NEXIVUE

User Manual

IP CAMERA

V.1.00

Foreword

General

This manual introduces the functions, configuration, general operation, and system maintenance of network camera.

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Symbol	Meaning
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, may result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and car plate number. You need to follow your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- This manual provides general instructions applicable to supported IPC models. Certain features, functions, and configuration options may vary depending on the specific model. Please refer to your IPC model's specifications for supported features.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.

- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

Electrical Safety

- All installation and operations shall conform to your local electrical safety codes.
- The power source shall conform to the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Note that the power supply requirement is subject to the device label.
- Make sure that the power supply is correct before operating the device.
- A readily accessible disconnecting device shall be incorporated in 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.

Environment

- Do not aim the device at strong light to focus, such as lamp light and sunlight otherwise, it might cause over brightness or light marks, which are not the device malfunction, and affect the longevity of Complementary Metal-Oxide Semiconductor (CMOS).
- Do not place the device in a damp, dusty extremely hot or cold environment, or the locations with strong electromagnetic radiation or unstable lighting.
- Keep the device away from any 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 allowed 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.
- Install the device in a location where only the professional staff with relevant knowledge of safety guards and warnings can access. An accidental injury might happen to the non-professionals who enter the installation area when the device is operating normally.

Operation and Daily Maintenance

- Do not touch the heat dissipation component of the device to avoid scalding.
- Carefully follow the instructions in the manual when performing any disassembly operation about the device; otherwise, it might cause water leakage or poor image quality due to unprofessional disassembly. Please contact after-sale service for desiccant replacement if there is condensed fog on the lens after unpacking or when the desiccant turns green. (Not all models are included with the desiccant).
- It is recommended to use the device together with lightning arrester to improve lightning protection effect.
- It is recommended to ground the device to enhance reliability.

- Do not touch the image sensor (CMOS) directly. Dust and dirt could be removed with air blower, or you can wipe the lens gently with soft cloth that is moistened with alcohol.
- You can clean the device body with soft dry cloth, and for stubborn stains, use the cloth with mild detergent. To avoid possible damage on device body coating which could cause performance decrease, do not use volatile solvent such as alcohol, benzene, diluent and so on to clean the device body, nor can strong, abrasive detergent be used.
- Dome cover is an optical component. Do not touch or wipe the cover with your hands directly during installation or operation. For removing dust, grease or fingerprints, wipe gently with moistened oil-free cotton with diethyl or moisten soft cloth. You can also remove dust with an air blower.

WARNING

- Strengthen the protection of network, device data and personal information by adopting measures which include but not limited to using strong passwords, modifying password regularly, upgrading firmware to the latest version, and isolating computer network. For some device with old firmware versions, the ONVIF password will not be modified automatically along with the modification of the system password, and you need to upgrade the firmware or manually update the ONVIF password.
- Use standard components or accessories provided by manufacturers and make sure that the device is installed and maintained by professional engineers.
- The surface of the image sensor should not be exposed to laser beam radiation in an environment where a laser beam device is used.
- Do not provide two or more power supply sources for the device unless otherwise specified. A failure to follow this instruction might cause damage to the device.

Table of Contents

Foreword 2
General 2
Safety Instructions 2
Privacy Protection Notice 2
About the Manual 2
Important Safeguards and Warnings 3
Electrical Safety 3
Environment 3
Operation and Daily Maintenance 3
1. Overview 7
1.1. Introduction 7
1.2. Setup IP Camera 7
2. Getting started 9
2.1 Using Nexivue Finder 9
2.2 Device Initialization Settings 10
3. Basic Configuration 13
3.1 Login 13
3.2 Plug-in Installation 14
3.2.1 Plug-in Types and Browser Support 14
3.3 Live Stream 15
3.3.1 Live Stream Interface 16
3.4 Video Playback 21
3.4.1 Video Playback Interface 21
3.5 Snapshot Playback 23
3.5.1 Snapshot Playback Interface 23
3.6 Settings 24
3.6.1 Local Config 24
3.6.2 General 26
3.6.3 Network 32
3.6.4 Video Settings 48
3.6.5 Image Settings 51
3.6.6 Event 60
3.6.7 Record Management 79

3.7 Maintain 85
3.7.1 Version 85
3.7.2 Upgrade 86
3.7.3 Default 87
3.7.4 Maintenance 88
3.7.5 Import And Export 88
3.7.6 Log 89
4. Appendix - 1 Cybersecurity Recommendations 90

1. Overview

1.1. Introduction

An IP camera (Internet Protocol camera) is a type of digital video camera that receives control data and sends image data through internet. They are commonly used for surveillance, requiring no local recording device, but only a local area network.

The NEXIVUE IP Camera is designed to make surveillance reliable and easy viewing reality with smart features. It allows users to easily view and check activities anytime, anywhere using NVR, Local Web UI, Laptop. These cameras include high-level features of HD Video streaming 1080P@30fps (2MP)/2592x1944@30fps (5MP)/3840x2160@20fps (8MP), Smart analytics like Motion Detection, Night vision support, and Network connectivity via Ethernet support.

1.2. Setup IP Camera

The common networking mode for IP Camera is to connect IPC to PC via switch or a router. NEXIVUE IP Camera can be powered either by POE or 12V DC Adaptor and below diagram illustrates the basic connectivity for the IP Camera.

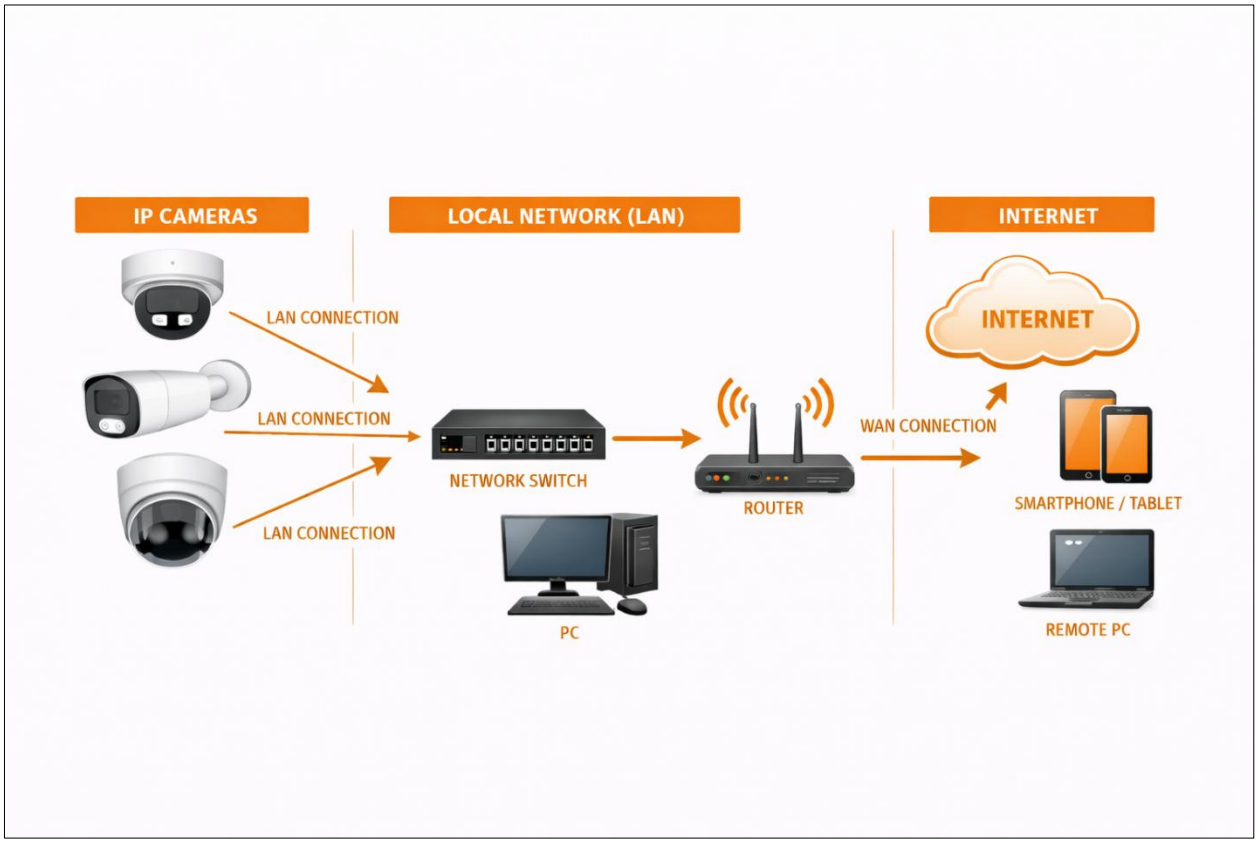

Figure 1-1 General IPC Network

Before you have access to a network camera via the Internet, you need to acquire its IP address. The camera will be in DHCP mode by default, with **192.168.1.100** as the IP address, or users can search for IP addresses via the NEXIVUE Finder Tool.

For setting up the IP Camera, you have to follow the steps below:

Step 1 Power up the IP Camera using PoE or 12V DC adaptor.

Step 2 Connect an IP Camera to a network via Ethernet cable. Once the connection has been established, the device will get an IP address. After a successful connection user can access the Web GUI by entering the Camera IP address in the browser.

If Ethernet is not connected:

- The device will not obtain an IP address or internet connection.
- All the functionalities utilizing either an IP address or the Internet will be restricted.

If Ethernet is connected:

- The device will get the IP address
- Streaming and all other functionalities will be via Ethernet and can be started.

2. Getting started

Before using the IP camera, you must set a login password. Setting a strong password helps protect personal privacy, device data, and network security. The camera can be accessed using Nexivue Finder tool, Client software, and a Web browser.

2.1 Using Nexivue Finder

This section explains the login process using Nexivue Finder tool.

<u>Step 1</u> Install Nexivue Finder

- Install and launch the Nexivue Finder tool.
- The tool will automatically search for all activated devices within the local network (LAN).
- Device information, such as device type, IP address, and firmware version, will be displayed in the list.

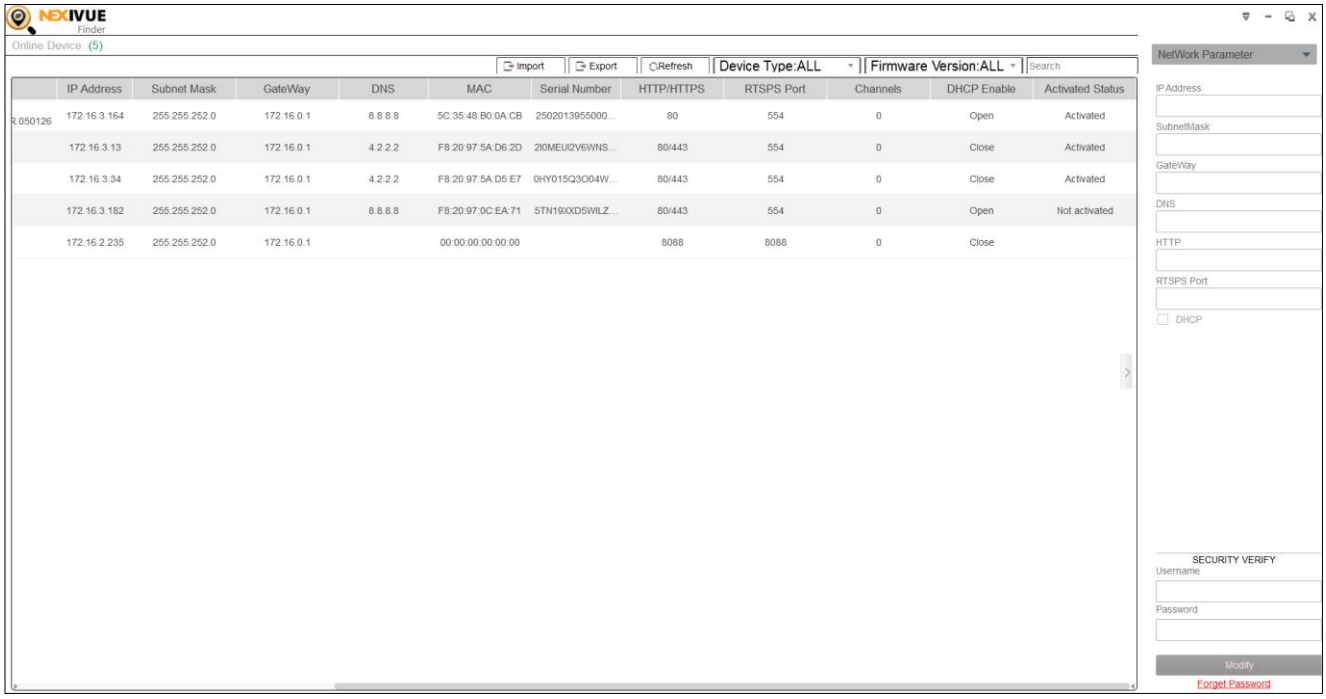

Figure 2-1 Nexivue Finder page

- All cameras use the default factory IP address 192.168.1.100.
- Ensure the computer's IPv4 address is in the same network segment as the camera.
- To change the IP address of a device, select the device and enter the administrator password, and modify the IP address, subnet mask, and gateway as required. You can also use DHCP to assign the IP address.

Step 2 Select the IP Camera

- From the device list displayed in the Nexivue Finder window, identify the required IP camera using its device name, IP address, or MAC address.
- Double-click the camera you want to configure.
- Once selected, proceed with network configuration, password setup, or web login as required.

2.2 Device Initialization Settings

After selecting the required IP camera in Nexivue Finder, the system will guide you through the initial device setup (if the device is not initialised), including time zone configuration and administrator password settings.

Step 1 Time Zone Setting

- Select the preferred **Date Format** from the drop-down list.
- Choose the appropriate **Time Zone** according to your location.
- (Optional) Click **Sync PC** to synchronize the camera time with the computer system time.
- Verify the **Device Time** displayed on the screen.
- Click **Next Page** to proceed.

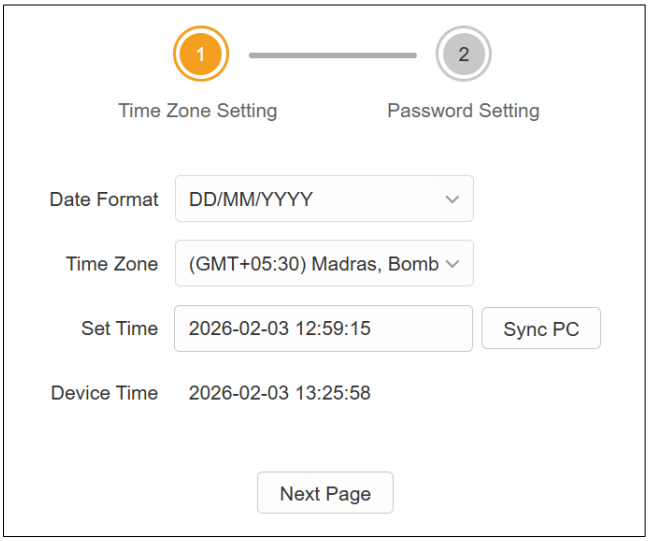

Figure 2-2 Time zone setting

Step 2 Set the password, security questions, email, and mobile no. for admin account.

- Entering an email address is optional; however, it is strongly recommended for enhanced security purposes.

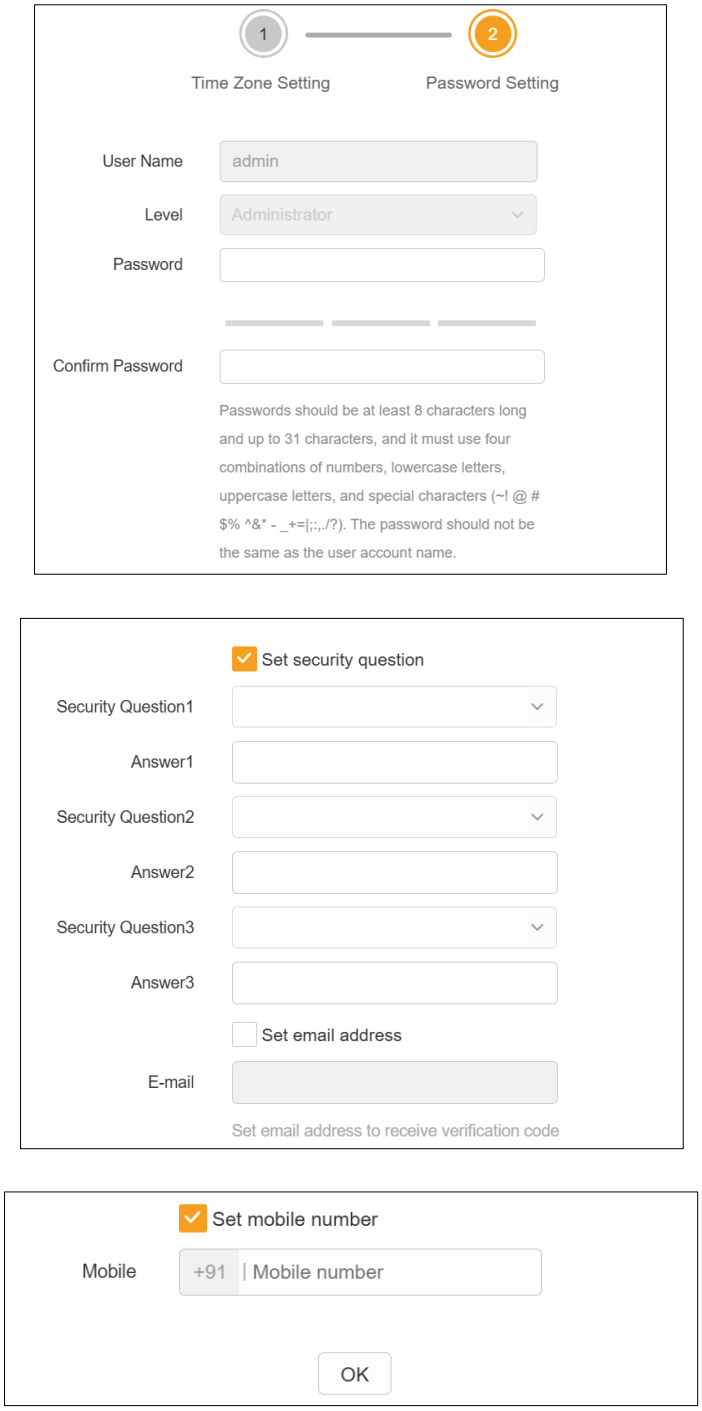

Figure 2-3 Password setting

Parameter	Description
User Name	The default username is admin.
Level	The default level is Administrator.
Password	The password should be at least 8 characters long and up to 31 characters, and it must use four combinations of numbers, lowercase letters, uppercase letters, and special characters (~ ! @ # $ % ^ & * _+|:;,./?). The password should not be the same as the user account name.
Confirm Password	
Security Questions	Need to select the questions and fill in accordingly to reset the password
Email	(Optional) Check the Email check box and enter an email address for password reset. When you need to reset the password of the admin account, a security code for password resetting will be sent to the reserved email address.
Mobile	Enter the mobile number for password reset When you need to reset the password of the admin account, a security code for password resetting will be sent to the reserved mobile number.

Table 2-1 Description of password configurations

3. Basic Configuration

The section introduces the basic configuration, including login, live view, playback, camera configuration, network configuration, storage configuration and system configuration.

3.1 Login

This section introduces how to log in to and log out of the web interface.

- You need to initialize the camera before logging in to the web interface.
- When initializing the camera, keep the PC IP and device IP in the same network.
- Follow the instruction to download and install the plug-in for the first login.

Step 1 Open a web browser, enter the camera's full IP address (http://192.168.1.100) in the address bar, and press Enter.

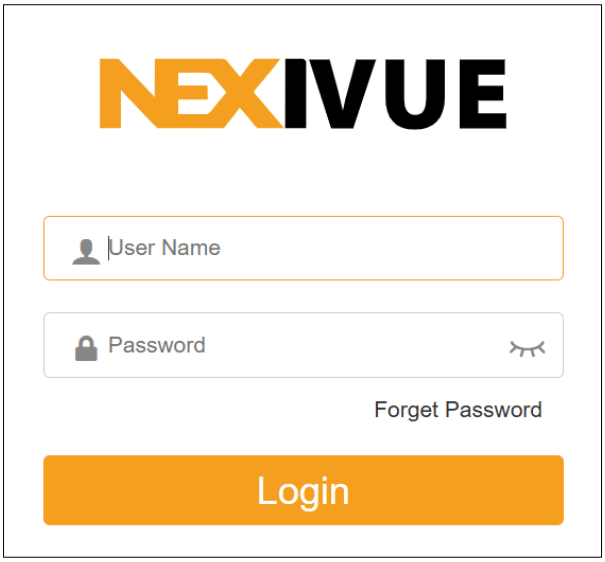

Figure 3-1 Login page

Step 2 Enter the username and password. The username is admin by default.

- Click **Forget password?** and you can reset the password through the email address or mobile no. that are set during the initialization.

Step 3 Click **Login** to display the main webpage.

3.2 Plug-in Installation

After successfully logging in to the camera via a web browser, download and install the required plug-in to enable video preview and configuration.

Step 1 On the Nexivue IPC webpage, in the upper-right corner, click **Download Plug-in** icon.

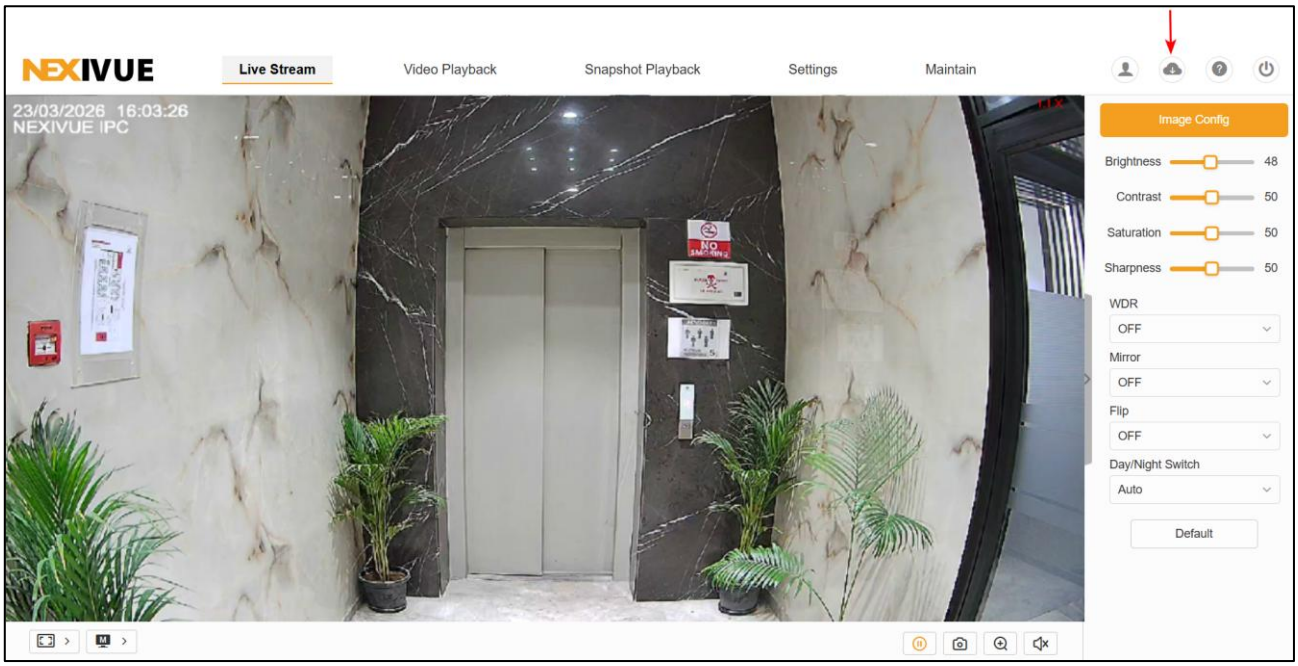

Figure 3-2 Download plug-in

Step 2 Open the file and perform the on-screen instructions to complete the installation.

Step 3 After installation, re-enter the camera IP address and login details to view live video.

- Close the browser before installing the plug-in; otherwise, installation may fail.
- Some devices support Chrome 57+, Firefox 52+, or newer Edge browsers without plug-ins, but certain configuration functions may be limited.

3.2.1 Plug-in Types and Browser Support

Feature	Middleware Plug-in	Go Plug-in
Supported Browsers	Google Chrome, Firefox, Edge	Google Chrome, Firefox, Safari, Edge
Supported Video Formats	H.264, H.265, MJPEG	H.264, H.265
Device Function Support	Supports all device functions	Limited functionality

H.265 Performance	No resolution limitation	Resolution above 2 MP may be limited
MJPEG Support	Fully supported	Preview and playback only via IE or Middleware
Intercom & Local Configuration	Supported	Not Supported
Safari Compatibility	Not applicable	Does not support real-time preview or audio
Installation Notes	Ensure ports 53788–53797 are free	No additional installation notes

Table 3-1 Description of features supported by Middleware and go plug-in

- For complete functionality and best performance, it is recommended to use the Middleware Plug-in or access the device using an IE browser.
- If plug-in installation fails, temporarily disable antivirus software and try installing the plug-in again.

3.3 Live Stream

On the main interface of the device, you can view live, playback, snapshots, operate and configure.

- **Live Stream**: Used for previewing the device monitoring screen and operation control.
- **Video Playback**: Find and playback videos by time or type.
- **Snapshot Playback**: View pictures by type.
- **Settings**: Enter the device config interface for system config and function configuration.
- **Maintain:** Used to view device information, logs, software upgrades, device restart and other operations.

- Different models of network cameras have slightly different in functions, please refer to the actual function interface for specific functions.

In the upper right corner of the interface, you can view the following options:

- : Hover on the **User** icon to view currently logged-in users.
- : Click the **Download Plug-in** icon to download the plug-in.
- : Click the **Help** icon to view online help document.
- : Click the **Logout** to log out the currently logged-in users.

3.3.1 Live Stream Interface

This section includes the system menu, stream type, live view function bar, and window aspect ratio options.

Click **Live Stream** on the main webpage to enter the **Live** page.

