MEGApix® 5MP Vandal Dome IP Camera

DWC-MV95WiATW



User's Manual Ver. 06/26

Before installing and using the camera, please read this manual carefully.
Be sure to keep it handy for future reference.

Safety Notes

- This product is intended to be supplied by a Listed Power Unit, marked with 'Limited Power Source', 'LPS' on the unit, output rated minimum 12V/2 A or POE 48V/ 350mA or AC24V (depending on models), no more than 2000m altitude of operation and 60 degrees C.
- As for the modes with PoE function, the function of the ITE being investigated under the IEC 60950-1 standard is considered not likely to require connection to an Ethernet network with outside plant routing, including campus environment, and the ITE is to be connected only to PoE networks without routing to the outside plant.
- Do not try to disassemble the camera; to prevent electric shock, do not remove screws or covers.
- There are no user-serviceable parts inside. Please contact the nearest service center as soon as possible if there is any failure.
- Avoid incorrect operation, shock vibration and heavy pressing, which can cause damage to the product.
- Do not use a corrosive detergent to clean the main body of the camera. If necessary, please use a soft dry cloth to wipe dirt; for hard contamination, use neutral detergent. Any cleanser for high-grade furniture is applicable.
- Avoid aiming the camera directly towards extremely bright objects, such as the sun, as this may damage the image sensor.
- Please follow the instructions to install the camera. Do not reverse the camera, or the reversing image will be received.
- Do not work the camera in case the temperature, humidity and power supply are beyond the limited stipulations.
- Keep away from heat sources such as radiators, heat registers, stoves, etc.
- Do not expose the product to the direct airflow from an air conditioner.
- This manual is for using and managing the product. We may reserve the right to amend the typographical errors, inconsistencies with the latest version, software upgrades, product improvements, interpretation and modification. These changes will be published in the latest version without special notification.
- All pictures, charts and images in this manual are only for the description and explanation of our products. In this manual, the trademarks, product names, service names, company names and products that our company does not own are the properties of their respective owners.

Disclaimer

- Concerning the product with internet access, the use of the product shall be wholly at your own risk. Our company shall not be responsible for abnormal operation, privacy leakage, or other damages resulting from cyber-attack, hacker attacks, virus inspection, or other internet security risks; however, our company will supply timely technical support if necessary.
- Surveillance laws vary from country to country. Check all laws in your local region before using this product for surveillance purposes. We shall not take responsibility for any consequences resulting from illegal operations.

Cybersecurity Recommendations

- Use a strong password. At least 8 characters or a combination of characters, numbers and upper- and lowercase letters should be used in your password.
- Change the passwords periodically to ensure that only authorized users can access the system (recommended time is 90 days).
- It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.
- It is recommended to set up a security system for your router. Important ports such as HTTP, HTTPS and dual ports cannot be closed.
- It is not recommended to expose the device to the public network. When it is necessary to be exposed to the public network, please set the external hardware security system and the corresponding security system policy.
- It is not recommended to use the v1 and v2 functions of SNMP.
- To enhance the security of WEB client access, please create a TLS certificate to enable HTTPS.
- Use black- and white- lists to filter the IP address. This will prevent everyone, except those specified IP addresses, from accessing the system.
- If you add multiple users, limit the functions of guest accounts.
- If you enable UPnP, it will automatically try to forward ports in your router or modem. It is very convenient for users, but this will increase the risk of data leakage when the system automatically forwards ports. Disabling UPnP is recommended when the function is not used in real applications.
- Check the log. If you want to know whether unauthorized users have accessed your device, you can check the log. The system log will show you which IP addresses were used to log in to your system and what was accessed.

Regulatory Information

FCC Information

1. FCC compliance

The products have been tested and found in compliance with the council FCC rules and regulations, part 15 subpart B. These limits are designed to provide reasonable protection against harmful interference. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used following the instruction manual, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. The user will be required to correct the interface at their own expense in case harmful interference occurs.

2. FCC conditions:

The operation of this product is subject to the following two conditions: (1) this device may not cause a harmful interface and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Information

CE The products have been manufactured to comply with the following directives.
EMC Directive 2014/30/EU

RoHS

The products have been designed and manufactured following Directive EU RoHS Directive 2011/65/EU and its amendment Directive EU 2015/863 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.



2012/19/EU (WEEE directive): The Directive on waste electrical and electronic equipment (WEEE Directive). To improve the environmental management of WEEE, the improvement of collection, treatment and recycling of electronics at the end of their life is essential. Therefore, the product marked with this symbol must be disposed of responsibly.

Directive 94/62/EC: The Directive aims at the management of packaging and packaging waste and environmental protection. The packaging and packaging waste of the product in this manual must be disposed of at designated collection points for proper recycling and environmental protection.

REACH(EC1907/2006): REACH concerns the Registration, Evaluation, Authorization and Restriction of Chemicals, which aims to ensure a high level of protection of human health and the environment through better and earlier identification of the intrinsic properties of chemical substances. The product in this manual conforms to the rules and regulations of REACH. For more information on REACH, please refer to the DG GROWTH or ECHA websites.

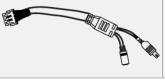
Table of Contents

1 Introduction 1
1.1 Product and Accessories 1
1.2 Parts identification 1
2 Installation 2
2.1 Installation 2
2.2 Cabling 4
2.3 Managing the SD Card 4
3 Network Setup 5
3.1 IP Finder 5
4 Live View 7
5 Network Camera Configuration 10
5.1 Camera Configuration 10
5.1.1 Camera Parameters 10
5.1.2 Video Configuration 13
5.1.3 Audio Configuration 14
5.1.4 OSD Configuration 15
5.1.5 Privacy Mask 15
5.1.6 ROI Configuration 17
5.1.7 Zoom/Focus 18
5.2 Network Configuration 19
5.2.1 IPv4 and IPv6 19
5.2.2 Port 20
5.2.3 ONVIF 21
5.2.4 DDNS 22
5.2.5 SNMP 24
5.2.6 802.1x 25
5.2.7 RTSP 27
5.2.8 RTMP 29
5.2.9 UPNP 30
5.2.10 SMTP 31
5.2.11 FTP 33
5.2.12 HTTPS 35
5.2.13 QoS 37
5.3 Event Configuration 38
5.3.1 Video Tampering Detection 38
5.3.2 Line Crossing 40
5.3.3 Perimeter Intrusion 42
5.4 Alarm Configuration 44
5.4.1 Motion Detection 44
5.4.2 Other Alarms 46
5.4.3 Alarm In 48
5.4.4 Alarm Out 49

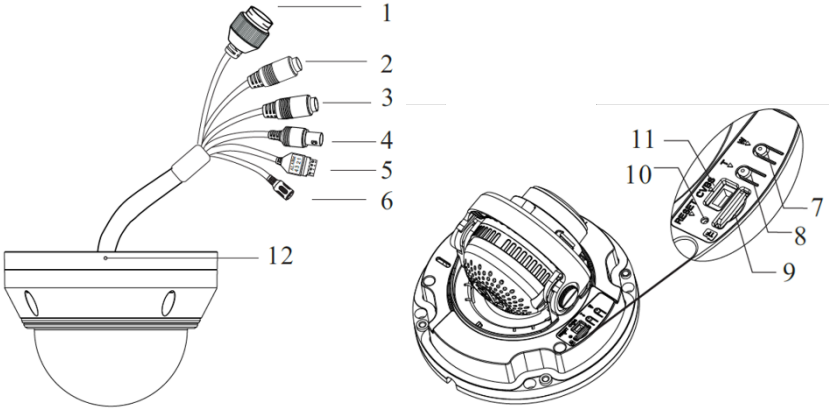
5.5 Security Configuration 51
5.5.1 User Configuration 51
5.5.2 Online User 53
5.5.3 Block and Allow Lists 54
5.5.4 Security Service 54
5.6 System Configuration 56
5.6.1 Basic Information 56
5.6.2 Time Zone&DST 57
5.6.3 Date and Time 57
5.6.4 Storage 58
5.7 Maintenance Configuration 61
5.7.1 Backup and Restore 61
5.7.2 Reboot 61
5.7.3 Upgrade 62
5.7.4 Operation Log 63
6 Playback 65
6.1 Image Playback 65
6.2 Video Search 66
7 Appendix 69
7.1 Troubleshooting 69
7.2 Dimensions 70
7.3 Specifications 72
Warranty Information 74
Limits and exclusions 75

1 Introduction

1.1 Product and Accessories

WHAT'S IN THE BOX					
Quick setup and Installation Guides		1 set	Tapping Screws PA 4x25 – 4pcs		1 set
Mounting Template		1	Plastic Plugs – 4pcs		1 set
Waterproof Cap		1 set	Rubber Plug		1
Hexagonal Wrench 0.11" (3mm)		1	2nd CVBS Local Testing Output and DC12V Input		1 set

1.2 Parts identification

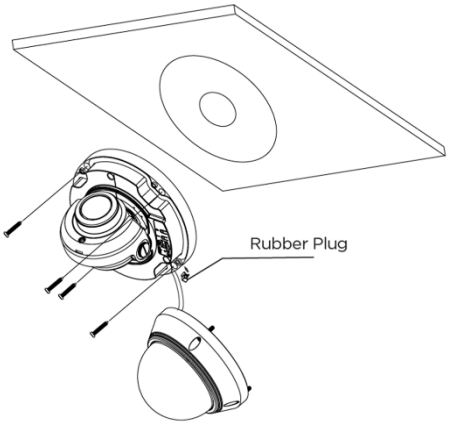


Number	Description	Number	Description	Number	Description
1	Network Cable	5	Alarm Input/Output	9	Micro SD Card Slot
2	Audio Input	6	Power Cable	10	Reset Button
3	Audio Output	7	Zoom -	11	DC In and CVBS Interface
4	CVBS Test Video Output	8	Zoom +	12	Microphone Built-in

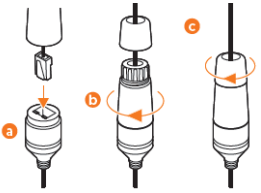
2 Installation

2.1 Installation

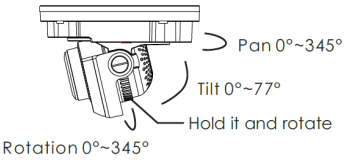
1. The mounting surface must be able to bear at least five times the weight of your camera.
2. Do not let the cables get caught in improper places, or the electric line cover be damaged. This may cause a breakdown or fire.
3. For the installation process, remove the dome cover from the camera base using the included wrench.
4. Using the mounting template sheet or the camera itself, mark and drill the necessary holes in the wall or ceiling.
5. Pass wires through and make all necessary connections. See 2.2 Cabling for more information.
6. Mount the camera to the mounting surface using the included screws and anchors.



7. To use the camera's waterproof wiring:
   a. Install the LAN cable into (a).
   b. (b) will be assembled to (a) with a 1/4 turn.
   c. Thread (c) tightly to (b).

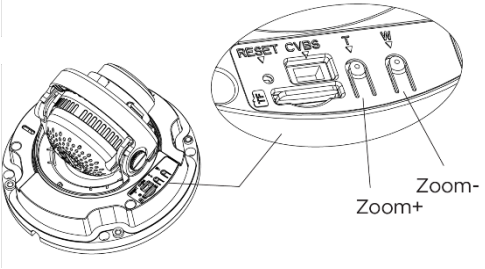


8. Adjust the camera module's tilt and angle.
   a. Tilt: 0 ~ 77°
   b. Pan and Rotation: 0 ~ 345°



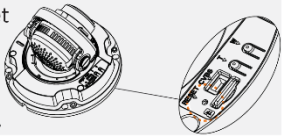
9. Adjust the camera's zoom using the T and

W buttons at the base of the camera.



10. Place the dome cover on the camera using the wrench to tighten the screws on the dome.

Resetting the camera: To reset the camera, use the tip of a paper clip or a pencil and press the reset button at the base of the camera. Pressing the button for five (5) seconds will initiate a camera-wide reset of all the settings, including network settings.

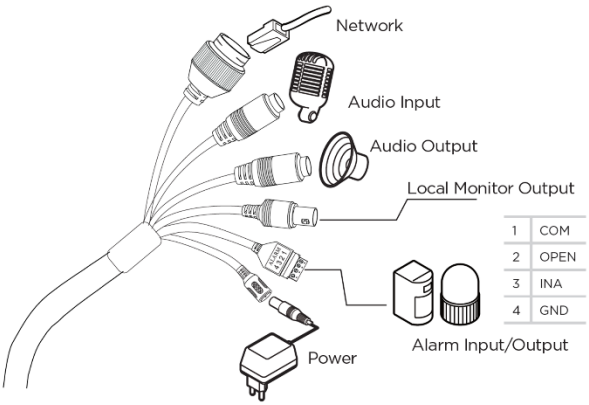


2.2 Cabling

1. When using a PoE Switch or PoE Injector, connect the camera using an Ethernet cable for both data and power.
2. When not using a PoE Switch or PoE Injector, connect the camera to the switch using an Ethernet cable for data transmission and use a power adapter to power the camera.

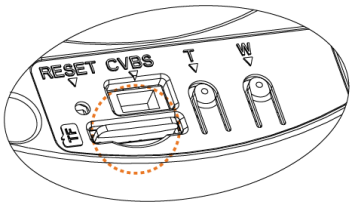
Power requirements	Power consumption
DC12V, PoE (IEEE 802.3af class 3). Adapter not included.	<9W

3. Use the diagram below to connect power, network and audio to the camera.



2.3 Managing the SD Card

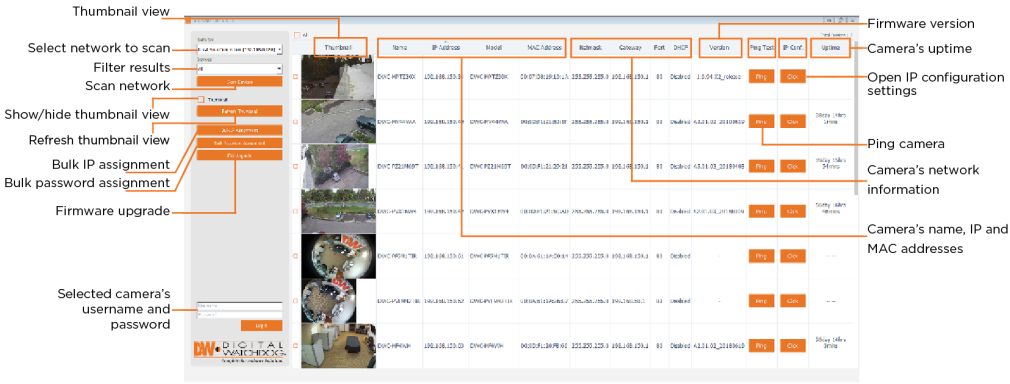
1. To install the camera's SD Card, locate the SD card slot at the base of the camera module by loosening the lock screw at the base of the camera.
2. Insert a class 10 SD/SDHC/SDXC card into the SD card slot by pressing the SD card until it clicks.
3. To remove the SD card, press the card inward until it clicks to release from the card slot, then pull it out from the slot.



3 Network Setup

3.1 IP Finder

Use the DW® IP Finder™ software to scan the network and detect all MEGApix® cameras, set the camera's network settings or access the camera's web client.



Network Setup

1. To install the DW IP Finder, go to http://www.digital-watchdog.com.
2. Enter "DW IP Finder" in the search box at the top of the page.
3. Go to the "Software" tab on the DW IP Finder page to download the installation file.
4. Follow the installation Wizard to install DW IP Finder. Launch DW IP Finder, enter the camera login, then click the "Scan Devices" button. The software will scan the selected network for ONVIF-compliant devices and will list the results in the table. Double-click on a detected camera in the search results to configure the *Camera Settings* using DW IP Finder.



- Select DHCP to allow the camera to receive its IP address automatically from the DHCP server.
- Select "Static" to manually enter the camera's IP address, (Sub) Netmask, Gateway and DNS information.

  * The camera's IP must be set to Static if connecting to Spectrum® IPVMS.
- Contact your network administrator for more information.

- Default TCP/IP information: DHCP

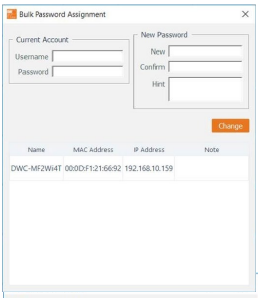
5. When connecting to the camera for the first time, a password must be set. To set up a password for your new camera:

    a. Check the box next to your new camera in the IP Finder's search results. You can select multiple cameras.

    b. Click "Bulk Password Assign" on the left.

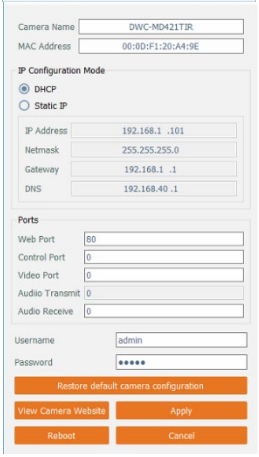
    c. In the pop-up window, enter admin/ admin in the current username and password fields. Enter a new username and password to the right.

    d. Press "change" to apply all changes.



6. Select a camera from the list by double-clicking on the camera's image or clicking on the 'Click' button under the IP Conf. column. The pop-up window will show the camera's current network settings, allowing admin users to adjust the settings as needed.

7. To access the camera's web page, go to the IP Config page and click on 'View Camera Website'. To save the changes made to the camera's settings, input the username and password of the camera and click Apply.



'Port forwarding' has to be set in your network's router for external access to the camera.

4 Live View

Once the camera's network settings have been set up properly, you can access the camera's web viewer.

