



User Guide

VIGI PC Client

About This Guide

This User Guide provides information for managing devices via TP-Link VIGI PC Client.

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.

<u>Underlined</u>	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://support.vigi.com/>.
- Product specifications can be found on the product page at <https://www.vigi.com>.
- For technical support, the latest version of the Quick Installation Guide, User Guide and other information, please visit <https://support.vigi.com/>.

Contents

- About This Guide II
- Introducing VIGI PC Client 1
 - Introduction..... 2
- Getting Started 3
 - System Requirements..... 4
 - Install the Software..... 4
 - Manage the Login 5
- Add Devices 7
 - Auto Add Device 8
 - Manually Add Device 10
 - Import Device 11
- Live View 12
 - Configure the Screen Layout..... 13
 - Configure Live View Settings via Toolbar 15
- Playback 17
 - Instant Playback 18
 - Play Normal Recordings..... 18
 - Playback Recordings of Events..... 19
 - Playback Operations 21
 - Basic Playback Operations 21
 - Edit Recordings 22
 - Export Recordings 22

AI Monitoring (for Enterprise Edition)	23
Event Center (for Enterprise Edition)	26
Recording Export	29
Download Center	31
Site Map (for Enterprise Edition)	33
Device Management	35
Device Management.....	36
Change Camera Settings.....	37
Device Information	37
System Log.....	37
Image.....	38
OSD	40
Privacy Mask	41
Video.....	41
Audio.....	42
ROI.....	43
Advanced Settings	43
PTZ (Only for Models with Motorized Lens)	43
Arming Schedule and Processing Mode	44
Message.....	44
Motion Detection.....	45
Camera Tempering.....	45
Scene Change Detection	46
Line Crossing Detection.....	46
Intrusion Detection	47
Region Entering Detection.....	48
Region Exiting Detection.....	48
Loitering Detection.....	49
Object Abandoned/Removal Detection	50
Abnormal Sound Detection.....	50
Vehicle Detection	51
Human Detection	51

Smart Frame.....	51
Access Exception	52
Sound Alarm.....	52
Alarm Server.....	52
Alarm Input	52
Alarm Output.....	53
VCA	53
Update Firmware.....	53
Reboot Device	54
Recording Schedule	54
Change NVR Settings.....	54
Device Information	54
System Log.....	54
System Information.....	55
Recording Control.....	55
Recording Schedule	56
Hard Drive Management	56
Internet Connection.....	57
Network Isolation.....	57
Port.....	58
UPnP	59
Email.....	60
IP Restriction	60
DDNS.....	60
SNMP.....	61
Openapi.....	61
Change Basic Settings.....	61
Modify Device Time.....	62
Interface Output	62
Change Password.....	63
Upgrade Firmware.....	63
Import and Export Configuration File	63
Reboot Device	64



Introducing VIGI PC Client

This chapter covers the basic functionalities of VIGI PC Client.

1.1 Introduction

VIGI PC Client can automatically detect devices on the same LAN for seamless addition, improving operation efficiency. VIGI PC Client supports Work without Login / Personal Edition / VIGI VMS / VIGI Cloud VMS modes—switch freely to unify device control and adapt security management across all scenarios. You can also easily access VIGI VMS and VIGI Cloud VMS through PC client.

Personal Edition: With a user-friendly interface and simple operation, the Personal edition is suited for small-scale scenarios, enhancing surveillance efficiency and user experience.

Use without Login: Easily manage small local systems with an intuitive interface, keeping your data private and secure.

The software provides multiple functionalities, including:

Live View: Watch live on the open screen with an auto-optimized layout for the best multi-device viewing experience.

Playback: The Timeline design enables quick playback searches by time, date, or events, saving you time and ensuring you never miss a detail.

Recording Export: Select the time and device, and videos will be automatically exported and merged by day in the background, providing a hassle-free download experience.

Download Center: Manage the download tasks.

Device Management: Features a variety of configuration settings, including picture parameters, events, network settings, and recording schedules, for more convenient management.

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.

2

Getting Started

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

- [System Requirements](#)
- [Install the Software](#)
- [Manage the Login](#)

♥ 2.1 System Requirements

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

■ For small monitoring scale (1-8 channels)

CPU: Intel i5-12400 (6 cores and 12 threads) & AMD Ryzen 5 5600G (6 cores and 12 threads)

GPU: NVIDIA GTX 1650 (4GB GDDR6) & AMD RX 6400 (4GB GDDR6)

Memory: 16GB DDR4 3200MHz (dual channel)

Network: Gigabit network card + PoE switch

■ For medium monitoring scale (8-64 channels)

CPU: Intel i7-12700K (12 cores and 20 threads) & AMD Ryzen 7 7700X (8 cores and 16 threads)

GPU: NVIDIA RTX 3060 (12GB GDDR6) & AMD RX 6600 XT (8GB GDDR6)

Memory: 32GB DDR4 3600MHz / DDR5 4800MHz

Network: 2.5G network card + 48-port PoE switch

■ For large surveillance scale (64+ channels) (server level)

CPU: Intel Xeon Silver 4310 (12 cores 24 threads) & AMD EPYC 7302P (16 cores 32 threads)

GPU: NVIDIA Tesla T4 (16GB GDDR6) ×2 & AMD Radeon Pro V620 (32GB HBM2) ×2

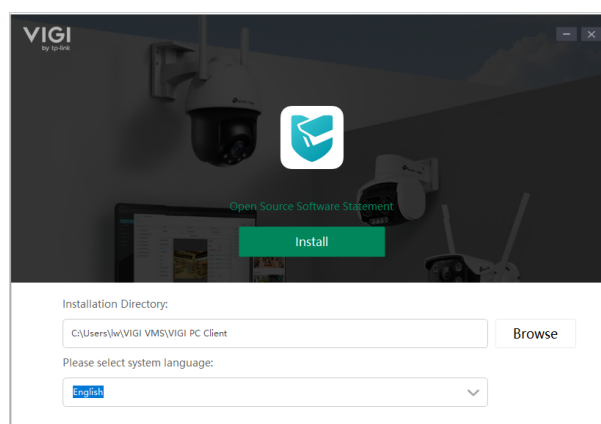
Memory: 64+GB DDR5

Network: 10G NIC + 40G core switch

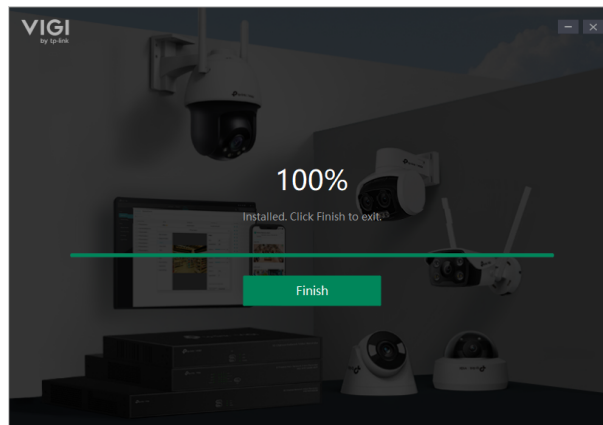
♥ 2.2 Install the Software

Follow the steps to install the VIGI PC Client software:

1. Download the PC Client software at <https://www.vigi.com/support/download/vigi-pc-client/> and double click the installation package to start the installation.
2. Click **Install** and wait for the installation to complete.



3. Click **Finish**.

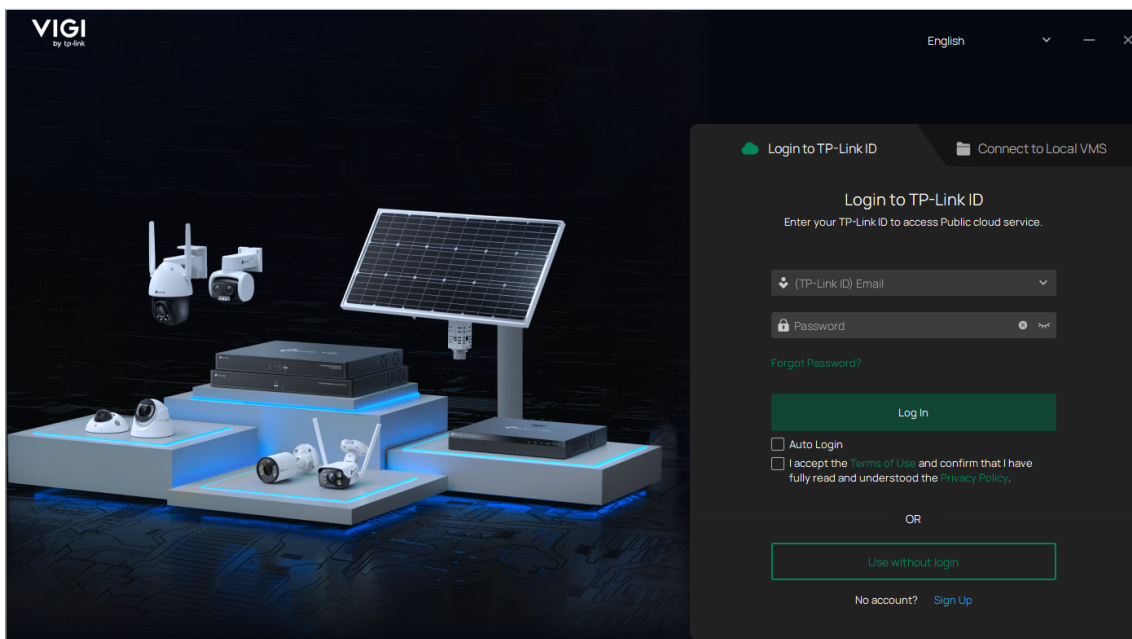


♥ 2.3 Manage the Login

1. Double click the PC Client icon to open the VIGI PC Client software.



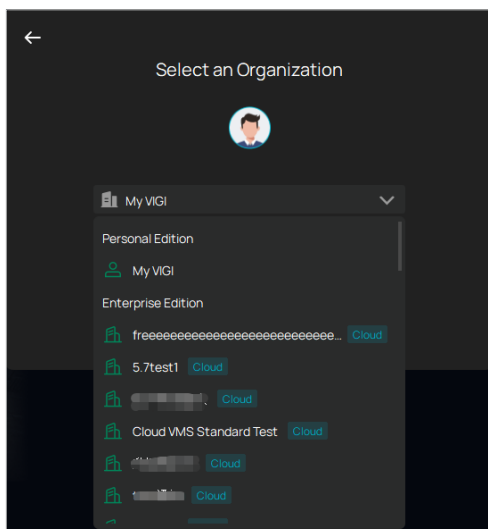
2. You will see the login page. It provides several login methods. Log in to the PC Client software as needed.