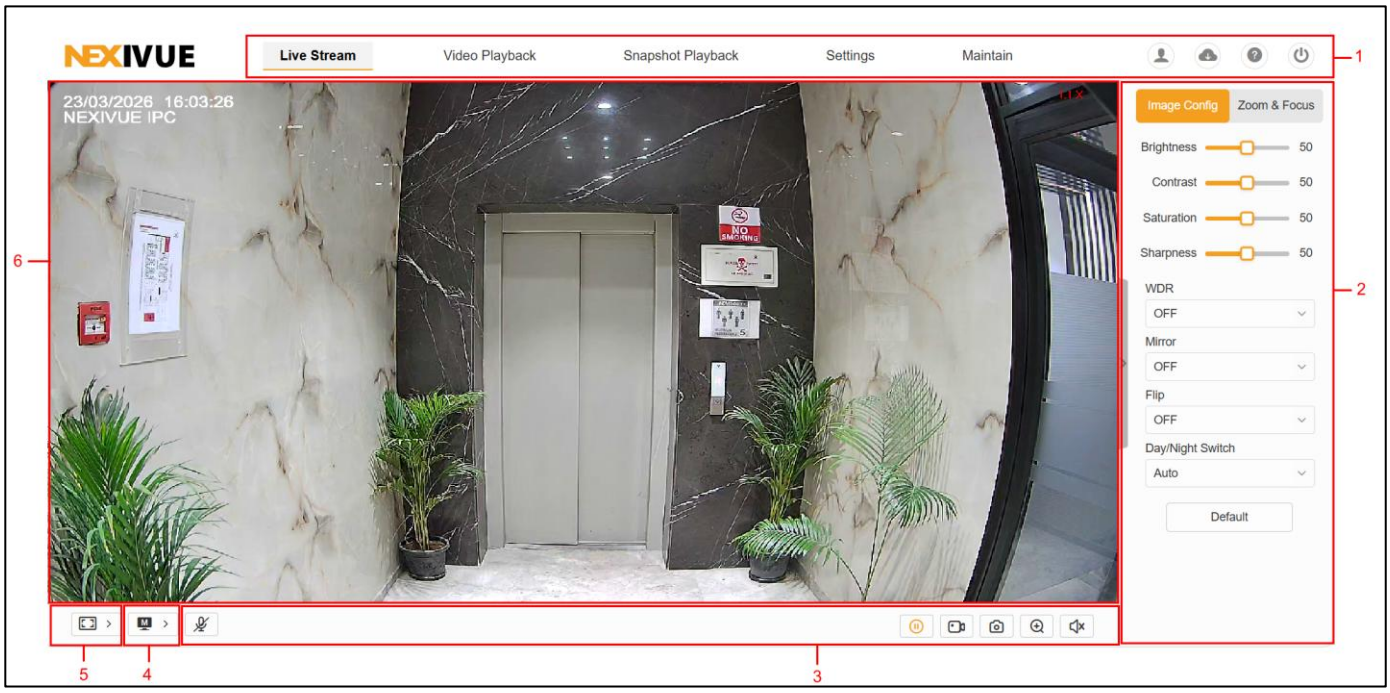

Figure 3-3 Live

No.	Function	Description
1	Navigation bar	Provides access to main functions, including Live Stream, Video Playback, Snapshot Playback, Settings, and Maintenance. Also includes system icons for user account, download plug-in, help, and logout.
2	Image Config and Zoom & Focus panel	Allows configuration of image parameters (Brightness, Contrast, Saturation, Sharpness, WDR, Mirror, Flip, Day/Night) and control of Zoom & Focus functions.
3	Live view function bar	Provides live view operations such as audio enable/disable, snapshot capture, digital zoom, recording, and playback controls.
4	Stream type	Allows selection of the stream type, such as Main Stream, Sub-Stream, or Third Stream.
5	Aspect ratio option	Provides live view aspect ratio options, including 16:9, 4:3, and 1:1.
6	Live view window	Displays the real-time video stream from the IP camera.

Table 3-2 Description of live interface

3.3.1.1 Image Config

The Image Configuration panel allows users to adjust camera image parameters to achieve optimal video quality under different lighting and installation conditions. Drag the slider to adjust image parameters, including brightness, contrast, saturation, and sharpness.

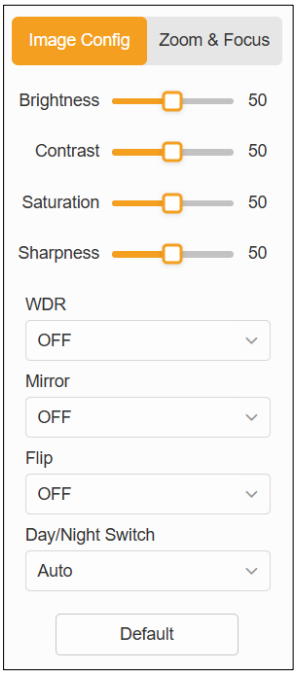

Figure 3-4 Image config

Option	Description
Brightness	Adjust the overall image brightness and changes the value when the image is too bright or too dark. The bright and dark areas will have equal changes.
Contrast	Change the value when the image brightness is proper, but the contrast is not enough.
Saturation	Adjust the image saturation. The higher the value, the deeper the color.
Sharpness	Enhances edge details in the image to improve clarity.
WDR	Select **OFF**, **Low**, **Medium**, or **High** to balance bright and dark areas. Use higher levels in scenes with strong backlight.
Mirror	Select **OFF**, **Horizontal**, **Vertical**, or **Vertical and Horizontal** to flip the image orientation as required by the installation.
Flip	Select **OFF**, **90°**, **180°**, or **270°** to flip the image orientation as per the requirement.
Day/Night Switch	Select **Auto**, **Day**, **Night**, or **Scheduled-Switch** to control the switching between day (color) and night (B/W) display.
Default	Click to restore all image parameters to factory default settings.

Table 3-3 Description of Image configuration options

3.3.1.2 Zoom & Focus panel

This section introduces the options and controls that help users quickly adjust their view and stay focused on key details.

Icon	Function	Description
− Zoom +	Zoom- Zoom+	When holding down the − button, the lens is pulled away and the scene becomes smaller. When holding down the + button, the lens is pulled closer and the scene is enlarged
− Focus +	Focus- Focus+	In manual focus mode, click − to make nearby objects clear, or click + to make distant objects clear.
− Iris +	Iris- Iris+	When the monitoring screen is dark, iris is priority in the exposure mode. Or in manual mode, click + to increase the iris, conversely, click − to reduce the iris.
	One Key Focus	Manually focus the lens
	Lens Initialization	Initialize the lens parameters.

Table 3-4 Description of zoom & focus panel

3.3.1.3 Live View Function Bar

This section introduces the shortcuts supported when viewing live videos.

Icon	Function	Description
	Audio	Click the icon to enable or disable audio output.
	Digital Zoom	When you turn on the digital zoom function, you can hold down the left mouse button and click on the place where the video surveillance screen needs to be enlarged, and then pull out a rectangular area to the right to zoom in on the area. After viewing, left-click anywhere on the video screen to return to the normal screen.
	Snapshot	Click the icon to capture a picture of the current view. The path to save the captured images can be viewed at **C:\Program Files (x86)\NEXIVUE\IPC\192.168.1.100\Pic\2026-03-23** • The IP address included in the path refers to the assigned IP address of the camera. • Captured snapshots are automatically saved in a date-wise folder.
	Record	On and off of Local video recording. The path of local video recording can be viewed at **C:\Program Files (x86)\NEXIVUE\IPC\192.168.1.100\Record\2026-03-23** • The IP address included in the path refers to the assigned IP address of the camera. • Captured videos are automatically saved in a date-wise folder.
	Play/Stop	Click the icon to play or stop the live view.
	Talk	Click the icon to enable or disable the two-way audio talk.

Table 3-5 Description of live view function bar

3.3.1.3 Configuring Encoding

On the bottom-left side of the **Live** page, click on the right side of the stream to select the video stream.

Figure 3-5 Configure video stream

- **Main Stream:** It has a large bit stream value and an image with high resolution, but also requires a large bandwidth. This option can be used for storage and monitoring.
- **Sub Stream:** It has a small bit of stream value and a smooth image and requires less bandwidth. This option is normally used to replace mainstream when the bandwidth is not enough.
- **Third Stream:** It has a very small bit stream value with basic image quality and requires minimal bandwidth.
- means the current stream is mainstream; means the current stream is sub stream 1; means the current stream is sub stream 2.

3.3.1.4 Aspect Ratio

This section introduces the options available for adjusting the aspect ratio of the live view window. On the bottom-left of the Live page, click on the right side of the full screen option to adjust the screen size.

Figure 3-6 Aspect Ratio options

Option	Description
	Expands the video to full-screen mode for a larger and clearer view, hiding other interface elements. Full-screen mode is the default view.
16:9	Displays the video in widescreen format, ideal for modern monitors and TVs.
4:3	Displays the video in a standard format, suitable for older monitors or applications where a narrower view is preferred.
1:1	Displays the video in a square format, useful for focused monitoring or specific display requirements.

Table 3-6 Description of adjustment bar

3.4 Video Playback

This section introduces video playback features that allow users to search and view recorded videos easily.

- Ensure that a compatible SD card is properly inserted and initialized in the device.
- Before playing back video, configure the record time range, record storage method, record schedule, and record control.

3.4.1 Video Playback Interface

Click the **Video Playback** on the navigation bar, and the playback interface will be displayed.

Figure 3-7 Video playback

No.	Function	Description
1	Search Panel	• Select a date from the calendar. • Set the **Start Time** and **End Time**. • Choose the **File Type**, including All, Regular, Motion Detection, External Alarm, Intrusion, Line-Cross Detection, Loitering Detection, and People Gathering. • Click **Search** to view matching videos on the timeline. • Dates marked with green dots indicate the availability of video playback recordings, regardless of the recording type.

2	Zoom control	Allows you to zoom in or zoom out on the timeline to view recordings in more detail. • : Click the icon to zoom-out the timeline. • : Click the icon to zoom-in the timeline.
3	Audio control	Allows you to enable or disable audio during video playback.
4	Digital zoom	When playing back the video, press and hold the mouse to select the area you want to zoom in on the playback interface and release the mouse. Click the right mouse button to restore the enlargement, and then press the button to turn off the digital zoom in.
5	Snapshot	Captures and saves a snapshot image from the playback video.
6	Download	Click the Download button to pop up the video file download interface
7	Progress bar	Displays the record type and the corresponding period. Click any point in the colored area, and the system will play back the recorded video from the selected moment. Each record type has its own color, and you can see their relations in Record Type Indicators.
8	Play control bar	Control's playback • : Click the icon to play back recorded video. • : Click the icon to stop playing back recorded video. • : Click the icon to jump back 30 seconds backward. • : Click the icon to jump 30 seconds forward.
9	Record Type Indicators	Different colors icons indicate various recording types: • : Indicates the **Regular** recording type • : Indicates the **Motion Detection** recording type • : Indicates the **External Alarm** recording type • : Indicates the **Intelligent** recording type.

Table 3-7 Description of video playback interface

3.5 Snapshot Playback

This section includes snapshot playback features that allow users to search and view recorded snapshots easily.

3.5.1 Snapshot Playback Interface

On the navigation bar, click **Snapshot Playback** to enter the image search interface. This interface can query, view and download images that are stored in the SD card.

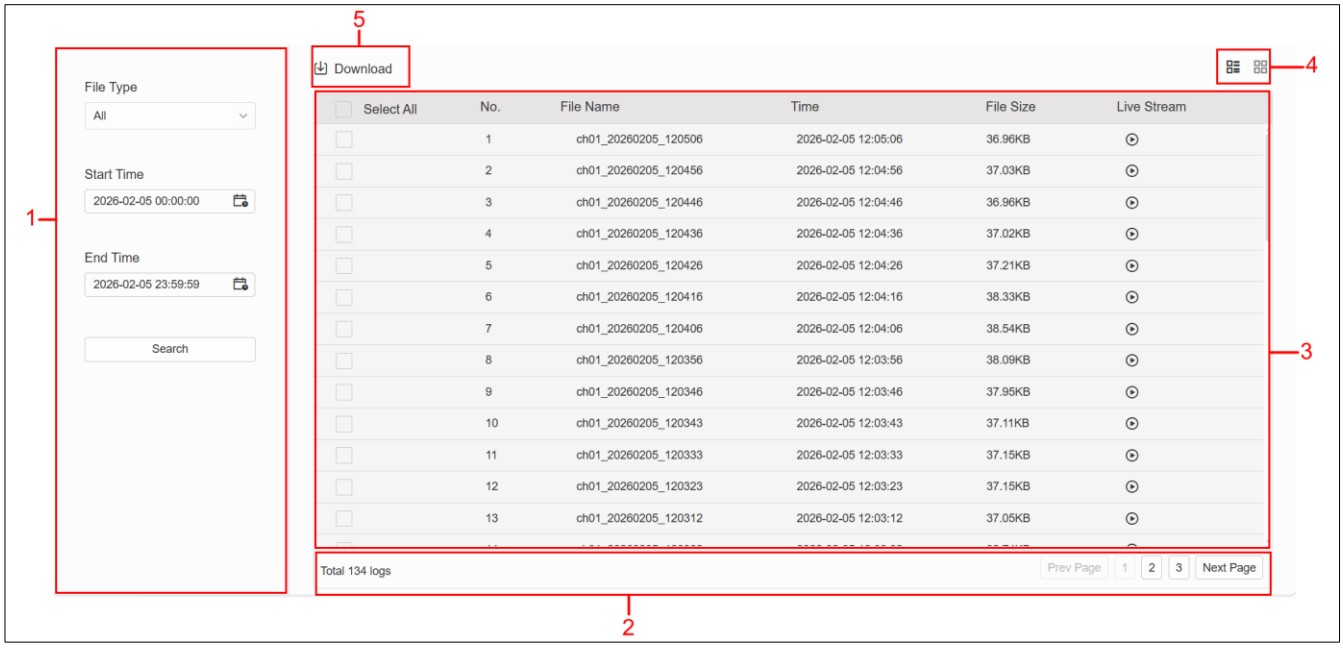

Figure 3-8 Snapshot Playback

No.	Function	Description
1	Search Panel	• Choose the **File Type**, including All, Regular, Motion Detection, External Alarm, Intrusion, Line-Cross Detection, Loitering Detection, and People Gathering. • Set the **Start Time** and **End Time**. • Click **Search** to view snapshots that meet the criteria.
2	Log Status	Displays the total number of available records and provides page navigation controls to browse through the file list.
3	Record List	Shows the list of recorded files with details such as **File No.**, **File Name**, **Time**, **File Size**, and **Live Stream** to preview the images.
4	View Mode	Allow you to switch between different display layouts: • : Display image files as a list • : Display image files as thumbnails

5	Download	Downloads the selected recorded video files to the local device. • Snapshots can be downloaded individually or by using **Select All** to download all at once.

Table 3-8 Description of snapshot playback interface

3.6 Settings

This section provides access to local configuration, account management, network settings, video and image settings, event configuration, and recording management.

3.6.1 Local Config

The Local Config section allows users to configure local storage paths for video files, snapshots, and playback recordings.

Procedure

Step 1 Navigate to **Settings** > **Local Config** > **Local Config**.

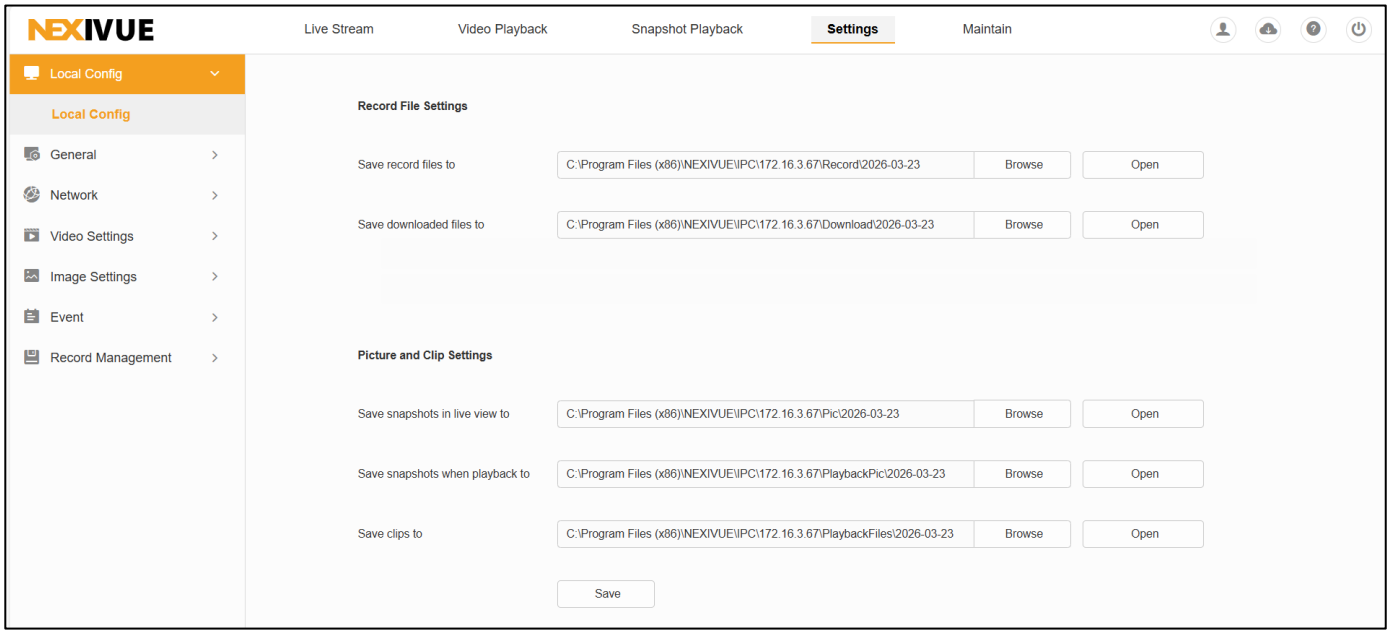

Figure 3-9 Local config

- By default, files are saved to **C:\Users\NEXIVUE\IPC\192.168.1.100**. After downloading and installing the plug-in, the default save path changes to **C:\Program Files (x86)\NEXIVUE\IPC\192.168.1.100**.
- The IP address included in the path refers to the assigned IP address of the camera.

Step 2 Under **Record File Settings**, configure the following paths as required:

Save record files to:

- Click **Browse** to select the local folder where recorded video files will be saved.
- Click **Open** to directly open the selected folder.

Save downloaded files to:

- Click **Browse** to set the local folder for downloaded playback files.
- Click **Open** to view the selected folder.

Step 3 Under **Picture and Clip Settings**, configure storage paths for images and clips:

Save snapshots in live view to:

- Select the folder where snapshots captured during live viewing will be stored.

Save snapshots when playback to:

- Select the folder where snapshots captured during video playback will be stored.

Save clips to:

- Select the folder where clipped video files from playback will be saved.

Step 4 Click **Save** after configuring all required paths.

3.6.2 General

The General section covers time configuration, daylight saving time settings, user management, and access control options.

3.6.2.1 General Settings

Time Settings

Step 1 Navigate to **Settings** > **General** > **General** > **Time Settings**.

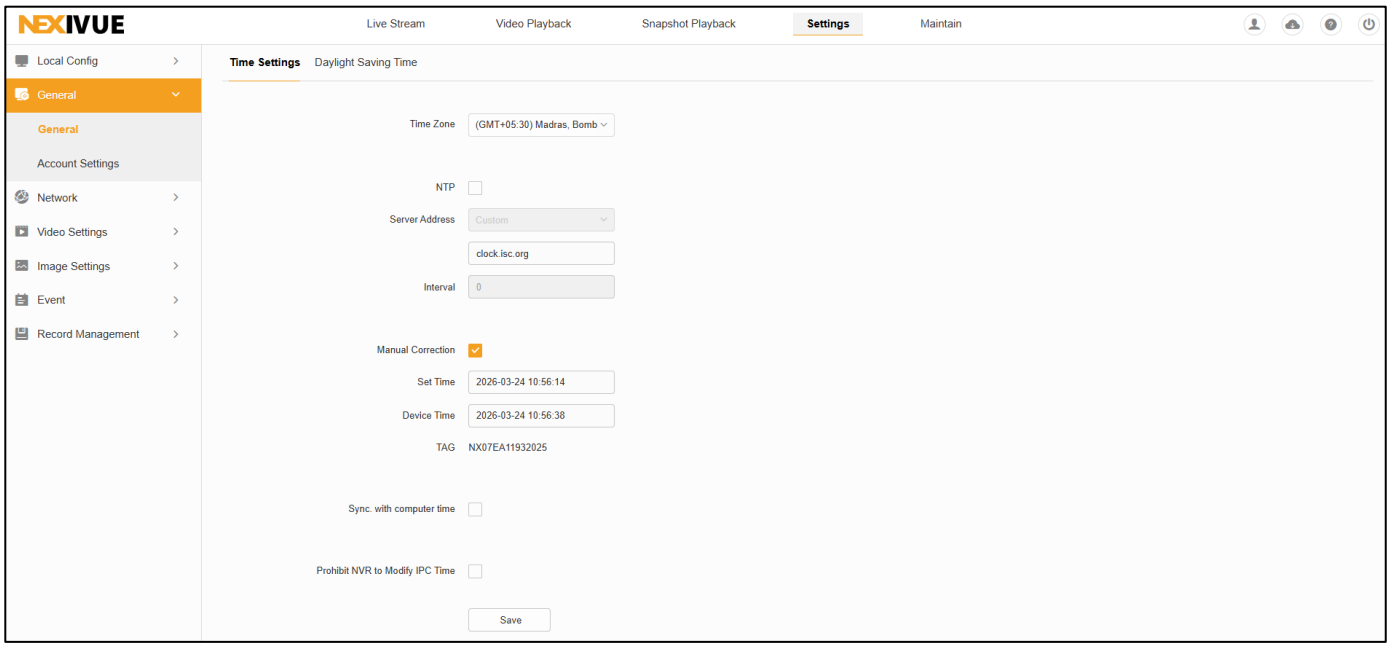

Figure 3-10 Time Settings

Step 2 Set the time zone and time configuration method for the device:

- From the **Time Zone** drop-down list, select the appropriate time zone for the device location.
- Enable **NTP** to synchronize time automatically using an NTP server.
  - Select or enter the **Server Address**.
  - Set the **Interval** for time synchronization.
- Enable **Manual Correction** to set the time manually.
  - Click **Set Time** and enter the required date and time. Device Time displays the current time of the device for reference.

- You can configure the time using either NTP synchronization or Manual Correction. Only one option can be selected at a time.

- Enable **Sync. with computer time** to synchronize the device time with the local computer. The current computer time will be displayed and applied to the device.

- If required, enable **Prohibit NVR to Modify IPC Time** to prevent the NVR from changing the camera time.

Step 3 Click **Save** to apply the time settings.

Daylight Saving Time

Daylight Saving Time (DST) automatically adjusts the camera time when local time changes. It ensures correct timestamps for recording, playback, and event logs.

Step 1 Navigate to **Settings** > **General** > **General** > **Daylight Saving Time**.

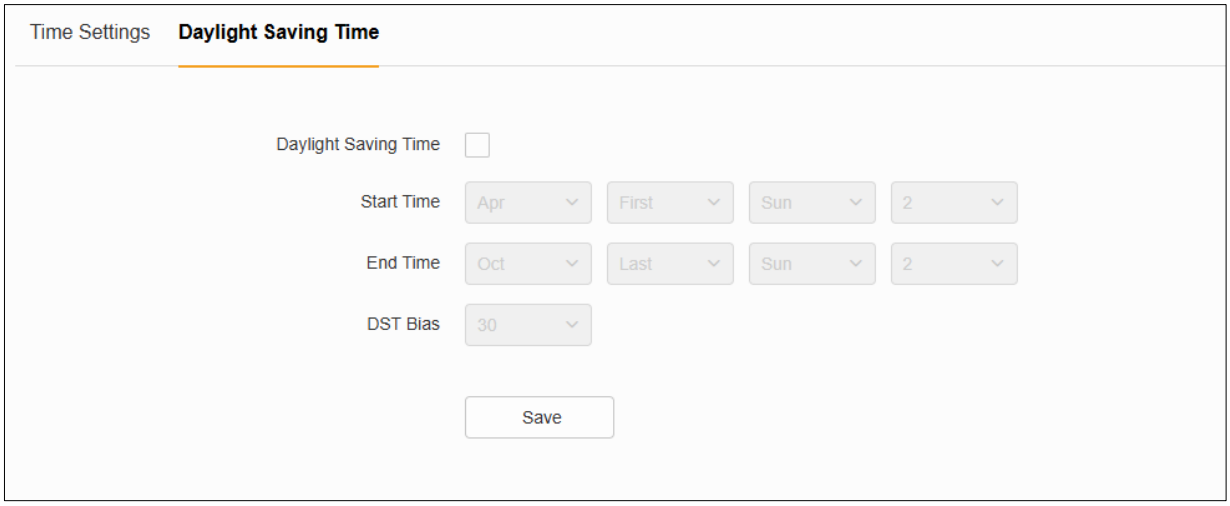

Figure 3-11 Daylight saving time

Step 2 Enable the **Daylight Saving Time** option by selecting the checkbox.

Step 3 Configure the **Start Time** and **End Time** including month, week, day, and hour.

Step 4 Set the **DST Bias** to define the time offset applied during the daylight saving period.

Step 5 Click **Save** to apply the Daylight Saving Time settings.

3.6.2.2 Account Settings

This section provides options for managing user accounts, viewing current active users, and monitoring or controlling any unauthorized access to the device.

User Management

This page provides options to add new users and edit existing user details.

Step 1 Navigate to **Settings** > **General** > **Account Settings** > **User Management**.

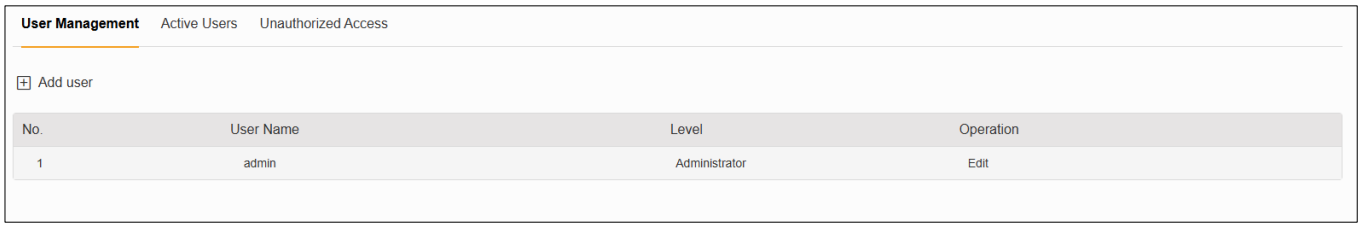

Figure 3-12 User Management

Step 2 Click **Add User** to add a new user account.

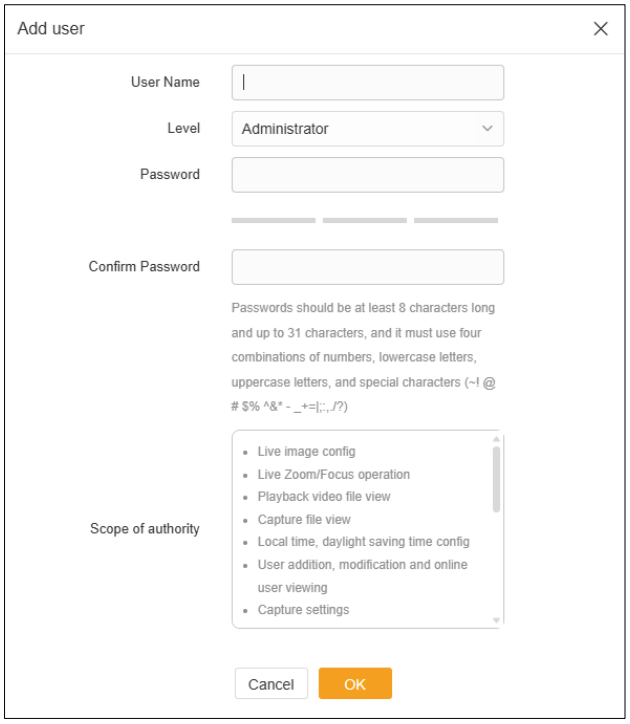

Figure 3-13 Add User

Step 3 Enter a **User Name** for the new account.

