MEGApix® InterCam™ IP Camera

DWC-INTCAM02- 2.1MP/1080p door station IP camera

User's Manual Ver. 02/25

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 the 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 corrosive detergent to clean the camera's main body. 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.
- The camera will not work if the temperature, humidity, and power supply exceed the limited stipulations.
- Avoid 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 and inconsistencies with the latest version, software upgrades and product improvements, and interpretation and modification. These changes will be published in the newest version without special notification.
- This manual's pictures, charts, and images are only for describing and explaining our products. In this manual, the trademarks, product names, service names, company names, and products 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 be responsible for abnormal operations, privacy leakage, or other

damages resulting from cyber-attacks, 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 lower-case letters should be used in your password.
- Change the passwords periodically to ensure only authorized users can access the system (the recommended time is 90 days).
- It is recommended that the service default ports (like HTTP-80, HTTPS-443, etc.) be changed to reduce the risk of outsiders accessing them.
- It is recommended that you set up a security system for your router. Important ports such as HTTP, HTTPS and dual ports cannot be closed.
- It is not recommended that the device be exposed 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 a passlist 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 to comply 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, it may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If harmful interference occurs, the user must correct the interface at his own expense.

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 restricting 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, improving the 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 to manage 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 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

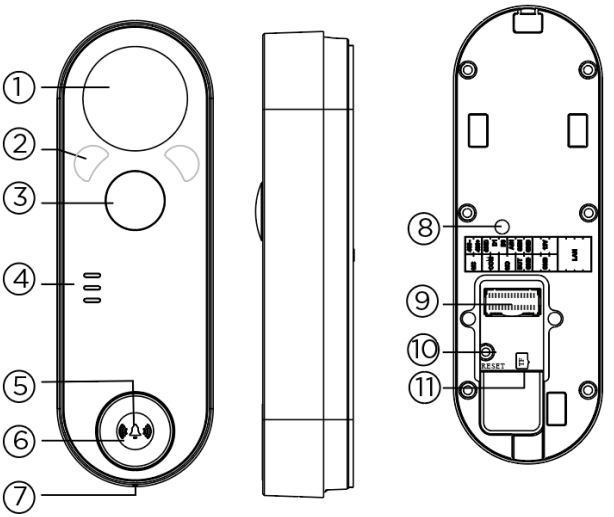
1. Introduction

1.1. Product and Accessories

Make sure that you have the following items supplied with your camera. If any 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 Guide	
Tilting Adapter Bracket	
Sun Shield Cover	
Mounting Template	
Cables	
Accessories Bag for Door Station Installation	2x Tapping Screws (4x25mm) and Anchors (6x29mm)
	1x Set Mounting Plate and Lock Screw (4x9mm)
	1x L-Wrench 5/64" (2mm)
	1x Back Panel Cover and 2x Screws (2x5mm)
	1x Set Waterproof Cap
Accessories Bag for Tilting Adapter Installation	2x Tapping Screws (4x25mm) and Anchors (6x29mm)
	2x Tilting Screws (4x8mm)
Accessories Bag for Sun Shield Installation	2x Tapping Screws (4x25mm) and Anchors (6x29mm)
	1x L-Wrench 5/64" (2mm)
	1x Lock Screw (4x9mm)
	3x Base Plate Screws (4x8mm)
	1x Sun Shield Screw (3x5mm)

1.2. Parts identification



Number	Description	Number	Description
1	White Light LED	7	Microphone
2	IR LEDs	8	Anti-Tamper Button
3	Camera	9	Terminal
4	Speaker	10	Reset Button
5	Alarm Indicator	11	SD Card Slot
6	Call Button		

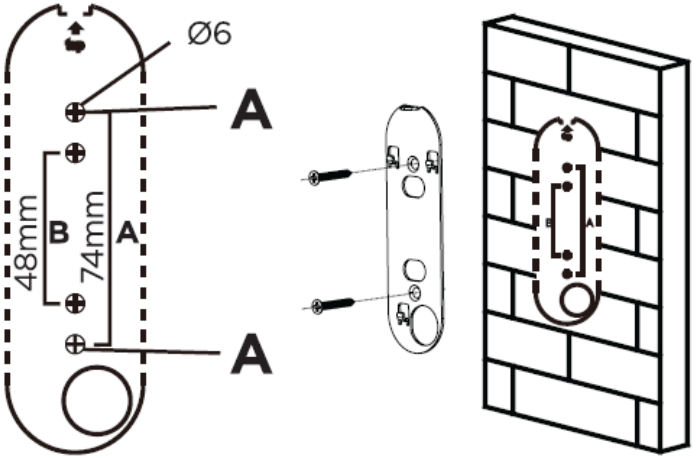
LED color indicators:

- Red: Start Recording
- Flashing Red: Network Disconnect
- Flashing Blue: Doorbell Button Activated
- Green: Standby Mode at Night
- Flashing Green: Firmware Upgrading

2. Installation

2.1. Preparing the Camera

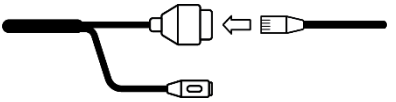
1. The mounting surface must bear at least five times the weight of your camera.
2. Mark and drill the holes marked 'A' in the mounting surface using the mounting template.
3. Secure the mounting template only the mounting surface using the machine screws and anchors included with the camera.



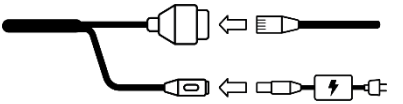
2.2. Powering the Camera

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.



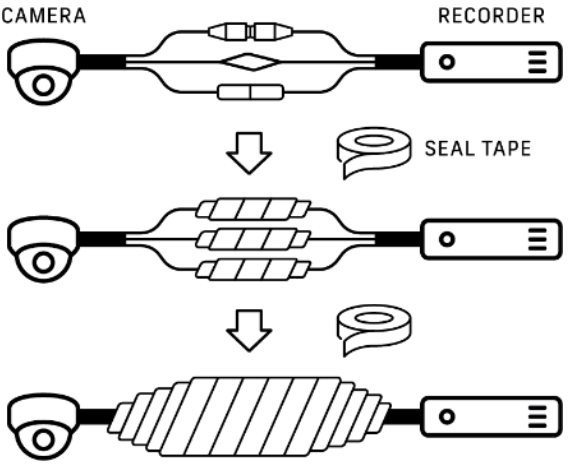
Use a non-PoE Switch to connect data using an Ethernet cable and use a power adapter to power the camera.

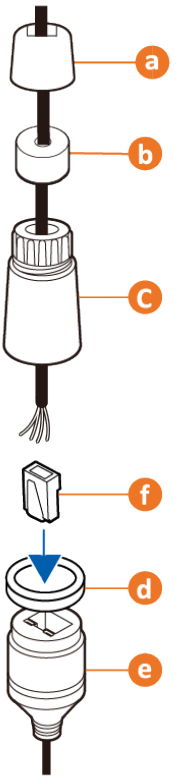


Power requirements	Power consumption
DC12V, PoE, adapter not Included.	<6W

To use the camera's waterproof wiring:

In extreme environments, use an outdoor-rated sealer.



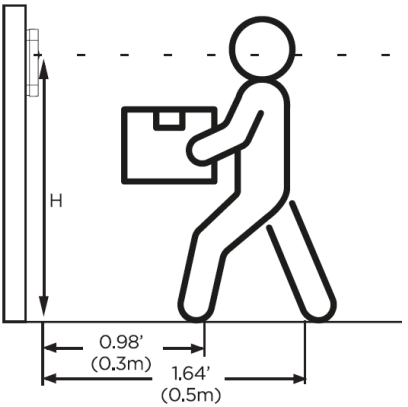


2.3. Installing the Camera

2.3.1. Height Requirements

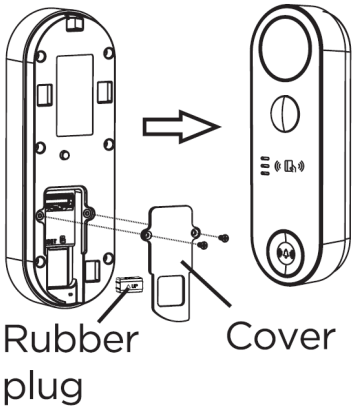
The recommended installation height is 4.75′ (1.45m)

Height	Distance	Human Height Range
4.75’ (1.45m)	0.98’ (0.3m)	0.98’ (0.3m)
	5.9’ ~ 5.51’ (1.4m~1.68m)	5.9’ ~ 5.51’ (1.4m~1.68m)
	1.64’ (0.5m)	1.64’ (0.5m)

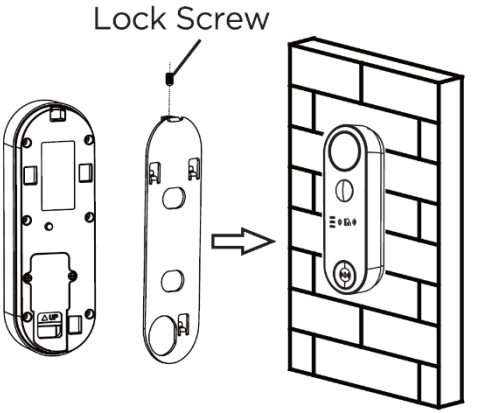


2.3.2. Direct Mounting Surface Installation

1. Use the cover and panel screws (2x5mm) to secure and lock the camera's control panel. Use the rubber plug to hold the cables in place.

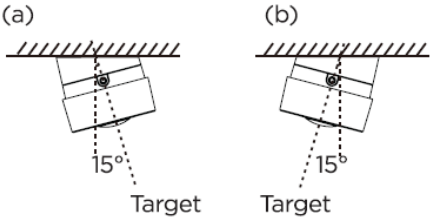


2. Attach the camera to the mounting plate using the lock screw (4x9mm) and L-wrench included with the camera.

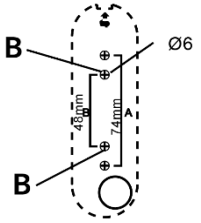


2.3.3. Installation Using the Tilting Adapter

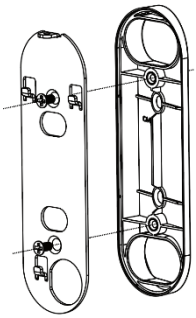
The adapter bracket allows users to mount the camera at a 15° angle.