To open the camera Web Menu using the DW IP Finder application:

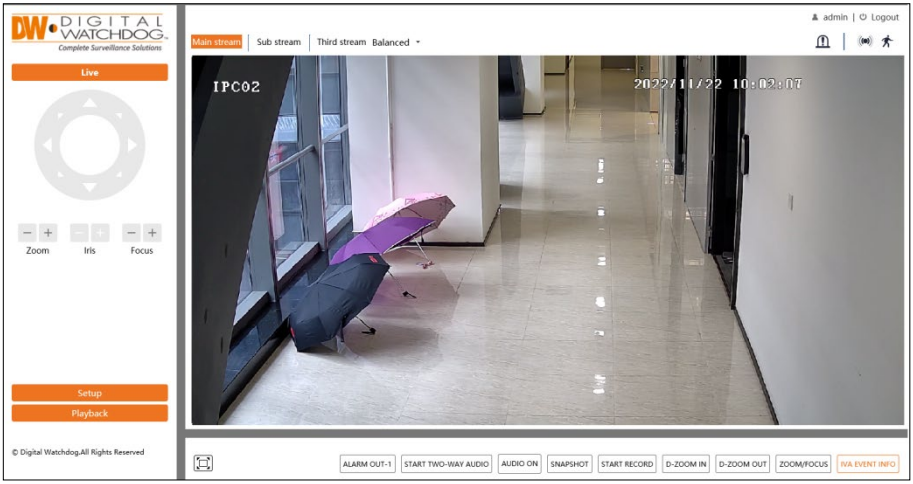
1. Scan the network for the IP camera using DW IP Finder.
2. Double-click on the camera's view in the results table.
3. Press the 'View Camera Website' button. The camera's web viewer will open up in your default web browser.
4. Enter the camera's username and password to log in to the camera. (default username/password: admin/admin).

To open the camera Web Menu using a web browser:

1. Open a web browser.
2. Enter the camera's IP address and port into the address bar. Example: http://<ipaddress>:<port>. Port forwarding may be necessary to access the camera from a different network. Contact your network administrator for more information.
3. Enter the camera's username and password to log in to the camera.



Note: If you are accessing the camera with a web browser for the first time, you must set an Admin password for the camera. After logging in, the following window will be shown:



Icon	Description	Icon	Description
	Fullscreen		SD card recording indicator
ALARM OUT-1	Turn alarm output on/off.		Sensor alarm (on supported models)
START/STOP TWO-WAY AUDIO	Start/stop two-way audio (on supported models)		Motion alarm (on supported models)
AUDIO ON/OFF	Turn on/off audio (on supported models)		Color abnormal
SNAPSHOT	Snapshot		Abnormal clarity
START RECORD	Start/stop local recording (on supported models)		Scene change
D-ZOOM IN	Digital zoom in the live image		Line crossing
D-ZOOM OUT	Digital zoom out the live image		Alarm output
ZOOM/FOCUS	AZ control (only available for cam models with motorized zoom lens)		Perimeter Intrusion
IVA EVENT INFO	Event rule information display		

Smart alarm indicators will flash only when the camera supports those functions and events are enabled.

In fullscreen mode, you can double-click with the mouse or press the ESC key on the keyboard to exit the fullscreen view.

Click the ZOOM/FOCUS button to show the AZ control panel. This is available on supported models.

Icon	Description	Icon	Description
	Zoom -		Zoom +
	Focus -		Focus +
	One key focus (use after manual lens adjustment and the image is out of focus)		

5 Network Camera Configuration

In the camera's web client, click on the "Setup" tab at the top right to go to the setup menu.

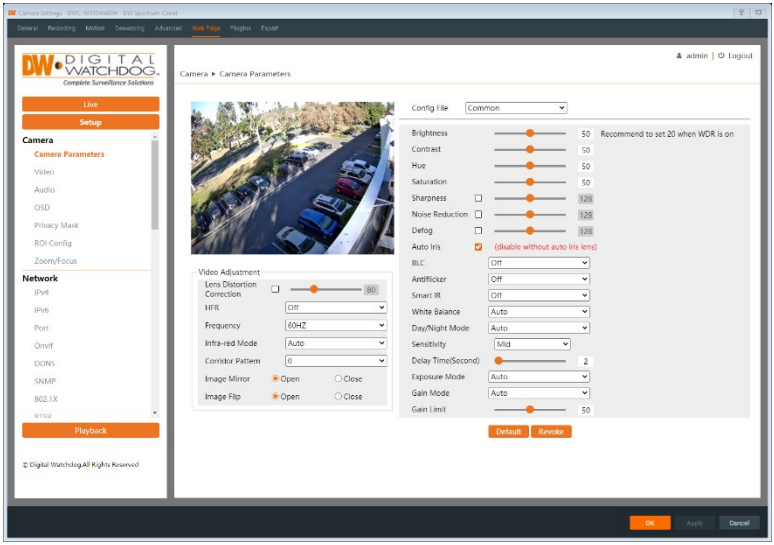
Note: Click the "Save" button to save any changes to the settings before changing menus.

5.1 Camera Configuration

Camera Configuration includes Display, Video/Audio, OSD, Video Mask and ROI (region of interest) setup.

5.1.1 Camera Parameters

Go to the Setup> Camera> Camera Parameters interface as shown below. The image's brightness, contrast, hue and saturation settings for Common, Day mode, and Night Mode can be set up separately. Changes to the image can be quickly seen by switching the Configuration File type.



Brightness: Set the brightness level of the camera's image.

Contrast: Set the color gradient between the brightest/darkest parts of the image.

Hue: Set the total color degree of the image.

Saturation: Set the degree of color purity. A high *Saturation* will make the image appear more vibrant.

Sharpness: Set the resolution level of the image plane and the sharpness level of the image edge.

Noise Reduction: Decrease the visual noise to make the image appear less grainy due to electronic interference. Increasing this value will make the image clearer but will also reduce the image resolution.

Defog: Clear the camera's image in a foggy, dusty, smoggy, or rainy environment.

Auto Iris: If your camera is using a motorized auto-focus iris lens, enable this setting to allow the camera to automatically focus the image after zooming in/out.

Backlight Compensation (BLC):

- Off (default): Turn off the backlight compensation function.
- HWDR: When enabled, a wide dynamic range will automatically adjust the camera to provide a better image by balancing highly contrasted areas simultaneously in the field of view by lowering the brightness of the bright area and increasing the brightness of the dark area.

The stream will temporarily stop for a few seconds while the mode is changing from non-WDR to WDR mode.

- HLC: Highlight compensation will lower the brightness of the entire image by suppressing overexposed areas of the image and will reduce the size of the light halo effect.
- BLC: backlight compensation will adjust camera auto-exposure to increase light exposure in the darkest areas of an image.

Anti-flicker:

- Off (default): Turn off the anti-flicker function. This is used mostly in outdoor installations.
- 50Hz: reduces flicker in 50Hz lighting conditions.
- 60Hz: reduces flicker in 60Hz lighting conditions.

Smart IR: Select "ON" or "OFF". This function will automatically prevent image overexposure and underexposure by controlling the brightness of the IR lights.

White Balance: Adjusts the color temperature to match the color of the environmental light source to give white objects a white coloration and a more natural appearance.

Day/Night Mode:

- Auto: automatically changes between Day mode and Night mode; depends upon the *Sensitivity* setting
- Day: forces the camera to remain in the full-color mode
- Night: forces the camera to remain in black/white image and

- Timing: the camera will switch day/night mode following a schedule.

Shutter Mode: Choose "Auto" or "Manual". If "Manual" is selected, the digital shutter speed can be adjusted.

Gain Mode: Choose "Auto" or "Manual". If "Auto" is selected, the gain value will be automatically adjusted according to the environment. If "Manual" is selected, the gain value shall be set manually. A higher value will result in a brighter image.

Lens Distortion Correction: If the image appears warped, enable this function and adjust the level to correct the distortion. (available for fisheye models only)

HFR: High Frame Rate. If "ON" is selected, the maximum frame rate of the Main stream can be set to 60 fps /50fps.

Frequency: Select either 50Hz (EU/Asia) or 60Hz (N/S America).

Infra-red Mode:

- Auto: The camera will automatically turn IR lights ON/OFF when switching between Day/Night modes.
- ON: forces camera IR lights to remain ON.
- OFF: forces camera IR lights to remain OFF.

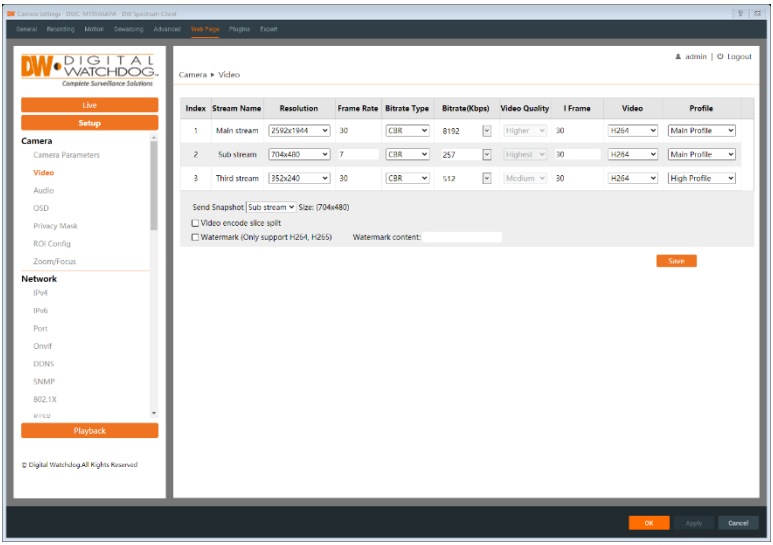
Corridor Pattern: Corridor viewing modes can be used for situations such as long hallways. 0 (default), 90, 180 and 270-degree options are available. The video resolution should remain at 1080p or below if this function is used.

Image Mirror: invert the current video image horizontally.

Image Flip: Invert the current video image vertically.

5.1.2 Video Configuration

Go to Setup>Camera >Video interface as shown below. In this interface, set the resolution, frame rate, bitrate type, and video quality of the camera, depending on network conditions.



Three video streams can be adjusted.

Resolution: Adjusts the camera stream resolution.

Frame rate: Adjusts image FPS (frames per second). A high frame rate results in a smoother video.

Bitrate type:

- CBR: constant bitrate; compression bitrate is kept constant and allows video quality to vary.
- VBR: variable bitrate; compression bitrate will be adjusted according to scene changes. For example, for scenes that do not have much movement, the bitrate will be kept at a lower value. This can help optimize network bandwidth usage.

Bitrate (CBR must be enabled) determines processing power for video streaming, where a higher bitrate results in better image quality.

Video Quality: (VBR must be enabled); The higher the image quality, the higher the bitrate will be required.

I-Frame interval: Determines how many partial frames (P-frames) may be inserted between full frames (group of pictures) in the video stream. If there is not much movement in the scene, setting the value higher than the frame rate

may potentially result in less bandwidth usage. However, if the value is set too high and there is a high frequency of movement in the video, there is a risk of frame skipping.

Video Compression: Determines the maximum data rate and video resolution for a video stream. Select H.264, H.265, or MJPEG (unavailable for the Main stream) according to system storage requirements.

Profile: (H.264) Baseline, main and high profiles are selectable.

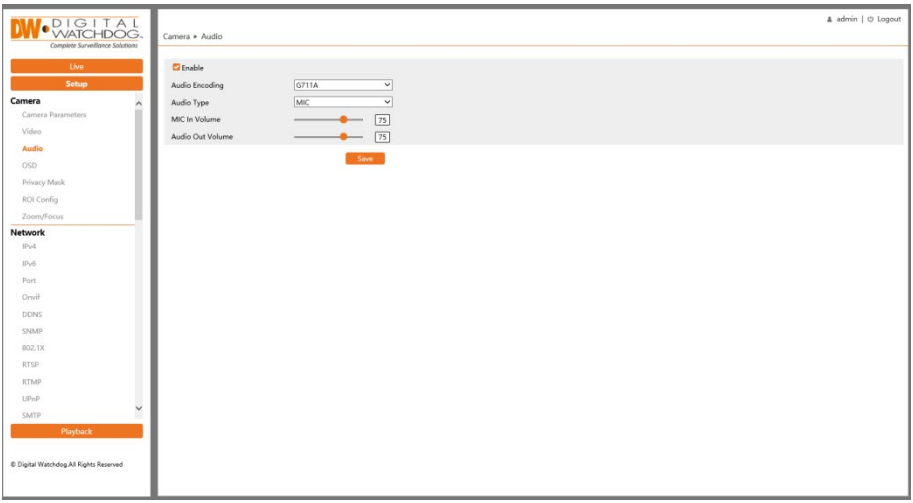
Send Snapshot: Select how many snapshots to generate when sending event notifications.

Videos encode slice split: Enable this function to improve the camera image when using a low-performance PC.

Watermark: Enable the display of a watermark when viewing locally recorded video playback in the search interface. Text entered into *Watermark content* will display.

5.1.3 Audio Configuration

Go to Setup>Camera>Audio as shown below. In this interface, set the audio settings required for your setup. (Availability varies by model).



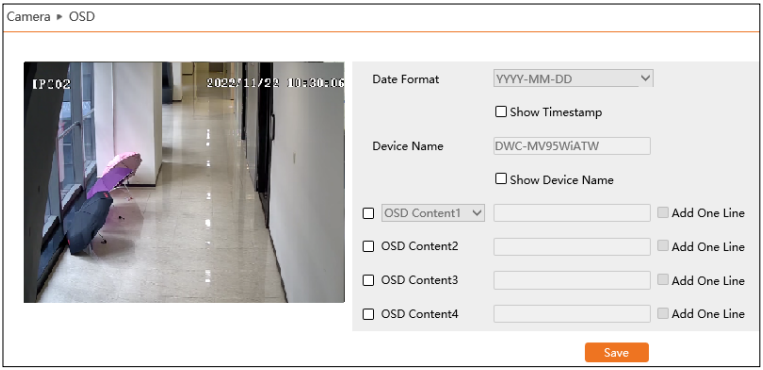
The audio can be turned on or off as needed.

Audio Encoding: G711A and G711U are selectable.

Audio Type: LIN. And MIC (available for camera models with built-in microphones only) is selectable.

5.1.4 OSD Configuration

Go to Setup>Camera>OSD interface as shown below. In this interface, set the on-screen display that will overlay the camera video.



Date Format: Set how the calendar date will appear; enable "*Show Timestamp*" to include the current time.

Device Name: Enable "*Show Device Name*" to display the model number in the overlay.

OSD Content: Add additional lines of text to the overlay.

After enabling the OSD settings, you may drag and drop to reposition the overlay items. Click the "Save" button to save any setting changes.

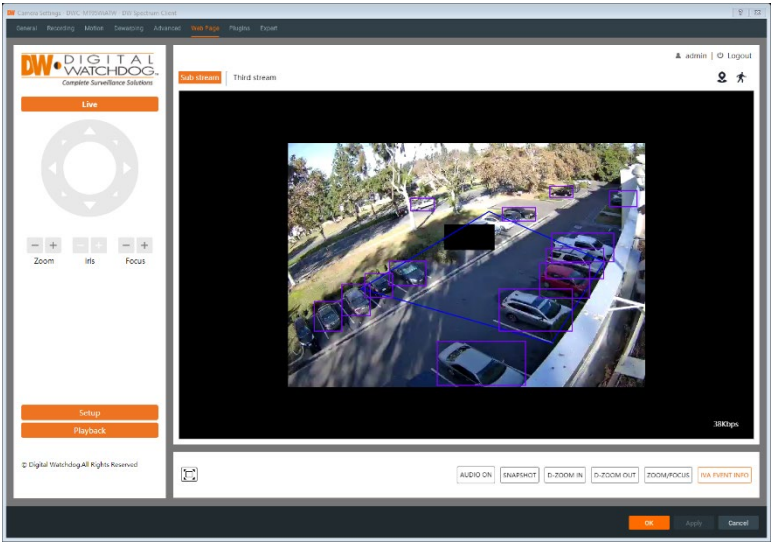
5.1.5 Privacy Mask

Go to the Setup> Camera> Privacy Mask interface as shown below. A maximum of 4 zones can be set up. In this interface, you can create privacy mask zones to black out areas of the camera image.



To set up a video mask:

1. Enable Video Mask.
2. Click the "Draw Area" button and draw the video mask area.
3. Click the "Save" button to save the settings.
4. Return to viewing the live video to verify that the area masking appears correctly.

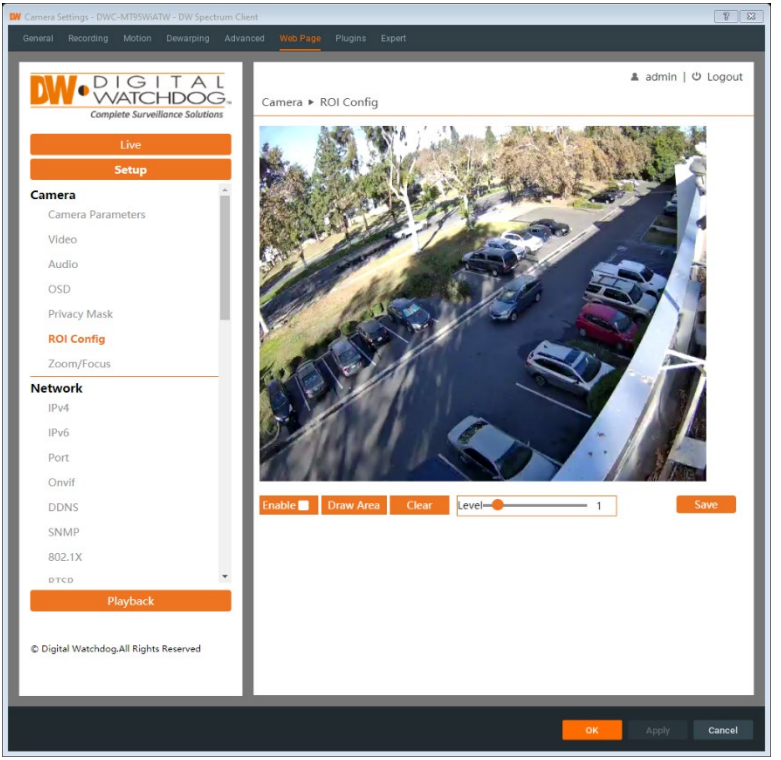


To clear the video mask:

Click the "Clear" button to delete the currently selected video mask area.

