User Guide

Wired Camera Web Interface

This guide uses the Omada 8MP Turret web page for demonstration.
Features and pictures may differ from your actual product.

© 2026 TP-Link 1900004175 REV1.0.0

Contents

About This Guide

This User Guide provides information for using and managing cameras via a web browser. It explains functions of cameras and shows you how to configure them.

Conventions

When using this guide, notice that:

- Features available in cameras may vary due to your region, device model, and firmware version. All images, steps, and descriptions in this guide are for demonstration purposes only and may not reflect your actual experience.
- The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.
- This guide uses the specific formats to highlight special messages. The following table lists the conventions that are used throughout this guide.

Underlined	Indicates hyperlinks. You can click to redirect to a website or a specific section.
Teal	Indicates contents to be emphasized and texts on the web page, including the menus, tabs, buttons and so on.
>	The menu structures to show the path to load the corresponding page.
Caution	Reminds you to be cautious, and ignoring this type of note might result in device damage or data loss.
Note	Indicates information that helps you make better use of your device.

More Information

- For technical support, the latest version of the User Guide and other information, please visit https://support.omadanetworks.com/.
- The Quick Installation Guide can be found where you find this guide or inside the package of the product.

Login

This chapter guides you on how to log in to the web UI of the camera:

- Connect the Camera to Network
- Log in to the Web Interface

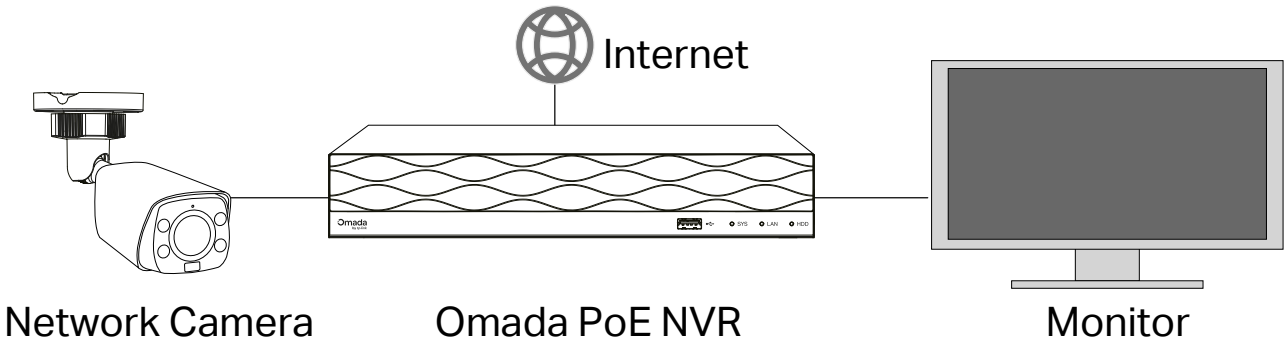
After the cameras are added to network, multiple methods are provided for you to monitor and manage cameras. You can manage and monitor the cameras remotely via the Omada Guard app, and you can also directly monitor and manage your camera via a web browser. Check the support page of the product for more manuals at https://support.omadanetworks.com/.

1. 1 Connect the Camera to Network

The camera works with an NVR for easier batch access and management. You can add cameras to network via an NVR.

1. Connect your cameras to the same network as your NVR (as shown below).
2. Power on your cameras.
3. Follow the NVR manual to add and activate your cameras.

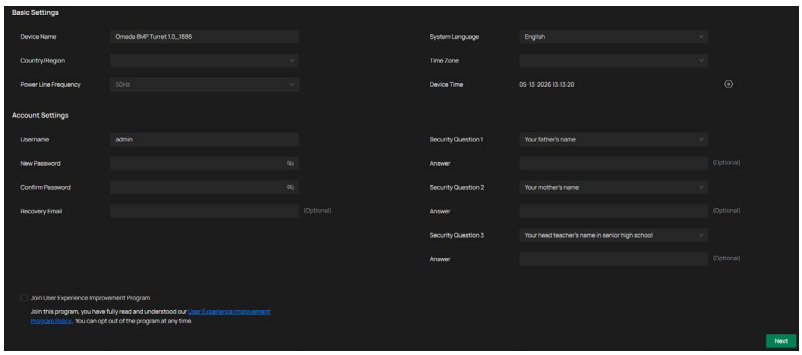
Note: You can follow the Quick Start Guide included in the package to mount and add cameras to your network.



1. 2 Log in to the Web Interface

With an intuitive user interface, it is easy to configure and manage the camera via a web browser. Follow the steps below to log in to the web UI of the camera for the first time.

1. Find the camera's IP address on your router's client page.
2. On your local computer, open a web browser and enter https://camera's IP address (https://192.168.0.60 by default).



3. Configure the Basic Settings.

Device Name	By default it is the model name. You can change device name as needed.
Country/Region	Select your region.
Power Line Frequency	Select 50Hz or 60Hz to reduce image flickering based on local electrical standards.
System Language	Set the interface language displayed in the web client.
Time Zone	Ensures recorded events and logs show accurate timestamps.
Device Time	Displays the current system time, used for all logs, video recordings, and event triggers. If needed, you can click the Settings icon to change the time settings, including 24/12 hour format, specifying a time, etc.

4. Configure the Account Settings.

Username	By default it is admin. You can change it as needed.
New Password	Create a secure and strong password by referring to the web instructions.
Confirm Password	Re-enter the password
Recovery Email	(Optional) Enter a Recovery Email to receive password-reset information if needed.
Security Question&Answer	(Optional) Set up Security Questions to receive password-reset information if needed.

5. Check the box to Join User Experience Improvement Program if needed, then click **Next**, and follow the web instructions to initialize the camera and you will proceed to the main interface.

Note:

1. For future logins, use the default username **admin** and the password you set for this camera.
2. If you forgot the password, click **Forgot password?** and follow the web instructions to reset the password.

2

Live View and Playback

With your camera's Live View and Playback features, you can access the camera's interface, view real-time footage, adjust display settings, and navigate essential controls. Additionally, you'll discover how to review recorded video and manage playback tools for efficient monitoring and security management. This chapter contains the following sections:

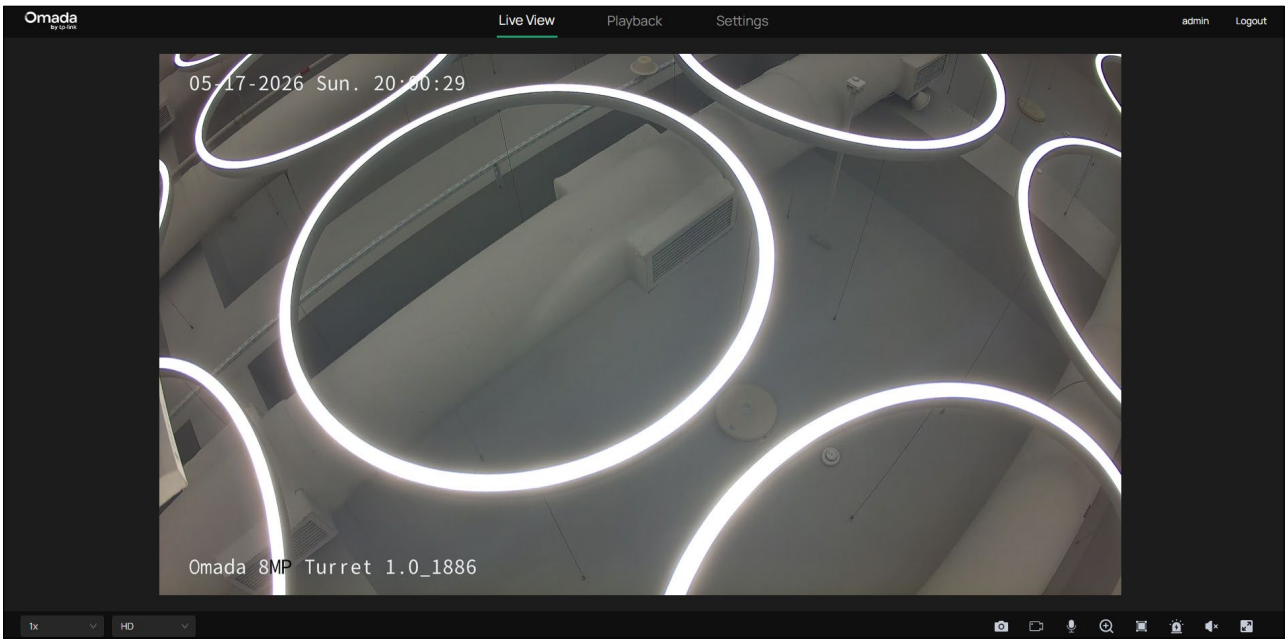
2. 1 Live View

The Live View page is the primary interface for real-time monitoring. It allows users to view live video streams, capture manual recordings or snapshots.

To access the camera's live stream from a local computer:

1. Identify the camera's IP address (The default is 192.168.0.60) via your gateway's client list.
2. Open a web browser and enter https://[camera's IP address] (e.g., https://192.168.0.60).
3. Log in using your custom username and password.
4. The interface will default to the Live View tab upon successful login.

Note: This is for demonstration only.



1x	Select the aspect ratio. 1x refers to the original window size. 4:3 refers to 4:3 window size. 16:9 refers to 16:9 window size. 100% refers to self-adaptive window size.
HD	Click to change the resolution type. **HD** stands for high definition. **SD** stands for standard definition. HD offers a higher pixel count and therefore a sharper, more detailed image than SD.

	**Screenshot**: Click to capture a screenshot.
	**Record**: Click to start or stop recording the live stream directly to your local computer.
	**Talk**: (Supported models only) Click and hold to speak through the camera's built-in speaker.
	**Electronic Zoom**: Click to see more details of any area in the image.
	**Smart Frame**: After enabling the Smart Frame feature under Settings > Camera > Stream > Advanced Settings, use this switch to choose whether to display detection frames on the current web preview screen.
	**Alarm**: (Only for certain cameras) Click to trigger the sound alarm and lasts about 10 seconds.
	**Volume**: (Only for certain cameras) Click to adjust the volume of the speaker.
	**Full Screen:** Click to change the live view image to the entire screen.

2. 2 Playback

The Playback module allows you to search, and review previously recorded footage stored on your camera's microSD card/Net HDD. You can examine historical events with granular control over playback speed and timing. To configure which specific events trigger a recording, please refer to the **Detecting Events and Alarms chapter**.

Use Video Playback tab to review continuous or event-based video streams using a chronological timeline. To review recorded footage, follow these steps:

1. Navigate to the Playback tab from the top navigation bar.
2. Select the desired Type and define your Time range using the calendar tool.
3. Click Search to populate the timeline or results list.
4. Use the Timeline at the bottom to scrub through video. Click  to start the stream.

5. The interface will default to the Live View tab upon successful login.

	Hit to pause or resume the playback.
1x	**Speed Playback**: Increase the speed for fast-forward or decrease for slow-motion review.
24H	**Time Span**: Click to change the period of time between 10 minutes to 24 hours.
	Screenshot: Take manual snapshots for the image.
	Record: Click once to begin recording, and click again to end it; the recordings will be automatically saved to your designated path.
	Digital Zoom: Zoom in to get a closer look at the image for finer details; zoom out for a wider panoramic image.
	Volume: Click to adjust the volume of the speaker.
	Full Screen: Click to change the playback image to the entire screen.

3

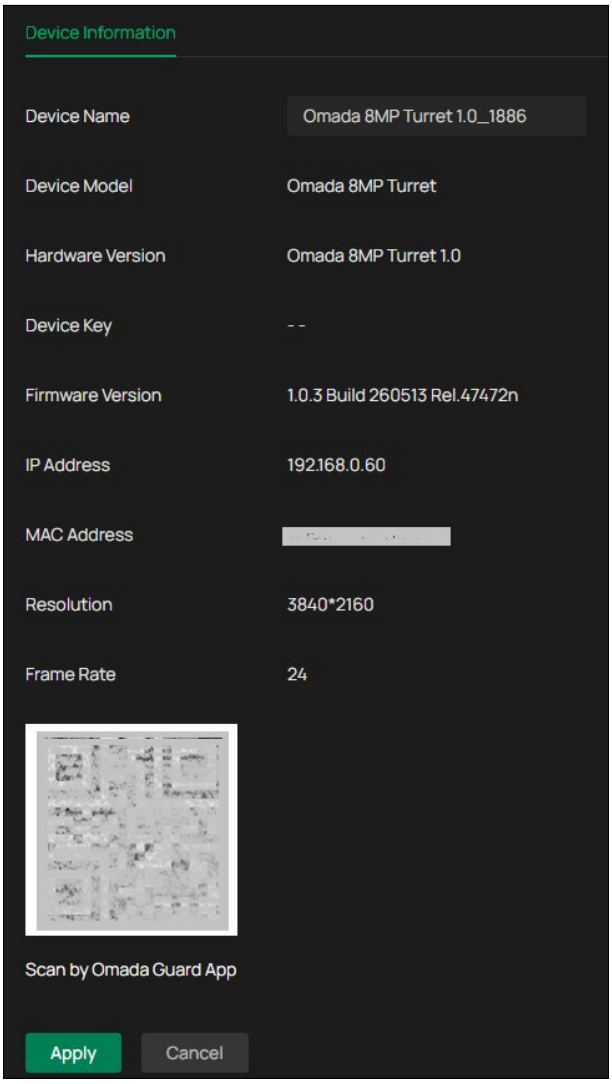
View Device Information

This chapter introduces how to check the system logs and view your device information on the web UI. This chapter contains the following sections:

3. 1 View Device Information

You can view basic information about the camera, including device model, firmware version, network information, stream information, and device QR code.

Go to **Settings** > **Information** > **Device Information** > **Device Information**.

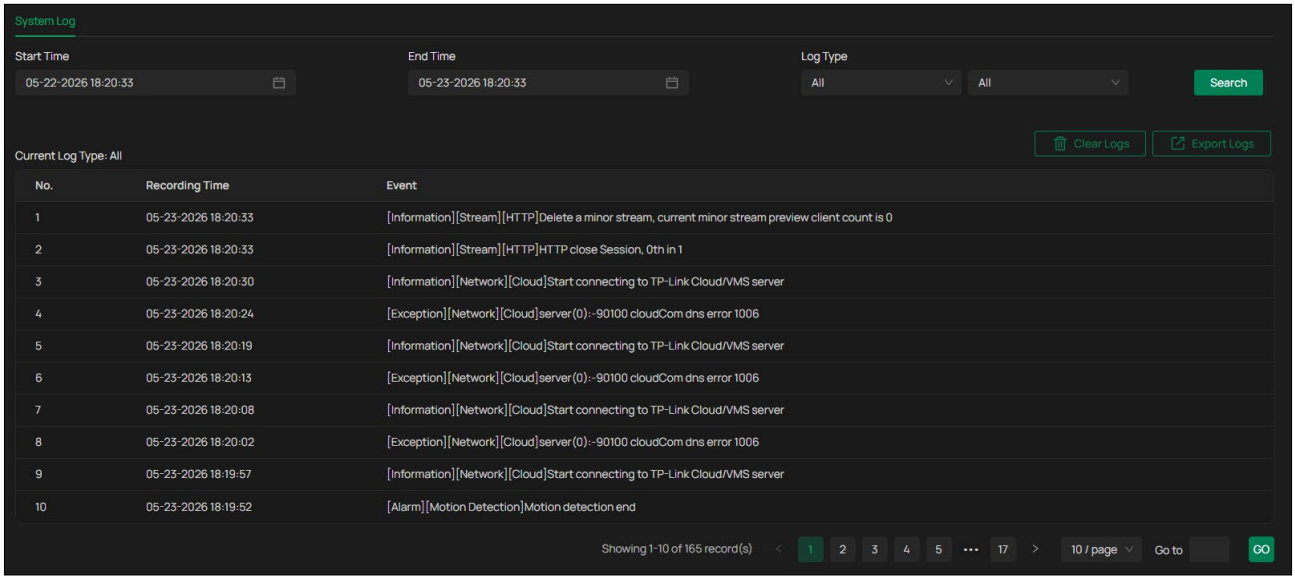


3. 2 View System Logs

The camera uses logs to record, classify, and manage system and device messages. You can search, view, and export the logs.

1. Go to **Settings** > **Information** > **System Log** > **System Log**.

2. Specify search conditions, including the Start Time, End Time, and Log Type, and click **Search**. The filtered logs that match the search conditions will appear in the table.



Start/End Time	Specify a time range to filter the logs based on the recording time.
Log Type	Select a type from the drop-down list to filter the logs. **All**: All types of logs. **Alarm**: Alarms triggered by events, such as tampering, line crossing, and area intrusion. **Exception**: Abnormal events that may influence the camera's functions, such as video signal loss and hard drive errors. **Operation**: Actions that take place on the camera, such as login and upgrade. **Information**: Informational messages, such as device information.
Clear Logs	Click to delete all logs.
Export Logs	Click to save log files to your computer.