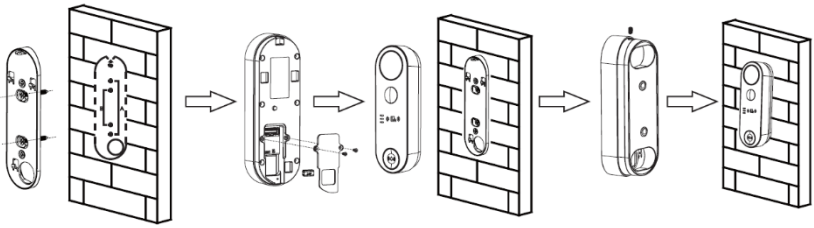
1. Mark and drill the holes marked 'B' in the mounting surface using the mounting template.



2. Secure the mounting plate onto the tilting adapter using the two (2) tilting screws (4x8mm).

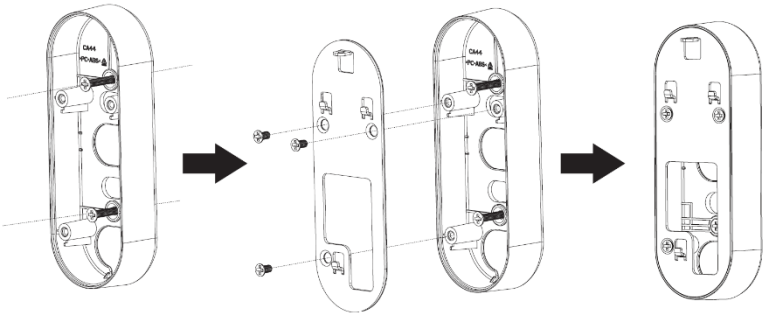


3. Pass wires through and mount the camera to the mounting plate and tilting adapter using the cover and panel screws (2x5mm) and lock screw (4x9mm). (Repeat STEP 2.3.2, #1~2).

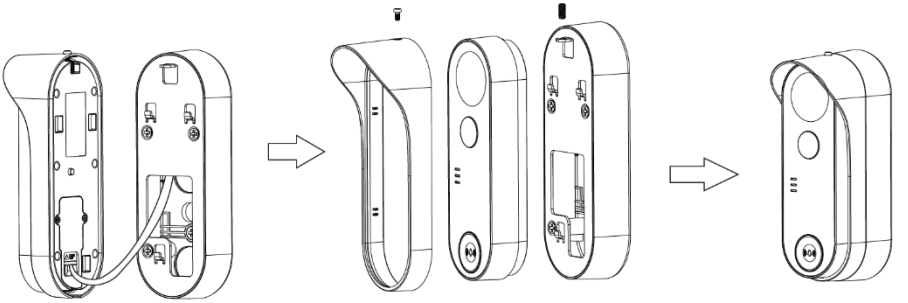


2.3.4. Installation Using the Sun Shield Cover

1. Mark and drill the holes in the mounting surface using the sun shield's junction box. Use the tapping screws and anchors to secure the junction box.
2. Secure the plate onto the junction box using the three (3) base plate screws (4x8mm).

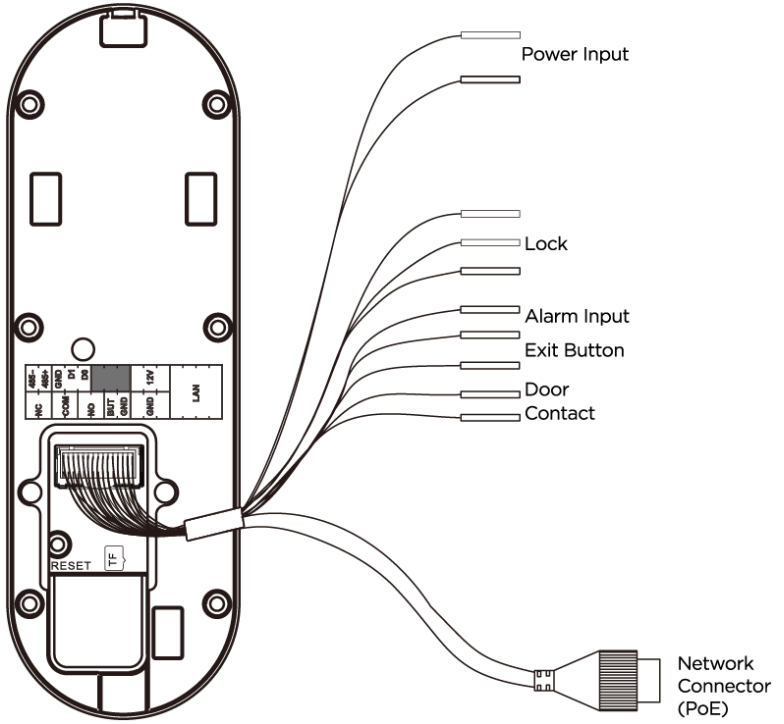


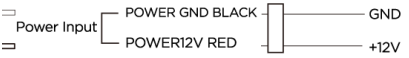
3. Pass wires through and mount the camera to the sun shield's base using the cover and panel screws (2x5mm) and lock screw (4x9mm). (Repeat STEP 2.3.2, #1~2).
4. Secure the sun shield external cover to the camera using the screw (3x5mm).

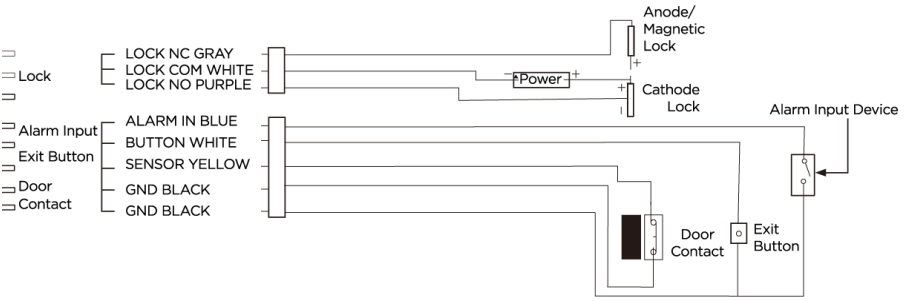


2.4. Cabling

The diagram below connects power, network and audio to the camera.

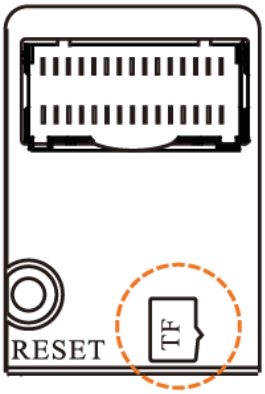






2.5. Managing the SD Card

1. Remove the control panel cover in the back 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.



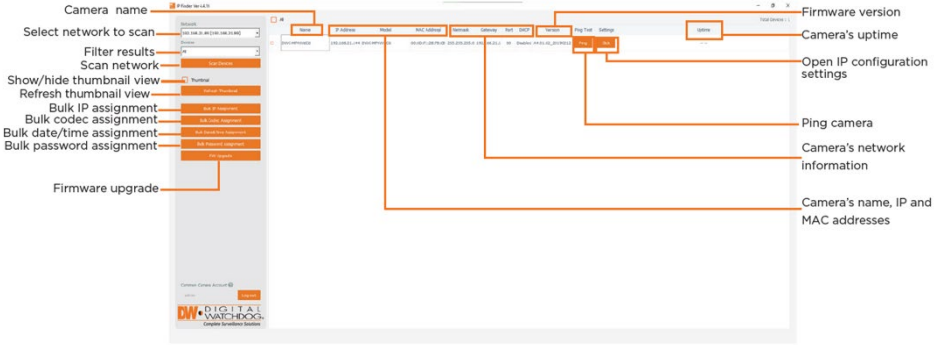
2.6. Resetting the Camera

Resetting the camera:
Press the reset button in the camera's control panel for five (5) seconds to initiate a 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.

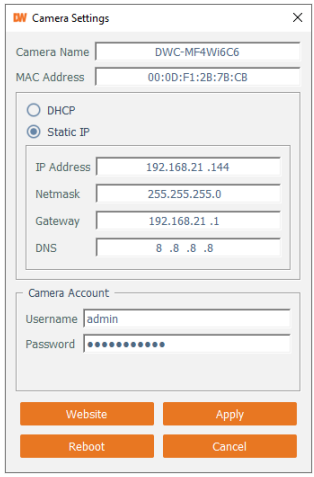


1. To install DW IP Finder, use a web browser and go to http://www.digital-watchdog.com.
2. Enter "DW IP Finder" on the search box at the top of the page.
3. Go to the "Software" tab on the DW IP Finder page to download and install the installation file.
4. Open DW IP Finder and click 'Scan Devices.' 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. A password must be set when connecting to the camera for the first time. To use DW IP Finder for *Bulk Password Assignment*:

a. Check the box in the IP Finder's search results next to the camera. 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 at least 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 popup 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. Click the' Website' button to access the camera's web page.
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.

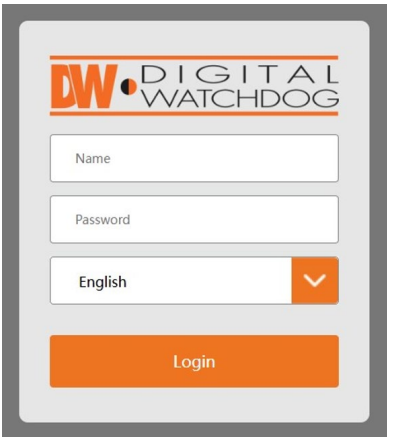
- To access the camera from an external network, port forwarding must be set in your network's router.

