VZ-AIPVM-N & VZ-AIPVM-P SERIES

10",23",27",32" & 43" AI PUBLIC VIEW MONITOR

WEB BASED AIPVM-N & AIPVM-P USER MANUAL

ViewZ®

www.viewzusa.com

This device complies with NDAA (National Defense Authorization Act).

Please read this manual thoroughly before use, and keep it handy for future reference.

07232025-Rev. B

CONTENTS

CONTENTS

CONTENTS

WARNING STATEMENTS

Important Safety Instructions

This manual describes how to use AI PVM's web management system, including network access, network configuration and troubleshooting.

This manual is intended for:

- Technical support engineers
- Maintenance engineers
- IP camera operators

To access this web management page, user does not need to install additional software.

Important Safety Instructions

DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. **NOTICE** is used to address practices not related to personal injury.
NOTE	Calls attention to important information, best practices and tips. **NOTE** is used to address information not related to personal injury, equipment damage, and environment deterioration.

QUICK REFERENCE GUIDE

1. Login and Logout

CAUTION

We recommend to use **Google Chrome, Mozilla Firefox or Microsoft Edge** latest version to access the ViewZ web management system. **To run the full function of ViewZ web management system,** you should **run the browser as administrator**.

Login

Step 1 Open the web browser. Enter the IP address of the PVM IP camera (default value: 192.168.0.120) in the address box and then press Enter. When user initially access this web management system, user needs to make user's own password (super administrator) as shown in Figure 1-1.

Figure 1-1 Create Password Page

Figure 1-2 General Login Page

Factory Default IP address : 192.168.0.120
Factory Default Subnet Mask : 255.255.255.0
Factory Default Gateway : 192.168.0.1
Factory Default DNS 1 : 192.168.0.1
Factory Default DNS 2 : 192.168.0.2

Caution: IP address and gateway address should be set with the same IP parameters. For example, if IP address is "A.B.C.0 ~ 255", then gateway address should be set as "A.B.C.0 ~ 255" (however, IP and gateway address cannot be the same.)

Step 2 After user created a password, the system will automatically load in the general login page. From this point, user can access the general login page.

Step 3 Enter the user name and created password as shown in Figure 1-2.

Note

- The default user name is **admin** (super administrator), but there is no default **admin** password.
- If user losts the **admin** password, user cannot access this web management system anymore. In this case, user should do hardware reset to get back the control - please refer the **VZ-AIPVM-UserManual** file. So, we recommend customers to create an Administrator account after 1st login - please refer page 27 or Setting / System / User.
- User can change the system display language from the login page - please refer page 24 or Setting / System / Settings / System.

QUICK REFERENCE GUIDE

1. Login and Logout

Step 4 After login, the main page (Live View) will be displayed as shown in Figure 1-3.

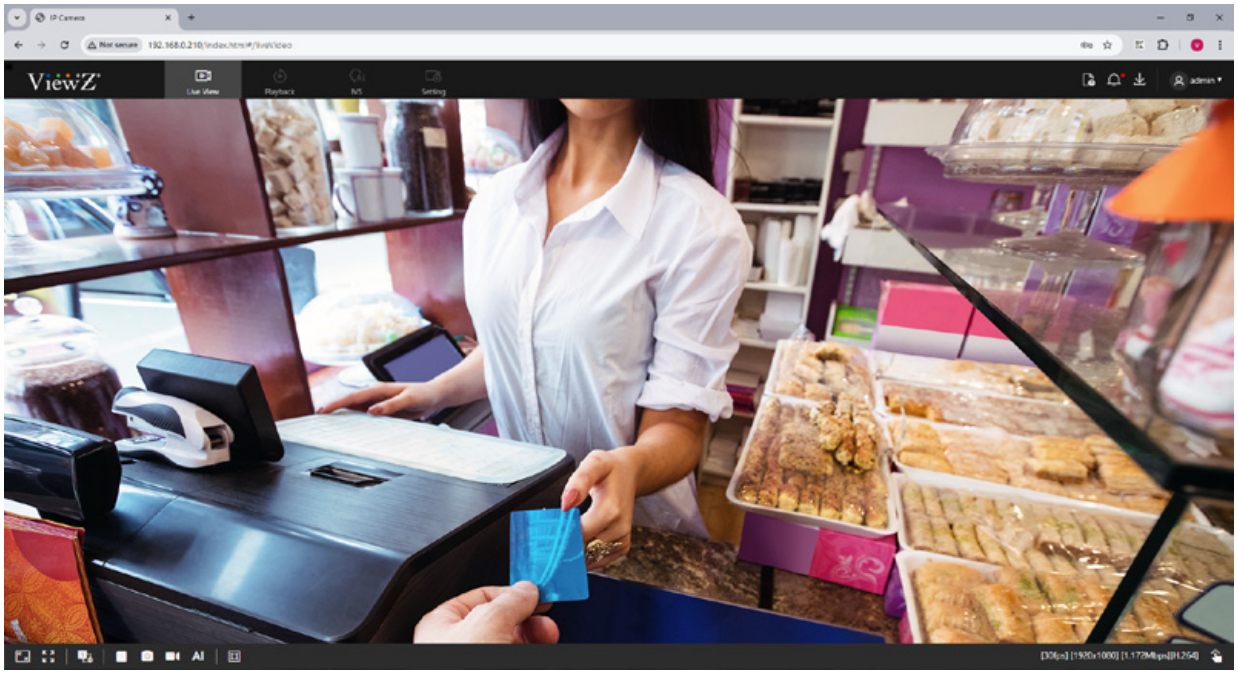
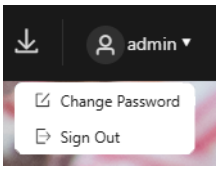


Figure 1-3 Main Page (Live View)

Logout

To log out of the system, click the 'Sing Out' in the upper right corner of the main page. The login page is displayed after you log out of the system.



QUICK REFERENCE GUIDE

2. Main Page Layout - Live View

On the main page, user can see real-time video, receive alarm and fault notifications, set parameters, change the password, and log out of the system. Figure 1-3 shows the main page layout. Table 1-1 describes the features on the main page.

Figure 1-3 Main Page Layout

Table 1-1 Interface Parameters

No.	ELEMENT	DESCRIPTION
1	LIVE VIEW	Real-time video stream is displayed in this area. User can also set sensor parameters.
2	PLAYBACK	User can select options to play recorded video by using Micro SD card (MAX 256GB).
3	INTELLIGENT VIDEO SYSTEM (IVS)	User can setup options to set multi-target, intrusion, smart motion, single & double line crossing, multi-loitering, single bad, gun detect, wrong-way, parameter & people count
4	SETTING	User can setup device configuration, including network, image, PTZ, event, storage, audio/video streams, user, log, maintenance, security and onvif.
5	NOTE	User can see the description of intercom function
6	ALARM	When the device generates an alarm, the alarm icon is displayed. User can click to view the alarm information. NOTE : When the device accepts an alarm signal, the alarm icon will display within 10s in the web management system.
7	DOWNLOAD	User can download backup data and other files.
8	ADMIN	User can change the password & sign out.

QUICK REFERENCE GUIDE

2. Main Page Layout - Live View

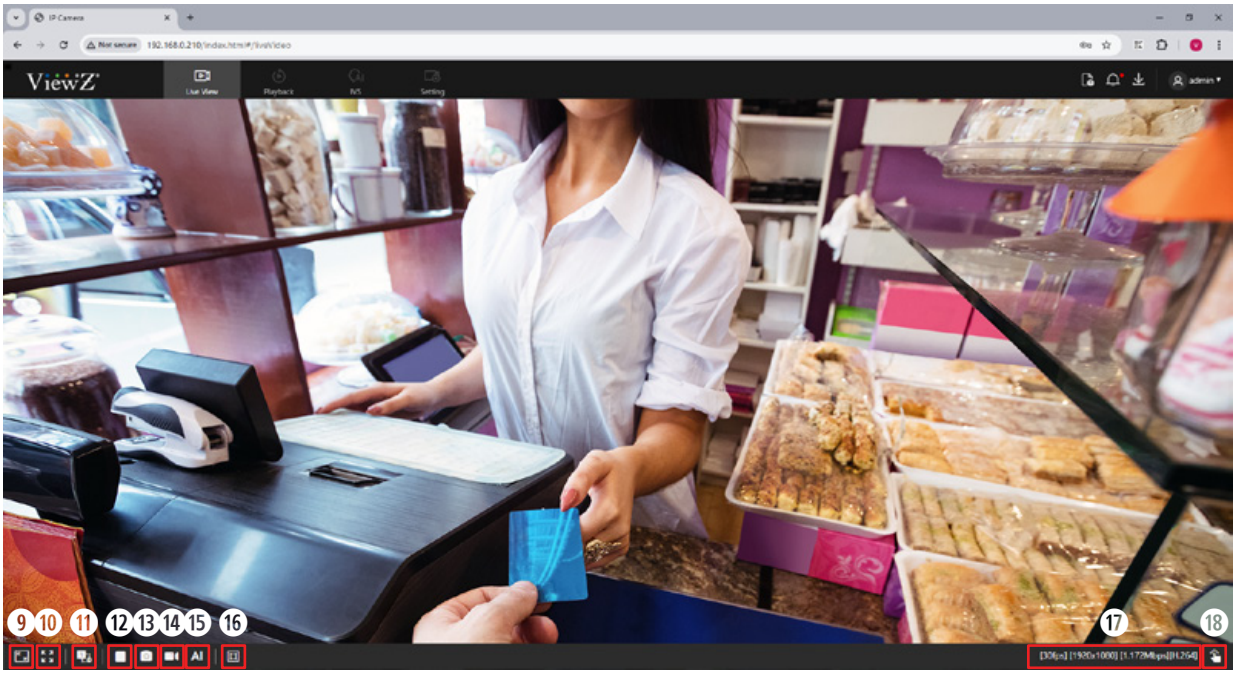


Figure 1-3 Main Page Layout

Table 1-1 Interface Parameters

No.	ELEMENT	DESCRIPTION
9	STRETCH	Click the icon to stretch the display
10	FULL SCREEN	Click the icon to make full screen. To exit the full screen, click 'ESC' key
11	STREAM SWITCH	Click the icon to switch the video stream
12	PLAY & STOP	Click the icon to stop the live video & to play the live video.
13	SNAPSHOT	Click the icon to take & save a screen shot into the local computer.
14	LOCAL RECORD	Click the icon to record & save the live video into the local computer.
15	AI SNAPSHOT	Click the icon AI to take and record AI screen shots
16	SMART PICTURE FRAME	Click the icon to setup the target frame & intelligent marking
17	LIVE VIEW INFO	Display the current live stream info - frame rate, resolution, bit rate & video encode type
18	I/O	Click the icon to zoom in the live view

QUICK REFERENCE GUIDE

3. Main Page Layout - Live View / AI

On the main page, user can easily take & record the real time screen shot images & videos.

Figure 1-4 Main Page AI Layout

Step 1 Click the icon AI in the bottom left corner of the main page.
When user click '**AI**' button, the **AI** window is displayed on right area, as shown in Figure 1-4.

Step 2 User can choose which screen shots will be taken & recorded, such as GUN, Face & Body/Motion. Click 'Detail' text to see the info of screen shot - recorded time & screen shot type.

Step 3 Click the icon on the upper right corner of the AI main page.
When user click this button, user can see the full screen mode and setup the option to save the screen shot into the inserted SD card.

Note
When user click **'AI'** button, user can only see the simplified **AI** view windows. The screenshots will be keep stacking on the right window area. If user wants to see the separated screen shots, categorized by types, click 'Expand' button to see full **AI** mode.

QUICK REFERENCE GUIDE

3. Main Page Layout - Live View / AI

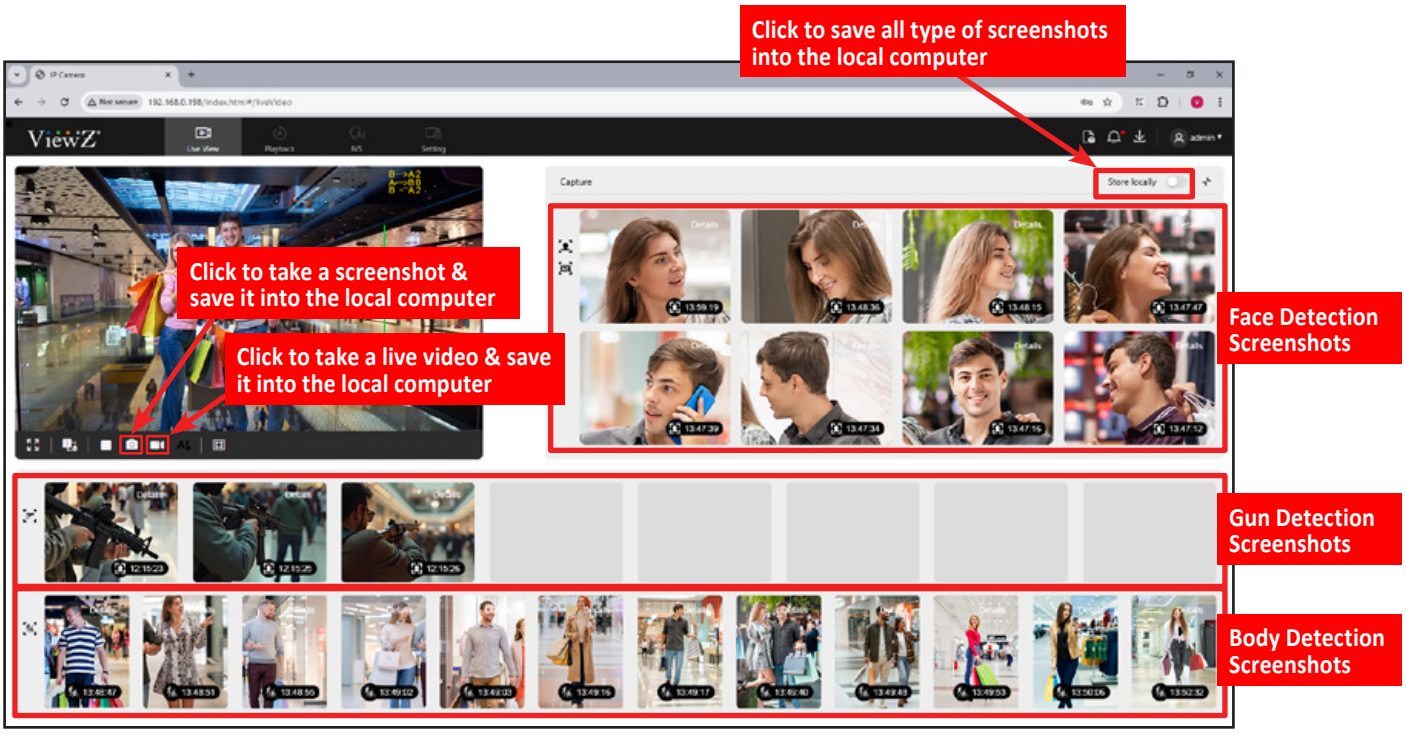


Figure 1-4 Main Page AI Layout

Table 1-2 AI Main Page Parameters

Parameter	DESCRIPTION	Setting
Store Locally	Enable/disable saving screen shots into the local computer. NOTE If camera will take lots of screen shots, the system would be slowing down.	Default Value: OFF
Face, Gun & Body	Capture the human face, gun & body screen shots NOTE Gun - camera only takes a gun screen shot Body - camera takes a body (motion) screen shot	N/A

QUICK REFERENCE GUIDE

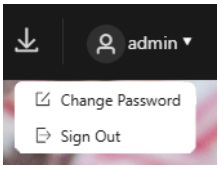
4. Change the Password

Description

User can change the password for logging in to the system.

Procedure

Step 1 Click the icon admin ▾ in the upper right corner of the main page.
When user click '**Change Password**' button, the **Change Password** window is displayed, as shown in Figure 1-5 and Figure 1-6.



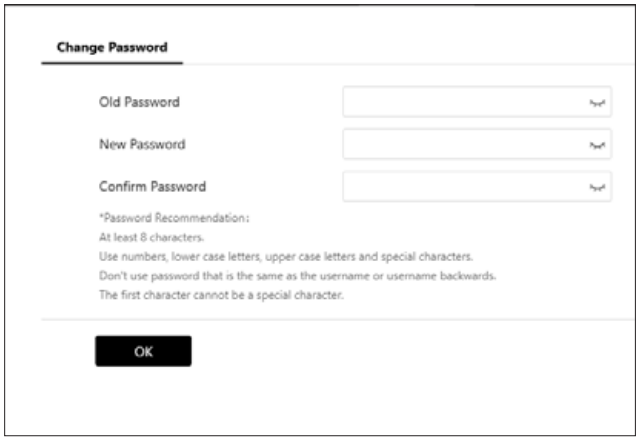


Figure 1-5 Password Dialog Box

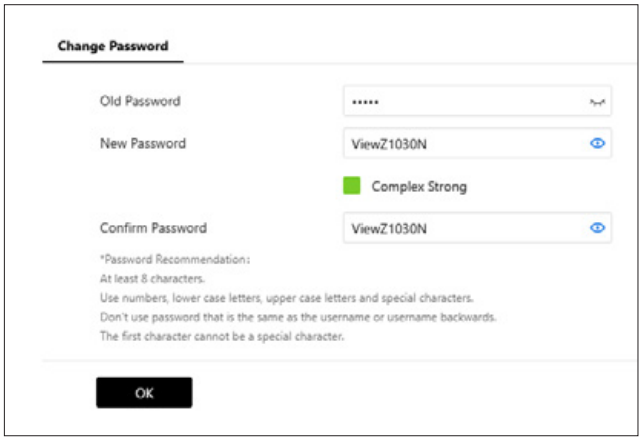


Figure 1-6 Password Change

Step 2 Enter the old password, new password, and confirm the new password.

Step 3 Click OK
If the message "Change own password success" is displayed, the password has been successfully changed. If the password change fails, the cause will be displayed. (For example, the new password length couldn't be less than eight.)

Step 4 Enter the old password, new password, and confirm the new password.

Note

- User can find the **Change Password** feature on **Setting > System > Change Password**.
- Refer to page 26

QUICK REFERENCE GUIDE

5. Browser Error

Note

- If user uses the Internet Explorer or Internet Explorer mode on Microsoft Edge and try to access our web management system, user will see the error message like below picture. ViewZ web management system only support Chrome, Firefox and Edge.

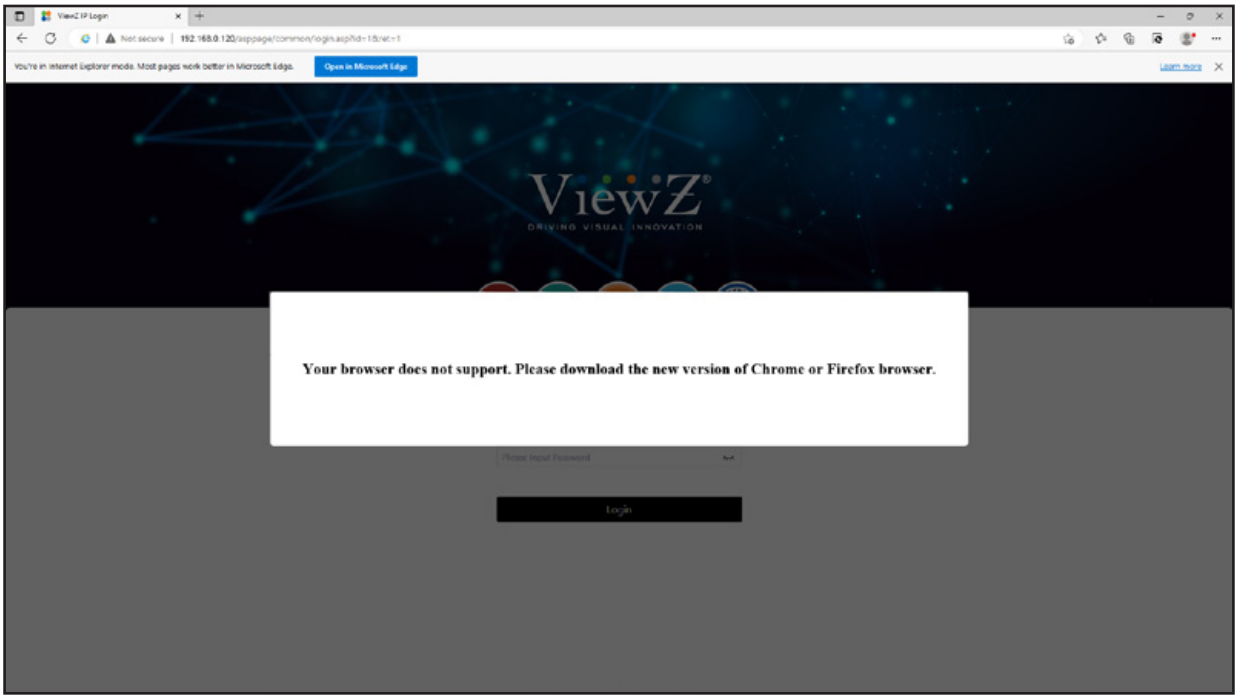


Figure 1-7 Error Message on Internet Explorer

SEARCHING IP CAMERA

1. Searching Real Time IP Camera

Note
User can browse real-time video in the web management system.

Preparation

- To ensure that real-time video can be played properly, you must perform the following operations when you log in to the web management system for the first time:
- On the computer, open **Control Panel > Internet Options(Properties) > Security > Trusted sites > Sites**.
- On the displayed dialog box, type "**http://192.168.0.120**" or **desired IP address** and then click Add, as shown in Figure 2-1.

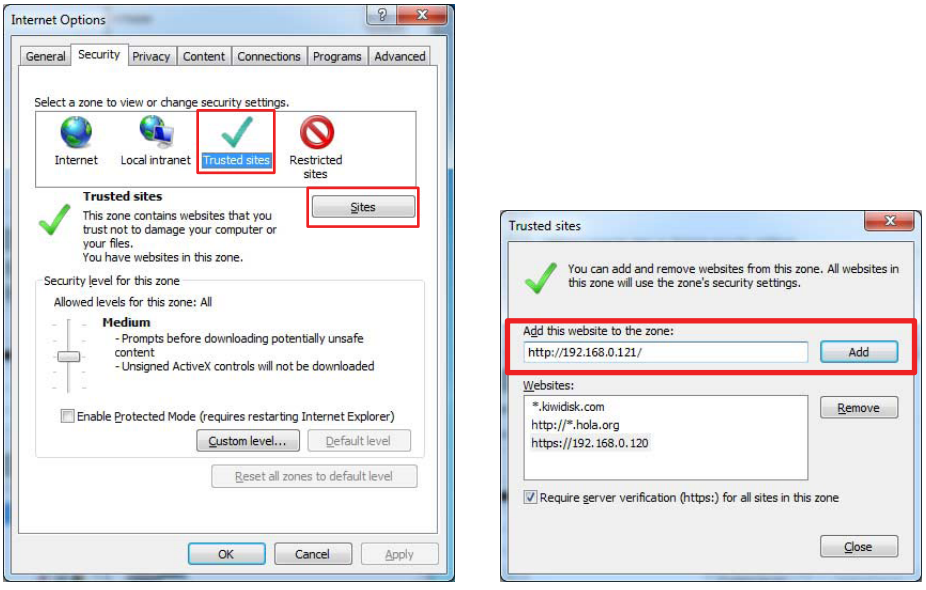


Figure 2-1 Add a trusted site

Note

- If user's network security limit the network access, user might not see the live video. In this case, user need to do this step.
- If user can see the live video without this step, user does not need to do this step.

PLAYBACK

1. Review the Recorded Video

Description

Click **Playback** on the top menu, to review recorded video.
This function requires the SD card, NAS server and FTP server. On this feature, user can see recorded videos, take a snapshot and save/download videos or images.

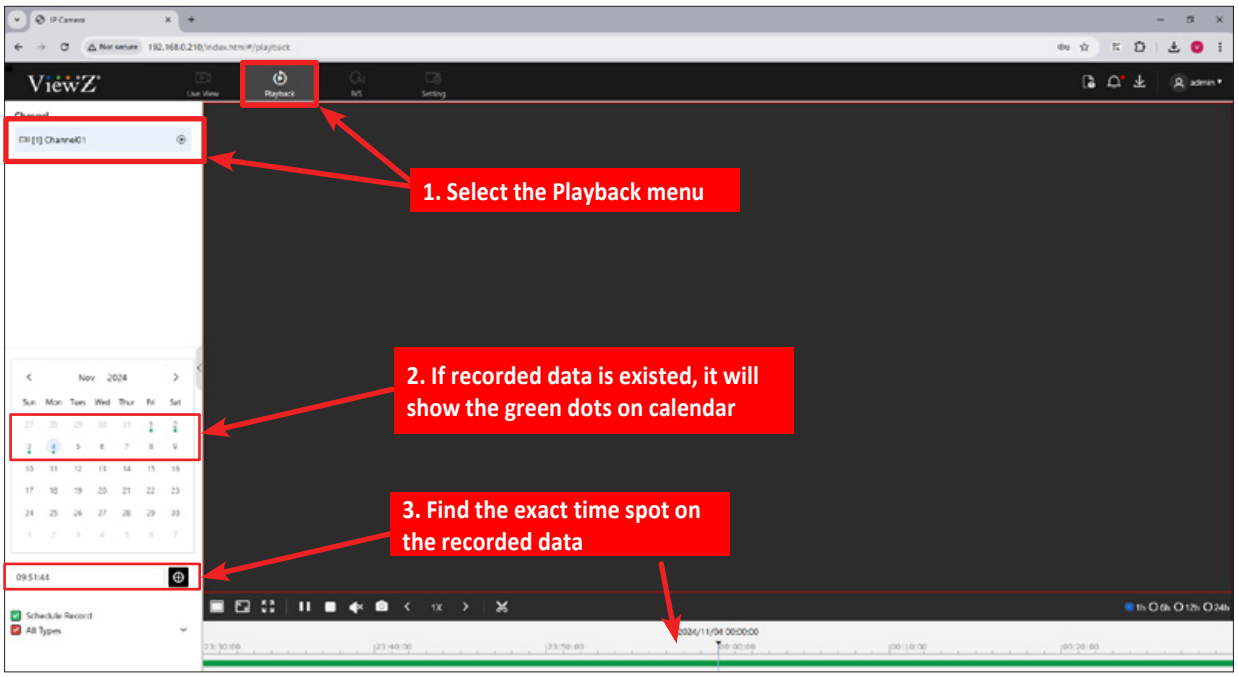


Figure 3-2 Playback Page

On the **Playback** page, user can perform the following operations:

- Click this date icon to load the recorded data
- Click 09:51:44 to find the recorded video of exact time.
  Type the exact time and click this icon to find the recorded video of exact time.
- Drag the time

Note

- When the SD card, NAS Server or FTP server is connected to the AI PVM, this PLAYBACK feature is available.

PLAYBACK

1. Review the Recorded Video

Description

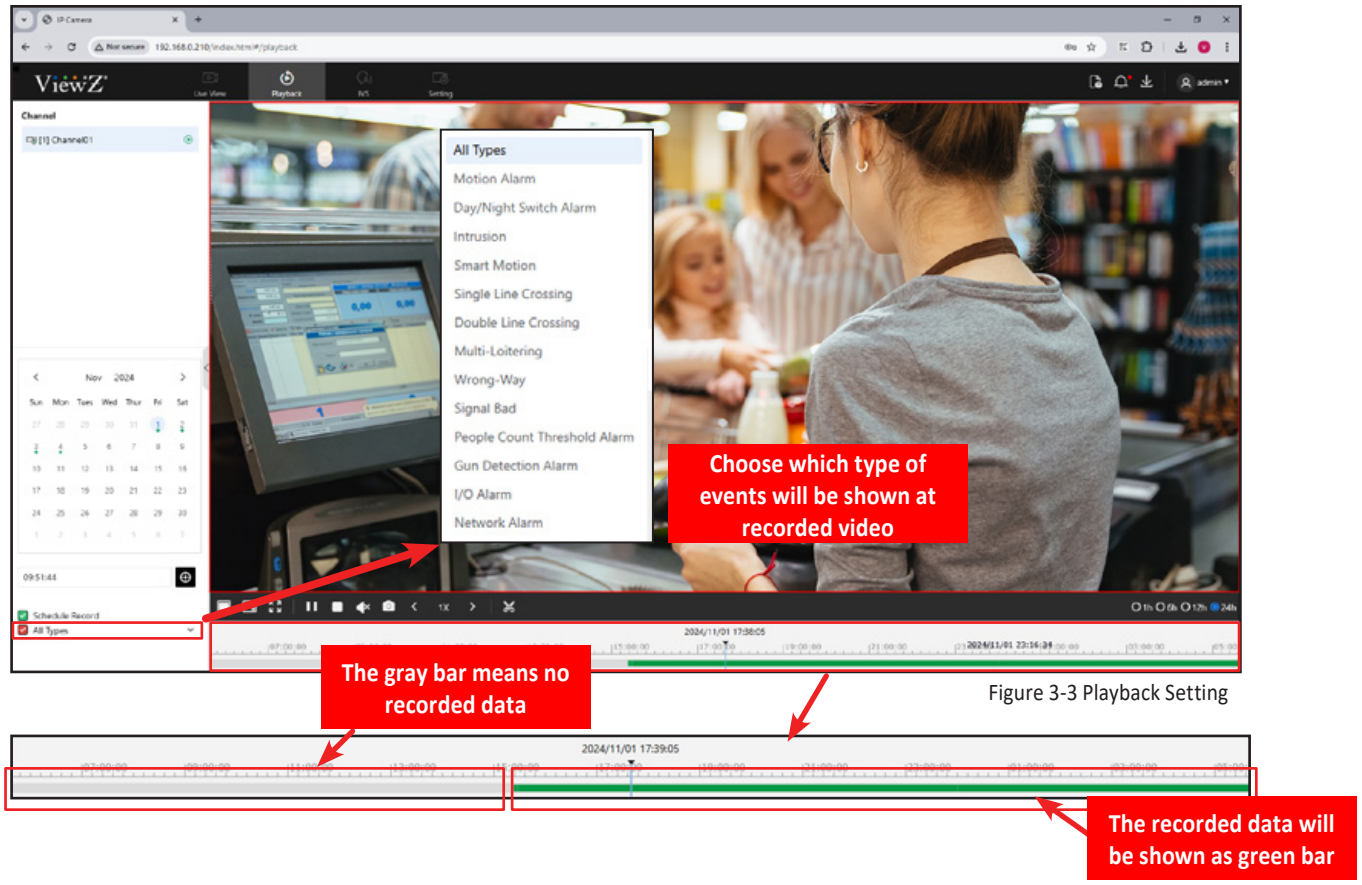


Figure 3-3 Playback Setting

On the **Playback** page, you can perform the following operations:

- Click Schedule Record to enable recording video.
- Click All Types to select which type of events will be shown at time table. User can select it among; All Types, Motion Alarm, Day/Night Switch Alarm, Intrusion, Smart Motion, Single Line Crossing, Double LIne Crossing, Multi-Loitering, Wrong-Way, Single Bad, People Count Threshold Alarm, I/O Alarm and Network Alarm

PLAYBACK

1. Review the Recorded Video

Description

User can also setup the location of backup, schedule and recording stream type. When setup is done, click START to make a backup file.

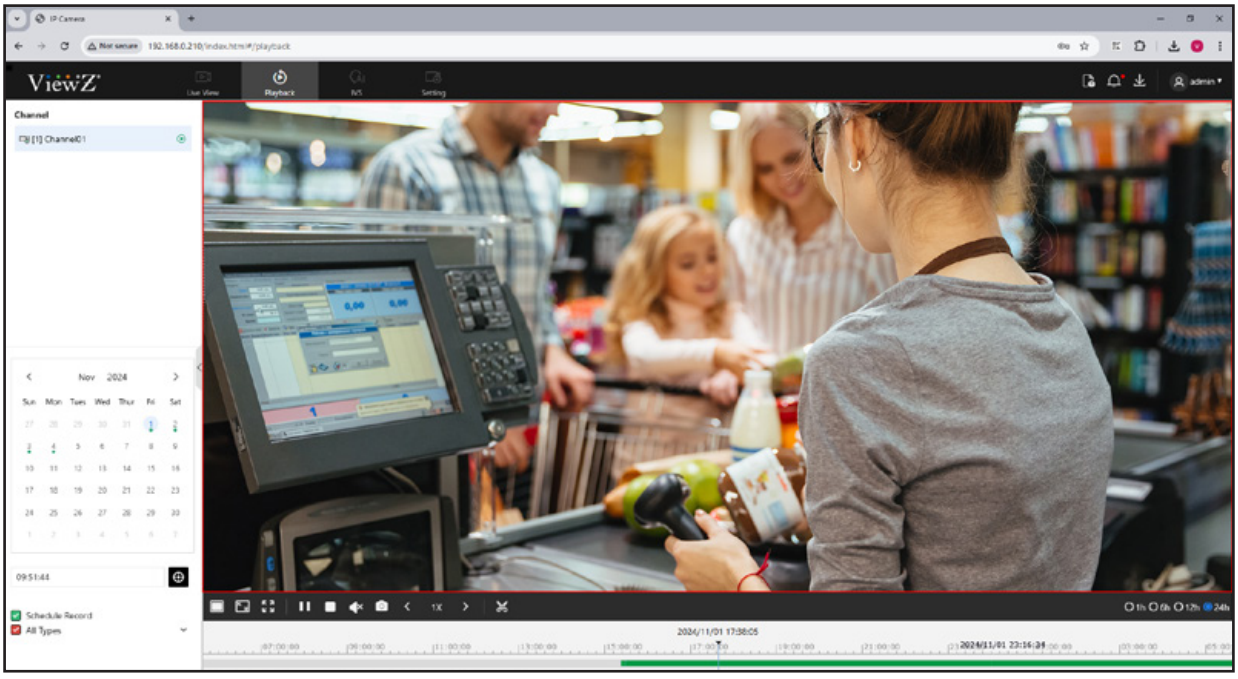


Figure 3-4 Playback Setting

On the **Playback** page, you can perform the following operations:

- Click to see single view of the recorded video.
- Click to see the recorded video as window scale.
- Click to see the recorded video as full screen.
- Click to play the recorded video.
- Click to pause the playing video.
- Click to stop the playing video.
- Click to turn on/off the sound of playing video.
- Click 1X to set the speed of playing video (1/16, 1/8, 1/4, 1/2, 1, 2, 4, 8 times)
- Click to take a snapshot of playing video. The saved snapshot will be saved on the selected location on backup setting. See Figure 2-6.
- Click to make a backup and the time period.
- Click 1h 6h 12h 24h to set the time interval on time table.

SETTING / QUICK START

1. Setting - Quick Start

Description

User can quickly access the main feature via Quick Start.

- **Local Network** - Refer to page 39 or **Setting>Network>Settings>Local Network** about the detailed feature
- **Video** - Refer to page 63 or **Setting>Video/Audio>Video** about the detailed feature
- **Display** - Refer to page 70 or **Setting>Image>Display** about the detailed feature
- **OSD** - Refer to page 85 or **Setting>Image>OSD** about the detailed feature
- **Date & Time** - Refer to page 20 or **Setting>System>Settings>Date&Time** or about the detailed feature

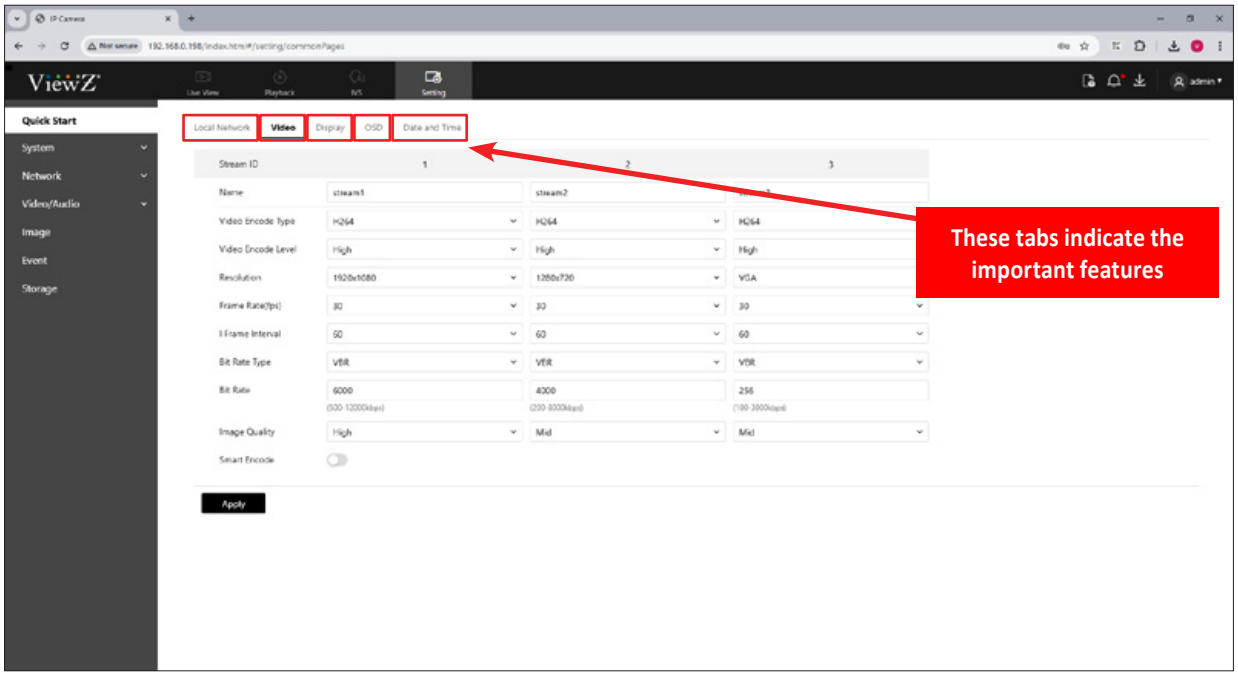


Figure 4-2 Quick Start

SETTING

System

Description

The device information includes:

- Device ID, name, type, model, and MAC address
- Hardware and software versions
- Number of video channels, number of alarm input channels, number of alarm output channels, and number of serial ports

Note

- User can modify the device name. All other parameters can only be viewed.
- When the device is upgraded, the device information will be updated automatically.

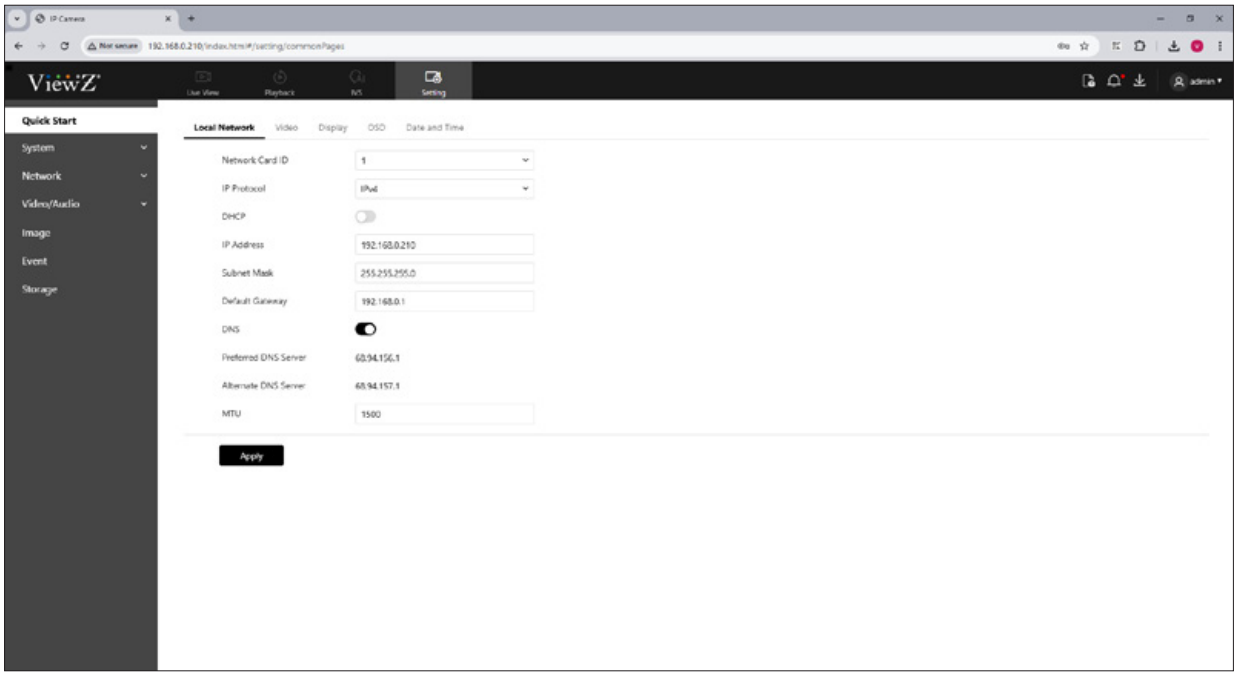


Figure 4-1 Setting

SETTING / DEVICE INFO

1. Configuration of AI PVM's Information

Procedure

The **Configuration > Device Info** page is displayed, as shown in Figure 4-3.