4

Change Camera Settings

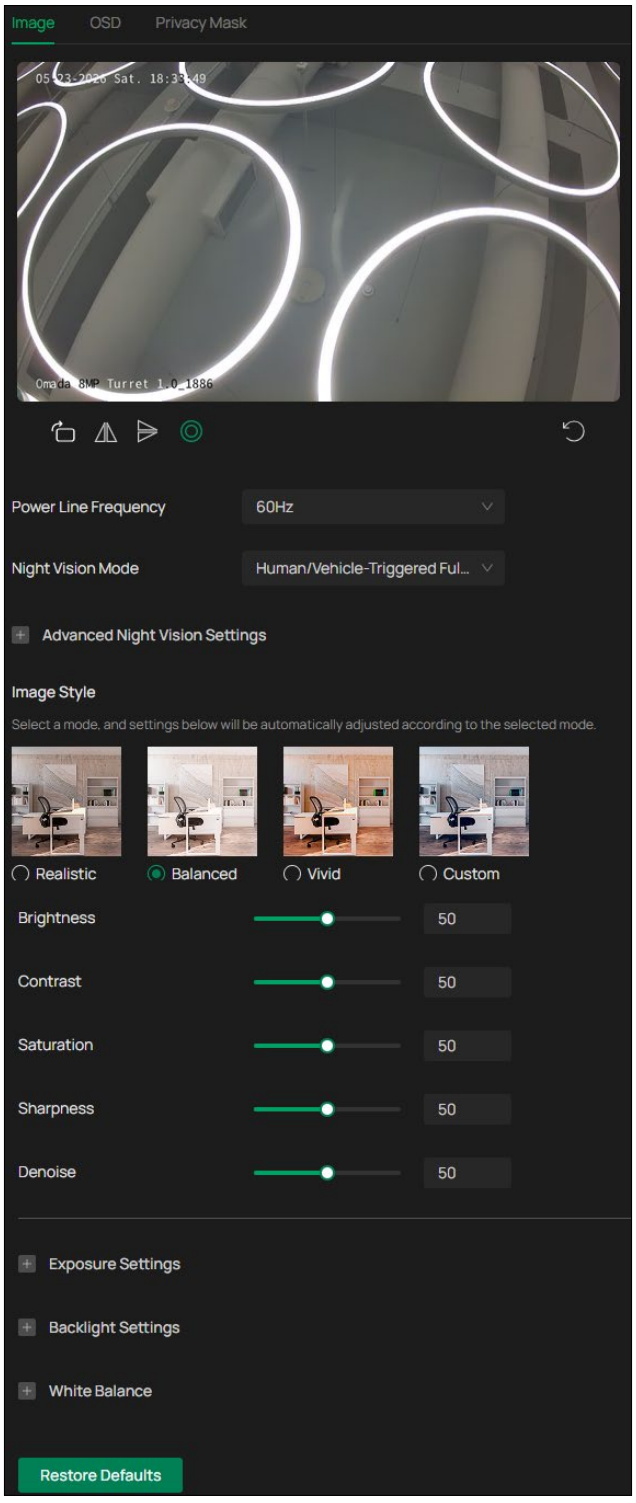
This chapter introduces how to change the camera display settings and camera streams settings. It contains the following sections:

4. 1 Camera Display Settings

You can adjust image features according to your needs.

4. 1. 1 Image Settings

1. Go to **Settings** > **Camera** > **Display** > **Image**.
2. Configure the following parameters.



Rotation/ Mirror	Choose to turn the live view image by 90 degrees or mirror the image on your display.  **Rotation 90°**: Tap to turn the live view image by 90 degrees.  **Left-Right**: Tap to mirror the image on the vertical axis.  **Up-Down**: Tap to flip the image on the horizontal axis.  **Center**: Tap to rotate the image by 180 degrees around its center.
General Settings	
Power Line Frequency	Set the Power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights.
Night Vision Mode	**Human/Vehicle Triggered Full-Color**: The camera switches to the full-color mode once it detects a person or vehicle. **Auto Color**: The camera turns on or off the white supplement light according to the light condition of the environment. **Auto IR**: The camera turns on or off the IR supplement light according to the light condition of the environment. **White LED Always On**: White supplement light is on. **IR Always On**: IR supplement light is on. **Off**: Supplement light is off.
Advanced Night Vision Settings	
Day/Night Switch Sensitivity	Decide the ambient light intensity that can trigger the switch of the light. The lower the value is, the easier it is to trigger the supplement light.
Delayed Switch	Decide how long the camera waits to turn on or off the light when the ambient light reaches the threshold to trigger the switch.
White Light Intensity	**Auto**: The cameras automatically adjusts the white supplement intensity based on environmental light levels. **Manual**: Drag the slide bar to manually adjust the intensity of the white light. The light gets brighter when the value increases.
Infrared Light Intensity	**Auto**: The cameras automatically adjusts the IR supplement intensity based on environmental light levels **Manual**: Drag the slide bar to manually adjust the intensity of the infrared light. The light gets brighter when the value increases.

Always Full-Color at Live View	When enabled, the camera will automatically turn on Full-Color Night Vision when you stream Live Video.
Image Style	
Image Style	Select a mode, Realistic, Balanced, Vivid or Custom, and the image settings will be automatically adjusted according to the selected mode.
Brightness	Increasing the value will lighten the image.
Contrast	Increasing the value will increase the difference between the brighter and darker parts.
Saturation	Increasing the value will enrich the color of the image.
Sharpness	Increasing the value will sharpen the image.
Denoise	Increasing the value will make the image clearer and the less noise it will have. However, for fast-moving objects, an excessively high value may result in slight motion blur.
Exposure Settings	
Exposure	Select the exposure mode as needed. **Auto**: The camera adjusts the exposure automatically. **Manual**: The image exposure is fixed. If you select **Manual**, adjust the slide bar of Gain to specify its value, and select a shutter speed. Higher gain and slower shutter speed result in brighter images. **Low Motion Blur**: Prioritizes a fast shutter speed to reduce "ghosting" or trailing behind moving targets. While this may result in a slightly darker image in low light, it ensures that moving objects (like license plates or faces) remain sharp and identifiable.
Anti-flicker	This function minimizes influences caused by flickering.
Backlight Settings	
BLC Area	BLC (Backlight Compensation) optimizes the camera to increase light exposure for darkened areas and helps you to see details more clearly. Select an area to compensate light. If you select **Custom**, draw a blue rectangle on the live view image as the BLC area.

WDR	WDR (Wide Dynamic Range) can improve the image quality under high-contrast lighting conditions where both dimly and brightly lit areas are present in the field of view. If you select **On**, the camera balances the light of the brightest and darkest areas automatically. You may set the gain value, or the sensor's sensitivity, manually.
White Balance	
White Balance	White balance is a process of removing unrealistic color casts, so that objects which appear white in person are rendered white in the image. **Auto**: The camera adjusts the color temperature automatically. **Locked**: The camera keeps the current color settings all the time. **Daylight/Natural Light/Incandescent/Warm Light**: The camera adjusts the color temperature to remove the color casts caused by the corresponding light. **Custom**: Drag the slide bar to configure the color temperature, and the camera keeps the settings all the time. You can configure the corresponding color temperature in the current environment to eliminate the effects of unrealistic color bias.
Restore Defaults	Click to restore to factory default settings.

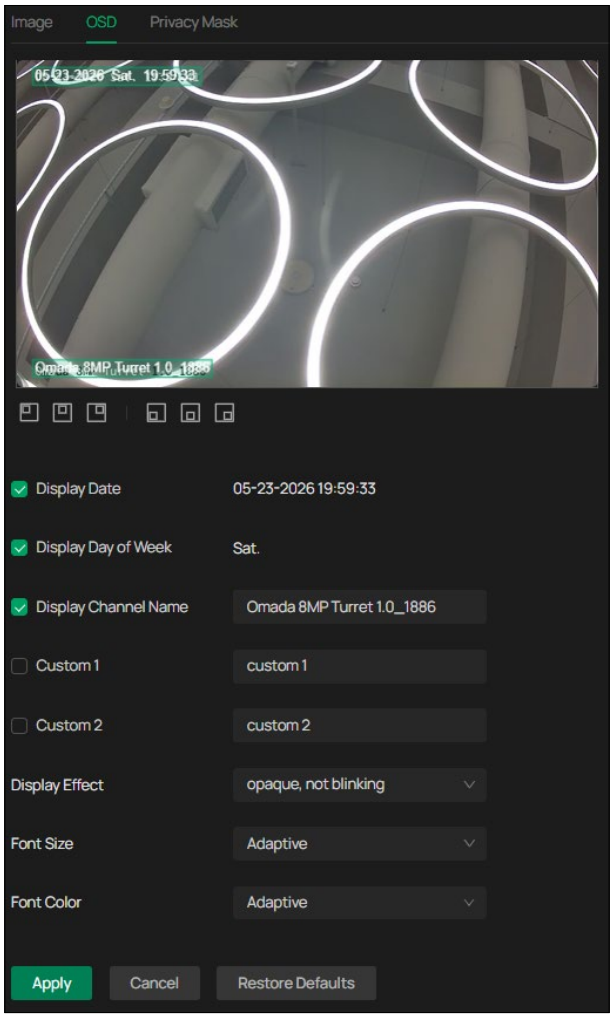
4. 1. 2 OSD Settings

You can configure OSD (On Screen Display) to edit the information displayed in Live View and recordings.

Follow the steps below to configure OSD settings.

1. Go to **Settings** > **Camera** > **Display** > **OSD**.
2. Configure the following parameters, and click **Apply**.

Note: Tap the Position icon at the bottom of the live view to adjust where items appear on the screen.



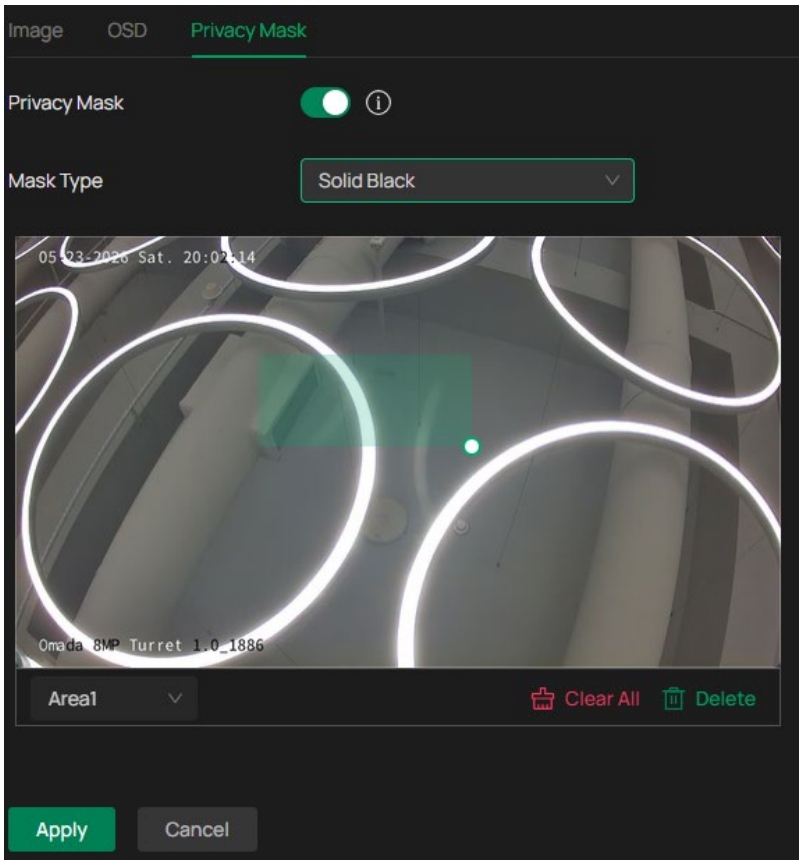
	Select the text in the image, then click the icon, and the text will display in the corresponding position.
Display Date	Check to display the date on the image.
Display Day of Week	Check to display the week on the image.
Display Channel Name	Check to display the channel name on the image. You can also check **Custom** and specify a text to display.
Display Effect	Set the blinking display effect of the OSD.
Font Size	Set the font size or select **Adaptive** to adjust the size based on the image.
Font Color	Set the font color or select **Adaptive** to adjust the color based on the image..
Restore Defaults	Click to restore to factory default settings.

4. 1. 3 Privacy Mask

Privacy Mask conceals parts of the image from view and protects your privacy. The area you set cannot be recorded and monitored.

Follow the steps below to configure Privacy Mask.

1. Go to Settings > Camera > Display > Privacy Mask.
2. Enable Privacy Mask. Draw the privacy area on the preview screen (the blue square in the picture below). Drag the area to adjust its size and location. For Mask Type, you may choose Solid Black or Mosaic, which determines the display effect of the area.



3. To remove a certain privacy area, select it and click Delete.
4. To remove all privacy areas, click Clear.
5. Click Apply.

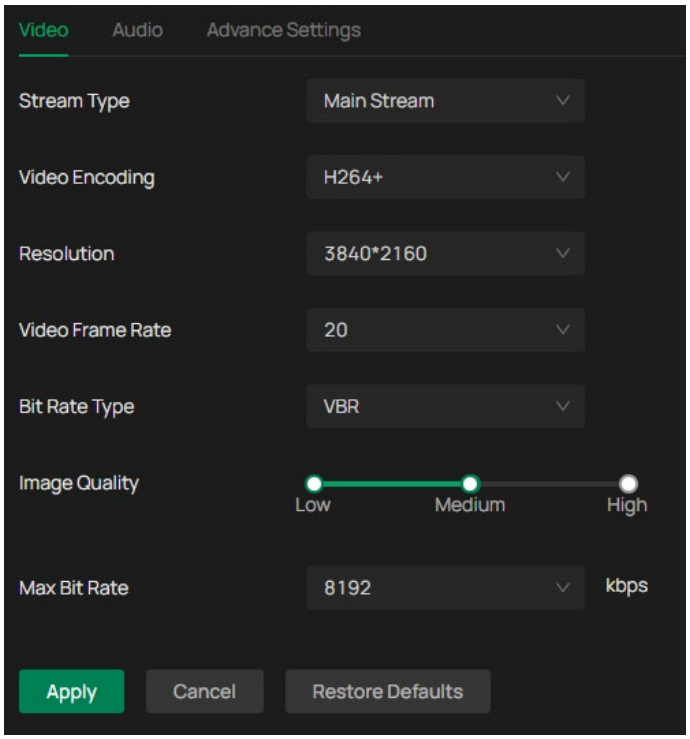
4. 2 Camera Stream Settings

In Stream Settings, you can configure video stream levels, and change the audio output settings. Video stream levels decide the video quality in Live View and recording.

4. 2. 1 Video Settings

Follow the steps below to configure video settings.

1. Go to **Settings** > **Camera** > **Stream** > **Video**.
2. Configure the following parameters, and click **Apply**.



Stream Type

Main Stream is the primary video feed used for recording and provides the highest video quality. It has higher definition and higher bandwidth than sub stream.

Sub Stream is a secondary video feed that is used mainly for remote viewing from computers from outside the network.

Video Encoding

Video encoding format determines how video data is compressed for transmission and storage.

H.264: Delivers good image quality at moderate file sizes, compatible with nearly all video management systems and devices.

H.264+: Further reduces bandwidth and storage requirements, especially in static scenes, without significantly lowering image quality.

H.265: Provides similar video quality as H.264 but at roughly 50% lower bit rates, making it ideal for saving bandwidth and storage, especially for high-resolution video like 4K.

H.265+: Achieves even greater bandwidth and storage savings by intelligently compressing static areas of the video while preserving detail in moving objects.

Note:

H.265 and H.265+ require more processing power for decoding. Ensure your hardware or software systems support the chosen codec.

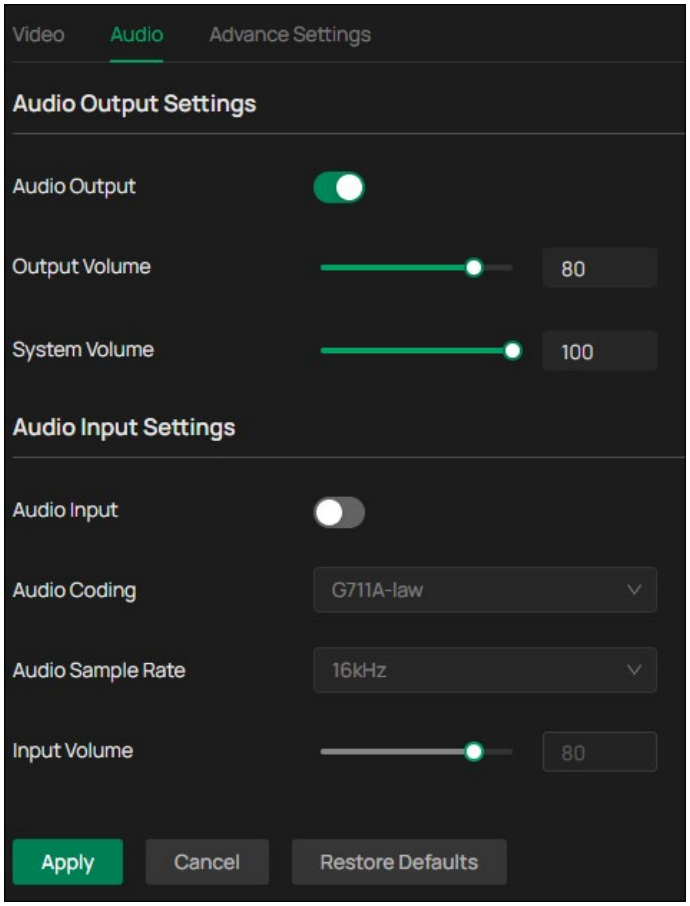
Resolution	The screen displays images more clearly when the resolution increases.
Video Frame Rate	The video is more fluent when the rate increases.
Bite Rate Type	The Max Bit Rate setting controls how much data the camera uses to encode video, which directly affects image quality and network bandwidth usage. You can choose between two modes: CBR (Constant Bit Rate): The camera maintains a fixed bit rate regardless of the scene's complexity. VBR (Variable Bit Rate): The bit rate adjusts dynamically based on scene complexity.
Image Quality	When VBR is selected as the Bit Rate Type, set the video quality as high, medium, or low. The higher the quality level, the more bandwidth the camera may use during complex scenes.
Max Bit Rate	Specify the upper limit of data the camera can use per second when encoding video. Higher bit rates allow for clearer, more detailed images and consume more network bandwidth.
Restore Defaults	Click to restore to factory default settings.