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:

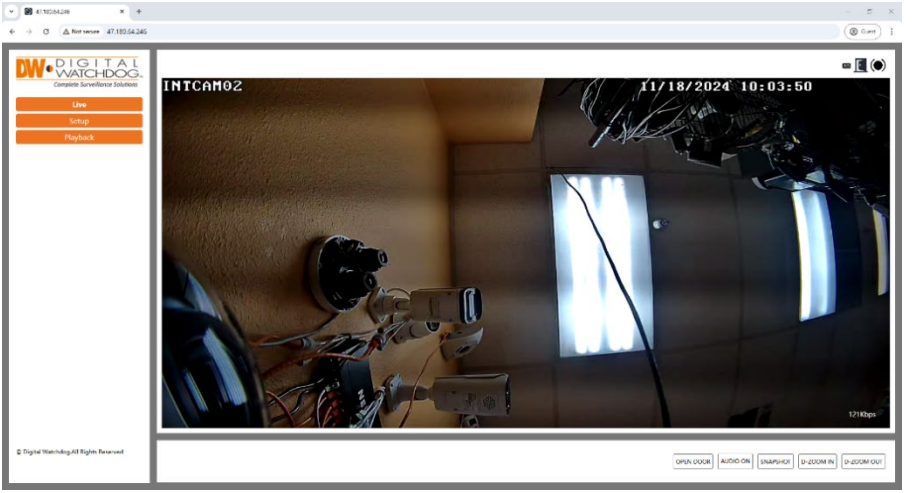
1. Find the camera using DW IP Finder.
2. Double-click on the camera's view in the results table.
3. Press the 'Website' button. The camera's web viewer will open in your default web browser.
4. Enter the camera's username and password that was set up in DW IP Finder. If you did not set up a new username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

After logging in, the following window will be shown.



The following table shows the icons' instructions on the live view interface.

Left navigation bar:

- Live: View live video from the camera.
- Setup: Go to the camera's settings menu.
- Playback: Open the search and playback from the SD card.

Bottom navigation bar:

- Open Door: Manually unlock the door.
- Audio On: Turn on audio from the camera's built-in microphone.
- Snapshot: capture a snapshot of the camera's current live view. The Snapshot will be saved locally on the viewing computer as a JPEG file.
- D-Zoom In: Digitally zoom into the camera's view.

- D-Zoom Out: Digitally zoom out of the camera's view.

Top navigation bar:

- SD Card: When the icon lights up, the camera records video on the local SD card.
- Door Open: when the icon lights up, the door connected to the camera is open.
- Alarm In: when the icon lights up, the camera's alarm input is activated.

* Plug-in free live view: the local recording is not supported, and the preview mode switch (real-time/balanced/fluent mode) is unavailable.

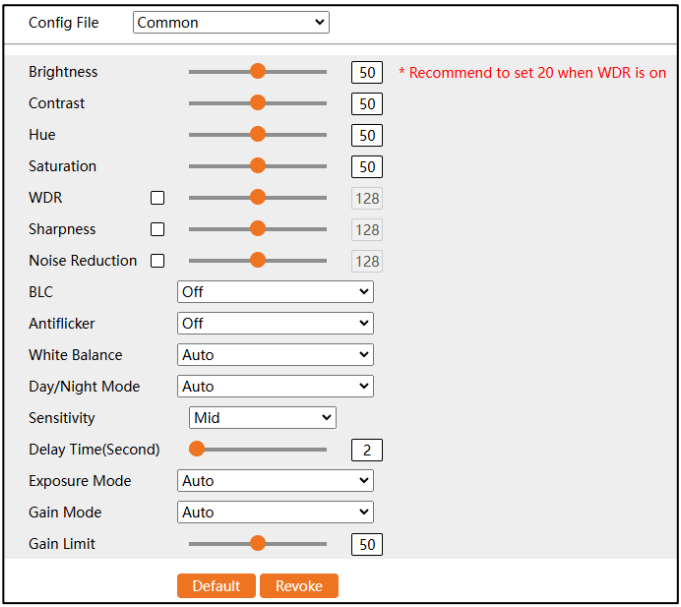
5. Web Configuration

In the Webcam client, choose "Setup" for the configuration interface.

5.1. Camera Settings

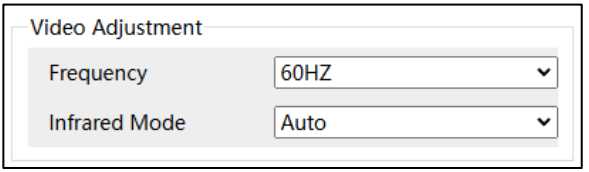
5.1.1. Display Settings

Use the menu options below to adjust the camera's image, color and brightness. All settings can be adjusted separately for common day and night schedules. Edits will be shown in the preview screen on the left.



- **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 image plane's resolution level and the image edge's sharpness level.
- **Noise Reduction**: Decrease the noise and make the image more thorough. Increasing the value will improve the noise reduction effect, but it will also 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 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 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 antiflicker function, which is mostly used 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 required to trigger switching Day/Night modes.
  - Delay Time (Seconds): Set when 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 automatically adjust according to the 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."

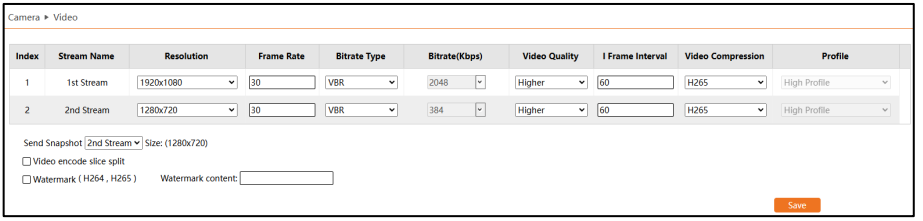


**NOTE: If selected/enabled for some items, the camera will reboot automatically. After that, clicking the "Default" button will not take effect.

- **Default**: Click to reset all settings to their default settings.
- **Revoke:** Click to undo the last settings change.

5.1.2. Video Configuration

Set the Resolution, Frame rate, Bitrate type, video quality, etc. Three video streams are available for configuration in this menu. The viewing experience is subject to the actual network conditions.

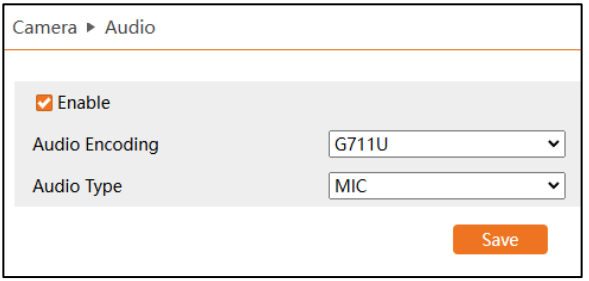


- **Resolution**: Adjust the stream resolution from the options in the drop-down menu.
- **Frame rate**: The higher the frame rate, the more individual frames will be shown per second. A higher FPS results in smoother video but will increase the video stream's bitrate.
- **Bitrate type**: Select between CBR and VBR bitrate types. Bitrate is related to image quality.
    - CBR: Compression bitrate will remain constant, with changes occurring 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 camera's network bandwidth usage.
- **Bitrate (Kbps)**: The bitrate type must be set to CBR to adjust this setting manually. A higher bitrate will result in better image quality.
- **Video Quality**: The bitrate type must be set to VBR to adjust this setting manually. 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 result 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: The highest quality H.264 profile has the highest amount of compression: increased data rate and need for decoder performance.
- **Send Snapshot:** Select which video stream to use when creating a snapshot from the camera.
- **Video Encoder Slice Split:** Enable this function to improve the image when using a low-performance PC.
- **Watermark:** The watermark can be displayed when playing back the locally recorded video in the search interface. To enable it, check the watermark box and enter the watermark text.

5.1.3. Audio Configuration

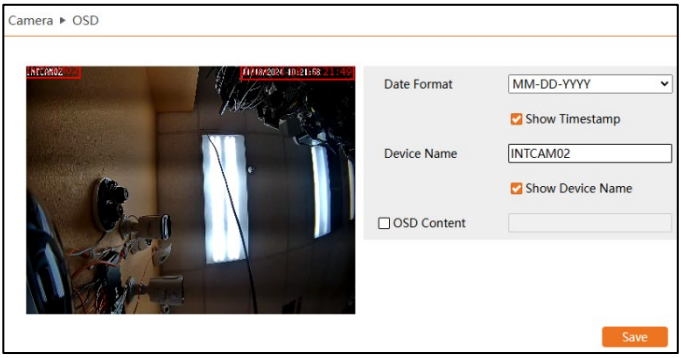
Use the interface below to enable the camera's audio.



- **Enable:** Enable audio settings for using a microphone. The audio can be turned on or off 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 MIC, an audio socket connecting a wired microphone.

5.1.4. OSD Configuration

Users can add time stamps and device name information to the camera's video.



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

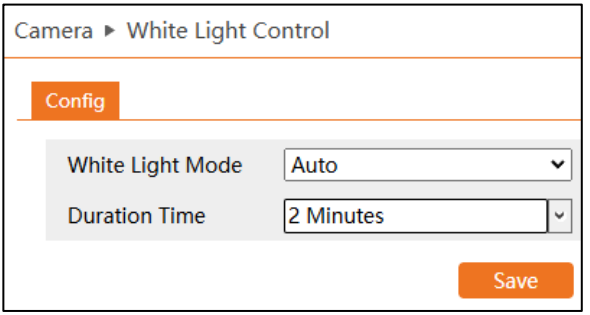
Click the "Save" button to apply the settings.

- **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 the customization of the overlay text—a maximum of 15-characters.

Click 'Save' to save all settings.

5.1.5. White Light Control

Use the below interface to control when the camera's white light LEDs are activated and for how long.



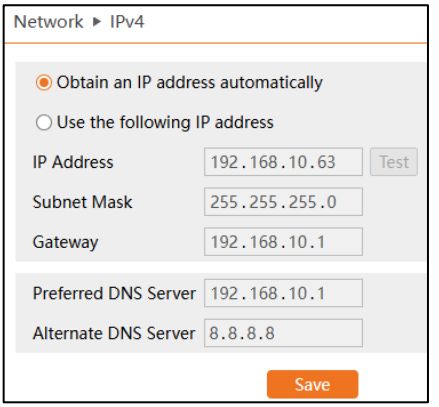
- **White Light Mode:** "OFF," "Manual," or "Auto" is optional. In low illumination conditions, this mode can be enabled.
- **Auto**: The white light will be automatically enabled when collecting a face in low illumination conditions. If the auto mode is selected, the duration time should be set to save energy. For example, the white light is on, and the duration is set to "2 minutes"; if no face appears in the detection area after 2 minutes, the white light will be turned off automatically.
- **Manual**: Select this mode and click "Save". The white light will be turned on. In this mode, you can also set the brightness of white light as needed.
- **Duration Time:** Once the white light is activated, select the duration before the white light turns off.

