NEXIVUE

User Manual

Network Video Recorder

V.1.00

Foreword

General

This user’s manual (hereinafter referred to as "the Manual") introduces the installation, functions and operations of the Network Video Recorder (NVR) devices (hereinafter referred to as "the Device"). Read carefully before using the Device and keep the manual safe for future reference.

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 NVR models. Certain features, functions, and configuration options may vary depending on the specific model. Please refer to your NVR 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 a rated voltage which conforms to the 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 a 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 in 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 can be removed with an air blower, or you can wipe the lens gently with a soft cloth that is moistened with alcohol.
- You can clean the device body with a soft dry cloth, and for stubborn stains, use the cloth with mild detergent. To avoid possible damage to the device body coating, which could cause performance decrease, do not use volatile solvents such as alcohol, benzene, diluent and so on to clean the device body, nor can strong, abrasive detergents 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 a soft cloth. You can also remove dust with an air blower.

 **WARNING**

- Strengthen the protection of the network, device data and personal information by adopting measures which include but are not limited to using strong passwords, modifying passwords regularly, upgrading firmware to the latest version, and isolating the computer network.
- 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. Features 7
2. Starting the Device **9**
2.1 Device Initialization Settings 9
3. Basic Configuration **12**
3.1 Login 12
3.2 Resetting Password 13
3.3 Plug-in Installation 20
3.4 Live Stream 21
3.4.1 Live Stream Interface 21
3.5 Settings 27
3.5.1 System Setup 27
3.5.2 Network 37
3.5.3 Camera 53
3.5.4 Event 71
3.5.5 Record Management 93
3.5.6 Alerts 100
3.6 Video Playback 101
3.6.1 Video Playback Interface 101
3.7 Snapshot Playback 104
3.7.1 Snapshot Playback Interface 104
3.8 Maintain 105
3.8.1 Version 105
3.8.2 Upgrade 106

3.8.3 Default 107
3.8.4 Device Auto Maintenance 107
3.8.5 Import And Export 108
3.8.6 Channel Information 109
3.8.7 Log 109
3.8.8 Diagnose Info 110
4. Local Operations 111
4.1 Local Login 111
4.2 Main Menu 112
4.3 Live View 114
4.3.1 Live View Control Bar 114
4.3.2 Shortcut Menu 116
4.4 Video Playback 117
4.5 Backup 119
4.6 Settings 120
4.6.1 System Setup 120
4.6.2 Network Settings 122
4.6.3 Camera Settings 122
4.6.4 Event Settings 128
4.6.5 Record Management Settings 128
4.6.6 Alert Settings 128
4.7 Maintain 128
5. Appendix - 1 Cybersecurity Recommendations 129

1. Overview

1.1. Introduction

The NVR is a high-performance network video recorder. This product supports local live view, multiple-window display, recorded file local storage, remote control and mouse shortcut menu operation, and remote management and control functions.

This product supports center storage and client-end storage. The monitor zone in the front-end can be set anywhere. Working with other front-end devices such as IPC and VMS, this series product can establish a strong surveillance network through the CMS. In the network system, there is only one network cable from the monitor center to the monitor zone in the whole network. There is no audio/video cable from the monitor center to the monitor zone. The entire project is characterized by simple connections, low cost, and low maintenance.

This NVR can be widely used in areas such as public security, water conservancy, transportation and education.

1.2. Features

Playback

- Supports independent real-time recording for each channel. At the same time, it supports functions such as smart search, forward play, network monitor, record search and download.
- Supports various playback modes: slow play, fast play, backward play and frame-by-frame play.
- Supports time title overlay so that you can view the event's accurate occurrence time.
- Supports specified zone enlargement.

Storage

- With corresponding settings (such as alarm settings and schedule settings), you can back up related audio/video data in the network video recorder.
- You can take records via the web, and the record files are saved on the PC where the client is located.

Alarm

- Respond to external alarm simultaneously. Based on the user’s pre-defined relay settings, the system can process the alarm input correctly and send user screen or voice prompts (supporting pre-recorded audio).
- Supports settings of the central alarm server, so that the system can automatically notify users of the alarm information. Alarm input can be derived from various connected peripheral devices.
- Alert you of alarm information via email.

Network Surveillance

- Send audio/video data compressed by IPC to client-ends through the network, and then the data will be decompressed and displayed.
- Supports a maximum of 128 connections at the same time.
- Transmits audio/video data by protocols such as HTTP, TCP, UDP, MULTICAST and RTP/RTCP.
- Transmits some alarm data or alarm info by SNMP.
- Supports web access in WAN/LAN.

Window Split

- Adopt video compression and digital processing to display several windows in one monitor.
- Support 1/4/8/9/16/25/36 window split in preview and 1/4/9/16 window split in playback, depending on the selected models.

Record

- Supports regular record, motion record, alarm record and intelligent record. Save recorded files to the HDD and search or play them back locally or via the web.

Backup

- Supports network backup and USB record backup. You can back up the record files to devices such as a peripheral USB 2.0 device.

Network Management

- Supervise NVR configuration and control power via Ethernet.
- Supports web management.

Peripheral Equipment Management

- Supports peripheral device control, and you can freely set the control protocol and connection port.
- Supports transparent data transmission such as RS-485.

2. Starting the Device

⚠

- For device security, connect the NVR to the power adapter first and then connect the device to the power socket.
- The rated input voltage matches the device power button. Make sure the power wire connection is OK, and then press the power button.
- Always use a stable current; if necessary, a UPS is the best alternative measure.

Step 1 Connect the NVR and the computer to the same network.

Step 2 Connect the power cable and turn on the NVR using the power switch.

Step 3 Ensure that the NVR has obtained a valid IP address.

After the device starts, the system defaults to multiple-channel display mode.

2.1 Device Initialization Settings

After selecting the required NVR in Nexivue Finder, the system will guide you through the initial device setup (if the device is not initialized), 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 NVR time with the computer system time.
- Verify the **Device Time** displayed on the screen.
- Click **Next Page** to proceed.

