MEGApix® 4MP Turret IP Camera

DWC-VSTB04Bi - Turret Camera with Fixed Lens - White
DWC-VSTB04BiB - Turret Camera with Fixed Lens - Black
DWC-VSTB04Mi - Turret Camera with Vari-Focal Lens

User's Manual Ver. 05/24

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 to 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, 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 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 of amending the typographical errors, inconsistencies with the latest version, software upgrades and product improvements, interpretation and modification. These changes will be published in the latest version without special notification.
- All pictures, charts, images in this manual are only for description and explanation of our products. In this manual, the trademarks, product names, service names, company names, products that are not owned by our company 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 be irresponsible 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 the 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 lower-case 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 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 your device has been accessed by unauthorized users or not, 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 regulation's 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 his 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 refers to 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 refers to conforms to the rules and regulations of REACH. For more information on REACH, please refer to DG GROWTH or ECHA websites.

Table of Contents

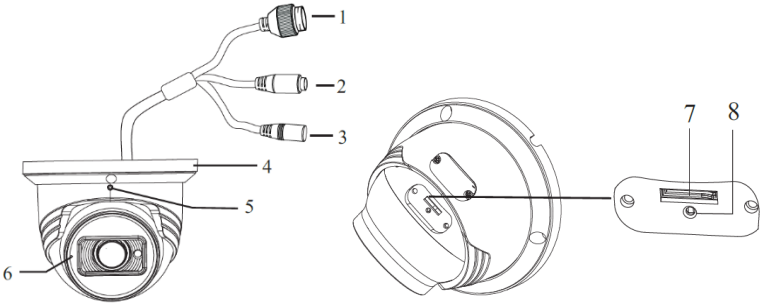
1 Introduction

1.1 Product and Accessories

Make sure that you have the following items supplied with your camera. If any of these items are missing or damaged, notify your vendor immediately. Keep the packing utilities for moving or storage purposes afterward.

WHAT'S IN THE BOX					
Quick Setup and Installation Guides		1 set	Tapping Screws – 3pcs		1 set
Mounting Template		1	Plastic Plugs – 3pcs		1 set
Waterproof Cap		1 set	Rubber Plug		1
Hexagonal Wrench 0.07" (2mm)		1			

1.2 Parts Identification



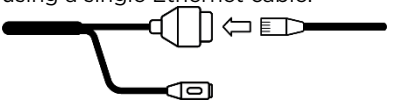
Number	Description	Number	Description
1	Network Cable	5	Fixed Screw
2	Audio Input (3.5mm)	6	Built-in Microphone
3	Power Cable	7	Micro SD Card
4	Mounting Base	8	Reset Button

2 Installation

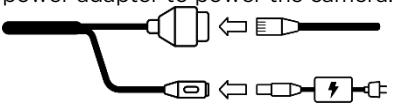
2.1 Powering the Camera

Pass the wires through and make all necessary connections.

Use a PoE Switch or PoE Injector to connect data and power to the camera using a single Ethernet cable.



Use a non-PoE Switch to connect data using an Ethernet cable and use a power adapter to power the camera.

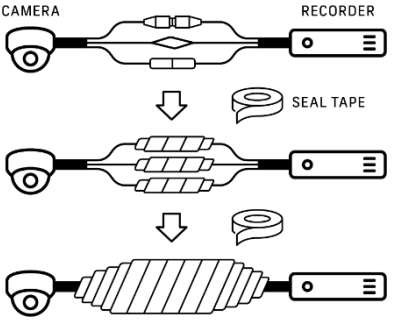


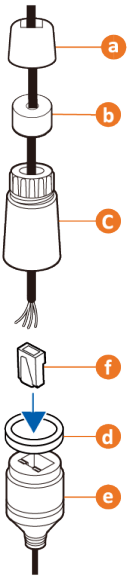
Model	Power requirements	Power consumption
DWC-VSTB04Bi	DC12V, PoE (IEEE 802.3af class 2). Adapter not Included.	<5W
DWC-VSTB04Mi	DC12V, PoE (IEEE 802.3af class 3). Adapter not Included.	<8W

2.2 Installation

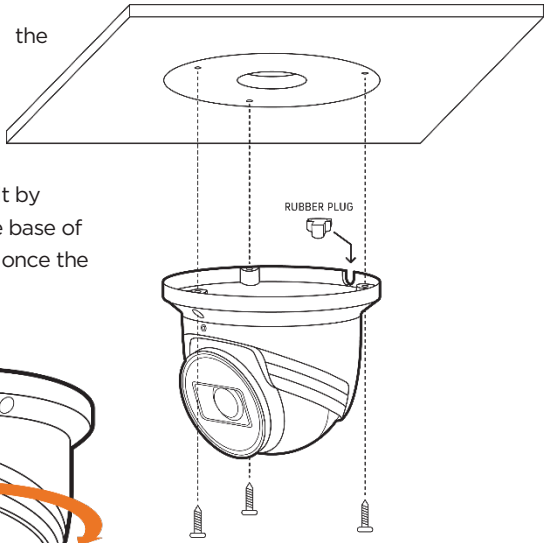
1. The mounting surface must bear at least five times the weight of your camera.
2. Using the mounting sheet or the camera itself, mark and drill the necessary holes in the wall or ceiling.
3. Pass wires through and make all necessary connections. See **2.2 Cabling** for more information.
4. To use the camera's waterproof wiring:

   In extreme environments, use an outdoor-rated sealer.

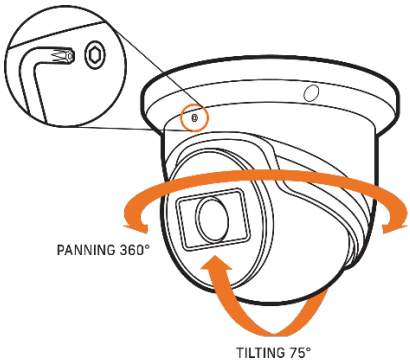




5. Mount the camera using the included screws and anchors.



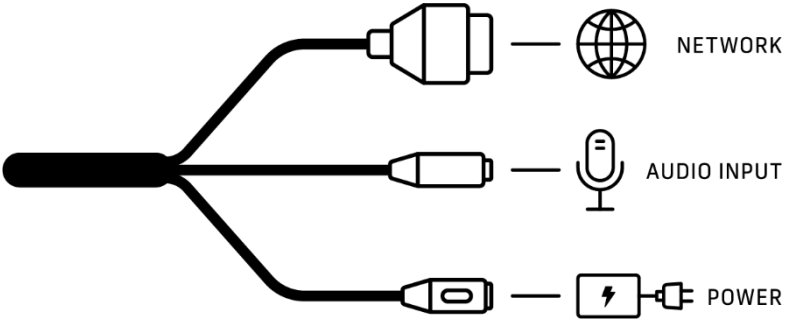
6. Adjust the camera's pan and tilt by loosening the lock screw at the base of the camera. Tighten the screw once the adjustment is complete.



7. Remove the protective film from the dome. Softly wipe the dome with lens tissue or a microfiber cloth with ethanol to remove any dust or smudges left from the installation process.

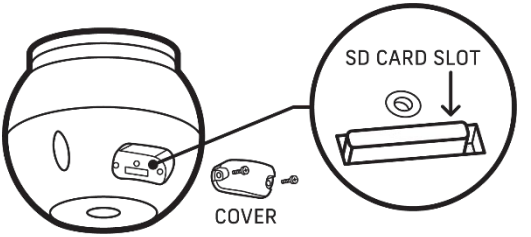
2.3 Cabling

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



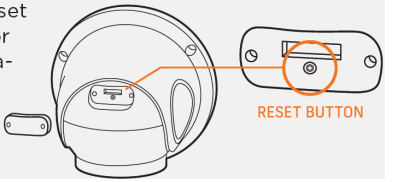
2.4 Managing the SD Card

1. Loosen the fixed screw at the base of the camera to rotate the camera module and remove the control panel cover to access the SD card slot at the base of the camera.
2. Insert class 10 SD/SDHC/SDXC card into the SD card slot (max 256GB).
3. Press the card inward until it clicks to release from the card slot..



2.5 Resetting the Camera

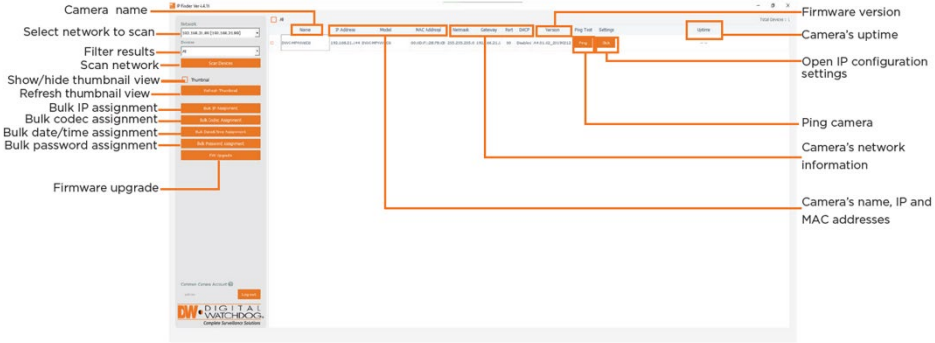
Resetting the camera: Press the reset button at the base of the camera for five (5) seconds to initiate a camera-wide reset of all the settings, including network settings.



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.

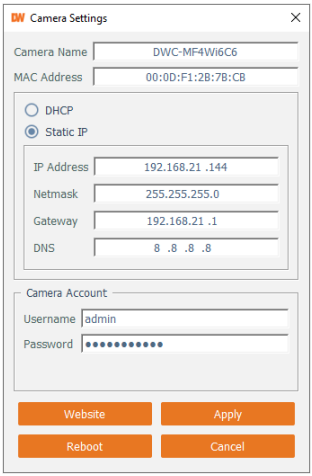


1. To install DW IP Finder, use a web browser and go to: http://www.digital-watchdog.com.
2. Enter "DW IP Finder" on the search box at the top of the page.
3. Go to the "Software" tab on the DW IP Finder page to download and install the installation file.
4. Open DW IP Finder and click 'Scan Devices'. It will scan the selected network for all supported devices and list the results in the table. During the scan, the DW® logo will turn gray.
5. When connecting to the camera for the first time, a password must be set. To use DW IP Finder for *Bulk Password Assignment*:

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

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

c. Enter admin/admin for the current username and password. Enter a new username and password to the right. Passwords must have a minimum of eight (8) characters and at least four (4) combinations of uppercase and lowercase letters, numbers and special characters. Passwords should not contain the User ID.



d. Click "change" to apply all changes.

6. Select a camera from the list by double-clicking on the camera's name or clicking on the 'Click' button. The pop-up window will show the camera's current network settings. Admin users can adjust the settings as needed. The camera's network settings are set to DHCP by default.
7. To access the camera's web page, click on the 'Website' button.
8. To save changes made to the camera's settings, enter the username and password of the camera's admin account and click 'Apply'.

•

Select 'DHCP' for the camera to automatically receive its IP address 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.

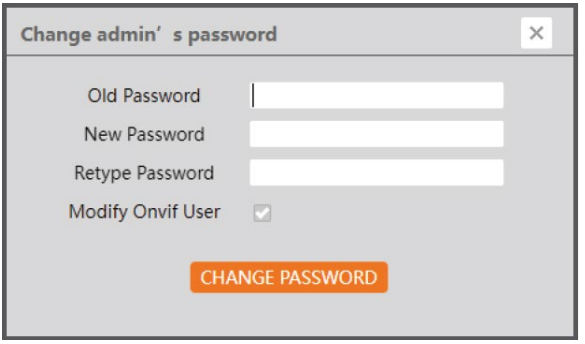
To access the camera from an external network, port forwarding must be set in your network's router.

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 using DW IP Finder:

1. Find the camera using DW IP Finder.
2. Double-click on the camera's view in the results table.
3. Press the 'Website' button. The camera's web viewer will open up in your default web browser.
4. Enter the camera's username and password that was set up in DW IP Finder. If you did not set up a new username and password via DW IP Finder, a message will direct you to set up a new password for the camera before gaining access.



To open the camera using the web browser:

1. Open a web browser.
2. Enter the camera's IP address and port in 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 you set up in DW IP Finder.

NOTE: The GUI display may differ by camera models.

Icon	Description	Icon	Description
AUDIO ON/OFF	Enable/disable audio (on supported models)		SD card recording indicator
SNAPSHOT	Snapshot		Motion alarm (on supported models)
START RECORD	Start/stop local recording (on supported models)		Color abnormal
D-ZOOM IN	Digital zoom in the live image		Abnormal clarity
D-ZOOM OUT	Digital zoom out the live image		Scene change
ZOOM/FOCUS	AZ control (only available for the model with motorized zoom lens)		Line crossing
IVA EVENT INFO	Event rule information display		Perimeter Intrusion

NOTE: Line Crossing and Perimeter Intrusion cannot be enabled at the same time.

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

*Plug-in free live view: local recording is not supported.

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" button to go to the setup menu.