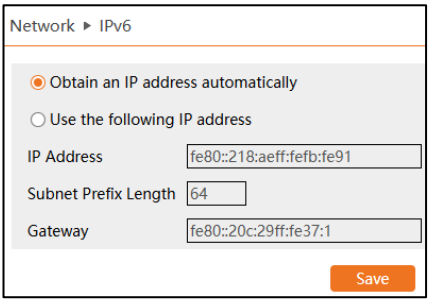
Click 'Save' to save all settings.

5.2. Network Configuration

5.2.1. IPv4 and IPv6

Use IPv4 or IPv6 network addresses to configure the camera's network connection.

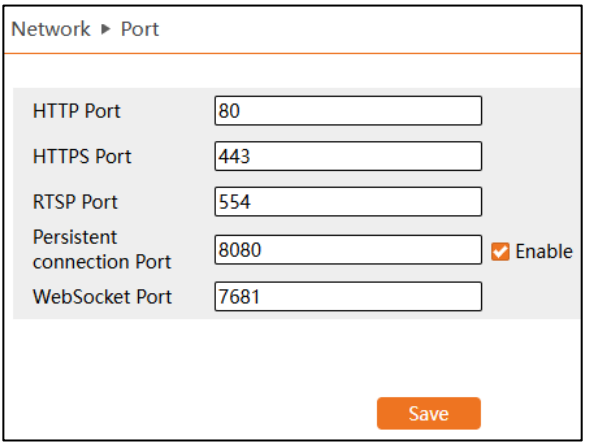




- **Obtain an IP address automatically:** DHCP will obtain an IP address from DHCP network devices.
- **Use the following IP address:** Manually assign an IP address, subnet mask, gateway and DNS server preferences for the camera.
    - Test: Click the Test button to check the local network for the availability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

5.2.2. Port

Configure the camera's HTTP, data, and RTSP port settings.

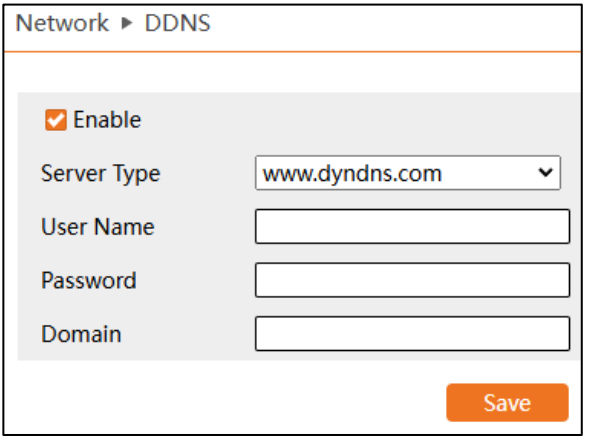


- **HTTP Port**: The default HTTP port is 80. It can be changed to any unoccupied port.
- **HTTPS Port**: The default HTTPS port is 443. It can be changed to any unoccupied port. (Some models may not support)
- **Data Port**: The default data port is 9008. Please change it as necessary.
- **RTSP Port**: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

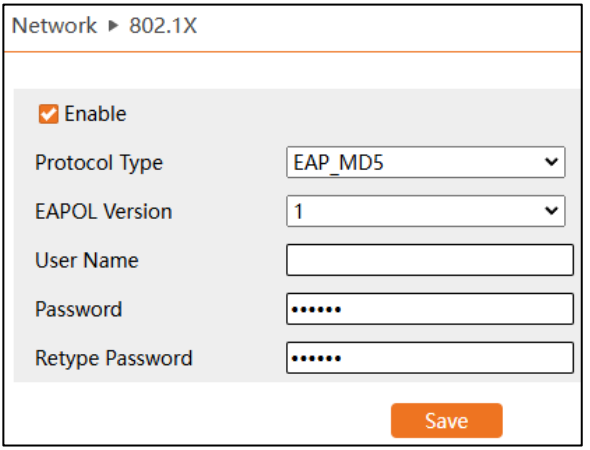


To set up a DDNS:

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.

5.2.4.802.1x

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.



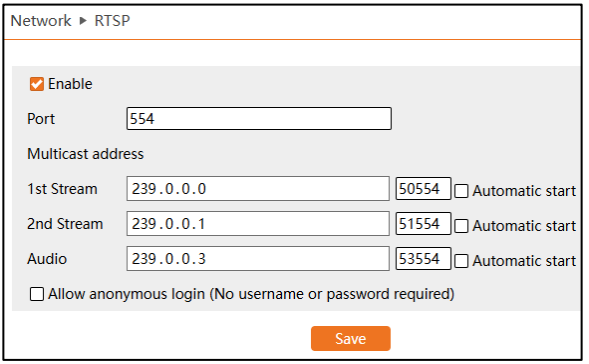
Connect the camera to a network switch that supports 802.1x protocol. The switch can be treated as an authentication system to find the device in a local network. If the camera connected to the switch's network interface has passed the switch's authentication, it can be accessed via the local network.

- **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.

5.2.5. RTSP

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

****NOTE:** A multicast device will be needed for one-to-many 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 multiple cameras are 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. The video cannot be played if it is set to TCP mode.

**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 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 the video.

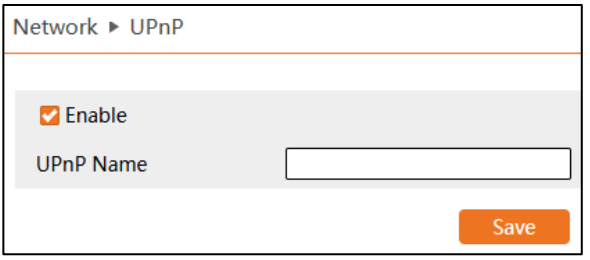
- **Multicast Address:**
  - 1st Stream: *rtsp://IP address: rtsp port/profile1?transportmode=mcast*
  - 2nd Stream*: rtsp://IP address: rtsp port/profile2?transportmode=mcast*
  - 3rd Stream: *rtsp://IP address: rtsp port/profile3?transportmode=mcast*
- **Audio:** The video and audio will play automatically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

5.2.6. UPnP

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

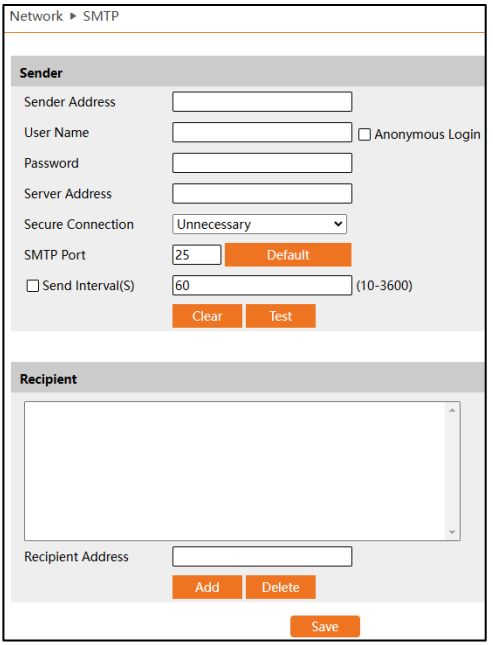
Go to Setup>Network>UPnP.

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



5.2.7. Email

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.



You can configure the following:

- **Sender Address:** Enter an email address that the camera can use to send notifications.
- **Username:** Enter the username or email address to log in to the email account.
- **Password:** Enter the password used to log in to the email 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 email service.
- **Send Interval(S)**: Set the time interval for an email's frequency. 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. Two separate email notifications will be sent if one motion alarm event is triggered and then

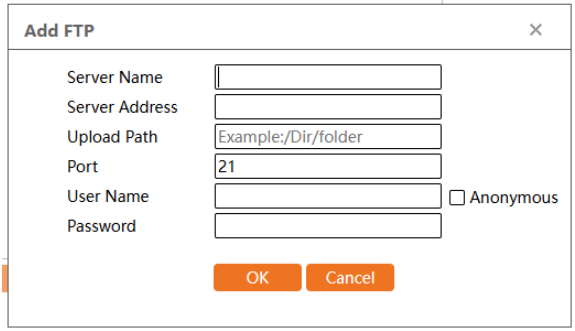
another motion detection alarm event is triggered after 60 seconds. If multiple separate alarms have been triggered simultaneously, numerous notifications will be sent separately.

  - After configuring the settings, click the "Test" button to send a test email.

- **Recipient Address**: Enter the destination email address that will receive the notifications.

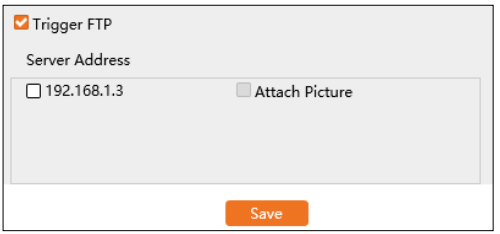
5.2.8. FTP

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



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 FTP server's IP address or domain name.
   - **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 to log in to the FTP server.
2. Click "OK" to close the configuration window, then click the "Save" button to apply the settings. You can enable "Trigger FTP" to assign the FTP connection when configuring event settings for intrusion, line crossing, etc.