■ Log in with TP-Link ID (for Cloud device management)

- 1) Enter your TP-Link ID and password, check **I accept the Terms of Use and confirm that I have fully read and understood the Privacy Policy**, and click **Log In**. If you want to automatically log in to the client without entering the password in the future, check **Auto Login**.
- 2) Select an organization to start using the PC client to manage your devices. Personal Edition is suited for small-scale scenarios while Enterprise Edition is suited for large-scale scenarios with multiple branches and sites.

Note: If you don't have a TP-Link ID yet, click the Sign Up at the bottom of the page to register a TP-Link first.

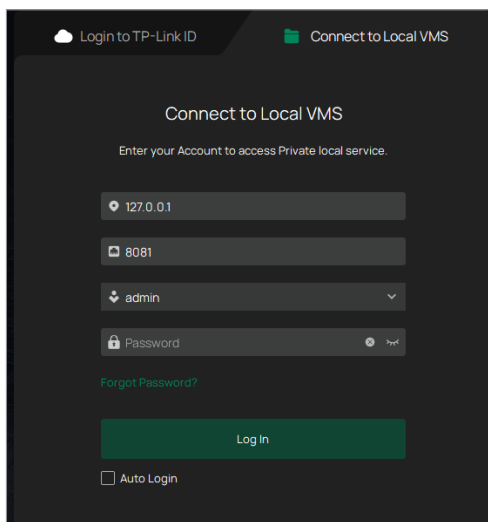


■ Use Without Login (for local device management)

Click **Use Without Login**, and you will enter the PC Client management page.

■ Connect to Local VMS

If you already install local VMS in your computer, and add devices, you can enter the local VMS account to connect the PC Client to your local VMS to manage the added devices using the PC Client software. If you want to automatically connect to the local VMS without entering the password in the future, check **Auto Login**.



3

Add Devices

This chapter provides step-by-step instructions for adding devices using the VIGI PC Client. This chapter covers the following sections:

- [Auto Add Device](#)
- [Manually Add Device](#)
- [Import Device](#)

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

1. Go to the **Device Management** page to enter the device management page.

Device Name	Status	Model	IP Address	MAC Address	Firmware	Action
InSight S225 1.0_AE99	Online	InSight S225	Remote Device	...	1.0.2 Build 250121 Rel.43208n	[Refresh] [Settings] [Delete]
VIGI C540S 1.0_1957	Online	VIGI C540S	Remote Device	...	2.0.4 Build 240913 Rel.56881n	[Refresh] [Settings] [Delete]
18FVIGI NVR2016H-16M...	Online	VIGI NVR2016H-16M...	Remote Device	...	1.3.0 Build 250401 Rel.53960n	[Settings] [Delete]
VIGI C400P-2.8 1.0	Offline	VIGI C400P-2.8	Remote Device	...	1.0.5 Build 210702 Rel.64208n	[Delete]

2. On the device management page, you'll find the device list showing all devices added to the current site. Within the Device List, you can add new devices or remove devices.
3. Click the **Add** button on the top right corner, and the **Add Device** window will appear.

♥ 3.1 Auto Add Device

1. On the **Add Device** page, click **Auto Discover**. A list of detected devices will appear. Check the boxes of the desired devices and click **Apply**.

Add Device

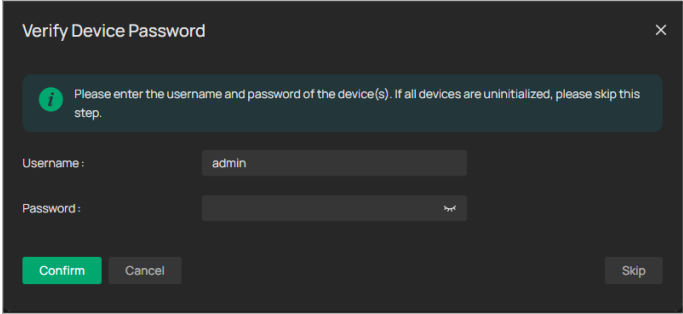
Mode: Auto Discover Manually Add Import

Device Name, Model, IP Rescan

Device Name	Model	IP Address	MAC Address	SN/Device ID
VIGI C485 1.0_65...	VIGI C485	192.168.0.60

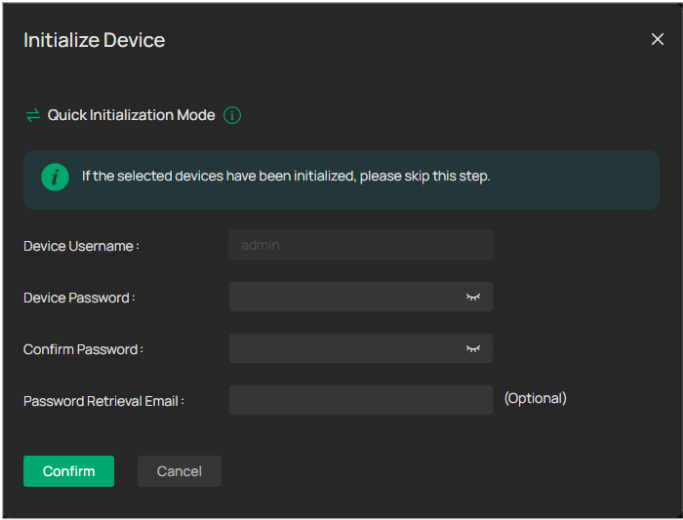
Apply Cancel

2. Verify the device password. If the device is uninitialized, click **Skip**.



A dark-themed dialog box titled "Verify Device Password" with a close button (X) in the top right corner. It contains an information icon and a message: "Please enter the username and password of the device(s). If all devices are uninitialized, please skip this step." Below this, there are two input fields: "Username:" with the text "admin" and "Password:" which is empty. At the bottom, there are three buttons: "Confirm" (green), "Cancel" (gray), and "Skip" (gray).

3. Set a device password to initialize the device. You can also enter your email to retrieve the password if you forget the password.



A dark-themed dialog box titled "Initialize Device" with a close button (X) in the top right corner. It features a toggle switch for "Quick Initialization Mode" with a help icon. Below is an information icon and a message: "If the selected devices have been initialized, please skip this step." The form includes four input fields: "Device Username:" with the text "admin", "Device Password:", "Confirm Password:", and "Password Retrieval Email:" (marked as optional). At the bottom, there are two buttons: "Confirm" (green) and "Cancel" (gray).

4. Then return to the device list page, and you can see the newly added device.

♥ 3.2 Manually Add Device

1. Go to the **Add Device** page and click on **Manually Add**. You can choose to add a device with its serial number or device ID.

Add Device [Close]

Mode: [Auto Discover] [Manually Add] [Import]

Add By ⓘ : ☒ Serial Number ☐ Device ID

i 1. Make sure the device is online.
2. If you add an uninitialized device, please add it via Device ID, and the device will be initialized using the set password.

SN: [Text Box] [Red Minus Icon]

[+ Insert a row](#)

[Apply] [Cancel]

2. Enter the device's Serial Number or Device ID which can be found on the product label. You can click **Insert a row** to enter more devices' serial numbers or device ID for batch configuration.
3. Click **Apply**, then return to the device list page, and you can see the newly added device.

♥ 3.3 Import Device

1. Go to the **Add Device** page and click on **Import**.

Add Device [Close]

Mode : [Auto Discover] [Manually Add] [Import]

File :

i 1. Make sure the device is online.
2. If you add an uninitialized device, please add it via Device ID, and the device will be initialized using the set password.
3. Download the [template](#) and fill in your devices' information. Then import the file.
Up to 1500 devices can be imported at a time.

[Browse]

Please select a .xlsx, .xls, .csv file.

[Apply] [Cancel]

2. Click **Template** to download the template to fill in your device information.

	A	B
1	SN/Device ID	Device Password
2		
3		
4		

3. Click **Apply**, then return to the device list page, and you can see the newly added device.

4

Live View

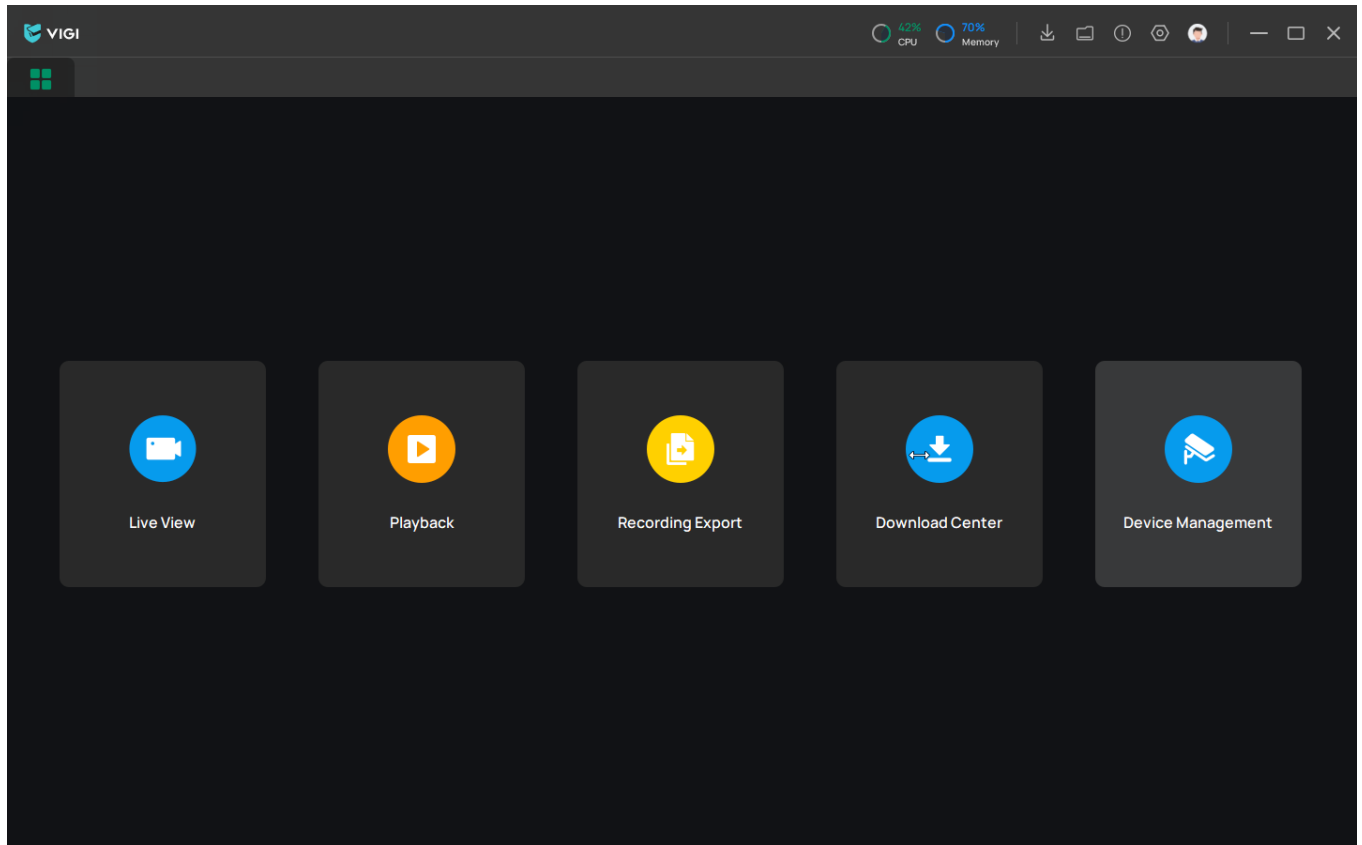
In Live View, you can monitor devices in real time and respond to abnormal conditions with quick operations, such as screenshot, recording, zooming in the image, muting the device and triggering real-time alarm. This chapter contains the following sections:


