



Network Camera
Web Operation Manual
XYZ DIGITAL PVT LTD

NOTE AS IMPORTANT

The following cybersecurity recommendations are for reference only. Some series of the products may not support all the recommendations that are listed below.

Cybersecurity Recommendations

1. Change the default Passwords and create strong password

The password change is required to maintain its security ,so that our systems do not get hacked due to weak or default passwords. It is strongly recommended to change the default password immediately and choose a strong password whenever possible. A strong password must have at least 8 characters long that contains a special character, numbers, an upper-case, and lower-case letters.

2. Update Firmware

As per the standard procedure in the cctv -industry, we recommend you keep NVR and IP camera firmware updated to ensure the system is up to date with the latest security files.

A few Tips to improve your security.

1. Change Passwords Regularly:

Regularly change the passwords to your devices to ensure that only authorized users can access the system.

2. Change Default HTTP Ports:

- Change default HTTP ports for systems as required. These ports were used to communicate and view video feeds remotely.
- These ports can be changed to any set of numbers between 1-65535. Avoid the default port numbers that can reduce the risk of unauthorized being able to guess which ports you're using.

3. Enable HTTPS/SSL:

Prebuilt certificate for HTTPS.

4. Security Exception:

Security exceptions may be triggered by unauthorized access attempts, invalid user roles, incorrect encryption protocols, or connection requests from untrusted devices. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

5. Connect IP Cameras to PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

6. Isolate NVR and IP Camera Network:

The network your NVR and IP camera reside on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs to function properly.

Electrical safety

- All installation and operation should conform to your local electrical safety codes.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with voltage rated by DC 12 V and POE, according to the limited power source requirement of IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Ensure the power supply is correct before operating the device.
- A readily accessible disconnect device shall be incorporated into the building installation wiring.
- Prevent the power cable from being trampled or pressed, especially the plug, power socket and the junction extruded from the device.
- We assume no liability or responsibility for all the fires or electrical shock caused by improper handling or installation.

Environment

- Do not aim the device at strong light to focus, such as lamp light and sun light, otherwise it might cause over brightness or light marks, which are not the device malfunction, and affect the longevity of Charge Coupled Device (CCD) or Complementary Metal-Oxide Semiconductor (CMOS).
- Do not place the device in a damp or dusty environment, extremely hot or cold temperatures, or the locations with strong electromagnetic radiation or unstable lightning.
- Keep the camera away from water or other liquid to avoid damage to the internal components.
- Keep the indoor device away from rain or damp to avoid fire or lightning.
- Keep sound ventilation to avoid heat accumulation.

- Transport, use and store the device within the range of humidity and temperature.
- Heavy stress, violent vibration or water splashes are not allowed during transportation, storage and installation.
- Pack the device with standard factory packaging or the equivalent material when transporting the device.

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate numbers, Email address, phone numbers, GPS, and so on. You need to follow the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures including but not limited to providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The Manual is for reference only. If there is any inconsistency between the Manual and the actual product, the actual product shall govern.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The Manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's Manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Manual. Please contact customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Table of Contents

1. Overview of the Product	
2. Start Configuration on web page	
2.1 Device Initialisation	
2.2 Default username & password	
2.3 Change to new password &Reset Password with mail	
3. Live	
4. Setup with Device information.....	
5. Time setting.....	
6. Audio setting.....	
7. Video setting.....	
7.1 Video.....	
7.2 Display setting.....	
7.3 Day & Night.....	
7.4 OSD Setting.....	
7.5 Privacy Masking.....	
8. Event Setting.....	
8.1 Motion detection.....	
8.2 Video Tampering.....	
8.3 Human Detection.....	
8.4 Line Intrusion.....	
9. Network Setting.....	
10. Email setting.....	
11. Maintenance.....	
11.1 Factory Setting.....	
11.2 OTA.....	

1. Overview of the Product

An IP (Internet Protocol) camera is a digital surveillance device that connects to a network using a network cable. It can also be connected through a router or switch, allowing real-time video transmission over the network or local network. The networking mode for an IP camera is to connect an IP camera to PC via router or switch or using a network cable.

Before you access a network camera via the internet, you need to obtain its IP address. Users can search for the IP address of the network camera via an *IP* search tool.

2. Starting Configuration on webpage

In this section, it describes the device initial config operation that includes Device Initialization, Device Login, and Reset Password in a WEB interface.

2.1 Device Initialization

Device initialization is required for first-time use only. This manual is focused on the operation on the web page. You can also initialize the device through the IP search tool, NVR (Network Video Recorder).

Note:

- To ensure device security, protect your password after device initialization and update it regularly.
- During initialization, make sure the PC IP and camera IP are on the same network.
- We recommend using Internet Explorer or Google Chrome.

-Open the web browser, enter the IP address of the device in the address bar, and then press **Sign in**.

NOTE: By default, the IP address is in DHCP, you have to find IP address on NVR.

2.2 Default Username & Password -Enter the IP address of camera, you will get interface of camera put default username-**admin** and Password-**123456** and then click on **Sign in (As shown in figure 2.2)**

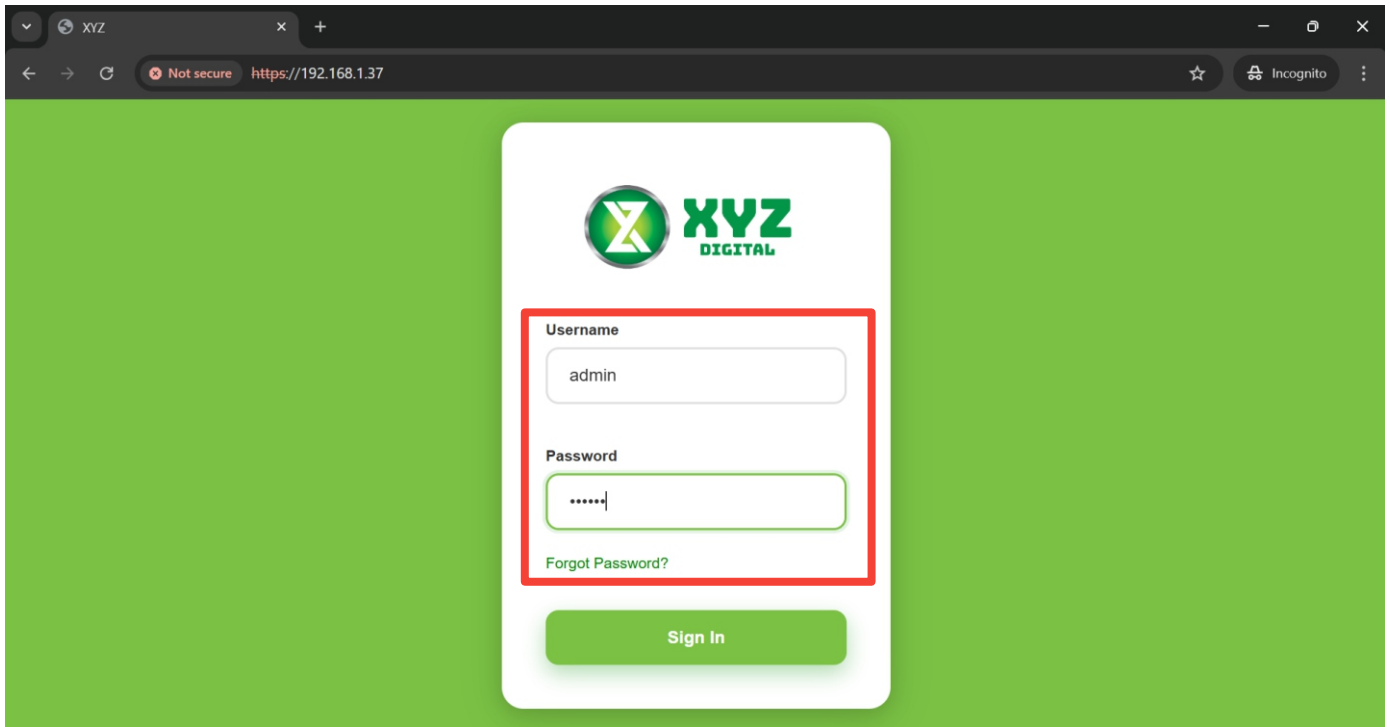


Fig-2.2

2.3 Change to new password & Reset Password with mail-After that you will get an email address column (enter your mail id for future password recovery) and create a new password then save & continue. **(As shown in figure 2.3)**

NOTE: New password is created to enhance your security.

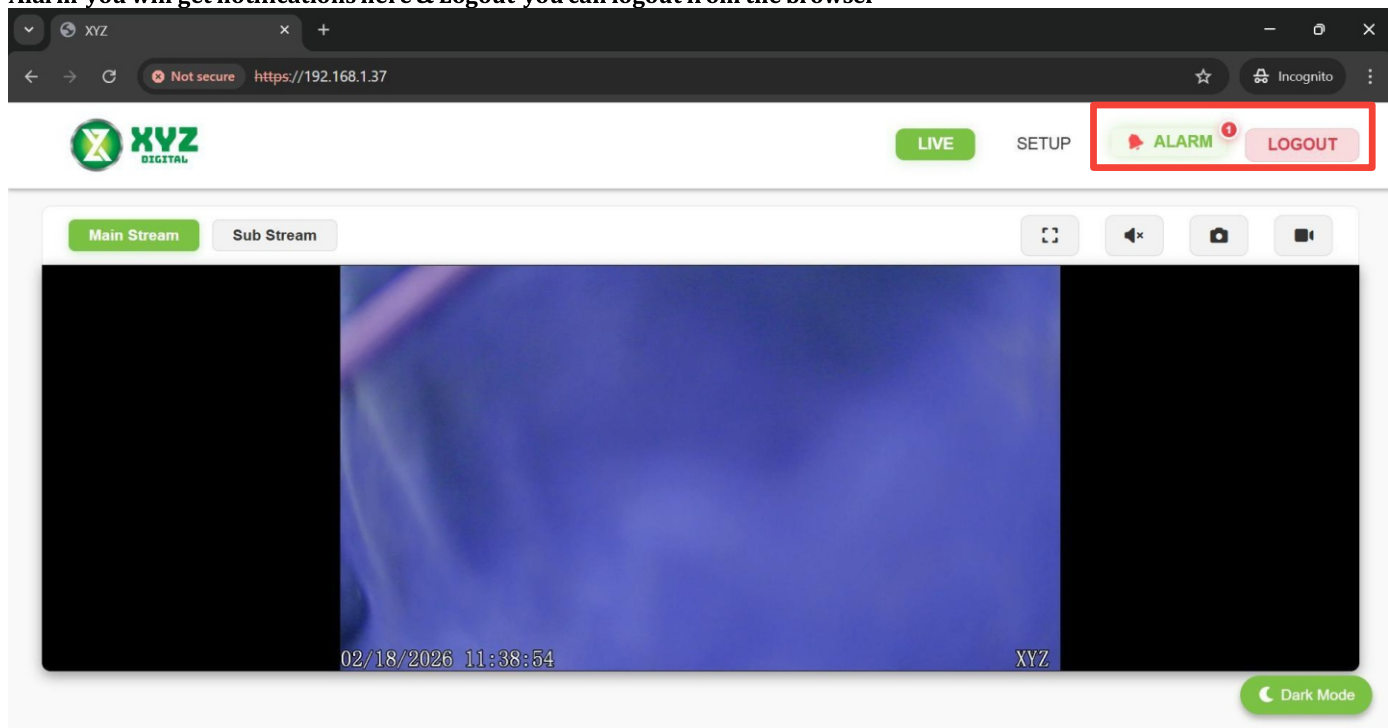
Fig- 2.3

Again login the page with a new password,you will get Live Option,click on Live to view the video .

