User Guide

Wired Camera Web Interface

This guide uses the InSight S345ZI web page for demonstration.
Features and pictures may differ from your actual product.

© 2025 TP-Link 1900001120 REV1.0.2

Contents

About This Guide 1

Login 2

1. 1 Connect the Camera to Network 3

1. 2 Log in to the Web Interface 3

Live View 6

View Device Information 9

3. 1 View System Logs 10

3. 2 View Device Information 11

Change Camera Settings 12

4. 1 Camera Display Settings 13

4. 1. 1 Image Settings 13

4. 1. 2 OSD Settings 17

4. 1. 3 Privacy Mask 18

4. 2 Camera Stream Settings 19

4. 2. 1 Video Settings 19

4. 2. 2 Audio Settings (Only for some models) 20

4. 2. 3 ROI 21

4. 2. 4 Advanced Settings 21

Events 24

5. 1 Arming Schedule and Linkage Method 25

5. 2 Motion Detection 26

5. 3 Camera Tampering 27

5. 4 Scene Change Detection 28

5. 5 Line Crossing Detection 29

5. 6 Intrusion Detection 31

5. 7 Region Entering Detection 33

5. 8 Region Exiting Detection 35

5. 9 Loitering Detection 37

5. 10 Object Abandoned/Removal Detection 39

5. 11 Abnormal Sound Detection 41
5. 12 Vehicle Detection 41
5. 13 Human Detection 42
5. 14 LPR 43
5. 15 Exception Event 44
5. 16 Smart Frame 45
5. 17 Light Alarm (Only for some models) 45
5. 18 Sound Alarm (Only for some models) 46
5. 19 Alarm Server 46
5. 20 Alarm Input 47
5. 21 Alarm Output 48

Recording and Storage 49
6. 1 Recording Schedule 50
6. 2 Storage Management 51

Network Management 53
7. 1 Internet Connection 54
7. 2 Port 55
7. 3 Platform Access 56
7. 4 Email 57
7. 5 Port Forwarding 57
7. 6 IP Restriction 58
7. 7 Multicast 59
7. 8 Server 60
7. 9 Upload 61
7. 10 ONVIF 62
7. 11 SNMP 62
7. 12 DDNS 63

Cloud Service 65

System Settings 67
9. 1 Configure Basic Settings 68
9. 2 Modify System Time 68
9. 3 Manage User Accounts 68
9. 4 System Management 71
9. 5 Upgrade Firmware 72

9. 5. 1 Online Upgrade 72
9. 5. 2 Local Upgrade 72
9. 6 Reboot Device Regularly 73

About This Guide

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

Conventions

When using this guide, notice that:

- Features available in VIGI 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://www.vigi.com/us/support.
- The Quick Installation Guide can be found where you find this guide or inside the package of the product.
- To ask questions, find answers, and communicate with TP-Link users or engineers, please visit https://community.tp-link.com to join TP-Link Community.

1

Login

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

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

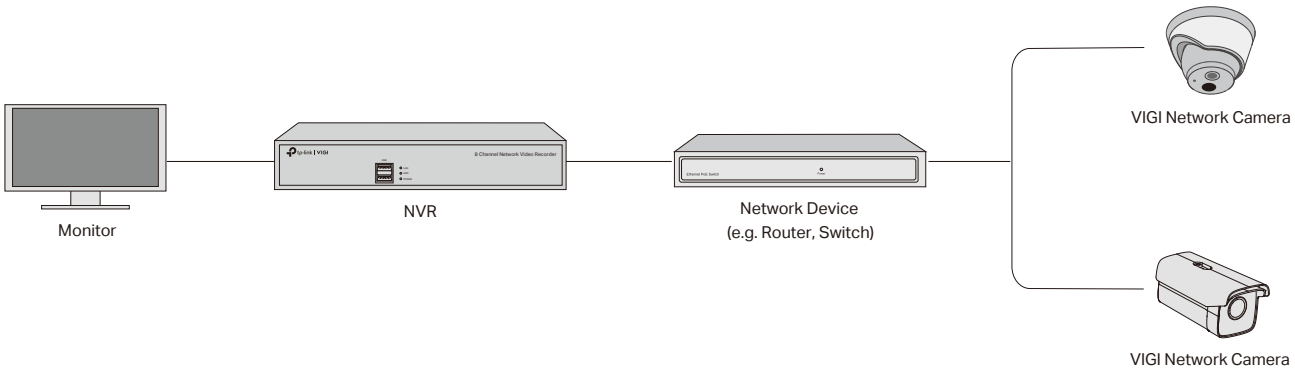
After the cameras are added to network, multiple methods are provided for you to monitor and manage cameras. You can manage and monitor the cameras remotely via the VIGI app, and you can also directly monitor and manage your camera via a web browser. Check the support page of the product for more manuals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

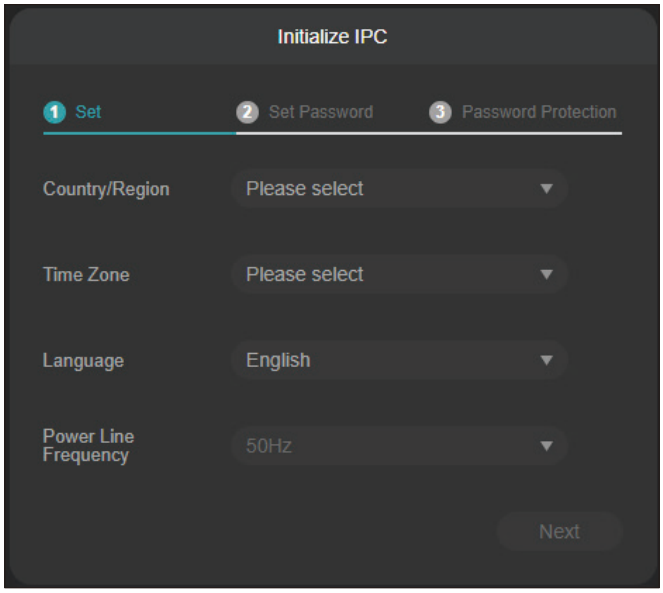


1. 2 Log in to the Web Interface

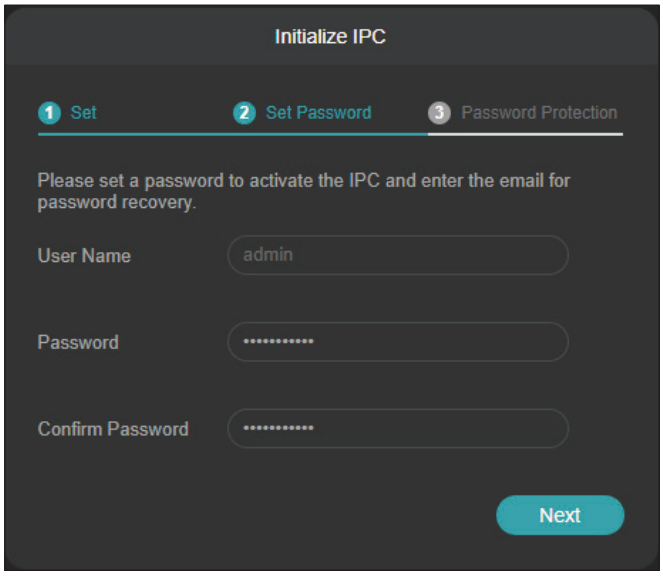
With an intuitive user interface, it is easy to configure and manage the camera via a web browser. Follow the steps below to log in to the web UI of the camera for the first time.

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. Select your **Country/Region** and **Time Zone**.



4. Set a password to activate the camera. Click **Next**.

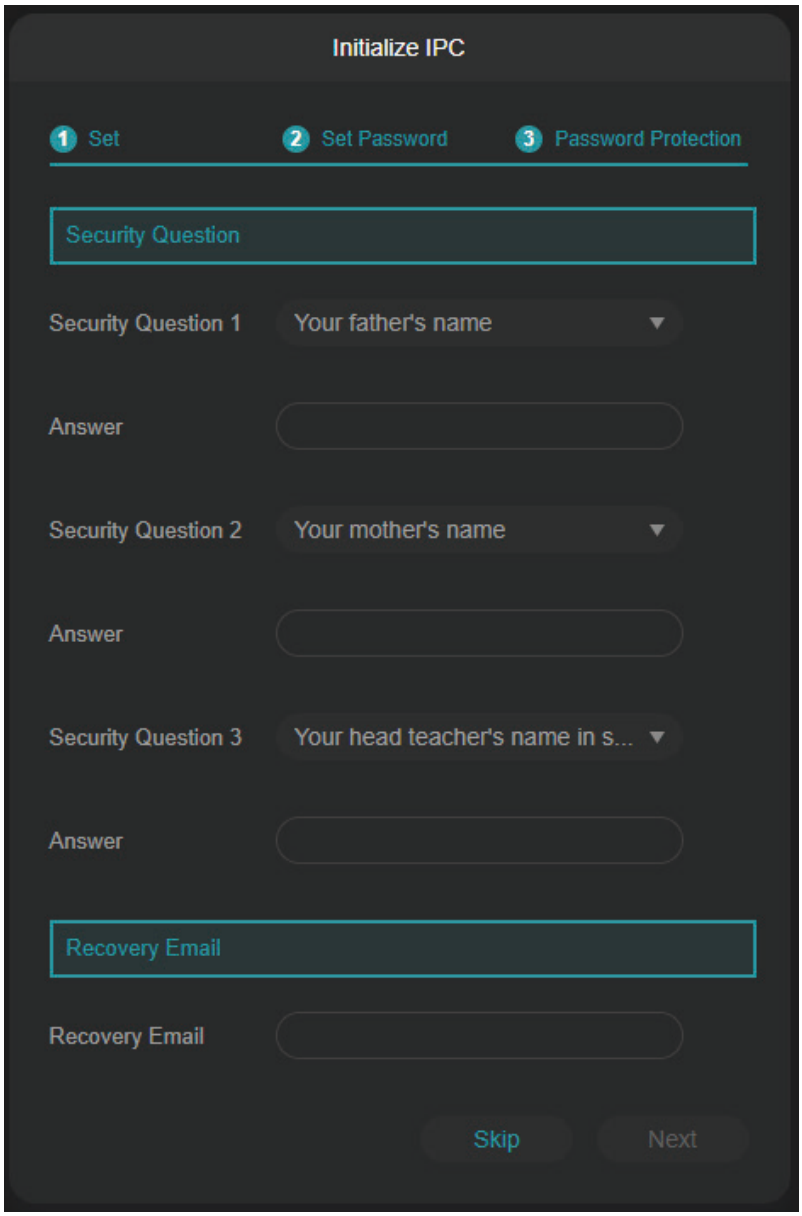


Now, you can log in to the camera using the password set here.

5. Set Password Protection. If you forget password, you can reset it with your security questions or recovery email.

   Select your security questions and input your answer.

Enter your email address to receive the verification code during the recovery operation process.



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

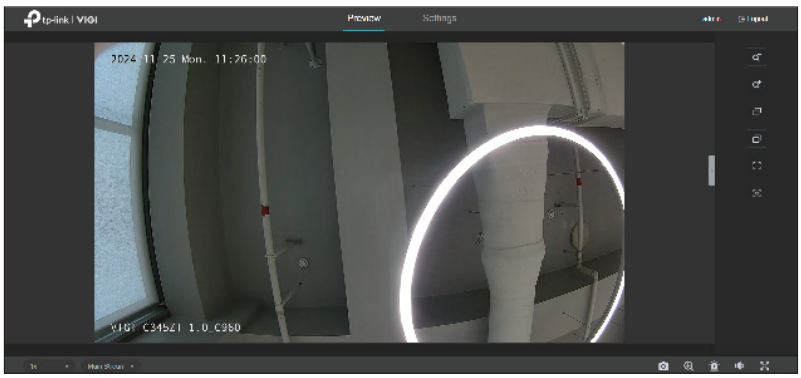
Live View

You can monitor the camera in real time and respond to abnormal conditions with quick operations, such as zooming in the image and capturing screenshots.

This chapter introduces the live view parameters and function icons.

1. Find the camera's IP address on your gateway'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. Log in with the default username admin and the password you set for this camera.
4. You can view the live video on the Preview page.

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.
Main Stream	Click to change the stream type. **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
	Screenshot: Click to capture a screenshot.
	Digital Zoom: Click to see more details of any area in the image.
	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.
	Zoom Out: Click to zoom out the live image.
	Zoom In: Click to zoom in the live image.
	Focus -: Shorten the focal length.
	Focus +: Increase the focal length.
	Lens Initialization: (Only for the camera with motorized lens) Click to reset lens when long time zoom or focus results in blurred image.
	Auxiliary Focus: (Only for the camera with motorized lens) Click to focus automatically.

3

View Device Information

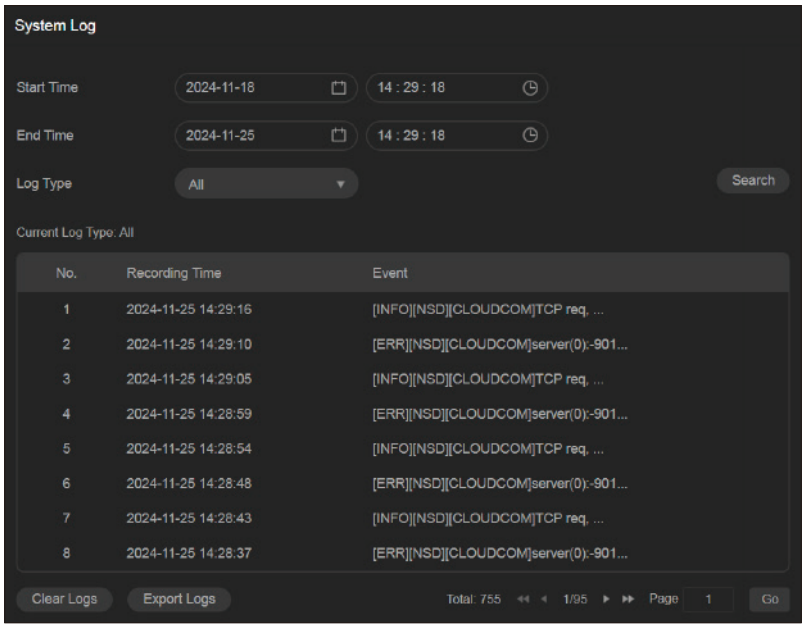
This chapter introduces how to check the system logs and view your device information on the web UI. This chapter contains the following sections:

- View System Logs
- View Device Information

3. 1 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.

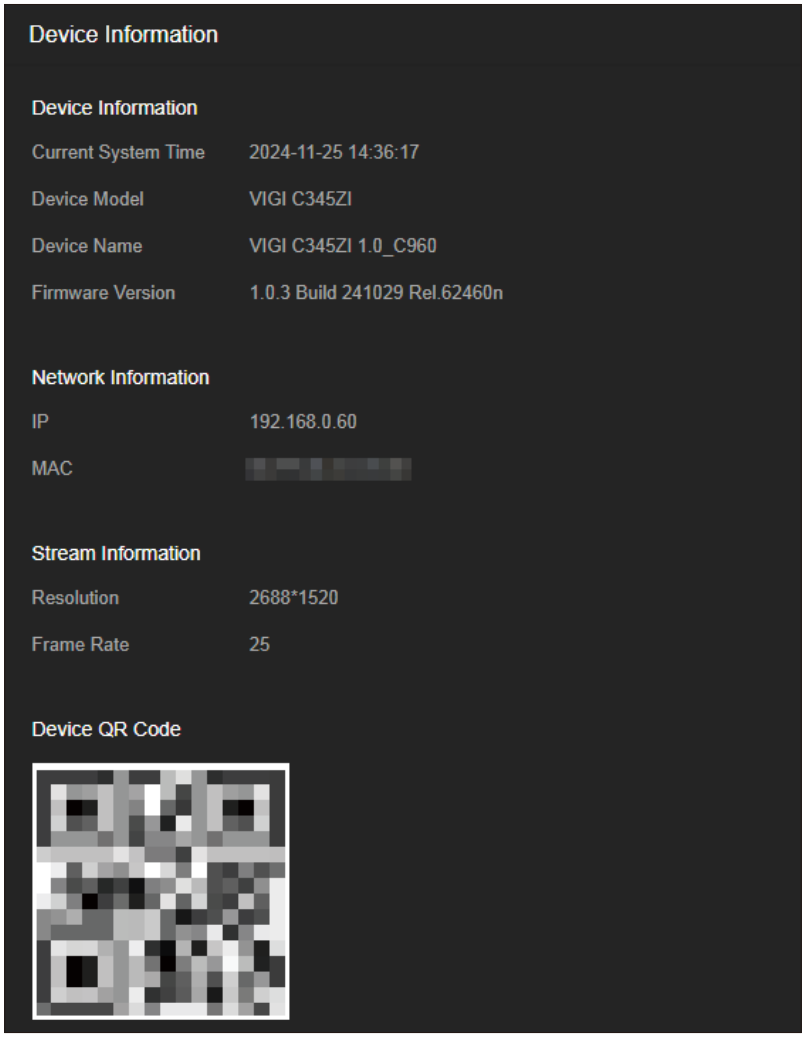


Start/End Time	Specify a time range to filter the logs based on the recording time.
Log Type	Select a type from the drop-down list to filter the logs. All: All types of logs. Alarm: Alarms triggered by events, such as tampering, line crossing, and area intrusion. Exception: Abnormal events that may influence 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.

3. 2 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.