5.1.6 ROI Configuration

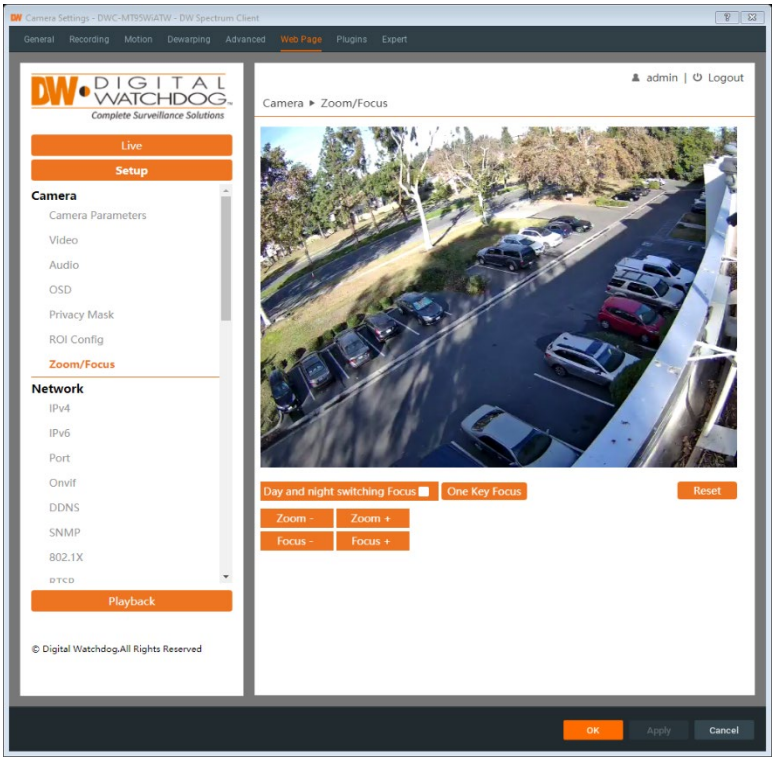
Go to Setup>Camera>ROI Config interface as shown below. An area in the image can be set as a region of interest. This area will have a higher bitrate than the rest of the image, resulting in better image quality for the selected ROI area.



1. Check "Enable" and then click the "Draw Area" button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the "Save" button to save the settings.

5.1.7 Zoom/Focus

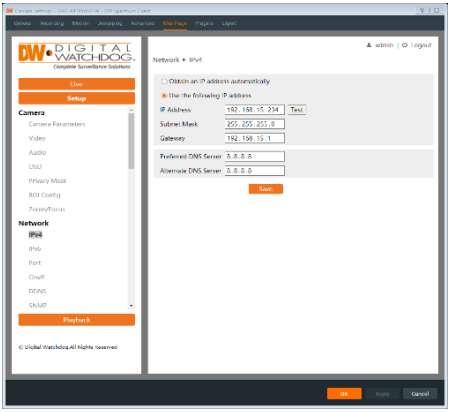
This function is only available for models with a motorized zoom lens. Within this section, zoom and focus can be controlled. If the image is out of focus after a manual adjustment, one-key focus can be used to set the focus automatically. Go to Setup>Camera>Zoom/Focus interface to set.

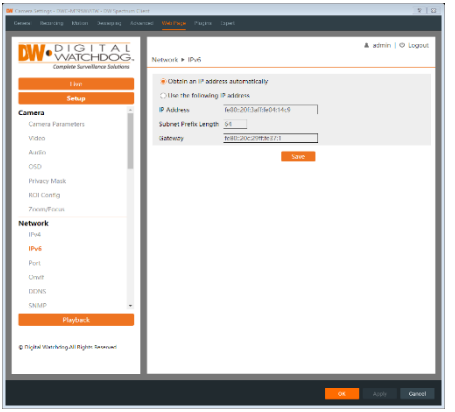


5.2 Network Configuration

5.2.1 IPv4 and IPv6

Go to Setup>Network>IPv4/IPv6 interface as shown below. There are two ways to set up the network connection.





Obtain an IP address automatically: (DHCP) the camera will automatically be assigned an IP address from a connected DHCP server or router.

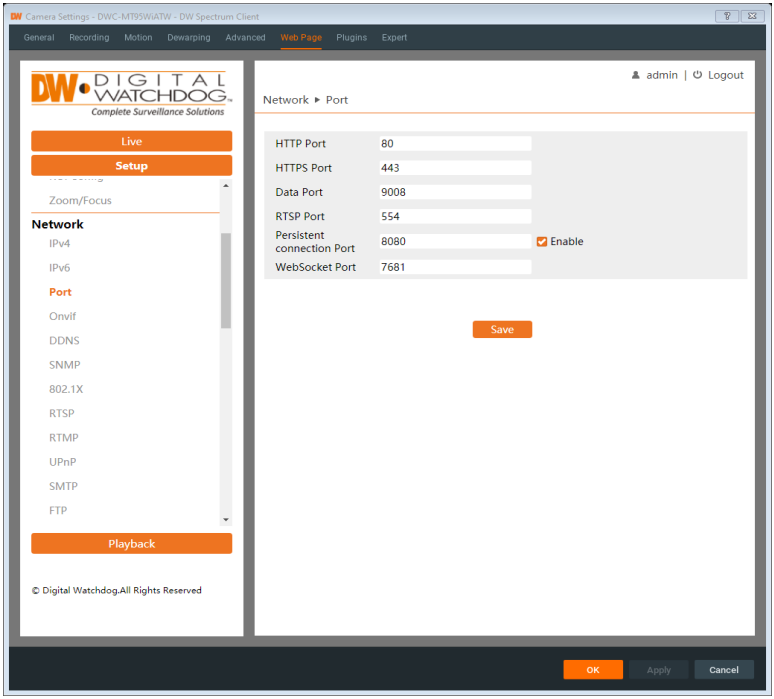
Use the following IP address: Manually assign an IP address to the camera; you must also manually assign the Subnet Mask and Gateway settings.

Test: Test the effectiveness of the IP address by clicking this button.

DNS Server: Set the address of the preferred routing server for external network connections.

5.2.2 Port

Go to Setup>Network>Port interface as shown below. HTTP port, Data port and RTSP port can be set.



HTTP Port: The default HTTP port is 80. It can be changed to any port that is not occupied.

HTTPS Port: The default HTTPS port is 443. It can be changed to any port that is not occupied. (Some models may not support it).

Data Port: The default data port is 9008. Please change it as necessary.

RTSP Port: The default port is 554. Please change it as necessary.

Persistent Connection Port: The port is used for a persistent connection of the third-party platform to push smart data, like face pictures.

WebSocket Port: Communication protocol port for a plug-in-free preview.

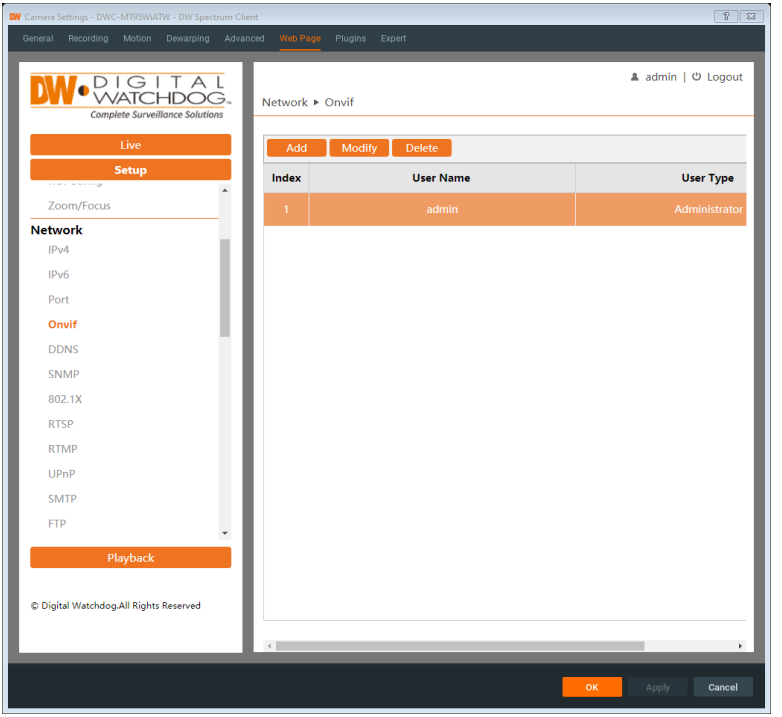
5.2.3 ONVIF

NOTE: In firmware updates 5.1.2.0.54839 and newer, the 'Onvif' configuration menu has been merged with the 'User' menu for streamlined user management.

Go to Setup>Network>ONVIF interface as shown below. The camera can be searched and connected with ONVIF-compliant platforms via the ONVIF/RTSP protocol.

If "Activate ONVIF User" is enabled in the device activation interface, the ONVIF user can be activated simultaneously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use this ONVIF user profile to authenticate connections with the camera.

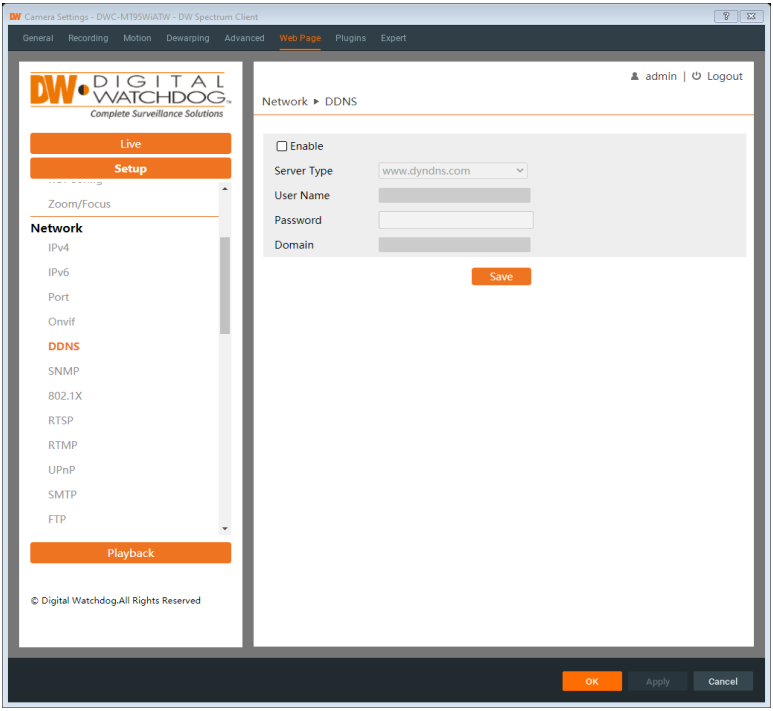
You can also add additional ONVIF users to this interface if needed.



5.2.4 DDNS

Go to Setup>Network>DDNS interface as shown below. If the camera is set up with a DHCP connection, DDNS can be set to create a URL for Internet connections. To set up DDNS:

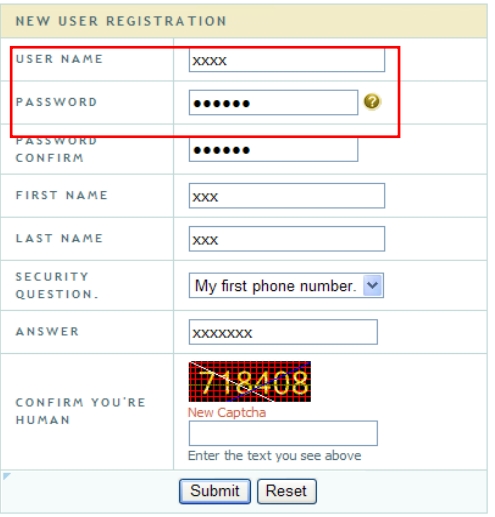
1. Go to Setup>Network>DDNS.



2. Apply for a domain name using a DDNS service.

For example, www.dvrdyndns.com:

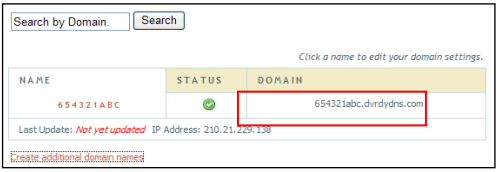
Enter www.dvrdydns.com in the IE address bar to visit its website. Then click the "Registration" button.



Create a domain name.



After the domain name is successfully applied, the domain name will be listed below.



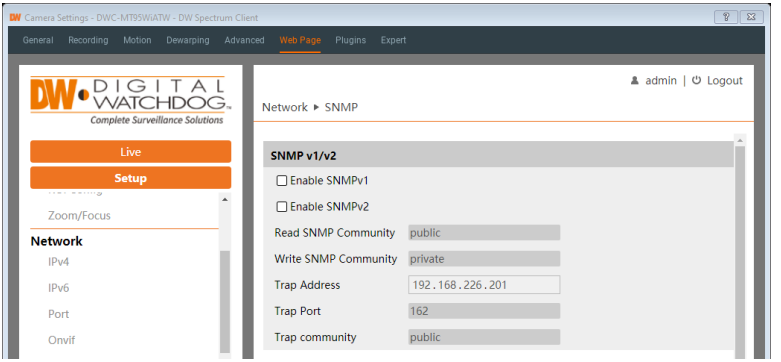
3. Enter the username, password, and domain in the DDNS configuration interface.

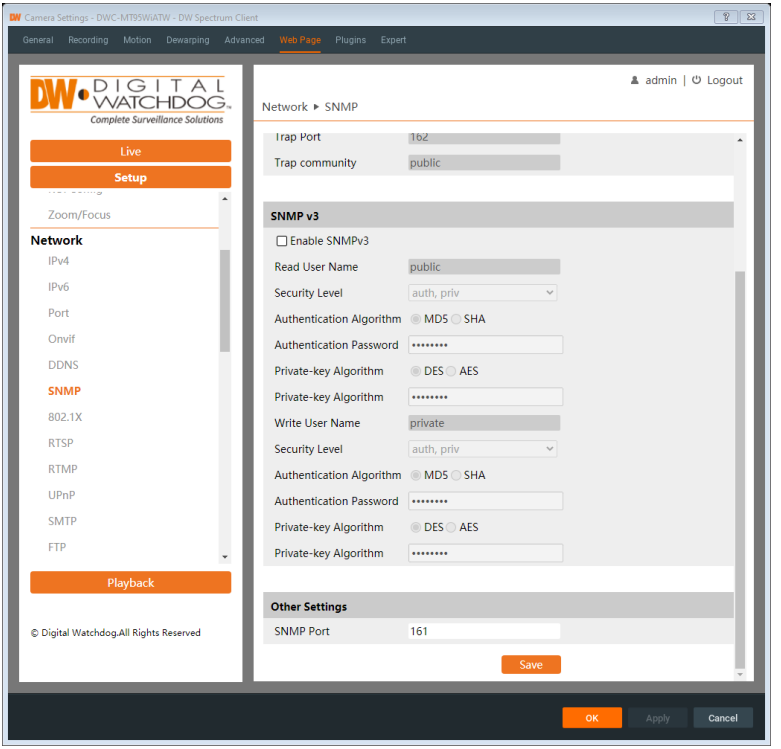
4. Click the "Save" button to save the settings.

5.2.5 SNMP

Go to Setup>Network>SNMP interface as shown below. The SNMP function can be used to get camera status, parameters and alarm information, or to remotely manage the camera. Before using SNMP, install an SNMP management tool (not included) and set the parameters such as the SNMP port and trap address.

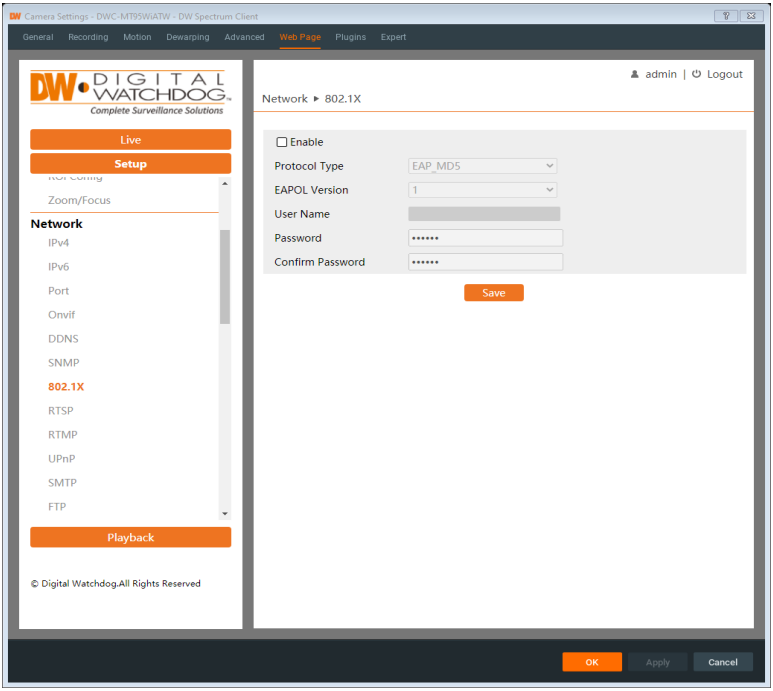
1. Go to Setup>Network>SNMP.
2. Configure the SNMP registration information according to the SNMP management tool.
3. Click the "Save" button to save the settings.





5.2.6 802.1x

Go to Setup>Network>802.1X interface as shown below. When enabled, the camera's data can be protected using an authentication framework for port-based Network Access Control (PNAC) setups. When the camera is connected to the network with IEEE 802.1X, user authentication will be required.



