VIGI
by tp-link

User Guide

VIGI VMS System

Applicable to VIGI VMS of Version 1.8.X

 1910013952 REV1.1.0

About This Guide

This User Guide provides information for managing devices via TP-Link VIGI VMS platform.

Conventions

When using this guide, notice that:

- Features available of VIGI devices may vary due to your region, device model, firmware version, and app version. All images, steps, and descriptions in this guide are only examples 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.
Bold	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

- The latest firmware can be found at Download Center at https://www.tp-link.com/support.
- Product specifications can be found on the product page at https://www.tp-link.com.
- For technical support, the latest version of the Quick Installation Guide, User Guide and other information, please visit https://www.tp-link.com/support.
- 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.

Contents

1

Introducing VIGI VMS

This chapter covers the basic functionalities of VIGI VMS.

1. 1 Introduction

VIGI VMS is a local-deployed software system designed for centralized management of medium-scale surveillance projects like supermarkets, hotels and schools. It includes features such as real-time video monitoring, user permission management, alarm handling, evidence collection, and virtual map integration, aiming to enhance your video management efficiency.

The software provides multiple functionalities, including:

Device Access: Detect and add IPCs and NVRs.

Device Management: Remotely configure the IPCs and NVRs, reboot and upgrade the devices, and edit image and video parameters, etc.

Real-time Monitoring: Check the surveillance video in real-time, monitor the site, and perform functions of intercom, alarm, PTZ control, etc.

Alarm Events: Receive and deal with the alarm events, view the event's details, and solve the exceptions in time.

Video Playback: Backtrack and search for videos.

E-Map: Upload the map or floor plan to VMS, and label the monitoring points straightforwardly.

User & Site: Support multi-user access and multi-site for flexible control of the permission of varied users.

Cloud Access: Supports VMS remote login and management.

Maintenance & Management: Manage the logs, record the user's operation, and configure the history and alarm logs.

This user manual describes the functions, configurations and operation steps of VIGI VMS. To ensure proper usage and stability of the software, please read the manual carefully before installation and operation.

1. 2 Latest Changes

Compared to the previous 1.5 version, the 1.8 version has the key following updates:

- Includes free trials for advanced AI features, including AI Search, People Counting, and Auto Snapshot.
- Supports the display of device ID on the device settings page.
- Supports custom load names and disabling power output in Solar Panel Management.
- Supports copying email alert and FTP settings to other devices on the camera settings page.
- Features optimized UI design, menu layout, and Design Tool module.

2

Getting Started

This chapter guides you on how to start VIGI VMS. This chapter includes the following sections:

2. 1 System Requirements

For VIGI VMS to operate efficiently on your computer, below are the minimum system requirements:

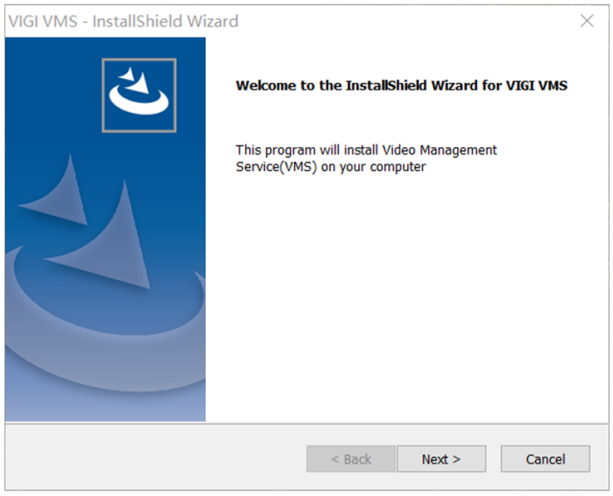
Items	Requirements
Operating System	Microsoft Windows Server 2008 (64-bit) Microsoft Windows 7 (64-bit) Microsoft Windows 10 (64-bit) Microsoft Windows 11 (64-bit)
CPU	Intel Core i5 Processor and above
Memory	4GB and above
Browser Version	Microsoft Edge 106 and above Google Chrome 107 and above Firefox 106 and above

2. 2 Install the Software

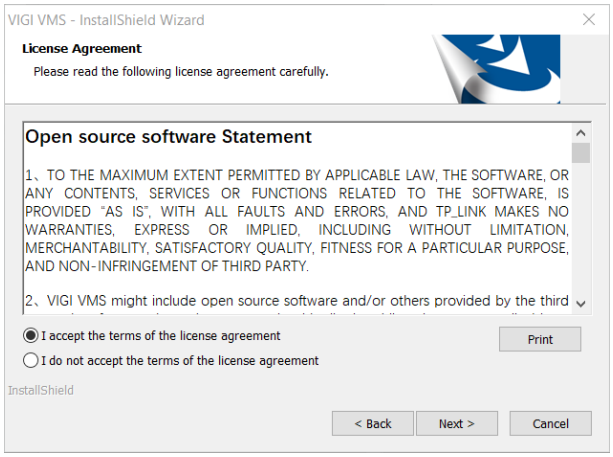
Follow the steps to install the VIGI VMS software:

1. Open the VMS installation package on the host where the installation package has been downloaded.

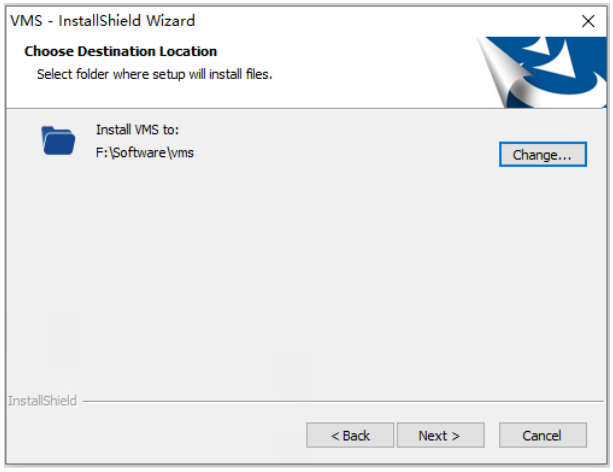
2. Click **Next**.



3. Check **I accept the terms of the license agreement**, then click **Next**.

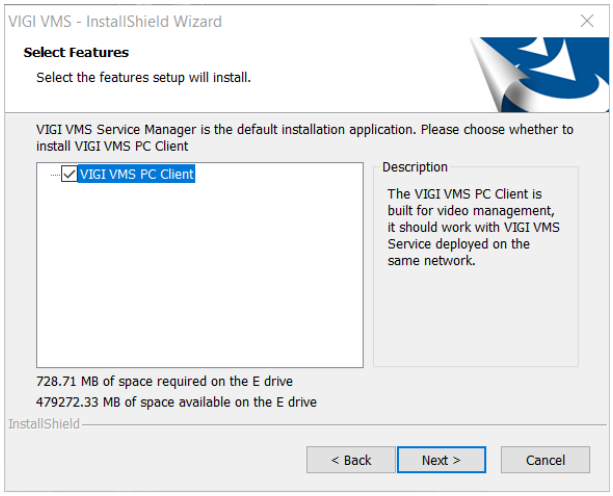


4. Choose the destination location to install the VMS, and click **Next**.

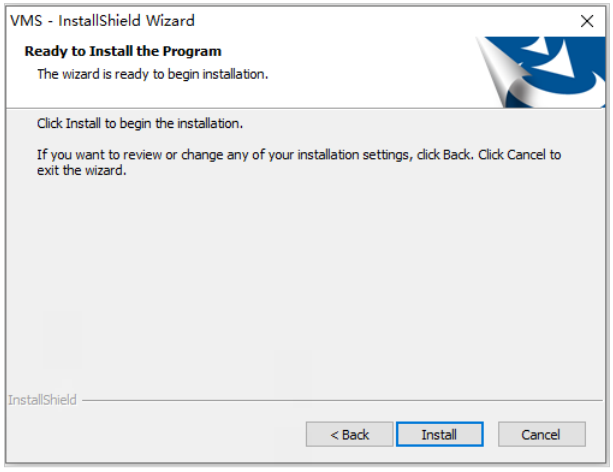


5. Check VIGI VMS PC Client as needed, and click **Next**.

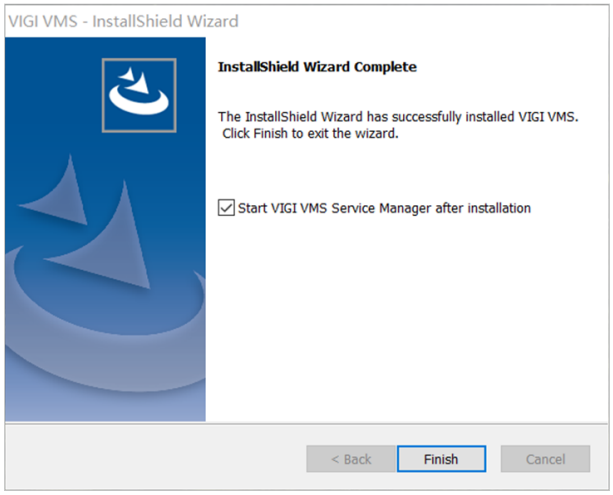
Note: We recommend installing VIGI VMS PC Client for better user experience.



6. Click **Install**. Please wait until the installation completes.



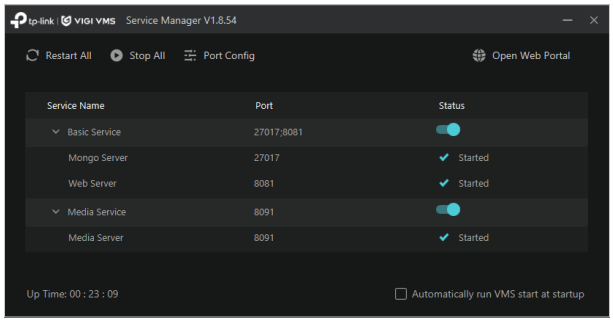
7. When the installation is done, the InstallShield Wizard Complete window pops up. Click **Finish** to end the installation.



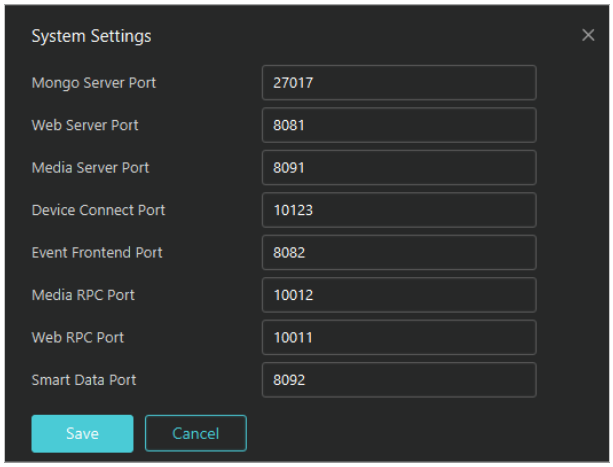
2. 3 Start the Software

1. Open the VIGI VMS Service Manager.

2. In the VMS start page, enable **Basic Service** and **Media Service**.



3. (Optional) To edit its ports during startup, you can click **Port Config**.



Ports	Explanation
Mongo Server Port	The address where the protocol tries to establish the connection. This port is required when VIGI VMS accesses the MongoDB database through this port.
Web Server Port	The communication endpoint that allow data to flow between a client and a server over the internet. This port is required when customer access the VIGI VMS web service via https.
Media Server Port	VIGI VMS manages VIGI devices through this port when customers watch live views or playback.
Device Connect Port	This port is required when VIGI devices connect to the VIGI VMS, establish the remote control terminal session between VIGI VMS and VIGI devices.
Event Frontend Port	This port is needed when VIGI devices report events to VIGI VMS.
Media RPC Port	The port used for remote procedure calls (RPC) to transmit media streams, like video or audio, between devices on the network.

Web RPC Port	The port used for RPC communications that facilitate web-based interactions, such as managing camera settings or accessing live streams through a browser.
Smart Data Port	The port used to transmit smart data, often referring to analytics or event-triggered information, from the camera to external systems for further processing or storage.

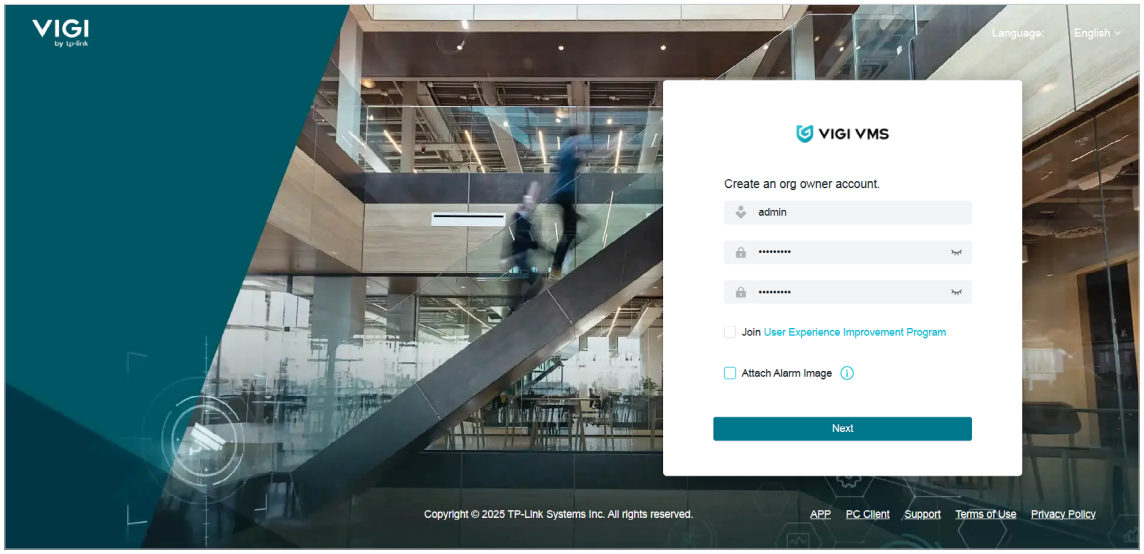
2. 4 Manage the Login

1. When visiting the VMS login page for the first time, you need to create an admin account. Enter the username and password (the password should be at least 8 characters long), and click **Next**.

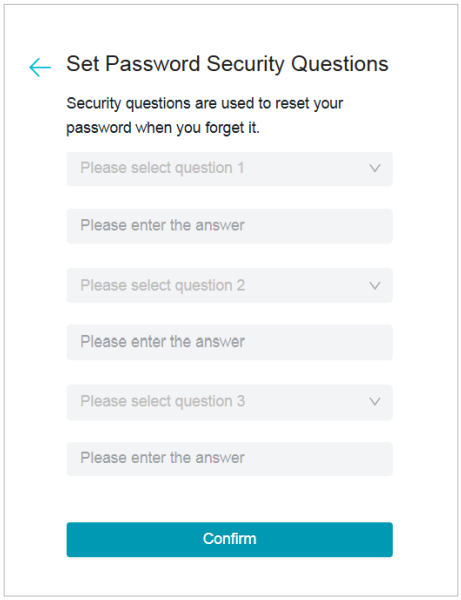
   Note:

   We strongly suggest that you create a password of your choice, ensuring it has at least 8 characters and includes at least three of the following types: uppercase letters, lowercase letters, numbers, and special characters.

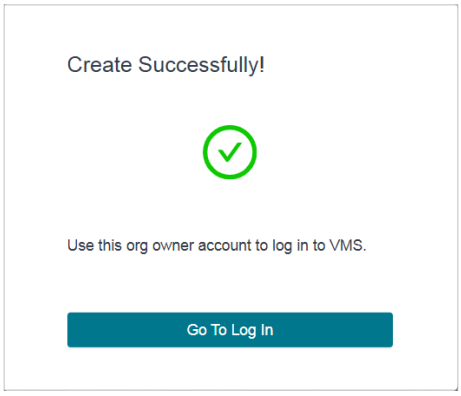
   We advise changing your password regularly; for high-security systems, updating it monthly or even weekly can provide better protection.



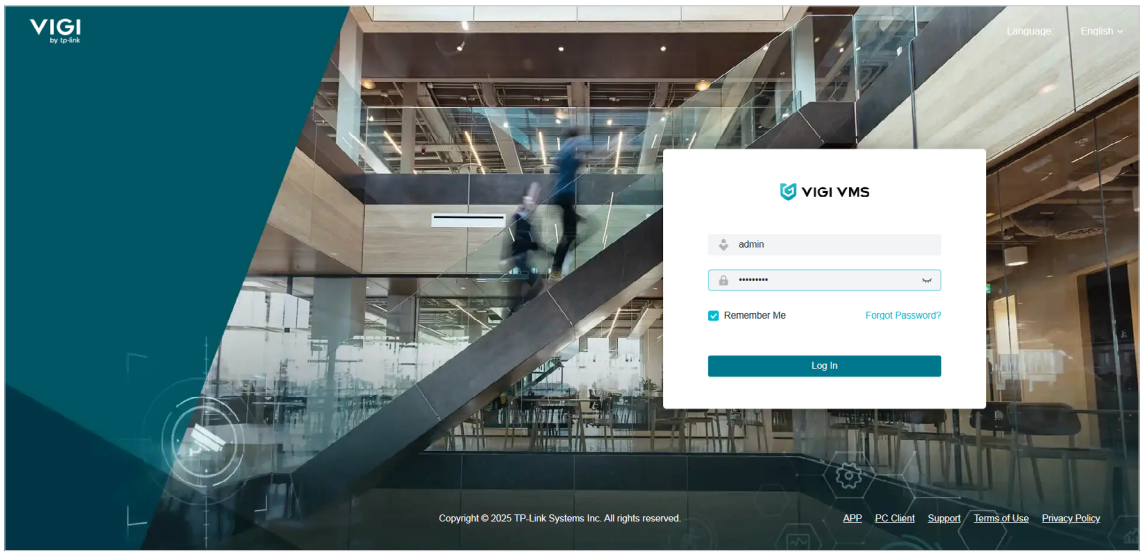
2. Set password security question. If you forget the password in future logins, answer these questions to reset the password.



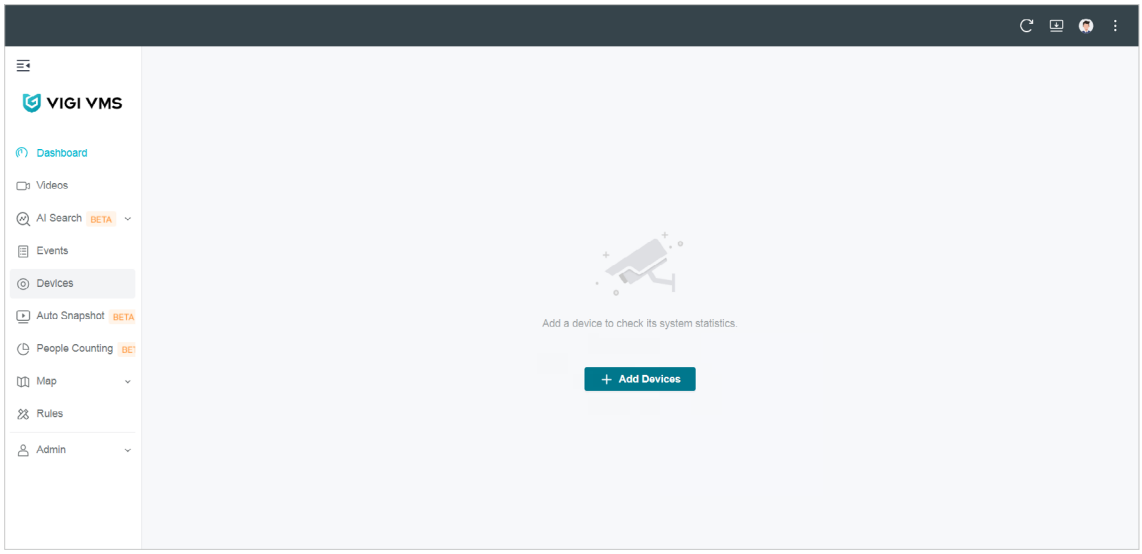
3. Click **Go To Log In**.



4. Click **Confirm** to jump to the login page. Enter your username and password again. Click **Log in**.



5. Now you have successfully logged in to the VMS main screen.



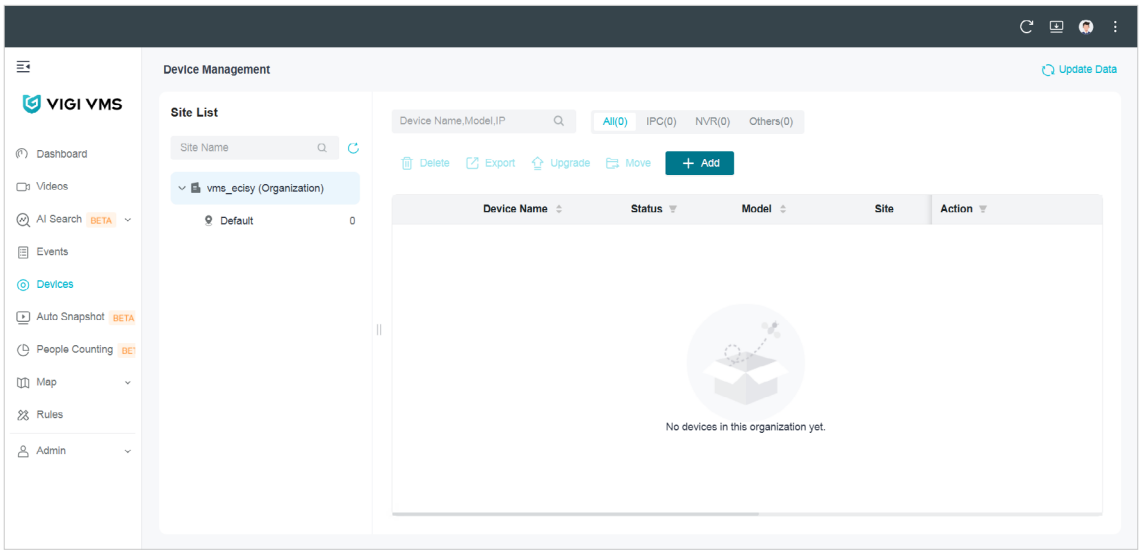
3

Add Monitoring Devices

This chapter provides step-by-step instructions for adding and managing monitoring devices within the VIGI VMS. This chapter covers the following sections:

VIGI VMS offers several options for adding devices, such as Auto Add, Manual Add, and Remote Add. Additionally, it allows for batch additions, which makes it easy and convenient to add a large number of devices at once.

1. Hover the cursor over the menu bar on the left side of the main screen to reveal the names of each function. Click **Device** to enter the device management page.

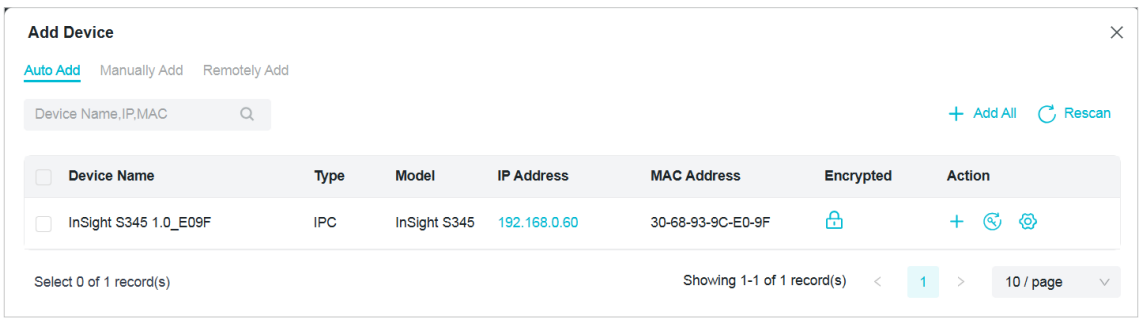


2. On the device management page, you'll find the Site List in the sidebar. When you first use VMS, the system automatically creates a default site for you. You have the option to modify, add, or remove sites in the **Admin > Site** section.
3. The Device List is displayed on the main screen of the device management page, showing all devices added to the current site. Within the Device List, you can add new devices, transfer devices to different sites, or remove devices from the current site.
4. Click + Add on the top right corner of the **Device List**, and the **Add Device** window will appear.

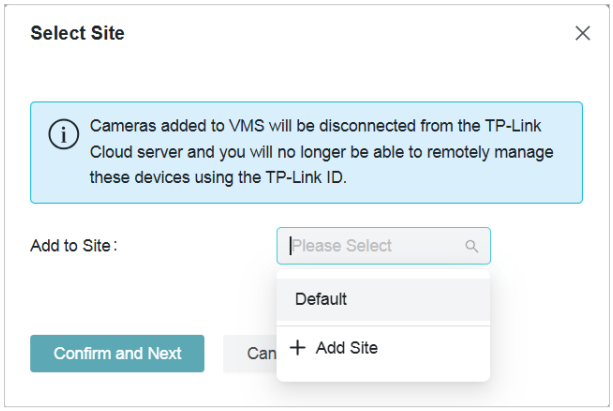
3. 1 Auto Add Device

3. 1. 1 When the device and the VMS server are in the same network segment

1. On the **Add Device** page, click **Auto Add**. A list of detected devices will appear. To add a device, click + on its right. If you wish to add several devices simultaneously, check the boxes next to them and click **Add All**.



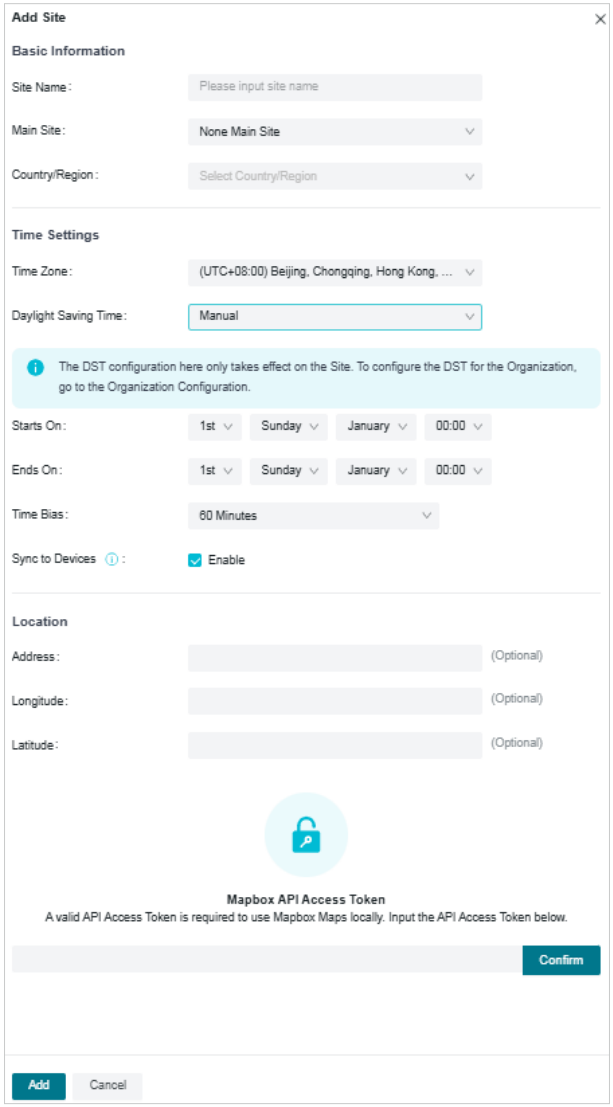
2. Choose a site from the drop-down list in **Add to Site** and click **Confirm and Next**.



3. (Optional) Create a new site:

   1) Click on **Add Site**.

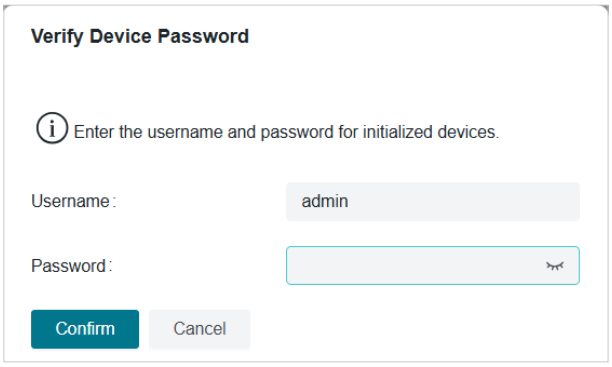
2) Set up the following parameters:



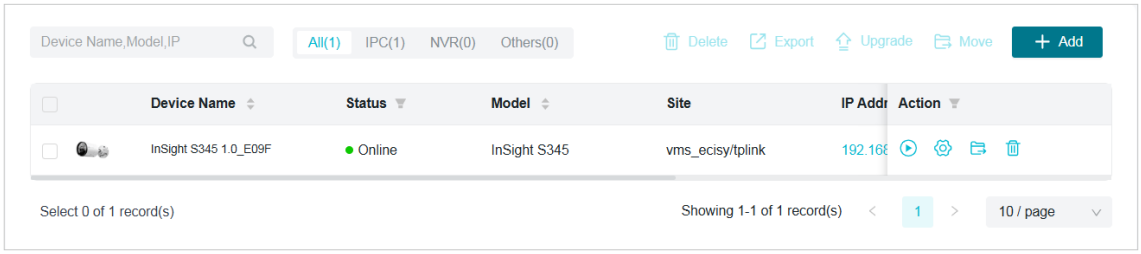
Feature	Explanation
Site Name	Enter a descriptive name for the site.
Main Site	Enter the primary location or central hub where the camera system is managed or monitored.
Country/Region	Select the location of the site.
Time Zone	Select the time zone of the site.

Daylight Saving Time	Set DST (daylight saving time) parameters. 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 and the bias time (the difference in minutes between standard time and daylight-saving time for a specific time zone).
Sync to Devices	Enable Sync to Devices to synchronize the time across all devices with the PC running VMS.

4. A prompt will appear asking you to verify your device password. Enter your username and password, and click Confirm.

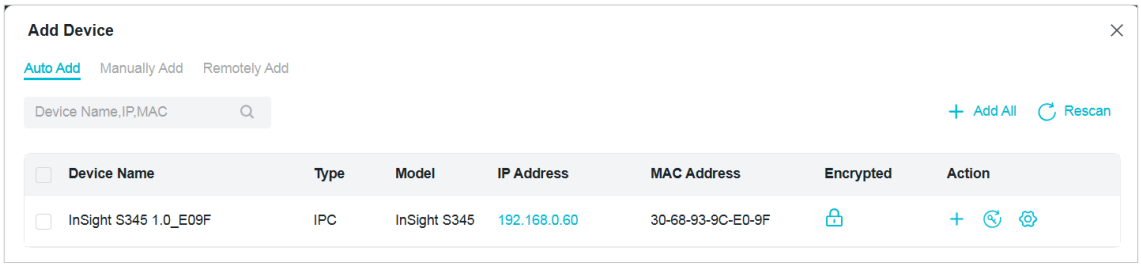


5. Return to the **Device List** page to check if the device is listed. If it is, the device has been added successfully. To add an NVR device, follow the same instructions.

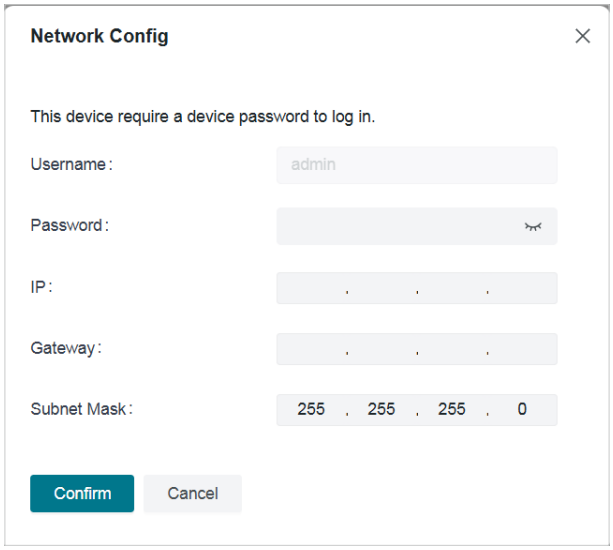


3. 1. 2 When the device and the VMS server are different network segments

1. Ensure the device's IP address is in the same network segment as the VMS server. If not, click to adjust the network settings and click **+** to add it automatically.



2. Configure the device to match the VMS server's network segment and click **Confirm**.



Note: If they are already in the same segment, follow the steps in When the device and the VMS server are in the same network segment to proceed.

3. 2 Manually Add Device

To add a device in the VMS using its IP address, go to the **Add Device** page and click on **Manually Add**. You can choose to add an IPC with a single IP or multiple IPs.

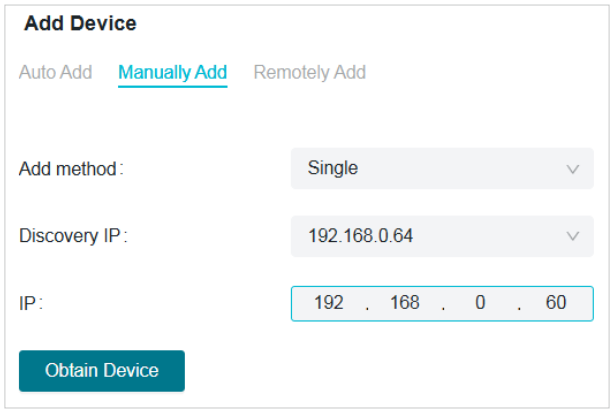
- **To add a device via a single IP:**

  1) Select **Single** from the **Add method** drop-down.

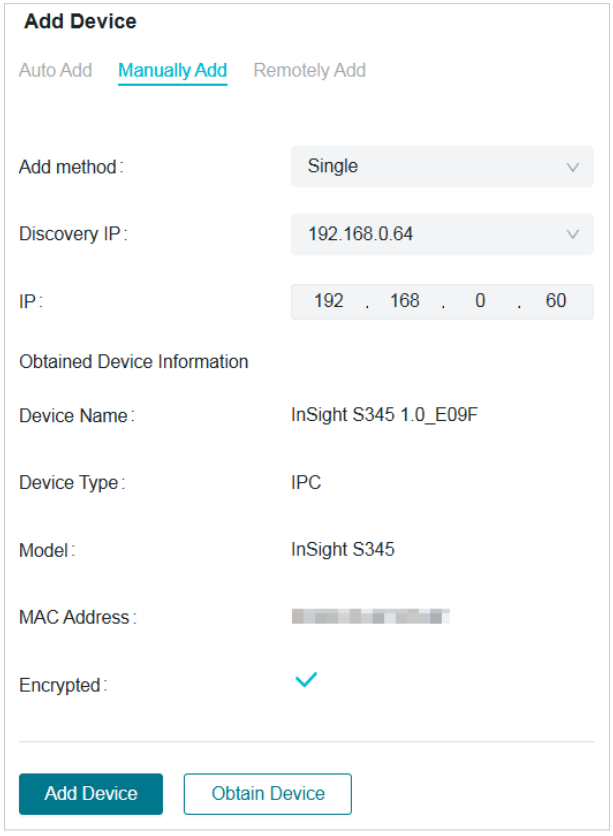
  2) Choose the device's IP from the **Discovery IP** drop-down.

  3) Enter the server's IP in the IP field.

  4) Click **Obtain Device**.



5) Review the **Obtained Device Information** and click **Add Device**.



To add devices via multiple IPs:

If the devices' IP addresses are in the same segment, include them in the VMS by specifying the starting and ending IP addresses.