Step 1 Click **Setting** on the top menu, **System > Settings > Device Info**.

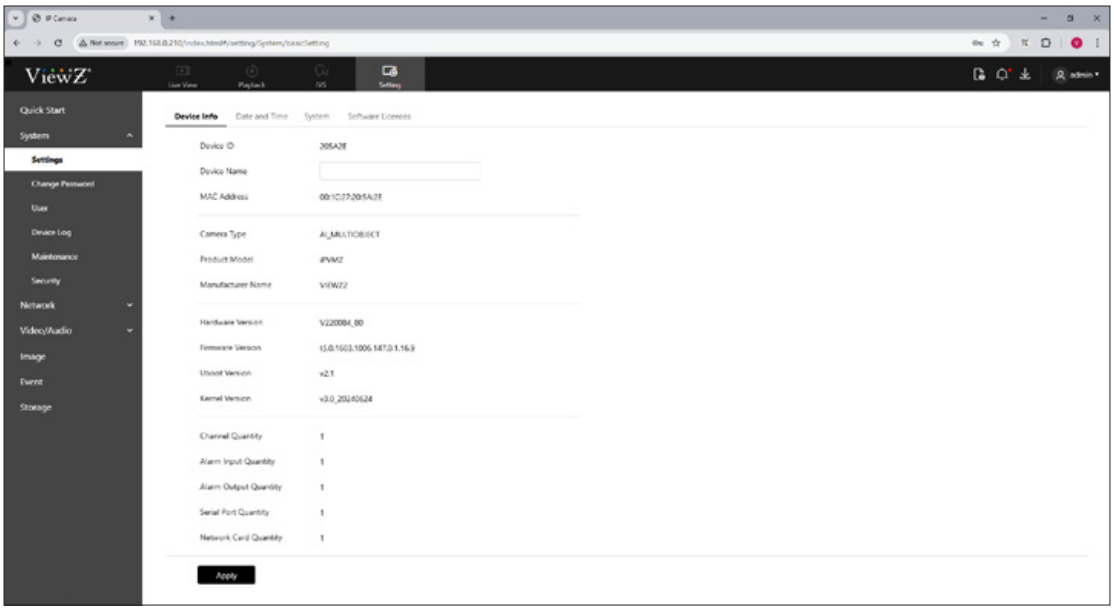


Figure 4-3 Device Info

Step 2 View the device information, set the device **Name** parameters as shown in Table 4-1.

SETTING / DEVICE INFO

1. Configuration of AI PVM's Information

Procedure

Table 4-1 Device Info Parameters

Parameter	DESCRIPTION	Setting
Device ID	Unique device identifier used by the platform to distinguish the devices.	The parameter cannot be modified.
Device Name	Name of the device. NOTE The device name cannot exceed 32 bytes or 10 simplified characters; otherwise, the modification fails.	Enter a value manually.
MAC Address Camera Type Product Model Manufacturer Name Hardware Version Software Version Uboot Version Kernel Version Channel Quantity Alarm Input Qty. Alarm Output Qty. Serial Port Qty. Network Card Qty. Network Card	These parameters cannot be modified.	N/A

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, it means the updated value is confirmed.
- If the message "Apply failed!" is displayed, you must apply for the Parameter Configure permission from an administrator. Please refer to page 27.

SETTING / DATE & TIME

1. Configuration of AI PVM's Information

Description

The Date & Time information includes:

- Time zone, current device time
- NTP (Network Time Protocol)
- Daylight saving time

Procedure

The **Settings > Date and Time** page is displayed, as shown in Figure 4-4.

Step 1 Click **Setting** on the top menu, **System > Settings > Date and Time**.

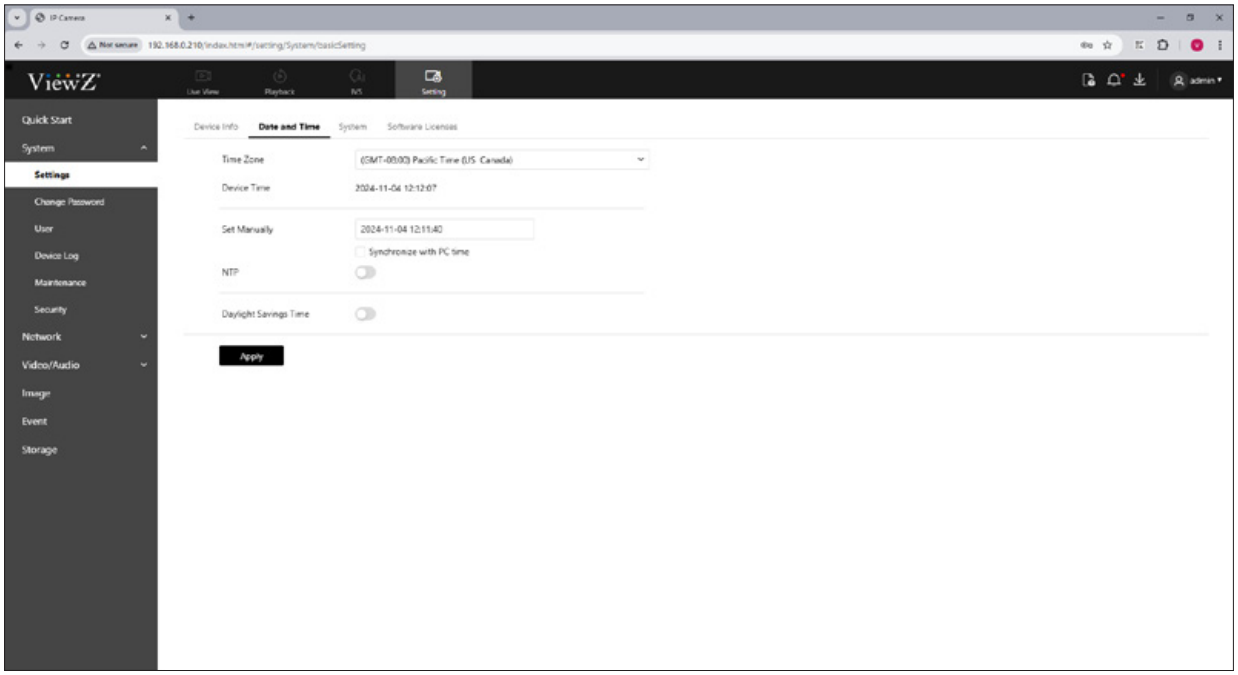


Figure 4-4 Date and Time

Step 2 View the device information, set the **Date & Time** parameters as shown in Table 4-2.

SETTING / DATE & TIME

1. Configuration of AI PVM's Information

Procedure

Table 4-2 Date & Time Parameters

Parameter	DESCRIPTION	Setting
Time Zone	Choose the time line based on Greenwich time. Select a value from the drop-down list.	Default Value: Pacific Time
Device Time	Display the current device time	N/A
Set Manually	Setup the device time manually or synchronize with PC time.	Select a time format from the list
NTP	Enable & disable NTP time NOTE Set server address, port number & interval time	Click the button to enable/disable NTP and enter a value manually
Daylight Saving Time	When the DST Begin-Time meets, the device time will automatically be 1 hour earlier. When the DST End-Time meets, the device time will automatically be 1 hour later.	Click the button to enable/disable

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, and the system will save the settings.
- If other information is displayed, set the parameters correctly.

Note

- The Date & Time Format is;
  YYYY: Year, **MM**: Month, **DD**: Day, **HH**: Hour, **MM**: Minute, **SS**: Seconds and **WW**: Weekday
- User can select one of format types like below;
  YYYY-MM-DD HH:MM:SS WW
  HH:MM:SS YYYY-MM-DD WW
  MM/DD/YYYY HH:MM:SS WW
  HH:MM:SS MM/DD/YYYY WW
  DD/MM/YYYY HH:MM:SS WW

SETTING / SYSTEM

1. Setup Language

Description & Procedure

User can choose the system language, as shown in Figure 4-5.

Step 1 Click **Setting** on the top menu, **System > Settings > System**.

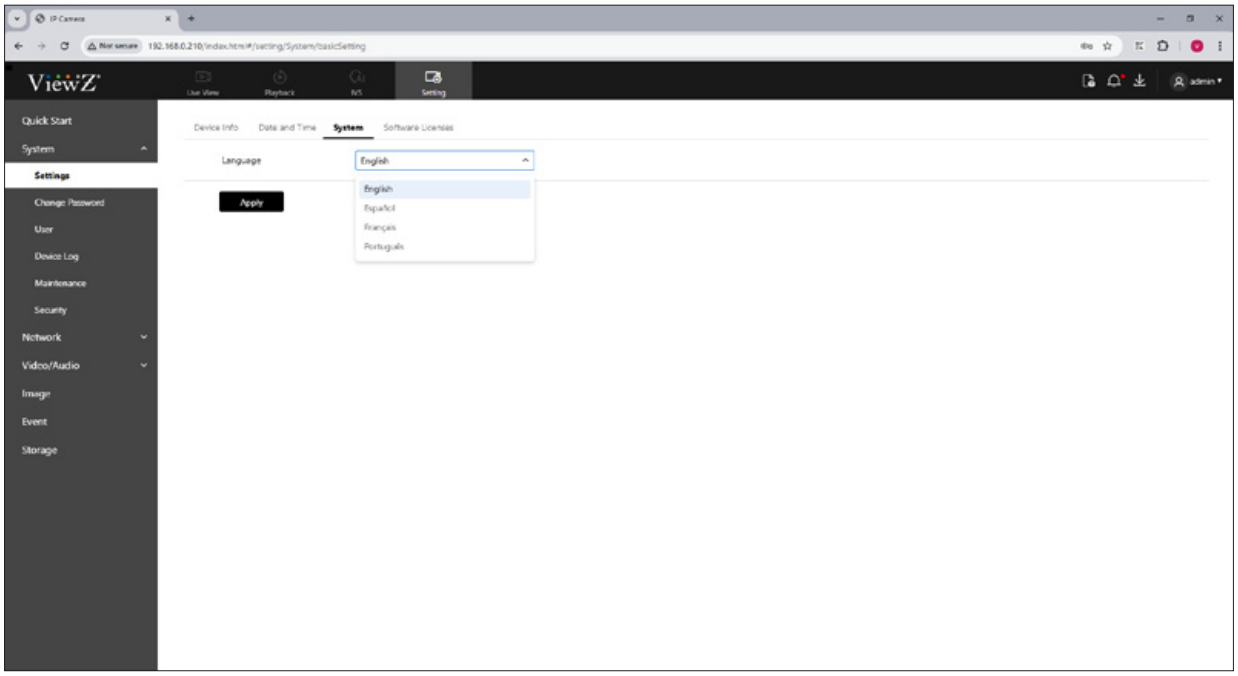


Figure 4-5 System-Language

Step 2 Set **Language** parameters as shown in Table 4-3.

Table 4-3 Language Parameters

Parameter	DESCRIPTION	Setting
Language	User can choose the default language **NOTE** Please choose a language among English, Spanish, French & Portuguese	Select a value from the drop-down list box. The default language is English

Step 3 Click **Apply** button to use the selected language.

- If the message "Apply success!" is displayed, and the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / SW LICENSE

1. Checkup the AI PVM's License Information

Description & Procedure

User can check the system software license info, as shown in Figure 4-6.
Step 1 Click **Setting** on the top menu, **System > Settings > Software License**.

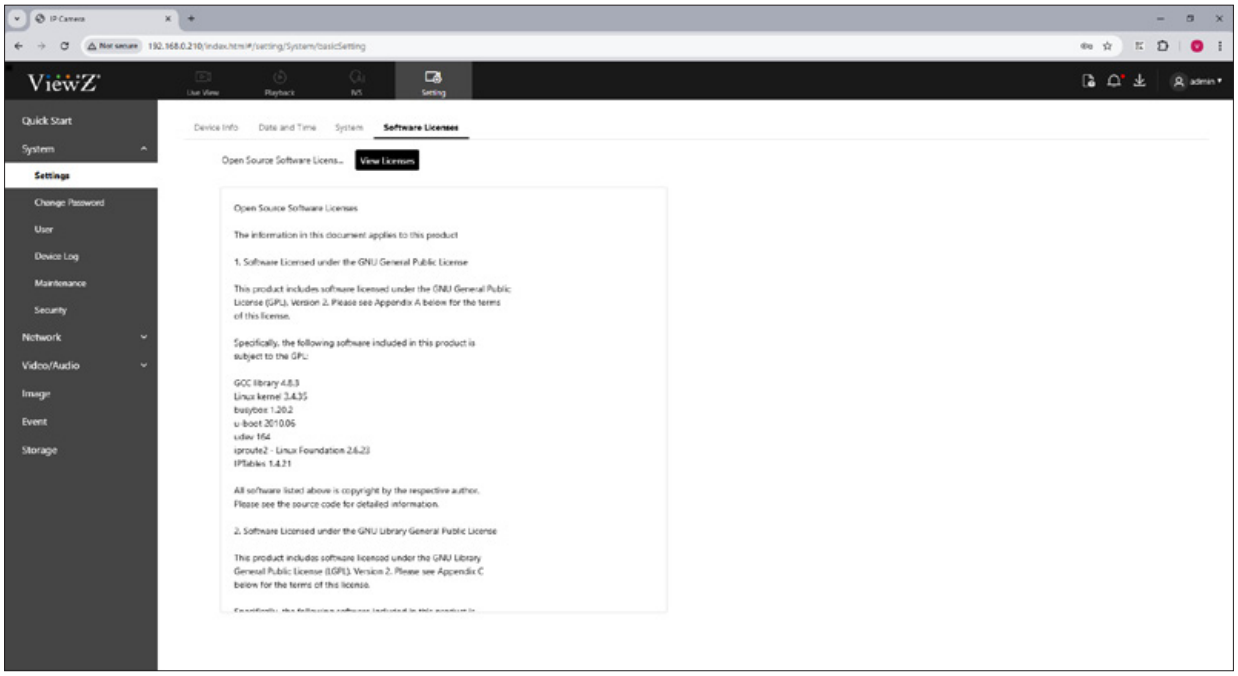


Figure 4-6 Software License Info

SETTING / CHANGE PASSWORD

1. Setup Password

Description & Procedure

User can change the password, as shown in Figure 4-7.

Step 1 Click **Setting** on the top menu, **System > Change Password**.

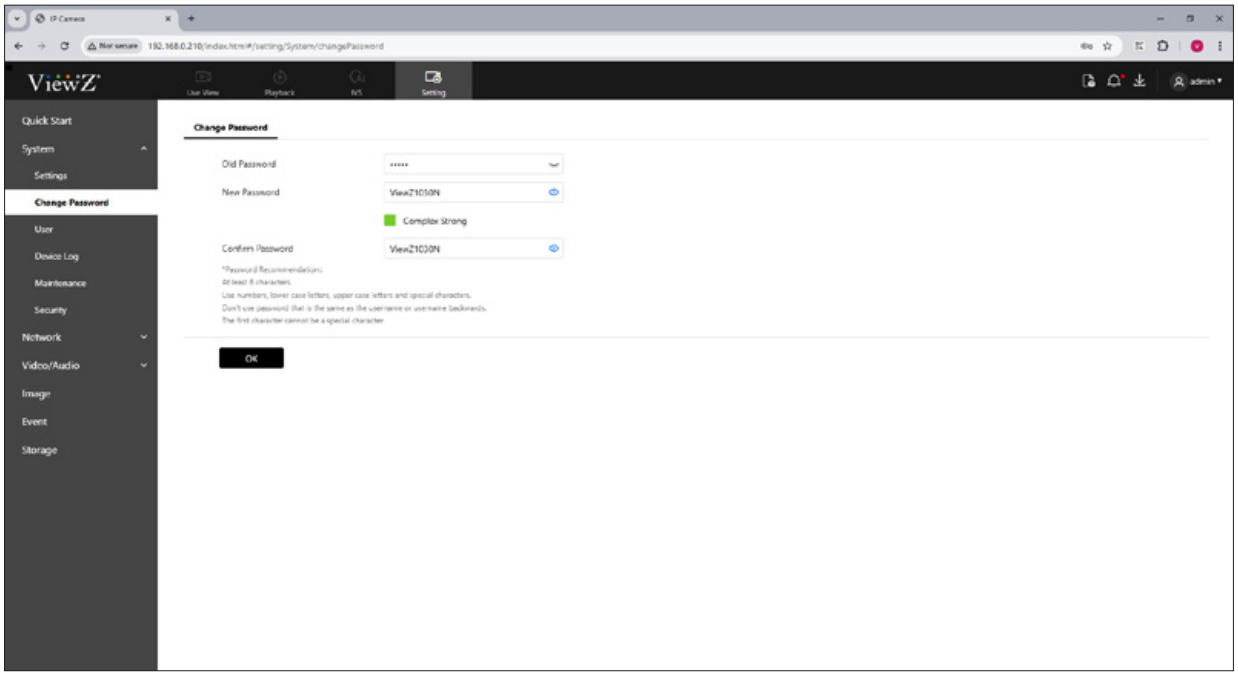


Figure 4-7 Change Password

Step 2 Enter the old password, new password, and confirm the new password as shown in Table 4-4.

Table 4-4 Password Parameters

Parameter	DESCRIPTION	Setting
Password	User can change the login password of super admin **NOTE** Please type the old password & new password. The new password requires at least 8 characters.	N/A

Step 3 Click **OK** button to apply the updated password.

- If the message "Apply success!" is displayed, and the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / USER

1. Setup the User Account

Description & Procedure

User can add, modify & delete the user account. Also, user can see the accessed user and listed users, as shown in Figure 4-8.

Step 1 Click **Setting** on the top menu, **System > User**.

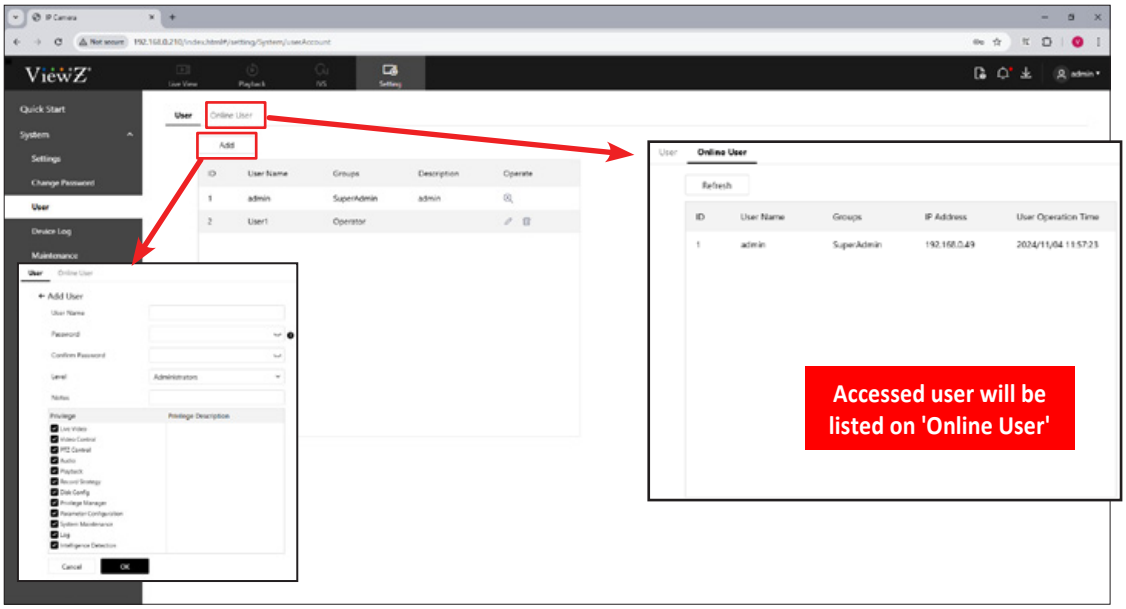


Figure 4-8 User Account

Step 2 Set **User** parameters as shown in Table 4-5.

Table 4-5 User Parameters

Parameter	DESCRIPTION	Setting
User	List the registered user accounts	N/A
Online User	List the connected user accounts	N/A
ID	User ID	N/A
User Name	User name for login	N/A
Groups (Level)	Permission group where an user belongs. The default permission groups are Administrators, Operator, and Media user.	When add / edit the user account, user can select the group (level)
Description (Notes)	Comment of user	When add / edit the user account user can add / edit the description
Operate	Edit, view and delete the user account, account role, password and level	N/A

SETTING / USER

1. Setup the User Account

Procedure

Step 3 Add, modify or delete the user account as shown in Table 4-6.

Table 4-5 User Parameters

Parameter	DESCRIPTION	Setting
Add	Click Add to add an user account	User name, Password, Group (Level), Privilege (access control), Comment (Note)
Modify	Click to edit the user account	Password, Group (Level), Comment Privilege (access control),
Delete	Click to delete the user account	N/A
View	Click to see the user account **NOTE** This icon only shows at **Super Admin** ***Super Admin*** account cannot be edited	N/A

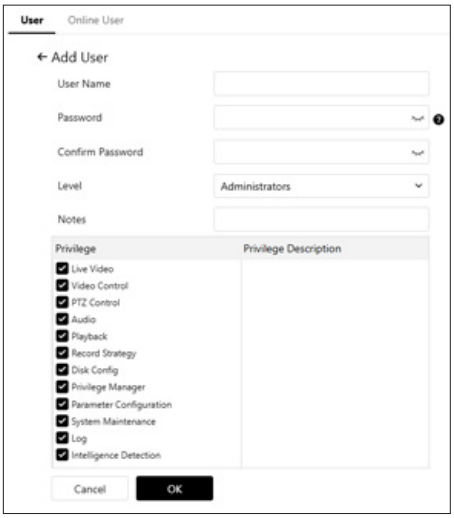


Figure 4-9 User Account - Administrator

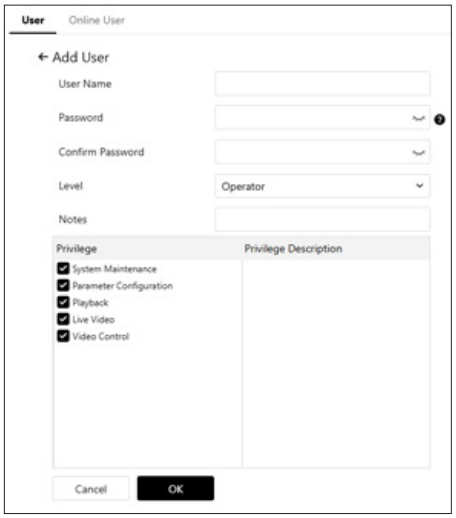


Figure 4-9 User Account - Operator

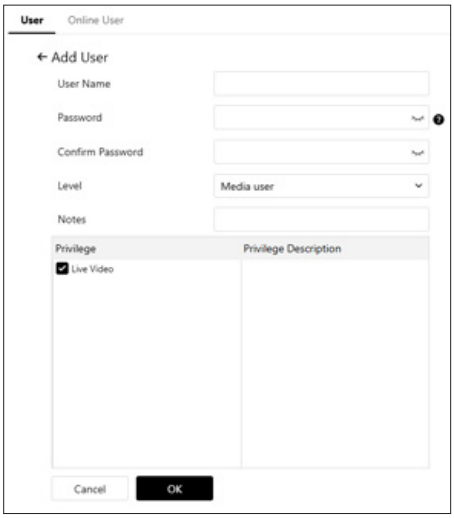


Figure 4-9 User Account - Media User

Note

- The default **Super Admin** account is '**admin/admin**'

SETTING / DEVICE LOG

1. Search & Download the Operation Log

Description & Procedure

User can find & download the operation log, as shown in Figure 4-11.

Step 1 Click **Setting** on the top menu, **System > Device Log > Operation Log**.

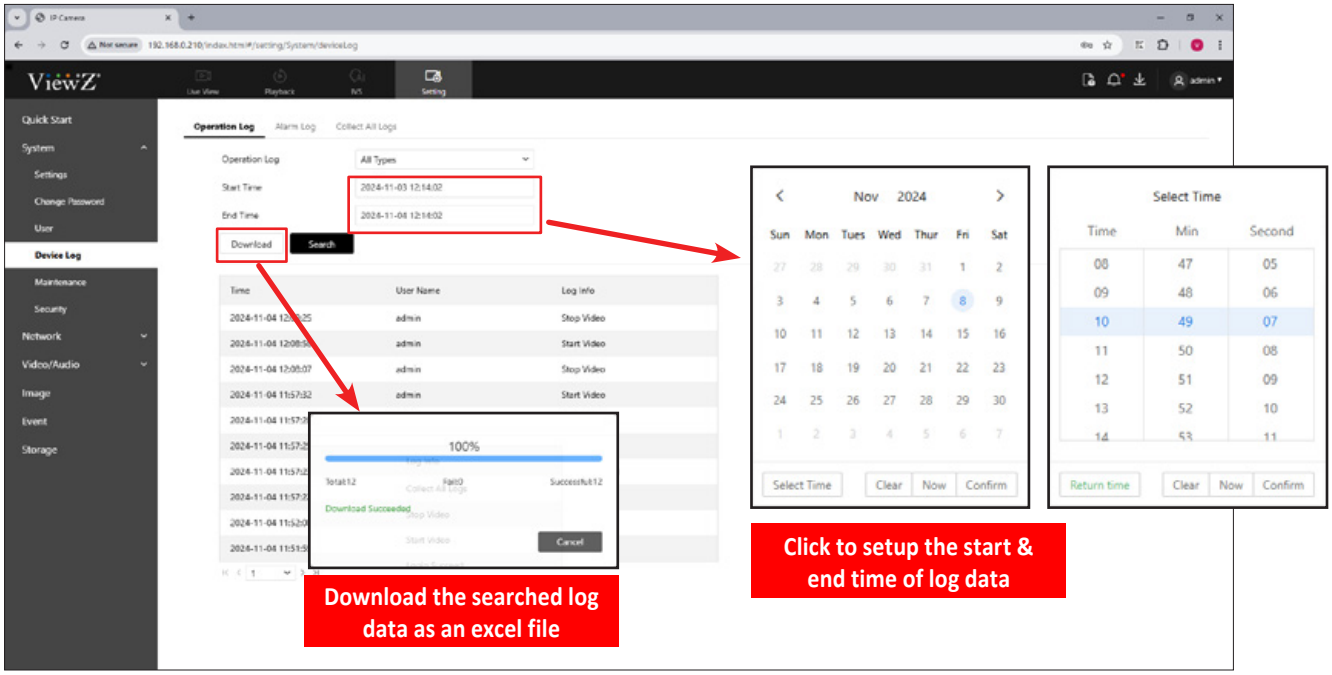


Figure 4-10 Operation Log

Step 2 Set **Operation Log** parameters as shown in Table 4-6.

Table 4-6 Operation Log Parameters

Parameter	DESCRIPTION	Setting
Operation Log	Search & download the operation log data	All Type, Privilege Manager, System Maintenance, Device, Record Operation
All Type	Search & download all log of operational data	N/A
Privilege Manager	Search & download the log of login, logout & all user account relatives	N/A
System Maintenance	Search & download the log of system maintenance	N/A
Device	Search & download the log of device data	N/A
Record Operation	Search & download the log of record operation	N/A
Search	Search the operation log data	N/A
Download	Download the operation log data as excel file	N/A

SETTING / DEVICE LOG

2. Search & Download the Alarm Log

Description & Procedure

User can find & download the alarm log, as shown in Figure 4-12.

Step 1 Click **Setting** on the top menu, **System > Device Log > Alarm Log**.

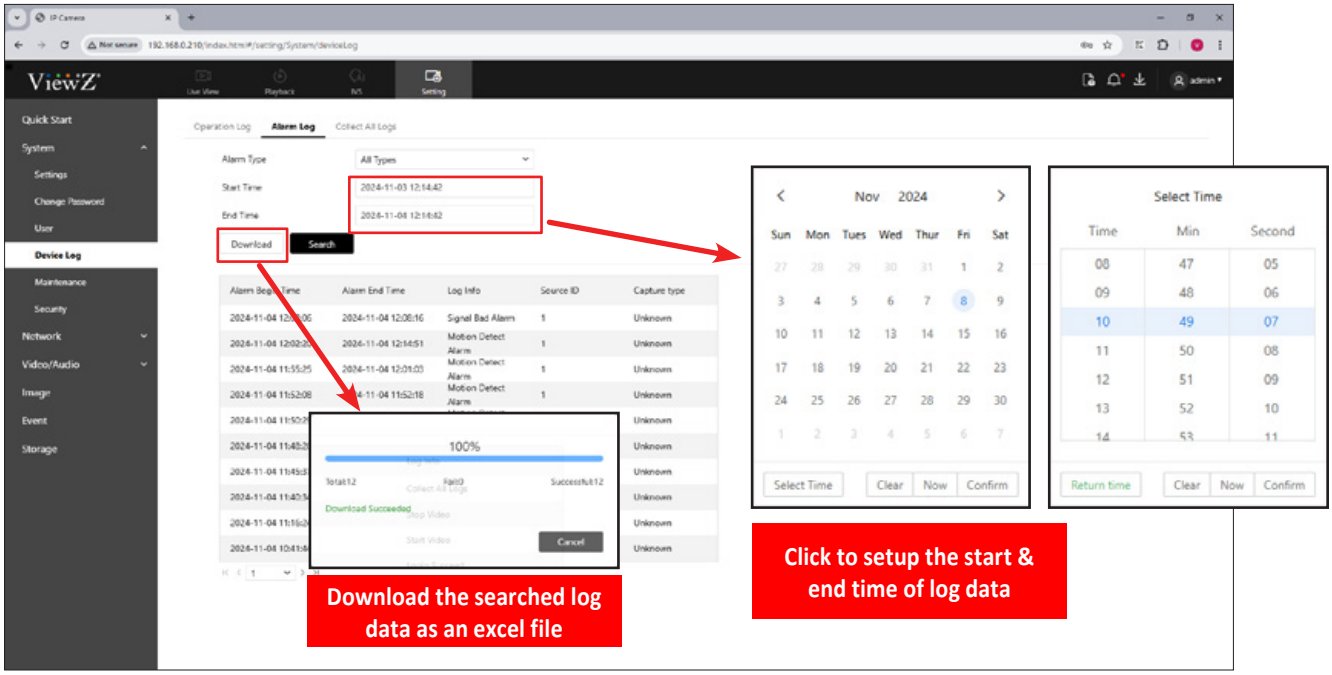


Figure 4-11 Alarm Log

Step 2 Set **Alarm Log** parameters as shown in Table 4-7.

Table 4-7 Alarm Log Parameters

Parameter	DESCRIPTION	Setting
Alarm Log	Search & download the alarm log data	All Type, Security Alarm, Disk Alarm, Record Alarm, Intelligent Analysis Alarm
All Type	Search & download all alarm log	N/A
Security	Search & download the security alarm log	N/A
Disk	Search & download the disk alarm log	N/A
Record	Search & download the record alarm log	N/A
Intelligent Analysis	Search & download the IVS alarm log	N/A
Search	Search the alarm log data	N/A
Download	Download the alarm log data as excel file	N/A

SETTING / DEVICE LOG

3. Collect All Log

Description & Procedure

User can find & download all log, as shown in Figure 4-12.

Step 1 Click **Setting** on the top menu, **System > Device Log > Collect All Logs**.

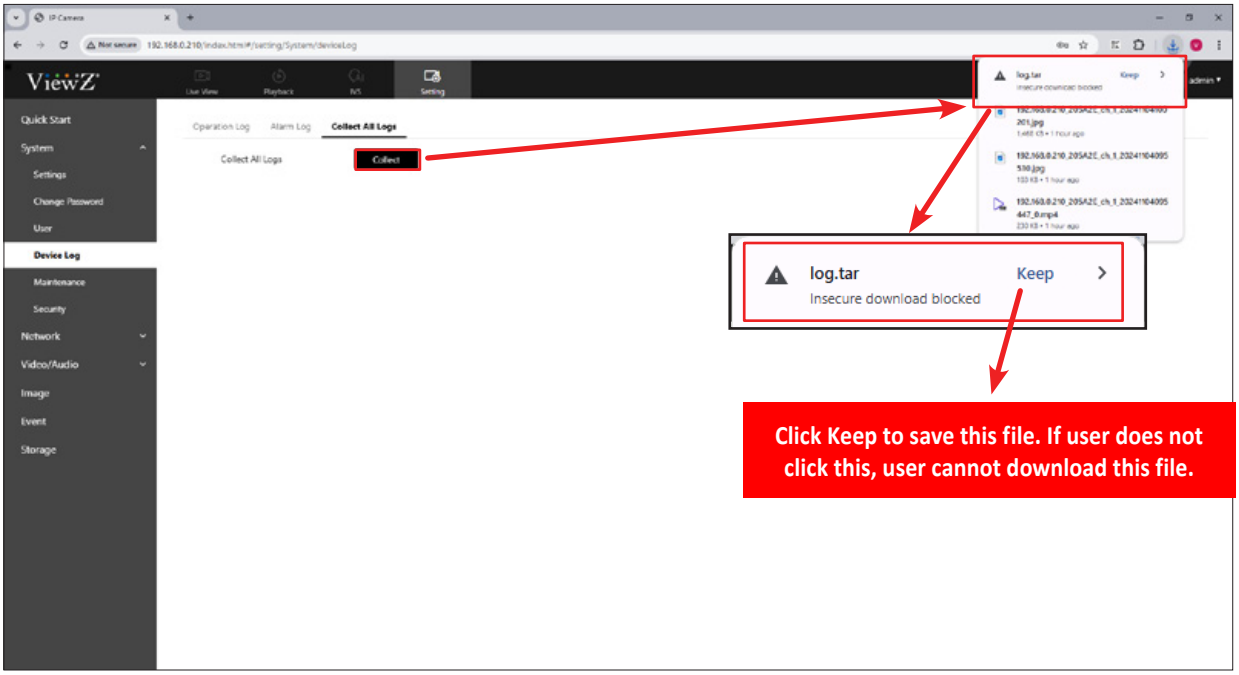


Figure 4-12 Collect All Log

Step 2 Set **Collect All** parameters as shown in Table 4-8.

Table 4-8 Collect All Log Parameters

Parameter	DESCRIPTION	Setting
Collect	When user click this button, the system will collect all log data and download a zipped file as TAR format	N/A

Note

- The zipped file will be saved at the default path of browser.
- Based on the personal setting of browser, the file could not be allowsed to download. In this case, please adjust your setup for downloading files from AI PVM.

SETTING / MAINTENANCE

1. Setup the Maintenance - Reboot

Description & Procedure

User can immediately or periodically reboot AI PVM, as shown in Figure 4-13.

Step 1 Click **Setting** on the top menu, **System > Maintenance > Reboot**.

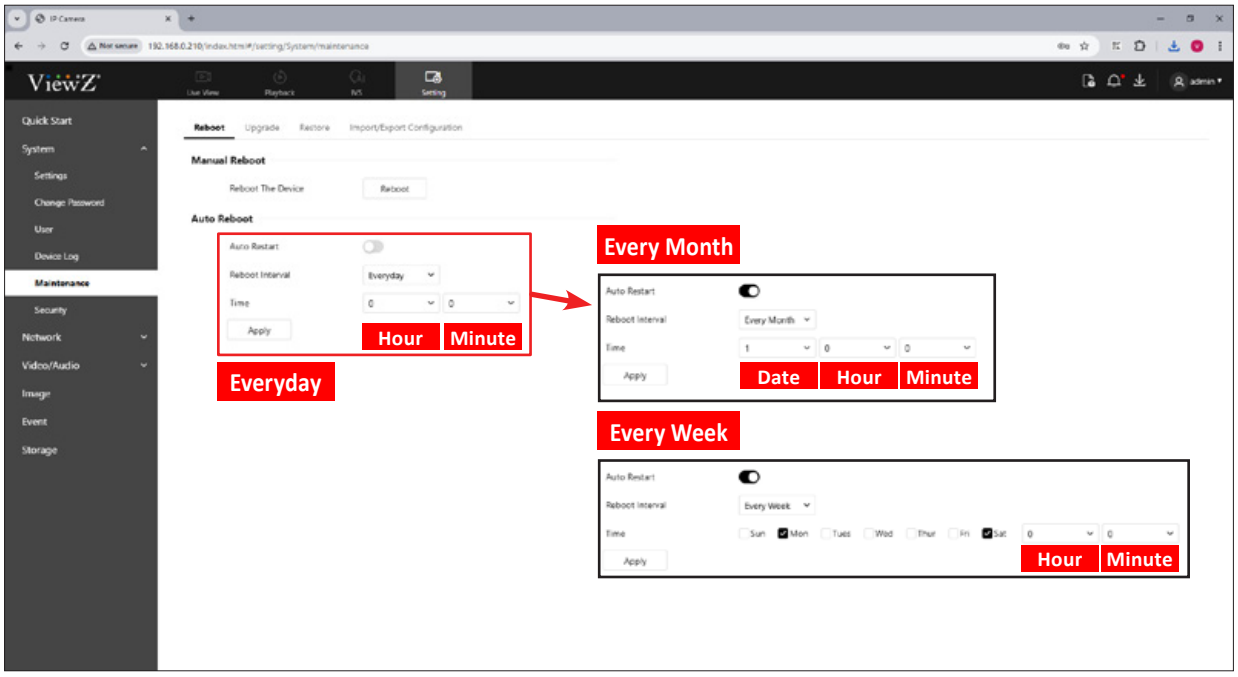


Figure 4-13 Reboot

Step 2 Set **Reboot** parameters as shown in Table 4-9.

Table 4-9 Reboot Parameters

Parameter	DESCRIPTION	Setting
Manual Reboot	Reboot the AI PVM immediately	N/A
Auto Restart	Enable / Disable the reboot system	N/A
Reboot Interval	Select the interval	Everyday, Every Week, Every Month
Time-Everyday	Select the time	Hour and Minute
Time-Every Week	Select the time	Weekday, Hour and Minute
Time-Every Month	Select the time	Date, Hour and Minute

SETTING / MAINTENANCE

2. Setup the Maintenance - Upgrade

Description & Procedure

User can upgrade firmware, as shown in Figure 4-14.

Step 1 Click **Setting** on the top menu, **System > Maintenance > Upgrade**.

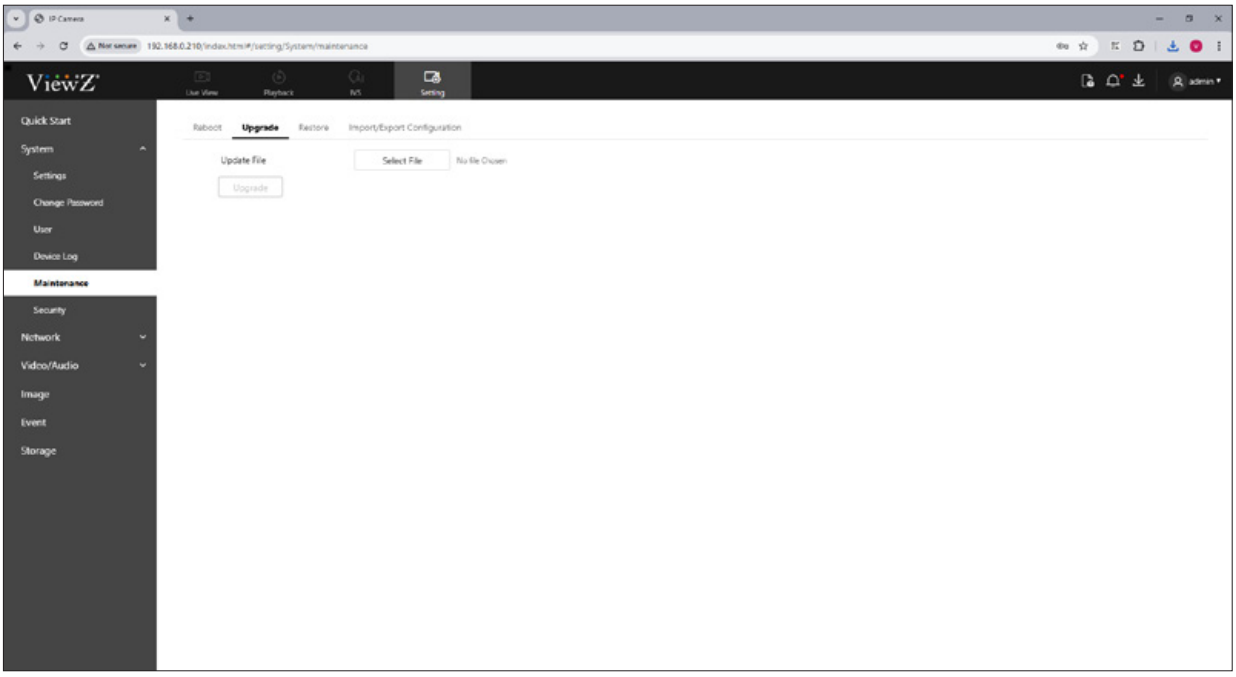


Figure 4-14 Upgrade

Step 2 Set **Upgrade** parameters as shown in Table 4-10.

