IDIS®

Network Camera

Operation Manual

DC-D4212R

Powered by Direct IP®

Before reading this manual

This is a basic operation manual for use of an IDIS network camera. 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 manual.
- The information in this document is believed to be accurate as of the date of publication even though explanation about some functions may not be incorporated. The manufacturer is 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.
- It is recommended that first-time users of this network camera 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 Symbols

Symbol	Publication	Description
⎓	**IEC60417, No.5031**	Direct current

In-Text

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

Safety Precautions

WARNING

RISK OF ELECTRIC SHOCK

DO NOT OPEN

WARNING: TO REDUCE THE RISK OF ELECTRIC SHOCK,

DO NOT REMOVE COVER (OR BACK).

NO USER-SERVICEABLE PARTS INSIDE.

REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.

Important Safeguards

1. Read Instructions

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

2. Retain Instructions

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

3. Cleaning

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

4. Attachments

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

5. Water and/or Moisture

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

6. Placing and Accessories

Do not place this equipment on an 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.

Do not place this equipment in an enclosed space. Sufficient ventilation is required to prevent an increase in ambient temperature which can cause malfunction or the risk of fire.

7. Power Sources

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

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.

This equipment should be remain readily operable.

8. Power Cord

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

9. Lightning

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

10. Overloading

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

11. Objects and Liquids

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

12. Servicing

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

13. Damage requiring Service

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

A. When the power-supply cord or the plug has been damaged.
B. If liquid is spilled, or objects have 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.

14. Replacement Parts

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

15. Safety Check

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

16. Field Installation

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

17.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.

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

© 2019 IDIS Co., Ltd.
IDIS Co., Ltd. reserves all rights concerning this manual.
Use or duplication of this manual in part or whole without the prior consent of IDIS Co., Ltd. is strictly prohibited.
Contents of this manual are subject to change without prior notice for reasons such as functionality enhancements.

Registered Trademarks

IDIS is a registered trademark of IDIS Co., Ltd.
Other company and product names are registered trademarks of their respective owners.

This product contains software built partially on open-source content. Codes for the corresponding open-source content are available for download depending on whether or not the source is publicly available under a 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.oepnssl.org/). Also, this product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

Table of Contents

1

Part 1 - Remote Setup 7

Remote Setup 7
Quick Setup 8
System 8
General 9
Date/Time 10
User/Group 10
Network 11
IP Address 11
FEN 13
Port/QoS 14
Bandwidth Control 15
Security 16
IEEE 802.1X 17
Video 17
Camera 18
Streaming 21
Webcasting 23
MAT 24
Privacy Masking 25
Event Action 25
Email 26
Remote Callback 26
FTP Upload 27
Event 28
Motion Detection 29
Trip-Zone 30
Tampering 31
System Event 32

2 **Part 2 - IDIS Web 33**

Web Live Mode 35

3 **Part 3 - Appendix 37**

Setup Menu Tree (Remote Setup) 37

Index 38

Part 1 - Remote Setup

Configure basic network camera settings and all other system settings.

Screen images may vary depending on the model.

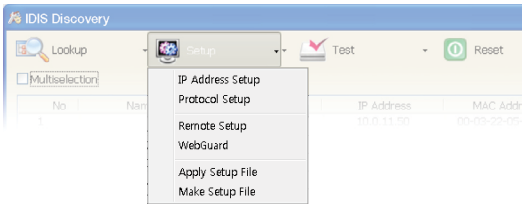
Remote Setup

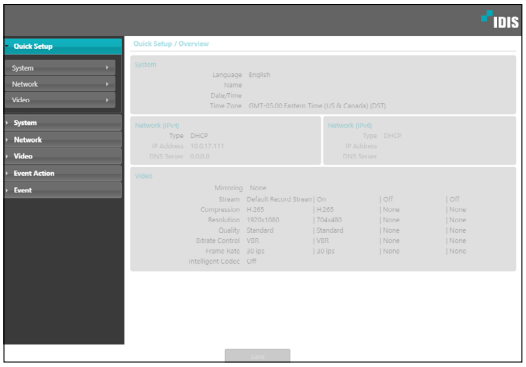
1 Launch the IDIS Discovery program and then from the main screen, select a network camera whose settings you wish to change.

2 Click on the **Setup** icon.

3 Select **Remote Setup** from the **Setup** menu to load the **Remote Setup** screen. Alternatively, you can select **Network Camera** from the main screen and then right-click to access the **Remote Setup** screen.

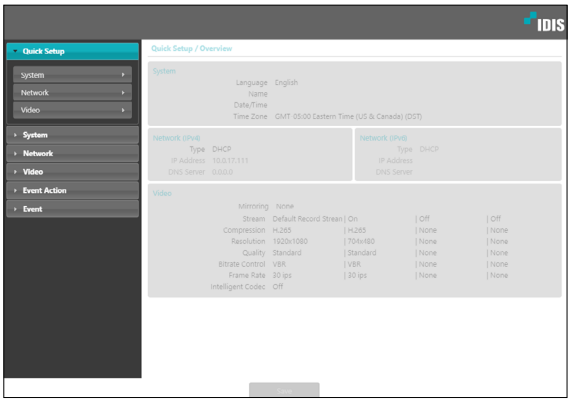
- System settings can also be changed using a remote program.
- Remote Setup works with the following web browsers when the web browsers support HTML5: Microsoft Internet Explorer version 10 or later, Google Chrome, Mozilla Firefox, or Apple Safari. It may not work properly with Microsoft Internet Explorer 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.





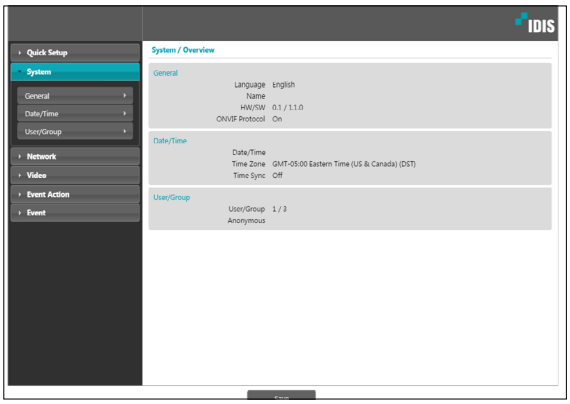
From the Remote Setup screen, select the menu on the left to display the current settings. Select an option under the menu to change the corresponding settings. Once you have changed the settings, click **Save** to apply the settings.

Quick Setup



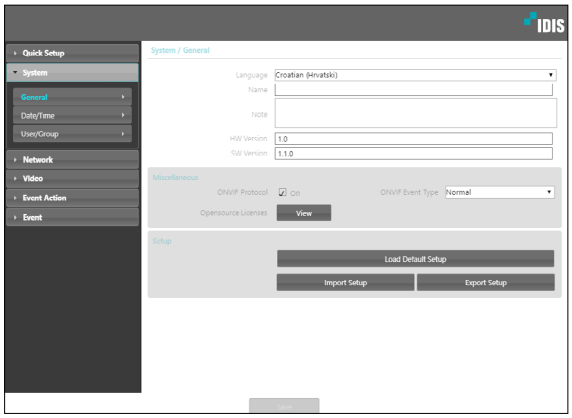
Quick Setup allows you to set up **System**, **Network**, **Video**, and other basic settings needed for camera use.