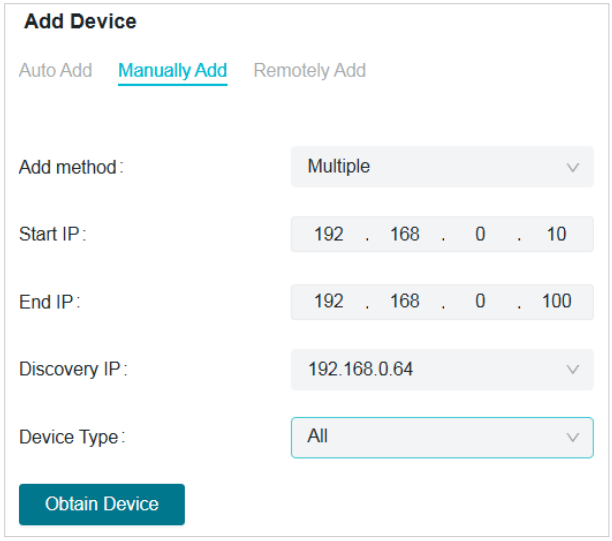
1) Select **Multiple** from the **Add method** drop-down.

2) Enter the **Start IP** and **End IP**.

3) Choose the device's IP from the **Discovery IP** drop-down.

4) Select the device type.

5) Click **Obtain Device**, review the **Obtained Device Information**, and click **Add Device**.



3. 3 Remotely Add Device

Step 1: Allow the device to access VMS.

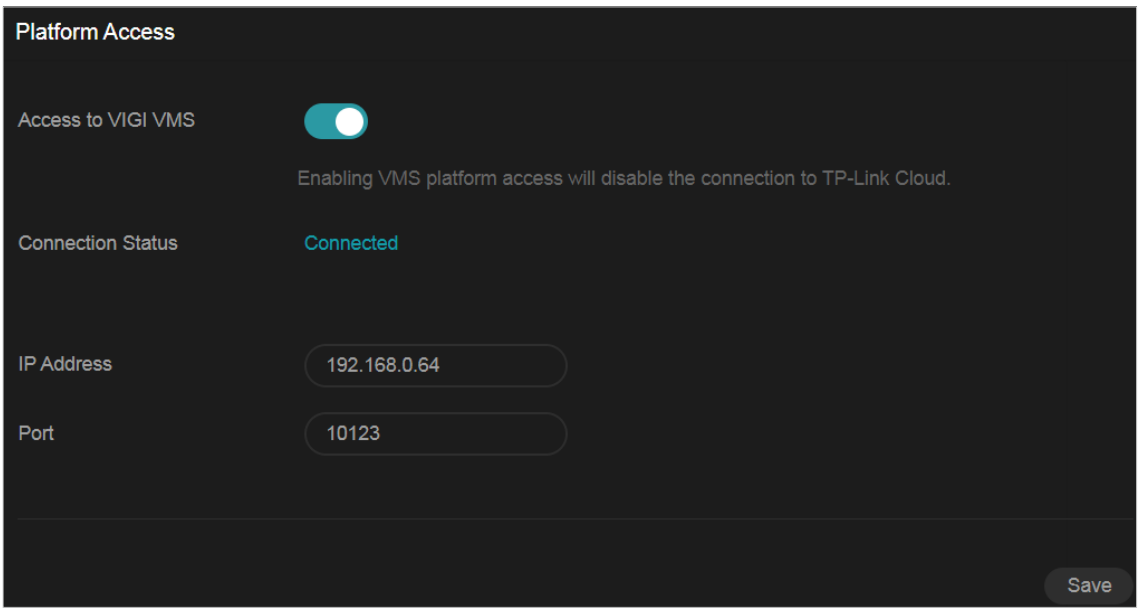
1) Open a web browser, type the device's IP address into the address bar, and press **Enter**.

2) On the device's web management page, navigate to **Settings > Network Settings > Platform Access**.

3) Enable **Access to VIGI VMS**.

4) Enter the IP address of the VMS server.

5) Set the Port to 10123 and click **Save**. After a few moments, if the **Registration Status** shows as Connected, the device has successfully linked to VMS.



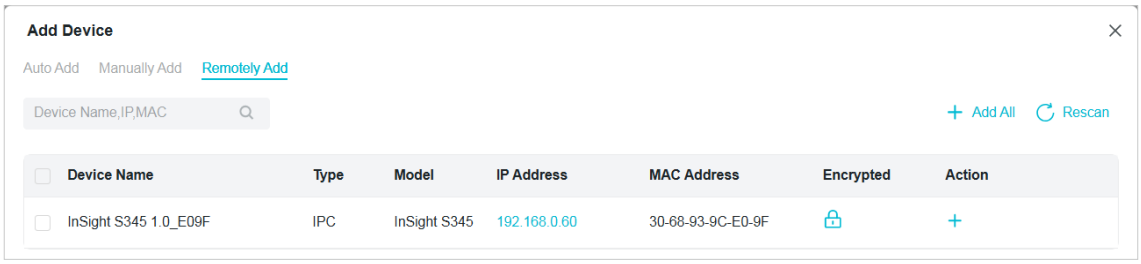
Step 2: Log in to VMS and follow the instructions to add the device remotely:

1) Click **Device** in the sidebar to enter the device management page.

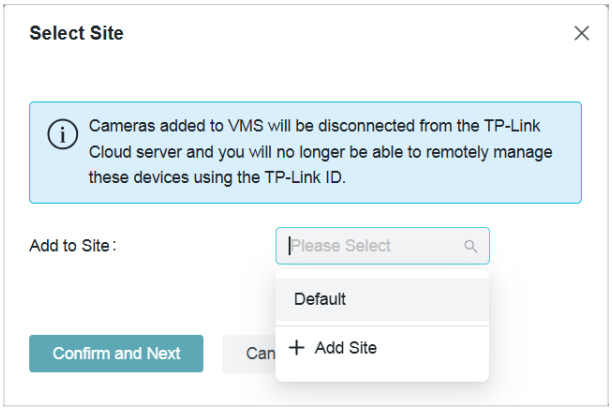
2) Click 

in the top right corner of the **Device List** to open the **Add Device** window. Click **Remotely Add**.

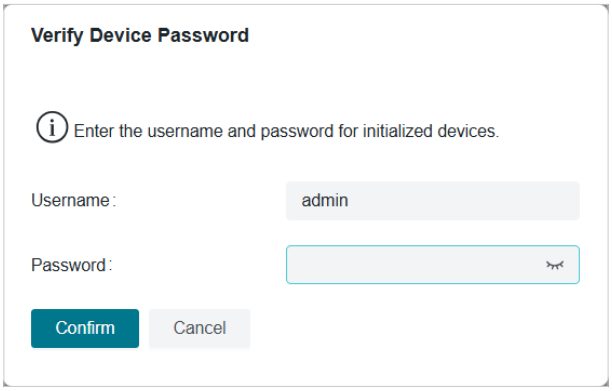
3) In the **Action** column next to the device you want to add, click  to open the **Select Site** window.



4) From the drop-down list of **Add to Site**, select the site where you wish to add the device and click **Confirm and Next**. If you need to create a new site, please refer to (Optional) Create a new site:



5) In the **Verify Device Password** window, input the device's username and password, and click **Confirm**.



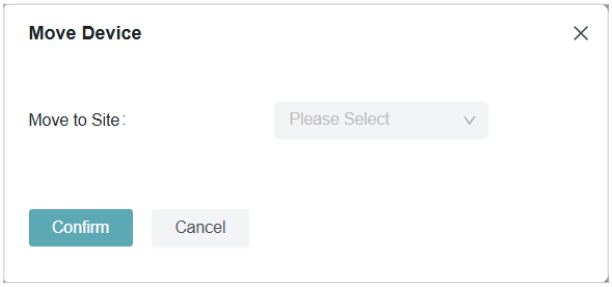
6) Return to the **Device List** page to check if the device is listed. If it appears, the device has been successfully added.

Note: If you remove a remote device from VMS, Access to VIGI VMS will be disabled on the device's web management page, allowing it to connect to other platforms. To reconnect the device to VMS remotely, you will need to re-enable Access to VIGI VMS on the device's web management page.

3. 4 Move Device to Another Site

To relocate devices to different sites, you can adjust the site settings after adding the device in the **Device List**.

1. Click , and the Move Device window will appear.



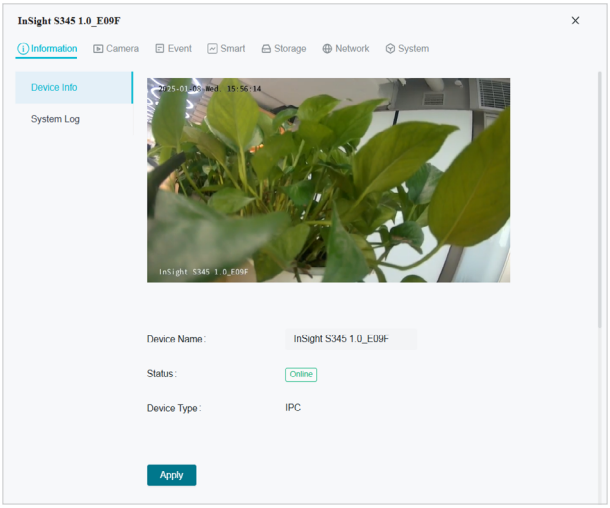
2. From the drop-down menu, choose the new site where you want the device to be transferred.
3. Click **Confirm** to finalize the move.

4

Change Camera Settings

This chapter guides you on how to change the settings of your monitoring devices via VIGI VMS. This chapter includes the following sections:

To change device settings, choose the site where your device is located, find your device in the list, and click . The parameters to modify include **Device Name**, **Local Upgrade**, **Video Settings**, **Smart Event**, **System Management**, **Network Settings**.



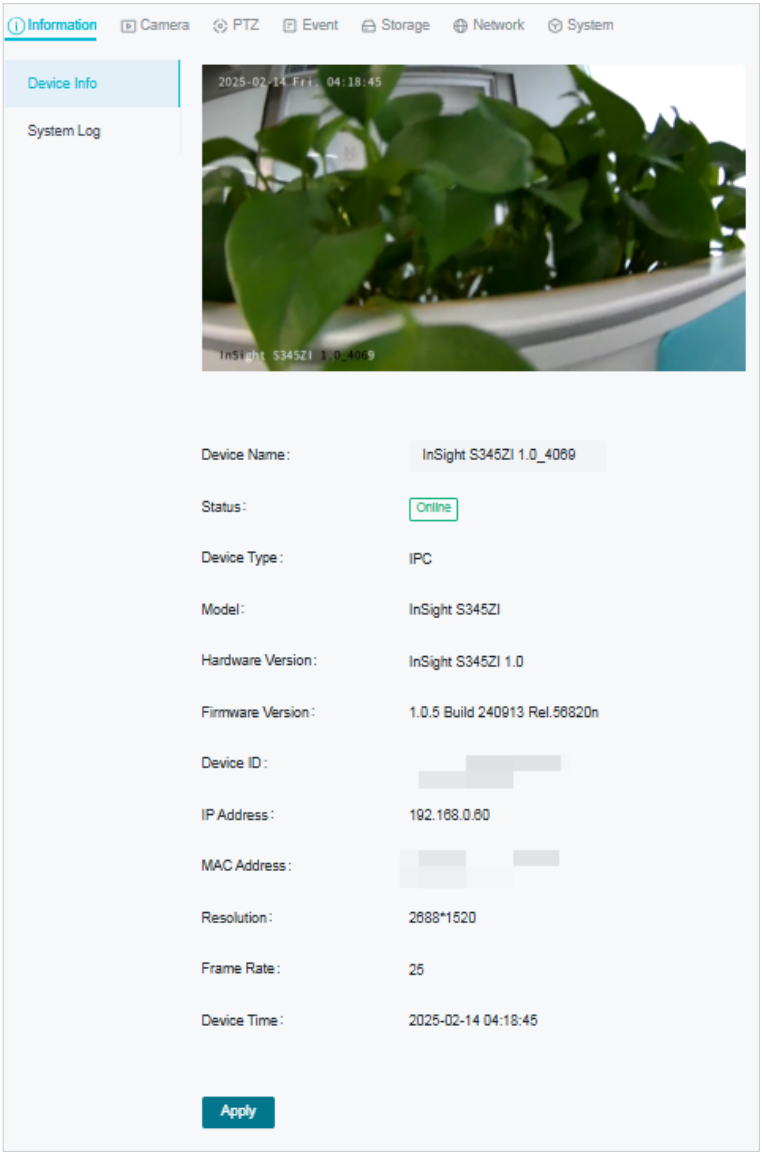
4. 1 Information

4. 1. 1 Device Information

You can view basic information about the camera, including device name, status, device type, model, hardware and firmware version, device ID, IP address, MAC address, resolution, frame rate, and device time.

1. Go to **Devices**, choose the site where your device is located, find your device in the list, and click .
2. In the panel that appears on the right, head over to **Information** > **Device Info**.

3. You may edit its name in the **Device Name** field and click **Apply**.

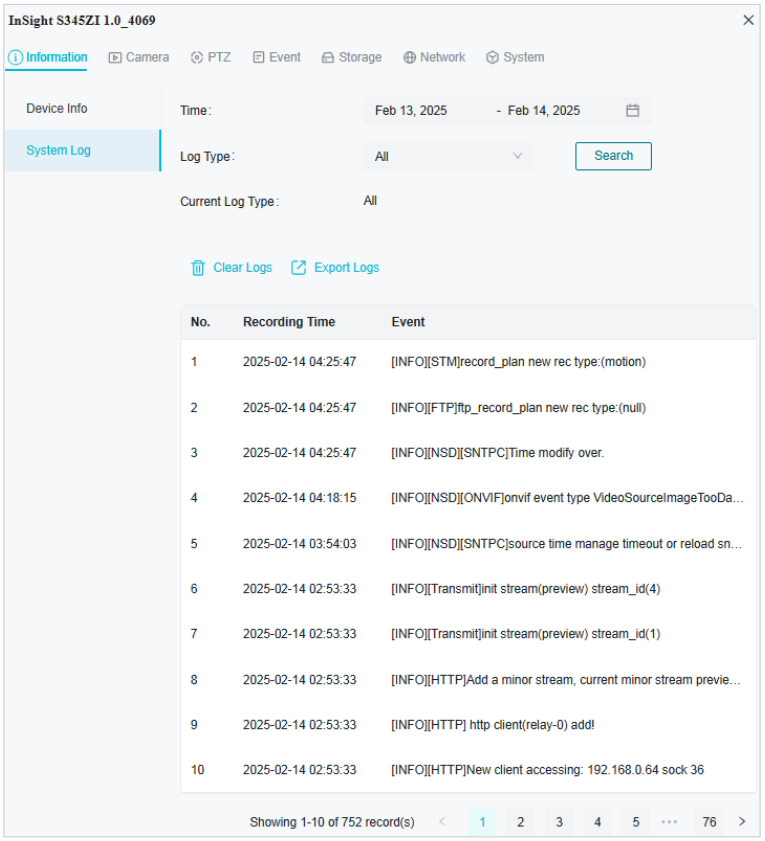


4. 1. 2 System Log

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

1. Go to **Devices**, choose the site where your device is located, find your device in the list, and click .
2. In the panel that appears on the right, head over to **Information** > **System Log**.

3. 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.



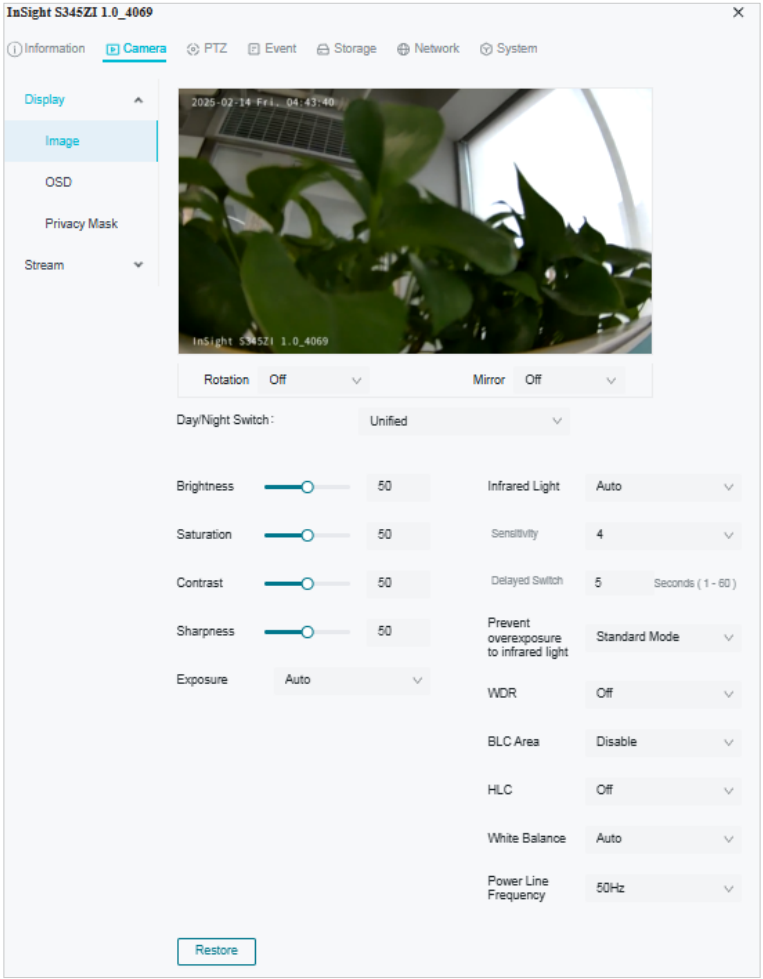
Start/End Time	Specify a time range to filter the logs based on the recording time.
Log Type	Select a type from the drop-down list to filter the logs. **All**: All types of logs. **Alarm**: Alarms triggered by events, such as tampering, line crossing, and area intrusion. **Exception**: Abnormal events 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. 2 Camera Display Settings

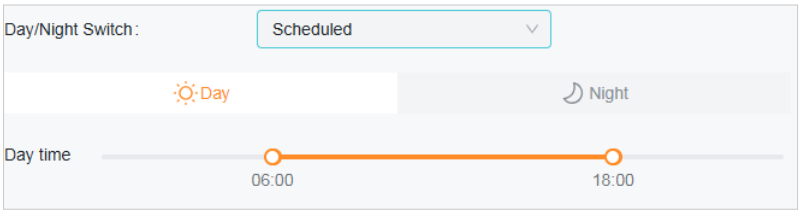
4. 2. 1 Image

You can adjust various image settings of your network camera to optimize video quality for different environments. You can modify parameters such as brightness, contrast, sharpness, exposure, and more, as well as configure advanced features like Day/Night switching, infrared light sensitivity, and white balance, Use these settings to fine-tune the camera's performance based on lighting conditions and specific monitoring needs.

1. Go to **Devices**, choose the site where your device is located, find your device in the list, and click .
2. In the panel that appears on the right, head over to **Camera** > **Display** > **Image**.
3. 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 **Center**, you rotate the image by 180 degrees around its center.
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.
Brightness	Increasing the value will lighten the image.
Saturation	Increasing the value will enrich the color of the image.
Contrast	Increasing the value will increase the difference between the brighter and darker parts.
Sharpness	Increasing the value will sharpen the image.
Infrared Light	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.

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 brighter the environment, the dimmer the infrared supplement light. **Enhanced Mode**: This mode intensifies its protection against overexposure, by darkening the bright areas of the image. **Manual**: Manually adjust the brightness of image. The higher the value is, the dimmer the image gets.
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.
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.
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 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.

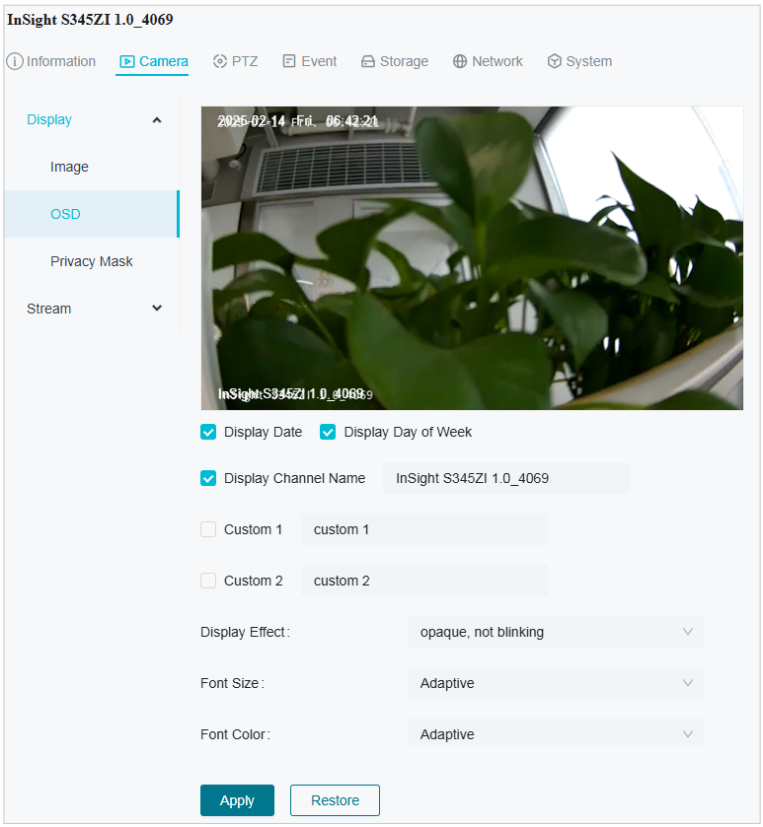
4. 2. 2 OSD

The OSD (On-Screen Display) settings interface allows you to customize the information displayed on the camera feed. You can choose to display key details such as the date, day of the week, and

channel name directly on the video stream. Additionally, you can adjust the display effect, including transparency and font size or color, to suit your preferences. This feature enhances video monitoring by providing relevant information without interrupting the live view, offering flexibility in how data is shown on-screen.

Follow the steps below to configure OSD settings.

1. Go to **Devices**, choose the site where your device is located, find your device in the list, and click .
2. In the panel that appears on the right, head over to **Camera** > **Display** > **OSD**.
3. Configure the following parameters, and click **Apply** to save your settings.



Display Date	Check the box to display the current date on the camera feed.
Display Day of the Week	Check the box to display the current date on the camera feed.
Display Channel Name	The camera's channel name can be displayed on the screen for easy identification. This option is enabled by default.
Custom Labels	You can add up to two custom labels (Custom 1 and Custom 2) by entering the desired text in the fields. This is useful for specific identifiers.
Display Effect	Choose the display effect for the on-screen text.

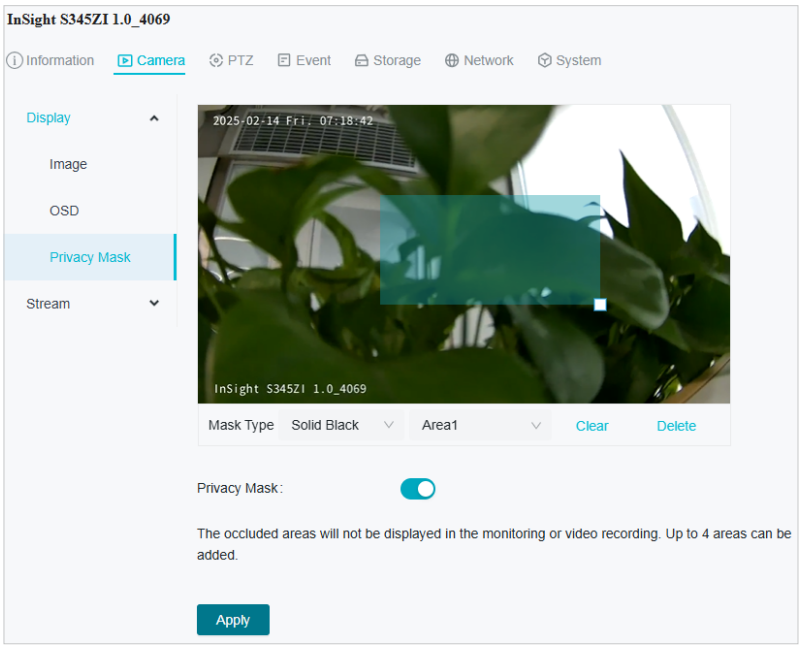
Font Size	Set the font size. You may select "Adaptive" to automatically adjust the font size based on the screen resolution or manually set the desired font size.
Font Color	Set the font color. You may choose "Adaptive" for the camera to automatically adjust the font color, or select a specific color for customization.
Restore	Click to revert to factory default settings.

4. 2. 3 Privacy Mask

Privacy Mask hides parts of the image from view, ensuring your privacy by preventing these areas from being recorded or monitored.

Follow these steps to configure the Privacy Mask:

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel that appears on the right, head over to **Camera** > **Display** > **Privacy Mask**.
3. Enable **Privacy Mask**. Enable Privacy Mask. Draw the desired privacy area on the preview screen (represented by the blue square in the image below). You can adjust the size and position by dragging the area. For the Mask Type, you can select either Solid Black or Mosaic to control the display effect of the masked area.



4. To remove a specific privacy area, select it and click **Delete**.
5. To remove all privacy areas, click **Clear**.
6. Click **Apply**.

4. 3 Camera Stream Settings

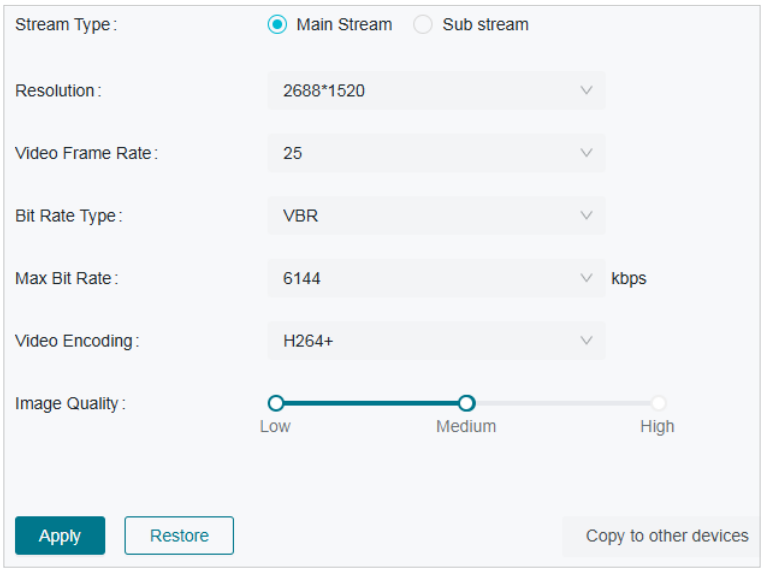
In Stream Settings, you can configure video stream levels, change the audio output settings and ROI (Region of interest) level.

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. 3. 1 Video

Follow the steps below to configure video settings.

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel that appears on the right, head over to **Camera** > **Stream** > **Video**.
3. Configure the following parameters, and click **Apply**.



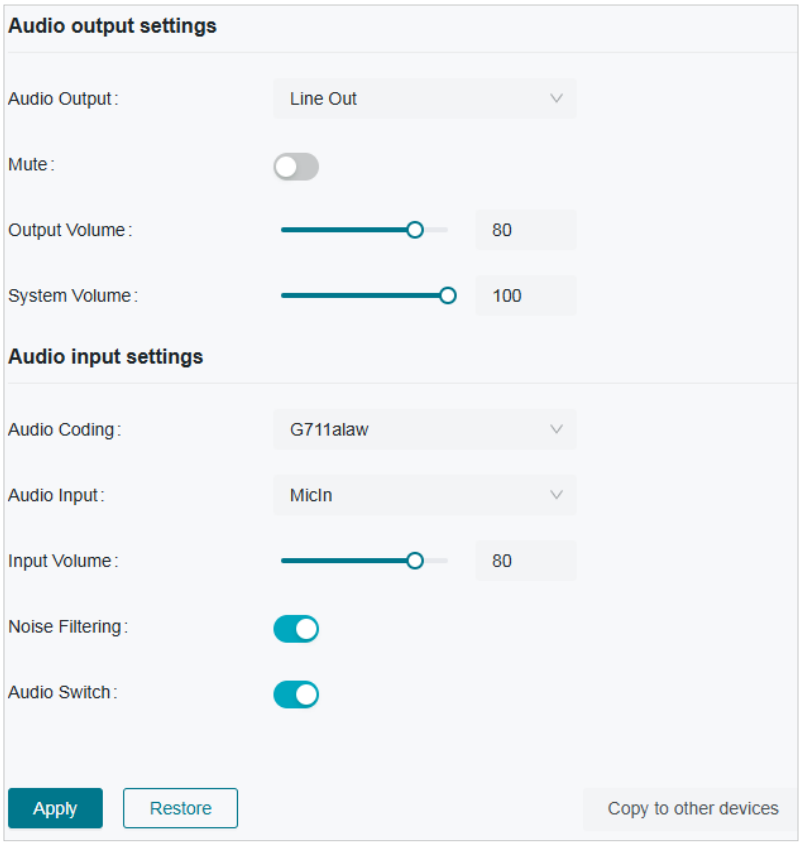
Stream Type	Main Stream is the primary video feed used for recording and provides the highest video quality. It has higher definition and higher bandwidth than sub-stream. Sub-stream is a secondary video feed that is used mainly for remote viewing from computers from outside the network.
Resolution	The 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.

Max Bit Rate	Specify the upper limit of bit rate.
Video Encoding	Select the encoding type of the stream. H.265 reduces the file size and saves the bandwidth better than H.264.
Image Quality	When VBR is selected as the Bit Rate Type, set the video quality as high, medium, or low.
Restore	Click to revert to factory default settings.
Copy to Other Devices	Use this option to apply these settings to other devices in your system.

4. 3. 2 Audio

Follow the steps below to configure video settings.

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Camera** > **Stream** > **Audio**.



Audio Output	Choose the desired audio output option.
Mute	Toggle to turn the audio on or off. When enabled, it silences the output.
Output Volume	Adjust the volume of the audio output by moving the slider.

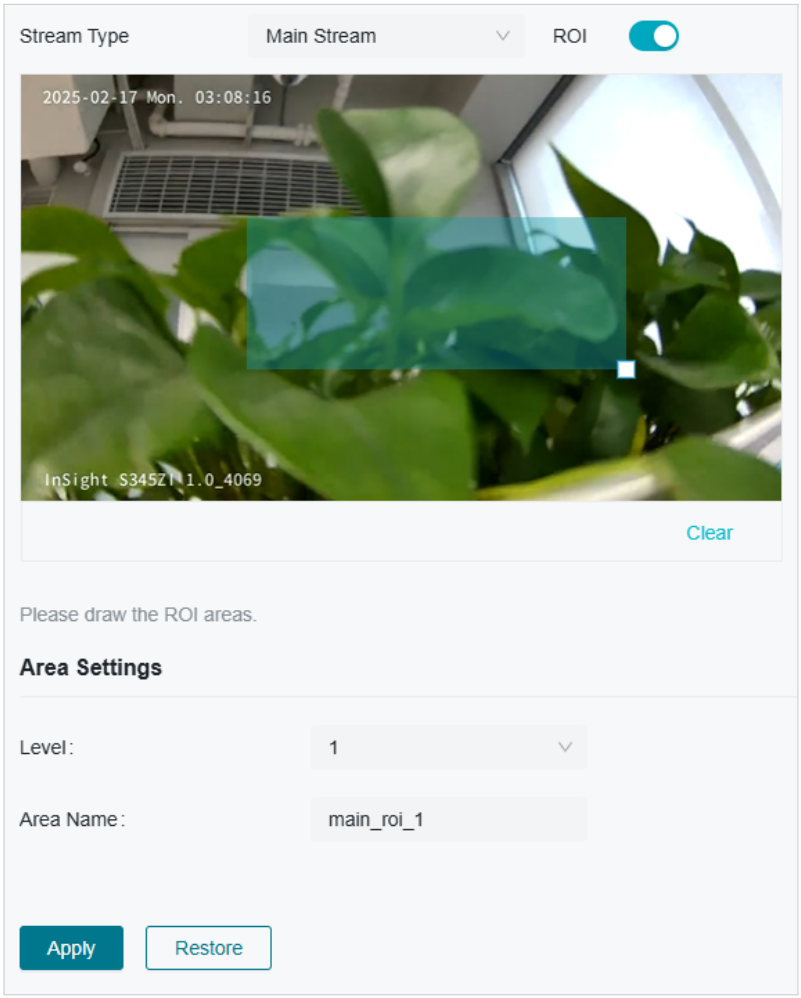
System Volume	This controls the overall system's audio level. The higher the setting, the louder the system's audio will be.
Audio Coding	Select an audio encoding type. Audio Coding is the process of converting analog audio into digital data by compressing it for efficient storage or transmission. The default option, G711alaw, is a codec used to encode and compress audio signals for clear voice transmission, primarily used in Europe, with a focus on low-latency, high-quality voice communication.
Audio Input	Select the input source for audio.
Input Volume	Adjust the volume of the input device by moving the slider.
Noise Filtering	Enable this option to filter out background noise from the audio input. When activated, it helps improve the clarity of the captured sound, especially in noisy environments.
Audio Switch	This toggle controls whether the audio input is active. Turn it on to allow the device to capture sound, and off to disable audio input.
Restore	Click to revert to factory default settings.
Copy to Other Devices	Copy the current settings to other devices within your system.

4. 3. 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 **Devices**. Select the site where your device is located, find the device in the list, and click  .
2. In the panel on the right, go to **Camera** > **Stream** > **ROI**.

3. 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 **Apply**.



4. 3. 4 Advanced Settings

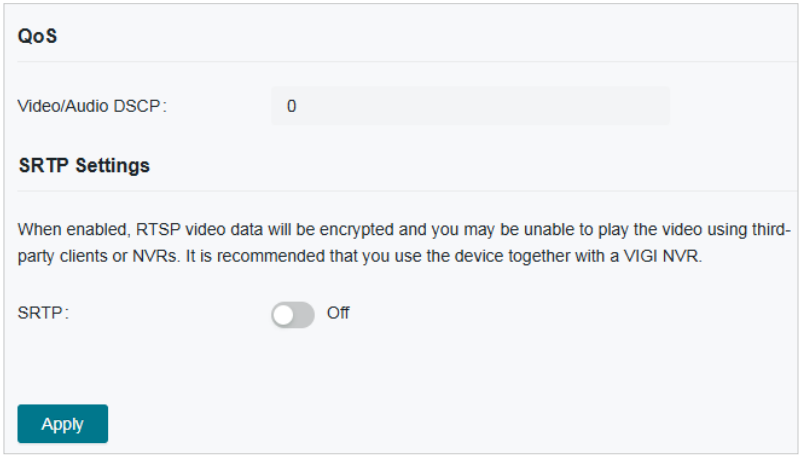
In Advanced Settings, you can set QoS and SRTP.

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 uni-cast and multi-cast applications.

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .

2. In the panel on the right, go to **Camera** > **Stream** > **Advanced Settings**.



3. Set Video/Audio DSCP.

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

4. 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.

5. Click **Apply**.

4. 4 PTZ (Only for Models with Motorized Lens)

VIGI VMS provides PTZ control operations via control panel, such as zoom in, zoom out, and auxiliary focus. You can also open a new window for controlling the PTZ.

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .