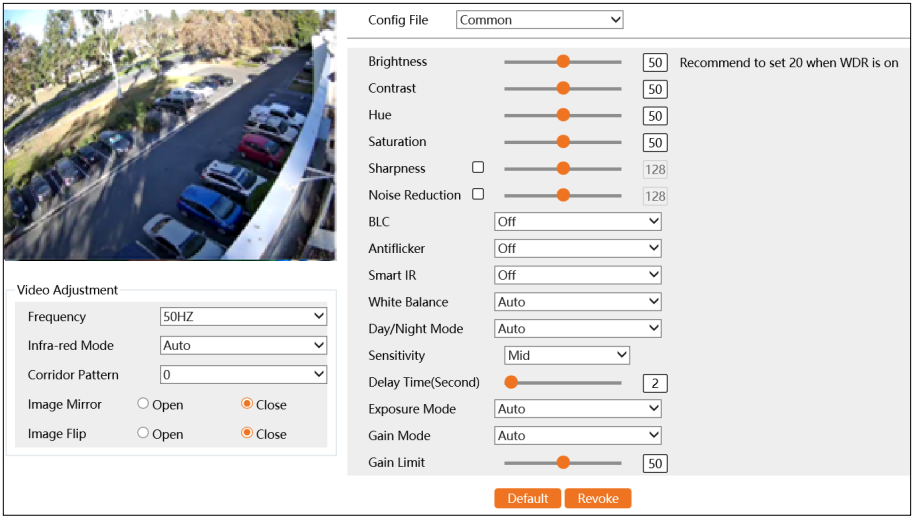
NOTE: Where applicable, click the "Save" button to apply changes to the settings.

5.1 Camera Configuration

Camera Configuration includes the *Camera Parameters, Video, Audio, OSD, Privacy Mask* and *ROI Configuration* menus.

5.1.1 Camera Parameters

Go to Setup>Camera>Camera Parameters interface as shown below. The settings for image *Brightness, Contrast, Hue* and *Saturation* and other parameters for Common, Day and Night configurations can be set up separately. The image effect can be quickly seen by switching the configuration file using the *Config File* drop-down at the top of the menu.



- **Brightness**: Set the brightness level of the camera's image.
- **Contrast**: Set the color difference between the brightest and darkest parts.
- **Hue**: Set the total color degree of the image.
- **Saturation**: Set the degree of color purity. The purer the color, the brighter the image is.
- **Sharpness**: Set the resolution level of the image plane and the sharpness level of the image edge.
- **Noise Reduction**: Decrease the noise and make the image more thorough. Increasing the value will make the noise reduction effect better but it will reduce the image resolution.
- **Backlight Compensation (BLC)**:
  - Off: Disables the backlight compensation function. It is the default mode.
  - HWDR: WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field of the view by lowering the brightness of the bright area and increasing the brightness of the dark area. The recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.
  - HLC: Lowers the brightness of the entire image by suppressing the brightness of the image's bright area and reducing the size of the halo area.

- BLC: If enabled, the auto exposure will activate according to the scene so that the object of the image in the darkest area will be seen clearly.

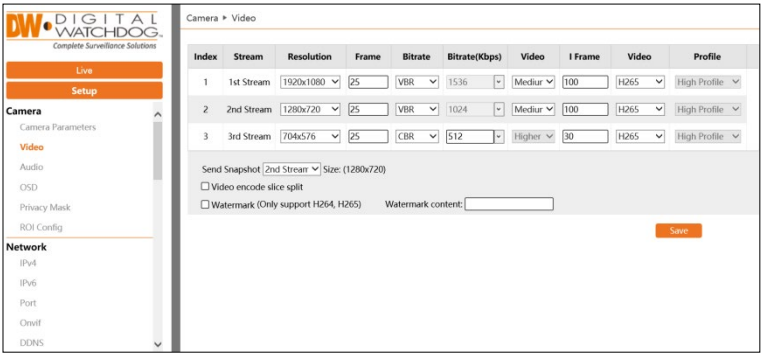
- Antiflicker:
  - Off: Disables the anti-flicker function. This is used mostly in outdoor installations.
  - 50Hz: Reduces flicker in 50Hz lighting conditions.
  - 60Hz: Reduces flicker in 60Hz lighting conditions.

- **Smart IR**: Choose “ON” or “OFF”. This function can effectively avoid image overexposure and underexposure by controlling the brightness of the IR lights according to the actual conditions to make the image more realistic. Please enable it as needed.
  - **White Balance**: Adjust the color temperature according to the environment automatically.
  - **Day/Night Mode**: Choose “Auto”, “Day”, “Night”, or “Timing”.
    - Sensitivity: Set the general amount of environmental light that is required to trigger switching Day/Night modes.
    - Delay Time (Seconds): Set the amount of time that the camera will delay switching between Day/Night modes when triggered.
  - **Exposure Mode**: Choose “Auto” or “Manual”. If “Manual” is chosen, 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 actual situation. If “Manual” is selected, the gain value shall be set manually. The higher the value is, the brighter the image is.
  - **Gain Limit:** Set the maximum digital gain level for the camera image. There are two separate configurations for Auto or Manual Gain Modes.
  - **Frequency**: 50Hz and 60Hz can be optional.
  - **Infra-red Mode**: Choose “Auto”, “ON” or “OFF”.
  - **Corridor Pattern**: Corridor viewing modes can be used for situations such as long hallways. 0, 90, 180 and 270 are available. The default value is 0. The video resolution should be 1080P or below if this function is used.
  - **Image Mirror**: Turn the current video image horizontally.
  - **Image Flip**: Turn 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, video quality, etc. Three video streams are available for configuration in this menu. Viewing experience is subject to the actual network conditions.



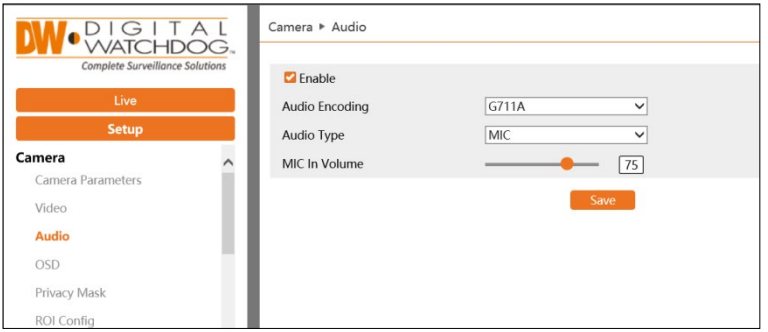
- **Resolution**: Adjust the stream resolution from the available options in the drop-down menu.
- **Frame rate**: The higher the frame rate, the more individual frames will be shown per second. A higher FPS results in smoother video but will increase the bitrate of the video stream.
- **Bitrate type**: Select between CBR and VBR bitrate types. Bitrate is related to image quality.
    - CBR: Compression bitrate will remain constant, of change in the video scene.
    - VBR: Compression bitrate will be adjusted according to scene changes. For example, for scenes that do not have much movement, the bitrate will remain at a lower value. This can help optimize the network bandwidth usage of the camera.
- **Bitrate (Kbps)**: Bitrate type must be set to CBR to manually adjust this setting. A higher bitrate will result in better image quality.
- **Video Quality**: Bitrate type must be set to VBR to manually adjust this setting. The higher the image quality, the more bitrate will be required.
- **I-Frame interval**: Determines how many frames are allowed between a “group of pictures” when a new scene begins in a video, until that scene ends, and if an entire group of frames (or pictures) can be considered as a “group of pictures”. If there is not much motion in the scene, setting the value higher than the frame rate can potentially resulting in less bandwidth usage. However, if the

value is set too high and there is a lot of movement in the video, there is a risk of frame-skipping.

- **Video Compression:** Select between MJPEG, H264, and H265 compression options. MJPEG is not available for the mainstream. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate and image quality.
- **Profile**: Video Compression must be set to H.264 to adjust this setting. Choose between Base Line, Main Profile and High Profile.
    - Base Line: Simple profile used for low-power devices. Color information is sampled at half the vertical and half the horizontal resolution of b/w information.
    - Main Profile: Includes all functionality of Base Line but with improvements to frame prediction.
    - High Profile: Highest quality H.264 profile with highest amount of compression. Increased data rate and need of decoder performance.
- Send Snapshot: Select which video stream to use when creating a snapshot from the camera.
- Video Encode Slice Split: Enable this function for an improved image when using a low-performance PC.
- Watermark: When playing back the locally recorded video in the search interface, the watermark can be displayed. To enable it, check the watermark box and enter the watermark text.

5.1.3 Audio Configuration

Click the “Audio” tab to go to the audio interface as shown below.



- **Enable:** Enable audio settings to use a microphone. The audio can

be enabled or disabled as needed.

- **Audio Encoding**: Select between G711A and G711U audio codecs.
    - G711A: Provides more quantization levels at lower signal levels.
    - G711U: Provides more resolution to higher range signals.
- **Audio Type**: Select between LINE-IN and MIC-IN for audio. Use MIC-IN for models using a built-in microphone.
    - MIC: An audio socket for connecting a wired microphone.
    - LIN: An audio socket for connecting external audio devices that use strong voltage currents.

5.1.4 OSD Configuration

Go to Setup>Camera>OSD interface as shown below.

Set on-screen display (OSD) settings for time stamp, device name, OSD content and picture overlap. Click-and-drag to reposition OSD objects.

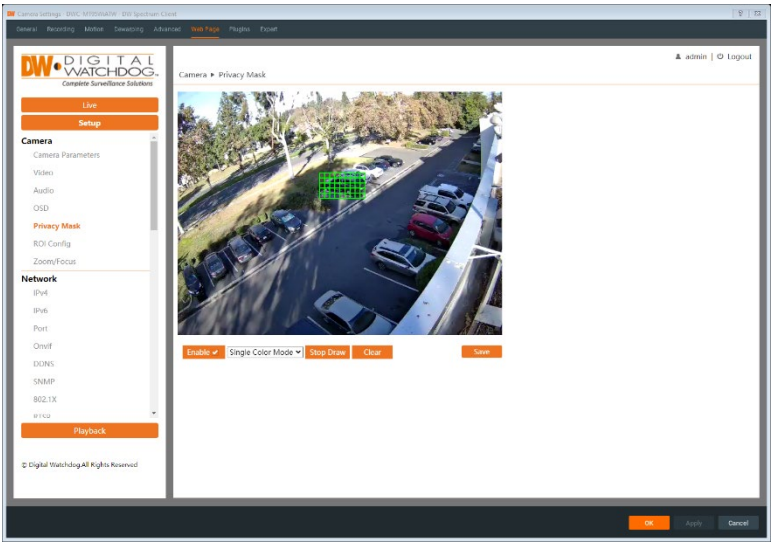
Click the “Save” button to apply the settings.

- **Date Format:** Enable Show Timestamp to overlay the live display with the current date and time. Select your preferred date/time format.
- **Device Name:** Enable Show Device Name to overlay the live display with the camera name. Edit the name as needed.
- **OSD Content:** Enable to overlay customized text. Maximum of 15-characters.

5.1.5 Privacy Mask

Go to Setup>Camera>Privacy Mask interface as shown below.

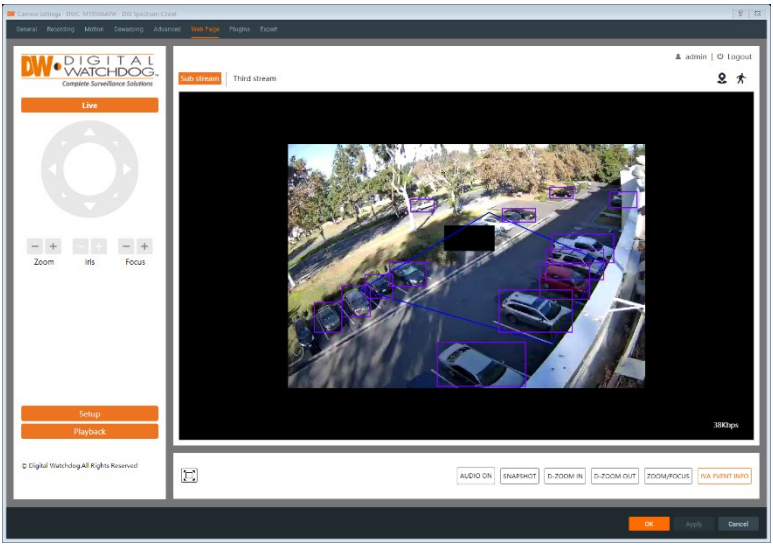
Create a virtual mask to overlay and obscure selected areas of the camera display. A maximum of four (4) privacy mask zones can be set at a time.



To set up a privacy mask:

1. Check the 'Enable' box to allow the mask to allow the mask to overlay the live display.
2. Click the "Draw Area" button and use the mouse to draw the privacy mask area.
3. Click the "Save" button to apply the settings.
4. Verify that the masked area appears in live view.

Click the "Clear" button to delete the privacy mask areas.

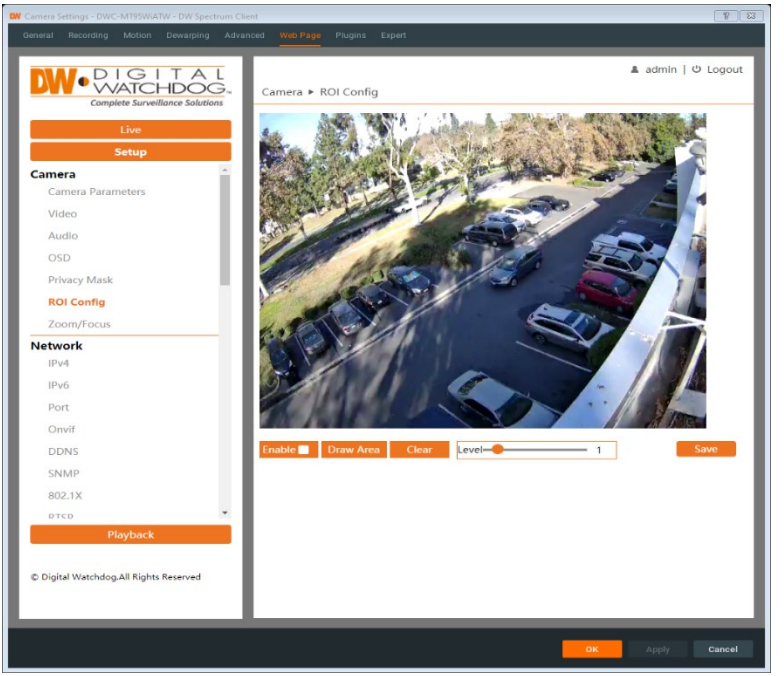


5.1.6 ROI Configuration

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 identified area.