- [Configure the Screen Layout](#)
- [Configure Live View Settings via Toolbar](#)

♥ 4.1 Configure the Screen Layout

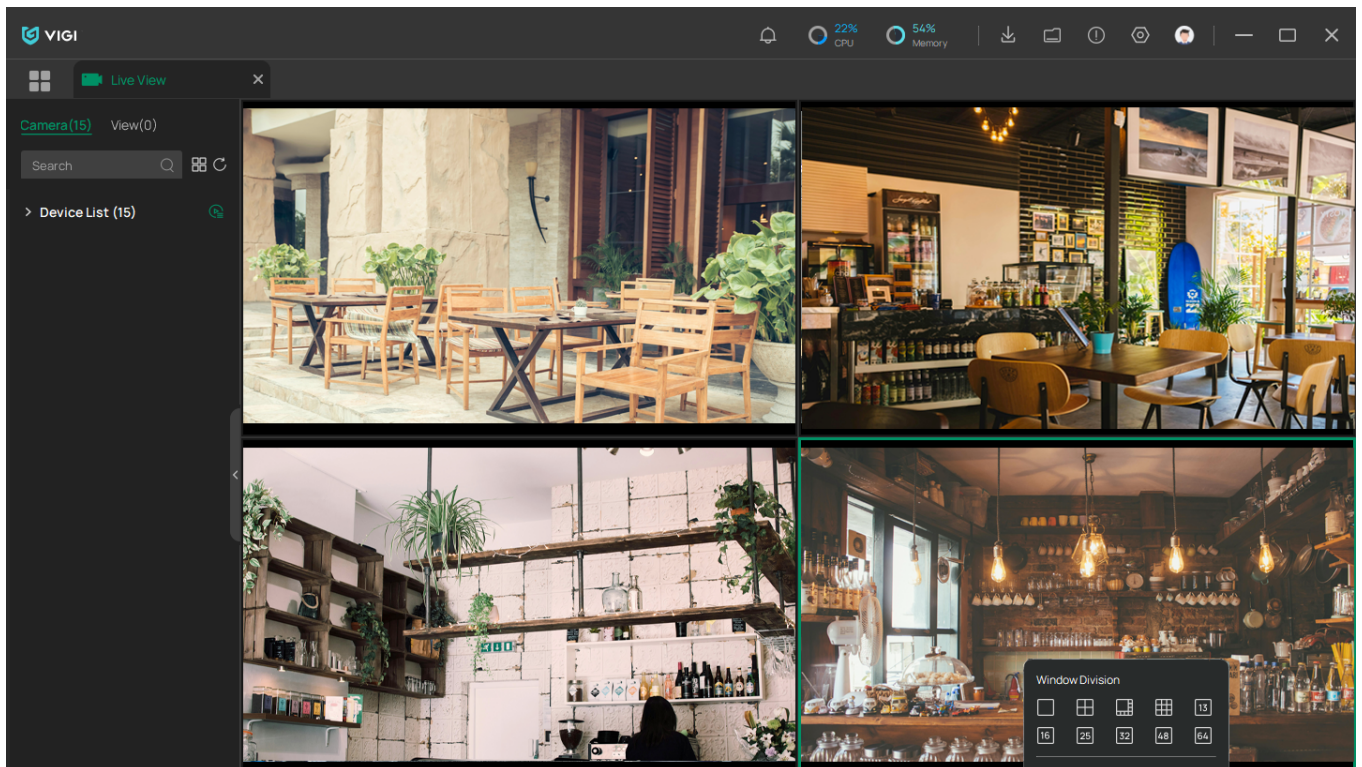
The PC Client displays the videos on several screens. You can flexibly configure the screen layout in both Live View.

1. Click on Live View to enter the Live View page.



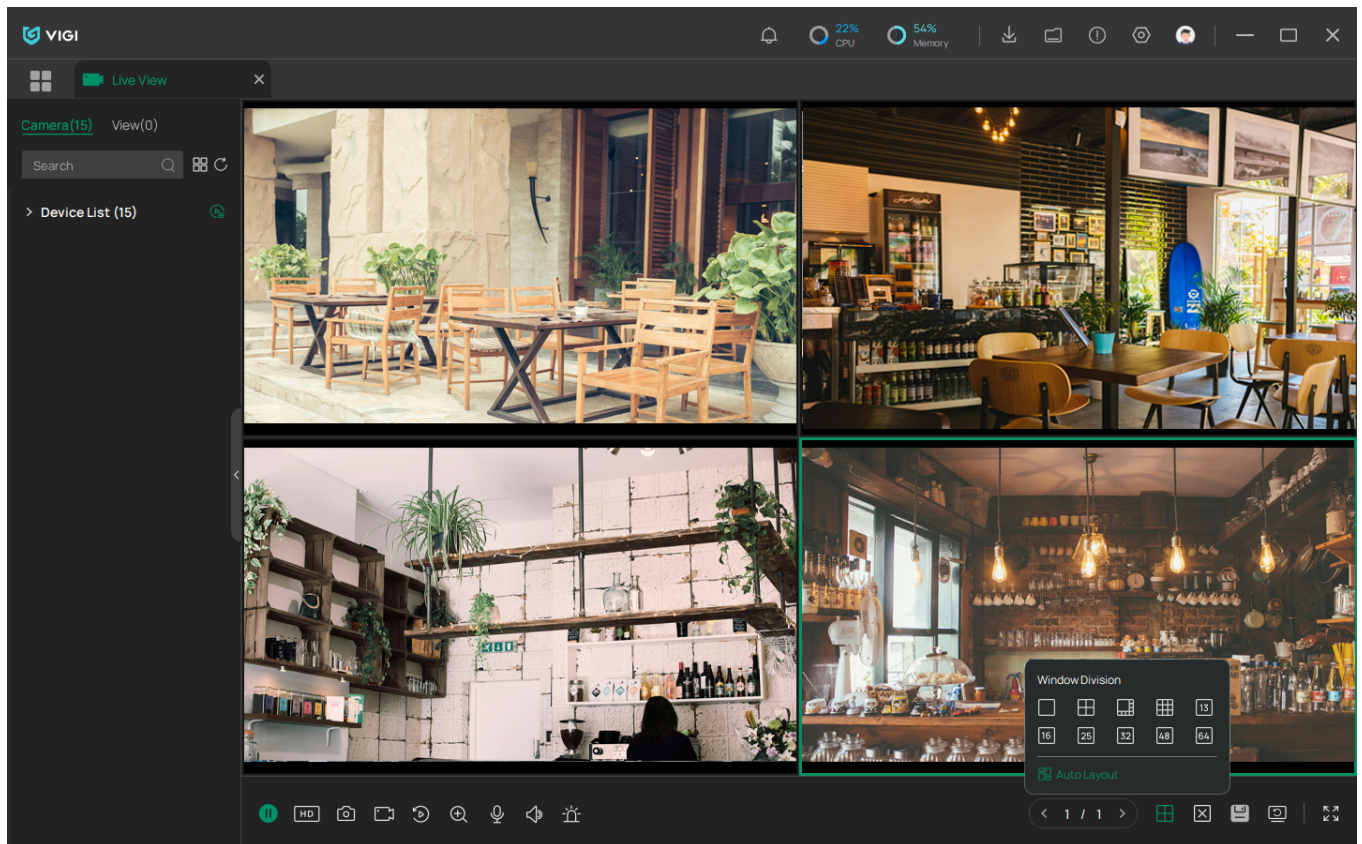
2. Click the  icon and choose your desired layout.

3. Double click the devices you want to monitor, then you will see the images of the devices on the screens.



♥ 4.2 Configure Live View Settings via Toolbar

In Live View, select a device screen and configure its Live View settings via the toolbar.



Click to play/pause the live view.



Click to change the image resolution, HD or SD.



Click to take a screenshot.



Click to start recording.



Click to view the instant playback (5-min Playback).



Click to zoom in/out the live image.



(Microphone needed and only for certain cameras) Click the icon and then Start Talk to talk. With this function, you can talk to people in the monitor area in real time.



(Only for certain cameras) Click and use the slide bar to adjust the volume.



(Only for certain cameras) Click to manually start the alarm.



(Only for the camera with Pan&Tilt) Click to enter the Preview of Pan&Tilt. You can adjust the camera location and call the presets.



Click the corresponding buttons to change the number of displayed screens



Click to clear all screens.



(Only for Enterprise Edition) Click to save a custom layout of device feeds for easy access later.



Click to resume the live view.



Click to enter full screen.

5

Playback

This function allows you to play the history recordings and edit them, such as exporting clips. You can easily search the recordings based on the device, date, and event. This chapter contains the following sections:

- [Instant Playback](#)
- [Play Normal Recordings](#)
- [Playback Recordings of Events](#)
- [Playback Operations](#)

PC Client supports the following two playback modes:

- **Instant Playback**

Play the video of a single channel recorded in the last five minutes.


- **Normal Playback**

Play the recordings of one day, including the continuous and motion detection recordings.

- **Event Playback**

Play the recordings with events detected.