Table 4-10 Upgrade Parameters

Parameter	DESCRIPTION	Setting
Select File	Find a firmware file from PC and click UPGRADE button to apply	N/A

Step 3 When the file is selected, click **Upgrade** button to update the system.

- If the message "Apply success!" is displayed, and the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / MAINTENANCE

3. Setup the Maintenance - Restore

Description & Procedure

User can restore the parameters as factory default, as shown in Figure 4-15.

Step 1 Click **Setting** on the top menu, **System > Maintenance > Restore**.

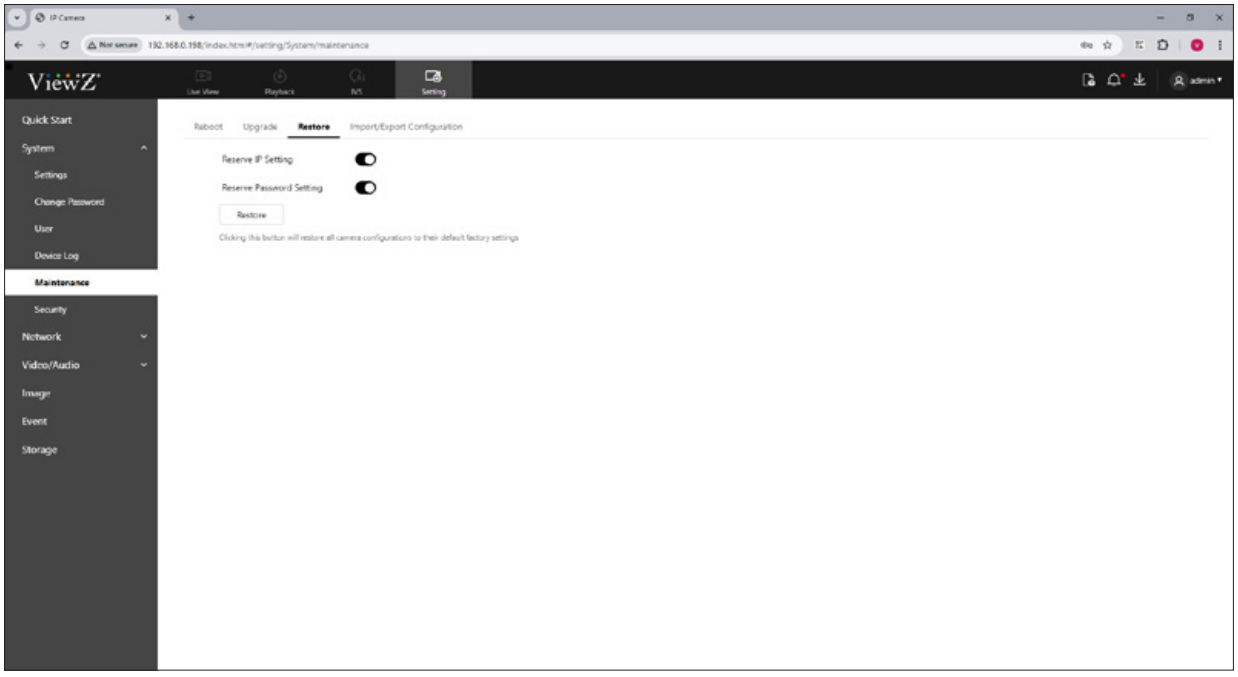


Figure 4-15 Restore

Step 2 Set **Restore** parameters as shown in Table 4-11.

Table 4-11 Restore Parameters

Parameter	DESCRIPTION	Setting
Reserve IP Setting	Keep the IP address info, even if the system is restored	Default Value: ON
Reserve Password Setting	Keep the current user password, even if the sytem is retored	Default Value: OFF
Restore	Restore all setting as factory default value	N/A

Step 3 Click **Restore** button to restore all setting values as factory default.

- If the message "Apply success!" is displayed, and the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / MAINTENANCE

3. Setup the Maintenance - Import/Export Configuration

Description & Procedure

User can import/export configuration, as shown in Figure 4-16.

Step 1 Click **Setting** on the top menu, **System > Maintenance > Import/Export Configuration**.

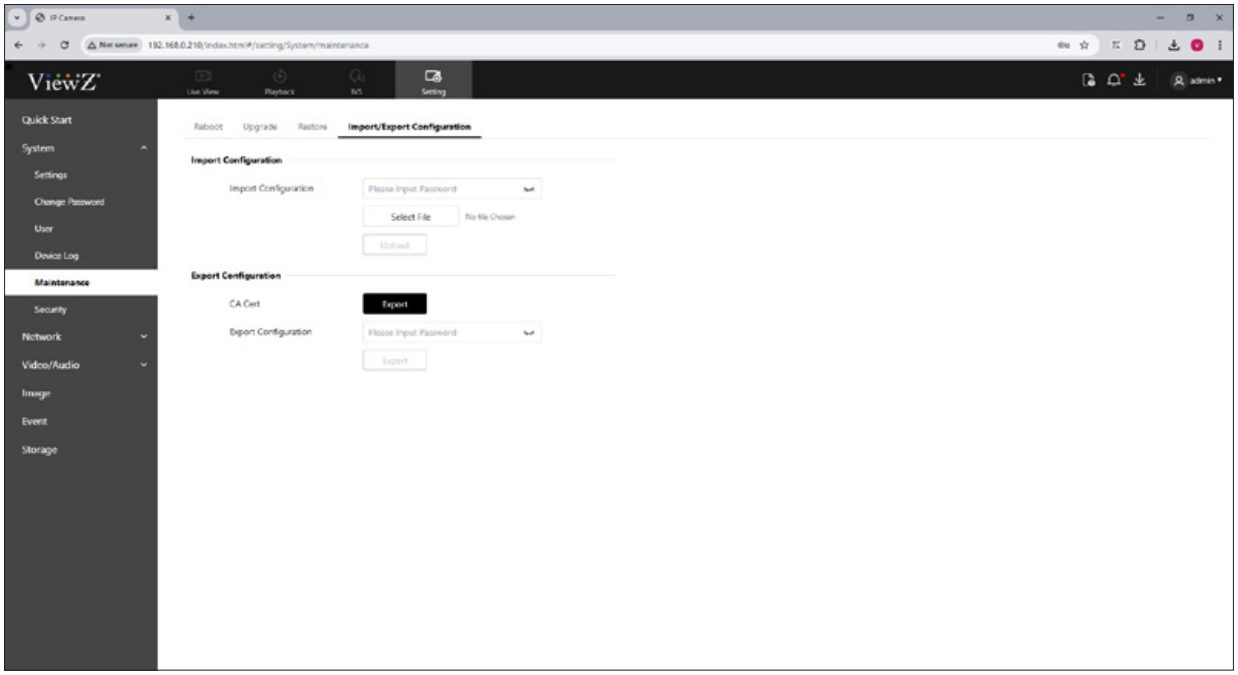


Figure 4-16 Import/Export Configuration

Step 2 Set **Import/Export Configuration** parameters as shown in Table 4-12.

Table 4-12 Import/Export Configuration Parameters

Parameter	DESCRIPTION	Setting
Import Configuration	Import the configuration data **NOTE** Type the admin password, select the data file and upload & apply it.	N/A
Export Configuration	Export the configuration data **NOTE** Type the admin password & export data file	N/A

Note

- The import/export configuration data file is 'XXX.CRT' format.

SETTING / SECURITY

1. Setup IP Filter

Description & Procedure

User can allow/block IP addresses, as shown in Figure 4-17.
Step 1 Click **Setting** on the top menu, **System > Security > IP Filter**

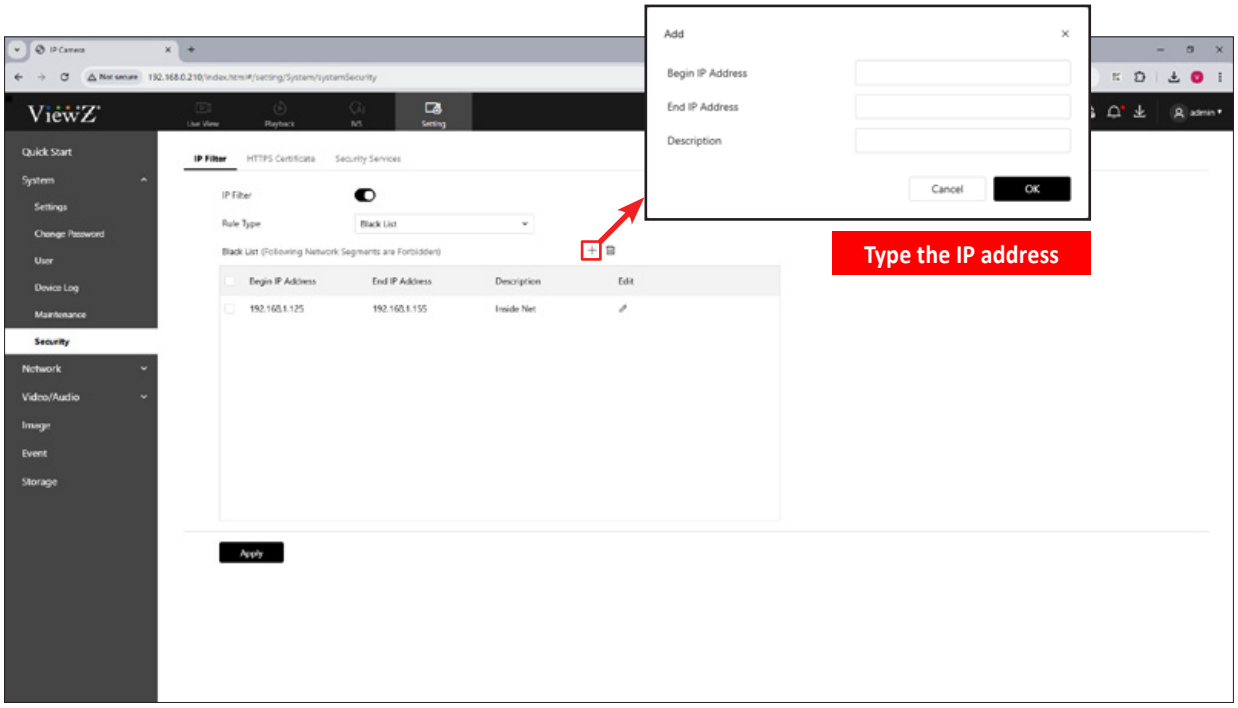


Figure 4-17 IP Filter

Step 2 Set **IP Filter** parameters as shown in Table 4-13.

Table 4-13 IP Filter Parameters

Parameter	DESCRIPTION	Setting
IP Filter	Enable/disable the IP filter function	Default Value: OFF
Rule Type	Select Black List or White List	Default Value: Black List
Black List	Add/edit/delete the blocked IP address	
	Type the IP address - XXX.XXX.XXX.XXX	
White List	Add/edit/delete the allowed IP address	
	Type the IP address - XXX.XXX.XXX.XXX	

Note
- If user needs to block/allow the specific IP addresses range, please use 'Begin & End IP addresses'.

SETTING / SECURITY

2. Setup HTTPS Certificate

Description & Procedure

User can add HTTPS certificate, as shown in Figure 4-18.

Step 1 Click **Setting** on the top menu, **System > Security > HTTPS Certificate**

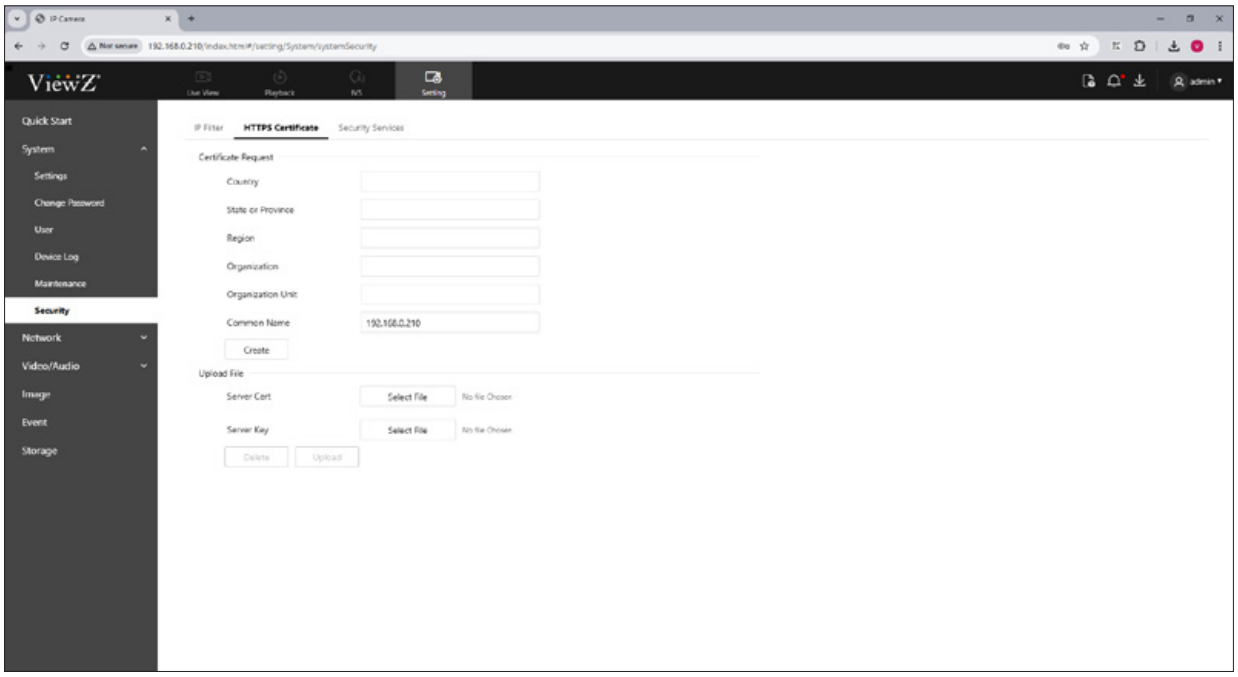


Figure 4-18 HTTPS Certificate

Step 2 Set **HTTPS Certificate** parameters as shown in Table 4-14.

Table 4-14 HTTPS Certificate Parameters

Parameter	DESCRIPTION	Setting
Certificate Request	Setup the HTTPS certification	N/A
Upload File	User can upload & apply HTTPS certification & key file	N/A
Server Cert	Upload & apply the server certification file	N/A
Server Key	Upload & apply the server key file	N/A

SETTING / SECURITY

3. Setup Security Services

Description & Procedure

User can setup limited login request, as shown in Figure 4-19.

Step 1 Click **Setting** on the top menu, **System > Security > Security Services**

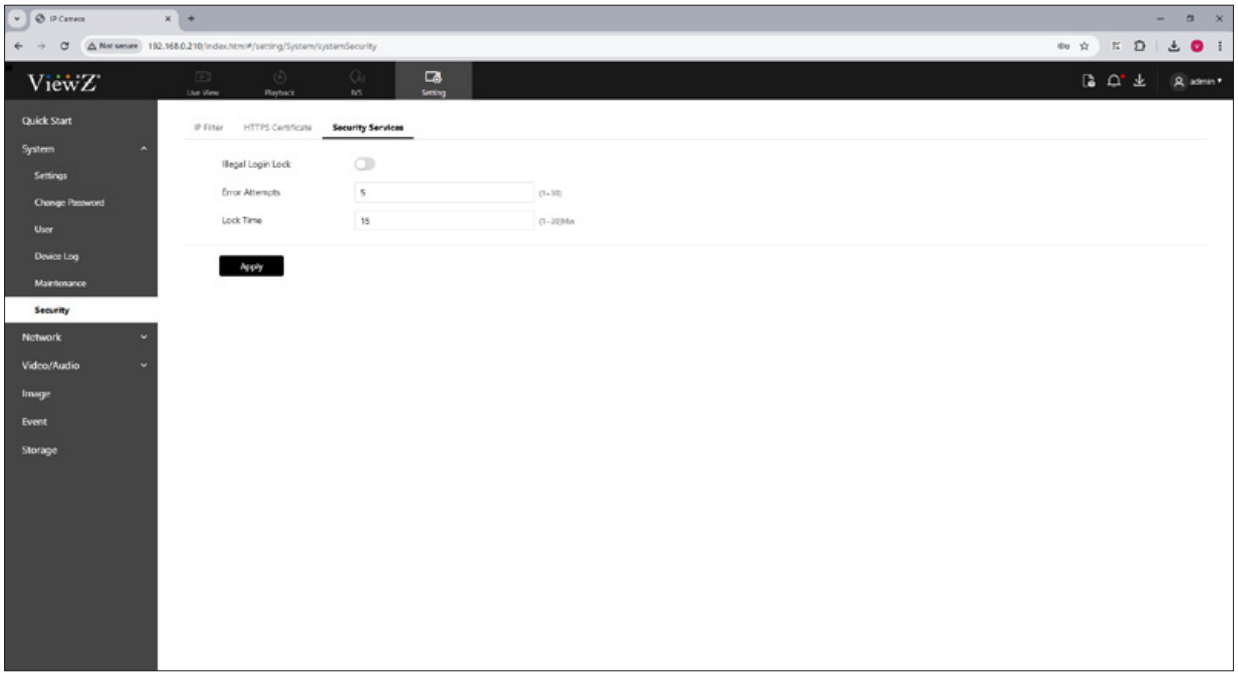


Figure 4-19 Security Service

Step 2 Set **Security Service** parameters as shown in Table 4-15.

Table 4-15 Security Service Parameters

Parameter	DESCRIPTION	Setting
Illegal Login Lock	Enable/disable function	Default Value: OFF
Error Attempts	Set the number or login request	1 ~ 30 times
Lock Time	Set the number or lockout time	1 ~ 30 minutes

Step 3 Click **Apply** button to apply the updated value of **Error Attempts** & **Lock Time**.

- If the message "Apply success!" is displayed, and the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / NETWORK

1. Setup Local Network

Description & Procedure

User can setup the network information, as shown in Figure 5-1.

Step 1 Click **Setting** on the top menu, **Network > Settings > Local Network**

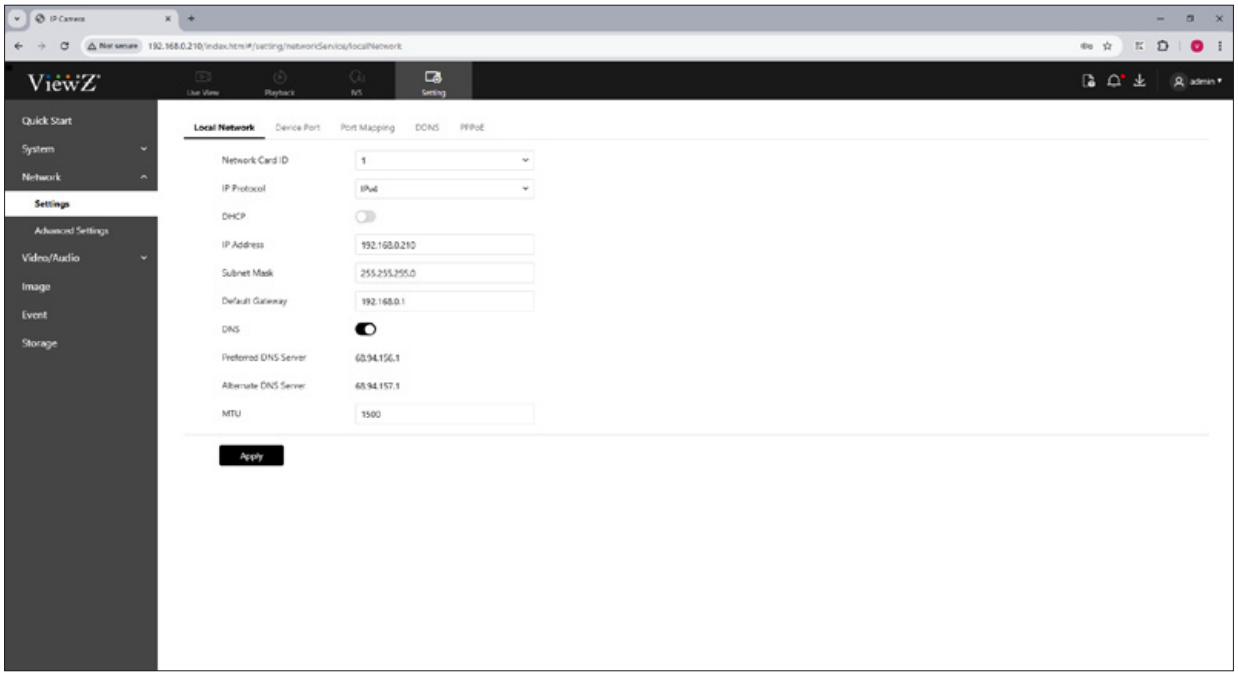


Figure 5-1 Local Network

Step 2 Set **Local Network** parameters as shown in Table 5-1.

Table 5-1 Local Network Parameters

Parameter	DESCRIPTION	Setting
Local Network	Setup the IP configuration	N/A
Network Card ID	Display the network card ID	Default Value: 1
IP Protocol	IPv4 is the IP protocol that uses an address length of 32 bits - IPv4 or IPv6	Default Value: IPv4
DHCP	IP address that the DHCP server assigns to the device. **NOTE** If DHCP enabled, Subnet Mask/Default Gateway/ IP address is automatically assigned	Default Value: OFF

SETTING / NETWORK

1. Setup Settings - Local Network

Description & Procedure

Table 5-1 Local Network Parameters

Parameter	DESCRIPTION	Setting
IP Address	Device IP address that can be set as required.	Default Value: 192.168.0.120
Subnet Mask	Subnet mask of the network adapter	Default Value: 255.255.255.0
Default Gateway	This parameter must be set if the client accesses the device through a gateway	Default Value: 192.168.0.1
DNS	DNS - Domain Name Server **NOTE** The connected network will automatically provides AI PVM's DNS address.	Default Value: ON
Preferred DNS Server	IP address of a primary DNS server	Default Value: 192.168.0.1
Alternate DNS Server	IP address of a secondary DNS server If the preferred DNS server is faulty, the device uses the alternate DNS server to resolve domain names.	Default Value: 192.168.0.2
MTU	Set the maximum value of network transmission data packets. **NOTE** The MTU value ranges from 1280to1500, with the default value at 1500. Please do not change it arbitrarily.	Default Value: 1500

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, click Confirm. The system saves the settings. The message "Set network parameter success, please login system again" is displayed. Use the new IP address to log into the web management system.
- If the message "Invalid IP Address", "Invalid Subnet Mask", "Invalid Default Gateway", "Invalid Primary DNS", or "Invalid Space DNS" is displayed, set the parameters correctly.

SETTING / NETWORK

2. Setup Settings - Device Ports

Description

You must configure the Control port, HTTP port, Real Time Streaming Protocol (RTSP) port and HTTPS port for device route mapping in a LAN, as shown in Figure 5-2.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Settings > Device Port**

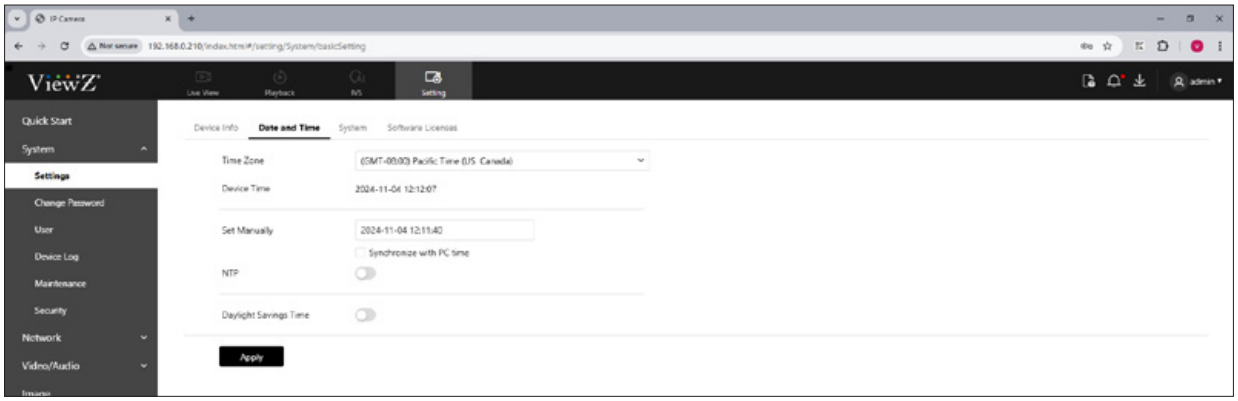


Figure5-2 Device Port

Step 2 Set **Device Port** parameters as shown in Table 5-2.

Table 5-2 Device Port Parameters

Parameter	DESCRIPTION	Setting
Control Port	Port used for audio and video transfer and signaling interaction	Default Value: 30001
HTTP Port	Port used in web access	Default Value: 80
RTSP Port	RTSP protocol port	Default Value: 554
HTTPS Port	Hyper Text Transfer Protocol over Secure Socket Layer	Default Value: 443

Note

- It's not recommended to modify the control port, f or details about the value ranges of the control port, HTTP port and SSL Control port, see the communication matrix.

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, and the system saves the settings.
- If the message "Invalid Control Port, please input an integer between 1025 and 65535" is displayed, enter correct port numbers.

SETTING / NETWORK

3. Setup Settings - Port Mapping

Description

Port mapping helps establish a mapping relationship between the private network and the external network. Port mapping allows outside computers to access intranet devices so that the network works efficiently, as shown in Figure 5-3.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Settings > Port Mapping**

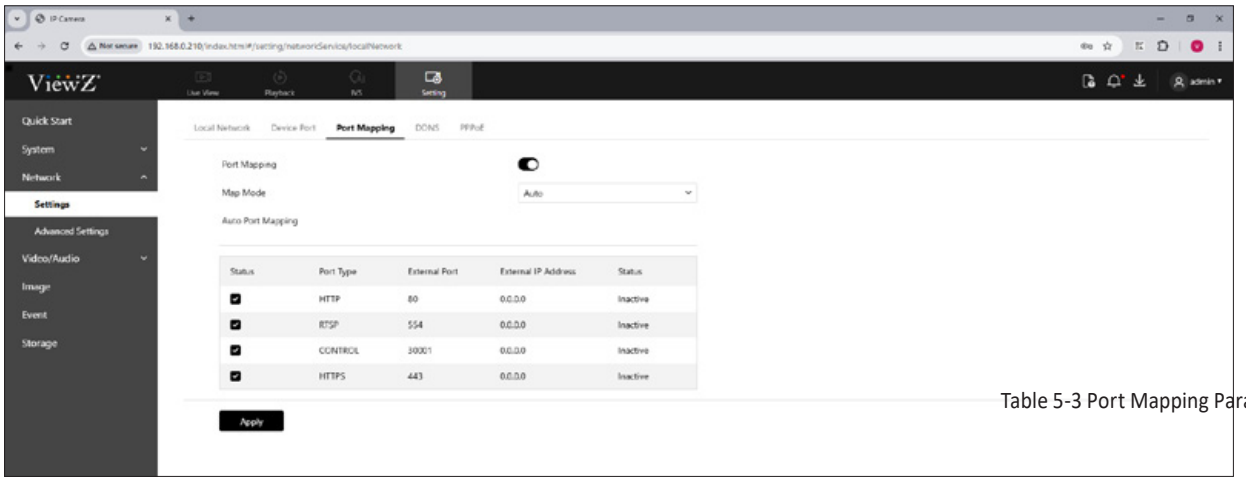


Figure 5-3 Port Mapping

Step 2 Set **Port Mapping** parameters as shown in Table 5-3.

Table 5-3 Port Mapping Parameters

Parameter	DESCRIPTION	Setting
Port Mapping	Device IP address that can be set as required.	Default Value: OFF
Map Mode	Mode of port mapping - auto or manual	Default Value: AUTO
Auto Port Mapping	When user select the manual mode, user can change the external port number & port mapping.	N/A
Status	Enable/disable each port mapping	Default Value: ON
Port Type	HTTP, RTSP, Control and HTTPS	N/A
External Port	Set the port number	N/A

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, and the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / NETWORK

4. Setup Settings - DDNS

Description

Connect the specified camera to the Internet, and obtain the user name and password for logging into the Dynamic Domain Name System (DDNS) server, as shown in Figure 5-4.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Settings > DDNS**

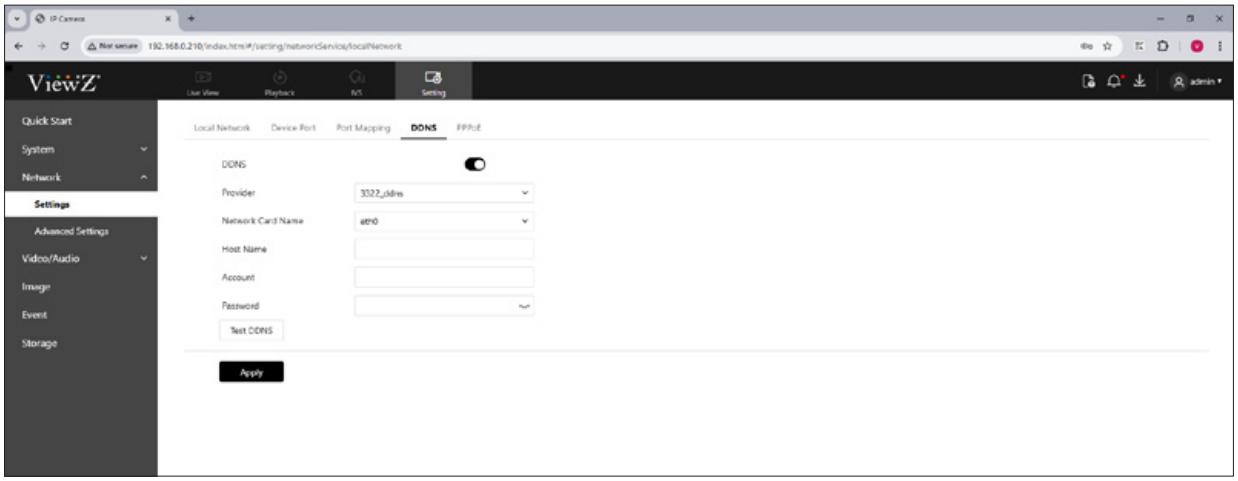


Figure 5-4 DDNS

Step 2 Set **DDNS** parameters as shown in Table 5-4.

Table 5-4 DDNS Parameters

Parameter	DESCRIPTION	Setting
DDNS	Enable/disable the DDNS service	Default Value: OFF
Provider	DDNS service provider. Currently, only 3322_DDNS and 3322_DDNS Dyndns are supported	Default Value: 3322_ddns
Network Card Name	Display the network card name	Default Value: eth0
Host Name	Type the address of host name	Default Value: Blank
Account	User ID/Name for login to the DDNS server	Default Value: Blank
Password	Password for login to the DDNS server	Default Value: Blank

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, and the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / NETWORK

5. Setup Settings - PPPoE

Description

If a PPPoE connection is used, you need to enter the user name and password on the PPPoE page. After you restart the device, the PPPoE settings take effect and the device obtains a public IP address, as shown in Figure 5-5.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Settings > PPPoE**

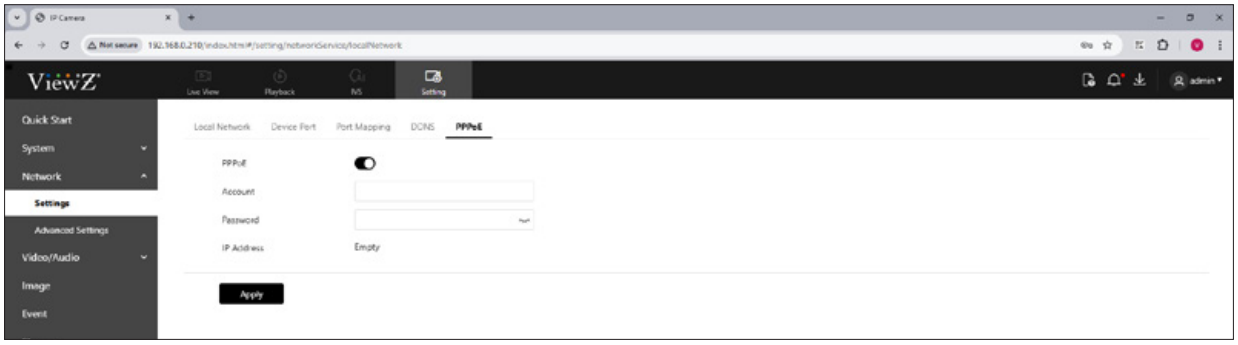


Figure 5-5 PPPoE

Step 2 Set **PPPoE** parameters as shown in Table 5-5.

Table 5-5 PPPoE Parameters

Parameter	DESCRIPTION	Setting
PPPoE	Enable/disable PPPoE dialing	Default Value: OFF
Account	User ID/Name for login to the PPPoE	Default Value: Blank
Password	Password for login to the PPPoE	Default Value: Blank

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, and the system will save the settings.
- If other information is displayed, set the parameters correctly.

Note

- User needs to have PPPoE's username and password from the network carrier

SETTING / NETWORK

6. Setup Advanced Settings - FTP

Description

If the File Transfer Protocol (FTP) button is enabled, the device will automatically send the snapped alarm JPG images to specified FTP server, as shown in Figure 5-6.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Advanced Settings > FTP**

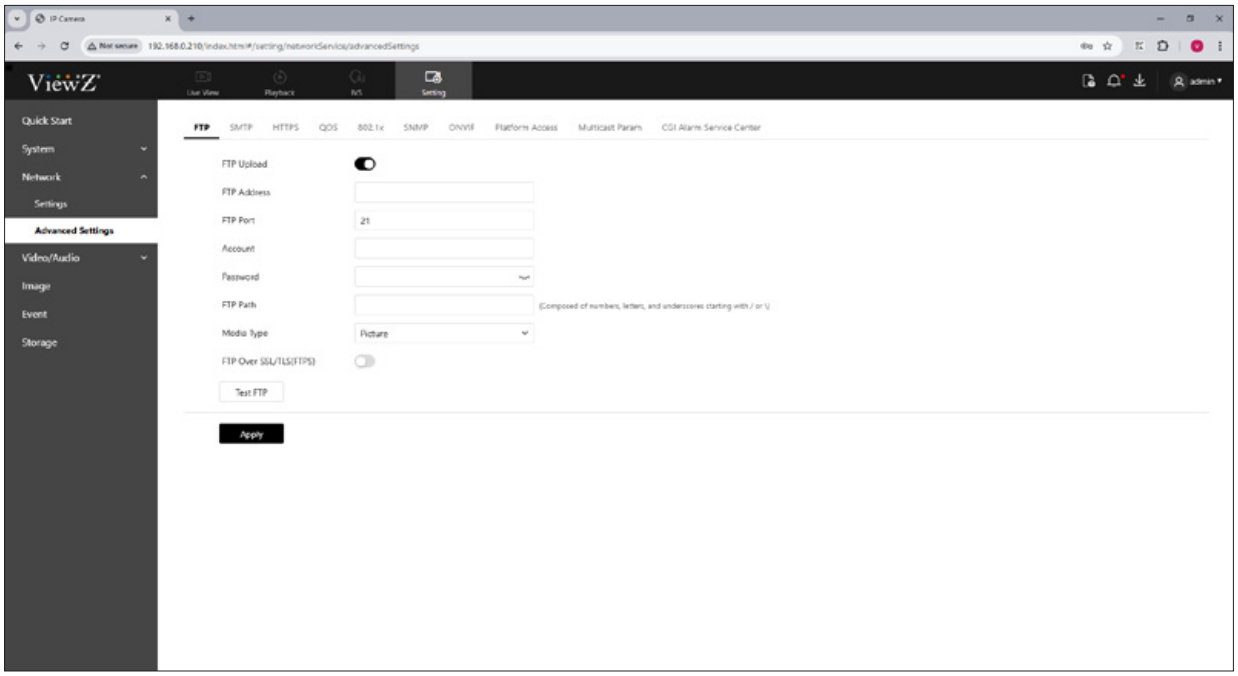


Figure 5-6 FTP

Step 2 Click **FTP Upload** to enable this function

Step 3 Set **FTP** parameters as shown in Table 5-6.

SETTING / NETWORK

6. Setup Advanced Settings - FTP

Procedure

Table 5-6 FTP Parameters

Parameter	DESCRIPTION	Setting
FTP Address	Manually type IP address of FTP server	Default Value: Blank
FTP Port	Port of FTP server	Default Value: 21
Account	FTP server account.	Default Value: Blank
Password	FTP server password	Default Value: Blank
FTP Path	FTP Path to save the JPG image	Default Value: Blank
Media Type	Select the media type to send picture or video file	Default Value: Picture
FTP Over SSL/TLS	Set the SSL/TLS server connection	Default Value: Off
Test FTP	Test FTP connection	N/A

Step 4 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

Note

- Click Test FTP button to verify the parameter, shows “Test succeed”, the parameters are right. If it shows “Test failed”, you need modify the information correctly.

SETTING / NETWORK

7. Setup Advanced Settings - SMTP

Description

If the Simple Mail Transfer Protocol (SMTP) function is enabled, the device will automatically send JPG images and alarm information to specified email addresses when an alarm is generated, as shown in Figure 5-7.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Advanced Settings > SMTP**

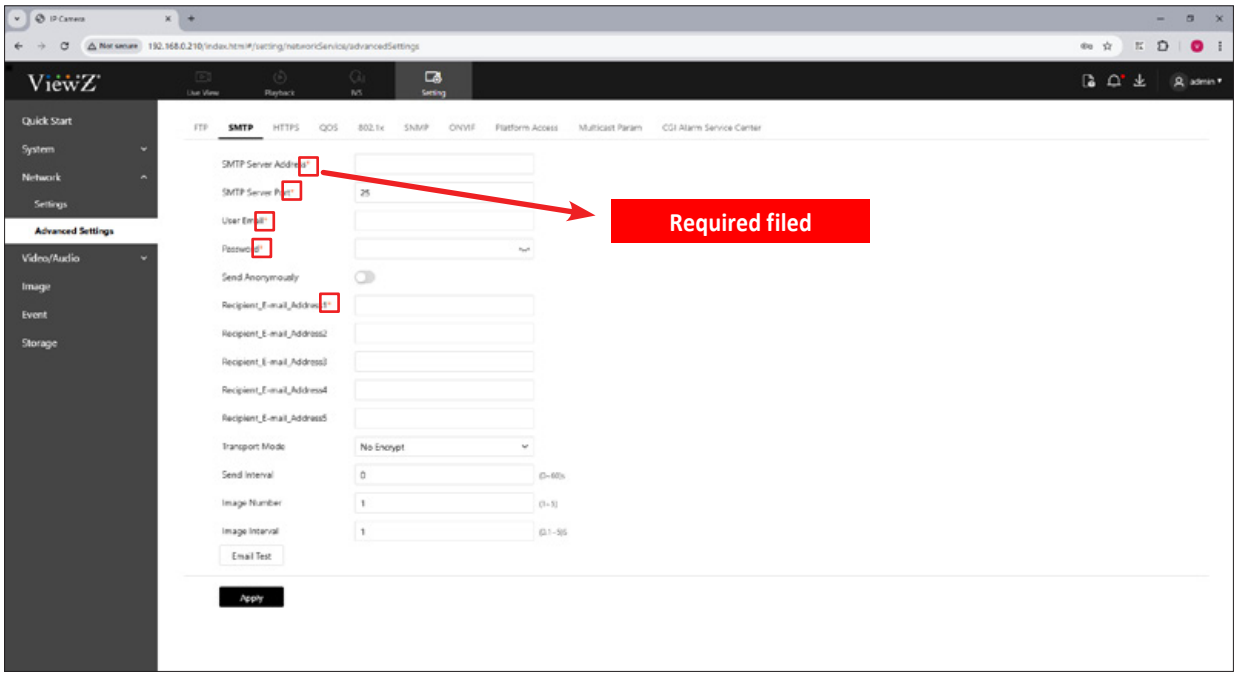


Figure 5-7 SMTP

Step 2 Set **SMTP** parameters as shown in Table 5-7.