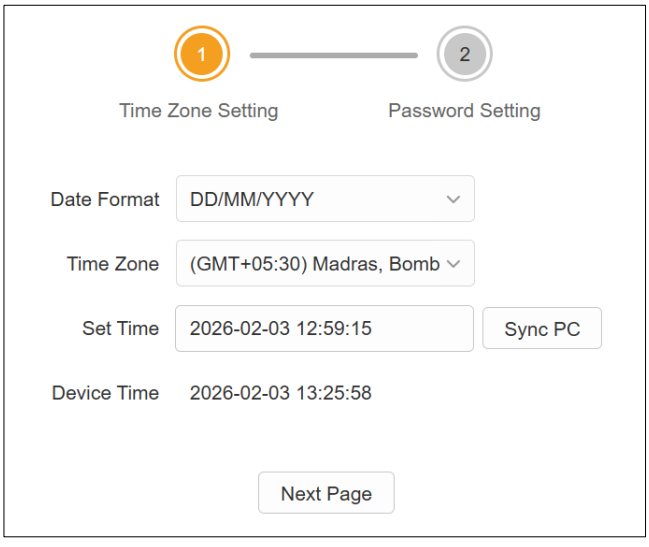


Figure 2-1 Time zone setting

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

- Registering a recovery e-mail address is optional. However, we recommend configuring it so you can easily reset your device password using the e-mail recovery process whenever needed.

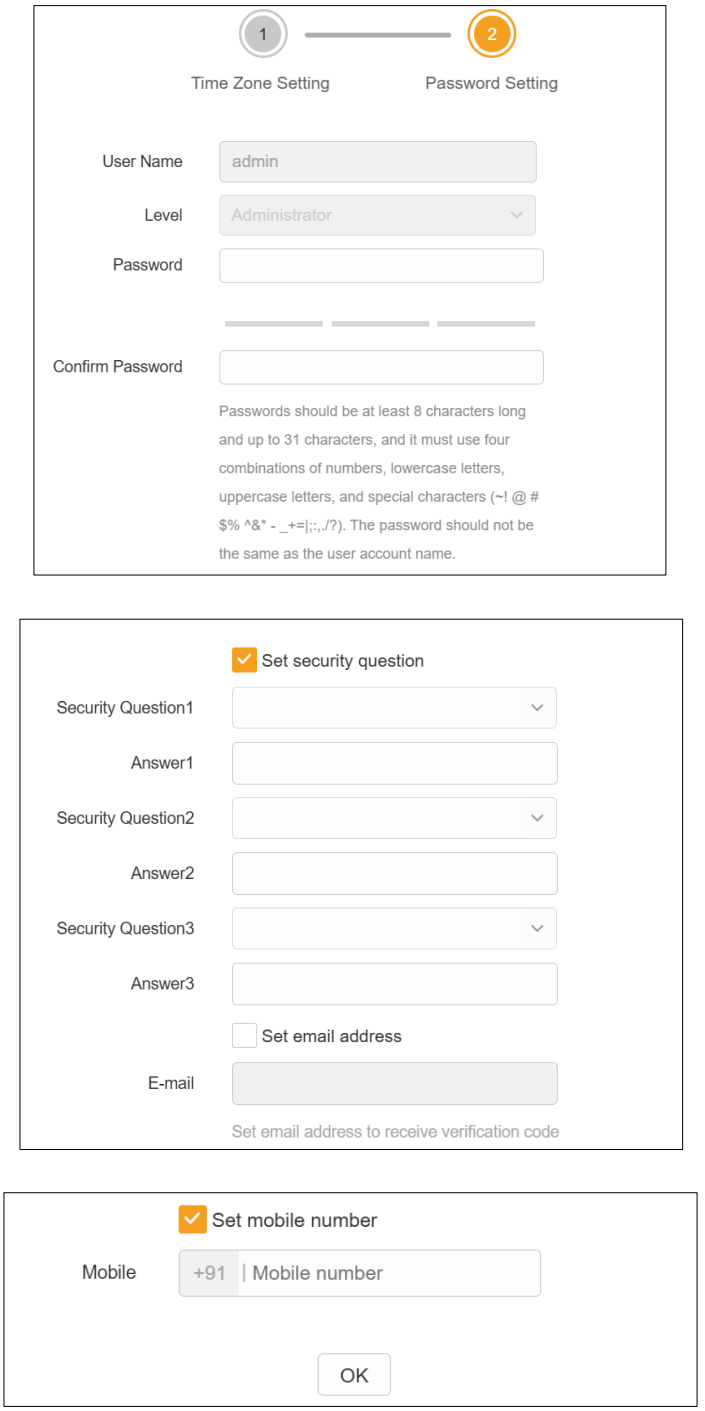


Figure 2-2 Password setting

Parameter	Description
User Name	The default username is admin.
Level	The default level is Administrator.
Password Confirm 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.
Security Questions	Need to select the questions and fill in accordingly to reset the password.
Email	(Optional) Check the Email checkbox 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 device before logging in to the web interface.
- When initializing the device, 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 device's full IP address (http://192.168.10.200) in the address bar, and press **Enter**.

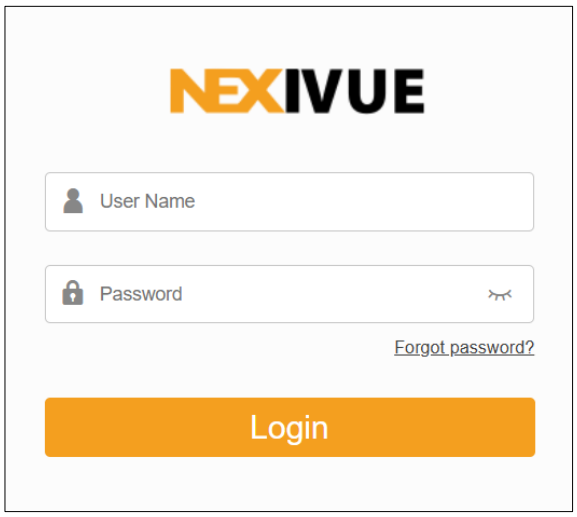


Figure 3-1 Login page

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

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

- The default administrator account is admin. The password is the one that was configured during initial settings. To ensure your account security, we recommend you keep your password secure and change it regularly.
- Click to display the password.