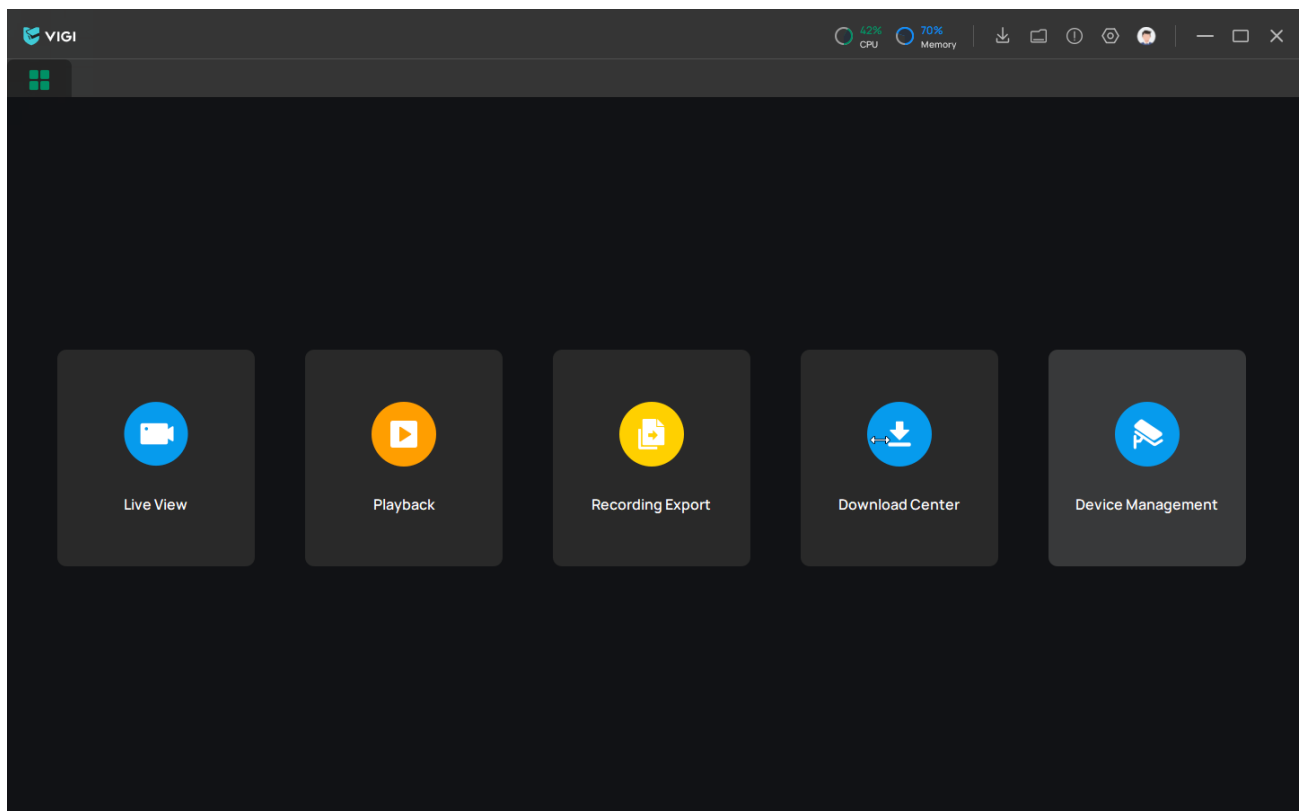
♥ 5.1 Instant Playback


You can replay the video recorded in the last five minutes via Instant Playback. Click a device on Live View, click  in the toolbar to start instant playback.

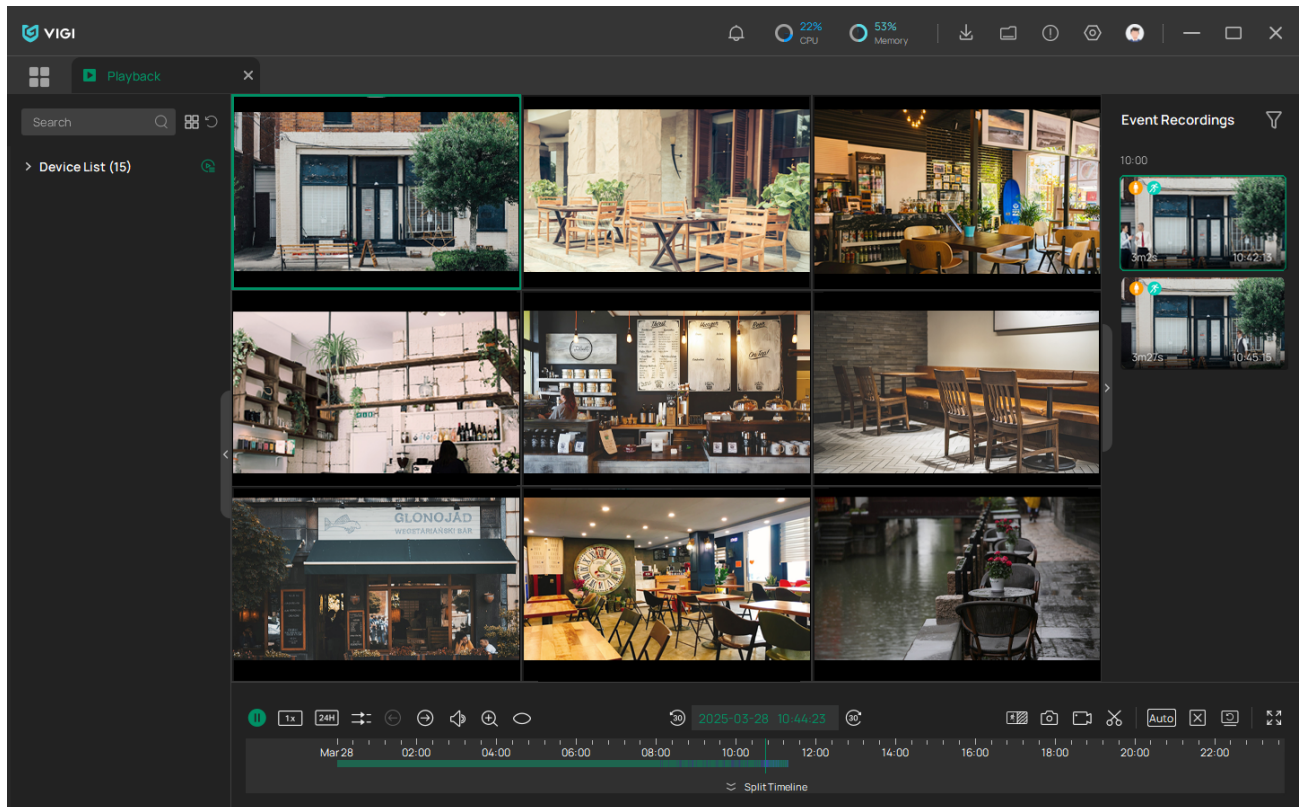
♥ 5.2 Play Normal Recordings


Normal Recordings are video files from the continuous and motion detection recordings. Follow the steps below to play normal recordings.

1. Click on **Playback** to open the Playback module.



2. Select a device and select a date in the calendar. You can also click the  on the right and click **Confirm** to filter the event recordings.



3. Double click a recording in the list or click  to play the recordings.

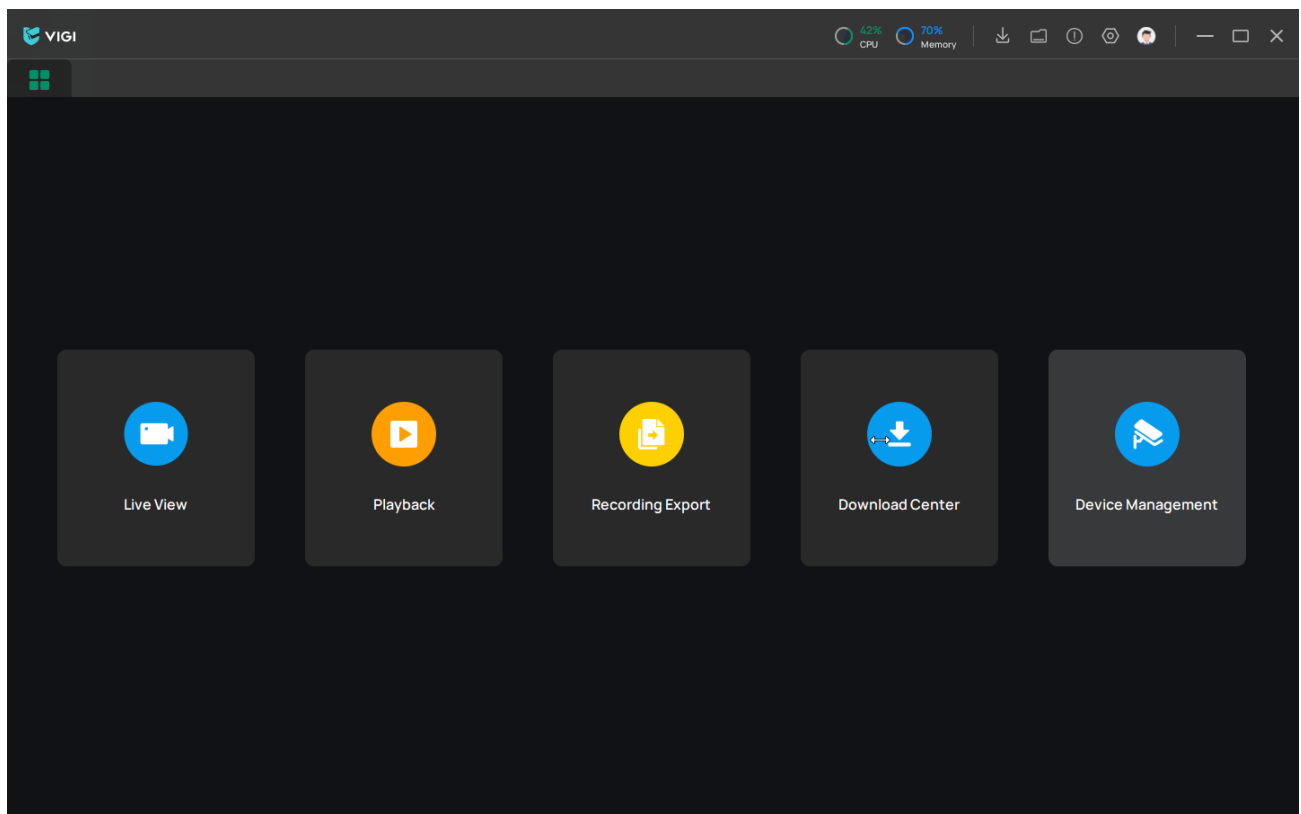
For more playback operations, refer to [5. 4 Playback Operations](#).