To use this function, the camera shall be connected to a network switch supporting the 802.1x protocol. The network switch can be regarded as an authentication system that is used to find the camera in a local network. If the camera connected to the network interface of the network switch has passed the authentication of the switch, it can be accessed through the local network.

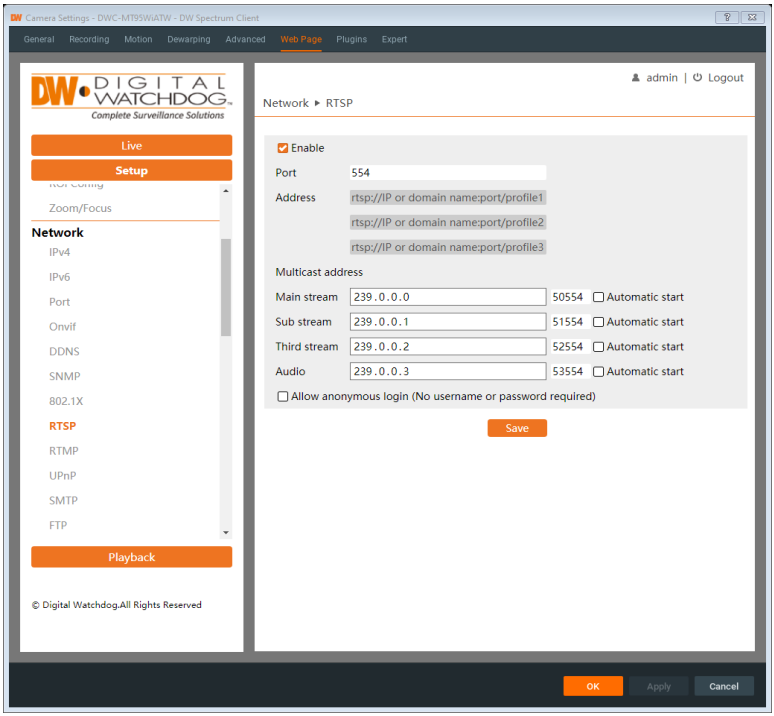
Protocol Type: Keep the default settings.

EAPOL Version: Keep the default settings.

Username/Password: The username and password must be the same as the username and password that are registered in the authentication server.

5.2.7 RTSP

Go to Setup>Network>RTSP interface as shown below. The camera's Real-Time Streaming Protocol (RTSP) stream is used for establishing and controlling media sessions between endpoints.



Select "Enable" to enable the RTSP function.

Port: Access port of the streaming media. The default number is 554.

RTSP Address: The RTSP address (unicast) format that can be used to play the stream in a media player. The address format is

Main stream: "rtsp://IP or domain name:port/profile 1"

Substream: "rtsp://IP or domain name:port/profile 2"

Third stream: "rtsp://IP or domain name:port/profile 3"

Multicast Address

Mainstream: The address format is

"rtsp://IP address: rtsp port/profile1?transportmode=mcast".

Substream: The address format is

“rtsp://IP address: rtsp port/profile2?transportmode=mcast”.

Third stream: The address format is

“rtsp://IP address: rtsp port/profile3?transportmode=mcast”.

Audio: After entering the main/substream into a VLC player, the video and audio will play automatically.

If "Allow anonymous login..." is checked, there is no need to enter the username and password to view the video.

If "autostart" is enabled, the multicast received data should be added to a VLC player to play the video.

Additional Note:

1. This camera supports local play through a VLC player. Enter the RTSP address (unicast or multicast, e.g., rtsp://192.168.226.201:554/profile1?transportmode=mcast) in a VLC player to realize the simultaneous play with the web client.

2. The IP address mentioned above cannot be the address of IPv6.

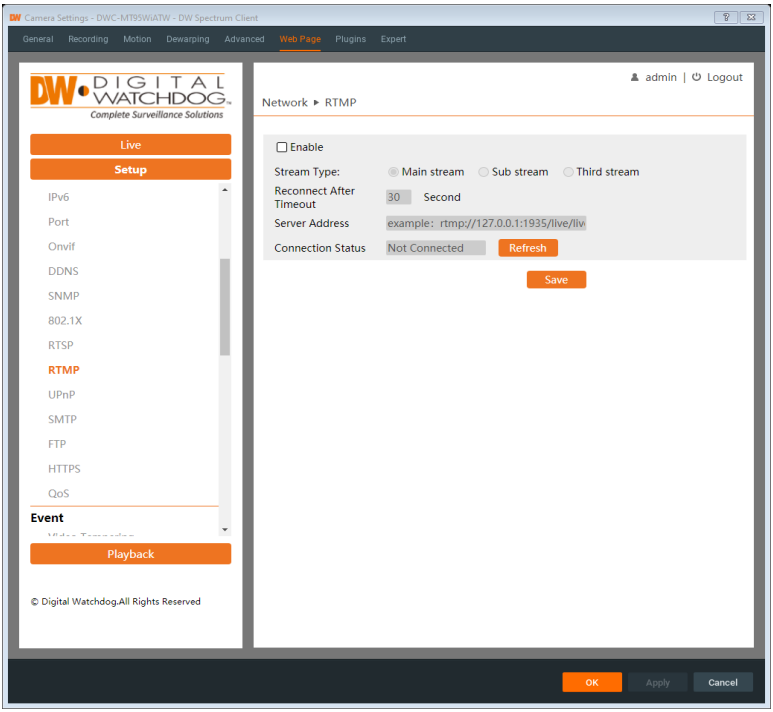
3. Avoid the use of the same multicast address in the same local network.

4. When playing the video through the multicast streams in a VLC player, please pay attention to the mode of the VLC player. If it is set to TCP mode, the video cannot be played.

5. If the coding format of the video of the Mainstream is MJPEG, the video may become disordered at some resolutions.

5.2.8 RTMP

You can provide access to third-party websites to host the camera's live stream using a Real-Time Messaging Protocol (RTMP). Go to Setup→Network→RTMP interface as shown below.



To use RTPM, check "Enable" and configure the following:

Stream Type: Select the video stream that will be sent to the third-party host.

Reconnect After Timeout: If the connection is lost between the camera and the host, the camera will automatically attempt to reconnect with the host after the set amount of time (seconds)

Server Address: Enter the third-party server address to which the stream data will be sent.

Connection Status: Click "Save" to apply the changes, then click "Refresh" to view the connection status.

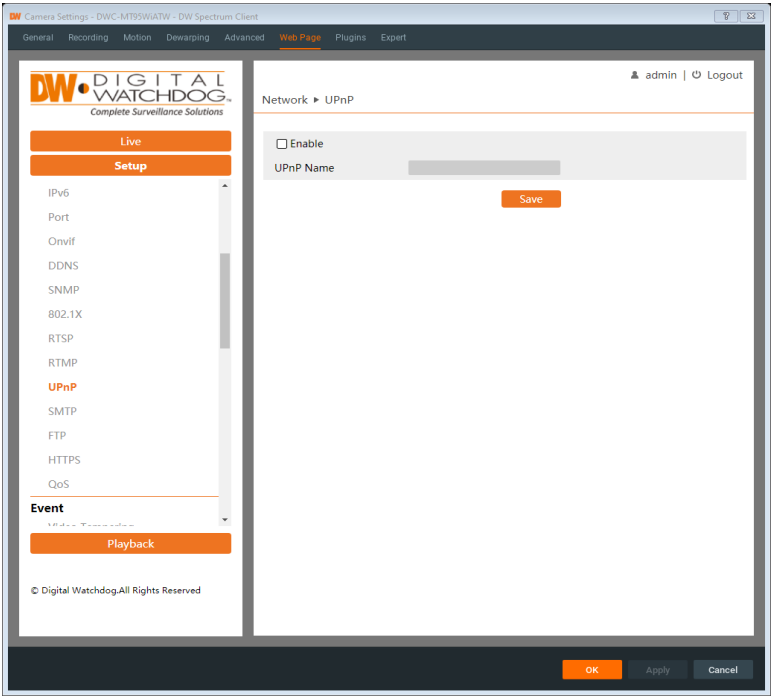
5.2.9 UPNP

If this function is enabled, the camera can be quickly accessed through the LAN.

Go to Setup>Network>UPnP interface as shown below.

To use UPnP, enable UPNP and enter the UPnP name.

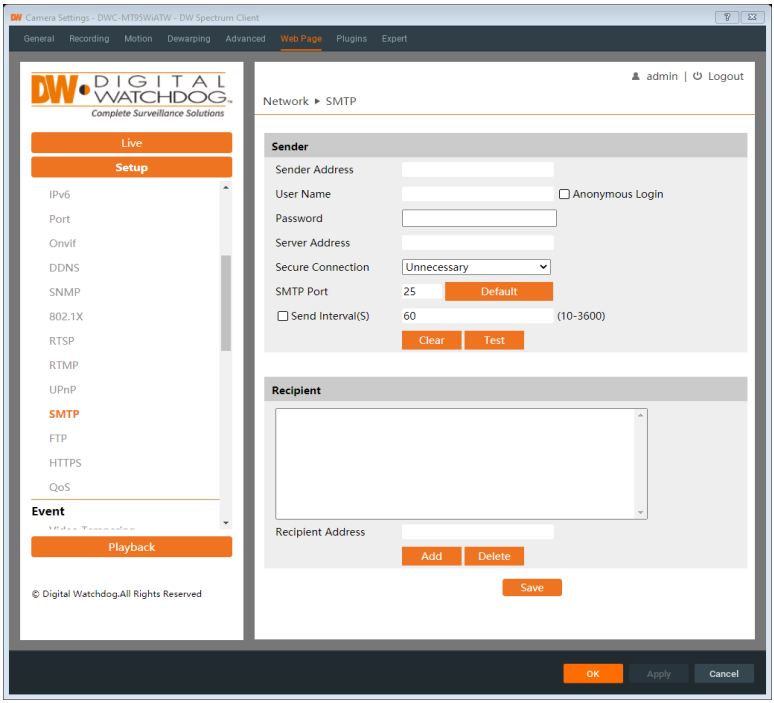
Click "Save" to apply the changes.



5.2.10 SMTP

If you need to send an e-mail notification directly from the camera when an alarm is triggered or the IP address is changed, configure the following:

Go to Setup>Network >SMTP interface as shown below.



Sender Address: The camera does not come with its own e-mail service. Enter the sender's e-mail address to provide an e-mail service.

Username/Password: Enter the sender's e-mail address and password to provide authentication.

Server Address: Enter the SMTP IP address or hostname of the e-mail service. For example, "smtp.gmail.com".

Secure Connection: Select the connection type as needed.

SMTP Port: Enter the SMTP port value of the SMTP server according to your e-mail service. This may differ depending on whether the e-mail service uses SSL or TLS security protocols.

Send Interval(S): The time interval of sending the e-mail. For example, if it is set to 60 seconds and multiple motion detection alarms are triggered within 60 seconds, they will be considered as only one alarm event, and only one e-mail will

be sent. If another motion alarm event is triggered after 60 seconds, a second e-mail will be sent. To send multiple event alerts simultaneously, multiple event rules must be made separately.

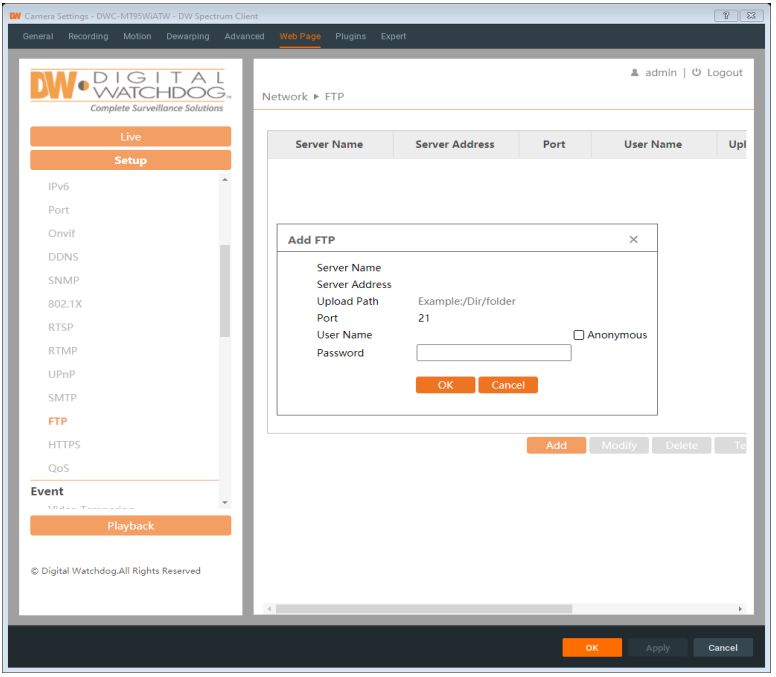
Test: Click this button to test the SMTP connection after configuring the settings.

Recipient Address: Enter the e-mail address that will be receiving the notification. If a message should be included with the e-mail, enter it in the text box. Click "Add" to add a recipient.

Click "Save" to apply changes to the settings.

5.2.11 FTP

After an FTP server is set up, captured pictures from events will be uploaded to the FTP server. Go to Setup>Network >FTP interface as shown below.



To add an FTP server:

1. Click "Add" to enter the FTP information, then configure the following:

Server Name: Enter the name of the FTP server.

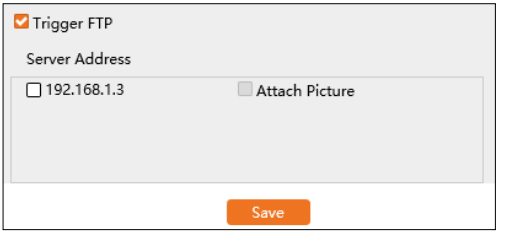
Server Address: Enter the IP address or domain name of the FTP server.

Upload Path: Enter the file directory where files will be uploaded.

Port: Enter the port of the FTP server.

Username and Password: Enter the username and password that are used to log in to the FTP server.

2. Click "Save" to apply the changes. In the event setting interface, trigger FTP as shown below.



Rule of FTP storage path: /device MAC address/event type/date/time/
For example, a face detection alarm occurs.
FTP file path: \00-18-ae-a8-da-2a\VFD\2021-01-09\14 \
Event name table:

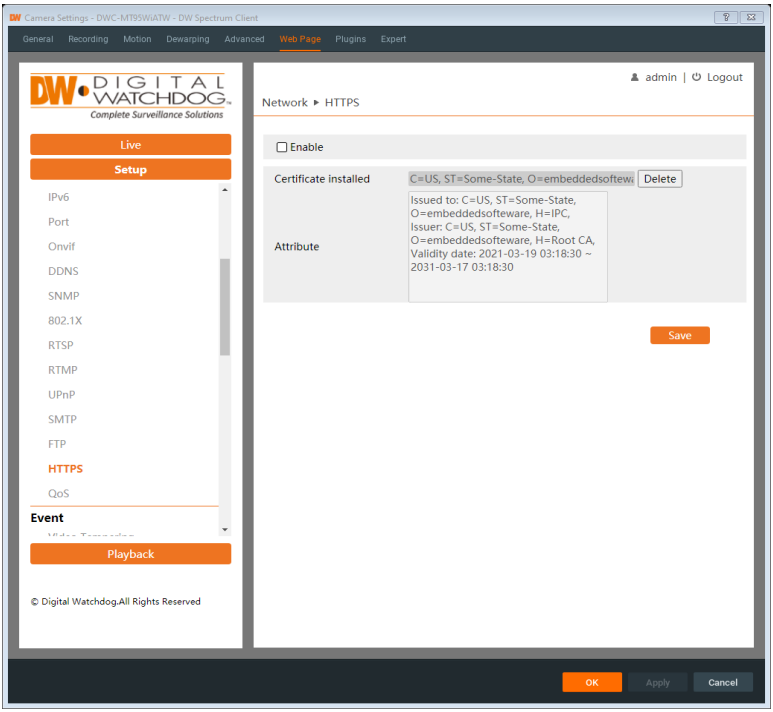
File Name	Event Type
MOTION	Motion Detection
SENSOR	Sensor Alarm
TRIPWIRE	Line Crossing Detection
PERIMETER	Region Intrusion Detection
AVD	Video Exception
SDFULL	SD Full
SDERROR	SD Error

TXT file content:
device name: xxx mac: device MAC address Event Type time:
For example:
device name: IPC mac: 00-18-ae-a8-da-2a MOTION time: 2021-03-16 12:20:07

5.2.12 HTTPS

HTTPS certificate supplies encryption for the camera and protects user privacy when streaming video.

Go to Setup >Network>HTTPS interface as shown below.



There is a self-signed SSL certificate installed by default, as shown above.

Enable this function and save it to encrypt the camera. The camera can then be accessed over an HTTPS connection by entering the camera URL.

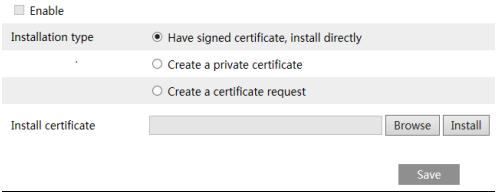
The URL format is: “https://<IP Address>:<HTTPS port>”

Example: *https://192.168.1.80:443*

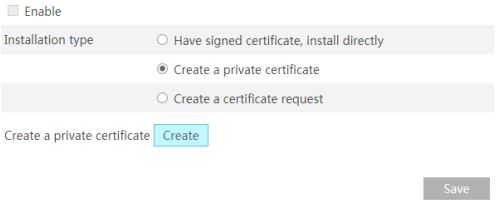
Private Certificate Note

A private SSL certificate can be applied instead if users do not want to use a self-signed certificate created by the camera.