3. Live video (Shown In figure below)

Mainstream & Substream are two different video stream method

Alarm-you will get notifications here & Logout-you can logout from the browser



4.SETUP-when you click on setup,you will get device information(with software version and Device model Number)(As shown in figure 4)

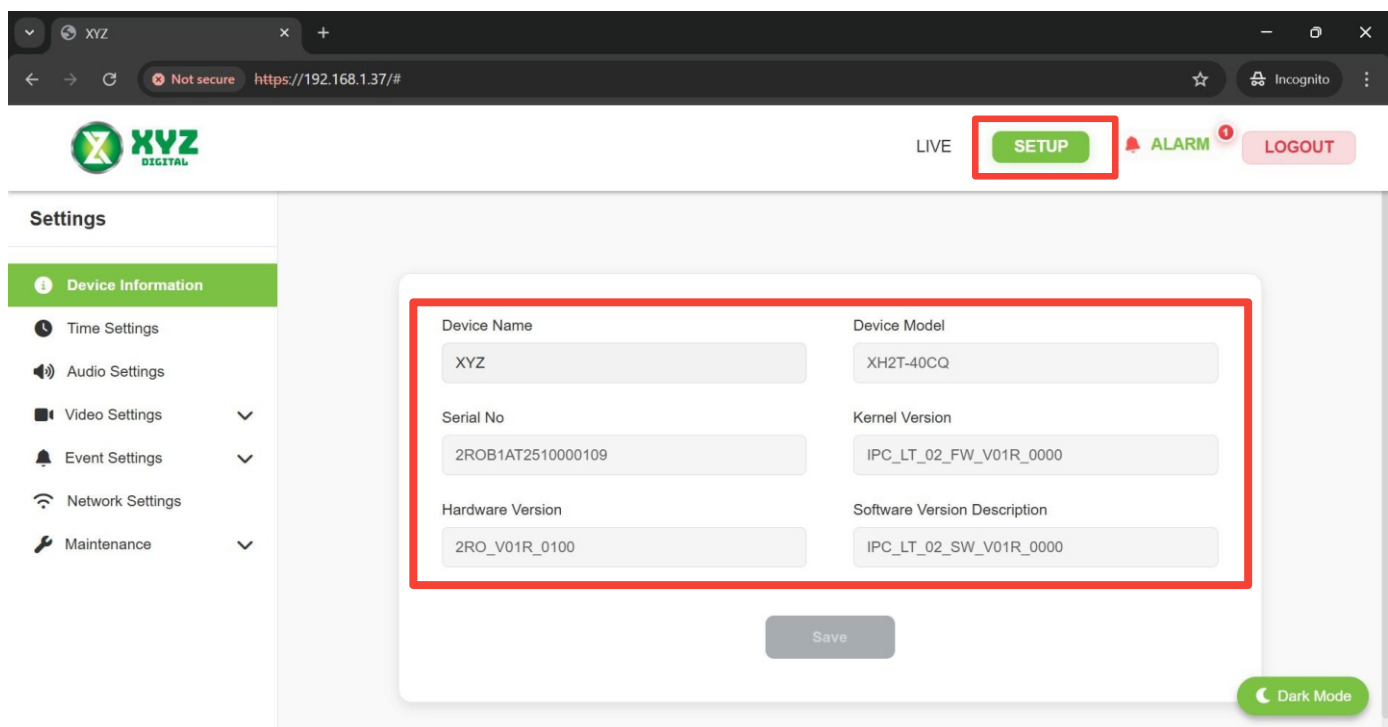


Fig- 4

5-After that you will get **TIME SETTINGS**(you can change time Zone in this interface)
(As shown in figure 5)

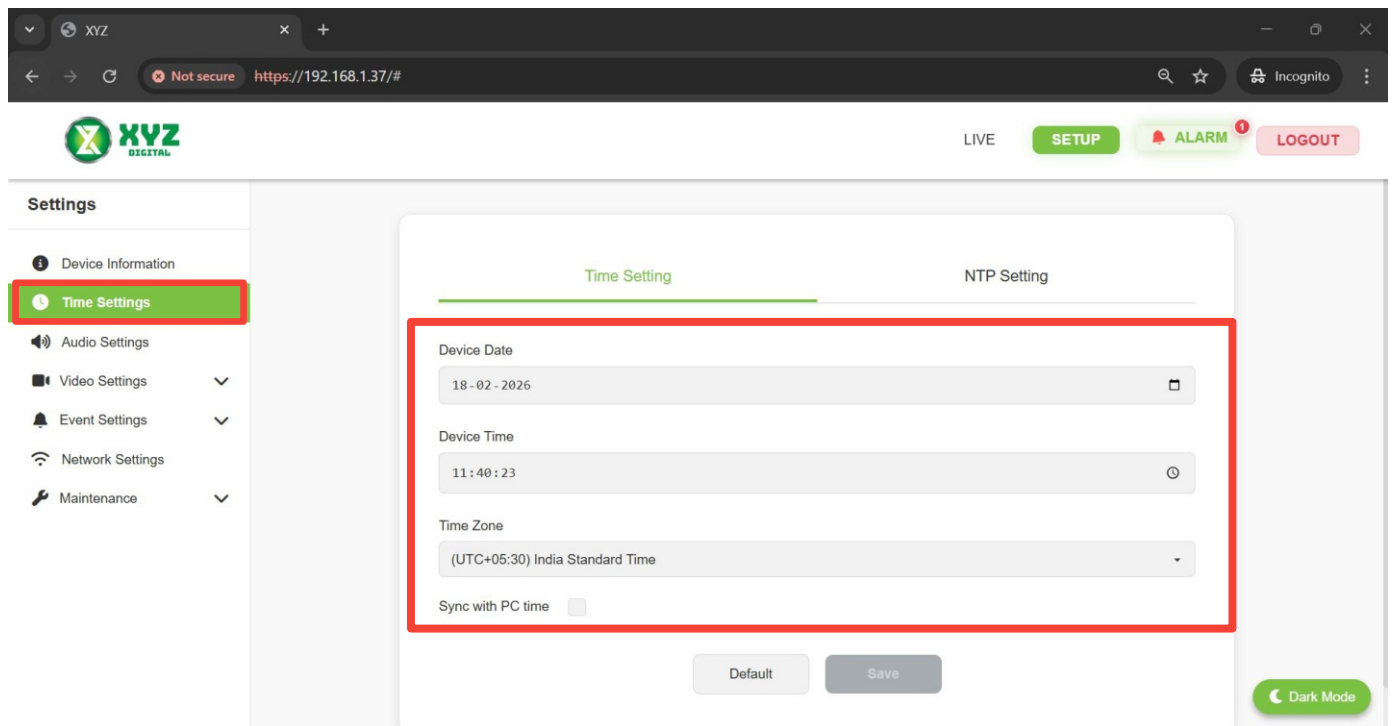


Fig-5

6-AUDIO SETTINGS(In this section user can manage input & output volume as per their requirements)
(As shown in figure 6)

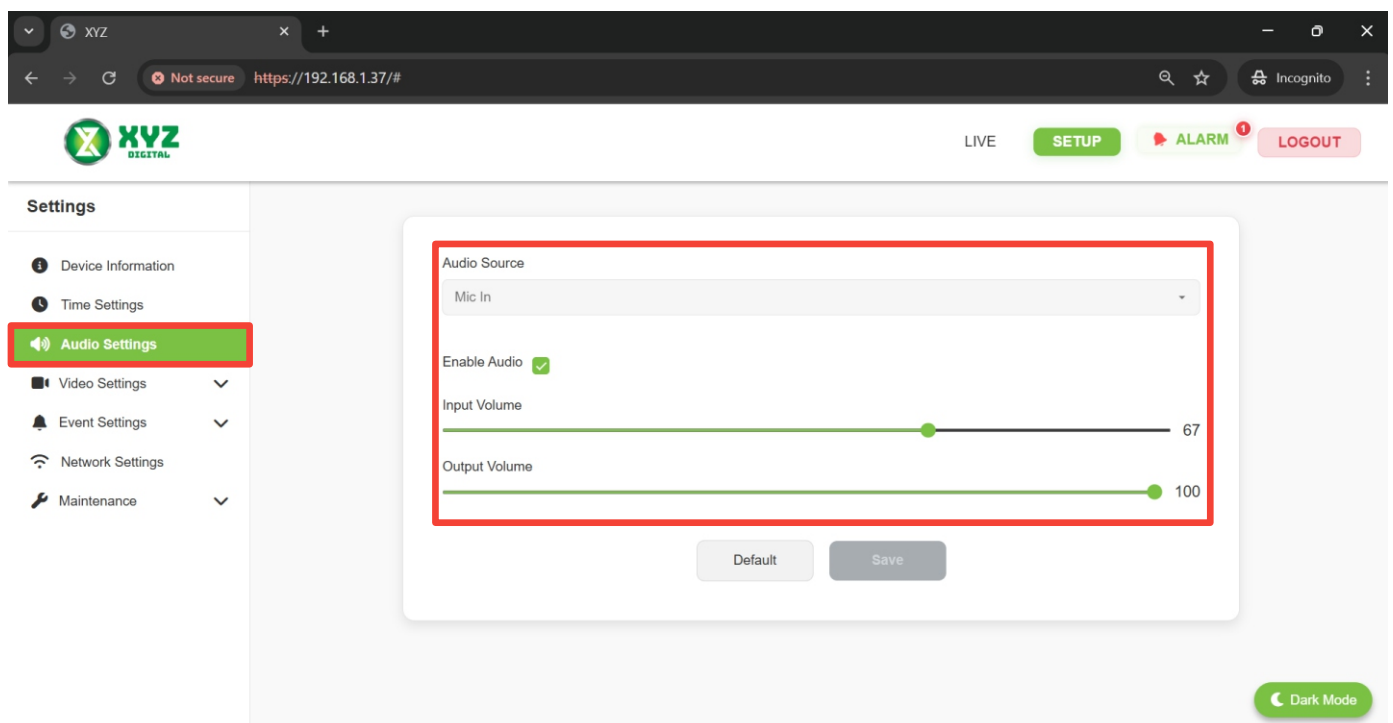


Fig-6

7- IDEO SETTING

7.1 -VIDEO-In this setting User can manage Video parameters with Codec Method

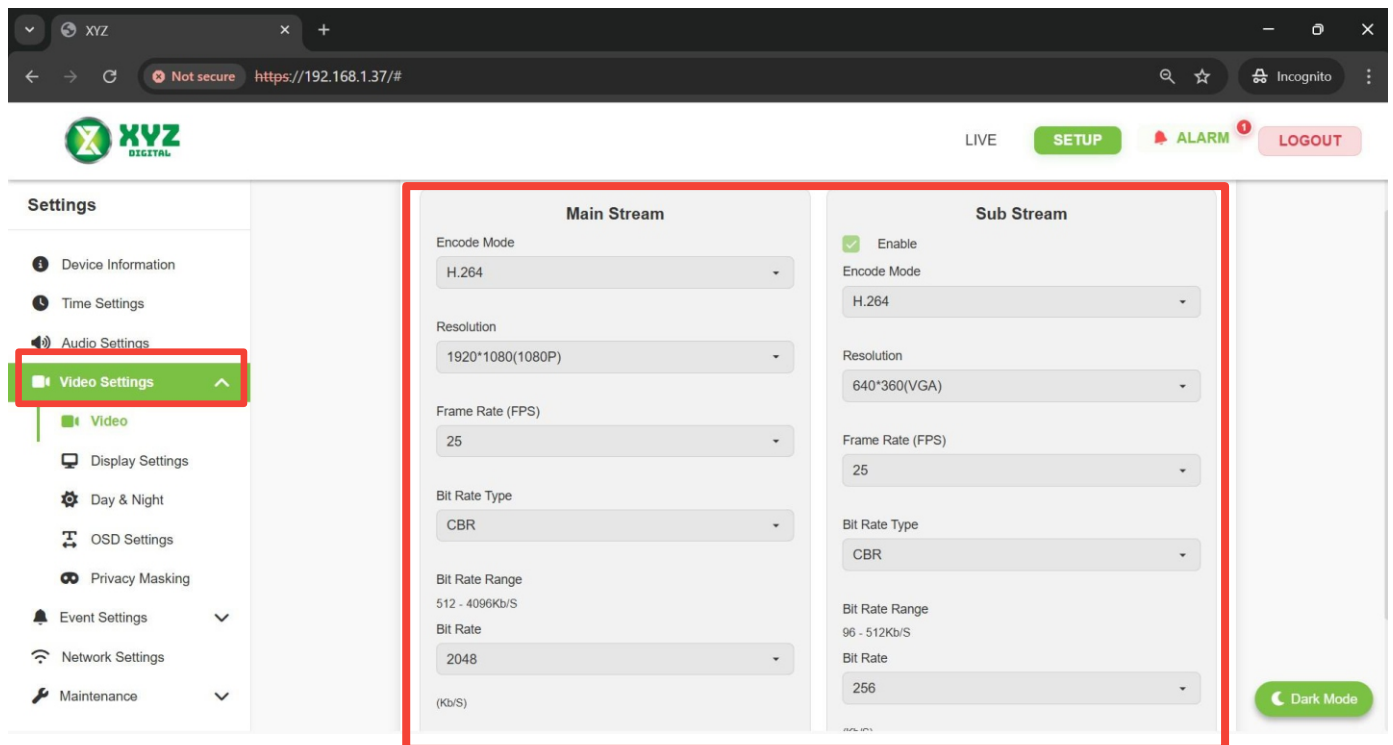


Fig 7.1

7.2- DISPLAY SETTINGS-In this section user can manage picture setting,exposure setting and White balance

7.2.1-PICTURE SETTINGS-User can manage these settings(adjusting image control Brightness, Contrast, Saturation,Hue) with this option.(As shown in figure 7.2.1)