A Maximum of eight (8) ROI regions can be set at a time.



To create an ROI area:

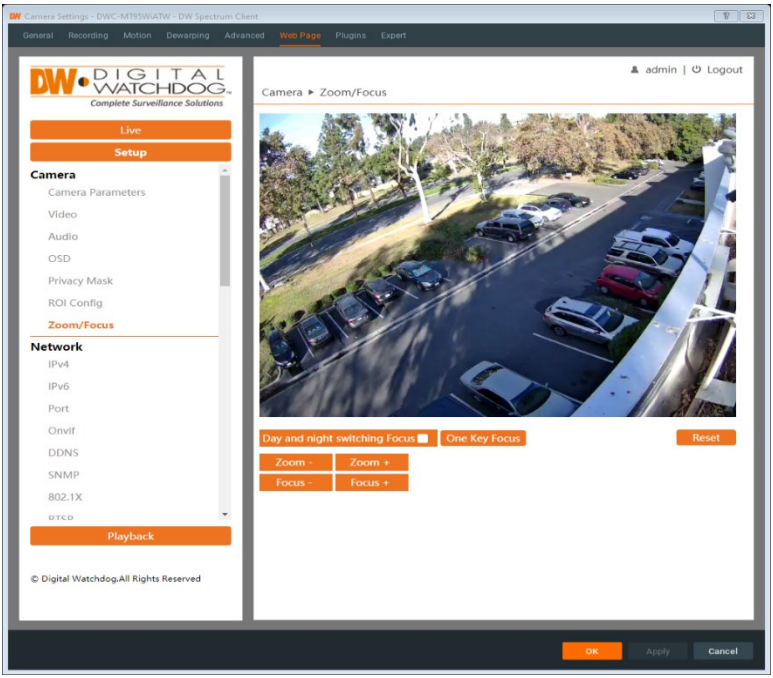
1. Check “Enable” then click the “Draw Area” button.
2. Drag the mouse to draw the ROI area.
3. Set the sensitivity level of the ROI area.
4. Click the “Save” button to apply the settings.

5.1.7 Zoom/Focus

Go to Config>Image>Zoom/Focus interface to adjust the zoom and focus of the camera.

If the image is out of focus after a manual adjustment, one key focus can be used to set the focus automatically.

NOTE: This function is only available for models with a motorized zoom lens.

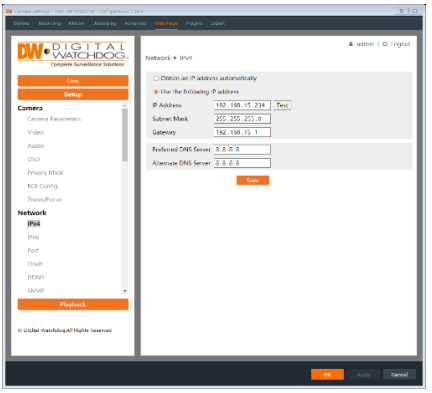

Camera Settings - DWC-MT95WiATW - DW Spectrum Client
General
Recording
Motion
Dewarping
Advanced
Web Page
Plugins
Expert
DIGITAL WATCHDOG
Complete Surveillance Solutions
admin | Logout
Live
Setup
Camera
Camera Parameters
Video
Audio
OSD
Privacy Mask
ROI Config
Zoom/Focus
Network
IPv4
IPv6
Port
Onvif
DDNS
SNMP
802.1X
Playback
© Digital Watchdog,All Rights Reserved
Camera ▸ Zoom/Focus
Day and night switching Focus
One Key Focus
Reset
Zoom -
Zoom +
Focus -
Focus +
OK
Apply
Cancel

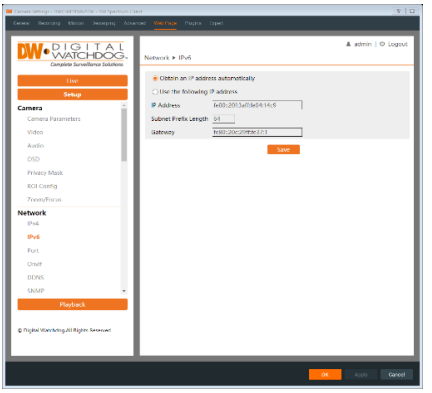
5.2 Network Configuration

5.2.1 IPv4 and IPv6

Go to Setup>Network>TCP/IP interface as shown below.

Use either IPv4 or IPv6 network addressing to configure the network connection for the camera.



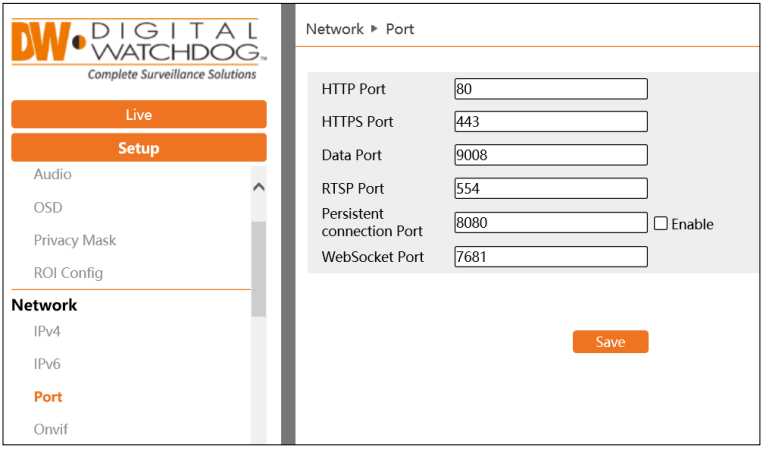


- **Obtain an IP address automatically:** Obtain an IP address automatically by DHCP from a DHCP network devices.
- **Use the following IP address:** Manually assign an IP address, subnet mask, gateway and DNS server preferences for the camera.
    - Test: Click the Test button to check the local network for availability of a manually entered IP address.

5.2.2 Port

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

Configure the HTTP port, Data port and RTSP port settings of the camera.



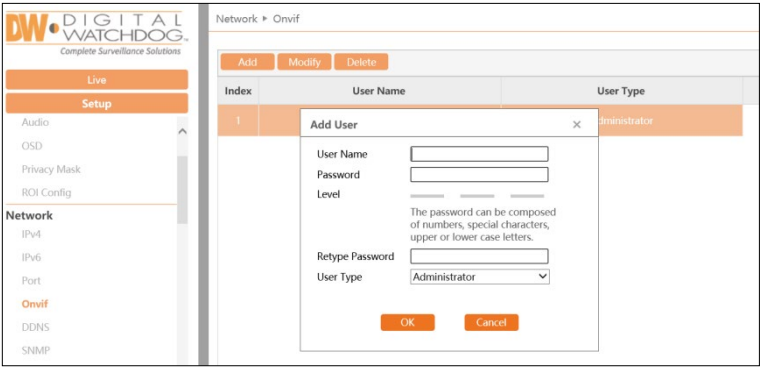
- **HTTP Port**: The default HTTP port is 80. It can be changed to any unoccupied port.
- **HTTPS Port**: The default HTTPS port is 443. It can be changed to any unoccupied port. (Some models may not support)
- **Data Port**: The default data port is 9008. Please change it as necessary.
- **RTSP Port**: 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 plug-in free preview.

5.2.3 ONVIF

The camera can be searched and connected to a VMS platform via ONVIF/RTSP protocol.

If “Activate Onvif User” was enabled in the initial device activation interface, the ONVIF user login will be activated simultanously. Use the ONVIF user information to login when connecting to a VMS.

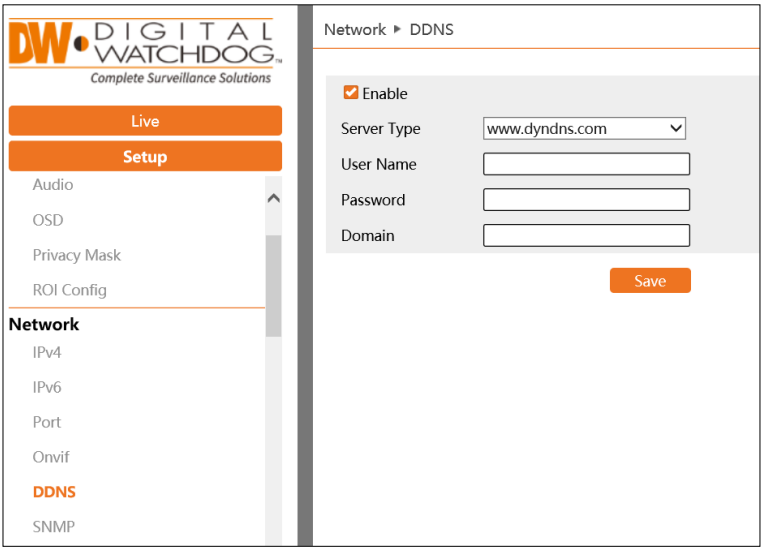
- Add: Click to create a new ONVIF user profile.
- Modify: Click to edit the currently selected ONVIF user profile.
- Delete: Click to delete the currently selected ONVIF user profile. The Administrator profile cannot be removed.



5.2.4 DDNS

If the camera is set up with a DHCP connection, DDNS can be set up for a URL to connect over the Internet.

NOTE: Subscription fees for DDNS registration may apply. Some VMS platforms may provide complimentary DDNS services.



To set up a DDNS:

1. Go to Setup>Network>DDNS and Enable DDNS.
2. Select a Service Type for the camera:

- www.dydns.com
- www.no-ip.com

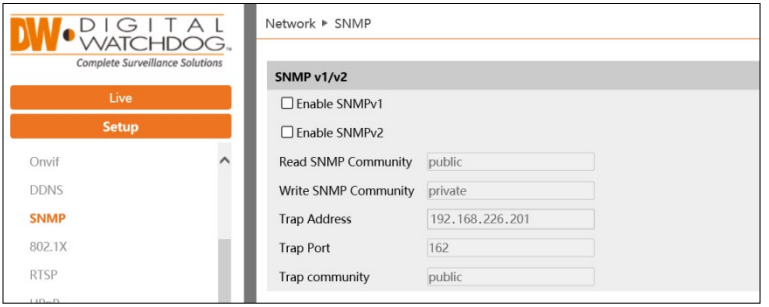
3. Visit the selected Service Type's website and register a domain name.
4. Enter the username, password and domain for the registered DDNS configuration.
5. Click the "Save" button to apply the settings.

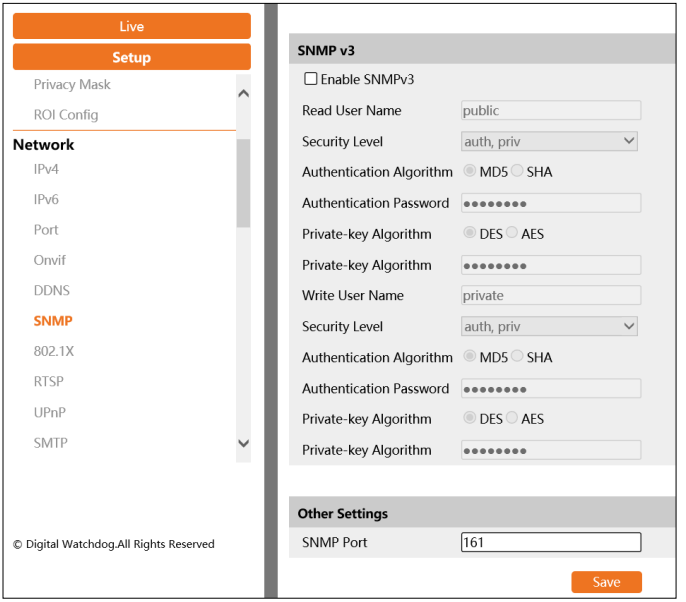
5.2.5 SNMP

Use the SNMP function to remotely monitor camera status, parameters, alarm information or to remotely manage the camera.

To configure SNMP:

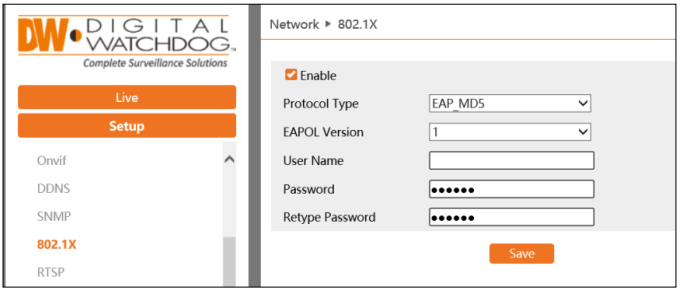
1. Go to Setup>Network>SNMP.
2. Before using SNMP, please install an SNMP management tool and set the parameters of the SNMP, such as SNMP port and trap address information.





5.2.6 802.1x

Enable 802.1x to protect the camera data with authentication and port-based network access control. User authentication will be required when the camera is connected to the network.