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

3.2 Resetting Password

You can reset the password using the security questions, registered email address, or mobile number if you forget the password for the admin account.

Step 1 On the device login page, click **Forgot password**.

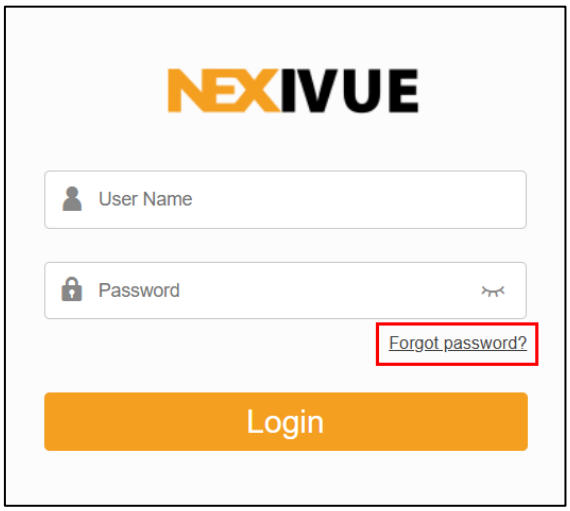


Figure 3-2: Forgot Password

Step 2 Click **Confirm** to continue.

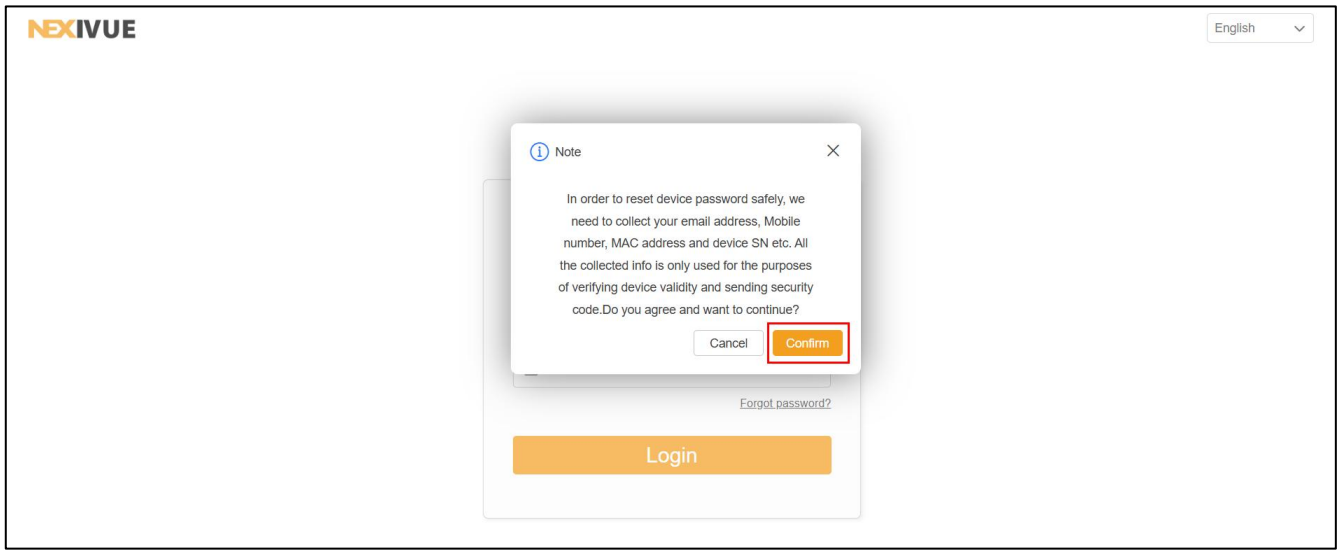


Figure 3-3: Confirm to Continue

Step 3 Select a verification mode (**Mobile Number Verification**, **E-mail Verification, or Security Question Verification**).

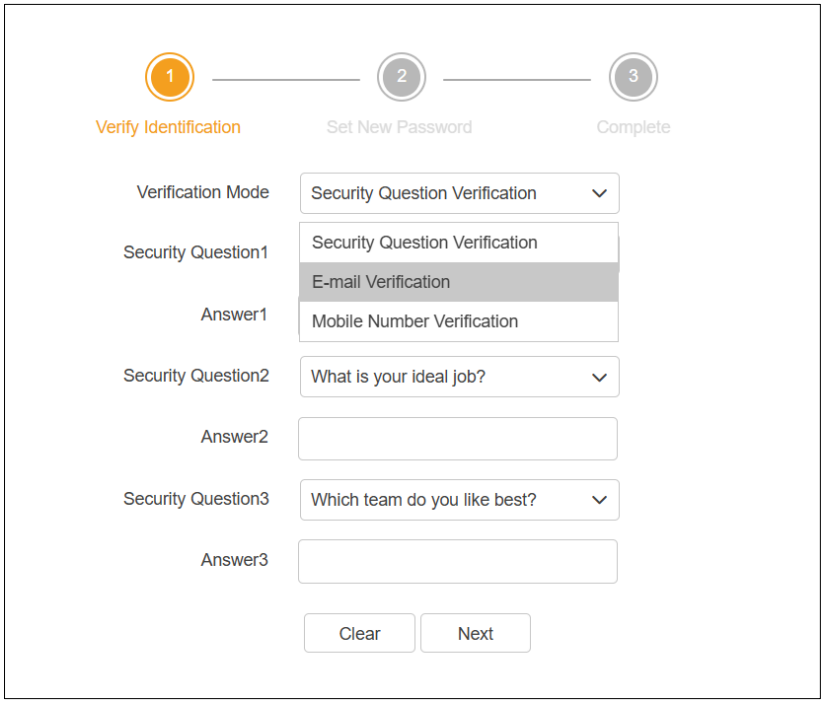


Figure 3-4: Verify Identification

Resetting Password Using Mobile or Email Verification Mode

1. Select **Verification Mode** as **Mobile Number Verification** or **Email Verification**.
2. Click **Next** to continue. A Password Reset QR Code is displayed on the screen.