Step 4 From the **Level** drop-down list, select the required user level:

- **Administrator**: Full access to live view, playback, system configuration, device management, and user management.

- **Operator**: Access to live view, playback, and most system configuration and maintenance features, excluding user management.
- **User**: Basic access to live view functions, including image viewing and zoom/focus operations only.

Step 5 Enter a **Password** and **Confirm Password** for the user.

- Ensure that the passwords should be at least 8 characters long and up to 31 characters, and it must use four combinations of numbers, lowercase letters, uppercase letters, and special characters (~! @ # $% ^&* - _+=|;:,./?)

Step 6 Click **OK** to save the user or click **Cancel** to exit without saving.

Related Operations

- You can modify the password of the admin.
- You can update E-mail ID, mobile number and security questions/answers for password reset.
- You can create/delete a new user and modify permission level.

Edit User Information

- Click **Edit** to change the password and level of the existing account.

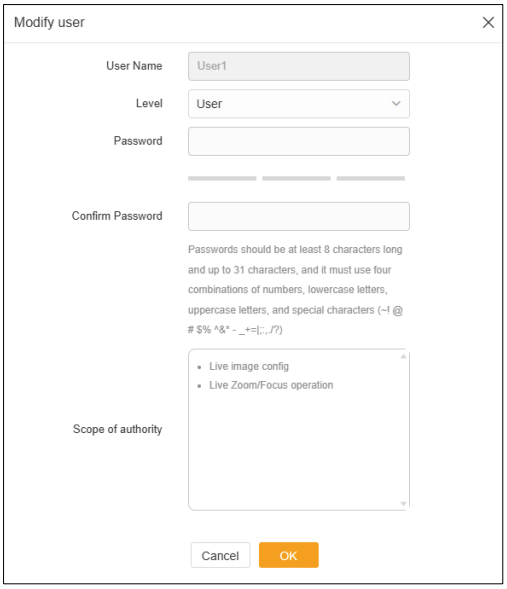

Figure 3-14 Modify User

- Enter the new password and select the level according to your requirements.
- Click **OK** to save the user or click **Cancel** to exit without saving.

Modify Level

- You cannot change the level of the admin account.

- Click **Level** to only change the level of the user account.

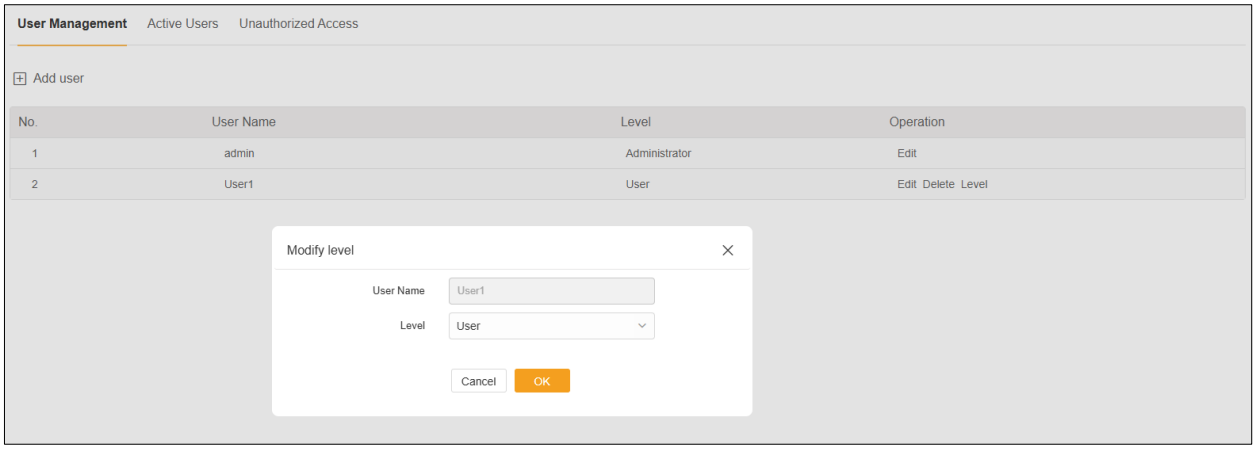

Figure 3-15 Modify level

- Select the level of the user account according to your requirements.
- Click **OK** to save the user or click **Cancel** to exit without saving.

Delete User

- Admin account cannot be deleted.

- Click **Delete** to delete the existing user account.

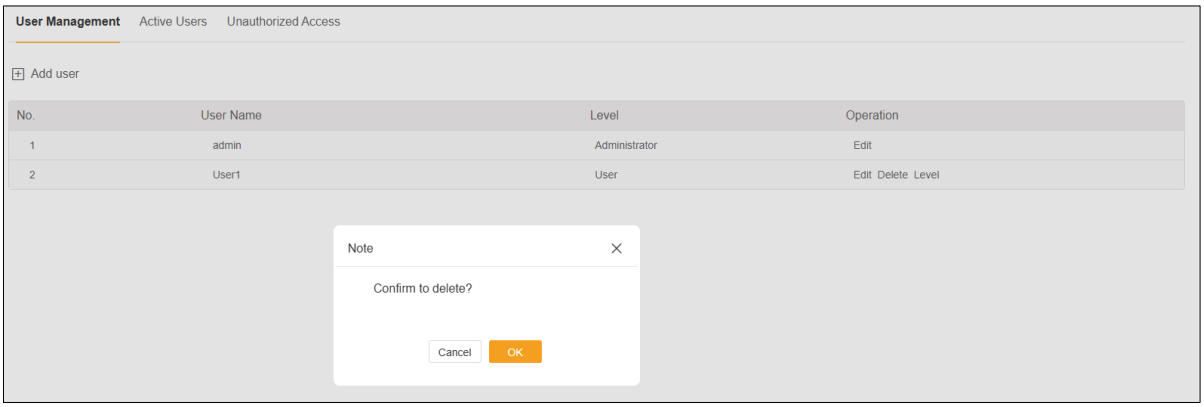

Figure 3-16 Delete user

- Click **OK** to confirm.

Active Users

This section displays the list of users who are currently logged in to the device along with their user level, IP address, and operation time.

Figure 3-17 Active users

- Click **Refresh** to update the active user list to show the latest login and activity information.

Unauthorized Access

This section allows you to configure security settings to prevent unauthorized access by locking the device after a defined number of illegal login attempts.

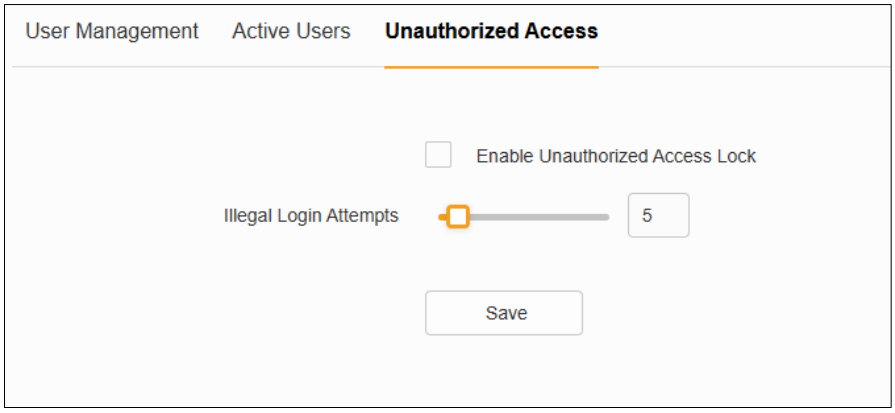

Figure 3-18 Unauthorized access

Step 1 Enable **Unauthorized Access Lock** by selecting the checkbox.

Step 2 Set the **Illegal Login Attempts** value using the slider or input box to define the maximum number of failed login attempts allowed.

Step 3 Click **Save** to apply the settings.

3.6.3 Network

This section introduces network configuration.

- The camera has connected to the network.

3.6.3.1 Net Settings

TCP/IP

This section displays the network configuration settings of the device. It allows you to configure IPv4 and IPv6 network parameters, enable or disable DHCP, set DNS servers, and define communication ports such as HTTP, HTTPS, and RTSP for network access and streaming.

Procedure

Step 1 Navigate to **Settings** > **Network** > **Net Settings** > **TCP/IP**.

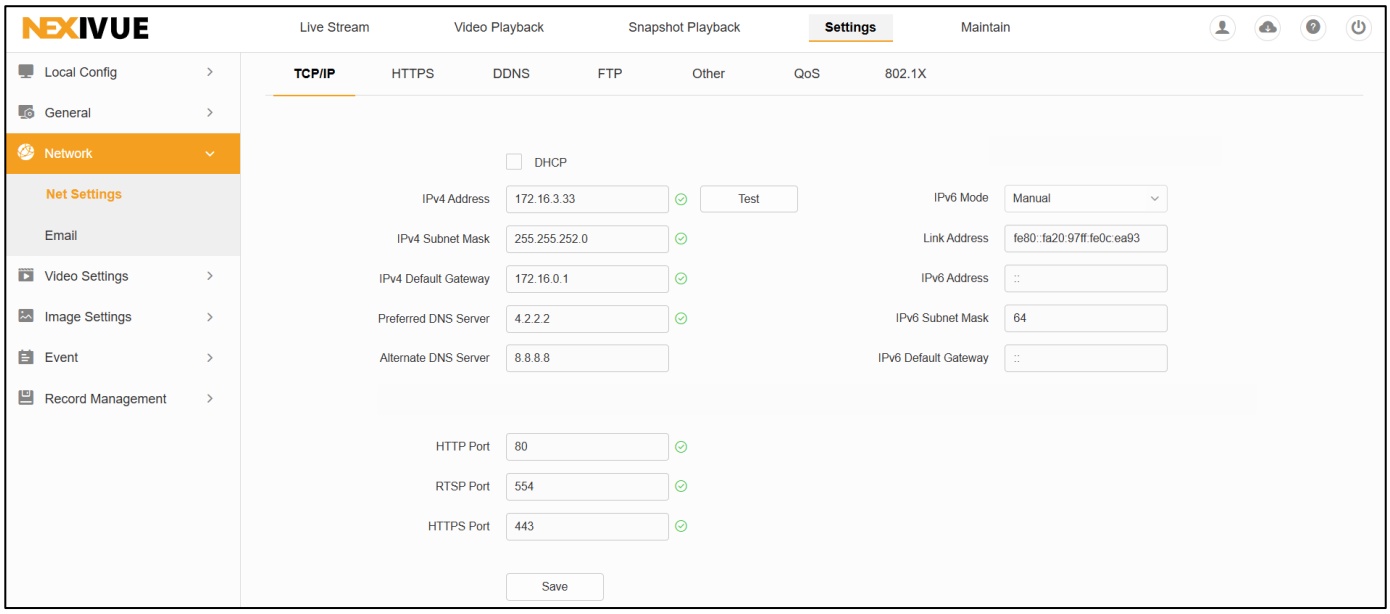

Figure 3-19 TCP/IP

Step 2 Configure TCP/IP parameters.

Parameter	Description
DHCP	When enabled, the device automatically obtains the IPv4 address and related network parameters from the network. Manual IPv4 settings are disabled.
IPv4 Address	Set the device IPv4 address manually when DHCP is disabled.
Test	Click to verify whether the configured IPv4 address is available on the network before saving.
IPv4 Subnet Mask	Configure the subnet mask corresponding to the IPv4 address.
IPv4 Default Gateway	Configure the default gateway for IPv4 network communication.
IPv6 Mode	Select the IPv6 configuration method: **Manual**, **DHCP**, or **Route Advertisement**. • When **IPv6 Mode** is set to **DHCP** or **Route Advertisement**, the **IPv6 Address**, **IPv6 Subnet Mask**, and **IPv6 Default Gateway** fields are automatically disabled, as these parameters are obtained from the network and do not require manual configuration.
IPv6 Address	Configure the IPv6 address when **IPv6 Mode** is set to **Manual**.
IPv6 Subnet Mask	Configure the IPv6 subnet mask when **IPv6 Mode** is set to **Manual**.
IPv6 Default Gateway	Configure the IPv6 default gateway when **IPv6 Mode** is set to **Manual**.
Preferred DNS Server	Enter the IP address of the preferred DNS server to enable functions that require domain name access.
Alternate DNS Server	Enter the IP address of the alternate DNS server for backup DNS resolution.
HTTP Port	Configure the HTTP port used for web access. If modified, the port number must be added after the IP address in the browser.
HTTPS Port	Configure the HTTPS port for secure web access. If modified, the port number must be added after the IP address in the browser.
RTSP Port	Configure the RTSP port for real-time video streaming. Ensure the selected port is available.

Table 3-9 Description of TCP/IP parameters

Step 3 Click **Save** to save and apply all configured TCP/IP parameters.

HTTPS

The HTTPS protocol is a network protocol constructed by the SSL+HTTP protocol that can perform encrypted transmission and identity authentication, which can improve the security of WEB access.

Procedure

Step 1 Navigate to **Settings** > **Network** > **Net Settings** > **HTTPS**.

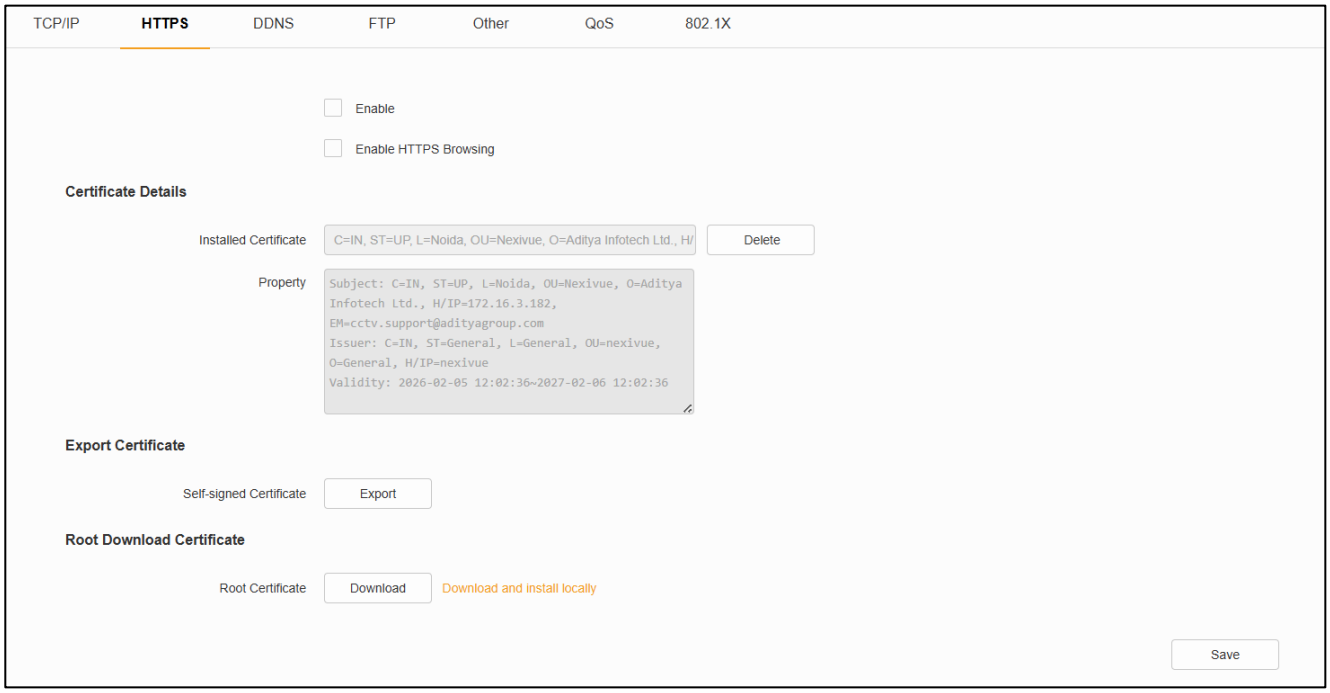

Figure 3-20 HTTPS

Step 2 Check **Enable** to activate the HTTPS service.

Step 3 Check **Enable HTTPS Browsing** to allow secure access to the device via a web browser

- If a certificate is already installed, its details will be displayed under **Certificate Details**.
- If you want to import a new certificate, please click **Delete** to remove the installed certificate first.

Step 4 Create a certificate or install an authenticated certificate.

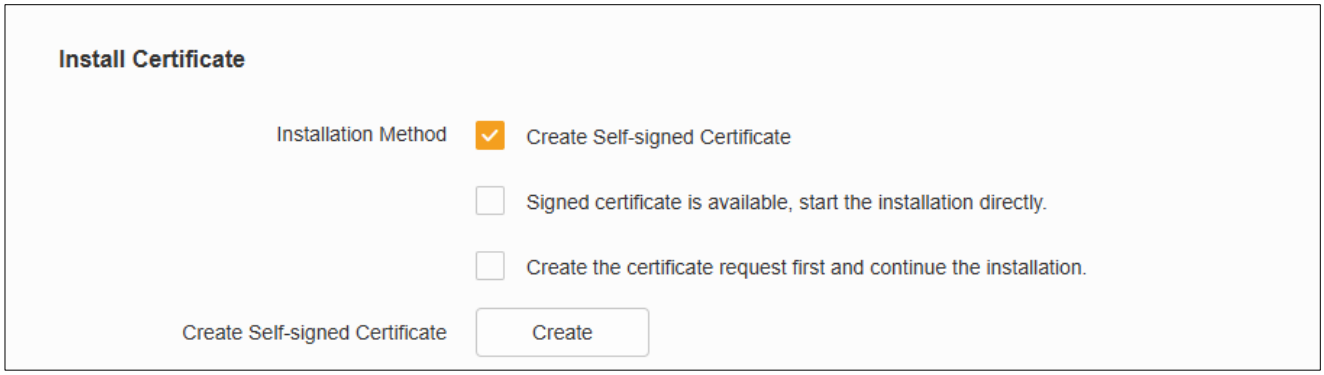

Figure 3-21 Install Certificate

- For creating a self-signed certificate:

  Step 1 Check the **Create Self-signed Certificate** checkbox and click **Create**.

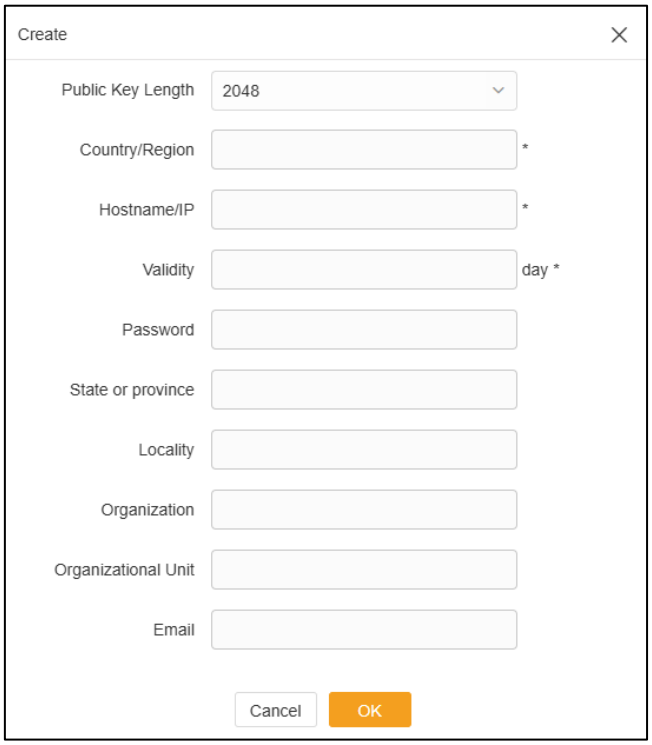

Figure 3-22 Create dialog box

Step 2 Enter details such as country, domain name/IP, validity period, and other required parameters.

Step 3 Click **OK** to generate the certificate.

- For installing a signed certificate:

Figure 3-23 Install certificate (1)

Step 1 Check the **Signed certificate is available, start the installation directly** checkbox.

Step 2 Click **Browse** to select the signed certificate file.

Step 3 Click **Install**, then click **Save**.

- For creating a certificate request:

Figure 3-24 Install certificate (2)

Step 1 Check the **Create the certificate request first and continue the installation** checkbox and click **Create**.

Step 2 Enter details such as country, domain name/IP, validity period, and other required parameters.

Step 3 Click **OK** to generate the request.

Step 4 Download the request and submit it to a certification authority.

Step 5 After receiving the signed certificate, delete the certificate request.

Step 6 Click **Browse** to select the signed certificate file.

Step 7 Click **Install**, then click **Save**.

Step 5 Under **Export Certificate**, click **Export** to export a self-signed certificate.

Step 6 Under **Root Download Certificate**, click **Download** to download the root certificate.

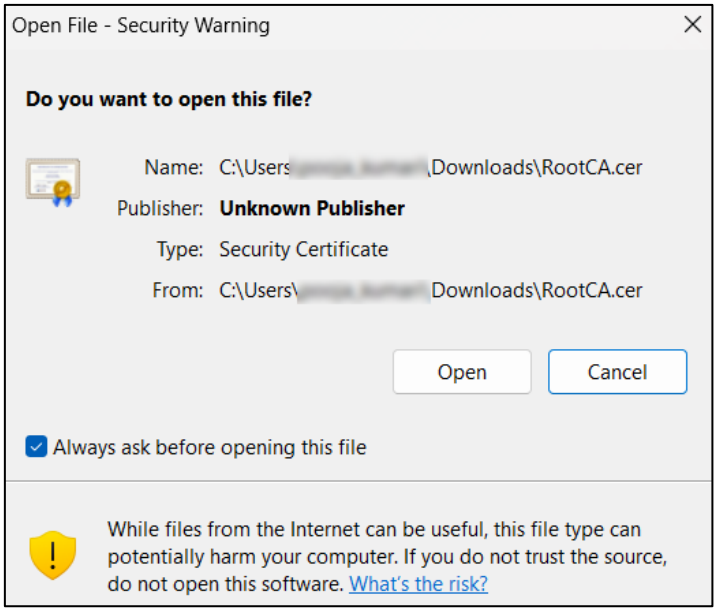

Figure 3-25 File download

Step 7 Click **Open**.

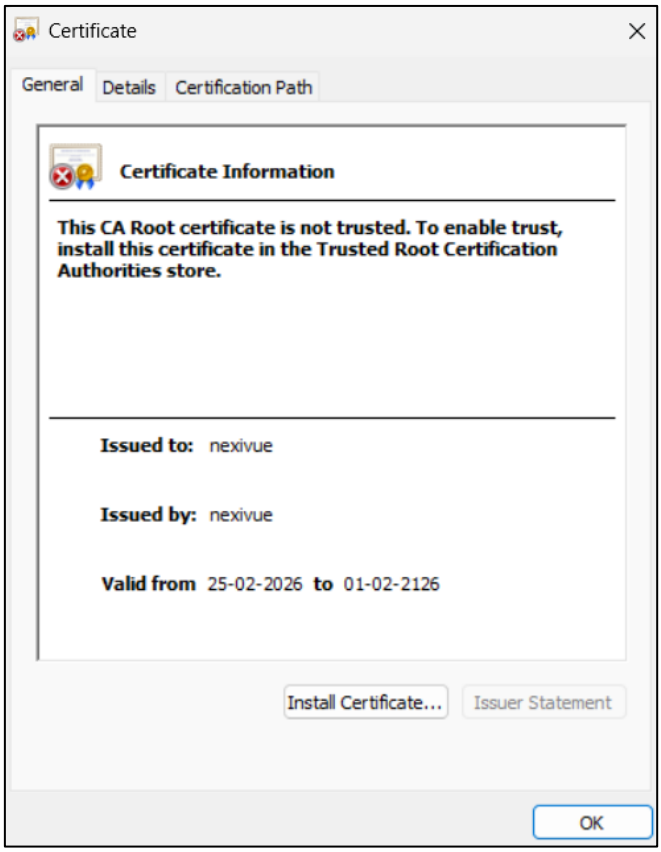

Figure 3-26 Certificate information

Step 8 Click **Install Certificate**.

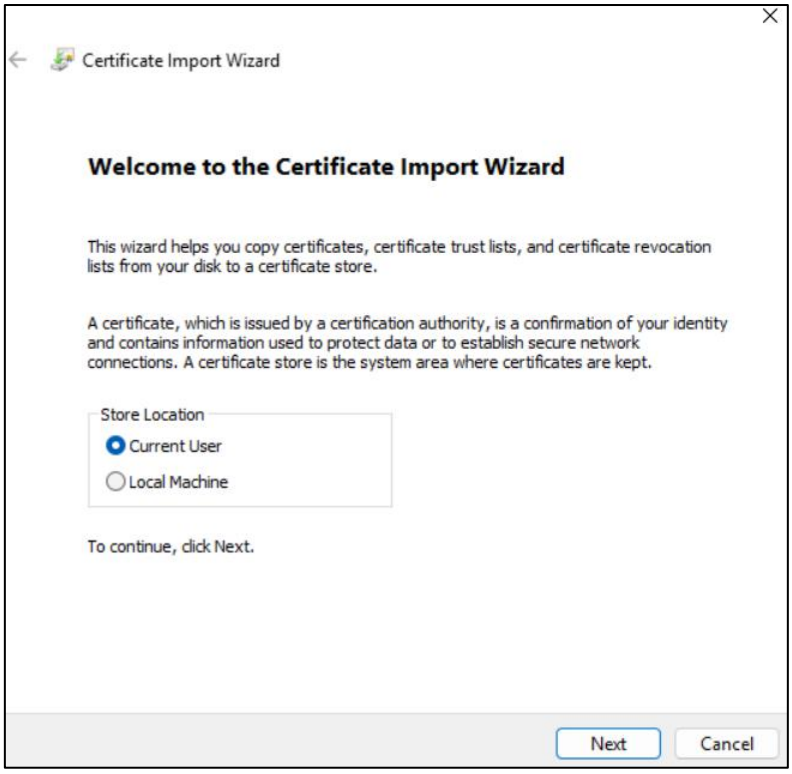

Figure 3-27 Certificate import wizard

Step 9 Click **Next**.