System



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

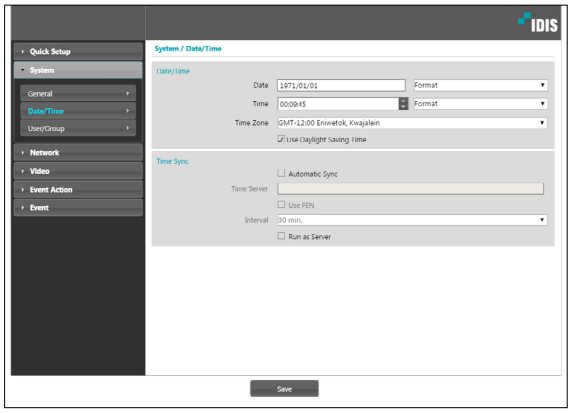
General



- **Language**: Select the language you wish to use for remote setup.
- **Name**: Enter a name for the camera. (Up to 31 alphanumeric characters, including spaces)
- **Note**: Enter a description for the camera.
- **HW Version/SW Version**: Indicates the camera's hardware and software versions.
- **Miscellaneous**
  - **ONVIF Protocol**: Select to enable ONVIF protocol use. However, ONVIF Protocol is available only to users belonging to the standard user groups (**Administrator**, **Operator**, and **User**). When you have connected to the camera by using the ONVIF protocol, only the currently enabled streams or events are supported and you cannot change it. There may be some more settings that cannot be changed, too. If you want to change those settings, connect to the camera by using the IDIS Discovery program.
  - **ONVIF Event Type**
    - **Normal:** This is the usual way the camera delivers events.
    - **Standard:** This is the ONVIF standard event delivery method.
  - **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 11**.
  - **Import Setup**: Open a setup file and apply its settings to the camera. 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 11**.
  - **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 camera. Doing so can interfere with establishing a connection with the other camera.
- If IP Address, Port, and/or SSL settings have 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.

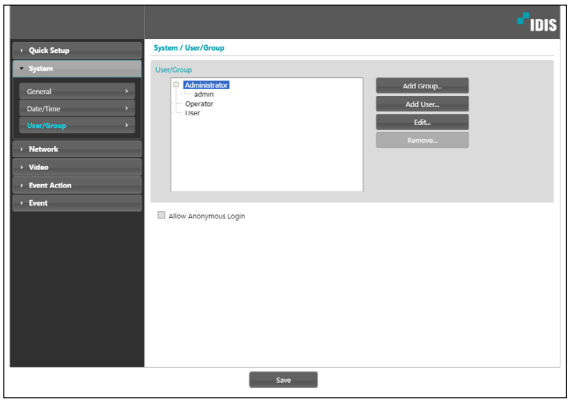
Date/Time



- **Date/Time**: Change the camera's date/time settings and display formats and configure the time zone and daylight saving time settings. Click **Save** 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

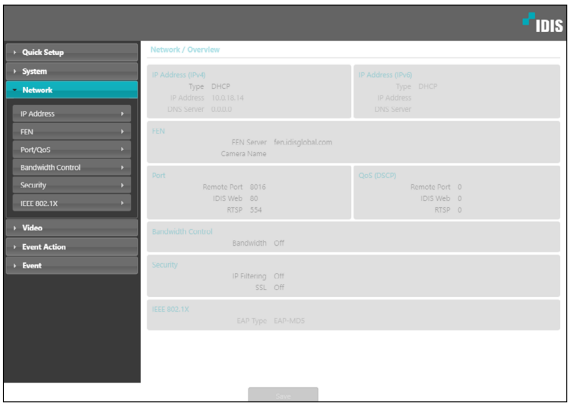


- **User/Group**: Change remote camera control permission settings for users and user groups.
  - **Add Group**: Add a new user group. Designate a name for the group and then specify control authorities.
  - **Add User**: Add a new user. Designate a name for the user, select which group to add the user 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.
- **Allow Anonymous Login**: Select if you are using Webcasting. For more information on webcasting,

refer to the **Webcasting on page 23**.

- **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.
- Standard groups (**Administrator**, **Operator**, and **User**) cannot be edited or deleted. Authorities assigned here apply identically to ONVIF protocol user groups.
- 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.

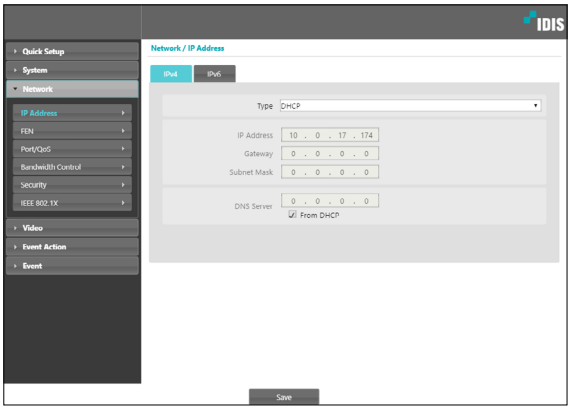
Network



Change the network settings, enable FEN and security features, and control network bandwidth use.

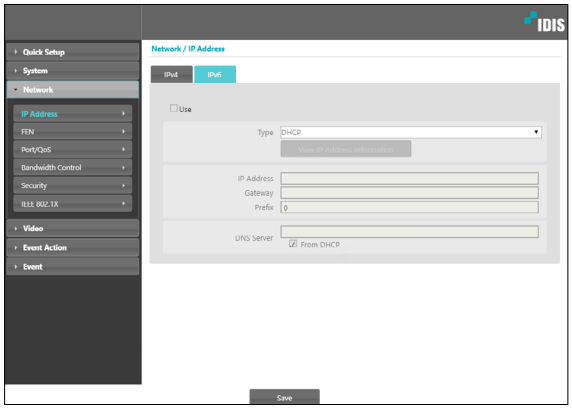
IP Address

IPv4



- **Type**: Select the type of network you are using. 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.
  - **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 **Save** 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 camera 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.

IPv6

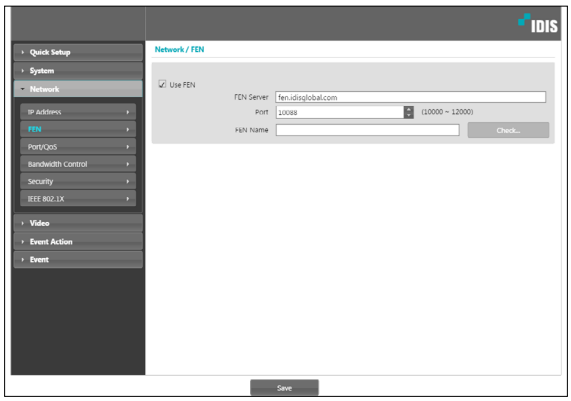


- Check **Use** to activate IPv6.
- **Type**: Select the type of network you are using. If this option has been changed, click **Save** to apply the current settings, and then restart Remote Setup. If you do not restart Remote Setup, the changes afterwards will not be applied.
  - **Manual**: Select 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 **Save** to retrieve IP address and other network settings automatically from the DHCP server or the router. If it can not be received automatically, it will be created automatically from the camera.
- **View IP Address Information:** The IPv6 address assigned to the IP camera is shown.
- **DNS Server**: Enter the DNS server's IP address. If the camera is connected to the network via DHCP, select the **From DHCP** option to retrieve the DNS server's IP address from the DHCP server or the router automatically. If it can not be received automatically, it will be created automatically from the camera. The updated address will be displayed upon the subsequent connection.

- Contact your network administrator for more information on the camera's network connection type, the DNS server's IP address, and other related information.
- If using DHCP, the camera's IP address may change from time to time. We therefore recommend that you use the **FEN** feature.
- If using IPv6, some network function may be limited.