2. In the panel on the right, go to **PTZ** and configure the following parameters.

	Zoom Out	(Only for certain cameras) Click to zoom out the live image.
	Zoom In	(Only for certain cameras) Click to zoom in the live image.
	Focus -	(Only for certain cameras) Shorten the focal length.
	Focus +	(Only for certain cameras) 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.

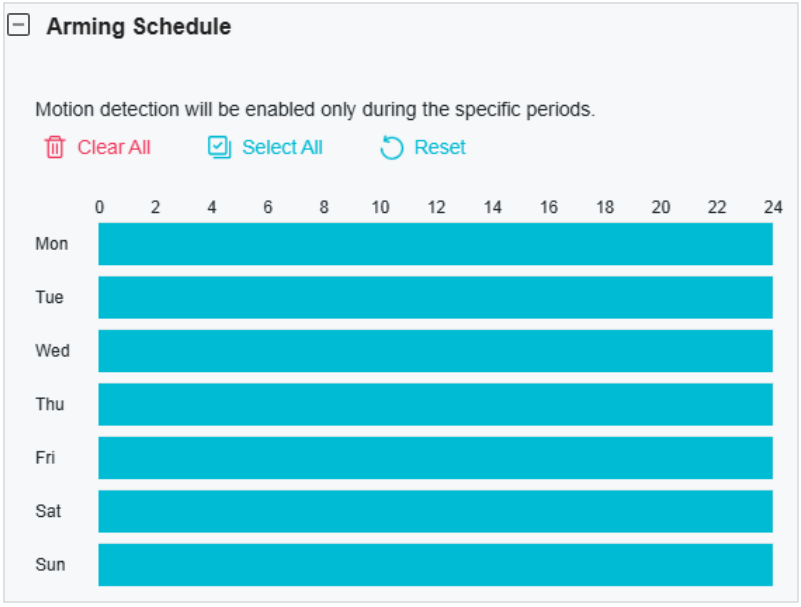
4. 5 Event

This feature enables you 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:

4. 5. 1 Arming Schedule and Processing Mode

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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** and locate Arming Schedule and Processing Mode in the related event interface.

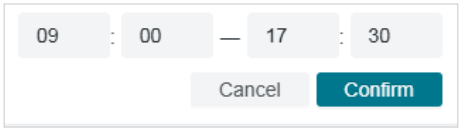


3. Drag the time bar to draw desired valid time.

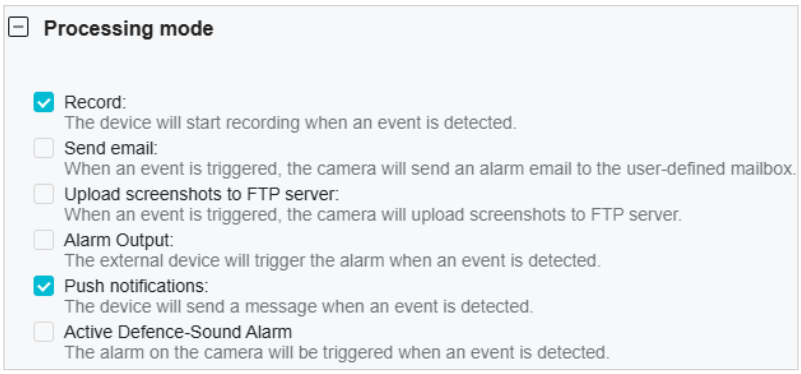
Note:

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

4. Double click the time block you have drawn and a pop up window will appear. Fine-tune the start time and end time (with an accuracy of a minute) and click **Confirm**. You may copy a schedule for a day to any other days.

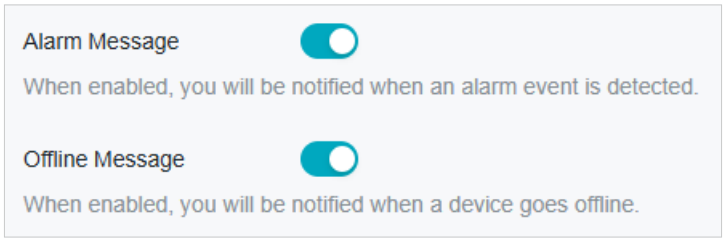


5. Set processing modes as needed.



4. 5. 2 Message

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Message** and configure the following parameters.

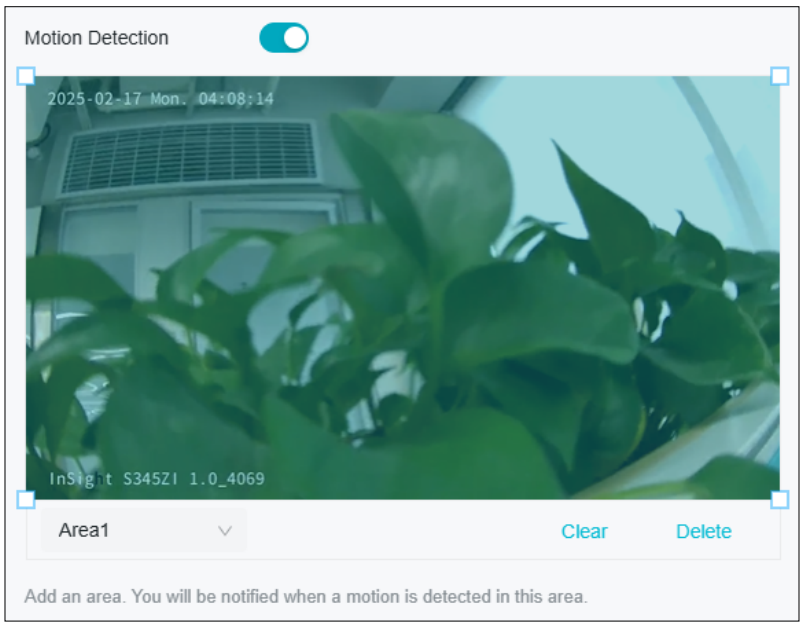


4. 5. 3 Motion Detection

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 **Devices**. Select the site where your device is located, find the device in the list, and click .

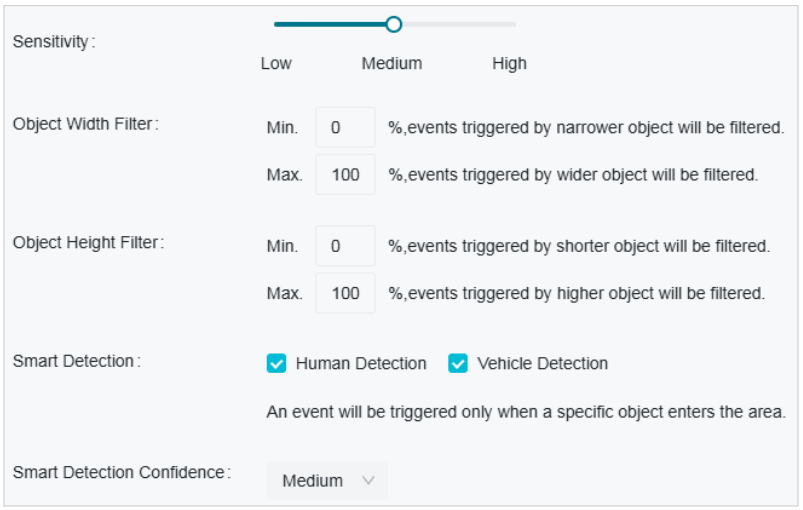
2. In the panel on the right, go to **Event** > **Basic Event** > **Motion Detection**.



3. 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 drag the whole area to move it. You may delete a selected area and clear all areas.

   Note: You may customize up to four areas.

4. 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.

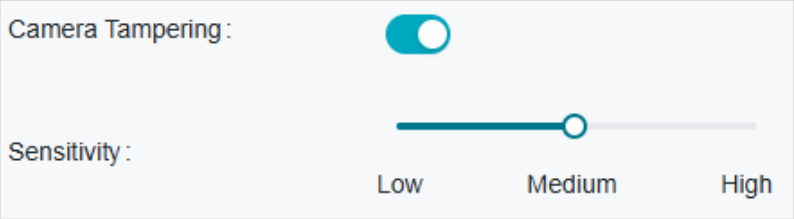
Smart Detection	Choose whether you want to detect humans only, vehicles only, or both. The function is available only for cameras which support human detection and vehicle detection.
Smart Detection Confidence	Select the detection type from High, Medium, and Low. The function is available only for the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

5. Refer to Arming Schedule and Processing Mode for settings if needed.
6. Click **Apply**.

4. 5. 4 Camera Tempering

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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Basic Event** > **Camera Tempering**.



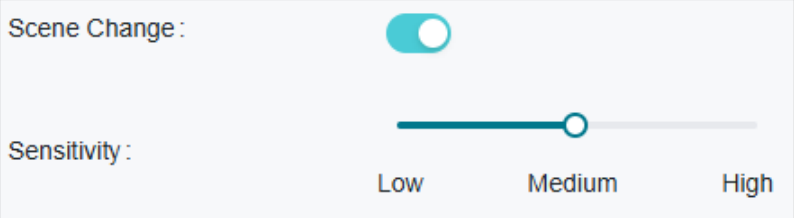
3. Enable **Camera Tampering**.
4. Set the sensitivity of video tampering. A higher value can trigger the alarm actions more easily.
5. Refer to Arming Schedule and Processing Mode for settings if needed.
6. Click **Apply**.

4. 5. 5 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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Basic Event** > **Scene Change**.

3. Click the toggle to turn on **Scene Change**.



4. Specify **Sensitivity**. The higher the value is, the more easily the change of the scene can be detected.
5. Refer to Arming Schedule and Processing Mode for settings if needed.
6. Click **Apply**.

4. 5. 6 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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Smart Event** > **Line Crossing Detection**. Click the toggle to turn it on.

3. 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.
Smart Detection	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.
Smart Detection 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.

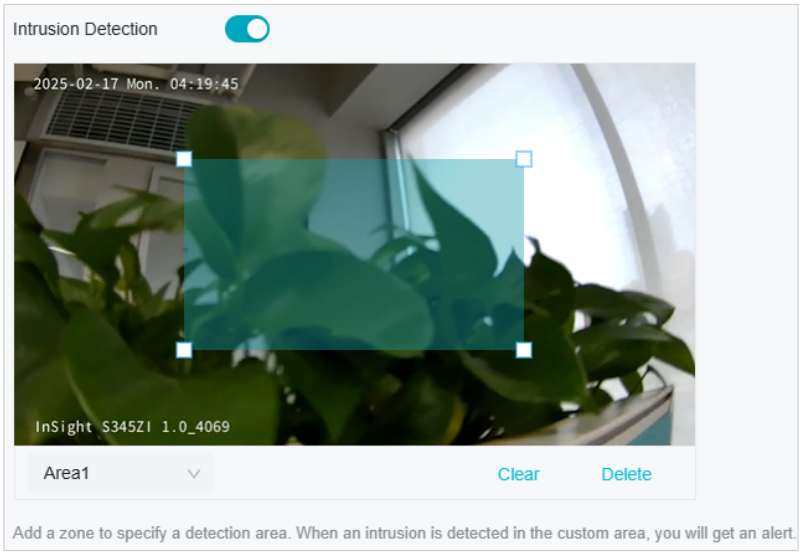
4. Refer to Arming Schedule and Processing Mode for settings if needed.
5. Click **Apply**.

4. 5. 7 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 **Devices**. Select the site where your device is located, find the device in the list, and click  .

2. In the panel on the right, go to **Event** > **Smart Event** > **Intrusion Detection**. Click the toggle to turn it on.



3. 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.

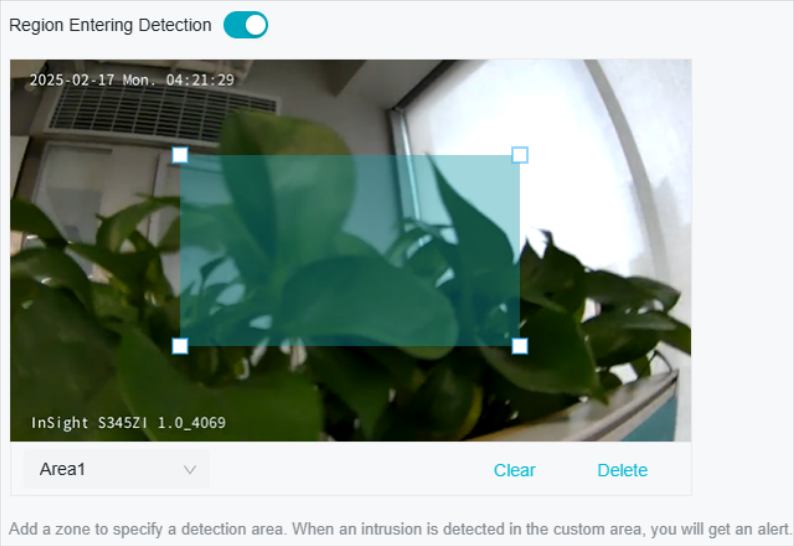
Sensitivity	The higher the value is, the more easily an intrusion action can be detected.
Percentage	Set the percentage of intrusion detection. When an object takes up the specific percentage of the area, the alarm actions will be triggered.
Intrusion Time	Intrusion time stands for the threshold a target 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.
Smart Detection	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.
Smart Detection 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 Processing Mode for settings if needed.
5. Click **Apply**.

4. 5. 8 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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Smart Event** > **Region Entering Detection**. Click the toggle to turn it on.



3. 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.

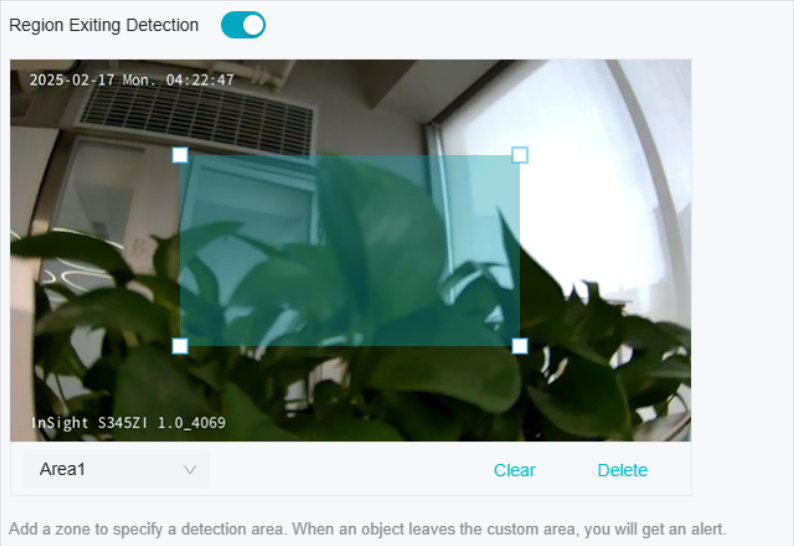
Sensitivity	Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.
Object Width Filter	Set the minimum and maximum width for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.
Object Height Filter	Set the minimum and maximum height for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.
Smart Detection	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.
Smart Detection 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 Processing Mode for settings if needed.
5. Click **Apply**.

4. 5. 9 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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Smart Event** > **Region Exiting Detection**. Click the toggle to turn it on.



3. 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.

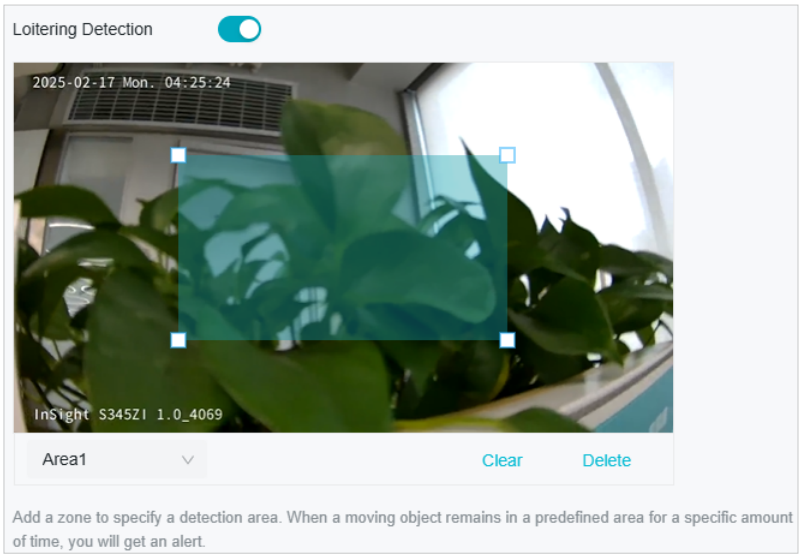
Sensitivity	Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.
Object Width Filter	Set the minimum and maximum width for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.
Object Height Filter	Set the minimum and maximum height for the target to be detected. Only targets with sizes between the maximum and minimum value will be detected.
Smart Detection	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.
Smart Detection 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 Processing Mode for settings if needed.
5. Click **Apply**.

4. 5. 10 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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Smart Event** > **Loitering Detection**. Click the toggle to turn it on.



3. 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.

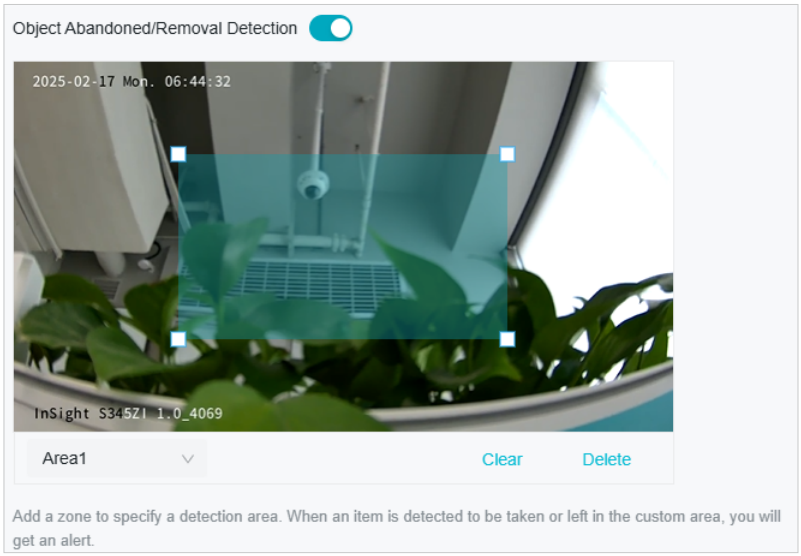
Sensitivity	Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.
Loitering Time	It stands for the threshold for the time of the object loitering in the region. If the time that one object stays exceeds the threshold, the alarm is triggered.
Object Width Filter	Set the 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.
Smart Detection	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.
Smart Detection 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 Processing Mode for settings if needed.
5. Click **Apply**.

4. 5. 11 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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Smart Event** > **Object Abandoned/Removal Detection**. Click the toggle to turn it on.



3. 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.

4. Refer to Arming Schedule and Processing Mode for settings if needed.
5. Click **Apply**.

4. 5. 12 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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Smart Event** > **Abnormal Sound Detection**. Click the toggle to turn it on.

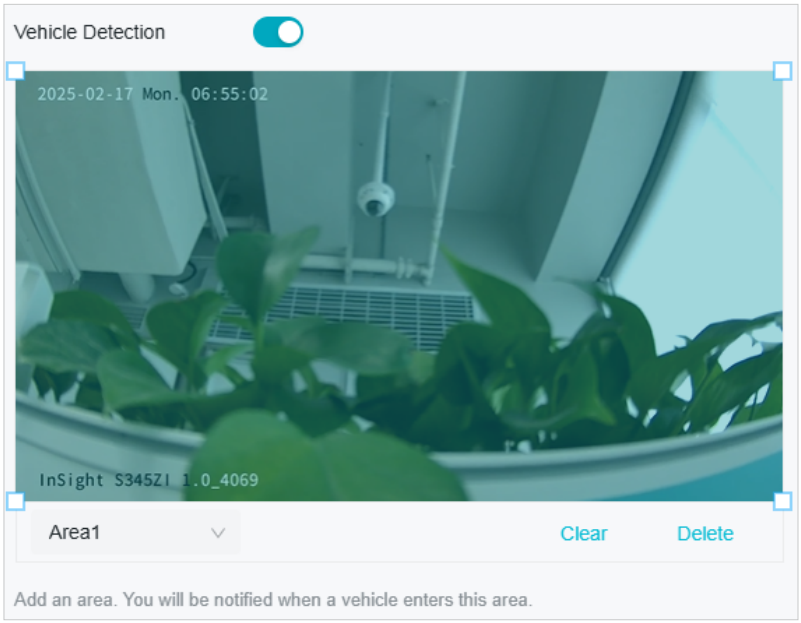
3. Adjust the value of sensitivity and alert threshold. The higher the sensitivity and the lower the threshold, the easier it gets to trigger linkage methods.
4. Refer to Arming Schedule and Processing Mode for settings if needed.
5. Click **Apply**.

4. 5. 13 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 **Devices**. Select the site where your device is located, find the device in the list, and click .

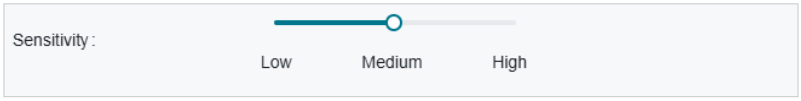
2. In the panel on the right, go to **Event** > **Smart Event** > **Abnormal Sound Detection**. Click the toggle to turn it on.



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

   Note: You may draw up to four areas.

4. Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.



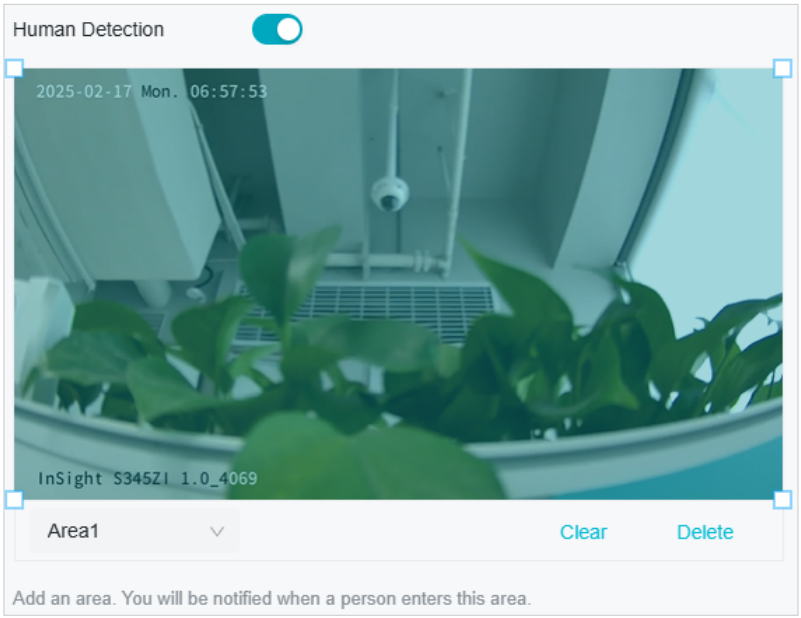
5. Refer to Arming Schedule and Processing Mode for settings if needed.
6. Click **Apply**.

4. 5. 14 Human Detection

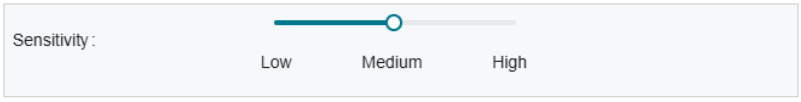
Human detection triggers alarm actions when cameras detect persons are moving in the specified areas. You can customize the area settings, select the triggered actions and set the alarm schedule. Follow the steps below to finish the configuration.

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .

2. In the panel on the right, go to **Event** > **Smart Event** > **Abnormal Sound Detection**. Click the toggle to turn it on.



3. Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.

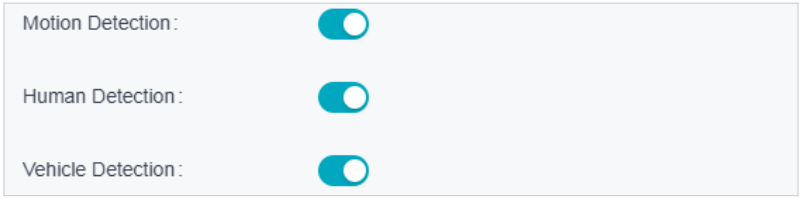


4. Refer to Arming Schedule and Processing Mode for settings if needed.
5. Click **Apply**.

4. 5. 15 Smart Frame

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

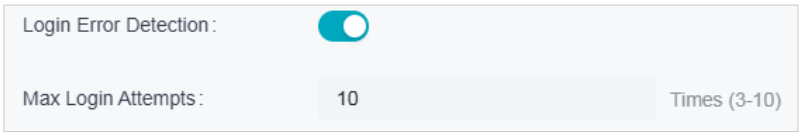
1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Smart Event** > **Abnormal Sound Detection**. Click the toggle to turn it on.
3. Click the toggles to specify the type of detection: motion, human, or vehicle. You may enable more than one types. Click **Apply**.



4. 5. 16 Access Exception

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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Exception Event** > **Access Exception**. Click the toggle to turn it on.



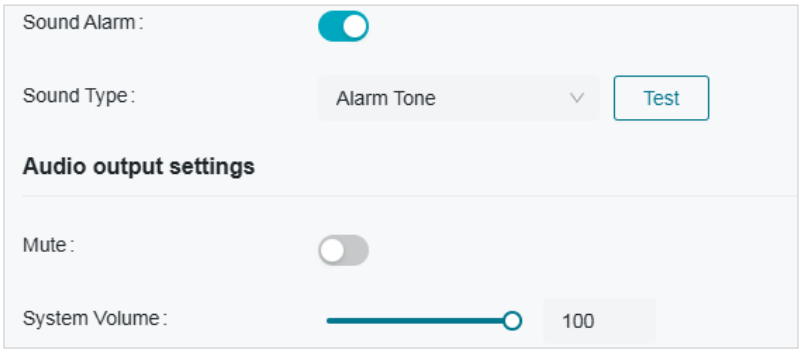
3. Enable **Login Error Detection** to limit the login attempts:
4. Set the maximum login attempts. The number should between 3 and 10
5. Click **Apply**.

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

4. 5. 17 Sound Alarm

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

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Active Defence** > **Sound Alarm**. Click the toggle to turn it on. Select the **Alarm Type**, and click **Test**.

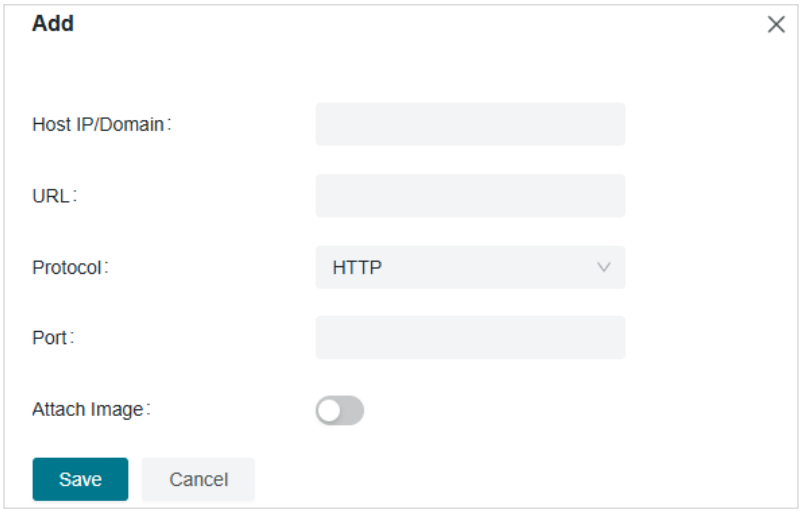


3. Under Audio Output Settings, click the toggle to mute or drag the slide bar to set the system volume.
4. Refer to Arming Schedule and Processing Mode for settings if needed.
5. Click **Apply**.

4. 5. 18 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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Alarm Server**.
3. Click **Add**.



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

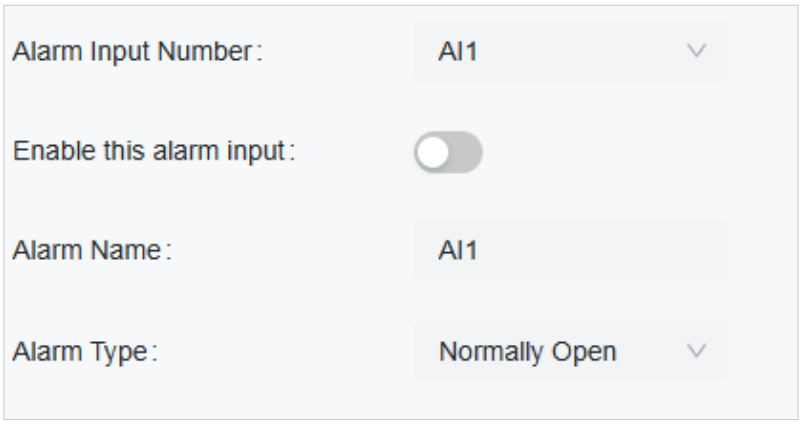
   Note: HTTP and HTTPS are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.

5. Click **Save**.

4. 5. 19 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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Alarm Device** > **Alarm Input**.



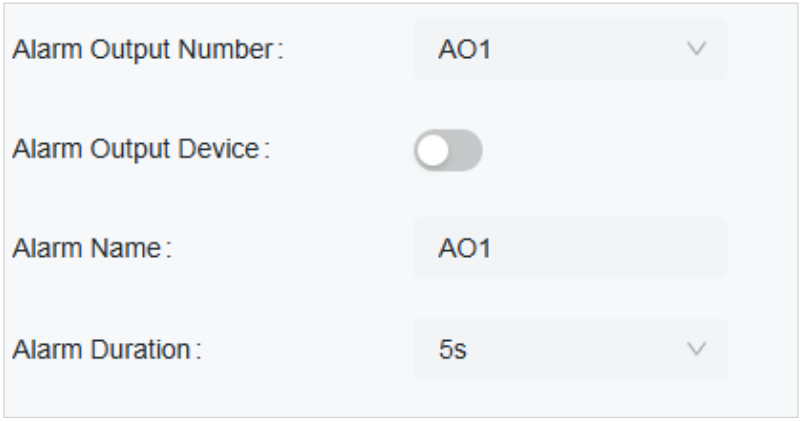
3. Select an Alarm Input Number.
4. Check Enable This Alarm Input.

5. Edit the Alarm Name.
6. Select the Alarm Type from the drop-down 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.
7. Refer to Arming Schedule and Processing Mode for settings if needed.
8. Click **Apply**.

4. 5. 20 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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Event** > **Alarm Device** > **Alarm Output**.



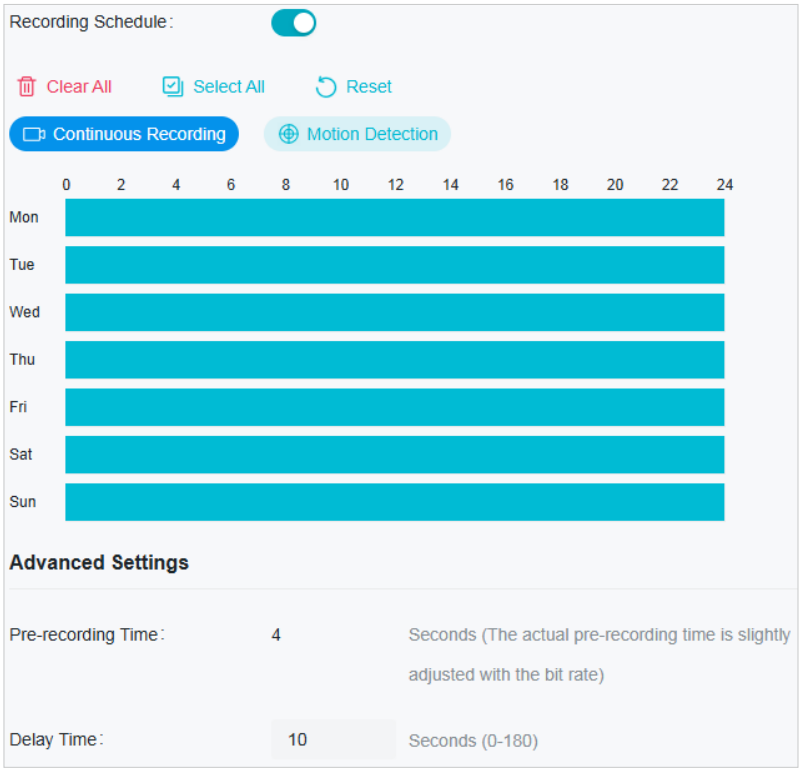
3. Select the Alarm Output Number according to the alarm interface connected to the external alarm.
4. Enable the Alarm Output Device.
5. Edit the Alarm Name.
6. Select the Alarm Duration from the drop-down list.
7. Refer to Arming Schedule and Processing Mode for settings if needed.
8. Click **Apply**.

4. 6 Storage

4. 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.

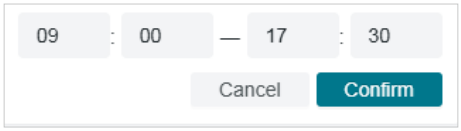
1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Storage** > **Recording Schedule**.



3. Enable **Recording Schedule**, select Continuous Recording or Motion Detection, then select the time period.

Continuous Recording	The camera will record continuously.
Event Recording	The camera will record when a movement 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.

4. Double click the time block you have drawn and a pop up window will appear. Fine-tune the start time and end time (with an accuracy of a minute) and click **Confirm**. You may copy a schedule for a day to any other days.

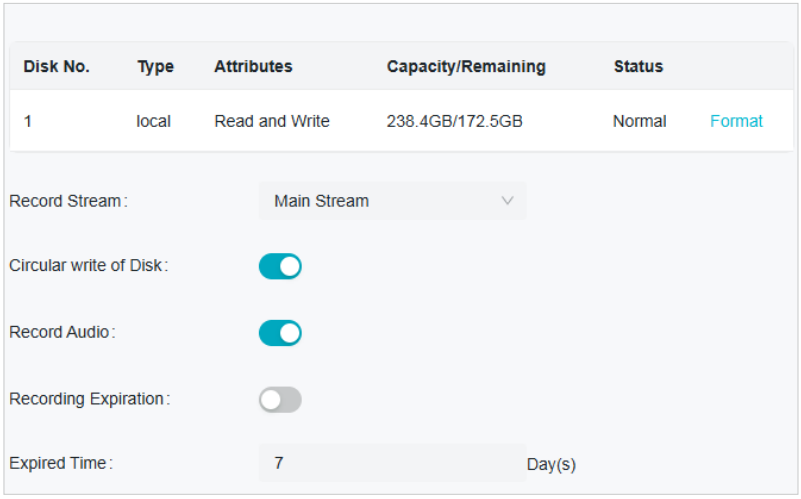


5. Click **Apply**.

4. 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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Storage** > **Storage Management**.



3. Click **Format** to initialize the memory card.

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

4. 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. **Sub-stream** 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 cannot be recovered.
Expired Time	Set the time when recordings will be automatically deleted.

5. Click **Apply**.

4. 7 Network

With proper network configurations, you can connect your camera to the Internet, build up mapping between internal and external ports.