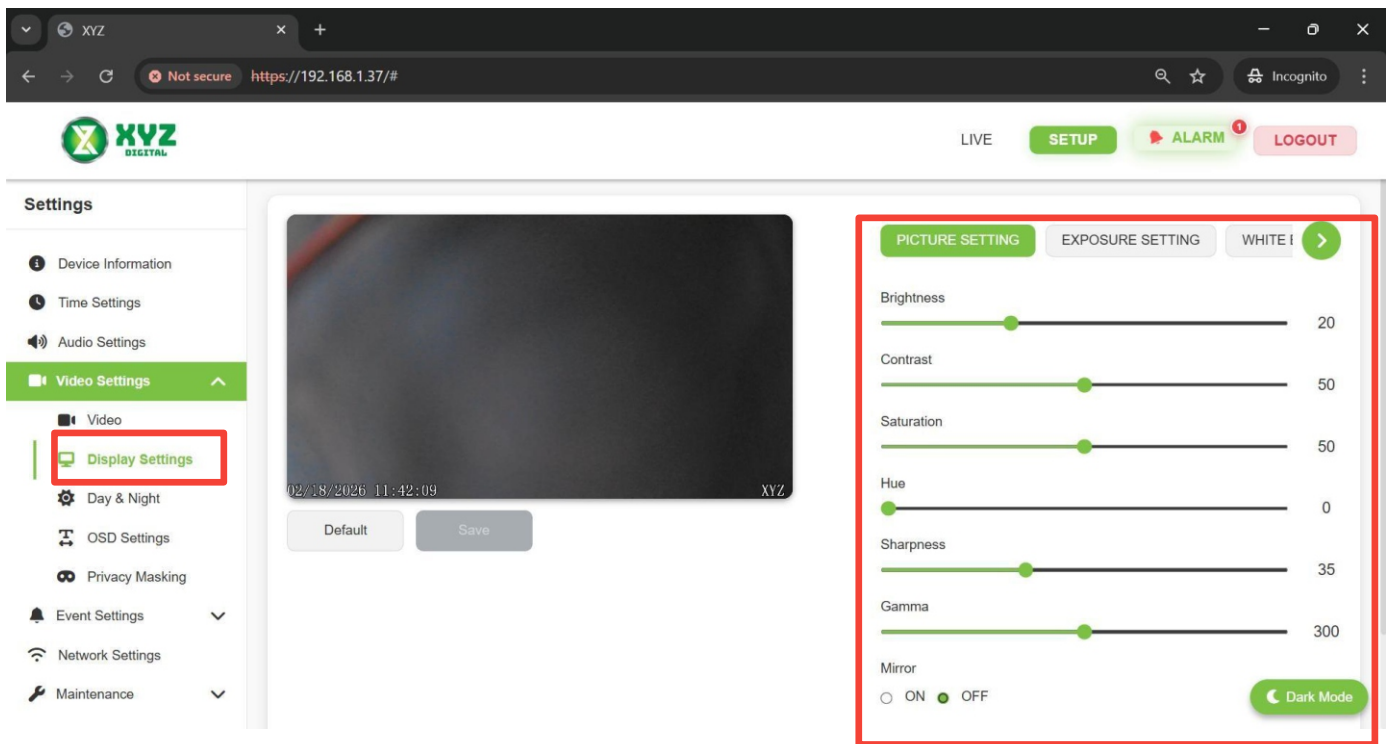


Fig- 7.2.1

7.2.2-EXPOSURE SETTINGS-control how much light reaches the sensor, balancing brightness and clarity by adjusting these factors.(As shown in Figure- 7.2.2)

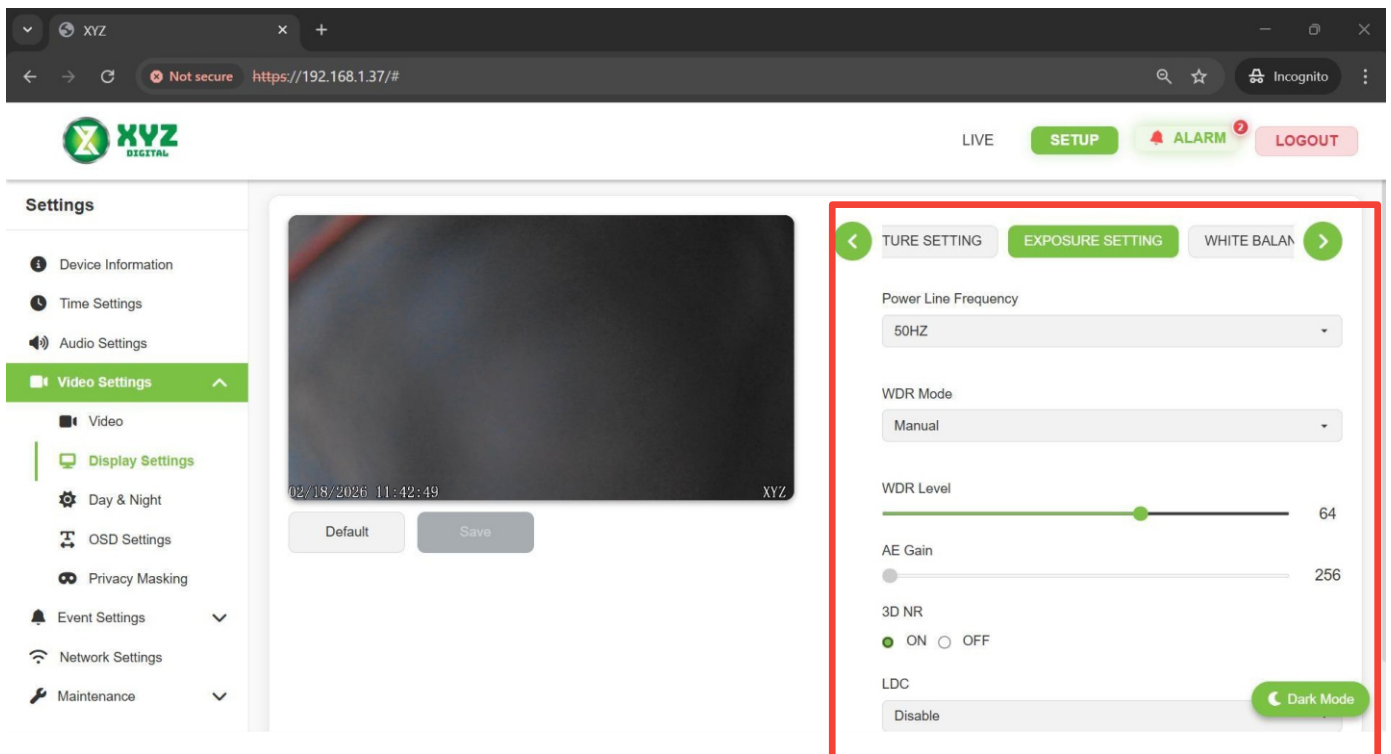


Fig- 7.2.2

7.2.3-WHITE BALANCE-Camera automatically detects and corrects color casts in real-time, great for dynamic lighting.(As shown in Figure- 7.2.3)

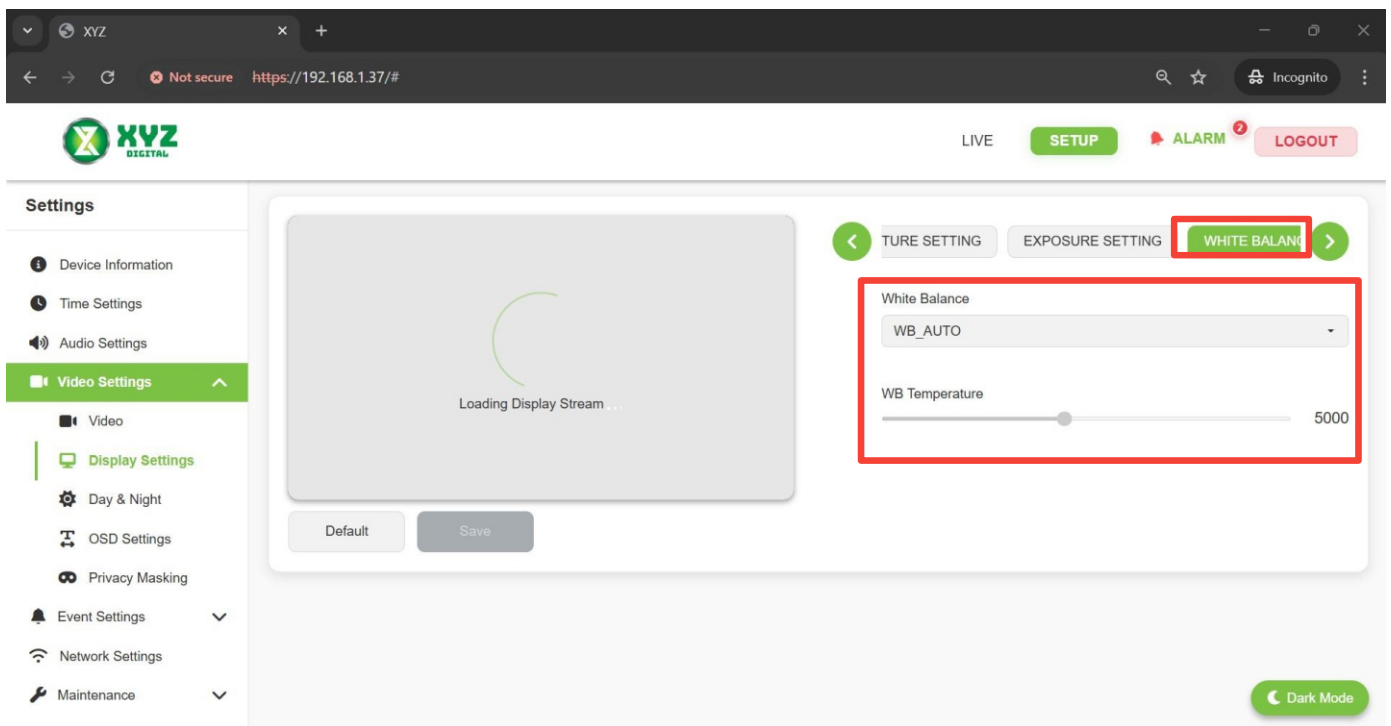


Fig- 7.2.3

7.3- DAY & NIGHT-In this section you will get Image setting, Illuminator settings& advance option

7.3.1-IMAGE SETTINGS-In this User can keep the mode according to the nature of the camera.(As shown in Figure- 7.2.3)

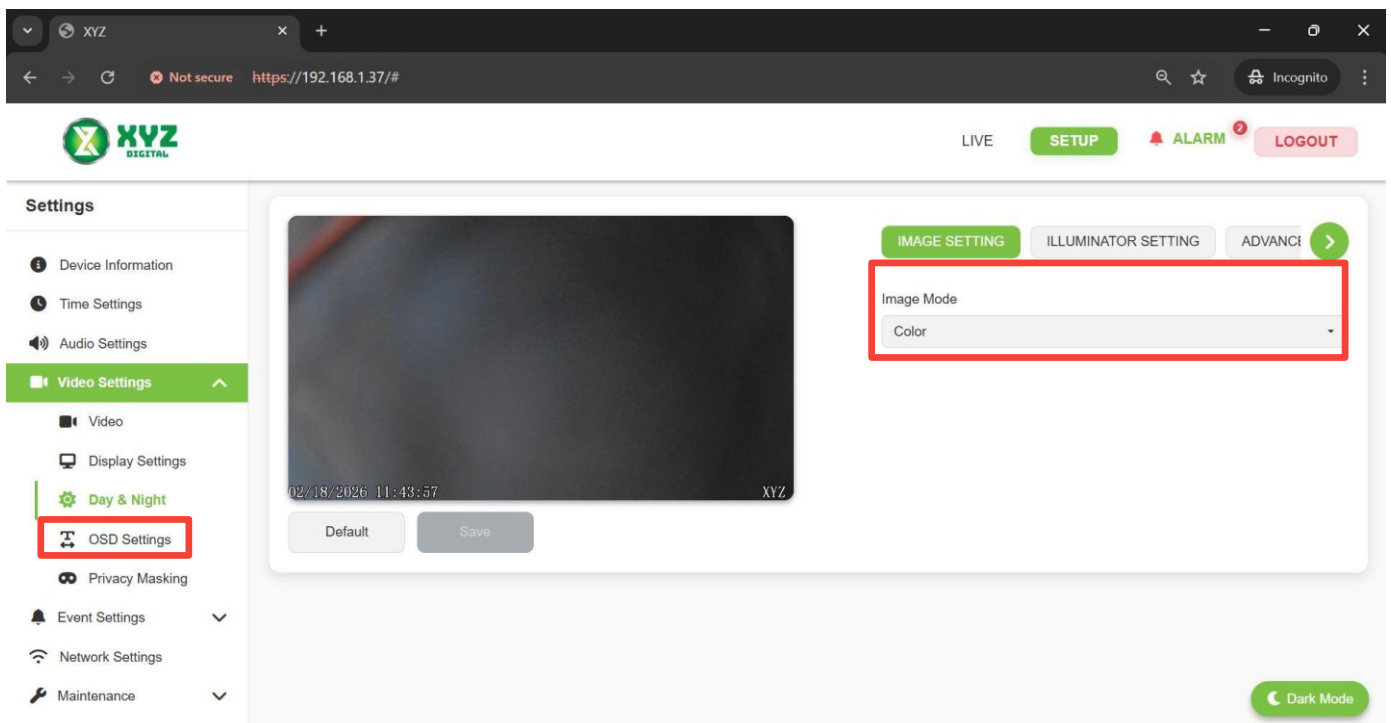


Fig- 7.3.1

7.3.2-ILLUMINATOR SETTINGS- User can control the led light, mode & brightness

(As shown in Figure- 7.3.2)