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

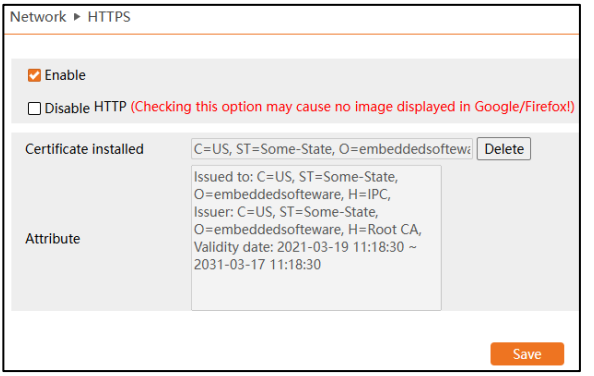
TXT file content will appear as follows:

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

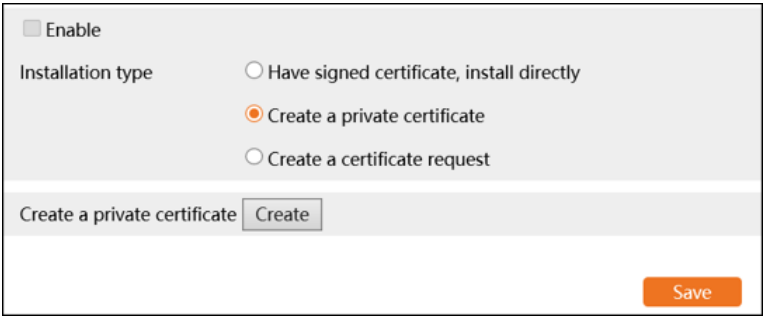
For example – *device name: IPC mac: 00-18-ae-a8-da-2a MOTION time: 2021-03-16 12:20:07*

5.2.9.HTTPS

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



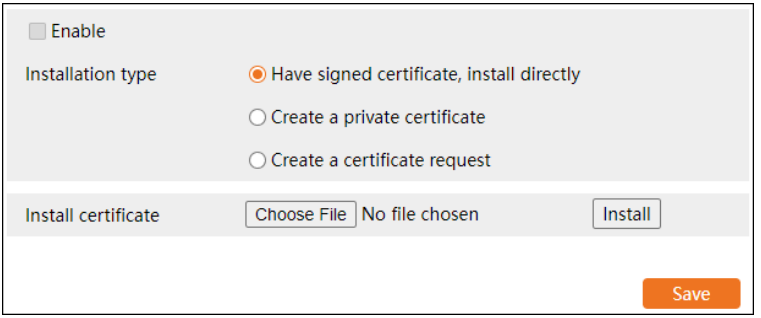
- **Enable:** Enable the HTTPS function to activate the encryption feature. Once activated, a web browser can access the camera web interface with "https://."
- **Certificate Installed:** A self-signed certificate is installed by default.
    - A private certificate can be created if users don't want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



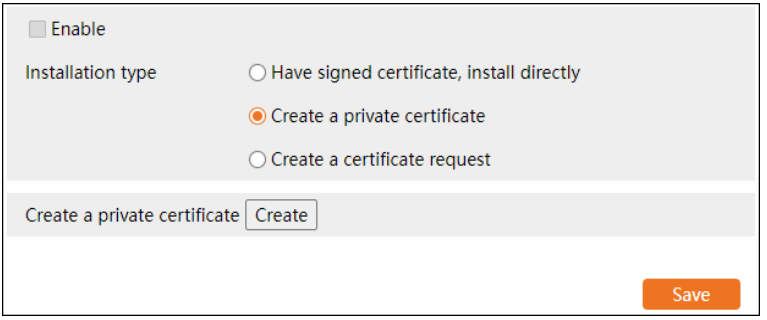
Creating a Private Certificate

To add a private certificate, you can either upload a certificate purchased from an SSL 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.



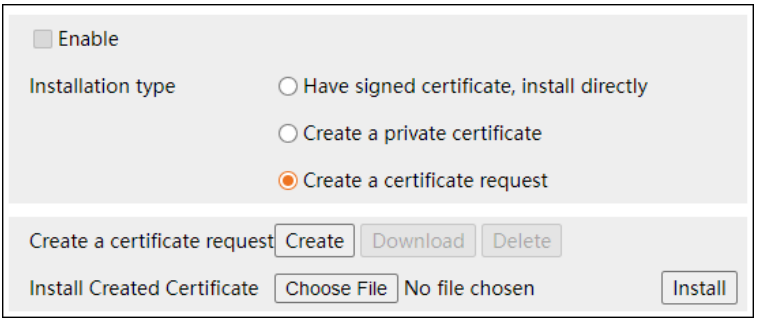
Configure the following to complete the form:

- Country: Enter the country (two-letter abbreviation).
- Domain: Enter the camera's IP address or URL domain.
- 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 location's state or province (two-letter abbreviation).
- Region: Enter the city or region of the location.
- Organization: Enter the name of the owner's organization.

- Unit: Enter the unit name or number of the organization.
- Email: Enter the administrator's email address.

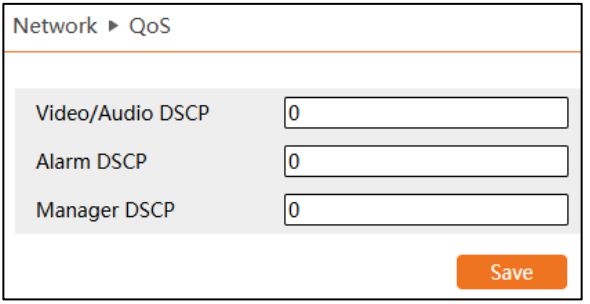
Click "OK" to save the settings.

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



5.2.10. 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 congestion by using this function.



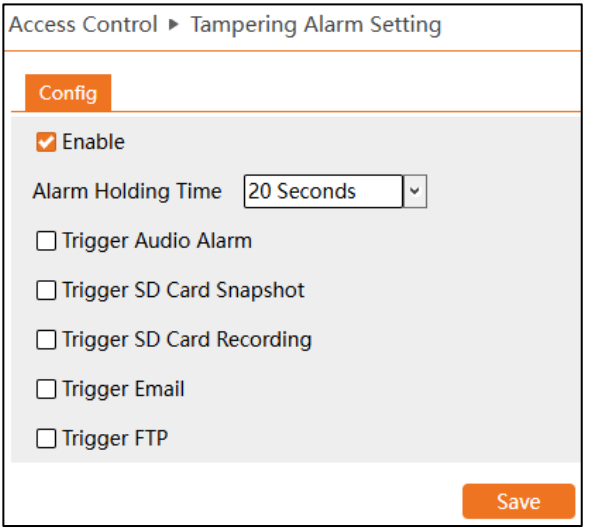
- **Video/Audio DSCP:** The range is from 0 to 63.
- **Alarm DSCP:** The range is from 0 to 63.
- **Manager DSCP:** The range is from 0 to 63.

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

5.3. Access Control

5.3.1. Tampering Alarm Settings

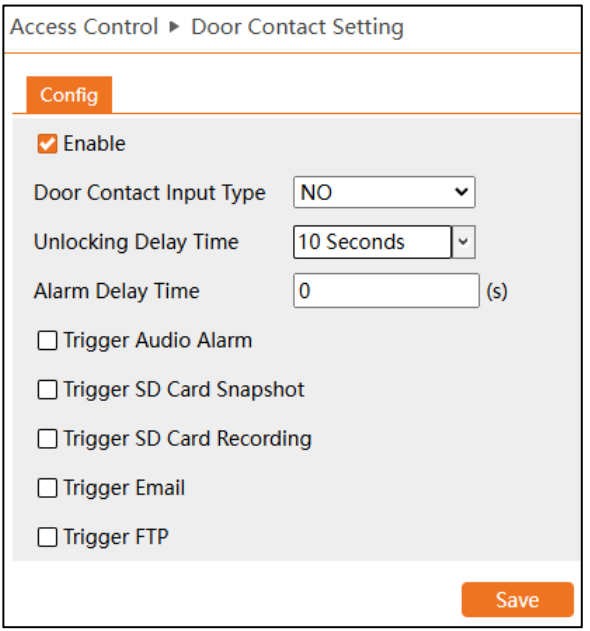
The camera's analytics engine can detect attempts to move or damage the camera. When a tampering effort is detected, the camera can execute a list of responses to alert users and trigger alarms.



- **Enable:** Enable to activate tampering 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 the camera to take a still image when the alarm is triggered (SD card required).
- **Trigger SD Card Recording:** Enable the camera to record video to the SD card when the alarm is triggered (SD Card required).
- **Trigger Email:** Enable the camera to use SMTP to send email notifications when the alarm is triggered.
- **Trigger FTP:** Enable the camera to send snapshots and recordings to an external FTP server when the alarm is triggered.

5.3.2. Door Contact Settings

Use the settings below to adjust the camera's lock and unlock settings.



- **Door Contact Input Type:** NO (normal open) or NC (normal close)
- **Unlocking Delay Time**: the allowable unlocking time. For example, if it is set to 10 seconds, alarms will be triggered when the door is not closed after 10 seconds.
- **Alarm Delay Time**: Set the alarm delay time when the door contact faults are detected. For example, if it is set to 3s when detecting the failure of the door contact, alarms will be triggered 3s later. (The value ranges from 0~999. If "0" is selected, alarms will be triggered immediately.)

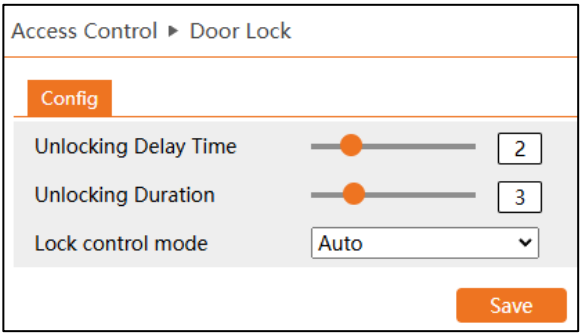
  Please select the alarm trigger options as needed.

  - **Trigger Audio Alarm:** If enabled, the camera will trigger the audio alarm as set in the camera's settings.
  - **Trigger SD Card Snapshot:** If enabled, the camera will save a snapshot to the SD card.
  - **Trigger SD Card Recording:** The camera will save a recording video to the SD card if enabled.
  - **Trigger Email:** If enabled, the camera will send an email notification as set in the camera's settings.

- **Trigger FTP:** The camera will save a recording video to an FPT server if enabled.

5.3.3. Door Lock Settings

Once the access control device is connected to the device, you can set unlocking mode in this interface.