4

Change Camera Settings

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

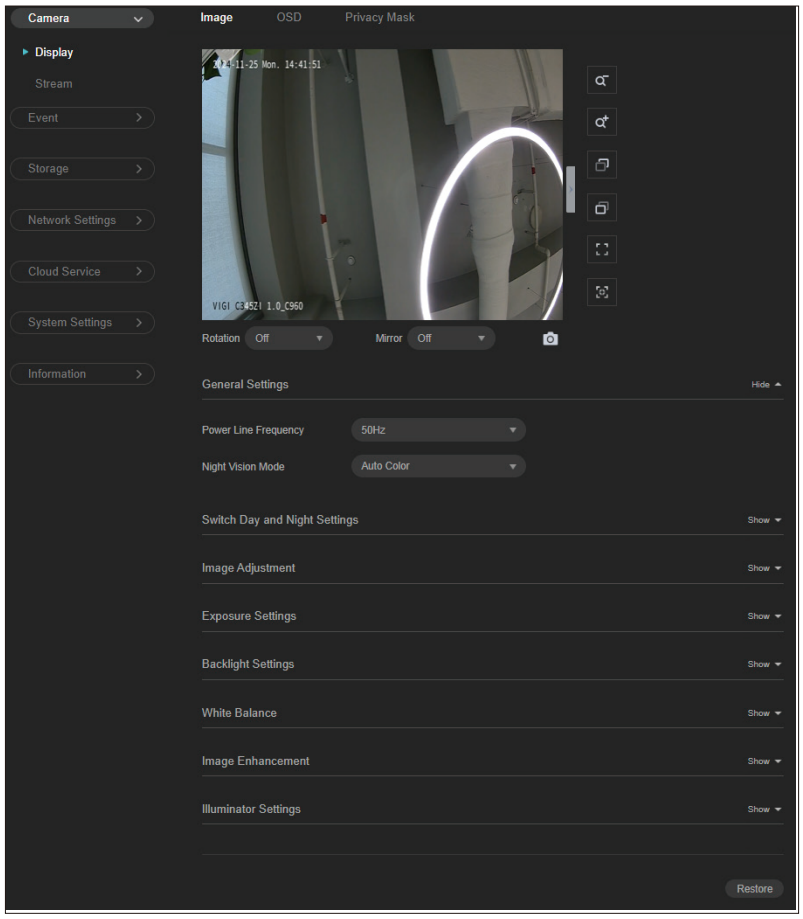
- Camera Display Settings
- Camera Stream Settings

4. 1 Camera Display Settings

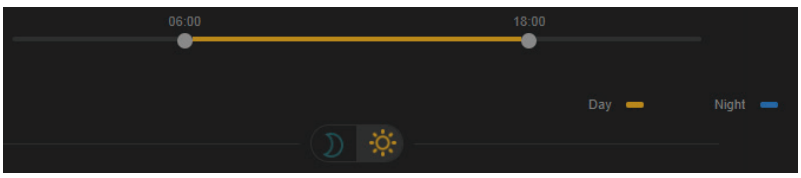
You can adjust image features according to your needs.

4. 1. 1 Image Settings

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



Rotation	Choose to turn the live view image by 0, 90 or 270 degrees on your display. When you select **Off**, the image displays normally.
Mirror	Select the mirror mode as needed. When you select **Off**, the image displays normally. By choosing **Left-Right**, you mirror the image on the vertical axis. By choosing **Up-Down**, you flip the image on the horizontal axis. By choosing **Central**, you 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. **Custom**: Select it to configure **Day/Night Switch** and **Illuminator**.
Switch Day and Night Settings	
Day/Night Switch	Select a method to switch the image settings of day and night. **Unified**: The camera applies the same image settings throughout a day. **Scheduled**: The camera switches the image mode of day and night at your specified time. If you select this method, adjust the slide bar to specify the switch time.  **Auto**: The camera switches the image mode of day and night automatically according to the light condition of the environment.
Image Adjustment	
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.

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 brigher images. **Anti-flicker**: This function minimizes influences caused by flickering.
Backlight Settings	
BLC Area	BLC (Backlight Compensation) optimises 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.
HLC	HLC (Highlight compensation) can compensate for brighter parts of your image, maintaining detail in brighter parts of the image that would otherwise be blown out.
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 may specify the red/blue gain values separately. The higher the value is, the more intense the red/blue color is.

Image Enhancement	
Prevent overexposure to infrared light	Select the standard mode or enhanced mode or manually adjust the brightness of image. **Standard Mode**: In this mode, the brightness of the infrared light will be automatically adjusted to prevent overexposure. The brigher the environment, the dimmer the infrared supplement light. **Enhanced Mode**: This mode intensifies its protection against overexposure, by darking the bright areas of the image. **Manual:** Manually adjust the brightness of image. The higher the value is, the dimmer the image gets.
Illuminator Settings	
Illuminator	Select a mode to decide the usage of white supplement light. The available options vary due to the mode set in **Night Vision Mode** and **Day/Night Switch**. **Auto**: The camera turns on the white light once it detects the environment gets dark, and keeps the light off in a sufficiently lit environment. You can customize the values in **Sensitivity** and **Delayed Switch**. **Scheduled**: Specify the time to turn on and off the white light. **Always On/Off**: The white light is on/off all the time.
Sensitivity	Decide the ambient light intensity that can trigger the switch of the white light. The lower the value is, the easier it is to trigger the white light.
Delayed Switch	Decide how long the camera waits to turn on or off the white light when the ambient light reaches the threshold to trigger the switch..
Lighting Mode	**Infrared Lighting**: The infrared supplement light is on all the time. **Human/Vehicle Trigger Full-Color**: The camera turns on the full-color mode once it detects a person or vehicle. **White Light Illumination**: The white supplement light is on all the time. With this selected, you may customize **White Light Intensity** parameters.
White Light Intensity	**Smart White Light-Standard**: The camera illuminate a white light when detecting a target. **Smart White Light-Soft**: The camera illuminates a warmer white light when detecting a target. **Manual:** Drag the slide bar to manually adjust the intensity of the white light. The light gets brighter when the value increases.

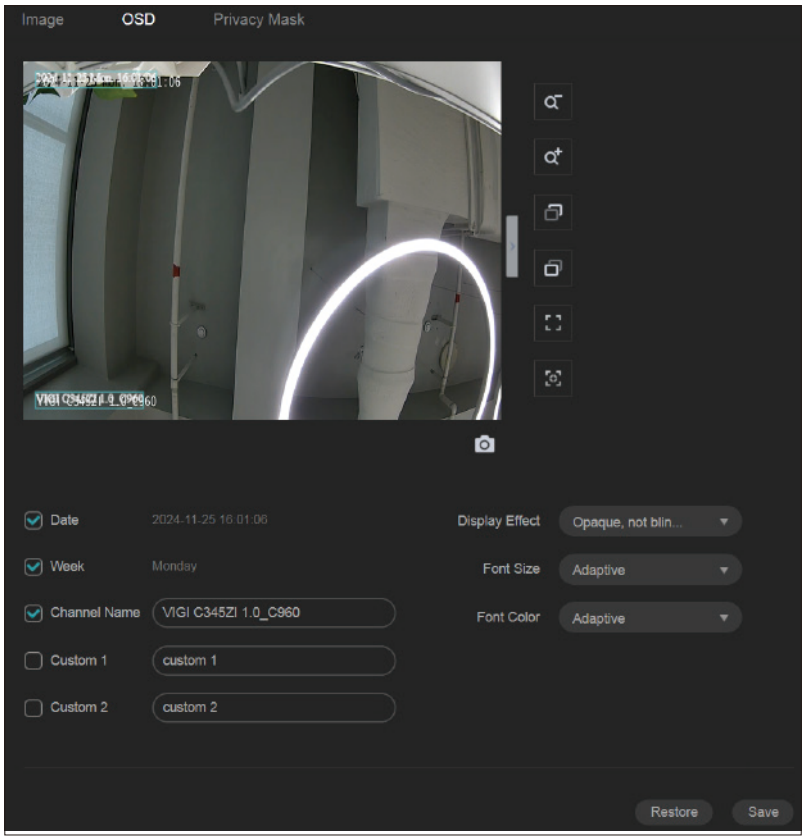
Always Full-Color at Live View	The camera will automatically turn on Full-Color Night Vision when you stream Live Video.
Restore	Click to restore to factory default settings.

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 **Save** to save your settings.



Date	Check to display the date on the image.
Week	Check to display the week on the image.
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 display effect of the image.

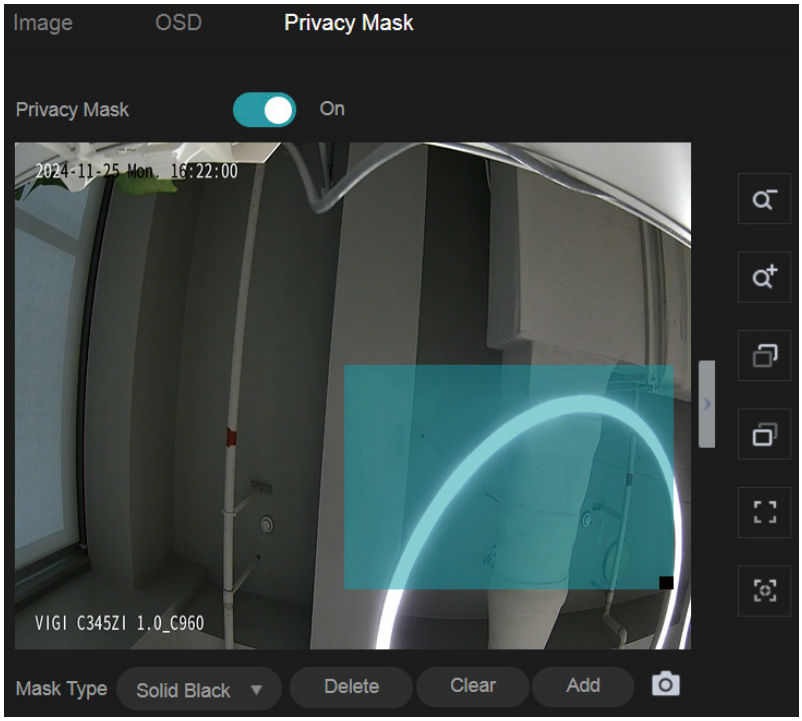
Font Size	Set the font size.
Font Color	Set the font color.
Restore	Click to restore to factory default settings.

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 **Add** to automatically add an area on the center of the screen.
6. Click **Save**.

4. 2 Camera Stream Settings

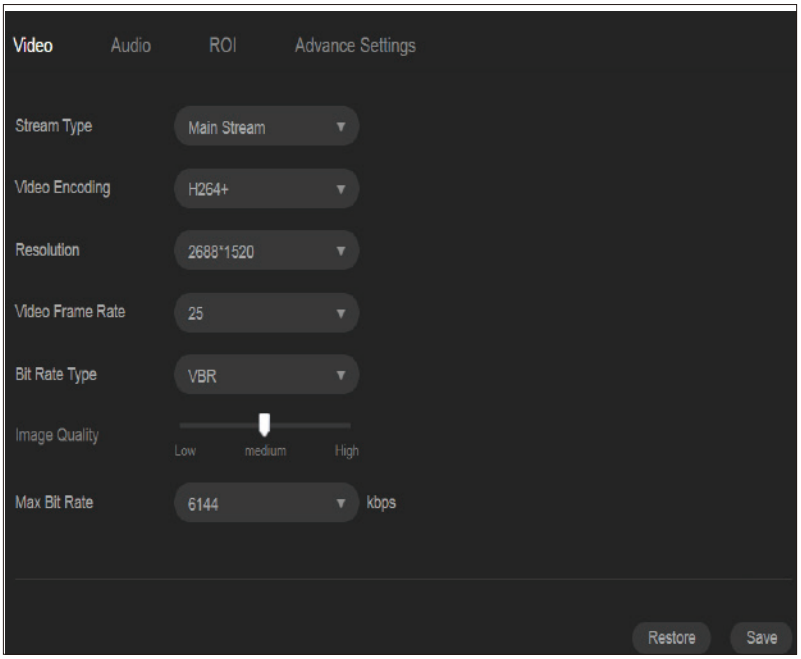
In Stream Settings, you can configure video stream levels, change the audio output settings and ROI (Region of interest) level.

Video stream levels decide the video quality in Live View and recording, and you can adjust the video quality of certain area by specifying the ROI level.

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 **Save**.



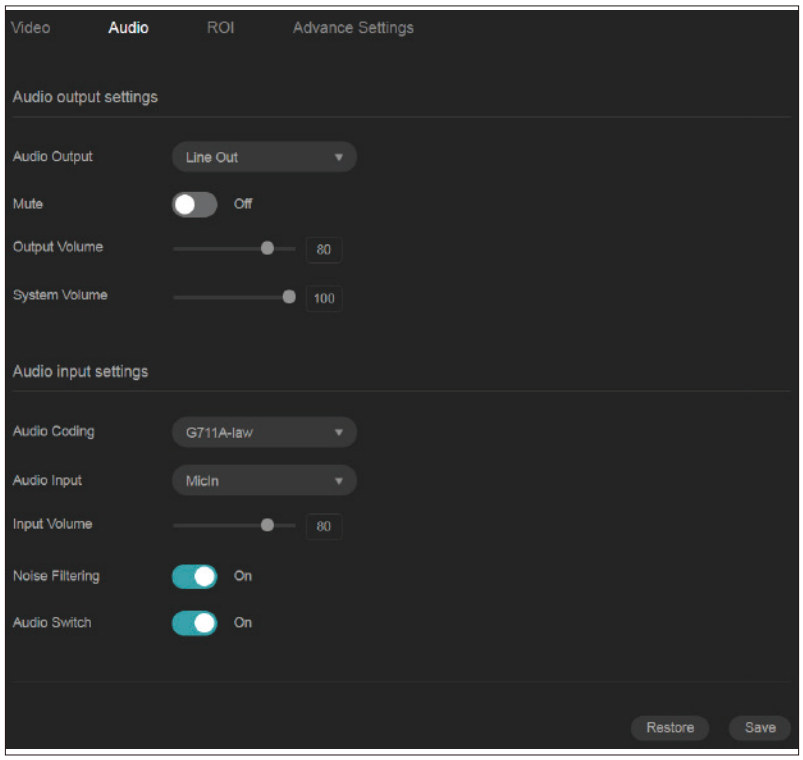
Stream Type	Main Stream is the primary video feed used for recording and provides the highest video quality. It has higher definition and higher bandwidth than substream. Substream is a secondary video feed that is used mainly for remote viewing from computers from outside the network.
Video Encoding	Select the encoding type of the stream. H.265 reduces the file size and saves the bandwidth better than H.264.
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	VBR: The bit rate changes with the image within Maximum Bit Rate. CBR: The bit rate is Maximum Bit Rate all the time.
Image Quality	When VBR selected as the bit rate type, set the video quality as high, medium, or low.
Max Bit Rate	When VBR selected as the bit rate type, specify the upper limit of bit rate. When CBR selected as the bit rate type, specify the bit rate.
Restore	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 **Save**.



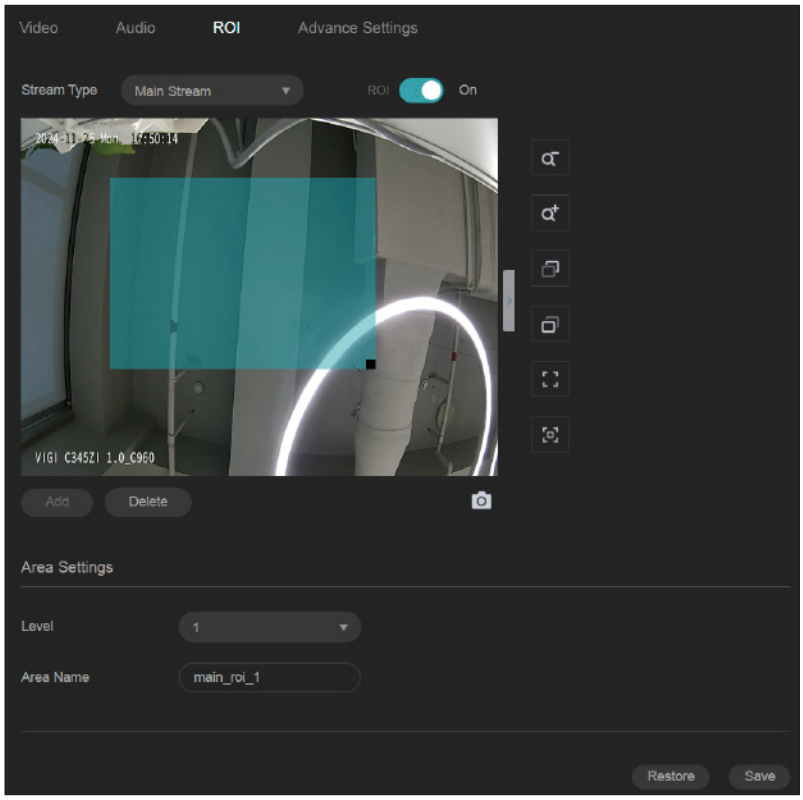
Mute	Toggle to mute the speaker of the camera.
Output Volume	Adjust the volume of the speaker.
System Volume	Adjust the volume of the sound alarm.

Audio Coding	Select the encoding type of the audio.
Audio Input	Select audio input device.
Input Volume	Adjust the volume of the input device.
Noise Filtering	Enable noise filtering to remove the noise from the video.
Audio Switch	Turn on the microphone.
Restore	Click to restore to factory default settings.

4. 2. 3 ROI

ROI (region of interest) concentrates on delivering high quality video from interested region. In ROI, you can configure the interest level of a specified area in each channel. The level 1–6 is ranked from low to high. The higher the ROI level, the better image quality.