4. 2. 2 Audio Settings (Only for some models)

Follow the steps below to configure video settings.

1. Go to **Settings** > **Camera** > **Stream** > **Audio**.

2. Configure the following parameters, and click Apply.



Audio Output	Toggle on to allow the camera to deliver sound.
Output Volume	Adjust the volume of the speaker.
System Volume	Adjust the volume of the sound alarm.
Audio Input	Toggle on to turn one the camera's microphone.
Audio Coding	Select the encoding type of the audio.
Audio Sample Rate	Sampling number per second. The higher the sample rate (e.g., 16kHz is higher than 8kHz), the more samples will be in a second, the richer the sound details captured, and the clearer the sound quality.
Input Volume	Adjust the volume of the microphone.
Restore Defaults	Click to restore to factory default settings.

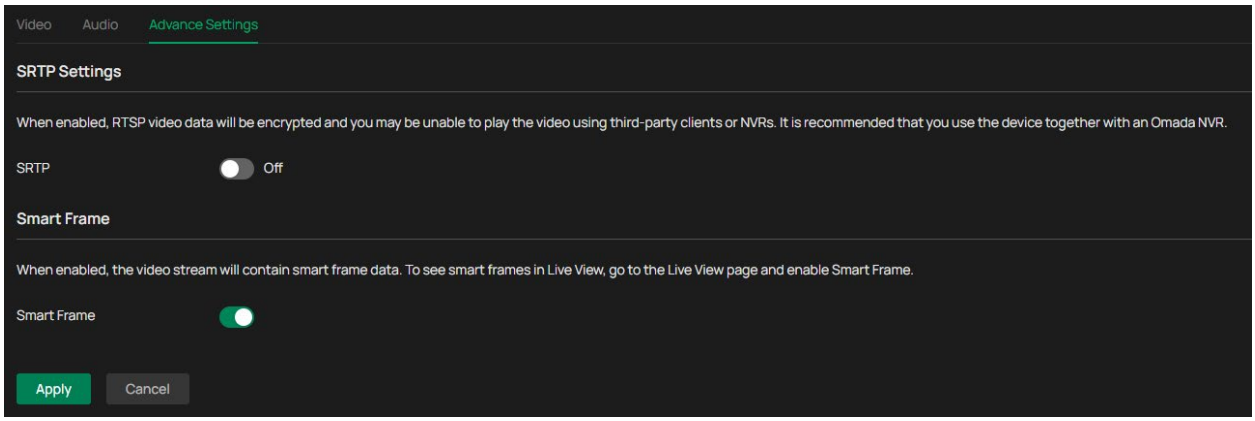
4. 2. 3 Advanced Settings

In Advanced Settings, you can configure SRTP and Smart Frame.

SRTP (Secure Real-time Transport Protocol) is a Real-time Transport Protocol (RTP) internet protocol, intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in both unicast and multicast applications.

When Smart Frame is enabled, the video stream will contain smart frame data. To see smart frames in Live View, go to the Live View page and enable Smart Frame.

1. Go to **Settings** > **Camera** > **Stream** > **Advanced Settings**.



2. Enable SRTP if needed. When enabled, RTSP video data will be encrypted and you may be unable to play the video using third-party clients or NVRs. It is recommended that you use the device together with an NVR.
3. Enable Smart Frame if needed. When Smart Frame is enabled, the video stream will contain smart frame data. To see smart frames in Live View, go to the Live View page and enable Smart Frame.
4. Click **Apply**.

5

Events

This chapter guides you on how to configure the event settings and alarm actions when your cameras detect different types of events. The camera monitors your pre-defined areas and you'll be automatically alerted to any suspicious activity in your home and office. This chapter includes the following sections:

5. 1 Arming Schedule and Linkage Method

Arming schedule determines when a camera's motion detection, recording, or other event-based features are active. It allows you to automate when the camera is actively monitoring and recording, based on a predefined schedule. Linkage methods are the responses to the detected incidents or targets during the scheduled time. This configuration is optional.

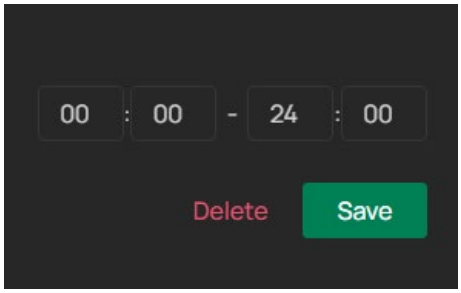
1. Go to **Settings** > **Event**, and locate Arming Schedule and Linkage Method in the related event interface.

2. Drag the time bar to draw desired valid time.

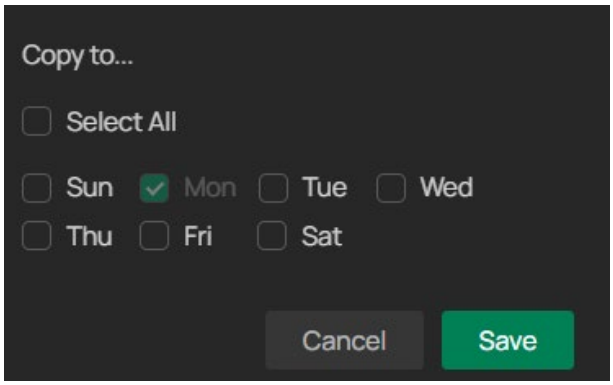
   Note:

- Each cell represents one hour.
- The default setting is 24/7.
- Up to six time periods can be configured for a day.

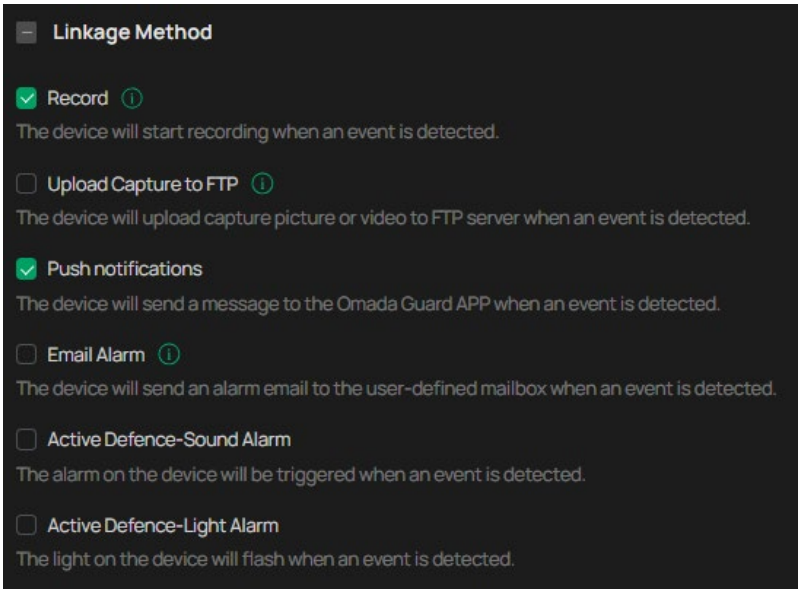
3. Click a time block and an edit button will appear. Enter the pop-up window to fine-tune the Start Time and End Time (with an accuracy of a minute) and check **Save**.



4. Click  to copy a schedule for a day to any other days. In the pop-up window, select the days of the week where you need to copy the time.



5. Set linkage methods as needed. You can click the corresponding information behind each method to enter the configuration page to change the settings.

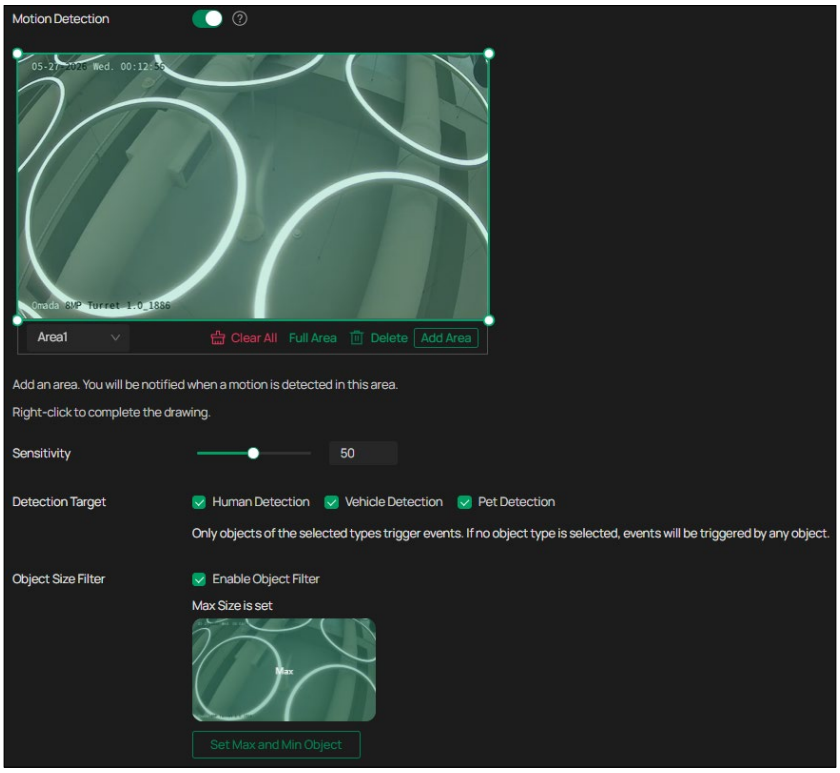


6. Click Apply.

5. 2 Motion Detection

Motion detection allows cameras to detect the moving objects in the monitored area and triggers alarm actions. You can customize the motion detection settings, set the alarm schedule, and select the linkage methods. Follow the steps below to finish the configuration.

1. Go to **Settings** > **Event** > **Motion Detection.** Toggle on to enable **Motion Detection**.



2. Draw areas for motion detection on the preview screen. The whole screen is selected by default. You may drag the corners to change the shape of the area and drag the whole area to move it. You may delete a selected area, clear all areas, expand the selected areas to the full screen, or add another area. Then configure the motion detection settings. You can manually draw an area by clicking the mouse on the image. Right-click to end drawing, click the midpoint of a line segment to add an endpoint, double-click an endpoint to delete it, and you can draw up to 16 polygons.

   Note: You may customize up to four areas.

3. In Area Settings section, you may modify the following parameters:

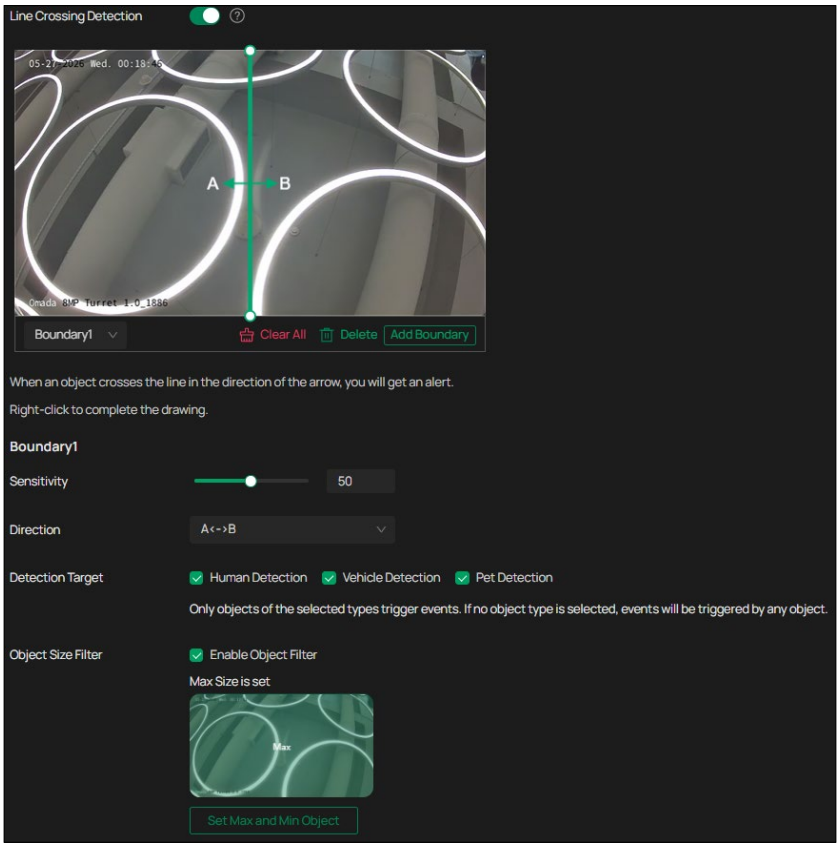
Sensitivity	Drag the slide bar to adjust the value. The higher the value is, the easier it is to trigger an alarm.
Detection Target	Select the target type, human, vehicle or pet. Only objects of the selected types trigger events. If no object type is selected, events will be triggered by any object.
Object Size Filter	Click Set Max and Min Object to define the smallest and largest object sizes that will trigger events.

4. Refer to Arming Schedule and Linkage Method for settings if needed.
5. Click **Apply**.

5. 3 Line Crossing Detection

Line crossing detection triggers alarm actions when cameras detect that moving objects cross a customized virtual line. Follow the steps below to finish the configuration.

1. Go to **Settings** > **Event** > **Line Crossing Detection**, and toggle on to enable it.



2. Draw lines on the preview screen. Select the line and configure its settings.

   Note: You can draw up to four lines and need to configure settings for each line.

Sensitivity	The higher the value is, the easier it is to detect a target that crosses the line.
Direction	Choose the direction from which the target crosses the line. A->B: Only the target crossing the configured line from the A side to the B side can be detected. B->A: Only the target crossing the configured line from the B side to the A side can be detected. A<->B: The target going across the line from both sides can be detected and alarms are triggered.
Detection Target	Select the target type, human, vehicle or pet. Only objects of the selected types trigger events. If no object type is selected, events will be triggered by any object.

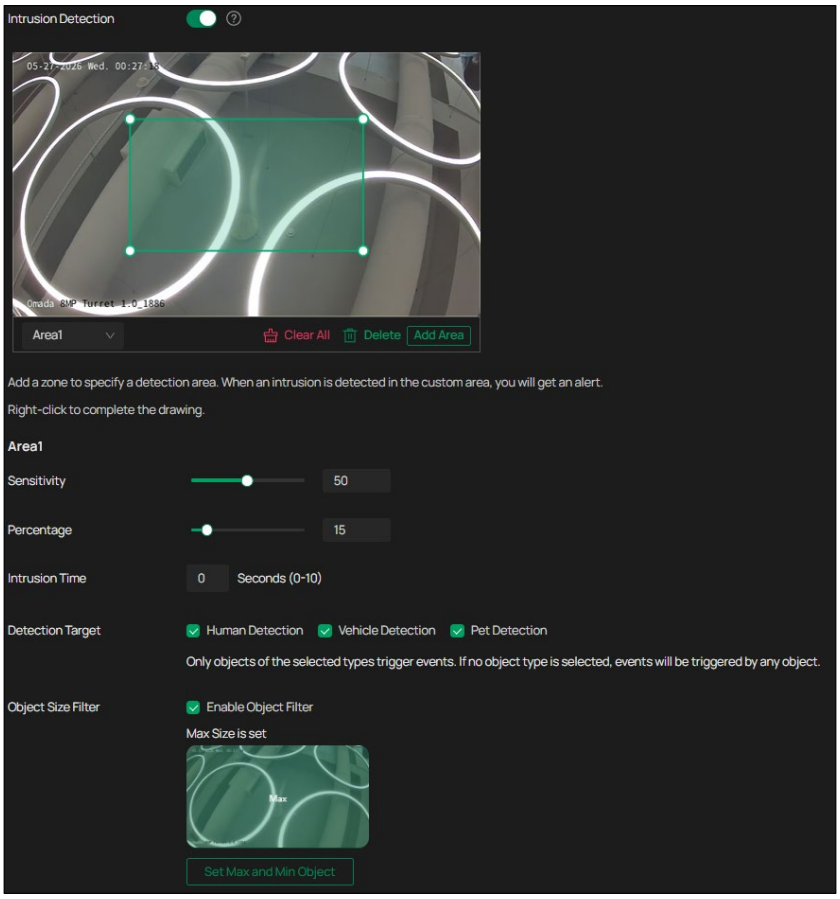
Object Size Filter	Click Set Max and Min Object to set the minimum and maximum object to filter the corresponding events.

3. Refer to Arming Schedule and Linkage Method for settings if needed.
4. Click **Apply**.

5. 4 Intrusion Detection

Intrusion detection is used to detect objects entering and loitering in a predefined virtual region. Once it happens, the camera will take linkage methods. Follow the steps below to finish the configuration.

1. Go to **Settings** > **Event** > **Intrusion Detection**, and enable it.



2. Draw intrusion areas on the preview screen. Select the area and configure the settings. You can manually draw an area by clicking the mouse on the image. Right-click to end drawing, click the midpoint of a line segment to add an endpoint, double-click an endpoint to delete it, and you can draw up to 16 polygons.