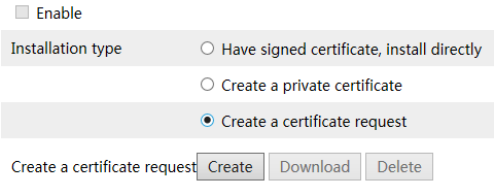
Click "Delete" to remove the default certificate. The following interface will be displayed.



- **Have signed certificate, install directly:** Select if there is a signed certificate already available. Copy the certificate to the computer, then click "Browse" to select it from the file directory. Click "Install" to add it to the camera.
- **Create a private certificate:** Select to create a certificate manually. Click the "Create" button to create a private certificate. Enter the country (only two letters available), domain (camera's IP address/domain), validity date, password, province/state, region and so on. Then click "OK" to save the settings.



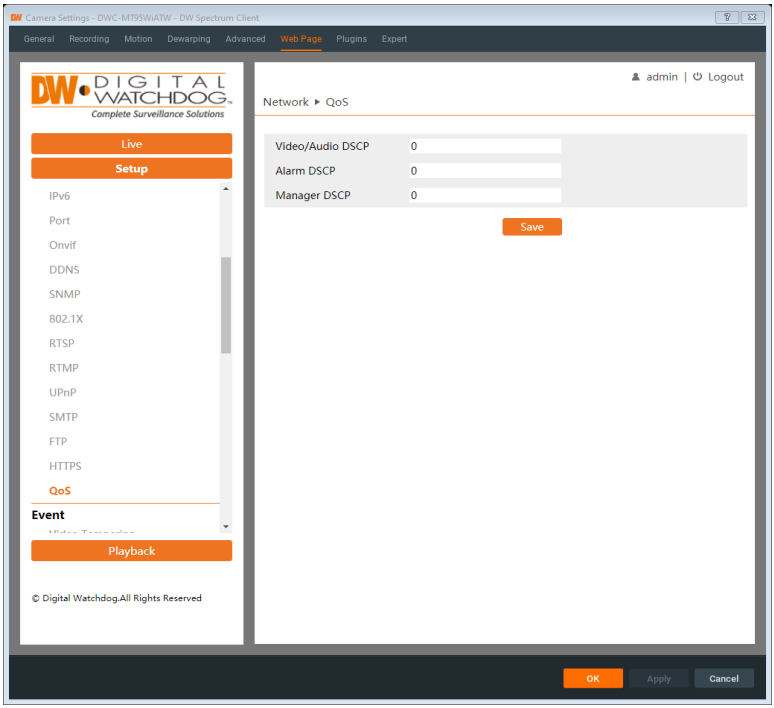
- **Create a certificate request:** Select to request a private certificate. Click "Create" to create the certificate request. Then download the certificate request and send it to the trusted certificate authority for signature. After receiving the signed certificate, import the certificate to the device.



5.2.13 QoS

QoS (Quality of Service) function is used to supply different quality services for different network applications. With a deficient bandwidth, the router or switch will sort the data streams and transfer them according to their priority to resolve network delay and network congestion by using this function.

Go to Setup>Network>QoS interface as shown below.



Configure the QoS priority. Generally speaking, the higher the range number, the higher the priority will be.

Video/Audio DSCP: Set the Video/Audio DSCP priority (0~63)

Alarm DSCP: Set the Alarm DSCP priority (0~63)

Manager DSCP: Set the Manager DSCP priority (0~63).

5.3 Event Configuration

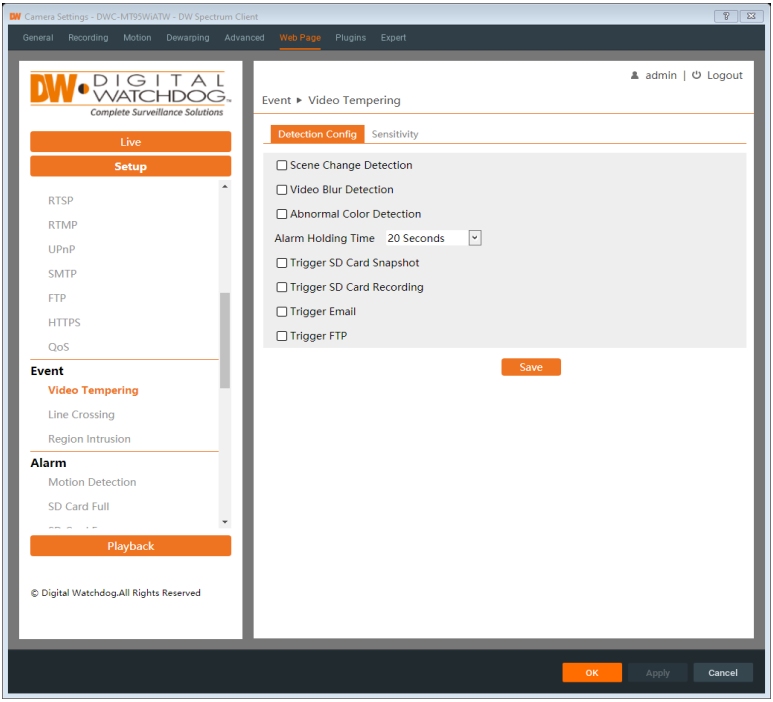
For more accuracy, here are some recommendations for installation.

- Cameras should be installed on stable surfaces, as vibrations can affect the accuracy of detection.
- Avoid pointing the camera at reflective surfaces (like shiny floors, mirrors, glass, lake surfaces and so on) that may blind the camera.
- Avoid places that are narrow or that have too much shadowing.
- Avoid a scenario where the target object color is similar to the background environment color. For example, a red vase in front of a red-painted wall.
- At any time of day or night, please make sure the image of the camera is clear and with adequate and even light, avoiding overexposure or too much darkness on both sides.

5.3.1 Video Tampering Detection

This function can detect changes in the surveillance environment affected by external factors such as bagging, spraypainting the camera, and other attempts to sabotage the camera.

Go to the Config>Event>Video Tampering Detection interface as shown below.



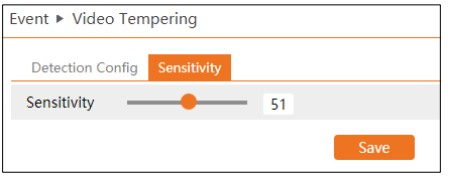
To set Video Tampering detection:

1. Enable the applicable detection types as desired.
    - **Scene Change Detection**: Alarms will be triggered if the scene of the monitor video has changed.
    - **Video Blur Detection**: Alarms will be triggered if the video becomes blurry.
    - **Abnormal Color Detection**: Alarms will be triggered if the image is abnormal due to color deviation.

2. Set the "Alarm Holding Time" and alarm trigger actions if tampering is detected. The setup steps are the same as for motion detection. Please refer to the Motion Detection (2.4.1) section of this user manual for details.

3. Click the "Save" button to save the settings.

4. To set the sensitivity of the Video Tampering detection types, click the "Sensitivity" tab to go to the interface as shown below.



Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox. Click the "Save" button to save the settings.

The sensitivity value of Scene Change Detection: The higher the value is, the more sensitive the system is to the amplitude of the scene change.

The sensitivity value of Video Blur Detection: The higher the value, the more sensitive the system is to the blurriness of the image.

The sensitivity value of Abnormal Color Detection: The higher the value, the more sensitive the system is to the color shift of the image.

※ The requirements of the camera and the surrounding area for Tampering Detection:

1. Auto-focus should not be enabled for video tampering detection.

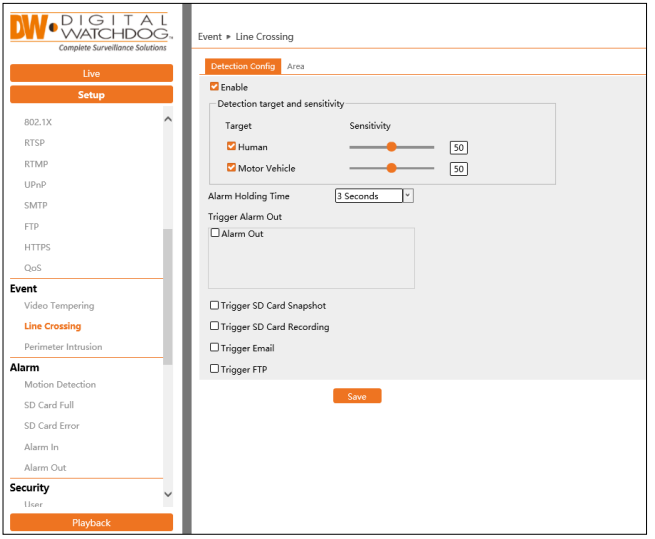
2. Try not to enable video tampering detection when light changes will vary significantly in the environment.

3. Please contact us for more detailed application scenarios.

5.3.2 Line Crossing

Line Crossing: Alarms will be triggered if the target crosses the pre-defined alarm lines.

Go to Setup>Event>Line Crossing interface as shown below.



To set up Line Crossing:

1. Enable the line crossing alarm and select the detection target.

Detection Target and sensitivity: select the object target types that will trigger the Line Crossing alarm. All object types can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if line-crossing detection is enabled.

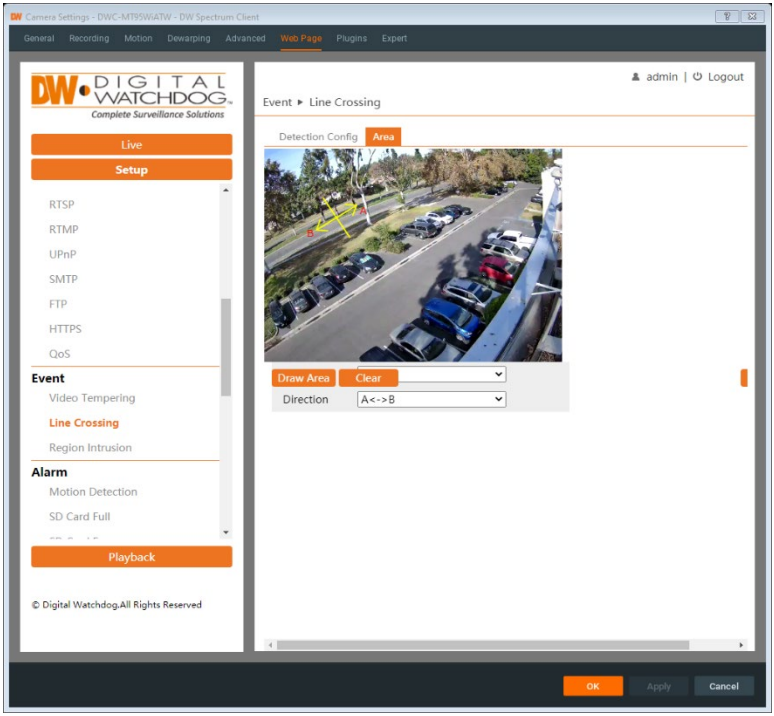
- **Human:** The alarm will be triggered if someone crosses the pre-defined alarm lines.
- **Motor Vehicle**: The alarm will be triggered if a vehicle with four or more wheels (eg., a car, bus, or truck) crosses the pre-defined alarm lines.

2. Set the alarm holding time for how long the alert will remain active after triggering.

3. Set alarm trigger options. The setup steps are the same as for motion detection. Please refer to the Motion Detection (2.4.1) section for details.

4. Click the "Save" button to save the settings.

5. Set the area and sensitivity of the line crossing alarm. Click the "Area and Sensitivity" tab to go to the interface as shown below.



6. Set the alarm line number and direction. Up to 4 lines can be added. Multiple lines cannot be added simultaneously.
   - **Direction**: A<->B, A->B, and A<-B optional. This indicates the direction of someone or a vehicle crossing over the alarm line.
   - **A<->B**: Alarms will be triggered when someone or a vehicle crosses over the alarm line from B to A or from A to B.
   - **A->B**: Alarms will be triggered when someone or a vehicle crosses over the alarm line from A to B.
   - **A<-B**: Alarms will be triggered when someone or a vehicle crosses over the alarm line from B to A.
7. Click the "Draw Area" button and then drag the mouse to draw a line in the image. Click the "Stop Draw" button to stop drawing. Click the "Clear" button to delete the lines. Click the "Save" button to save the settings.
8. Set the schedule of the line-crossing alarm. The setup steps of the schedule are the same as the schedule recording setup. Refer to the Schedule Recording section for more details.

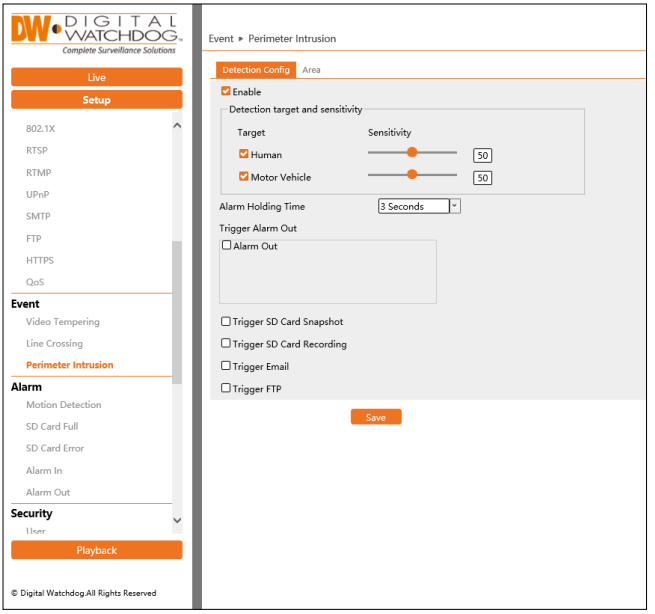
※ Configuration of the camera and surrounding area

1. The auto-focusing function should not be enabled for line crossing detection.
2. Avoid scenes with many trees or scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.
3. Cameras should be mounted at a height of 2.8 meters or above.
4. Keep the mounting angle of the camera at about 45°.
5. The detected objects should not be less than 1% of the entire image, and the largest sizes of the detected objects should not be more than 1/8 of the entire image.
6. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.
7. Adequate light and clear scenery are crucial for line-crossing detection.

5.3.3 Perimeter Intrusion

Perimeter Intrusion: Alarms will be triggered when a tracked target passes into the pre-defined exclusion areas. This function can apply to important supervised places or prohibited areas, like military administrative zones, high-danger areas, no-entry areas, etc.

Go to Setup>Event>Perimeter Intrusion interface as shown below.



Detection Target and Sensitivity

1. Select the target objects that will trigger the event and set the detection sensitivity.

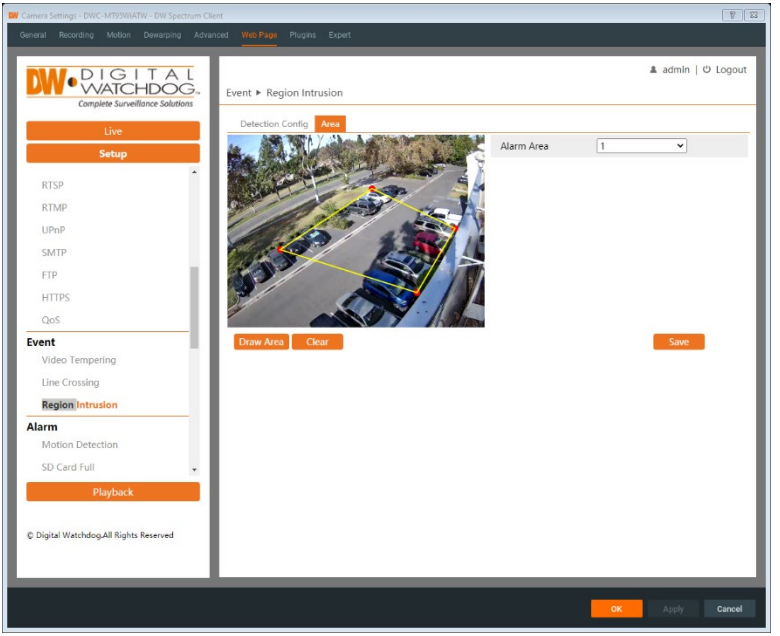
- **Human:** Select it, and then alarms will be triggered if someone intrudes into the pre-defined area.
- **Motor Vehicle**: Select it, and then alarms will be triggered if a vehicle with four or more wheels (e.g., a car, bus, or truck) intrudes into the pre-defined area.

2. Set the alarm holding time for how long the alert will remain active after triggering.

3. Set alarm trigger options. The setup steps are the same as Motion Detection. Refer to the Motion Detection section for details.

4. Click the "Save" button to save the settings.

5. Click the "Area" tab to set the alarm area for perimeter intrusion detection as shown below.



6. Set the alarm area number on the right side. Up to 4 alarm areas can be added.

Click the "Draw Area" button and then click around the area where you want to set it as the alarm area in the image on the left side (the alarm area should be a closed area).

Click the "Stop Draw" button to stop drawing.

Click the "Clear" button to delete the alarm area. Click the "Save" button to save the settings.

7. Set the schedule for the perimeter intrusion detection. The setup steps of the schedule are the same as the schedule recording setup (See Schedule Recording).

※ Configuration requirements of the camera and surrounding area

1. The auto-focusing function should not be enabled for perimeter intrusion detection.

2. Avoid scenes with many trees or scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.

3. Cameras should be mounted at a height of 2.8 meters or above.

4. Keep the mounting angle of the camera at about 45°.

5. The detected objects should not be less than 1% of the entire image, and the largest sizes of the detected objects should not be more than 1/8 of the entire image.