1. Go to **Settings** > **Camera** > **Stream** > **ROI**.
2. Select the stream type and enable ROI. Draw an area on the preview screen (the blue square in the picture below). Drag to adjust its size and location. Specify the ROI level and click **Save**.



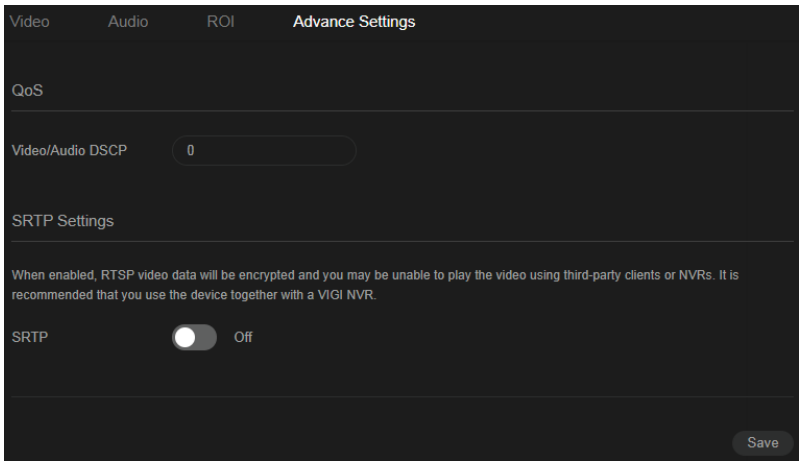
4. 2. 4 Advanced Settings

In Advanced Settings, you can set QoS and SRTP.

QoS (Quality of Service) can help improve the network delay and network congestion by setting the priority of data sending.

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.

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



2. Set Video/Audio DSCP.

   Network can identify the priority of data transmission. The bigger the DSCP value is, the higher the priority is.

3. 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 a VIGI NVR.

4. Click **Save**.

5

Events

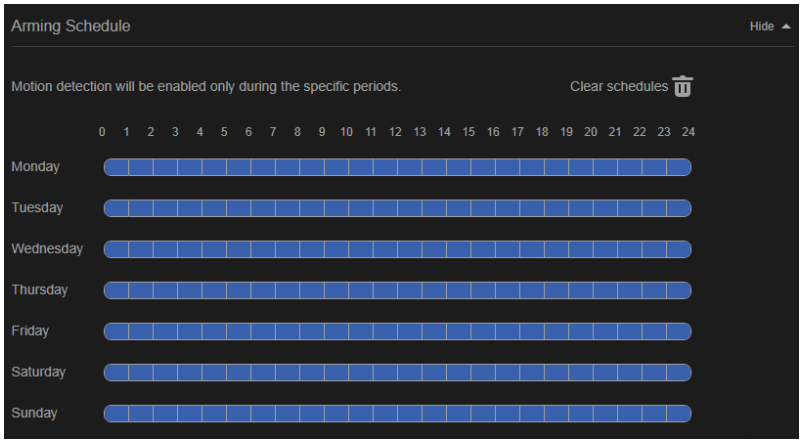
This chapter guides you on how to configure the event settings and alarm actions when your cameras detect different types of events. VIGI camera monitors your pre-defined areas and you'll be automatically alerted to any suspicious activity in your home and office. This chapter includes the following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

- Arming Schedule and Linkage Method
- Motion Detection
- Camera Tampering
- Scene Change Detection
- Line Crossing Detection
- Intrusion Detection
- Region Entering Detection
- Region Exiting Detection
- Loitering Detection
- Object Abandoned/Removal Detection
- Abnormal Sound Detection
- Vehicle Detection
- Human Detection
- LPR
- Exception Event
- Smart Frame
- Light Alarm (Only for some models)
- Sound Alarm (Only for some models)
- Alarm Server
- Alarm Input
- Alarm Output

5. 1 Arming Schedule and Linkage Method

Arming schedule is a customized time period in which the device performs certain tasks. Linkage is the response to the detected certain incident or target 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.

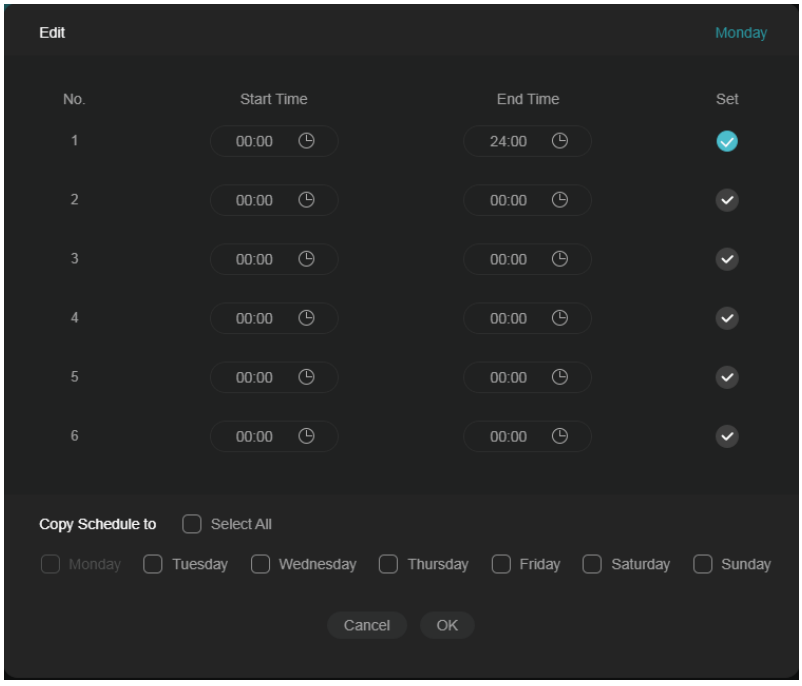


2. Drag the time bar to draw desired valid time.

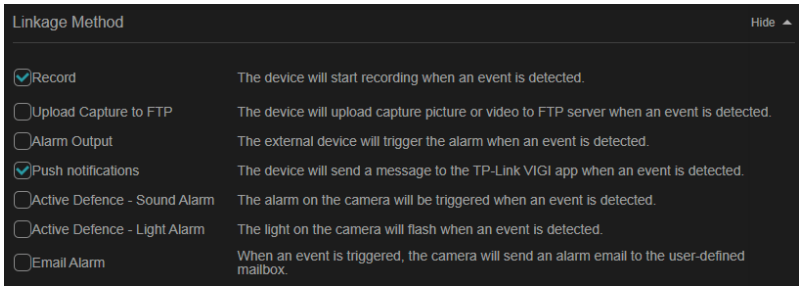
   Note:

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

3. Move your mouse to the right of a day's blocks and an edit button will appear. Click and enter the pop-up window to finetune the Start Time and End Time (with an accuracy of a minute) and check Set. You may copy a schedule for a day to any other days. Click **OK** when you are done.



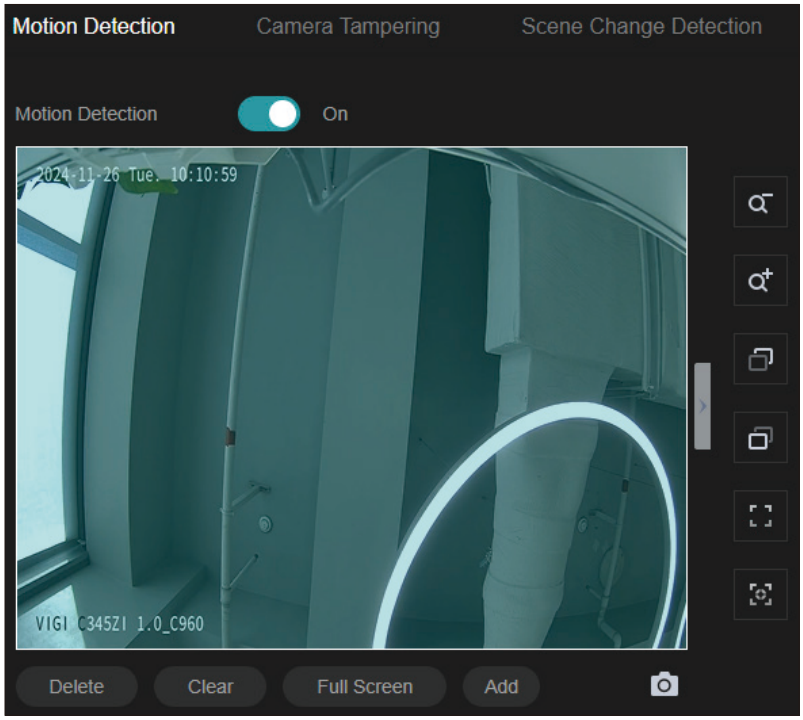
4. Set linkage methods as needed.



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 triggered actions. Follow the steps below to finish the configuration.

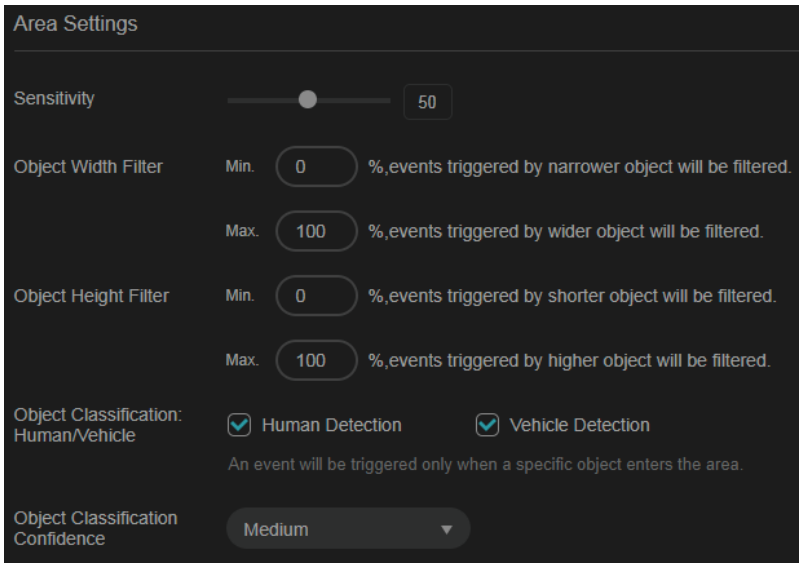
1. Go to Settings > Event > Basic Event > Motion Detection. Click the toggle to turn on Motion Detection.



2. Draw quadrilaterals 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 drage the whole area to move it. You may delete an selected area, clear all areas, expand the selected areas to the full screen, or add another area. Then configure the motion detection settings.

   Note: You may customize up to four areas.

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



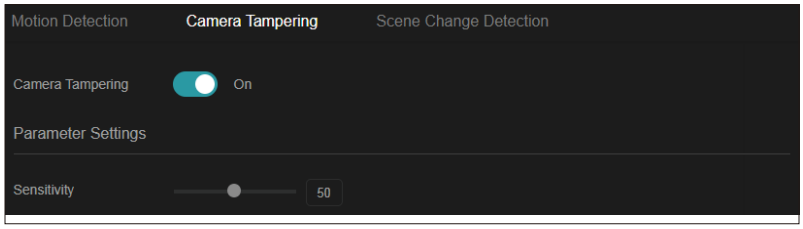
Sensitivity	Adjust the value of sensitivity. The higher the value is, the easier it is to trigger an alarm.
Object Width Filter	Set the minimum and maximum object width to filter the corresponding events.
Object Height Filter	Set the minimum and maximum object height to filter the corresponding events.
Object Classification: Human/Vehicle	Choose whether you want to detect humans only, vehicles only, or both. The function is available only for cameras which support human detection and vehicle detection.
Object Classification Confidence	Select the detection type from High, Medium, and Low. The function is available only for the cameras which support human detection and vehicle detection.

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

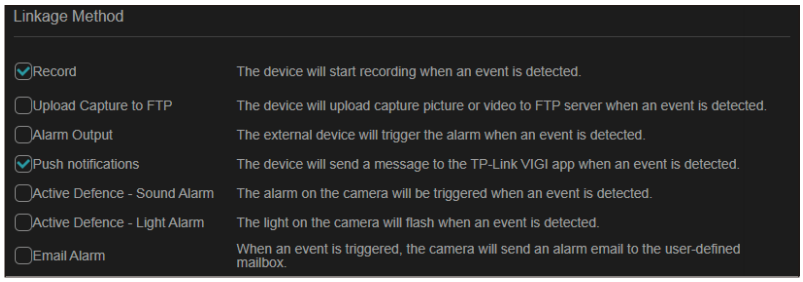
5. 3 Camera Tampering

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

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



2. Enable **Camera Tampering**.
3. Set the sensitivity of video tampering. A higher value can trigger the alarm actions more easily.
4. Set the Linkage Method. Note that the options vary by model.

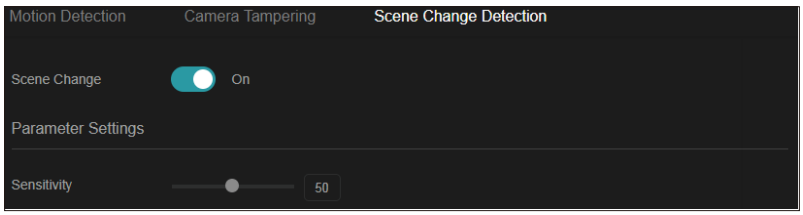


5. Refer to Arming Schedule and Linkage Method for settings if needed.
6. Click **Save**.

5. 4 Scene Change Detection

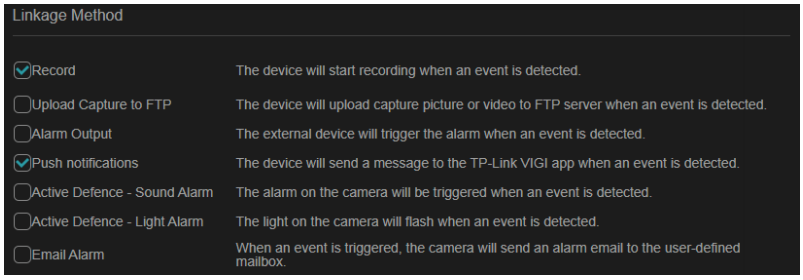
Scene change detection function detects the change of video security environment affected by the external factors, such as intentional rotation of the camera. Certain actions can be taken when the alarm is triggered. Follow the steps below to finish the configuration.

1. Go to **Settings** > **Event** > **Basic Event** > **Scene Change Detection.**
2. Click the toggle to turn on **Scene Change**.



3. Specify **Sensitivity**. The higher the value is, the more easily the change of the scene can be detected.

4. Refer to Arming Schedule and Linkage Method for settings if needed.

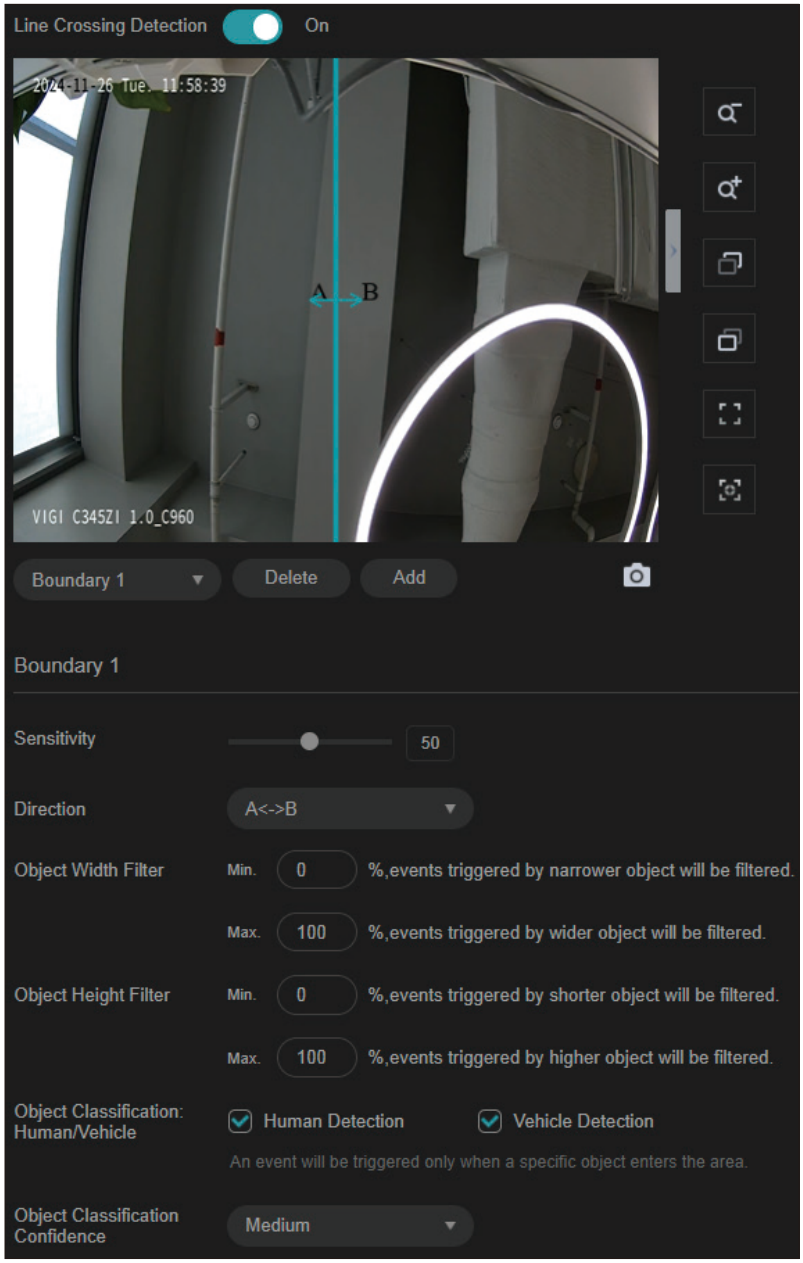


5. Click Save.

5. 5 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 > Smart Event, select Line Crossing Detection from the drop-down list, and click the toggle to turn it on.