SETTING / NETWORK

7. Setup Advanced Settings - SMTP

Procedure

Table 5-7 SMTP Parameters

Parameter	DESCRIPTION	Setting
SMTP Server Address	Type IP address of the SMTP server	Default Value: Blank
SMTP Server Port	Type Port number of the SMTP server	Default Value: 25
User Name	Type User name of the mailbox for sending emails	Default Value: Blank
Password	Type Password of the mailbox for sending emails	Default Value: Blank
Send Anonymously	Send email as anonymous name	Default Value: Blank
Recipient E-mail Address1	Email address of 1st recipient	Default Value: Blank
Recipient E-mail Address2	Email address of 2nd recipient	Default Value: Blank
Recipient E-mail Address3	Email address of 3rd recipient	Default Value: Blank
Recipient E-mail Address4	Email address of 4th recipient	Default Value: Blank
Recipient E-mail Address5	Email address of 5th recipient	Default Value: Blank
Transport Mode	Email encryption mode. Set this parameter based on the encryption modes supported by the SMTP server	Default Value: No Encrypt No Encrypt, SSL, STARTTLS
Send Interval	Set the interval time of sending email	Default Value: 0 sec (0 ~ 60)
Image Number	Type the number of images which will be sent	Default Value: 1 (1 ~ 5)
Image Interval	Set the interval time of capturing image	Default Value: 1 sec (0.1 ~ 5)

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / NETWORK

8. Setup Advanced Settings - HTTPS

Description

If user wants to access the web controller via HTTPS, user need to set the port number.
As an example, if user turn on HTTPS, setup the IP address as 192.168.0.120 & the port number as 443, then user can access the web controller via “https://192.168.0.120:443”, as shown in Figure 5-8.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Advanced Settings > HTTPS**

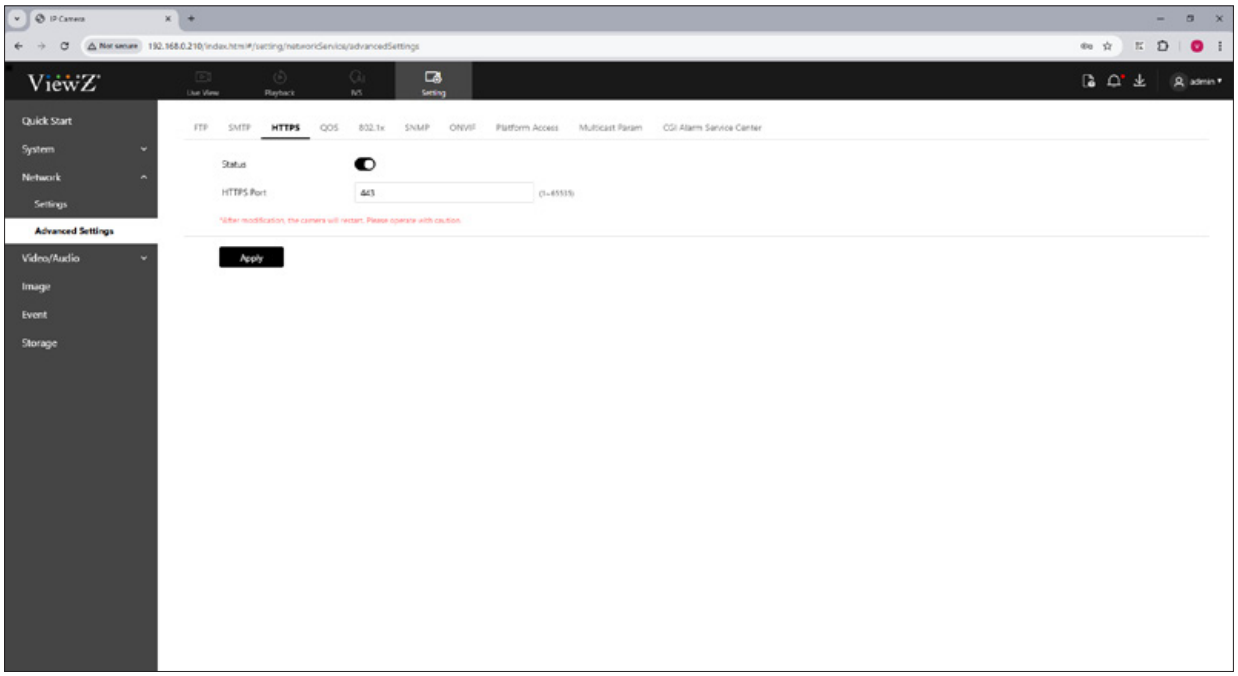


Figure 5-8 HTTPS

Step 2 Click **Status** to enable setup HTTPS port number.

Step 3 Type the port number on HTTPS port tab - 1 ~ 65535. The default value is 443.

SETTING / NETWORK

9. Setup Advanced Settings - QOS

Description

If the device is connected to a router or switch with a QOS function, and the priority rule of the corresponding mark is configured on the network device, the network device will preferentially pass the data packet of the corresponding mark, as shown in Figure 5-9.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Advanced Settings > QOS**

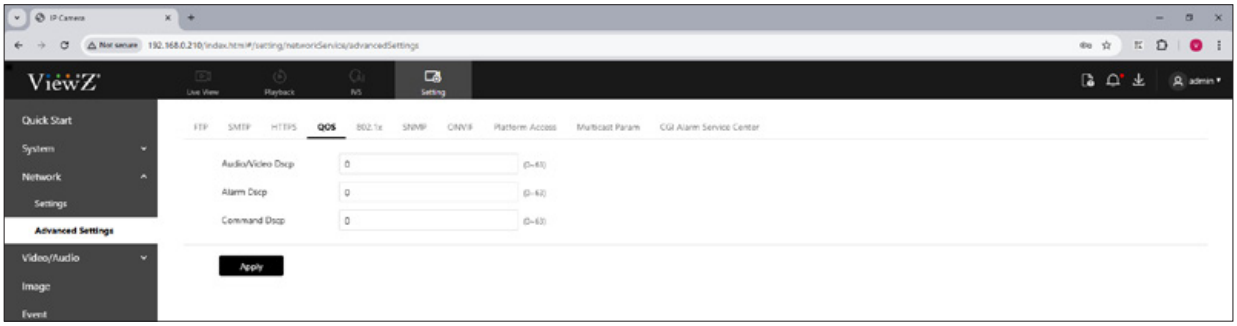


Figure 5-9 QoS

Step 2 Set **QOS** parameters as shown in Table 5-8.

Table 5-8 QOS Parameters

Parameter	DESCRIPTION	Setting
Audio/Video DSCP	Classify & manage the network traffic of AI PVM's audio/video data	Default Value: 0 (0 ~ 63)
Alarm DSCP	Classify & manage the network traffic of AI PVM's alarm data	Default Value: 0 (0 ~ 63)
Command DSCP	Classify & manage the network traffic of AI PVM's command data	Default Value: 0 (0 ~ 63)

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

Note

- Differentiated Services Code Point (DSCP) is used to classify data packets and manage network traffic based on their importance or service requirements.

SETTING / NETWORK

10. Setup Advanced Settings - 802.1x

Description

The 802.1x authentication must be configured on the device port. Authentication of user devices connected to the port is used to control access to network resources, as shown in Figure 5-10.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Advanced Settings > 802.1x**

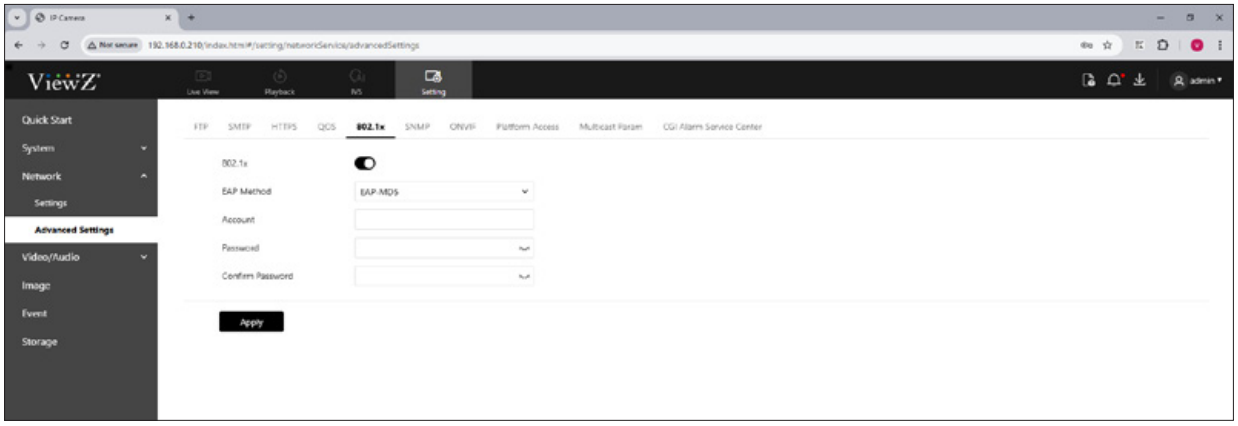


Figure 5-10 802.1x

Step 2 Click **802.1x** button to enable 802.1x.

Step 3 Select the **EAP** Method (Extensible Authentication Protocol) from drop-down list. **EAP-MD5** or **EAP-TLS** can be chosen.

Step 4 Type the **Account** (username) and **Password**/**Confirm Password**.

Step 5 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / NETWORK

11. Setup Advanced Settings - SNMP

Description

Simple Network Management Protocol (**SNMP**) is an Internet Standard protocol, supports SNMP v1, SNMPv2c and SNMPv3 network protocol. Choose the proper SNMP protocol version and set the SNMP protocol parameter to collect and organize information about managed devices on IP networks, as shown in Figure 5-11.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Advanced Settings > SNMP**

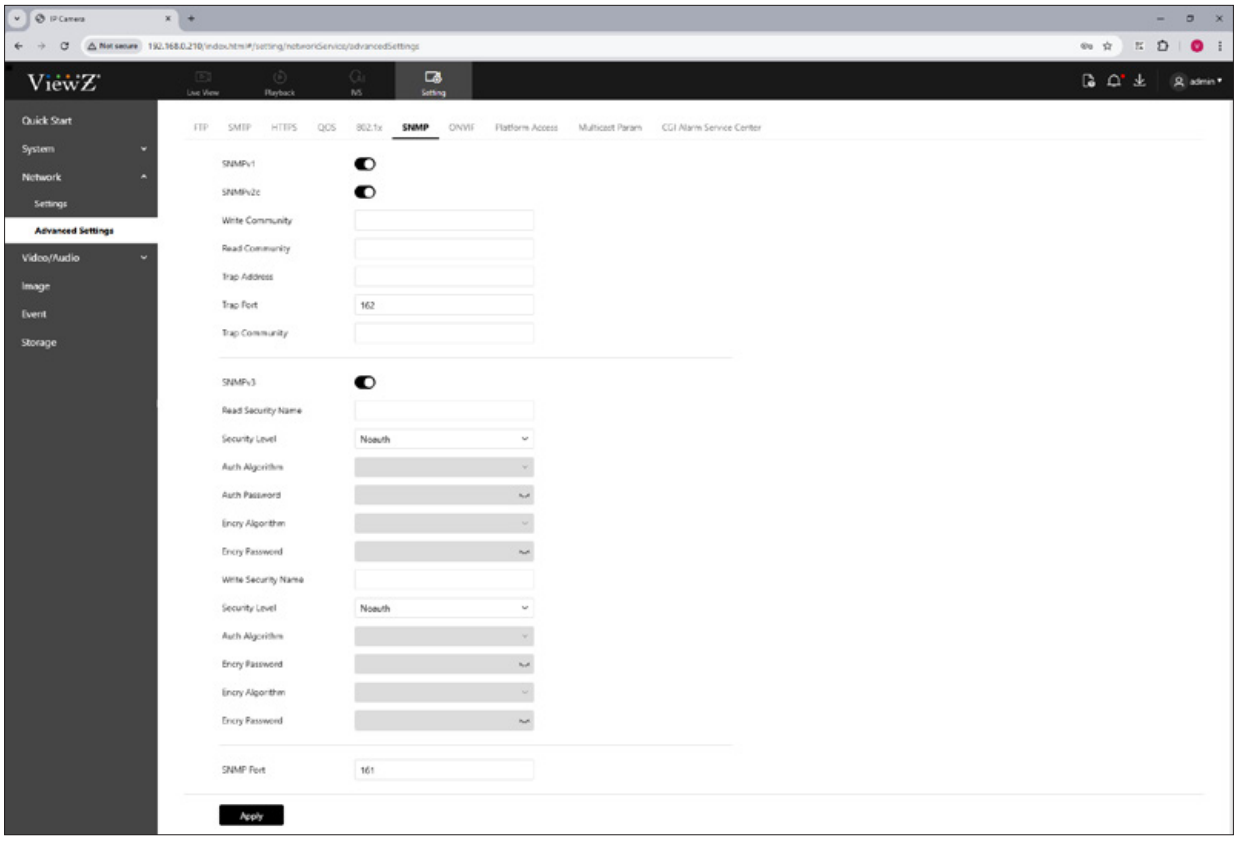


Figure 5-11 SNMP

Step 2 Click the **SNMPv1**, **SNMPv2C** and **SNMPv3** button to enable SNMPv1, SNMPv2C and SNMPv3

Step 3 Set **SNMP** parameters as shown in Table 5-9.

SETTING / NETWORK

11. Setup Advanced Settings - SNMP

Procedure

Table 5-9 SNMP Parameters

Parameter	DESCRIPTION	Setting
SNMPv1/SNMPv2c	Version of SNMP. SNMPv1 and SNMPv2c use communities to establish trust between managers and agents. Agents support three community names, write community, read community and trap.	Default Value: OFF
Write Community	Name of write community. The write community only can modify data	Default Value: Blank
Read Community	Name of read community. The write community only can read data	Default Value: Blank
Trap Address	IP address of the trap	Default Value: Blank
Trap Port	Management port of accepting message from trap	Default Value: Blank
Trap Community	Community string of trap. The trap community string allows the manager to receive asynchronous information from the agent.	Default Value: Blank
SNMPv3	Version of SNMP. SNMPv3 uses community strings, but allows for secure authentication and communication between SNMP manager and agent	Default Value: OFF
Read Security Name	Name of read security	Default Value: Blank
Write Security Name	Name of write security	Default Value: Blank
Security Level	Security Level between SNMP manager and agent, includes three levels: No auth: No authentication and no encryption Auth Password: Authentication but no encryption Priv: Authentication and encryption	Default Value: Noauth Noauth, Auth Password, Priv

SETTING / NETWORK

11. Setup Advanced Settings - SNMP

Procedure

Table 5-9 SNMP Parameters

Parameter	DESCRIPTION	Setting
Auth Algorithm	Authentication Algorithm, includes MD5 and SHA **NOTE** When user select '**Auth Password**', Auth Algorithm & Auth Password will be enabled	Default Value: Blank
Auth Password	Authentication password	Default Value: Blank
Encrypt Algorithm	Encryption Algorithm, includes DES and AES. **NOTE** When user select '**Priv**', Encrypt Algorithm & Password will be enabled	Default Value: Blank
Encrypt Password	Encryption password	Default Value: Blank
SNMP Port	Port of SNMP	Default Value: 161

Step 4 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

Note

- The feature & description of **Write Security Name** is same with **Read Security Name**.

SETTING / NETWORK

12. Setup Advanced Settings - Onvif

Description

When an ONVIF-compliant device connects to the platform, you must authenticate the user name and password to ensure the connection security, as shown in Figure 5-12.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Advanced Settings > Onvif**

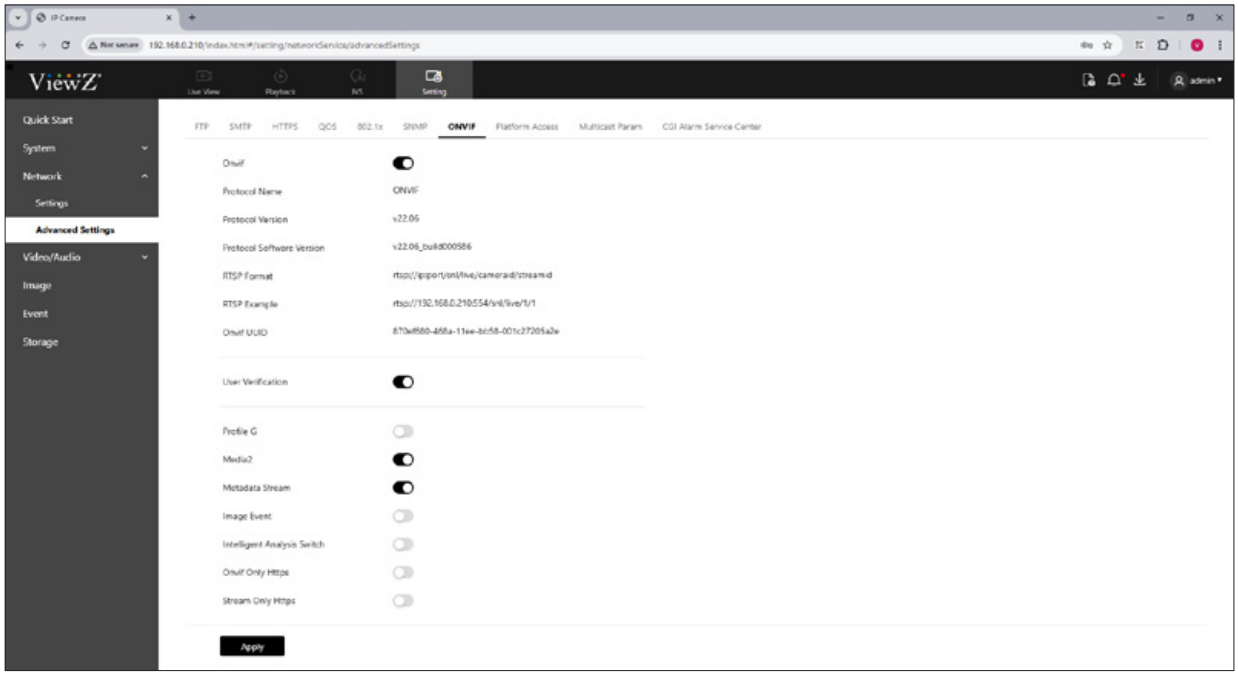


Figure 5-12 Onvif

Step 2 Click the **Onvif** button to enable Onvif

Step 3 Set **Onvif** parameters as shown in Table 5-10.

SETTING / NETWORK

12. Setup Advanced Settings - Onvif

Procedure

Table 5-10 Onvif Parameters

Parameter	DESCRIPTION	Setting
Protocol Name	Type of the access protocol	N/A
Protocol Version	Version number of the access protocol	N/A
Protocol SW Ver.	Software version number of the access protocol	N/A
RTSP Format	URL rule of Real Time Streaming Protocol	N/A
RTSP Example	URL example of Real Time Streaming Protocol	N/A
Onvif UUID	Universally Unique Identifier	N/A
User Verification	When user selects the User Verification check box, the user name and password must be the same as those for logging in to the device web page. **NOTE** When an ONVIF-compliant device connects to the platform, you must authenticate the user name and password to ensure the connection security.	Default Value: ON
Profile G	Enable Onvif profile G	Default Value: OFF
Media 2	Enable Media 2	Default Value: ON
Metadata Stream	Enable Metadata Stream	Default Value: ON
Image Event	Enable Image Event	Default Value: OFF
Intelligent Analysis Switch	Enable active Onvif	Default Value: OFF
Onvif only Https Event only Https	Onvif can use a more secure HTTPS mode for connection, command interaction and video data transmission, which are transmitted in an encrypted way to enhance network security	Default Value: OFF

Step 4 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / NETWORK

13. Setup Advanced Settings - Platform Access

Description

If the AI PVM and platform system are not at the same local network, you can connect device and platform system to the external server. You should build a server for platform in advance, platform's remote IP/Port and IP camera are mapping port to external network, as shown in Figure 5-13.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Advanced Settings > Platform Access**

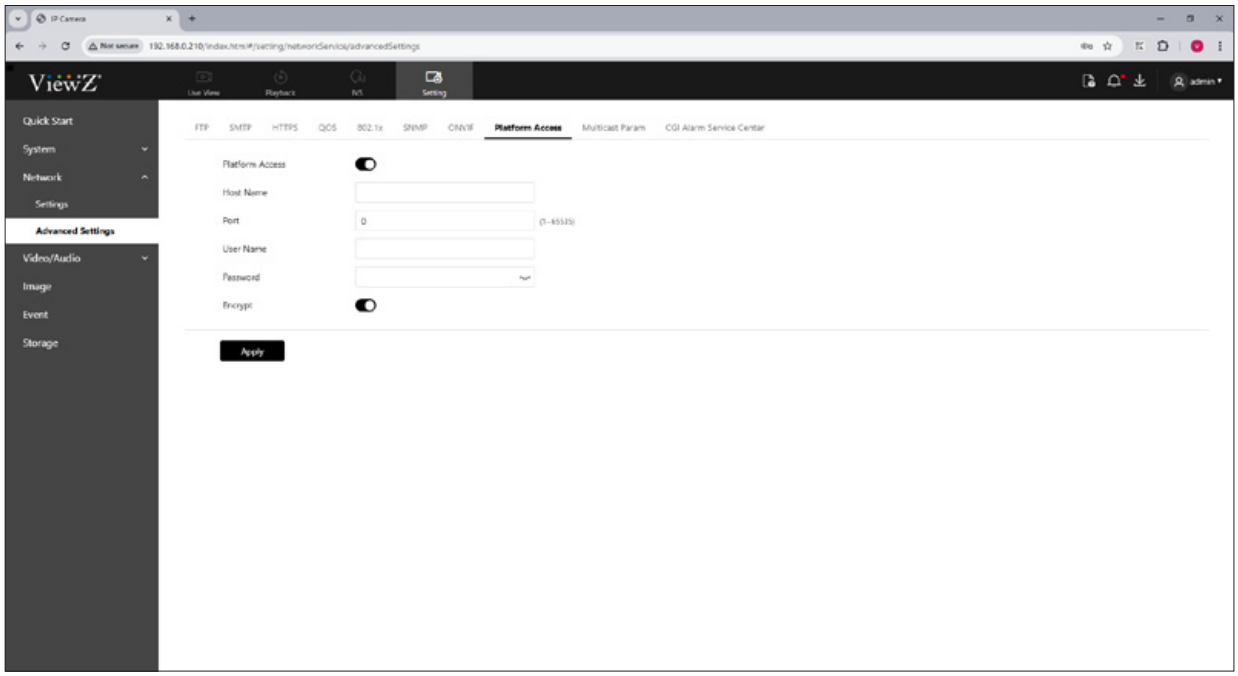


Figure 5-13 Platform Access

Step 2 Click the **Platform Access** button to enable Platform Access

Step 3 Set **Platform Access** parameters as shown in Table 5-11.

SETTING / NETWORK

13. Setup Advanced Settings - Platform Access

Procedure

Table 5-11 Platform Access Parameters

Parameter	DESCRIPTION	Setting
Host Name	HTTP/HTTPS web address of ViewZ IMS server	Default Value: Blank
Port Number	The port number of ViewZ IMS server	Default Value: 0 (1 ~ 65535)
User Name	The user name of ViewZ IMS server	Default Value: Blank
Password	The password of ViewZ IMS server	Default Value: Blank
Encrypt	Enable/disable the connect encryption	Default Value: OFF

Step 4 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

Note

- This feature is only available when using ViewZ IMS program.
- This feature is specifically designed when ViewZ IMS server and AI PVMs are located on the different network or location. Both ViewZ IMS server and AI PVM should be connected on the Internet.
- This feature shuold be cooperated with the setup of ViewZ IMS program.

SETTING / NETWORK

14. Setup Advanced Settings - Multicast Parameters

Description

You can setup multicast stream ID, video port, audio port and source port in multicast parameter page, as shown in Figure 5-14.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Advanced Settings > Multicast Parameters**

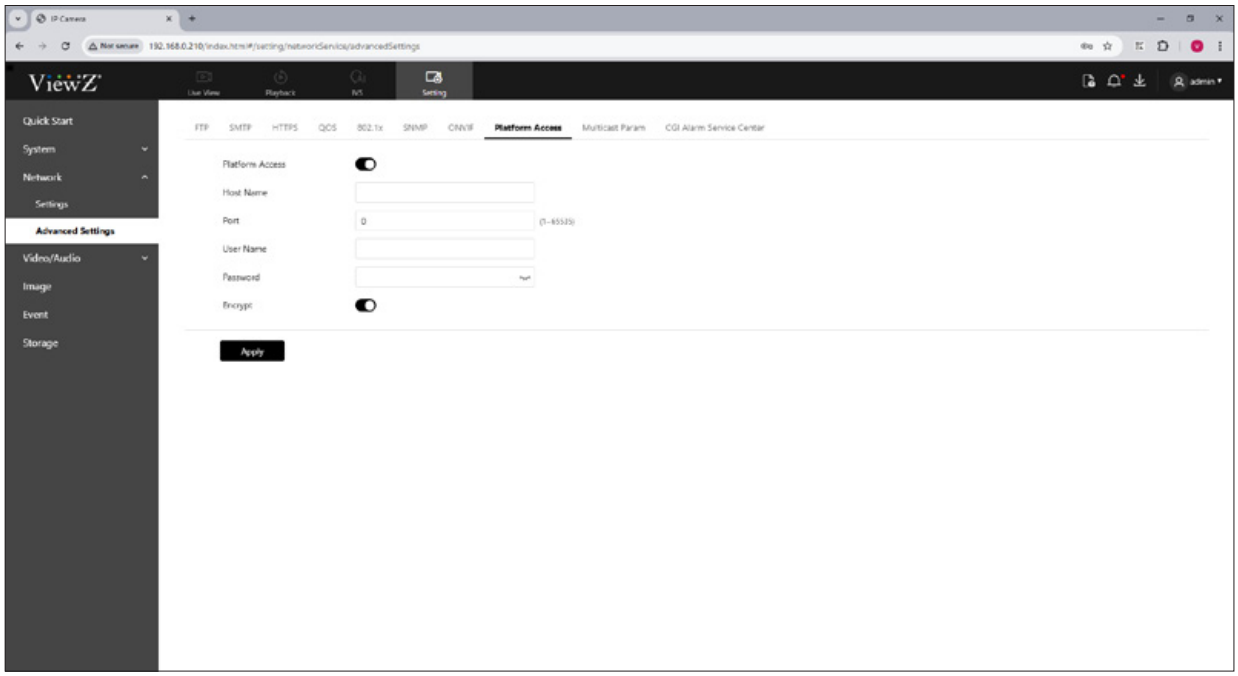


Figure 5-14 Multicast Parameters

Step 2 Set **Multicast** parameters as shown in Table 5-12.

SETTING / NETWORK

14. Setup Advanced Settings - Multicast Parameters

Procedure

Table 5-12 Multicast Parameters

Parameter	DESCRIPTION	Setting
Stream ID	ID of Stream	Default Value: 1
Video Port	Port that receives video data	Default Value: 25330
Video Address	IP address that receives multicast data	Default Value: 238.255.255.255
Audio Port	Port that receives audio data	Default Value: Blank
Audio Address	IP address that receives multicast data	Default Value: Blank
Source Port	Port that receives source data	Default Value: 25530
Source Address	IP address that receives multicast data	Default Value: 238.255.255.255

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / NETWORK

15. Setup Advanced Settings - CGI Alarm Service Center

Description

ViewZ AI PVM can push the alarm message by CGI with Start URL and End URL, and send data to CGI Server via HTTP protocol. CGI alarm message is composed by the head of User-Agent of HTTP. Because HTTP protocol can get and send the data to CGI Server. Therefore, to integrate CGI alerts, user needs to parse the User-Agent field in the HTTP URL to get the alert information, as shown in Figure 5-15.

Procedure

Step 1 Click **Setting** on the top menu, **Network > Advanced Settings > CGI Alarm Service Center**

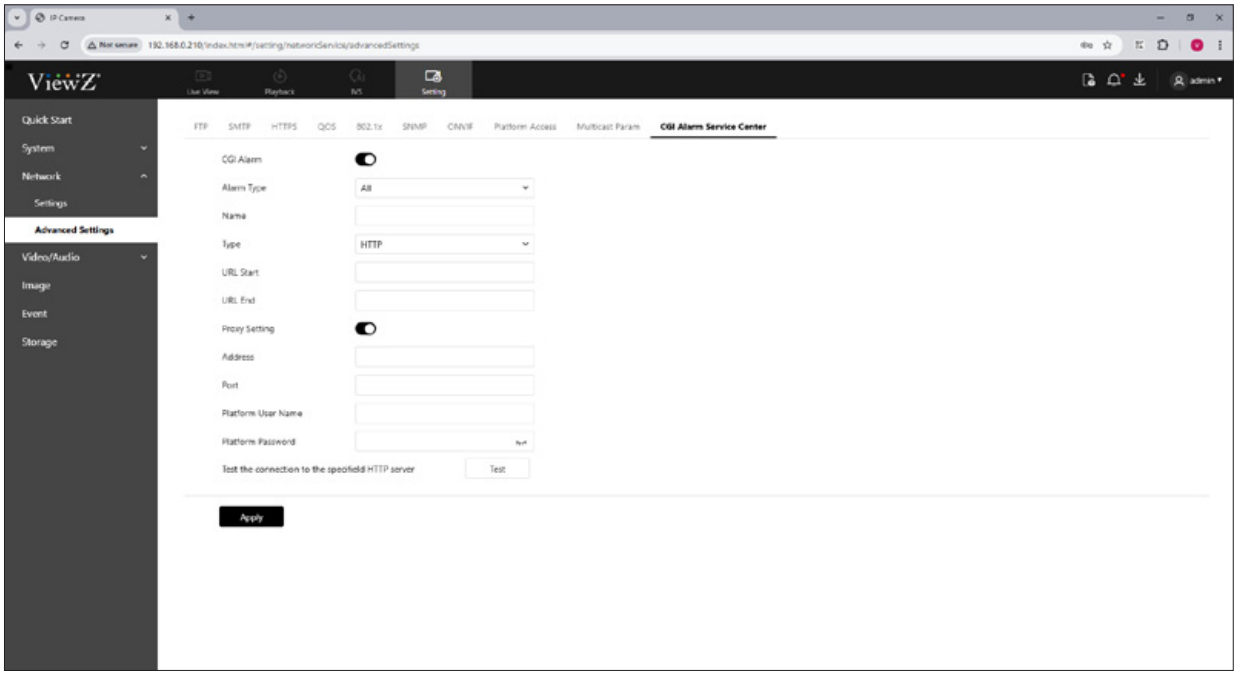


Figure 5-15 CGI Alarm Service Center Parameters

Step 2 Set **CGI Alarm Service Center** parameters as shown in Table 5-13.

Note

- CGI Alarm Service function is mainly using for alarm transmission. If user has user's own server which supports http protrocol, user can integrate ViewZ's CGI Alarm Service into user's server according to ViewZ CGI alarm format so that user can receive the alarm notifications on user's server. Please refer to page 60 and 61.

SETTING / NETWORK

15. Setup Advanced Settings - CGI Alarm Service Center

Procedure

Table 5-13 CGI Alarm Service Center Parameters

Parameter	DESCRIPTION	Setting
CGI Alarm	Enable/disable CGM Alarm	Default Value: OFF
Alarm Type	All alarm types can be chosen, users can choose one to alarm, or choose all.	Default Value: All Temp Threshold Warning, Temp Threshold Alarm, Motion Alarm, Temp Diff Warning
Name	Name of CGI Alarm	Default Value: Blank
Type	Type of CGI Alarm	Default Value: HTTP
URL Start	Push the alarm message by CGI with start URL	Default Value: Blank
URL End	Push the alarm message by CGI with end URL	Default Value: Blank
Proxy Setting	Enable/disable the Proxy connection setup. User can setup the forwarder server of CGI alarm	Default Value: OFF
Address	IP address of Forwarder server (or ViewZ IMS Server)	Default Value: Blank
Port	Port of Forwarder server (or ViewZ IMS Server)	Default Value: Blank
Platform UserName	User Name of Forwarder server (or ViewZ IMS Server)	Default Value: Blank
Platform Password	Password of Forwarder server (or ViewZ IMS Server)	Default Value: Blank
Test	User can test the successful connection to proxy server (or ViewZ IMS Server)	N/A

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

Note

- The example of **URL Start** is *http://XXX.XXX.XXX.XXX:80/MajorAlarmType & MinorAlarmType & SourceName & DeviceID & DeviceIP & AlarmTime & Description*
- The example of **URL End** is *http://XXX.XXX.XXX.XXX:80/MajorAlarmType & MinorAlarmType & SourceName & DeviceID & DeviceIP & AlarmTime & Description*

SETTING / NETWORK

15. Setup Advanced Settings - CGI Alarm Service Center

Procedure

Note

- When AI PVM sends CGI alarm, there are major and minor alarm types. It means each alarm has its own priority when sending alarm signal.

Alarm Types on all alarms of AI PVM

► **Major Alarm Type**
1) **Security Alarm**
► **Minor Alarm Type**
1) **IO Alarm**: Alarm input connects with GND when set to normal open; or alarm input disconnects from GND when set to normal close.
2) **Motion Alarm**: Motion detection alarm
3) **Network Disconnection Alarm**: When camera drops offline (disconnects from network), it will send alarm once the network is recovered.
4) **Abnormal Noise Alarm** (applicable for models with microphone): A sudden increase of noise or sound nearby the camera.

Alarm Types with SD Card

► **Major Alarm Type**
1) **SD Card Alarm**
► **Minor Alarm Type**
1) **SD Card Full**, 2) **SD Card not installed**, 3) **SD Card not formatted**

Alarm Types on IVS

► **Major Alarm Type**
1) **Intelligent Analysis Alarm**
► **Minor Alarm Type**
1) **Line Crossing Alarm**: Someone/something goes cross the line that user draws on the video.
2) **Intrusion Alarm**: Someone/something breaks into the area that user draws on the video.
3) **Double Line Crossing Alarm**: Someone/something goes cross the two lines in sequence that the user draws on the video.
4) **Multi Loiter Alarm**: Someone/something suspected loiters in the area that user draws on the video.
5) **Wrong Direction Alarm**: Someone/something move against the direction that user draws on the video.

Alarm Types on Temperature

► **Major Alarm Type**
1) **Temperature Alarm**
► **Minor Alarm Type**
1) **Temperature Threshold Warning**, 2) **Temperature Threshold Alarm**
3) **Temperature Difference Warning**, 4) **Temperature Difference Alarm**

SETTING / VIDEO/AUDIO

1. Setup VIDEO

Description

Video refers to the continuous transmission of live video data from a camera to a device, network, or platform over the Internet or a local network, as shown in Figure 6-1.

Procedure

Step 1 Click **Setting** on the top menu, **Video/Audio > Video > Video**

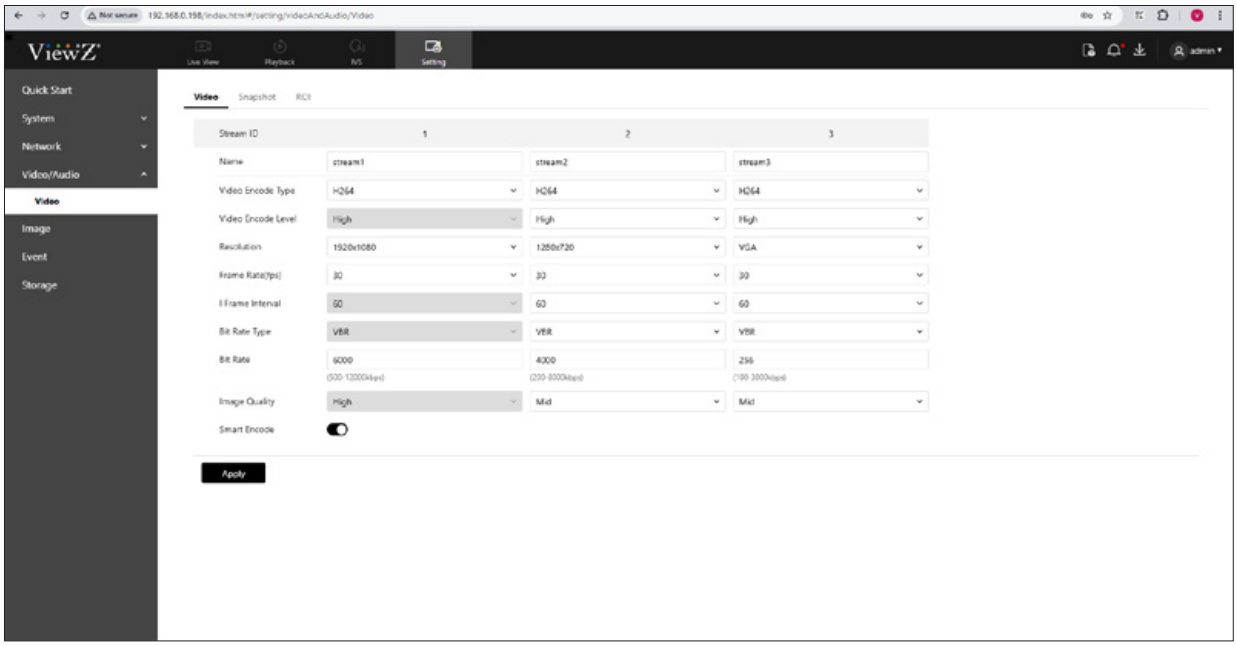


Figure 6-1 Video

Step 2 Set **Video** parameters as shown in Table 6-1.

SETTING / VIDEO/AUDIO

1. Setup VIDEO

Procedure

Table 6-1 Video Parameters

Parameter	DESCRIPTION	Setting
Stream ID	The device supports 3 streams and **Stream 1** & **2** can use H.264 code. - **Stream 1** stands for the best stream performance of the device supports - **Stream 2** offers comparatively low-resolution options - **Stream 3** is the lowest resolution. Some models may only have 2 streams	N/A
Name	Stream name which can consist of character, number underline. The value cannot exceed 32 bytes.	Default Value: stream1
Video Encode Type	The video encode determines the image quality and network bandwidth required by a video. User can select one among MJPEG, H.265 & H.264	Default Value: H.264

Note

- MJPEG - MJPEG is a standard intra-frame compression encode. The compressed image quality is good. No mosaic is displayed on motion images. MJPEG does not support proportional compression and requires large storage space. Recording and network transmission occupy large hard disk space and bandwidth. MJPEG is not applicable to continuous recording for a long period of time or network transmission of videos. It can be used to send alarm images.
- H.264 - H.264 consists of H.264 low Profile, H.264 Main Profile and H.264 High profile. The performance of H.264 High Profile is higher than that of H.264 Main Profile, and the performance of H.264 Main Profile is higher than that of H.264 Base Profile. If a hardware decoding device is used, select the appropriate encode based on the decoding performance of the device. H.264 High Profile has the highest requirements on the hardware performance, and H.264 Base Profile has the lowest requirements for the hardware performance.
- H.265 - H.265 is the advanced video encoding standard. It's the improvement standard from H.264. H.265 improves the streams, encoding quality and algorithm complexity to make configuration optimization.