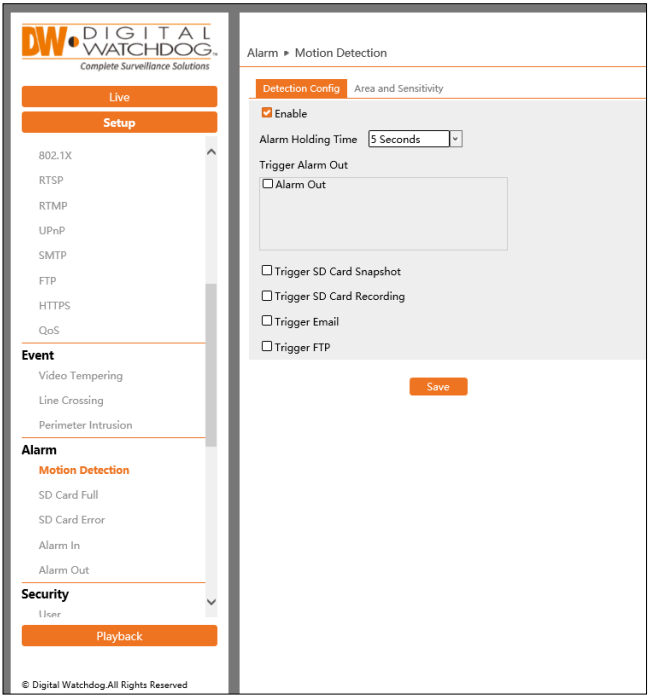
6. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.

7. Adequate light and clear scenery are crucial to perimeter intrusion detection.

5.4 Alarm Configuration

5.4.1 Motion Detection

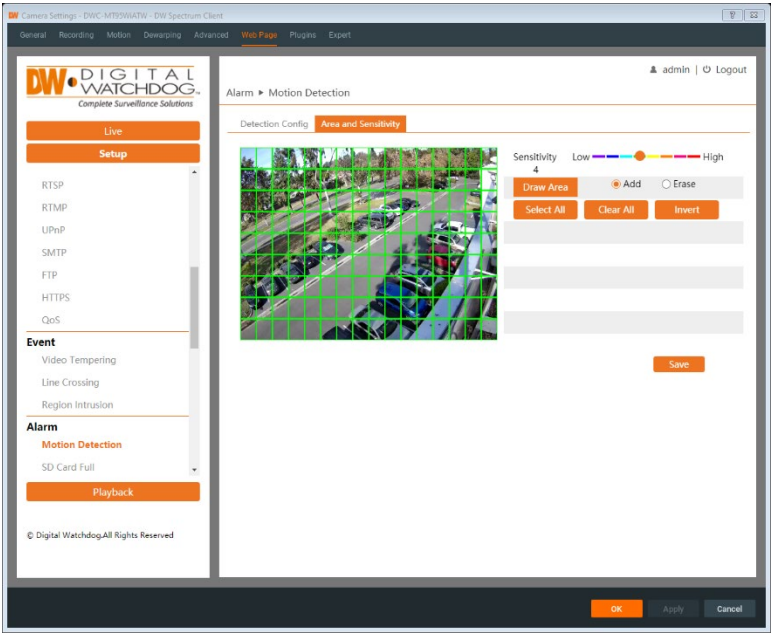
Go to the Setup> Alarm> Motion Detection interface as shown below to set a motion detection alarm.



1. Check the "Enable" checkbox to activate motion-based alarms. If unchecked, the camera will not send out any signals to trigger motion-based recording to the NVR or CMS, even if there is motion in the video.

- **Alarm Out:** If selected, this would trigger an external relay output that is connected to the camera on detecting a motion-based alarm.
- **Trigger SD Card Snapshot:** If selected, the system will capture images on motion detection and save the images on an SD card.
- **Trigger SD Card Recording:** If selected, the video will be recorded on an SD card on motion detection.
- **Trigger E-mail**: If "Trigger E-mail" and "Attach Picture" are checked (e-mail address must be set first in the E-mail configuration interface), the captured pictures and triggered event will be sent to those addresses.
- **Trigger FTP**: If "Trigger FTP" and "Attach Picture" are checked, the captured pictures will be sent to an FTP server address. Please refer to the FTP configuration section for more details.

2. Set motion detection area and sensitivity. Click the "Area and Sensitivity" tab to go to the interface as shown below.



3. Move the "Sensitivity" scroll bar to set the sensitivity. A higher sensitivity value means that motion will be triggered more easily.

Select "Add" and click "Draw". Drag the mouse to draw the motion detection area; Select "Erase" and drag the mouse to clear the motion detection area.

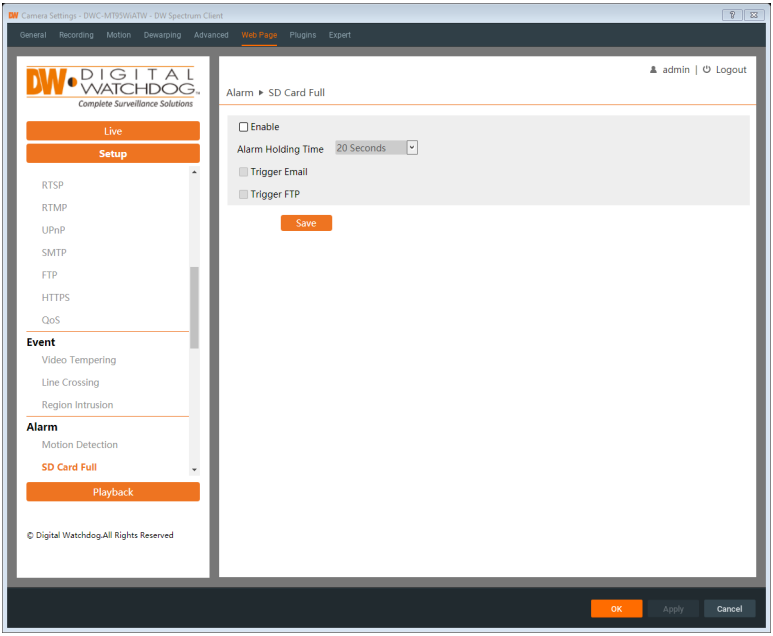
After that, click "Save" to save the settings.

4. Set the schedule for motion detection. The schedule setup steps for motion detection are the same as the schedule recording setup (See Schedule Recording).

5.4.2 Other Alarms

SD Card Full

1. Go to Setup>Alarm>SD Card Full interface as shown below.



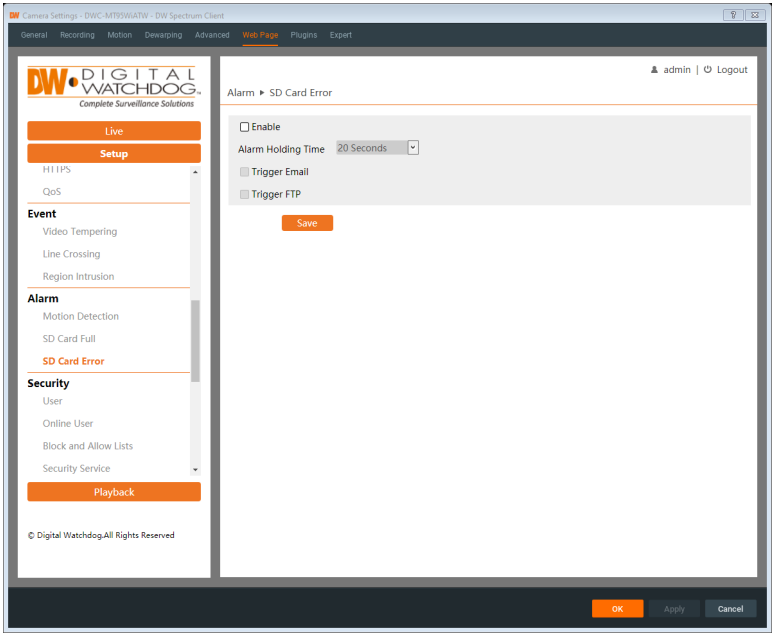
2. Click "Enable" and set the alarm holding time.

3. Set alarm trigger options. The setup steps are the same as for motion detection. Please refer to the Motion Detection (2.4.1) section for details.

SD Card Error

When there are errors in writing on the SD card, an alarm will be triggered.

1. Go to Setup>Alarm>SD Card Error as shown below.



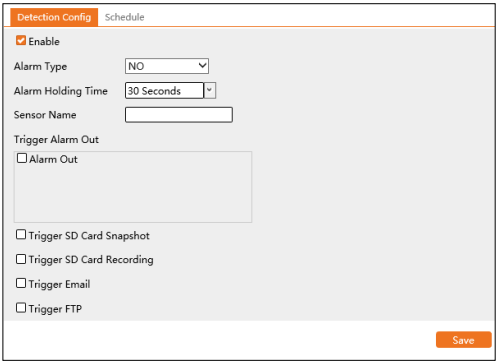
2. Click "Enable" and set the alarm holding time.

3. Set alarm trigger options. Trigger alarm out, e-mail and FTP. The setup steps are the same as for motion detection. Please refer to the Motion Detection (2.4.1) section for details.

5.4.3 Alarm In

This function is available for cameras with alarm input support. To set the sensor alarm (alarm in):

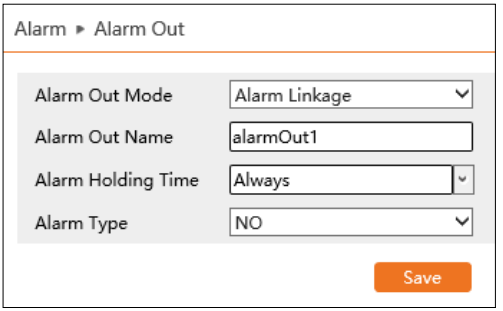
Go to Setup>Alarm> Alarm In interface as shown below.



1. Click "Enable" and set the alarm type, alarm holding time and sensor name.
2. Set alarm trigger options. The setup steps are the same as for motion detection. Please refer to the Motion Detection (2.4.1) section for details.
3. Click the "Save" button to save the settings.
4. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See Schedule Recording).

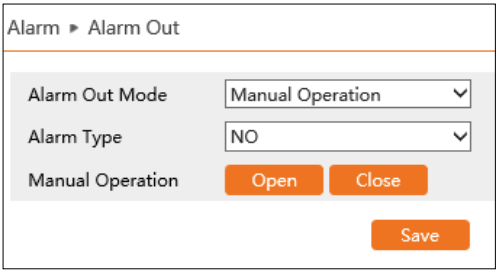
5.4.4 Alarm Out

This function is only available for some models. Go to Setup>Alarm>Alarm Out interface as shown below.

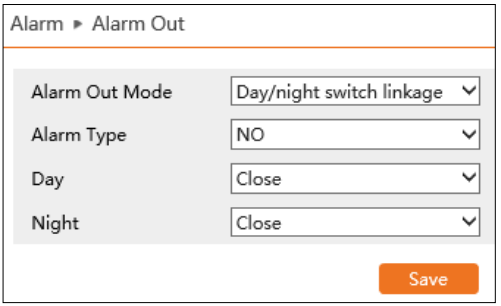


Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage and timing are optional.

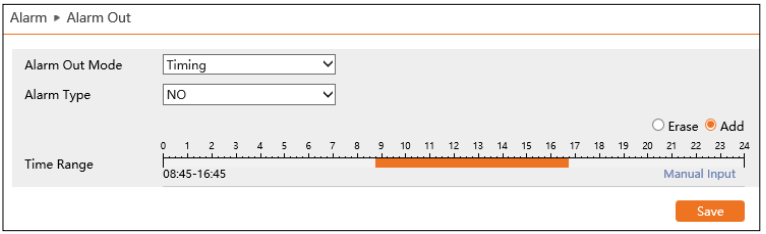
- **Alarm Linkage**: Select an alarm out name, alarm holding time at the "Alarm Holding Time" pull-down list box and alarm type.
- **Manual Operation**: Select the alarm type and click "Open" to trigger the alarm immediately; click "Close" to stop the alarm.



- **Day/Night Switch Linkage**: Select the alarm type and then choose to open or close the alarm when the camera switches to day mode or night mode.



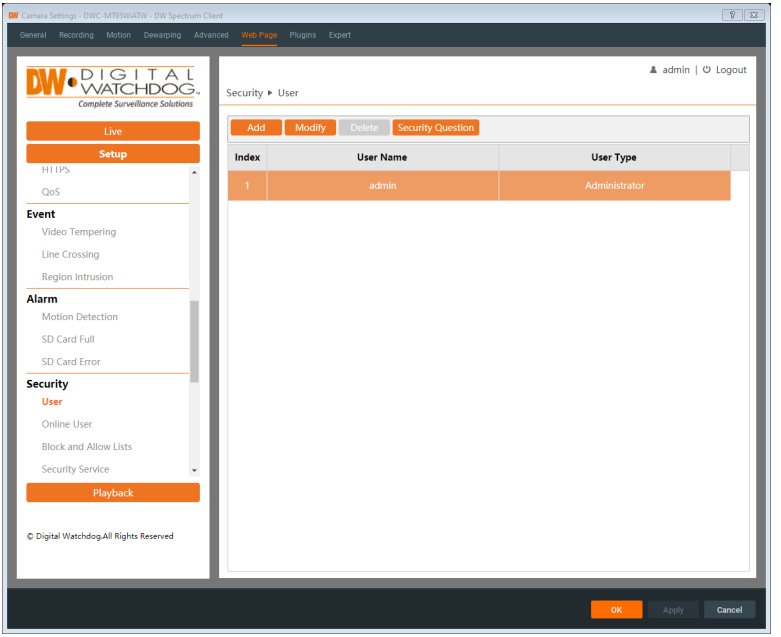
- **Timing**: Select the alarm type. Then click "Add" and drag the mouse on the timeline to set the schedule of the alarm out; click "Erase" and drag the mouse on the timeline to erase the set schedule. After this schedule is saved, the alarm will be triggered at the specified time.



5.5 Security Configuration

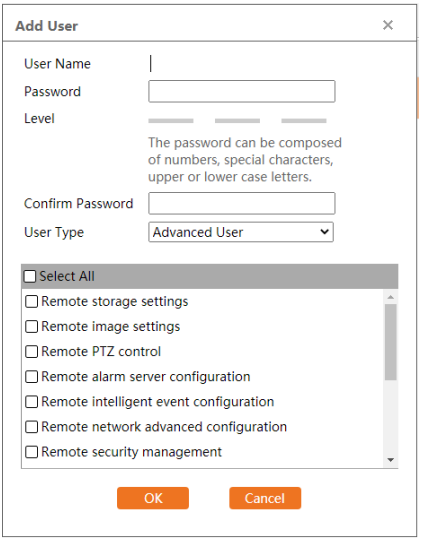
5.5.1 User Configuration

Go to Setup>Security>User interface as shown below.



To Add User:

3. Click the "Add" button to pop up the following textbox.



2. Enter the username in the "Username" textbox.

3. Enter the password in the "Password" and "Confirm Password" text boxes. Please set the password according to the requirements of the password security level (Go to Setup>Security>Password Security interface to set the security level).

It is recommended to set a high-level password that shall be composed of numbers, special characters, and upper- or lowercase letters for your account security.

4. Choose the user type and select the desired user permissions.

5. Click the "OK" button, and then the newly added user will be displayed in the user list.

Modify user:

1. Select a user to modify the password if necessary in the user configuration list box.

2. The "Edit user" dialog box pops up by clicking the "Modify" button.

3. Enter the old password of the user in the "Old Password" text box.

4. Enter the new password in the "New password" and "Confirm Password" text boxes.

5. Select the user permissions for an advanced or normal user.

6. Click the "OK" button to save the settings.

Note: When the password level is set to "Strong", the password cannot be set the same as the previous five.

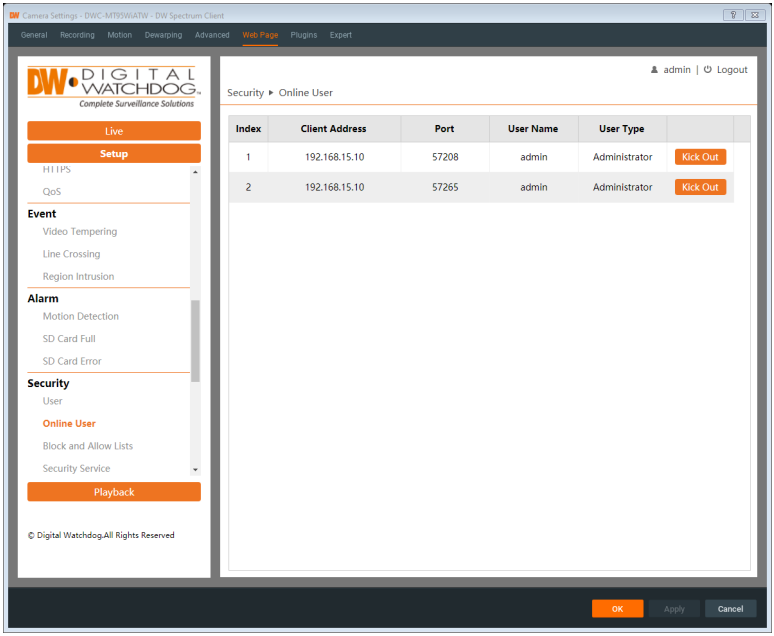
Delete user:

1. Select the user to be deleted in the user configuration list box.
2. Click the "Delete" button to delete the user.

Note: The default administrator account cannot be deleted.