♥ 5.3 Playback Recordings of Events

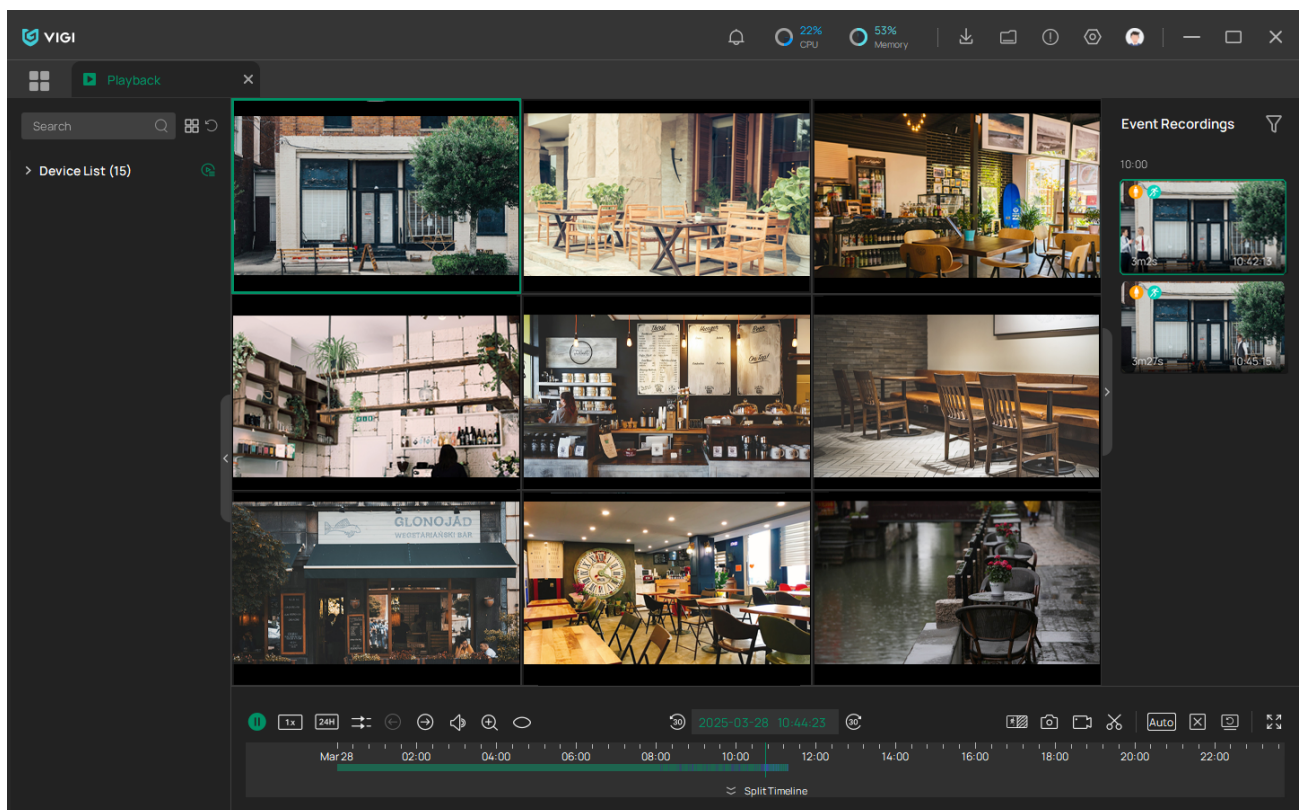
With Events configured, the NVR and cameras can detect and react to events. In Event Recordings, you can search, play, and edit the videos recorded when certain events are detected, including motion, line crossing and area intrusion.

Note: If you have never configured Events on the device, there are no recordings of events.

1. Click on **Playback** to open the Playback module.



2. Click the  on the right and click **Confirm** to filter the event recordings.



3. Double click a recording in the list to play the event recordings.
- For more playback operations, refer to [5.4 Playback Operations](#).















♥ 5.4 Playback Operations

In the Playback module, you can use the icons and buttons in the toolbar and on the right panel to adjust the display, edit and back up the recordings.

Note: The operations are not available in Instant Playback.

5.4.1 Basic Playback Operations

The following icons are supported when playing recordings:

	Click to select from the list to change the playing speed.
	Click to set the time span length.
	Click to switch between synchronous playback and asynchronous playback.
	Click to play the previous/next event recording.
	Click and slide to adjust the volume.
	Click to zoom in or out via Digital Zoom.
	(For certain models) Click to change the fisheye mode.
	Jump forward/backward by 30 seconds.
	Click to select a date.
	Click to select the recording type.
	Click to take a screenshot.
	Click to start recording.
	Click to export or edit the recording. The Export feature is available only for devices that are on the same LAN as the PC Client.
	Click to select the screen layout.




Click to clear all screens.

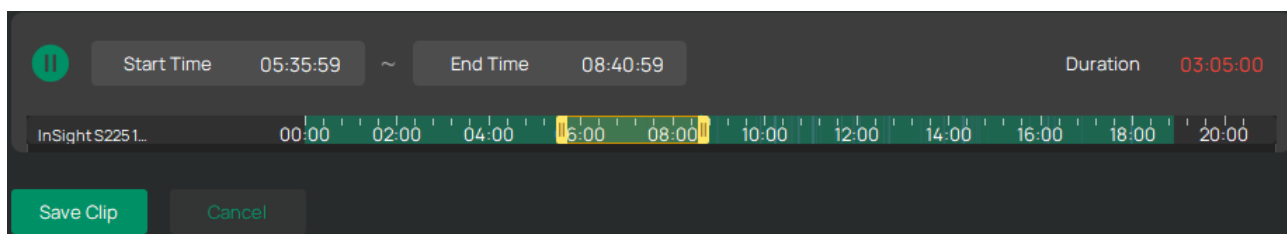


Click to load the recording again.

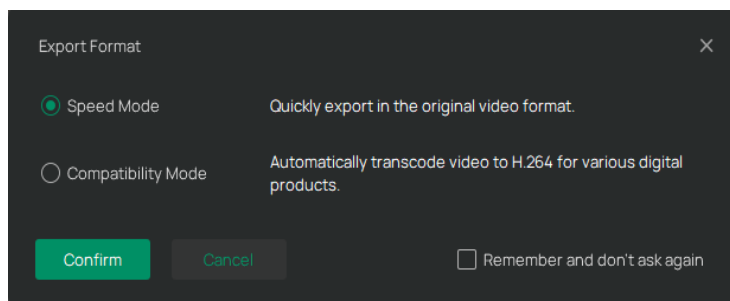
5.4.2 Edit Recordings

Follow the steps below to clip video files.

1. In Playback, select a device and select a date to load the recording. Click , and click **Edit** to edit the recording.
2. Click the recordings in the time bar to select a start time and end time or drag the slide to select the time.




3. Click **Save Clip**. A window will pop up, select the export mode, and the clip will be exported. You can check the export progress in the **Download Center**.



5.4.3 Export Recordings

In Playback, you can easily search the desired recordings based on devices, time, and events, and back up them in batches. This feature is available only for devices that are on the same LAN as the PC Client.

Note: To back up the recordings, an external storage is required.

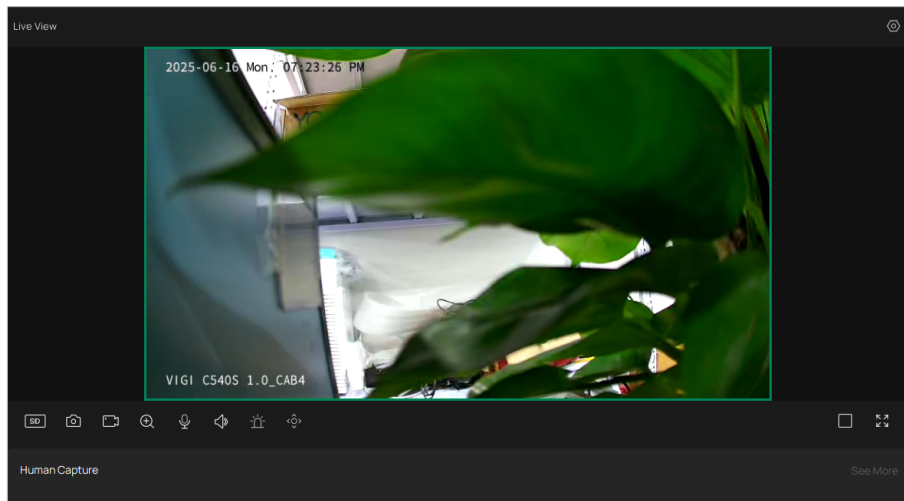
1. In Playback, select a device and select a date to load the recording. Click , and click **Export** to export the recordings.
2. Specify the path to export the recordings. Click **Start Backup** and wait until backup is completed.



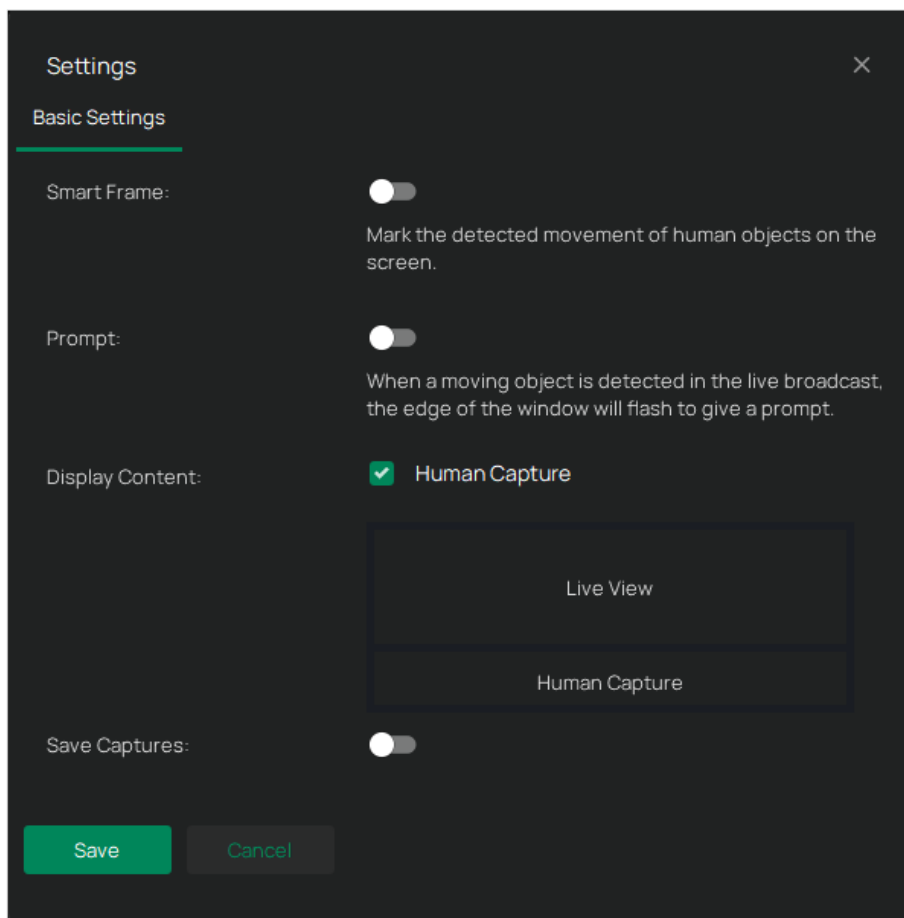
AI Monitoring (for Enterprise Edition)

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. Log in to the **Enterprise Edition** and click on **AI Monitoring** to load the following page.



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 the Settings icon on the top right corner to configure the basic settings.



- 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.