SETTING / VIDEO/AUDIO

1. Setup VIDEO

Procedure

Table 6-1 Video Parameters

Parameter	DESCRIPTION	Setting
Resolution	A higher resolution means better image quality **NOTE** The variation of resolution is based on the IP camera model	Default Value: 1920 x1080 1920 x1080, 1280x720, D1, VGA, 640x360, CIF, QVGA
Frame Rate (fps)	Frame rate is the number of images, snapshots or frames that a camera can take per second. The frames per second determine the smoothness of a video. A video, which frame rate is higher than 22.5 (22.5 f/s), is considered as smooth by human eyes. Frame rates for different frequencies are as follows: 50 Hz: 1 ~ 25 f/s | 60 Hz: 1 ~ 30 f/s **NOTE** The frequency is set on the Device Configuration > Camera page. The biggest MJPEG coding format frame rate is 12 frames per second.	Default Value: 30 (1 ~ 30)
Bit Rate Type	The bit rate is the number of bits transmitted per unit of time. The following bit rate types are supported but higher bandwidth. **Constant bit rate (CBR)** - The compression speed is fast; however, improper bit rate may cause vague motion images. **Variable bit rate (VBR)** - The bit rate changes according to the image complexity. The encoding efficiency is high and the definition of motion images can be ensured.	Default Value: VBR

SETTING / VIDEO/AUDIO

1. Setup VIDEO

Procedure

Table 6-1 Video Parameters

Parameter	DESCRIPTION	Setting
Bit Rate Range	Setup the number of frames between 2 consecutive Intra-Frames is referred to as I-Frame Intervals.	Default Value: 60 (1 ~ 90)
Bit Rate Range	Indicates the maximal value of the bit rate. The different models may have different ranges, please refer to actual product	Default Value: 6000 (100 ~ 12000kbps)
Image Quality	The video quality of camera output User can select one of High, Mid, Low, Lower & Lowest	Default Value: High
Smart Encode	Enable/disable smart encode on stream 1 • Smart encode includes H.264 & H.265. • The storage space will be reduced 50 % when smart encode is enabled. • Only main stream supports smart encode.	N/A

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / VIDEO/AUDIO

2. Setup Snapshot

Description

Snapshot allows the camera to capture a still image at a specific time interval, as shown in Figure 6-2.

Procedure

Step 1 Click **Setting** on the top menu, **Video/Audio > Video > Snapshot**

Figure 6-2 Snapshot

Step 2 Set **Snapshot** parameters as shown in Table 6-2.

Table 6-2 Snapshot Parameters

Parameter	DESCRIPTION	Setting
Snapshot Resolution	Select a resolution of snapshot	Default Value: 1280x720 1920 x1080, 1280x720, D1, VGA, 640x360, CIF, QVGA
Snapshot Quality	Select a quality of snapshot	Default Value: Mid High, Mid, Low

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / VIDEO/AUDIO

3. Setup ROI

Description

ROI stands for "**Region of Interest**," which refers to a specific area within the camera's view that you can designate to focus on for enhanced monitoring and analysis, allowing the camera to capture higher quality details only from that selected region, while potentially reducing the data needed to transmit from the entire image area, as shown in Figure 6-3.

Procedure

Step 1 Click **Setting** on the top menu, **Video/Audio > Video > ROI**

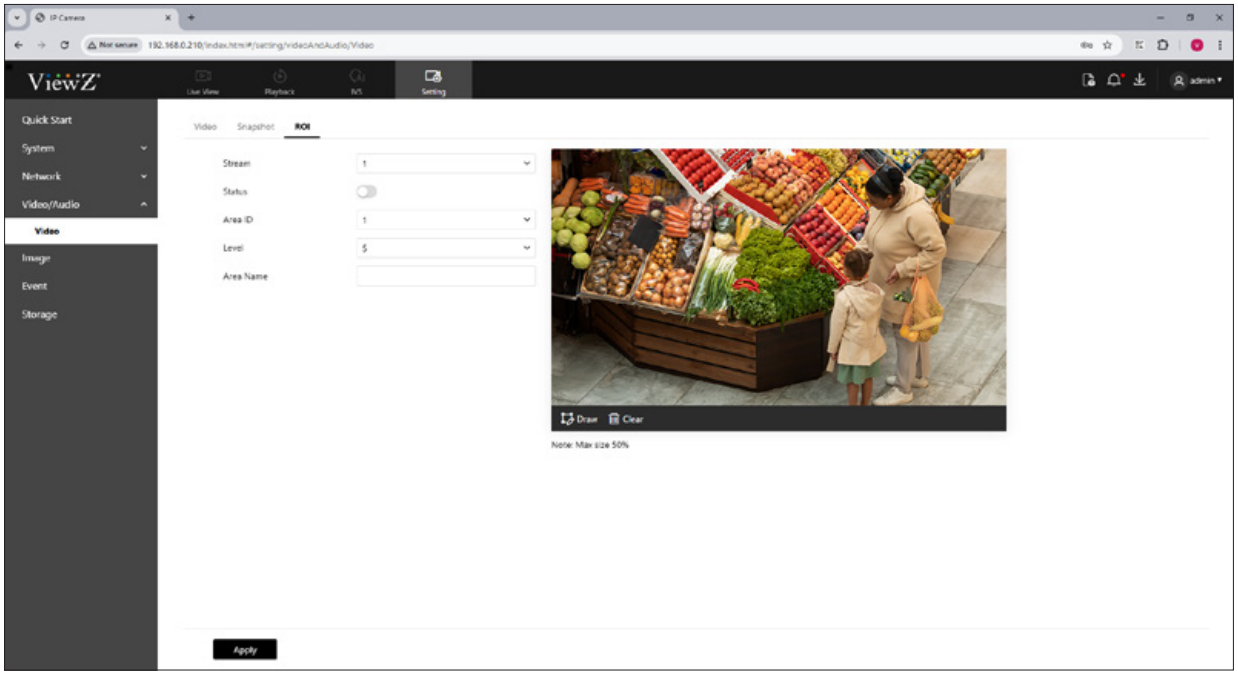


Figure 6-3 ROI

Step 2 Set **ROI** parameters as shown in Table 6-3.

SETTING / VIDEO/AUDIO

3. Setup ROI

Procedure

Table 6-3 ROI Parameters

Parameter	DESCRIPTION	Setting
Stream	Stream ID	Default Value: 1 (1 ~ 3)
Status	Enable/disable the ROI	Default Value: Off
Area ID	Area ID of ROI	Default Value: 1 (1 ~ 8)
Level	The visual effect of ROI. The higher the level is, the clearer the area is; the more blurred outside the area.	Default Value: 5 (1 ~ 5)
Area Name	The marked name used for areas **NOTE** The password value cannot be exceeded over 32 bytes	Default Value: Blank

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / IMAGE

1. Setup Display

Description

The detailed information refers to next chapters as shown in Figure 7-1.

Procedure

Step 1 Click **Setting** on the top menu, **Image > Display**

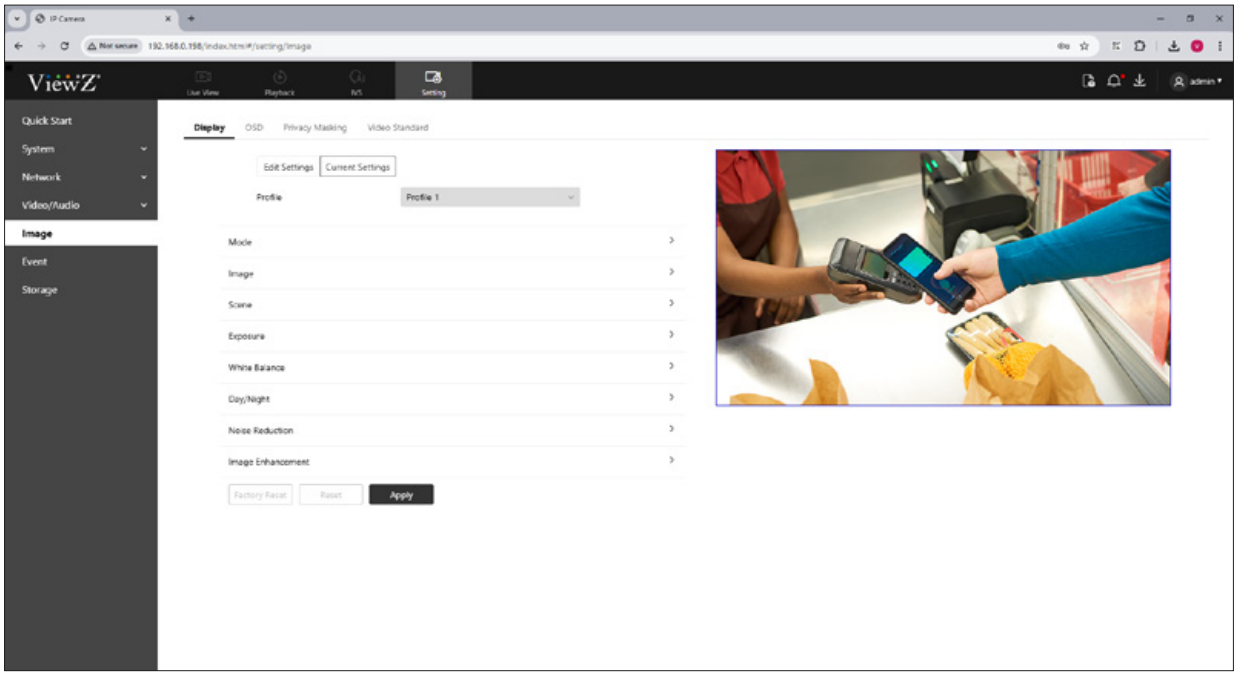


Figure 7-1 Display

Step 2 Select '**Edit Setting**' and '**Profile**' to edit the parameters

Note

- All image settings can be modified on the **Edit Settings** mode. And user can select a profile and make 4 profiles.
- If user click/perform **Factory Reset** button, all parameters of Display will be restored to the factory settings
- If user click/perform **Reset** button, all edited value of Display will be recovered to the last settings

SETTING / IMAGE

2. Setup Display - Mode

Description

The **Mode** refers to a camera that automatically switches between "Day" (color) and "Night" (black and white) modes based on the ambient light levels, as shown in Figure 7-2.

Procedure

Step 1 Click **Setting** on the top menu, **Image > Display > Mode**

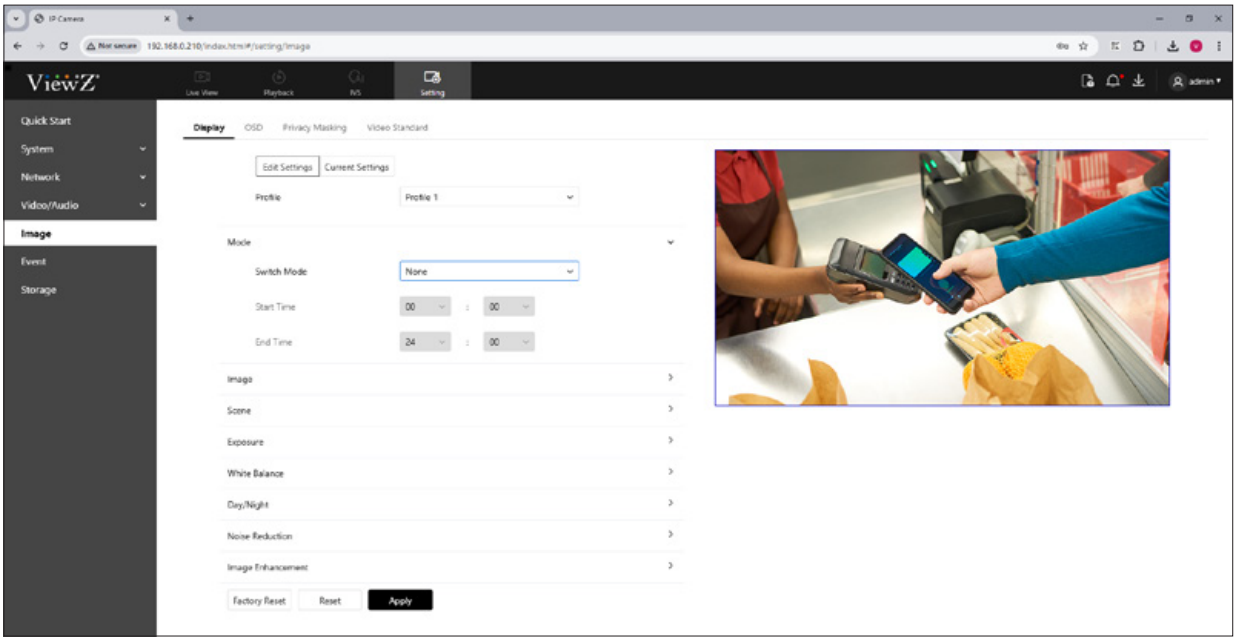


Figure 7-2 Mode

Step 2 Choose a Switch Mode - None, Time Mode, D/N Linkage Mode.

- **Time Mode**: User can setup a profile with Start/End time. Also, if user setup 4 profiles and assign the sequential time table, then, 4 profiles will be sequentially displaying.
- **D/N Linkage Mode**: User can setup the switching time of day & night mode.
- **None**: Display the current profile.

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / IMAGE

3. Setup Display - Image

Description

In a security camera, "brightness" controls the overall lightness or darkness of the image, "saturation" adjusts the intensity of colors, "contrast" defines the difference between light and dark areas, and "sharpness" determines how clearly details and edges are visible in the image, as shown in Figure 7-3.

Procedure

Step 1 Click **Setting** on the top menu, **Image > Display > Image**

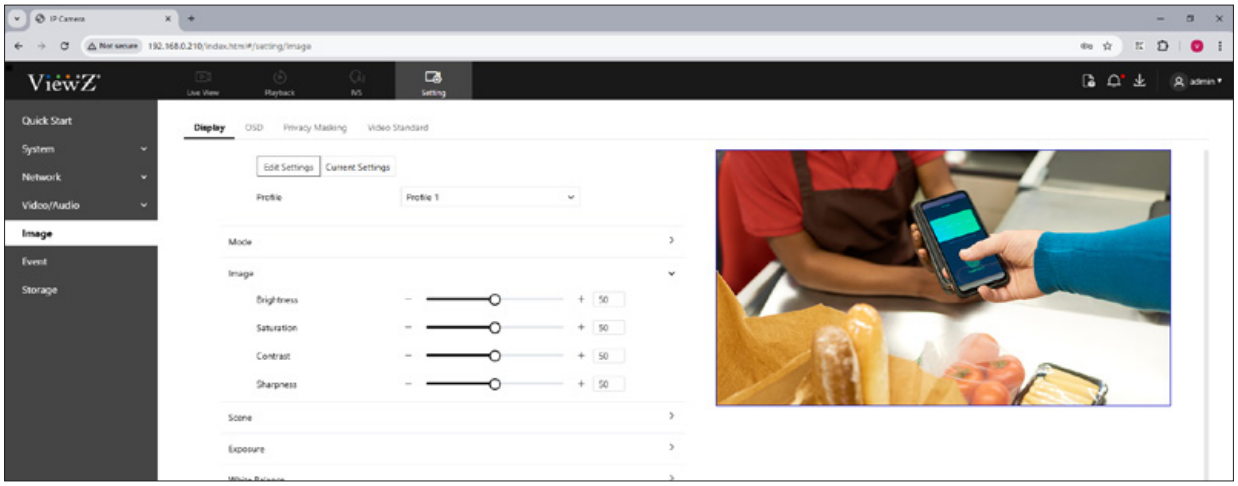


Figure 7-3 Image

Step 2 Set **Image** parameters as shown in Table 7-1.

Table 7-1 Image Parameters

Parameter	DESCRIPTION	Setting
Brightness	Adjust the brightness	Default Value: 50 (0 ~ 100)
Saturation	Adjust the color saturation	Default Value: 50 (0 ~ 100)
Contrast	Adjust the contrast	Default Value: 50 (0 ~ 100)
Sharpness	Adjust the sharpness	Default Value: 50 (0 ~ 100)

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / IMAGE

4. Setup Display - Scene

Description

The Scene mode refers to a preset configuration that adjusts the camera's settings based on a specific situation or time of day, as shown in Figure 7-4.

Procedure

Step 1 Click **Setting** on the top menu, **Image > Display > Scene**

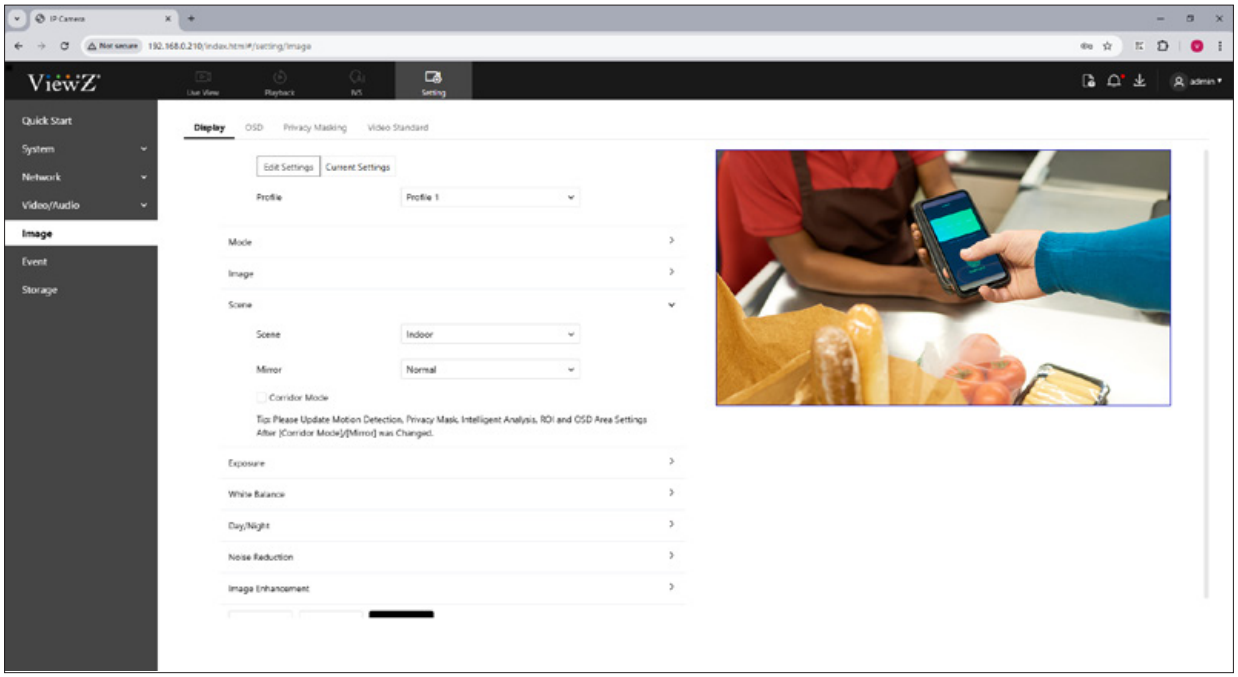


Figure 7-4 Scene

Step 2 Set **Scene** parameters as shown in Table 7-2.

SETTING / IMAGE

4. Setup Display - Scene

Procedure

Table 7-2 Scene Parameters

Parameter	DESCRIPTION	Setting
Scene	It indicates the working mode of camera **Outdoor**: It applies to outdoor scenarios **Indoor**: It applies to indoor scenarios	Default Value: Outdoor
Mirror	It is used to select the pixel location of an image **Normal**: The image does not flip **Horizontal**: The image flips to the left and right **Vertical**: The image flips up and down **Horizontal & Vertical**: The image rotates at 180°	Default Value: Normal
Corridor Mode	The image rotates 90° clockwise when aisle mode is enabled. For some models, when you choose stream 2 or 3, H.265 or H.264 video encode type, resolution chosen CIF or QVGA, it may not play the live video. Please apply this for some models.	Default Value: Disable

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / IMAGE

5. Setup Display - Exposure

Description

The exposure setting on cameras refers to the amount of time the iris will stay open and is exposed to light, as shown in Figure 7-5.

Procedure

Step 1 Click **Setting** on the top menu, **Image > Display > Exposure**

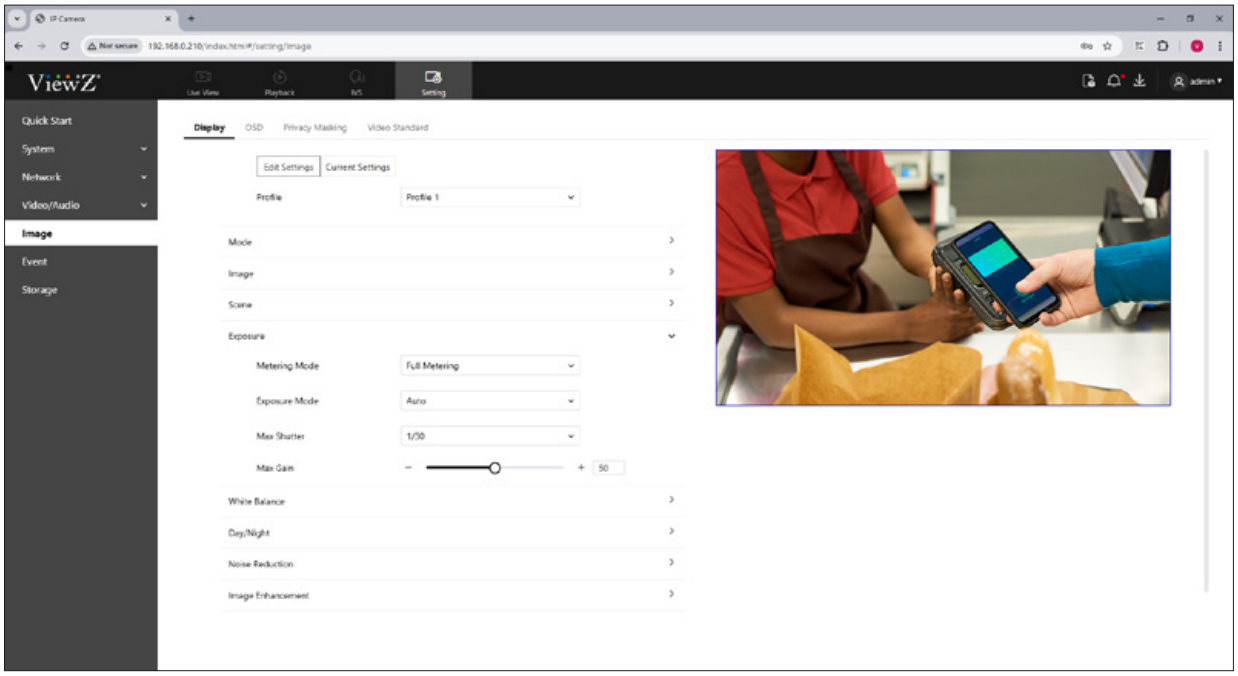


Figure 7-5 Exposure

Step 2 Set **Exposure** parameters as shown in Table 7-3.

SETTING / IMAGE

5. Setup Display - Exposure

Procedure

Table 7-3 Exposure Parameters

Parameter	DESCRIPTION	Setting
Metering Mode	User can choose a metering area. **Full Metering**: During metering, all areas of an image has equal weight, that is, all areas are involved in the metering. **Spot Metering**: During metering, the central spot of an image has the highest weight. **Partial Metering**: During metering, the middle area (1/2 of the total area) of an image has the highest weight, and other areas have the lowest weight.	Default Value: Full Metering
Exposure Mode	The exposure modes include: **Auto**: The system set auto exposure mode based on the monitoring environment. **Manual**: User can adjust the brightness of camera view by setting the following 3 items: **Shutter**, **Iris** and **Gain Setting**. **Shutter Priority**: User can setup **Shutter Setting** to fixed values. The iris and gain are automatically adjusted by the system.	Default Value: Auto
Max Shutter	The device automatically adjusts the shutter time based on the ambient brightness. The shutter time is less than or equal to the value of this parameter	Default Value: 1/30 1/30, 1/60, 1/120, 1/125, 1/150, 1/200, 1/250, 1/500
Max Gain	The device automatically adjusts the gain based on the external light. The gain is less than or equal to the value of this parameter.	Default Value: 50 (0 ~ 100)

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / IMAGE

6. Setup Display - White Balance

Description

White Balance (WB) refers to the color balance of an image, as shown in Figure 7-6.

Procedure

Step 1 Click **Setting** on the top menu, **Image > Display > White Balance**

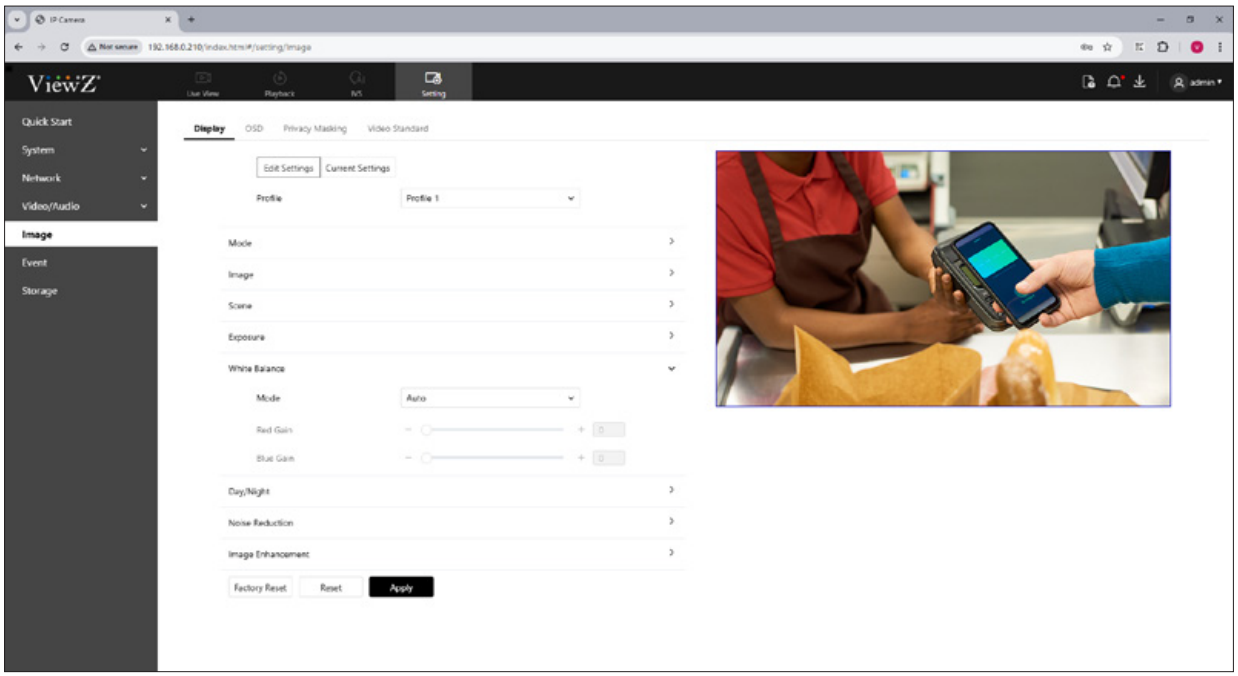


Figure 7-6 White Balance

Step 2 Set **White Balance** parameters as shown in Table 7-4.

SETTING / IMAGE

6. Setup Display - White Balance

Procedure

Table 7-4 White Balance Parameters

Parameter	DESCRIPTION	Setting
Mode	Select **White Balance** (**WB**) mode according to different scenes for better image color reproduction. **Auto**: Automatic **WB** mode, the system automatically performs white balance based on the monitoring environment. **Tungsten**: Camera setting is used to adjust for warm light sources like tungsten light bulbs and candles **Fluorescent**: Compensates for the cool shade of fluorescent light to produce warmer & brighter photos **Daylight**: Camera setting is using for balancing the color temperature of a photo to match the color of natural light during the day **Shadow**: Lighten shadows and darken highlights in camera video **Manual**: Manual **WB** mode, user can manually control the White Balance mode based on the monitoring environment.	Default Value: Auto
Red Gain	It indicates the gain applied to red channels. As the value increases, the color temperature becomes lower.	Default Value: 0 (0 ~ 100)
Blue Gain	It indicates the gain applied to blue channels. As the value increases, the color temperature becomes higher. **NOTE** Red & Blue Gain parameter is valid when Manual Mode is set to Customized.	Default Value: 0 (0 ~ 100)

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / IMAGE

7. Setup Display - Day/Night

Description

The camera fill light has 4 modes, including intelligent dual light (the current fill light will switch to warm light after an alarm is triggered, and switch back to the original fill light for fill light 30s after the alert is released.), warm light, infrared lamp and close (Choose to close the fill light and the color of image will stay in the previous mode). Different cameras can be set in different fill light modes, please set them according to the actual scene.
The brightness of the supplemental light can be set to either automatic or manual. In automatic mode, it adjusts based on the current environment. In manual mode, you can adjust the brightness by dragging the slider or setting a specific value, as shown in Figure 7-7.

Procedure

Step 1 Click **Setting** on the top menu, **Image > Display > Day/Night**

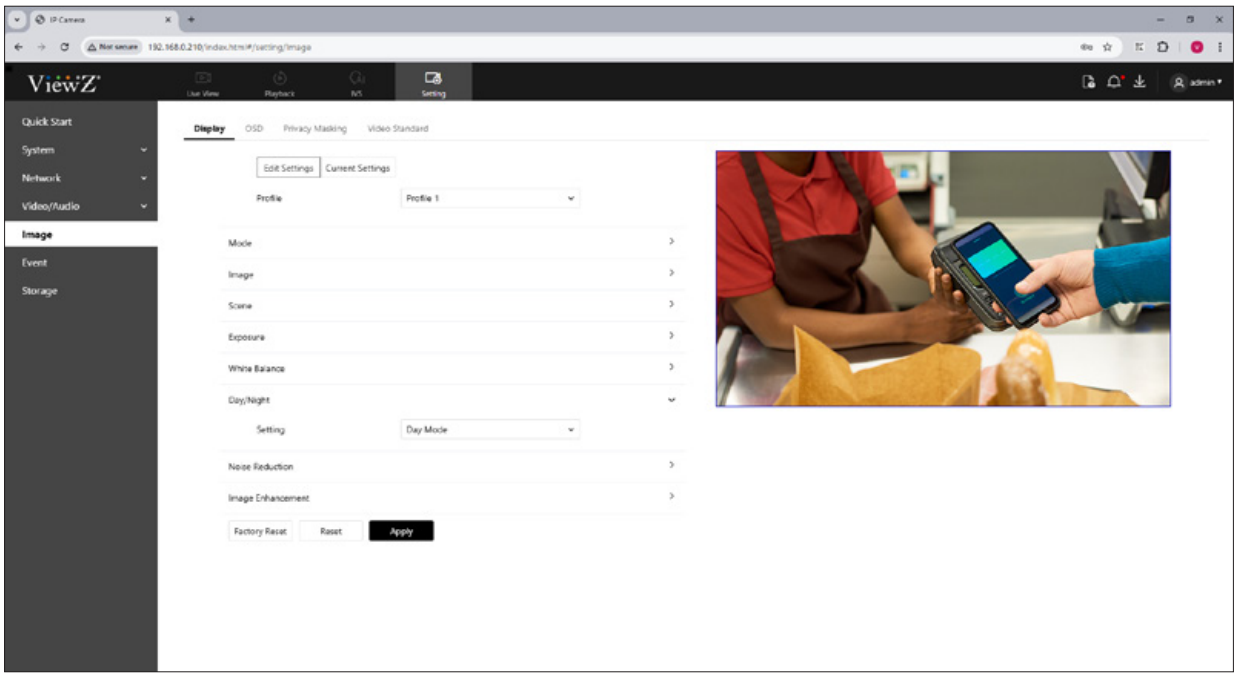


Figure 7-7 Day/Night

Step 2 Set **Day/Night** parameters as shown in Table 7-5.

SETTING / IMAGE

7. Setup Display - Day/Night

Procedure

Table 7-5 Day/Night Parameters

Parameter	DESCRIPTION	Setting
Setting	It can be set to Auto, Day, Night or Timer. **Auto mode**: The image color and filter status are automatically switched based on the ambient brightness. The filter keeps infrared light from reaching the sensor during the day; The filter allows all light to reach the sensor at night. **Day mode**: The image is colored, and the filter is in the day state, preventing infrared light from entering the sensor. **Night mode**: The image is black and white, and the filter is in the night state, allowing infrared light to enter the sensor. **Timer**: Switching between day mode and night mode according to the set time.	Default Value: Auto
Delay(s)	The delay time of day to night or night to day **NOTE** This parameter is valid in auto mode	Default Value: 0 (0 ~ 180)
DTN Time	Time of day mode to night mode	Default Value: 18:00
NTD Time	Time of night mode to day mode	Default Value: 06:00

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / IMAGE

8. Setup Display - Noise Reduction

Description

Noise reduction in security cameras is an image processing technique that removes visible noise from a video signal to improve image quality, as shown in Figure 7-8.

Procedure

Step 1 Click **Setting** on the top menu, **Image > Display > Noise Reduction**

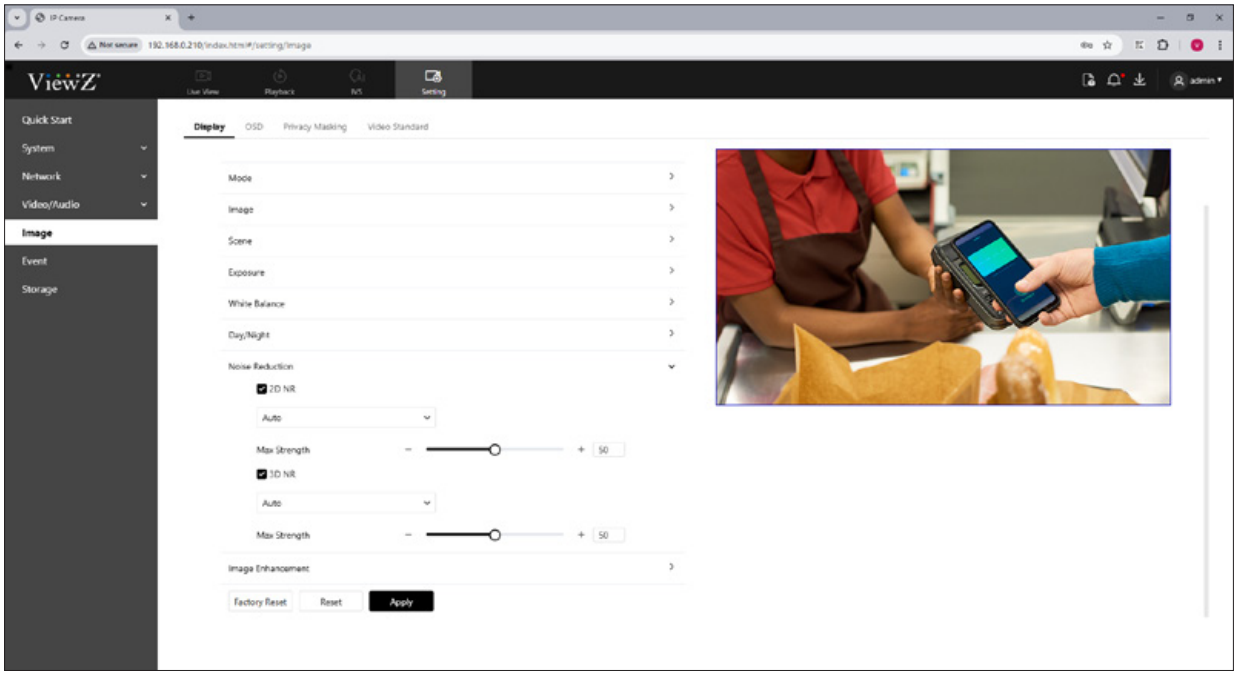


Figure 7-8 Noise Reduction

Step 2 Set **Noise Reduction** parameters as shown in Table 7-6.

SETTING / IMAGE

8. Setup Display - Noise Reduction

Procedure

Table 7-6 Noise Reduction Parameters

Parameter	DESCRIPTION	Setting
2D NR	Reduce noise of image	Default Value: Auto Auto, Manual
3D NR	Reduce noise of image	Default Value: Auto Auto, Manual
Max Strength	It is valid in auto noise filter mode. When the parameter value is 0, the noise filter is disabled. When the parameter value is greater than 0, the noise filter is enabled, and the system automatically adjusts the noise filter level based on the ambient brightness without exceeding the value of this parameter	Default Value: 50 (0 ~ 100)
Fixed Strength	It is valid in a manual noise filter mode	Default Value: 50 (0 ~ 100)

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / IMAGE

9. Setup Display - Image Enhancement

Description

Image Enhancement features that can improve the quality of images captured by security cameras in different lighting conditions, as shown in Figure 7-9.

Procedure

Step 1 Click **Setting** on the top menu, **Image > Display > Image Enhancement**

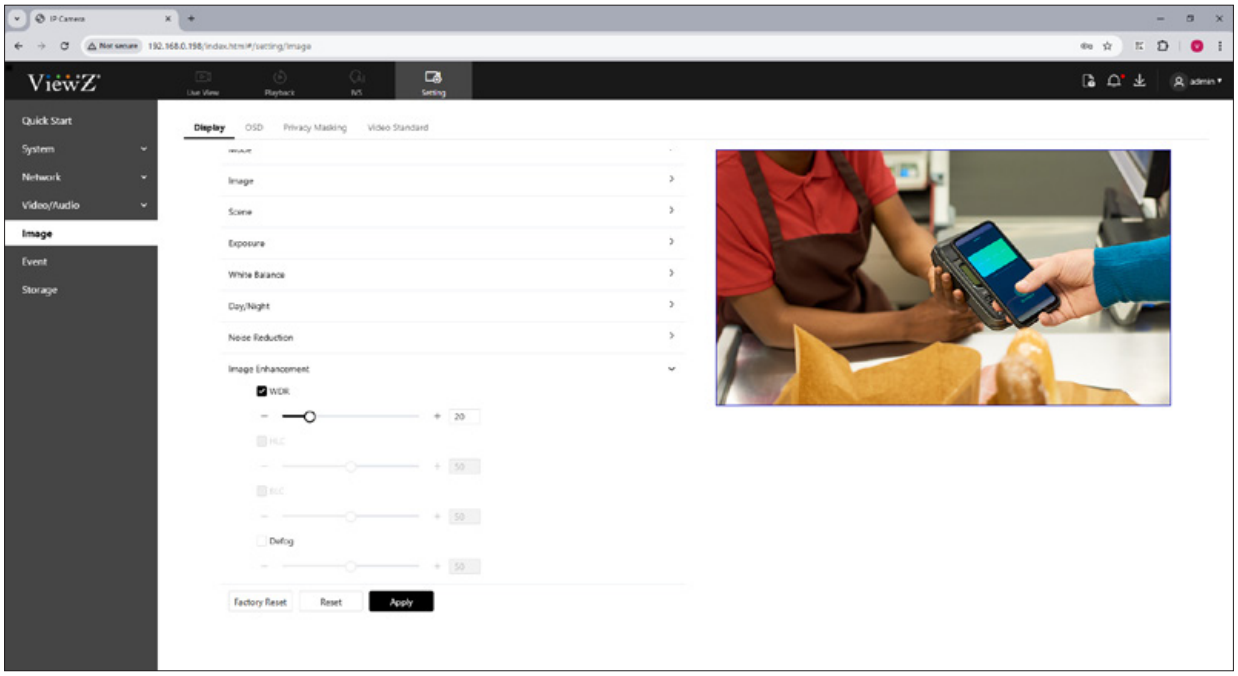


Figure 7-9 Image Enhancement

Step 2 Set **Image Enhancement** parameters as shown in Table 7-7.

SETTING / IMAGE

9. Setup Display - Image Enhancement

Procedure

Table 7-7 Image Enhancement Parameters

Parameter	DESCRIPTION	Setting
WDR	It is used to display the foreground and background at the same time in the environment with a large brightness difference. When the brightness difference is larger, you can increase the **WDR** level to obtain better image effect.	Default Value: 50 (0 ~ 100)
HLC	It provides a clearer view of an image in the highlight environment. When **HLC** is enabled, the total brightness of an image is reduced, allowing you to view objects in front of the highlight.	Default Value: 50 (0 ~ 100)
BLC	It provides a clearer view of an image in the backlight environment. When **BLC** is enabled, the total brightness of an image increases, allowing you to view objects in front of the backlight. Meanwhile, the objects behind the backlight are exposed excessively	Default Value: 50 (0 ~ 100)
DeFog	It provides a clearer view of an image in the fogged environment when **DeFog** is enabled. As the value increases, the image becomes clearer. Only apply for some models.	Default Value: 50 (0 ~ 100)

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

Note

- WDR, HLC & BLC cannot be chosen at the same time

SETTING / IMAGE

10. Setup OSD

Description

The on-screen display (OSD) function allows you to display the device name, channel ID and name, time, and other customized contents on videos. You can drag the OSD frames to anywhere you want to put, as shown in Figure 7-10.

- When the resolution is D1 and CIF, the OSD customized in web interface can show at most 22 words normally.
- The OSD support simplified Chinese, English, digital and some special character only.