FEN

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

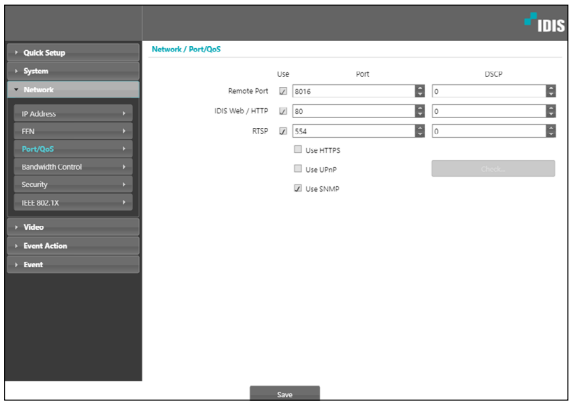


- **FEN Server**: Enter the FEN Server's IP address or domain name.
- **Port**: Enter the FEN Server's port number.
- **FEN Name**: Enter a camera name you wish to register to the FEN Server. Click **OK** to check the name's availability.

- **Use FEN** is a feature that allows you to register a unique name for a camera that utilizes a dynamic IP address to the FEN Server and connect to the camera using the registered name instead of an IP address, which can change from time to time. Moreover, you can access the camera without having to configure NAT (Network Address Translation) device settings even when the camera 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 **Save** 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.
- **FEN Server**'s default address is **fen.idisglobal.com**. DNS server must be configured under network setup to ensure normal operation.
- 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 special characters, the connection may not be made when the WebGuard or remote setting is accessed by FEN name through the Web browser. (If you can not access special characters, you can access by changing the encoding.)

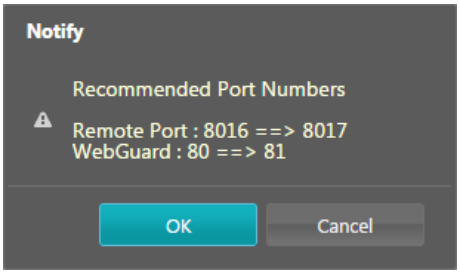
The FEN Server operated by IDIS is a service to its clients and may go offline without notice for server update purposes or due to an unexpected failure.

Port/QoS



- **Use/Port**: Enable/disable ports and designate corresponding port numbers. **Remote Port** and **IDIS Web / HTTP** ports are enabled by default and cannot be disabled. By enabling IDIS Web and RTSP ports, you will be able to use the IDIS Web program or a media player that supports RTSP (Real-Time Streaming Protocol) service to connect to the camera. When the HTTP port is enabled, you can run the camera'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 camera is connected to the network via an IP router (or NAT), select this option to connect to the camera 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.



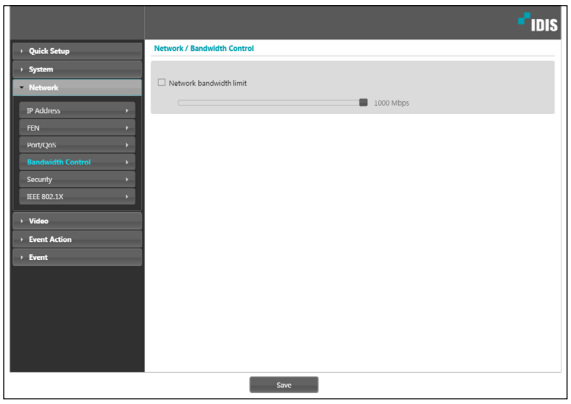
  Click **Apply** to use the recommended port numbers.
- **Use SNMP**: Select this option to enable SNMP (Simple Network Management Protocol).

- 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.
- It is not allowed to use the same port number for more than one function.
- You can connect to the camera using a media player that supports RTSP service and monitor its video feed. If the camera is connected to the network via an IP router (or NAT) or is behind a firewall, you must open the ports. (All ports if using UDP protocol and RTSP ports if using TCP protocol) This feature may not be supported by al media player. In addition, video display on certain media players may not be smooth depending on the network status, video streaming compression method used, and/or the resolution setting. Connection methods are as follows:
  - **Via PC**: Launch the media player (such as VLC) and then enter **rtsp://ID:Password@IP Address: RTSP Port Number/trackID='Stream Number'** (Stream Number: 1 if Primary, 2 if Secondary, and 3 if Tertiary). (e.g.: rtsp://admin:@10.0.152.35:554/trackID=1 (User: admin, Password: None, Camera IP Address: 10.0.152.35, RTSP Port Number: 554, Stream: Primary))

- Port numbers of the remote program must be updated whenever the camera's port numbers are changed.
- ONVIF protocol may not function if using HTTPS.

Bandwidth Control

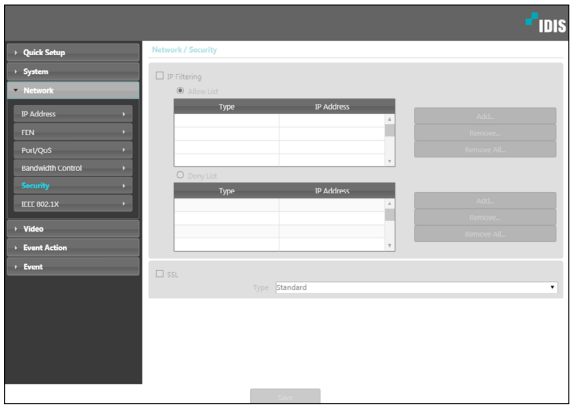
Regulates the camera's network bandwidth use based on network traffic fluctuations.



Select **Network Bandwidth limit** and then specify the maximum bandwidth. The camera 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.

Security

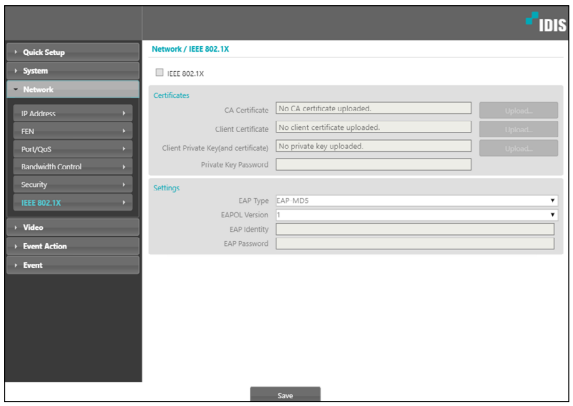


- **IP Filtering**: Select this option to enable IP Filtering. IP Filtering allows camera access from certain IP addresses and blocks access from others.
  - **Add**: Add new IP addresses to Allow List or Deny List. Select the **Host** option to add one IP address at a time. Select the **Group** option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

- 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 camera 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/)

IEEE 802.1X

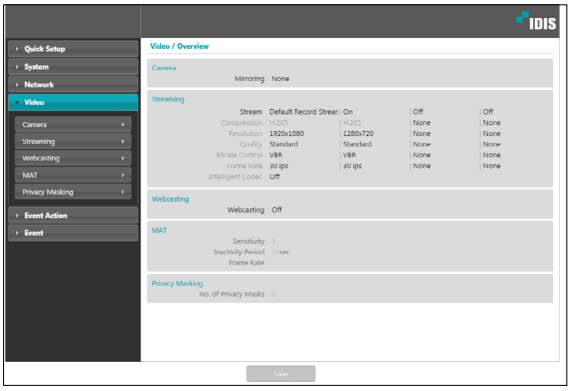
Select the **IEEE 802.1X** option to enable IEEE 802.1X network connection authentication.