   Note: You may draw up to four areas and need to configure settings for each area.

Sensitivity	The higher the value is, the more easily an intrusion action can be detected.

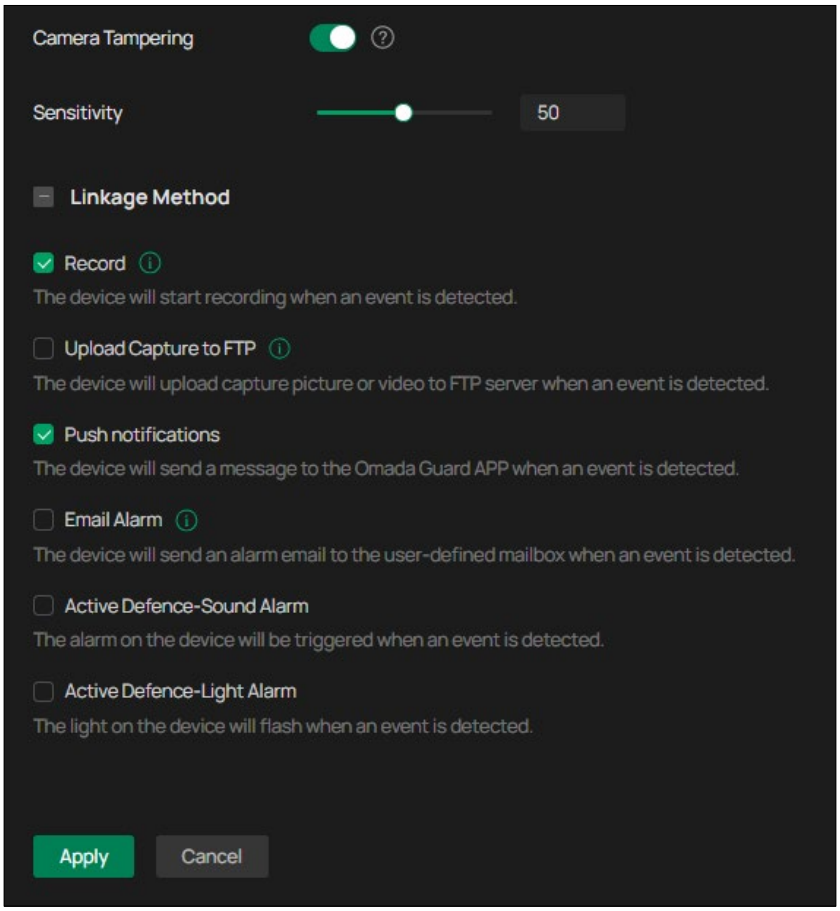
Percentage	Set the percentage of intrusion detection. When an object takes up the specific percentage of the area, the alarm actions will be triggered.
Intrusion Time	Intrusion time stands for the threshold a target loiters in the area. Any stay longer than the intrusion time will trigger the linkage action.
Detection Target	Select the target type, human, vehicle or pet. Only objects of the selected types trigger events. If no object type is selected, events will be triggered by any object.
Object Size Filter	Click Set Max and Min Object to set the minimum and maximum object to filter the corresponding events.

3. Refer to Arming Schedule and Linkage Method for settings if needed.
4. Click **Apply**.

5. 5 Camera Tampering

Camera tampering triggers alarm actions when an area of camera's lens is purposely blocked, obstructed or vandalized. You can customize the camera tampering settings, and select the linkage methods. Follow the steps below to finish the configuration.

1. Go to **Settings** > **Event** > **Camera Tampering.**



2. Enable **Camera Tampering**.
3. Set the sensitivity of camera tampering. A higher value can trigger the alarm actions more easily.
4. Select the linkage methods if needed.
5. Click **Apply**.

6

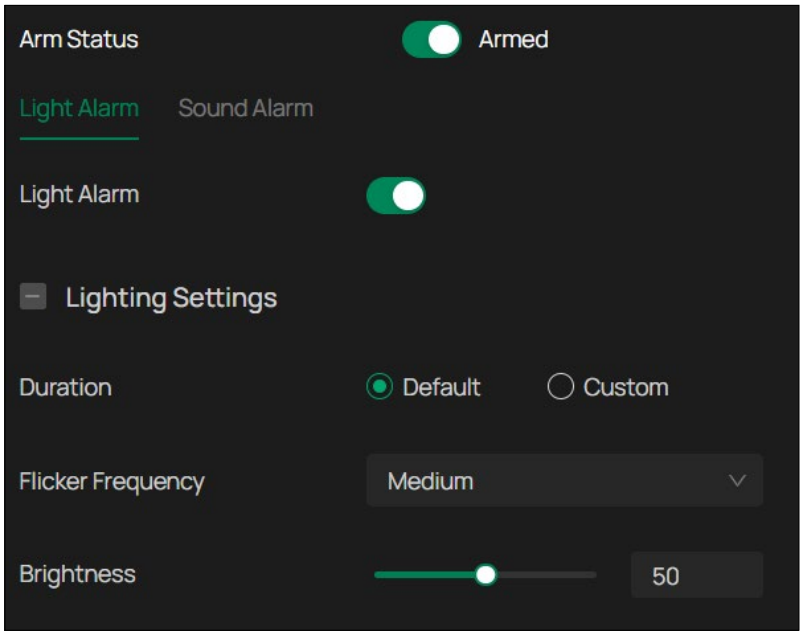
Alarm

This chapter guides you on how to configure the light alarm and sound alarm. This chapter includes the following sections:

6. 1 Light Alarm (Only for some models)

With Light Alarm enabled, the light on the camera will flash when an event is detected. Follow the steps below to finish the configuration.

1. Go to **Settings** > **Alarm** > **Active Defence** > **Light Alarm** and toggle to enable the light alarm. It is enabled by default.



2. Configure the following parameters.

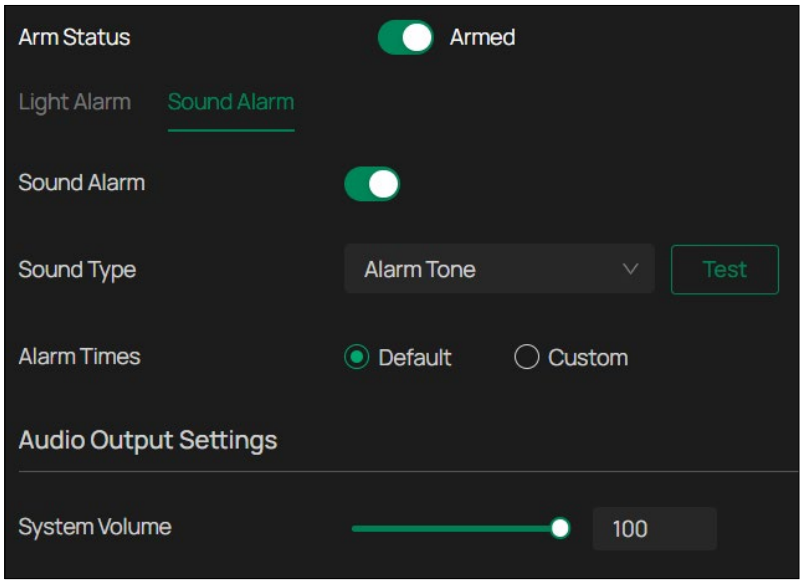
Duration	Select the Duration mode. In the Default mode, once an event triggers the light alarm, the light will flash continuously as long as the event continues to trigger, with no time limit. Each event triggers only once, and each flash lasts 5 seconds. In the Custom mode, you can customize the light alarm duration. The default value in custom mode is 5 seconds, meaning the light will flash for 5 seconds after the event triggers the alarm and then stop. Users can customize the duration from 5 to 35 seconds.
Flicker Frequency	From the drop-down menu, choose a flicker frequency: Low, Medium, or High.
Brightness	Drag the slider to adjust brightness between 0 and 100. Higher values increase the brightness of the light alarm.

4. Refer to Arming Schedule and Linkage Method to set arming schedule if needed, and the light alarm will be triggered only during the specific periods.
5. Click **Apply**.

6. 2 Sound Alarm (Only for some models)

Enable Sound Alarm, then the alarm on the camera will be triggered when an event is detected.

1. Go to **Settings** > **Alarm** > **Active Defence** > **Sound Alarm** to toggle on to enable the sound alarm. It is enabled by default.
2. Enable **Sound Alarm**, select the **Sound Type**, and click **Test**.



3. Select the alarm times mode.

   In the Default mode, once an event triggers an alarm, the alarm audio will play continuously as long as the event continues, without any time limit.

   In the Custom mode, you can customize the number of alarm sounds. The default value in custom mode is 5 sounds, meaning that the alarm audio will play 5 times after an event triggers an alarm. Users can customize the number of alarm sounds from 1 to 50.

4. Under Audio Output Settings, drag the slide bar to set the system volume.
5. Refer to Arming Schedule and Linkage Method to set arming schedule if needed, and the sound alarm will be triggered only during the specific periods.
6. Click **Apply**.

7

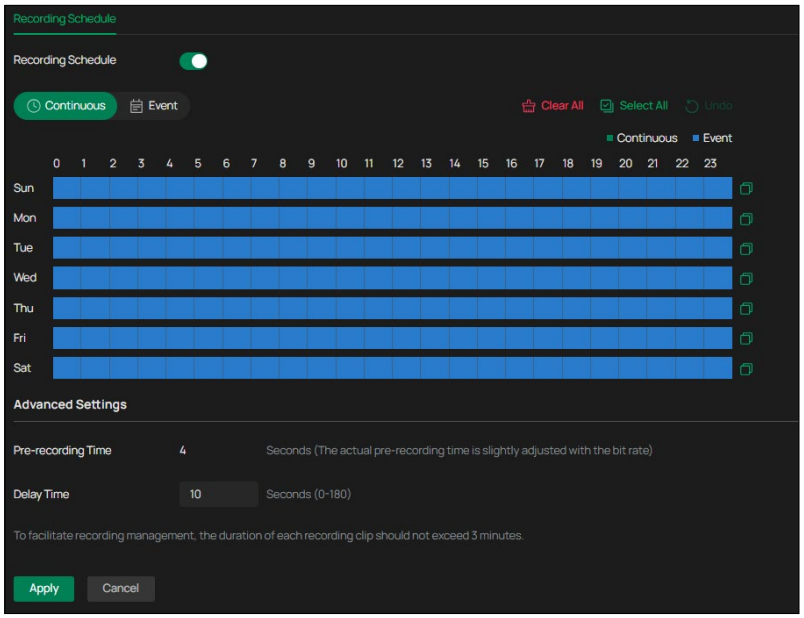
Recording and Storage

This chapter guides you on how to view and configure recording and storage settings on your camera. You can set your own recording schedules and parameters. This chapter includes the following sections:

7. 1 Recording Schedule

Recording schedule section provides convenience and flexibility for the daily monitoring of your camera. You can customize the recording schedules. You can set different schedules for each day. In Advanced Settings page, you can set the pre-recording time and delay time for recording.

1. Go to **Settings** > **Storage** > **Recording Schedule**, and enable it.



2. Select Continuous or Event.

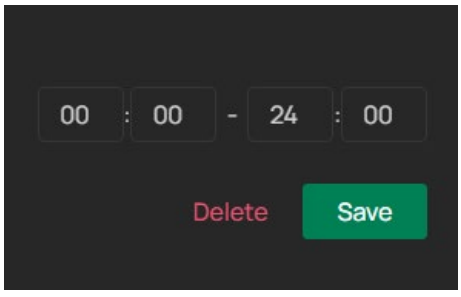
Continuous	The camera will record continuously.
Event	The camera will record when an event is detected.

4. Drag the time bar to draw desired valid time.

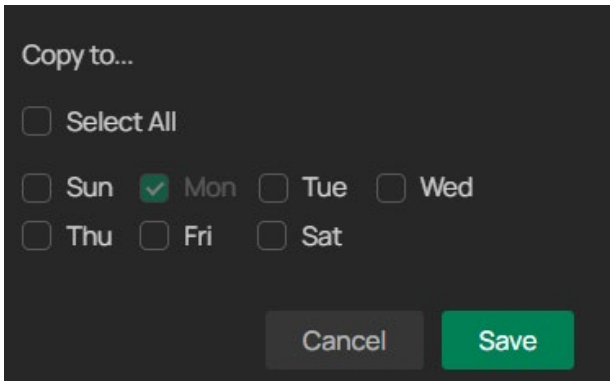
   Note:

- Each cell represents one hour.
- The default setting is 24/7.
- Up to 24 time periods can be configured for a day.

5. Click a time block and an edit button will appear. Enter the pop-up window to fine-tune the Start Time and End Time (with an accuracy of a minute) and check **Save**.



6. To copy a schedule from one day to others, click . In the pop-up window, select the days you want to copy the schedule to.



7. You can view the pre-recoding time and configure the delay time.

Pre-recording Time	4 seconds is preset for cameras to record before an event
Delay Time	The time is set for cameras to record after an event. For example, if you set the post-record time as 5 seconds, it records till 11:00:05 as motion detection ends at 11:00.

8. Click **Apply**.

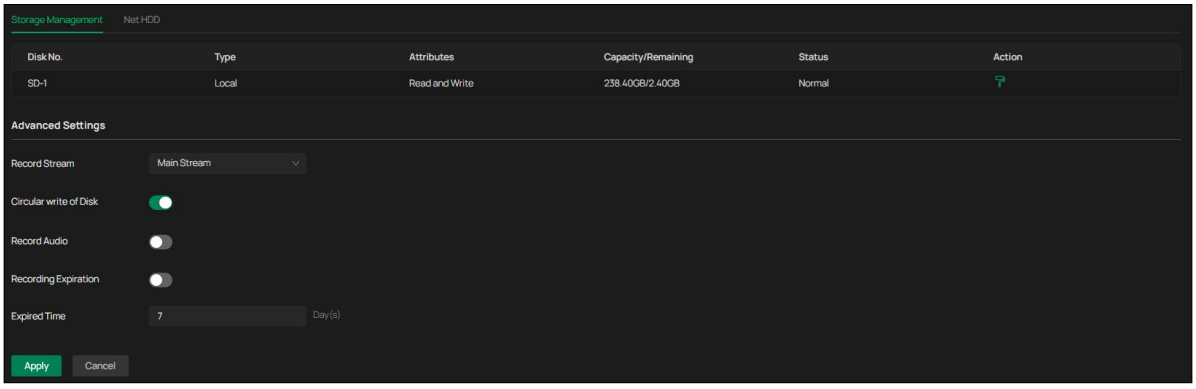
7. 2 Storage Management

In Storage Management, you can configure the properties and disk group of SD card. You can also configure the NFS shared directory provided by a NAS server as a Net HDD.

7. 2. 1 Configure Local Storage

In Storage Management, you can view the parameters and configure the properties and disk group of SD card. You can also enable the camera to overwrite the earlier recording files when the SD card is full.

1. Go to **Settings** > **Storage** > **Storage Management** > **Storage Management**.



2. Click to initialize the memory card.

When the Status of memory card turns from Uninitialized to Normal, the memory card is ready for use.

3. Specify advanced settings.

Record Stream	Select the stream type for recording. **Main Stream** stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission. **Substream** usually offers comparatively low resolution options, which consumes less bandwidth
Circular Write of Disk	Enable **Circular Write of Disk** to overwrite the video records when the storage space is full. Otherwise the camera cannot record new videos. When multiple Net HDDs are in the same directory, circular overwriting may not work. It is recommended to separate Net HDDs in different directories.
Record Audio	Enable to record audio and video simultaneously.
Recording Expiration	Enable **Recording Expiration** to delete recordings when they exceed the expired time. Note that once the recordings are deleted, they cannot be recovered. This feature does not work for Net HDD.
Expired Time	Set the time when recordings will be automatically deleted.

5. Click **Apply**.

7. 2. 2 Configure Net HDD

Configure the NFS shared directory provided by a NAS server as a Net HDD. With this feature, the camera can record and store video data directly to the NAS over the network, without relying on an NVR, enabling centralized storage and backup.

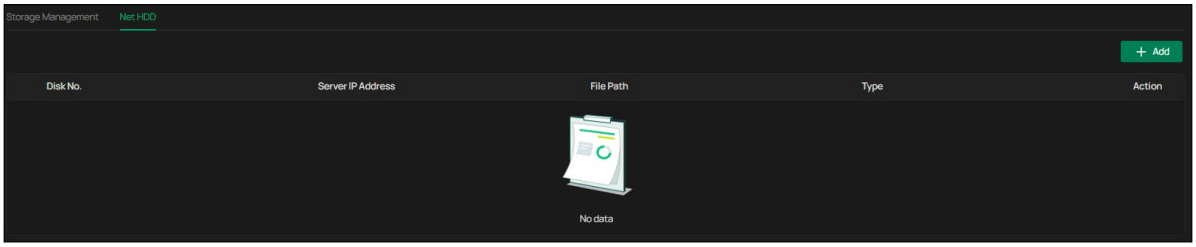
Notes:

1. The NAS Server must support the NFS protocol, and the NFS version must be NFS v3 or above.

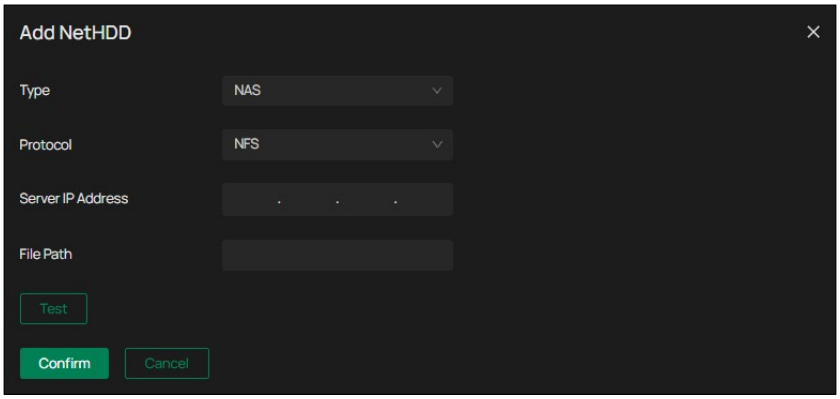
2. Ensure that the IP address of the Omada Camera is granted read/write (RW) access to the shared path on the NAS server.