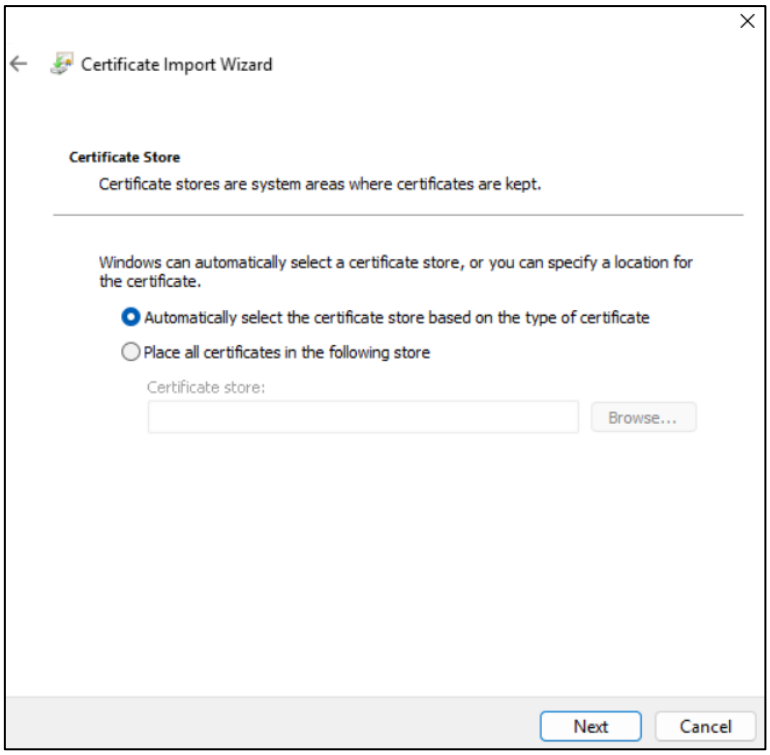

Figure 3-28 Certificate store

Step 10 Select the storage location and click **Next**.

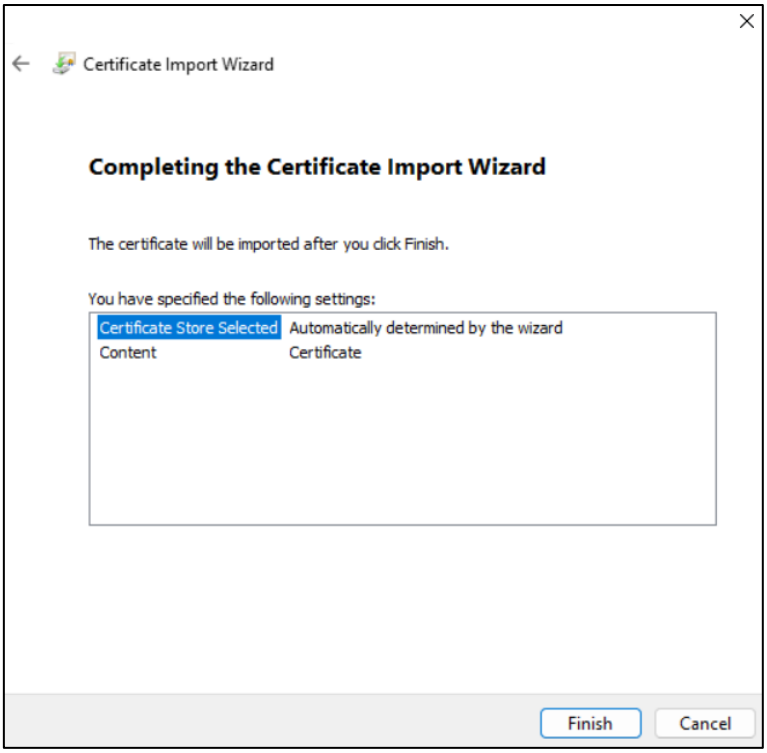

Figure 3-29 Finish page

Step 11 Click **Finish** and a dialog box showing **The import was successful** pops up.

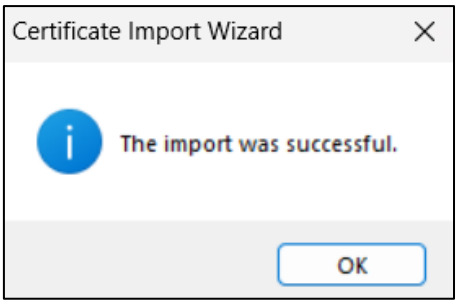

Figure 3-30 Import succeeds

DDNS

DDNS updates the device IP automatically, so you can always access the camera using the same domain name.

Procedure

Step 1 Navigate to **Settings** > **Network** > **Net Settings** > **DDNS**.

- Check the type of DNS server supported by the camera.
- Third party server might collect your device information after DDNS is enabled.
- Register and log in to the DDNS website, and then you can view the information of all the connected devices in your account.
- The correct LAN IP address, mask, gateway and DNS server must be set for DDNS function. Please go to TCP/IP interface to confirm or configure.
- When accessing through the DDNS domain name, it is required that the IPC must be connected to the Internet.

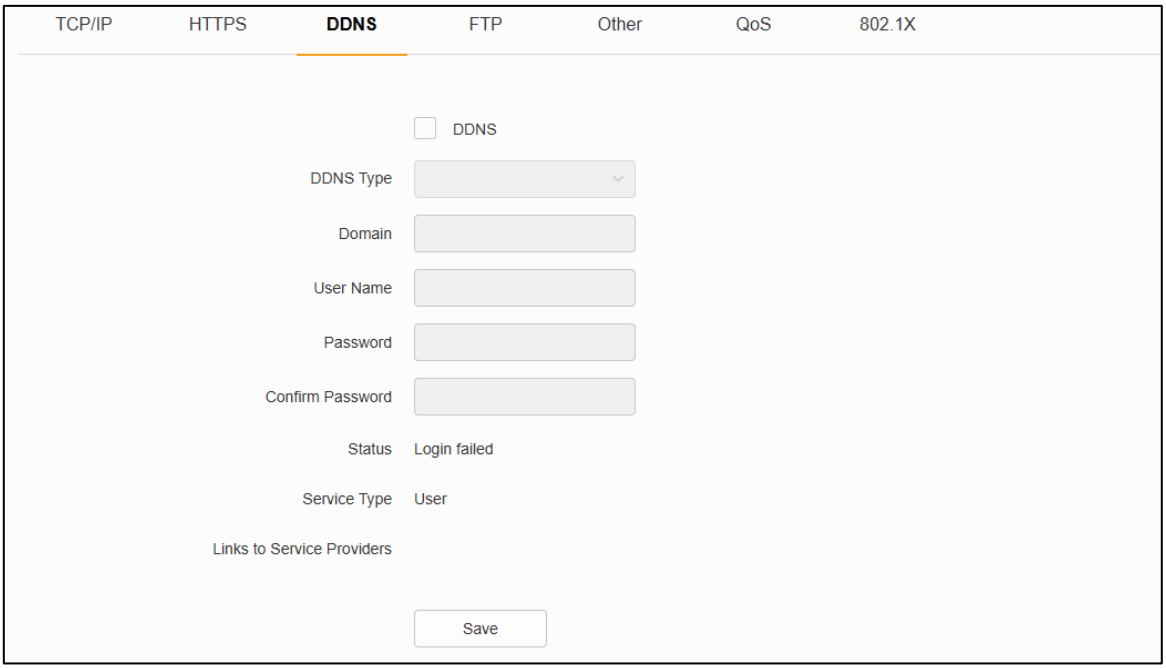

Figure 3-31 DDNS

Step 2 Check the **DDNS** checkbox.

Step 3 Select **DDNS Type**, and configure the parameters as needed.

Parameter	Description
DDNS Type	Select the DDNS service provider. Supported options include Dyn and NO-IP. The name and web address of the DDNS service provider, see the matching relationship below: • NO-IP DDNS web address: dynupdate.no-ip.com • Dyndns DDNS web address: members.dyndns.org

Domain	The domain name you registered on the DDNS website.
User Name	Enter the username and password that you got from the DDNS server provider. You need to register an account (including username and password) on the DDNS server provider's website.
Password	
Confirm Password	
Status	Displays the current DDNS connection status (for example, login successful or failed).
Service Type	Displays the account type used for DDNS service.
Links to Service Providers	Provides quick access links to supported DDNS service provider websites.

Table 3-10 Description of DDNS parameters

FTP

This page allows you to configure FTP/SFTP settings to upload snapshots or alarm files to a remote server for storage and backup. FTP can be enabled only when it was selected as a destination path.

Procedure

Step 1 Navigate to **Settings** > **Network** > **Net Settings** > **FTP**.

Step 2 Select the **Enable** check box and select the **FTP Protocol** type.

- You select **FTP** or **SFTP** from the drop-down list. **SFTP** is recommended to enhance network security.

Step 3 Configure FTP parameters.

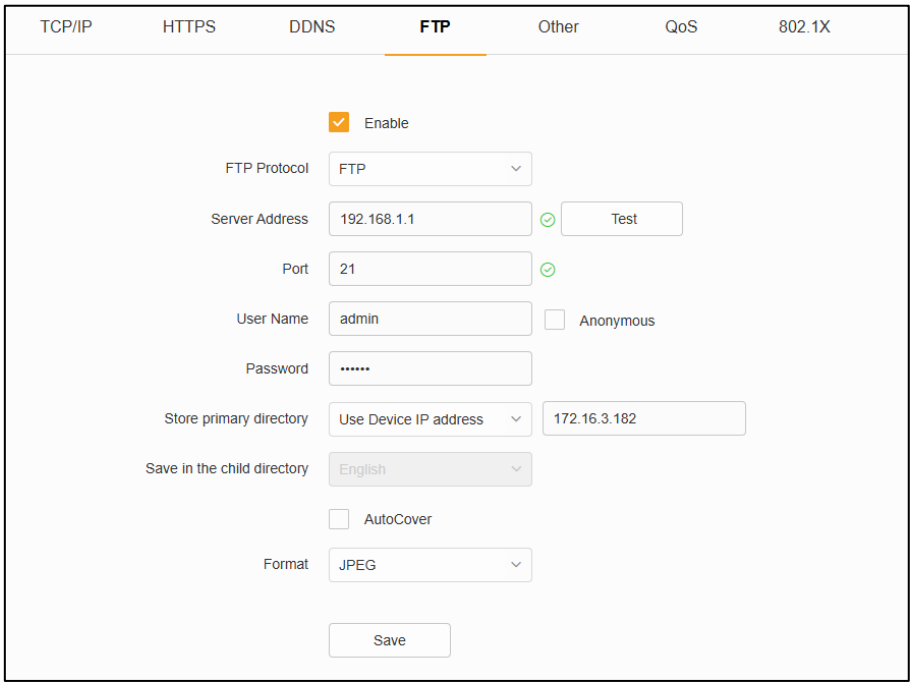

Figure 3-32 FTP

Parameter	Description
Server Address	The IP address of the FTP/SFTP server where files will be uploaded.
Test	Verify the connectivity between the device and the FTP/SFTP server.
Port	Specify the communication port number of the FTP/SFTP server. By default, the port number is 21.
Username	The username to log in to the FTP/SFTP server.
Password	The password to log in to the FTP/SFTP server.
Anonymous	Allows login to the FTP server without a username and password when supported by the server.
Store Primary Directory	The main directory where files will be stored. Options include: • **Use Device IP Address:** Creates a folder using the device IP address. • **Use OSD:** Creates a folder using the device OSD name. • **Custom:** Allows manual entry of the storage directory name.
Save in the Child Directory	Saves files inside a subfolder under the primary directory.
AutoCover	Automatically overwrites old files when the storage space becomes full.
Format	The file format used to save uploaded files. By default, it's JPEG.

Table 3-11 Description of FTP parameters

Step 4 Click **Save**.

Step 5 Click **Test** to test whether FTP function works normally.

Other

This section provides additional network service options to enhance device security, compatibility, and remote management.

Procedure

Step 1 Navigate to **Settings** > **Network** > **Net Settings** > **Other**.

Step 2 Configure the other network services according to your requirements.

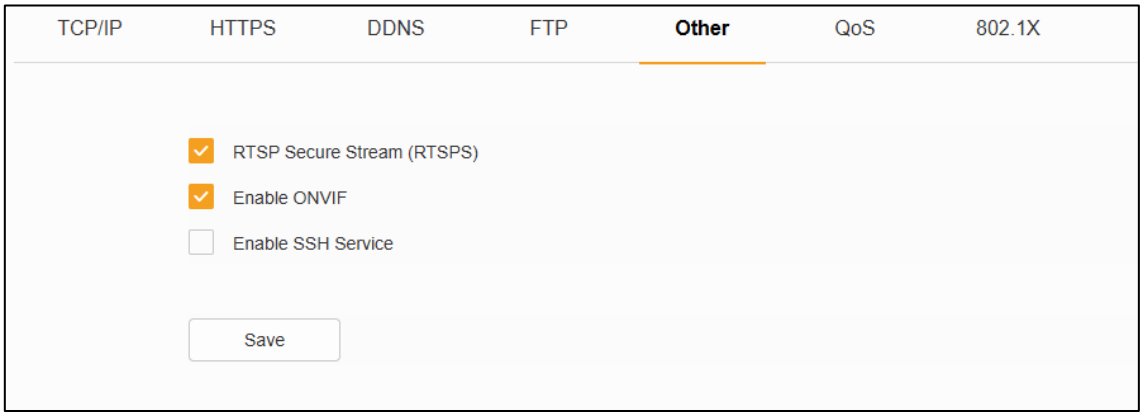

Figure 3-33 Other network services

Option	Description
RTSP Secure Stream (RTSPS)	Enable encrypted RTSP streaming to protect video data during transmission.
Enable ONVIF	Allows ONVIF protocol support for interoperability with third-party NVRs and video management systems.
Enable SSH Service	Enable secure shell (SSH) access for advanced maintenance and troubleshooting.

Table 3-12 Description of network services

Step 3 Click **Save** to save the configured settings.

QoS

You can solve problems such as network delay and congestion with this function. It helps to assure bandwidth, reduce transmission delay, packet loss rate, and delay jitter to improve experience. 0–63 means 64 degrees of priority; 0 for the lowest and 63 the highest.

- The QoS function requires the support of network devices (such as routers) on the transmission path.
- Some cameras do not support the QoS function; please refer to the actual interface.

Procedure

Step 1 Navigate to **Settings** > **Network** > **Net Settings** > **QoS**.

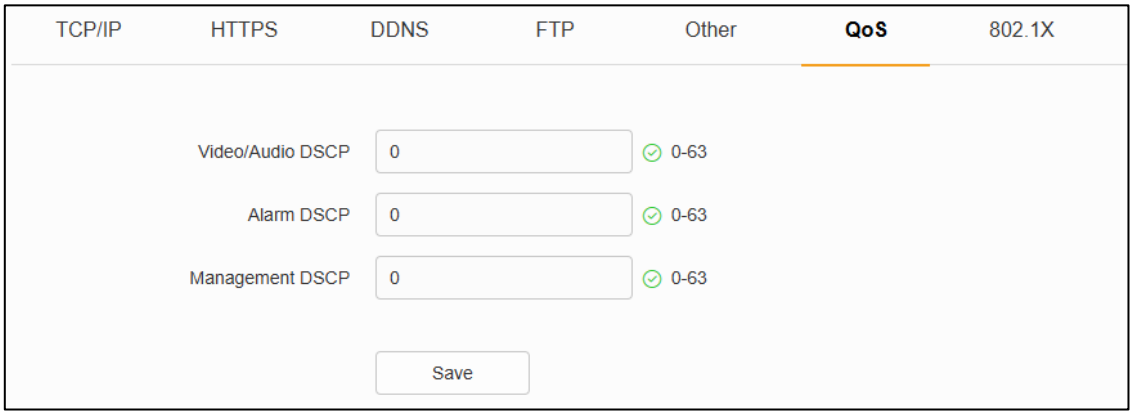

Figure 3-34 QoS

Step 2 Configure QoS parameters.

Option	Description
Video/Audio DSCP	Set the DSCP value (0–63) to prioritize video and audio data packets on the network.
Alarm DSCP	Assign a DSCP value (0–63) to prioritize alarm and event-related data traffic.
Management DSCP	Define the DSCP value (0–63) for device management and control traffic.

Table 3-13 Description of QoS parameters

Step 3 Click **Save** to save the configured settings.

802.1X

This section is used to configure IEEE 802.1X network access control, allowing the device to authenticate with the network before gaining access, thereby enhancing network security. Cameras can access the LAN only after successfully passing 802.1X authentication.

- Some cameras do not support the 802.1X function; please refer to the actual interface.

Procedure

Step 1 Navigate to **Settings** > **Network** > **Net Settings** > **802.1X**.

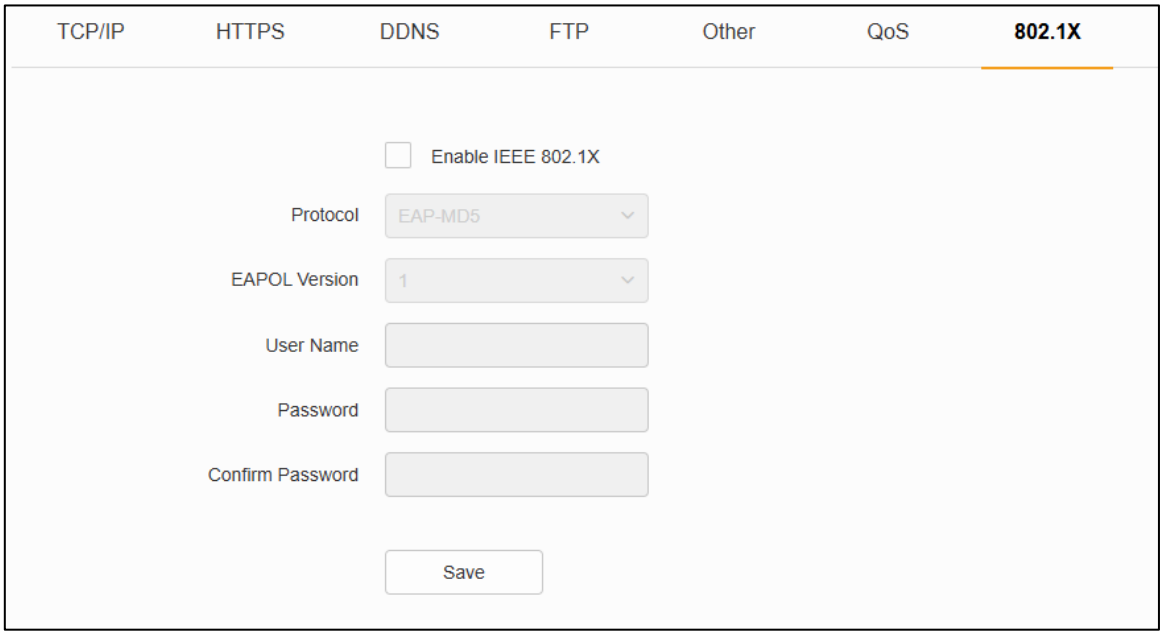

Figure 3-35 802.1X

Step 2 Check the **Enable IEEE 802.1X** check box and then configure the parameters.

Option	Description
Protocol	Select the authentication method used for 802.1X access: • **EAP-MD5:** Password-based authentication with basic security, no certificate support. • **EAP-LEAP:** Cisco-based authentication using dynamic keys for enhanced security.
EAPOL Version	Displays the EAP over LAN version applied according to the selected protocol.
User Name	Enter the username provided by the authentication server for 802.1X access.
Password	Enter the password associated with the 802.1X user account.

Confirm Password	Re-enter the password to confirm accuracy.

Table 3-14 Description of 802.1X parameters

Step 3 Click **Save** to save the configured settings.

3.6.3.2 Email

By setting the email parameter, it will send email to the specified mailbox when an alarm occurs.

Procedure

Step 1 Navigate to **Settings** > **Network** > **Email**.

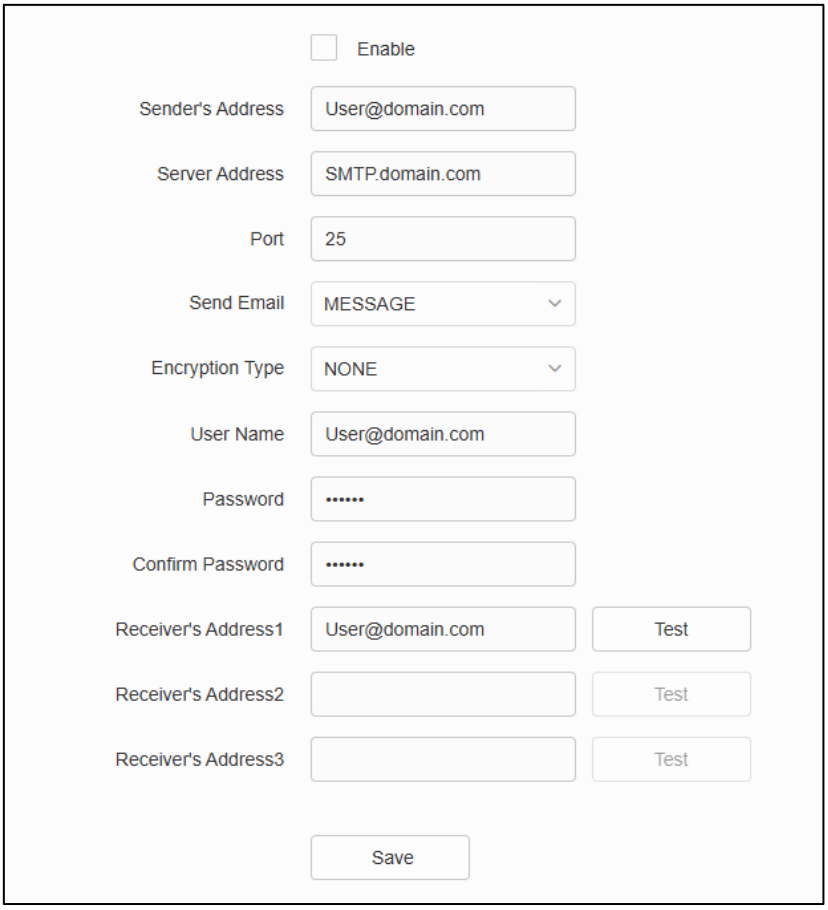

Figure 3-36 Email

Step 2 Check the **Enable** checkbox to enable email notification function.

Step 3 Configure the email parameters.

Parameter	Description
Sender's Address	Email address used by the device to send notification emails.
Server Address	SMTP server address provided by the email service provider.
Port	Port number used by the SMTP server (for example, 25, 465, or 587).
Send Email	Select the type of content to be sent in the email notification: • **Message:** Sends a text-based email containing event or alarm information. • **JPEG:** Sends an email with a captured JPEG image attached along with the event information.
Encryption Type	Select the encryption method for email transmission: • **None:** Sends emails without encryption. • **SSL:** Uses SSL encryption to secure email communication. • **TLS:** Uses TLS encryption to provide secure and reliable email transmission.
User Name	Username for SMTP server authentication, usually the sender's email address.
Password	Password corresponding to the SMTP user account.
Confirm Password	
Receiver's Address 1	Email address to receive alarm or event notifications.
Receiver's Address 2	
Receiver's Address 3	
Test	Sends a test email to verify the email configuration.

Table 3-15 Description of email parameters

Step 4 Click **Save** to save the configured settings.

3.6.4 Video Settings

Video Settings allow you to configure video encoding parameters and audio settings to optimize video quality, bandwidth usage, and sound recording according to your monitoring requirements.

- Some IP cameras support different configurations; please refer to the actual interface.

3.6.4.1 Encode

This section allows you to configure video stream parameters such as compression format, resolution, frame rate, and bit rate to optimize video quality, storage usage, and network bandwidth.

Procedure

Step 1 Navigate to **Settings** > **Video Settings** > **Encode**.

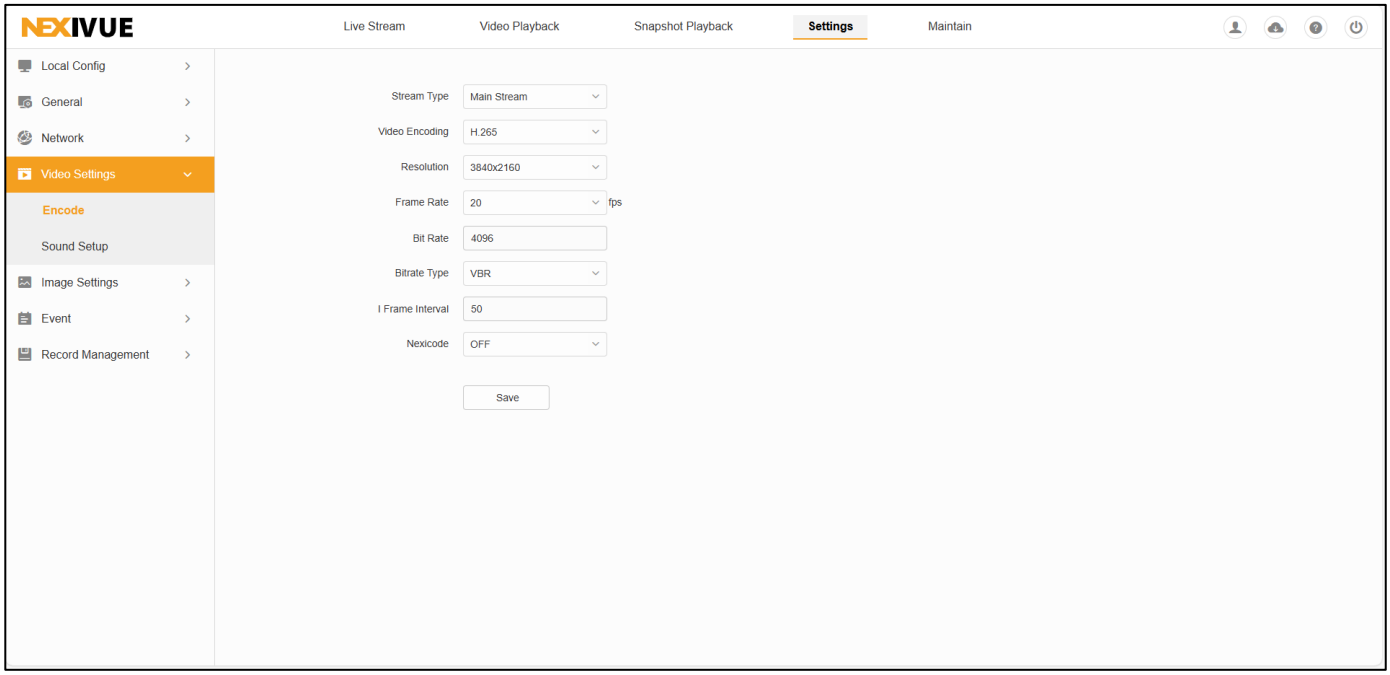

Figure 3-37 Encode

Step 2 Configure the encoding settings as required for video quality, bandwidth, and storage.