- **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

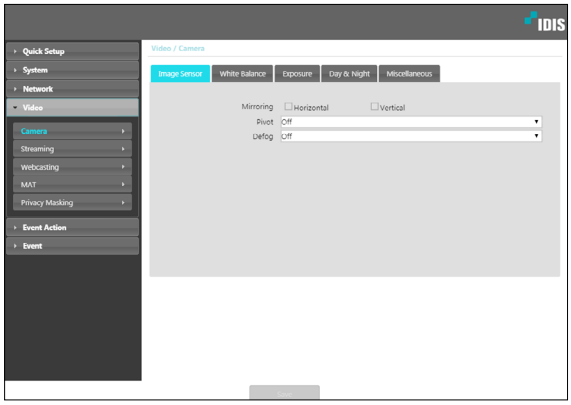


Configure **Camera**, **Streaming**, **Webcasting**, **MAT**, and **Privacy Masking** options.

Camera

Image Sensor

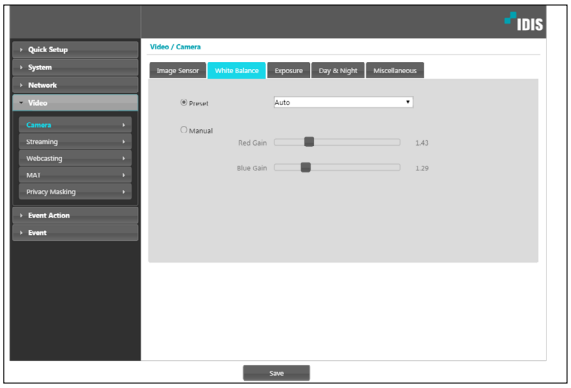
Configure **Image Sensor** settings.



- **Mirroring**: Select Horizontal Reverse or Vertical Reverse to flip the image horizontally or vertically.
- **Pivot**: Select a direction to rotate images 90 degrees clockwise or counterclockwise. If vertical resolution is less than 320, this function is not supported. If you enable this function, you can monitor more efficiently long and narrow space such as hallways, corridors, etc. If both Mirroring and Pivot functions are enabled, Mirroring functions first, then Pivot.
- **Defog:** Disables or enables the Defog feature. When it is enabled, image with a fog is adjusted.

White Balance

Configure **White Balance** settings.



- **Preset**: Use preconfigured white balance settings.
  - **Auto**: Allow the system to adjust the white balance automatically. The system will assess the lighting conditions and adjust the white balance automatically.
  - **Hold:** Hold the current white balance.
  - **INCANDESCENT - FLUORESCENT COLD**: Select a lighting type to apply the appropriate white balance.

If the **Preset** is **Hold** and the WDR mode is changed, a reset is required.

- **Manual**: Adjust the white balance manually. Adjust Red and Blue gain values. Greater the value, greater the intensity of the corresponding color.

If the white balance does not work properly under the following specific conditions, select **Manual** or **Hold.**

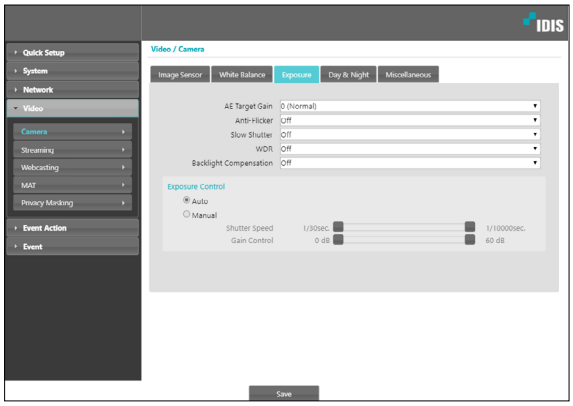
- When the surrounding environment of the object is out of the color temperature correction range

- When the surrounding environment of the object is dark

- The camera is pointed directly at the fluorescent lamp or installed in a place where the lighting change is severe.

Exposure

Configure **Exposure** settings.

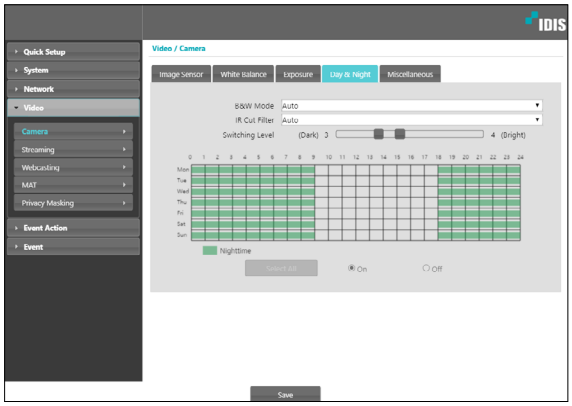


- **AE Target Gain**: Specify exposure compensation's target gain. Exposure is compensated automatically based on the specified target gain. Higher the gain, brighter the images.
- **Anti-Flicker**: If the lights in the area where the camera is located use alternating current, specify the frequency of the lights to minimize flickering. Matching the frequencies can reduce flickering. (NTSC: 60Hz, PAL: 50Hz) When using WDR, flickering can be present in poor environments even if Anti-Flicker is turned on.
- **Slow Shutter**: Activate **Slow Shutter**. The electronic shutter's speed will decrease to the specified level under low-lighting conditions to allow more light in and therefore produce brighter images.
- **WDR:** Disables or enables the WDR(Wide Dynamic Range). When the very dark and very bright areas exist simultaneously on the screen, WDR allows you to recognize the both areas.
- **Backlight Compensation**: Enable/disable the Backlight Compensation feature. If using WDR, Backlight Compensation OFF does not work.
  - **ON**: When images are too bright overall due to backlight, objects are exposed brighter under backlight circumstances.
  - **HSBLC** (High Suppress Backlight Compensation): When a certain area of images is too bright due to backlight under low lighting conditions and it causes the other area to be too dark, this function provides the other area of images brightly and clearly by blocking the backlight in the certain area. Dark parking lot entrances and gas station entrances at night, for example (HSBLC compensates for the bright light coming from incoming vehicle headlights and makes it possible to see the license plates).
  -
- **Exposure Control:** Adjust Shutter Speed and gain. This option is available only when **Anti-Flicker** and **Slow Shutter** are both set to **Off**.
  - **Auto:** The system will assess the lighting conditions and adjust the shutter speed and gain automatically.
  - **Manual:** Use the slider to select the desired shutter speed and gain. Select the most suitable minimum and maximum shutter speeds and gains for the lighting conditions in the area where the camera is located.

With certain features, selecting **Auto** automatically loads settings suitable for the camera's installation environment.

Day & Night

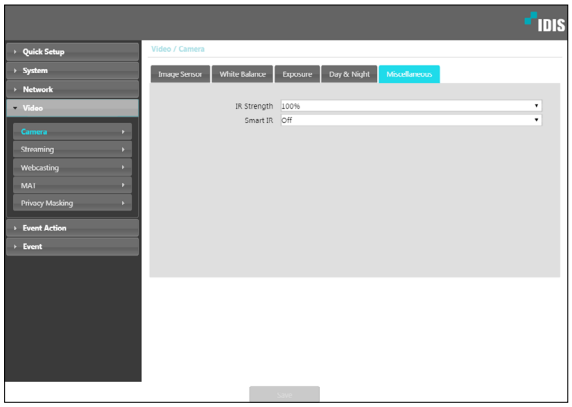
Configure **Day & Night** settings.