3. To maintain stable network access and optimal performance, it is recommended to keep the NAS Server and the Omada Camera within the same subnet.

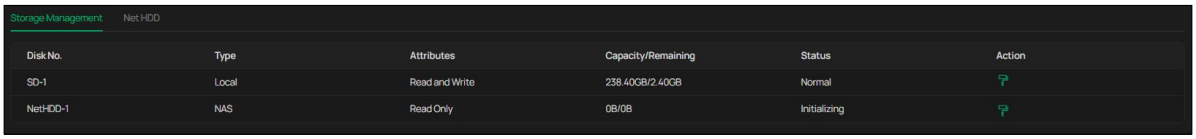
1. Go to **Settings** > **Storage** > **Storage Management** > **Net HDD** to load the following page.



2. Click the **Add** button to add a net HDD. Currently, the maximum single storage is 1TB, with a total capacity of 2TB. The larger the storage space, the longer the formatting time will be and the specific time depends on network conditions and server performance. Note that there is a limit to the number of Net HDD entries that can be added. Once the maximum limit of 2 is reached, the "+Add" button will be disabled.
3. Enter the IP address of your NAS Server and the file path of the configured NFS shared directory. Click **Test**.



4. Go to **Settings** > **Storage** > **Storage Management** > **Storage Management**. In the Disk list, you can see the newly added NetHDD-1. At this stage, its attribute is "Read Only". Click the icon on the right to format the newly added NetHDD-1.



5. After formatting is complete, the NetHDD-1 attribute changes to "Read and Write", correctly displays the disk Capacity and Remaining available space, and the status changes to "Normal". Click **Apply** to save the configuration.

8

Network Management

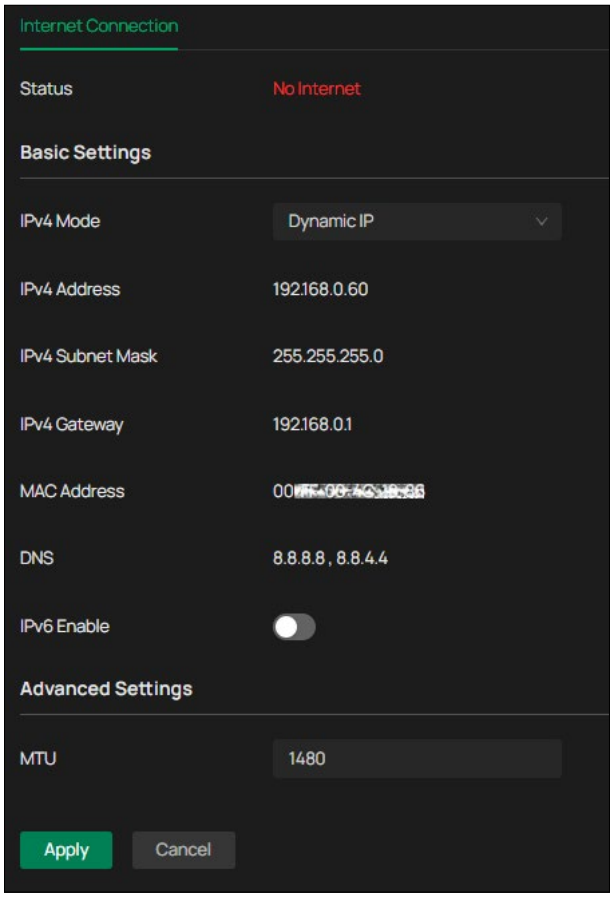
With proper network configurations, you can connect your camera to the internet, build up mapping between internal and external ports. This chapter contains the following sections:

8. 1 Internet Connection

In Internet Connection, you can view the connection status and configure the camera to obtain a dynamic or static IP address.

Follow the steps below to configure the network settings.

1. Go to **Settings** > **Network Settings** > **Connect**.



2. Configure the following:

Status	Displays the current internet status.
IPv4 Mode	Configure the camera to obtain a dynamic or static IP address.
IPv4 Address	Specify an IP address for the camera. The IP address should be in the same segment as the gateway; otherwise, the camera cannot connect to the internet.
IPv4 Subnet Mask	Enter the subnet mask.
IPv4 Gateway	Enter the IP address of the gateway device to which the data packets will be sent. This IP address should be in the same segment as the camera's IP address.

MAC Address	A unique identifier permanently assigned to the camera's network interface card (NIC). It is used to identify the camera on a local network, enabling it to communicate with other devices on the same network segment.
DNS	Enter the IP address of the DNS server.
IPv6 Enable	Enable to configure IPv6 settings. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.
MTU	Specify MTU (Maximum Transmission Unit) to decide the largest size of data unit that can be transmitted in the network. A larger unit can improve the efficiency with more data in each packet, but it may increase the network delay because it needs more time to transmit. Therefore, if you have no special needs, it is recommended to keep the default value.

Note: The cameras should be in the same segment with the NVR, so that the NVR can discover and manage them.

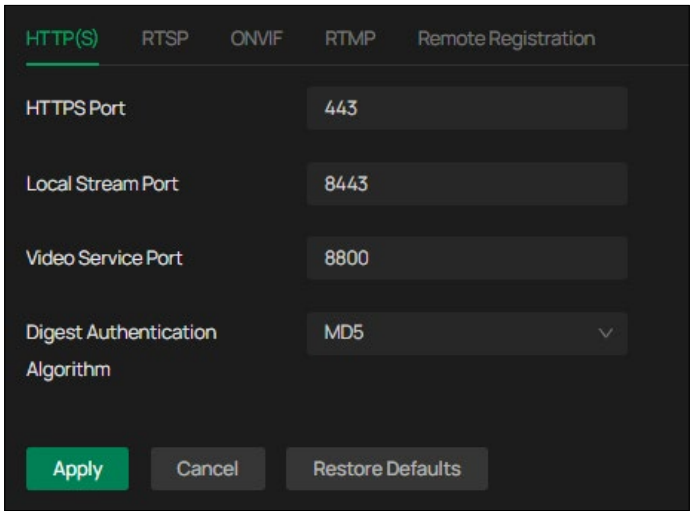
3. Click **Apply**.

8. 2 Network Service

In Network Service, you can configure the HTTPS port and service port of devices that can be used to access the camera through the network. When managing and monitoring the devices via the Omada Central or the Omada Guard app, the ports configured here are used for communications of corresponding protocols.

8. 2. 1 HTTPS Service

1. Go to **Settings** > **Network Settings** > **Network Service** > **HTTP(S)**.



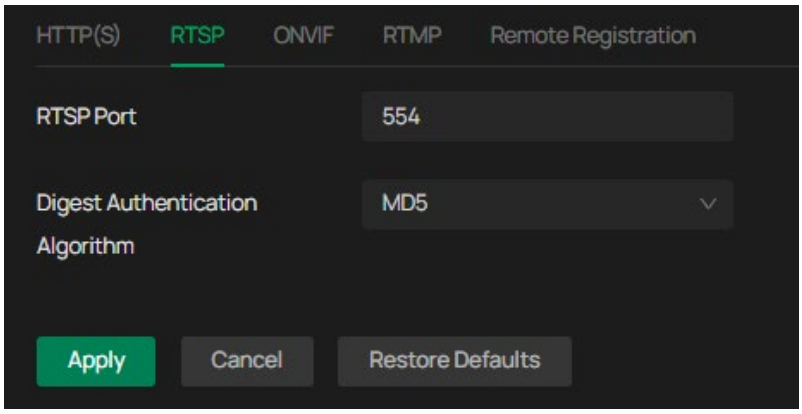
2. Specify HTTPS port and service ports.

HTTPS Port	Specify a port for HTTPS protocol.
Local Stream Port	Specify a port for protocols of video services.
Video Service Port	Specify a port to access the camera's live streaming web interface.
Digest Authentication Algorithm	Choose between MD5, SHA256, and MD5/SHA256.

3. Click **Apply**.

8. 2. 2 RTSP Service

1. Go to **Settings** > **Network Settings** > **Network Service** > **RTSP**.



2. Configure the following ports:

RTSP Port	Specify a port for RTSP (Real Time Streaming Protocol) protocol. RTSP is an application layer protocol for connecting, transferring, and streaming media data in real time from IP cameras connected to the network. rtsp://username:password@ip:port/streamNo ip – IP of the Camera. port – Default port is 554. This can be skipped. streamNo – Stream number. Stream1 refers to the main stream; stream2 refers to the substream. Example URL: rtsp://admin:123456@192.168.1.60:554/stream1 This will display the main stream of the camera, where admin is the user name and 12345 is the password.

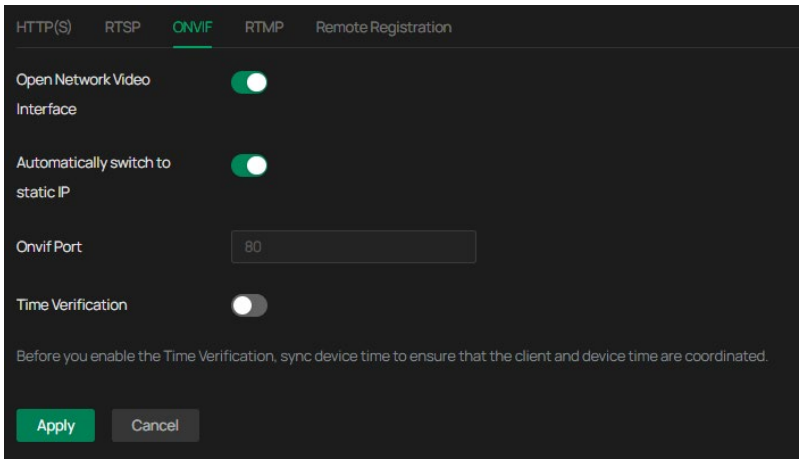
Digest Authentication Algorithm	Choose between MD5, SHA256, and MD5/SHA256.

8. 2. 3 ONVIF

ONVIF (Open Network Video Interface Forum) is an open industry standard that enables IP cameras to work seamlessly with third-party video management systems, recorders, and software platforms. By enabling ONVIF, the camera can be discovered, configured, and controlled by other ONVIF-compliant devices—regardless of brand.

Enable ONVIF if you need to use third-party management devices.

1. Go to **Settings** > **Network Settings** > **Network Service** > **ONVIF**.



2. Configure the following:

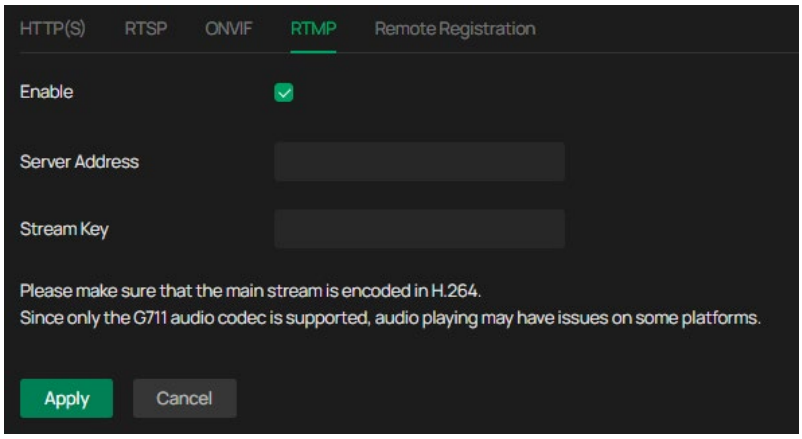
Open Network Video Interface	Enables ONVIF support, allowing the camera to connect with third-party video management systems that support the ONVIF protocol.
Automatically switch to static IP	When enabled, the device will automatically switch to a static IP address during ONVIF communication to ensure stable connectivity.
Onvif Port	For firmware version 1.6 and onwards, ONVIF uses port 80 and 2020 by default for communication; for earlier versions, the default port for ONVIF is 2020.
Time Verification	Ensures secure ONVIF access by verifying time consistency between the device and the client. Note: Before enabling Time Verification, make sure the device time is synchronized with the client to avoid authentication issues.

3. Click **Apply**.

8. 2. 4 RTMP

RTMP (Real-Time Messaging Protocol) is a widely used streaming protocol that allows your IP camera to broadcast live video to platforms such as YouTube, Facebook Live, or custom media servers. This enables real-time video sharing over the internet with low latency and broad compatibility.

1. Go to **Settings** > **Network Settings** > **Network Service** > **RTMP**, and enable it.



2. Configure the following parameters.

   Note: Ensure the main stream is encoded using H.264, as this is the only supported video codec for RTMP streaming.

   Additionally, the G711 audio codec is used; some platforms may experience audio playback issues due to limited support for this format.

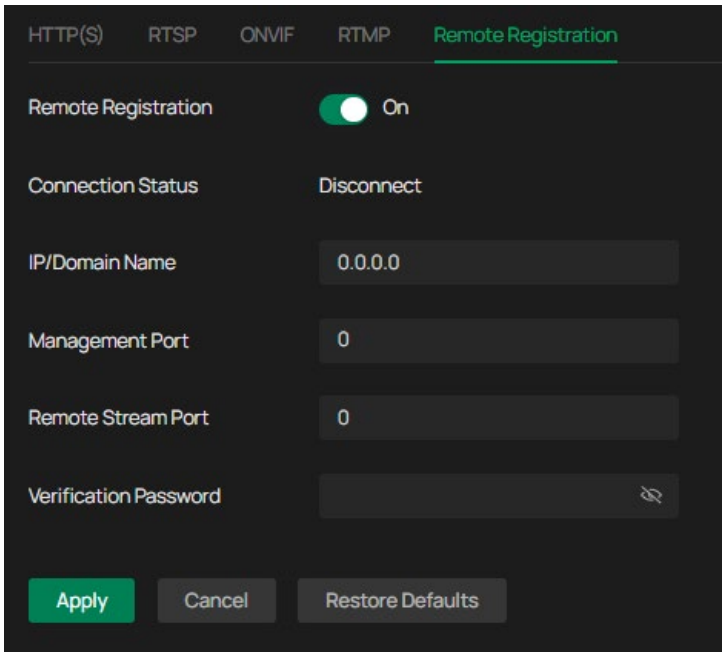
Server Address	Enter the RTMP server URL provided by your streaming platform. This defines the destination where your camera's video stream will be sent.
Stream Key	Enter the unique stream key assigned by your platform. This authenticates and links your camera's feed to your specific live stream.

3. Click **Apply**.

8. 2. 5 Remote Registration

The Remote Registration feature allows the camera to connect to a remote management platform or server. This is typically used for centralized monitoring and management across different network segments.

Follow these steps to register the device to a remote server:

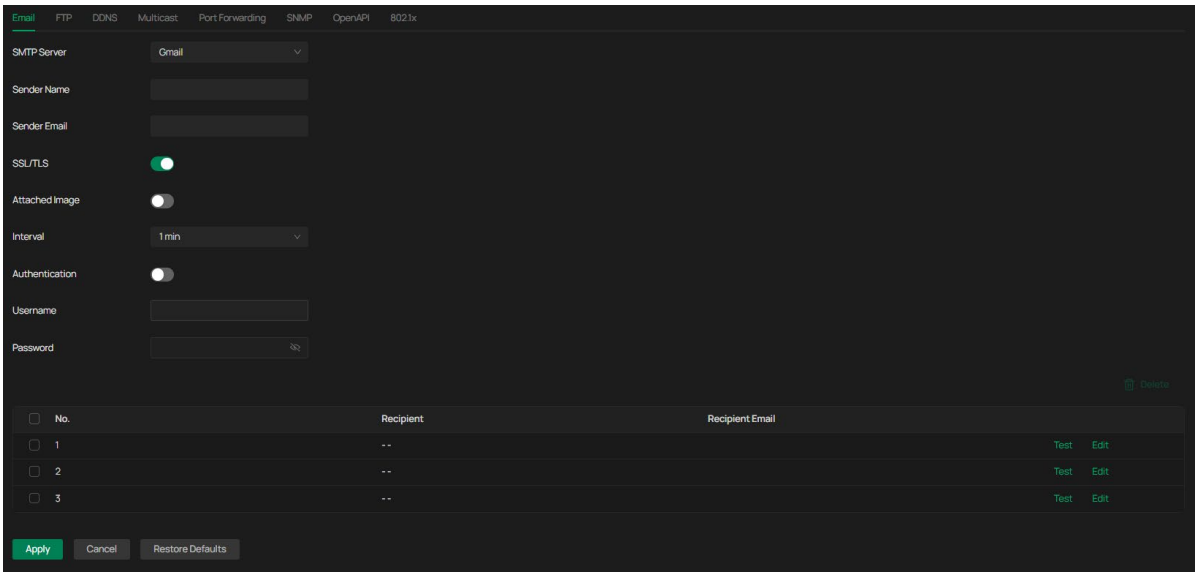


1. Go to **Settings** > **Network Settings** > **Network Service** > **Remote Registration**, and enable it.
2. In the IP/Domain Name field, enter the static IP address or the Fully Qualified Domain Name (FQDN) of the destination server.
3. Configure Ports:
   1) Management Port: Enter the port number used for device management communication (assigned by the server).
   2) Remote Stream Port: Enter the port number designated for video data transmission.
4. Enter the registration password required by the remote server in the Verification Password field.
5. Click **Apply**.