5.5.2 Online User

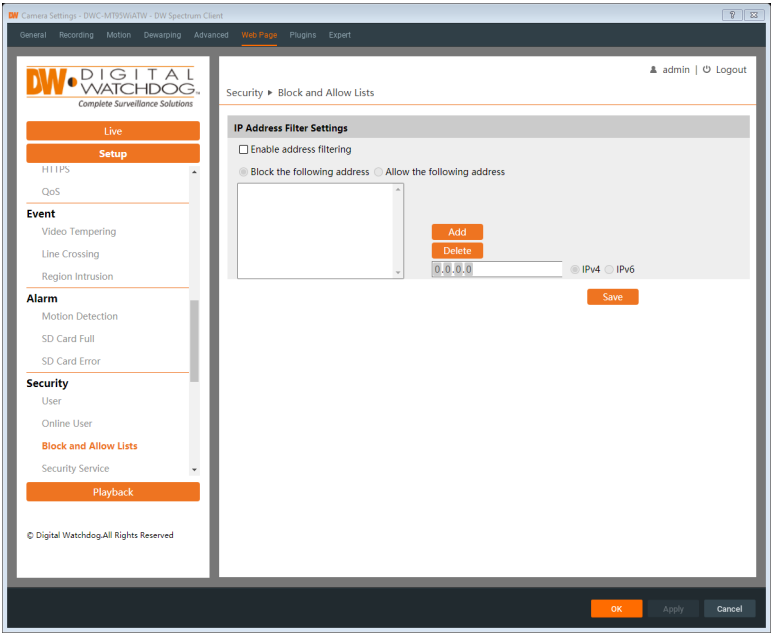
Go to Setup>Security>Online User to view the user who is viewing the live video.



Note: An administrator user can "kick out" (remove) all the other users, including other administrators.

5.5.3 Block and Allow Lists

Go to Setup>Security>Block and Allow Lists interface as shown below.



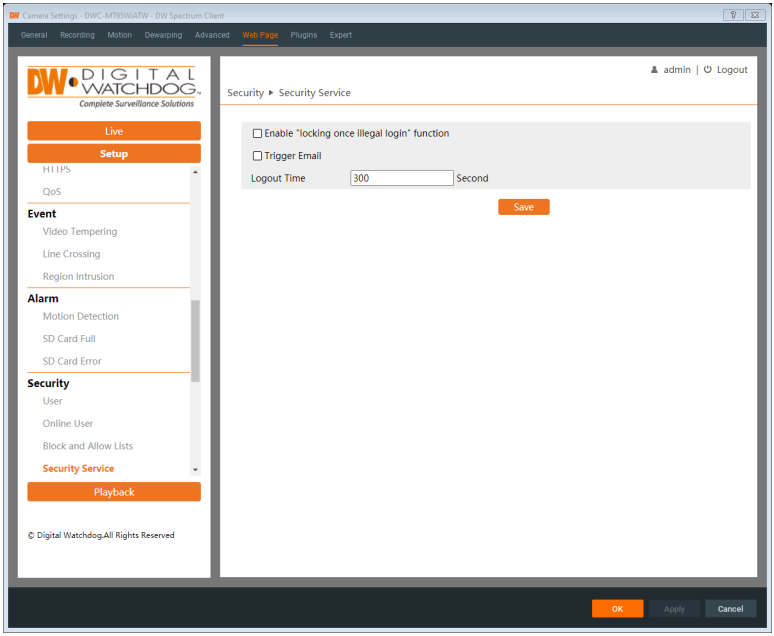
The setup steps are as follows:

1. Check the "Enable address filtering" checkbox.

2. Select "Block/Allow the following address", IPv4/IPv6/MAC and then enter the IP address or MAC address in the address box and click the "Add" button.

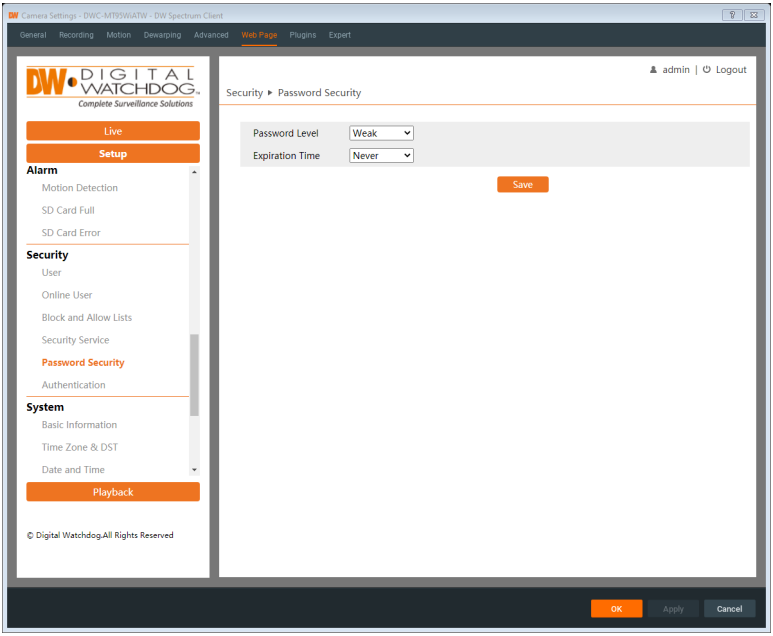
5.5.4 Security Service

Go to Setup>Security>Security Service Interface as shown below.



To prevent malicious password unlocking, the "locking once illegal login" function can be enabled here. If this function is enabled, a login failure after trying six times will lock the login interface. The camera can be logged in to again after half an hour or after the camera reboots.

Password Security



Please set the password level and expiration time for the camera as needed.

Password Level (requirements)**:**

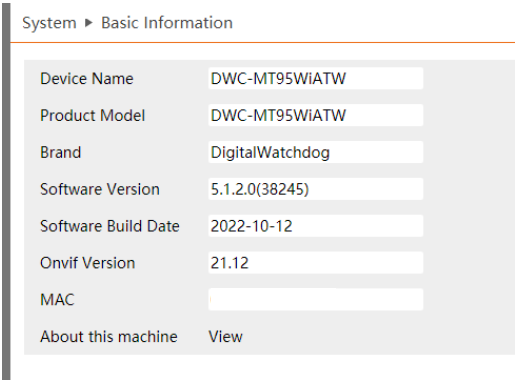
- Weak level: Numbers, special characters, and upper- or lowercase letters can be used. You can choose one of them or any combination of them when setting the password.
- Medium Level: 8~16 characters, including at least two of the following categories: numbers, special characters, upper case letters and lower case letters.
- Strong Level: 8~16 characters. Numbers, special characters, uppercase letters and lowercase letters must be included.

For your account security, it is recommended to set a strong password and change your password regularly.

5.6 System Configuration

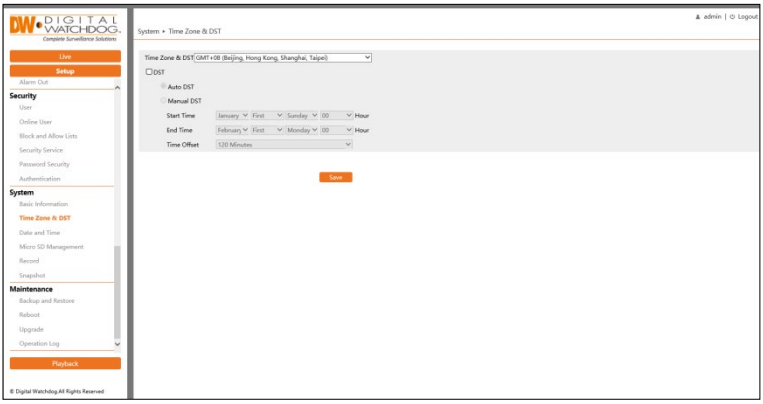
5.6.1 Basic Information

Basic Information lists the system information of the device, including model, name, firmware version, MAC address and more.



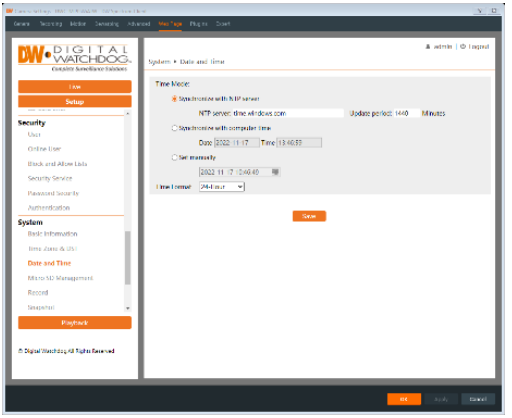
5.6.2 Time Zone&DST

The time zone and DST must be set up when accessing the camera for the first time.



5.6.3 Date and Time

Under Setup>System>Date and Time, users can adjust the camera's date and time.



5.6.4 Storage

Go to Setup>System>Micro SD Management to go to the interface as shown below.

SD Card Management

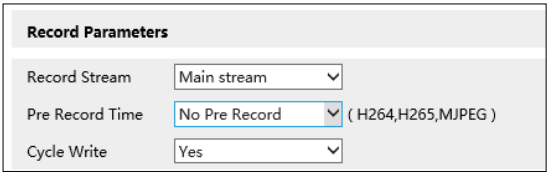
Click the "Format" button to format the SD card. All data will be cleared by clicking this button.

Click the "Eject" button to stop writing data to the SD card. Then the SD card can be ejected safely.

- **Snapshot Quota**: Set the limit of captured pictures on the SD card.
- **Video Quota**: Set the limit of record files on the SD card.

Schedule Recording Settings

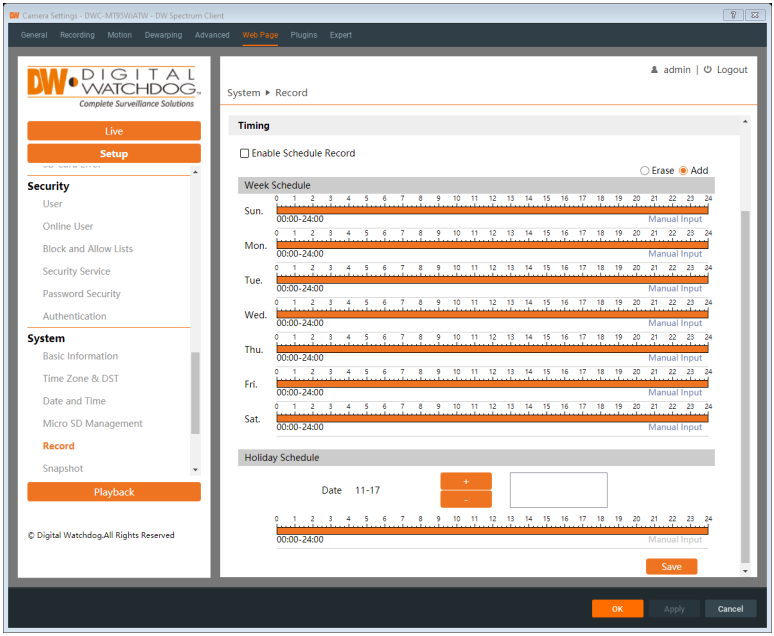
1. Go to Setup>SystemRecord to go to the interface as shown below.



2. Set record stream, pre-record time, and cycle writing.
   - **Record Stream:** Select the video stream for recording.
   - **Pre-Record Time:** Set the time to record before the actual recording begins.

- **Cycle Write:** Select "Yes" to allow the camera to overwrite old recorded video archives to continue recording when the SD card is full.

3. Set schedule recording. Check "Enable Schedule Record" and set the schedule.



Weekly Schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided into one-hour increments. Green means scheduled. Blank means unscheduled.

"Add": Add the schedule for a special day. Drag the mouse to set the time on the timeline.

"Erase": Delete the schedule. Drag the mouse to erase the time on the timeline.

Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularity (minutes).

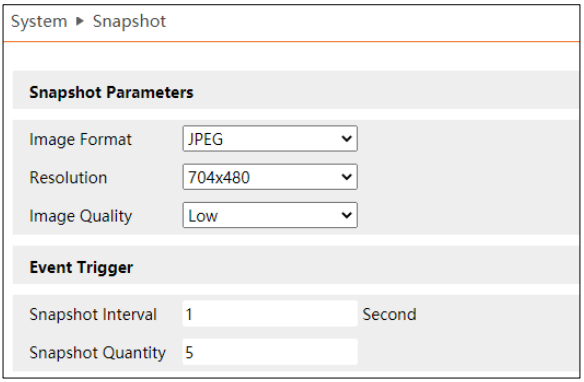
Day schedule

Set the alarm time for a special day, such as a holiday.

Note: Holiday schedule takes priority over weekly schedule.

Snapshot Settings

Go to Setup>System>Snapshot to go to the interface as shown below.



Set the format, resolution and quality of the image saved on the SD card and the snapshot interval, quantity and the timing snapshot here.

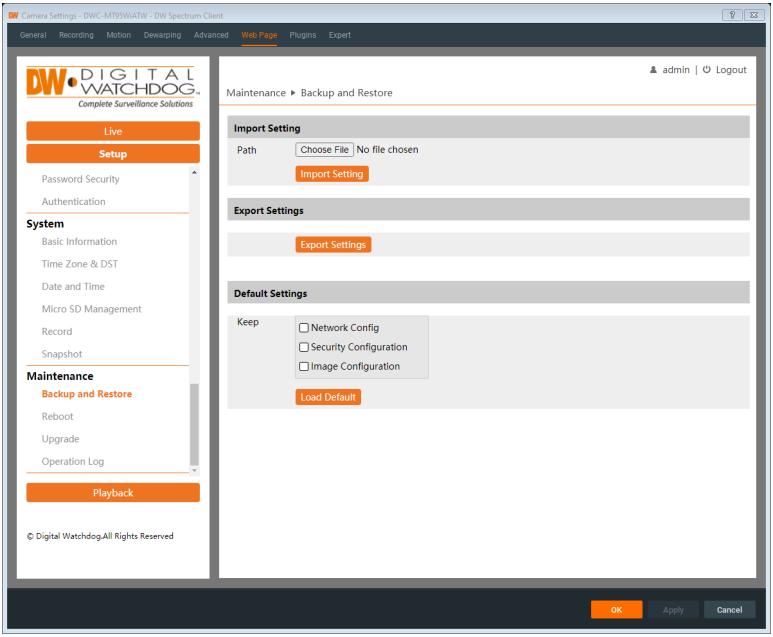
- **Snapshot Interval:** Set the amount of time (seconds) between snapshots.
- **Snapshot Quantity**: Set the maximum quantity of snapshots that will be taken. The actual quantity of snapshots may be less than this number. Supposing the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of snapshots.

Timing Snapshot: Enable timing snapshot first, and then set the snapshot interval and schedule. The setup steps of the schedule are the same as the scheduled recording (See Schedule Recording).

5.7 Maintenance Configuration

5.7.1 Backup and Restore

Go to Setup>Maintenance>Backup&Restore.



Import & Export Settings

Configuration settings of the camera can be exported from one camera to another camera.

1. Click "Choose File" to select the save path for importing or exporting information on the PC.

2. Click the "Import Setting" or "Export Setting" button.

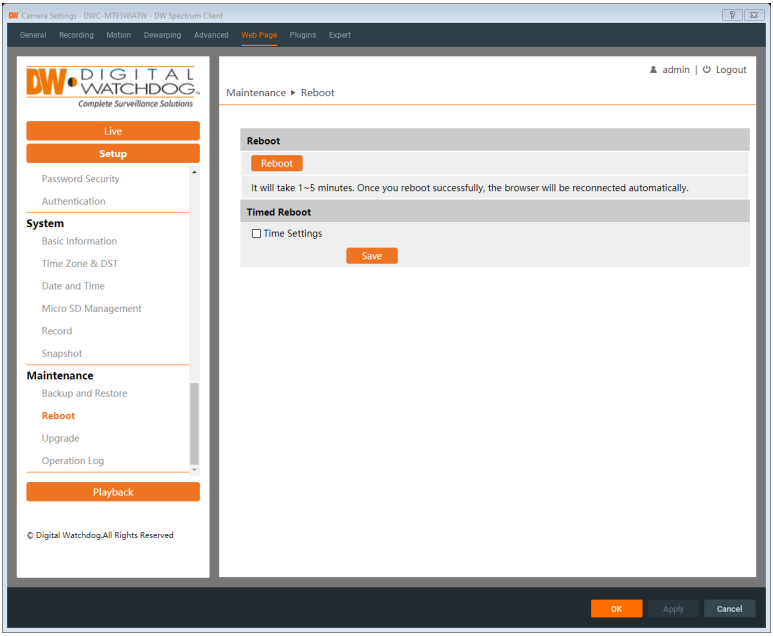
Default Settings

Click the "Load Default" button to restore all system settings to the default factory settings except those you want to keep.

5.7.2 Reboot

Go to Setup>Maintenance>Reboot.

Click the "Reboot" button to reboot the device.

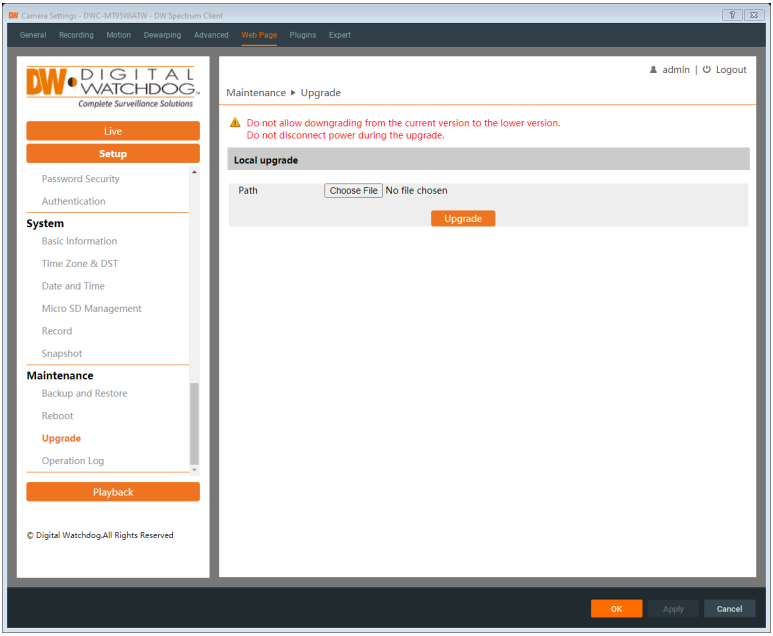


Timed Reboot Setting:

If necessary, the camera can be set up to reboot at a time interval. Enable "Time Settings", set the date and time and then click the "Save" button to save the settings.