- **B&W Mode**: Display the images in greyscale for greater clarity in low-lighting conditions.
  - **On/Off**: Enable/disable B&W Mode.
  - **Auto**: Allow the system to enable/disable B&W Mode automatically.
  - **Schedule**: Set up a B&W Mode schedule. B&W Mode is enabled on days and times designated as **Nighttime** and disabled at all other times. Select **On** or **Off** at the bottom of the schedule table and then click or drag on the dates and times to select/unselect as **Nighttime**. Select **On** or **Off** and then click **Select All/Clear All** to select/unselect all dates and times as Nighttime.
- **IR Cut Filter**: IR Cut Filter blocks out the infrared spectrum. You can ensure clear images at all times by blocking out the infrared spectrum in high-lighting conditions and allowing the infrared spectrum to pass through in low-lighting conditions.
  - **Nighttime Mode**/**Daytime Mode**: Disables or enables the IR cut filter.
  - **Auto**: Allow the system to enable/disable IR Cut Filter automatically.
  - **Schedule**: Sets up the IR cut filter schedule. The IR cut filter is disabled during the date and time scheduled as **Nighttime** and enabled during the rest. Set up or release Nighttime by selecting **On** or **Off** in the bottom and clicking or dragging the date and time area in the table. Selecting On or Off and clicking the **Select All/Clear All** button sets up or releases Nighttime for all dates and time.
- **Switching Level:** Sets up the switching level between daytime and nighttime modes. For example, if the darkness level is set to **3** and the brightness level to **5**, the system switches to nighttime mode when in lighting conditions of level 3 or below and to daytime mode when in lighting conditions of level 5 or over. It is recommended that you do not set up the darkness level and brightness level identically; otherwise, this function may not work properly. This functions only when **B&W Mode** or **IR Cut Filter** is set to **Auto**.

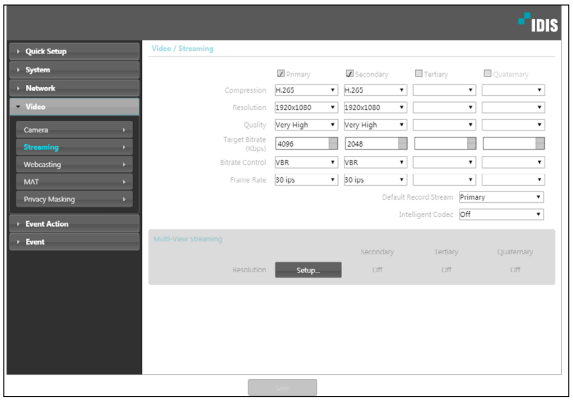
Miscellaneous

Configure **Miscellaneous** settings.



- **IR Strength:** Set the brightness of the IR LED. The higher the value is set, the brighter it is.
- **Smart IR:** Prevent the object from being saturated by IR light. Select **On** to always control saturation and select **Auto** to control saturation only when the zone is over-saturated.

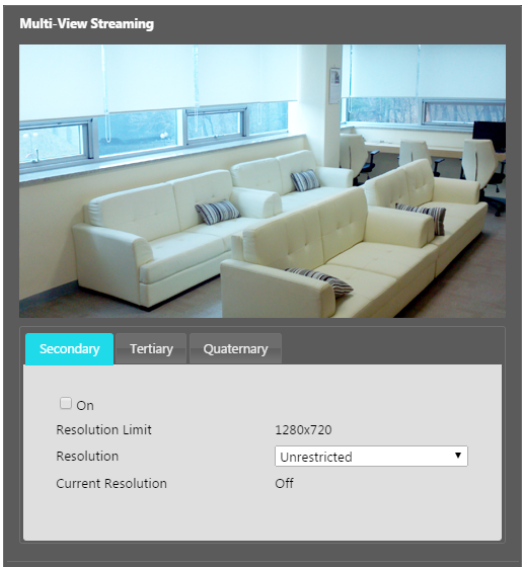
Streaming



- **Primary/Secondary/Tertiary/Quaternary**: Multistreaming is supported. Enable/disable streaming use. The stream you set first has priority.

- **Compression**: Choose the streaming compression method. The H.265 compression does not support ONVIF Protocol and RTSP.
- **Resolution**: Choose a resolution setting for video streaming. The resolution varies depending on the camera model. The current stream resolution cannot be higher than the higher stream resolution.
- **Quality**: Choose a quality setting for video streaming.
- **Target Bitrate(Kbps):** Set the target bitrate. When **Quality** is set to **Manual**, you can configure the value of the target bitrate. If not, the set value of the target bitrate for each **Quality** appears.
- **Bitrate Control**: Choose a bitrate control mode for video compression.
  - **CBR (Fixed Bitrate):** Maintains the current bitrate regardless of motion change in the video.
  - **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. The fame rate of the current stream cannot be higher than the fame rate of the higher stream if those stream resolutions are same.
- **Default Record Stream**: Choose a stream to use for recording. This setting, however, may not apply if a recording stream has been designated from the remote program or the SD memory card recording feature has been enabled.
- **Intelligent Codec:** Analyze real-time video intelligently to minimize bitrate while maintaining frame rate and image quality.
- **Multi-View Streaming**: Designate a specific area of the screen and stream images from that area only. (not supported for the primary stream) Click **Setup** to designate a streaming area.

  Select **On** and then specify the streaming area's resolution.

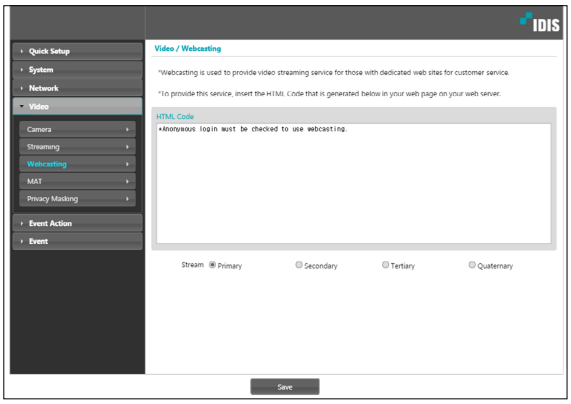


- **Resolution Limit**: Indicates the maximum resolution that can be set for the streaming area.
- **Resolution**: Designate a streaming area. Designated area is marked in red on the screen. You can adjust the resolution of the area or reposition the area by dragging and dropping using the mouse.
- **Current Resolution**: Displays the resolution of the designated streaming area.

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

Webcasting

Use the webcasting service to view live images from the camera on a web site.

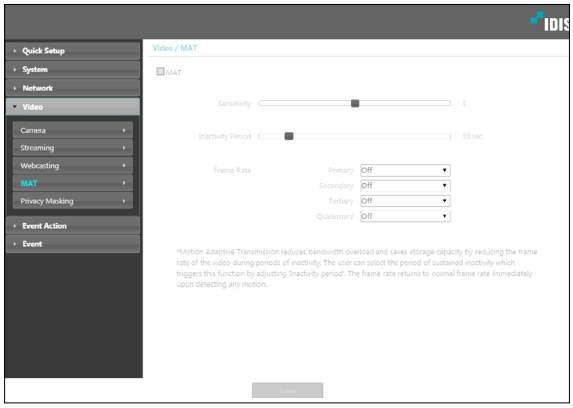


- **HTML Code**: Copy and paste the html code shown on the screen within the code of the web page you want the video to be displayed.
- **Stream**: Choose a stream to use for webcasting. Only a stream currently in use can be selected.

In order to use the webcasting service, the **Allow Anonymous Login** option under **System > User/ Group** must be selected.

MAT

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

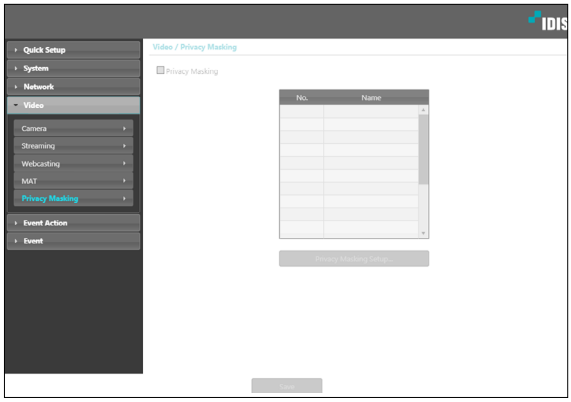


- **Sensitivity**: Set the motion detection sensitivity. Higher values will result in more sensitive motion detection.
- **Inactivity Period**: Set the Inactivity Period. If motion is not detected for the duration of time specified, video is transmitted and recorded using the frame rate designated below 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. When the slow shutter mode is enabled under **Video > Camera** menu, the fame rate may change. 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.