Note: If the Connection Status remains "Disconnect" after clicking **Apply**, verify your network gateway settings and ensure the specified ports are open on the server-side firewall.

8. 3 Email

When the email is configured and enabled as a linkage method, the device sends an email notification to all designated recipients if an alarm event is detected.



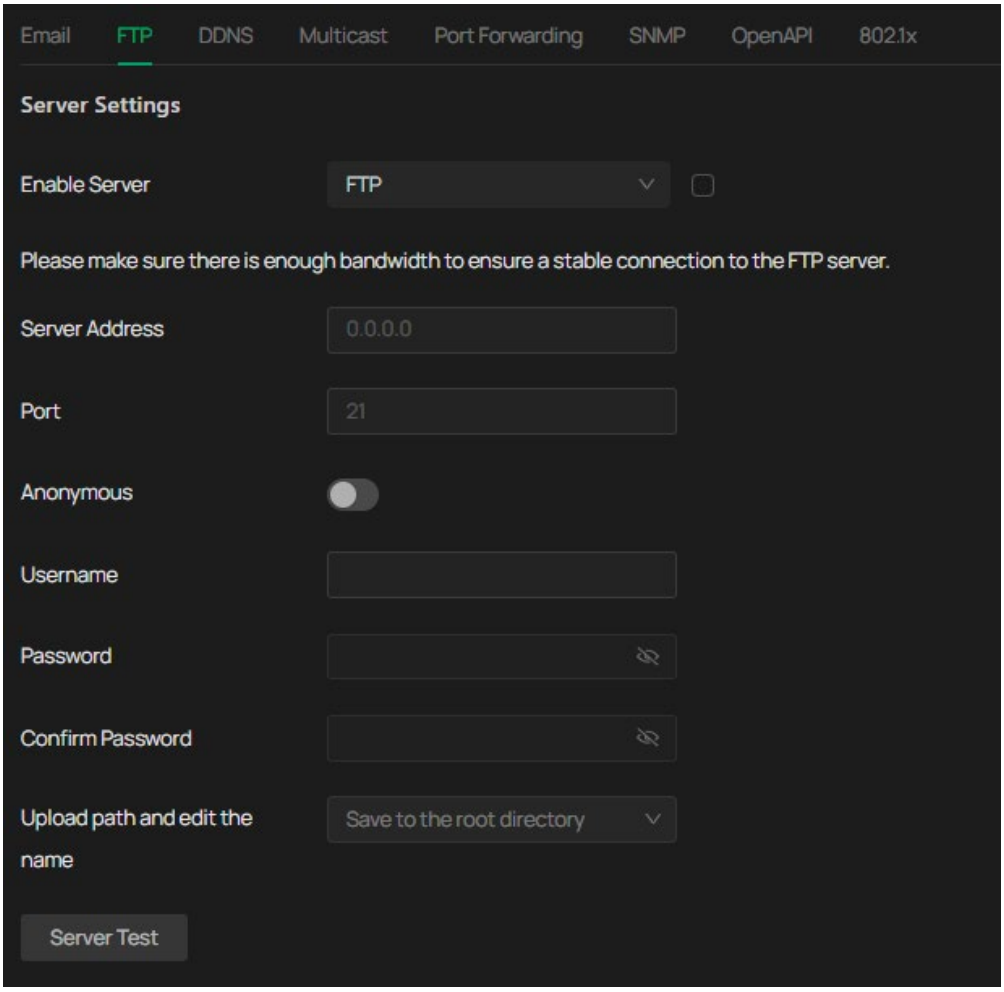
1. Go to **Settings** > **Network Settings** > **Advanced** > **Email**, and enable it.
2. Select the SMTP Sever and input the sender's email information, including the Sender's name, Sender Email, SMTP Server, and SMTP Port.
3. Enable SSL/TLS if needed and emails will be sent after encrypted.
4. Enable Attached Image to receive notification with alarm pictures. The notification email has a certain number of attached alarm pictures about the event with configurable image capturing interval.
5. If your email server requires authentication, enable Authentication and input your username and password to log in to the server.
6. Input the recipient's information, including the recipient's name and address.
7. Click **Test** to see if the function is well configured.
8. Click **Apply**.

8. 4 FTP

8. 4. 1 FTP Sever

You can configure an external FTP Server to serve as a remote storage destination for the camera's data. This feature supports multiple recording and capturing methods to ensure comprehensive data redundancy.

1. Go to **Settings** > **Network Settings** > **Advanced** > **FTP**.



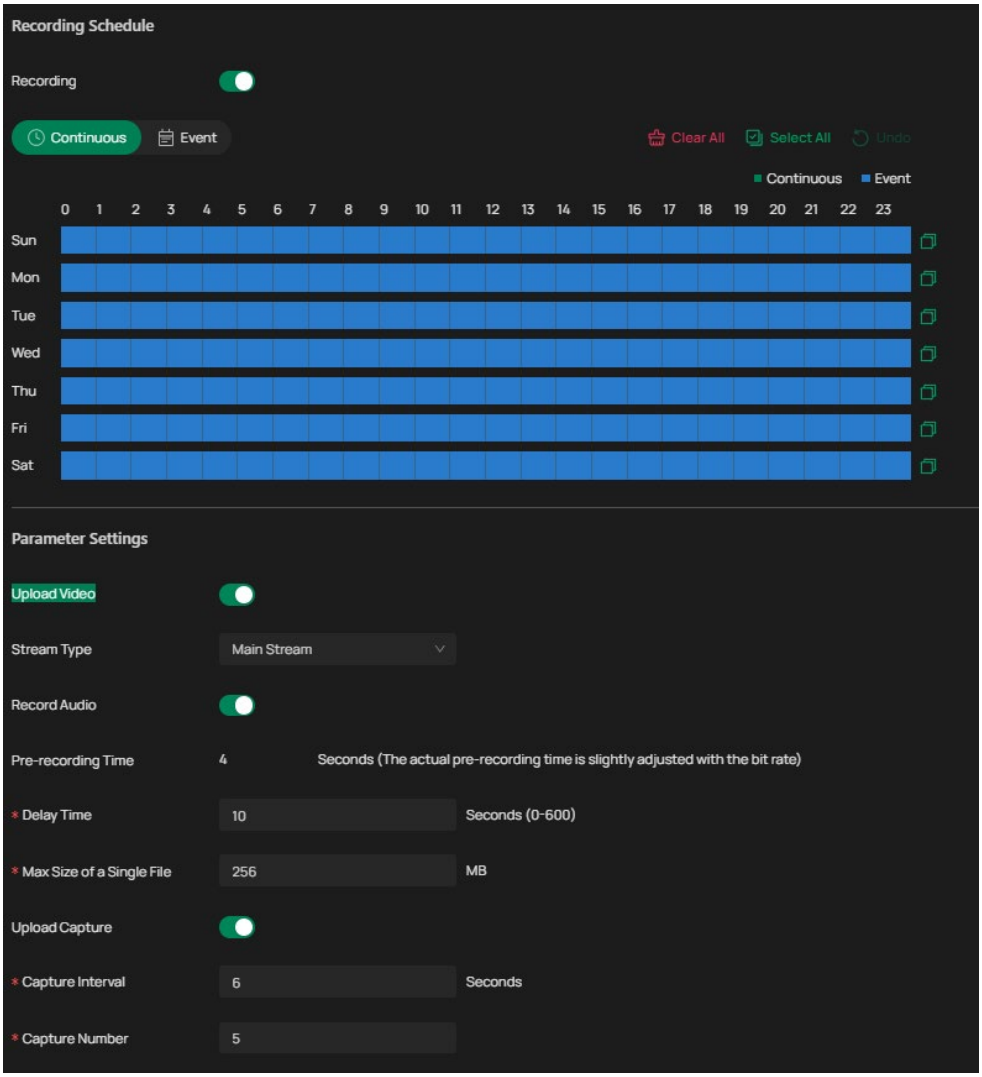
2. Check Enable Server. FTP and SFTP are selectable. The files uploading is encrypted by using SFTP protocol.
3. Enter Server Address and Port. They stand for the FTP server address and corresponding port.
4. Set Username and Password and confirm the password. The FTP user should have the permission to upload pictures.
5. If the FTP server supports picture uploading by anonymous users, you can check Anonymous to hide your device information during uploading.

   Note: Anonymous login is not supported when SFTP protocol is selected.
6. Select the saving path of images uploaded in the dropdown box of Upload Path and Edit the Name.
7. Click **Sever Test** to verify the FTP server.
8. Click **Apply**.

8. 4. 2 FTP Upload

You can configure the parameters of videos and images to be uploaded to the FTP server.

1. Go to **Settings** > **Network Settings** > **Advanced** > **FTP**, locate the recording schedule section.



2. Enable Recording Schedule and follow the steps in Recording Schedule.
3. Enable Upload Video and Upload Capture as needed. Upload Video allows the system to automatically send recorded video clips to the configured FTP server. Upload Capture allows the system to upload snapshot images captured during events.
4. Configure the following parameters:

Stream Type	Select the stream type for recording. **Main Stream** stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission. **Substream** usually offers comparatively low resolution options, which consumes less bandwidth
Record Audio	Enable to record audio and video simultaneously.

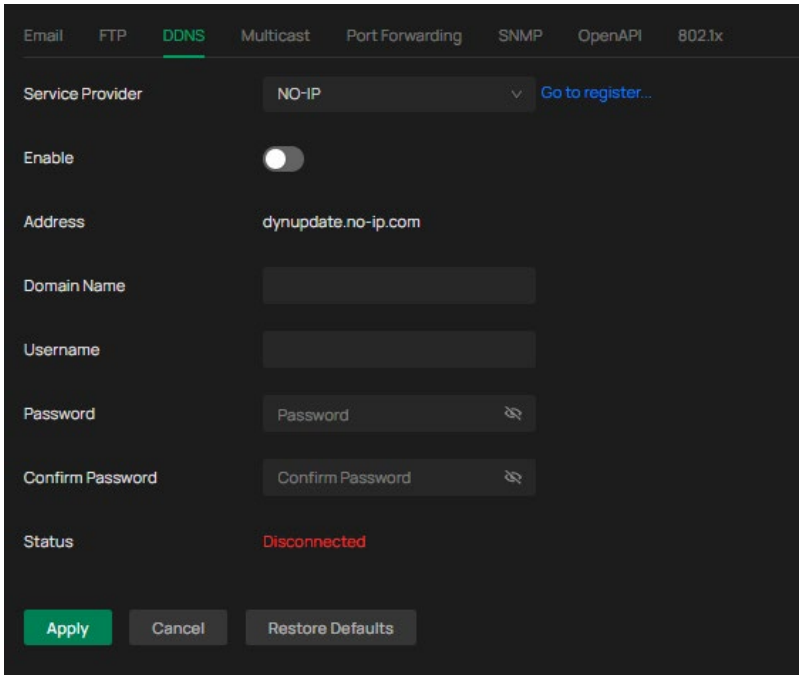
Delay Time	The time is set for cameras to record after the scheduled time or event. For example, if you set the post-record time as 5 seconds, it records till 11:00:05 as motion detection ends at 11:00.
Max Size of a Single File	Set the size limit of a single file.
Capture Interval	The camera takes the capture when it reaches the capture interval.
Capture Number	The number of captures taken during one interval.

5. Click Apply.

8. 5 DDNS

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name. Registration on the DDNS server is required before configuring the DDNS settings of the device.

1. Go to Settings > Network Settings > Advanced > DDNS.



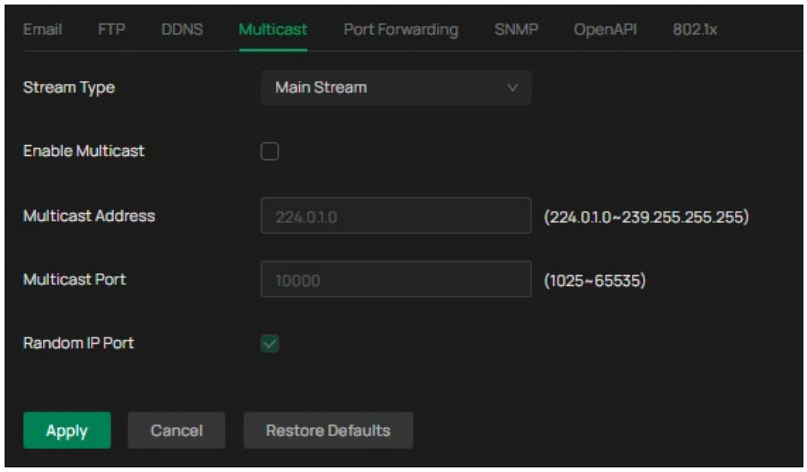
2. Select the type of Service Provider for domain name resolution.
3. Enter the domain name information, and click Apply.

8. 6 Multicast

When Multicast is enabled, multiple users within the same local network can view the live video stream simultaneously without increasing the camera's CPU load or consuming additional upload bandwidth for each connection.

Follow the steps below to configure Multicast.

1. Go to **Settings** > **Network Settings** > **Advanced** > **Multicast**.
2. Select the stream type, then enable **Multicast**.



3. Disable Random IP Port and specify a static address and port, or enable Random IP Port.
4. Click **Apply**.

After Multicast enabled, you can watch the video with the URL rtsp://A:B:C:D/multicastStreamN, for example, rtsp://192.168.0.3/multicastStream1. A.B.C.D is the IP address of the camera, and N can be number 1 or 2 that indicates the stream, 1 for main stream and 2 for substream.

8. 7 Port Forwarding

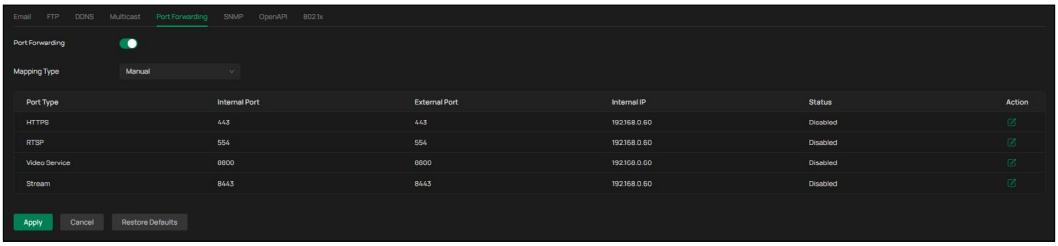
Port Forwarding is used to establish the mapping between the internal port and external port. When Port Forwarding is enabled, you can access the device and watch the videos when accessing the external port remotely.

Note: The cameras should be connected to the internet, and Port Forwarding should be enabled on the gateway.

Follow the steps below to configure Port Forwarding.

1. Go to **Settings** > **Network Settings** > **Advanced** > **Port Forwarding**.

2. Enable Port Forwarding and specify a mapping type. If you select **Auto** as the mapping type, the mappings are established automatically. If you select **Manual** as the mapping type, click to specify the external port.



Port Type	Displays the protocol type.
Internal Port	Displays the port of the camera to be converted.
External Port	Displays the external port opened by the gateway.
Internal IP	Displays the IP address of the camera that needs to be converted.
Status	Displays the status of mapping.

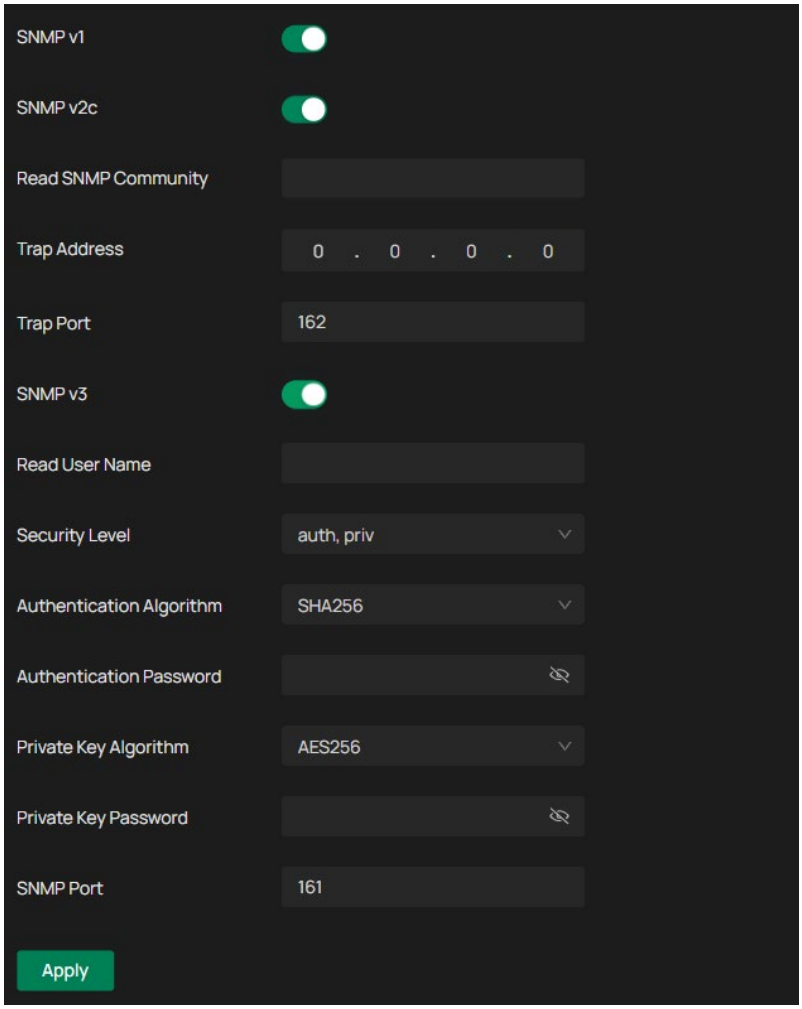
3. Click **Apply**.