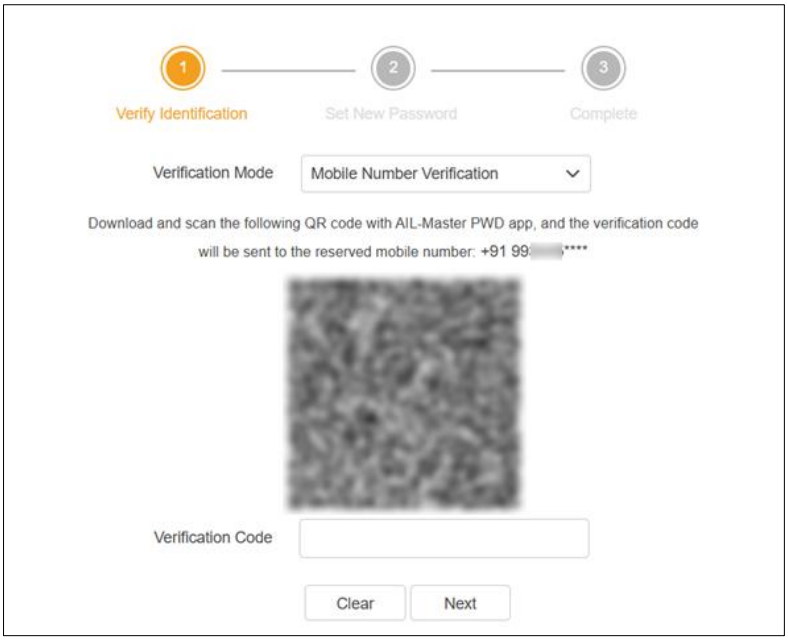
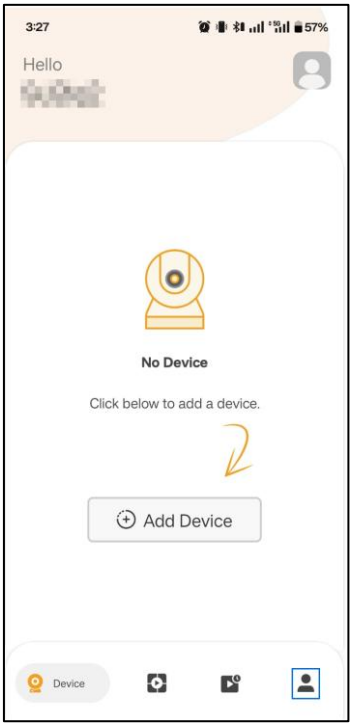


Figure 3-5: Password Reset QR Code

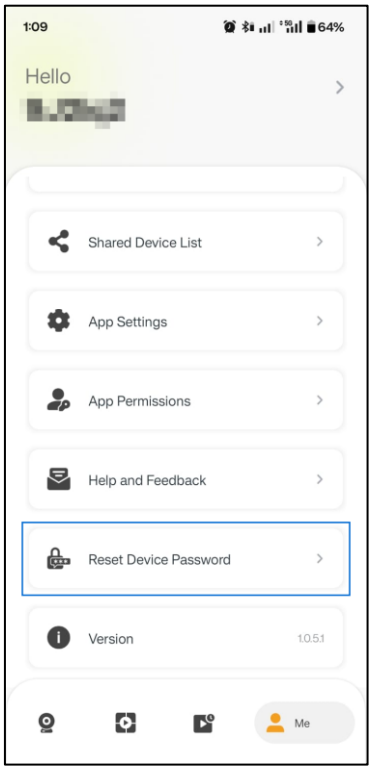
3. Now scan this QR code using the password reset QR code scanner of the Nexivue Mobile App.

Follow these steps to open the QR code scanner

- Open the Nexivue app and in the bottom-right corner, click **Me** icon.



- Tap **Reset Device Password**. The QR code scanner screen is displayed.



- Scan the QR code, and after successful scanning, a confirmation message is displayed in the Nexivue app.