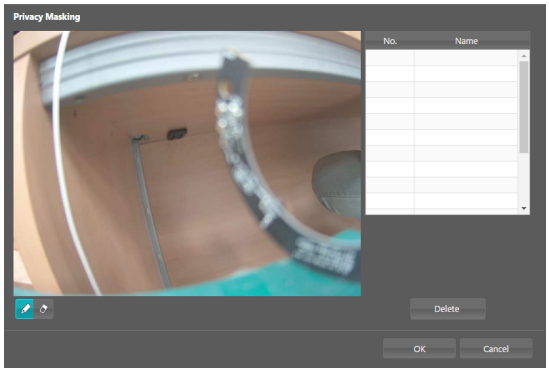
MAT (Motion Adaptive Transmission) is a feature that lowers the frame rate when motion is not detected to reduce the load on the network and save on storage space. Based on the specified sensitivity setting, no movement will be assumed if there is no change between two consecutive images.

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.



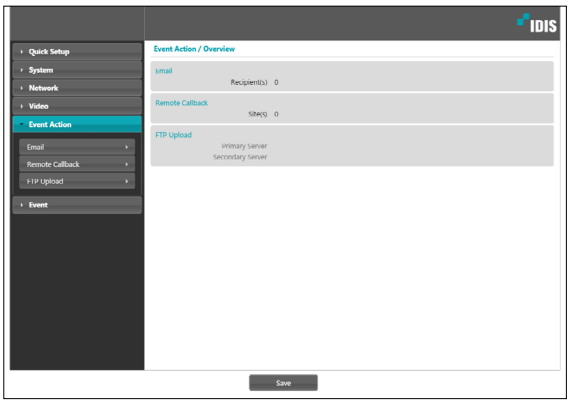
- **Privacy Masking Setup**: Set up privacy masks(up to 8).



- **(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.

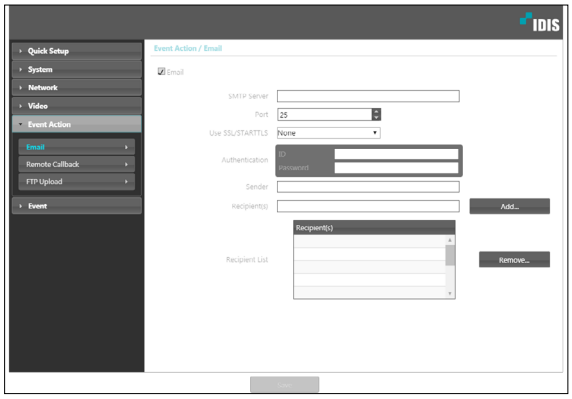
Event Action

Designate event detection alert actions.



Email

Select **Email** to send out emails.

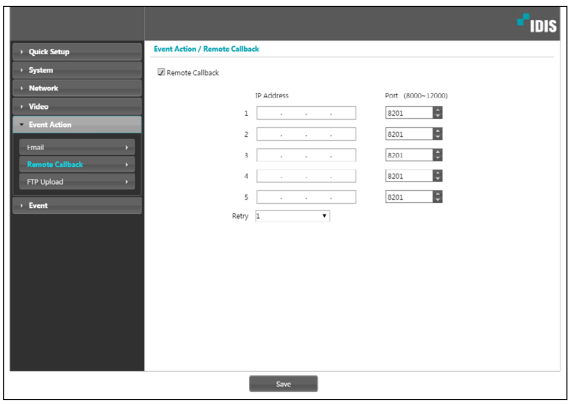


- **SMTP Server/Port**: Enter the SMTP server's IP address (or domain name) and port number you received from the network administrator. If a DNS server has been set up during network configuration, you can enter a domain name instead of an IP address.
- **Use SSL/STARTTLS**: If using an SMTP server 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.

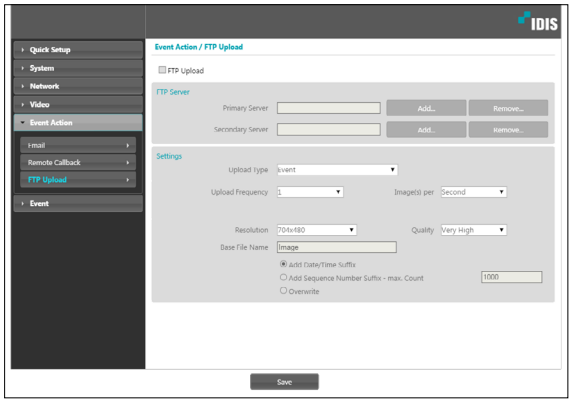
- Not supported from the IDIS Web program.
- The camera must be registered to the remote system in order to use the **Remote Callback** feature.



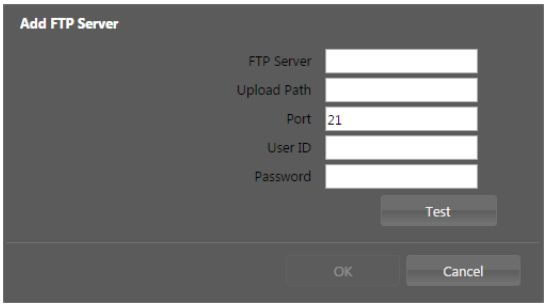
- **IP Address**: Enter the IP address and port number of the remote system that will receive the messages.
- **Retry**: Designate how many reattempts to make if message delivery fails.

FTP Upload

Select **FTP Upload** to upload .jpg image of the event detected to an FTP server.



- **FTP Server**: Click **Add** to register a new FTP server. Click **Remove** to remove a registered FTP server. When an event is detected, a .jpg image of the event detected image is uploaded to the Primary Server. If the upload to the Primary Server fails, the file will be uploaded to the Secondary Server. Upload to the Secondary Server will continue to be attempted until successful. Fill out the fields below and click **Test** to test the FTP server connection settings. Once the test is complete, click **OK**.



- **FTP Server**: Enter the FTP server's IP address (or domain name).
- **Upload Path**: Designate the file upload path.
- **Port**: Enter the FTP server's port number.
- **User ID, Password**: Enter the user ID and password needed for connecting to the FTP server.

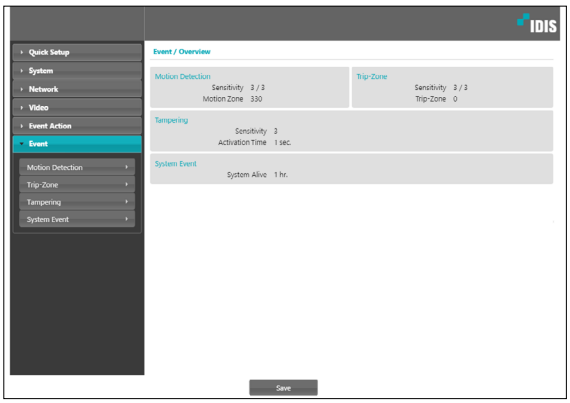
- **Settings**: Configure image and upload settings.
  - **Upload Type**: Choose an upload type. Select **Always** to upload images using the settings below, irrespective of event detection. Select **Event** to upload images using the settings below when an event is detected.
  - **Upload Frequency**: Activated only when Upload Type has been set to **Always**. Designate the upload speed. The specified number of images will be uploaded to the FTP server during the specified period of time.
  - **Upload 1 image per**: Activated only when Upload Type has been set to **Event**. Designate the upload speed. Select **Upload** for and specify a duration. Images will be uploaded for the specified duration at the specified upload speed. Select **Upload while event status is active** to upload images at the specified speed only while event status is active.