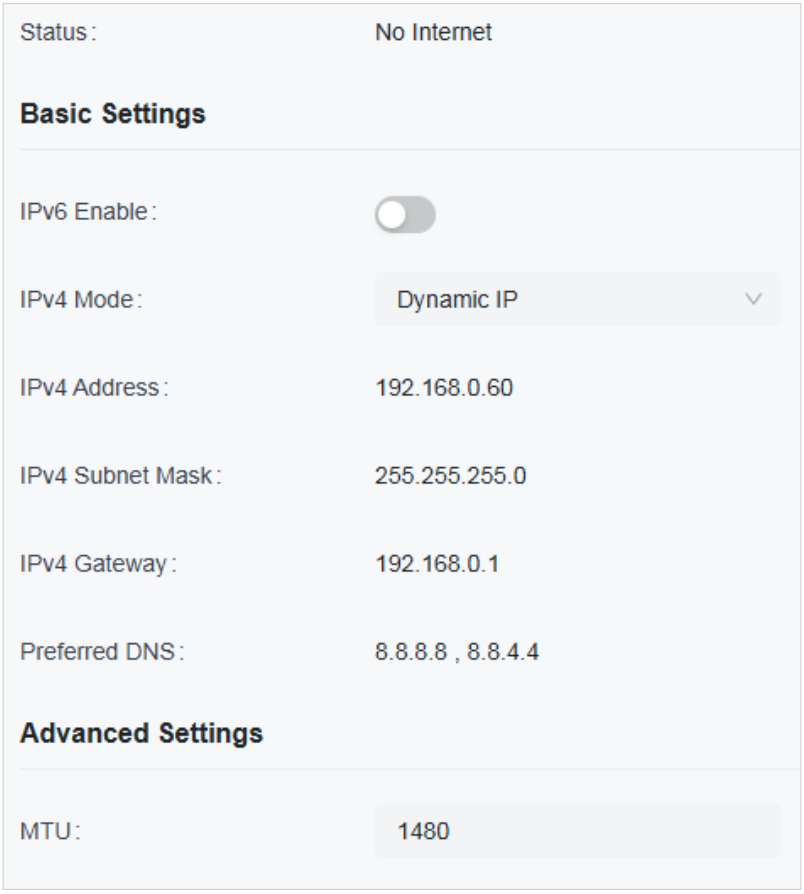
4. 7. 1 Internet Connection

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 **Devices**. Select the site where your device is located, find the device in the list, and click  .

2. In the panel on the right, go to **Network** > **Internet Connection**.



Status	Displays the current Internet status.
IPv6 Enable	Enable to configure IPv6 settings. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other. Three IPv6 modes are available. **Router Advertisement**: The IPv6 address is generated by combining the route advertisement and the device Mac address. Note that this mode requires the support from the router that the device is connected to. **DHCP**: The IPv6 address is assigned by the server, router, or gateway. **Manual**: Input IPv6 Address, IPv6 Subnet Mask, and IPv6 Gateway. Consult the network administrator for required information.
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.
Preferred / Alternative DNS	Enter the IP address of the DNS server.
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.
Adaptive IP	Enable this option if you want to set the camera's IP to change according to the network topology.

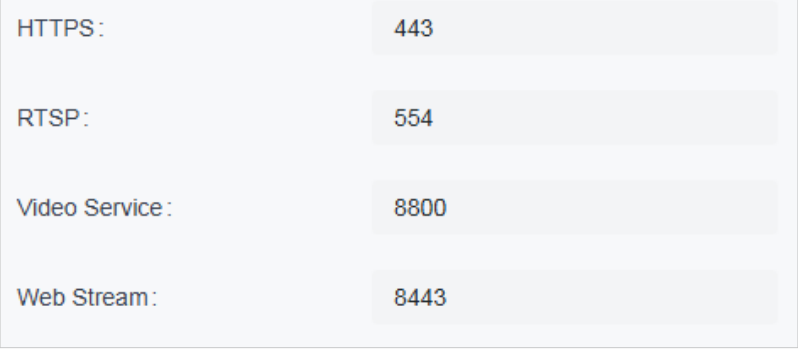
Note: The cameras should be in the same segment with the NVR, so that the NVR can discover and manage them.

3. Click **Apply**.

4. 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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Network** > **Port**.



3. Specify HTTPS port and service port.

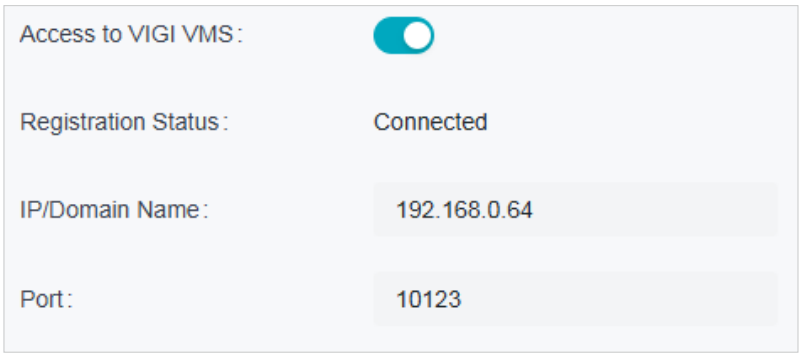
HTTPS	Specify a port for HTTPS protocol.
RTSP	Specify a port for RTSP (Real Time Streaming Protocol) protocol. RTSP is an application layer protocol for connecting, transferring, and streaming media data in real time from IP cameras connected to the network. rtsp://username:password@ip:port/streamNo 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.
Video Service	Specify a port for protocols of video services.
Web Stream	Specify a port to access the camera's live streaming web interface.

4. Click **Save**.

4. 7. 3 Platform Access

You can access a specific IP camera to the VIGI VMS with the Platform Access enabled.

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Network** > **Platform Access**.
3. Enable Access to VIGI VMS.

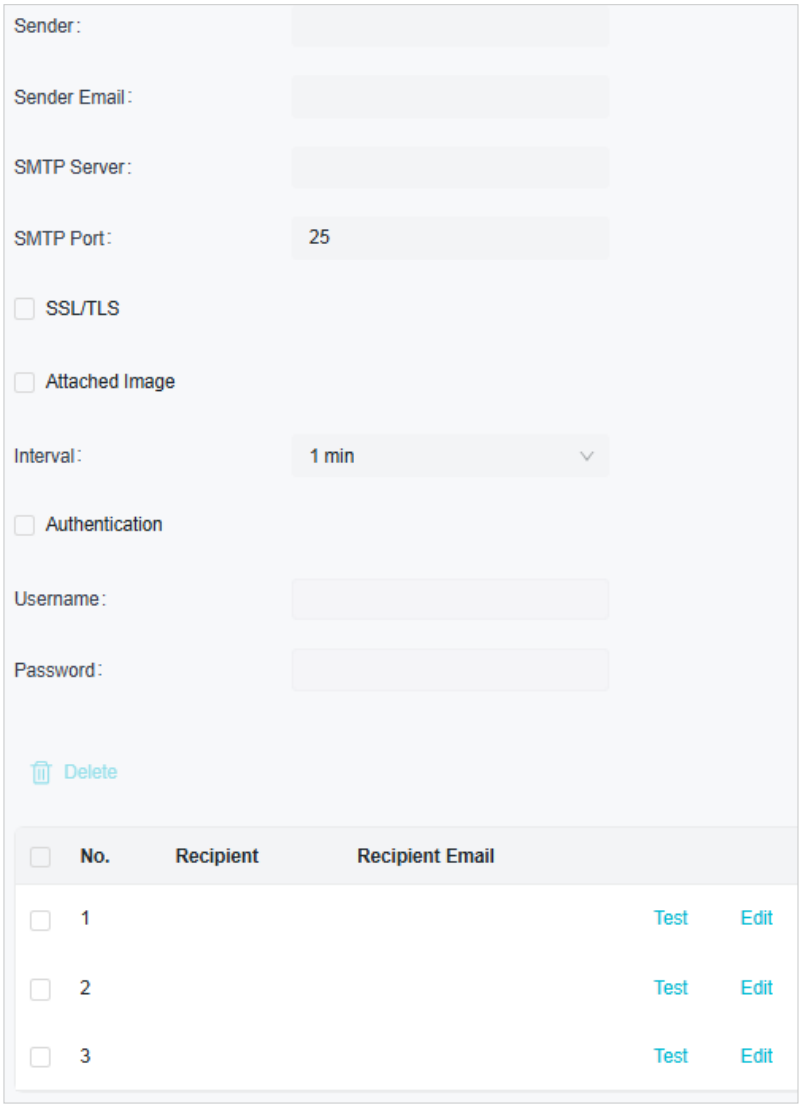


4. Enter the IP Address and the Port number.
5. Click **Apply**.

4. 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. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Network** > **Email**.



3. Input the sender's email information, including the Sender's name, Sender Email, SMTP Server, and SMTP Port. It is recommended to configure the SMTP port number to the default value of 25.
4. Enable SSL/TLS if needed and emails will be sent after encrypted.
5. 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.
6. If your email server requires authentication, check Authentication and input your username and password to log in to the server.
7. Click **Edit** to Input the recipient's information, including the recipient's name and address.

8. Click **Test** to see if the function is well configured.
9. Click **Apply**.

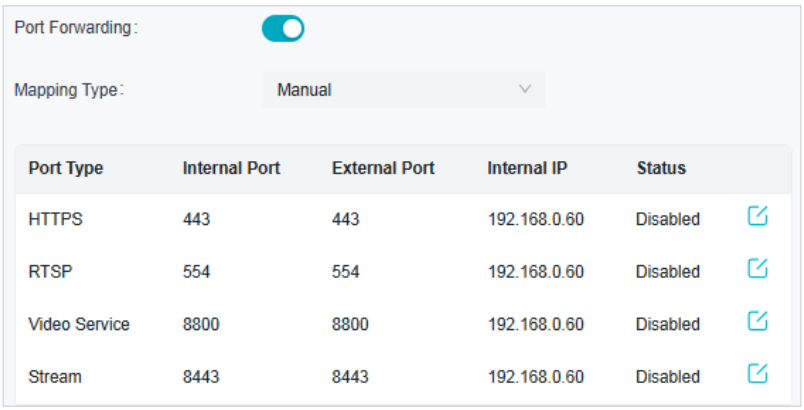
4. 7. 5 Port Forwarding

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 **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Network** > **Port Forwarding**.
3. 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.
Restore	Click to restore the settings to default factory settings.

4. 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,

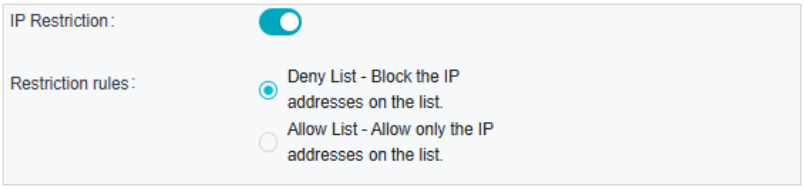
and Port is the number of RTSP external port. N can be number 1 or 2 that indicates the stream, 1 for main stream and 2 for sub-stream.

4. 7. 6 IP Restriction

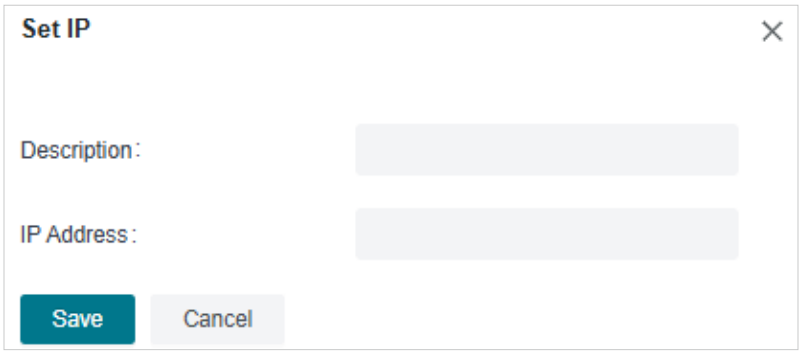
When IP Restriction is enabled, you can add IP addresses to the deny list or allow list to restrict the access to the camera. The IP address in the deny list cannot access the camera, while only the IP addresses in the allow list can access the camera.

Follow the steps below to configure IP Restriction.

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Network** > **IP Restriction**.
3. 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.



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



5. Click **Save**.

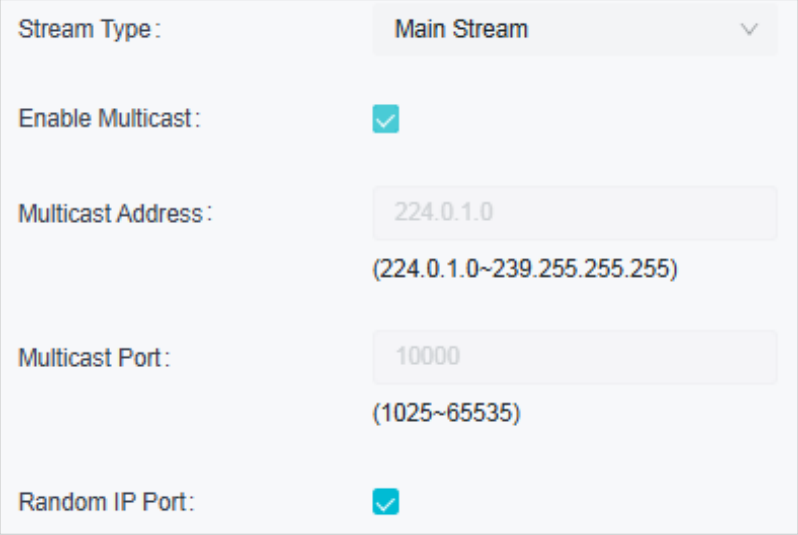
4. 7. 7 Multicast

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

Follow the steps below to configure Multicast.

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Network** > **IP Restriction**.

3. Select the stream type, then enable **Multicast**.



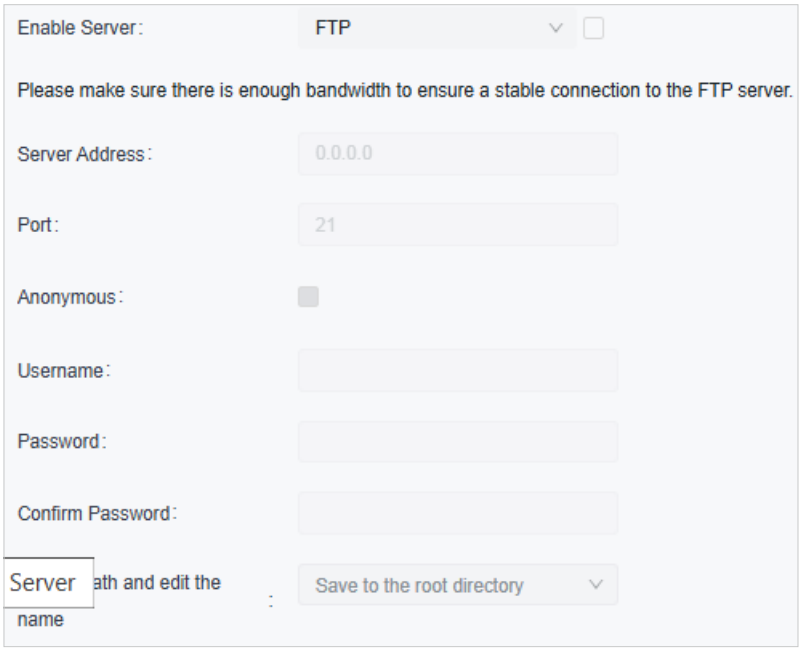
4. Disable Random IP Port and specify a static address and port, or enable Random IP Port.
5. Click **Apply**.

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.

4. 7. 8 Server

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

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Network** > **FTP Settings** > **Server**.



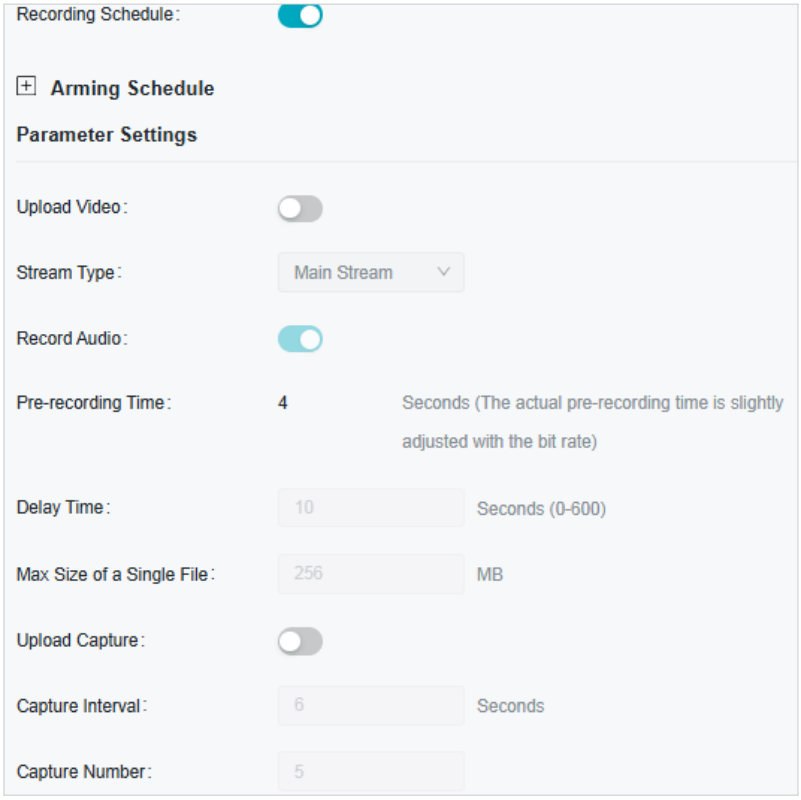
3. Check Enable Server. FTP and SFTP are selectable. The files uploading is encrypted by using SFTP protocol.
4. Enter Server Address and Port. They stand for the FTP server address and corresponding port.
5. Set Username and Password and confirm the password. The FTP user should have the permission to upload pictures.
6. 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.
7. Select the saving path of images uploaded in the dropdown box of Upload Path and Edit the Name.
8. Click **Test** to verify the FTP server.
9. Click **Apply**.

4. 7. 9 Upload

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

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Network** > **FTP Settings** > **Upload**.



3. Enable Recording Schedule and refer to Arming Schedule and Processing Mode for settings if needed.
4. Enable Upload Video and Upload Capture as needed.

5. Configure the following parameters:

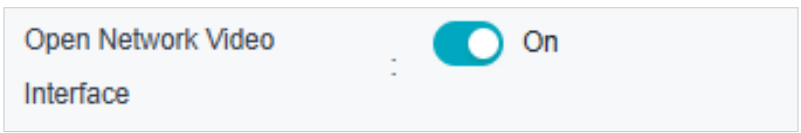
Stream Type	Select the stream type for recording. **Main Stream** stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements 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.

6. Click **Apply**.

4. 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

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Network** > **Advanced** > **ONVIF**.
3. Enable ONVIF if you need to use third-party management devices. 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.

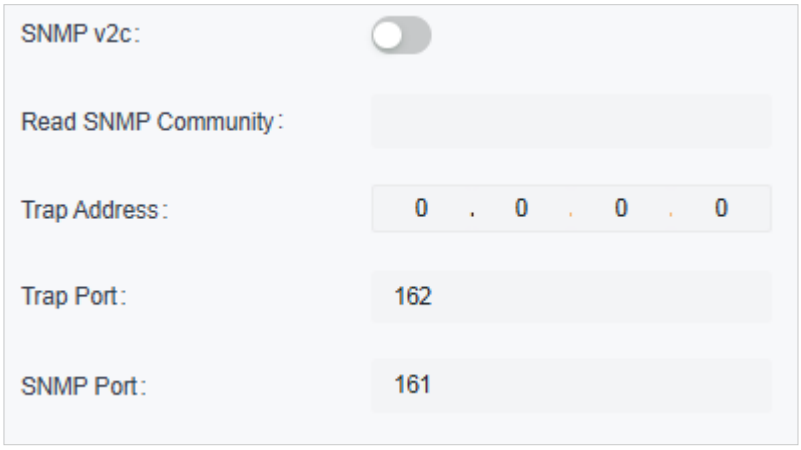


4. Click **Apply**.

4. 7. 11 SNMP

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

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **Network** > **Advanced** > **SNMP**.



3. Enable SNMP v2c.
4. 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.
5. 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.

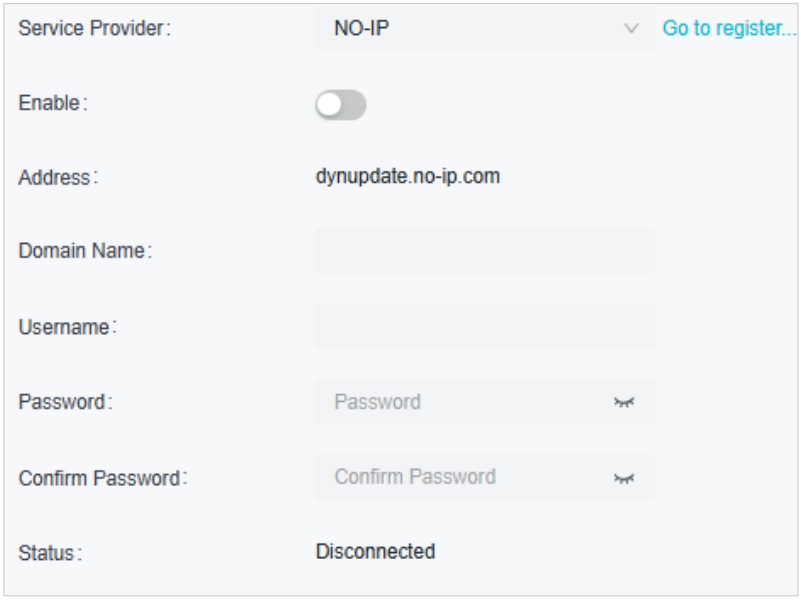
6. Click **Apply**.

4. 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 **Devices**. Select the site where your device is located, find the device in the list, and click .

2. In the panel on the right, go to **Network** > **Advanced** > **DDNS**.



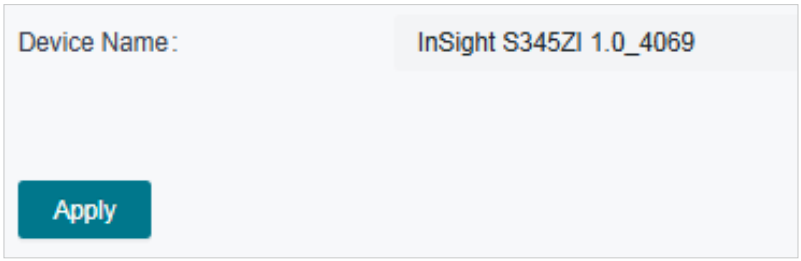
3. Select the type of Service Provider for domain name resolution.
4. Enter the domain name information, and click **Apply**.

4. 8 System

System settings enable 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.

4. 8. 1 Change Device Name

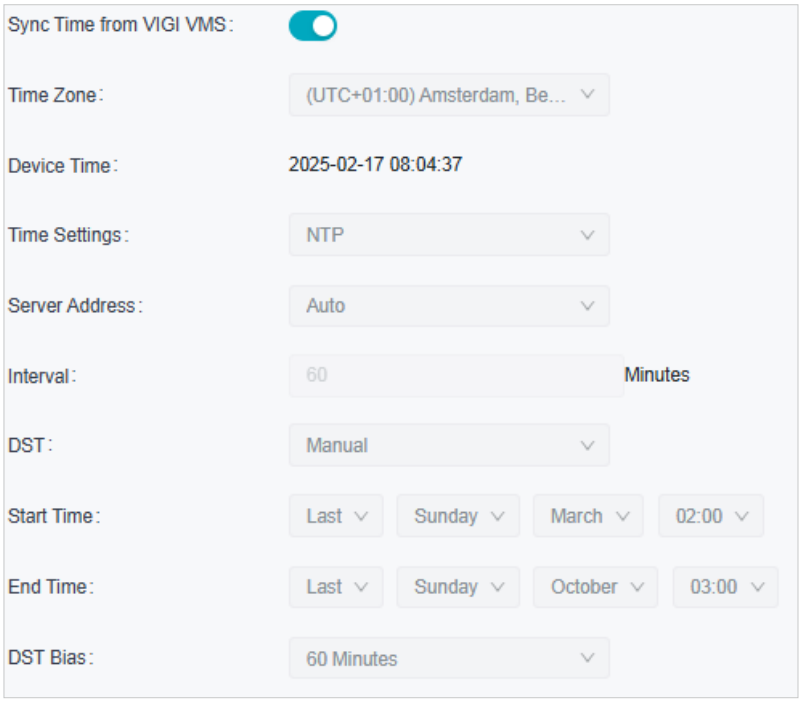
1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **System** > **Basic Settings** > **Basic Settings**.
3. View and change the name of your camera.
4. Specify the Web Session Timeout. You will be logged out when you make no operation (not including viewing live image) to the device via web browser within the set timeout period.



4. 8. 2 Modify Device Time

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

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **System** > **Basic Settings** > **Date**.



3. Select your time zone.
4. 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.

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.

5. (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.

6. Click **Apply**.

4. 8. 3 Change Password

To ensure the security of your network camera, it's important to periodically update your login credentials. Follow the steps to change the password for your device.

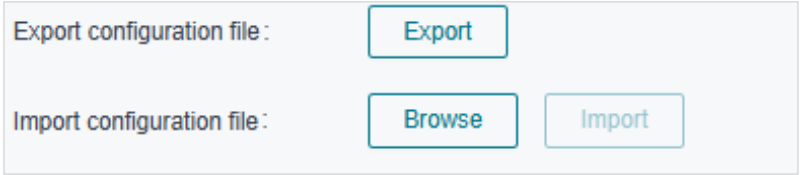
1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **System** > **User Management** > **Change Password**.

3. Enter the current password, type the new password, and confirm it.
4. Click **Apply** to save the changes.

4. 8. 4 System Management

You can reset the camera to factory default settings, import and export the configuration file of your camera.

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **System** > **System Management** > **System Management**.



3. To export the configuration file, click **Export**.
4. To import the configuration file, click **Browse** to select your file, then click **Import**.

4. 8. 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:

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

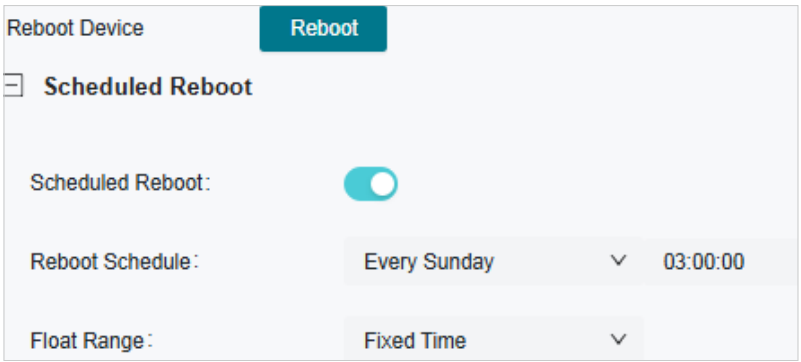
To upgrade device firmware, follow these steps:

1. Download the latest firmware file for the camera from **https://www.tp-link.com/sg/support/download/**.
2. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
3. In the panel on the right, go to **System** > **System Management** > **System Management**.
4. Click **Browse** to locate the downloaded new firmware file, and click **Update**.
5. Wait a few minutes for the upgrade and reboot to complete.

4. 8. 6 Reboot Device Regularly

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

1. Go to **Devices**. Select the site where your device is located, find the device in the list, and click .
2. In the panel on the right, go to **System** > **System Management** > **System Management**.
3. Enable **Scheduled Reboot**.
4. Select the day and time and specify the Float Range. When Fixed Time is selected, 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.
5. Click **Apply**.



5

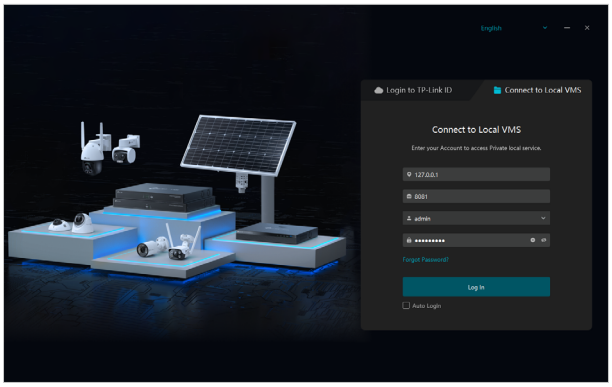
Monitor via PC Client

The PC client features Live View, Playback, AI Monitoring, Event Center, Download Center, Evidence Collection, and AI Search. This chapter includes the following sections:

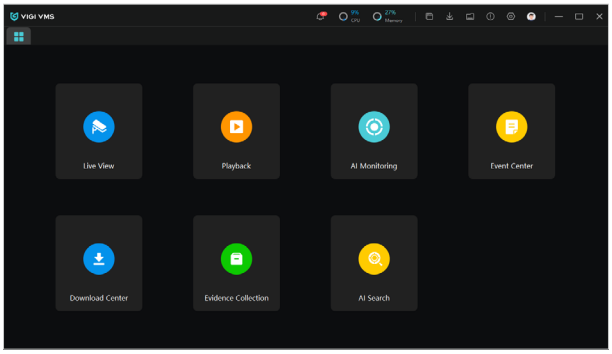
5. 1 Account

Follow these steps to log into the PC client and update your password for secure access to your network camera system. This process will help you manage and monitor your devices, ensuring your credentials remain protected.

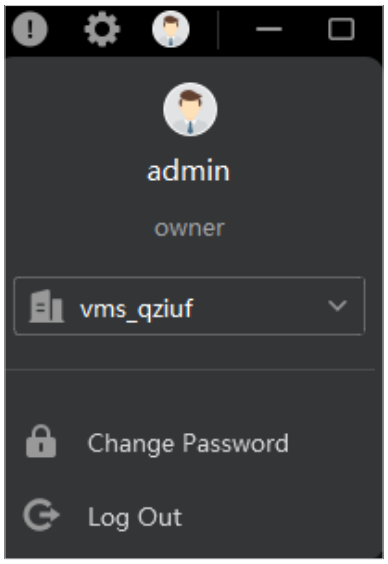
1. Download the PC client by clicking  on the top right corner of the main screen.
2. Open the PC client to enter the login page. Enter the IP address, port, username, and password, and click **Log In** to go to the main screen. If you click **Forgot Password?**, the VMS webpage will pop up.



3. The main screen is shown below:

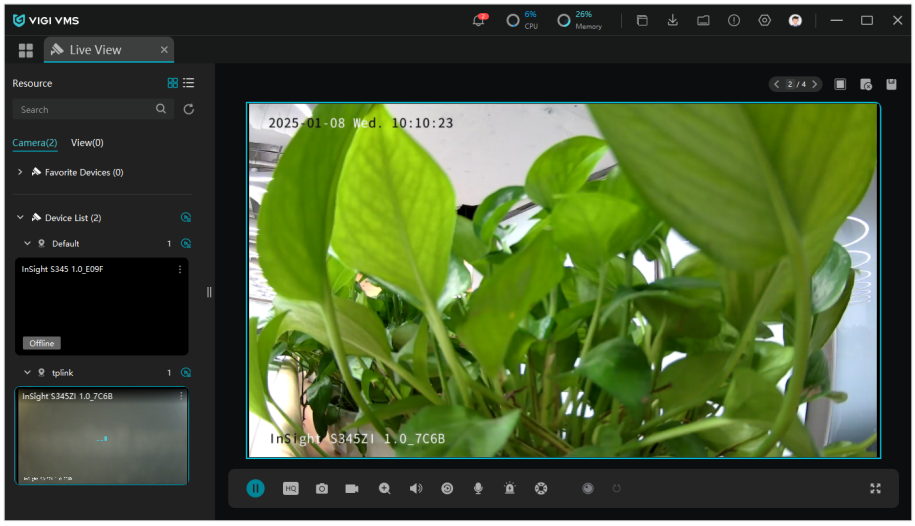


4. On the main screen of the PC client, click on the top right corner, and click **Log Out** to go back to the login page. Click **Change Password**, and the VMS web page will pop up. In the VMS drop-down list, you can change the site.



5. 2 Live View

In this section, users can easily interact with live video feeds, customize display settings, and organize their favorite camera views. These features help enhance the monitoring experience, allowing for a more efficient and tailored surveillance setup.



1. To show a video feed on the right, double click the thumbnail on the left, or click in the upper right corner of the video thumbnail, then click Play.
2. To add a camera feed to your favorite list for quick access, click and select Favorite.
3. To adjust the aspect ratio of the video feed, click and then click Ratio.

   1) 1x refers to the original window size.

2) 4:3 refers to 4:3 window size.

3) 16:9 refers to 16:9 window size.

4) 100% refers to the self-adaptive window size, adjusting based on the video content.

4. For detailed configuration, navigate to the toolbar at the bottom or use the quick config options available in the upper right.

Icon	Function Name	Description and Operation
	Play/Pause	Start or stop the live view feature.
	Resolution	Change the video display resolution.
	Screenshot	Take manual snapshots for the live view window.
	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.
	Mute	Toggle the live view cameras between mute and unmute.
	Instant Playback	Replay the last 30 seconds of video.
	Talk	Communicate with someone near the camera.
	Alarm	Send siren alerts and instant notifications.
	Pan/Tilt	(Available for select models only) Used for adjusting the image's brightness; a larger iris allows more light in, resulting in a brighter picture.
	Panoramic	(Available for select models only) Click to display a wide-angle or 360-degree view of the monitored area.
	Cruise	(Available for select models only) Click or hold the left mouse button to rotate the PTZ. Click once to rotate the PTZ horizontally in a continuous motion, and click again to halt the rotation.

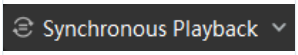
	Full Screen	View the live feed in full screen; press the Esc key to exit full screen mode.
	Number of Screen	Select how many camera feeds appear on the screen, such as 1, 4, 9, or 16. You may watch up to 64 views simultaneously.
	Clear All	Reset the display by removing all active video feeds and returning the layout to default.
	Save View	Save a custom layout of camera feeds for easy access later.

5. 3 Playback

The Playback interface allows you to review video recordings from your cameras and navigate through events and footage with ease.

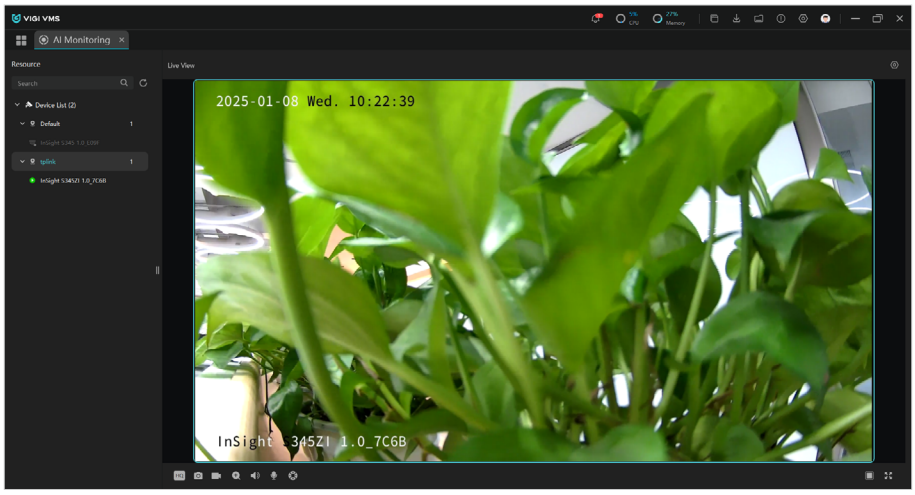
1. Locate the Device List on the left side. Click on a camera to view its footage on the main screen. Specify a date below the display window.
2. In the Event Recordings section, click a thumbnail. Watch the selected event recording immediately.
3. Drag the playback bar along the timeline. Use the time skip buttons to move forward or backward by intervals (e.g., 30 seconds).
4. For detailed configuration, navigate to the toolbar at the bottom or use the quick config options available in the upper right.