Connect the camera to a network switch that supports 802.1x protocol. The switch can be treated as an authentication system to find the device in a local network. If the camera connected to the network interface of the switch has passed the authentication of the switch, it can be accessed via the local network.

- **Protocol Type:** Please use the default settings (EAP_MD5)

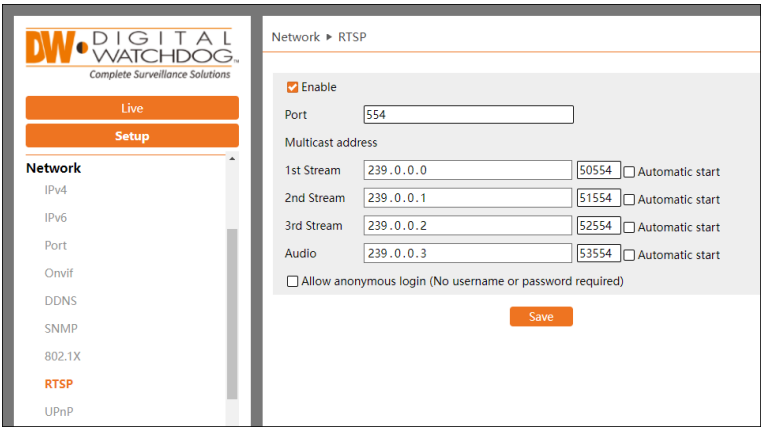
- **EAPOL Version:** Please use the default settings (EAPOL version 1)
- **Username and Password:** The username and password must be the same as the username and password applied for and registered in the authentication server.

5.2.7 RTSP

A maximum of up to three (3) simultaneous RTSP connections are supported at a time.

To enable RTSP, configure the RTSP Port or Multicast address settings, go to Setup>Network>RTSP.

NOTE: A multicast device will be needed when using multicast for one-to-many routing or many-to-many routing through the local network. RTSP connections with the 1st, 2nd or 3rd stream can be done directly between the camera and the receiving computer.



The 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) with a VLC media player to view multicast streams. Do not use the IPv6 address of the camera if using local play through a media player.

If there are multiple cameras being viewed through multicast, avoid using the same multicast address in the same local network.

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.

NOTE: If the coding format of the video for the mainstream is MJPEG, the video may be distorted at some resolutions.

- **Enable:** Select "Enable" to enable the RTSP function.

RTSP Address

- **Port**: Access port of the streaming media. The default number is 554.
- **RTSP Address**: The RTSP address (unicast) format that can be used to view the stream with a media player.
    - 1st Stream: *rtsp://Camera_IP:Port/profile1*
    - 2nd Stream: *rtsp://Camera_IP:Port/profile2*
    - 3rd Stream: *rtsp://Camera_IP:Port/profile3*

NOTE: When prompted to enter the RTSP stream login information, use the direct camera login credentials (admin) to validate the connection.

Multicast Address

If the "Automatic Start" setting is enabled, the received multicast data should be added to a VLC player to view video.

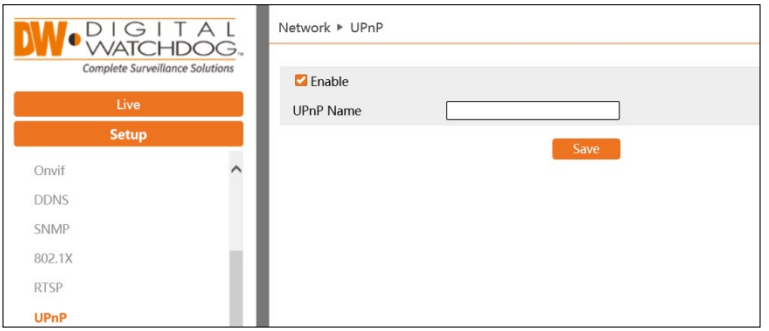
- **Multicast Address:**
    - 1st Stream: *rtsp://IP address: rtsp port/profile1?transportmode=mcast*
    - 2nd Stream*: rtsp://IP address: rtsp port/profile2?transportmode=mcast*
    - 3rd Stream: *rtsp://IP address: rtsp port/profile3?transportmode=mcast*
- **Audio:** Having entered the main/sub stream in a VLC player, the video and audio will play automatically.
- **Allow Anonymous Login:** When enabled, there is no need to enter the username and password to view the video when using RTSP.

5.2.8 UPNP

If this function is enabled, the camera can be identified by its assigned UPnP device name and be quickly accessed through the LAN.

Go to Setup>Network>UPnP.

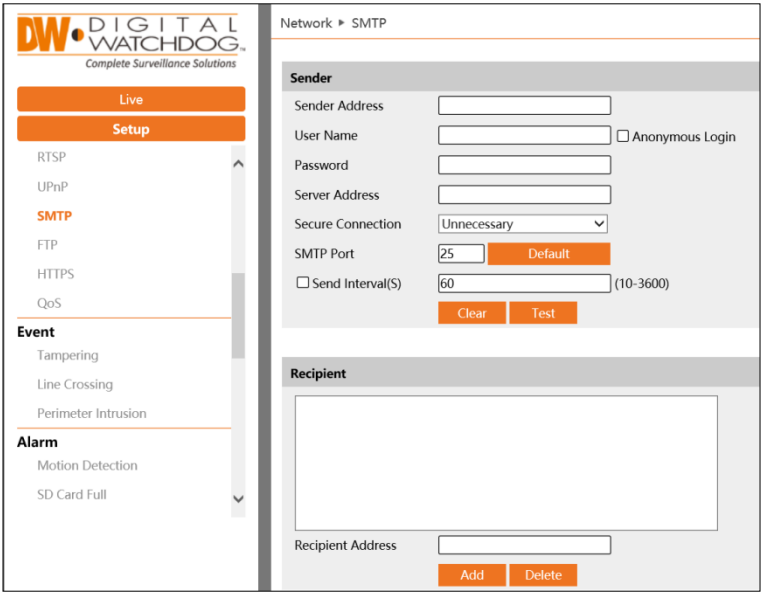
Enable UPNP and enter a UPnP name, then click the "Save" button to apply the settings.



5.2.9 SMTP

If you need the camera to send an email when an alarm is triggered or when the IP address is changed, you must provide email access for the camera to send email notifications. Otherwise, if you are using a VMS with the camera, you can use the SMTP setup of the VMS instead.

Go to Setup>Network >SMTP to configure the simple mail transfer protocol for the camera.



You can configure the following:

- **Sender Address:** Enter an e-mail address that the camera can use for

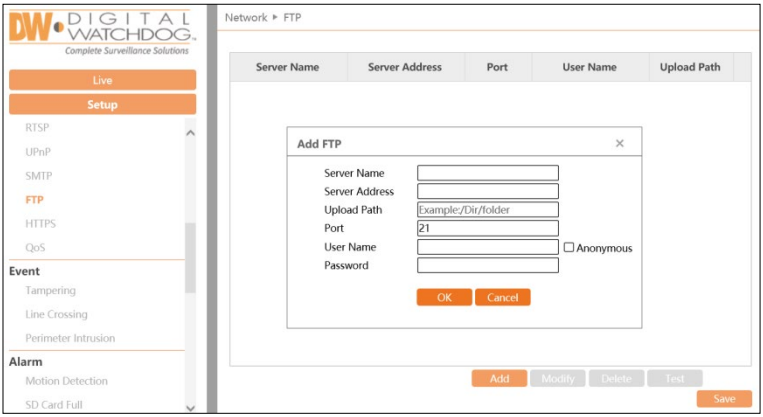
sending notifications.

- **Username:** Enter the username or e-mail address used to log in to the e-mail account.
- **Password:** Enter the password used to log in to the e-mail account.
- **Server Address:** Enter the IP address to the server if routing through a server.
- **Secure Connection:** Select the preferred method of encryption.
- **SMTP Port**: Enter the SMTP port of the e-mail service.
- **Send Interval(S)**: Set the time interval of how frequently an e-mail can be sent. For example, if 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 email notification will be sent. If one motion alarm event is triggered and then another motion detection alarm event is triggered after 60 seconds, two separate e-mail notifications will be sent. If multiple, separate alarms have been triggered simultaneously, multiple notifications will be sent separately.
    - Click the "Test" button to send a test e-mail after configuring the settings.
- **Recipient Address**: Enter the destination e-mail address that will receive the notifications.

5.2.10 FTP

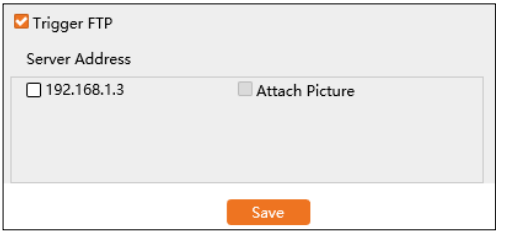
Set up an FTP server configuration to send snapshot images when an event alarm has been triggered. Snapshots will then be uploaded to the designated FTP server, depending on the event rule.

Go to Setup>Network >FTP.



To configure FTP settings:

1. Click the “Add” button to configure FTP server information for 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 folder directory where files will be uploaded.
   - **Port**: Enter the port number of the FTP server.
   - **Username and Password**: Enter the username and password that are used to log in to the FTP server.
2. Click “OK” to close the configuration window then click the “Save” button to apply the settings. When configuring event settings for intrusion, line crossing, etc., you can then enable “Trigger FTP” to assign the FTP connection.



Rule of FTP storage path: */device MAC address/event type/date/time/*

Example 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 will appear as follows:

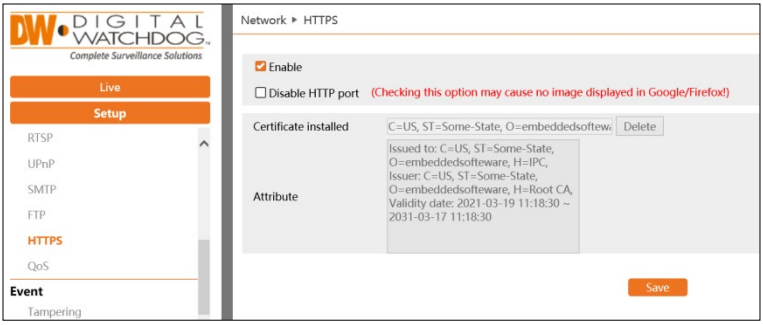
device name: xxx_mac: device MAC address Event Type time: YYYY-MM-DD:hh:mm

For example – *device name: IPC mac: 00-18-ae-a8-da-2a MOTION time: 2021-03-16 12:20:07*

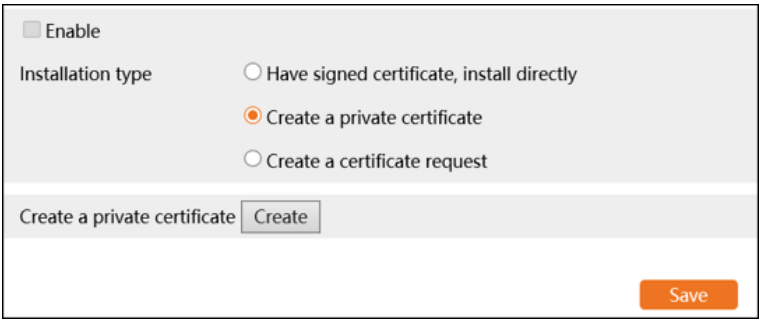
5.2.11 HTTPS

HTTPS supplies authentication requirements and protects user privacy by implementing a self-signed security certificate or by uploading a purchased certificate.

Go to Setup >Network>HTTPS as shown below.



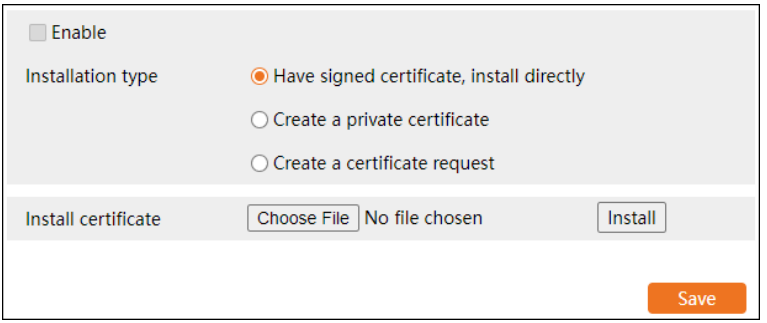
- **Enable:** Enable the HTTPS function to activate the encryption feature. Once activated, the camera web interface can then be accessed by with "https://" using a web browser.
- **Certificate Installed:** A self-signed certificate is installed by default.
    - A private certificate can be created if users don't want to use the default one. Click "Delete" to cancel the default certificate. The following interface will be displayed.
    - Attribute: Displays the creation details of the certificate.



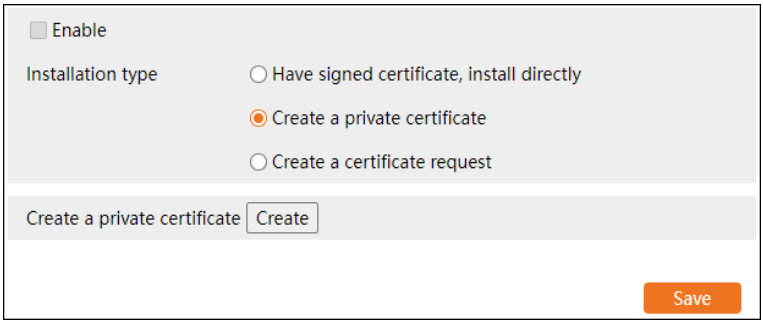
Creating a Private Certificate

To add a private certificate, you can either upload a certificate purchased from an SSL certificate vendor or create a private certificate in the camera. After deleting the default certificate, select the preferred *Installation Type*.