Procedure

Step 1 Click **Setting** on the top menu, **Image > OSD**

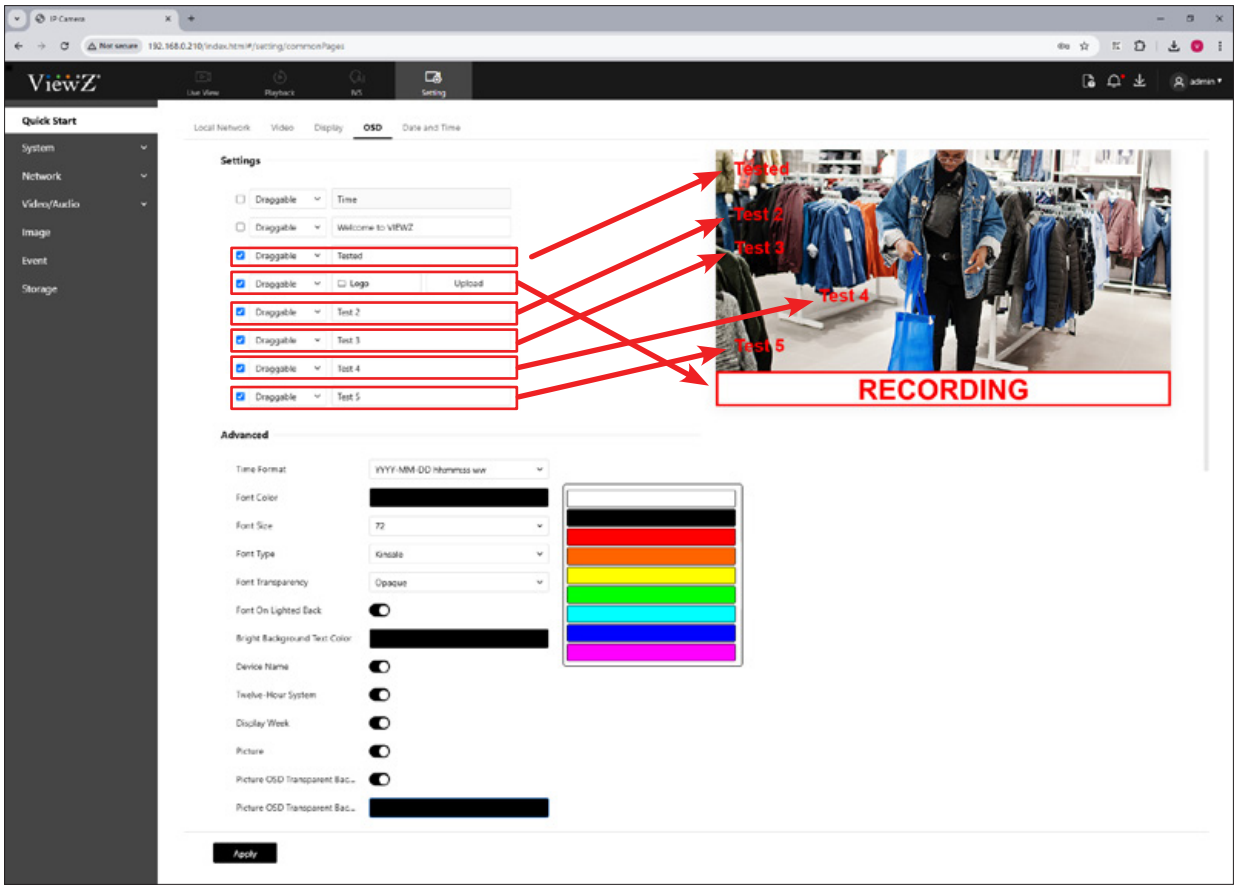


Figure 7-10 OSD

Step 2 Set **OSD** parameters as shown in Table 7-8.

SETTING / IMAGE

10. Setup OSD

Procedure

Table 7-8 OSD Parameters

Parameter	DESCRIPTION	Setting
Setting-Time	Display the time on screen	N/A
Setting-Device Name	Display the device name on screen	N/A
Setting-Logo	Display the logo/image file on screen	N/A
Setting-Text	Display the text on screen. User can type texts and check the check box ☑ to save it	N/A
Time Format	Format in which the time is displayed	Default Value: YYYY-MM-DD hh:mm:ss ww
Font Color	Set the font color of text, time & device name	Default Value: Blank
Font Size	Set the font size	Default Value: 16 16,18,24,30,32,36,48,60,72,84,96
Font Type	Select the font type	Default Value: Blank
Font Transparency	Select the font transparency Lucency, Translucency, Sub Translucency, Opaque	Default Value: Opaque
Font on Lighted Back	Enable to display the font on lighted back	Default Value: OFF
Bright Background Text Color	Set the text color on the bright background	Default Value: Blank
Device Name	Enable to display the device name on screen	Default Value: OFF
12-Hour System	Enable to display the time as 12 hour format	Default Value: OFF
Display Week	Enable to display the week day	Default Value: OFF
Picture	Enable to display the image	Default Value: OFF
Picture OSD Transparent Background	Enable to display the image	Default Value: OFF
Picture OSD Transparent Background Color	Set the text color on the bright background	Default Value: Blank

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / IMAGE

11. Setup Privacy Masking

Description

Privacy masking refers to the process of obscuring specific portions of a camera's field of view to comply with privacy regulations, as shown in Figure 7-11.

Procedure

Step 1 Click **Setting** on the top menu, **Image > Privacy Mask**

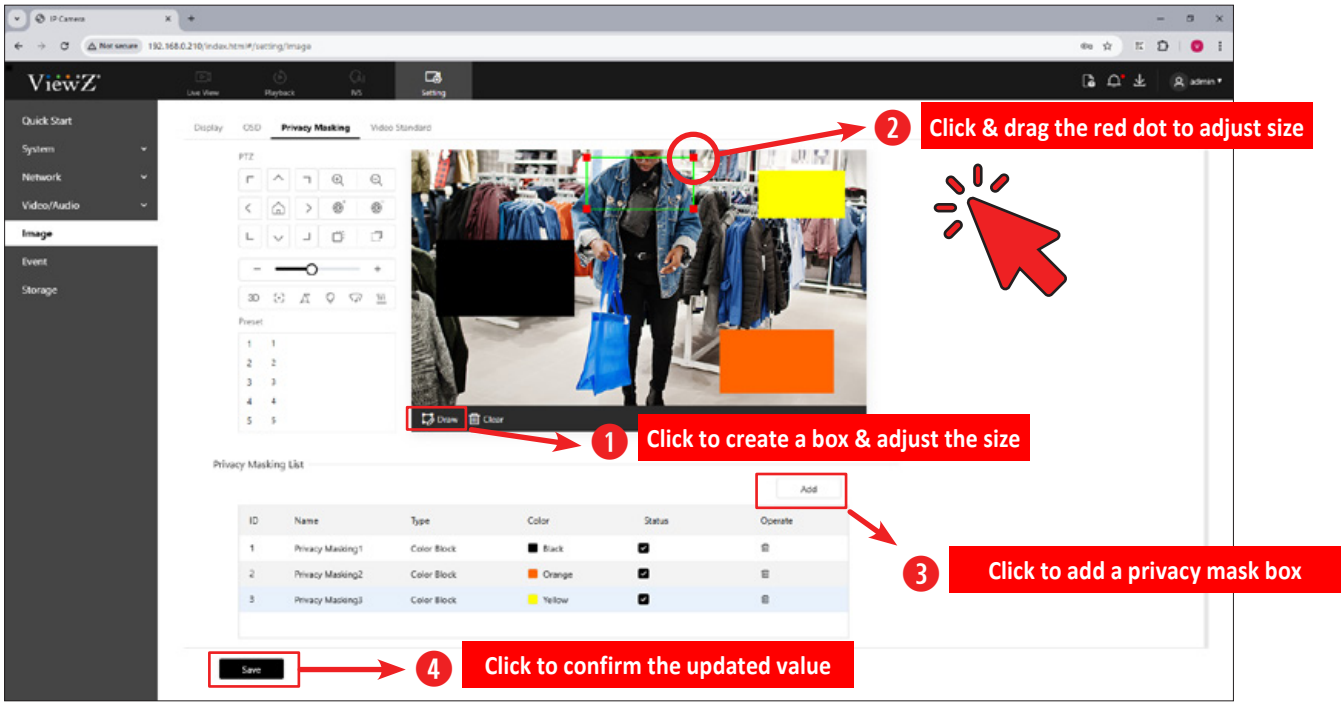


Figure 7-11 Privacy Mask

Step 2 Click the **Draw** button to create a privacy mask box and then adjust the box size & location.

Step 3 Click the **Add** button to confirm a privacy mask box. When you add a privacy mask box, it will be listed on the **Privacy Masking List**.

Note

- The maximum percentage of an image that can be masked depends on the device model. Read the tip displayed on the page. The maximum privacy masking area is 4.
- You can click **Clear** button to configure the masked areas again.
- **Delete** button is to delete Masking area. Modify button is to re-draw the masking area of current masking.

SETTING / IMAGE

11. Setup Privacy Masking

Procedure

Table 7-9 Privacy Mask Parameters

Parameter	DESCRIPTION	Setting
ID	ID of Privacy Masking	N/A
Name	Name of Privacy Masking. User can edit the name of privacy masking box	Default Value: Privacy Masking #
Type	Type of privacy masking	Default Value: Color Block
Color	Color of privacy masking. User can edit the color by clicking color box	Default Value: Black
Status	Enable/disable the selected privacy masking area	Default Value: ON
Operate	Delete the selected privacy masking area	N/A
Draw	Create a privacy masking area	N/A
Clear	Delete a privacy masking area	N/A

Step 4 Set **Privacy Mask** parameters as shown in Table 7-9.

Step 5 Click **Save** to apply the adjustment & confirm**.**

- If the message "Save succeed!" is displayed, the system successfully save & apply the settings.
- If other information is displayed, set the parameters correctly.

SETTING / IMAGE

12. Setup Video Standard

Description

The different video formats are used to reinforce national copyright laws and prevent the distribution of movies and television without permission. For example, a camcorder sold in Europe won't be able to play its videos on an American television, and vice versa, as shown in Figure 7-12.

Procedure

Step 1 Click **Setting** on the top menu, **Image > Video Standard**

Figure 7-12 Video Standard

Step 2 Set **Video Standard** parameters as shown in Table 7-10.

Table 7-10 Video Standard Parameters

Parameter	DESCRIPTION	Setting
Standard	User can select the video format NTSC: Used in USA, South Korea, Japan, Taiwan & etc. PAL: Used in Europe, China, India, Pakistan & etc.	Default Value: NTSC
Refresh Frequency	This value is automatically decided by the video format 60 Hz: corresponds to NTSC system 50 Hz: corresponds to PAL system	Default Value: 60

Step 3 Click **Apply** and then the confirmation popup window will be displayed. Click OK to process it. Then, the AI PVM will be restarted and the updated video format will be applied.

- If the message "Apply Success!" is displayed, the system successfully save & apply the settings.

SETTING / EVENT

1. Setup Event - Motion Alarm

Description

On the Motion Alarm page, you can perform the following operations:

- Enable the motion detection function.
- Set the motion detection arming time.
- Set the motion detection area.
- Configure the motion alarm output channel.
- When the alarm output function is enabled and the camera detects that an object moves into the motion detection area within the schedule time, the camera generates an alarm and triggers linkage alarm output.

Procedure

Step 1 Click **Setting** on the top menu, **Event > Motion Alarm**

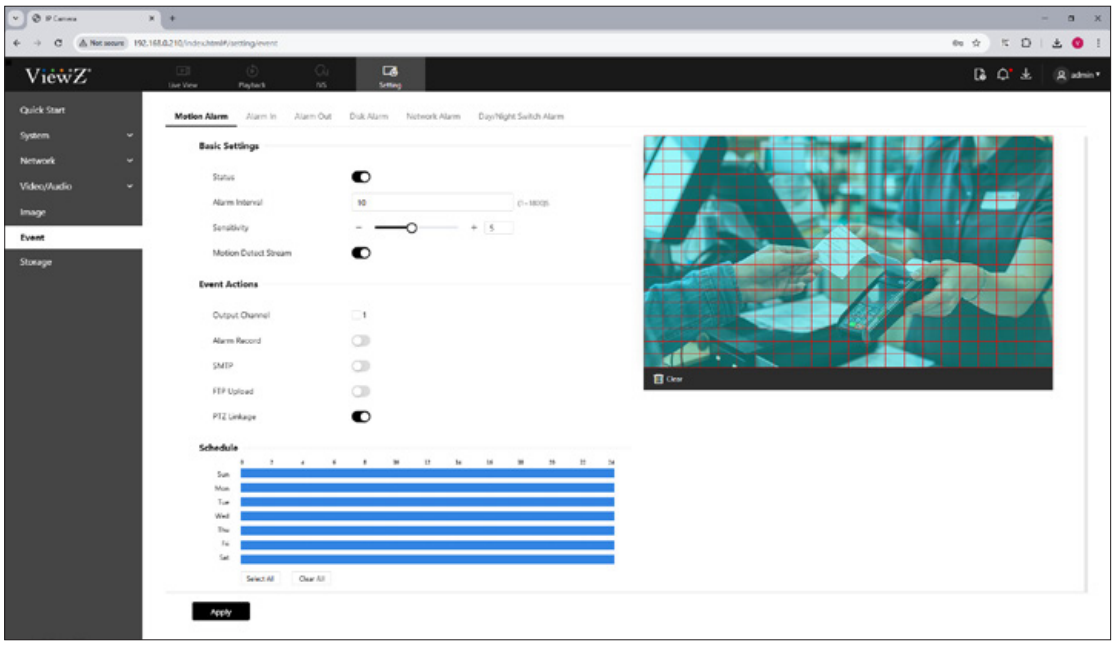


Figure 8-1 Motion Alarm

Step 2 Click the **STATUS** button to enable motion alarm.

Step 3 Set **Motion Alarm** parameters as shown in Table 8-1.

Step 4 Adjust the **Alarm Interval** (1-1800 seconds) and configure **Sensitivity -** Number 1 is the minimum and & 10 is the maximum detection sensitivity. Turn on the **Motion Detect Stream**, when camera detects the motion, it will show tracking of object.

SETTING / EVENT

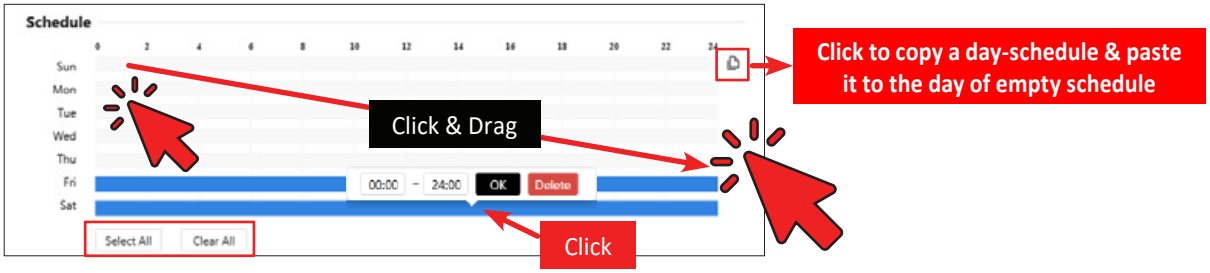
1. Setup Event - Motion Alarm

Procedure

Table 8-1 Motion Alarm Parameters

Parameter	DESCRIPTION	Setting
Status	Click Status to enable motion alarm	Default Value: OFF
Alarm Interval	During the interval, the same alarm will be only sent once.	Default Value: 1 (1 ~ 1800) sec
Sensitivity	The sensitivity of motion detection. When the value is higher, the alarm can be triggered more easily with lower accuracy.	Default Value: 5 (1 ~ 10)
Motion Detect Stream	Enable/disable showing the moving path of object when the device detects the moving.	Default Value: OFF
Output Channel	If user check this, then setup the Output Channel & the device is connected to an external alarm indicator, the alarm indicator signals when an alarm is triggered.	Default Value: OFF
Alarm Record	The device will record alarm with SD card	Default Value: OFF
SMTP	Enable/disable the SMTP connection.	Default Value: OFF
FTP Upload	Enable/disable File Transfer Protocol.	Default Value: OFF
PTZ Linkage	Enable/disable PTZ control.	Default Value: OFF

Step 5 Configure the **Schedule** time setting.



To setup the schedule of motion detection, user need to make a time table on Schedule

- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time or **Clear All** to remove all time.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

SETTING / EVENT

1. Setup Event - Motion Alarm

Procedure

Step 6 Configure the detection area.
1. Press and hold the left mouse button, and drag in the video area to draw a detection area (box shape).

Figure 8-2 Motion Alarm Setting - Setup motion detection area

2. Press and hold the left mouse button, and drag in the video area to draw a detection area.

Note
- Click **Clear** to delete a detection area.
- Click **Reverse** to select the area out of specified frames as the detection area.

Step 7 Select **Output Channel**.

Step 8 Turn on **Alarm Record** to save the motion detection on SD card.

Step 9 Turn on the **SMTP** notice. If you turn on, system will send an email about motion detection alarm.

Step 10 Turn on the **FTP Upload** to save & upload the motion detection video/image file on FTP server.

Step 11 Click **Apply** button to apply the updated parameters.
- The message "Apply success!" is displayed. The system successfully save & apply the settings.
- If other information is displayed, set the parameters correctly.

SETTING / EVENT

2. Setup Event - Alarm In

Description & Procedure

When receiving an alarm from the alarm input port, the camera performs linkage alarm output, and operate based on the linkage policy, as shown in Figure 8-3.

On the I/O Alarm Linkage page, user can perform the following operations:
- Enable the I/O alarm function.
- Configure the I/O alarm schedule.
- Configure the alarm output channel.

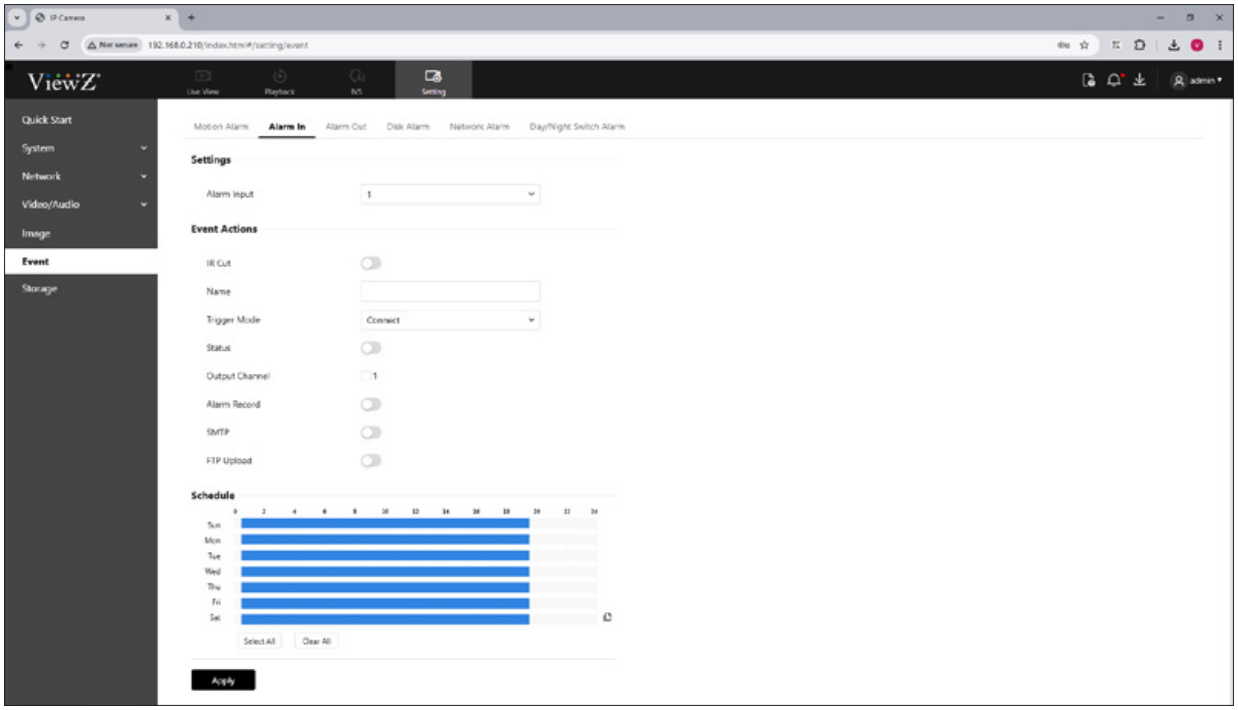


Figure 8-3 Alarm In

Note
- This feature does not support on the current version of AI PVM.

SETTING / EVENT

3. Setup Event - Alarm Out

Description & Procedure

When receiving an alarm from the alarm input port, the camera performs linkage alarm output, and operate based on the linkage policy, as shown in Figure 8-4.

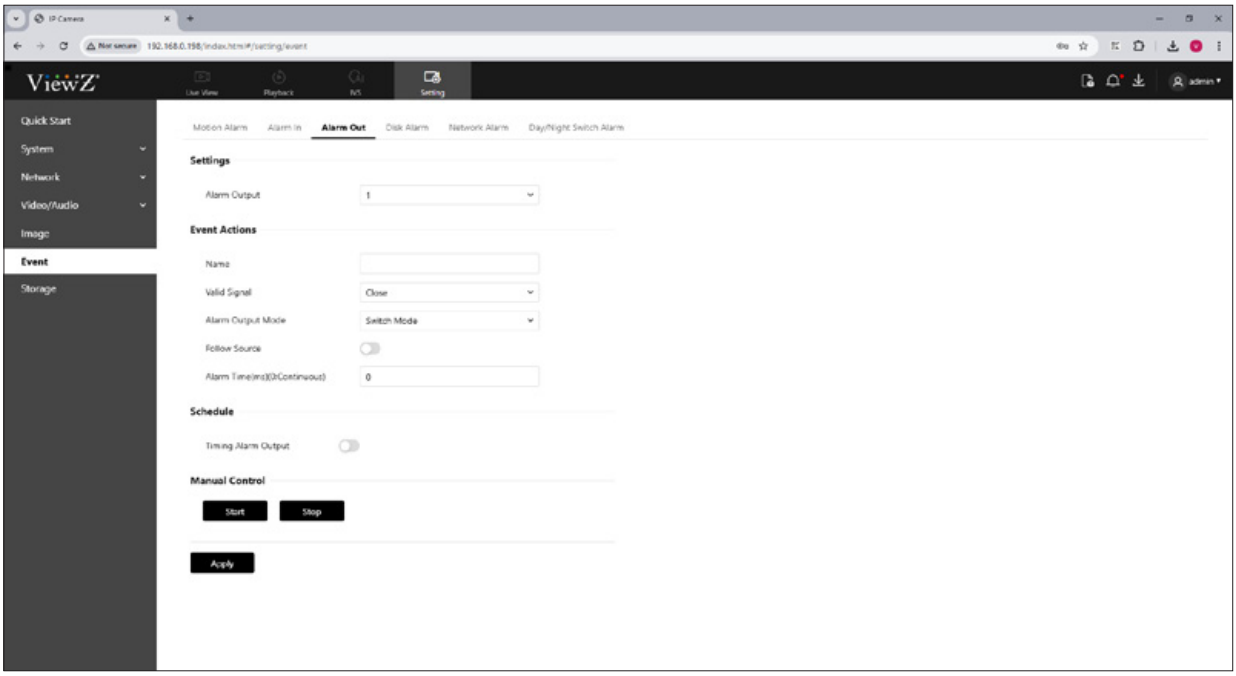


Figure 8-4 Alarm Out

Note

- This feature does not support on the current version of AI PVM.

SETTING / EVENT

4. Setup Event - Disk Alarm

Description

When receiving an alarm from the alarm input port, the camera performs linkage alarm output, and operate based on the linkage policy, as shown in Figure 8-5.

Procedure

Step 1 Click **Setting** on the top menu, **Event > Disk Alarm**

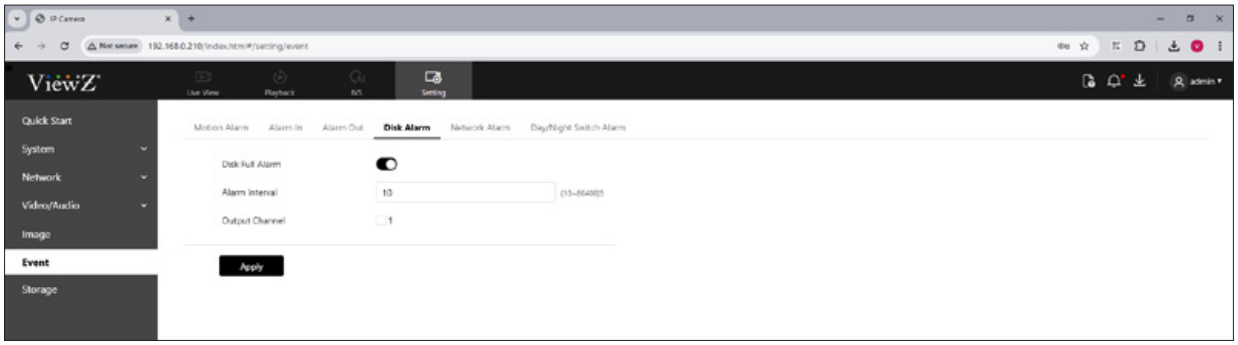


Figure 8-5 Disk Alarm

Step 2 Set **Disk Alarm** parameters as shown in Table 8-2.

Table 8-2 Disk Alarm Parameters

Parameter	DESCRIPTION	Setting
Disk Full Alarm	Enable/disable the SD card disk full alarm	Default Value: OFF
Alarm Interval	Set the alarm interval time	Default Value: 10 (10 ~ 86400) sec
Output Channel	Refer to the actual product	Default Value: OFF

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / EVENT

5. Setup Event - Network Alarm

Description

When receiving an alarm from the alarm input port, the camera performs linkage alarm output, and operate based on the linkage policy, as shown in Figure 8-6.

Procedure

Step 1 Click **Setting** on the top menu, **Event > Network Alarm**

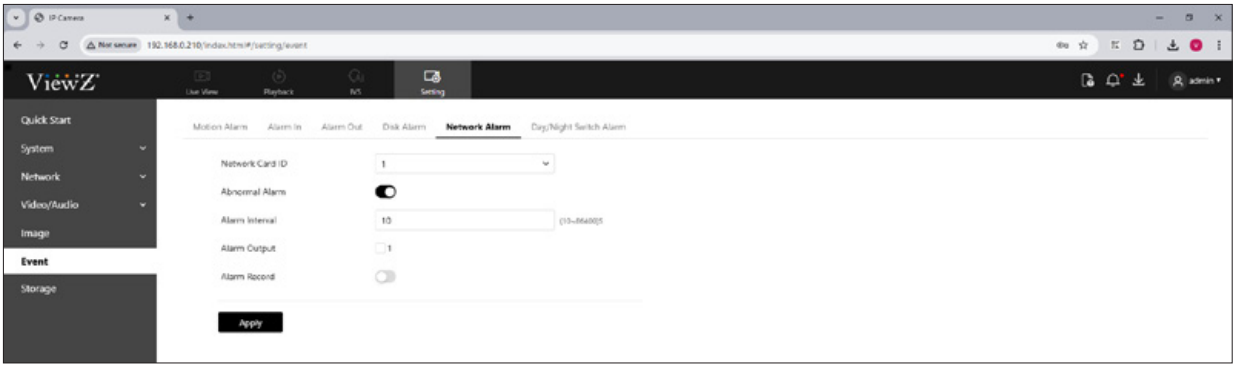


Figure 8-6 Network Alarm

Step 2 Set **Network Alarm** parameters as shown in Table 8-3.

Table 8-3 Network Alarm Parameters

Parameter	DESCRIPTION	Setting
Network Card ID	ID of the network card. AI PVM currently has 1 card	Default Value: 1
Abnormal Alarm	Enable/disable the abnormal alarm	Default Value: OFF
Alarm Interval	Setup the alarm of abnormal activity on the network	Default Value: 10 (10 ~ 86400) sec
Alarm Output	Setup the output channel number. User can enable alarm record when user insert SD card in advance.	Default Value: OFF
Alarm Record	Setup the alarm of abnormal activity on the network	Default Value: OFF

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / EVENT

6. Setup Event - Day/Night Switch Alarm

Description

When receiving an alarm from the alarm input port, the camera performs linkage alarm output, and operate based on the linkage policy, as shown in Figure 8-7.

Procedure

Step 1 Click **Setting** on the top menu, **Event > Day/Night Switch Alarm**

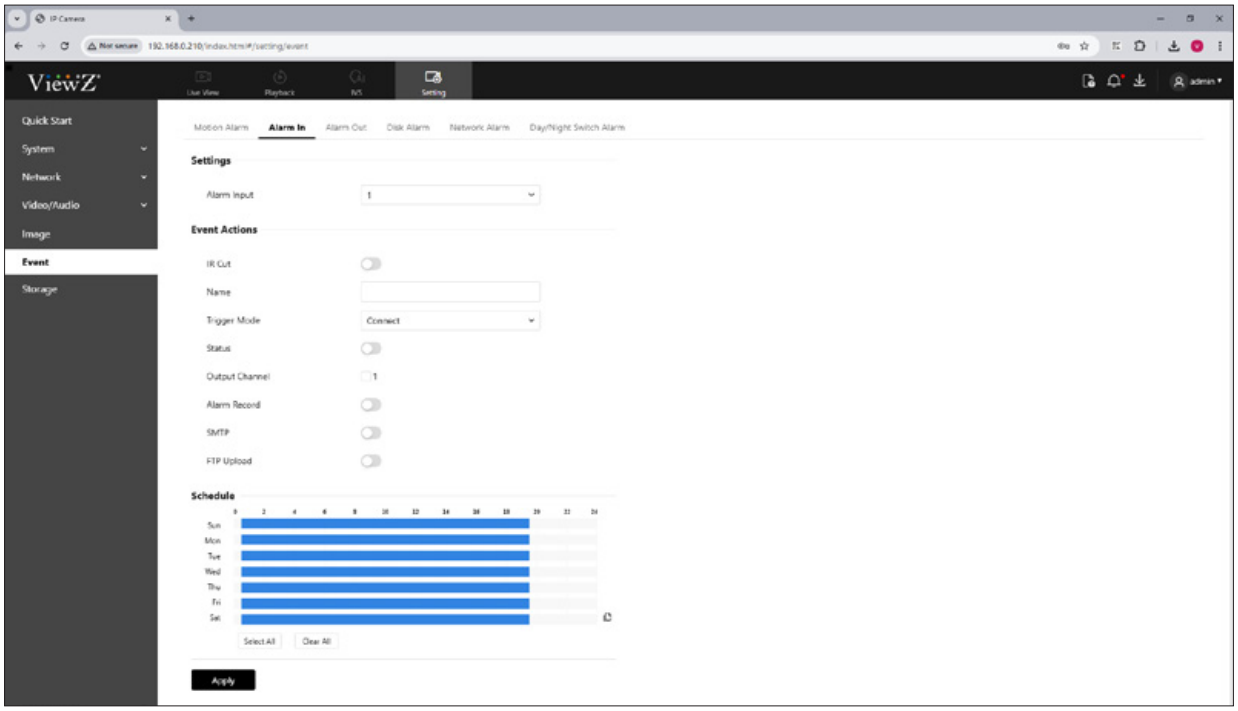


Figure 8-7 Day/Night Switch Alarm

Step 2 Set **Day/Night Switch Alarm** parameters as shown in Table 8-4.

SETTING / EVENT

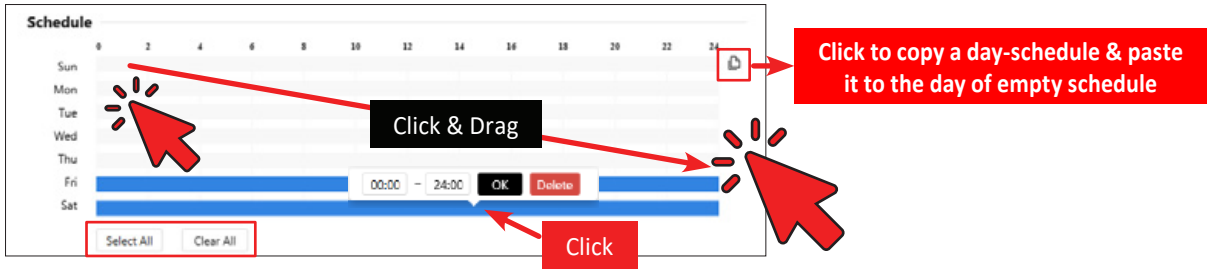
6. Setup Event - Day/Night Switch Alarm

Procedure

Table 8-4 Day/Night Switch Alarm Parameters

Parameter	DESCRIPTION	Setting
Status	Enable/disable Day/Night Switch Alarm	Default Value: OFF
Output Channel	Linkage the output channel alarm device to send alarm information.	Default Value: OFF
Alarm Record	The device will record alarm on the SD card.	Default Value: OFF
SMTP	When an alarm occurs, the device can send e-mail. The e-mail parameters should be set in advance. The parameter of SMTP can be setup at Setting > Network > Advanced Settings > SMTP	Default Value: OFF
FTP Upload	When an alarm occurs, the device will send alarm information to FTP server. The FTP parameters should be set in advance. The parameter of FTP can be setup at Setting > Network > Advanced Settings > FTP	Default Value: OFF

Step 3 Configure the **Schedule** time setting.



To setup the schedule of motion detection, user need to make a time table on Schedule

- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time or **Clear All** to remove all time.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

Step 4 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / STORAGE

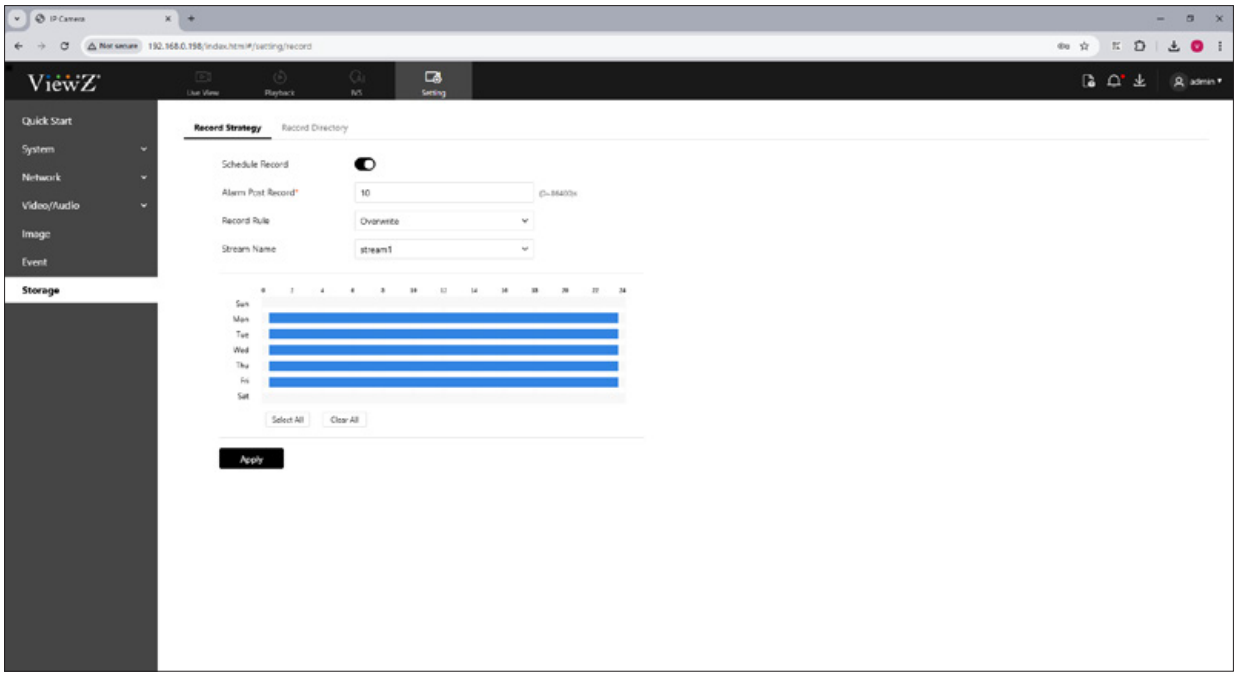
1. Setup Storage - Record Strategy

Description

User can configure the scheduled recording function, alarm recording function, recording quality, and recording rules, as shown in Figure 9-1.

Procedure

Step 1 Click **Setting** on the top menu, **Storage > Record Strategy**



Step 2 Set **Record Strategy** parameters as shown in Table 9-1.

SETTING / STORAGE

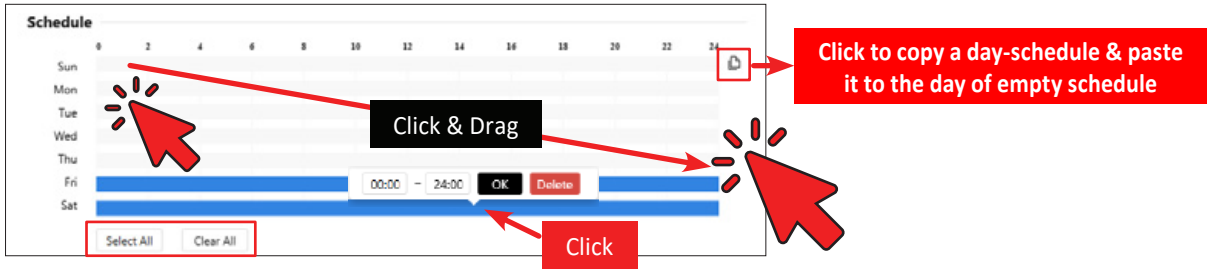
1. Setup Storage - Record Strategy

Procedure

Table 9-1 Record Strategy Parameters

Parameter	DESCRIPTION	Setting
Schedule Record	Enables/disable schedule record that you can configure the time policy.	Default Value: OFF
Alarm Post Record	Recording duration (in seconds) after an alarm is generated	Default Value: 10 (10 ~ 86400) sec
Record Rule	Rule for saving recordings. The options are as follows: **Overwrite**: Overwrite the recording file **Retention**: managing and safeguarding records for a set amount of time (99999 days)	Default Value: Overwrite
Stream Name	Select one of 3 streaming videos	Default Value: stream1

Step 3 Configure the **Schedule** time setting.



To setup the schedule of **Record Strategy**, user need to make a time table on Schedule

- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time or **Clear All** to remove all time.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

Step 4 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

SETTING / STORAGE

2. Setup Storage - Record Directory

Description

Recording files can be stored in an SD card, FTP, or NAS server, as shown in Figure 9-2.

Procedure

Step 1 Click **Setting** on the top menu, **Storage > Record Directory**

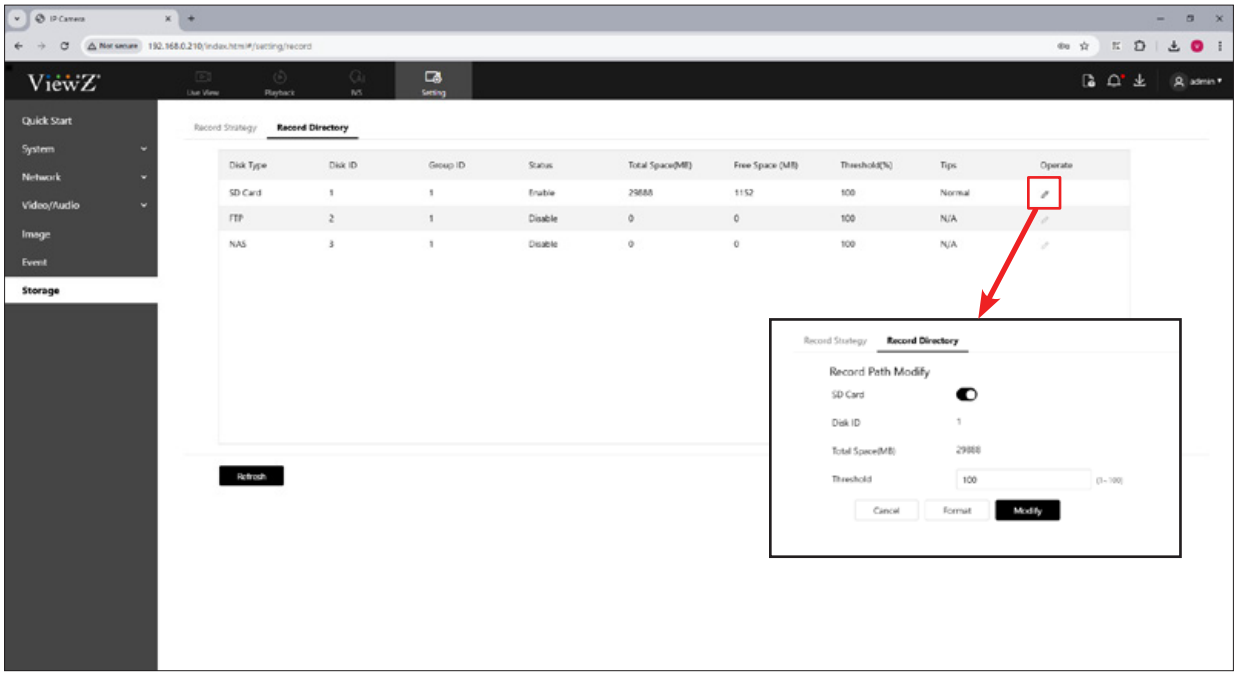


Figure 9-2 Record Directory

Step 2 Set **Record Directory** parameters as shown in Table 9-2.