With Port Forwarding enabled, you can remotely watch the videos with the URL rtsp://A.B.C.D:Port/streamN, for example, rtsp://10.0.1.47:28736/stream1. A.B.C.D is the WAN IP address of the gateway, and Port is the number of RTSP external port. N can be number 1 or 2 that indicates the stream, 1 for main stream and 2 for substream.

8. 8 SNMP

SNMP (Simple Network Management Protocol) enables your network management system (NMS) to monitor camera status, including uptime, network performance, and basic device health. Once configured, the camera can be integrated into a centralized monitoring platform for proactive management.

1. Go to **Settings** > **Network Settings** > **Advanced** > **SNMP**.



The camera supports SNMP v1, SNMP v2c, and SNMP v3. Select the version required by your NMS and configure its parameters.

SNMP v2c uses a community string for authentication.

1. In the SNMP v2c section, enter a Read SNMP Community string.

The default is often public, but you should replace this with a strong, unique string.

2. In Trap Address, enter the IP address of the NMS that will receive SNMP trap messages.
3. Confirm the Trap Port. The standard trap port is 162.

SNMP v3 offers user-based authentication and encryption.

1. In the SNMP v3 section, enter a Read User Name to identify the SNMP user.
2. Select a Security Level. The Security Level determines how SNMP v3 protects communication between the camera and the NMS:

no auth, no priv	This level provides neither authentication nor encryption. It is the least secure option and should only be used on fully trusted, isolated networks.

auth, no priv	This level provides authentication but no encryption. It ensures that messages come from a verified source, although the contents of the messages can still be read on the network.
auth, priv	This level provides both authentication and encryption. It offers the highest level of protection and is recommended for most environments.

3. Choose an Authentication Algorithm. The Authentication Algorithm verifies the identity of the sender. You can choose from the following options:

MD5	Offers basic security and is considered an older standard. It should be used only if required by your existing NMS.
SHA	Provides stronger protection and is widely supported.
SHA-256	Offers enhanced security and is recommended when supported by your NMS.

   A stronger authentication algorithm provides better protection against tampering.

4. Set a strong Authentication Password.
5. If using the priv level, choose a Private Key Algorithm.

DES	Provides basic, legacy encryption and offers the lowest level of security.
AES	Provides modern and secure encryption suitable for most environments.
AES256	Provides the highest level of encryption and is recommended when supported by your NMS.

   Using AES or AES256 will provide stronger protection in secure deployments.

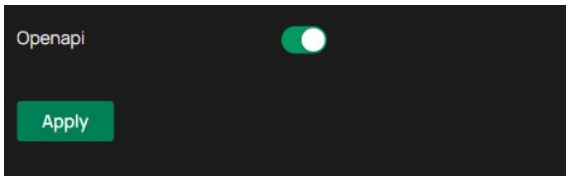
6. Set a Private Key Password.
7. Confirm the SNMP Port for queries. The standard port is 161.

After completing the settings for your chosen SNMP version, click Apply to activate SNMP on the camera.

8. 9 OpenAPI

For integration with custom software or third-party systems, you can use the OpenAPI. The OpenAPI allows you to manage Allow/Block Lists, and trigger outputs programmatically, providing flexibility for large-scale or customized workflows.

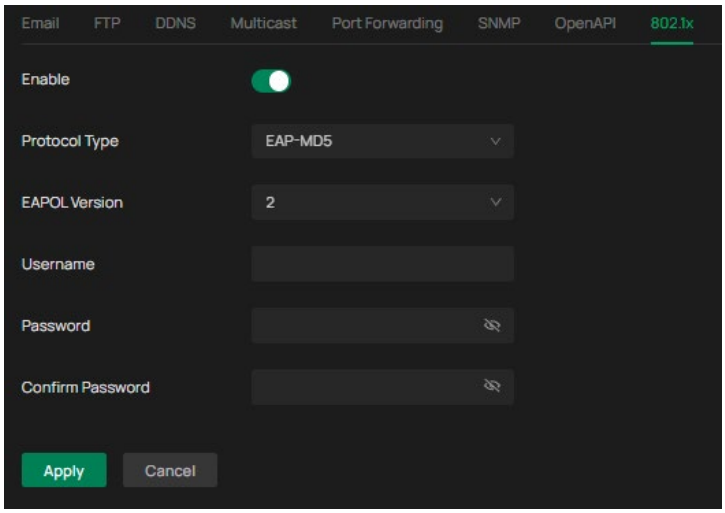
To enable this function, go to Settings > Network Settings > Advanced > Openapi.



8. 10 802.1x

802.1x is a network access control protocol that enhances security by requiring authentication before a device (like your IP camera) can connect to the network. When enabled, the camera must verify its identity through a configured authentication method before accessing the network, helping prevent unauthorized devices from joining.

1. Go to Settings > Network Settings > Advanced > 802.1x.



2. Configure the following:

Protocol Type	Select the authentication method used by your network: EAP-MD5: Basic authentication using a username and password. EAP-LEAP: Cisco proprietary protocol that supports mutual authentication. EAP-PEAP: Encapsulates authentication within a secure TLS tunnel for improved security. Choose the protocol type that matches your network's configuration.

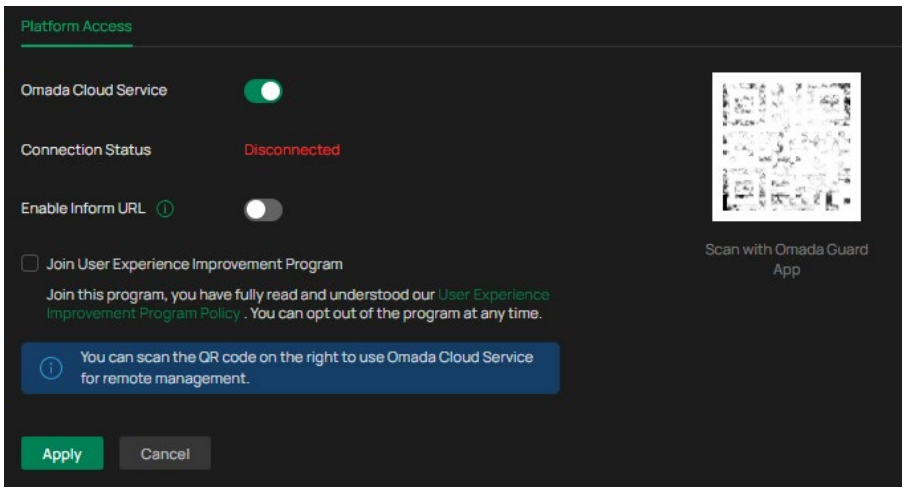
EAPOL Version	Choose the version of EAP over LAN (EAPOL) protocol used for communication: 1: Compatible with older network infrastructures. 2: Used in most modern networks for enhanced performance and compatibility.

3. Specify username, password, and click **Apply**.

8. 11 Platform Access

You can enable Omada Cloud Service to allow adding device by scanning the device key of the device or enable inform url to enter the URL of your local Omada Guard application to enable device management by the local Omada Guard application. These two features cannot be enabled at the same time.

1. Go to **Settings** > **Network Settings** > **Platform Access**.



2. If you enable **Omada Cloud Service**, check the box to join our improvement program, and click **Apply**. Then you can scan the QR code with your Omada Guard app to add the camera and manage it remotely with the Omada Guard app.
3. If you Enable Inform URL, enter the Inform URL/IP Address of your Local Omada Guard Application to tell the device where to discover it. This feature is typically used in Layer 3 deployments to enable device management by Local Omada Guard Application. Check the box to join our improvement program, and click **Apply**.

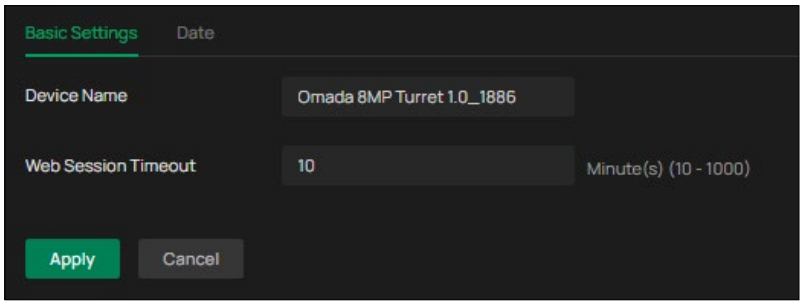
9

System Settings

This chapter guides you to configure the basic and advanced settings of your camera, export and import settings. You can create and modify administrator accounts based on your needs. This chapter includes the following sections:

9. 1 Configure Basic Settings

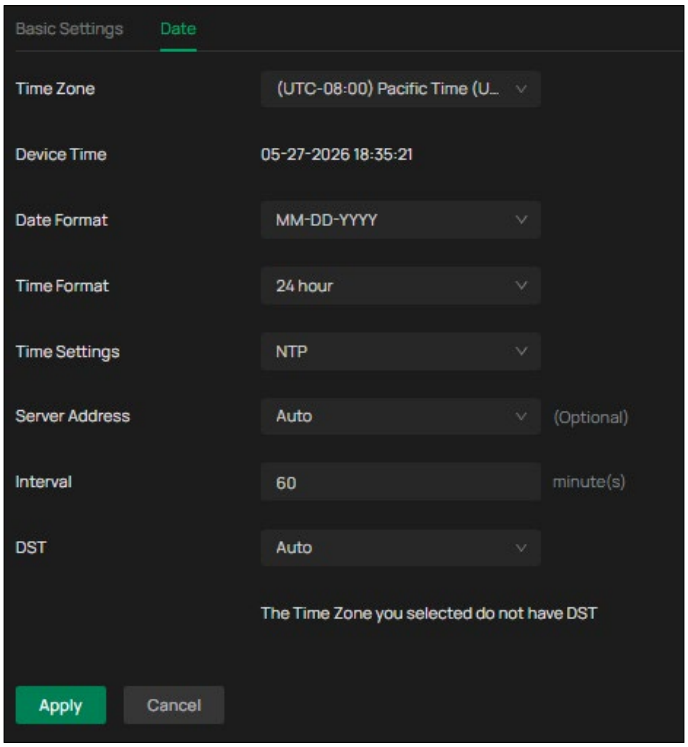
1. Go to **Settings** > **System Settings** > **Basic Settings** > **Basic Settings**.
2. View and change the name of your camera.
3. Specify the Web Session Timeout. You will be logged out when you make no operation (not including viewing live image) to the device via web browser within the set timeout period.



9. 2 Modify System Time

You can select the time zone and set the time synchronization mode to Manual or NTP mode for the camera.

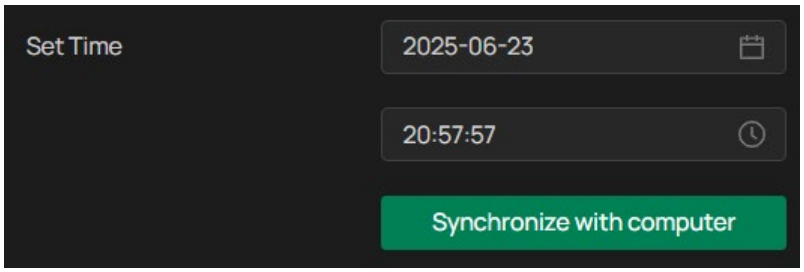
1. Go to **Settings** > **System Settings** > **Basic Settings** > **Date**.



2. Select your time zone, and set the date format and time format.
3. Configure your time settings.

   Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs on User Datagram Protocol (UDP), which in turn runs on IP, or you can manually set the

system time. If you do not want to expose your camera to the network, you can choose Manual. You may also click Synchronize with computer to synchronize the time settings of your camera with that of your PC.



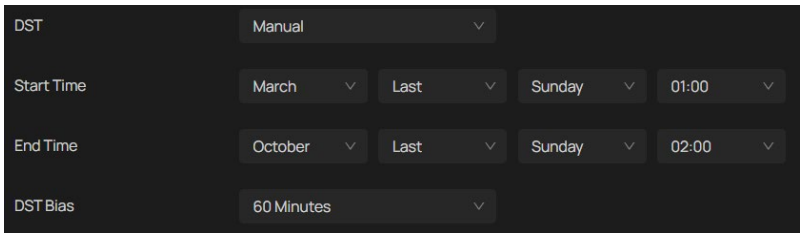
Server address	Enter the IP address of the NTP server.
Interval	Time interval between the two synchronizing actions with NTP server. Note: The interval can be set from1 to 10080 minutes, and the default value is 60 minutes.

4. (Optional) Set DST (daylight saving time) parameters.

   DST is the practice of setting the clocks forward one hour from standard time during the summer months, and back again in the fall. DST Bias is the difference in minutes between standard time and daylight-saving time for a specific time zone.

   You can select Auto at the dropdown list. Note that to update the time automatically with the DST, internet connection is required.

   Or you can select Manual and specify the date/time of the DST period.



   Note:

   1. In some time zones, DST is not observed.

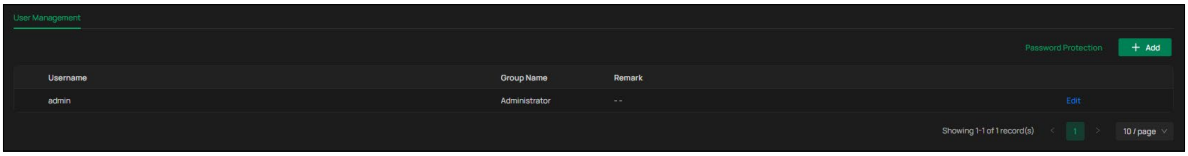
   2. If the camera is connected to an NVR, you only need to configure NTP and DST settings on the NVR, which will be synchronized with the camera.

5. Click Apply.

9. 3 Manage User Accounts

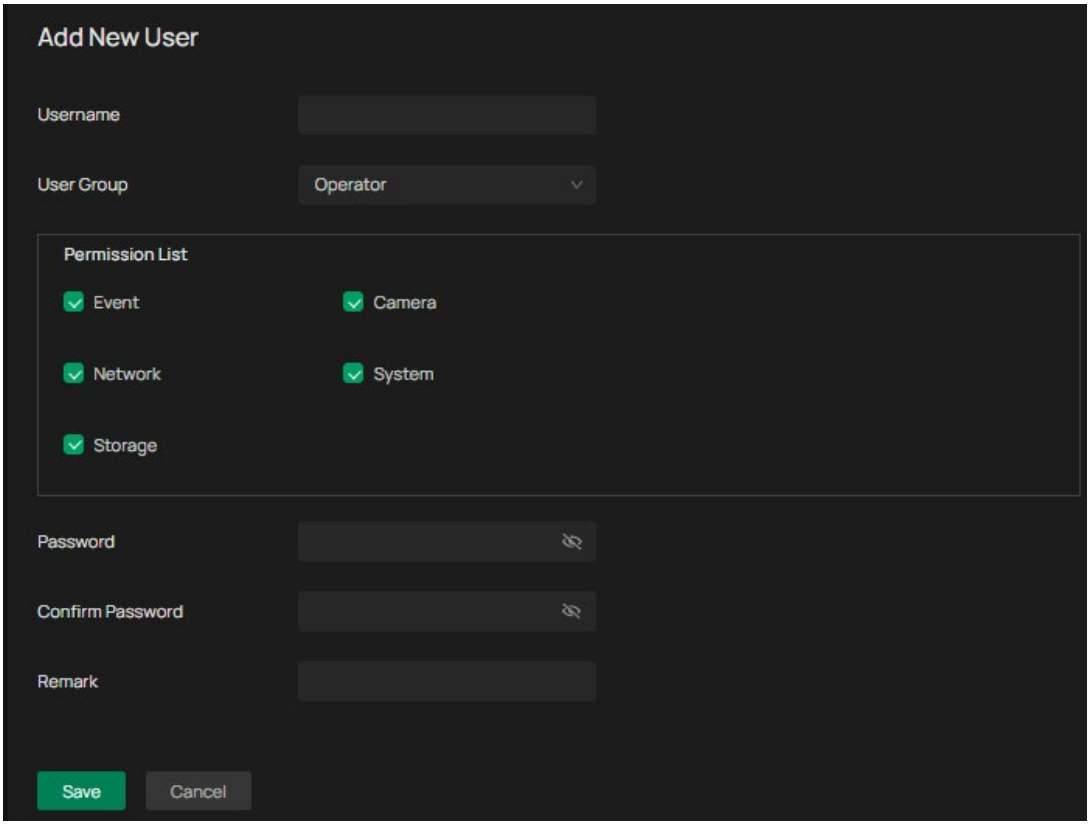
You can modify the default user account (admin) based on your needs. The Administrator user name is admin and the password is set when you set up your camera for the first time.

