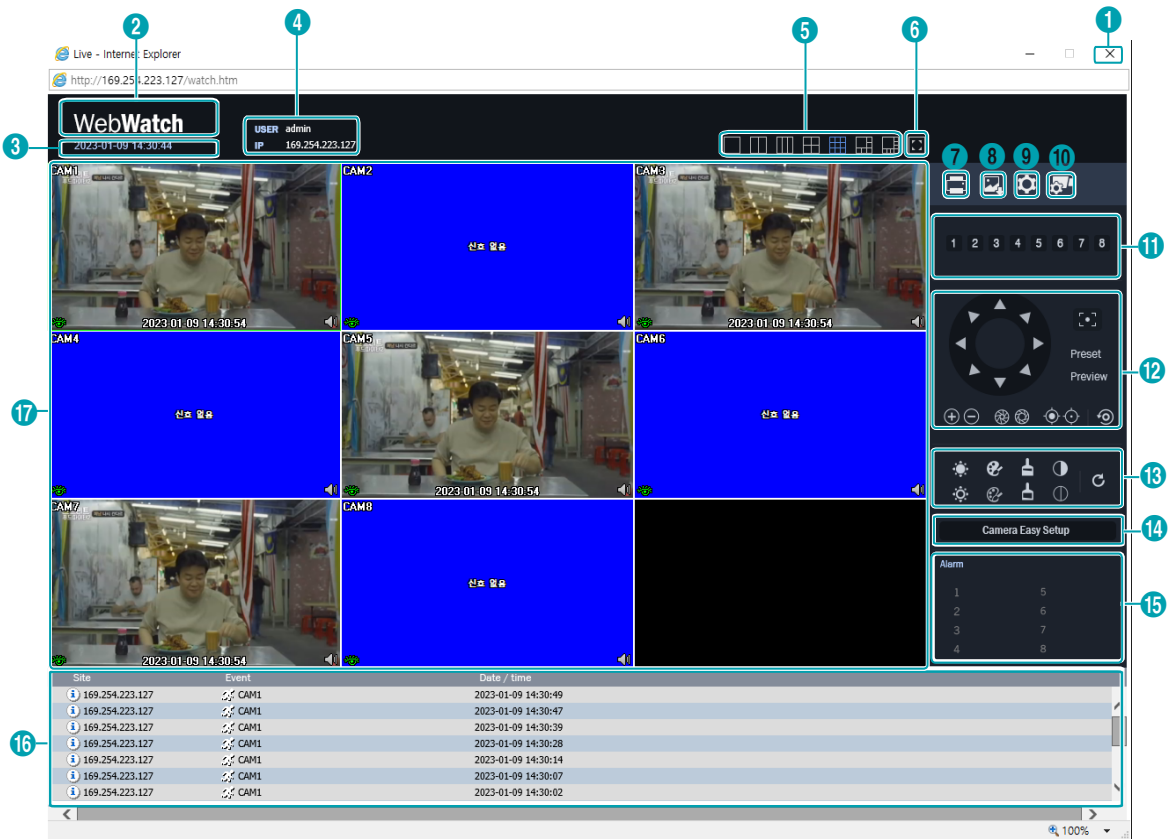
A screenshot of the WebGuard login window. The window has a blue header with the word "LOGIN" in white. Below the header, the text "WEBGUARD LOGIN" is displayed. The main area contains two input fields: "ID" and "PASSWORD". To the right of the "PASSWORD" field are two buttons labeled "[LOGIN]" and "[EXIT]".



- Do not close the login window while WebGuard is running. Switching over to Web Live or Web Search mode can cause a script error, requiring you to restart the WebGuard program.
- If running WebGuard on Internet Explorer 7.0, the bottom section of the screen may get cut off if the address bar or the status bar is shown. In this case, change Internet Options so that the address bar or the status bar is hidden. (**Tools → Internet Options → Security → Custom level... → Allow websites to open windows without address or status bars (Enable)**)
- To use WebGuard on Microsoft Windows Vista or above, launch Internet Explorer by right-clicking on the icon and selecting the **Run as administrator** option. Otherwise, certain WebGuard functions might not be available.
- Launching a new version of WebGuard for the first time can cause Internet Explorer to load information from the previous version. In this case, navigate to **Tools → Internet Options → General**, delete temporary Internet files, and then restart WebGuard.
- On Microsoft Windows Vista or above, lowered image transmission rate can prevent the screen from being displayed or updated. In this case, we recommend that you disable the computer's auto tuning function. Open the command prompt as an administrator. (**Start → Accessories → Command Prompt → Right-Click** and then select **Run as administrator**) Type in "**netsh int tcp set global autotuninglevel=disable**" and then press Enter. Restart the computer to apply the change. To enable auto tuning again, launch the command prompt as an administrator and then type in "**netsh int tcp set global autotuninglevel=normal**". Restart the computer to apply the change.

Web Live Mode

A remote web monitoring program that allows you to monitor images from remote locales in real-time.



1	Press ✕ to terminate WebGuard.
2	Place the mouse pointer on the WebWatch logo to check WebGuard's version.
3	Displays the current time..
4	Displays login information of Webguard.
6	Select the desired mode. Changing the mode places the selected camera in the first cell of the layout that will be changed.
6	View the video in full screen. Press the ESC key on the keyboard to return to the previous screen.
7	Print the current video screen using a printer connected to the computer.
8	Save the current video screen as an image file.
9	Configure rendering mode and OSD settings. Select rendering mode to adjust the video output rate or select which OSD elements to display on the screen from the OSD list.
10	Load the encoder setup window.
11	Indicates the camera's number.