- **Resolution/Quality**: Choose the resolution and quality of the images to upload to the FTP server. Range of resolution settings you can use here can vary depe nding on the resolution setting applied under **Video** > **Streaming**.
- **Base File Name**: Enter a name for the files to be uploaded to the FTP server and then choose file identification options. Select **Add Date/Time Suffix** to add event detection date and time information to each image file. Select **Add Sequence Number Suffix - max. Count** to number the image files based on the order of event detection. Select **Overwrite** to overwrite the previous image with the new image. Event type is automatically added to the file names.

- When specifying the **Upload Path** or **Base File Name**, you cannot use special characters such as \, /, #, *, |, :, ", <, >, and ?.
- The resolution of FTP upload image can change depending on the resolution setting applied under **Video** > **Streaming**.
- Set speed settings for Upload Frequency and Upload 1 image per options in consideration of the FTP server's performance. FTP uploads can fail if the configured speed is higher than what the FTP server can handle.

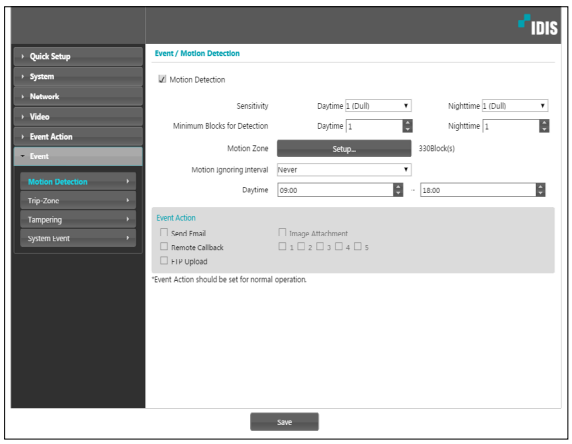
Event

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.



- **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 blocks.
  - **(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.

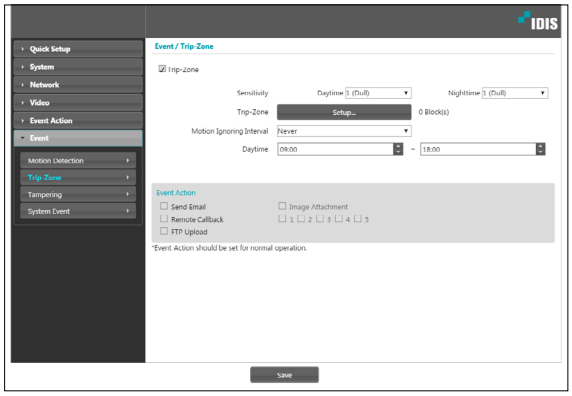
    - Not supported from the IDIS Web program.
    - The camera must be registered to the remote system in order to use the **Remote Callback** feature.
  - **FTP Upload**: Select this option if you wish to upload images to the FTP server

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 trip zone blocks.
  - **(Single Block)**: Select/unselect trip zone blocks individually.
  - **(Zone)**: Select/unselect multiple trip zone blocks.
  - **(All)**: Select/unselect all trip zone 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.

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

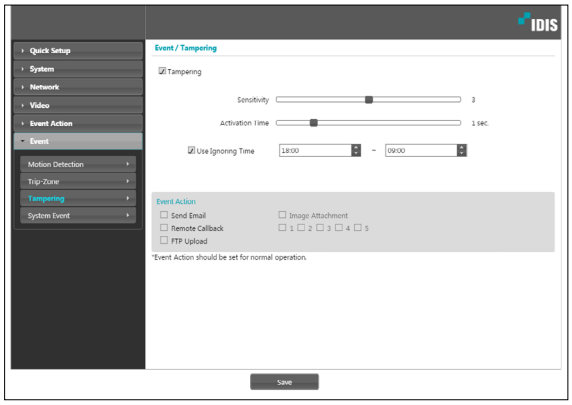
  - **FTP Upload**: Select this option if you wish to upload images to the FTP server.

    - **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.



- **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.
- **Use Ignoring Time**: Define the event ignoring time. Tampering detections taking place during the defined time range will not be assumed 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.

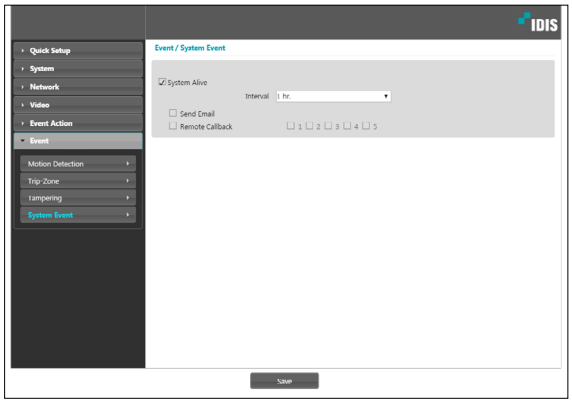
    - Not supported from the IDIS Web program.
    - The camera must be registered to the remote system in order to use the **Remote Callback** feature.

  - **FTP Upload**: Select this option if you wish to upload images to the FTP server.

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.
- **Remote Callback** is not supported on IDIS Web.
- The camera must be registered to the remote system in order to use the **Remote Callback** feature.

Part 2 - IDIS Web

IDIS Web 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 or Chrome.

System requirements for running IDIS Web are as follows:

OS: Microsoft® Windows® XP (Service Pack 3)*Internet Explorer only*, Microsoft® Windows® Vista (Service Pack 1), Microsoft® Windows® 7 (Home Premium, Professional, Ultimate), Microsoft® Windows® 8 (Pro, Enterprise)

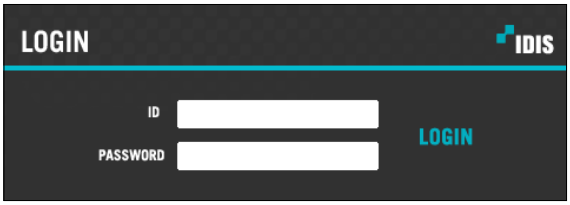
- CPU: Intel Pentium IV 2.4GHz or above (Core 2 Duo E4600 recommended)
- RAM: 1GB or more
- VGA: 128MB or more (1280x1024, 24bpp or above)
- Internet Explorer: Version 10 or later 32-bit
- Chrome: Google Chrome 22.0.1229.0 or above (59.xxx or above recommended)

1 Launch Internet Explorer or Chrome and then enter the following information in the address bar.

- http://IP Address:Port Number (IDIS Web connection port number selected during camera IP address and port number setup)
- Or http://FEN Server Address/FEN name (FEN Server address and FEN name registered to the FEN Server)
- Or http://web.idisglobal.com (it is required to enter the camera IP address when logging in. If the camera uses the FEN feature, you can enter the FEN name registered to the FEN server instead of the camera IP address after selecting the USE FEN option)

- If the Use HTTPS option has been selected during IDIS Web port number setup, enter https instead of http. If prompted with a security certificate warning, select "Continue to this website (not recommended)." If the IDIS Web 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 IDIS Web connection port number has been set to 80 (443 when entering https).
- If connecting by entering http://web.idisglobal.com, it is required to enter the Watch port number.
- Contact your network administrator for the IP address of the camera you wish to connect to the IDIS Web pot number.