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.

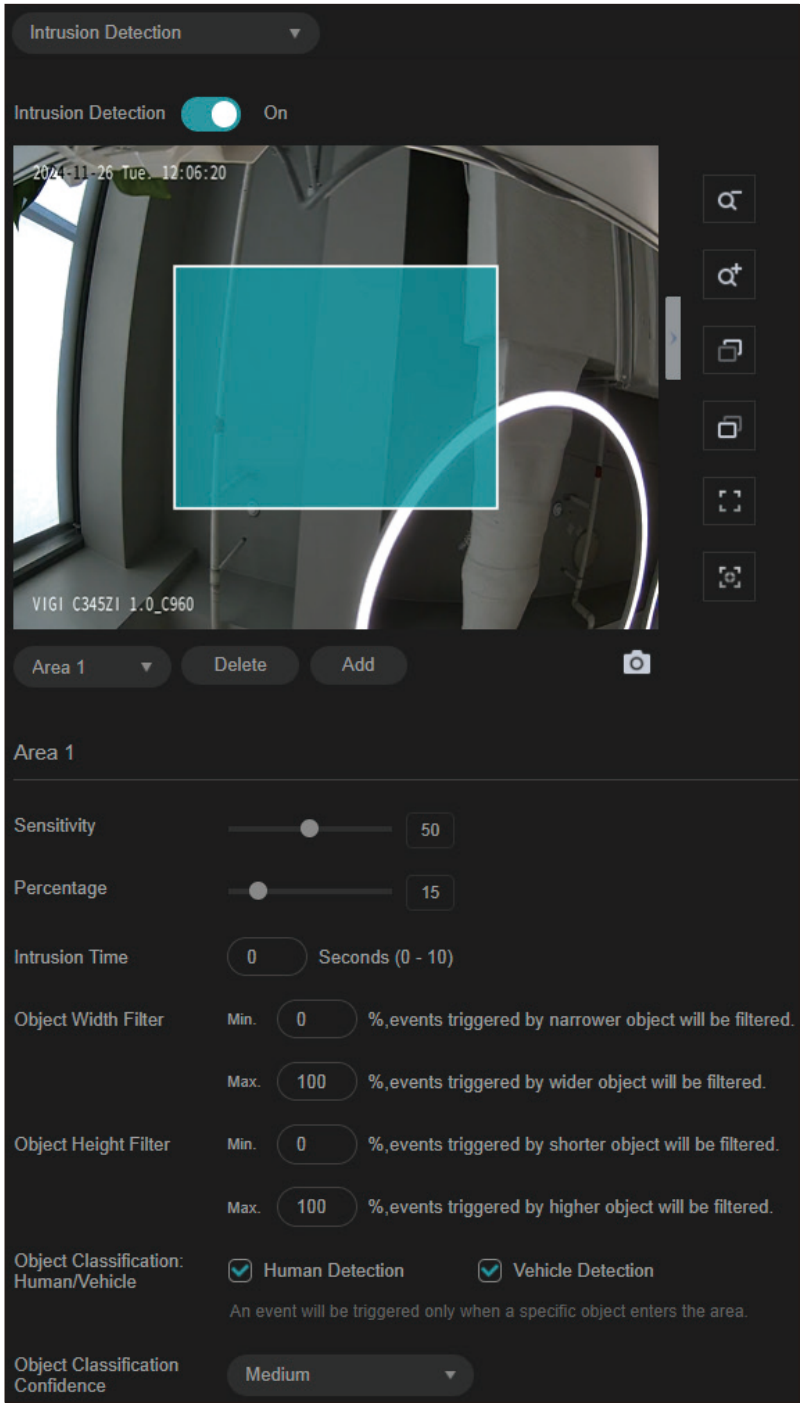
Direction	Choose the direction from which the target crosses the line. A->B: Only the target crossing the configured line from the A side to the B side can be detected. B->A: Only the target crossing the configured line from the B side to the A side can be detected. A<->B: The target going across the line from both sides can be detected and alarms are triggered.
Object Width Filter	Set the minimum and maximum width for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.
Object Height Filter	Set the minimum and maximum height for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.
Object Classification: Human/Vehicle	Choose whether you want to detect humans only, vehicles only, or both. The function is available only for cameras which support human detection and vehicle detection.
Object Classification Confidence	Select the detection type from High, Medium, and Low. The function is available only for the cameras which support human detection and vehicle detection.

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

5. 6 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 actions. Follow the steps below to finish the configuration.

1. Go to Settings > Event > Smart Event, select Intrusion Detection from the drop-down list, and enable it.



2. Draw intrusion areas on the preview screen. Select the area and configure the settings.

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.

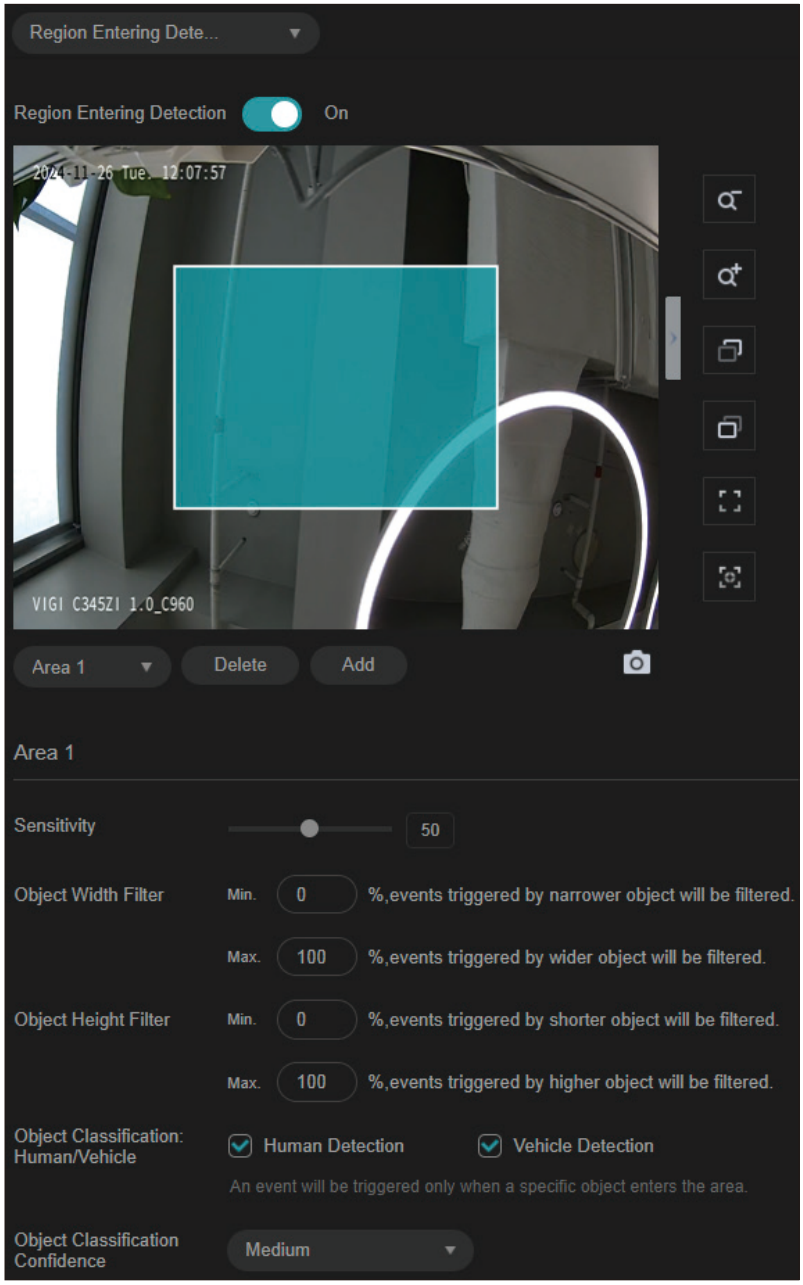
Intrusion Time	Intrustion time stands for the threshold a target loiters in the area. Any stay longer than the intrusion time will trigger the linkage action.
Object Width Filter	Set the minimum and maximum width for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.
Object Height Filter	Set the minimum and maximum height for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.
Object Classification: Human/Vehicle	Choose whether you want to detect humans only, vehicles only, or both. The function is available only for cameras which support human detection and vehicle detection.
Object Classification Confidence	Select the detection type from High, Medium, and Low. The function is available only for the cameras which support human detection and vehicle detection.

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

5. 7 Region Entering Detection

Region entering detection triggers alarm actions when cameras detect moving objects enter the specified regions. You can customize the region settings, select the triggered actions and set the alarm schedule. Follow the steps below to finish the configuration.

1. Go to Settings > Event > Smart Event. Select Region Entering Detection from the drop-down list and enable it.



2. Draw shapes for area entrance detection on the preview screen.

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

Sensitivity	Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.
Object Width Filter	Set the minimum and maximum width for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.
Object Height Filter	Set the minimum and maximum height for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.

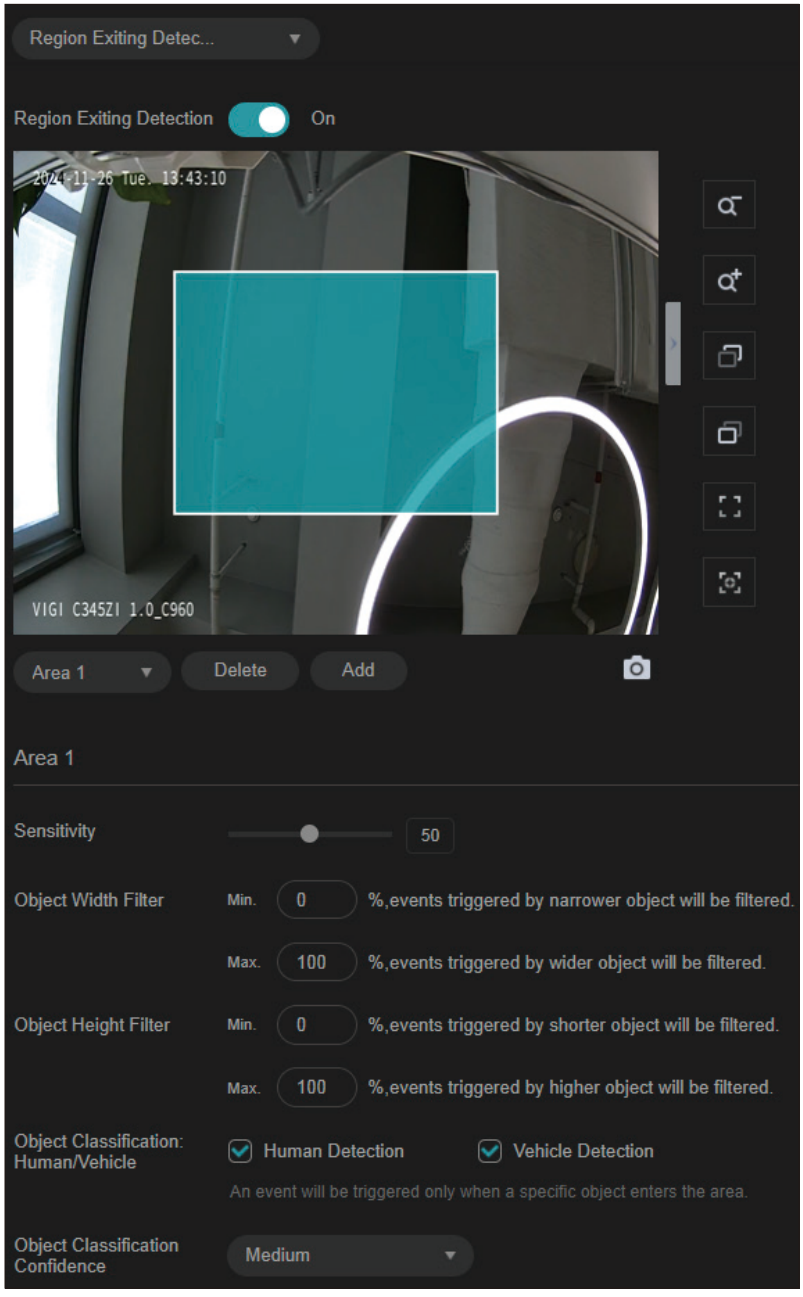
Object Classification: Human/Vehicle	Choose whether you want to detect humans only, vehicles only, or both. The function is available only for cameras which support human detection and vehicle detection.
Object Classification Confidence	Select the detection type from High, Medium, and Low. The function is available only for the cameras which support human detection and vehicle detection.

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

5. 8 Region Exiting Detection

Region exiting detection triggers alarm actions when cameras detect moving objects exit the specified regions. You can customize the region settings, select the triggered actions and set the alarm schedule. Follow the steps below to finish the configuration.

1. Go to **Settings** > **Event** > **Smart Event**, select **Region Exiting Detection** from the drop-down list, and enable it.



2. Draw shapes for area exiting detection on the preview screen.

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

Sensitivity	Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.
Object Width Filter	Set the minimum and maximum width for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.
Object Height Filter	Set the minimum and maximum height for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.

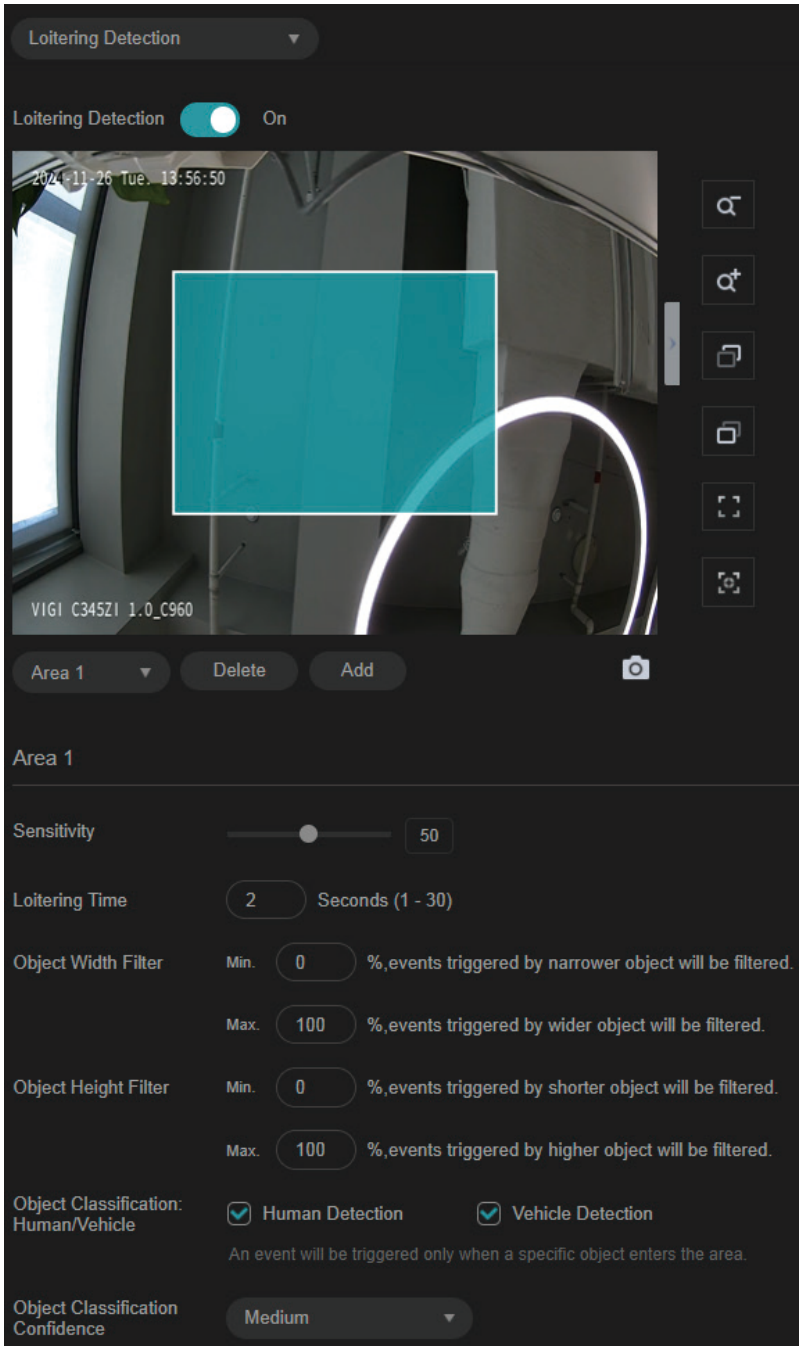
Object Classification: Human/Vehicle	Choose whether you want to detect humans only, vehicles only, or both. The function is available only for cameras which support human detection and vehicle detection.
Object Classification Confidence	Select the detection type from High, Medium, and Low. The function is available only for the cameras which support human detection and vehicle detection.

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

5. 9 Loitering Detection

Loitering detection triggers alarm actions when a moving object remains in a predefined area for a specific amount of time. You can customize the area settings, select the triggered actions and set the alarm schedule. Follow the steps below to finish the configuration.

1. Go to Settings > Event > Smart Event, select Loitering Detection from the drop-down list, and enable it



2. Draw shapes for area exiting detection on the preview screen.

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

Sensitivity	Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.
Loitering Time	It stands for the threshold for the time of the object loitering in the region. If the time that one object stays exceeds the threshold, the alarm is triggered.