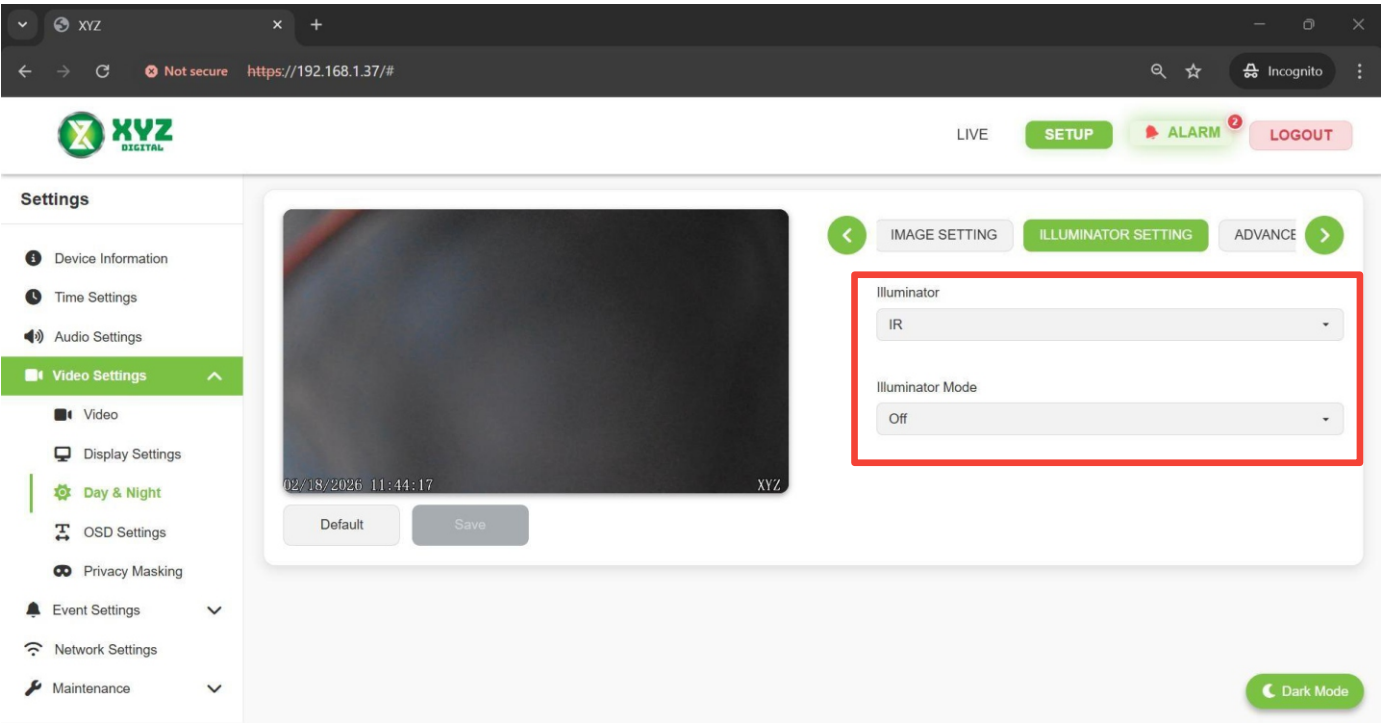


Fig- 7.3.2

7.3.3-ADVANCED OPTION-user can change led light image sensitivity to trigger the IR on particular environment(As shown in Figure- 7.3.3)

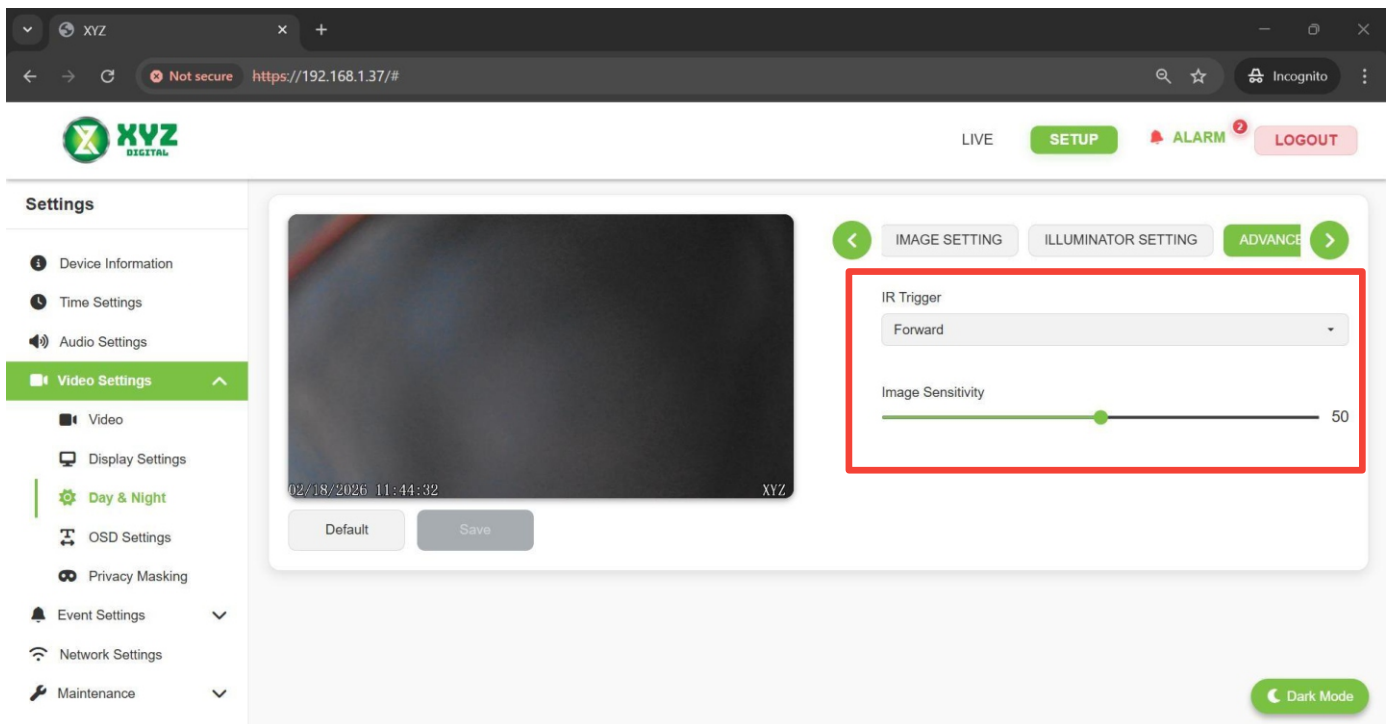


Fig- 7.3.3

7.4.-OSD SETTING(In this section you will get Time OSD & Title OSD)

7.4.1-TIME OSD-user can define the position of time display over the screen(As shown in Figure- 7.4.1)

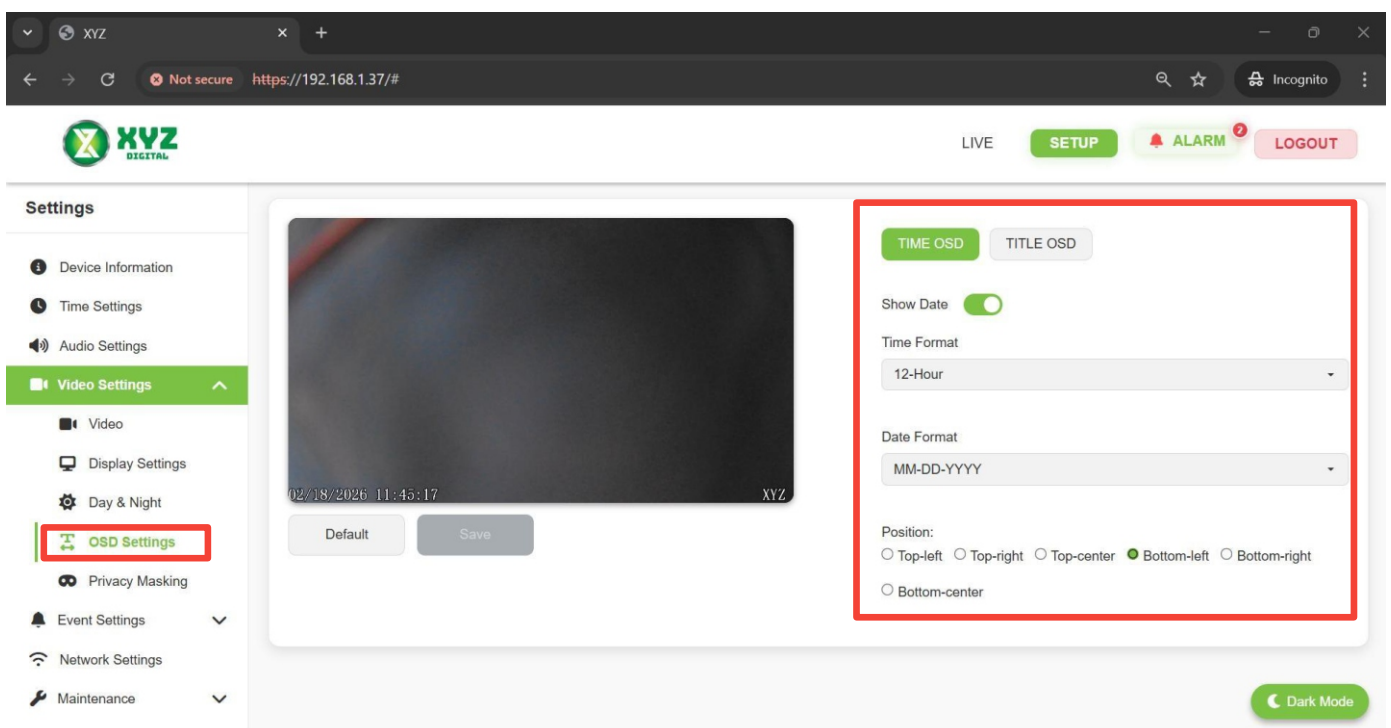


Fig- 7.4.1

7.4.2-TITLE OSD-user can define the position of Title display over the screen(As shown in Figure- 7.4.2)

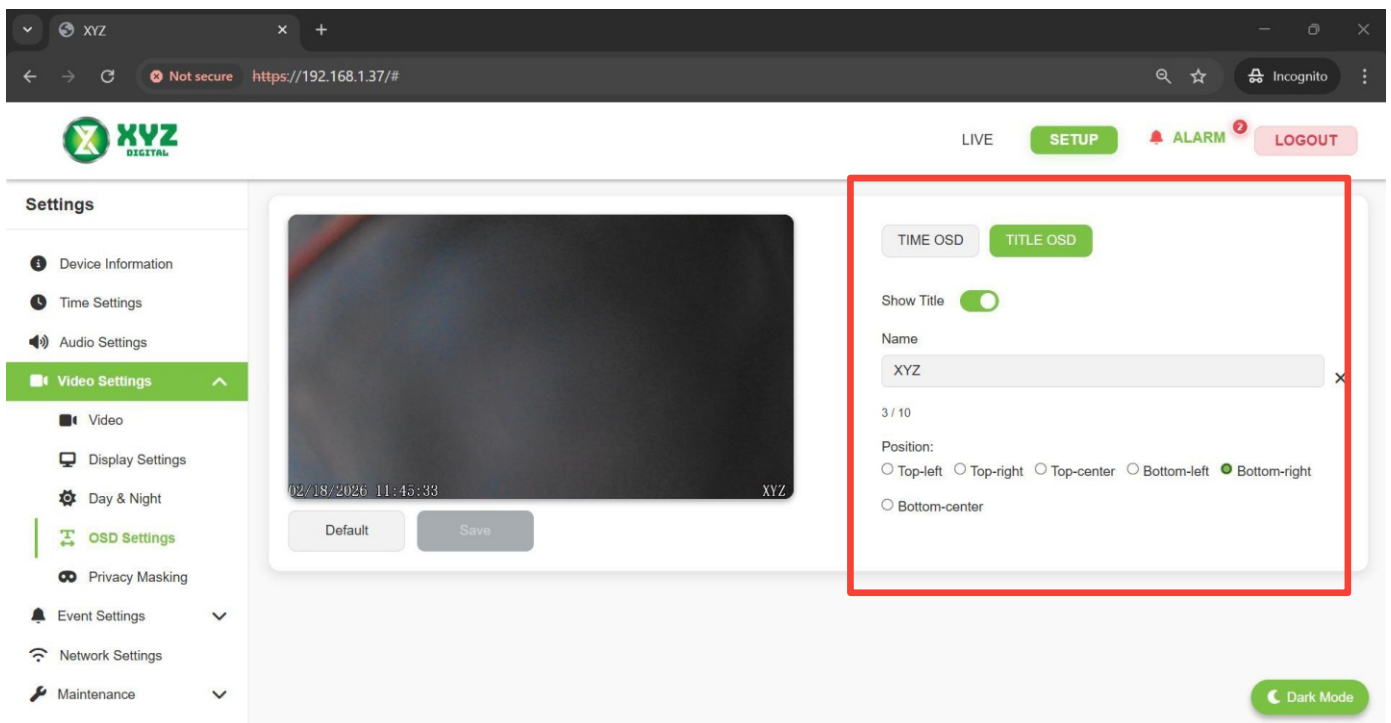


Fig- 7.4.2

7.5PRIVACY OPTION-used to block specific areas of a camera's field of view from being seen or recorded.(As shown in Figure- 7.5)