- **Have Signed Certificate:** If you have a signed certificate ready to be uploaded, click the "Choose File" button and select the private certificate. Click the "Install" button to upload the certificate to the camera.



- **Create a Private Certificate:** Click the "Create" button to enter the following interface.

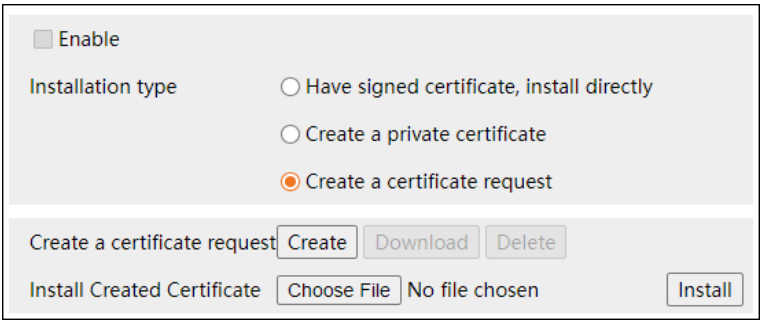


Configure the following to complete the form:

- Country: Enter the country (two-letter abbreviation).
- Domain: Enter the camera's IP address or URL domain of the camera.
- Validity Date: Enter the calendar day. The camera will automatically add the local date and time.
- Password: Enter a password to require additional authentication. Use of the same camera password is permitted.
- Province/State: Enter the state or province (two-letter abbreviation) of the location.
- Region: Enter the city or region of the location.
- Organization: Enter the name of the organization of the owner.
- Unit: Enter the unit name or number of the organization.
- Email: Enter the e-mail address that belongs to the administrator.

Click "OK" to save the settings.

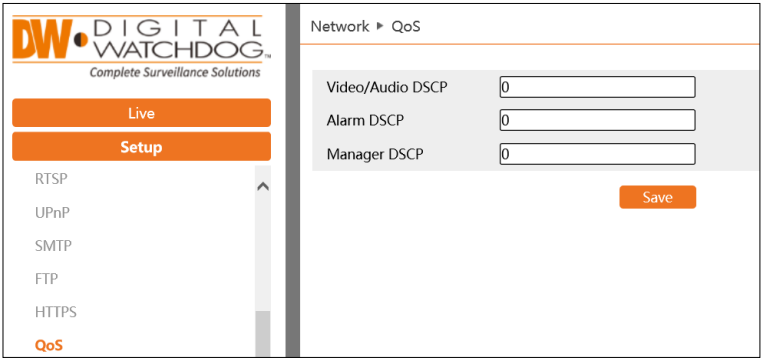
- **Create a Certificate Request:** Click the "Create" button to enter the interface. Then download the certificate request and send it to the trusted certificate authority for signature. After receiving the signed certificate, import the certificate to the device.



5.2.12 QoS

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

Go to Setup>Network>QoS.



- **Video/Audio DSCP:** The range is from 0 to 63.
- **Alarm DSCP:** The range is from 0 to 63.
- **Manager DSCP:** The range is from 0 to 63.

The larger the number is, the higher the priority will be considered.

5.3 Event Configuration

The camera uses scene learning to determine if the installation has been tampered with to determine if hardware sabotage has occurred.

To ensure that these detections are accurate, consider the following recommendations when installing the camera:

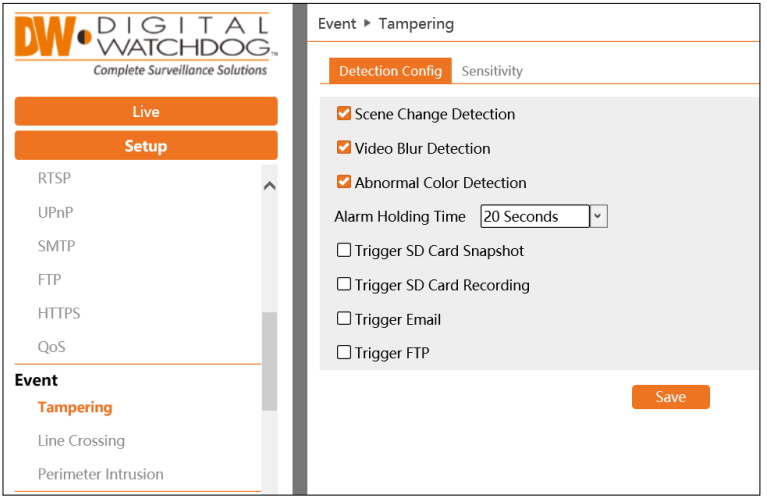
- Cameras should be installed on stable surfaces as vibrations can affect the accuracy of detection.
- Avoid pointing the camera at reflective surfaces like glossy floors, mirrors, glass, bodies of water, etc., where the camera's IR light can refract directly back into the camera or mirror images of a subject/person will commonly occur.
- Avoid places that are narrow or where there is a drastic difference in the presence of shadows.
- Avoid scenes where the color of the target object is the same as the background color.
- At any time of day or night, please make sure the camera view is unobscured and has adequate and evenly distributed light. Avoiding overexposure or too much darkness where there is a drastic contrast in lighting.

5.3.1 Tampering Detection

This function can detect changes in the surveillance environment affected by external factors.

To set Tampering Detection:

Go to Setup>Event>Tampering as shown below.

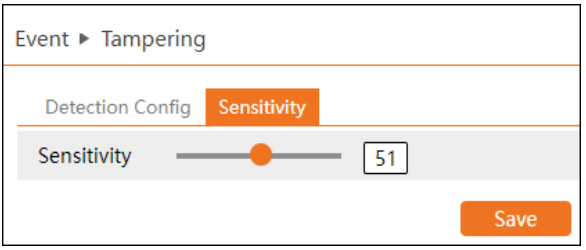


- **Scene Change Detection**: Alarms will be triggered if the scene has been considerably altered such as the lens becoming obscured, the camera is physically redirected, etc.
- **Video Blur Detection**: Alarms will be triggered if the video becomes blurred and out of focus.
- **Abnormal Color Detection**: Alarms will be triggered if the image suddenly becomes abnormally discolored.
- **Alarm Holding Time:** Set the alarm holding time. The alarm will remain active for the duration of the holding time.

Click the “Save” button to apply the settings.

Tampering Sensitivity

Click the “Sensitivity” tab to set the sensitivity of the Tampering detection.



- **Sensitivity:** Drag the slider to set the detection sensitivity value or manually enter the sensitivity value in the textbox. The higher the

value, the more sensitive the system will be for detection.

Click the “Save” button to save the settings.

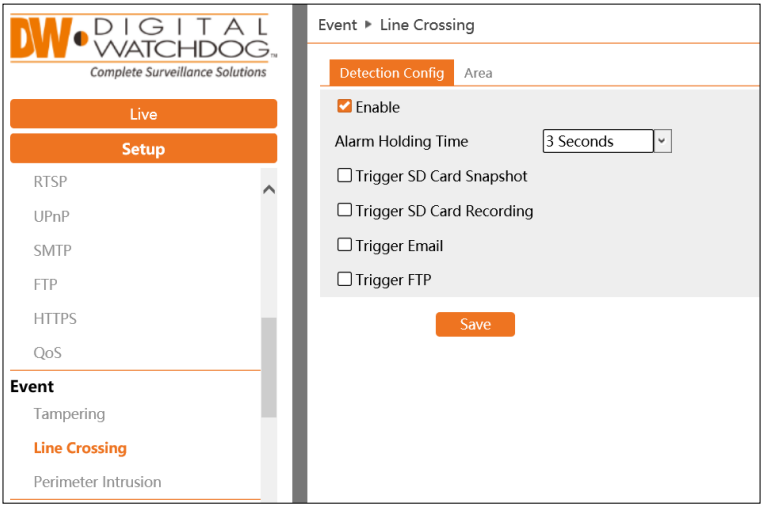
※ Recommendations for camera install and surrounding area

- Auto-focus should not be enabled for Tampering Detection.
- Do not enable Tampering Detection if lighting changes suddenly in the scene (lights being turned on/off, roaming spotlights, etc.)

5.3.2 Line Crossing

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

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



- **Enable:** Enable to activate Line Crossing detection.
- **Alarm Holding Time:** Set the alarm holding time. The alarm will remain active for the duration of the holding time.
- **Trigger SD Card Snapshot:** Enable to allow the camera to take a still image when the alarm is triggered (SD card required).
- **Trigger SD Card Recording:** Enable to allow the camera to record video to the SD card when the alarm is triggered (SD Card required).
- **Trigger Email:** Enable to allow the camera to use SMTP to send e-mail notifications when the alarm is triggered. Refer to *Section 5.2.9 SMTP* for more information.

- **Trigger FTP:** Enable to allow the camera to send snapshots and recordings to an external FTP server when the alarm is triggered. Refer to Section *5.2.10 FTP* for more information.

Line Crossing Area

Set the Line Crossing alarm area settings. Select the “Area” tab to draw the detection line.

- **Alarm Line:** Up to four (4) alarm lines at a time can be active. Select the preferred preset before drawing the detection line and click the “Save” button before drawing another alarm line.
- **Direction:** Select the direction that a target (person, vehicle, etc.) must cross the detection line to trigger the alarm.
  - **A<->B**: Alarms will be triggered when someone or a vehicle crosses over the alarm line from side B to side A or from A to B.
  - **A->B**: Alarms will be triggered when someone or a vehicle cross over the alarm line from side A to side B.
  - **A<-B**: Alarms will be triggered when someone or a vehicle cross over the alarm line from side B to side A.
- **Draw Area:** Click the “Draw Area” button and draw the alarm 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 apply the settings.

※ Recommendations for camera install and surrounding area

- Auto-focusing function may possibly interfere with line crossing

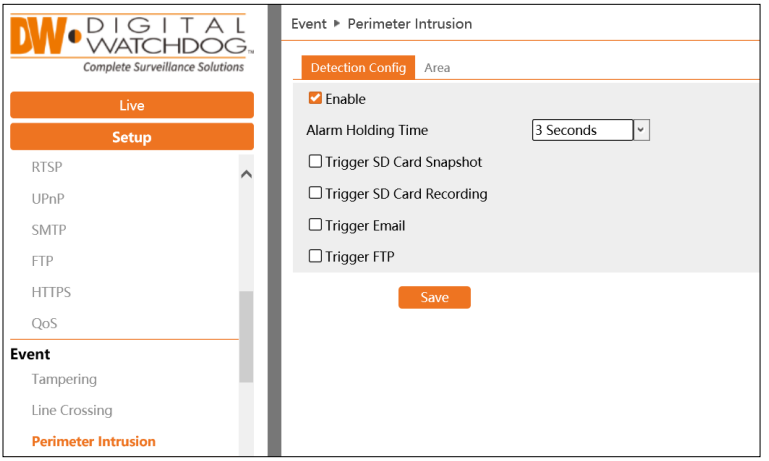
detection.

- Avoid aiming the camera at environments with plentiful foliage (trees, bushes, etc.) or with considerable lighting contrast. The feature works best will plentiful, even scene illumination.
- Cameras should be mounted at a height of 2.8 meters or higher.
- Keep the mounting angle of the camera at about 45°.
- The detected objects should occupy at least 1% of the entire image and the largest sizes of the detected objects should not be more than 1/8 of the entire image.
- Cameras should be able to view objects for at least 2 seconds in the detection area for accurate detection.
- Adequate light and clear scenery are crucial for line crossing detection.

5.3.3 Perimeter Intrusion

Perimeter Intrusion: Alarms will be triggered if a tracked target crosses into the pre-defined areas. This function can apply to important supervised locations, dangerous areas and prohibited areas.

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



- **Enable**: Enable to activate the Perimeter Intrusion feature.
- **Alarm Holding Time:** Set the alarm holding time. The alarm will remain active for the duration of the holding time.
- **Trigger SD Card Snapshot:** Enable to allow the camera to take a still

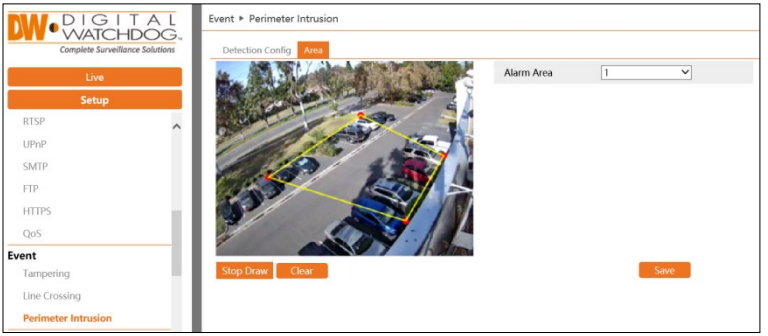
image when the alarm is triggered (SD card required).

- **Trigger SD Card Recording:** Enable to allow the camera to record video to the SD card when the alarm is triggered (SD Card required).
- **Trigger Email:** Enable to allow the camera to use SMTP to send e-mail notifications when the alarm is triggered. Refer to *Section 5.2.9 SMTP* for more information.
- **Trigger FTP:** Enable to allow the camera to send snapshots and recordings to an external FTP server when the alarm is triggered. Refer to Section *5.2.10 FTP* for more information.

Click the "Save" button to save the settings.

Perimeter Intrusion Area

Set the Perimeter Intrusion alarm area settings. Select the "Area" tab to draw the detection area.