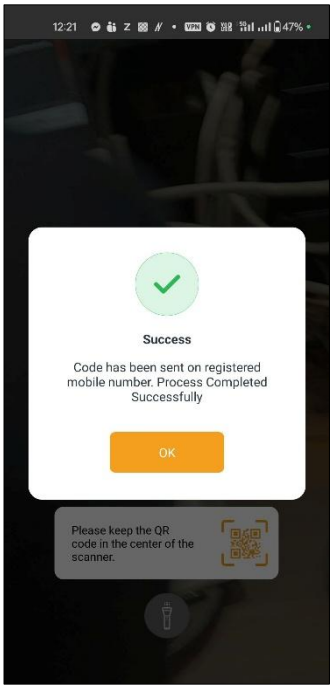


Figure 3-6: Confirmation Message

4. A verification code is sent to your registered mobile number or email address.

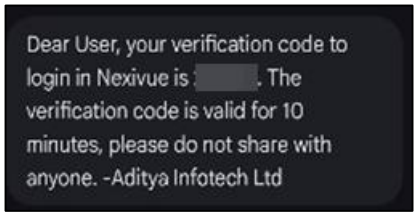


Figure 3- 7: OTP on Mobile Number



Figure 3-8: OTP on Email Address

5. Enter the verification code received on your registered mobile number or email address, and then click **Next**.

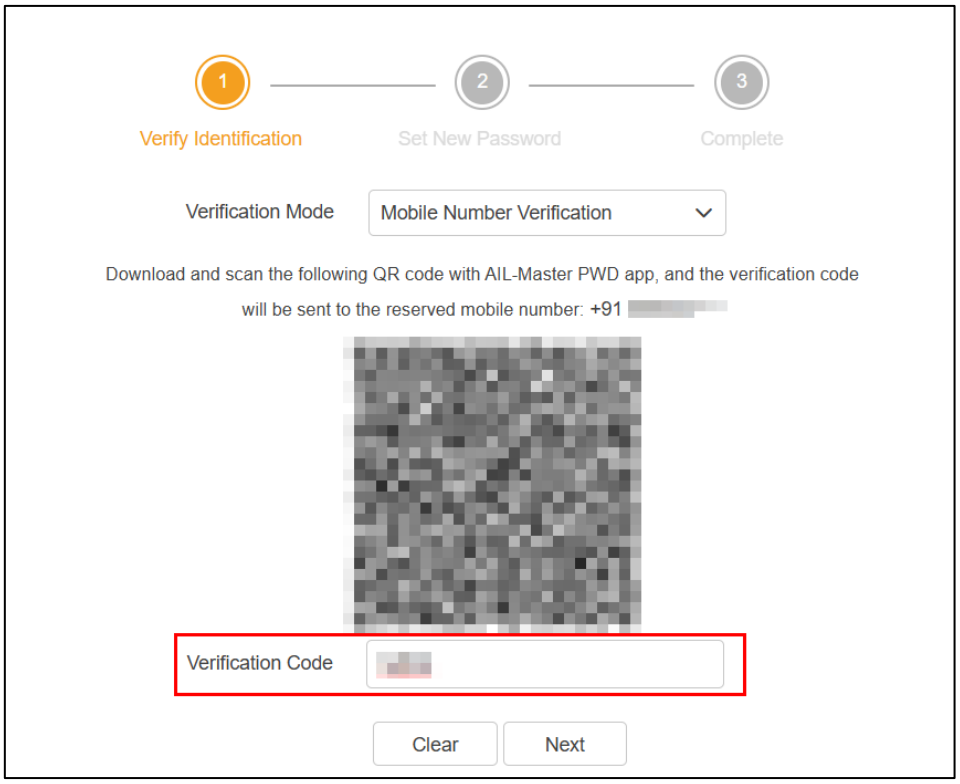


Figure 3-9: Enter Verification Code

6. Enter the new password, and then re-enter it to confirm. Click **Next** to continue.

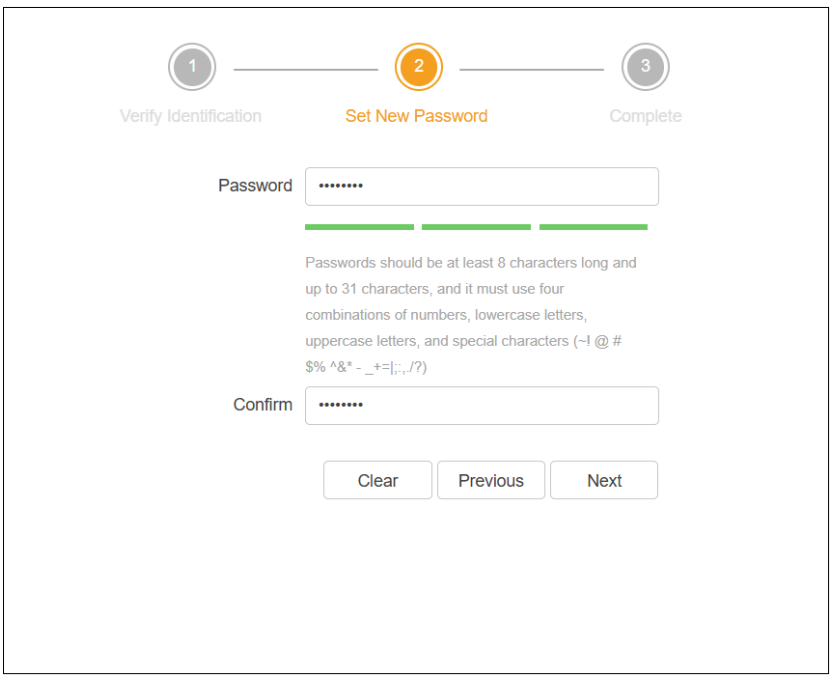


Figure 3-10: Enter Password

7. Click **Re-register** to complete the password reset process.

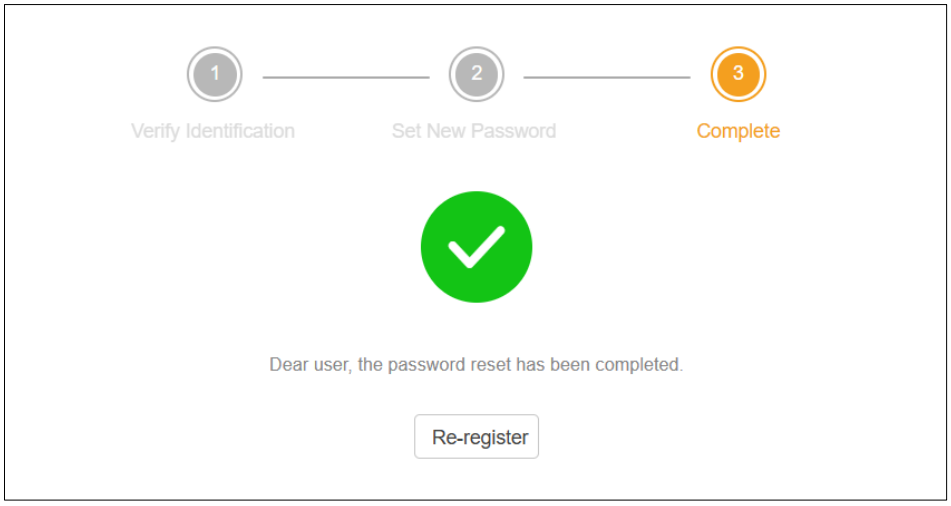


Figure 3-11: Re-register

The password has been successfully reset, and you can now log in with the new password.

Resetting Password Using Security Question Verification Mode

1. Select **Verification Mode** as **Security Question Verification**.
2. Answer the security questions and click **Next**.