Icon	Function Name	Description and Operation
	Screenshot	Take manual snapshots for the live view window.

	Record	Click once to begin recording, and click again to end it; the recordings will be automatically saved to your designated path.
	Video Clip	Click to choose a specific portion of the video, create a shorter clip from the full recording and save it as a separate video file.
	Digital Zoom	Zoom in to get a closer look at the image for finer details; zoom out for a wider panoramic image.
	Volume	Toggle the live view cameras between mute and unmute.
	Speed Playback	Increase the speed for fast-forward or decrease for slow-motion review.
	Synchronous/ Asynchronous Playback	Synchronous Playback means watching videos from multiple cameras at the same time, all playing back in sync. Asynchronous Playback is when you view videos from different cameras, but not at the same time. You switch between the recordings of each camera individually.
	Full Screen	View the live feed in full screen; press the Esc key to exit full screen mode.
	Number of Screen	Select how many camera feeds appear on the screen, such as 1, 4, 9, or 16. You may watch up to 64 views simultaneously.
	Clear All	Reset the display by removing all active video feeds and returning the layout to default.

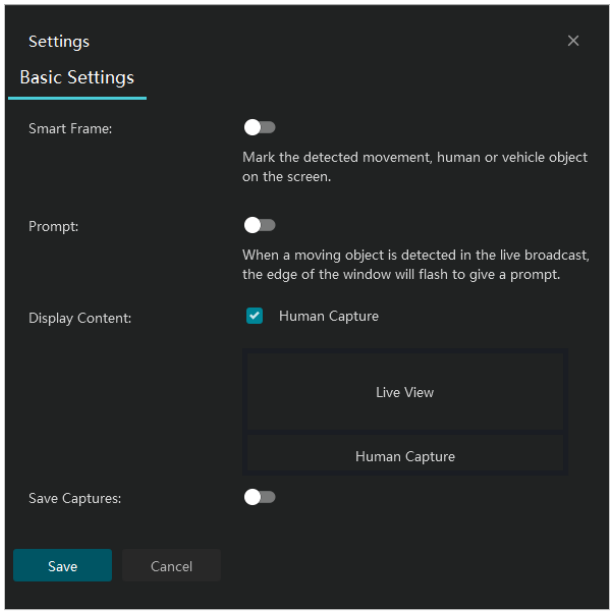
5. 4 AI Monitoring

The AI Monitoring module uses advanced AI technology to detect and highlight human figures in real-time. This feature enables enhanced surveillance by automatically identifying individuals in the camera's view.



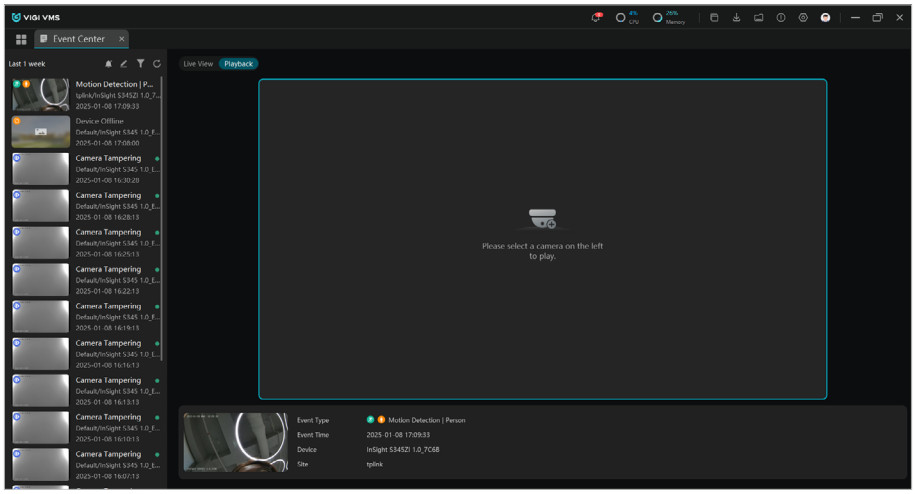
1. In the Device List, click on the camera you want to monitor. The Live View will display the camera's real-time feed.
2. The system will automatically detect human figures within the camera's field of view and highlight them in the Human Capture section.
3. To customize more settings, click on the top right corner to enter the **Settings** window and and click Save to apply the changes.
   1) Enable **Smart Frame** to mark detected movements, human figures, or vehicles within the live feed. This will highlight the detected objects on the screen.
   2) Enable **Prompt** to make the edges of the live window flash when a moving object (such as a person) is detected.
   3) In **Display Content**, make sure Human Capture is selected to ensure that detected humans are displayed below the live feed.

4) Enable **Save Captures** if you want to save human capture frames automatically for later use.



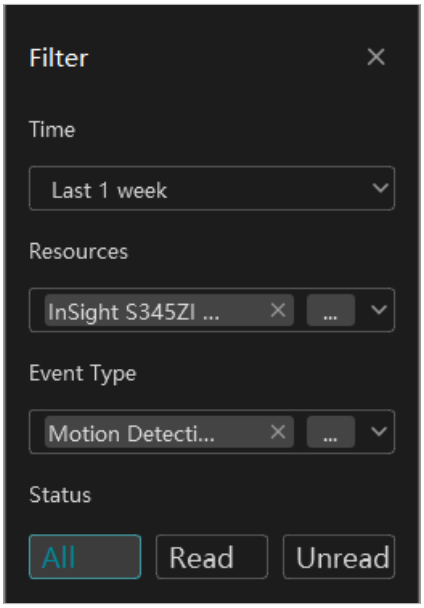
5. 5 Event Center

The Event Center module in the VIGI VMS is designed to help you efficiently monitor, filter, and review specific events captured by your cameras. Whether it's a motion detection alert, camera tampering, or any other significant activity, the Event Center provides a centralized location to quickly access, sort, and analyze recorded footage. With user-friendly filtering options and intuitive navigation, this module ensures that you can focus on the most important events in your surveillance system, improving your ability to respond to incidents in real time.



1. Click on a camera from the list on the left to load its video footage. The selected camera's footage will appear on the right, allowing you to watch the live or playback.

2. To filter events, click the Filter icon (located in the upper right corner of the left column). In the filter window, set the parameters and click **Confirm** to apply the filter.



Time	Choose a time range (e.g., "Last 1 week").
Resources	Select specific cameras.
Event Type	Choose the type of event (e.g., "Motion Detection" or "Camera Tampering").
Status	Choose whether to view "All", "Read", or "Unread" events.

3. (Optional) Click to update the event list with the latest footage or changes.
4. (Optional) Click to edit the list. You may select events to delete them.
5. View event details. In the lower section of the screen, details about each event are displayed, including event type, time, device, and site.

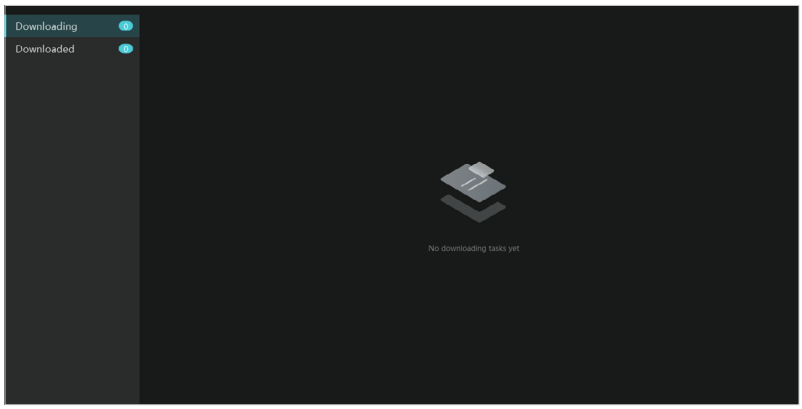
5. 6 Download Center

The Download Center module in the VMS provides a convenient way to manage and track the downloading of video footage or files. With this module, you can monitor ongoing downloads and view files that have already been downloaded. The interface allows you to efficiently manage your download tasks and keep track of the progress.

In the Download Center, there are two tabs:

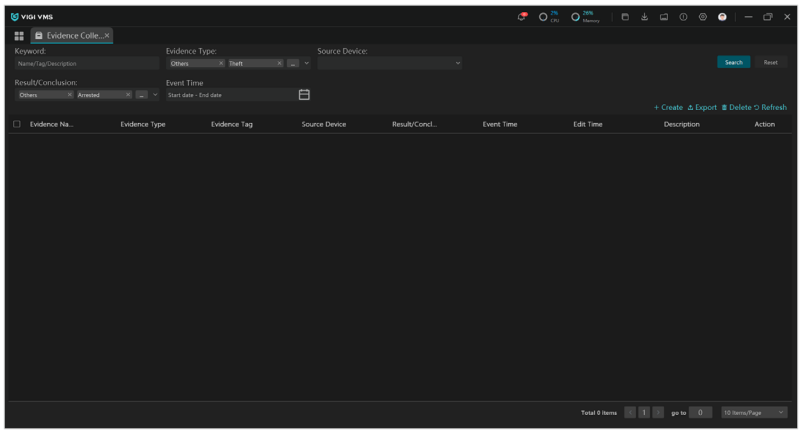
• Downloading: This tab shows any currently active downloading tasks. If no tasks are in progress, it will display a message saying "No downloading tasks yet."

• Downloaded: This tab displays the list of files that have already been downloaded.



5. 7 Evidence Collection

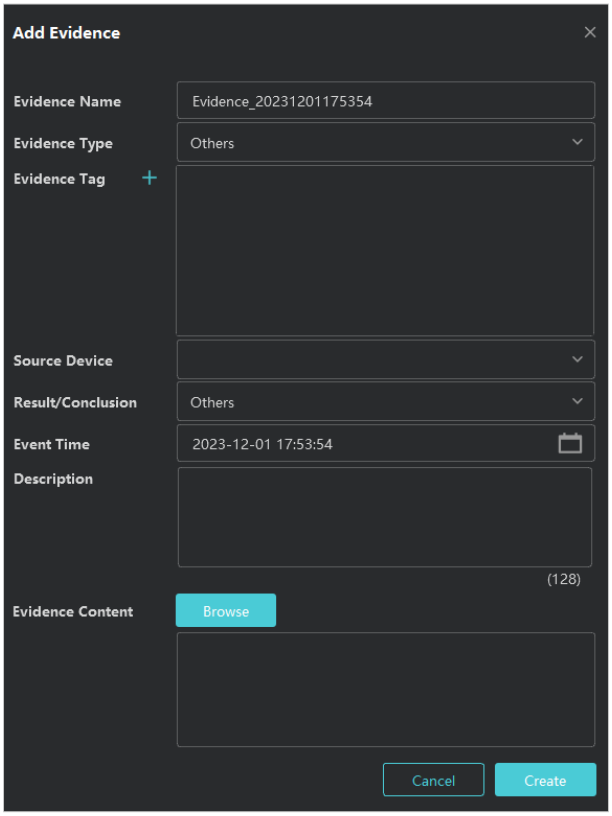
The Evidence Collection module in the VMS helps you manage and organize event data, allowing you to search for, tag, and handle evidence easily.



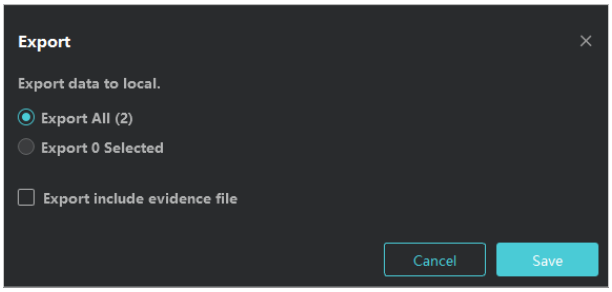
1. To start using the Evidence Collection module, first enter your search criteria. You can filter evidence by keyword, evidence type, result/conclusion, event time, and source device. After entering the criteria, click the Search button to display matching events.

Keyword	Enter relevant keywords (e.g., Name, Tag, and Description) to search for specific evidence.
Evidence Type	Select the type of evidence (e.g., Theft).
Result/ Conclusion	Choose the outcome of the event, such as “Arrested” or “Under Investigation.”
Event Time	Set a time range by specifying a Start date and End date.
Source Device	Select the camera or device that recorded the event.

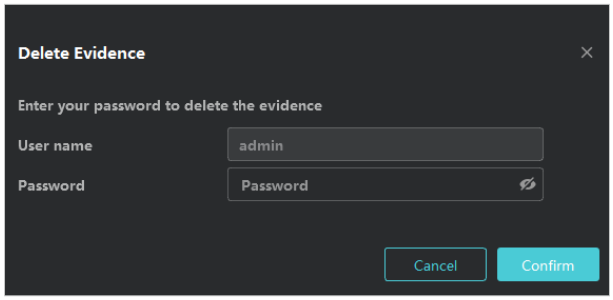
2. Once the results appear, review the evidence list, where you'll find details like the evidence number, event type, and source device. To edit any evidence entry, click under the action column and modify the necessary fields.



3. If you want to create new evidence, click the + Create button, fill in the required fields like evidence type, event time, and any relevant description, then save it.
4. For exporting evidence, click the Export button in the action column and follow the prompts to save the evidence.



5. If you need to delete any evidence, click Delete in the action column and enter the password to confirm the deletion.



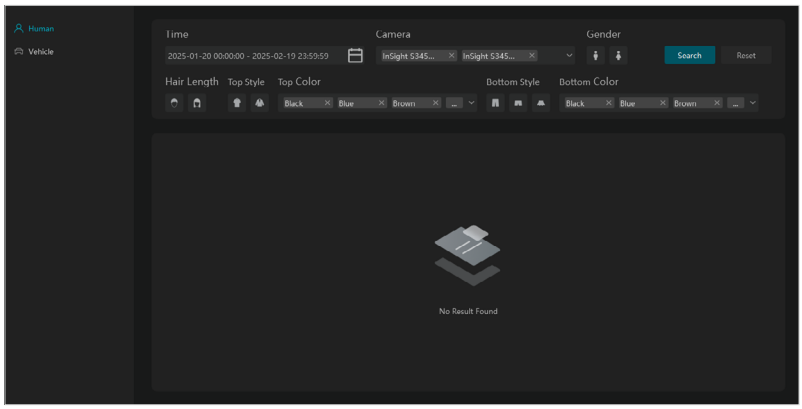
6. To refresh the evidence list and view the latest data, click the Refresh button. If you have multiple pages of results, use the pagination controls at the bottom to navigate between pages and select how many items you'd like to view per page (e.g., 10, 25, 50 items).

5. 8 AI Search

The AI Search feature in the VMS allows users to search for specific events and footage based on human or vehicle characteristics. By leveraging AI-based recognition, you can easily filter video content based on attributes like gender, clothing color, vehicle type, and more. This makes finding relevant footage quicker and more efficient, especially for large-scale surveillance setups.

5. 8. 1 Human Detection

1. Choose the Human tab on the left panel to filter results based on human-related attributes.



2. Set the following filter conditions:

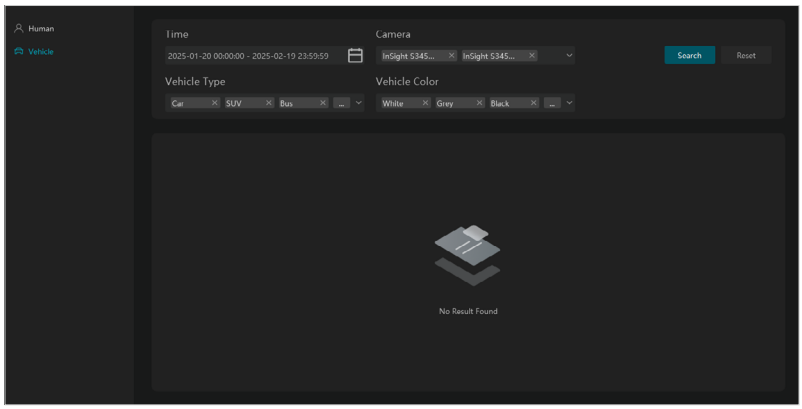
Time	Set the Time range by selecting the start and end dates to specify when the human-related event occurred.
Camera	Select the Camera from which the footage was recorded, or choose multiple cameras if needed.

Gender	Choose the Gender (Male/Female) to filter human recognition results by gender.
Hair Length	Select options like short, medium, or long.
Top Style	Select clothing type(s).
Top Color	Choose the color(s) of the top.
Bottom Style	Select the style(s) of the bottom wear.
Bottom Color	Select the color(s) of the bottom.

3. Click **Search** to display the relevant results based on your filter settings.

5. 8. 2 Vehicle Detection

1. Click the Vehicle tab to search for footage based on vehicle-related characteristics.



2. Set the following filter conditions:

Time	Select the Time range for when the vehicle-related event occurred.
Camera	Choose the Camera from which you want to view footage, or select multiple cameras.
Vehicle Type	Select the type(s) of vehicle.
Vehicle Color	Select the color(s) of vehicle.

3. Click **Search** to process your request and display the relevant vehicle footage.

6

Introduction to VMS Function Modules

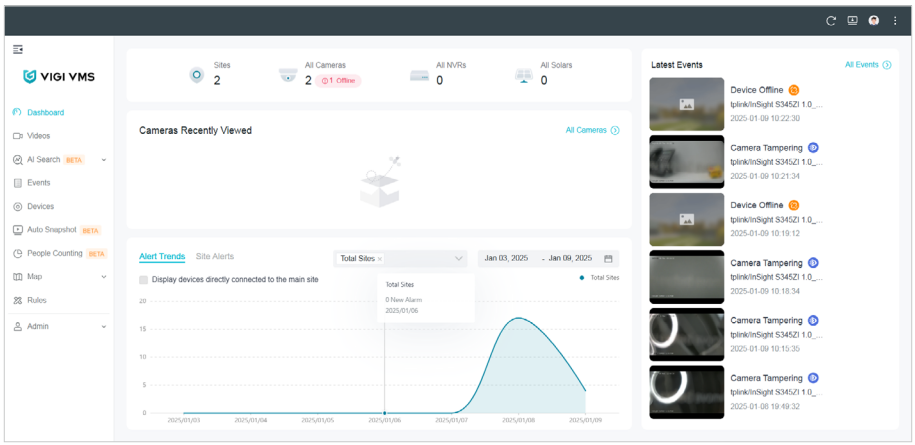
This chapter provides an overview of the various functional modules available within VIGI VMS. The modules cover essential features that allow you to effectively manage, configure, and monitor your security devices and system settings. By navigating through the following sections, users will gain a comprehensive understanding of how to leverage the VMS for optimal performance and ease of use.

- Dashboard
- Tutorial
- Videos
- Rules
- Map
- Events
- Devices
- Organization and Site
- User
- Account
- Log
- System Settings
- Cloud Access
- Forget Password

6. 1 Dashboard

The **Dashboard** consists of two main sections: resource statistics and alarm detection overview, providing you with a comprehensive view of global information.

Click **Dashboard** in the menu bar to access the **Dashboard** page.

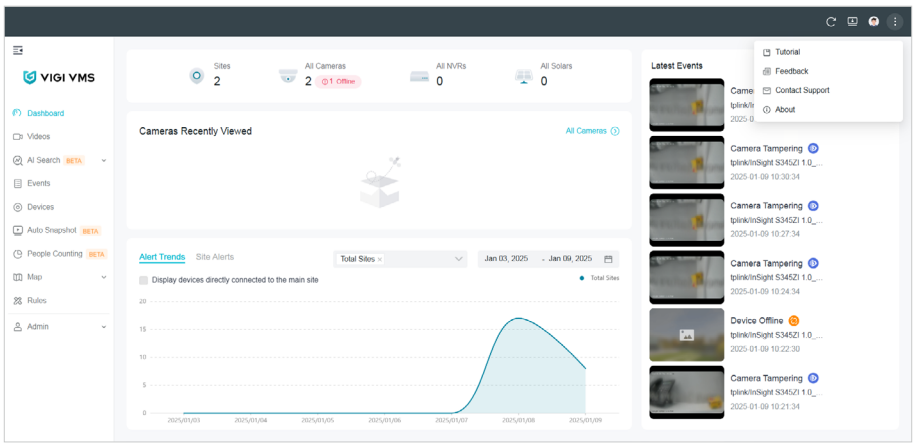


Sites	Displays the total number of sites (locations) monitored.
Cameras	Shows the number of cameras connected to the system. There may also be a notification indicating whether a camera is offline.
Cameras Recently Viewed	This section provides a list of cameras that have recently been accessed, allowing the user to quickly return to previously viewed camera feeds.
Alert Trends	This graph visualizes the frequency of alerts over a specified period. You can filter it by date range to track trends in system activity.
Site Alerts	Provides information about alerts specific to sites. Users can select a filter to view alerts for particular devices or all sites.
Latest Events	A list of recent events, showing detailed alerts with timestamps. This section allows users to quickly review any significant events or issues. Clicking on any event will open a detailed view

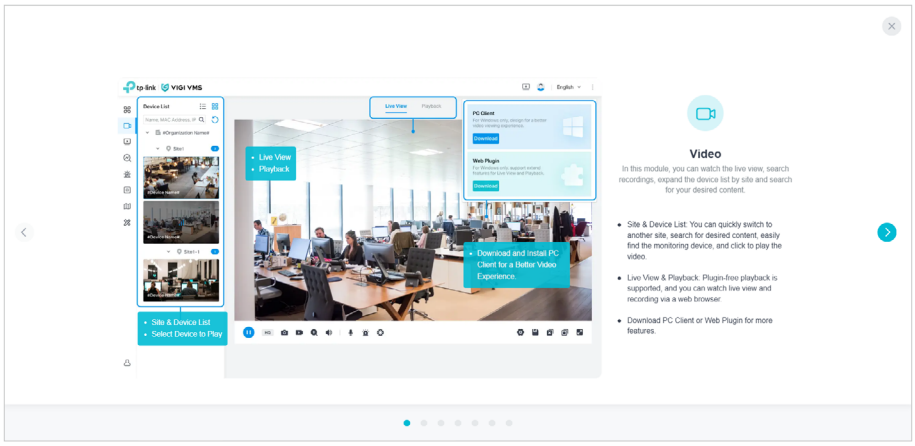
6. 2 Tutorial

The **Tutorial** page offers a summary of every VMS screen, making it easier for you to grasp the VMS system.

When you log in to VMS for the first time, the **Tutorial** page will be displayed. You can also access it anytime by clicking on the **Tutorial** option on the main screen.



The **Tutorial** page provides an overview of VMS features such as **Video**, **Events**, **Map**, **Device**, and **Admin**. Click the arrow to explore the introductions.



6. 3 Videos

To access the video options, click **Videos** in the menu bar. In **Videos**, you can check out both the **Live View** and **Playback** from your device.

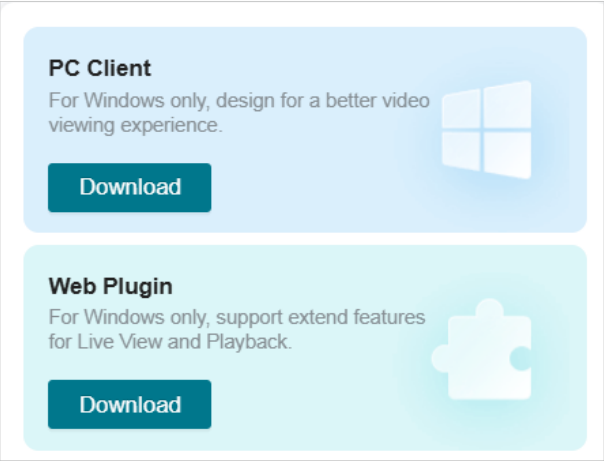
You can play the videos using either the web or the plugin. The web version offers basic functions like single-screen playback, pause, zoom in, and full screen. However, if you use the plugin, you'll unlock a wider range of features, including the ability to play 16 screens simultaneously, along with video and voice call capabilities.

6. 3. 1 Install the Plugins

VMS provides a plugin that allows for video live viewing and playback, enabling you to play up to 16 screens at once. With video and voice call functions, the plugin provides a pleasant user experience.

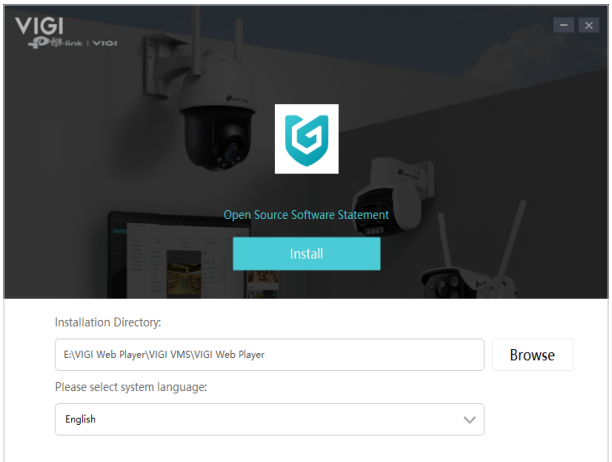
To install the plugin, follow the steps:

1. Click **Videos** in the menu bar on the left side of the main screen.
2. Click in the upper right corner of the page.

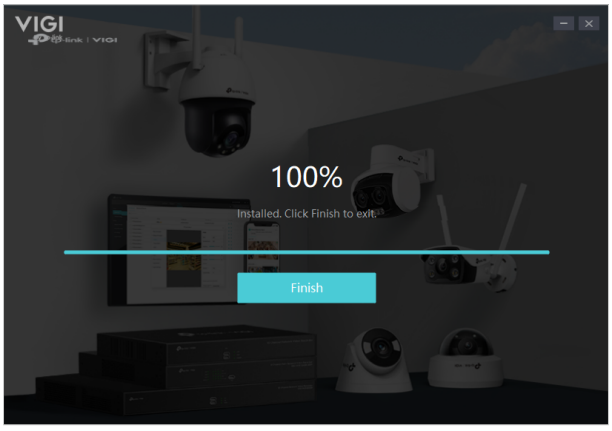


Note: If you are using VMS for the first time, make sure to click on Download It or Download Plugin to get the plugin installed.

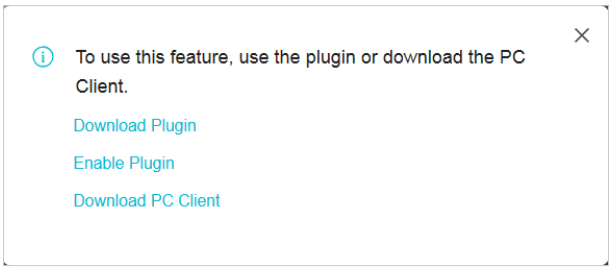
3. Click **Download**.
4. Double-click the installation package you downloaded, choose your preferred destination and language, then click **Install**.



5. Once the setup wizard is complete, click **Finish** to exit.



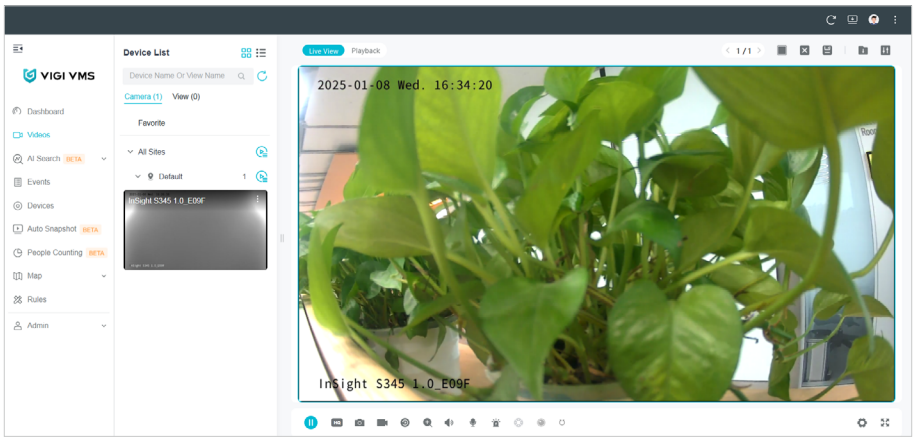
6. Go back to the VMS web interface, navigate to **Videos > Live View**, and click  or  at the bottom.
7. Click **Enable Plugin** in the prompt box that appears.



6. 3. 2 Live View

You can monitor your network cameras in real-time, allowing you to capture images, manually record footage, and control PTZ functions. The system supports a simultaneous live view across 16 screens.

In **Videos > Live View**, you can preview the surveillance feeds from all the devices linked to your site in real-time.



The live view toolbar makes it easier and faster to manage the live view window. You can take snapshots, record audio, and adjust the volume with just a few clicks.

Icon	Function Name	Description and Operation
	Play/Pause	Start or stop the live view feature.
	Resolution	Change the video display resolution.
	Screenshot	Take manual snapshots for the live view window.

	Record	Click once to begin recording, and click again to end it; the recordings will be automatically saved to your designated path.
	Instant Playback	Replay the last 30 seconds of video.
	Digital Zoom	Zoom in to get a closer look at the image for finer details; zoom out for a wider panoramic image.
	Volume	Toggle the live view cameras between mute and unmute. Adjust the volume by dragging the volume slider.
	Talk	Communicate with someone near the camera.
	Alarm	Send siren alerts and instant notifications.
	Pan & Tilt	(Available for select models only) Used for adjusting the image's brightness; a larger iris allows more light in, resulting in a brighter picture.
	Panoramic	(Available for select models only)
	Cruise	(Available for select models only) Click or hold the left mouse button to rotate the PTZ. Click once to rotate the PTZ horizontally in a continuous motion, and click again to halt the rotation.
	Settings	Click to configure display and stream parameters. For detailed operations, refer to Camera Display Settingss and Camera Stream Settings.
	Full Screen	View the live feed in full screen; press the Esc key to exit full screen mode.
	Number of Screen	Select how many camera feeds appear on the screen, such as 1, 4, 9, or 16. You may watch up to 64 views simultaneously.
	Clear All	Reset the display by removing all active video feeds and returning the layout to default.
	Save View	Click to save a snapshot of the live camera feed.
	System Settings	Click to change the destination folders for storing pictures and recordings.

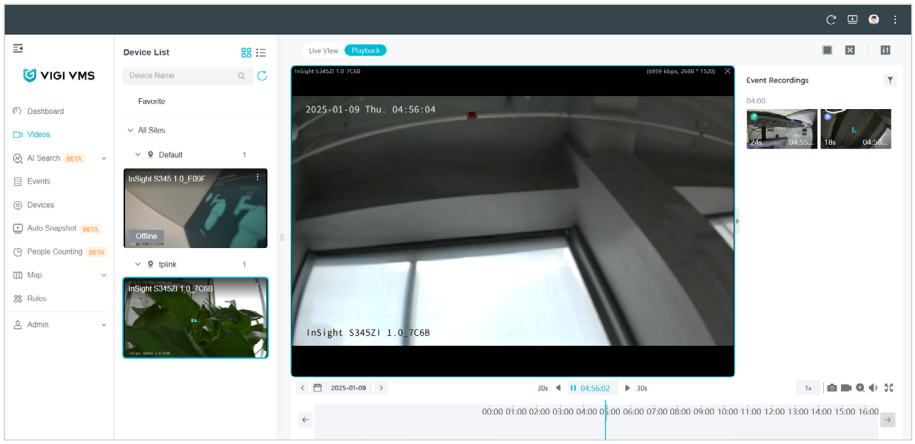
	Configuration	Select your viewing mode. For HTML5, you can watch the live feed from one camera at a time. For Web Plugin, you can view up to four camera feeds simultaneously.

6. 3. 3 Playback

Playback allows you to view a segment of the video that stands out or may not be clear at first glance. You can quickly access video files on the Live View page for an immediate review if necessary. You can watch playback from up to four cameras at once.

Before you start, make sure to record your video files and save them on storage devices like SD/SDHC cards, HDDs, DVRs, NVRs, network cameras, or storage servers.

1. Go to **Videos > Playback**.



2. Choose the camera from the device list on the left and specify a date below the display window. Double-click the event recording you want to watch from the right list.
3. Drag the playback bar along the timeline. Use the time skip buttons to move forward or backward by intervals (e.g., 30 seconds).
4. For detailed configuration, navigate to the toolbar at the bottom or use the quick config options available in the upper right.

Icon	Function Name	Description and Operation
1x	Speed Playback	Increase the speed for fast-forward or decrease for slow-motion review.
	Screenshot	Take manual snapshots for the live view window.

	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.
	Full Screen	View the live feed in full screen; press the Esc key to exit full screen mode.
	Number of Screen	Select how many camera feeds appear on the screen, such as 1, 4, 9, or 16. You may watch up to 64 views simultaneously.
	Clear All	Reset the display by removing all active video feeds and returning the layout to default.
	Configuration	Select your viewing mode. For HTML5, you can watch the live feed from one camera at a time. For Web Plugin, you can view up to four camera feeds simultaneously.

6. 4 Events

The Events feature in VIGI VMS is a crucial tool for monitoring and responding to irregular activities detected by your cameras. It helps security staff stay alerted to any potential security threats, allowing for rapid intervention. The system can trigger various linked actions, such as audio alerts or email notifications, to ensure immediate attention is given to any suspicious events.

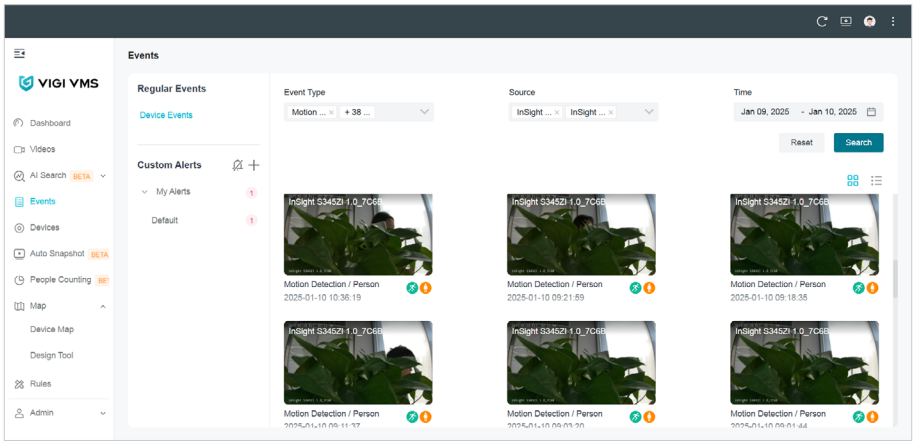
6. 4. 1 Device Event

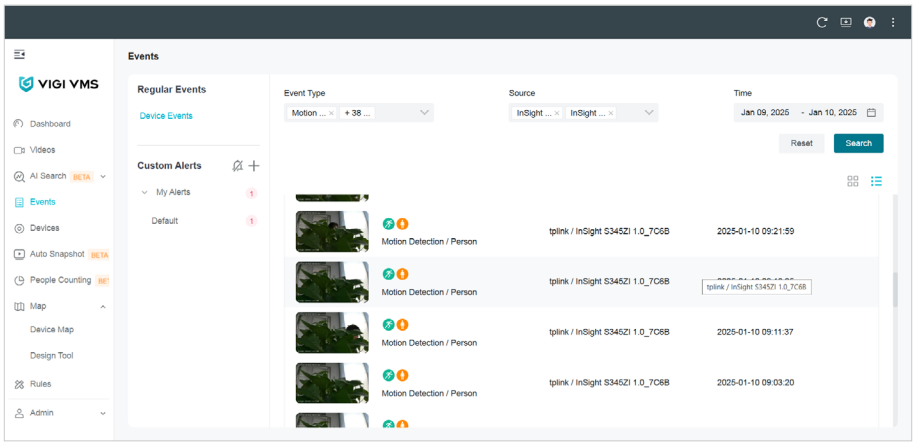
A Device Event records any alarm or alert triggered by the devices connected to the VMS system. These events may include motion detection, person detection, and other anomalies that require attention.