- **Alarm Area:** Up to 4 alarm areas at a time can be active. Select the preferred preset number before drawing the detection area and click the "Save" button before drawing another Perimiter Intrusion Area.
- **Draw Area:** Click the "Draw Area" button and draw the detection area for the Perimeter Intrusion Alarm. Click the "Stop Draw" button to stop drawing. Click the "Clear" button to delete the alarm area. Click the "Save" button to apply the settings.

※ Recommendations for camera install and surrounding area

- Auto-focusing function should not be enabled for perimeter intrusion detection.
- Avoid the scenes with many trees or the scenes with various light

changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.

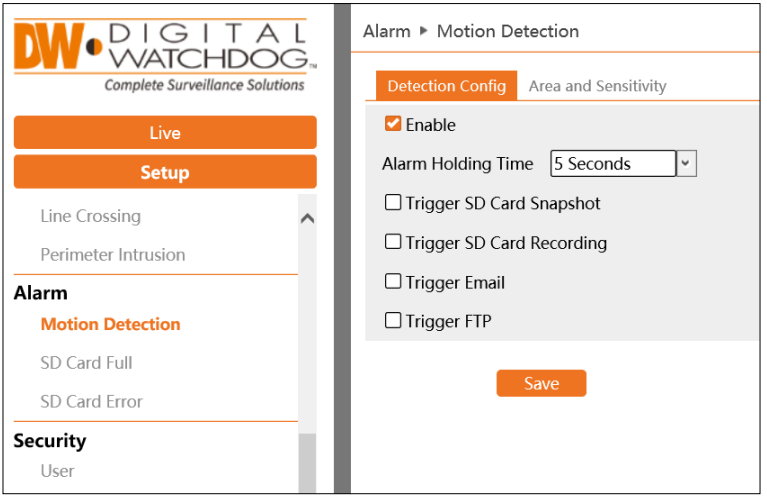
- Cameras should be mounted at a height of 2.8 meters or above.
- Keep the mounting angle of the camera at about 45°.
- The detected objects should not be less than 1% of the entire image and the largest sizes of the detected objects should not be more than 1/8 of the entire image.
- Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.
- Adequate light and clear scenery are crucial to perimeter intrusion detection.

5.4 Alarm Configuration

5.4.1 Motion Detection

The camera relies on motion detection settings to detect motion and to track object movements.

Go to Setup>Alarm>Motion Detection to enable motion detection alarm.



- **Enable:** Enable 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 occurring in the video.
- **Alarm Holding Time:** Refers to the interval time between the

adjacent motion detections. The alarm will remain active for the duration of the holding time. If there is motion detected while the alarm is still ongoing, it will be considered as continuous movement; otherwise, it will be considered as a single motion.

- **Trigger SD Card Snapshot:** Enable to allow the camera to take a still image when the alarm is triggered (SD card required).
- **Trigger SD Card Recording:** Enable to allow the camera to record video to the SD card when the alarm is triggered (SD Card required).
- **Trigger Email:** Enable to allow the camera to use SMTP to send e-mail notifications when the alarm is triggered. Refer to *Section 5.2.9 SMTP* for more information.
- **Trigger FTP:** Enable to allow the camera to send snapshots and recordings to an external FTP server when the alarm is triggered. Refer to Section *5.2.10 FTP* for more information.

Motion Area and Sensitivity

Set the motion detection area and the detection sensitivity.

Click the "Area and Sensitivity" tab to go to the interface as shown below.

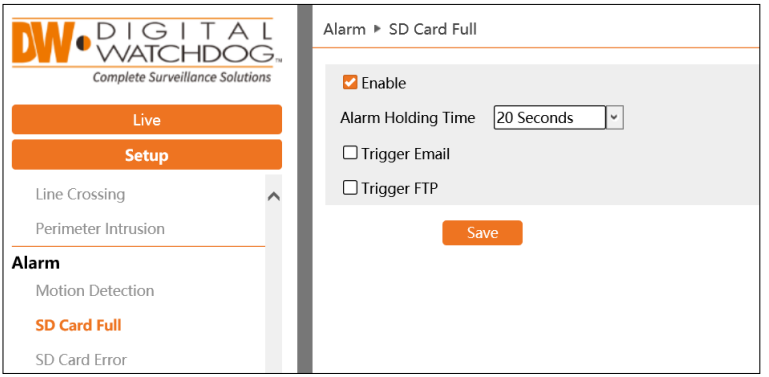
- **Sensitivity:** Move the "Sensitivity" slider to set the detection sensitivity. A higher sensitivity value means that the motion alarm will be triggered more easily.
- **Draw Area:** Select the "Add" toggle then click "Draw". Draw the motion detection area for the Motion Alarm in the grid. Highlighted squares in the grid indicate active detection areas. Select the "Erase" toggle to selected and clear motion detection areas from the grid. Click the "Save" to save the settings.

5.4.2 Other Alarms

SD Card Full

When the SD Memory Card has reached full-capacity a notification alarm will be triggered.

Go to Setup>Alarm>SD Card Full.

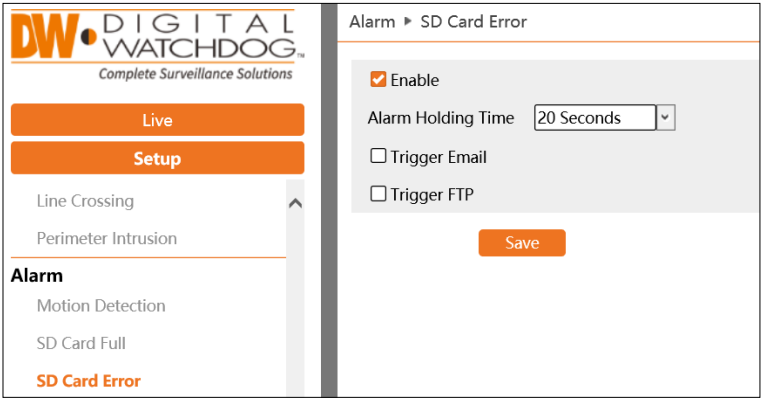


- **Enable:** Enable to activate the SD Card Full feature.
- **Alarm Holding Time:** Refers to the interval time between the adjacent motion detections. The alarm will remain active for the duration of the holding time.
- **Trigger Email:** Enable to allow the camera to use SMTP to send e-mail notifications when the alarm is triggered. Refer to *Section 5.2.9 SMTP* for more information.
- **Trigger FTP:** Enable to allow the camera to send snapshots and recordings to an external FTP server when the alarm is triggered. Refer to Section *5.2.10 FTP* for more information.

SD Card Error

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

Go to Setup>Alarm>SD Card Error.



- **Enable:** Enable to activate the SD Card Error feature.
- **Alarm Holding Time:** Refers to the interval time between the adjacent motion detections. The alarm will remain active for the duration of the holding time.
- **Trigger Email:** Enable to allow the camera to use SMTP to send e-mail notifications when the alarm is triggered. Refer to *Section 5.2.9 SMTP* for more information.
- **Trigger FTP:** Enable to allow the camera to send snapshots and recordings to an external FTP server when the alarm is triggered. Refer to Section *5.2.10 FTP* for more information.

5.5 Security Configuration

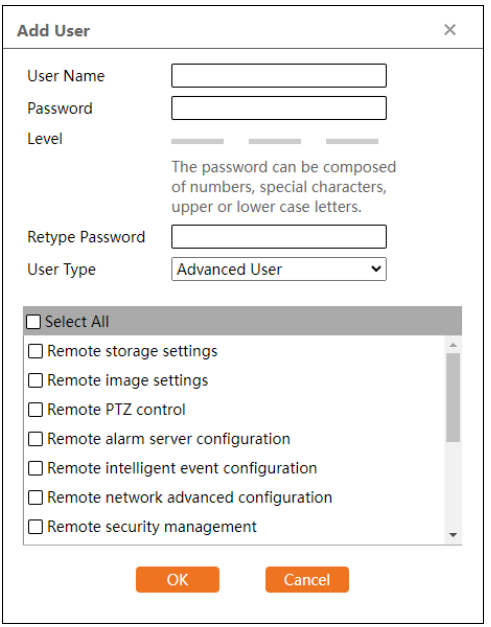
5.5.1 User Configuration

Use the *User Configuration* menu to directly configure the administrator password and user profiles of the camera.

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

Add User

Click the “Add” button to create a new user profile in the camera.



- **User Name:** Enter the username of the new user profile.
- **Password:** Create a password for the new user profile.
  - Level: Represents the overall password strength. Use a combination of numbers, special characters, capitalized letters, and lowercase letters when creating the password.
- **Retype Password:** Re-enter the password for the new user profile again.
- **User Type:** Select the preferred user role and select the user permissions.

Click the “OK” button to apply the settings and add the new user. The new user profile will be displayed in the users list.

Modify User

Select a user and click the “Modify” button to edit an existing user.

- **User Name:** Edit the username as needed.

- **Old Password:** To change the password, first enter the current password for the user. The *New Password* checkbox must be toggled.
- **New Password:** Enable the checkbox to prompt the password change and enter the new password for the user. The new password cannot be the same as the previous five (5) passwords.
- **Retype Password:** Re-enter the new password for the user.
- **User Type:** Change the preferred user role and user permissions as needed.

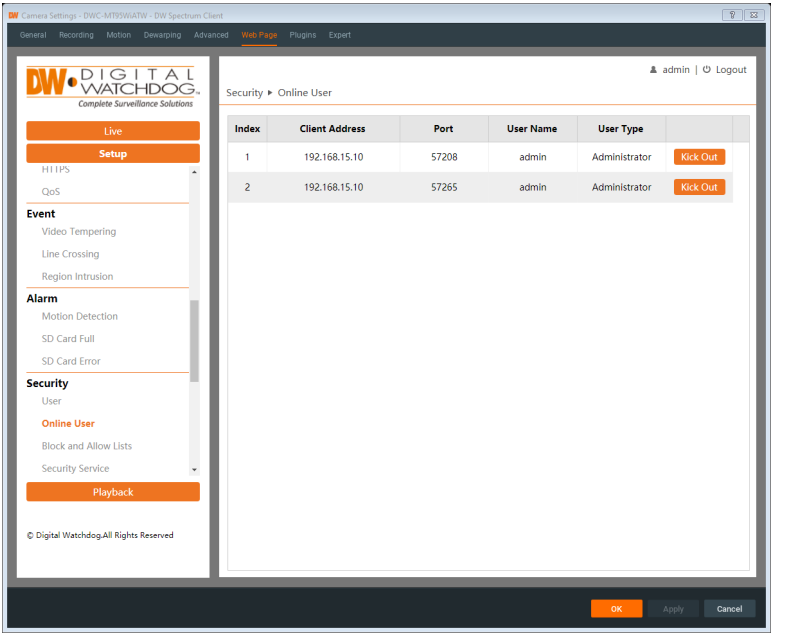
Click the “OK” button to save the settings.

Delete user:

Select a user and click the “Delete” button to delete an existing user. The *Administrator* user cannot be deleted.

5.5.2 Online User

Go to Setup>Security>Online User to view who is currently viewing live video from the camera by listing the IP address of the client, network port that is being accessed, and the user login that is being used.

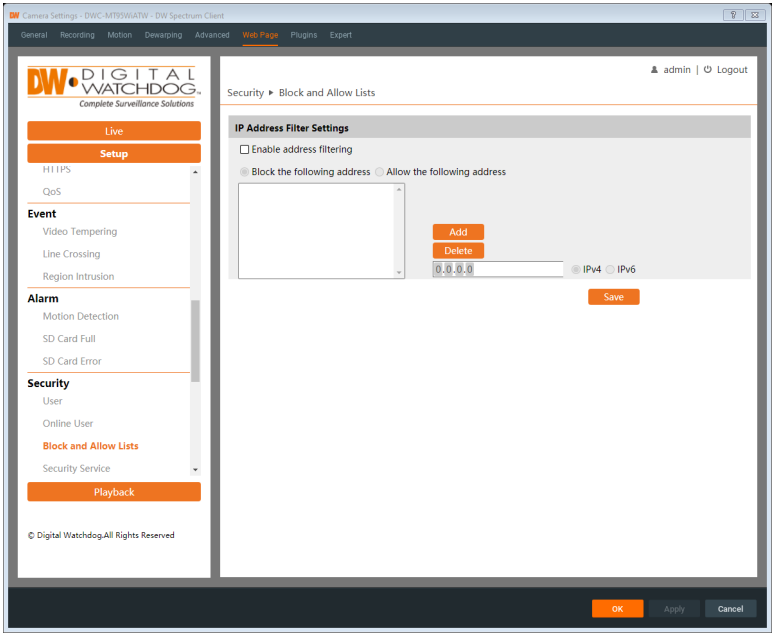


- **Kick Out:** An administrator user can kick out other users (including other administrators) from the camera. Kicking out a user will automatically add their IP address to the list of blocked users.

5.5.3 Block and Allow Lists

Manage a list of blocked and prioritized users by filtering IP addresses.