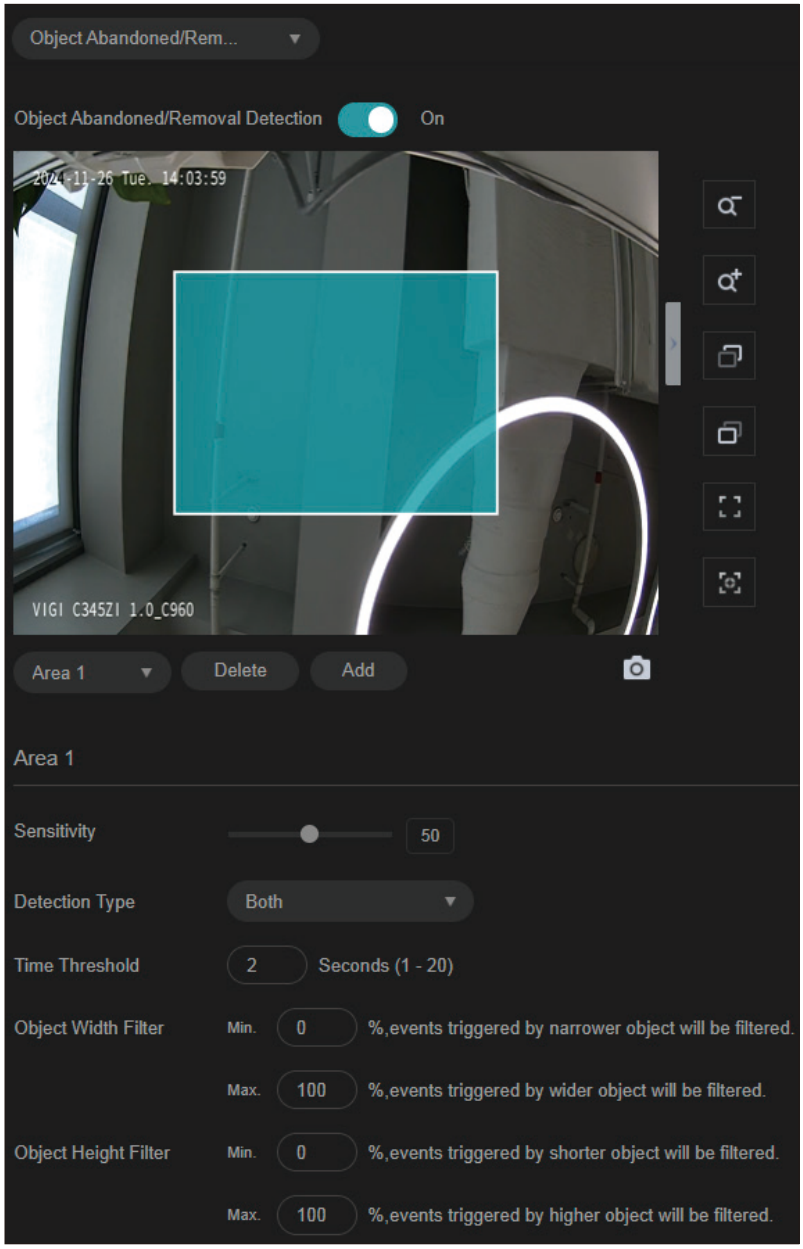
Object Width Filter	Set the minimum and maximum width for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.
Object Height Filter	Set the minimum and maximum height for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.
Object Classification: Human/Vehicle	Choose whether you want to detect humans only, vehicles only, or both. The function is available only for cameras which support human detection and vehicle detection.
Object Classification Confidence	Select the detection type from High, Medium, and Low. The function is available only for the cameras which support human detection and vehicle detection.

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

5. 10 Object Abandoned/Removal Detection

Object abandoned/removal detection triggers alarm actions when cameras detect objects are left behind or taken away in the specified areas. You can customize the area settings, select the triggered actions and set the alarm schedule. Follow the steps below to finish the configuration.

1. Go to **Settings** > **Event** > **Smart Event**, select **Object Abandoned/Removal Detection** from the drop-down list, and enable it.



2. Draw shapes for area exiting detection on the preview screen.

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

Sensitivity	Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.
Detection Type	Select the detection type.
Time Threshold	Set how long the object is left behind or taken away to trigger the event.
Object Width Filter	Set the minimum and maximum width for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.

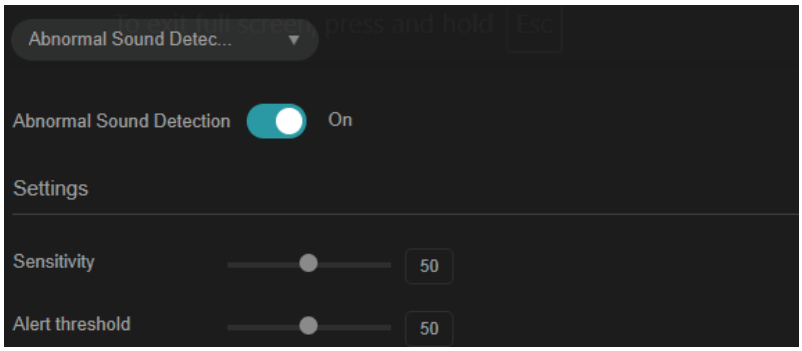
Object Height Filter	Set the minimum and maximum height for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.

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

5. 11 Abnormal Sound Detection

Abnormal sound detection identifies uncommon or irregular sounds and triggers alarm actions. You can select the triggered actions and set the alarm schedule. Follow the steps below to finish the configuration.

1. Go to **Settings** > **Event** > **Smart Event**, select **Abnormal Sound Detection** from the drop-down list, and click the toggle to turn it on.

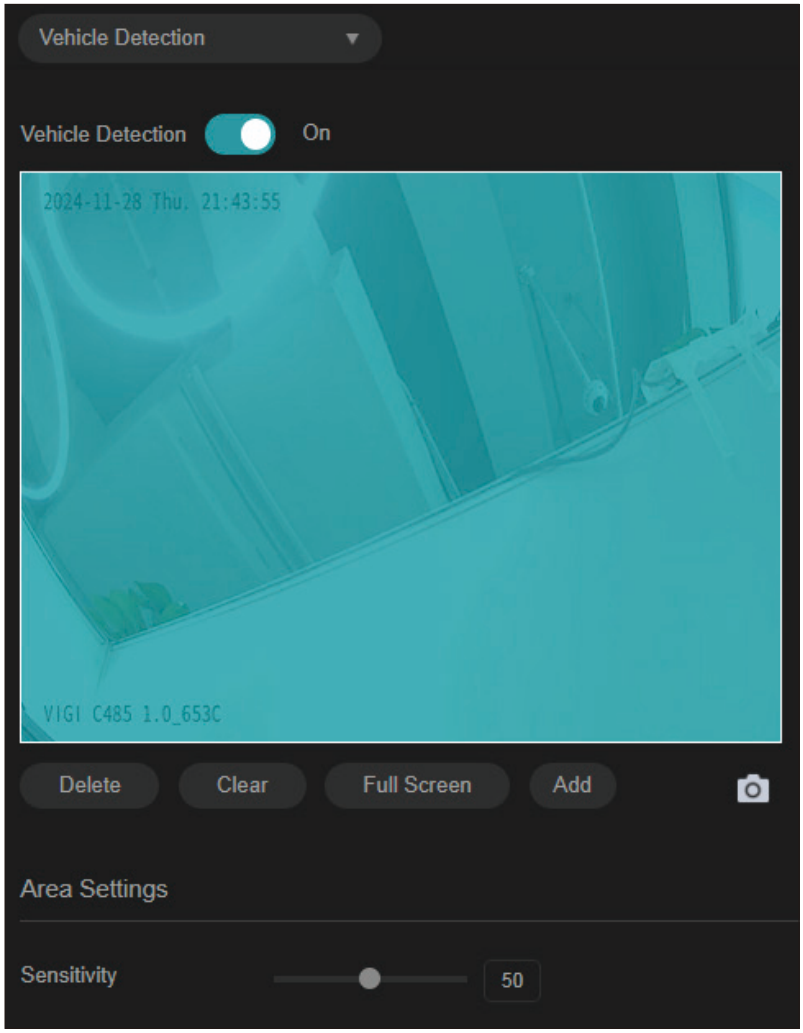


2. Adjust the value of sensitivity and alert threshold. The higher the sensitivity and the lower the threshold, the easier it gets to trigger linkage methods.
3. Refer to Arming Schedule and Linkage Method for settings if needed.
4. Click **Save**.

5. 12 Vehicle Detection

Vehicle detection triggers alarm actions when cameras detect vehicles are moving in the specified areas. You can customize the area settings, select the triggered actions and set the alarm schedule. Follow the steps below to finish the configuration.

1. Go to **Settings** > **Event** > **Smart Event**, select **Vehicle Detection** from the drop-down list, and click the toggle to turn it on.



2. Draw shapes for area exiting detection on the preview screen.

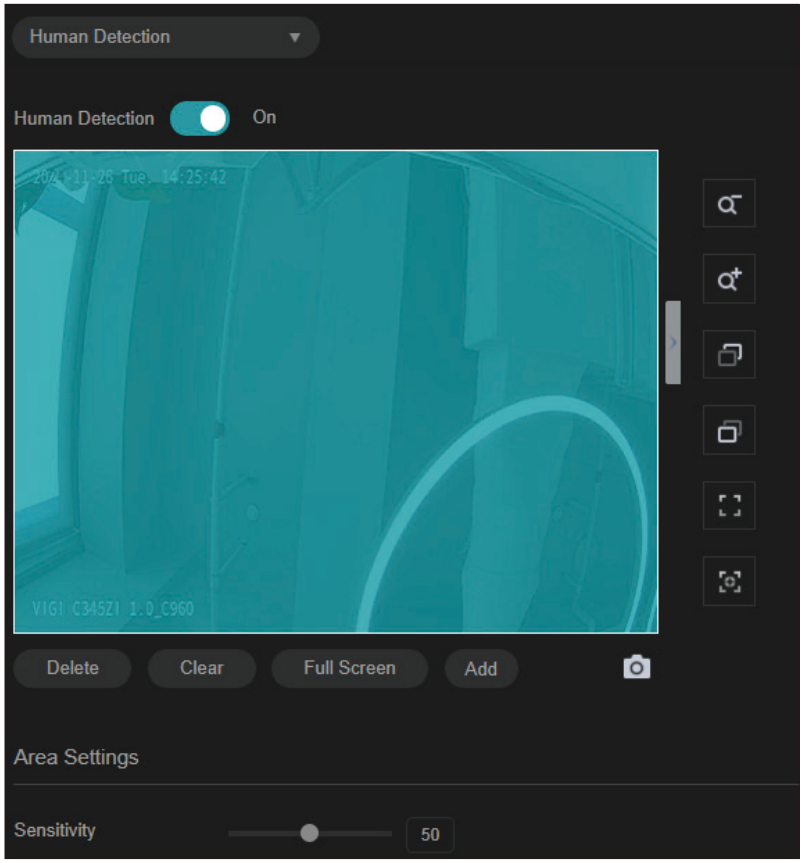
   Note: You may draw up to four areas.

3. Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.
4. Refer to Arming Schedule and Linkage Method for settings if needed.
5. Click **Save**.

5. 13 Human Detection

Human detection triggers alarm actions when cameras detect persons are moving in the specified areas. You can customize the area settings, select the triggered actions and set the alarm schedule. Follow the steps below to finish the configuration.

1. Go to **Settings** > **Event** > **Smart Event**, select **Human Detection** from the drop-down list, and click the toggle to turn it on.

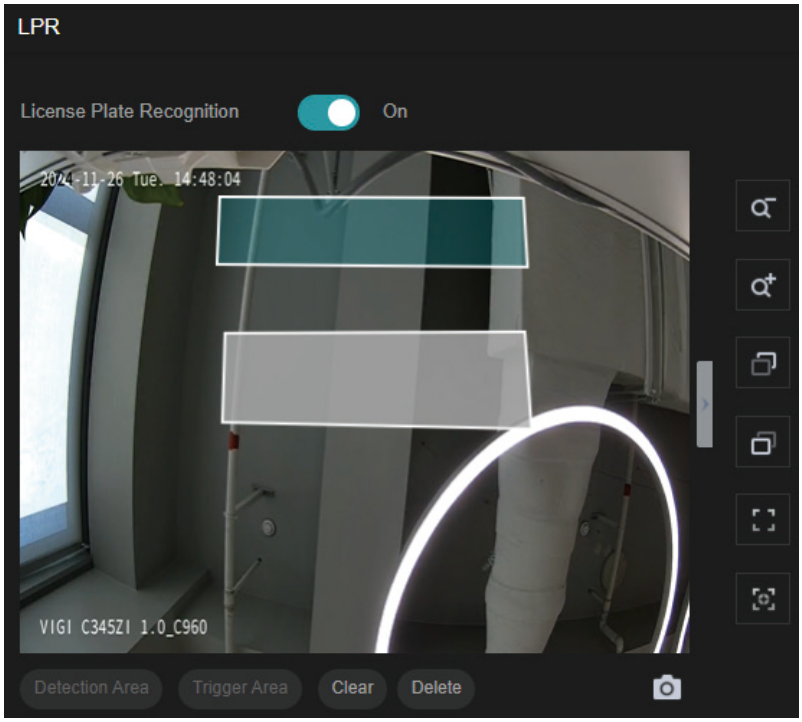


2. Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.
3. Refer to Arming Schedule and Linkage Method for settings if needed.
4. Click **Save**.

5. 14 LPR

LPR, or license plate recognition, captures and analyzes vehicle license plates in rea time. Follow the steps below to finish the configuration.

1. Go to Settings > Event > LPR and click the toggle to turn it on.

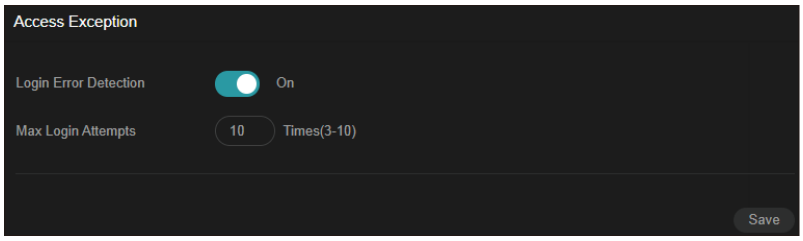


2. Define detection area (marked by blue) and trigger area (marked by white) by drawing shapes. Detection area specifies where you wish to detect motion; trigger area specifies where you wish to trigger alarm responses.
3. Click Save.

5. 15 Exception Event

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. Follow the steps below to finish the configuration.

1. Go to Settings > Event > Exception Event.



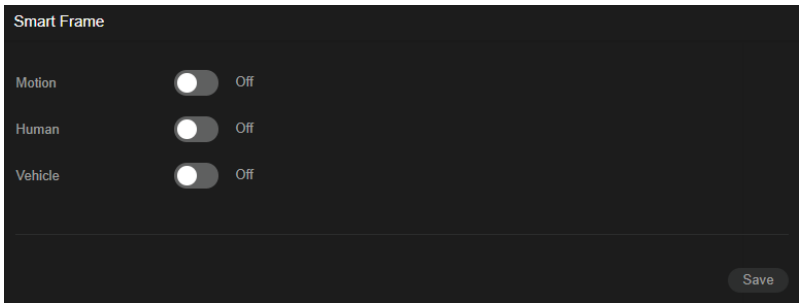
2. Enable Login Error Detection to limit the login attempts:
3. Set the maximum login attempts. The number should between 3 and 10
4. Click Save.

Note: To unlock the camera and try to log in again, power the camera off and then power it on.

5. 16 Smart Frame

Smart frame is an AI-powered function that can precisely mark and capture detected movement, people, or vehicle objects on the screen.

Click the toggles to specify the type of detection: motion, human, or vehicle. You may enable more than one types. Click Save.



5. 17 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.

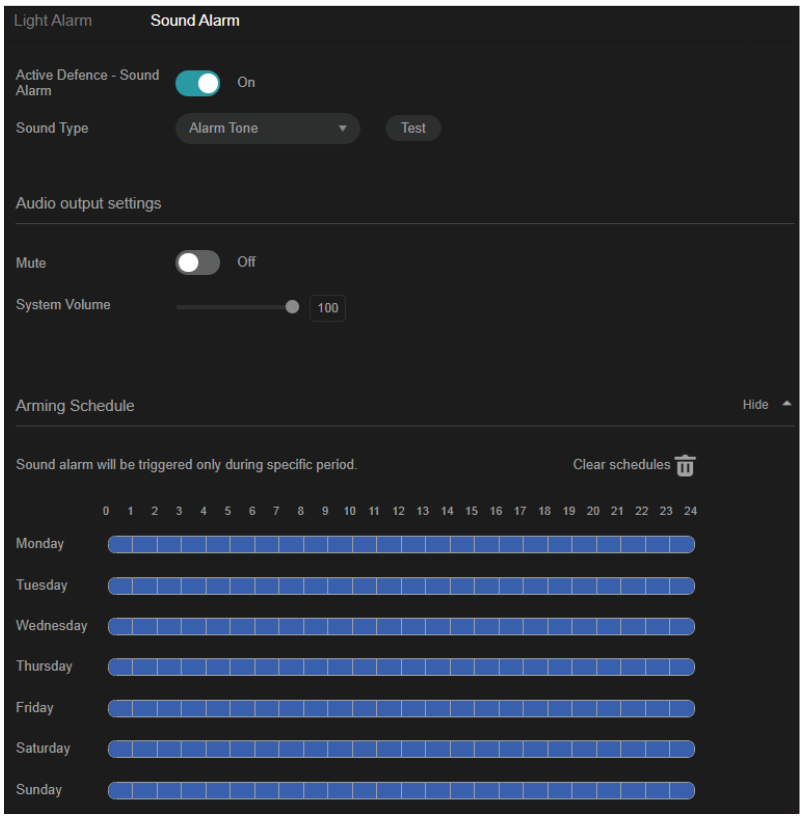
1. Go to Settings > Event > Active Defence > Light Alarm.
2. Enable Active Defence - Light Alarm.