■ Search for Smart Events

VMS allows you to search for specific smart events based on your preferences. Follow these steps to efficiently locate the events you need:

1. Click **Events** in the menu bar.
2. Once in the Events section, you'll see the list of recorded smart events. These events are organized by device type, event type, and time, allowing for easy filtering.
3. Click and to switch between two event viewing modes: Thumbnail Mode and List Mode. Thumbnail Mode shows you a small preview image of the event. List Mode provides a more detailed, text-based view of the events.



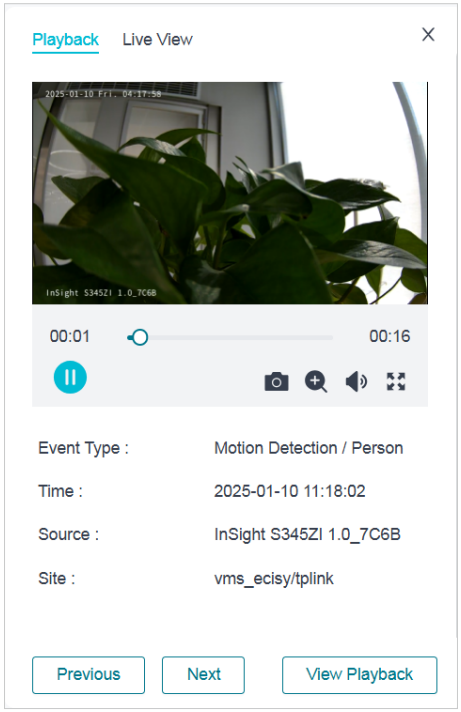


4. To narrow down your search, you can use filters. Choose the specific Event Type (e.g., Motion Detection, Person Detection) and Source (the camera or device responsible for the alert).
5. Set the desired Time Range to focus on events that occurred within a specific timeframe. After adjusting the filters, click Search to view the results.

Event Playback

The Event Playback feature allows you to view past events captured by your devices. This functionality helps you investigate suspicious activities or review event details to make informed decisions.

1. In the event list, find the event you want to review. Click on the event to view its playback and real-time preview.



2. A pop-up window will appear displaying the event's live view or playback. The time bar at the bottom of the playback window allows you to navigate through the event's timeline. You can pause or play the video using the controls at the bottom.
3. Click on to capture still images from the video.
4. Click to expand the video to full-screen mode for a better view.
5. To get a closer look at specific areas in the video, click . This will allow you to zoom in on the video for more details. You can also drag your mouse over the video to explore different areas, giving you a more detailed view of the footage.

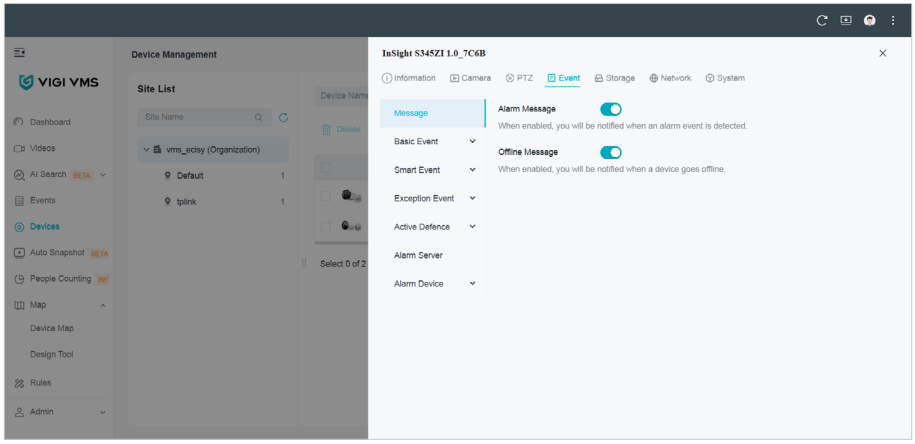
Enable/Disable the Message

To ensure that you are notified of important events and updates, you can enable or disable message notifications for specific devices. This includes receiving alerts for alarm events or offline status of the devices. Follow these steps to manage the message notifications for a device:

1. Click on the Devices tab in the menu on the left side.
2. In the Device List, find the device for which you want to manage message notifications. Click to open the device management settings.
3. Click **Events** > **Message**.
4. Enable Alarm Message or Offline Message as needed.

Alarm Message	Toggle this option on to receive notifications whenever an alarm event is triggered by the device.

Offline Message	Enable this to be notified when the device goes offline.

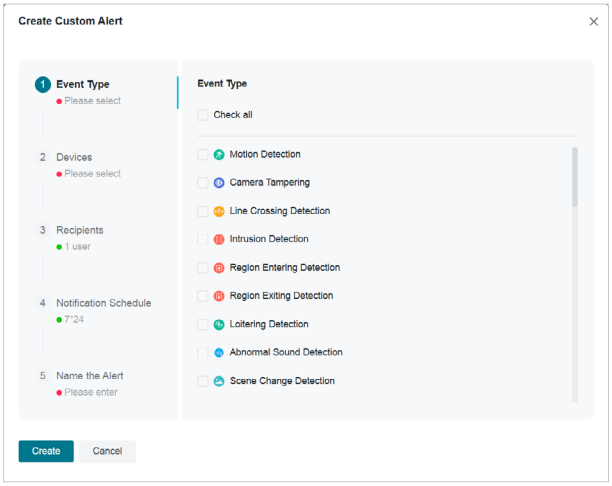


Note: The Offline Message feature is unavailable for IP cameras that are connected to a Network Video Recorder.

6. 4. 2 Custom Event

The Custom Event feature allows you to set up personalized alerts triggered by specific conditions defined in the event rules. By configuring custom events, you can receive notifications based on your chosen parameters, enhancing the monitoring capabilities of your system.

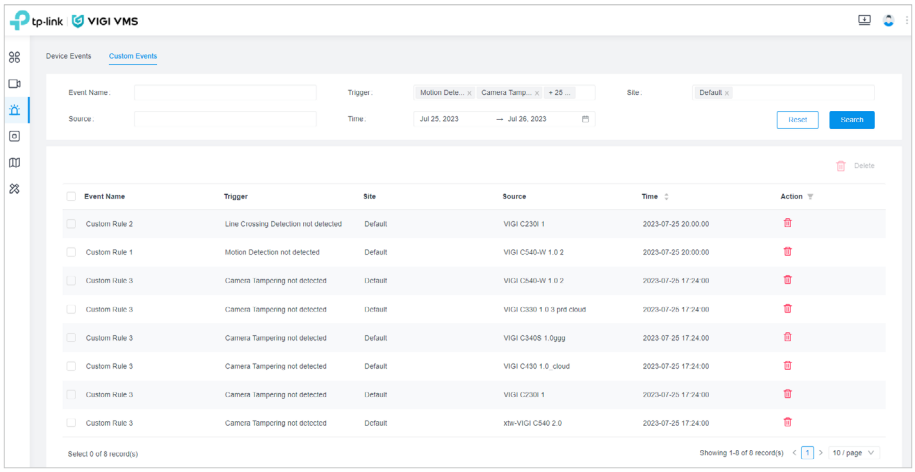
1. Click the **Events** tab and click + to enter the **Custom Event** page. This will bring you to the Custom Event creation page where you can define and configure your event rules.



2. In the Event Type section (Step 1), select the type of event you want to create.
3. In Step 2, select the devices for which you want to create the custom event.
4. In Step 3, you will choose the recipients of the alert. This can be a specific user or a group of users who will be notified when the event occurs
5. In Step 4, configure the Notification Schedule to determine when you want to receive event notifications. The default schedule is 24/7.

6. In Step 5, enter a Name for your custom alert.
7. After filling in all the necessary details, click the **Create** button at the bottom to save and activate your custom event alert.

After setting up your custom events, you can filter and view the triggered events based on the following criteria: event name, trigger event type, site, trigger device, and trigger schedule. By default, you can view events from the past three days. The system supports viewing events from the last 90 days, allowing you to review historical data and monitor patterns over time..

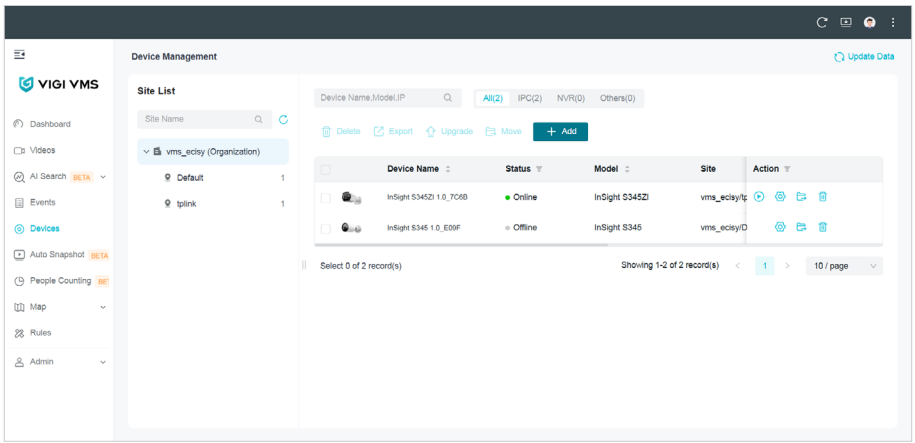


6. 5 Devices

The Device Management feature in the VMS allows you to easily manage and monitor the devices (such as cameras and NVRs) connected to your system. It provides detailed information about each device's status, model, IP address, and MAC address and helps you track and control the devices across your network.

In **Devices**, you can view all connected devices and their statuses (online or offline), edit device settings and configuration, add new devices to your system, and monitor device connection and IP/MAC address details.

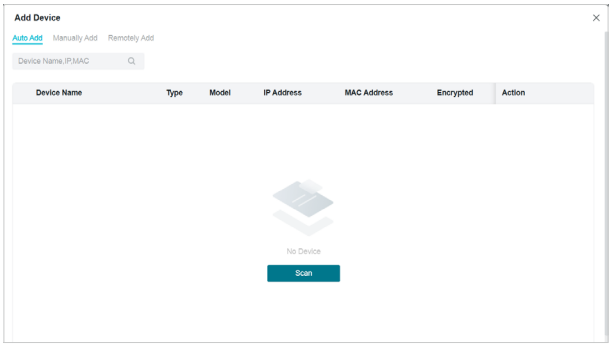
1. Click **Devices** in the menu bar.



2. The Site List on the left panel shows the available sites where devices are located. Select a site to manage the devices within it.
3. To update device data, click the Update Data button in the top-right corner of the interface.
4. You can sort and filter the device list by clicking on the column headers, such as Device Name, Status, Model, Site, IP Address, or MAC Address.
5. To manage a device, click the Action buttons (represented by icons) next to each device for further options like editing settings or viewing device details.

6. 5. 1 Add Device

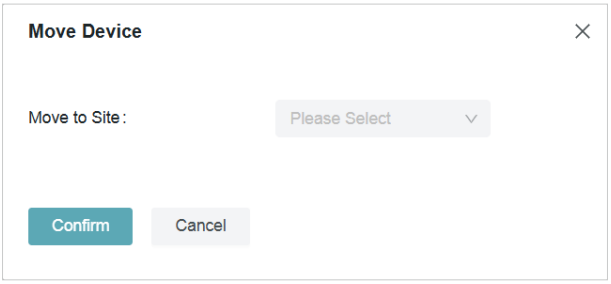
Click **Add** to add devices automatically or manually. For details, refer to Auto Add Device.



6. 5. 2 Move Device

Click to move the device to another site.

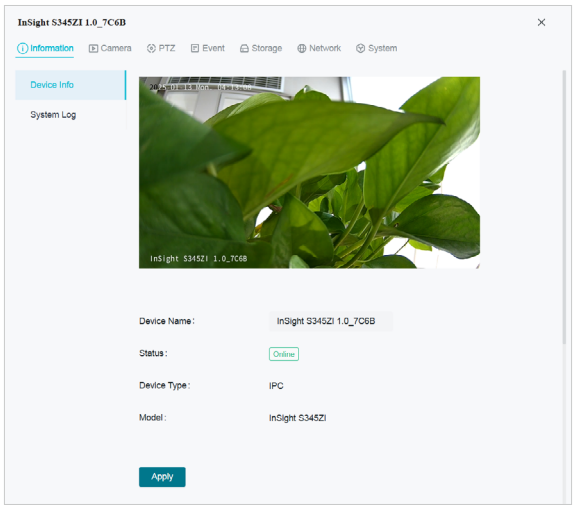
Select a destination site where you want to move your devices. For details, refer to Move Device to Another Site.



6. 5. 3 Edit Device

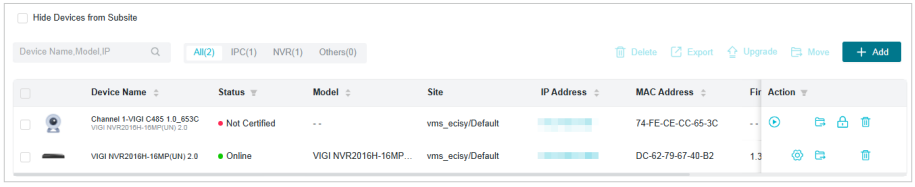
In **Edit Device**, you can make configurations of the devices, such as **Device Name**, **Local Upgrade**, **Video Settings**, **Smart Event**, **System Management**, **PTZ Settings** (for certain models), and **Network Settings**.

Click in the **Action** column. Refer to Change Camera Settings for detailed configuration.



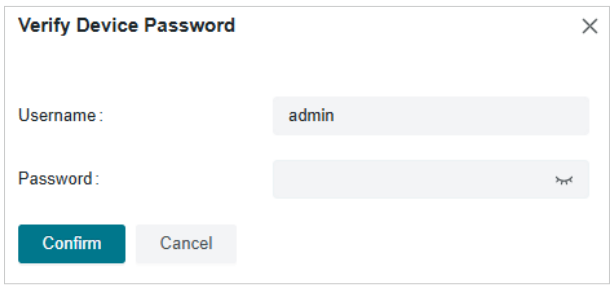
6. 5. 4 Child IPC Authentication

When an NVR is added to the VMS, any child IPCs (cameras connected to the NVR) will appear in the device list. For unauthenticated IPCs, a lock icon will be displayed in the **Action** column.

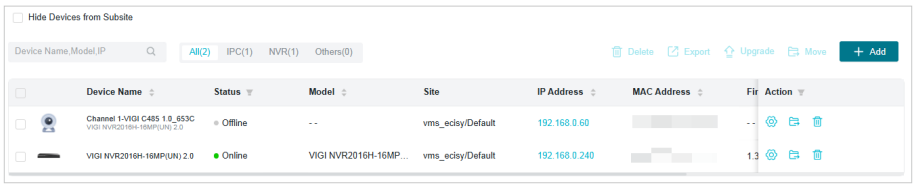


By following these steps, you will successfully authenticate child IPCs and ensure secure communication with the NVR.

1. Click .
2. A pop-up window will appear. Enter your username and password in the respective fields.
3. Click **Confirm** to authenticate the device.



Once authentication is successful, the lock icon will no longer appear for the corresponding IPC in the device list.



6. 6 Map

The Map feature in VMS offers a visual representation of where cameras and alarm input devices are situated within your environment. It helps in mapping out the physical locations of cameras, NVRs, and their respective directions. The E-map functionality also allows the organization of devices in hierarchical structures, making it easier to navigate from broad views, like an entire floor, down to specific rooms.

With the Map feature, you can search for monitors based on their physical locations and access real-time surveillance footage and alarm events. Key functionalities of the Map include an overview, the ability to add and manage maps, label them, and utilize the Designer Tool.

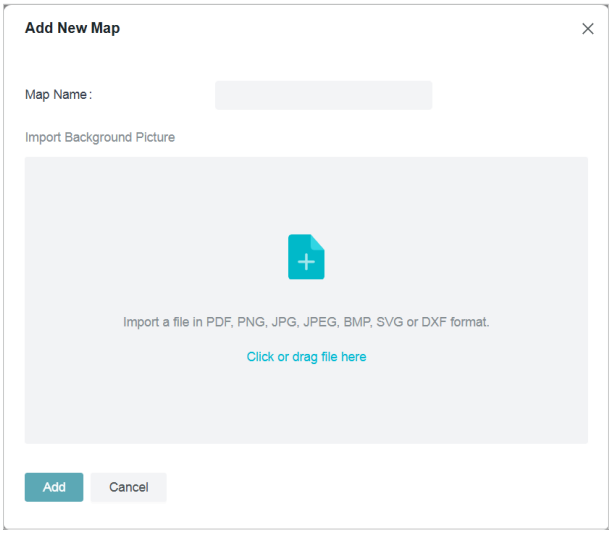
To access the Map page, simply click on **Map** in the menu bar and select **Device Map**.

6. 6. 1 Add Map

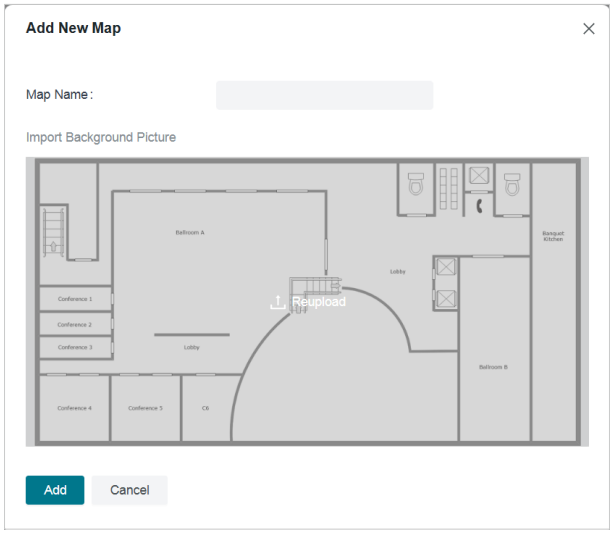
To add a new map to your system, follow these steps:

1. Click **Add New Map**, and click **+** or drag your file into the designated area.

Note: The system accepts various formats, including PNG, JPG, JPEG, BMP, SVG, and PDF.



2. Once the file is uploaded, you can preview the map. If you need to upload a different file, click **Reupload**.



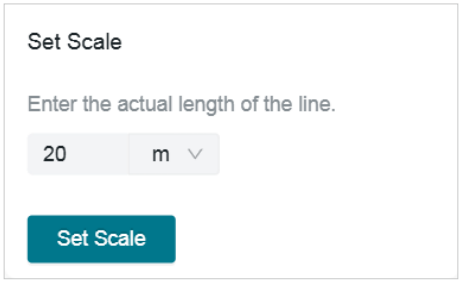
3. Enter a name for your map and click **Add**.

Note: The system allows for the uploading of multi-page PDF files, and you can choose a specific page for previewing and adding.

4. (Optional) Edit the map scale.

   The map scale defines the relationship between the distance shown on the map and the actual distance on the ground.

   To set the scale, adjust the line segment by dragging the two dots shown, or input the actual length of the line. Click **Set Scale**.



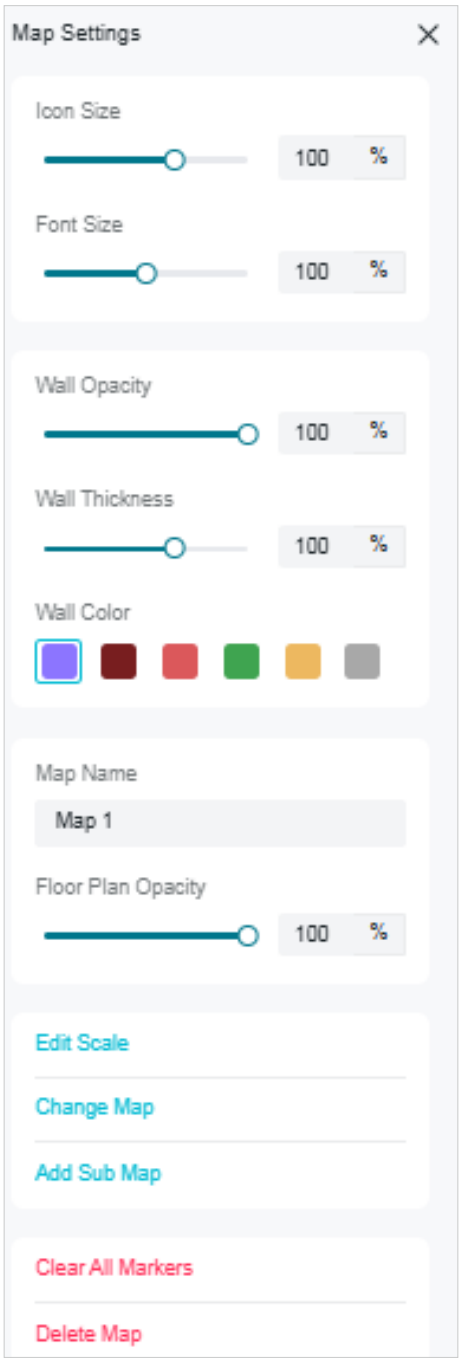
6. 6. 2 Manage Map

You can manage your maps with options to zoom in, zoom out, adjust layers, and generate heatmaps.

Icon	Name	Explanation and Operation
	Fit to Extent	Click to automatically resize the map, showing all active devices and camera placements in one unified view.
	Zoom In/Out	Adjust the map's level of detail. You can also use the scroll wheel on your mouse for smoother zoom adjustments.

	Layer	Click the Layer icon to reveal or hide specific layers. Check or uncheck the options to customize the map display according to your needs. Labels: Show device names on the map for easier identification. People Counting: Track and display people counting data, useful for areas with a lot of foot traffic. Monitoring Areas: Highlight specific zones that are under surveillance. People (Beta): If enabled, it shows detected people in various locations on the map.
	Heatmap: People	Click to a view heatmap that visualizes the intensity of activity or movement within various areas over a defined period. It's especially useful for identifying high-traffic zones.
	Heatmap Settings	Click to select your desired time frame (e.g., Recent 1 Hour, Recent 3 Hours).

You can click to customize the appearance and layout of your map, making it easier to adapt to your specific monitoring needs. Below are the settings you can adjust:



Icon Size	Adjust the size of the icons displayed on the map.
Font Size	Change the size of text displayed on the map, such as device names or labels. Increase the size for better readability, or reduce it to fit more text.
Wall Opacity	The Wall Opacity slider controls the transparency of walls on your map.

Wall Thickness	Adjust the width of the wall lines on your map.
Wall Color	Choose a color for the walls of the map by selecting one from the color options.
Map Name	Change this name to better organize and label your maps.
Floor Plan Opacity	Adjust the transparency of the floor plan. Lower opacity allows for a clearer view of overlaid elements like cameras and devices.
Edit Scale	Click to modify the scale of your map, ensuring accurate representation of real-world distances.
Change Map	Select to upload a new map if needed.
Add Sub Map	If your map contains multiple levels (e.g., different floors), use this option to add a sub-map.
Clear All Markers	Use this option to remove all markers from the map, which helps reset your view.
Delete Map	Click to permanently delete the map from the system.

6. 6. 3 Manage Hot Spot

The markers added to the map are called hotspots. These hotspots not only indicate the locations of the devices but also provide live views and alarm details related to surveillance activities.

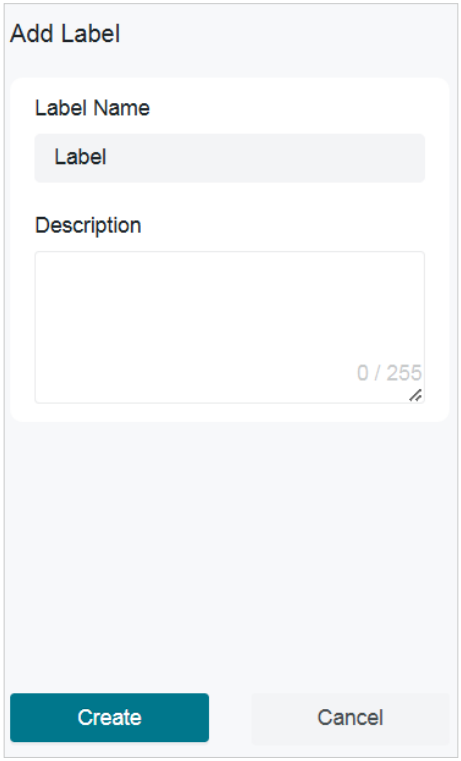
You can add labels to describe locations, create links to navigate to other maps, and include devices to monitor the online status of connected IPCs and NVRs. Additionally, you can view the monitoring range of IPCs and access real-time previews.

- **Add Label**

To add a label to a specific location on the map, follow these steps:

1. In the Edit page, click  in the top right corner of the screen.
2. Move your mouse cursor to the desired location on the map where you want to place the label. Once the location is selected, click on it.
3. In the pop-up that appears on the right, enter a name for the label. You can also add a description (optional) for more context.

4. Click **Create**.



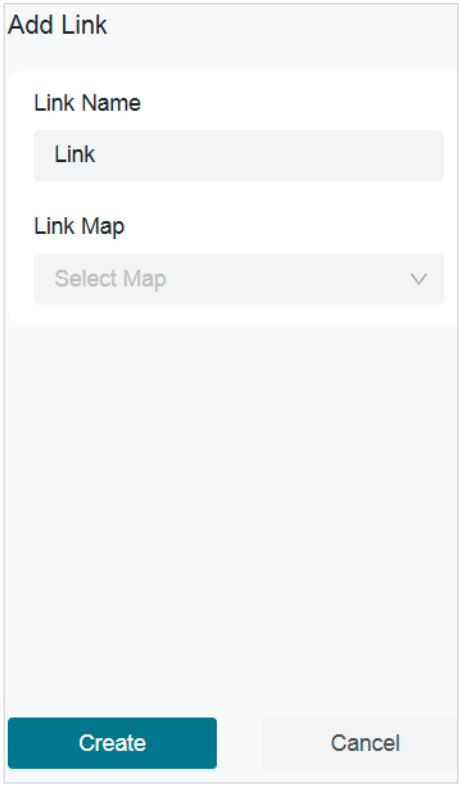
Add Link

You can add links to locations on the map and navigate to other maps.

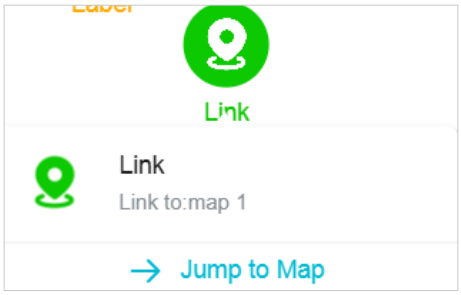
To add a label to a specific location on the map, follow these steps:

1. In the Edit page, click in the top right corner of the screen.
2. Move your mouse cursor to the desired location on the map where you want to place the label. Once the location is selected, click on it.

3. In the pop-up that appears on the right, enter a name for the link and select a map.



4. Click **Create**.
5. Once the link is created, hover your cursor over the icon, and a pop-up window will appear. Click on **Jump to Map** to view the map associated with this link.

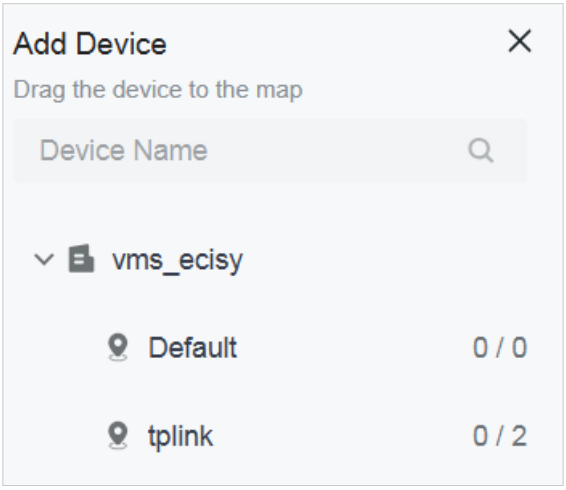


Add Device

Follow these steps to add a device:

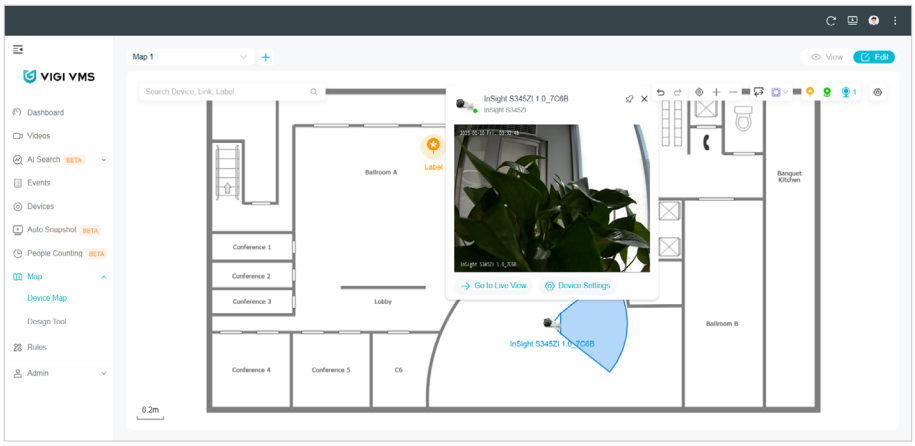
1. On the Edit page, click .

2. In the pop-up window on the right, select the device from the organization and site.

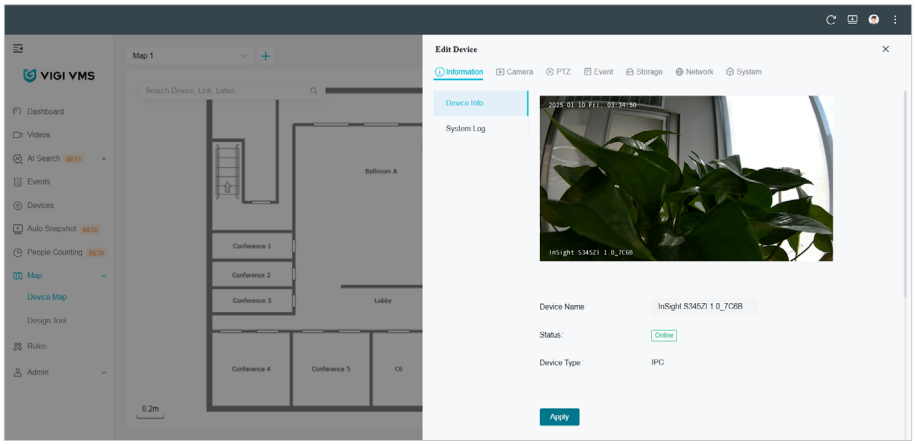


3. Drag the device to the map and click it to place the marker at your desired location. You may click and drag the colored area to adjust the surveillance angle and coverage.

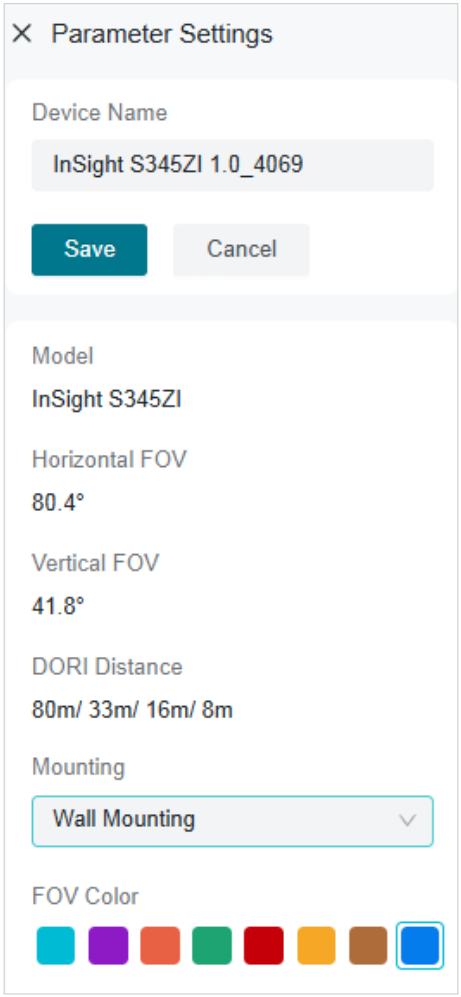
4. Click on the device marker, then click view the real-time monitoring feed. To access the Video page, click Go to Live View in the pop-up window.

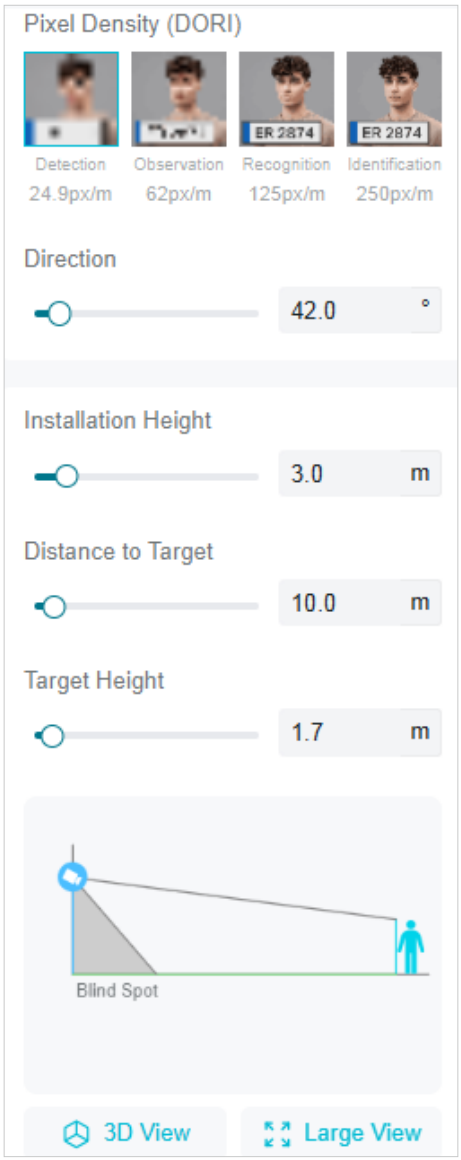


5. In the pop-up window, click **Device Settings** to configure the device.



6. Click the device marker and you can configure parameter settings.





Device Name	Enter the name of the device..
Model	Specifies the model number of the camera.
Horizontal FOV	Displays the horizontal field of view of the camera (measured in degrees).
Vertical FOV	Displays the vertical field of view of the camera (measured in degrees).
DORI Distance	Defines the distance (in meters) at which the camera can detect, observe, recognize, and identify objects.
Mounting	Select from the drop-down menu how the camera is physically set up.