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



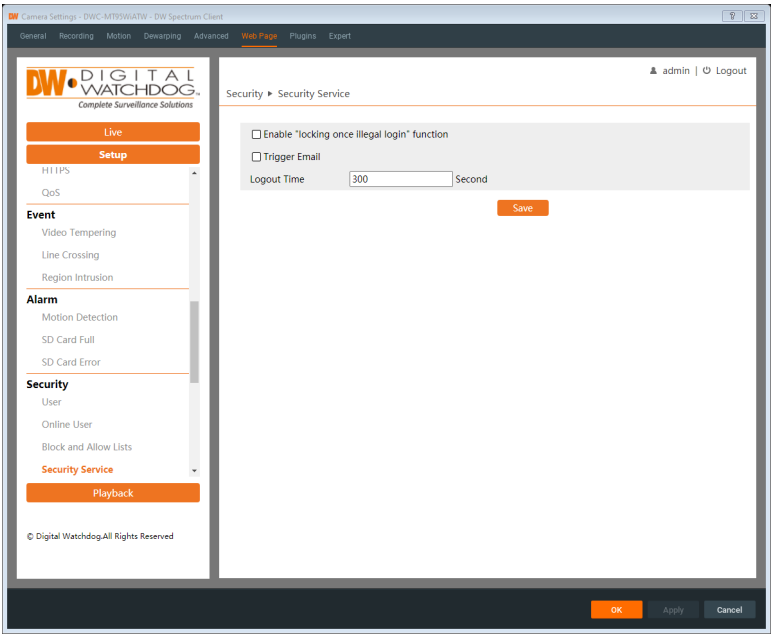
- **Enable Address Filtering:** Check the enable checkbox to activate IP filtering for the camera.
- **Allow/Block the Following Address:** Toggle to configure the list of blocked users or prioritized users.
- **IPv4/IPv6:** Toggle to enter either an IPv4 or IPv6 address. Enter the address into the address box then click the “Add” button to add to the list. To remove a user from the address filter, select the address and click the “Delete” button.

Click the “Save” button to apply the settings.

5.5.4 Security Service

Configure the auto-lock function for the camera in the *Security Service* menu.

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



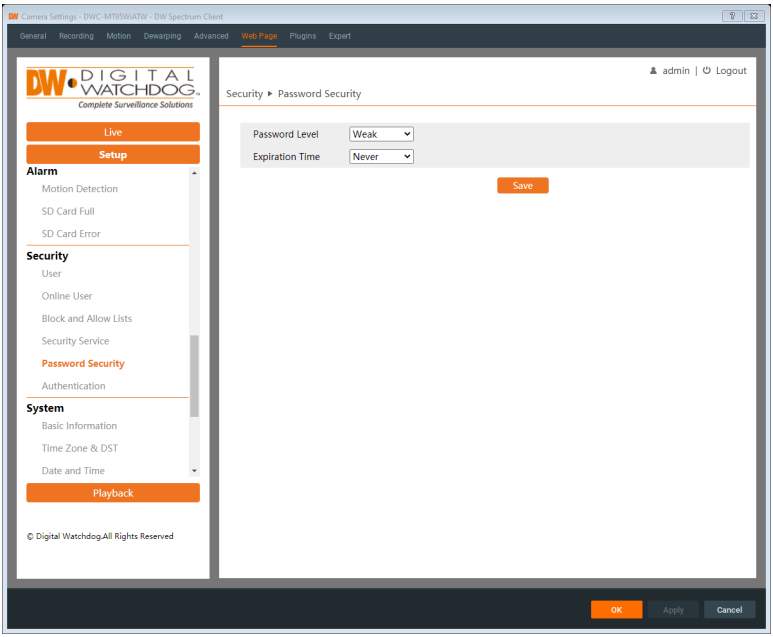
- **Enable “Locking Once Illegal Login” Function:** Enable this toggle to prevent brute force password attempts from unlocking the camera. If this function is enabled, the login failure will automatically lock after six failed attempts.
- **Trigger Email:**
- **Logout Time:** Configure the desired lease time for the camera to lock. The default settings will allow the camera to be logged into again after 30 minutes or after the camera has been rebooted.

Click the “Save Button to apply the settings.

5.5.5 Password Security

Set the desired password strength level and password expiration time limit for the camera.

Go to Setup>Security>Password Security as shown below.



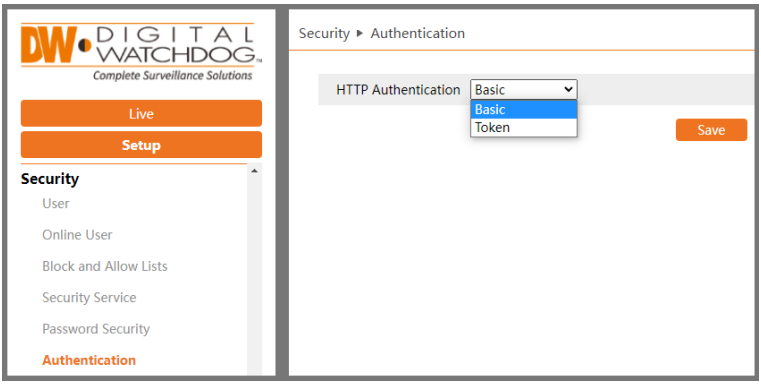
- **Password Level:**
  - Weak level: Numbers, special characters, uppercase or lowercase letters can be used. You can choose one of them or any combination of them when setting the password.
  - Medium Level: 8~16 characters, including at least two of the following categories: numbers, special characters, uppercase letters and lowercase letters.
  - Strong Level: 8~16 characters. Numbers, special characters, uppercase letters and lowercase letters must be included.
- **Expiration Time:** Set the amount of time before the camera requires that the Administrator password be updated.

Click the "Save" button to apply the settings.

5.5.6 Authentication

Set the http authentication protocol for the camera.

Go to Setup>Security>Authentication as shown below.

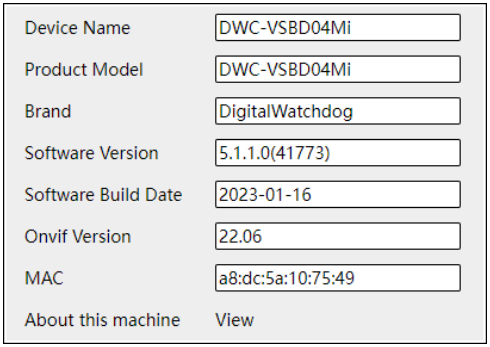


- **HTTP Authentication:** Select the preferred authentication protocol for connection with the camera.
  - Basic: Uses a basic username and password login to authenticate requests with the camera.
  - Token: An authentication scheme where the camera generates an encrypted string in response to a login request. The client must send this token in the authorization header whenever making requests with the camera. While considered to be more secure, this method also uses more overhead and may impact data speed with the camera.

5.6 System Configuration

5.6.1 Basic Information

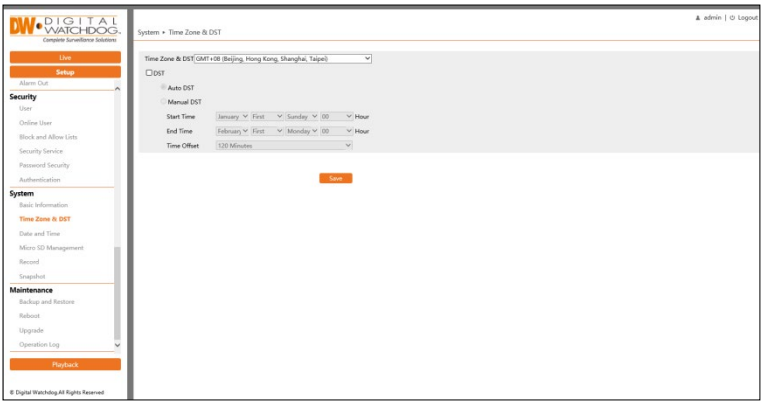
Basic Information lists the system information of the device including model, name, firmware version, Mac address and other information about the device.



5.6.2 Time Zone & DST

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

Go to Setup>System>Time Zone & DST to make adjustments as needed.

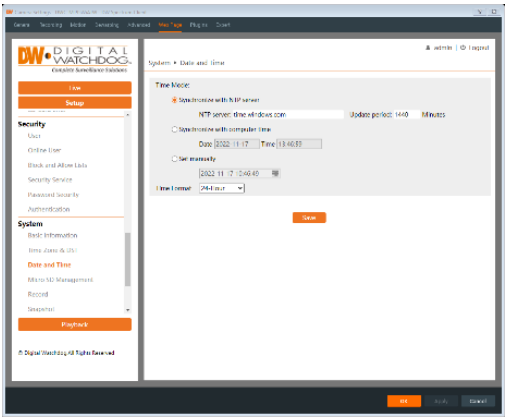


- **Time Zone & DST:** Select the current time zone of the camera.
- **DST:** Enable this toggle to activate the daylight savings time automatic function for the camera.
    - Auto DST: The camera will automatically change time settings on the second Sunday in March and the first Sunday in November to account for daylight savings time.
    - Manual DST: The camera will only change time settings at the manually specified times.
        - Start Time: Specify when the internal clock of the camera will move ahead.
        - End Time: Specify when the internal clock of the camera will move backward.
        - Time Offset: Select the amount of time (minutes) that the camera will change its internal clock.

5.6.3 Date and Time

Adjust the internal date and time settings of the camera.

Go to Setup>System>Date and Time to make adjustments as needed.

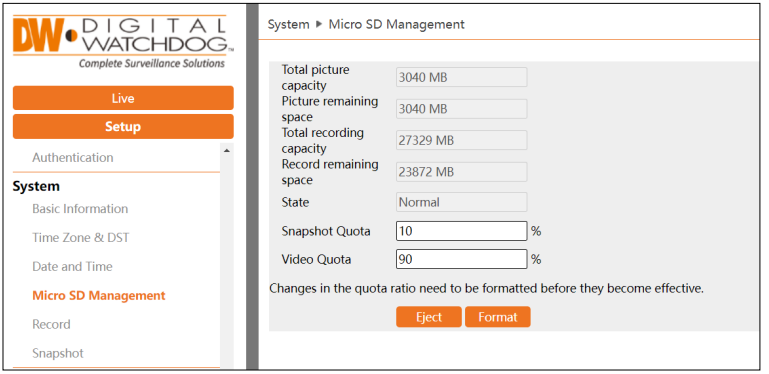


- **Synchronize with NTP Server:** Select this setting to have the camera periodically synchronize its time settings with an NTP server. The Windows Time service is used by default. An Internet connection needed for this option.
- **Synchronize with Computer Time:** Select this setting to have the camera synchronize with the current computer's date and time settings.
- **Set Manually:** Select this setting to manually set the internal date and time settings of the camera.
- **Time Format:** Select the preferred time format
    - 24-Hour: 00:00 ~ 23:59
    - 12-Hour: 12:00am ~ 11:59pm

5.6.4 Micro SD Management

Go to Setup>System>Micro SD Management to manage the SD Memory Card.

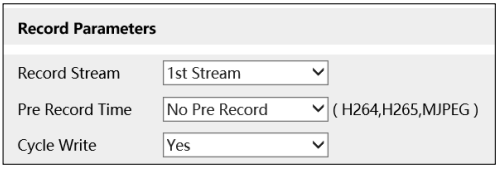
NOTE: SD Memory Card is not included with the camera. Consult your DW Sales Representative for SD Card needs.



- **Format:** Click this button to format the SD card. All data will be cleared.
- **Eject:** Click this button to stop writing data to the SD card before removing the SD Card from the camera.
- **Snapshot Quota**: Set the limit of captured pictures for the SD card.
- **Video Quota**: Set the limit of record files for the SD card.

5.6.5 Record

To adjust the recording parameters of the camera when using an SD card for storage go to Setup>Record to access the interface as shown below.

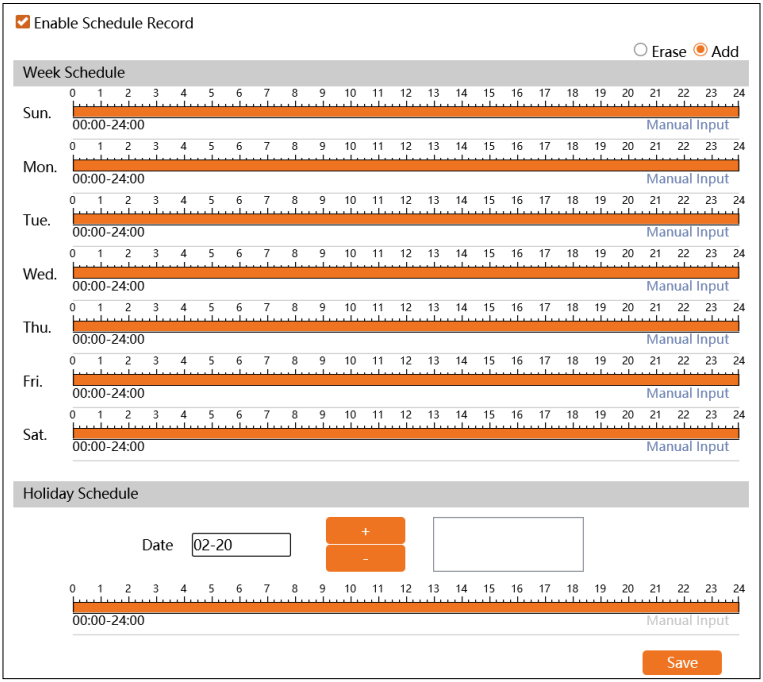


Record Parameters

- **Record Stream:** Select the camera's video stream that will be saved to the camera's storage.
- **Pre Record Time**: Set the fixed amount of time to begin recording before the operation to record is performed after an event has been triggered.
- **Cycle Write**: When set to "Yes", the camera will begin to overwrite old data on the SD card when storage is full.

Timing

- **Enable Schedule Record:** Enable this setting to have the camera follow a recording schedule when storing data to an SD card.
- **Week Schedule:** Set the schedule for the camera to record to the SD card throughout the week.
    - Add: Toggle to manually add a recording period from the schedule. Orange highlighted areas indicate that the camera is scheduled to record at that time.
    - Erase: Toggle to manually remove a recording period from the schedule.
    - Manual Input: Click on “Manual Input” to manually input the start and end recording times for that day.