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

5. 18 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 > Event > Active Defence > Sound Alarm.
2. Enable Active Defence - Sound Alarm, select the Alarm Type, and click Test.



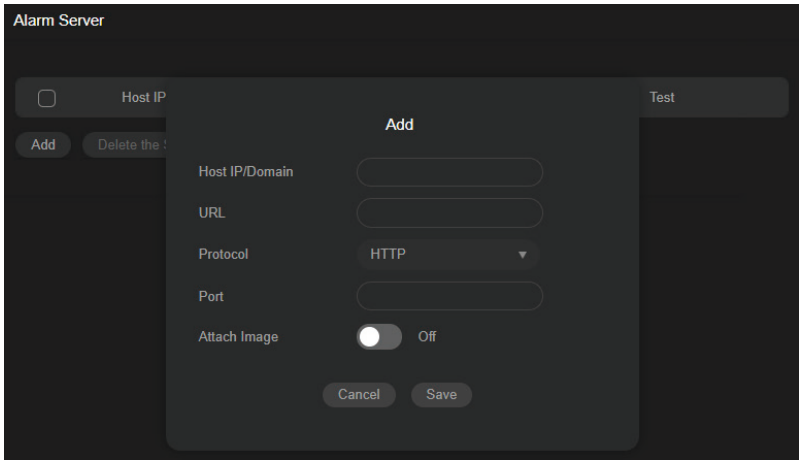
3. Under Audio Output Settings, click the toggle to mute or drag the slide bar to set the system volume.
4. Refer to Arming Schedule and Linkage Method for settings if needed.
5. Click Save.

5. 19 Alarm Server

The device can send alarms to destination IP address or host name through HTTP, HTTPS, or ISUP protocol. The destination IP address or host name should support HTTP, HTTP, or ISUP data transmission.

1. Go to Settings > Event > Alarm Server.

2. Click Add.



3. Enter Host IP/Domain, URL, and Port, and select Protocol. Enable Attach Image if needed.

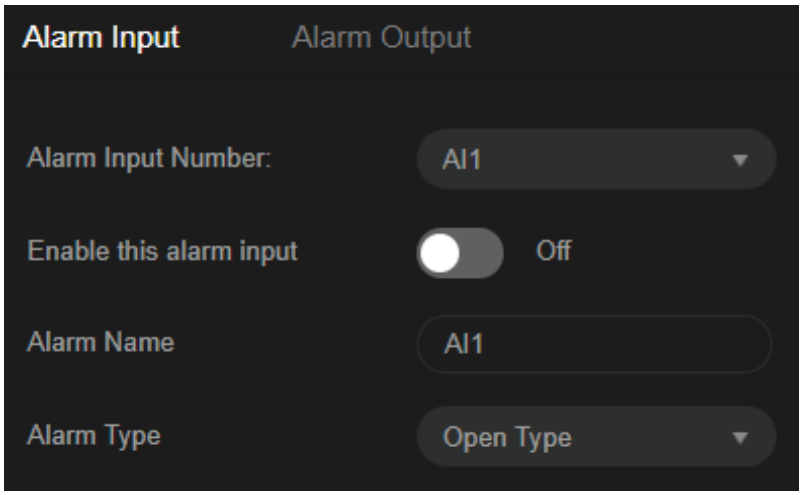
   Note: HTTP and HTTPS are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.

4. Click Save.

5. 20 Alarm Input

Alarm signal from the external device triggers the corresponding actions of the current device. Before you start, make sure the external alarm device is connected. See https://www.tp-link.com/hk/support/faq/4227/ for cable connection.

1. Go to Settings > Event > Alarm Device > Alarm Input.



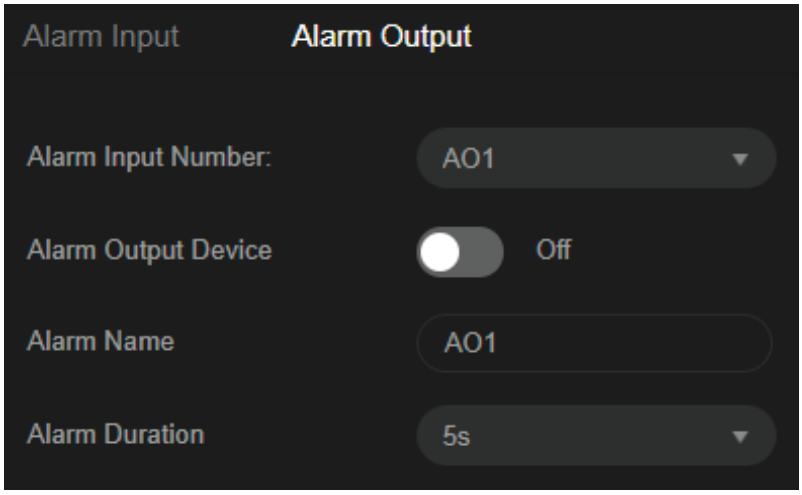
2. Select an Alarm Input Number.
3. Check Enable This Alarm Input.
4. Edit the Alarm Name.

5. Select the Alarm Type from the dropdown list. Open Type means that under normal conditions, the circuit is open and no current passes through the device. When the alarm is triggered, the current passes through the device and the device alarms. Close Type means that normally the circuit is closed, and the device will alarm in case of a circuit fault or alarm trigger.
6. Refer to Set Arming Schedule for setting scheduled time. Refer to Linkage Method Settings for setting linkage method.
7. Click Save.

5. 21 Alarm Output

If the device has been connected to an alarm output device, and the alarm output No. has been configured, the device sends alarm information to the connected alarm output device when an alarm is triggered. Before you start, make sure the external alarm device is connected. See https://www.tp-link.com/hk/support/faq/4227/ for cable connection.

1. Go to Settings > Event > Alarm Device > Alarm Output.



2. Select the Alarm Output Number according to the alarm interface connected to the external alarm.
3. Enable the Alarm Output Device.
4. Edit the Alarm Name.
5. Select the Alarm Duration from the dropdown list.
6. Click Save.

6

Recording and Storage

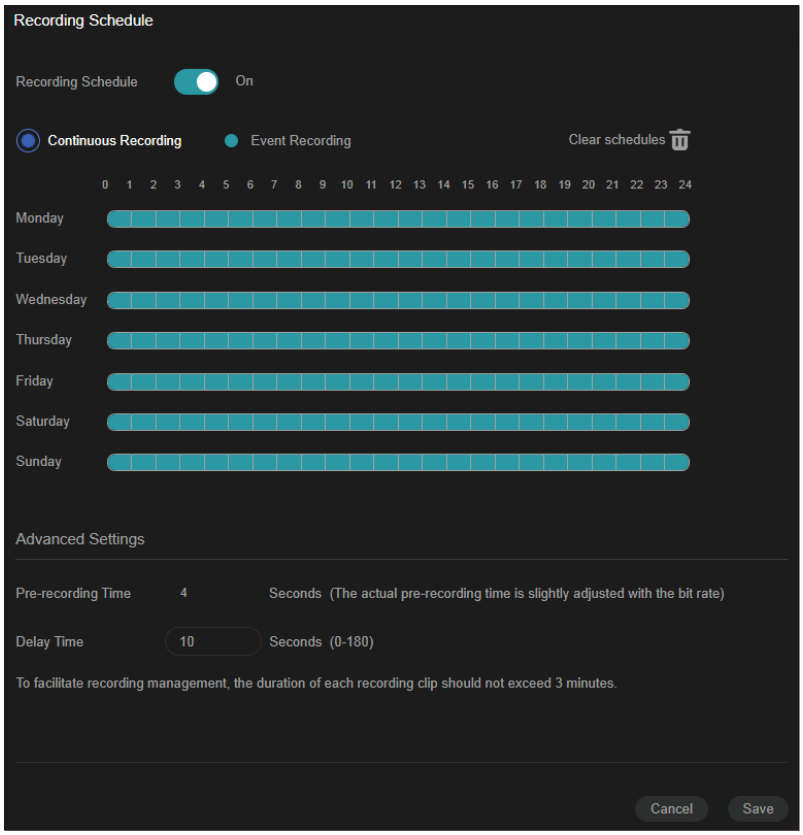
This chapter guides you on how to view and configure recording and storage settings on your camera. VIGI camera allows you to set your own recording schedules and parameters. This chapter includes the following sections:

- Recording Schedule
- Storage Management

6. 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.

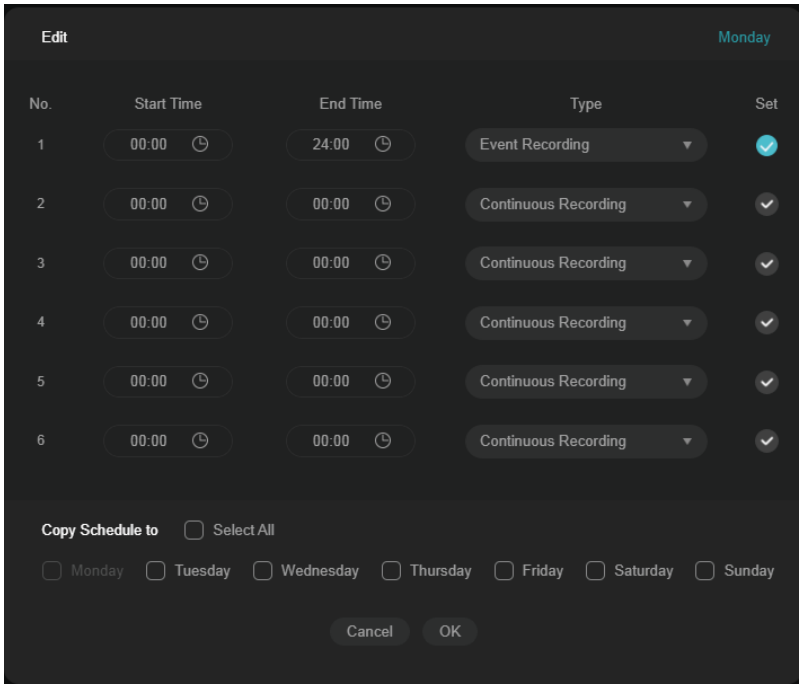


2. Enable Recording Schedule, select Continuous Recording or Event Recording, then select the time period.

Continuous Recording	The camera will record continuously.
Event Recording	The camera will record when an event is detected.
Pre-recording Time	The time is set for cameras to record before the scheduled time or event. For example, the schedule for continuous recording starts at 10:00. If you set the pre-recording time as 5 seconds, the camera starts to record at 9:59:55.
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.

3. Move your mouse to the right of a day's blocks and an edit button will appear. Click and enter the pop-up window to finetune the Start Time and End Time (with an accuracy of a minute). Select

Event Recording or Continuous Recording for each time period and check Set. You may copy a schedule for a day to any other days. Click OK when you are done.

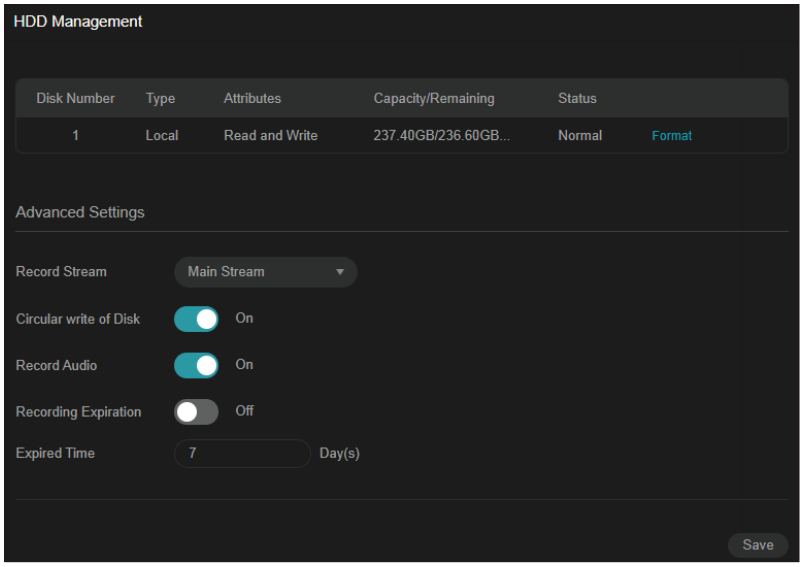


4. Click Save.

6. 2 Storage Management

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.



2. Click Format to initalize 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 Streams	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.
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 can not be recovered.
Expired Time	Set the time when recordings will be automatically deleted.

5. Click **Save**.

7

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:

- InternetInternet Connection
- Port
- Platform Access
- Email
- Port Forwarding
- IP Restriction
- Multicast
- Server
- Upload
- ONVIF
- SNMP
- DDNS

7. 1 Internet Connection

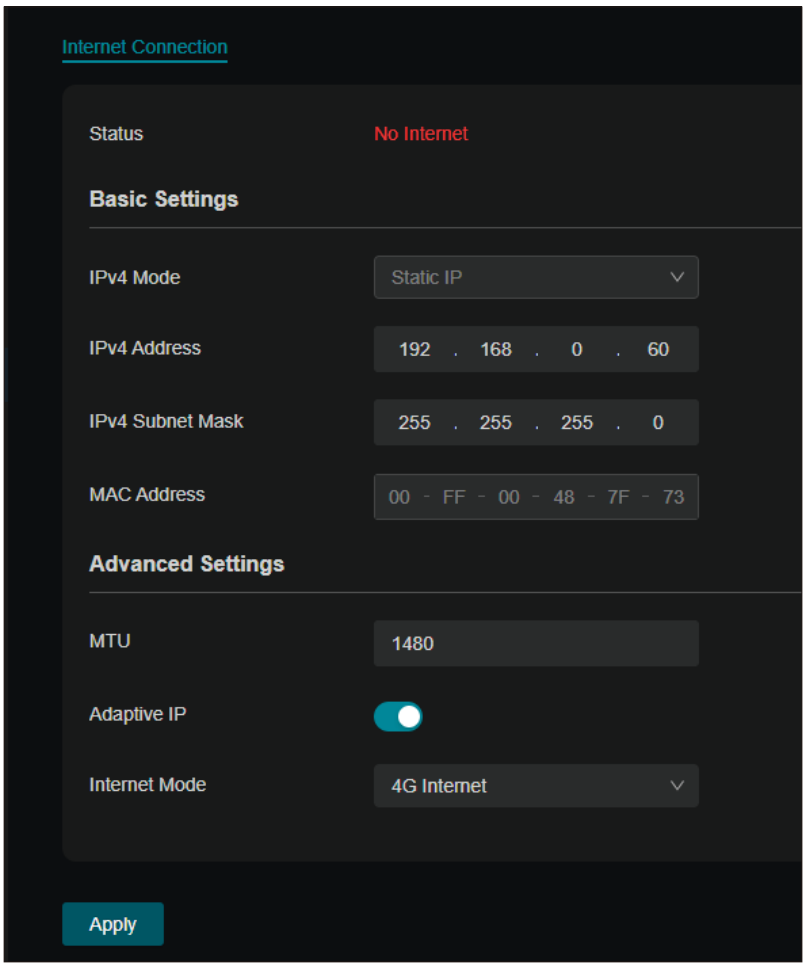
In Internet Connection, you can view the connection status, connect your camera to the internet using either the default 4G mode or a wired network connection, and adjust related network settings.

By default, the camera is set to 4G Internet mode. To connect, insert a valid SIM card and ensure it is successfully registered on the mobile network. Once connected, the camera can be added and managed remotely.

If needed, you can switch the Internet Mode to Wired Internet mode, in which case the configuration works the same way as on standard wired camera models.

Follow the steps below to configure the network settings.

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



2. Configure the required parameters as shown below.

Status	Displays the current internet connection status.
IPv4 Mode	Select whether the camera obtains an IP address automatically (Dynamic) or is assigned a fixed IP address (Static).

IPv4 Address	Specify an IP address for the camera. It must be in the same network segment as the gateway; otherwise, the camera will not connect to the internet.
IPv4 Subnet Mask	Enter the subnet mask for the network (e.g., 255.255.255.0).
IPv4 Gateway	Enter the IP address of the gateway device that routes the data. This address must be in the same segment as the camera's IP address.
Mac Address	Displays the unique hardware identifier of the camera's network interface. This value is read-only and cannot be changed.
DNS	Configure the Domain Name System (DNS) settings used to translate domain names into IP addresses.
Preferred / Alternative DNS	Enter the IP addresses of the primary (preferred) and secondary (alternative) DNS servers.
MTU	Specify the Maximum Transmission Unit (MTU), which defines the largest data packet that can be transmitted. A larger MTU can improve efficiency but may increase latency. If unsure, keep the default value.
Adaptive IP	Enable this option to allow the camera's IP address to adjust automatically according to changes in the network topology.
Internet Mode	Select the connection type: 4G Internet (default, requires a valid SIM card) or Wired Internet (standard Ethernet connection).