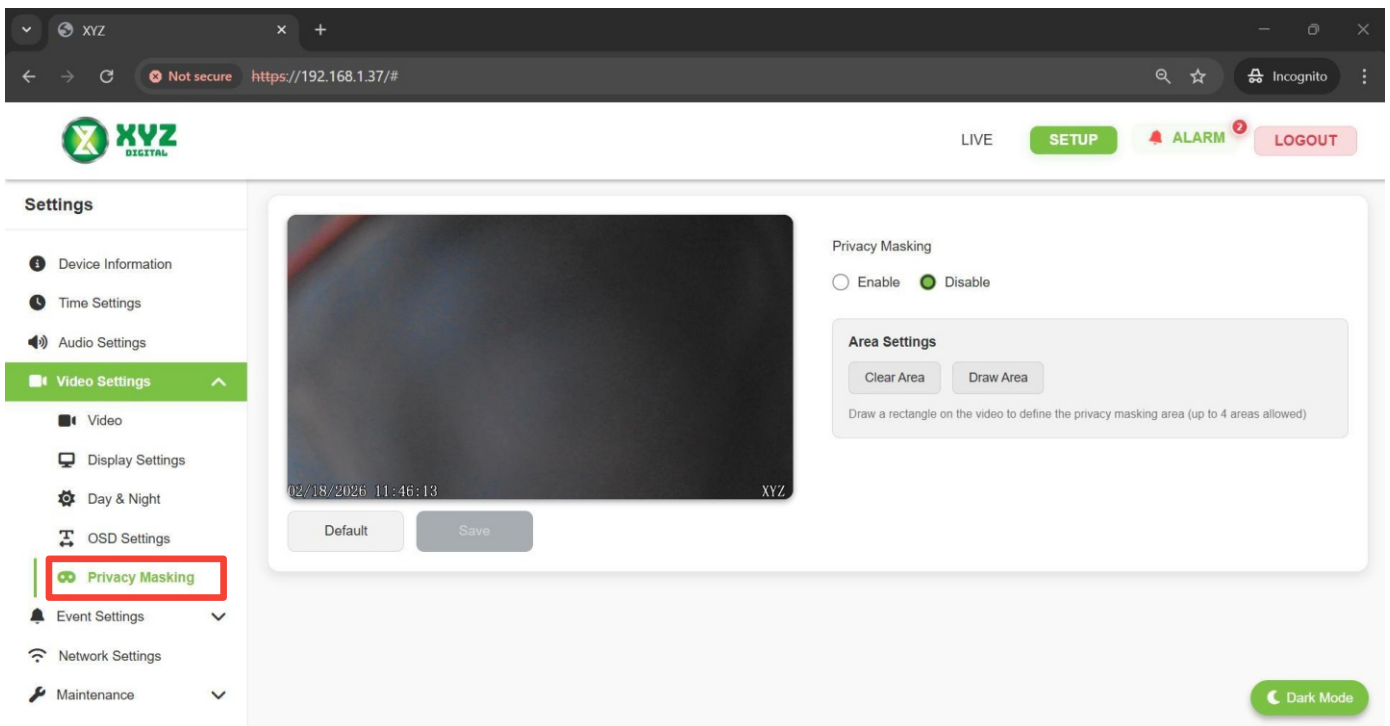


Fig- 7.5

8.EVENT SETTINGS-in this setting you will get motion detection and video tampering option

8.1-Motion Detection-SETUP-user can set motion detection by drawing the area with cooldown period & sensitivity level(As shown in Figure- 8.1)

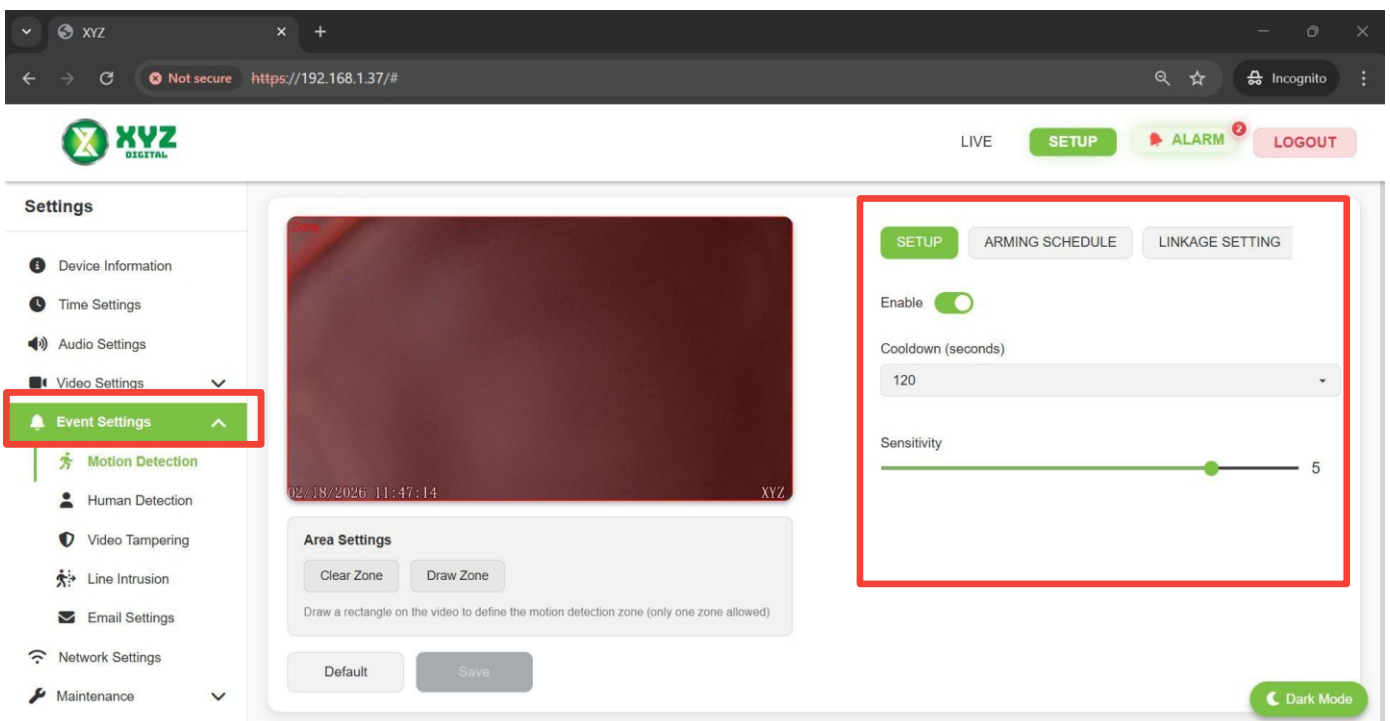


Fig- 8.1

ARMING SCHEDULE-user can set motion detection days and timings(As shown in Figure- 8.1)

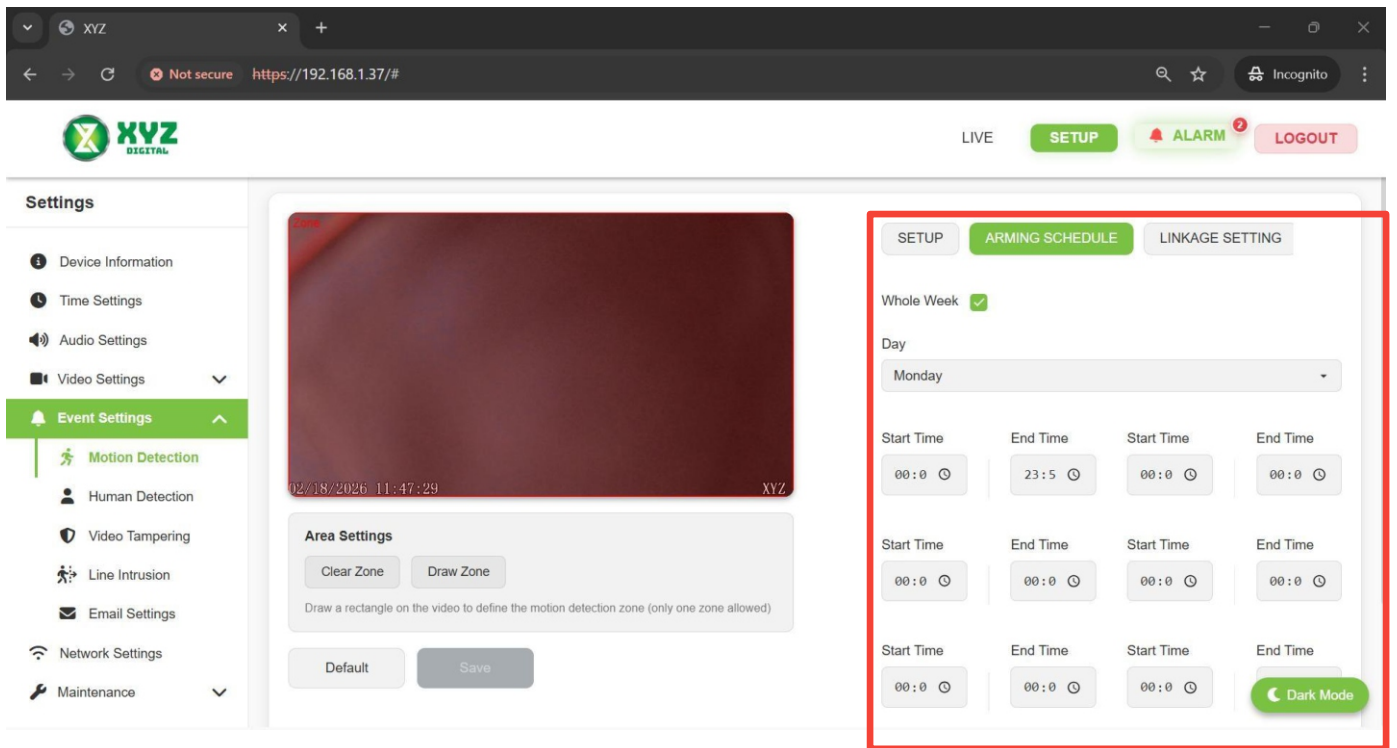


Fig- 8.1

8.1-LINKAGE SETTING-user can get notification on the basis of led lights.(As shown in Figure- 8.1)

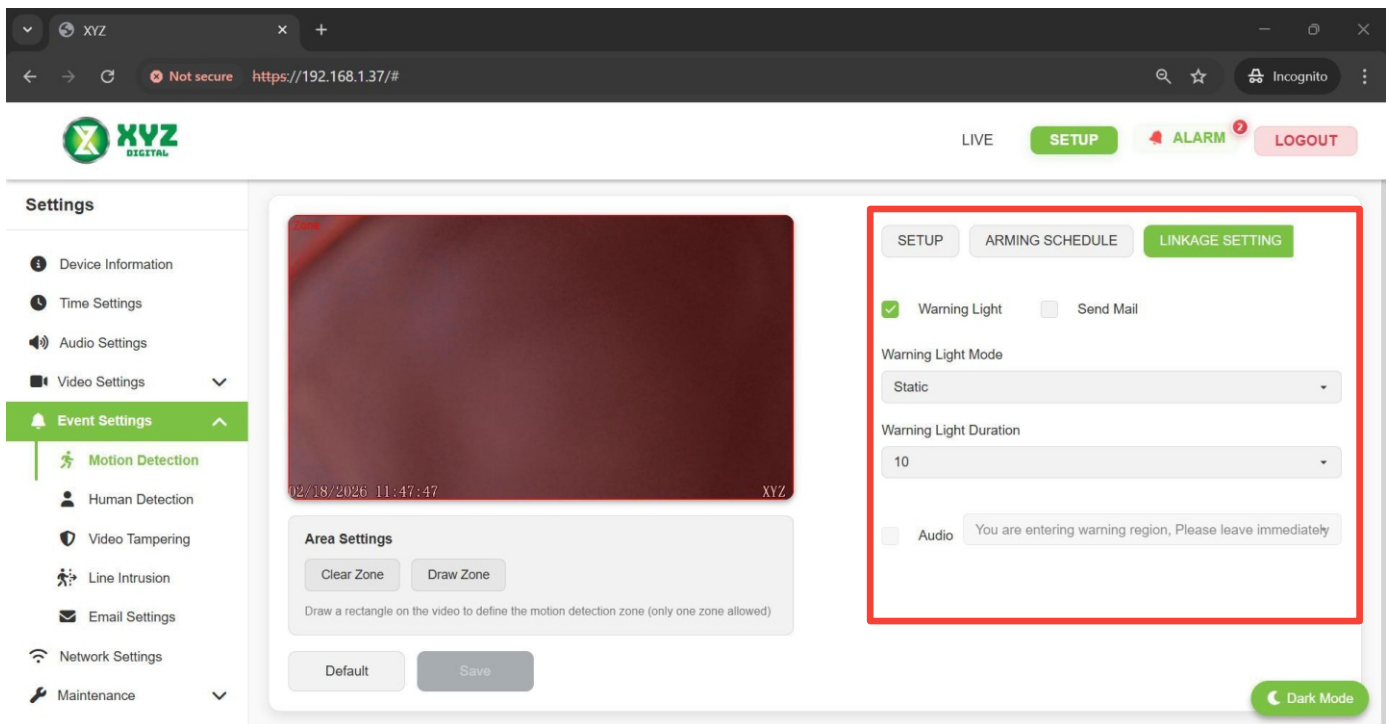


Fig- 8.1

8.2-VIDEO TAMPERING-user can set tamper detection notification with cooldown period(As shown in Figure-8.2)