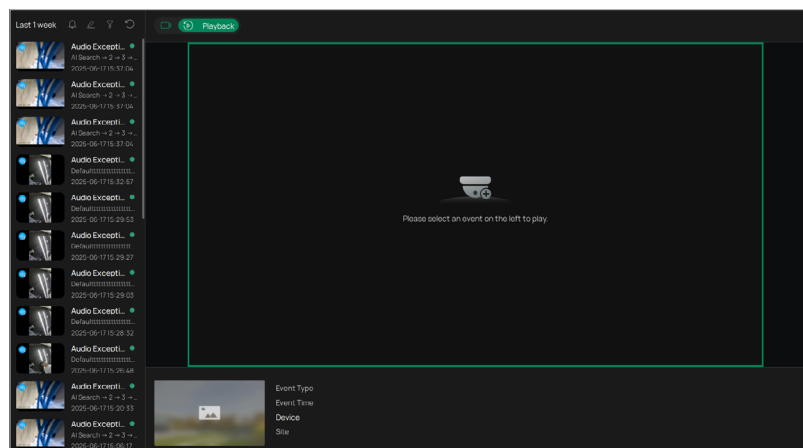
- 2) Enable **Prompt** to make the edges of the live window flash when a moving object (such as a person) is detected.
- 3) In **Display Content**, make sure Human Capture is selected to ensure that detected humans are displayed below the live feed.
- 4) Enable **Save Captures** if you want to save human capture frames automatically for later use.




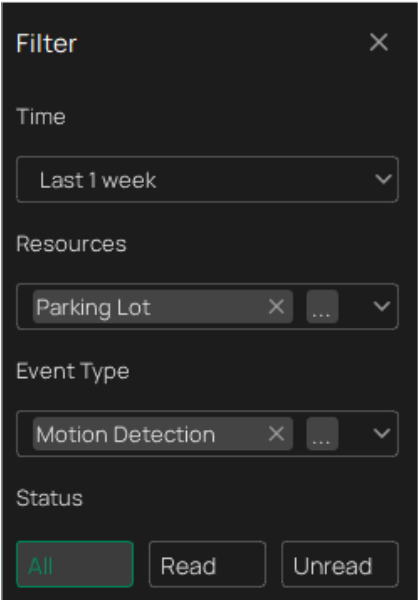
Event Center (for Enterprise Edition)

The Event Center module 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. Log in to the **Enterprise Edition** and click on **Event Center** to load the following page.



2. Select an event on the left to play. To filter events, click the  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.

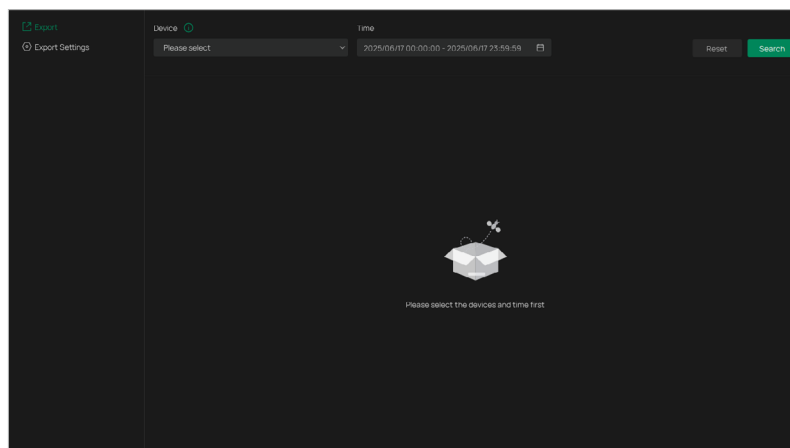
5. View event details. In the lower section of the screen, details about each event are displayed, including event type, time, device, and site.



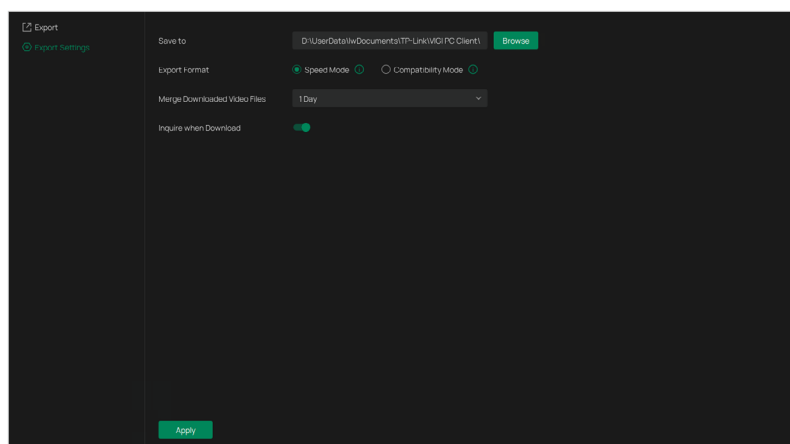
Recording Export

In the module, you can export the recordings to your local storage. This feature is available only for devices that are on the same LAN as the PC Client.

1. Log in to the **PC Client** and click on **Recording Export** to load the following page.



2. Go to **Export Settings** to configure the export mode and click **Apply** to save the settings.



Save to	Click Browse to select the folder where the recordings will be exported.
Export Format	Speed Mode: The recordings will be quickly exported in the original format. Compatible Mode: Recordings will be automatically converted to H.264 for use in a variety of digital products.
Merge Downloaded Video Files	Select a duration, and the recordings within this time period will be merged and exported as a video file. If you select Not Merge, the recordings will not be merged.
Inquire When Download	When this feature is enabled, you will be prompted to configure the export settings each time you download a recording.

3. Select a device that is on the same LAN as the PC Client, select the date, and then click **Search**. The relevant recordings will be listed. Click to export the recordings.



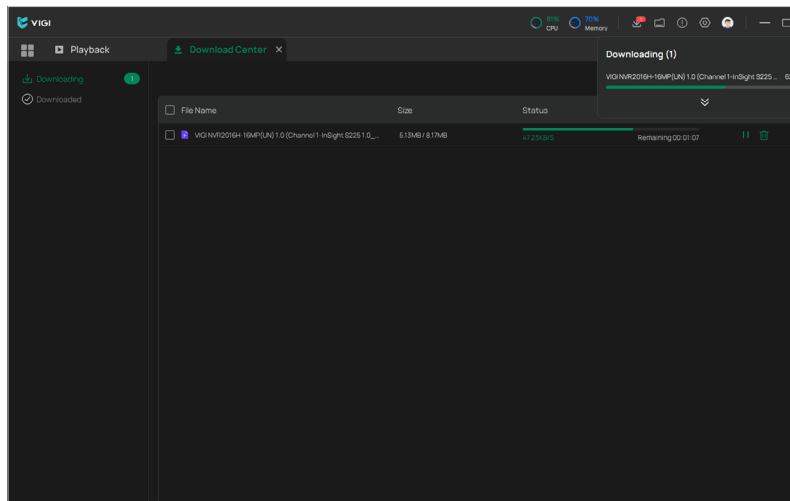
Download Center

The Download Center module 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.

Log in to the **PC Client** and click on **Download Center** to load the following page. Click the tabs to view the downloading tasks and downloaded list

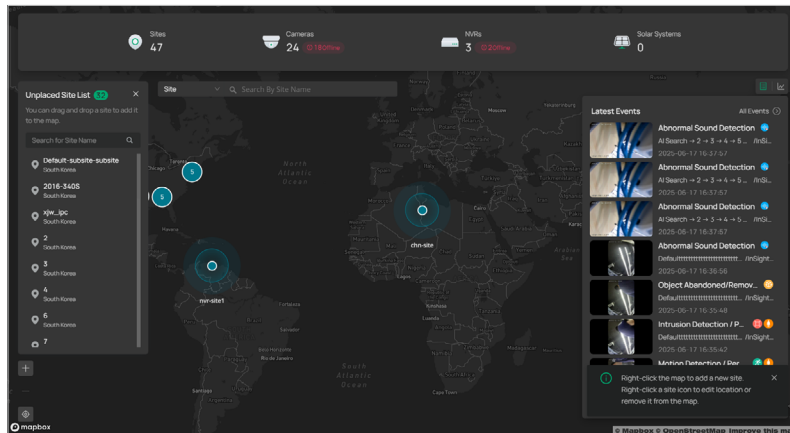




Site Map (for Enterprise Edition)

In **Enterprise Edition**, click on **Site Map**, and you will be redirected to VMS.

1. Log in to the **Enterprise Edition** and click on **Site Map**, and you will be redirected to VMS to load the following page.



2. You can view the site and device location in the map.



Device Management

In the Device Management module, you can add devices, change the cameras and NVR settings.

- [Device Management](#)
- [Change Camera Settings](#)
- [Change NVR Settings](#)

11.1 Device Management

Log in to the **PC Client** and click on **Device Management** to manage your devices using the PC Client software. The features for Personal Edition and Enterprise Edition are a little different.

Personal Edition







Device Name	Status	Model	IP Address	MAC Address	Firmware	Action
InSight S225 1.0_AE99	Online	InSight S225	Remote Device	8C-00-00-00-00-00	1.0.2 Build 250121 Rel 43208n	[Live View] [Settings] [Delete]
VIGI CS40S 1.0_1957	Online	VIGI CS40S	Remote Device	8C-00-00-00-00-00	2.0.4 Build 240913 Rel 56881n	[Live View] [Settings] [Delete]
18M VIGI NVR2016H-16M...	Online	VIGI NVR2016H-16M...	Remote Device	8C-00-00-00-00-00	1.3.0 Build 250401 Rel 53950n	[Live View] [Settings] [Delete]
VIGI C400P-2.8 1.0	Offline	VIGI C400P-2.8	Remote Device	8C-00-00-00-00-00	1.0.5 Build 210702 Rel 64208n	[Live View] [Settings] [Delete]

	Click to display the live view page of the device.
	Click to enter the camera's management page to change the camera's settings as needed.
	Click to delete the device from the PC Client if you no longer want to manage the.
	Click to update the device online if a firmware update is detected.


Enterprise Edition

Device Name	Status	Model	Site	Action
Channel 11-InSight S485 ...	Online	InSight S485	freeeeeeeeeeeeeeeee	[Live View] [Settings] [Delete]
Channel 10-InSight S655I ...	Offline	InSight S655I	freeeeeeeeeeeeeeeee	[Live View] [Settings] [Delete]
Channel 9-VIGI C445ZI 1.0...	Not Certified	--	freeeeeeeeeeeeeeeee	[Live View] [Settings] [Delete]
Channel 8-DS-2CD2043G...	Offline	--	freeeeeeeeeeeeeeeee	[Live View] [Settings] [Delete]
Channel 7-VIGI C540-W 2.0	Online	VIGI C540-W (UN)	freeeeeeeeeeeeeeeee	[Live View] [Settings] [Delete]
Channel 2-InSight S345ZI ...	Not Certified	InSight S345ZI	freeeeeeeeeeeeeeeee	[Live View] [Settings] [Delete]
Channel 1-VIGI C430I 计划...	Online	VIGI C430I	freeeeeeeeeeeeeeeee	[Live View] [Settings] [Delete]
nvr2016	Online	VIGI NVR2016H-16MP(...)	freeeeeeeeeeeeeeeee	[Live View] [Settings] [Delete]
InSight S385 1.0_9178	Online	InSight S385	freeeeeeeeeeeeeeeee	[Live View] [Settings] [Delete]

	Click the button and follow the web instructions to migrate a device from VIGI Personal Edition to VIGI Enterprise Edition.
	Click to display the live view page of the device.