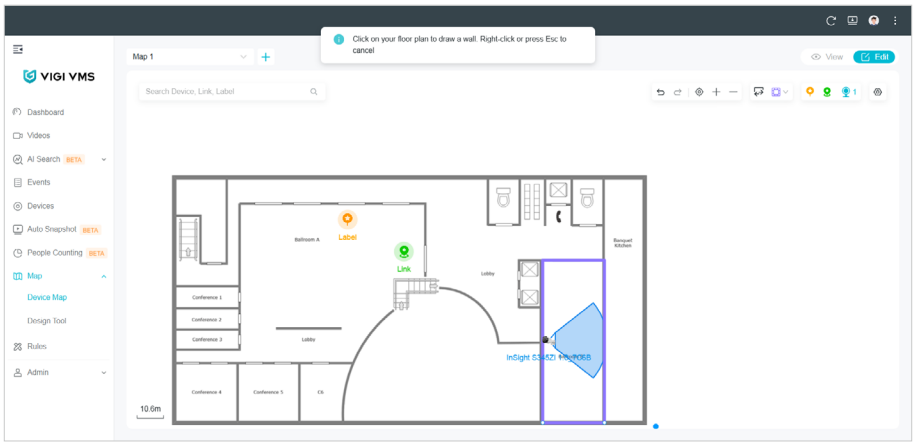
FOV Color	Select a color from the available options for the field of view to be represented in the map.
Pixel Density (DORI)	It represents the pixel density for different detection ranges: Detection, Observation, Recognition, and Identification. Choose the appropriate pixel density based on the range requirements of the surveillance task.
Direction	Specify the camera's orientation.
Installation Height	Set the height of the camera from the ground.
Distance to Target	Adjust the distance between the camera and the target object
Target Height	Adjust the height of the object or area being monitored.
Tilt Angle	Change the vertical angle at which the camera is pointed.
Blind Spot	View the blind spot area in 3D view or in a large picture.

6. 6. 4 Map Wall

To define walls on the map that block the camera's viewing angle, follow these steps:

1. Click Edit, and then click in the upper right corner of the screen.
2. Click on the map and drag your mouse to form a rectangle or line.

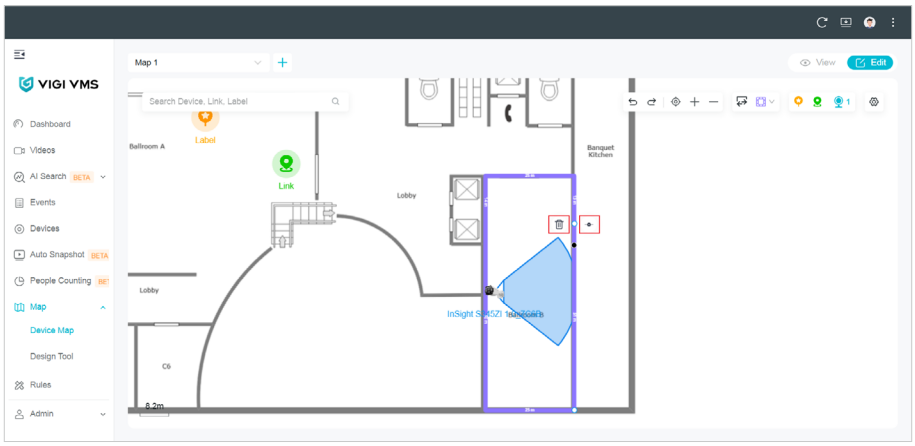
   Note: Click the map first and then drag your mouse to form a rectangle or line.



3. To split an existing wall, click on the wall and then click to divide it into two parts.

4. To delete a wall, click on the wall and then click .

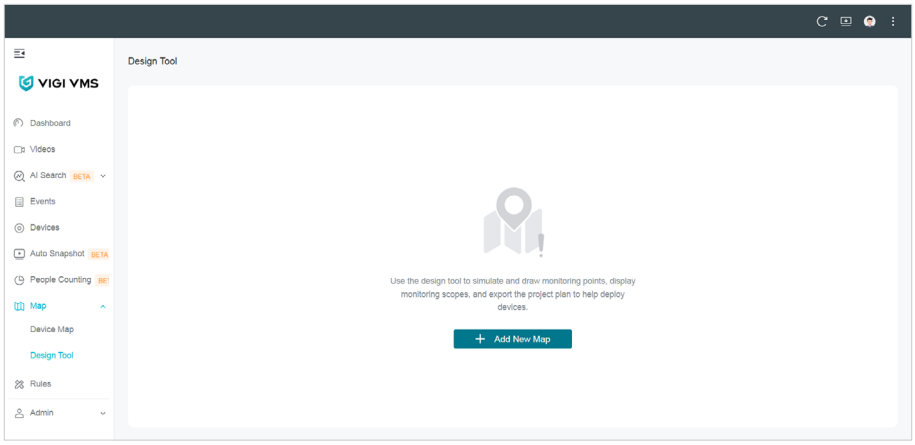
5. To modify the wall, click on the corner, intersection, or division point of the wall. Drag your mouse to adjust the size, length, or orientation of the wall to fit your desired layout.



6. 6. 5 Designer Tool

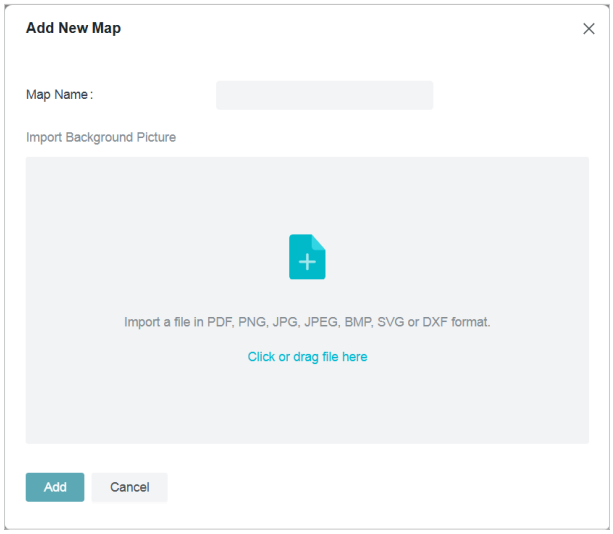
Designer Tool simulates real-world security scenarios by placing virtual devices on your map. Follow these steps to use the tool:

1. On the **Map** page, click **Designer Tool** in the navigation bar to open the tool:

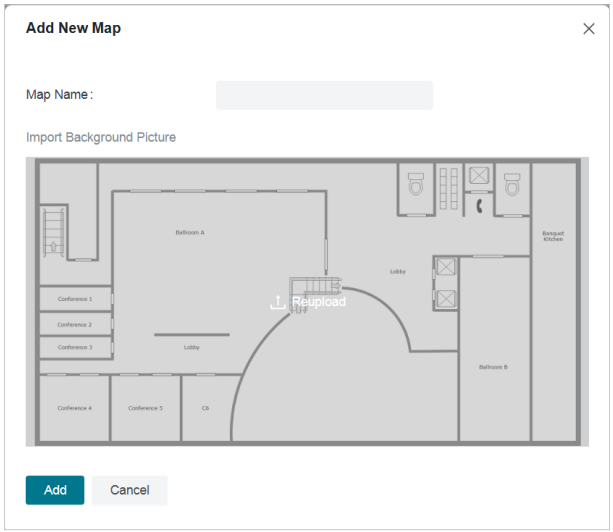


2. Click **Add New Map**.

3. Either click the + button or drag your file into the designated area to upload the map. Supported formats include PNG, JPG, JPEG, BMP, SVG, and PDF.

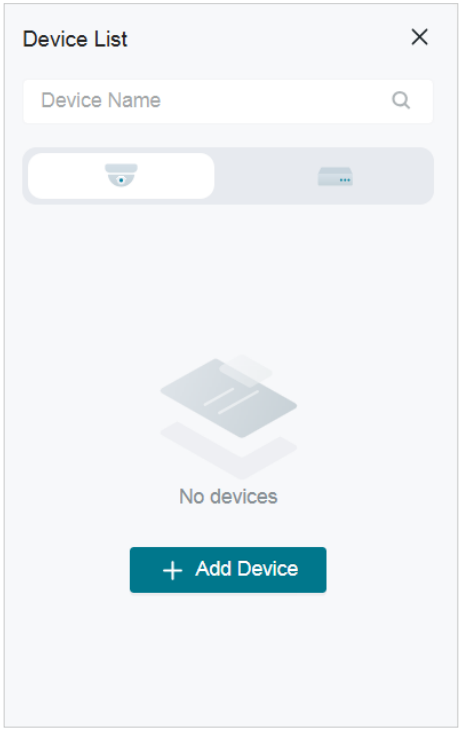


4. Once your file is uploaded, you can preview the map. If you need to change the file, click **Reupload**.

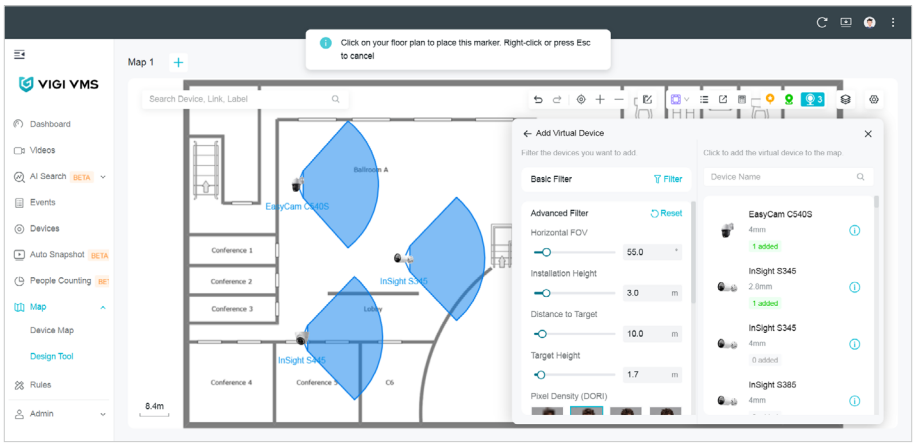


5. Enter a name for your map and click **Add**.
6. To view all current models of IPCs and NVRs with their parameter information, click in the upper right corner.

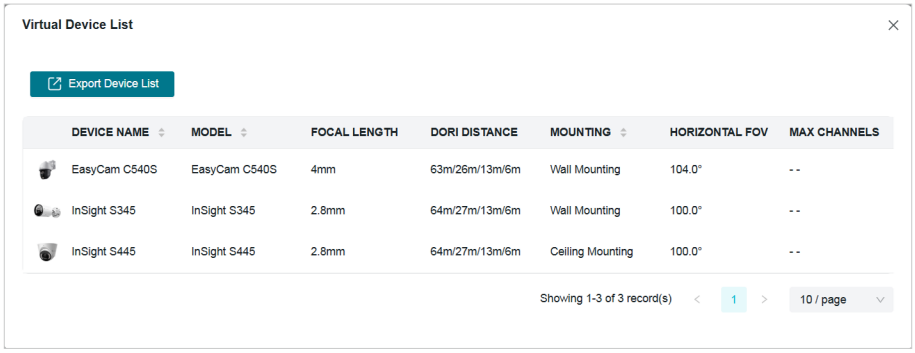
7. In the pop-up window of **Device List**, click **Add Device**.



8. Choose the device you want to add and drag it onto the map.



9. To view all the device markers you've added, click . You may click **Export Device List** to download the file.



10. To save the map with the added markers, click .

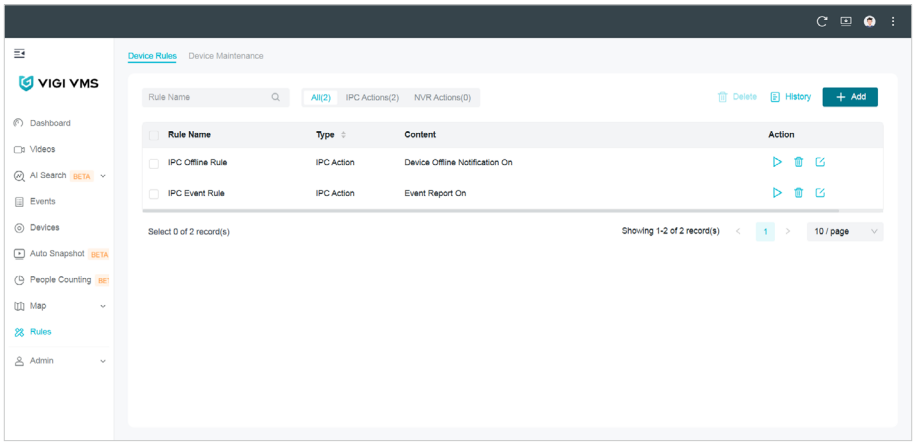
6. 7 Rules

In the Rules module, Device Rules enable you to set general rules for managing devices within your VMS. These rules allow for streamlined batch configuration of devices and tailored event processing. The rules are executed on the server side to effectively handle events triggered by the devices.

6. 7. 1 Device Rules

View Rules

1. Click **Rules** in the menu bar.
2. The main screen will display the list of active rules.
3. You can filter the list by type or use the fuzzy search bar for easier navigation.

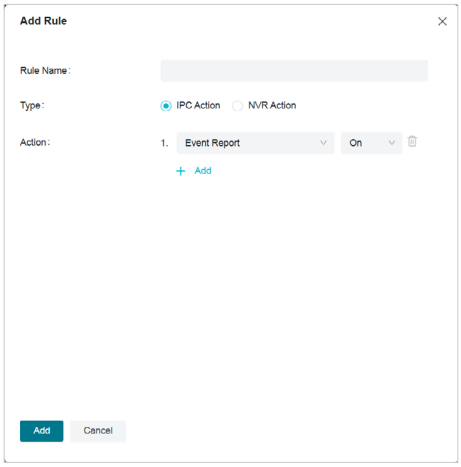


Add/Edit Rules

To add rules, follow these steps:

1. In the **Rules** section, click + Add in the top right corner.
2. A pop-up window will appear where you can fill in the necessary details for the new rule.
3. From the Action drop-down menu, choose the specific actions you want to configure for the device.

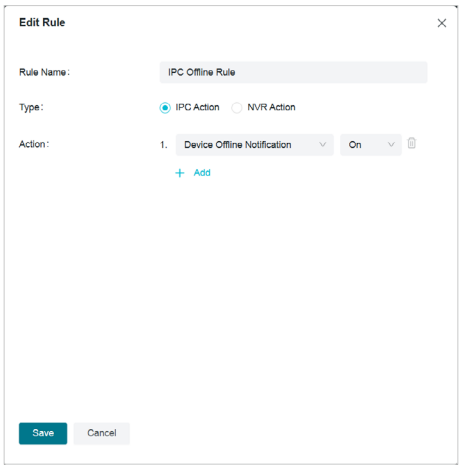
4. If you need to add additional actions, click **+ Add** below the drop-down. The actions will be executed in the order they are added.



5. Click **Add**.

To edit rules, follow these steps:

1. Click in the Action column of the rule list.
2. In the Edit Rule window that appears, modify the rule details as needed. From the Action drop-down menu, choose the specific settings you want for the device.
3. If you need to add more actions, click **+ Add** below the drop-down menu. The actions will be executed in the order they are added.



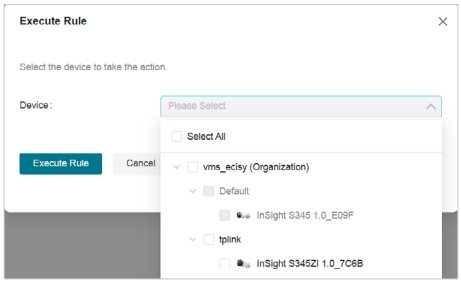
4. Click **Save** to apply your changes.

Execute Rules

To apply a rule to the selected devices, follow these steps:

1. In the rule list, click in the Action column.
2. On the **Execute Rule** page, check the box next to the device(s) you want the rule to affect.

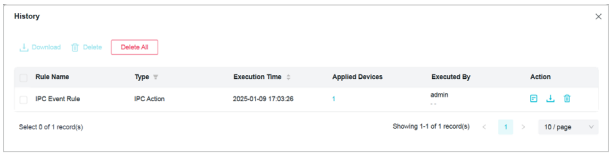
3. Click **Execute Rule** to apply the settings to the selected device(s).



View Rules History

Once a rule is executed, a history record is created. You can view this record by following these steps:

1. Click **History** to open the list of executed rule records.
2. To save the history, click **Download** to save it in .XLSX format.
3. For more details about a specific rule, click Details to view the rule's actions and results.
4. If you wish to download multiple history records at once, select the entries you want and click **Download**, or click **Download All** to save everything.

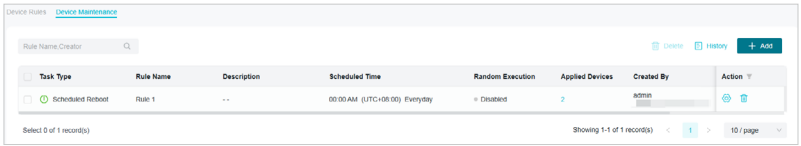


6. 7. 2 Device Maintenance

The Device Maintenance feature in VMS allows you to manage tasks related to device upkeep, such as scheduling reboots and configuring rules to automate these processes. This ensures the smooth operation of devices over time without requiring manual intervention.

View Device Maintenance Rules

1. To view existing maintenance rules, go to **Devices** > **Device Maintenance**.
2. You will see a list of all the scheduled tasks, including the Task Type, Rule Name, Description, Scheduled Time, and the Devices applied to each rule.

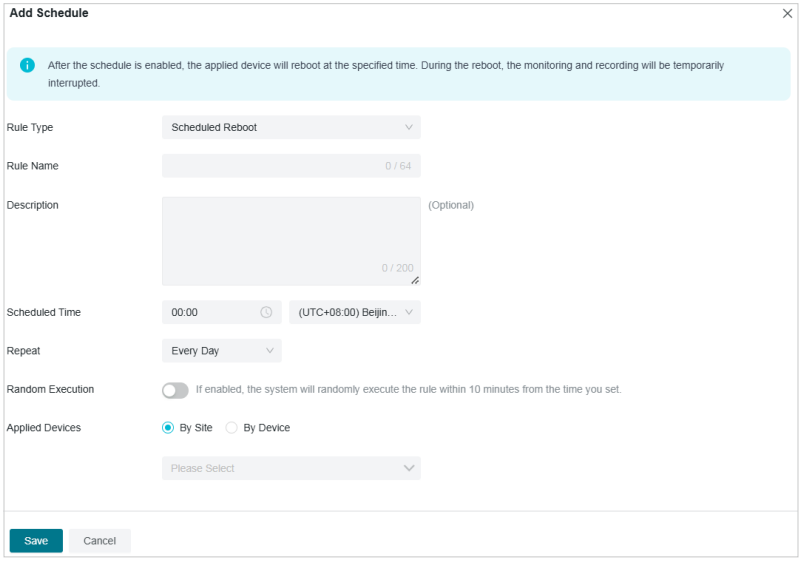


3. You may click  to edit the rule or click  to delete it.

Add a New Device Maintenance Schedule

To create a new device maintenance rule, follow these steps:

1. Click the **+ Add** button in the top right corner of the **Device Maintenance** page.



2. In the Add Schedule window, input the required details:

Rule Type	Select the type of maintenance task
Rule Name	Enter a name for your rule.
Description	Optionally, provide a description of the maintenance task.
Scheduled Time	Set the specific time when the device will be rebooted (e.g., 00:00). Ensure the time is set according to your local time zone.
Repeat	Choose how often the task will be repeated.
Random Execution	If enabled, the system will randomly execute the rule within 10 minutes from the scheduled time.
Applied Devices	Choose whether this rule applies to devices by Site or by Device. Select the relevant devices accordingly.

4. Once all details are filled out, click **Save** to create the maintenance schedule.

6. 8 Organization and Site

A site refers to a cluster of devices within the same geographical area. Devices are organized by geographical locations, and you must first set up the site before adding devices to it. Once the site is set up, you can manage the site and its devices, including adding, deleting, or editing the site details and managing users. The system allows a maximum of 50 users per site.

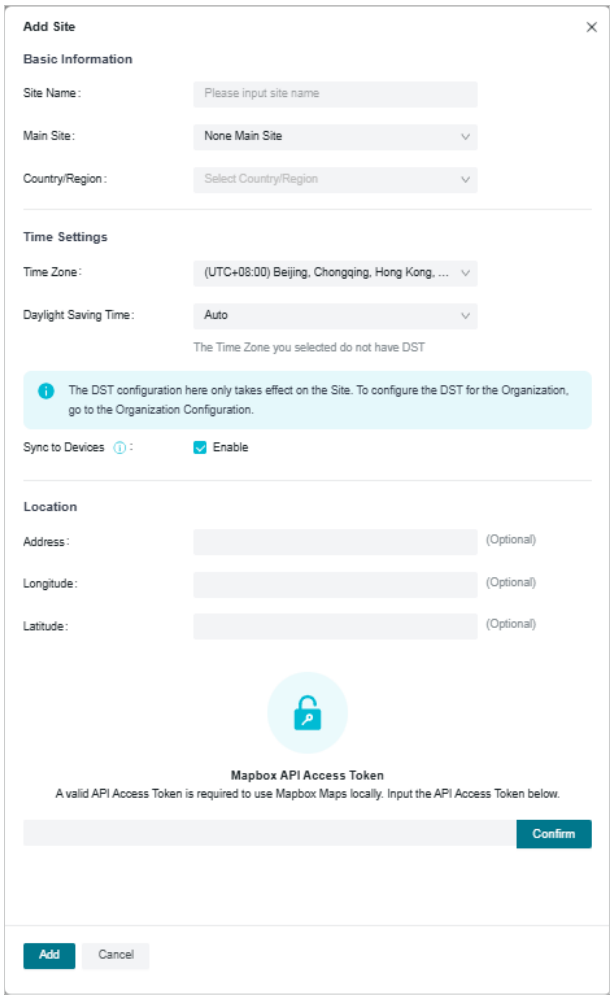
To access site management, navigate to **Admin** > **Org & Site** from the menu bar.

On the Site page, you will see Site Organization on the left side, with the site's details displayed on the right side.

6. 8. 1 Site List

In the Site List, you can manage all site-related information. You can view the list of existing sites, edit site and organization details, add new sites and sub-sites, refresh the site list, and delete any site.

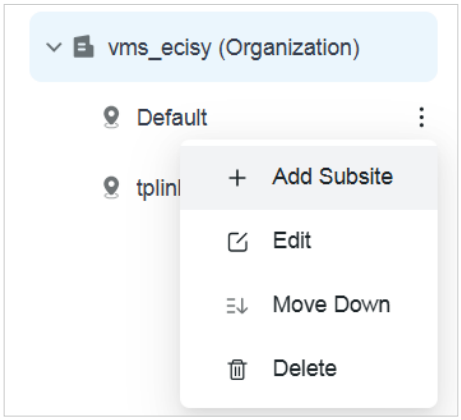
1. To add a site, click **Add Site**.
2. In the Add Site window, fill in required fields:



Site Name	Enter a name for the new site.

Main Site	If this is a sub-site, specify the main site.
Country/Region	Choose the country or region where the site is located.
Time Settings	Select the correct time zone.
Daylight Saving Time	Enable or disable based on whether your site observes DST.
Sync Details	Enable or disable synchronization with the main site.
Location	Fill in the location details (e.g., address, city).
Longitude & Latitude	Optionally provide the exact geographical coordinates.
Mapbox API Access Token	A Mapbox API Access Token is a unique string that associates your application with your Mapbox account, granting access to Mapbox's mapping and location services. Add the token if Mapbox API services are being used.

3. Once all the information is entered, click **Confirm** to add the site.
4. To add a subsite, click ⋮ **> Add Subsite** on the right of the site.

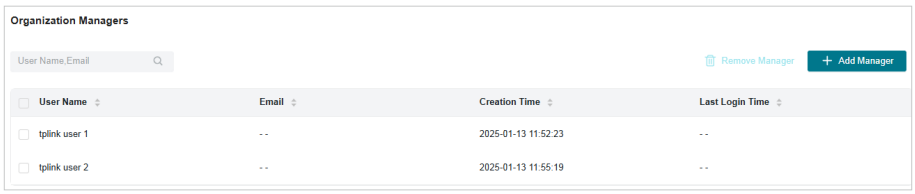


5. To delete a site, click ··· **> Delete** on the right of the site.

6. 8. 2 Organization Details

In **Organization Details**, you can edit and view organization information and organization administrators.

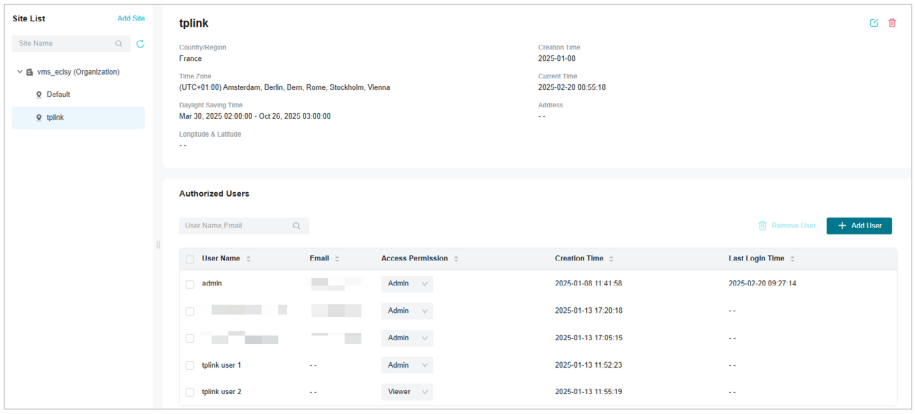
Click the organization name to open the **Organization Details** page, where you can see all Org Managers listed for the organization.



6. 8. 3 Site Details

Site details are displayed at the top of the Site page, where you can manage information about the site, edit the site settings, and delete the site.

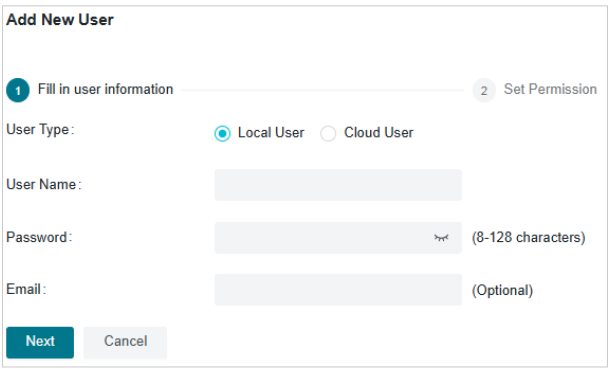
To make changes to a site, click Edit to modify the details such as site name, location, or configuration.



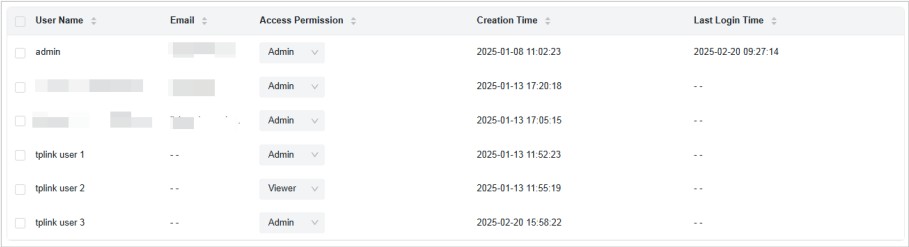
6. 8. 4 Site Users

Site Users allows you to manage user roles and permissions for your site. You can add new users, edit their roles, or delete users from the site.

Click **Add User** to add existing users of the system or new users to the site.



The administrator can edit the users' site roles, including **Admin**, **Viewer**, and **Live Only**.



The site roles are as follows:

Site Role	Permission
Admin	● Add, manage, and control the devices ● Preview and play back the videos of a site ● View and edit site settings
Viewer	● Preview and play back the videos of a site
Live Only	● Preview the videos of a site

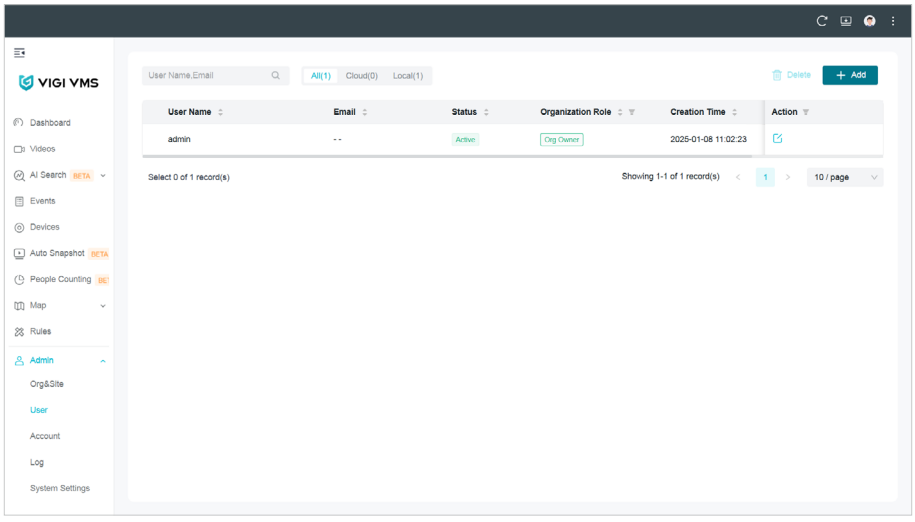
6. 9 User

In **User**, you can add, edit, delete, and search for the users, and set permission for them.

Go to **Admin > User**. On the User page, you can view the user list, and add, delete, and edit users.

6. 9. 1 User List

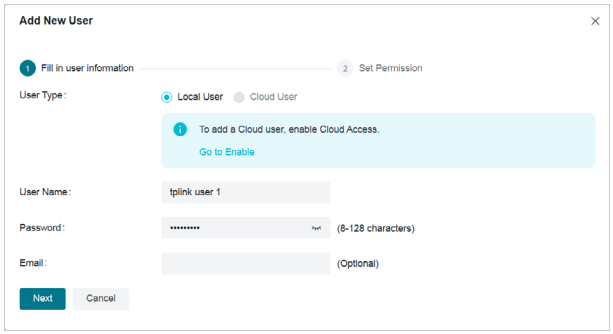
In **User List**, you can view all the users.



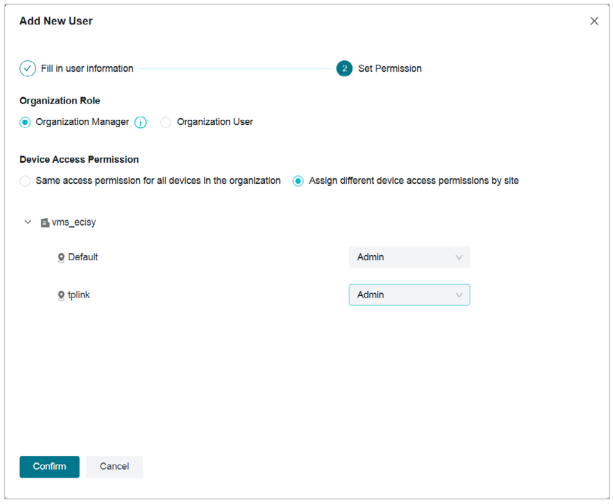
6. 9. 2 Add User

Follow the steps:

1. In the user list, click + Add on the top right corner.
2. In the pop-up window of **Add New User**, select **Local User** and fill in username, password, and email (optional).
3. Click **Next**.



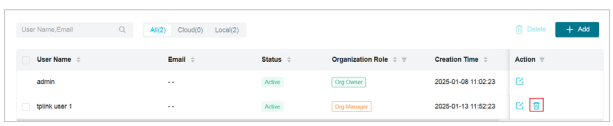
4. Set site permission for the new user, and click **Confirm**.



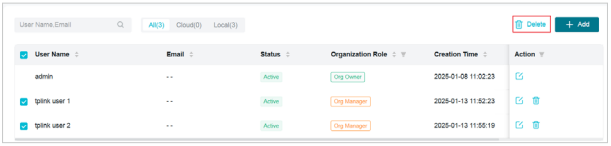
6. 9. 3 Delete User

There are two ways to delete user.

To delete a single user, in the user list, click on the corresponding entry.



To delete users in batches, tick the checkboxes on the right of the user names, then click **Delete** on the top right corner of the user list.

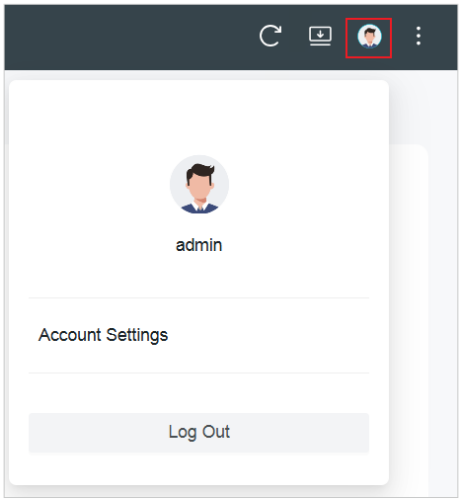


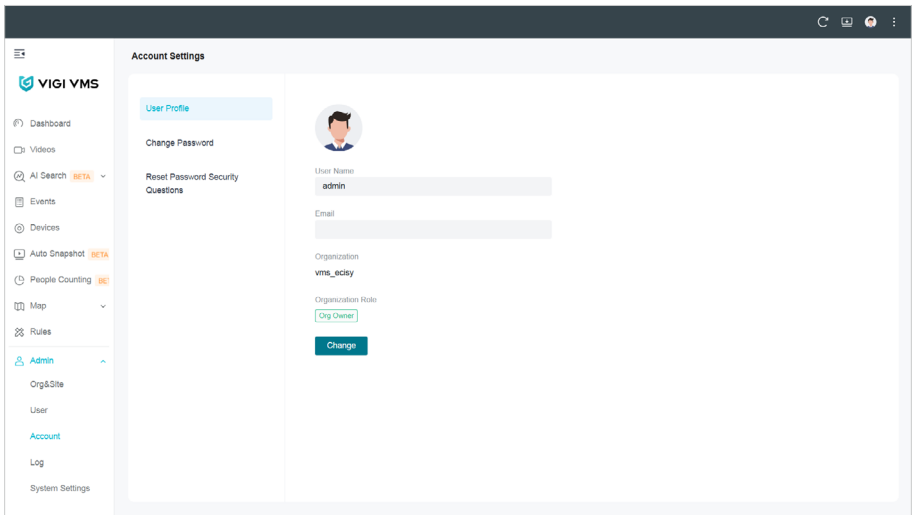
6. 10 Account

In **Account**, you can edit your personal account.

To enter the **Account** page, go to **Admin > Account** in the menu bar.

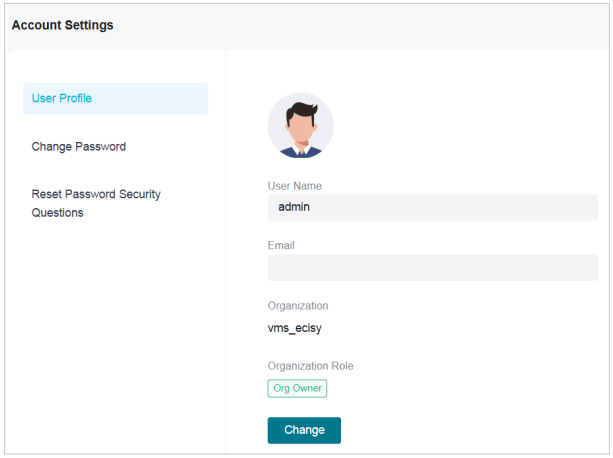
Or, on the VMS main screen, click your profile photo in the top right corner. In the popped-up drop-down list, select **Account**.