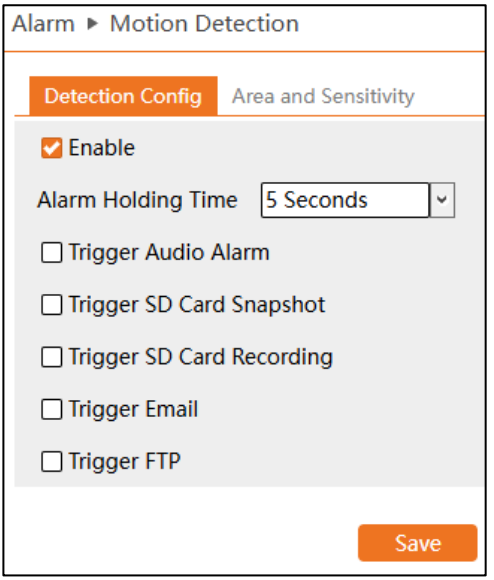


- **Unlocking Delay Time**: Set the door unlocking delay time. The time range is from 0 to 10 seconds. For example, the unlocking mode is "Swiping Card," the delay time is set to "2" seconds; the door will be opened 2 seconds later after successfully reading the card.
- **Unlocking Duration**: If the door has been unlocked for a period that exceeds the unlocking duration, the door will be automatically locked. The time range is from 0 to 10 seconds. For example, if the duration is set to "3" seconds, the unlocking door will automatically lock 3 seconds later.
- **Lock Type**: Choose "Auto," "NO," or "NC" as needed. If "Auto" is selected, the system will open the door according to the pre-defined unlocking condition. "NO" means "normally open"; "NC" means "normally closed".

5.4. Alarm Configuration

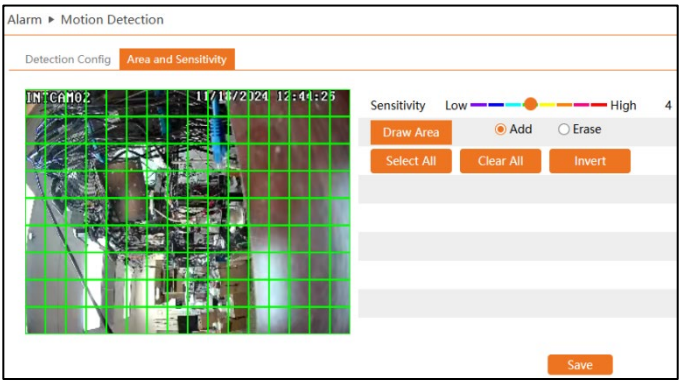
5.4.1. Motion Detection

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



- **Enable:** Enable to activate motion-based alarms. If unchecked, the camera will not send any signals to trigger motion-based recording to the NVR or CMS, even if motion occurs in the video.
- **Alarm Holding Time:** Refers to the interval between the adjacent motion detections. The alarm will remain active for the duration of the holding time. If motion is detected while the alarm is still ongoing, it will be considered continuous movement; otherwise, it will be viewed as a single motion.
- **Trigger SD Card Snapshot:** Enable the camera to take a still image when the alarm is triggered (SD card required).
- **Trigger SD Card Recording:** Enable the camera to record video to the SD card when the alarm is triggered (SD Card required).
- **Trigger Email:** Enable the camera to use SMTP to send email notifications when the alarm is triggered.
- **Trigger FTP:** Enable the camera to send snapshots and recordings to an external FTP server when the alarm is triggered.
- **Motion Area and Sensitivity**

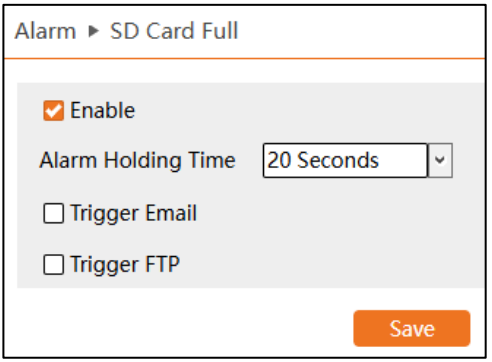
- Set the motion detection area and the detection sensitivity.
- Click the "Area and Sensitivity" tab to go to the interface as shown below.



- **Sensitivity:** Move the "Sensitivity" slider to set the detection sensitivity. A higher sensitivity value means the motion alarm will be more easily triggered.
- **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 select and clear motion detection areas from the grid. Click the "Save" to save the settings.

5.4.2. SD Card Full

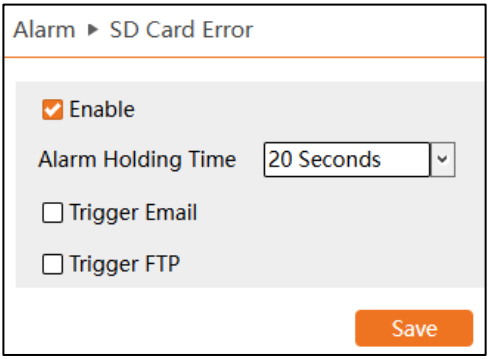
A notification alarm will be triggered when the SD Memory Card has reached full capacity. Click the "Save" button to save the settings.



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

5.4.3.SD Card Error

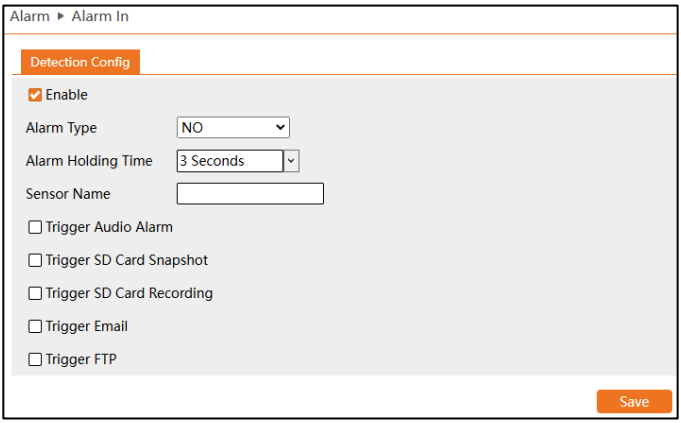
When there are errors in writing on the SD card, a notification alarm will be triggered.



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

5.4.4. Alarm In

To set sensor alarm (alarm in):



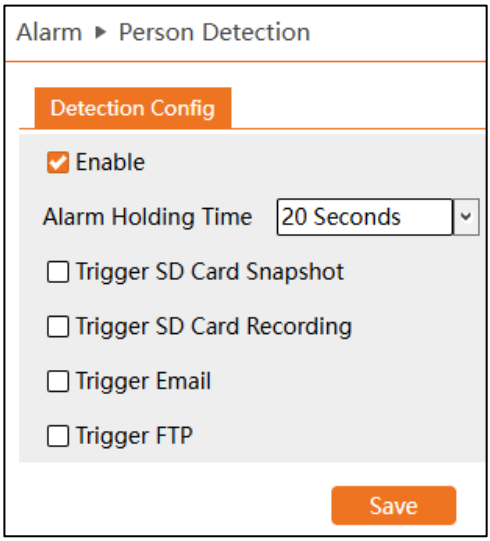
Click "Enable" and set the alarm type, alarm holding time and sensor name.

- **Alarm Holding Time**: Set how long the alarm will be on once motion is detected. If another motion is detected during this period, it will be considered continuous movement; otherwise, it will be viewed as a single motion.
- **Trigger Audio Alarm:** If enabled, the camera will trigger the audio alarm as set in the camera's settings.
- **Trigger SD Card Snapshot:** If enabled, the camera will save a snapshot to the SD card.
- **Trigger SD Card Recording:** The camera will save a recording video to the SD card if enabled.
- **Trigger Email:** If enabled, the camera will send an email notification as set in the camera's settings.
- **Trigger FTP:** The camera will save a recording video to an FPT server if enabled.

Click the "Save" button to save the settings.

5.4.5.Person Detection

Alarms will be triggered when the camera detects a person.



Enable person detection and then set the alarm holding time.

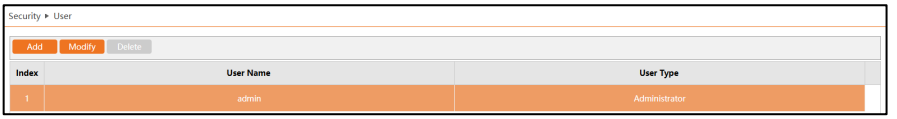
- **Alarm Holding Time**: Set how long the alarm will be on once motion is detected. If another motion is detected during this period, it will be considered continuous movement; otherwise, it will be viewed as a single motion.
- **Trigger Audio Alarm:** If enabled, the camera will trigger the audio alarm as set in the camera's settings.
- **Trigger SD Card Snapshot:** If enabled, the camera will save a snapshot to the SD card.
- **Trigger SD Card Recording:** The camera will save a recording video to the SD card if enabled.
- **Trigger Email:** If enabled, the camera will send an email notification as set in the camera's settings.
- **Trigger FTP:** The camera will save a recording video to an FPT server if enabled.

Click the "Save" button to save the settings.

5.5. Security Configuration

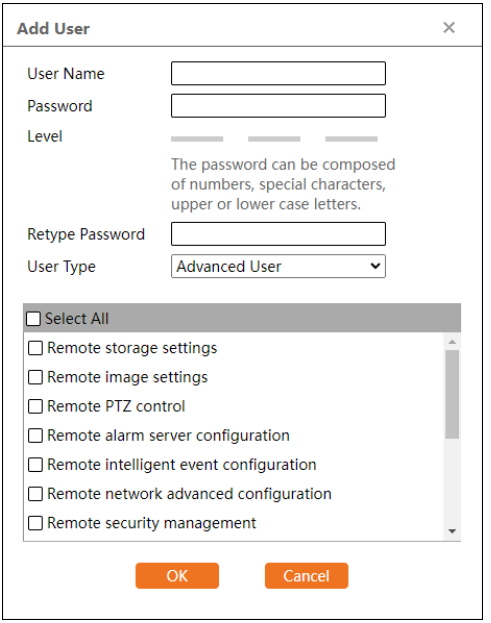
5.5.1. User Configuration

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



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. When creating the password, use a combination of numbers, special characters, capitalized letters, and lowercase letters.
- **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 latest user profile will be displayed in the user 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:** First, enter the user's current password to change the password. 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 identical to 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.