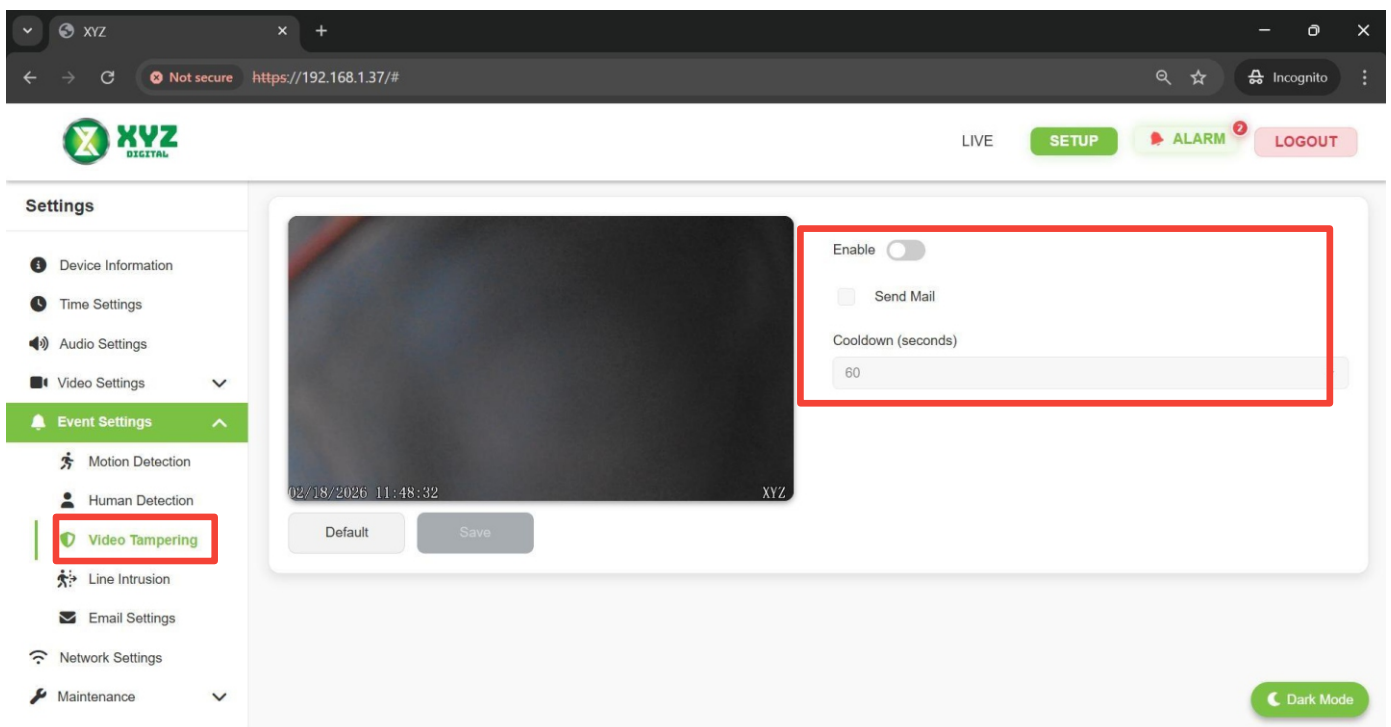


Fig- 8.2

8.3-Human Detection

SETUP – Users can enable or disable human detection and configure the cooldown period and sensitivity from the Setup tab.(As shown in Figure- 8.3)

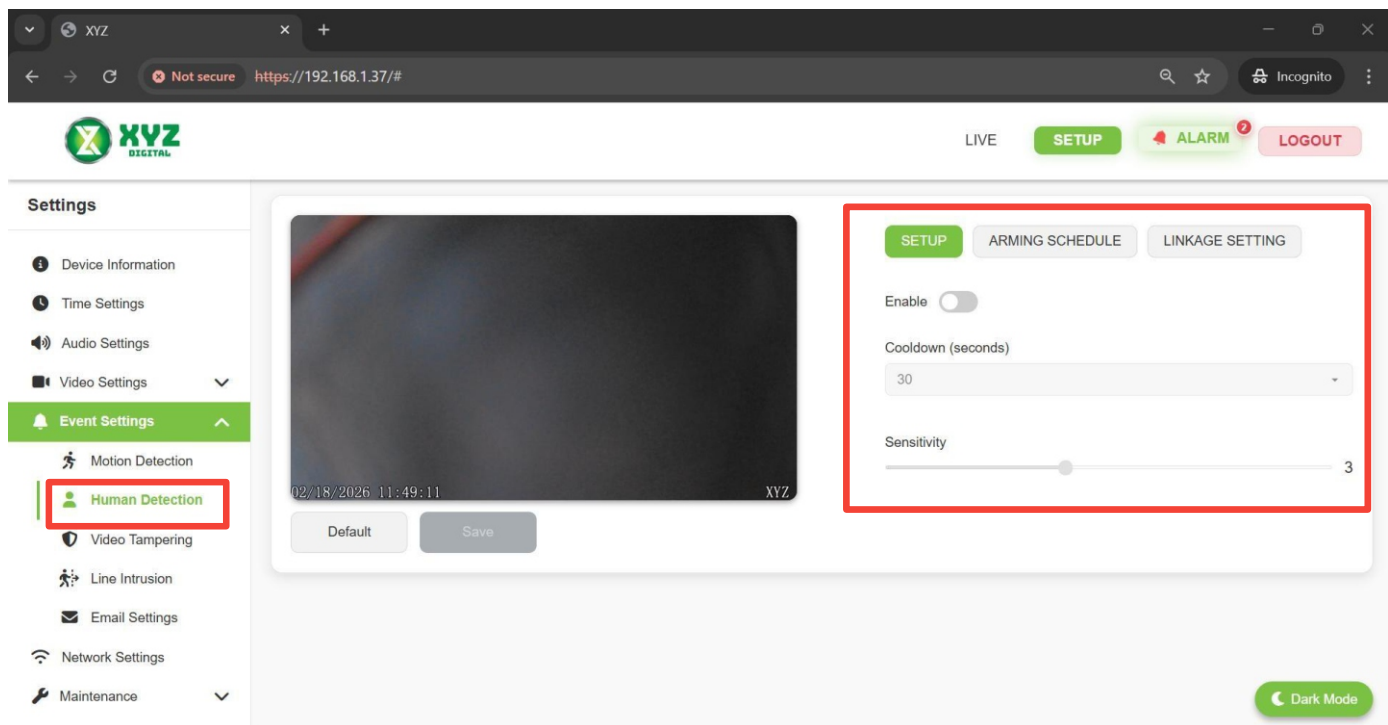


Fig- 8.3

-ARMING SCHEDULE-user can set human detection days and timings(As shown in Figure- 8.3)

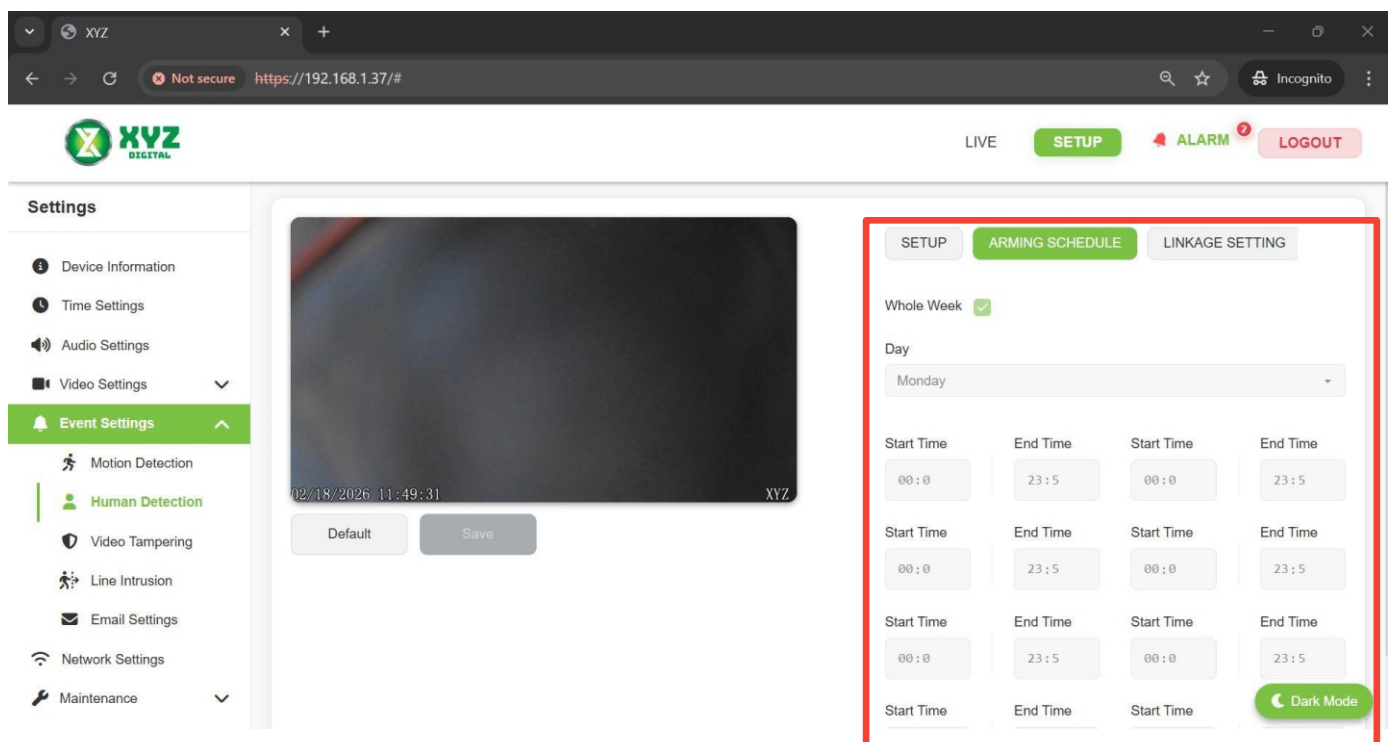


Fig- 8.3

-LINKAGE SETTING-user can get notification on basis of led lights. (As shown in Figure- 8.3)