Holiday Schedule

Set the recording schedule for a specific date.

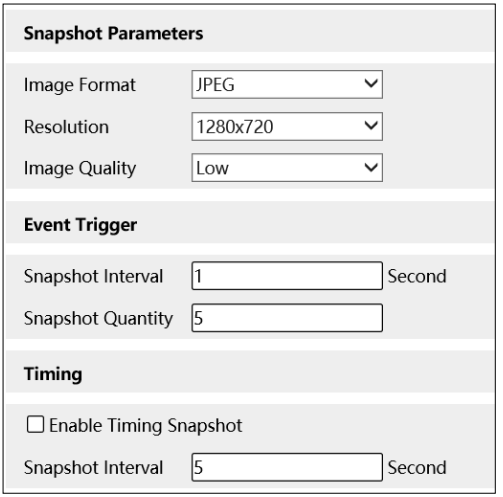
NOTE: Holiday schedule settings takes priority over the Week Schedule.

- **Date:** Enter the Month and Day (MM-DD) for the recording schedule.
    - +/–: Add or remove the selected date from the list.

5.6.6 Snapshot

Set the format, resolution and quality of the snapshot image that is saved to the SD card.

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



Snapshot Parameters

- **Image Format:** Image will be saved as JPEG.
- **Resolution:** Image will be saved at 640x480 resolution.
- **Image Quality:** Select the preferred image quality.

Event Trigger

- **Snapshot Interval:** Select the cooldown time for snapshot images when an event alarm has been triggered within the camera.
- **Snapshot Quantity**: The number you set here is the maximum quantity of snapshots that are permitted while remaining within the *Snapshot Interval* limit.

Timing

- **Enable Timing Snapshot**: Enable timing snapshot to have the camera regularly take snapshot images.
- **Snapshot Interval:** Select the cooldown time between snapshot images for the camera. For example, if set to “5 sec.” the camera

will take a snapshot every five (5) seconds.

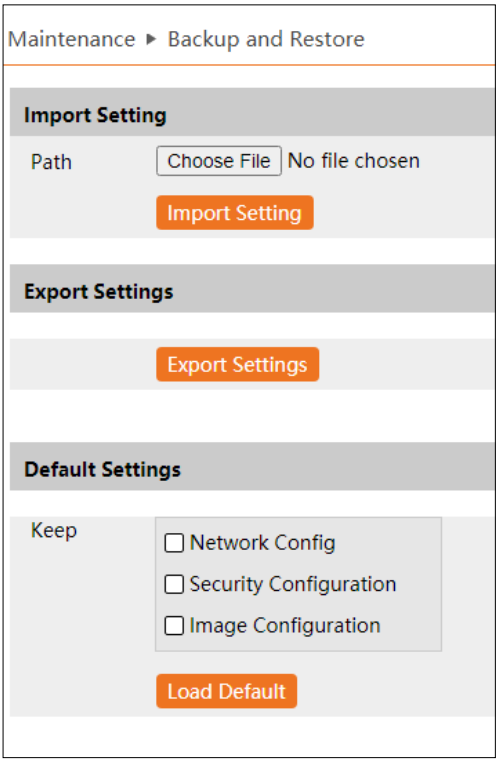
- Week Schedule: Set the schedule for the camera to regularly take snapshots. Setup is like setting the Recording Schedule of the camera (See Section 5.6.5 Record).
- Holiday Schedule: Set the schedule for the camera to regularly take snapshots on a specific date. Setup is like setting the Holiday Recording Schedule of the camera (See Section 5.6.5 Record).

5.7 Maintenance Configuration

5.7.1 Backup and Restore

Import or export camera setting configurations.

Go to Setup>Maintenance>Backup and Restore to go to the interface as shown below.



Import Setting

- **Path:** Click the “Choose File” button and select an exported configuration file to upload camera settings to the camera.

Export Settings

Click the “Export Settings” button to download a configuration file containing the camera settings to your computer.

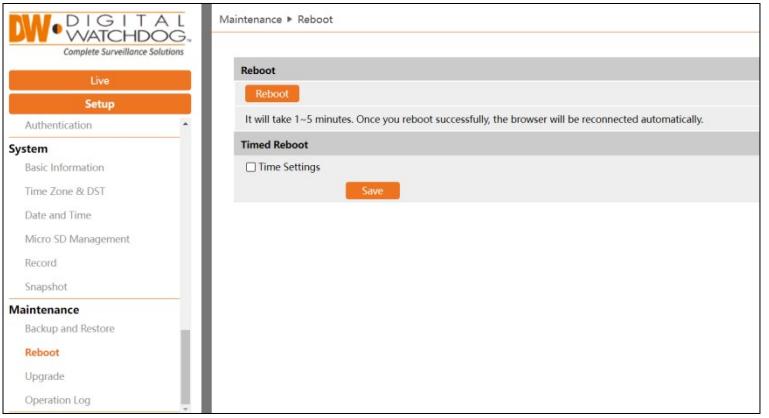
Default Settings

- **Keep:** Select which camera settings to keep before defaulting the camera.
- **Load Default:** Click the “Load Default” button to restore all system settings to the default factory settings. Settings selected in the *Keep* settings will remain unchanged.

5.7.2 Reboot

Reboot the camera virtually to restart the camera.

Go to Setup>Maintenance>Reboot to go to the interface as shown below.



Reboot

Click the “Reboot” button to reboot the device. The reboot process varies from 1-5 minutes, depending on the condition of the camera. Network connections will resume once the reboot has been completed.

Timed Reboot Setting:

If necessary, the camera can be set up to reboot at a regular time interval.

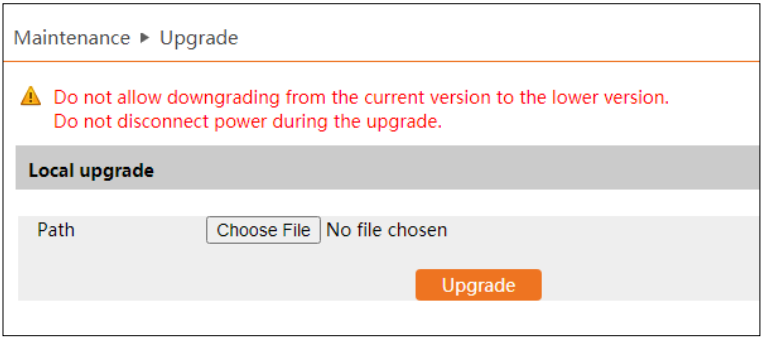
- **Time Settings:** Enable “Time Settings” to activate timed reboots.

- Week: Set the camera to reboot on a specific day of the week or daily at the scheduled time.
- Time: Set the time of the day (HH:MM) for the camera to automatically reboot on the scheduled day of the week.

5.7.3 Upgrade

Upload firmware files to the camera to update the camera firmware.

Go to Setup>Maintenance>Upgrade to go to the interface as shown below.



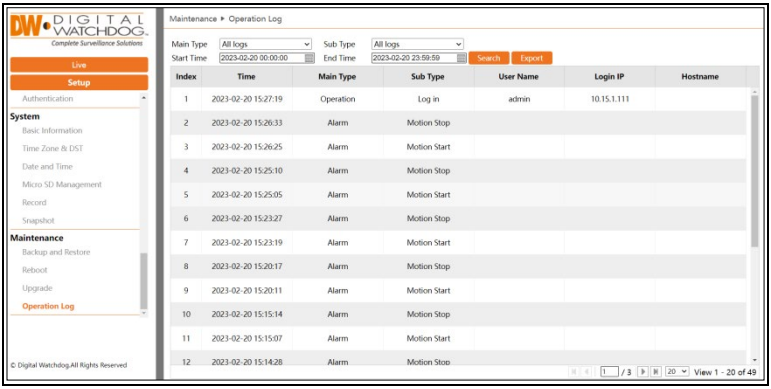
- **Path:** Click the "Choose File" button and select the upgrade file from the computer.
- **Upgrade:** After selecting the new firmware file in the *Path* setting, click this button to begin the firmware upgrade. The camera will automatically reboot after the firmware update has completed.

Caution! Do not close the browser or disconnect the camera from the network during the upgrade process.

5.7.4 Operation Log

View and export log records from the camera including information about alarms, connecting IP addresses, camera operation and setting changes.

Go to Setup>Maintenance>Operation Log to go to the interface as shown below.

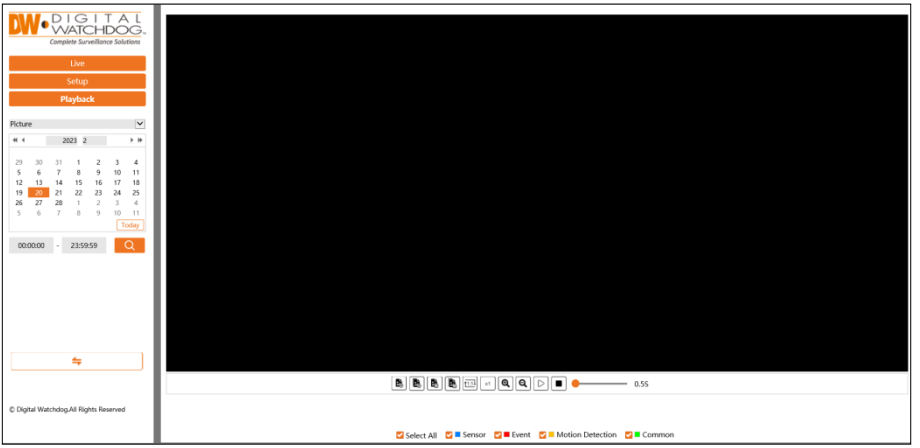


- **Main Type:** Select the category of log that you would like to view.
  - All Logs: View all major categories in a single list.
  - Alarm: View a list of event alarm occurrences logged by the camera.
  - Exception: View a list of IP addresses of clients denied access, client disconnections, SD card errors, etc.
  - Operation: View a list of setting change occurrences, user login/logout times, etc.
  - Information: View a list of DHCP activity, SD card activity, illegal login lock activity, etc.
- **Sub Type:** Select the sub-category of the log you would like to view.
- **Start Time:** Set the start date and time when filtering a specific timeframe for searching logs.
- **End Time:** Set the end date and time when filtering a specific timeframe for searching logs.
  - **Search:** Click this button to initiate the search function when filtering through logs.
  - **Export:** Click this button to export the log that is currently displaying as a .txt file.

6 Playback

6.1 Image Playback

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



To playback saved snapshot images from the camera:

1. Click the “Playback” button then use the dropdown and select “Picture”.
2. Set time: Select date and choose the start and end time.
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		Save all: Click this button to select the path for saving all

Icon	Description	Icon	Description
	the PC.		pictures on the PC.
	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 digitally zoom in.		Zoom out: Click this button to digitally zoom out.
	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 Playback

Click the “Playback” button to go to the interface as shown below. Videos that were recorded on the SD card can be played in this interface. SD card required.

To playback saved video from the camera:

1. Click the “Playback” button then use the dropdown and select “Record”.
2. Set search time: Select the date and choose the start and end time.
3. Click  to search for the video. Use the timeline bar to navigate footage.

Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Watermark display
	Enable/disable audio; drag the slider to adjust the volume after enabling audio.		

4. Select the alarm events at the bottom of the interface as needed.
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.

6.3 Specifications

	DWC-VSTB04Bi DWC-VSTB04BiB	DWC-VSTB04Mi
Image sensor	4MP 1/3" CMOS	
Total pixels	2560 × 1440	
Minimum scene illumination	0.005 lux (color)	
	0.0 lux (B/W)	
S/N ratio	≥50dB	
Focal length	2.8mm, 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°	92°~31°
IR distance	100ft range	164ft range
Audio in / out	1 audio input and 1 microphone built-in	
Audio compression	G.711A / U	
Event Trigger	Motion alarm/sensor alarm	
Pre/Post Recording	Pre: 1~5 sec., Post: 1~120 sec.	
Shutter mode	Auto, manual	
Shutter speed	1/2s ~ 1/100000s	
Auto gain control	Auto	
Day / night	Auto, day (color), night (B/W), schedule	
3D DNR	**Smart DNR™ 3D digital noise reduction**	
Wide dynamic range (WDR)	True WDR low, middle, high, 120dB	
Privacy zone	8 programmable privacy masks	
Video Analytics	Line crossing, perimeter intrusion, video tampering detection (scene change, video blur, abnormal color detection)	
Backlight Compensation (BLC)	Yes	
Mirror & Flip	Yes	
Alarm notifications	Notifications via email or FTP server	
Memory slot	Micro SD / SDHC / SDXC card up to 256GB (card not Included)	
LAN	802.3 compliance 10/100 LAN	
Video compression type	H.265, H.264, MJPEG	
Resolution	4MP, 3MP,2.1MP/1080P, 720P, D1, 480×240, CIF (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®, Mac® OS, Linux® Browser: MS Edge, IE, Chrome, Firefox	
Video management software	DW Spectrum® IPVMS	
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, ONVIF, NDAA	
Power requirement	DC 12V, PoE IEEE 802.3af Class 2. (Adapter not included)	DC 12V, PoE IEEE 802.3af Class 3. (Adapter not included)
Power consumption	<5W	<8W
Material	Metal turret housing	Metal turret housing
Housing color	DWC-VSTB04Bi: white DWC-VSTB04BiB: black	White
Dimensions	4.25″ x 3.77″ (108 x 96 mm)	5.16″ x 4.29″ (131.1 x 109 mm)
Weight	1.01 lb (0.46 kg)	1.41 lb (0.64 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 which 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 from vary from 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