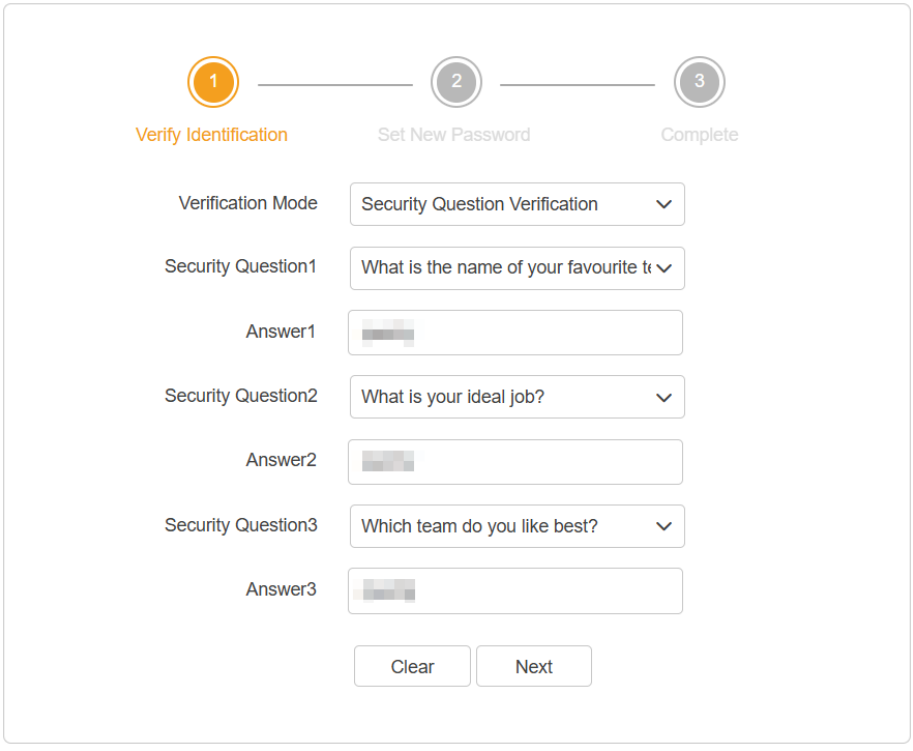


Figure 3-12 Security Question Verification

3. Enter the new password, and then re-enter it to confirm. Click **Next** to continue.

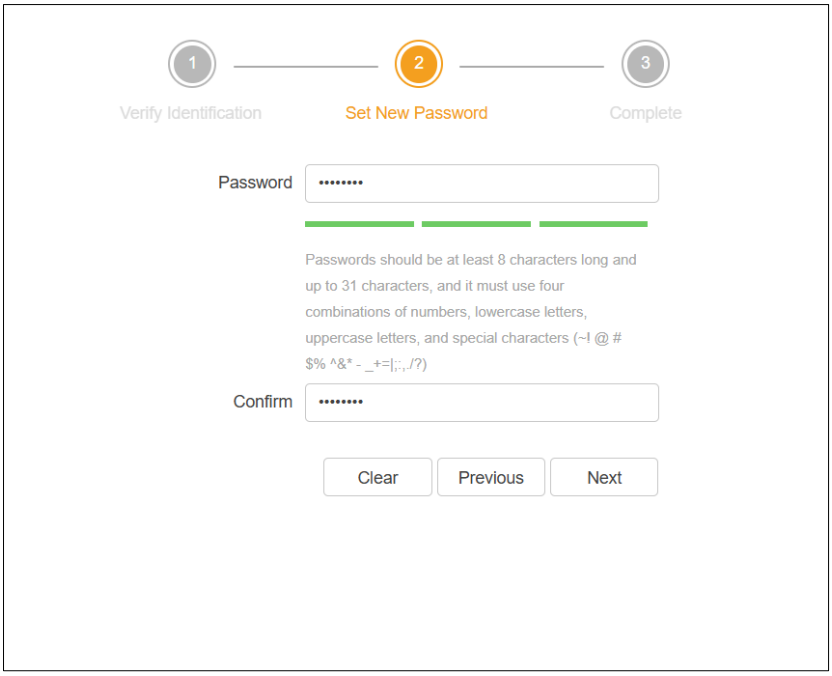


Figure 3-13: Enter Password

4. Click **Re-register** to complete the password reset process.

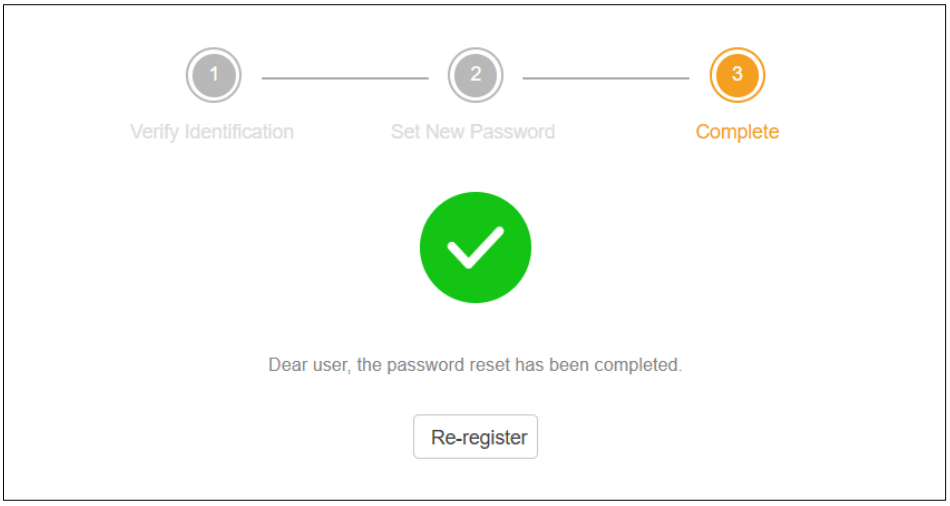


Figure 3-14: Re-register

The password has been successfully reset, and you can now log in with the new password.