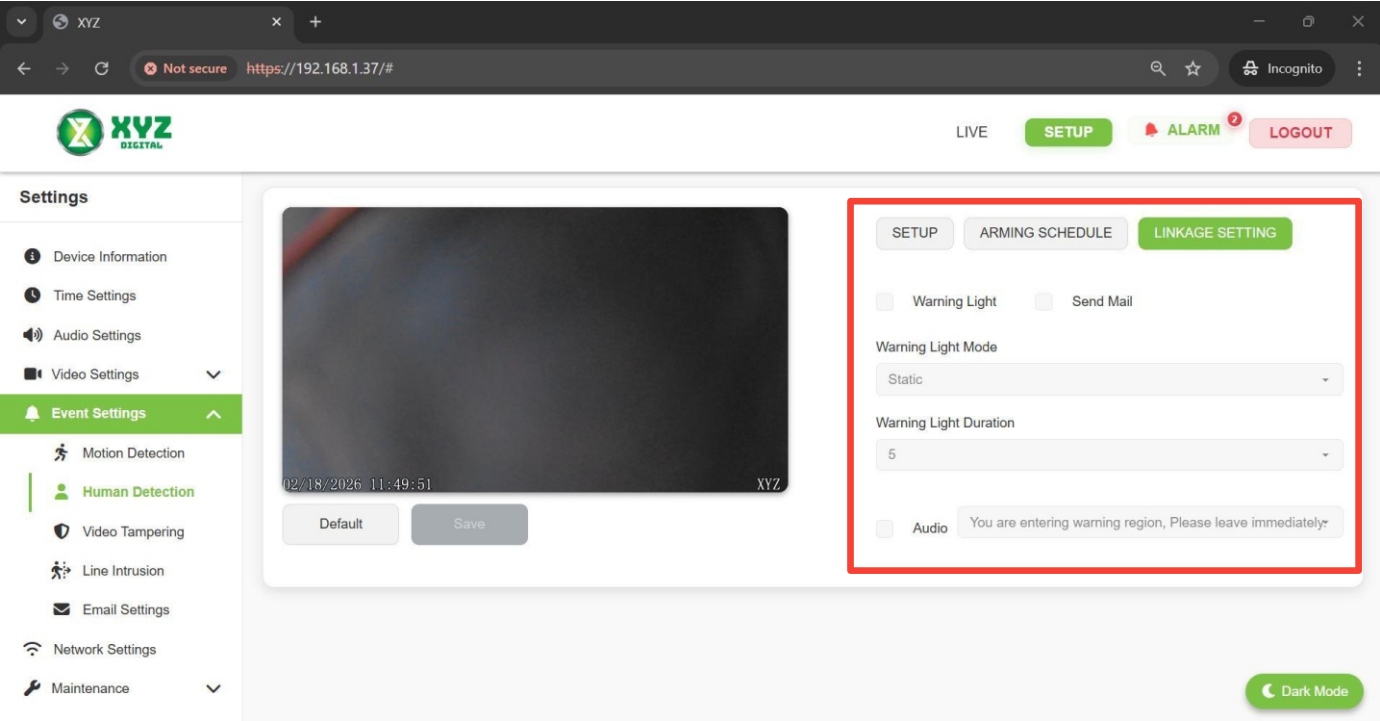
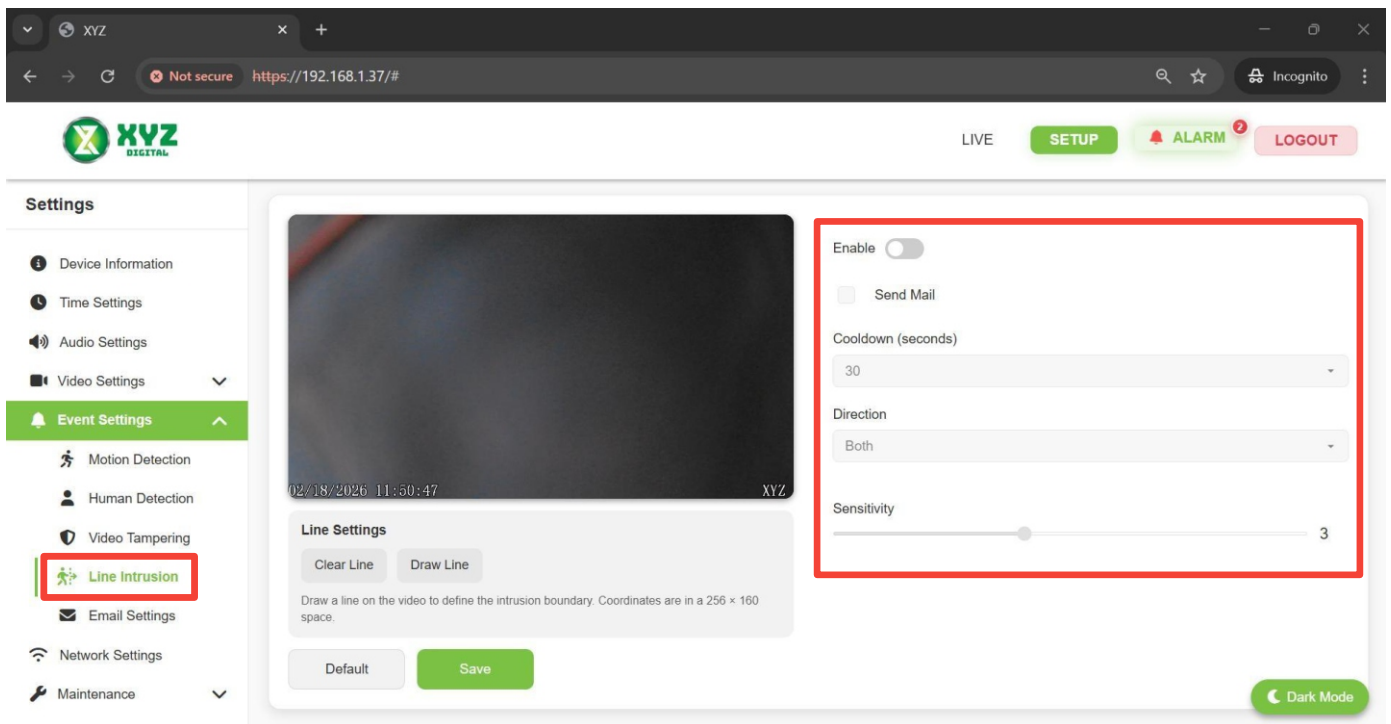


Fig- 8.3

8.4-Line Intrusion

The Line Intrusion feature allows users to draw a virtual boundary line across the video stream. An alert is triggered when a human figure crosses this line in a specified direction. This is ideal for monitoring entrances, perimeters, or restricted walkways where simple motion detection might cause too many false alarms.

(As shown in Figure- 8.4



(As shown in Figure- 8.4)

Line Intrusion Controls

Line Settings

- **Draw Line:** Click this button, then click and drag on the video preview to draw a straight boundary line. The line defines the "A" and "B" sides for direction-based detection.
- **Clear Line:** Removes the current intrusion line from the screen.
- **Boundary Info:** The line coordinates are processed in a normalized 256 x 160 coordinate space for device compatibility.

Action Buttons

- **Save:** Applies the line coordinates, direction, sensitivity, and alert settings to the device.
- **Default:** Resets the line and all detection parameters to factory defaults.

9-NETWORK SETTINGS-In this page you will network parameters like base configuration, RTSP & HTTP/HTTPS

BASE CONFIGURATION-User can set ip address (As shown in Figure- 9)

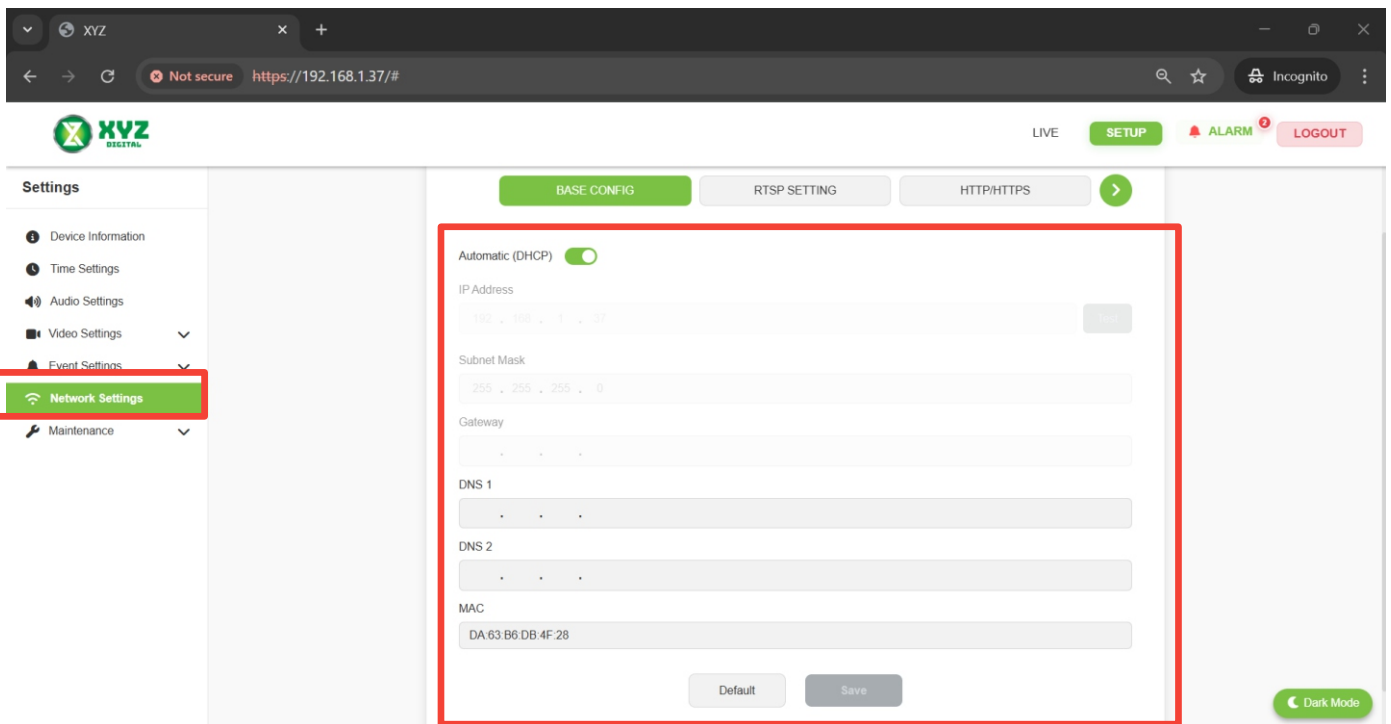


Fig-9

RTSP-user can create RTSP (Real-Time Streaming Protocol) settings by enabling the protocol in your IP camera finding its IP address and specific stream URL (e.g., `rtsp://user:pass@IP:Port/stream`), usually on default port 554, and then inputting these details into software like VLC or NVRs for live viewing, often requiring manual configuration of stream types (main/sub) and credentials.(As shown in Figure- 9.2

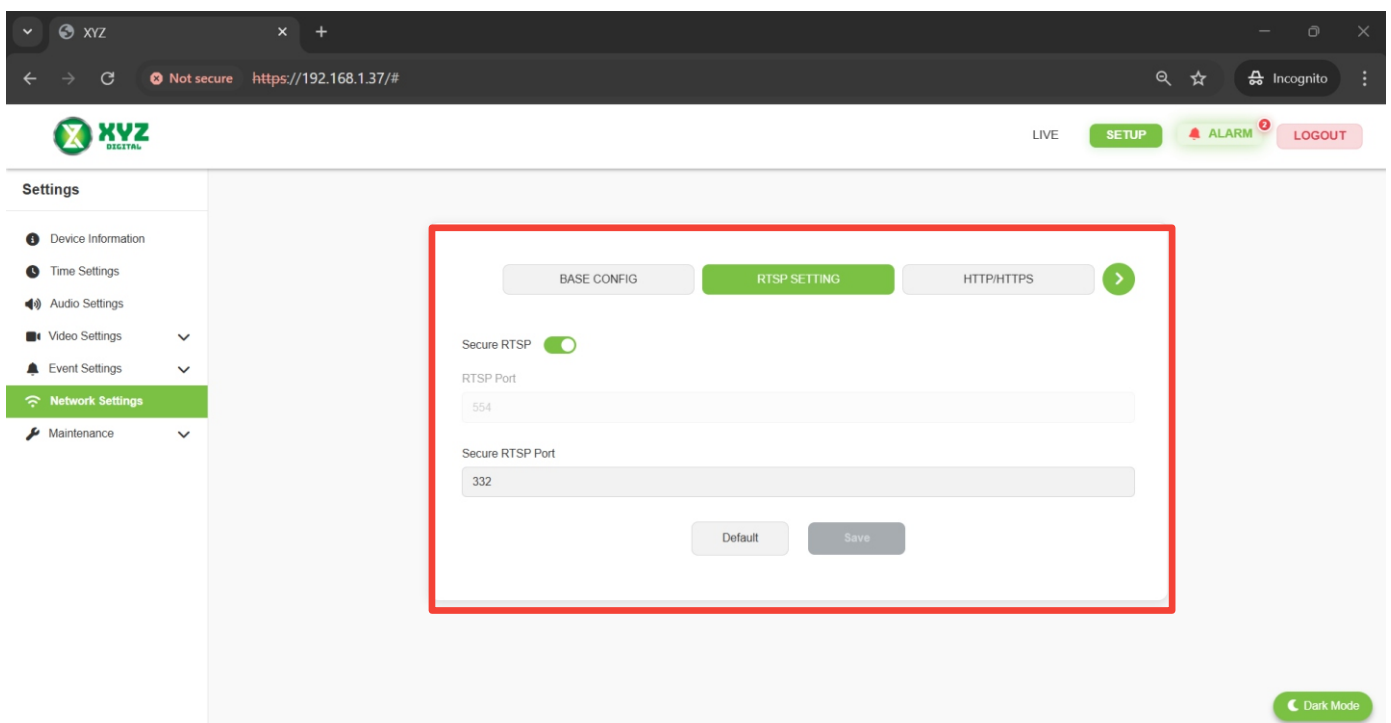


Fig-9

HTTP/HTTPS-HTTP is the standard, unencrypted way to access cameras (plain text, insecure), while HTTPS (HTTP Secure) encrypts traffic using SSL/TLS for secure login and data viewing(As shown in Figure- 9)