	Click to enter the camera's management page to change the camera's settings as needed.
	Click to move the device to another site.
	Click to enter the device password to verify the device.
	Click to delete the device from the PC Client if you don't want to manage the device any longer.
	Click to update the device online if a firmware update is detected.
	Click to export the detailed device information.

♥ 11.2 Change Camera Settings

To change the device settings, find your device in the list, and click . The parameters to modify include **Information**, **Camera**, **Event** and **System**. If your camera has connected to the NVR, you can also enter the NVR's settings page to change the camera settings.

11.2.1 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. In the panel that appears on the right, head over to **Information > Device Info**.
2. You may edit its name in the **Device Name** field and click **Apply**.

11.2.2 System Log

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

1. In the panel that appears on the right, head over to **Information > System Log**.
2. Specify search conditions, including the Time and Log Type, and click **Search**. The filtered logs that match the search conditions will appear in the table.

Time	Specify a time range to filter the logs based on the recording time.
------	--

Log Type	<p>Select a type from the drop-down list to filter the logs.</p> <p>All: All types of logs.</p> <p>Alarm: Alarms triggered by events, such as tampering, line crossing, and area intrusion.</p> <p>Exception: Abnormal events that may influence the camera's functions, such as video signal loss and hard drive errors.</p> <p>Operation: Actions that take place on the camera, such as login and upgrade.</p> <p>Information: Informational messages, such as device information.</p>
Clear Logs	Click to delete all logs.

11.2.3 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. In the panel that appears on the right, head over to **Camera > Display > Image**.
2. Configure the following parameters.

Rotation	<p>Choose to turn the live view image by 0, 90 or 270 degrees on your display.</p> <p>When you select Off, the image displays normally.</p>
Mirror	<p>Select the mirror mode as needed.</p> <p>When you select Off, the image displays normally.</p> <p>By choosing Left-Right, you mirror the image on the vertical axis.</p> <p>By choosing Up-Down, you flip the image on the horizontal axis.</p> <p>By choosing Center, you rotate the image by 180 degrees around its center.</p>
Day/Night Switch	<p>Select a method to switch the image settings of day and night.</p> <p>Unified: The camera applies the same image settings throughout a day.</p> <p>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.</p> <p>Auto: The camera switches the image mode of day and night automatically according to the light condition of the environment.</p>

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	<p>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.</p> <p>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.</p> <p>Scheduled: Specify the time to turn on and off the white light.</p> <p>Always On/Off: The white light is on/off all the time.</p>
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	<p>Select the standard mode or enhanced mode or manually adjust the brightness of image.</p> <p>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.</p> <p>Enhanced Mode: This mode intensifies its protection against overexposure, by darkening the bright areas of the image.</p> <p>Manual: Manually adjust the brightness of image. The higher the value is, the dimmer the image gets.</p>
WDR	<p>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.</p> <p>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.</p>

BLC Area	<p>BLC (Backlight Compensation) optimizes the camera to increase light exposure for darkened areas and helps you to see details more clearly.</p> <p>Select an area to compensate light.</p> <p>If you select Custom, draw a blue rectangle on the live view image as the BLC area.</p>
HLC	<p>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.</p>
White Balance	<p>White balance is a process of removing unrealistic color casts, so that objects which appear white in person are rendered white in the image.</p> <p>Auto: The camera adjusts the color temperature automatically.</p> <p>Locked: The camera keeps the current color settings all the time.</p> <p>Daylight/Natural Light/Incandescent/Warm Light: The camera adjusts the color temperature to remove the color casts caused by the corresponding light.</p> <p>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.</p>

11.2.4 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. In the panel that appears on the right, head over to **Camera > Display > OSD**.
2. 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.

11.2.5 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. In the panel that appears on the right, head over to **Camera > Display > Privacy Mask**.
2. 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.
3. To remove a specific privacy area, select it and click **Delete**.
4. To remove all privacy areas, click **Clear**.
5. Click **Apply**.

11.2.6 Video

Follow the steps below to configure video settings.

1. In the panel that appears on the right, head over to **Camera > Stream > Video**.
2. Configure the following parameters, and click **Apply**.

Stream Type	<p>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.</p> <p>Sub-stream is a secondary video feed that is used mainly for remote viewing from computers from outside the network.</p>
Resolution	The screen displays images more clearly when the resolution increases.

Video Frame Rate	The video is more fluent when the rate increases.
Video Encoding	Select the encoding type of the stream. H.265 reduces the file size and saves the bandwidth better than H.264.
Bite Rate Type	VBR: The bit rate changes with the image within Maximum Bit Rate. CBR: The bit rate is Maximum Bit Rate all the time.
Image Quality	When VBR is selected as the Bit Rate Type, set the video quality as high, medium, or low.
Max Bit Rate	Specify the upper limit of bit rate.
Copy to Other Devices	Use this option to apply these settings to other devices in your system.

11.2.7 Audio

Follow the steps below to configure audio settings.

1. In the panel that appears on the right, head over to **Camera > Stream > Audio**.
2. Configure the following parameters, and click **Apply**.

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.

11.2.8 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. In the panel on the right, go to **Camera > Stream > ROI**.
2. Select the stream type and enable ROI. Draw an area on the preview screen (the blue square in the picture below). Drag to adjust its size and location. Specify the ROI level and click **Apply**.

11.2.9 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. In the panel on the right, go to **Camera > Stream > Advanced Settings**.
2. Enable SRTP if needed. When enabled, RTSP video data will be encrypted and you may be unable to play the video using third-party clients or NVRs. It is recommended that you use the device together with a VIGI NVR.
3. Click **Apply**.

11.2.10 PTZ (Only for Models with Motorized Lens)

VIGI PC Client 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. 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.

11.2.11 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. In the panel on the right, go to **Event** and locate Arming Schedule and Processing Mode in the related event interface.

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

Note:

- Each cell represents one hour.
 - The default setting is 24/7.
 - Up to six time periods can be configured for a day.
3. 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.
 4. Set processing modes as needed.

11.2.12 Message

In the panel on the right, go to **Event > Message** and configure the following parameters.

Alarm Message	You will be notified when an alarm event is detected.
Offline Message	You will be notified when the device goes offline.

11.2.13 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. In the panel on the right, go to **Event > Basic Event > Motion Detection**.
2. Draw quadrilaterals for motion detection on the preview screen. The whole screen is selected by default. You may drag the corners to change the shape of the area and 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.

3. 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.

4. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
5. Click **Apply**.

11.2.14 Camera Tampering

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

1. In the panel on the right, go to **Event > Basic Event > Camera Tampering**.
2. Enable **Camera Tampering**.
3. Set the sensitivity of video tampering. A higher value can trigger the alarm actions more easily.
4. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
5. Click **Apply**.

11.2.15 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. In the panel on the right, go to **Event > Basic Event > Scene Change**.
2. Click the toggle to turn on **Scene Change**.
3. Specify **Sensitivity**. The higher the value is, the more easily the change of the scene can be detected.
4. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
5. Click **Apply**.

11.2.16 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. In the panel on the right, go to **Event > Smart Event > Line Crossing Detection**. Click the toggle to turn it on.
2. Draw lines on the preview screen. Select the line and configure its settings.

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

Sensitivity	The higher the value is, the easier it is to detect a target that crosses the line.
Direction	<p>Choose the direction from which the target crosses the line.</p> <p>A->B: Only the target crossing the configured line from the A side to the B side can be detected.</p> <p>B->A: Only the target crossing the configured line from the B side to the A side can be detected.</p> <p>A<->B: The target going across the line from both sides can be detected and alarms are triggered.</p>
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.
----------------------------	---

3. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
4. Click **Apply**.

11.2.17 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. In the panel on the right, go to **Event > Smart Event > Intrusion Detection**. Click the toggle to turn it on.
2. Draw intrusion areas on the preview screen. Select the area and configure the settings.

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

Sensitivity	The higher the value is, the more easily an intrusion action can be detected.
Percentage	Set the percentage of intrusion detection. When an object takes up the specific percentage of the area, the alarm actions will be triggered.
Intrusion Time	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.

3. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
4. Click **Apply**.

11.2.18 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. In the panel on the right, go to **Event > Smart Event > Region Entering Detection**. Click the toggle to turn it on.
2. Draw shapes for area entrance detection on the preview screen.

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

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

3. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
4. Click **Apply**.

11.2.19 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. In the panel on the right, go to **Event > Smart Event > Region Exiting Detection**. Click the toggle to turn it on.
2. Draw shapes for area exiting detection on the preview screen.

Note: You may draw up to four areas 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.

3. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.

4. Click **Apply**.

11.2.20 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. In the panel on the right, go to **Event > Smart Event > Loitering Detection**. Click the toggle to turn it on.
2. Draw shapes for area exiting detection on the preview screen.

Note: You may draw up to four areas 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.
----------------------------	---

3. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
4. Click **Apply**.

11.2.21 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. In the panel on the right, go to **Event > Smart Event > Object Abandoned/Removal Detection**. Click the toggle to turn it on.
2. Draw shapes for area exiting detection on the preview screen.

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

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

3. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
4. Click **Apply**.

11.2.22 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. In the panel on the right, go to **Event > Smart Event > Abnormal Sound Detection**. Click the toggle to turn it on.
2. Adjust the value of sensitivity and alert threshold. The higher the sensitivity and the lower the threshold, the easier it gets to trigger linkage methods.

3. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
4. Click **Apply**.

11.2.23 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. In the panel on the right, go to **Event > Smart Event > Vehicle Detection**. Click the toggle to turn it on.
2. Draw shapes for area exiting detection on the preview screen.
Note: You may draw up to four areas.
3. Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.
4. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
5. Click **Apply**.

11.2.24 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. In the panel on the right, go to **Event > Smart Event > Human Detection**. Click the toggle to turn it on.
2. Adjust the value of sensitivity. A higher value can trigger alarm actions more easily.
3. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
4. Click **Apply**.

11.2.25 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. In the panel on the right, go to **Event > Smart Event > Smart Frame**. Click the **IPC Smart Frame** or **NVR Smart Frame** tab.
2. Click the toggles to specify the type of detection: motion, human, or vehicle. You may enable more than one types. Click **Apply**.

11.2.26 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. In the panel on the right, go to **Event > Exception Event > Access Exception**. Click the toggle to turn it on.
2. Enable **Login Error Detection** to limit the login attempts:
3. Set the maximum login attempts. The number should be between 3 and 10
4. Click **Apply**.

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

11.2.27 Sound Alarm

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

1. 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**.
2. Under Audio Output Settings, click the toggle to mute or drag the slide bar to set the system volume.
3. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
4. Click **Apply**.