3.3 Plug-in Installation

After successfully logging in to the device via a web browser, download and install the required plug-in for proper operation of the web interface.

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

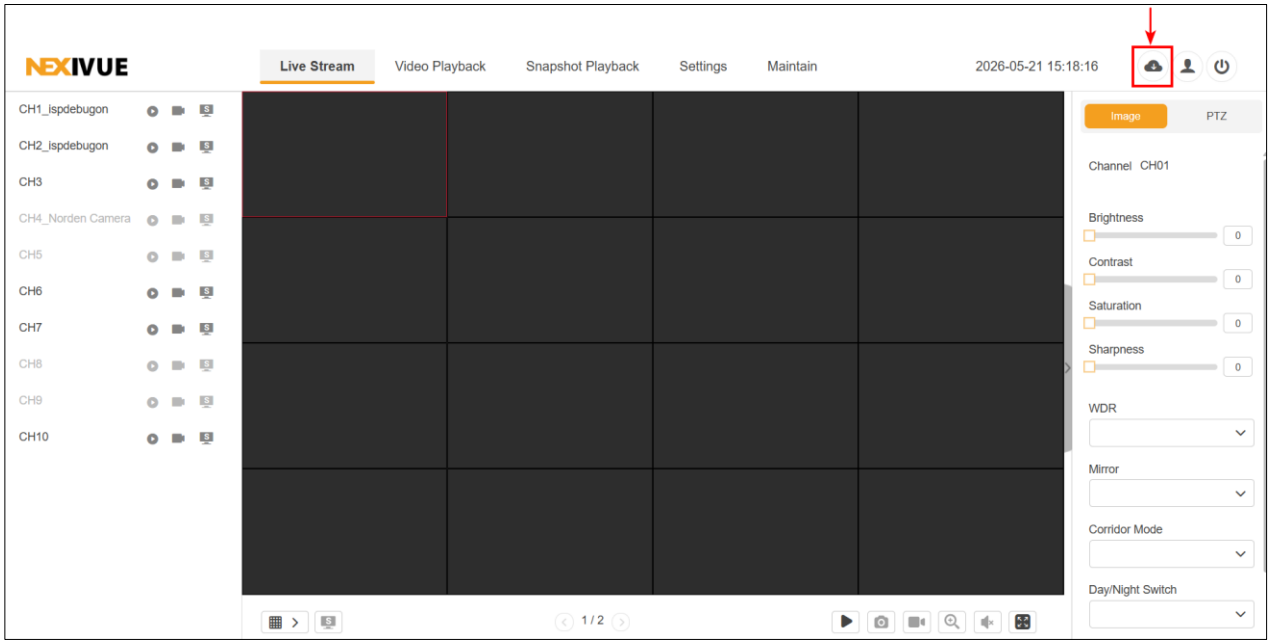


Figure 3-15 Download plug-in

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

Step 3 After installation, re-enter the device 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.

3.4 Main Interface

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 NVRs 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 user.
- : Click the **Download Plug-in** icon to download the plug-in.
- : Click the **Logout** icon to log out the currently logged-in user.

3.4.1 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.

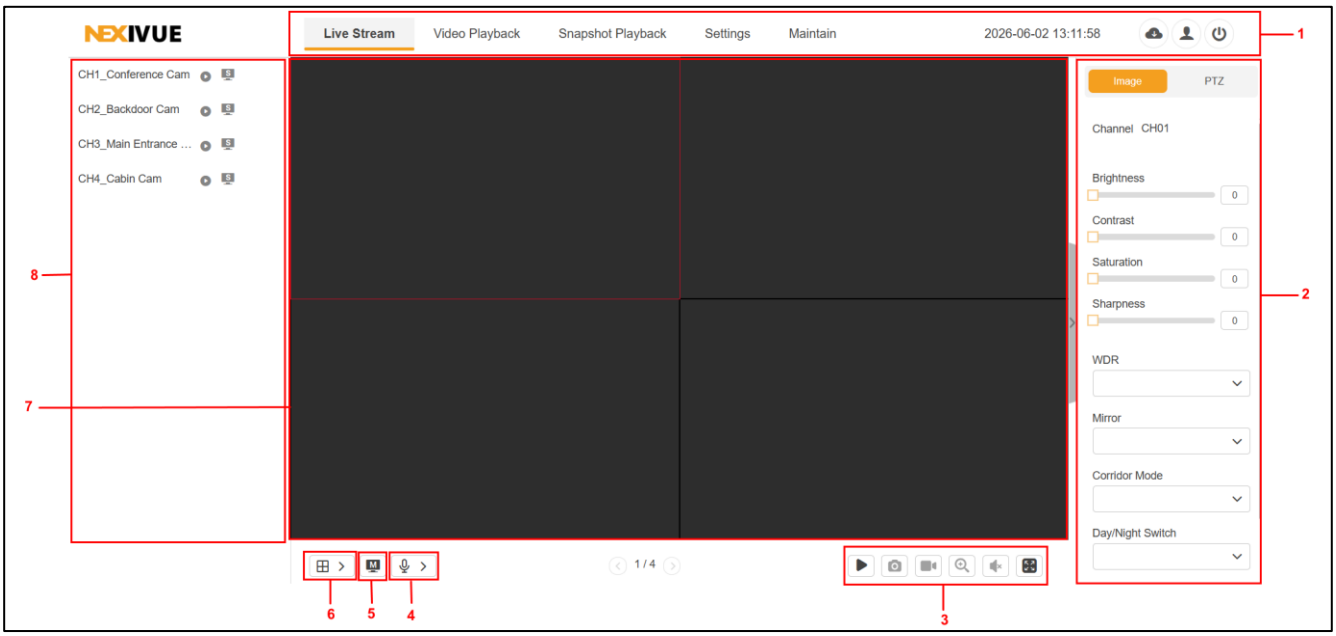


Figure 3-16 Live

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, and Logout.
2	Image Config and PTZ Control Panel	Allows configuration of image parameters (Brightness, Contrast, Saturation, Sharpness, WDR, Mirror, Flip, Day/Night) and control of PTZ parameters.
3	Live view function bar	Provides live view operations, including audio enable/disable, snapshot capture, digital zoom, start recording, and full screen zoom.
4	Talk	Enable or disable the two-way talk with the selected IPC. The function is only supported when the IPC has an in-built mic or an external mic attached to it.
5	Stream type	Allows selection of the stream type, such as Mainstream or Sub-Stream.
6	Window Layout	Provides different window layout options based on the number of channels supported by the device.
7	Live view window	Displays the live view of the active cameras in the selected layout.
8	Channel list	Displays the list of cameras connected to the device.