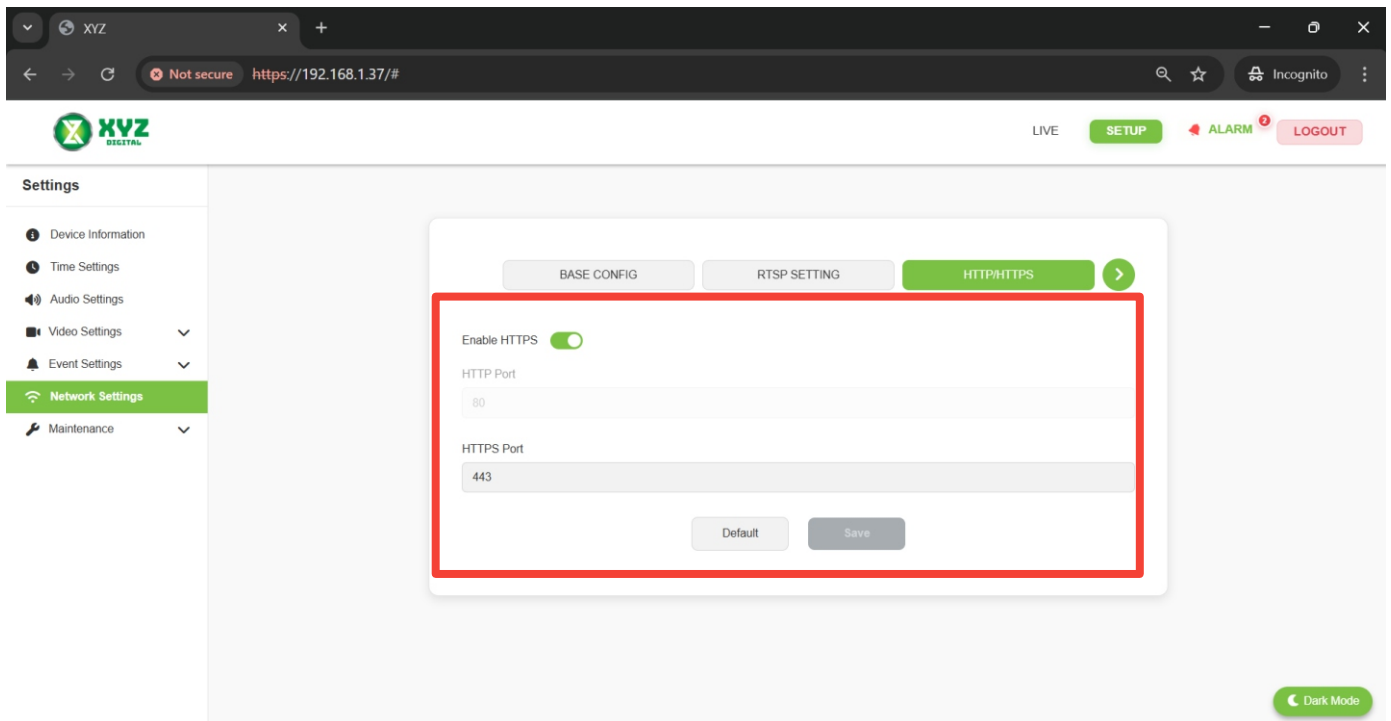


Fig-9

10- EMAIL SETTINGS-In this page user can set Email ID for notifications(As shown in Figure- 10)

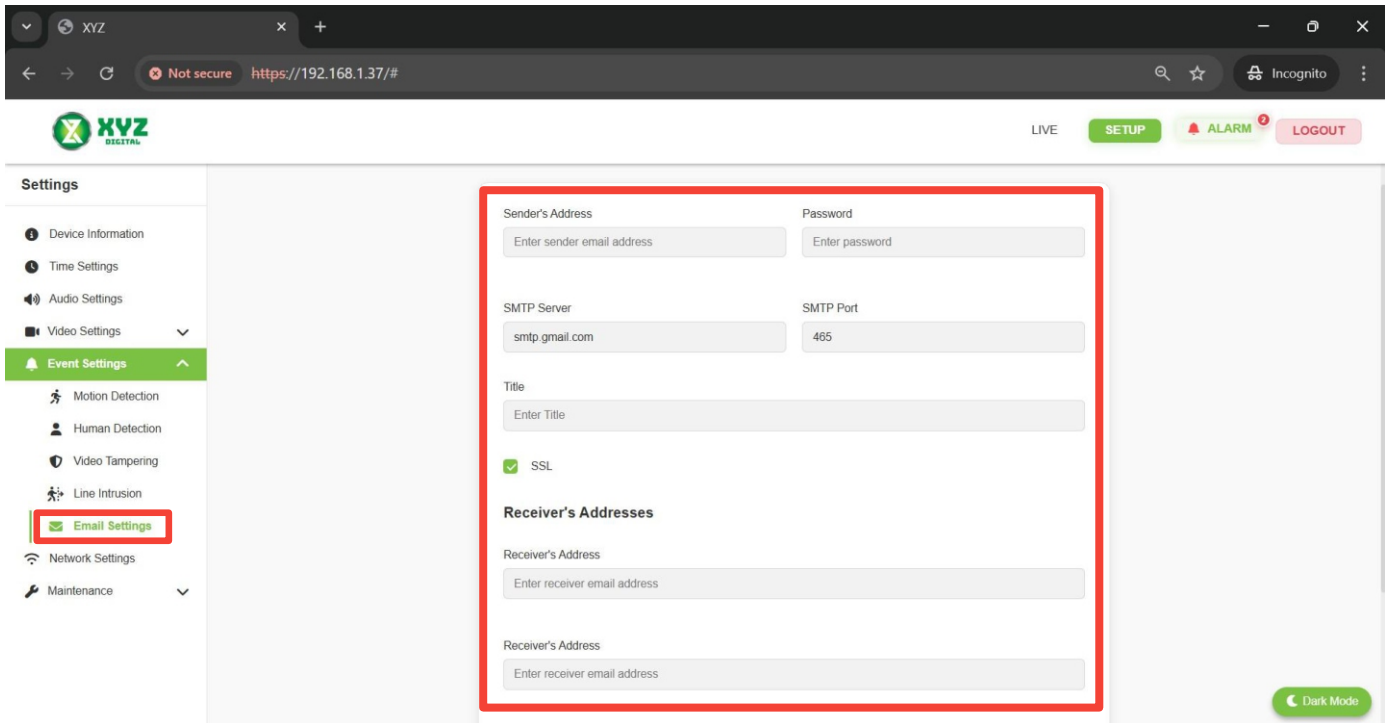


Fig-10

11- MAINTENANCE-In this section we have FACTORY reset option and OTA Updates

11.1-FACTORY RESET-In this interface user can perform default setting,factory setting and reboot the device.(As shown in Figure- 11.1)

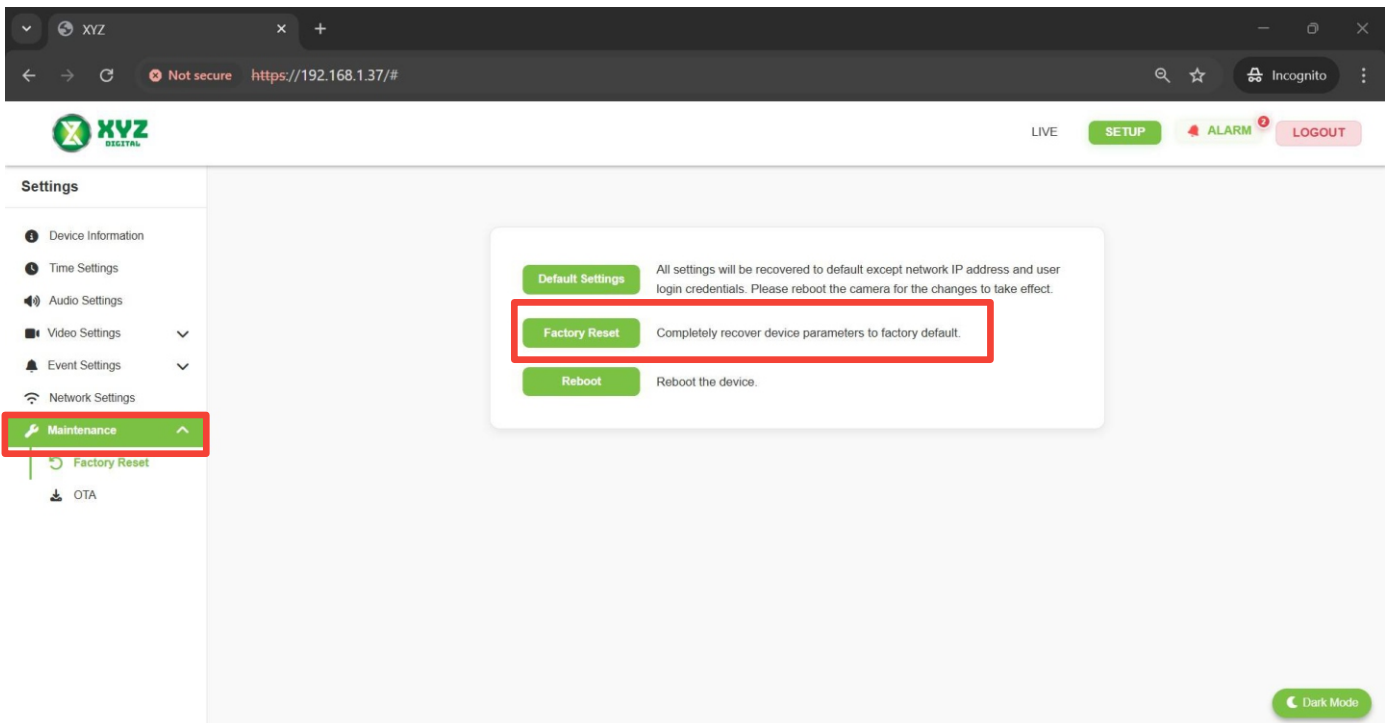


Fig-11.1

11.2-OTA UPDATES-

A method of delivering firmware, software, and configuration updates with the network(As shown in Figure-11.2)

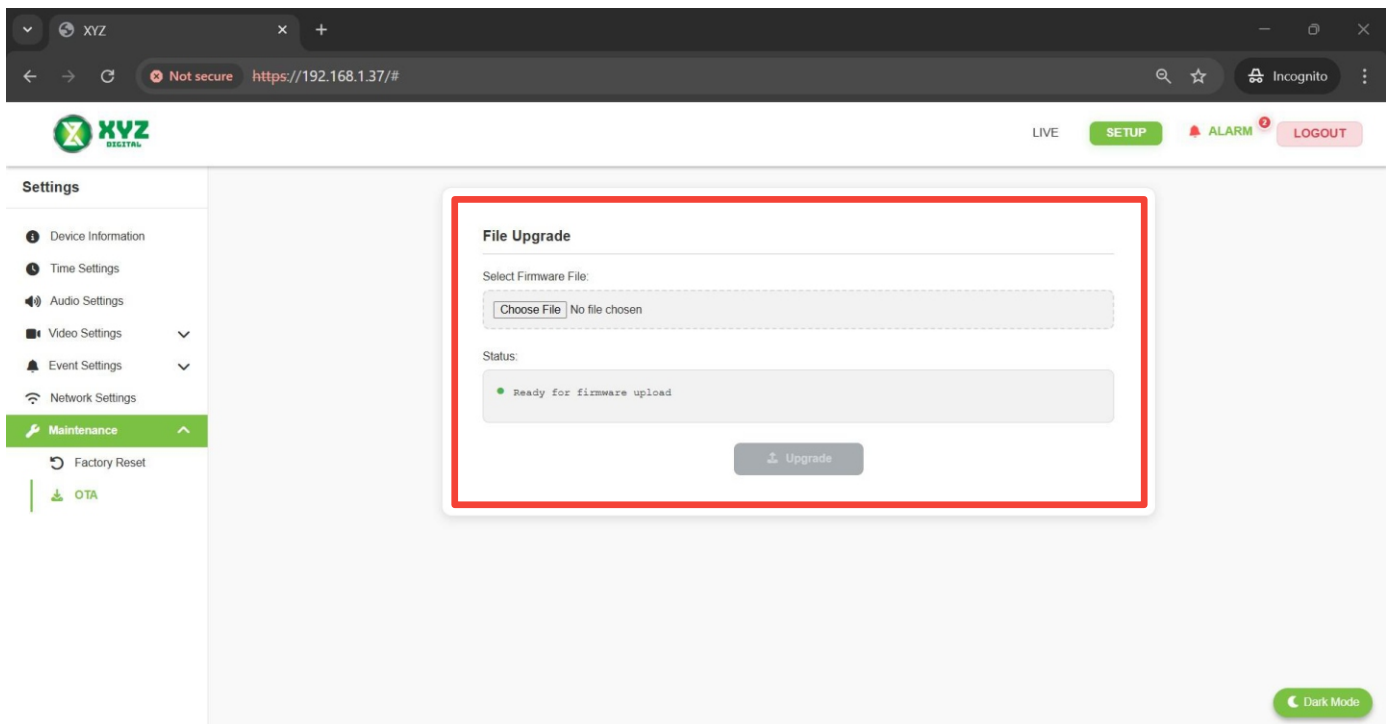


Fig-11.2

THANK YOU



CUSTOMER SUPPORT

+91 95997 01285

 www.xyzdigital.in

 Sales: xyzcctv123@gmail.com

 Support-technical@xyzdigital.in