11.2.28 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, HTTPS, or ISUP data transmission.

1. In the panel on the right, go to **Event > Alarm Server**.
2. Click **Add**.
3. Enter Host IP/Domain, URL, and Port, and select Protocol. Enable Attach Image if needed.
Note: HTTP and HTTPS are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.
4. Click **Save**.

11.2.29 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.

1. In the panel on the right, go to **Event > Alarm Device > Alarm Input**.
2. Select an Alarm Input Number.
3. Check Enable This Alarm Input.

4. Edit the Alarm Name.
5. Select the Alarm Type from the 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.
6. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
7. Click **Apply**.

11.2.30 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.

1. In the panel on the right, go to **Event > Alarm Device > Alarm Output**.
2. Select the Alarm Output Number according to the alarm interface connected to the external alarm.
3. Enable the Alarm Output Device.
4. Edit the Alarm Name.
5. Select the Alarm Duration from the drop-down list.
6. Refer to [Arming Schedule and Processing Mode](#) for settings if needed.
7. Click **Apply**.

11.2.31 VCA

You can go to the VCA module to configure Smart Analysis or Object Attribute Analysis. Please note that you can only enable one analysis at a time. Follow the steps below to finish the configuration.

1. In the panel on the right, go to **Event > VCA > Smart Analysis Configuration**.
2. Enable **Smart Event mode** or **Object Attribute Analysis**.
3. If you enable **Object Attribute Analysis**, you can set to enable **People Attribute Analysis** and **Vehicle Attribute Analysis**.

11.2.32 Update Firmware

TP-Link aims to provide 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 our official website www.vigi.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 NVR from our official website.
2. In the panel on the right, go to **System > Upgrade Firmware**.
3. Select the downloaded firmware file, and click **Upgrade**.
4. Wait a few minutes for the upgrade and reboot to complete.


11.2.33 Reboot Device

You can go to the System module to manually reboot the device or schedule to reboot the device regularly. Follow the steps below to finish the configuration.


1. In the panel on the right, go to **System > Reboot Device**.
2. Click the **Reboot** button to manually reboot the device. Or toggle on the **Reboot Schedule**, set the reboot time, and the device will reboot at the specific time regularly.

11.2.34 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.

1. In the panel on the right, go to **System > Recording Schedule**.
2. Toggle on the **Recording Schedule**, click **Continuous** and **Event** to configure the time for recording. You can click  icon to copy the settings to other days.

♥ 11.3 Change NVR Settings

To change the device settings, find your device in the list, and click . The parameters to modify include **Information**, **Camera**, **Storage**, **Event**, **Network** and **System**. Refer to **Change Camera Settings** for detailed instructions for camera settings.

11.3.1 Device Information

You can view basic information about the NVR, including device name, status, device type, channel, model, hardware and firmware version, device ID, device time, internet information, and storage information.

1. In the panel that appears on the right, head over to **Information > Device Info**.
2. You may edit its name in the **Device Name** field and click **Apply**.

11.3.2 System Log

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

1. In the panel that appears on the right, head over to **Information > System Log**.

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


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

11.3.3 System Information

The System Information section contains the Channel Information, Stream Information, Hard Drive Information, Internet Information and Event Information. You can check the corresponding detailed information by clicking each tab in the **Information > System Information**.

11.3.4 Recording Control

In this section, you can configure the recording settings for each channel

- In the panel on the right, go to **Storage > Recording Control**.
- Click the  button to configure the settings.

Recording Switch	Whether to enable recording for this channel.
Record Audio	Whether to record audio and video simultaneously.
Store Stream	<p>Select the stream type for the recording.</p> <p>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.</p> <p>Sub-stream usually offers comparatively low resolution options, which consumes less bandwidth</p>

Storage Disk Group	Select the disk group in which the recording will be stored.
--------------------	--

11.3.5 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. In the panel on the right, go to **Storage > Recording Schedule**.
2. 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.


3. 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.
4. Click **Apply**.

11.3.6 Hard Drive 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. In the panel on the right, go to **Storage > Hard Drive Management**.
2. 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.

3. Click the  button to edit the hard drive attributes. Configure it to Read only or Read and Write. Select the disk group which it will be in.
4. Enable **Circular Write of Disk** to overwrite the video records when the storage space is full. Otherwise the camera cannot record new videos
5. Click **Apply**.

11.3.7 Internet Connection

In Connect, you can view the connection status and configure the NVR to obtain a dynamic or static IP address.

Follow the steps below to configure the network settings.

1. In the panel on the right, go to **Network > Connect**.

Status	Displays the current Internet status.
Assign Subnet	Click to manually assign each connected camera a fixed IP.
IPv4 Mode	Configure the NVR to obtain a dynamic or static IP address.
IPv4 Address	Specify an IP address for the NVR. The IP address should be in the same segment as the gateway; otherwise, the NVR 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.

2. Click **Apply**.

11.3.8 Network Isolation

You can enable Network Isolation to isolate the NVR network from other devices, then other devices in the LAN cannot communicate with the NVR and its connected devices.

1. In the panel on the right, go to **Network > Network Isolation**.

2. Toggle on to enable **Network Isolation** and configure the following parameters as needed.

Internal IP	Specify the NVR's IP in a different subnet from other devices.
Start IP	Specify the start IP from which the NVR will use starting to assign to its connected devices.
Internal IPv6	Specify the NVR's IPv6 address if IPv6 mode is configured.
POE Access to Internet	When enabled, devices connected to the PoE ports can keep isolated from other devices and access the internet.

3. Click **Apply**.

11.3.9 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. In the panel on the right, go to **Network > Port**.
2. Specify HTTPS port and service port.

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

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


3. Click **Save**.

11.3.10 UPnP

UPnP is used to establish the mapping between the internal port and external port.

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

Follow the steps below to configure UPnP.

1. In the panel on the right, go to **Network > UPnP**.
2. Enable UPnP 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 NVR to be converted.
External Port	Displays the external port opened by the gateway.
Internal IP	Displays the IP address of the NVR that needs to be converted.
Status	Displays the status of mapping.

4. Click **Apply**.

11.3.11 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. In the panel on the right, go to **Network > Email**.
2. 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.
3. Enable SSL/TLS if needed and emails will be sent after encrypted.
4. 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.
5. If your email server requires authentication, check Authentication and input your username and password to log in to the server.
6. Click **Edit** to input the recipient's information, including the recipient's name and address.
7. Click **Test** to see if the function is well configured.
8. Click **Apply**.

11.3.12 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. In the panel on the right, go to **Network > IP Restriction**.
2. Enable IP Restriction and specify the restriction rule. If you select **Deny List**, the devices with the IP addresses specified in the table will not be able to access the camera. If you select **Allow List**, only the devices with the IP addresses specified in the table can access the camera.
3. Click **Add** to add the desired IP address, give a description to identify this IP address, then click **Save**.
4. Click **Save**.

11.3.13 DDNS

When you connect the router to a network, it will be assigned with a dynamic IP address and you can use this IP address to access the NVR. However, the IP address can change from time to time and you don't know when it changes. In this case, you might apply the DDNS (Dynamic Domain Name Server) feature on the NVR to allow you to access your NVR using a domain name without checking and remembering the IP address.

Follow the steps below to configure DDNS.

1. In the panel on the right, go to **Network > DDNS**.
2. Enable DDNS and specify the service provider, NO-IP, DynDNS or TP-Link DDNS. Enter the server address, domain name, username, password and domain name of your account.
3. Click **Apply**.

11.3.14 SNMP

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

1. In the panel on the right, go to **Network > SNMP**.
2. Enable SNMP v2c.
3. Enter the SNMP community name. Note that the access is Read only, meaning that the network management system can only view but not modify parameters of the specified view.
4. Configure the following parameters.

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

5. Click **Apply**.

11.3.15 Openapi

You can allow the NVR for Openapi connection. In the panel on the right, go to **Network > Openapi** to enable it, and click **Apply**.

11.3.16 Change Basic Settings

1. In the panel on the right, go to **System > Basic Settings > Basic Settings**.
2. View and change the name of your camera. Do not change the powerline frequency unless necessary.
3. Specify the Menu Timeout. You will be forced out of the menu after the period.
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.

11.3.17 Modify Device Time

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

1. In the panel on the right, go to **System > Basic Settings > Date**.
2. Select your time zone.
3. Configure your time settings.

Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs on User Datagram Protocol (UDP), which in turn runs on IP, or you can manually set the system time. If you do not want to expose your camera to the network, you can choose Manual.

Server address	Enter the IP address of the NTP server.
Interval	<p>Time interval between the two synchronizing actions with NTP server.</p> <p>Note: The interval can be set from 1 to 10080 minutes, and the default value is 60 minutes.</p>

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

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

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

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

Note:

1. In some time zones, DST is not observed.
 2. If the camera is connected to an NVR, you only need to configure NTP and DST settings on the NVR, which will be synchronized with the camera.
5. Click **Apply**.

11.3.18 Interface Output

In Interface Output, you can select the display resolution for your monitor and choose to display the channel number on the Live View screen and the images in the original scale. To configure these settings, right click on the Live View screen, go to **System > Basic Settings > Interface Output**.

Main Screen Display Preference	<p>Set the output interface for Main Screen when the device is connected to two monitors, HDMI or VGA.</p> <p>If Both is selected, both HDMI and VGA will be used as the output interface for Main Screen.</p>
--------------------------------	--

Resolution	Select the screen resolution according to your needs. With Adaptive selected, the NVR automatically selects the highest resolution supported by the screen.
Display Channel Number	Display the channel number on the Live View Screen.
Display Original Scale Screen	Display the images on the Live View screen in the original scale.

11.3.19 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. In the panel on the right, go to **System > User Management > Change Password**.
2. Enter the current password, type the new password, and confirm it.
3. Click **Apply** to save the changes.

11.3.20 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 NVR. Also, the latest firmware will be released at the our official website **www.vigi.com**, and you can download it for free.

Note:

1. Back up 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 NVR from our official website.
2. In the panel on the right, go to **System > Upgrade Firmware**.
3. Select the downloaded firmware file, and click **Upgrade**.
4. Wait a few minutes for the upgrade and reboot to complete.

11.3.21 Import and Export Configuration File

Follow the steps below to import and export the configuration file of your NVR.

Note: Before your operation, prepare an external storage device and plug it into the USB slot on the front panel of your NVR.

1. In the panel on the right, go to **System > System Management > System Management**.
2. For configuration file import, click **Browse** to select the file and click **Import**.

3. For configuration file export, click **Export** to export the current configuration.

11.3.22 Reboot Device

You can go to the System module to manually reboot the device or schedule to reboot the device regularly. Follow the steps below to finish the configuration.

1. In the panel on the right, go to **System > Reboot Device**.
2. Click the **Reboot** button to manually reboot the device. Or toggle on the **Scheduled Reboot**, set the reboot time, and the device will reboot at the specific time regularly.