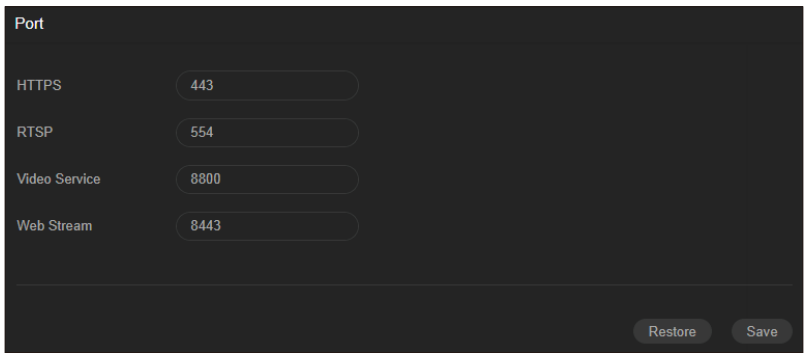
Note: The cameras should be in the same segment with the NVR, so that the NVR can discover and manage them.

3. Click **Apply**.

7.2 Port

In Port, 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 VIGI Security Manager or the VIGI app, the ports configured here are used for communications of corresponding protocols.

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



2. Specify HTTPS port and service port.

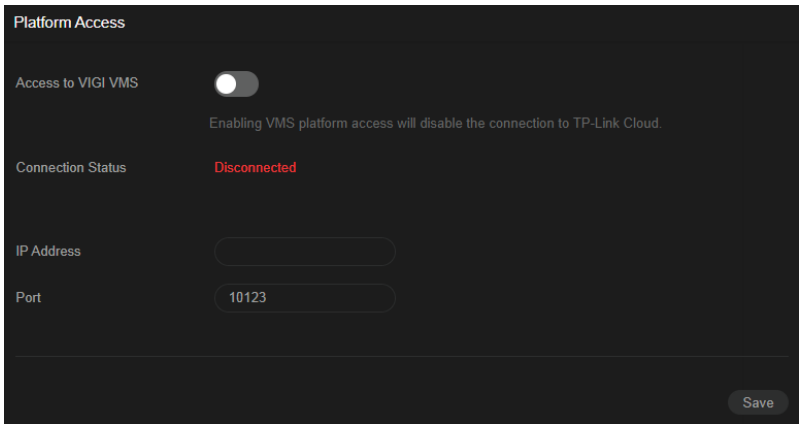
HTTPS	Specify a port for HTTPS protocol.
RTSP	Specify a port for RTSP protocol.
Video Service	Specify a port for protocols of video services.
Web Stream	Specify a port to access the camera's live streaming web interface.

3. Click **Save**.

7. 3 Platform Access

VIGI VMS is an application that streamlines batch device management via a single interface, integrating real-time video monitoring, an alarm center, and advanced features for effortless, robust security. You can access VIGI VMS with the Platform Access enabled.

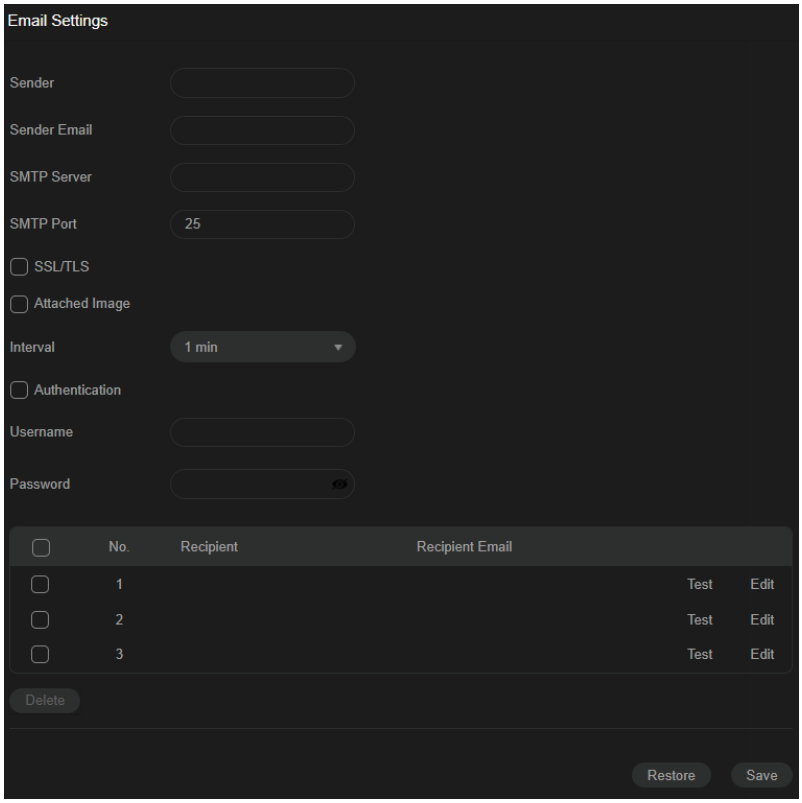
1. Enable Access to VIGI VMS.



2. Enter the IP Address and the Port number.
3. Click **Save**.

7. 4 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. Input the sender's email information, including the Sender's name, Sender Email, SMTP Server, and SMTP Port.
2. Enable SSL/TLS if needed and emails will be send after encrypted.
3. Check 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.
4. If your email server requires authentication, check Authentication and input your username and password to log in to the server.
5. Input the recipient's information, including the recipient's name and address.
6. Click Test to see if the function is well configured.
7. Click Save.

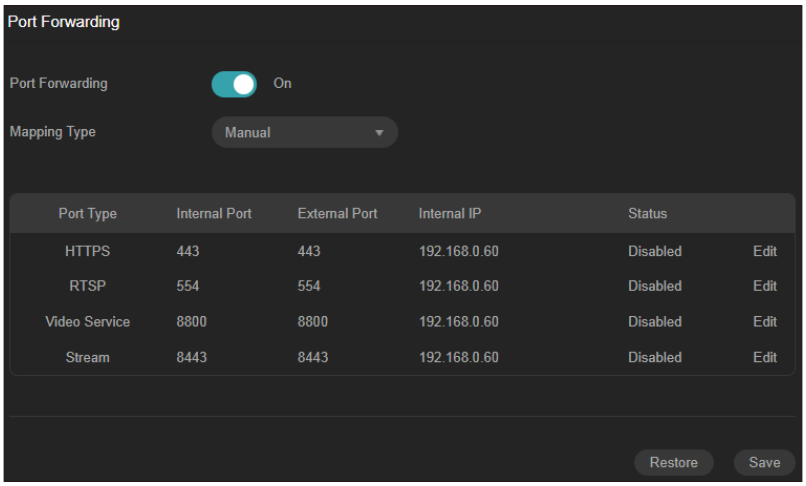
7. 5 Port Forwarding

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** > **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 **Edit** 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.
Restore	Click to restore the settings to default factory settings.

3. Click **Save**.

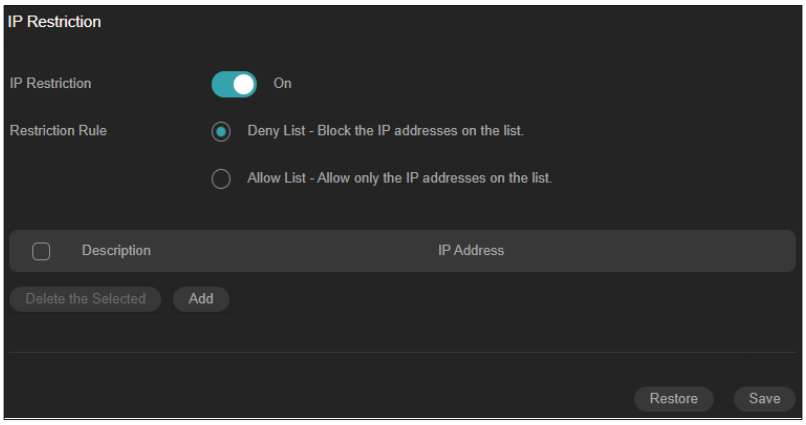
With Port Forwarding enabled, you can remotely watch the videos with the URL rtsp://A.B.C.D:Port/streamN, for example, rtsp://10.0.1.47:28736/stream1. A.B.C.D is the WAN IP address of the gateway, and Port is the number of RTSP external port. N can be number 1 or 2 that indicates the stream, 1 for main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

7. 6 IP Restriction

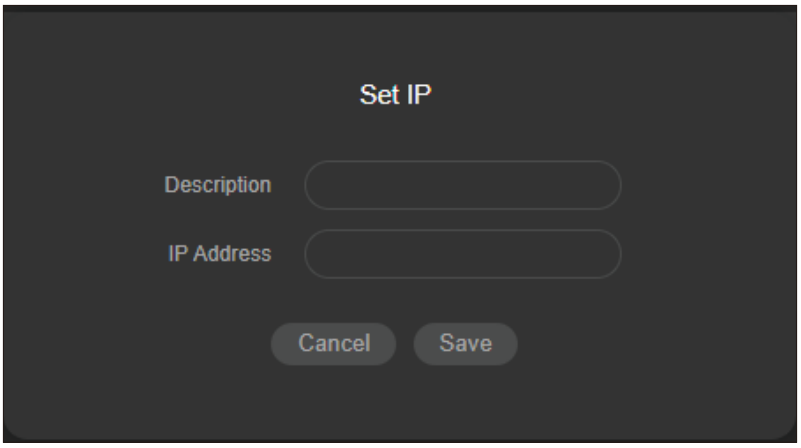
When IP Restriction is enabled, you can add IP addresses to the deny list or allow list to restrict the access to the camera. The IP address in the deny list cannot access the camera, while only the IP addresses in the allow list can access the camera.

Follow the steps below to configure IP Restriction.

1. Go to Settings > Network Settings > IP Restriction.
2. Enable IP Restriction and specify the restriction rule. If you select Deny List, the devices with the IP addresses specified in the table will not be able to access the camera. If you select Allow List, only the devices with the IP 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, then click Save.



4. Click Save.

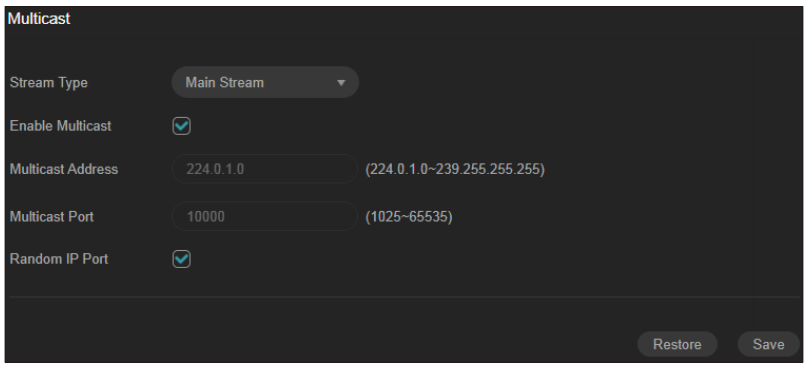
7. 7 Multicast

When Multicast is enabled, you can watch videos using the multicast address and port.

Follow the steps below to configure Multicast.

1. Go to Settings > Network Settings > Multicast.

2. Select the stream type, then enable Multicast.



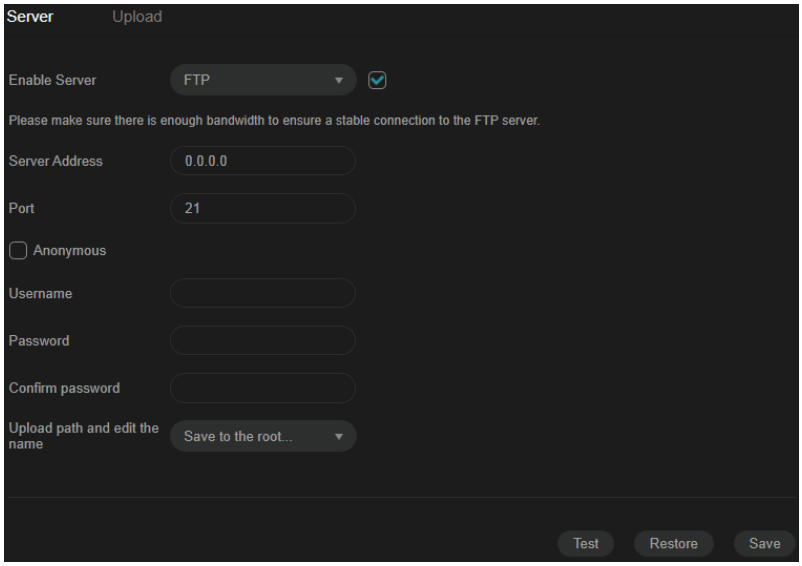
3. Disable Random IP Port and specify a static address and port, or enable Random IP Port.
4. Click Save.

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.

7.8 Server

You can configure the FTP server to save images which are captured by events.

1. Go to Settings > Network Settings > FTP Settings > Server.



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.

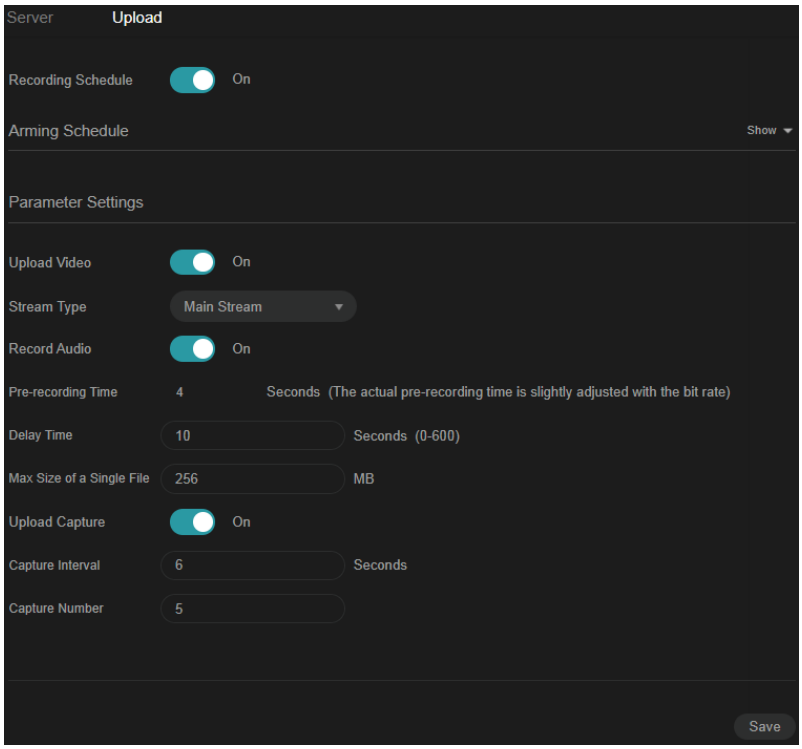
   Note: Anonymous login is not supported when SFTP protocol is selected.

6. Select the saving path of images uploaded in the dropdown box of Upload Path and Edit the Name.
7. Click Test to verify the FTP server.
8. Click Save.

7.9 Upload

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

1. Go to Settings > Network Settings > FTP Settings > Upload.



2. Enable Recording Schedule and follow the steps in Recording Schedule..
3. Enable Upload Video and Upload Capture as needed.
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

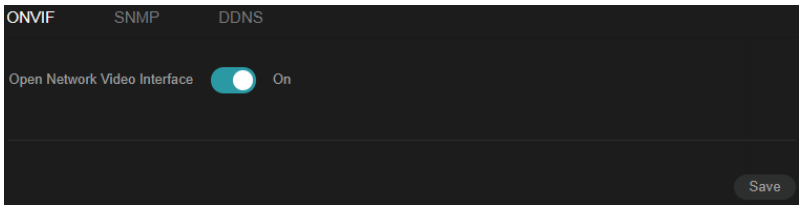
Record Audio	Enable to record audio and video simultaneously.
Pre-recording Time	The time period you set to record before the scheduled time. For example, the schedule for continuous recording starts at 10:00. If you set the pre-recording time as 5 seconds, the camera starts to record at 9:59:55.
Delay 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 Save.

7. 10 ONVIF

ONVIF, or Open Network Video Interface Forum, aims to provide a standard for the interface between different IP-based physical security devices. ONVIF specifications provide a consistent way for devices from multiple manufacturers to work together

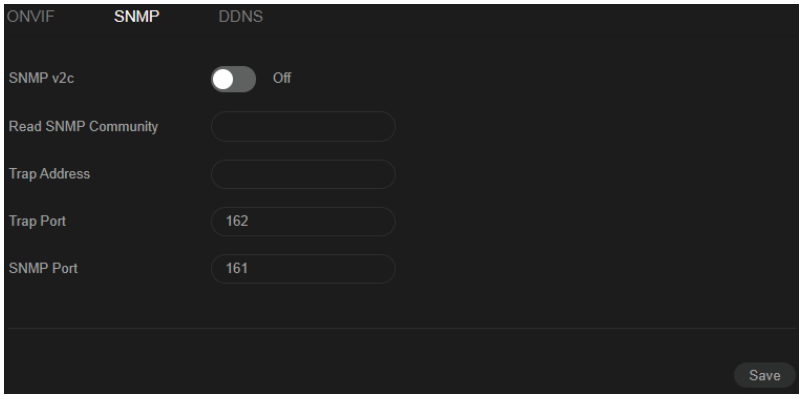
Enable ONVIF if you need to use third-party management devices. Go to Settings > Network Settings > Advanced > ONVIF.



7. 11 SNMP

You can set the SNMP, or Simple Network Management Protocol, to get device information in network management.

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



2. Enable SNMP v2c.
3. Enter the SNMP community name. Note that the access is Read only, meaning that the network management system can only view but not modify parameters of the specified view.
4. Configure the following parameters.