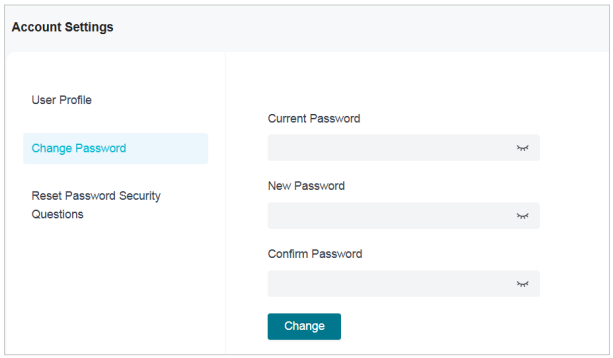
6. 10. 1 Edit User Name and Email

To edit **User Name** and **Email**, click **User Profile**.



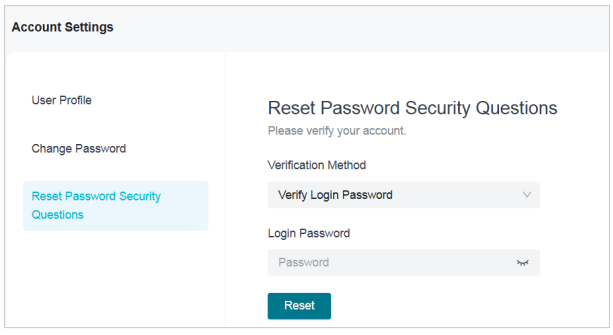
6. 10. 2 Change Password

To change password, click **Change Password**.

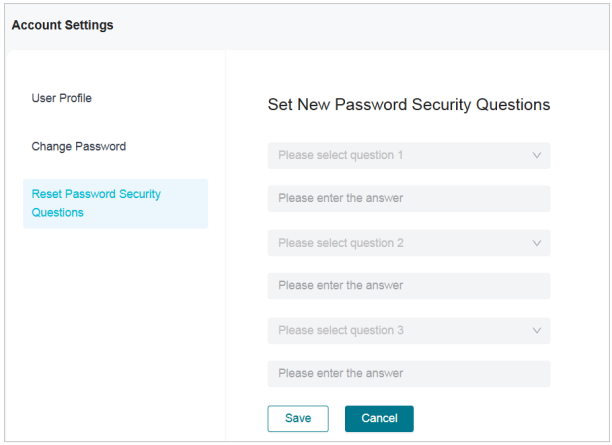


6. 10. 3 Reset Password Security Questions

To reset **Password Security Questions**, click **Reset Password Security Questions**.



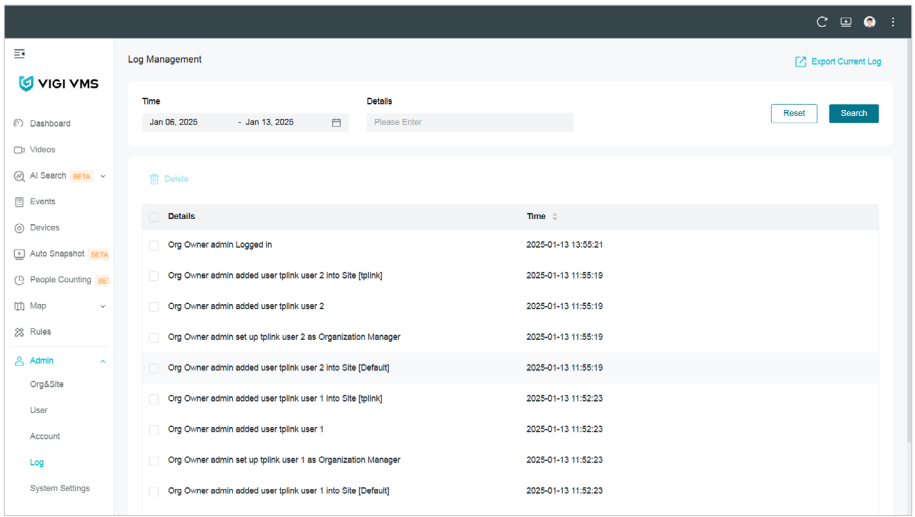
Before resetting password security questions, enter the current password, click **Reset**, then you can set the new password security questions.



6.11 Log

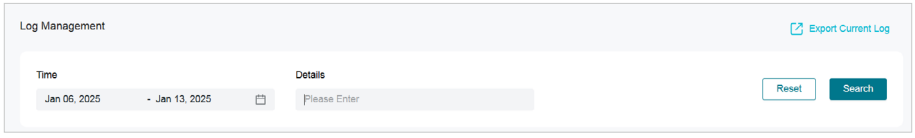
Logs can only be viewed and exported by the organization founder and organization administrator.

Go to **Admin > Log**. In Log Management, you can view the user name, log object, action, details, and create time.



Search for Log

To search for the needed logs, enter key words. You may filter logs by time range. Then click **Search**.



Export Log

To export the logs, click **Export Current Log.**

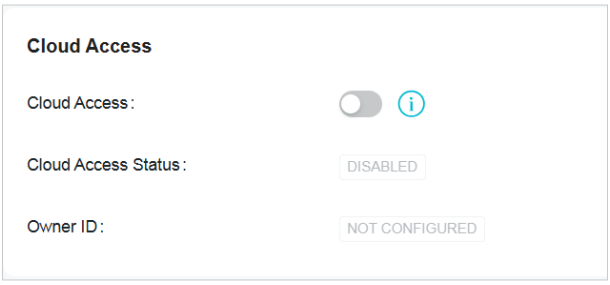
6. 12 System Settings

Only the organization founder and the organization administrator have the access to System Settings.

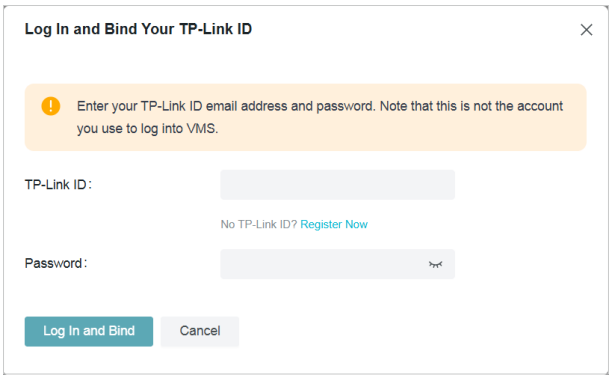
Go to **Admin > System Settings**. In **System Settings**, you can make configurations of the **Video Management System**, as presented as follows.

Change Cloud Access Settings

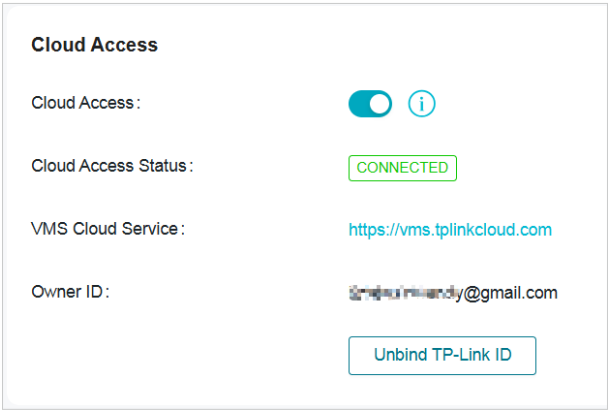
Enable Cloud Access. This feature allows for remote access to the VMS with a TP-Link ID.



Enter your TP-Link ID and password, and click **Log in and Bind**.



The status of Connected indicates success.



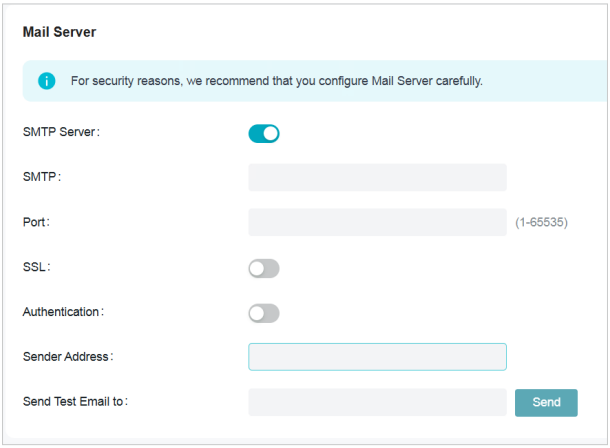
Note: The Cloud Access feature is currently not available in VMS version 1.8.

■ Edit Log Data Retention and Event Data Retention

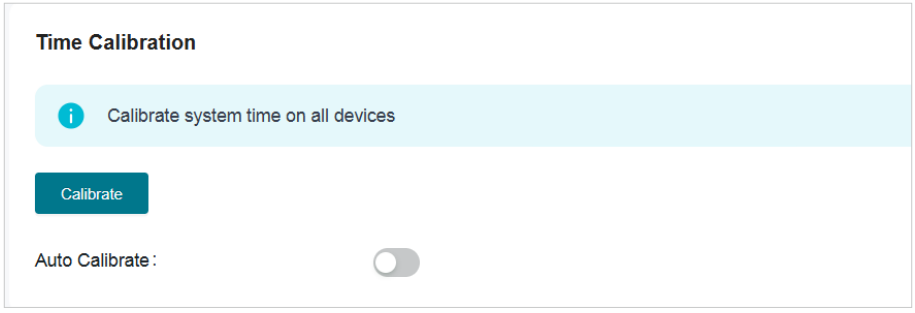
Set how long the log data and event data will be kept.

■ Configure the Mail Server

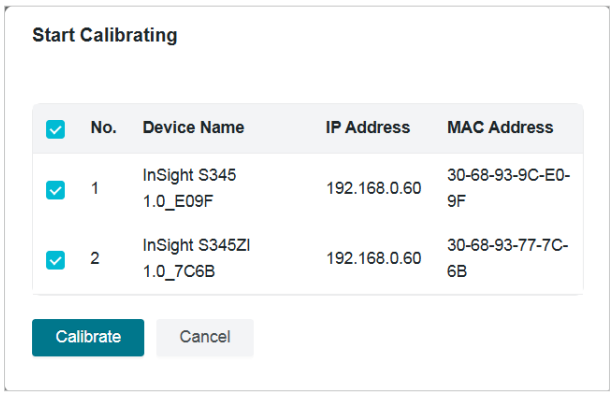
Enter the mail server settings.



■ Calibrate system time on all devices

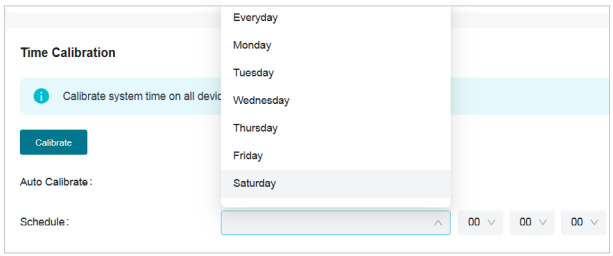


Click **Calibrate** to manually calibrate system time on the devices. Check the devices in the pop-up window. When finished, click **Calibrate**.



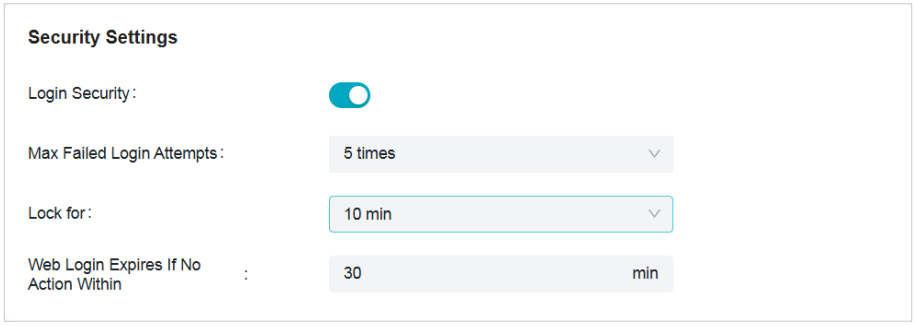
You may set a schedule for automatic time calibration.

Enable **Auto Calibrate**. Select the day of the week and time.



■ Configure login security settings:

You can set the maximum failed login attempts, and when the attempts reached, the account will be locked for a specific period.



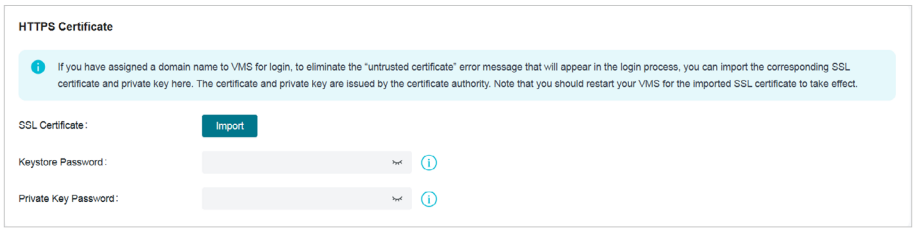
■ Configure HTTPS Certificate

If you have assigned a domain name to VMS for login, to eliminate the “untrusted certificate” error message that will appear in the login process, you can import the corresponding SSL certificate.

The certificate and private key are issued by the certificate authority.

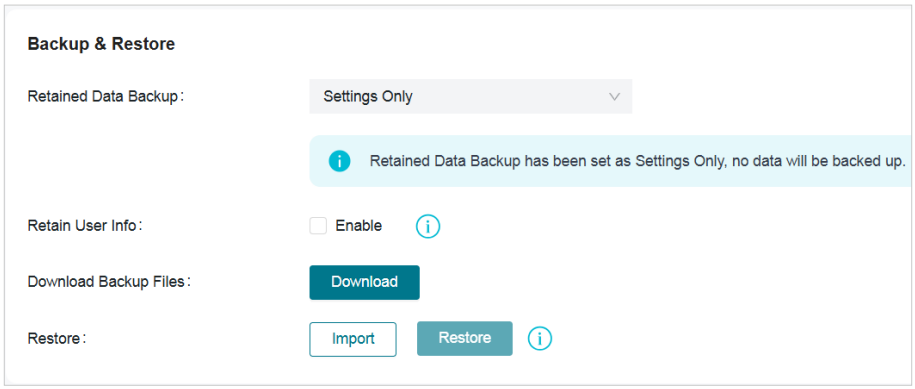
Enter keystone password and private key password if they are included in your certificate.

Note: You should restart your VMS for the imported SSL certificate to take effect.



Set Backup & Restore

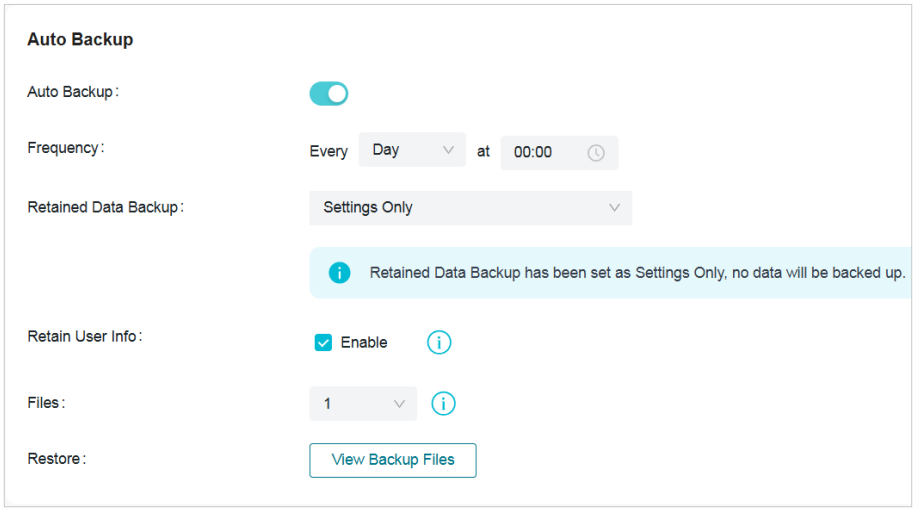
The local and cloud organization owners can back up and restore settings.



Set Auto Backup

The Auto Backup feature in the VMS system allows you to automatically back up your system settings, user information, and other essential data at regular intervals. This feature is useful for ensuring that your configuration and data are protected in case of system failures or unexpected disruptions.

Enable **Auto Backup** and set the parameters:

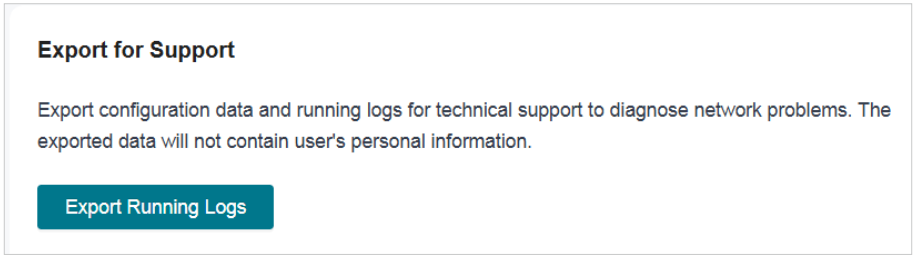


Parameters	Explanation

Frequency	Set how often the backup occurs.
Retained Data Backup	Choose what data to back up.
Retain User Info	With the option enabled, local and cloud user information will be retained.
Files	When the backup files exceed this number, the excess old backup files will be automatically deleted.
View Backup Files	View the list of backup files currently stored.
Restore	Option to restore data from a backup.

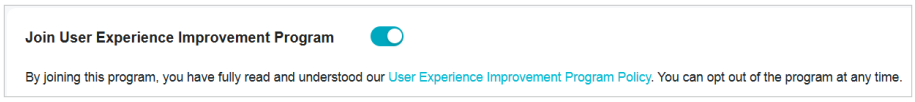
Export logs to seek technical support

Logs are useful for technical support teams to identify the issues. In VMS, the local and cloud organization owners can export data and running logs.



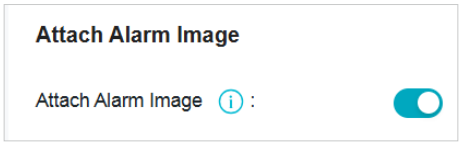
Join user experience improvement program

Determine whether to join our user experience improvement program to help us improve the product for better user experience.



Attach alarm images

When this feature is enabled, the device will attach an alarm thumbnail when uploading alarm information to VMS.



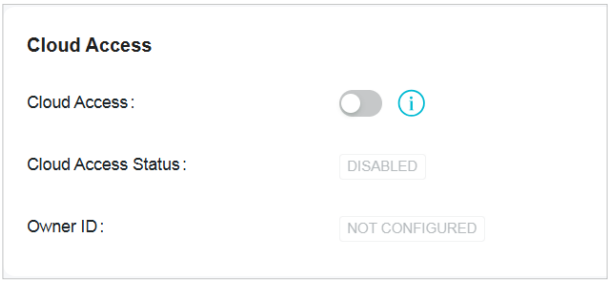
6. 13 Cloud Access

Cloud Access functions allow the user to access VMS remotely, realizing real-time management and surveillance. You need to first bind a cloud account to VMS, and use this account to access VMS via the cloud. To make multiple users access VMS, all you need to do is to invite them.

Note: The Cloud Access feature is currently not available in VMS version 1.8.

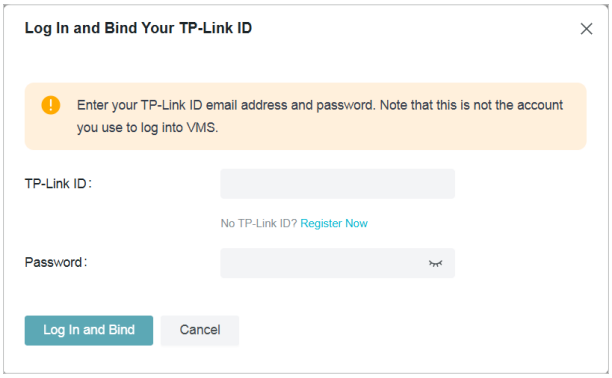
6. 13. 1 Configure Cloud Access

In **Admin > System Settings > Cloud Access**, you can bind cloud users to VMS, and check cloud access status.



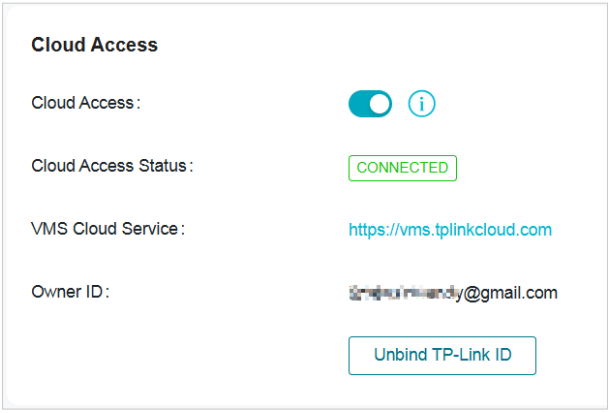
Bind a cloud user

1. When NOT CONFIGURED appears in Owner ID, it indicates that no cloud user has been bound to VMS yet.
2. Enable **Cloud Access**, and enter your TP-Link ID and password in the pop-up window.
3. Click **Log In and Bind**.

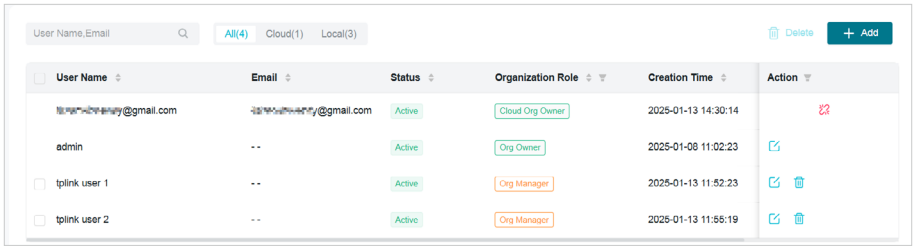


Note: The TP-Link ID should be registered in the VMS cloud, otherwise it cannot be bound. You can click Register Now to finish this step, and then bind your account to VMS.

When the binding process is completed, wait until the Cloud Access Status becomes CONNECTED, and you can access VMS via the cloud.



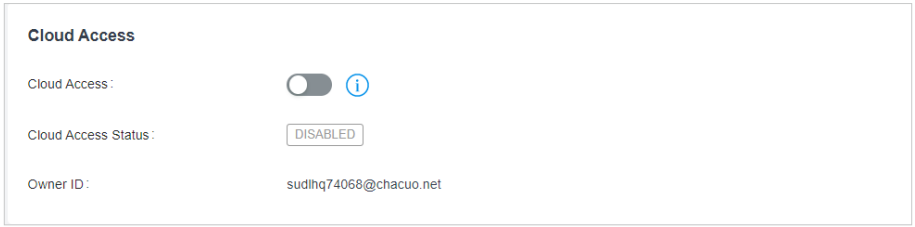
And your newly bound TP-Link account will appear on the user list (to check it out, go to **Admin > User**), whose organization role is Cloud Org Owner.



Enable/disable Cloud Access

When you have bound a cloud user to VMS, you can enable or disable Cloud Access by toggling on or off the button. If Cloud Access is disabled, all the cloud users bound or invited cannot access VMS via the cloud.

When Cloud Access is disabled, the **Cloud Access** page looks like this:

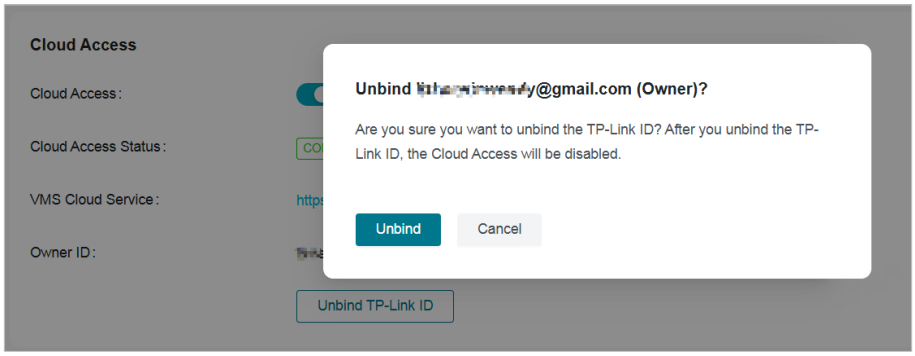


Unbind a cloud user

If a cloud user has been bound to VMS and the **Cloud Access Status** is CONNECTED, you can unbind the cloud user, and the invited cloud users will also be deleted from VMS. All the cloud users bound or invited will be unable to visit VMS via the cloud.

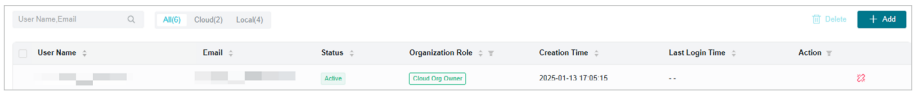
Option 1:

On the **Cloud Access** page, click Unbind TP-Link ID. In the pop-up window, click Unbind to unbind the cloud user.

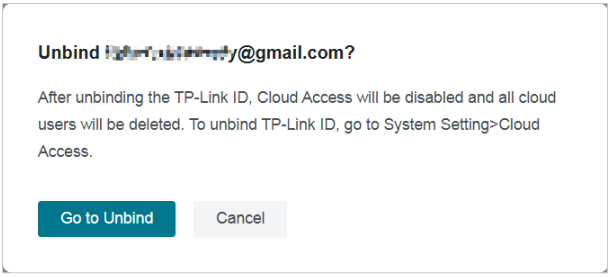


Option 2:

Go to **Admin > User**, locate the **Cloud Org Owner** in the user list, and click in the **Action** column.



Click **Go to Unbind** in the pop-up window.

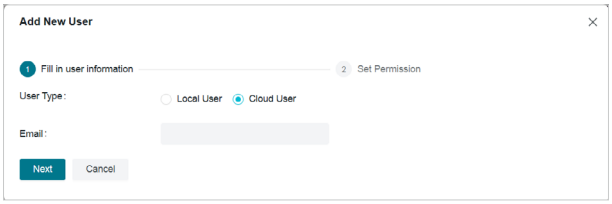


The page will be redirected to the **Cloud Access** page. Follow steps in Option 1 to complete the unbinding.

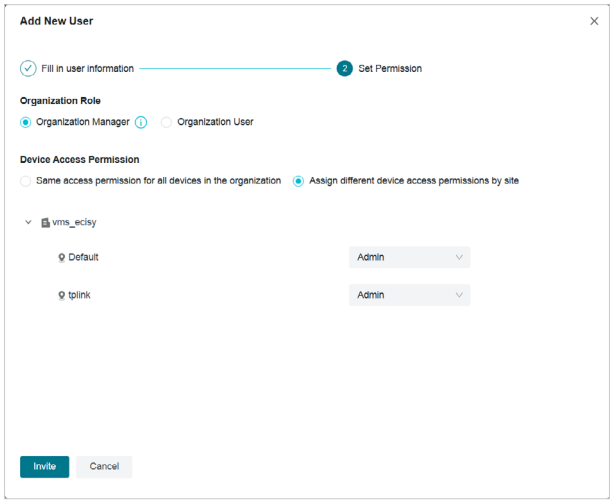
6. 13. 2 Invite a Cloud Users

Steps:

1. Click **Admin > User > Add** to invite a cloud user.
2. In the pop-up window, check **Cloud User**, enter an email address, and click **Next**.

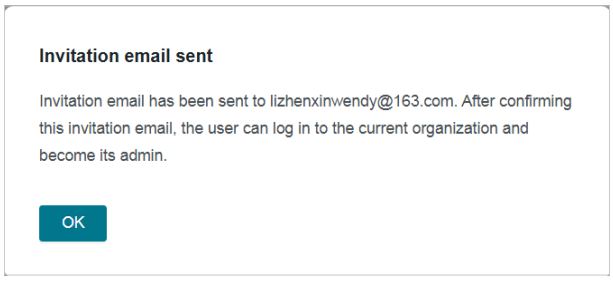


3. Assign the role and permissions of the new user and click **Invite**.



Roles	Explanation
Admin	● Add, manage, and control the devices ● Preview and play back the videos of a site ● View and edit site settings
Viewer	● Preview and play back the videos of a site
Live Only	● Preview the videos of a site
No Access	● No access to a site.

4. In the notification window, click **OK**. When a cloud user is invited successfully, the cloud user can visit VMS via the cloud.



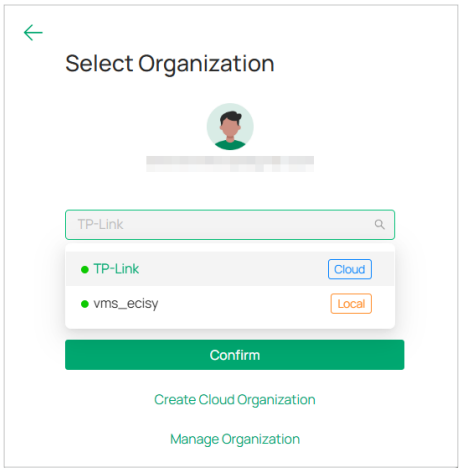
6. 13. 3 Access VMS via the Cloud

When Cloud Access is enabled and the Cloud Access Status shows Connected, bound or invited

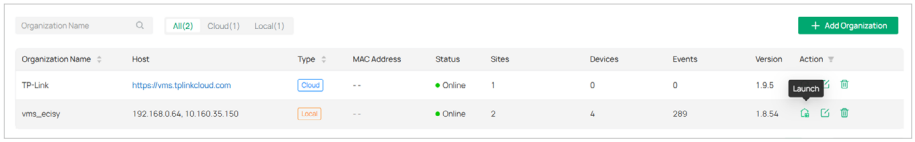
cloud users can log in to the system through the following steps:

1. Visit https://vms.tplinkcloud.com.

2. On the Select Organization page, choose your local VMS to log in.



3. Alternatively, on the Organization Management page (located at https://vms.tplinkcloud.com/#/manage-vms), click to enter your local VMS.



6. 14 Forget Password

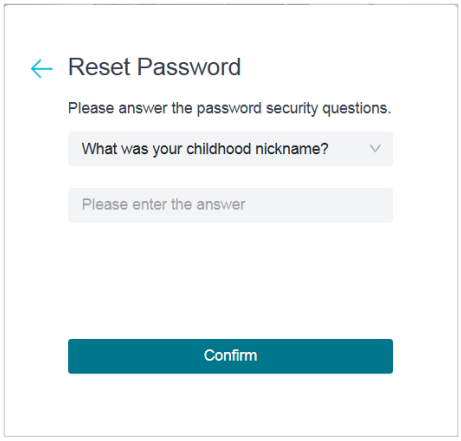
VMS supports password reset for the Org Owner who forgets the password. Local users with other roles can get the VMS password by contacting the **Org Owner**. The cloud user needs to retrieve the password via the cloud.

Org Owner can retrieve the password by security questions or the recovery email.

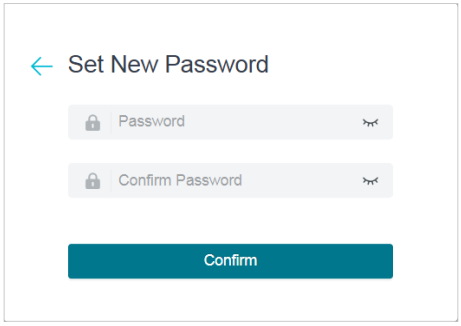
6. 14. 1 Retrieve Password via Security Questions

When registering as an **Org Owner**, you are required to set three security questions for password recovery. For details, refer to Manage the Login.

Click **Forgot Password?** on the login page, and enter the **Reset Password** page. Select one security question and answer it, and click **Confirm**.

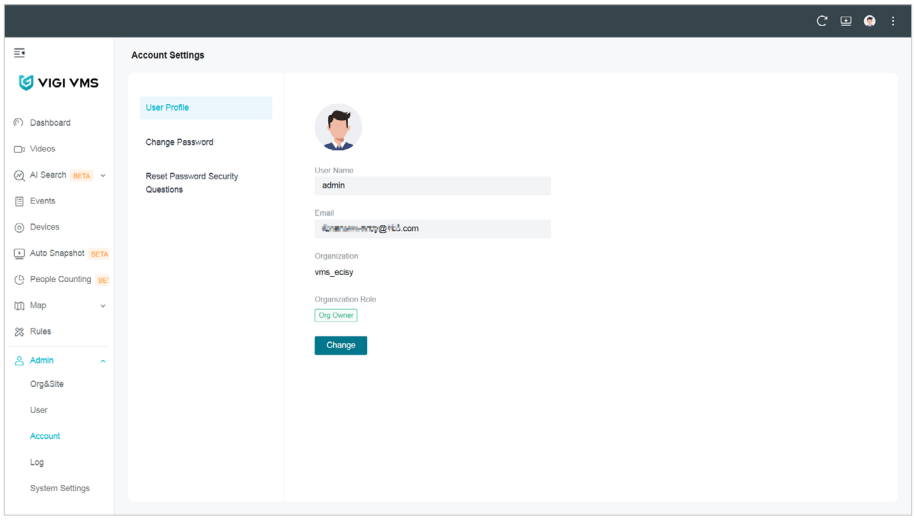


On the **Set New Password** page, enter your new password twice, and click **Confirm**. Then you can log in with the new password for future logins.



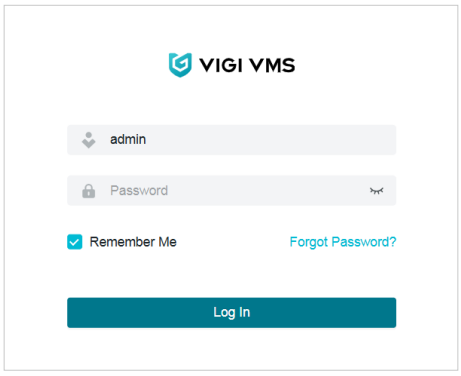
6. 14. 2 Retrieve Password via Email

When registering as an **Org Owner**, you can set a recovery email using a customized email server or TP-Link email server. If you skip this step, you can go to **System Settings**, enable email server or cloud access, go to **Admin** > **User Profile** and enter an email address which would be used as a recovery email.

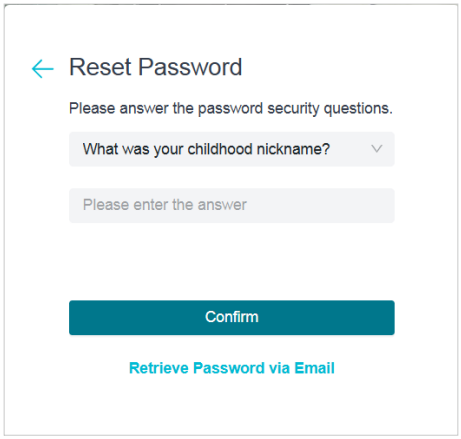


To retrieve your password by recovery email, follow the steps:

1. Click **Forgot Password?** on the login page.



2. On the **Reset Password** page, click **Retrieve Password via Email**.



3. Click **Send**, and a recovery email will be sent to your mailbox. Click the password reset link in the email to set a new password.