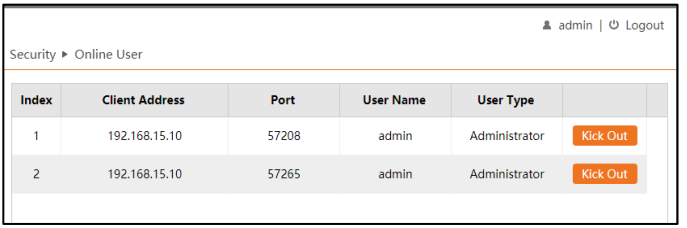
Click the "OK" button to save the settings.

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

View who is currently viewing live video from the camera by listing the IP address of the client, the network port being accessed, and the user login 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

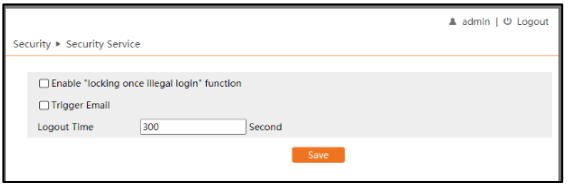
Manage a list of blocked and prioritized users by filtering IP addresses.

- **Enable Address Filtering:** Check the enable checkbox to activate IP filtering for the camera.
- **Allow/Block the Following Address:** The toggle will configure the list of blocked 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.



- **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:** Enable this toggle to send a notification email when this security feature is triggered.
- **Logout Time:** Configure the desired lease time for the camera to lock. The default settings will allow the camera to be logged in again after 30 minutes or after rebooting.

Click the "Save Button to apply the settings.

5.5.5. Password Security

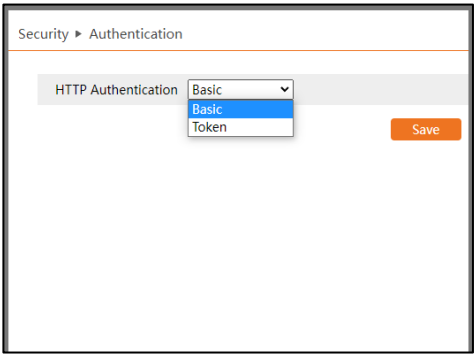
Set the camera's desired password strength level and password expiration time limit.

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

Click the "Save" button to apply the settings.

5.5.6. Authentication

Set the HTTP authentication protocol for the camera.

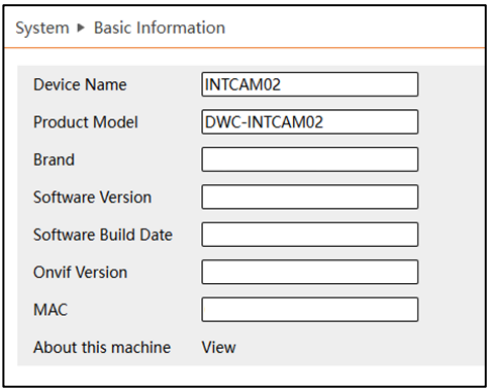


- **HTTP Authentication:** Select the preferred authentication protocol for connection with the camera.
    - Basic: A basic username and password login is needed to authenticate requests with the camera.
    - Token: An authentication scheme where the camera generates an encrypted string in response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

5.6. System Settings

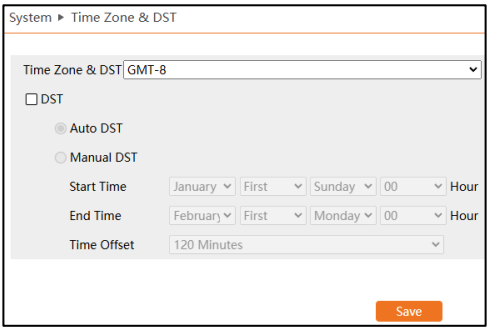
5.6.1. Basic Information

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



5.6.2. Time Zone and DST

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



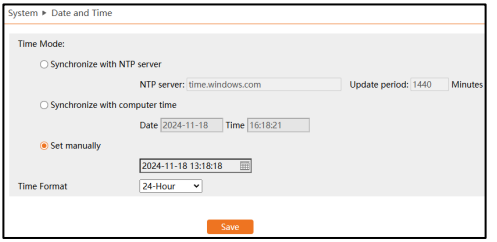
- **Time Zone & DST:** Select the camera's current time zone.
- **DST:** Enable this toggle to activate the camera's daylight savings time automatic function.
    - Auto DST: The camera will automatically change time settings on the second Sunday in March and the first Sunday in November to account for daylight savings time.
    - Manual DST: The camera will only change time settings at specified

times.

- Start Time: Specify when the camera's internal clock will move ahead.
- End Time: Specify when the camera's internal clock will move backward.
- Time Offset: Select the time (minutes) for which the camera will change its internal clock.

5.6.3. Date and Time

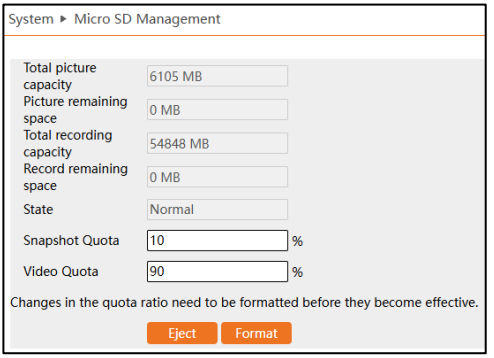
Adjust the camera's internal date and time settings.



- **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 is needed for this option.
- **Synchronize with Computer Time:** Select this setting to synchronize the camera with the current computer's date and time settings.
- **Set Manually:** Select this setting to set the camera's internal date and time settings manually.
- **Time Format:** Select the preferred time format
  - 24-Hour: 00:00 ~ 23:59
  - 12-Hour: 12:00am ~ 11:59pm

5.6.4. Storage

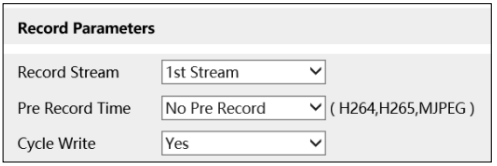
An SD Memory Card is not included with the camera. Consult your DW Sales Representative for SD Card needs.



- **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 for captured pictures on the SD card.
- **Video Quota**: Set the limit for recording files for the SD card.

5.6.5. Record

Adjust the recording parameters of the camera when using an SD card for storage.



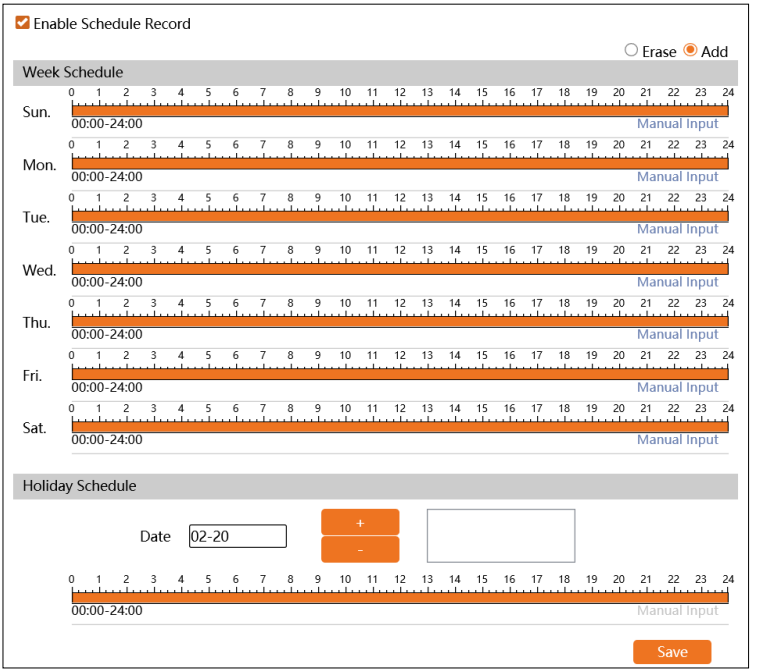
Record Parameters

- **Record Stream:** Select the 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 overwrite old data on the SD card when storage is full.

Timing

- **Enable Schedule Record:** Enable this setting so the camera follows a recording schedule when storing data on an SD card.

- **Week Schedule:** Set the schedule for the camera to record to the SD card throughout the week.
    - Add: Toggle will manually add a recording period from the schedule. Orange highlighted areas indicate that the camera is scheduled to record then.
    - Erase: Toggle to remove a recording period from the schedule manually.
    - Manual Input: Click on "Manual Input" to manually input the day's start and end recording times.



Holiday Schedule

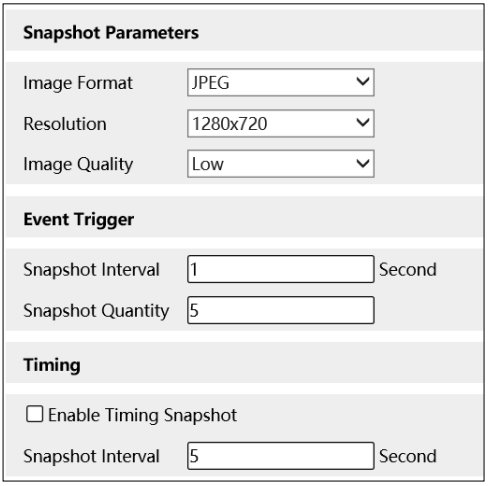
Set the recording schedule for a specific date.

****NOTE: Holiday schedule settings take priority over the weekly 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 saved to the SD card.



Snapshot Parameters

- **Image Format:** The image will be saved as JPEG.
- **Resolution:** The 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**: You set the maximum quantity of permitted snapshots while remaining within the *Snapshot Interval* limit.

Timing

- **Enable Timing Snapshot**: Enable timing snapshots so the camera can 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 take snapshots regularly. Setup is like setting the Recording

Schedule of the camera (See Section 5.10.5 Record).