Parameter	Description
Stream Type	Select the video stream type: • **Mainstream:** It has a large bit stream value and image with high resolution, but also requires a large bandwidth. This option can be used for storage and monitoring. • **Sub Stream:** It has a small bit stream value and a smooth image and requires less bandwidth. This option is normally used to replace mainstream when the bandwidth is not enough. • **Third Stream:** It has a very small bit stream value with basic image quality and requires minimal bandwidth.
Video Encoding	Select the compression format to balance video quality and storage efficiency: • **H.265:** Higher compression, same quality, lower bandwidth and storage. • **H.264:** Standard compression with broad compatibility and stable performance.
Resolution	Sets the output video resolution; higher resolution provides clearer images but uses more bandwidth.
Frame Rate (fps)	Define the number of frames per second; higher values provide smoother video motion.
Bit Rate	Specifies the amount of data used for video transmission; a higher bit rate improves quality but increases bandwidth usage.
Bitrate Type	The bit rate control type during video data transmission. You can select the bit rate type from: • **CBR (Constant Bit Rate):** The bit rate changes a little and stays close to the defined bit rate value. • **VBR (Variable Bit Rate):** The bit rate changes as the monitoring scene changes. • This parameter can only be configured when **Nexicode** is set as **OFF**.
I-Frame Interval	Set the interval between key frames (I-frames); lower values improve seek accuracy but increase bit rate. It is recommended to set I Frame Interval twice as big as Frame Rate(FPS). • This parameter can only be configured when **Nexicode** is set as **OFF**.
Nexicode	Enable or disable advanced encoding optimization to improve compression efficiency when supported.

	• When **Nexicode** is enabled, the **I-Frame Interval** and **Bitrate Type** options are automatically disabled, as these parameters are managed internally by **Nexicode** for optimized video compression and bandwidth usage.

Table 3-16 Description of encoding parameters

Step 3 Click **Save** to save the configured settings.

3.6.4.2 Sound Setup

This section allows you to configure audio input, encoding, and output parameters for synchronized audio recording and playback along with video streams.

Procedure

Step 1 Navigate to **Settings** > **Video Settings** > **Sound Setup**.

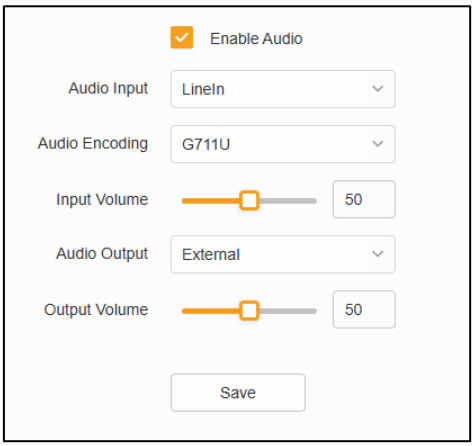

Figure 3-38 Sound Setup

Step 2 Configure the audio settings based on the connected audio devices and required audio quality.

- The **Enable Audio** checkbox is checked by default.
- Some IP cameras support different configurations; please refer to the actual interface.

Parameter	Description
Audio Input	Select the audio input source. By default, **LineIn** is selected for external audio input devices.
Audio Encoding	Define the audio compression format used for transmission. • **G711U:** µ-law encoding, commonly used in IP surveillance. • **G711A:** A-law encoding, optimized for better quality in some regions.

	• **AAC:** Advanced Audio Coding for higher audio quality at lower bitrates.
Input Volume	The gain control value of the audio input source, user can adjust 1-100 according to the actual volume demand.
Audio Output	Select the audio output mode. By default, **External** is selected for audio playback through an external speaker or device.
Output Volume	The gain control value of the audio output, the user can adjust 1-100 according to the actual volume demand.

Table 3-17 Description of sound setup parameters

3.6.5 Image Settings

This section introduces the available image settings and on-screen display (OSD) parameters for configuration.

3.6.5.1 Image

This section provides controls for focus, exposure, day/night behavior, white balance, video tuning, video enhancement, and backlight compensation to ensure the best image quality possible.

Step 1 Navigate to **Settings** > **Image Settings** > **Image**.

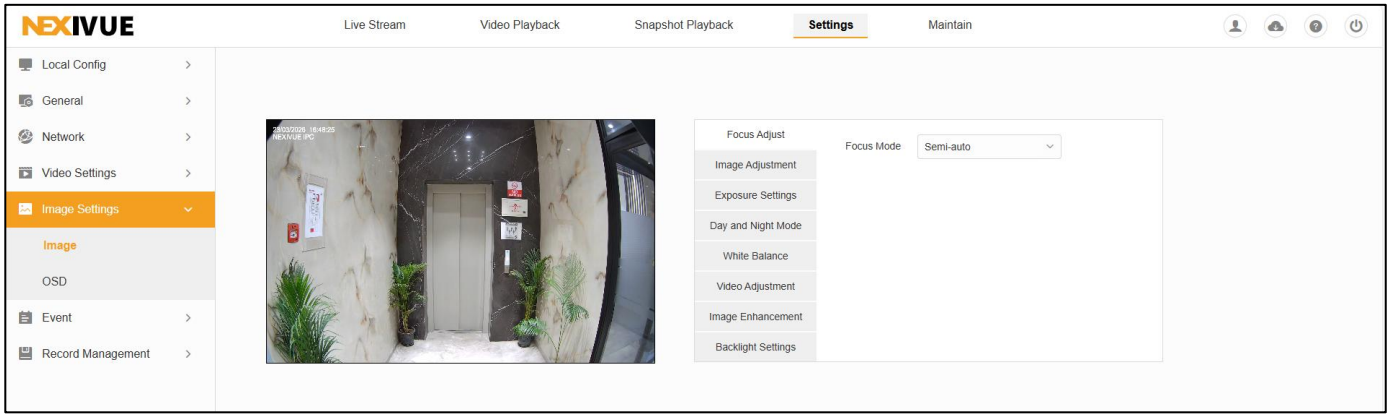

Figure 3-39 Image settings

Step 2 Configure different image controls as per the requirements.

Focus Adjust

You can configure the focus adjustment as needed.

Step 1 Navigate to **Settings** > **Image Settings** > **Image** > **Focus Adjust**.

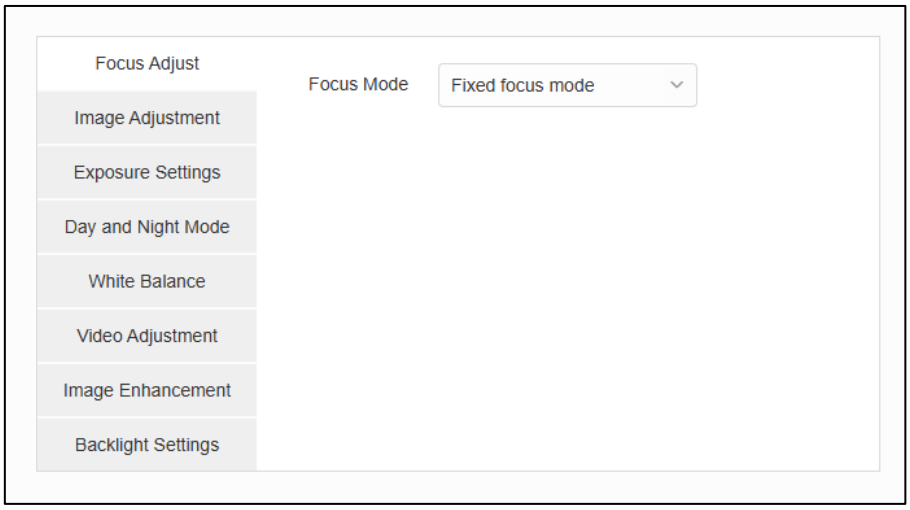

Figure 3-40 Focus Adjust

Step 2 Select the **Focus Mode** to adjust how the camera focuses on objects in the scene for clear and accurate image capture.

- **Auto:** Automatically adjusts focus continuously to keep the image sharp.
- **Semi-auto:** Adjusts focus when triggered, then holds the focus until changed again.
- **Manual:** Allows the user to manually set the focus position.
- **Fixed Focus Mode:** Uses a preset fixed focus, suitable for scenes with a constant distance.

Image Adjustment

You can configure the image adjustment parameters as needed.

Step 1 Navigate to **Settings** > **Image Settings** > **Image** > **Image Adjustment**.

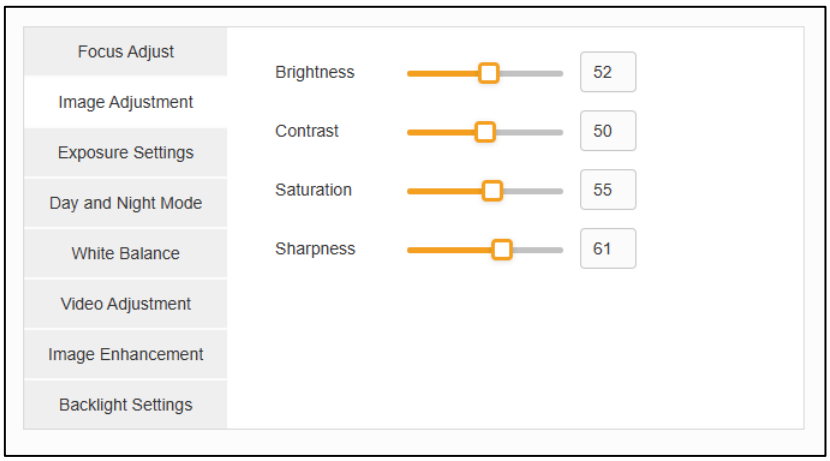

Figure 3-41 Image adjustment

Step 2 Configure image adjustment parameters by dragging the progress bar according to the actual environment.

Brightness, **Contrast**, **Saturation** and **Sharpness** valid values range from: 0-100, the default value is 50, which takes effect directly after mouse dragging.

Parameter	Description
Brightness	Changes the value to adjust the picture brightness. The higher the value is, the brighter the picture will be, and vice versa. The picture might be hazy if the value is configured too high.
Contrast	Changes the contrast of the picture. The higher the value is, the more the contrast will be between bright and dark areas, and the smaller the less. If the value is set too high, the dark area would be too dark, and the bright area would be easier to get overexposed. The picture might be hazy if the value is set too small.
Saturation	Makes the color deeper or lighter. The higher the value is, the deeper the color will be, and the lower the lighter. Saturation value does not change image brightness.
Sharpness	Changes the sharpness of picture edges. The higher the value is, the clearer the picture edges will be, and if the value is set too high, picture noises are more likely to appear.

Table 3-18 Description of image adjustment parameters

Exposure Settings

You can configure the exposure parameters as needed.

Step 1 Navigate to **Settings** > **Image Settings** > **Image** > **Exposure Settings**.

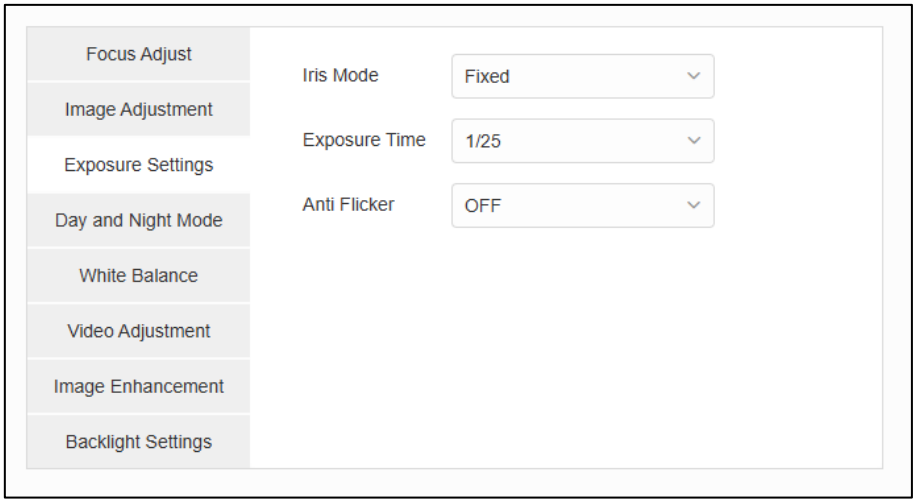

Figure 3-42 Exposure settings

Step 2 Configure the exposure setting parameters as needed.

Parameter	Description
Iris Mode	The iris value is set to a fixed value, and the device adjusts the shutter value then. If the image brightness is not enough and the shutter value has reached the upper or lower limit, the system adjusts the gain value automatically to ensure the image is at an ideal brightness.
Exposure Time	The camera electronic shutter time. Different exposure times can be set according to different camera scenes. If you use the manual aperture lens mode, the time set here is the longest exposure time; the camera will automatically adjust the exposure time according to the scene brightness.
Anti Flicker	Default off. When the image flickers in the indoor scene, the user can choose to enable it according to the actual scene, and set the level according to the actual environment.

Table 3-19 Description of exposure settings

Day and Night Mode

You can configure the day and night mode parameters as needed.

Step 1 Navigate to **Settings** > **Image Settings** > **Image** > **Day and Night Mode**.

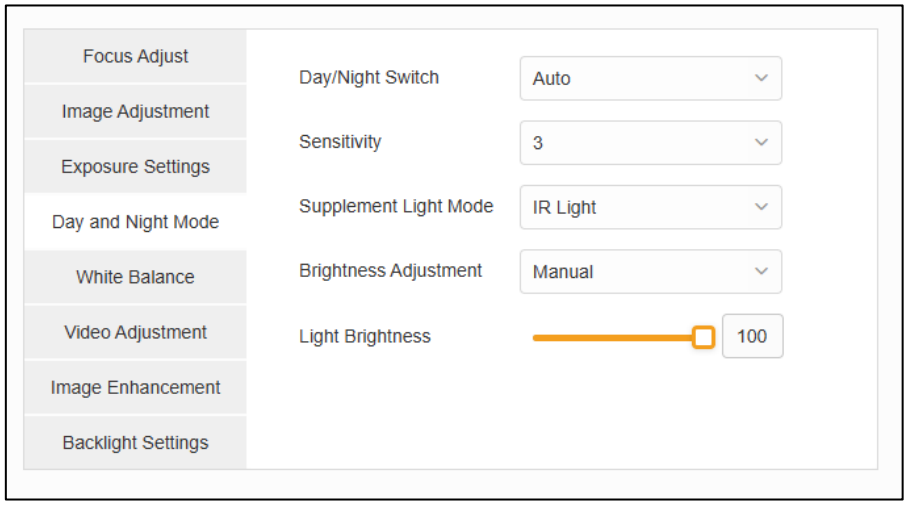

Figure 3-43 Day and Night Mode

Step 2 Configure the day and night mode parameters as needed.

Parameter	Description
Mode	You can select **Day/Night Switch** from **Auto**, **Day**, **Night**, and **Scheduled-Switch**. • **Day:** Displays images in full color for clear viewing under sufficient lighting conditions. • **Night:** Displays images in black and white to enhance visibility in low-light environments. • **Auto:** Automatically switches between day and night modes based on the surrounding ambient light levels. • **Scheduled-Switch:** Allows you to define the Start Time and End Time for daytime operation. Within the set time period, the camera operates in **Day** mode; outside this period, it automatically switches to **Night** mode.
Sensitivity	This configuration is available only when you set Auto in Mode. The higher the sensitivity, the easier it is to switch to day mode and the more difficult it is to switch to night mode; the lower the sensitivity, the easier it is to switch to night mode and the more difficult it is to switch to day mode.
Supplement Light Mode	You can select **IR Light**, **White light**, and **Intelligent**, depending on the device, light mode options will vary.
Brightness Adjustment	You can select **Auto** or **Manual**: • **Auto:** The device will adjust the light brightness automatically according to the scene environment. • **Manual:** Set the light brightness manually according to the required light intensity of the scene.
Light Brightness	Adjust the light brightness by dragging the progress bar according to the actual environment. The value ranges from 0 to 100.

Table 3-20 Description of day and night parameters

White Balance

You can configure the white balance parameters as needed.

Step 1 Navigate to **Settings** > **Image Settings** > **Image** > **White Balance**.

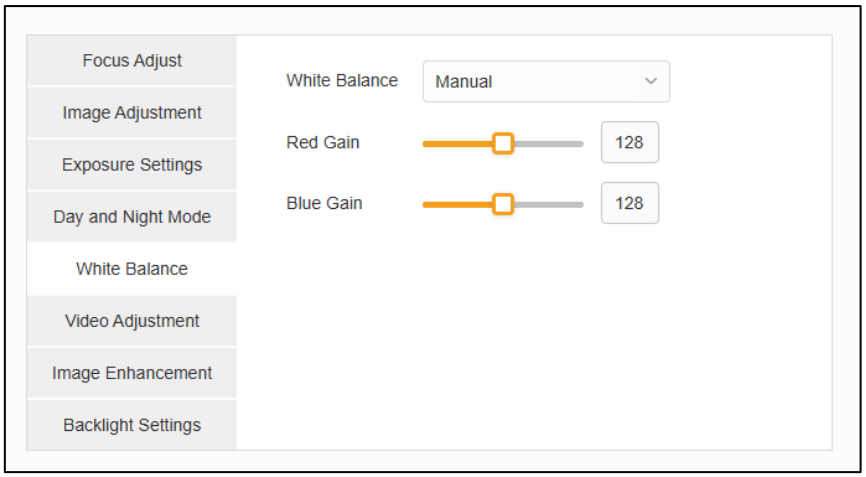

Figure 3-44 White balance

Step 2 Select the appropriate White balance according to the requirement.

- **Auto White Balance 1 (AWB1):** Automatically adjusts white balance under standard lighting conditions with a normal adjustment range.
- **Auto White Balance 2 (AWB2):** Automatically adjusts white balance with a wider adjustment range, making it suitable for more complex or varied lighting environments.
- **Manual White Balance:** Allows manual adjustment of **Red Gain** and **Blue Gain** values to achieve precise color balance as required. Drag the progress bar to adjust the **Red Gain** and **Blue Gain** as per the requirement. The value ranges from 0 to 255. The default value is 128.

Video Adjustment

You can configure the video adjustment parameters as needed, including mirror, flip, and video format.

Step 1 Navigate to **Settings** > **Image Settings** > **Image** > **Video Adjustment**.

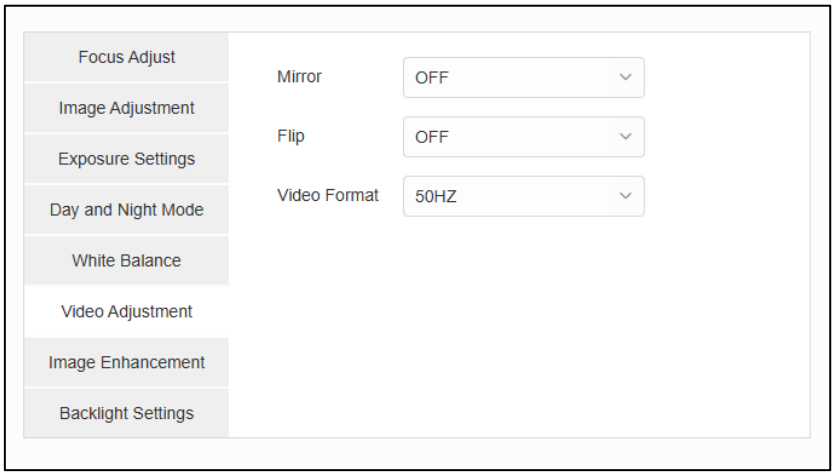

Figure 3-45 Video Adjustment

Step 2 Configure the video adjustment parameters.

Parameter	Description
Mirror	Select **OFF**, **Horizontal**, **Vertical**, or **Vertical and Horizontal** to flip the image orientation as required by the installation.
Flip	Select **OFF**, **90°**, **180°**, or **270°** to flip the image orientation as per the requirement.
Video Format	You can select from 50HZ and 60HZ. • **50HZ:** When the electric supply is 50HZ, the system adjusts the exposure according to ambient light automatically to ensure that there is no stripe appears. • **60HZ:** When the electric supply is 60HZ, the system adjusts the exposure according to ambient light automatically to ensure that there is no stripe appears.

Table 3-21 Description of video adjustment parameters

Image Enhancement

You can configure the image enhancement parameters, including WDR and Digital Noise Reduction.

Step 1 Navigate to **Settings** > **Image Settings** > **Image** > **Image Enhancement**.

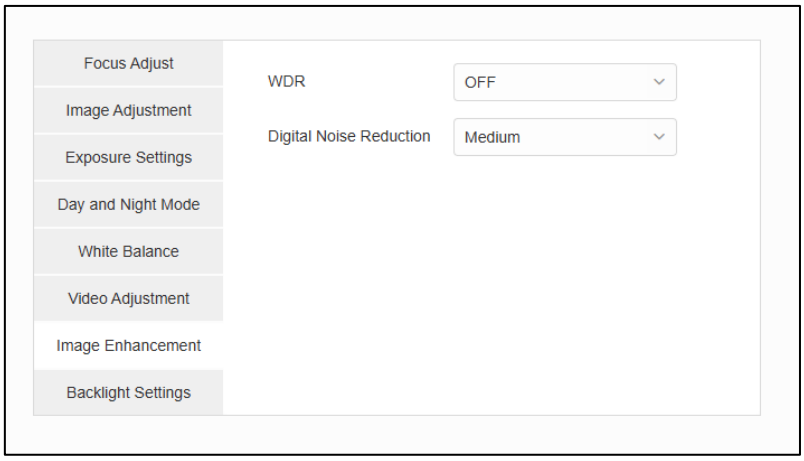

Figure 3-46 Image Enhancement

Step 2 Configure the image enhancement parameters.

Parameter	Description
WDR (Wide Dynamic Range)	Allows the camera to operate in wide dynamic mode to balance bright and dark areas in the scene. The WDR level can be set to **OFF**, **Low**, **Medium**, or **High**, allowing users to adjust the intensity based on actual lighting conditions.
Digital Noise Reduction	Applies advanced 3D digital noise reduction technology to reduce image noise and enhance image clarity. The noise reduction level can be configured to **OFF**, **Low**, **Medium**, or **High**, enabling users to control the strength of noise reduction as required.

Table 3-22 Description of image enhancement parameters

Backlight Settings

You can configure the backlight setting parameter as needed, including HLC and BLC.

Step 1 Navigate to **Settings** > **Image Settings** > **Image** > **Backlight Settings**.

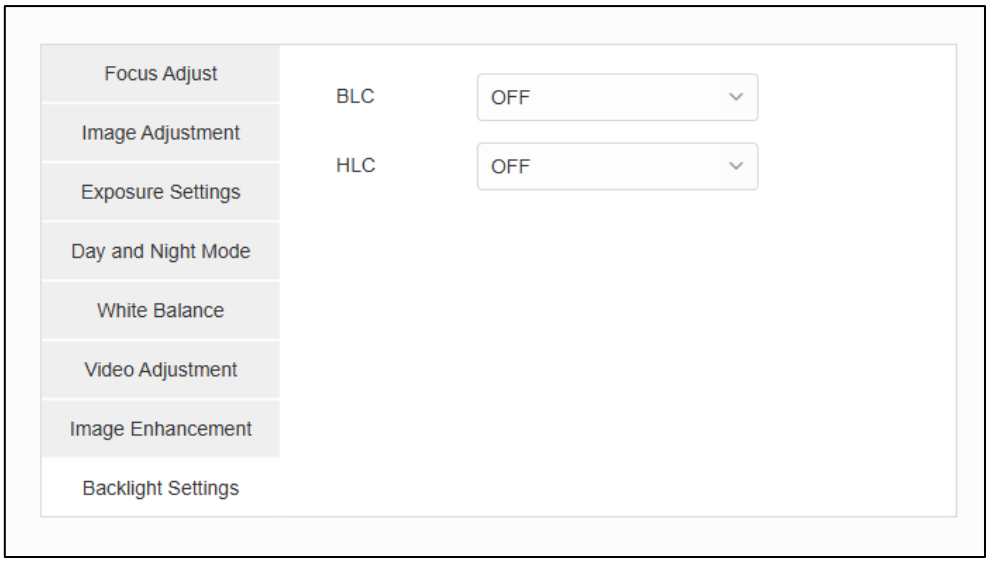

Figure 3-47 Backlight Settings

Step 2 Configure the backlight setting parameters.

Parameter	Description
BLC (Backlight Compensation)	Improves visibility of subjects when there is strong light behind them by adjusting overall exposure. The available options are ON, OFF, Left, Right, Up, Down, and Medium.
HLC (Highlight Compensation)	Suppresses extremely bright light sources (such as headlights or spotlights) to prevent overexposure and glare. The available options are ON and OFF. When enabling HLC, you can configure **Stronglight Suppression Intensity** and **Dark Area Boost Strength** by dragging the progress bar as per the requirement. The value ranges from 0 to 255.

Table 3-23 Description of backlight setting parameters

3.6.5.2 OSD

OSD refers to the information displayed on the monitor screen, which can display device name, date, day of the week, channel information and superimposed characters.

You can check the OSD information you want to display, and then you can set the OSD on the live screen to the position you want to display (top left, bottom left). You can also modify the format of the OSD text, time and date displayed on the preview screen.

Step 1 Navigate to **Settings** > **Image Settings** > **OSD**.

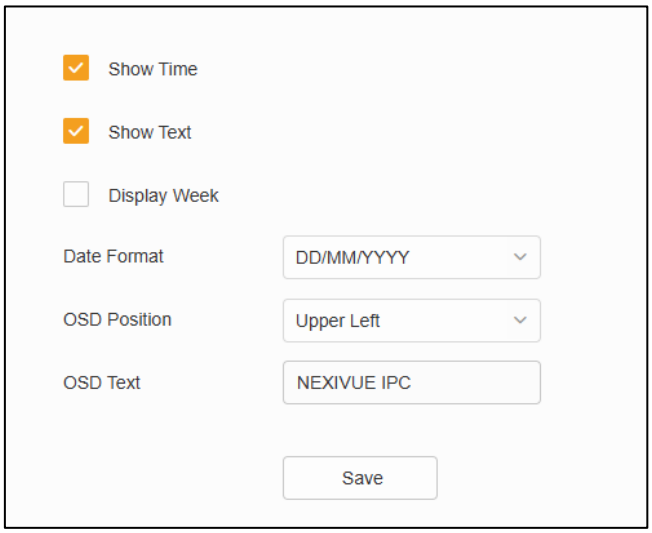

Figure 3-48 OSD

Step 2 Configure OSD parameters as per requirements.

Parameter	Description
Show Time	Enable or disable the display of the current date and time on the video.
Show Text	Enable or disable the display of custom text on the video (such as device name or location).
Display Week	Displays the day of the week along with the date when enabled.
Date Format	Set the format of the displayed date. Options include **DD/MM/YYYY**, **MM/DD/YYYY**, and **YYYY/MM/DD**.
OSD Position	Select the position of the OSD on the video. Options include **Upper Left** and **Lower Left**.
OSD Text	Allows you to enter custom text (for example, device name or site name) to be shown on the video.