12	<p>Used to control a PTZ at a remote location.</p> <ul style="list-style-type: none"> One push button<ul style="list-style-type: none">Press this button to find the optimum focus automatically.It is recommended to get an approximate focus using the manual focusing button before pressing the one push button for fast and efficient focusing.This button is not supported in the Onvif protocol. Zoom buttons / Focusing buttons <div><input checked="" type="checkbox"/> May not be supported depending on the model.</div>								
13	Adjust live video quality.								
14	<p>Configure camera easy setup. Select from presets or custom setup for the video mode according to daytime/nighttime.</p> <p>- Preset: Select from Natural, Vivid or De Noise / - User Custom: Manually configure the values of each setting (Sharpness, Contrast, Colors and Brightness).</p>								
15	Control the alarm out device connected to the encoder.								
16	<p>Event status window at the bottom of the screen displays a list of events detected at remote locales.</p> <table><tr><td></td><td>Motion Detection</td><td></td><td>Tampering</td></tr><tr><td></td><td>Video Loss</td><td></td><td>Tripzone</td></tr></table>		Motion Detection		Tampering		Video Loss		Tripzone
	Motion Detection		Tampering						
	Video Loss		Tripzone						
17	<p>Right-click on the screen to display the pop-up menu.</p> <ul style="list-style-type: none">Change Camera Title: Used to change the encoder's name. <div><input checked="" type="checkbox"/> Renaming the encoder in Web Live mode does not affect the encoder's name on the remote system. If no name is entered for the encoder, the name used at the remote locale is shown on the screen.</div> <div><div>Change Camera Title</div><div>Enable Audio</div><div>Aspect Ratio ▶</div><div>MultiStream ▶</div><div>Anti-Aliasing Screen</div></div> <ul style="list-style-type: none">Enable Audio: Enables audio transmission from remote locales. Select to display buttons. <table><tr><td></td><td>Enables playback of audio from the remote locale on speakers.</td></tr><tr><td></td><td>Enables audio communication from the remote locale.</td></tr><tr><td></td><td>Disables audio transmission.</td></tr></table> <div><input checked="" type="checkbox"/> If the remote locale connected to supports audio transmission, icon appears on the corresponding encoder screen.</div> <ul style="list-style-type: none">Aspect Ratio: Change the aspect ratio of the video displayed on the screen.<ul style="list-style-type: none">Fit to Screen: Fit the video to the size of the encoder screen.Fit to Aspect Ratio: Resizes camera screen to original aspect ratio of the video.Half Size (x0.5) - 4 Times Bigger (x4): Displays the encoder videos in the selected size based on the original size of the video. For example, original size (x1) displays the video in its original size. Half size (x0.5) through 4 times larger (x4) options are only available if there is enough space on the encoder screen to accommodate the selected size.MultiStream: If the encoder is running on multi-stream mode, you can choose between the streams.Anti-Aliasing Screen: Removes stair step effect (blocks) that are caused when zooming a video to improve overall quality of video output.		Enables playback of audio from the remote locale on speakers.		Enables audio communication from the remote locale.		Disables audio transmission.		
	Enables playback of audio from the remote locale on speakers.								
	Enables audio communication from the remote locale.								
	Disables audio transmission.								

Part 4 - Appendix

Troubleshooting

Problem	Check
Power LED will not turn on	<ul style="list-style-type: none">• Check the LAN cable.• Check that the power cable is connected or the power supply status of the PSE device to which the LAN cable is connected.
The system is unable to recognize network interface	<ul style="list-style-type: none">• Check the LAN cable.• Check the network LED.

Specifications

Video	Input	8 BNC
	Compression	H.264, H.265
	Resolution	2560x1920, 2560x1440, 1920x1536, 1920x1080, 1280x720, 960x576, 960x480, 960x288, 960x240, 720x576, 720x480, 720x288, 720x240, 704x480, 640x360, 480x288, 480x240, 352x288, 352x240
	Bitrate Control	VBR, CBR
	Frame Rate	(Channel) 10ips@5MP, 15ips@4M, 18ips@3M, 30ips@FHD/HD/960/720
Inputs/Outputs	Audio Input	4 RCA
	Ethernet	10M/100M/1000Mbps
	DC12V Input	Terminal Blocks
	LED	Power(Status), Network
	Button/Switch	Reset
Environmental Conditions	Operating Temperature	32°F to 104°F (0°C ~ 40°C)
	Operating Humidity	0% ~ 90%
General	Dimensions (W x H x D)	7.9" x 1.7" x 6.5" (200mm x 44mm x 164.2mm)
	Unit Weight	1.8 lbs. (0.82kg)
	Power Source	12V $\overline{\text{---}}$, PoE
	Power Consumption	12V $\overline{\text{---}}$, 0.8A, 10W PoE, IEEE 802.3af(Class 3), 10W
	Approval	FCC, CE, KC



These product specifications may change without prior notice.

COSTAR

COSTAR VIDEO SYSTEMS

101 Wrangler Drive, Suite 201 Coppell, Texas 75019

Phone: (469) 635-6800 Fax: (469) 635-6822

Toll-free: (888) 694-7827