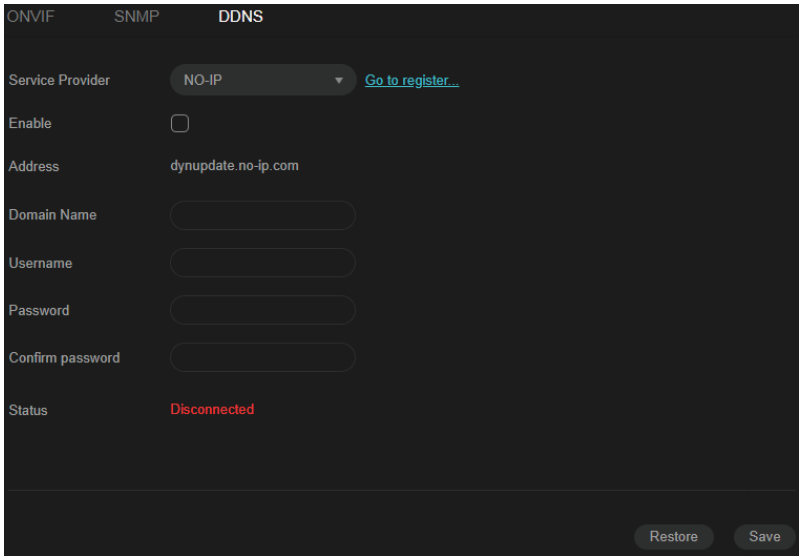
Trap Address	IP Address of SNMP host.
Trap Port	Port of SNMP host. The value is by default 162 and can range from 1 to 65535.
SNMP Port	An SNMP communication endpoint that identifies SNMP data transfers. By default the SNMP port is 161.

5. Click Save.

7.12 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 Save.

8

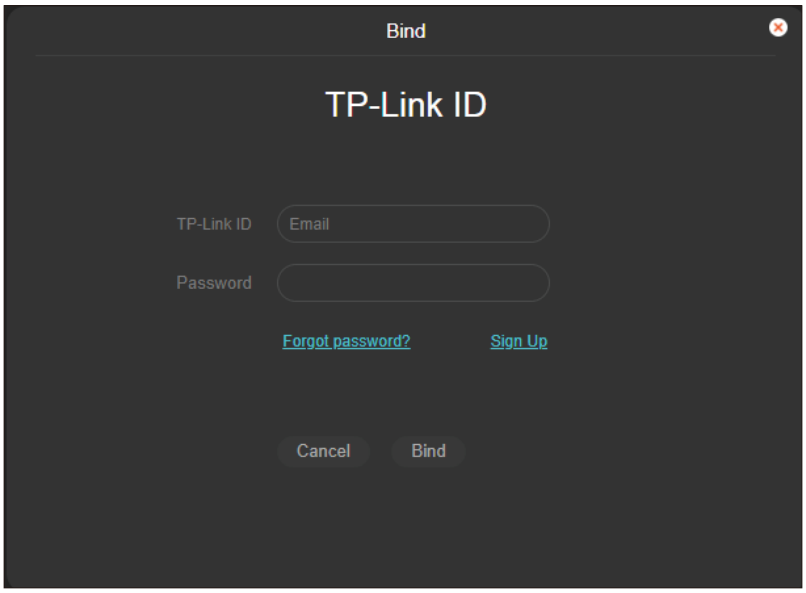
Cloud Service

After connecting your camera to the internet, you can manage it remotely via Cloud Services.

The camera supports remote management with the support of TP-Link Cloud Services. With a TP-Link ID bound, you can remotely monitor your areas on multiple platforms, including computers and mobile phones.

Follow the steps below to bind your TP-Link ID to the camera and download the VIGI app.

1. Go to **Settings** > **Cloud Service**.
2. Click **Go to Bind**. Enter your TP-Link ID and password and click **Bind**. If you do not have a TP-Link ID, click **Sign Up** to register.



3. After binding your TP-Link ID, download the VIGI app on your mobile phone by scanning the QR code below. Log in with your TP-Link ID. Then you can monitor the live view and manage the camera remotely on your computer or mobile phone.

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:

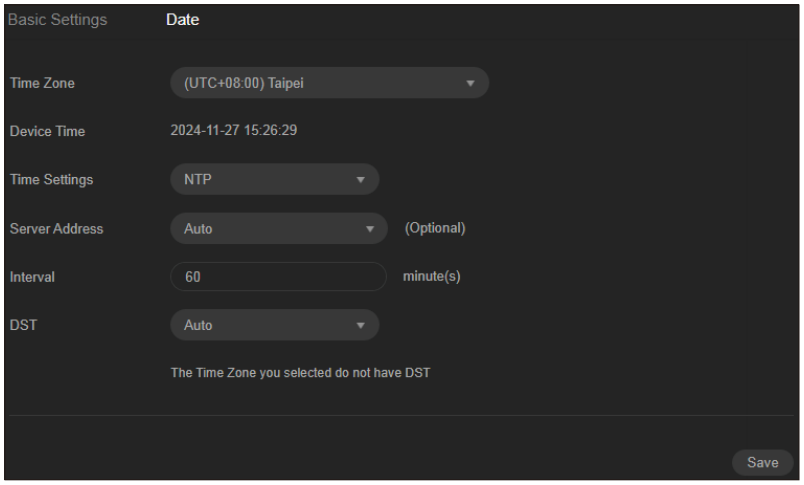
- Configure Basic Settings
- Modify System Time
- Manage User Accounts
- System Management
- Upgrade Firmware
- Reboot Device Regularly

9. 1 Configure Basic Settings

1. Go to Settings > System 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

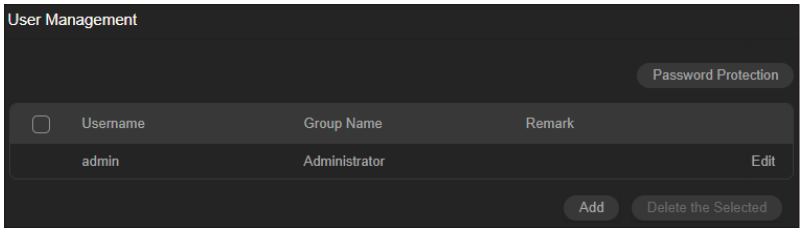
VIGI camera provides two methods to modify the system time. NTP (Network Time Protocol) can automatically get the system time from the internet, or you can manually set the system time. You can also select the time zone according to your region, and configure the DST settings. To configure these settings, go to Settings > System Settings > Date.



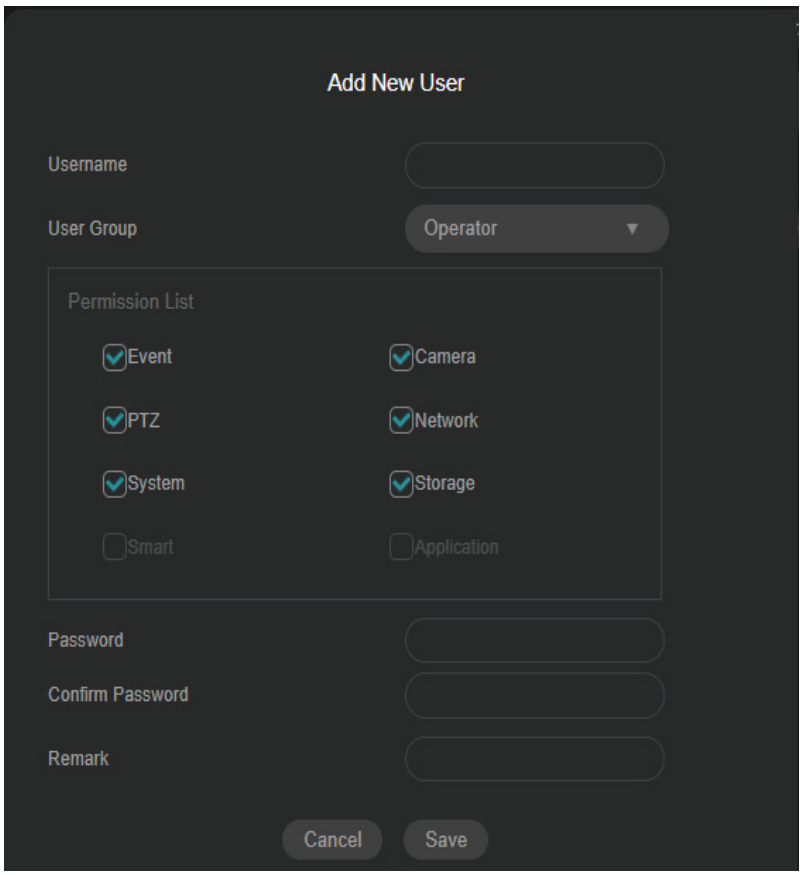
9. 3 Manage User Accounts

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.**

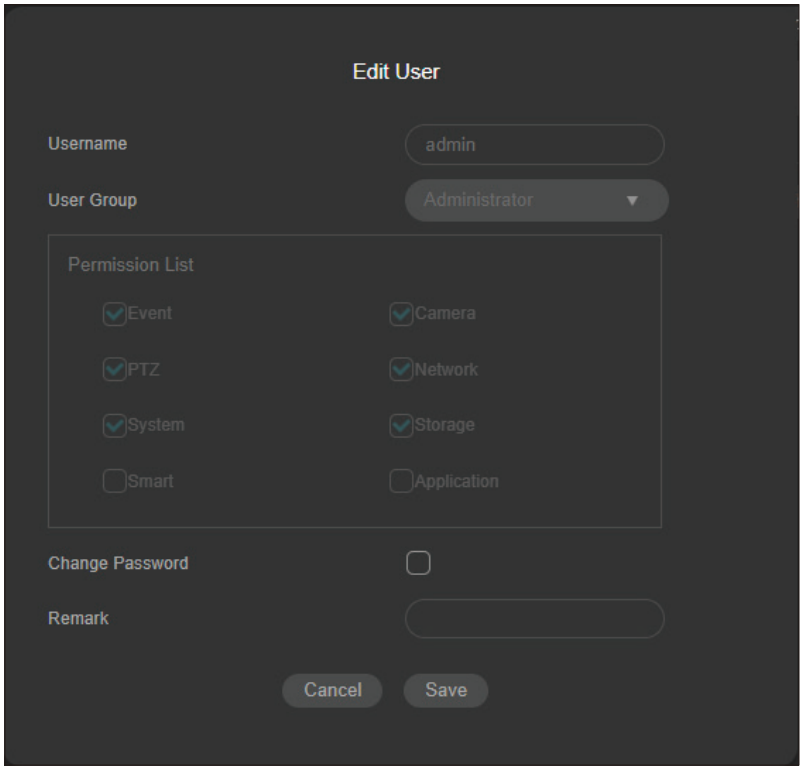


2. **Click Add**. Enter Username, select User Group, and enter Password. Assign remote permission to users based on needs.



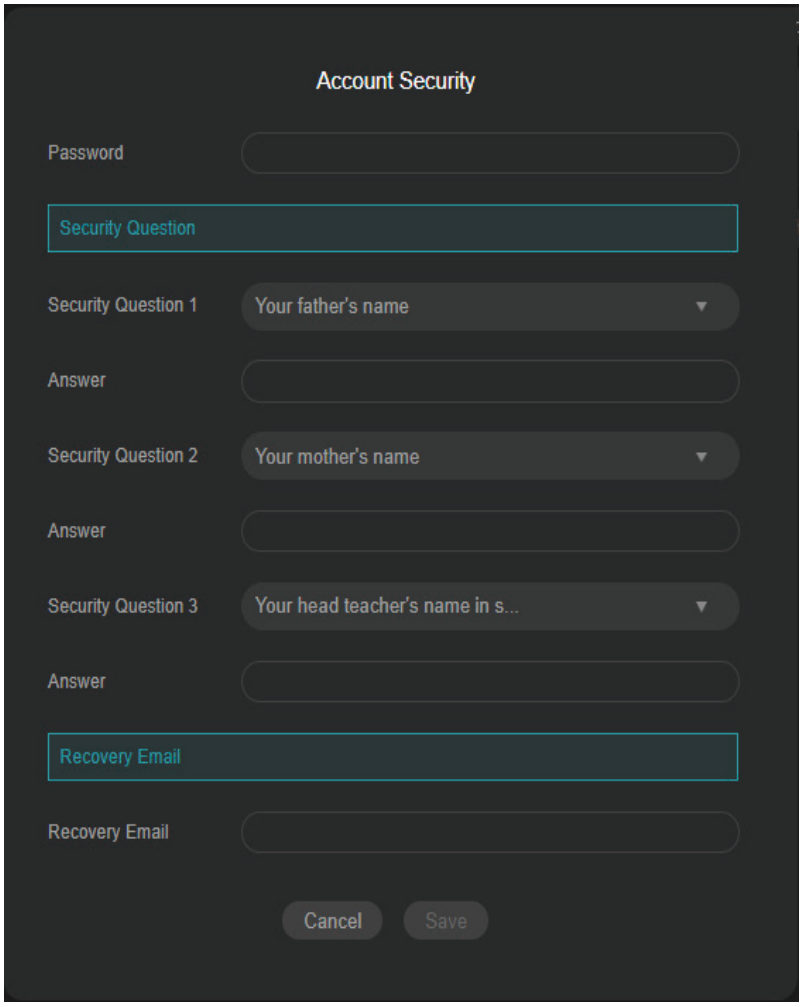
Administrator	The administrator has the authority to all operations and can add users and operators and assign permission.
Operator	Operators can be assigned all permission except for operations on the administrator and creating accounts.
User	Users can be assigned permission of viewing live video, setting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

3. Click **Edit** to change your username and password.



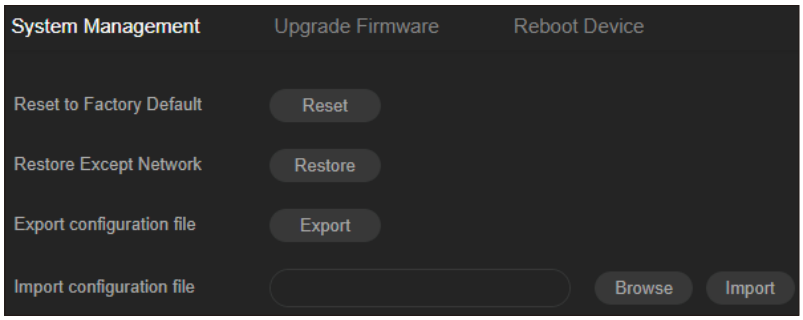
4. Click **Password Protection** for account security settings. You can reset the password by setting the security question or email. You can click Forget Password and answer the security question

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.



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:

To export the configuration file, click Export.

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

9. 5 Upgrade Firmware

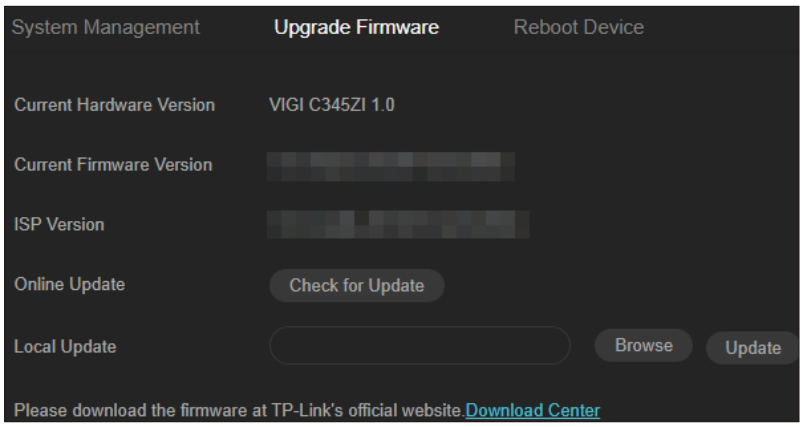
TP-Link aims at providing better network experience for users. We will inform you through the web management page if there's any update firmware available for your camera. Also, the latest firmware will be released at the TP-Link official website www.tp-link.com, and you can download it for free.

Note:

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

9. 5. 1 Online Upgrade

1. Go to Settings > System Settings > System Management > Upgrade Firmware.
2. Click Check for Update to see whether the latest firmware is released.



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

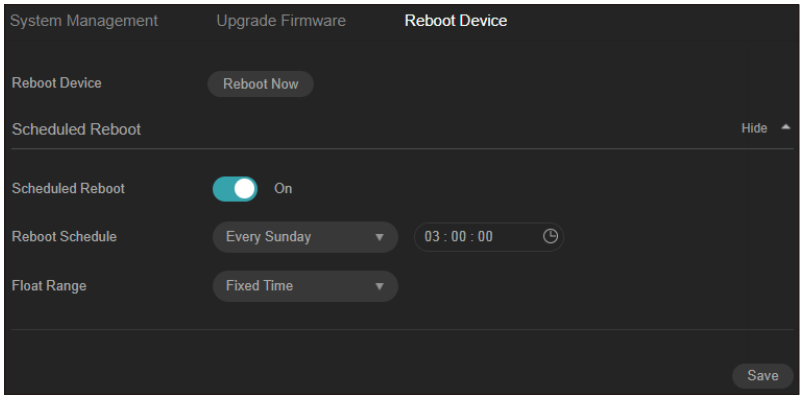
9. 5. 2 Local Upgrade

1. Download the latest firmware file for the camera from www.tp-link.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 upgrade 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 > Reboot Device.
2. Enable Scheduled Reboot.
3. Select the day and time and click Save to save your settings. Then your camera will reboot regularly at a specific time.



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