Table 3-24 Description of OSD parameters

3.6.6 Event

This section introduces intelligent event settings, including motion detection, privacy masking, video tampering, alarm input, alarm output, abnormality, intrusion detection, line crossing detection, people gathering detection, and loitering detection.

3.6.6.1 Detect

This part allows you to configure intelligent event detection features, enabling the camera to identify specific activities and trigger alerts or actions based on defined conditions.

Motion Detection

The motion detection function is often used for unattended surveillance recordings and automatic alarms.

Step 1 Navigate to **Settings** > **Event** > **Detect > Motion Detection.**

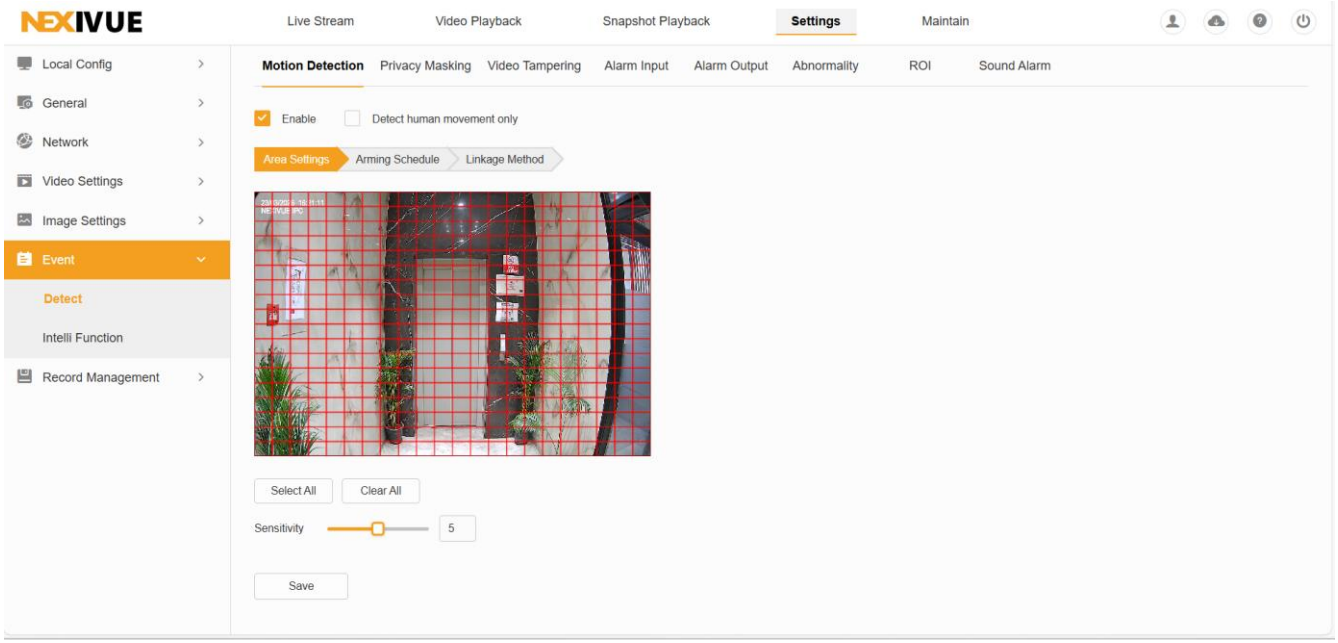

Figure 3-49 Motion detection

Step 2 Select the **Enable** checkbox to enable motion detection.

Step 3 (Optional) Enable **Detect human movement only** to reduce false alarms caused by non-human motion.

Step 4 Select the area and set the sensitivity of motion detection.

- Set the area for motion detection.
  - Move the mouse to the live screen, click the left mouse button to select the area range of motion detection, release the left mouse button to complete the area drawing.
  - Click **Select All** to select the complete area.
  - Click **Clear All** to clear all areas of the drawing.

- Adjust the **Sensitivity** level based on the environment and detection needs by dragging the progress bar. The default value is 5, and the switchable range is 0-10. The larger the value, the easier it is to trigger the alarm.
- Click **Save** to save the configured settings.

Step 5 Set arming schedule.

Figure 3-50 Arming schedule

Alarms will be triggered in the time period in green on the timeline.

- **Method 1:** Click on the time period for arming, two arrows will be displayed at both ends of the time period, move the adjustment arrows left and right to adjust the arming time.
- **Method 2:** Click the arming time, fill in the start time and end time manually, and click **Save** after setting. If you need to delete the time period, click **Delete** button to reset the time period. Click **All day** to apply motion detection for the entire 24-hour period.
- Click **Select All** to apply the schedule to all days.
- Click **Delete All** to clear all configured schedules.

- Multiple time periods can be set on the timeline of the same day, supporting up to 8 time periods.
- After setting the arming time for one day, if other times need to be set to the same arming time, click the button on the right side of the timeline, check **Select All** or a certain day, and then click **OK**.
- When the arming time is set, there can be no overlapping time between any two time periods.

- Click **Save** to save the configured settings.

Step 6 Set the linkage method.

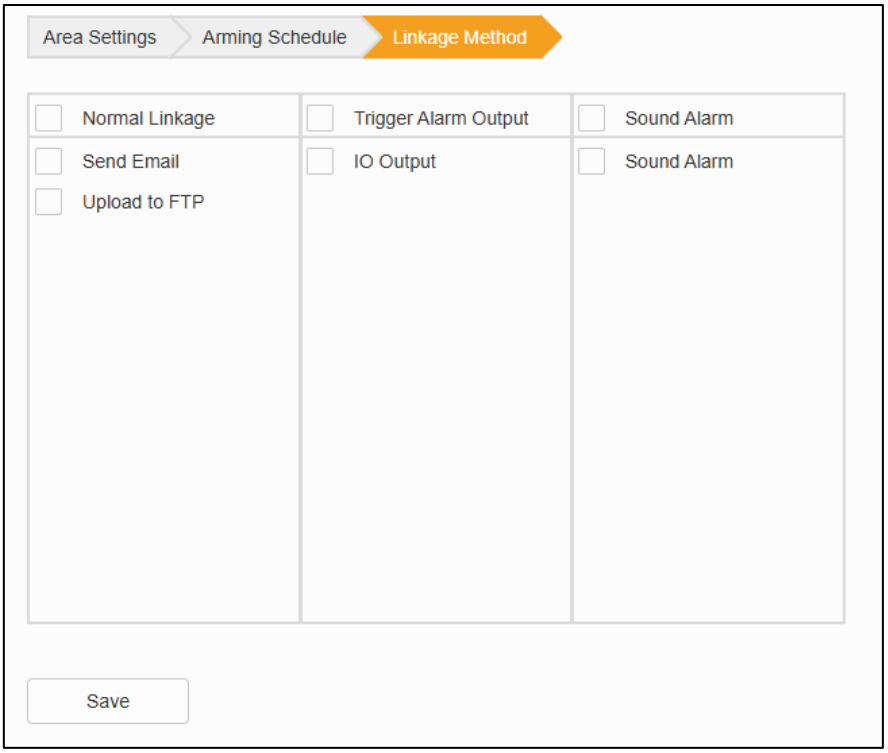

Figure 3-51 Linkage method

- Choose one or more linkage options based on how you want the system to respond when motion is detected.
- Multiple actions can be enabled at the same time.

Parameter	Description
Normal Linkage	Triggers standard event linkage actions, such as recording or snapshot, based on system configuration. • **Send Email:** Sends alarm notification and event information to the configured SMTP email recipient when motion is detected. • **Upload to FTP:** Uploads alarm data (such as snapshots or recordings) to the configured FTP server when an alarm occurs.
Trigger Alarm Output	Activate an external alarm device connected to the system when motion is detected. • **IO Output:** Sends an alarm signal through the IO output port to trigger connected alarm equipment.
Sound Alarm	Play a warning sound or audio alert through the device's built-in speaker when an alarm is triggered.

Table 3-25 Description of linkage method parameters

- Click **Save** to save the configured settings.

Privacy Masking

Privacy masking is a privacy protection function that is used to cover the privacy area of the monitoring screen, so that it cannot be seen in real-time video and video recording.

Step 1 Navigate to **Settings** > **Event** > **Detect** > **Privacy Masking**.

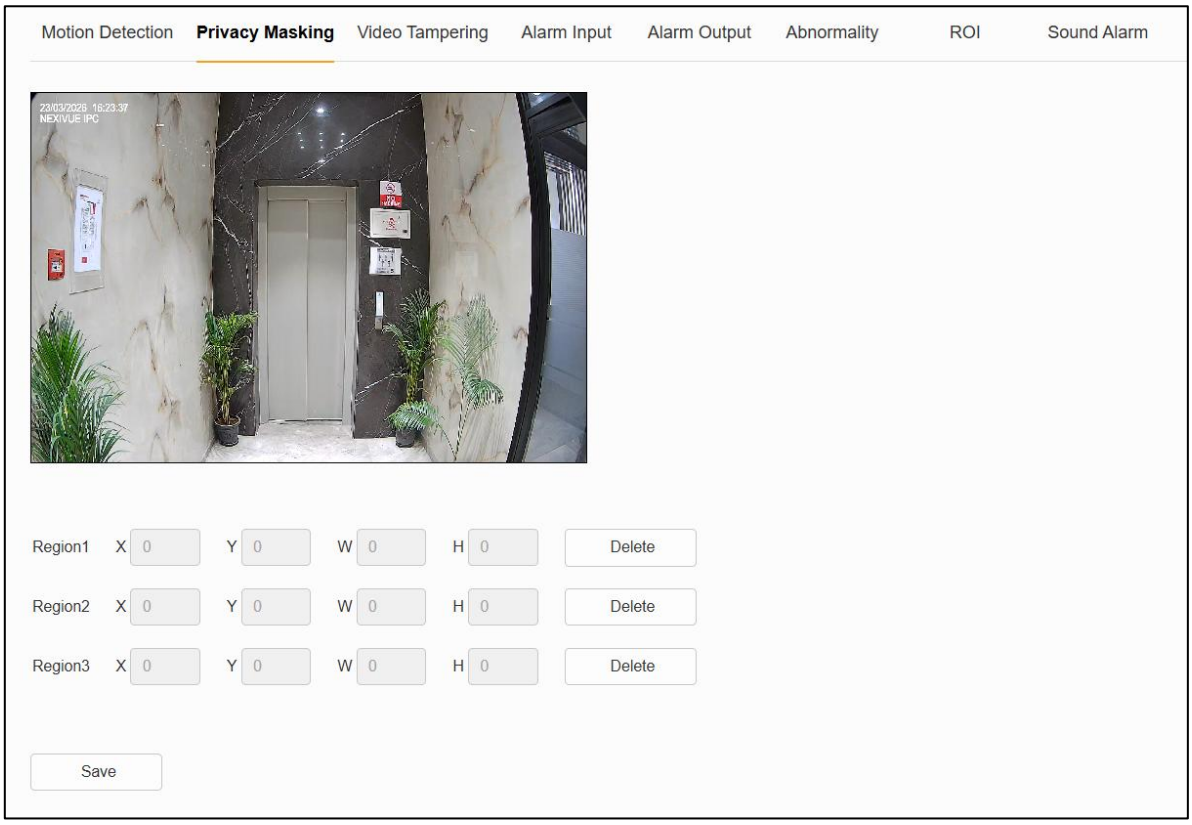

Figure 3-52 Privacy masking

Step 2 Hold the left mouse button and drag it to select the area.

- Region1, Region2, and Region3 will display the corresponding coordinates (X, Y), width (W) and height (H) of the area below.
- You can choose up to three blocking areas here.

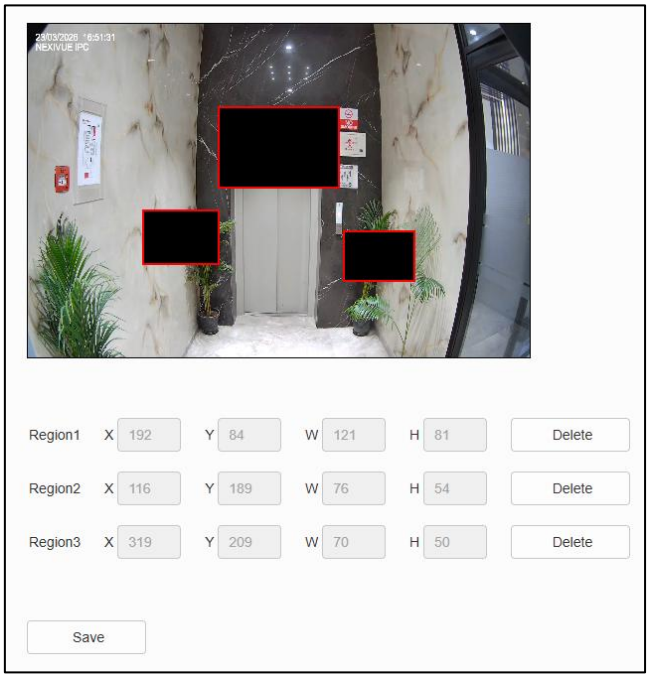

Figure 3-53 Privacy masking regions

Step 3 Click **Delete** to delete the blocking area.

Step 4 Click **Save** after completing the settings.

Video Tampering

Video tampering occurs when the defined monitoring area is obstructed by a person or other objects, preventing normal video monitoring. When a video tampering event is detected, users can promptly identify the cause and take necessary action to restore the monitoring view.

Step 1 Navigate **Settings** > **Event** > **Detect** > **Video Tampering**.

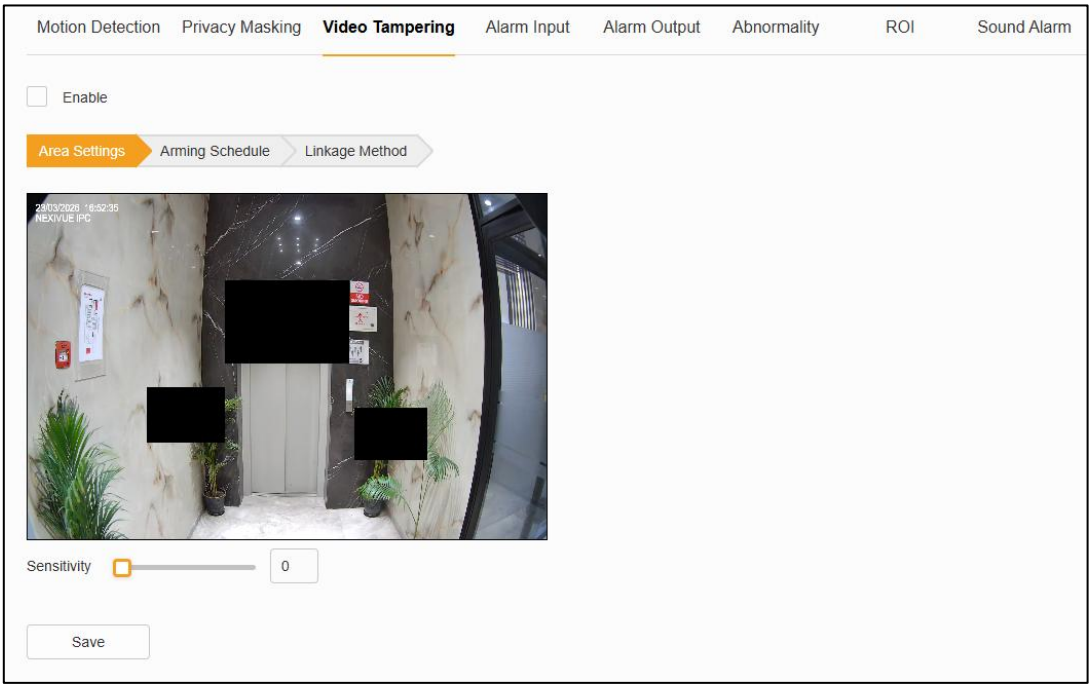

Figure 3-54 Video tampering

Step 2 Select **Enable** to turn on the video tampering.

Step 3 Select the area, set the sensitivity of the video tampering, and click **Save** to complete the setting.

Step 4 Set the arming time (For details, please refer to the motion detection arming schedule setting).

Step 5 Set the linkage mode. (For details, please refer to the motion detection linkage method setting).

Step 6 Click **Save** to save the configured settings.

Alarm Input

Prerequisites:

- IPC supports alarm input. For details, please refer to the actual device.
- Before configuration, the device needs to be connected to the alarm input device.
- By configuring the alarm input, the alarm signal received by the alarm input device can be transmitted to the IPC for further processing.

Step 1 Navigate **Settings** > **Event** > **Detect** > **Alarm Input**.

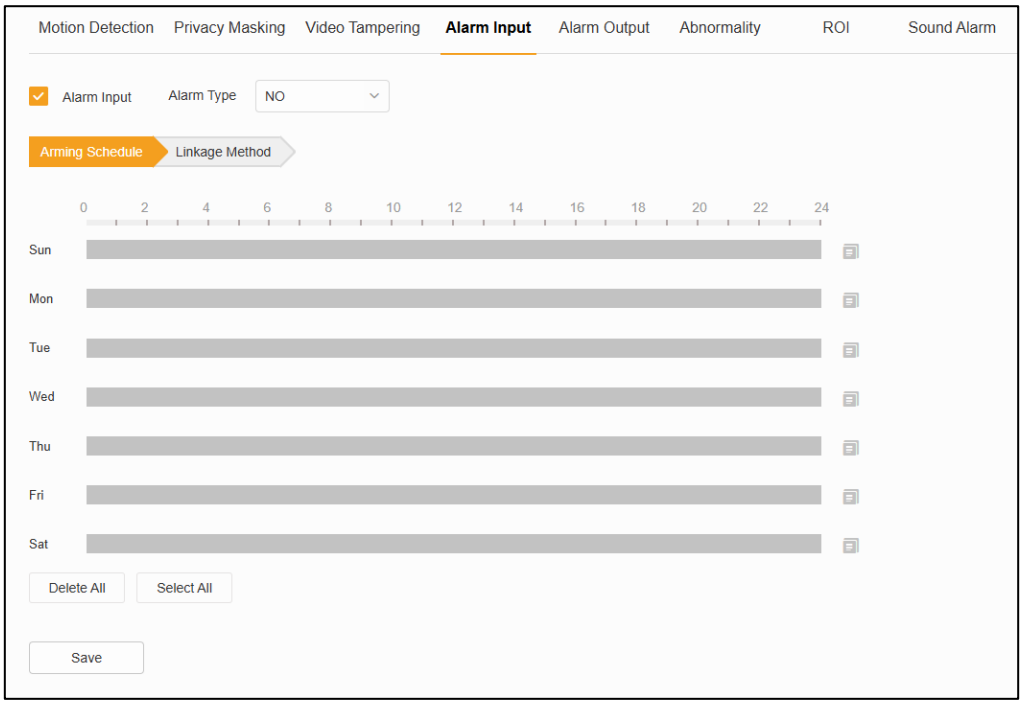

Figure 3-55 Alarm Input

Step 2 Check **Alarm Input** checkbox and select the **Alarm Type**: Normally Open (**NO**), Normally Closed (**NC**).

Step 3 Set the arming time (For details, please refer to the motion detection arming schedule setting).

Step 4 Set the linkage mode settings. (For details, please refer to the motion detection linkage method setting).

Step 5 Click **Save** to save the configured settings.

Alarm Output

Prerequisites: Before configuration, the device needs to be connected to the alarm output device, and by configuring the alarm output, the alarm signal of the IPC can be passed to the alarm output device.

Step 1 Navigate **Settings** > **Event** > **Detect** > **Alarm Output**.

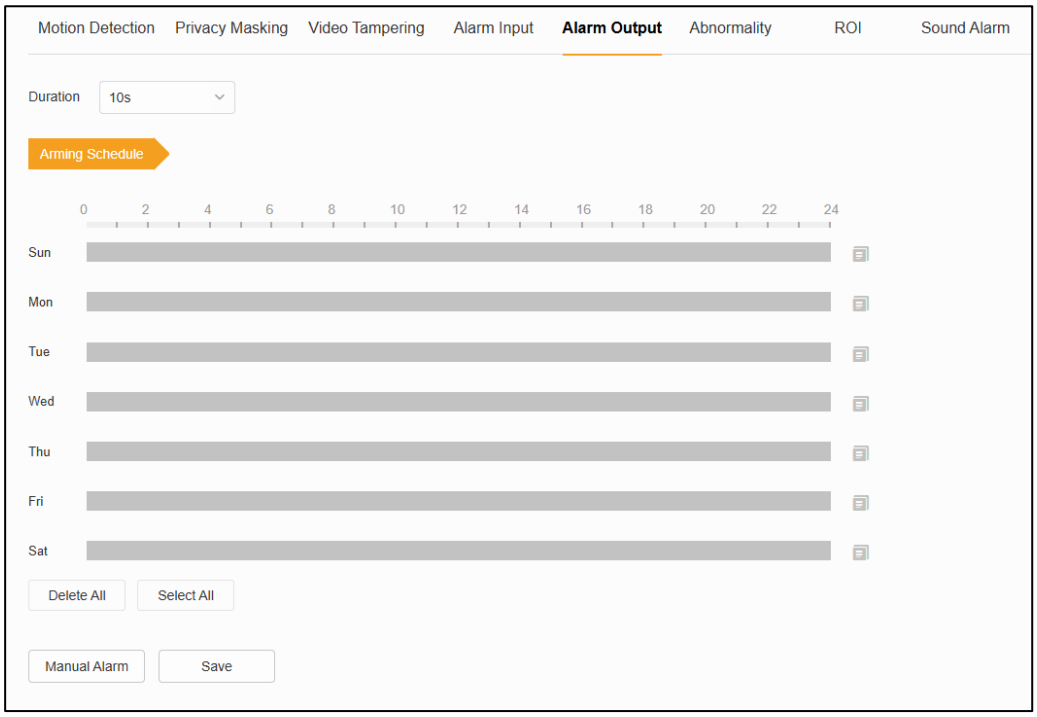

Figure 3-56 Alarm Output

Step 2 Set the alarm duration.

Step 3 Set the arming time (For details, please refer to the motion detection arming schedule setting).

- **Manual Alarm**: Manually control the alarm output device on the alarm output interface to link the alarm.

Step 4 Click **Save** to save the configured settings.

Abnormality

This section allows you to configure system actions when abnormal events occur, such as network disconnection, IP address conflict, or SD card issues. By setting exception types and corresponding responses, the device can promptly notify users or trigger alarms to ensure system reliability.

Step 1 Navigate **Settings** > **Event** > **Detect** > **Abnormality**.

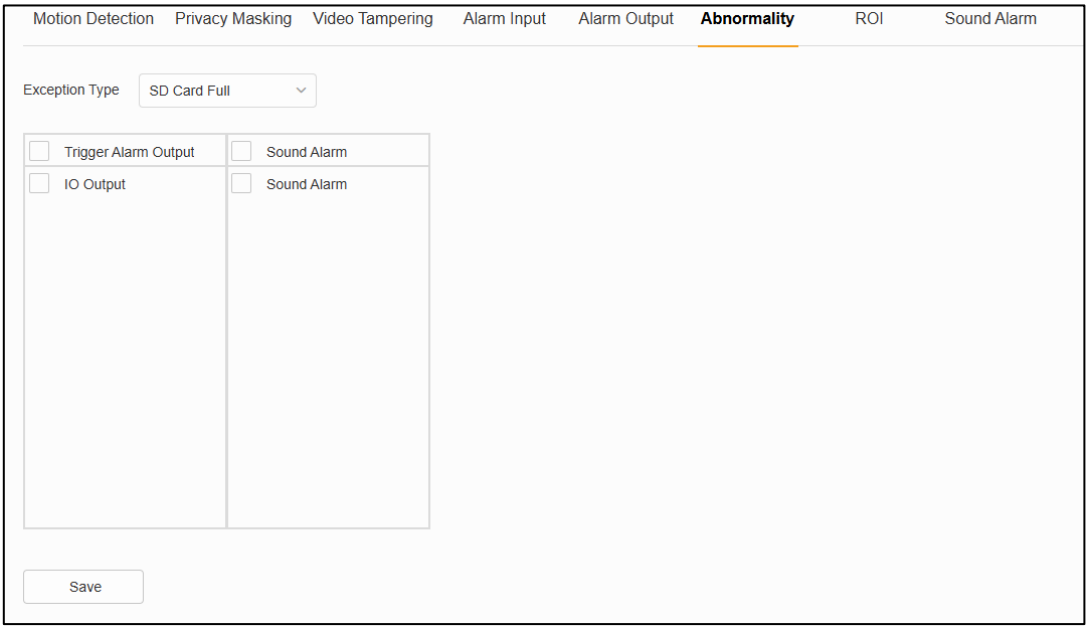

Figure 3-57 Abnormality

Step 2 From the **Exception Type** drop-down list, select the required abnormal event:

- **Network Disconnected**
- **IP Address Conflicted**
- **SD Card Full**

Step 3 Enable the required response options based on your needs.

Option	Description
Trigger Alarm Output	Activates an external alarm device connected to the system when motion is detected. • **IO Output:** Sends an alarm signal through the IO output port to trigger connected alarm equipment.
Sound Alarm	Plays a warning sound or audio alert through the device's built-in speaker when an alarm is triggered.

Table 3-26 Description of abnormality response options

Step 4 Click **Save** to save the configured settings.

ROI

ROI means region of interest setting. The user can use this function to set the most concerned and most interesting area on the video screen. IPC will improve the video image quality of the corresponding area when encoding the video, and reduce the encoding quality of other areas, so as to highlight the Image effect in the selected area.

- Some IP cameras support different configurations; please refer to the actual interface.

Step 1 Navigate **Settings** > **Event** > **Detect** > **ROI**.