1. Go to **Settings** > **System Settings** > **User Management.**



2. Click **Add**. Enter Username, select User Group, and enter Password. Assign remote permission to users based on needs.

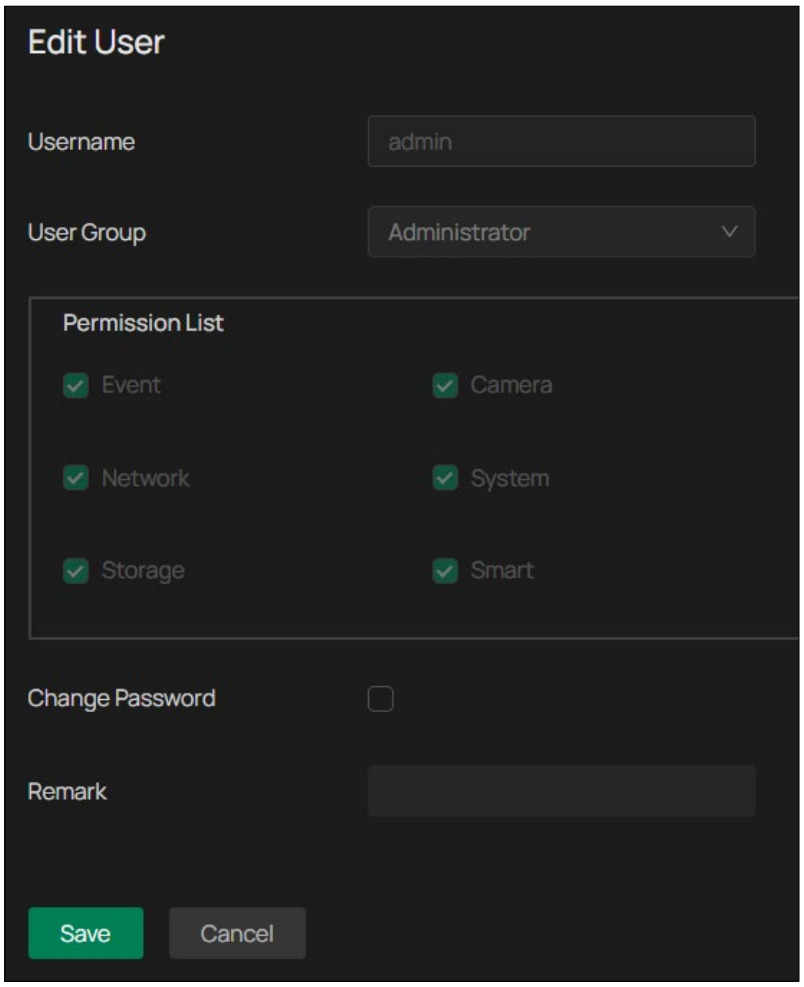
   Note: The system pre-defines a default user group: administrator, which has all the permission of the system. You can click Edit to view the details and operations. The permission list of the administrator cannot be edited.



Administrator	The administrator has the authority to all operations and can add users and operators and assign permission.
Operator	Operators can be assigned all permission except for operations on the administrator and creating accounts.
User	Users can be assigned permission of viewing live video, setting event parameters, changing camera settings, and changing their own passwords, but no permission for other operations.

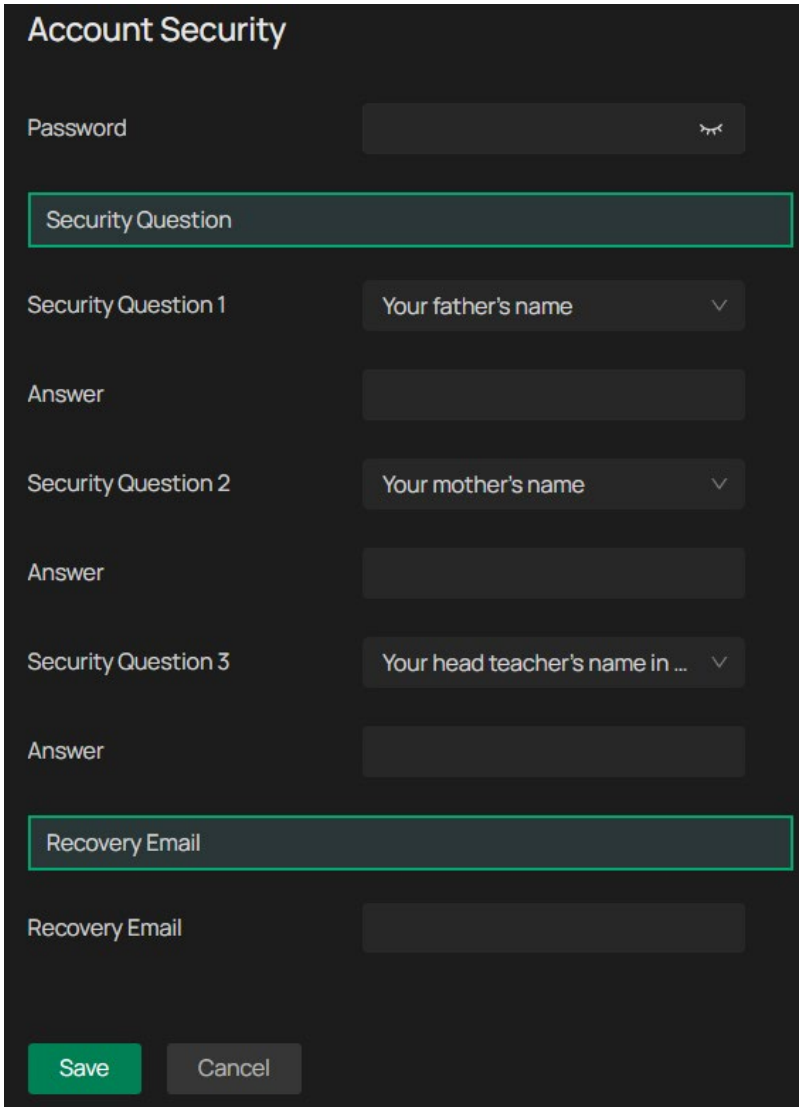
3. (Optional) After adding the role, you can do one or more of the following:

- **Set the permission for the user. Under the Permission List, check the accesses you grant to the user.**
- **Add a remark for the user. Enter your personalized notes in the Remark field.**



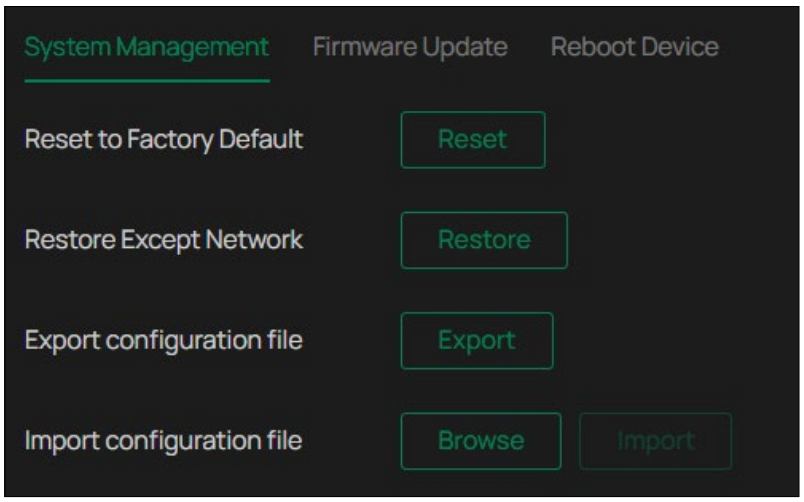
4. Click **Password Protection** for account security settings. You can reset the password by setting the security question or email. You can click **Forget Password** and answer the security question

to reset the admin password when access the device via browser. After setting the email, you can receive the verification code during the recovering operation process.



9. 4 System Management

You can reset the camera to factory default settings, import and export the configuration file of your camera. To configure these settings, go to **Settings** > **System Settings** > **System Management** > **System Management**.



To reset all the parameters to the factory default, click **Reset**.

To reset device parameters, excluding network settings, to the factory default, click **Restore**.

Note: After you click Restore, the port number you set in Network Settings will change.

To export the configuration file, click **Export**.

To import the configuration file, click **Browse** to select your file, then click **Import**.

9. 5 Update Firmware

TP-Link aims at providing better network experience for users. We will inform you through the web management page if there's any update firmware available for your camera. Also, the latest firmware will be released at the official website **www.omadanetworks.com**, and you can download it for free.

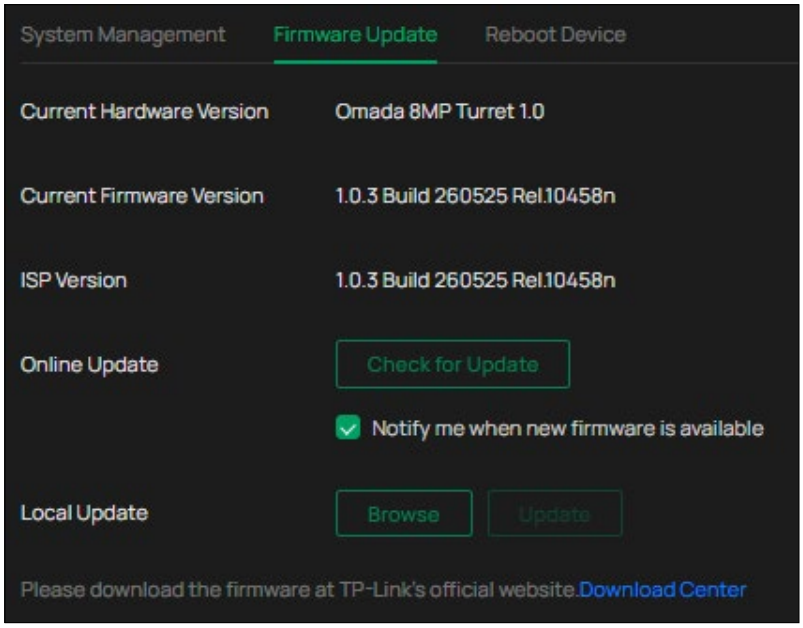
Note:

1. Backup your camera configuration before firmware upgrade.
2. Do NOT power off the camera during the firmware upgrade.

9. 5. 1 Online Update

1. Go to **Settings** > **System Settings** > **System Management** > **Firmware Update**.

2. Click **Check for Update** to see whether the latest firmware is released.



3. Navigate to the **Online Update** section, and click **Update** if there is new firmware.
4. Wait a few minutes for the update and reboot to complete.

9. 5. 2 Local Update

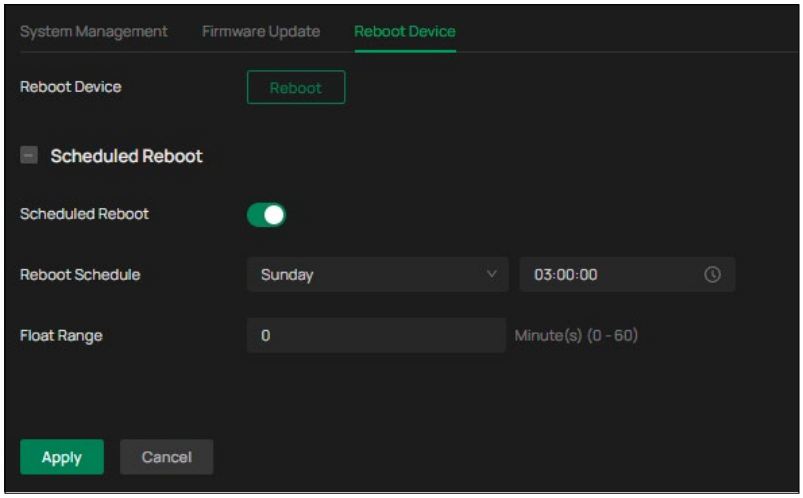
1. Download the latest firmware file for the camera from **www.omadanetworks.com**.
2. Go to **Settings** > **System Settings** >**System Management** > **Upgrade Firmware**.
3. Click **Browse** to locate the downloaded new firmware file, and click **Update**.
4. Wait a few minutes for the update and reboot to complete.

9. 6 Reboot Device Regularly

The Scheduled Reboot feature cleans the cache to enhance the running performance of the camera.

1. Go to **Settings** > **System Settings** > **System Management** > **Reboot Device**.
2. Enable **Scheduled Reboot**.
3. Select the day and time and specify the Float Range. When the float range is set to 0, the camera will reboot at exactly the time you set in the Reboot Schedule. You may select 1 to 60 minutes. Then your camera will reboot some time before or after the time you set in the Reboot Schedule.

4. Click Save.



Note: You can click the Reboot button to reboot the camera immediately.

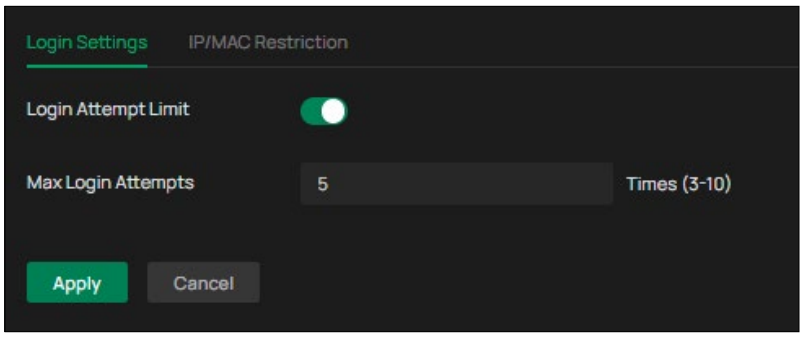
9. 7 Configure Security

In the Security module, you can configure the login settings to control the login attempts and configure the IP/MAC restriction to control the access to the camera.

9. 7. 1 Login Settings

Set the maximum login attempts to protect the security of your camera. The camera will be locked for 30 minutes if you enter the wrong password more than the specified attempts.

1. Go to Settings > System Settings > Security > Login Settings.
2. Enable Login Attempt Limit and set the maximum login attempts. The number should between 3 and 10.

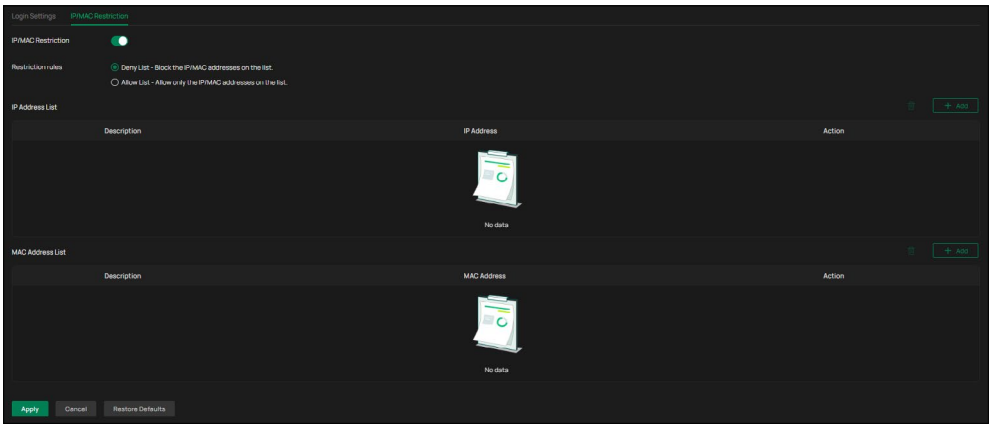


3. Click Apply.

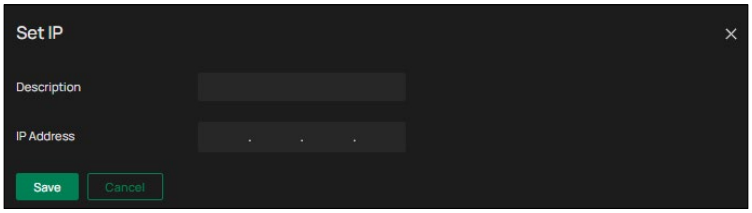
9. 7. 2 IP/MAC Restriction

You can manage a Deny List or an Allow List to control which devices are permitted to access the camera. This function supports filtering by both IP Address and MAC Address.

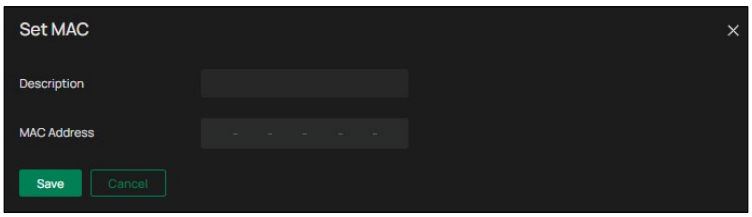
1. Go to **Settings** > **System Settings** > **Security** > **IP/MAC Restriction**.
2. Enable **IP/MAC Restriction** and specify the restriction rule. If you select **Deny List**, the devices with the IP/MAC addresses specified in the table will not be able to access the camera. If you select **Allow List**, only the devices with the IP/MAC addresses specified in the table can access the camera.



3. Click **Add** to add the desired IP address, give a description to identify this IP address, and click **Save**.



4. Click **Add** to add the desired MAC address, give a description to identify this MAC address, and click **Save**.



5. Click **Apply**.