SETTING / STORAGE

2. Setup Storage - Record Directory

Procedure

Table 9-2 Record Directory Parameters

Parameter	DESCRIPTION	Setting
Disk Type	Recording location which can be an SD card, FTP & NAS	N/A
Disk ID	Display the storage ID	N/A
Group ID	Display the group ID	N/A
Status	Connection status of storing availability	N/A
Total Space (MB)	Display the storage disk size	N/A
Free Space (MB)	Display the available storage disk size	N/A
Threshold (%)	The camera will alarm when used Space achieves the alarm threshold.	Default Value: 100 %
Tips	Status of the connection between the current AI PVM and recording directory detected automatically.	Default Value: N/A
Record Path Modify	User can enable/disable recording functionality	Default Value: OFF
Disk ID	Display the storage ID	N/A
Total Space (MB)	Display the storage disk size	N/A
Threshold (%)	The camera will alarm when used Space achieves the alarm threshold.	Default Value: 100 (1 ~ 100)
Format	Format the storage	N/A
Modify	Apply the updated parameter	N/A

Step 3 Click **Refresh** to check the updated value

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

IVS

IVS

Description

Click **IVS** to enter **IVS** setting page, users can set the deep learning, intelligent analysis, behavior analysis as shown in Figure 10-1. The detail settings will be introduced on the following chapters

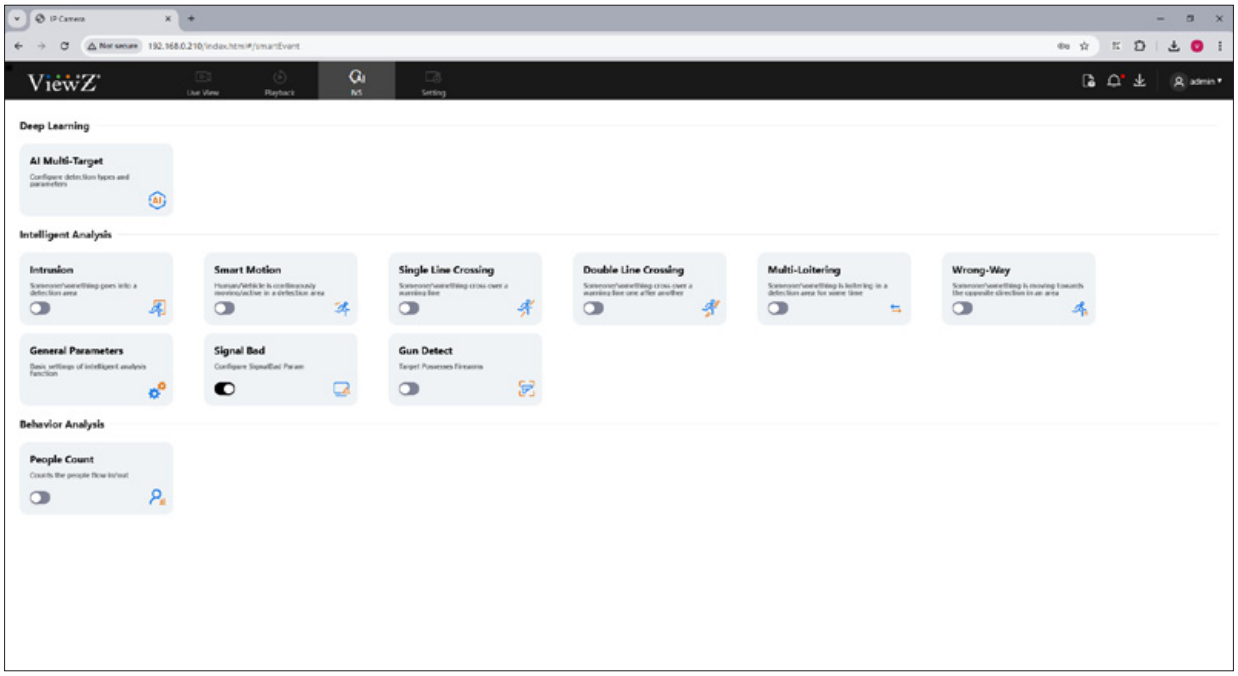


Figure 10-1 IVS

Note

- The different models have different IVS functions, please refer to actual product

IVS / DEEP LEARNING

1. IVS - Deep Learning - AI Multi-Target

Description & Procedure

User can setup the **AI Multi-Target**, as shown in Figure 10-2.

Step 1 Click **IVS** on the top menu, **Deep Learning > AI Multi-Target**

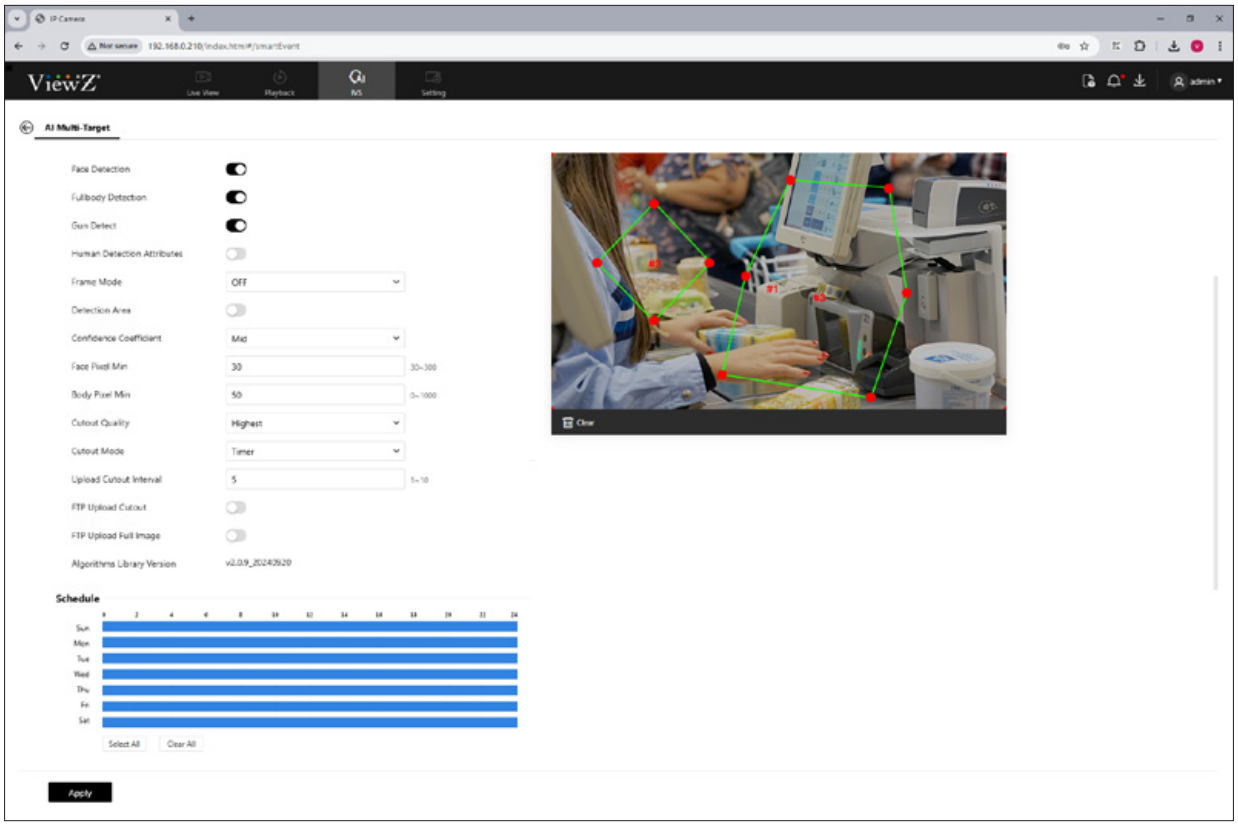


Figure 10-2 AI Multi-Target

Step 2 Set **AI Multi-Target** parameters as shown in Table 10-1.

IVS / DEEP LEARNING

1. IVS - Deep Learning - AI Multi-Target

Procedure

Table 10-1 AI Multi-Target Parameters

Parameter	DESCRIPTION	Setting
Face Detection	Enable/disable the AI PVM's camera will capture the face when someone appears in live video	Default Value: OFF
Fullbody Detection	Enable/disable the AI PVM's camera will capture a whole body when someone appears in live video	Default Value: OFF
Gun Detection	Enable/disable the AI PVM's camera will capture weapons when weapon appears in live video	Default Value: OFF
Human Detection Attributes	Enable/disable the AI PVM's camera will capture human when human appears in live video	Default Value: OFF
Frame Mode	Choose one to a trace box will show at live video. There are four modes can be chosen - **Full Frame**, **Four-Corner Frame**, **Mosaic** & **OFF**. Users can also choose OFF to close the box on showing	Default Value: OFF
Detection Area	Enable to show the detection area on live video	Default Value: OFF
Confidence Coefficient	The range of snapshots, there are three types, such as **Low**, **Mid** & **High**. The higher the confidence, the better the snapshot quality & the fewer snapshots.	Default Value: MID
Face Pixel Min	Face detection is on. It's the MIN face pixel that the device will capture. If the detected pixel is lower than the value, it will not be captured.	Default Value: 30 (30 ~ 300)
Body Pixel Min	Fullbody detection is on. It's the MIN face pixel that the device will capture. If the detected pixel is lower than the value, it will not be captured.	Default Value: 50 (0 ~ 1000)
Cutout Quality	The quality of snapshots, there are three modes can be chosen, such as **Low**, **Mid**, **High** & **Highest**.	Default Value: Highest
Cutout Mode	There are two modes can be chosen, such as **Timer** and **Optimal**.	Default Value: Timer

IVS / DEEP LEARNING

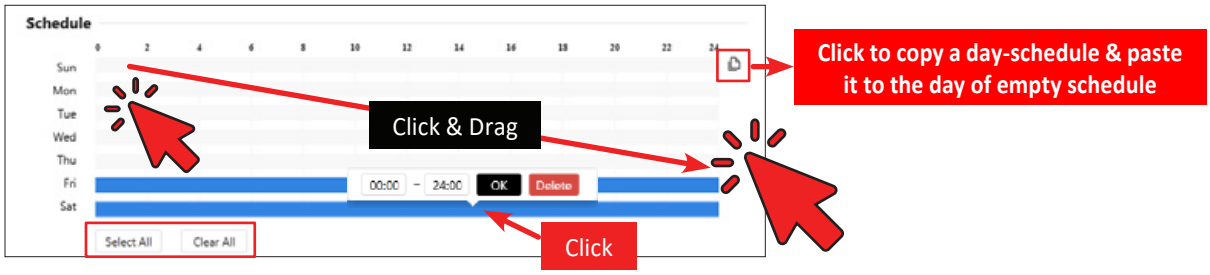
1. IVS - Deep Learning - AI Multi-Target

Procedure

Table 10-1 AI Multi-Target Parameters

Parameter	DESCRIPTION	Setting
Upload Cutout Interval	At timing mode, set the interval time of upload image	Default Value: 5 (1 ~ 10) sec
FTP Upload Cutout	Enable/disable this feature; **Setting > Network > Advanced Settings > FTP**, set FTP related parameters, the captured picture will be sent to the set FTP location	Default Value: OFF
FTP Upload Full Image	Capture a picture and send a whole image	Default Value: OFF

Step 3 Configure the **Schedule** time setting.



To setup the schedule of AI Multi-Target, user need to make a time table on Schedule

- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time-schedule or **Clear All** to remove all time-schedule.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

Step 4 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

IVS / INTELLIGENT ANALYSIS

1. IVS - Intelligent Analysis - Intrusion

Description

The **Intrusion** function refers to that an alarm is generated when target objects (people) enter the detection area, as shown in Figure 10-3.

Procedure

Step 1 Click **IVS** on the top menu, **Intelligent Analysis > Intrusion**

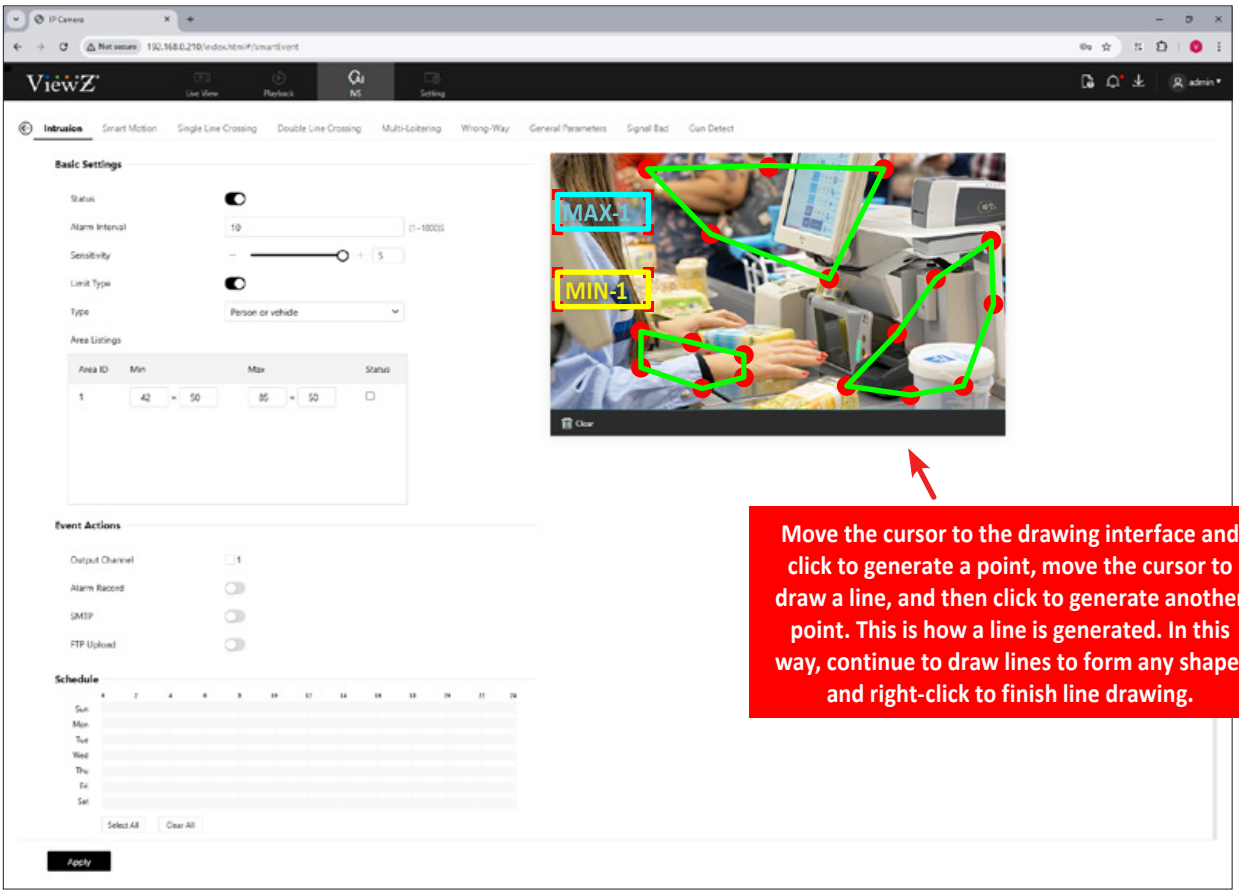


Figure 10-3 Intrusion

Step 2 Set **Intrusion** parameters as shown in Table 10-2.

Step 3 Setup **Deployment Area**

IVS / INTELLIGENT ANALYSIS

1. IVS - Intelligent Analysis - Intrusion

Procedure

Table 10-2 Intrusion Parameters

Parameter	DESCRIPTION	Setting
Status	Enable/disable the intrusion alarm	Default Value: OFF
Alarm Interval	During the time interval, the same alarm will be only sent once.	Default Value: 0 (1 ~ 1800) sec
Sensitivity	The sensitivity of detecting the target, when the value is high, the target can be detected easily, but the accuracy will be lower.	Default Value: 1 (1 ~ 5)
Limit Type	Enable to choose the limit type - person	Default Value: OFF
Area Listings	Set the areas will show in listings. Tick the status, the min and max detecting area show on area, user can drag the point to adjust the size of the detecting area, or modify the value directly.	Default Value: OFF
Output Channel	If user check to set the Output Channel and the device is connected to an external alarm indicator, the alarm indicator signals will send to external device when an alarm is triggered. NOTE The alarm output will only work for some models	Default Value: OFF
Alarm Record	The device will record alarm signal to the SD card	Default Value: OFF
SMTP	Enable/disable uploading onto SMTP server connection The parameter of SMTP can be setup at Setting > Network > Advanced Settings > SMTP	Default Value: OFF
FTP Upload	Enable/disable uploading onto FTP server connection The parameter of FTP can be setup at Setting > Network > Advanced Settings > FTP	Default Value: OFF

Note

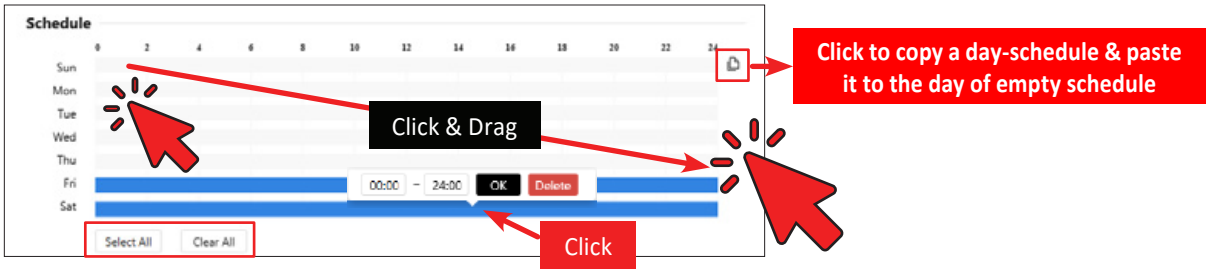
- On the deployment area, a drawn line cannot cross another one, or the line drawing fails.
- On the deployment area, any shape with 8 sides, can be drawn.
- On the deployment area, the quantity of deployment areas is up to 8.

IVS / INTELLIGENT ANALYSIS

1. IVS - Intelligent Analysis - Intrusion

Procedure

Step 4 Configure the **Schedule** time setting.



To setup the schedule of **Intrusion**, user need to make a time table on Schedule

- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time-schedule or **Clear All** to remove all time-schedule.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

Step 5 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

IVS / INTELLIGENT ANALYSIS

2. IVS - Intelligent Analysis - Smart Motion

Description

The Smart Motion function refers to that an alarm is generated when target objects (people) move at the deployment area, as shown in Figure 10-4.

Procedure

Step 1 Click **IVS** on the top menu, **Intelligent Analysis > Smart Motion**

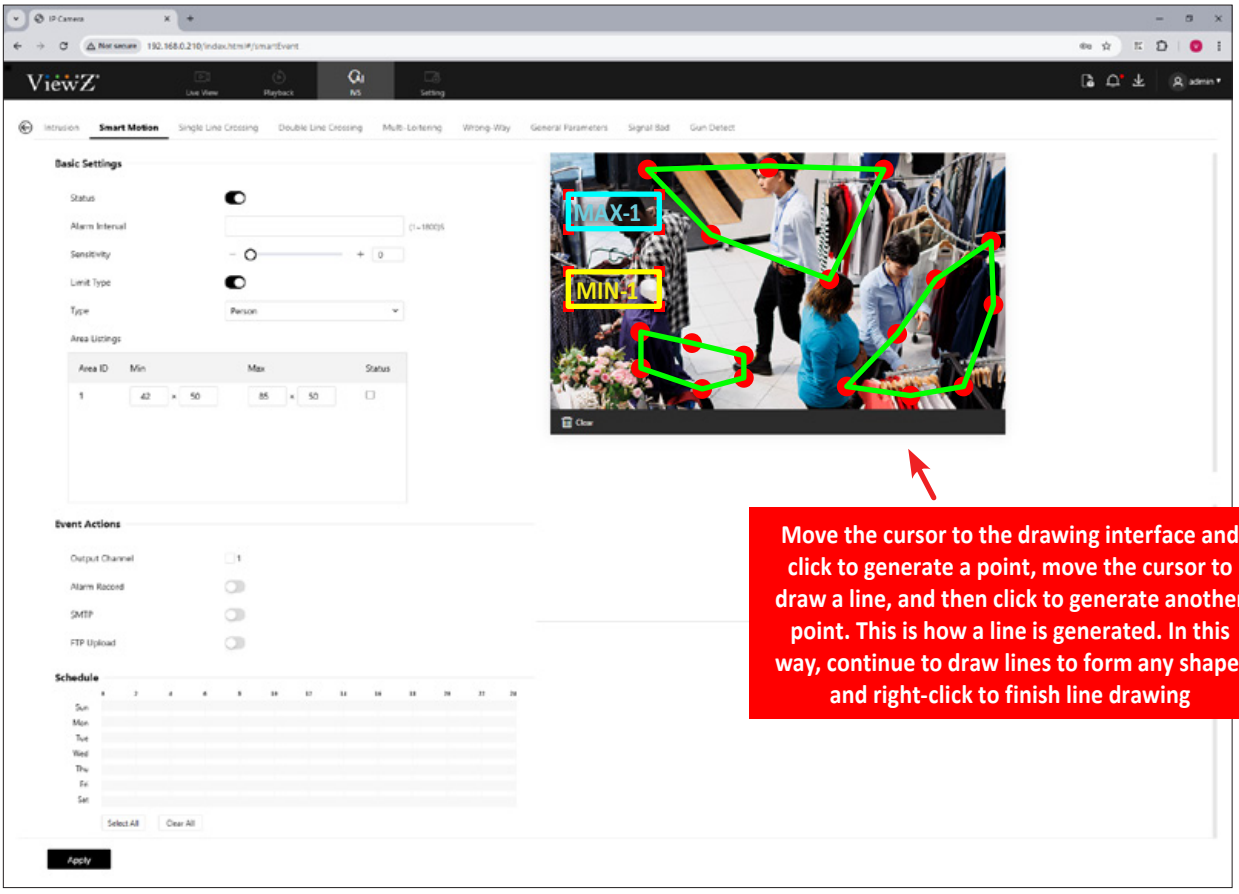


Figure 10-4 Smart Motion

Step 2 Set **Smart Motion** parameters as shown in Table 10-3.

Step 3 Setup **Deployment Area**

IVS / INTELLIGENT ANALYSIS

2. IVS - Intelligent Analysis - Smart Motion

Procedure

Table 10-3 Smart Motion Parameters

Parameter	DESCRIPTION	Setting
Status	Enable/disable the smart motion alarm	Default Value: OFF
Alarm Interval	During the time interval, the same alarm will be only sent once.	Default Value: 0 (1 ~ 1800) sec
Sensitivity	The sensitivity of detecting the target, when the value is high, the target can be detected easily, but the accuracy will be lower.	Default Value: 1 (1 ~ 5)
Limit Type	Enable to choose the limit type - person	Default Value: OFF
Area Listings	Set the areas will show in listings. Tick the status, the min and max detecting area show on area, user can drag the point to adjust the size of the detecting area, or modify the value directly.	Default Value: OFF
Output Channel	If user check to set the Output Channel and the device is connected to an external alarm indicator, the alarm indicator signals will send to external device when an alarm is triggered. NOTE The alarm output will only work for some models	Default Value: OFF
Alarm Record	The device will record alarm signal to the SD card	Default Value: OFF
SMTP	Enable/disable uploading onto SMTP server connection The parameter of SMTP can be setup at Setting > Network > Advanced Settings > SMTP	Default Value: OFF
FTP Upload	Enable/disable uploading onto FTP server connection The parameter of FTP can be setup at Setting > Network > Advanced Settings > FTP	Default Value: OFF

Note

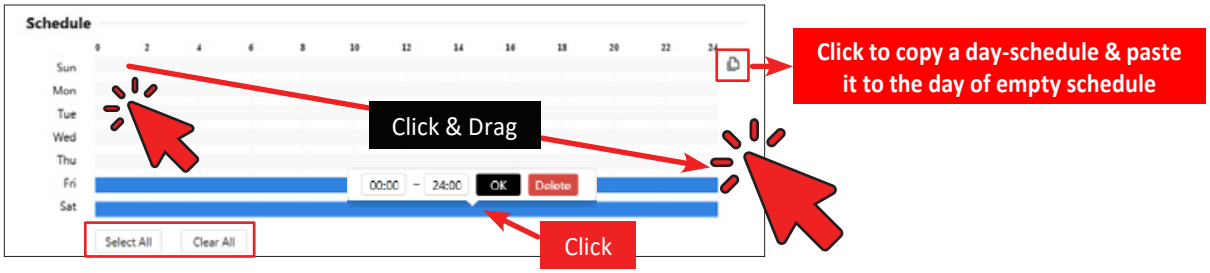
- On the deployment area, a drawn line cannot cross another one, or the line drawing fails.
- On the deployment area, any shape with 8 sides, can be drawn.
- On the deployment area, the quantity of deployment areas is up to 8.

IVS / INTELLIGENT ANALYSIS

2. IVS - Intelligent Analysis - Smart Motion

Procedure

Step 4 Configure the **Schedule** time setting.



To setup the schedule of **Smart Motion**, user need to make a time table on Schedule

- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time-schedule or **Clear All** to remove all time-schedule.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

Step 5 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

IVS / INTELLIGENT ANALYSIS

3. IVS - Intelligent Analysis - Single Line Crossing

Description

A single line crossing is a line that is set at a concerned position within the monitored field of view and specifies the forbidden travel direction, an alarm is generated when target objects (people) cross this line, as shown in Figure 10-5.

Procedure

Step 1 Click **IVS** on the top menu, **Intelligent Analysis > Single Line Crossing**

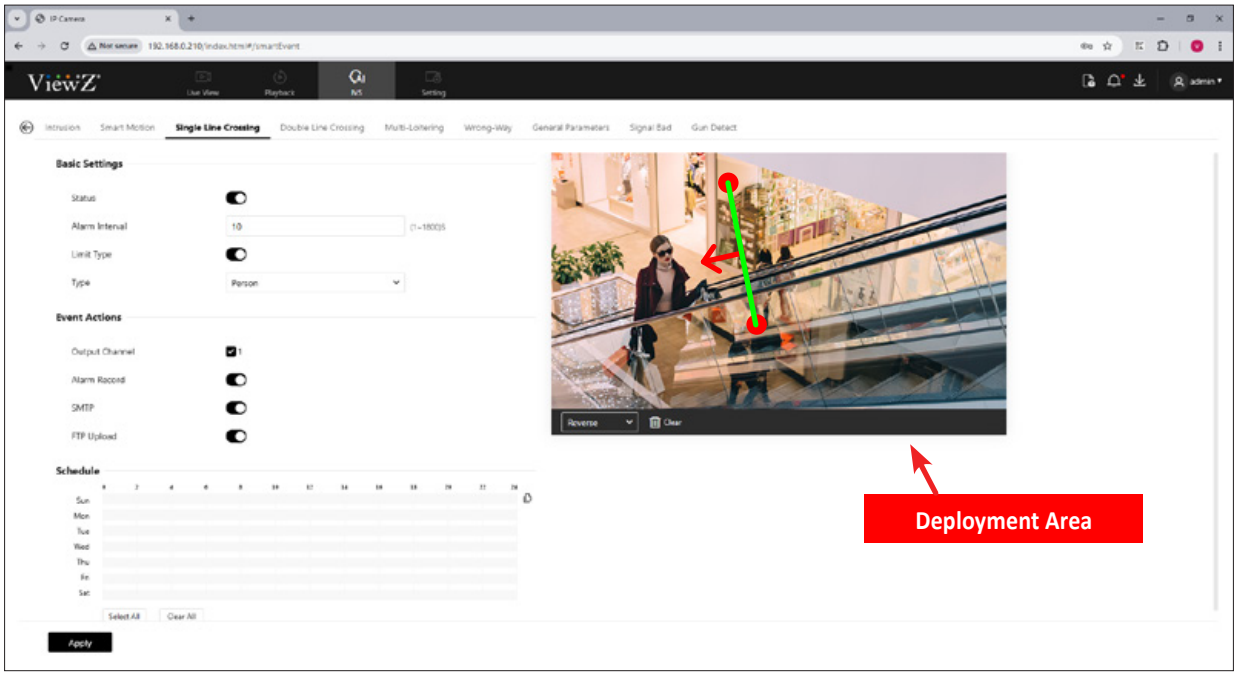


Figure 10-5 Single Line Crossing

Step 2 Set **Single Line Crossing** parameters as shown in Table 10-4.

Step 3 Setup **Deployment Area**

- **Drawing a line**: Move the cursor to the drawing interface, hold down the left mouse button, and move the cursor to draw a line. When you release the left mouse button, a single line crossing is generated.
- **Setting a single line crossing**: Click a line (and the trip line turns red) to select the single line crossing and set its direction as positive, reverse or bidirectional, or delete the selected line. You can also press and hold left mouse button at the endpoint of a single line crossing and move the mouse to modify the position and length of this single line crossing. You can right-click to delete the single line crossing.

IVS / INTELLIGENT ANALYSIS

3. IVS - Intelligent Analysis - Single Line Crossing

Procedure

Table 10-4 Single Line Crossing Parameters

Parameter	DESCRIPTION	Setting
Status	Enable/disable the single line crossing alarm	Default Value: OFF
Alarm Interval	During the time interval, the same alarm will be only sent once.	Default Value: 0 (1 ~ 1800) sec
Limit Type	Enable to choose the limit type - person	Default Value: OFF
Output Channel	If user check to set the Output Channel and the device is connected to an external alarm indicator, the alarm indicator signals will send to external device when an alarm is triggered. NOTE The alarm output will only work for some models	Default Value: OFF
Alarm Record	The device will record alarm signal to the SD card	Default Value: OFF
SMTP	Enable/disable uploading onto SMTP server connection The parameter of SMTP can be setup at Setting > Network > Advanced Settings > SMTP	Default Value: OFF
FTP Upload	Enable/disable uploading onto FTP server connection. The parameter of FTP can be setup at Setting > Network > Advanced Settings > FTP	Default Value: OFF

Note

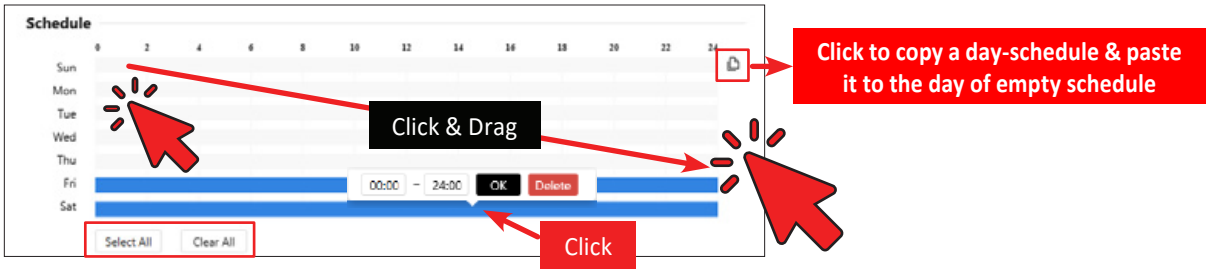
- On the deployment area, try to draw the single line crossing in the middle, because the recognition of a target takes time after target appearance on the screen and an alarm is generated only when the object is recognized to have crossed the single line crossing.
- On the deployment area, the single line crossing which detects person foot as the recognition target cannot be too short, because a short single line crossing tends to miss targets.

IVS / INTELLIGENT ANALYSIS

3. IVS - Intelligent Analysis - Single Line Crossing

Procedure

Step 4 Configure the **Schedule** time setting.



To setup the schedule of **Single Line Crossing**, user need to make a time table on Schedule

- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time-schedule or **Clear All** to remove all time-schedule.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

Step 5 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

IVS / INTELLIGENT ANALYSIS

4. IVS - Intelligent Analysis - Double Line Crossing

Description

Double line crossing refers to two lines that are set at a concerned special position within the field of view and specify the forbidden travel direction. when target objects (people) move along the set travel direction and cross these lines in a certain order (line 1 followed by line 2) in pass max time, an alarm is generated, as shown in Figure 10-6.

Procedure

Step 1 Click **IVS** on the top menu, **Intelligent Analysis > Double Line Crossing**

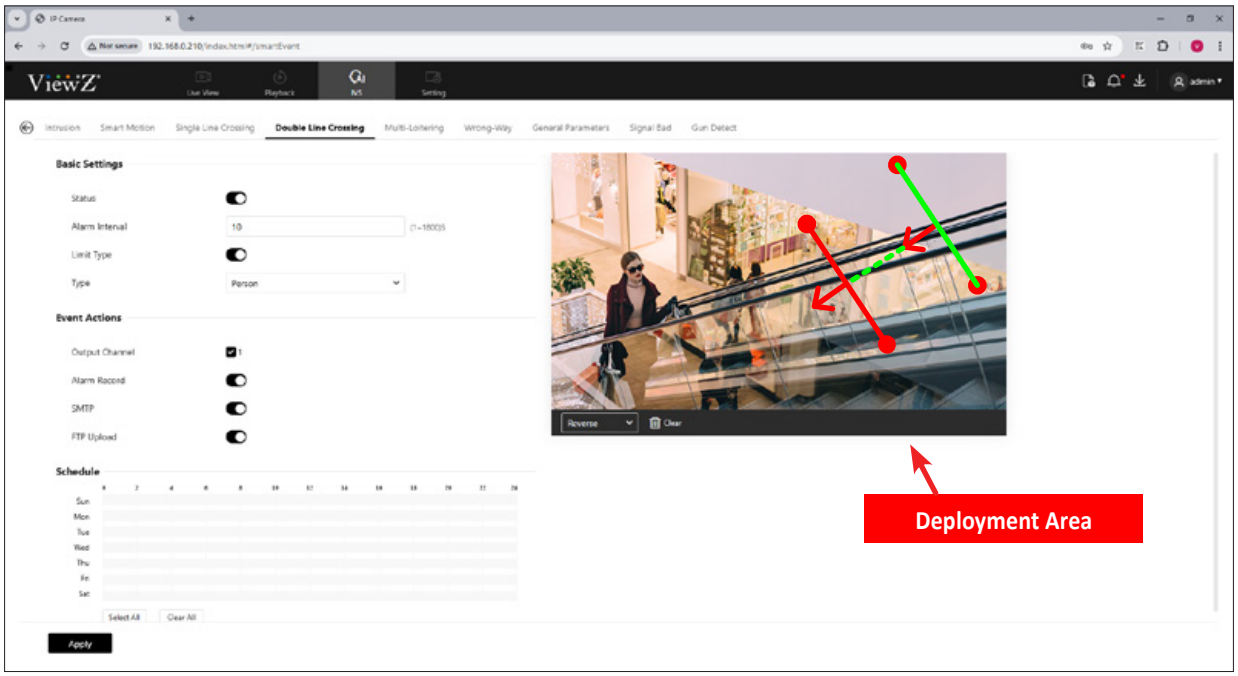


Figure 10-6 Double Line Crossing

Step 2 Set **Double Line Crossing** parameters as shown in Table 10-5.

Step 3 Setup **Deployment Area**

- **Drawing a line**: Move the cursor to the drawing interface, hold down the left mouse button, and move the cursor to draw two lines. When you release the left mouse button, two numbered virtual fences are generated. Choose either of the double line crossing to set the direction to Positive or Reverse.
- **Setting double line crossing**: Click one of the double line crossings (and the virtual fence turns red) to select this virtual fence and set the direction to **Positive** or **Reverse**, or delete the selected line. You can also press and hold left mouse button at the endpoint of a virtual fence and move the mouse to modify the position and length of this virtual fence. You can right-click to delete the double line crossing.

IVS / INTELLIGENT ANALYSIS

4. IVS - Intelligent Analysis - Double Line Crossing

Procedure

Table 10-5 Double Line Crossing Parameters

Parameter	DESCRIPTION	Setting
Status	Enable/disable the double line crossing alarm	Default Value: OFF
Alarm Interval	During the time interval, the same alarm will be only sent once.	Default Value: 0 (1 ~ 1800) sec
Limit Type	Enable to choose the limit type - person	Default Value: OFF
Output Channel	If user check to set the Output Channel and the device is connected to an external alarm indicator, the alarm indicator signals will send to external device when an alarm is triggered. NOTE The alarm output will only work for some models	Default Value: OFF
Alarm Record	The device will record alarm signal to the SD card	Default Value: OFF
SMTP	Enable/disable uploading onto SMTP server connection The parameter of SMTP can be setup at Setting > Network > Advanced Settings > SMTP	Default Value: OFF
FTP Upload	Enable/disable uploading onto FTP server connection. The parameter of FTP can be setup at Setting > Network > Advanced Settings > FTP	Default Value: OFF

Note

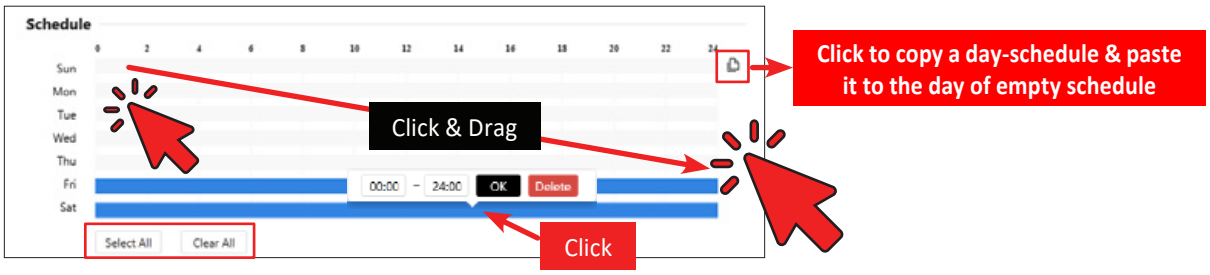
- The two virtual fences are in sequential order. An alarm is generated only when a target crosses virtual fence 1 and then virtual fence 2 within the set maximum passing time.
- Try to draw double line crossing in the middle, because the recognition of a target takes time after target appearance on the screen and an alarm is generated only when the object is recognized to have crossed the double line crossing.
- The double line crossing which detect person foot as the recognition target cannot be too short, because short double line crossing tends to miss targets.
- The double line crossing is not supported to modify the direction manually, you can change the direction by choosing Reverse.

IVS / INTELLIGENT ANALYSIS

4. IVS - Intelligent Analysis - Double Line Crossing

Procedure

Step 4 Configure the **Schedule** time setting.



- To setup the schedule of **Double LIne Crossing**, user need to make a time table on Schedule
- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time-schedule or **Clear All** to remove all time-schedule.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

Step 5 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

IVS / INTELLIGENT ANALYSIS

5. IVS - Intelligent Analysis - Multi-Loitering

Description

Multi-Loitering allows setting the shortest loitering time for multiple targets of specified type (people) within the deployment area in the field of view. When the loitering time of the multiple targets within this area meets the set shortest loitering time, an alarm is generated, as shown in Figure 10-7.