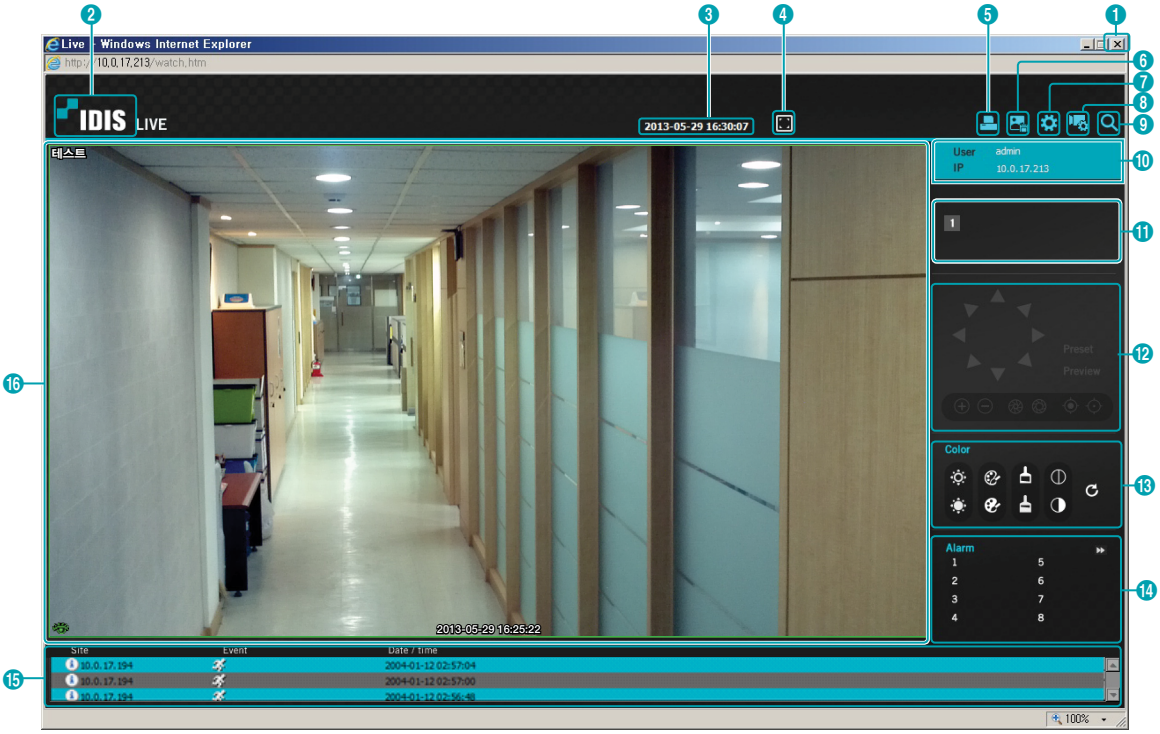
2 Enter the ID and password and click **LOGIN** to sign in



-
- IDIS Web does not work with Microsoft® Windows® 8 metro UI.
- Do not close the login window while IDIS Web is running. Switching over to Web Live or Web Search mode can cause a script error, requiring you to restart the IDIS Web program.
- To use IDIS Web on Microsoft Windows Vista or above, launch Internet Explorer by right-clicking on the icon and selecting the **Run as administrator** option. Otherwise, certain IDIS Web functions might not be available.
- When running IDIS Web, 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**))
- Launching a new version of IDIS Web 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 IDIS Web.
- 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.

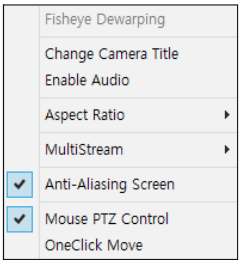
Web Live Mode

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



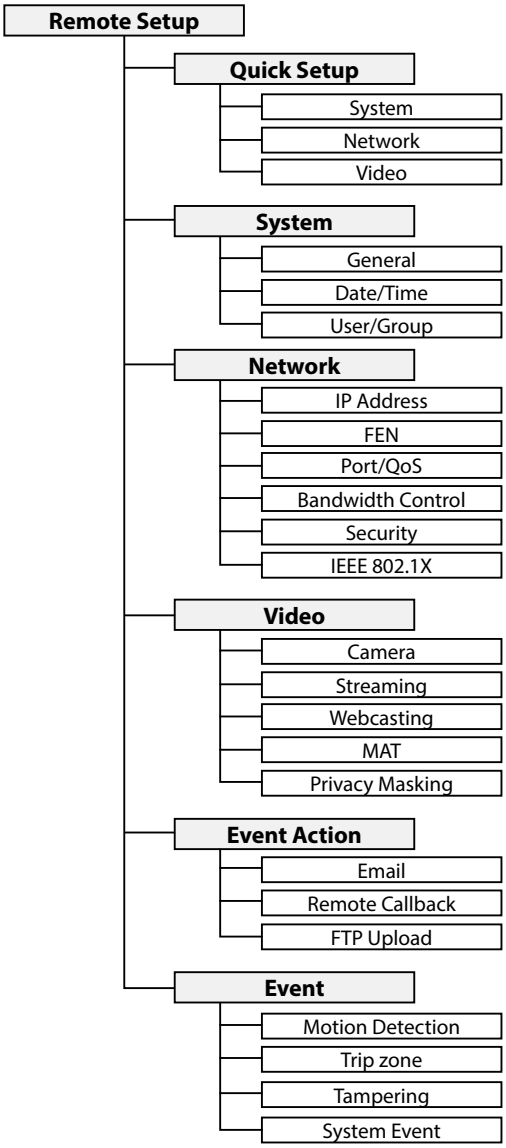
❶	Press ☒ to terminate IDIS Web.
❷	Place the mouse pointer on the logo to check IDIS Web's version.
❸	Displays the current time.
❹	Click ⛶ to view the video in full screen. Press the ESC key on the keyboard to return to the previous screen.
❺	Click to print the current video screen using a printer connected to the computer.
❻	Click to save the current video screen as an image file.
❼	Click to 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.
❽	Click to load the camera setup window.
❾	This function is not supported.

⑩	Shows login information.
⑪	Indicates the camera's number.
⑫	This function is not supported.
⑬	Used to adjust live video quality.
⑭	This function is not supported.
⑮	Event status window at the bottom of the screen displays a list of events detected at remote locales. Trip zone Tampering Motion Detection
⑯	Right-click on the screen to display the pop-up menu. Click to enable or disable each function. • **Fisheye Dewarping:** This function is not supported. • **Change Camera Title**: Used to change the camera's name. Renaming the camera in Web Live mode does not affect the camera's name on the remote system. If no name is entered for the camera, the name used at the remote locale is shown on the screen. • **Enable Audio**: This function is not supported. • **Aspect Ratio**: Change the aspect ratio of the video displayed on the screen. - **Fit to Screen**: Fit the video to the size of the camera 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 camera 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 camera screen to accommodate the selected size. • **MultiStream**: If the camera 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. • **Mouse PTZ Control**: This function is not supported.



Part 3 - Appendix

Setup Menu Tree (Remote Setup)



Index

B

Bitrate Control 22

C

Camera Name 9

Compression 22

D

Date/Time 10

DSCP 14

F

FEN Name 13

FEN Server 13

Frame Rate 22

I

IDIS Web port 14

IPFiltering 16

M

MAT 24

N

Network Bandwidth Limit 15

O

ONVIF Protocol 9

Q

Quality 22

R

Remote Port 14

Resolution 22

RTSP Port 14

S

SSL 16

T

Time Sync 10

U

Use FEN 13

Use HTTPS 14

User/Group 10

Use UPnP 14

IDIS Co., Ltd.

For more information, please visit at

www.idisglobal.com