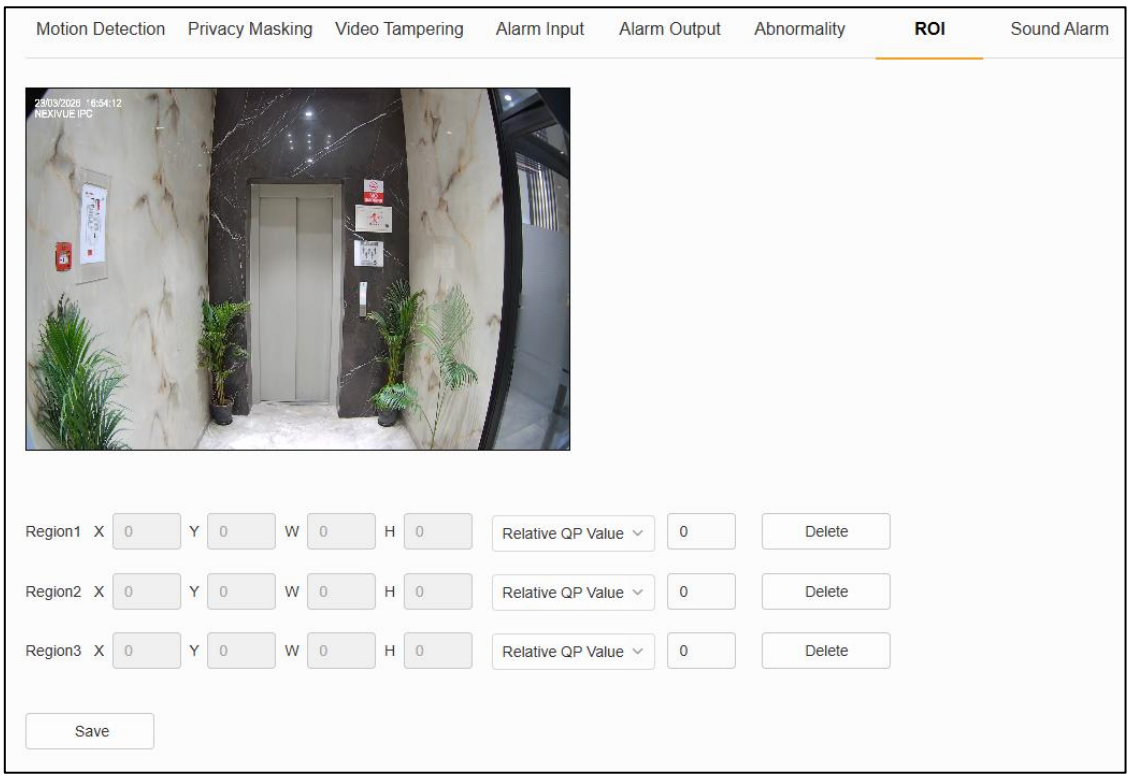

Figure 3-58 ROI

Step 2 Move the mouse to the live screen, press and hold the left mouse button to select the area range of ROI, and release the left mouse button to finish drawing the area. After the drawing is complete, the X, Y, W, H values corresponding to the area position are displayed below.

Step 3 Select **Relative QP Value** or **Absolute QP Value** in the corresponding area and enter the corresponding value.

Step 4 Click **Delete** to delete the selected region of interest.

Step 5 Click **Save** to complete the ROI settings.

Sound Alarm

After configuring the sound alarm, when the event is triggered, the speaker on the device can be linked to alarm.

- Some IP cameras support different configurations; please refer to the actual interface.

Step 1 Navigate **Settings** > **Event** > **Detect** > **Sound Alarm**.

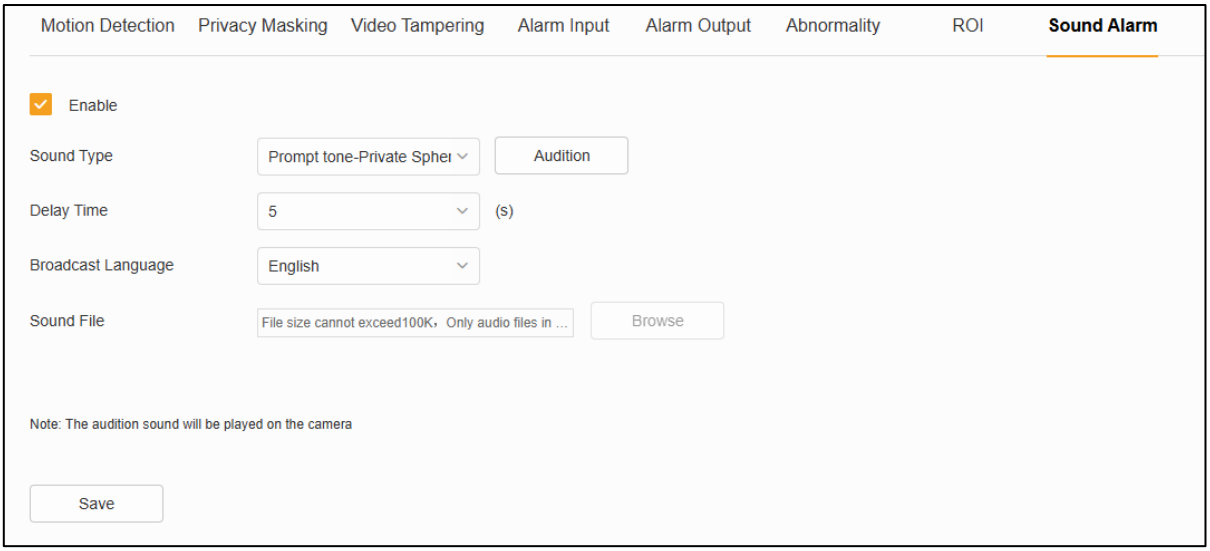

Figure 3-59 Sound Alarm

Step 2 Click **Enable** to turn on the sound alarm.

Step 3 Configure the sound alarm parameters.

Parameter	Description
Sound Type	Selects the type of alarm sound to be played.
Audition	Plays the selected sound through the camera speaker for preview before saving the configuration.
Delay Time (s)	Sets the delay time (in seconds) before the sound alarm is triggered after an alarm event occurs.
Broadcast Language	Selects the language used for the voice broadcast or prompt tone.
Sound File	Allows uploading a custom audio file for the sound alarm. Only audio files are supported, and the file size must not exceed 100 KB.

Table 3-27 Description of sound alarm parameters

Step 4 Click **Save** to save the configured settings.

3.6.6.2 Intelli Function

The Intelli Function enables intelligent video analytics to accurately detect specific behaviors such as intrusion, line crossing, loitering, and people gathering. By classifying targets (human or vehicle) and defining detection areas, it helps reduce false alarms and improves event accuracy.

Intrusion Detection

Intrusion detection is used to detect whether someone enters in the video setting area, and the alarm will be linked according to the judgment result.

Step 1 Navigate **Settings** > **Event** > **Intelli Function** > **Intrusion Detection**.

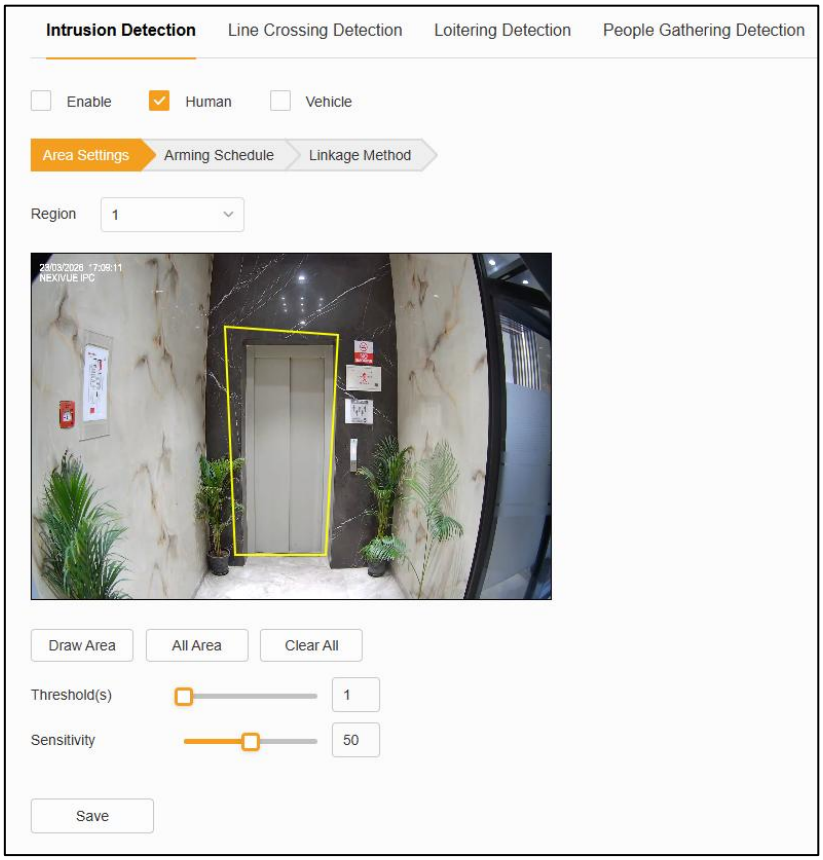

Figure 3-60 Intrusion detection

Step 2 Check **Enable** to enable the intrusion detection function.

Step 3 Select the target type:

- Human
- Vehicle
- Or both, based on monitoring requirements.

Step 4 Select the **Region**. The system supports setting up to 4 warning regions. After selecting a warning region, you need to make the following settings. After setting, please click **Save** below.

Parameter	Description
Draw Area	Click **Draw Area**, then move the mouse to the live view. Use the left mouse button to draw the endpoints of the quadrilateral warning region. Click anywhere on the preview screen to complete the area drawing. Click **Stop Drawing** to exit drawing mode.
Clear All	Clears all previously drawn intrusion detection areas from the screen.
All Area	Selects the entire camera view as the intrusion detection area.
Threshold (s)	Defines the minimum time the target must stay inside the warning area before an alarm is triggered. For example, if set to **5 seconds**, the alarm is generated only after the target remains in the area for 5 seconds. The default value is 1. Its value ranges from 0 to 10.
Sensitivity	Sets the sensitivity of detecting wandering; the default is **50**. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The larger the sensitivity, the easier it is to trigger the alarm.

Table 3-28 Description of intrusion detection parameters

Step 5 Set the arming time (For details, please refer to the motion detection arming time setting).

Step 6 Set the linkage method (For details, please refer to the motion detection linkage method setting).

Step 7 Click **Save** to save the configured settings.

Line Crossing Detection

Line cross detection is used to detect whether there is an object in the video crossing the set warning surface, and link the alarm according to the judgment result.

Step 1 Navigate **Settings** > **Event** > **Intelli Function** > **Line Crossing Detection**.

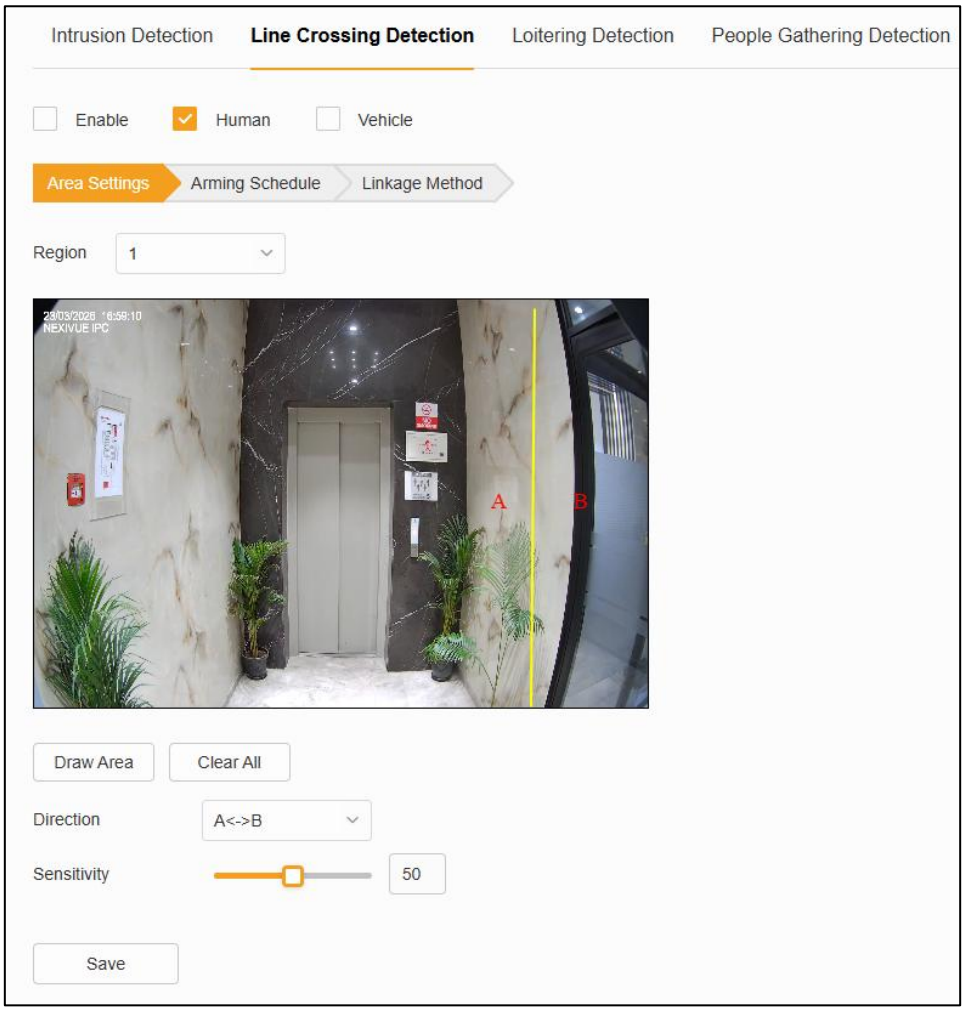

Figure 3-61 Line crossing detection

Step 2 Check **Enable** to enable the line crossing function.

Step 3 Select the target type:

- Human
- Vehicle
- Or both, based on monitoring requirements.

Step 4 Select the **Region**. The system supports setting up to 4 warning regions. After selecting a warning region, you need to make the following settings. After setting up, please click **Save** below.

Parameter	Description
Draw Area	Click **Draw Area** to display a line segment with arrows on the screen. Click and drag either endpoint to adjust the length of the line, or drag the entire line to reposition it. This completes the drawing of the line-crossing warning area.
Clear All	Clears all previously drawn warning areas from the screen.
Direction	Defines the direction that triggers an alarm when an object crosses the line. Available options are **A↔B**, **A→B**, and **B→A**. Selecting **A→B** triggers an alarm when an object crosses from A to B, while **B→A** triggers an alarm when crossing from B to A.
Sensitivity	Sets the sensitivity level for line-crossing detection. The default value is **50**. The value ranges from **0** to **100**. Adjust using the slider or by entering a value directly. Higher sensitivity increases the likelihood of alarm triggering.

Table 3-29 Description of line crossing detection parameters

Step 5 Set the arming time (For details, please refer to the motion detection arming time setting).

Step 6 Set the linkage method (For details, please refer to the motion detection linkage method setting).

Step 7 Click **Save** to save the configured settings.

Loitering Detection

Loitering detection is used to detect the target staying in the set area for more than the set time threshold, and then trigger a linkage alarm according to the judgment result.

Step 1 Navigate **Settings** > **Event** > **Intelli Function** > **Loitering Detection**.

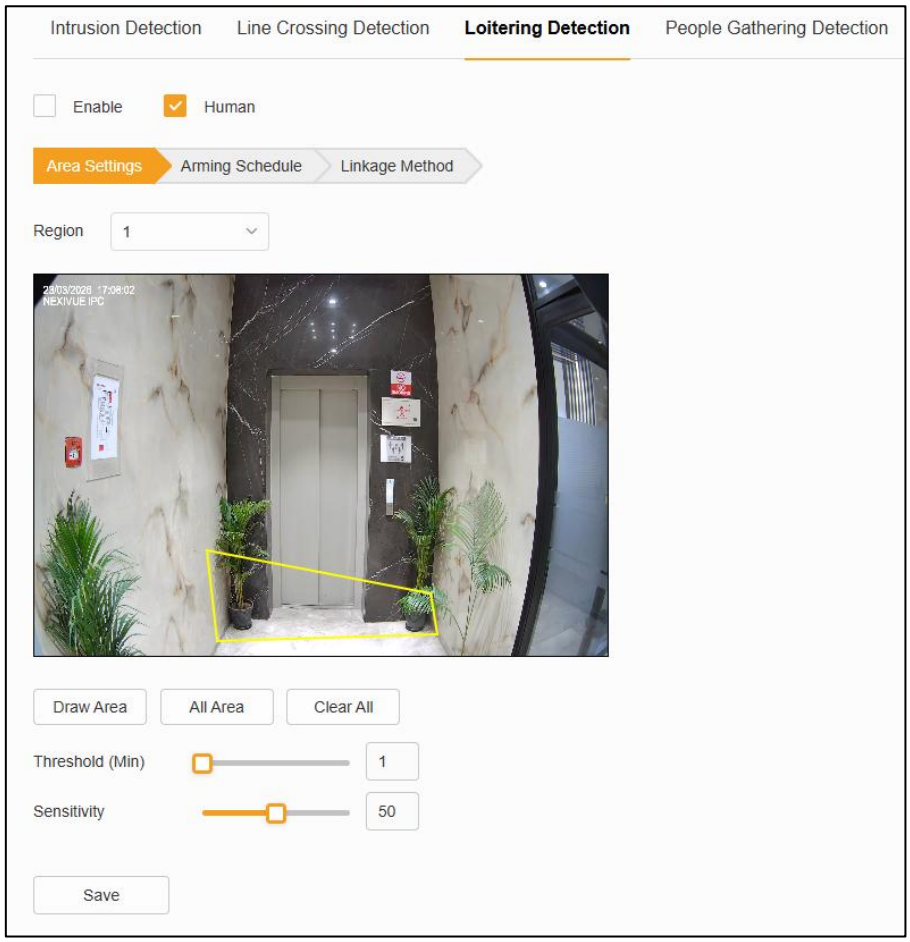

Figure 3-62 Loitering detection

Step 2 Check **Enable** to enable the loitering detection function.

Step 3 Select the target type:

- Human
- Vehicle
- Or both, based on monitoring requirements.

Step 4 Select the **Region**. The system supports setting up to 4 warning regions. After selecting a warning region, you need to make the following settings. After setting, please click **Save** below.

Parameter	Description
Draw Area	Click **Draw Area**, then move the mouse to the live view. Use the left mouse button to draw the endpoints of the quadrilateral warning region. Click anywhere on the preview screen to complete the area drawing. Click **Stop Drawing** to exit drawing mode.
Clear All	Clears all previously drawn loitering detection areas from the screen.
All Area	Selects the entire camera view as the loitering detection area.
Threshold (min)	Means the target in the detection area, after the continuous movement for a certain time to generate an alarm, the larger the time threshold, the longer the continuous movement of the target in the detection area to trigger the alarm. The default value is 1. Its value ranges from 0 to 10.
Sensitivity	Sets the sensitivity level for loitering detection. The default value is **50**. You can drag the slider or enter a value directly. Higher sensitivity increases the likelihood of triggering an alarm.

Table 3-30 Description of loitering detection parameters

Step 5 Set the arming time (For details, please refer to the motion detection arming time setting).

Step 6 Set the linkage method (For details, please refer to the motion detection linkage method setting).

Step 7 Click **Save** to save the configured settings.

People Gathering Detection

People gathering detection is used to detect whether the density of people in the set area exceeds the set threshold value and then trigger a linkage alarm according to the judgment result.

- This intelligent event function depends on the model, please refer to the actual device.

Step 1 Navigate **Settings** > **Event** > **Intelli Function** > **People Gathering Detection**.

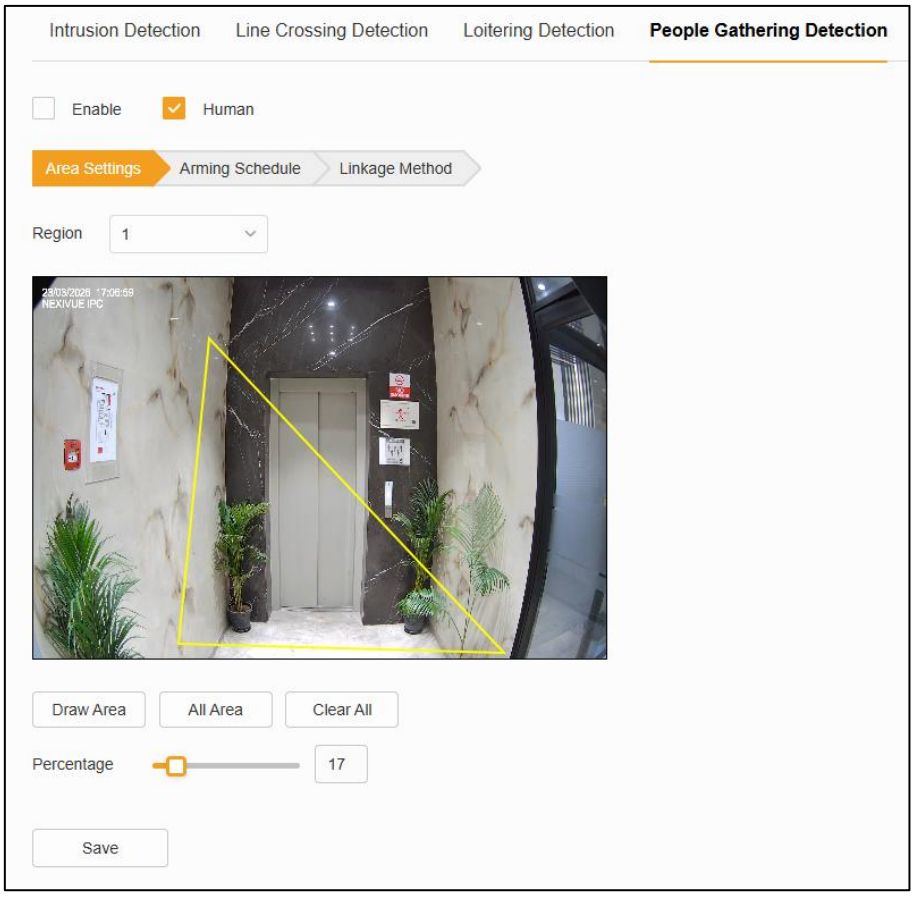

Figure 3-63 People gathering detection

Step 2 Check **Enable** to enable the people gathering function.

Step 3 Select the target type as Human.

Step 4 Select the **Region**. The system supports setting up to 4 warning regions. After selecting a warning region, you need to make the following settings. After setting, please click **Save** below.

Parameter	Description
Draw Area	Click **Draw Area**, then move the mouse to the live view. Use the left mouse button to draw the endpoints of the quadrilateral warning region. Click anywhere on the preview screen to complete the area drawing. Click **Stop Drawing** to exit drawing mode.
Clear All	Clears all previously drawn people gathering detection areas from the screen.
All Area	Selects the entire camera view as the people gathering detection area.
Percentage	It indicates the percentage of people in the whole warning region. When the occupancy percentage of people exceeds the set value, the system will generate an alarm. The default percentage is 50%. The larger the value, the more people can be accommodated in the warning area and the less likely to trigger an alarm.

Table 3-31 Description of people gathering parameters

Step 5 Set the arming time (For details, please refer to the motion detection arming time setting).

Step 6 Set the linkage method (For details, please refer to the motion detection linkage method setting).

Step 7 Click **Save** to save the configured settings.

3.6.7 Record Management

The Record Management section allows you to configure when and how the camera records video based on different events or continuous schedules. Users can define recording types, stream selection, and time periods to ensure important footage is captured efficiently while optimizing storage usage.

3.6.7.1 Schedule

This part allows users to define specific time periods for video recording and snapshots. By setting a customized weekly schedule, the camera can automatically record based on selected stream types and event conditions, ensuring efficient storage usage and continuous monitoring when required.

Steps to Configure Record Schedule

Step 1 Navigate to **Settings** > **Record Management** > **Schedule** > **Record Schedule**.

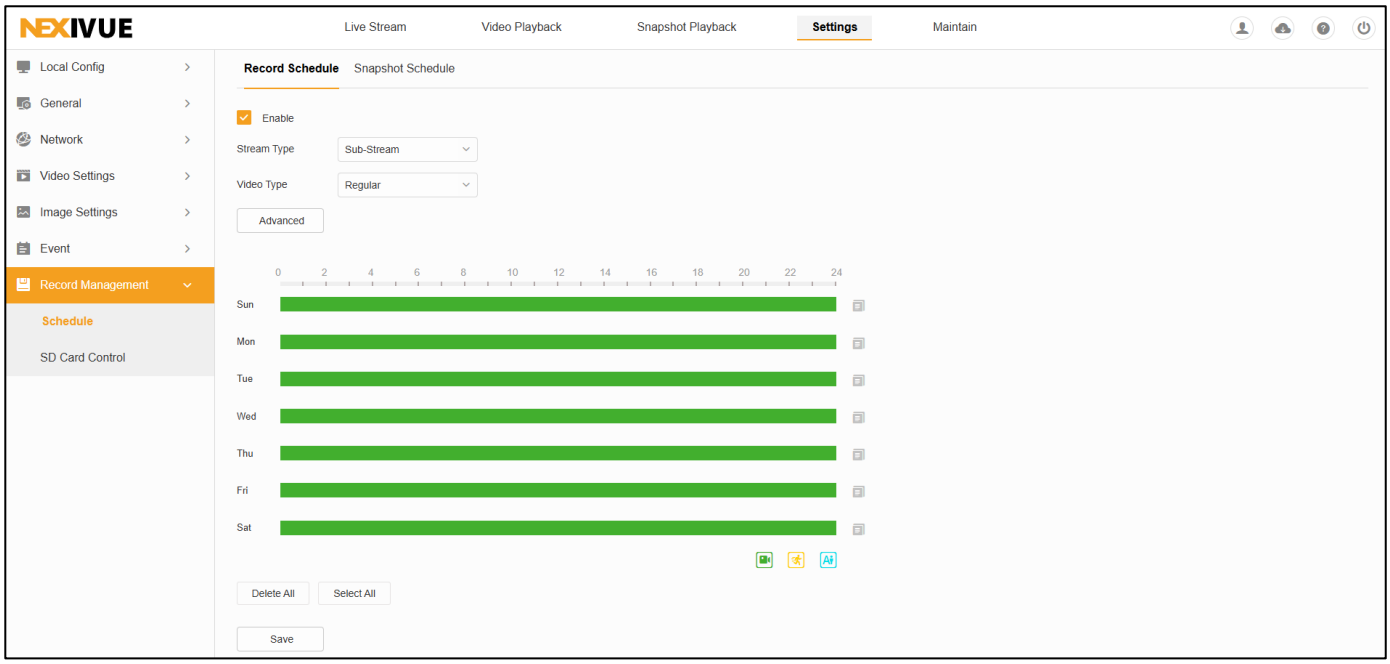

Figure 3-64 Record Schedule

Step 2 Check the **Enable** option to activate the recording schedule.

Step 3 Configure the required recording parameters.

Parameter	Description
Stream Type	Select the video stream type. • **Mainstream:** It has a large bit stream value and image with high resolution, but also requires a large bandwidth. This option can be used for storage and monitoring. • **Sub Stream:** It has a small bit stream value and a smooth image and requires less bandwidth. This option is normally used to replace mainstream when the bandwidth is not enough. • **Third Stream:** It has a very small bit stream value with basic image quality and requires minimal bandwidth.
Video Type	Select the recording mode. • **Regular** ( ): Records video continuously during the configured schedule, regardless of events or alarms. • **Motion Detection** ( ): Records video only when motion is detected in the configured detection area, helping reduce storage usage. • **External Alarm** ( ): Triggers recording when an external alarm input device (such as a sensor) is activated. • **Intelligent** ( ): Records video based on intelligent event detection, such as human or vehicle detection, improving accuracy and minimizing false alarms.
Advanced	Opens additional recording settings for fine-tuning parameters such as Pre-record, Post-record, or overwrite. • **Pre-record:** Indicates the pre-recording time before the video starts. **No Pre-record** means no pre-recording. The maximum pre-recording time is calculated at 2 Mbps bit rate. The higher the bit flow, the shorter the pre-recording time. There are 6 levels from **0s** to **30s** and unlimited. • **Post-record:** Indicates the video delay time, **5s** to **10mins** a total of 7 levels optional. • **Overwrite:** When the storage space is full, if **Overwrite** is checked, it will overwrite the earliest video file; if it is not checked, it will not be able to record after the storage space is full.