Procedure

Step 1 Click **IVS** on the top menu, **Intelligent Analysis > Multi-Loitering**

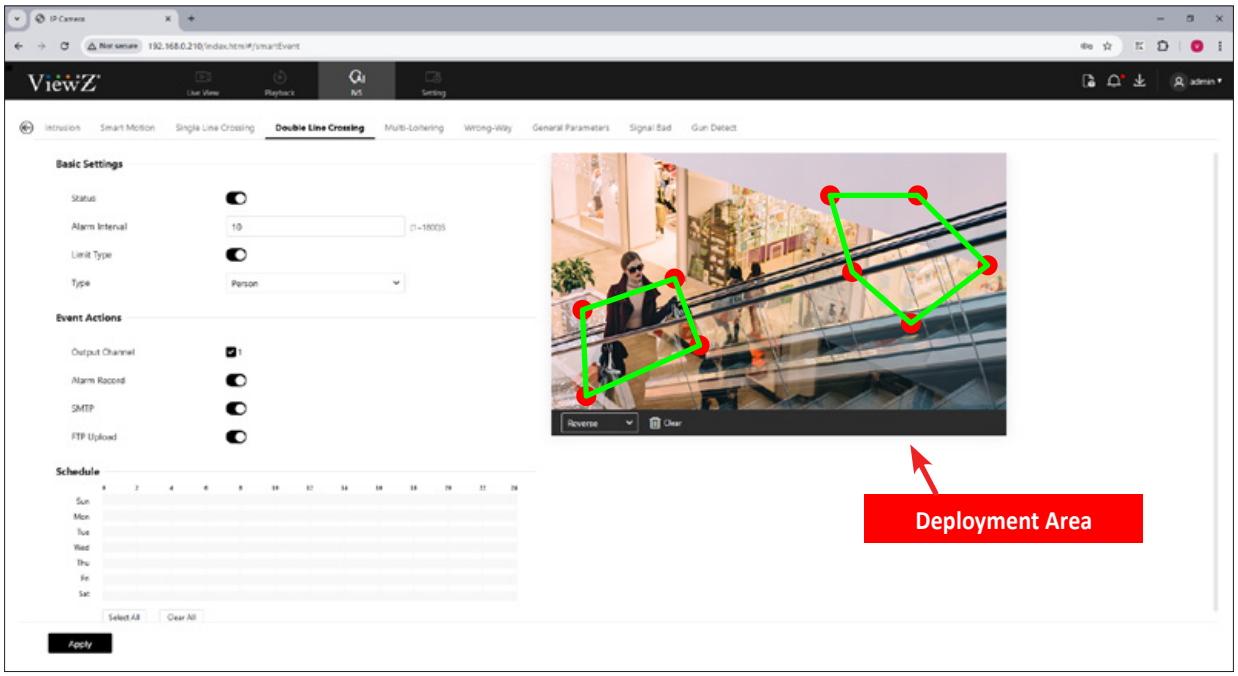


Figure 10-7 Multi-Loitering

Step 2 Set **Multi-Loitering** parameters as shown in Table 10-6.

Step 3 Setup **Deployment Area**

- Move the cursor to the drawing interface and click to generate a point, move the cursor to draw a line, and then click to generate another point. This is how a line is generated. In this way, continue to draw lines to form any shape, and right-click to finish line drawing,

Note

- A drawn line cannot cross another one, or the line drawing fails.
- Any shape with 8 sides at most can be drawn.
- The quantity of deployment areas is up to 8.

IVS / INTELLIGENT ANALYSIS

5. IVS - Intelligent Analysis - Multi-Loitering

Procedure

Table 10-6 Multi-Loitering

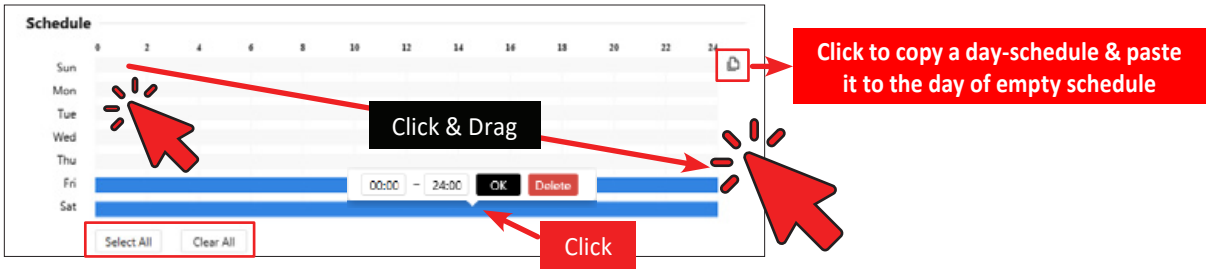
Parameter	DESCRIPTION	Setting
Status	Enable/disable the multi-loitering	Default Value: OFF
Alarm Interval	During the time interval, the same alarm will be only sent once.	Default Value: 0 (1 ~ 1800) sec
The Shortest Time	The time that a target object spends in loitering cannot be less than the shortest loitering time.	Default Value: 10 (5 ~ 60) sec
Limit Numbers	When Limit Numbers is set to OFF, an alarm is generated no matter how many people loiter. When Limit Numbers is set to ON, if the minimum number is set to 2 and the maximum number is set to 3, an alarm is generated for 2-3 people loitering. Other settings are the same as loitering.	Default Value: OFF
Area Listings	Set the areas will show in listings. Tick the status, the min and max detecting area show on area, user can drag the point to adjust the size of the detecting area, or modify the value directly.	Default Value: OFF
Output Channel	If user check to set the Output Channel and the device is connected to an external alarm indicator, the alarm indicator signals will send to external device when an alarm is triggered. NOTE The alarm output will only work for some models	Default Value: OFF
Alarm Record	The device will record alarm signal to the SD card	Default Value: OFF
SMTP	Enable/disable uploading onto SMTP server connection The parameter of SMTP can be setup at Setting > Network > Advanced Settings > SMTP	Default Value: OFF
FTP Upload	Enable/disable uploading onto FTP server connection The parameter of FTP can be setup at Setting > Network > Advanced Settings > FTP	Default Value: OFF

IVS / INTELLIGENT ANALYSIS

5. IVS - Intelligent Analysis - Multi-Loitering

Procedure

Step 4 Configure the **Schedule** time setting.



To setup the schedule of **Multi-Loitering**, user need to make a time table on Schedule

- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time-schedule or **Clear All** to remove all time-schedule.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

Step 5 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

IVS / INTELLIGENT ANALYSIS

6. IVS - Intelligent Analysis - Wrong-Way

Description

Wrong-Way allows setting the travel direction criteria for a target within an area on the video screen. It means someone/something is moving towards the opposite direction in an area, an alarm is generated, as shown in Figure 10-8.

Procedure

Step 1 Click **IVS** on the top menu, **Intelligent Analysis > Wrong-Way**

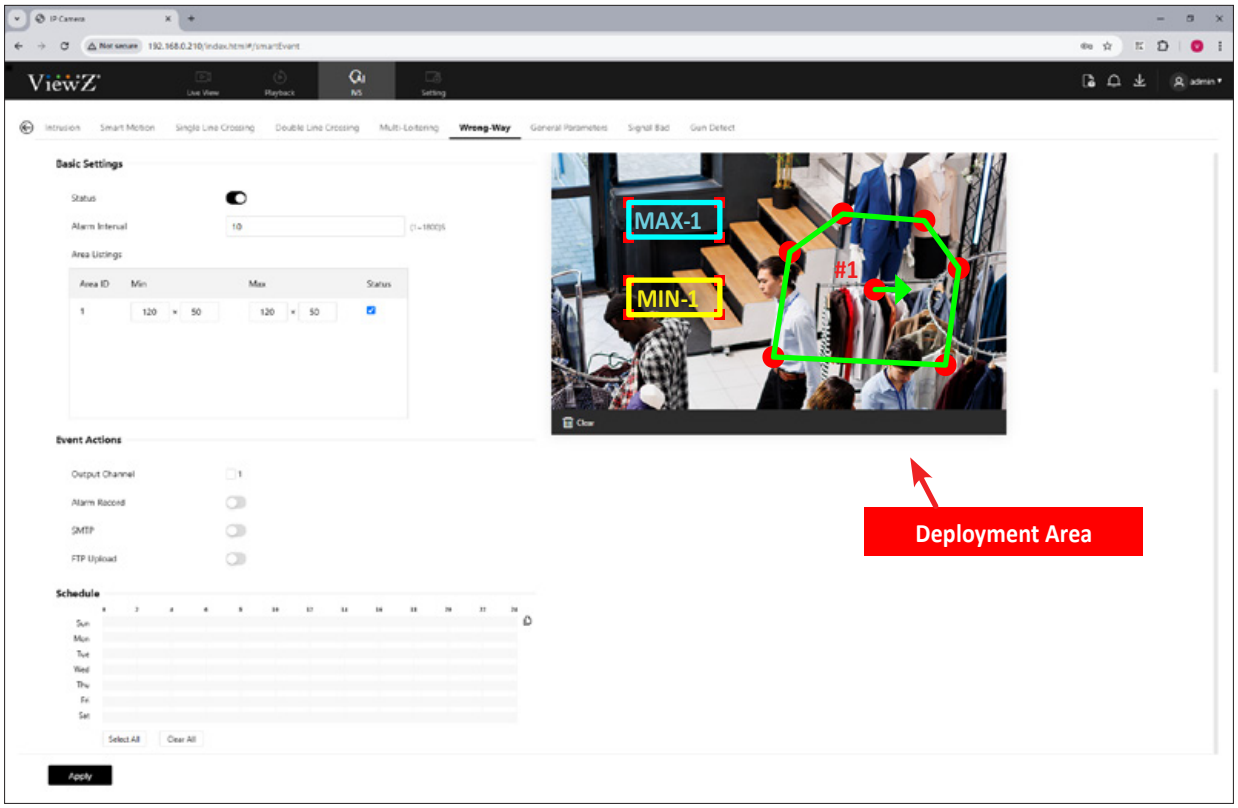


Figure 10-8 Wrong-Way

Step 2 Set **Wrong-Way** parameters as shown in Table 10-7.

Step 3 Setup **Deployment Area**

- Move the cursor to the drawing interface and click to generate a point, move the cursor to draw a line, and then click to generate another point. This is how a line is generated. In this way, continue to draw lines to form any shape, and right-click to finish line drawing, move the arrow in the field can set the direction of converse.

IVS / INTELLIGENT ANALYSIS

6. IVS - Intelligent Analysis - Wrong-Way

Procedure

Table 10-7 Wrong-Way

Parameter	DESCRIPTION	Setting
Status	Enable/disable the wrong way	Default Value: OFF
Alarm Interval	During the time interval, the same alarm will be only sent once.	Default Value: 0 (1 ~ 1800) sec
Area Listings	Set the areas will show in listings. Tick the status, the min and max detecting area show on area, user can drag the point to adjust the size of the detecting area, or modify the value directly.	Default Value: OFF
Output Channel	If user check to set the Output Channel and the device is connected to an external alarm indicator, the alarm indicator signals will send to external device when an alarm is triggered. NOTE The alarm output will only work for some models	Default Value: OFF
Alarm Record	The device will record alarm signal to the SD card	Default Value: OFF
SMTP	Enable/disable uploading onto SMTP server connection The parameter of SMTP can be setup at Setting > Network > Advanced Settings > SMTP	Default Value: OFF
FTP Upload	Enable/disable uploading onto FTP server connection The parameter of FTP can be setup at Setting > Network > Advanced Settings > FTP	Default Value: OFF

Note

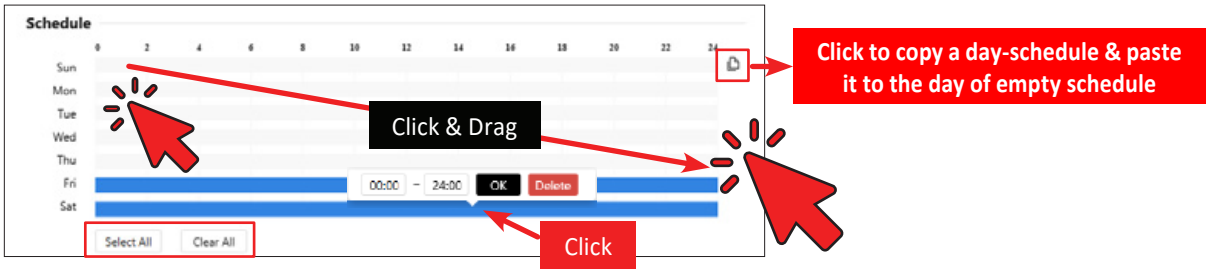
- A drawn line cannot cross another one, or the line drawing fails.
- Any shape with 8 sides at most can be drawn.
- The quantity of deployment areas is up to 8.

IVS / INTELLIGENT ANALYSIS

6. IVS - Intelligent Analysis - Wrong-Way

Procedure

Step 4 Configure the **Schedule** time setting.



To setup the schedule of **Wrong-Way**, user need to make a time table on Schedule

- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time-schedule or **Clear All** to remove all time-schedule.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

Step 5 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

IVS / INTELLIGENT ANALYSIS

7. IVS - Intelligent Analysis - General Parameters

Description

At **General Parameters** page, users can set target filtering to filter the target (people or others) at the setting filtering time. When targets occur in the detection area, it will not trigger the alarms of intelligent analysis, as shown in Figure 10-9.

Procedure

Step 1 Click **IVS** on the top menu, **Intelligent Analysis > General Parameters**

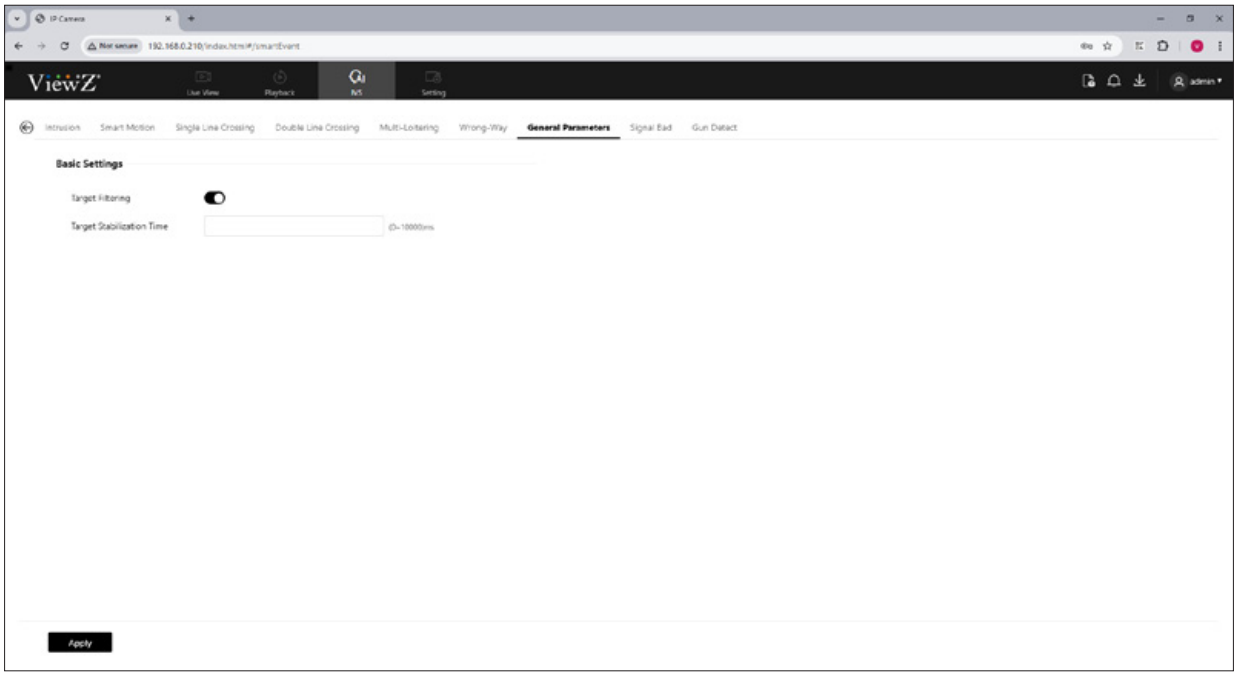


Figure 10-9 General Parameters

Step 2 Enable **Target Filtering** & set the **Target Stabilization Time**

Step 3 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

IVS / INTELLIGENT ANALYSIS

8. IVS - Intelligent Analysis - Signal Bad

Description & Procedure

Signal Bad alarm activates when someone tries to interfere with or obstruct the camera. Such as blocking, moving and physical tampering as shown in Figure 10-10.

Step 1 Click **IVS** on the top menu, **Intelligent Analysis > Signal Bad**

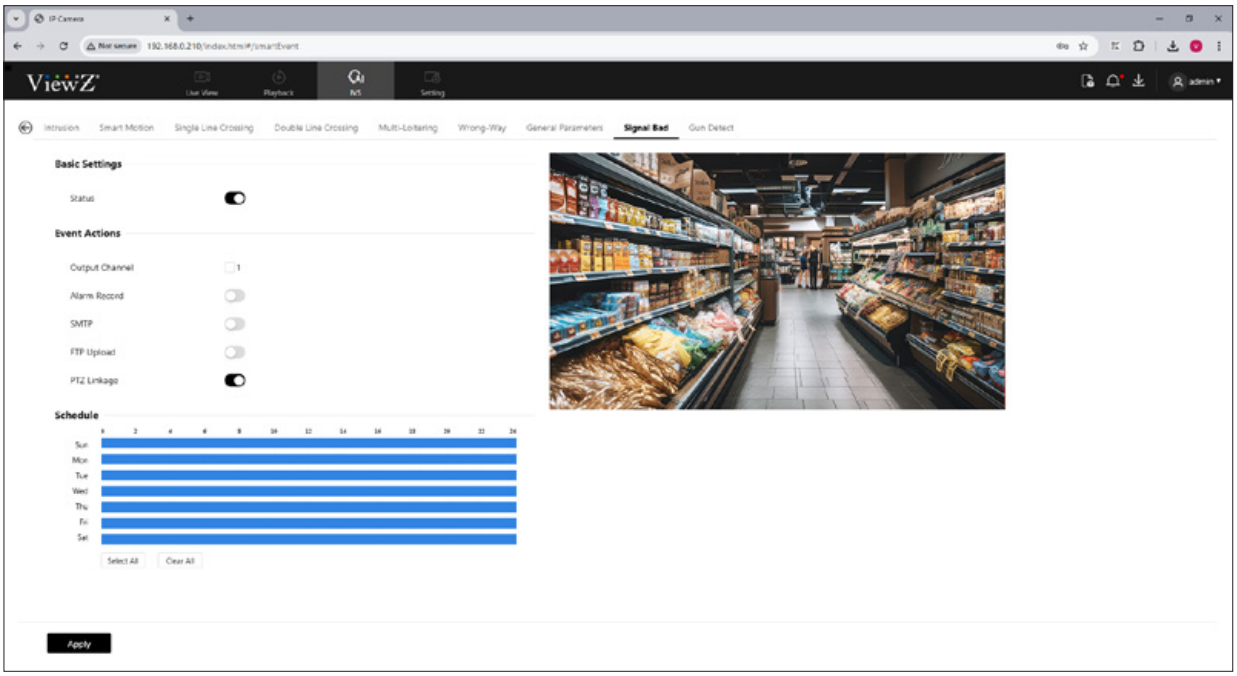


Figure 10-10 Signal Bad

Step 2 Set **Signal Bad** parameters as shown in Table 10-8.

Table 10-8 Signal Bad

Parameter	DESCRIPTION	Setting
Status	Enable/disable the signal bad	Default Value: OFF
Output Channel	If user check to set the Output Channel and the device is connected to an external alarm indicator, the alarm indicator signals will send to external device when an alarm is triggered. NOTE The alarm output will only work for some models	Default Value: OFF

IVS / INTELLIGENT ANALYSIS

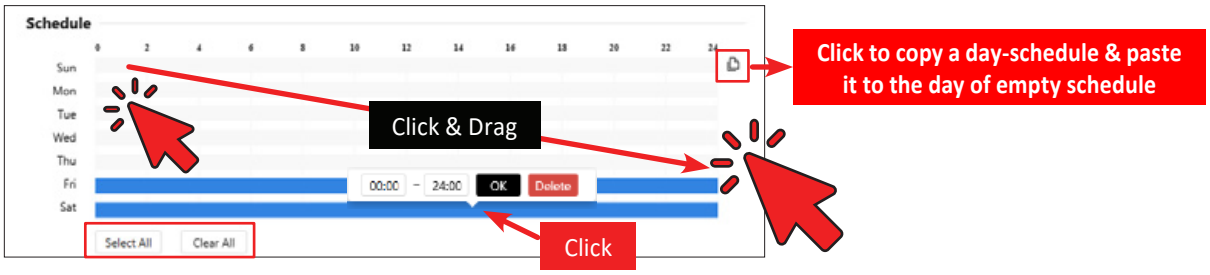
8. IVS - Intelligent Analysis - Signal Bad

Procedure

Table 10-8 Signal Bad

Parameter	DESCRIPTION	Setting
Alarm Record	The device will record alarm signal to the SD card	Default Value: OFF
SMTP	Enable/disable uploading onto SMTP server connection The parameter of SMTP can be setup at Setting > Network > Advanced Settings > SMTP	Default Value: OFF
FTP Upload	Enable/disable uploading onto FTP server connection The parameter of FTP can be setup at Setting > Network > Advanced Settings > FTP	Default Value: OFF
PTZ Linkage	Enable/disable PTZ control.	Default Value: OFF

Step 4 Configure the **Schedule** time setting.



To setup the schedule of **Gun Detect**, user need to make a time table on Schedule

- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time-schedule or **Clear All** to remove all time-schedule.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

Step 5 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

IVS / INTELLIGENT ANALYSIS

9. IVS - Intelligent Analysis - Gun Detect

Description

Gun Detect allows AI PVM to identify guns in video feeds. When a gun is detected, the system sends an alert to ViewZ IMS system & AI PVM's emergency alert, as shown in Figure 10-11.

Procedure

Step 1 Click **IVS** on the top menu, **Intelligent Analysis > Gun Detect**

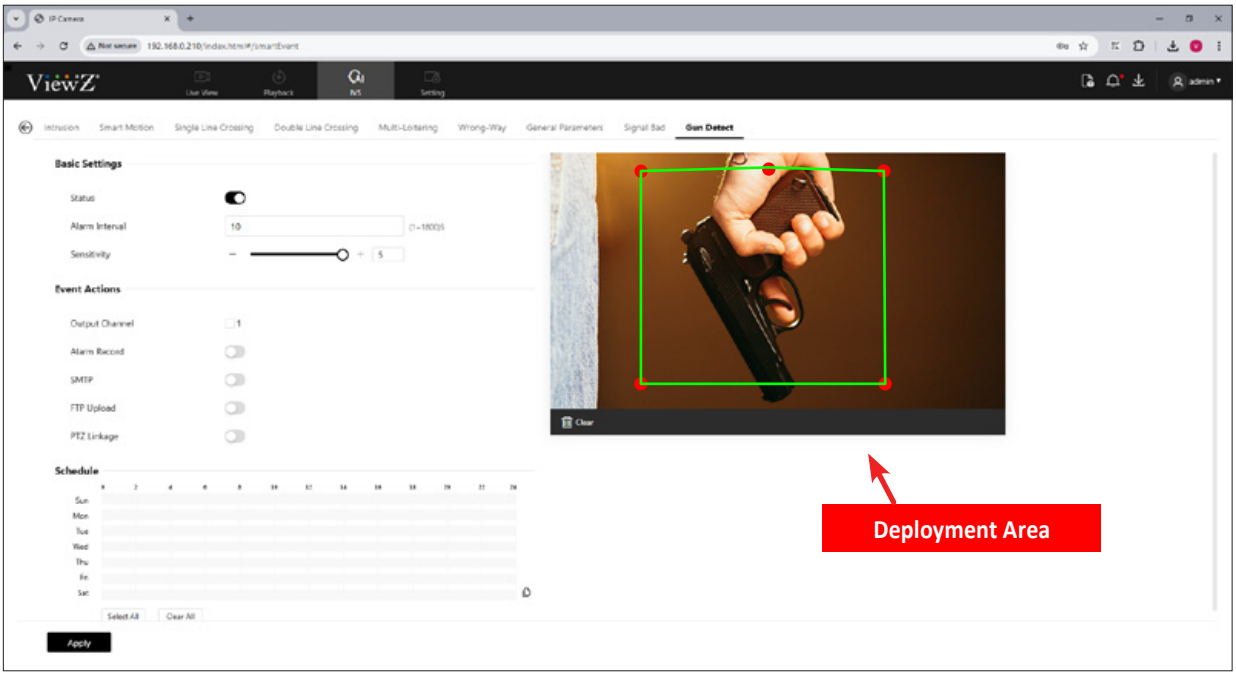


Figure 10-11 Gun Detect

Step 2 Set **Gun Detect** parameters as shown in Table 10-9.

Step 3 Setup **Deployment Area**

- Move the cursor to the drawing interface and click to generate a point, move the cursor to draw a line, and then click to generate another point. This is how a line is generated. In this way, continue to draw lines to form any shape, and right-click to finish line drawing, move the arrow in the field can set the direction of converse.

IVS / INTELLIGENT ANALYSIS

9. IVS - Intelligent Analysis - Gun Detect

Procedure

Table 10-9 Gun Detect

Parameter	DESCRIPTION	Setting
Status	Enable/disable the gun detect alarm	Default Value: OFF
Alarm Interval	During the time interval, the same alarm will be only sent once.	Default Value: 0 (1 ~ 1800) sec
Sensitivity	The sensitivity of detecting the target, when the value is high, the target can be detected easily, but the accuracy will be lower.	Default Value: 1 (1 ~ 5)
Output Channel	If user check to set the Output Channel and the device is connected to an external alarm indicator, the alarm indicator signals will send to external device when an alarm is triggered. NOTE The alarm output will only work for some models	Default Value: OFF
Alarm Record	The device will record alarm signal to the SD card	Default Value: OFF
SMTP	Enable/disable uploading onto SMTP server connection The parameter of SMTP can be setup at Setting > Network > Advanced Settings > SMTP	Default Value: OFF
FTP Upload	Enable/disable uploading onto FTP server connection The parameter of FTP can be setup at Setting > Network > Advanced Settings > FTP	Default Value: OFF
PTZ Linkage	Enable/disable PTZ control	Default Value: OFF

Note

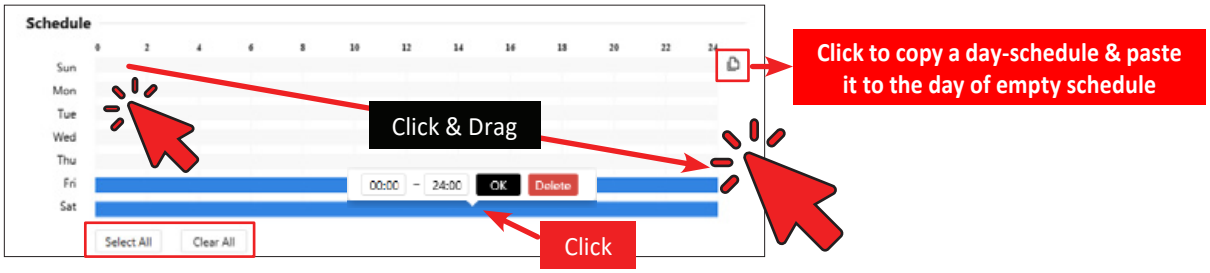
- On the deployment area, a drawn line cannot cross another one, or the line drawing fails.
- On the deployment area, any shape with 8 sides, can be drawn.
- On the deployment area, the quantity of deployment areas is up to 8.

IVS / INTELLIGENT ANALYSIS

9. IVS - Intelligent Analysis - Gun Detect

Procedure

Step 4 Configure the **Schedule** time setting.



To setup the schedule of **Gun Detect**, user need to make a time table on Schedule

- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time-schedule or **Clear All** to remove all time-schedule.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

Step 5 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

IVS / BEHAVIOR ANALYSIS

1. IVS - Behavior Analysis - People Count

Description

People Count allows AI PVM to count the number of people who come in/out, on the camera view of AI PVM, as shown in Figure 10-12.

Procedure

Step 1 Click **IVS** on the top menu, **Intelligent Analysis > People Count**

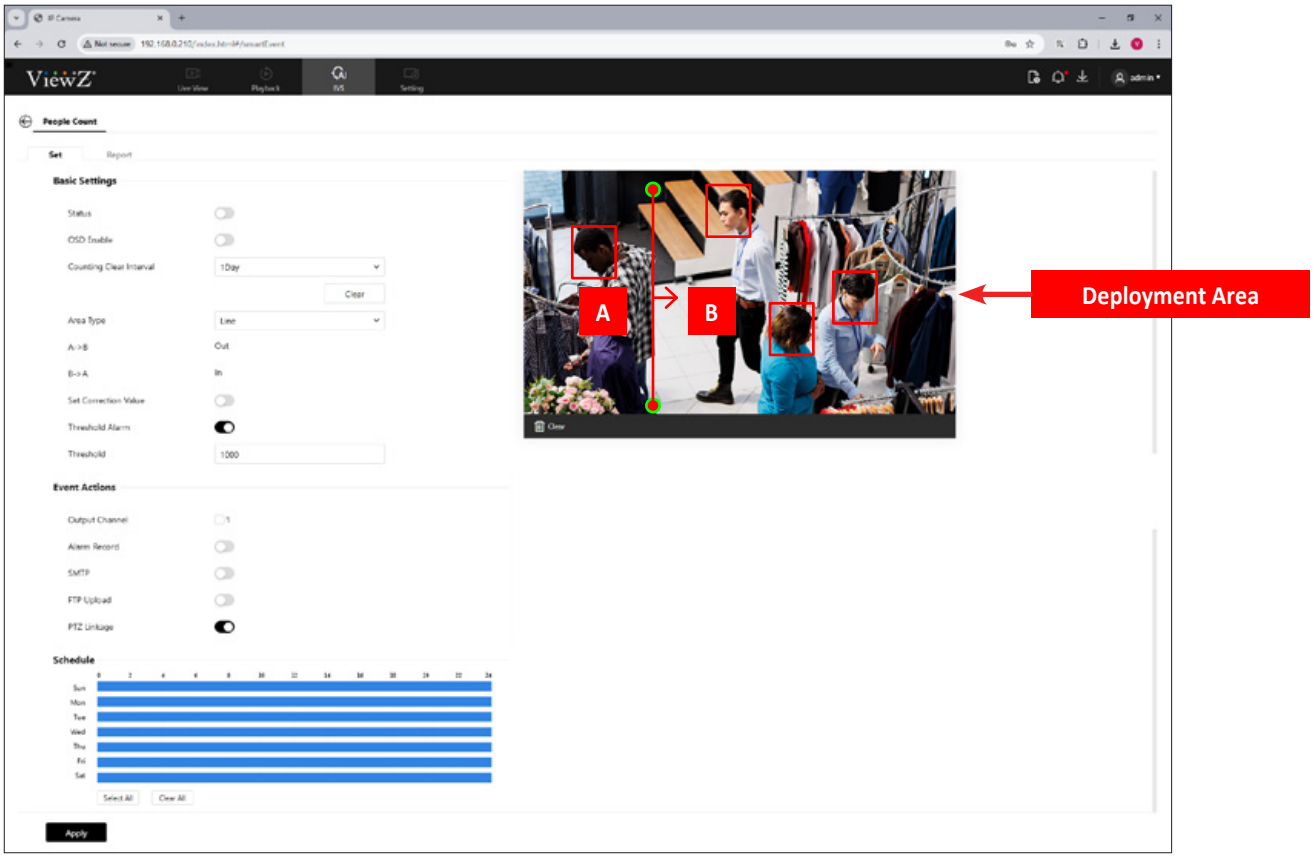


Figure 10-12 People Count

Step 2 Set **People Count** parameters as shown in Table 10-10.

Step 3 Setup **Deployment Area**

- On the deployment area, click to generate a point, hold & move the cursor to draw a line, and then release the cursor. This is how a line is generated.
- The starting point of arrow is the area 'A' and end point of arrow is the area 'B'
- When user generate a line and click top area & draw down, the arrow direction is the right and vice versa.

IVS / INTELLIGENT ANALYSIS

1. IVS - Behavior Analysis - People Count

Procedure

Table 10-10 People Count

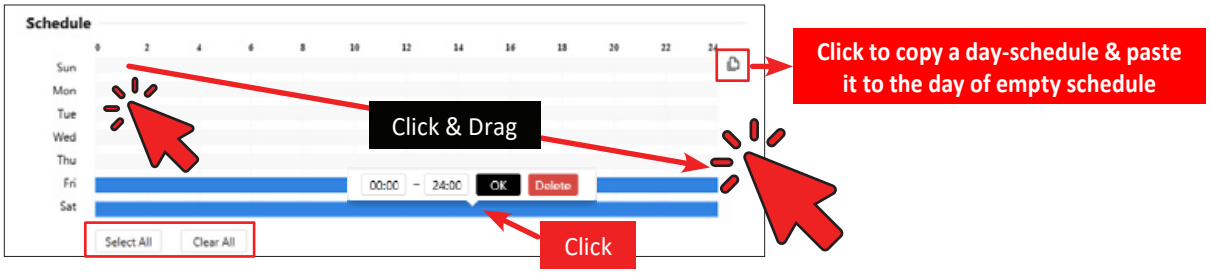
Parameter	DESCRIPTION	Setting
Status	Enable/disable the people count alarm	Default Value: OFF
OSD Enable	Enable the OSD, the count data will show on live video screen.	Default Value: OFF
Counting Clear Interval	The camera will clear counting data at the setting interval. Click **Clear** button to clear the data immediately.	Default Value: 12 Hour 10 min, half-hour, 1 hour, 12 hour, 1 day, custom time
Area Type	Draw a line on live video screen. The label of A and B indicate out and in. Out: A → B | In: B → A	Default Value: Line
Set Correction Value	Enable, set the count correction value, it can be positive or negative. For example, if there are 30 people enter the area before counting, input 30 to to correct. If 30 people go out the area, input -30.	Default Value: OFF
Threshold Alarm	Enable/disable the threshold alarm	Default Value: OFF
Output Channel	If user check to set the Output Channel and the device is connected to an external alarm indicator, the alarm indicator signals will send to external device when an alarm is triggered. NOTE The alarm output will only work for some models	Default Value: OFF
Alarm Record	The device will record alarm signal to the SD card	Default Value: OFF
SMTP	Enable/disable uploading onto SMTP server connection The parameter of SMTP can be setup at Setting > Network > Advanced Settings > SMTP	Default Value: OFF
FTP Upload	Enable/disable uploading onto FTP server connection The parameter of FTP can be setup at Setting > Network > Advanced Settings > FTP	Default Value: OFF
PTZ Linkage	Enable/disable PTZ control	Default Value: OFF

IVS / INTELLIGENT ANALYSIS

1. IVS - Behavior Analysis - People Count

Procedure

Step 4 Configure the **Schedule** time setting.



To setup the schedule of **People Count**, user need to make a time table on Schedule

- On the schedule, hold down the left mouse button, drag and release mouse to select the deployment time within 0:00-24:00 from Monday to Sunday.
- User can click **Select All** to setup all time-schedule or **Clear All** to remove all time-schedule.
- User can also copy & paste a daily schedule, click to copy to other days.
- User can setup a specific time range & delete a day schedule by clicking the blue bar on time table

Step 5 Click **Apply** button to apply the updated parameters.

- If the message "Apply success!" is displayed, the system will save the settings.
- If other information is displayed, set the parameters correctly.

IVS / BEHAVIOR ANALYSIS

2. IVS - Behavior Analysis - Report

Description

At people counting interface, user can view the data of people counting through setting query condition (choose the detail time at the date's pop-up window). There are 3 modes to show the data, such as line chart, histogram and list, as shown in Figure 10-13.

Procedure

Step 1 Click **IVS** on the top menu, **Intelligent Analysis > Report**

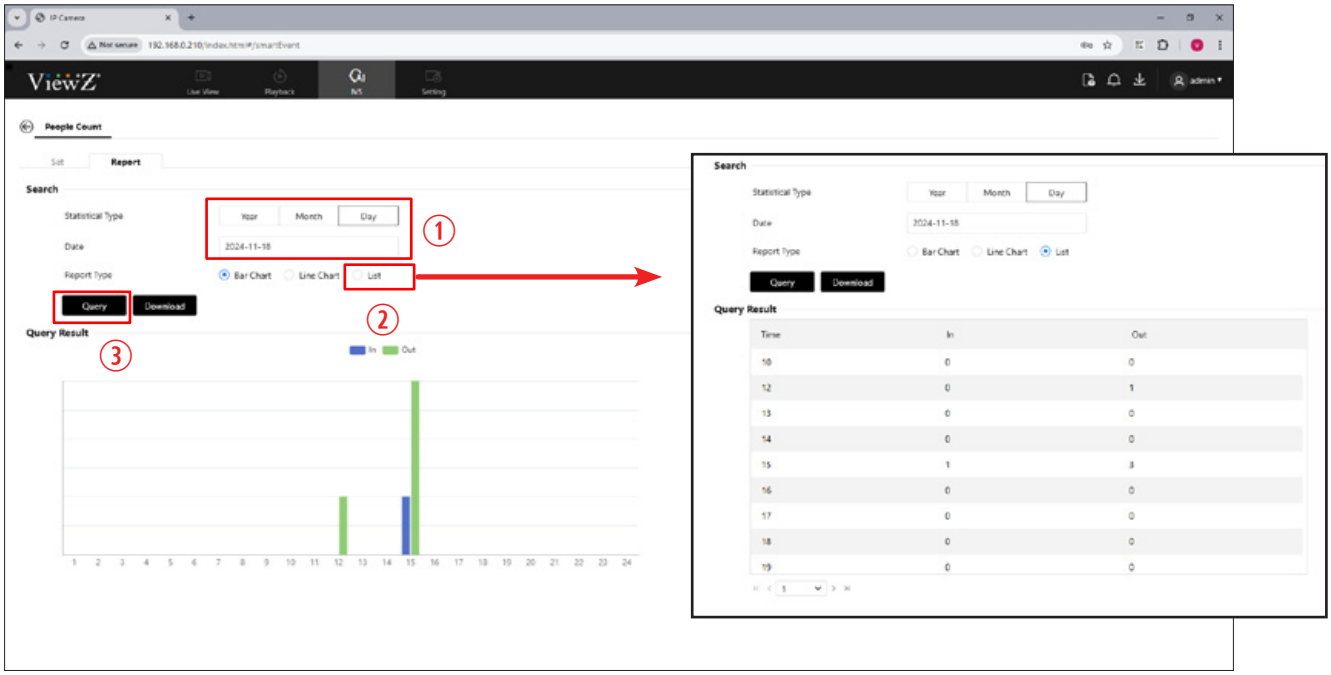


Figure 10-13 Report

Step 2 Select **Report** to download & see the report

Step 3 Select a statistical type - **Year**, **Month** & **Day**, and pick a **Year**, **Month** & **Date**

Step 4 Select a report type - **Bar Chart**, **Line Chart** and **List**

Step 5 Click **Query** to get the data from AI PVM and then the record will be shown at Query Result.

IVS / BEHAVIOR ANALYSIS

2. IVS - Behavior Analysis - Report

Procedure

Step 5 Click **Download** to save the data as an excel file into the local computer.

Note

- When user downloads an excel file (report file) and try to open this, user might see the warning or error message such as '***The file format and extension don't match~***' as shown in Figure 10-14.
  This message means the downloaded excel file does not match with the MS Office Excel version of user computer. But, there is no issue to open the downloaded excel file. Even if the MS Office Excel system could try to fix the issue automatically, we want user to ignore the error message and process to open an excel file.
- When user tries to open the downloaded excel file, came from **People Count Report**, **Operation Log**, **Alarm Log** and etc., user might see the similar or same warning message. Please ignore this warnig message to open & save log data.

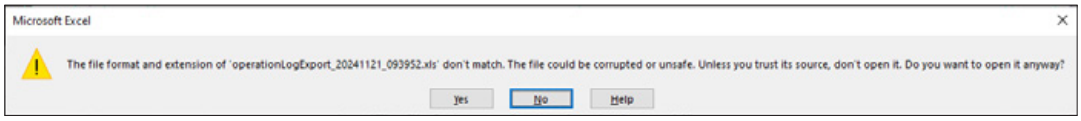


Figure 10-14 Excel Warning Message

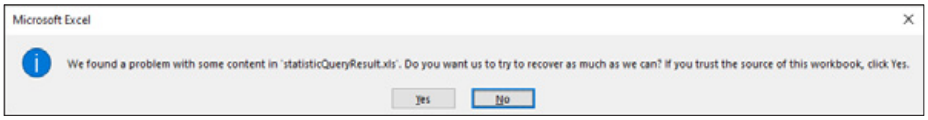


Figure 10-14 Excel Warning Message

NOTE

NOTE