5.7.3 Upgrade

Go to Setup>Maintenance>Upgrade. In this interface, the camera firmware can be updated.



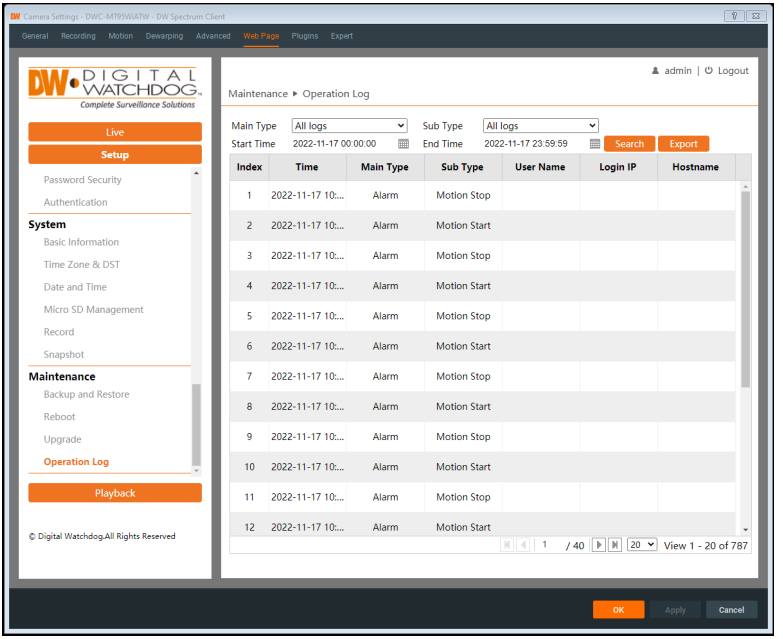
1. Click the "Browse" button to select the save path of the upgrade file
2. Click the "Upgrade" button to start upgrading the firmware.
3. The device will restart automatically

Caution! Do not close the browser or disconnect the camera from the network until the upgrade process has been completed. File corruption will occur if the camera is suddenly disconnected during the upgrade.

5.7.4 Operation Log

To query and export the log:

1. Go to Setup>Maintenance>Operation Log.



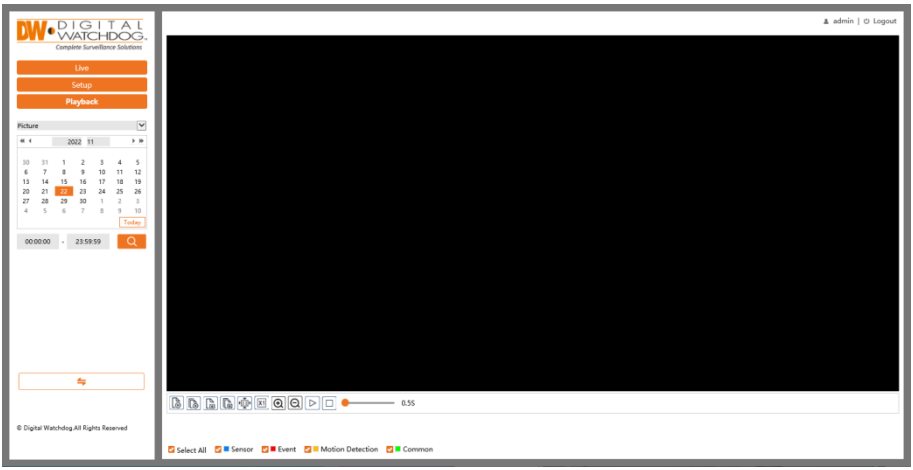
2. Select the main type, subtype, start and end time.
3. Click "Search" to view the operation log.
4. Click "Export" to export the operation log.

6 Playback

6.1 Image Playback

Click Playback to go to the interface as shown below. Images that are saved on the SD card can be found here.

SD Card Image Search



1. Choose "Picture".
2. Set time: Select the date and choose the start and end times.
3. Choose the alarm events at the bottom of the interface.
4. Click  to search the images.
5. Double-click a file name in the list to view the captured photos.

Click  to return to the earlier interface.

The descriptions of the buttons are shown as follows.

Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Save: Click this button to select the path for saving the image on the PC.		Save all: Click this button to select the path for saving all pictures on the PC.

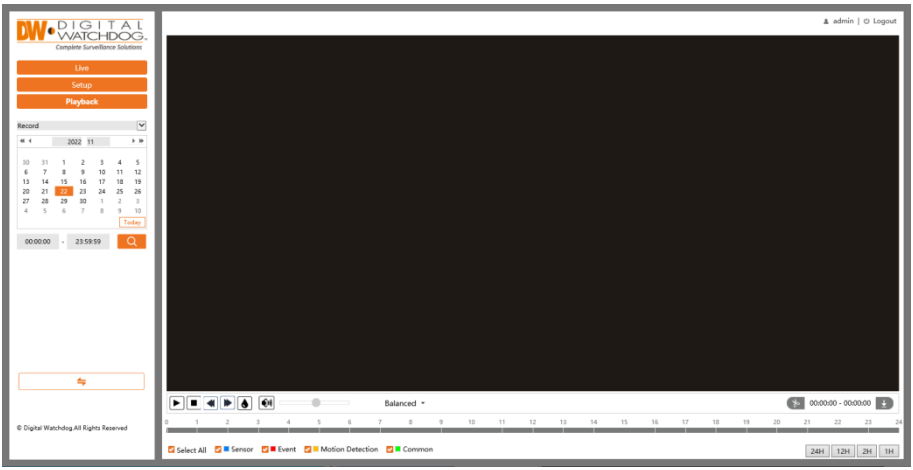
Icon	Description	Icon	Description
	Fit size: Click to fit the image on the screen.		Actual size: Click this button to display the actual size of the image.
	Zoom in: Click this button to zoom in digitally.		Zoom out: Click this button to zoom out digitally.
	Slide show play: Click this button to start the slide show mode.		Stop: Click this button to stop the slide show.
	Play speed: Play speed of the slide show.		

6.2 Video Search

SD Card Video Search

Click Search to go to the interface as shown below. Videos that were recorded on the SD card can be played in this interface.

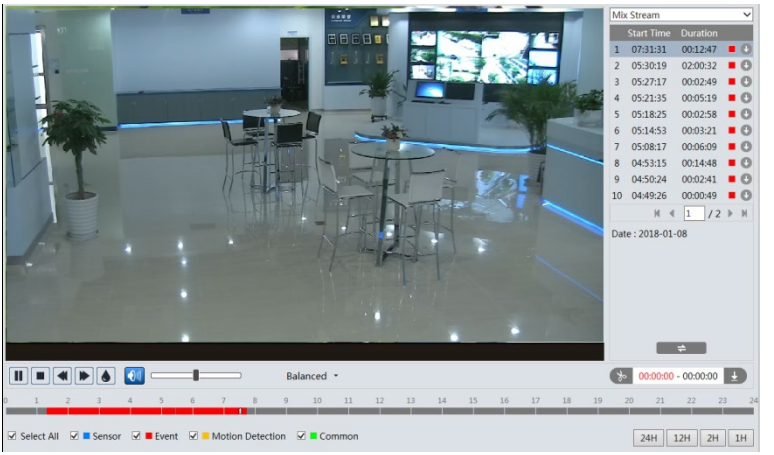
1. Choose "Record".
2. Set search time: Select the date and choose the start and end times.
3. Click  to search the images.



Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button

Icon	Description	Icon	Description
	Stop button		Speed down
	Speed up		Watermark display
	Turn audio on/off; drag the slider to adjust the volume after enabling audio.		

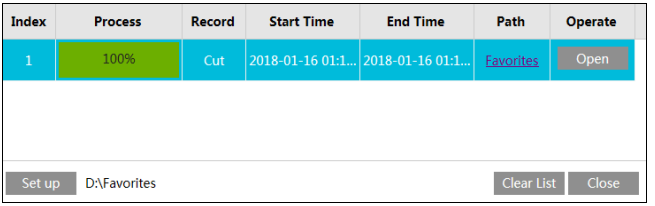
4. Select the alarm events at the bottom of the interface.
5. Select mix stream (video and audio stream) or video stream as needed.
6. Double-click on a file name in the list to start playback.



The timetable can be shown in 24H/12H/2H/1H format by clicking the corresponding buttons.

Video clips and downloading

1. Search the video files according to the steps above.
2. Select the start time by clicking on the timetable.
3. Click to set the start time, and then this button turns blue ( ).
4. Select the end time by clicking on the timetable. Then click to set the end time.
5. Click to download the video file on the PC.



Click "Set up" to set the storage directory for the video files.

Click "Open" to play the video.

Click "Clear List" to clear the downloading list.

Click "Close" to close the downloading window.

7 Appendix

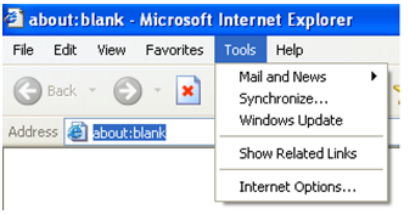
7.1 Troubleshooting

How to find the password?
A: Reset the device to the default factory settings.
Default IP: 192.168.226.201; Username: admin; Password: 123456

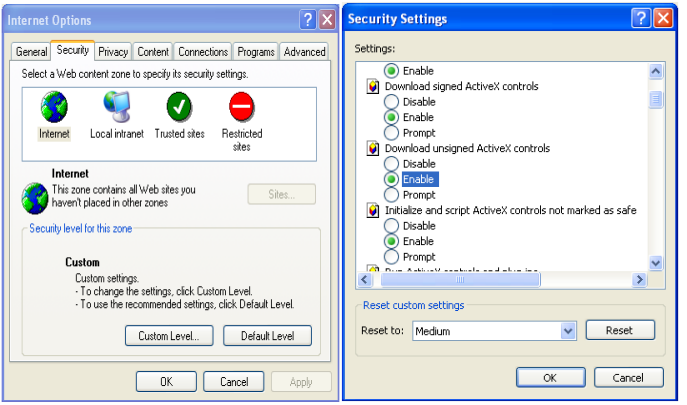
Fail to connect devices through the IE browser.
A: The network is not well connected. Check the connection and make sure it is connected well.
B: IP address is not available. Reset the IP address.
C: Web port number has been changed: contact the administrator to get the correct port number.
D: Exclude the above reasons. Restore to the default setting by IP-Tool.

IP tool cannot search devices.
The anti-virus software on your computer may cause it. Please exit it and try to search the device again.

Internet Explorer cannot download the ActiveX control.
A. IE browser may be set up to block ActiveX. Follow the steps below.
① Open IE browser and then click Tools-----Internet Options.



② Select Security------Custom Level....
③ Enable all the options under "ActiveX controls and plug-ins".
④ Click OK to finish the setup.
B. Other plug-ins or anti-virus blocks ActiveX. Please uninstall or close them.

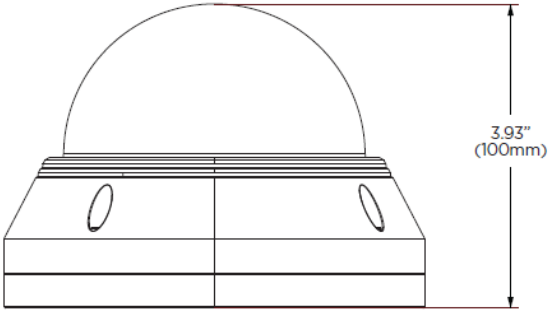


No sound can be heard.

A: The audio input device is not connected. Please connect and try again.

B: Audio function is not enabled at the corresponding channel. Please enable this function.

7.2 Dimensions


3.93"
(100mm)

7.3 Specifications

	DWC-MT95WW28 TW	DWC-MT95Wi28 TW	DWC-MT95Wi36 TW	DWC-MT95WIATW
IMAGE				
Image sensor	5MP 1/2.7" CMOS			
Total pixels	2592 × 1944			
Minimum scene illumination	0.0 lux (B/W)	0.02 lux (color)		0.01 lux (color)
		0.0 lux (B/W)		
S/N ratio	≥50dB			
LENS				
Focal length	2.8mm, F1.0	2.8mm, F1.6	3.6mm, F1.6	2.8 ~ 12mm, F1.4
Lens type	Fixed lens			Vari-focal lens with motorized zoom and auto-focus
Field of view (FoV)	94.8°	98.5°	81.4°	95.1° ~ 30°
IR distance	2 white light LEDs, 98ft range	100ft range		164ft range
I/O				
Audio in / out	1 audio input and 1 built-in microphone			
Audio compression	G.711A / U			
OPERATIONAL				
Shutter mode	Auto, manual			
Shutter speed	1/30s ~ 1/100000s			
Auto gain control	Auto			
Day/night	Auto, day (color), night (B/W), schedule			
Smart DNR™ 3D digital noise reduction	3D DNR			
Wide dynamic range (WDR)	True WDR low, middle, high			
Wide dynamic range (WDR) dB	120dB			
Privacy zone	4 programmable privacy masks			
Camera analytics	Line crossing, perimeter intrusion, video tampering detection (scene change, video blur, abnormal color detection), object classification (differentiate humans from objects)			
Backlight compensation (BLC)	Yes			
DeFog	Yes			
Mirror and flip	Yes			
Alarm notifications	Notifications via e-mail or FTP server			
Memory slot	Micro SD / SDHC / SDXC card up to 256GB (card not included)			
NETWORK				
LAN	802.3 compliance 10/100 LAN			
Video compression type	H.265, H.264, MJPEG			
Resolution	Mainstream: 5MP, 4MP, 2K, 3MP, 2.1MP/1080p, 720p (60Hz: 1 ~ 30fps; 50Hz: 1-25fps) Sub-stream: 720P, D1, CIF, 480×240 (60Hz: 1 ~ 30fps; 50Hz: 1-25fps) Third stream: D1, CIF, 480×240 (60Hz: 1 ~ 30fps; 50Hz: 1-25fps)			
Frame rate	Up to 30fps at all resolutions			
Video bitrate	64 Kbps ~ 8 Mbps			
Bitrate control	Multi-streaming CBR/VBR at H.264/ H.265 (controllable frame rate and bandwidth)			
Streaming capability	Dual stream at different rates and resolutions			
IP	IPv4, IPv6			
Protocol	UDP, IPv4, IPv6, DHCP, NTP, RTSP, RTP, RTCP, ICMP, IGMP, PPPoE, DDNS, SMTP, FTP, SNMP, HTTP, 802.1x, UPnP, HTTPS, QoS			
Security	IP filtering, MAC filtering, authentication (ID/PW), SSL/TSL			
ONVIF conformance	Yes			
Web viewer	OS: Windows®			
	Browser: Internet Explorer			
Video management	DW Spectrum® IPVMS			

software		
ENVIRONMENTAL		
Operating temperature	**-22°F ~ 140°F (-30°C ~ 60°C)**	
Operating humidity	**0–95% RH (non-condensing)**	
IP rating	**IP67-rated**	
IK rating	**IK10 impact-resistant**	
Other certifications	**FCC, CE, ROHS, POE, ONVIF**	
ELECTRICAL		
Power requirement	**DC 12V, PoE IEEE 802.3af Class 3. (Adapter not included)**	
Power consumption	<7W	**<9W**
MECHANICAL		
Material	**Metal turret housing**	
Dimensions	4.66" x 3.58" (118.6 x 91 mm)	**5.16" x 4.13" (131.1 x 105 mm)**
Weight	1.01 lbs. (0.46 kg)	**1.45 lbs. (0.66 kg)**
Warranty	5 year warranty	**5 year warranty**

* Specifications are subject to change without notice.

Warranty Information

Go to https://digital-watchdog.com/page/rma-landing-page/ to learn more about Digital Watchdog's warranty and RMA.

To obtain warranty or out-of-warranty service, please contact a technical support representative at:
1+ (866) 446-3595, Monday through Friday from 9:00 AM to 8:00 PM EST.

A purchase receipt or other proof of the date of the original purchase is needed before warranty service is rendered. This warranty only covers failures due to defects in materials and workmanship that arise during normal use. This warranty does not cover damages that occurs in shipment or failures which are caused by products not supplied by the Warrantor or failures which result from accident, misuse, abuse, neglect, mishandling, misapplication, alteration, modification, faulty installation, setup adjustments, improper antenna, inadequate signal pickup, maladjustments of consumer controls, improper operation, power line surge, improper voltage supply, lightning damage, rental use of the product or service by anyone other than an authorized repair facility or damage that is attributable to acts of God.

Limits and exclusions

There are no express warranties except as listed above. The Warrantor will not be liable for incidental or consequential damages (including, without limitation, damage to recording media) resulting from the use of these products or arising out of any breach of the warranty. All express and implied warranties, including the warranties of merchantability and fitness for a particular purpose, are limited to the applicable warranty period set forth above.
Some states do not allow the exclusion or limitation of incidental or consequential damages or limitations on how long an implied warranty lasts, so the above exclusions or limitations may not apply to you. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state
to state.

If the problem is not handled to your satisfaction, then write to the following address:
Digital Watchdog, Inc.
ATTN: RMA Department
16220 Bloomfield Ave
Cerritos, CA 90703

Service calls that do not involve defective materials or workmanship as determined by the Warrantor, in its sole discretion, are not covered. The cost of such service calls is the responsibility of the purchaser.

DIGITAL WATCHDOG®

Complete Surveillance Solutions

DW® East Coast office and warehouse: 5436 W Crenshaw St, Tampa, FL USA 33634
DW® West Coast office and warehouse: 16220 Bloomfield Ave, Cerritos, CA USA 90703
PH: 866-446-3595 | FAX: 813-888-9262
www.Digital-Watchdog.com
technicalsupport@dwcc.tv
Technical Support PH:
USA & Canada 1+ 866-446-3595
International 1+ 813-888-9555
French Canadian: + 1-904-999-1309
Technical Support Hours: Monday-Friday 9 a.m. to 8 p.m. Eastern Time