Table 3-32 Description of record schedule parameters

Step 4 Set the arming time for recording.

- **Method 1:** Click on the time period for arming, two arrows will be displayed at both ends of the time period, move the adjustment arrows left and right to adjust the arming time.
- **Method 2:** Click the arming time, fill in the start time and end time manually, and click **Save** after setting. If you need to delete the time period, click **Delete** button to reset the time period. Click **All day** to record the entire 24-hour period.
- Click **Select All** to apply the schedule to all days.
- Click **Delete All** to clear all configured schedules.

- Multiple time periods can be set on the timeline of the same day, supporting up to 8 time periods.
- After setting the arming time for one day, if other times need to be set to the same arming time, click the button on the right side of the timeline, check **Select All** or a certain day, and then click **OK**.
- When the arming time is set, there can be no overlapping time between any two time periods.

Step 5 Click **Save** to save the configured settings.

Steps to Configure Snapshot Schedule

Step 1 Navigate to **Settings** > **Record Management** > **Schedule** > **Snapshot Schedule**.

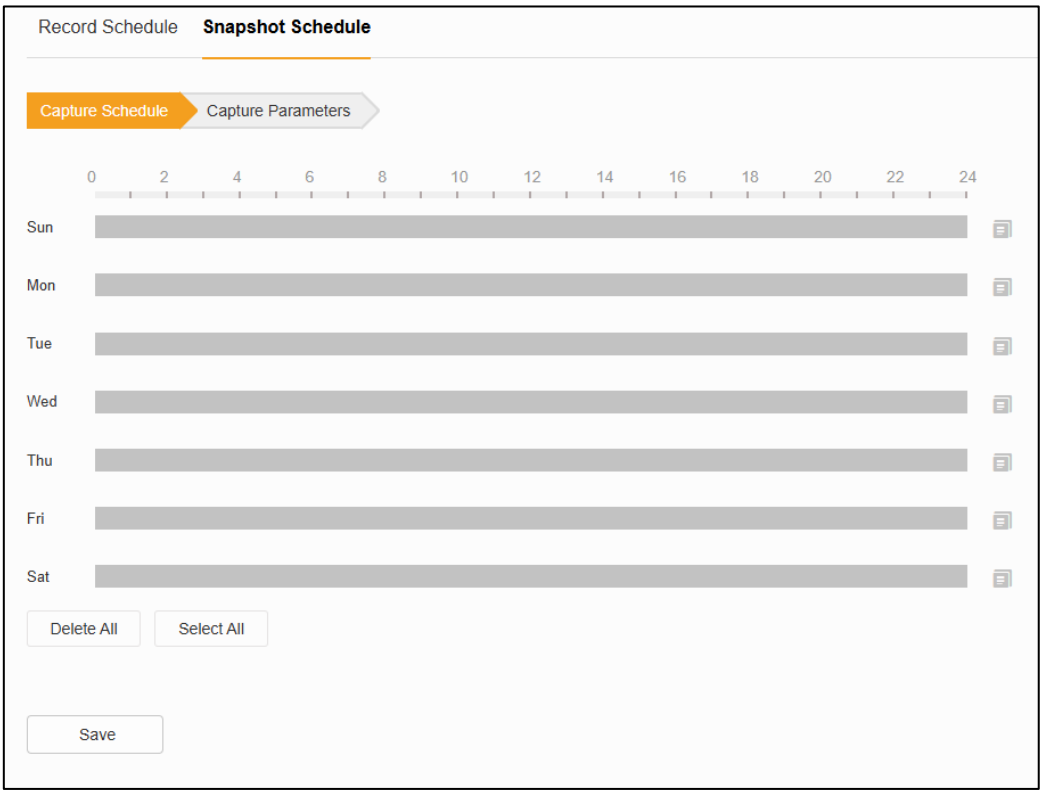

Figure 3-65 Snapshot Schedule

Step 2 Set the capture schedule (For details, please refer to Step 4 of **Record Schedule**).

Step 3 Click **Save** to save the configured settings.

Step 4 Configure the **Capture Parameters**.

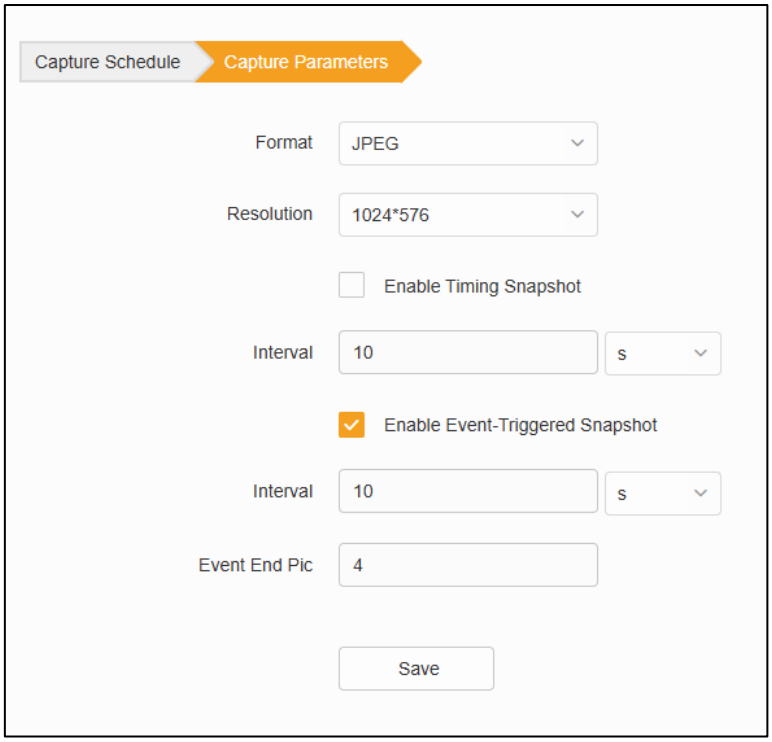

Figure 3-66 Capture parameters

Parameter	Description
Format	Defines the image format used for snapshots. Only **JPEG** format is supported.
Resolution	Select the resolution of the captured snapshot. Higher resolutions provide clearer images but consume more storage.
Enable Timing Snapshot	Enables periodic snapshot capture at fixed time intervals, regardless of events.
Interval (Timing Snapshot)	Sets the time gap between each timed snapshot. The value is configurable in seconds.
Enable Event-Triggered Snapshot	Enables snapshot capture when an event, such as motion detection or intelligent detection, occurs.
Interval (Event Snapshot)	Specifies the interval between consecutive snapshots during an active event.
Event and Pic	Sets the number of snapshots captured after the event ends, ensuring complete event coverage.

Table 3-33 Description of capture parameters

Step 5 Click **Save** to save the configured settings.

3.6.7.2 SD Card Control

Storage management is used to check the capacity and status of storage media and to format storage media.

Step 1 Navigate to **Settings** > **Record Management** > **SD Card Control** > **Record Management**.

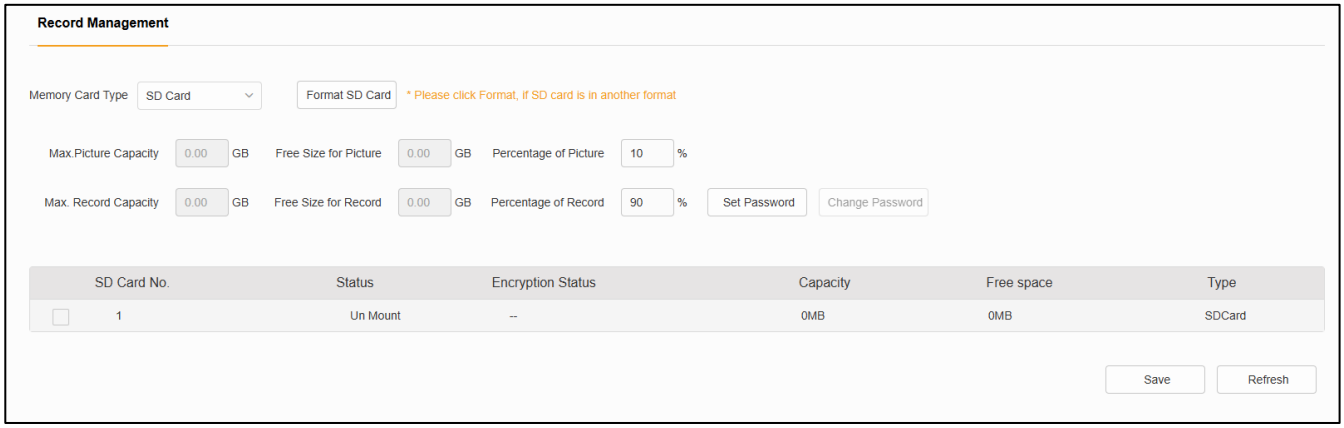

Figure 3-67 Record Management

Step 2 Configure the SD card control parameters.

Parameter	Description
Memory Card Type	Displays the detected storage type used by the device for local recording. Typically shows **SD Card** when a memory card is inserted.
Format SD Card	Formats the inserted SD card to the required file system for recording. Formatting is recommended if the SD card is in a different format or used for the first time.
Max. Picture Capacity	Shows the maximum storage capacity allocated for snapshot images on the SD card.
Free Size for Picture	Displays the currently available free space reserved for storing snapshot images.
Percentage of Picture	Defines the percentage of total SD card storage allocated for picture snapshots.
Max. Record Capacity	Shows the maximum storage capacity allocated for video recordings on the SD card.
Free Size for Record	Displays the currently available free space reserved for video recordings.
Percentage of Record	Defines the percentage of total SD card storage allocated for video recording files.
Set Password	Enables password protection for SD card data to prevent unauthorized access.

Change Password	Allows modification of the previously set SD card encryption password.
SD Card No.	Displays the index number of the detected SD card.
Status	Indicates the current state of the SD card, such as **Mounted** or **Un Mount**.
Encryption Status	Shows whether SD card encryption is enabled or disabled.
Capacity	Displays the total storage capacity of the inserted SD card.
Free Space	Shows the remaining available storage space on the SD card.
Type	Indicates the storage media type, such as **SD Card**.

Table 3-34 Description of SD card control parameters

Step 3 Click **Save** to save and apply all configured record management settings.

Step 4 (Optional) Click **Refresh** to reload the SD card status, update capacity, and free space information.

3.7 Maintain

This section provides essential system management and maintenance tools for the device. It allows you to check firmware and system information, perform firmware upgrades, restore factory default settings, and carry out routine system maintenance operations. Additionally, you can import and export configuration files for backup or deployment purposes, and access log records to review system events and troubleshooting information.

3.7.1 Version

This part provides comprehensive device information, including the Model Number, Firmware Version, Web Version, ONVIF Version, MAC Address, Serial Number (S/N), and Device ID. These details help in device identification, compatibility verification, firmware management, network configuration, and technical support reference.

Step 1 Navigate to **Maintain** > **Version** to view the version information.

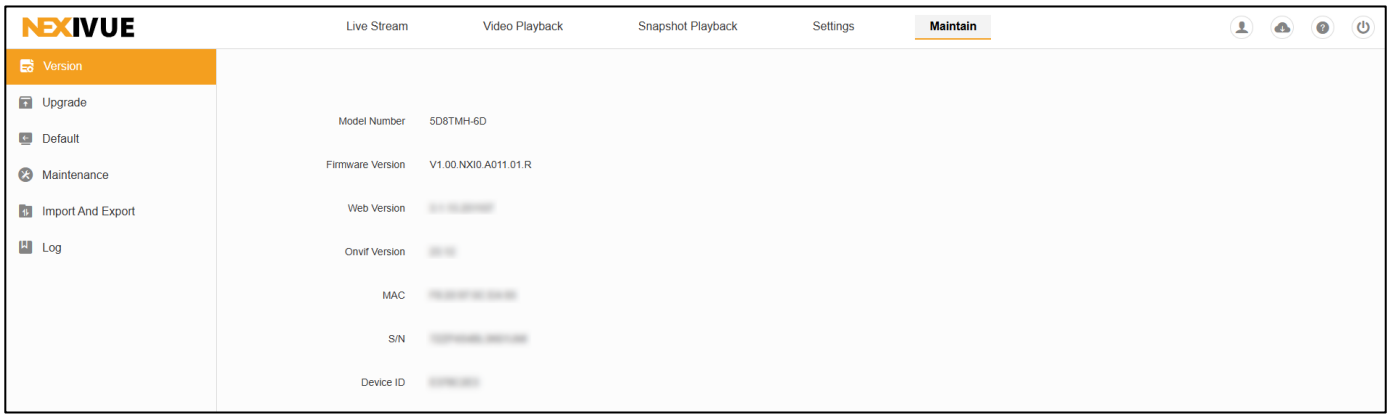

Figure 3-68 Version

3.7.2 Upgrade

This part allows you to update the device firmware through Manual Upgrade or Online (OTA) Upgrade to ensure optimal performance, new features, and security enhancements.

Step 1 Navigate to **Maintain** > **Upgrade**.

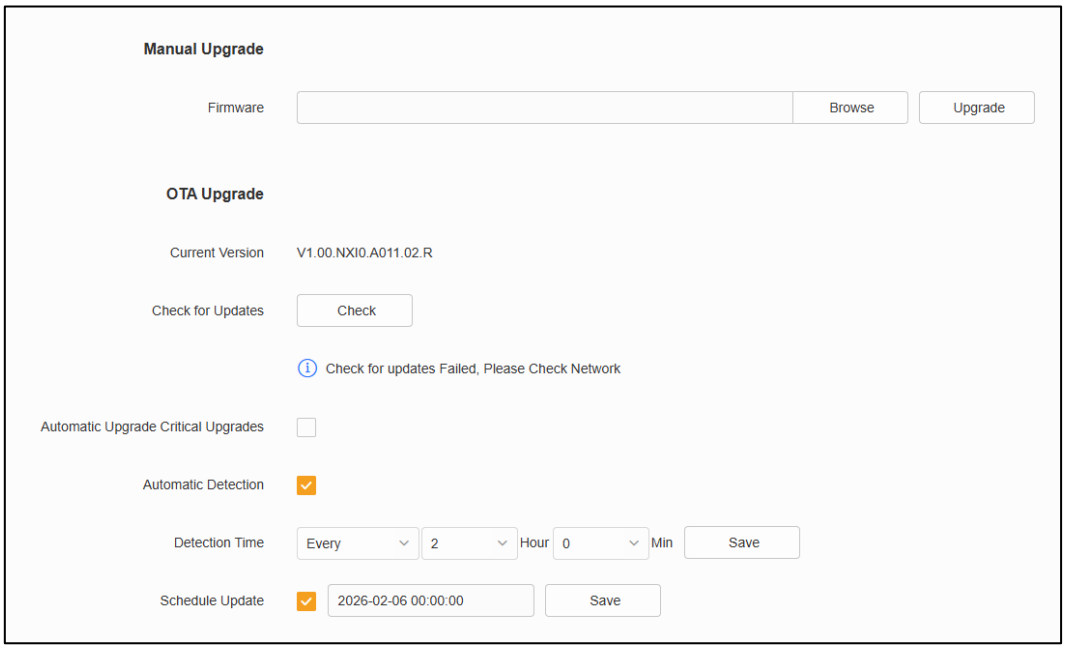

Figure 3-69 Upgrade

Step 2 Select the upgrading method according to the actual needs.

- Please do not power off during the upgrade.
- The device will automatically restart after the upgrade is complete.

- **Manual Upgrade**

  Use this method when you have the firmware file stored on your local computer.

  1. Click **Browse** and select the firmware file from your computer.
  2. Click **Upgrade** to start the upgrade process.

- **OTA Upgrade**

  This method allows the device to check, download, and install the latest firmware automatically via the network. Ensure the device is properly connected to the network.

  1. Click the **Check** button next to **Check for Updates**. If an update is available, it will be displayed.
  2. Check the box next to **Automatic Upgrade Critical Upgrades** if you want critical updates to install automatically.
  3. Check the **Automatic Detection** checkbox to automatically check for updates at scheduled intervals.
     a. Choose how frequently the device should check for updates:
        - Frequency (Every/Weekly/Monthly)

- Hours
- Minutes

b. Click **Save** to confirm.

4. Check the **Schedule Update** checkbox if you want updates installed at a specific date/time.
   a. Enter the desired schedule (format: YYYY-MM-DD HH:MM:SS).
   b. Click **Save** to finalize the schedule.

3.7.3 Default

This part allows you to revert the device to default or full factory settings.

Step 1 Navigate to **Maintain** > **Default**.

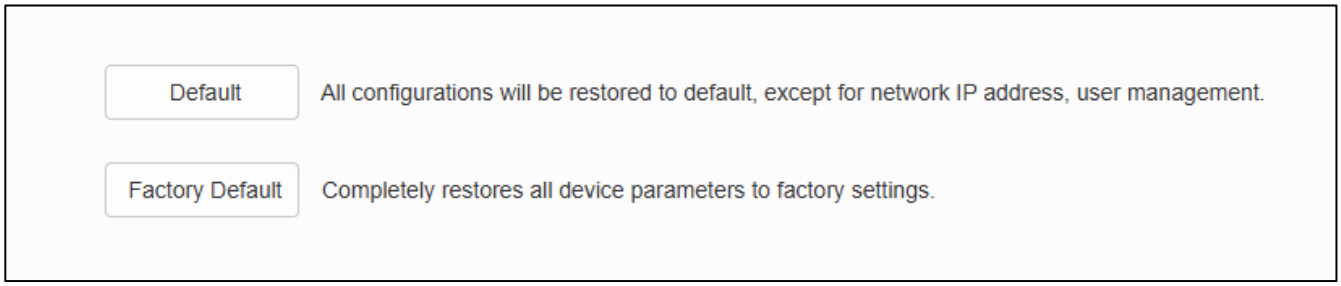

Figure 3-70 Default

Step 2 Select the reset method according to your need.

- After clicking **Default**, all parameters of the IPC except the network parameters will be automatically restored to the factory default settings.
- After clicking **Factory Default**, all parameters of the IPC will be automatically restored to the factory default settings.

- Please operate the **Factory Default** function with caution.

3.7.4 Maintenance

This section allows you to keep the device running smoothly by performing manual restarts or scheduling automatic timed restarts at regular intervals.

Step 1 Navigate to **Maintain** > **Maintenance**.

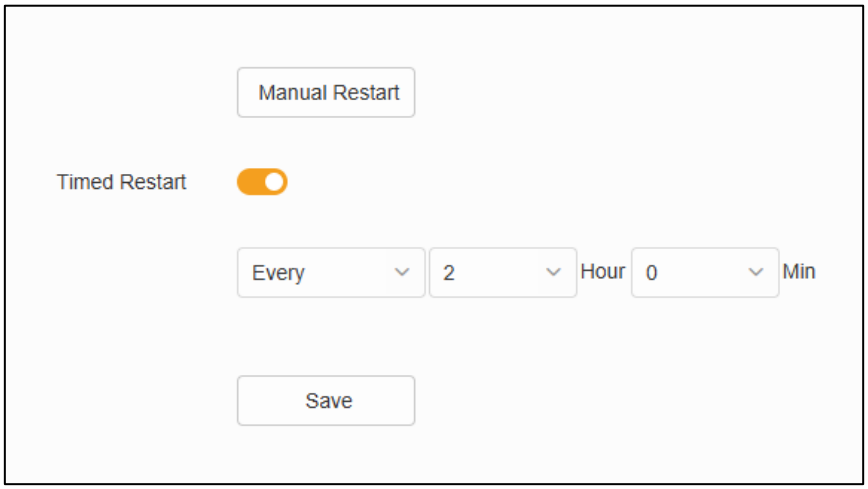

Figure 3-71 Maintenance

Step 2 Configure maintenance parameters.

- Click Manual Restart to immediately reboot the device.
- Turn on the Timed Restart toggle to activate scheduled restarts.
- Set the Restart Interval:
  - Frequency
  - Hour
  - Minute

Step 3 Click **Save** after adjusting the parameters.

3.7.5 Import And Export

This part allows you to import and export parameters as per your requirements.

Step 1 Navigate to **Maintain** > **Import And Export**.

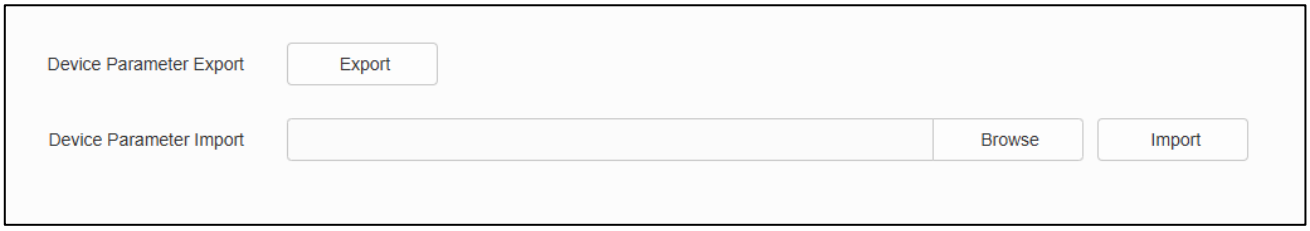

Figure 3-72 Import and export

Step 2 Click **Export** to export the parameters of the device and save them to the local computer.

Step 3 Click **Browse**, select the storage path of the device parameter file, and click **Import**. This is used to import the file of saved website device parameters.

3.7.6 Log

The log interface allows querying, displaying and exporting log information that is effectively saved on the SD card.

Step 1 Navigate to **Maintain** > **Log**.

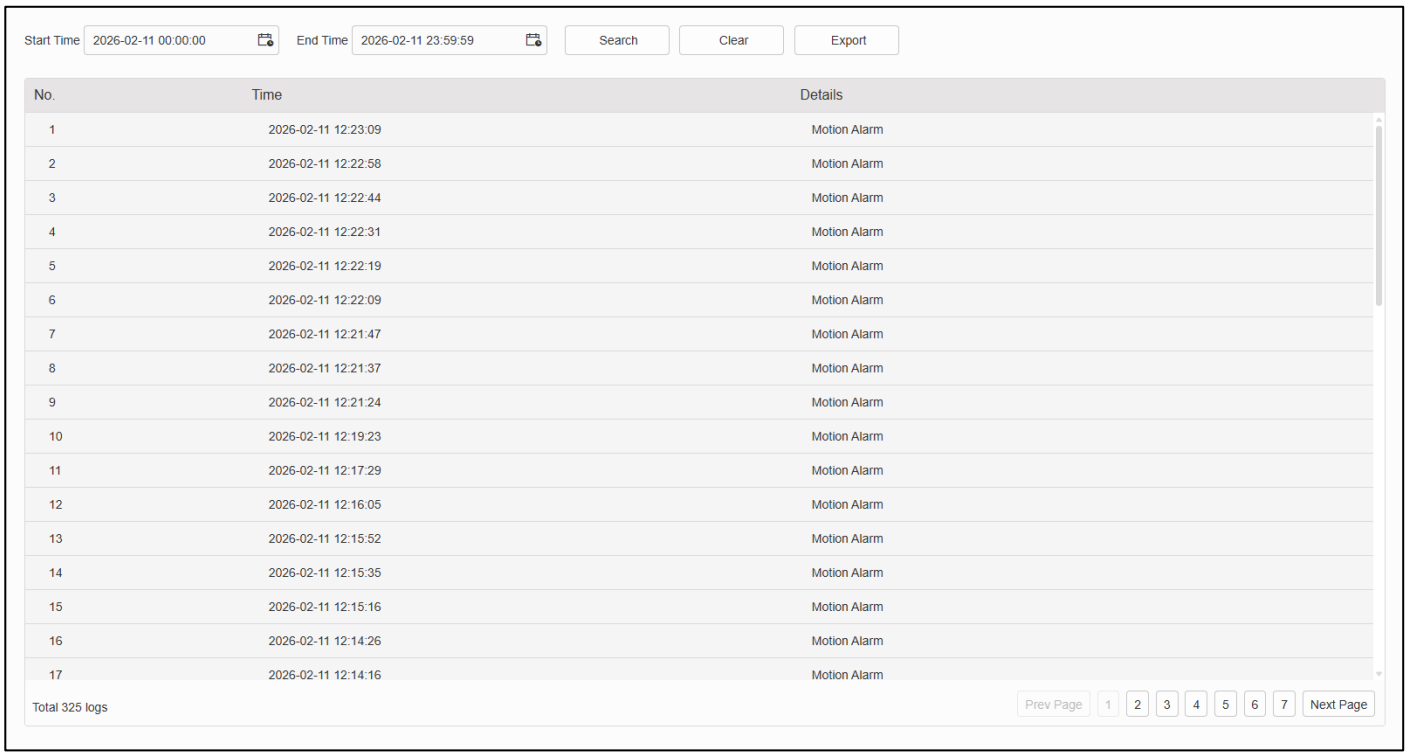

Figure 3-73 Log

Step 2 Enter the **Start Time** and **End Time** to define the log period you want to view.

Step 3 Click **Search** to display logs within the selected time range. Use the page numbers and **Next**/**Prev Page** buttons at the bottom to scroll through log entries.

- Click **Clear** if you want to delete all log records of the device so far.

Step 4 Click **Export** to download the displayed logs for backup or analysis.

4. Appendix - 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secure security system.

Mandatory actions to be taken for basic equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters.
- Include at least two types of characters; character types include upper- and lower-case letters, numbers, and symbols.
- Do not contain the account name or the account name in reverse order.
- Do not use continuous characters, such as 123, abc, etc.
- Do not use overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in the tech industry, we recommend keeping your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1) Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement

well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2) Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3) Set and Update Passwords Reset Information Timely

The equipment supports the password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please

modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4) Enable Account Lock

The account lock feature is enabled by default, and we recommend you keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5) Change Default HTTP and Other Service Ports

We suggest you change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6) Enable HTTPS

We suggest you enable HTTPS, so that you visit Web service through a secure communication channel.

7) MAC Address Binding

We recommend you, to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8) Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9) Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks. If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

a. SNMP: Choose SNMP v3 and set up strong encryption passwords and authentication passwords.
b. SMTP: Choose TLS to access mailbox server.
c. FTP: Choose SFTP and set up strong passwords.
d. AP hotspot: Choose WPA2-PSK encryption mode and set up strong passwords.

10) Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11) Secure Auditing

a. Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.

b. Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12) Network Log

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13) Construct a Safe Network Environment

To better ensure the safety of equipment and reduce potential cyber risks, we recommend:

a. Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
b. The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network to achieve the network isolation effect.
c. Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
d. Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

Thank you for choosing NEXIVUE!

Website: https://www.nexivuesecurity.com/

Email I'd: support@nexivuesecurity.com