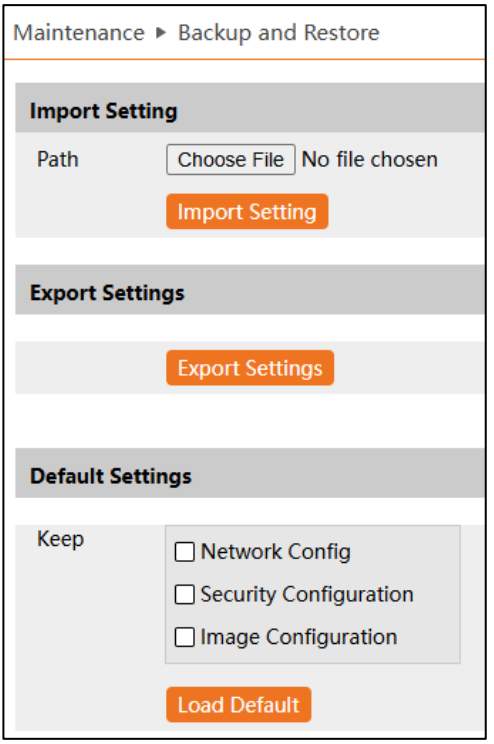
- Holiday Schedule: Set the schedule for the camera to take snapshots on a specific date regularly. Setup is like setting the Holiday Recording Schedule of the camera (See Section 5.10.5 Record).

5.7. Maintenance

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

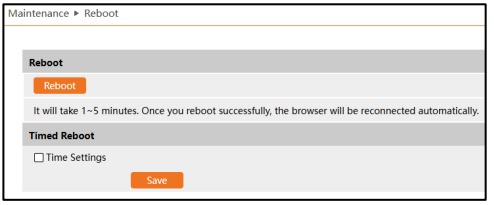
Click the "Export Settings" button to download a configuration file containing the camera settings to your computer.

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 it.



Reboot

Click the "Reboot" button to reboot the device. The reboot process varies from 1~5 minutes, depending on the camera's condition. Network connections will resume once the reboot has been completed.

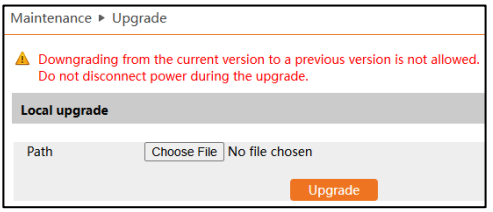
Timed Reboot Setting:

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.

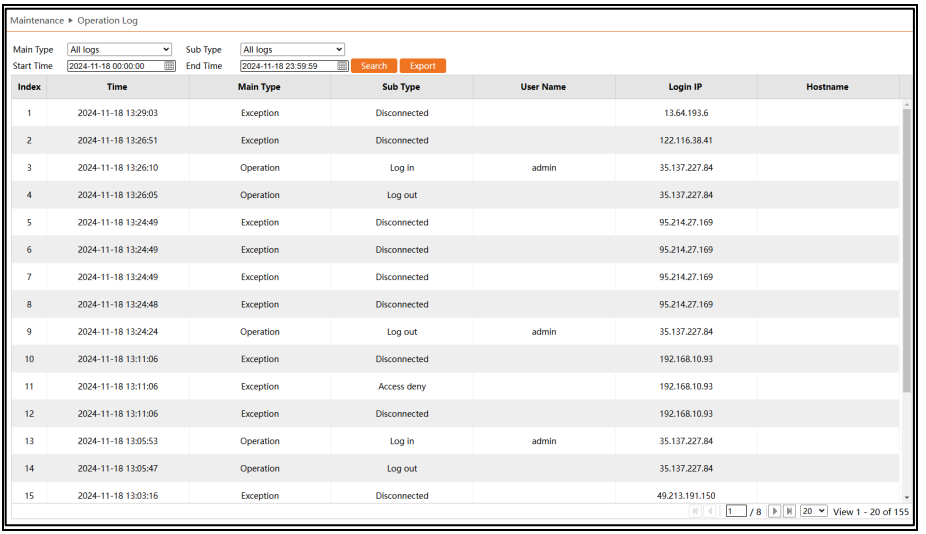


- **Path:** Click the "Choose File" button and select the upgrade file from the computer.
- **Upgrade:** After selecting the new firmware file in the *Path* setting, click this button to begin the upgrade. The camera will automatically reboot after the firmware update has been completed.

Caution! During the upgrade process, do not close the browser or disconnect the camera from the network.

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.

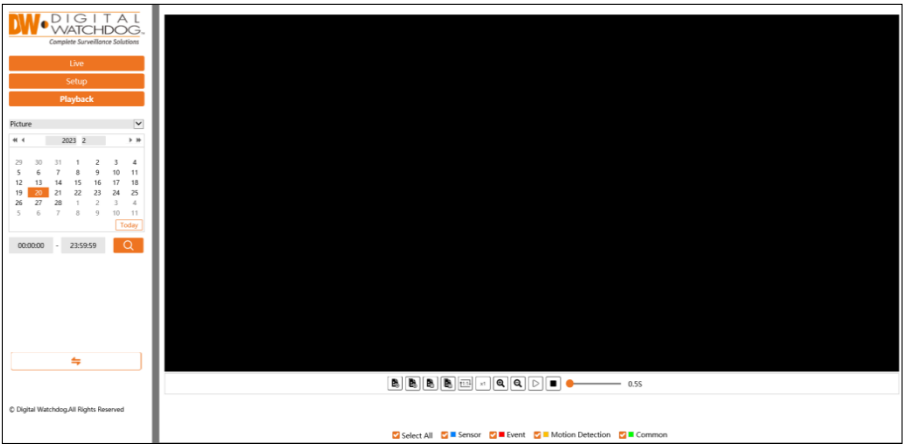


- **Main Type:** Select the category of log that you would like to view.
    - All Logs: View all major categories in a single list.
    - Alarm: View a list of event alarm occurrences logged by the camera.
    - Exception: View a list of IP addresses of clients denied access, client disconnections, 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:** When filtering through logs, click this button to initiate the search function.
    - **Export:** Click this button to export the log as a .txt file.

6.Playback

6.1. Image Playback

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



To playback saved snapshot images from the camera:

1. Click the "Playback" button, then use the drop-down and select "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 on 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.

Icon	Description	Icon	Description
	Save: Click this button to select the path to save the image on the PC.		Save all: Click this button to select the path to save all pictures on the PC.
	Fit size: Click to fit the image on the screen.		Actual size: Click this button to display the image in its actual size.
	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 Playback

Click the "Playback" button to go to the interface as shown below. Videos recorded on the SD card can be played in this interface—an SD card is required.

To playback saved video from the camera:

1. Click the "Playback" button, then use the drop-down and select "Record."
2. Set search time: Select the date and start and end times.
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
	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 as needed.
5. Select mix stream (video and audio stream) or video stream as needed.
6. Double-click on a file name on the list to start the playback.

.

7. Appendix

7.1. Troubleshooting

How do I find the password?

A: The admin password can be reset through the "Edit Safety Question" function.

Click "Forget Password" in the login window and enter the corresponding answer to the selected question in the popup window. After you correctly answer all questions, you can reset the admin password. If you forget the answer to the question, this way will be invalid; please contact your dealer for help.

B: The admin can reset the passwords of other users.

Fail to connect devices through 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: The web port number has been changed: contact the administrator for the correct port number.

D: Exclude the above reasons. Restore to the default setting by IP Finder.

IP Finder cannot search devices.

The anti-virus software in your computer may cause it. Please exit it and try to search the device again.

No sound can be heard.

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

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

7.2. Product Specifications

IMAGE	
Image sensor	2.1MP/1080p 1/2.8" CMOS
Total pixels	1920x1080
Minimum scene illumination	0 lux (white LED on)
Color temperature	Cold light, 5600K
White LED brightness (Lumen)	34.1lm
LENS	
Focal length	2.3mm, F2.2
Lens type	Fixed lens
Field of View (FoV)	Horizontal FoV: 139°, Vertical FoV: 74°, Diagonal FoV: 170°
IR distance	1ft - 10ft (0.3 - 3m) range
White light distance	1ft - 3ft (0.3 - 1m) range
I/O	
Audio in / out	1 speaker built-in and 1 microphone built-in
Audio compression	G.711A / U
Alarm in / out	1 alarm input
Door lock output	1 door lock output
Anti-tamper interface	1 CH
Reset button	1 CH
Doorbell button	Yes
LED indicator	Yes, green, white
OPERATIONAL	
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, 80dB
Privacy zone	Yes
Video Analytics	Person detection, video tampering detection (scene change, video blur, abnormal color detection)
Backlight Compensation (BLC)	Yes
Memory slot	Micro SD card up to 256GB (card not Included)
NETWORK	

LAN	802.3 compliance 10/100 LAN, RJ45
Video compression type	H.265+, H.265, H.264+, H.264, MJPEG
Resolution	1080P (1920×1080), 720P (1280×720), D1
Frame rate	Up to 30fps at all resolutions
Video bitrate	64 Kbps ~ 4 Mbps
Bitrate control	Multi-streaming CBR/VBR at H.264/ H.265 (controllable frame rate and bandwidth)
Streaming capability	Multi-stream at different rates and resolutions
IP	IPv4, IPv6
Protocol	UDP, DHCP, NTP, RTSP, DDNS, SMTP, FTP, UPnP, HTTPS, HTTP
Security	IP filtering, MAC filtering, authentication (ID/PW), SSL/TSL
ONVIF conformance	Yes
Web viewer	OS: Windows®, Mac® OS, Linux®
	Browser: Microsoft Edge, Google Chrome, Mozilla Firefox
Video management software	DW Spectrum® IPVMS
ENVIRONMENTAL	
Operating temperature	-4°F ~ 122°F (-20°C ~ 50°C)
Operating humidity	0–95% RH (non–condensing)
IP rating	IP65-rated
Other certifications	FCC, CE, ROHS, ONVIF, NDAA
ELECTRICAL	
Power requirement	DC 12V, PoE, adapter not included
Power consumption	<6W
MECHANICAL	
Material	Plastic door station housing
Dimensions	5.9” x 1.96” x 1.17” (150 × 50 × 29.8mm)
Weight	0.31 lb (0.145 kg)
Warranty	5 year warranty

* Specifications are subject to change without notice.

8. 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, from 9:00 AM to 8:00 PM EST, Monday through Friday.

A purchase receipt or other proof of the original purchase date 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 occur in shipment or failures that are caused by products not supplied by the Warrantor or failures that 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.

9.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 using 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; you may also have other rights 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.