Table 3-1 Description of live interface

3.4.1.1 Channel List

This panel provides quick access to live channel selection, viewing and stream type controls.

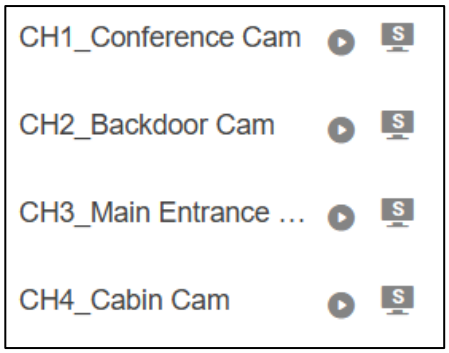


Figure 3-17 Channel list

Displays all available camera channels. You can start or stop the live view by clicking the Play ( ) icon on the respective channel.

You can select the desired stream type for each channel:

- (**Main Stream**): Its bit streams are big, and the definition is high. It occupies a large network bandwidth suitable for video wall surveillance, storage and more.
- (**Sub Stream**): Its definition is low, but it occupies a small network bandwidth. It is suitable for general surveillance, remote connection and more.

3.4.1.2 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.

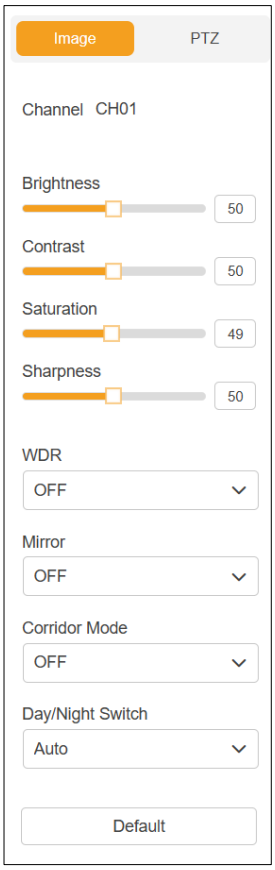


Figure 3-18 Image config

Option	Description
Brightness	Adjusts 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	Changes the value when the image brightness is correct, but the contrast is insufficient.
Saturation	Adjusts 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 **Horizontal and Vertical** to flip the image orientation as required by the installation.
Corridor Mode	Select **OFF**, **90°**, 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 3-2 Description of Image configuration options

3.4.1.3 PTZ Panel

You can use the PTZ control panel to perform operations such as directing the camera in eight directions, adjusting zoom, focus and iris settings, and quick positioning.

You can only access these features for PTZ cameras.

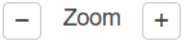
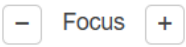
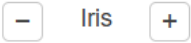
Icon	Function	Description
	Camera Direction Control	Control the device in eight directions, including up, down, left, right, left up, right up, left down and right down.
	Zoom- Zoom+	Click + to zoom in and click − to zoom out the live view image.
	Focus- Focus+	In manual focus mode, click − to make nearby objects clear, or click + to make distant objects clear.
	Iris- Iris+	When the monitoring screen is dark, iris is the priority in the exposure mode. Or in manual mode, click + to increase the iris, conversely, click − to reduce the iris.
	Speed	The speed value changes the PTZ camera's rotation speed. The larger the value, the faster the PTZ camera rotates. For example, the rotation with a speed of 7 is much faster than that of 1.
Preset		Configure and manage predefined PTZ camera positions that can be recalled instantly for quick monitoring of specific areas.
Patrol		Configure and manage automated PTZ movement sequences that cycle through multiple preset positions according to the defined patrol settings.

Table 3-3 Description of zoom & focus panel

3.4.1.4 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\NVR\192.168.10.200\Pic\2026-03-23** • The IP address included in the path refers to the assigned IP address of the device. • Captured snapshots are automatically saved in a date-wise folder.
	Record	On or off local video recording. The path of local video recording can be viewed at **C:\Program Files (x86)\NEXIVUE\NVR\192.168.10.200\Record\2026-03-23** • The IP address included in the path refers to the assigned IP address of the device. • Captured videos are automatically saved in a date-wise folder.
	Play/Stop	Click the icon to play or stop the live view of all the active channels.

	Talk	Click the icon to enable or disable the two-way audio talk.
	Full Screen	Expands the live view screen to occupy the entire screen, removing menus and controls. Press **Esc** to exit the full-screen view.

Table 3-4 Description of live view function bar

3.4.1.5 Configuring Stream Type

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



Figure 3-19 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.
- M means the current stream is mainstream; S means the current stream is sub stream.

3.4.1.6 Window Layout

This section introduces the options available for adjusting the window layout of the live view window. On the bottom-left of the Live page, click > on the right side of the window layout option to adjust the layout.



Figure 3-20 Window layout options

Option	Description
1	Displays one channel in full-screen mode.
	Splits the screen into 4 equal sections to display 4 channels simultaneously.
	Displays 6 channels on the screen in a multi-split arrangement for enhanced monitoring.
	Divides the screen into 8 sections to monitor multiple channels at the same time.
	Displays 9 channels in a 3×3 grid format.
	Displays 10 channels simultaneously in a customized split-screen arrangement.

	Shows 13 channels simultaneously in a mixed grid layout for wider coverage.
	Displays 16 channels in a 4×4 grid arrangement.

Table 3-5 Description of window layout options

3.5 Settings

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

3.5.1 System Setup

3.5.1.1 Local Config

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

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

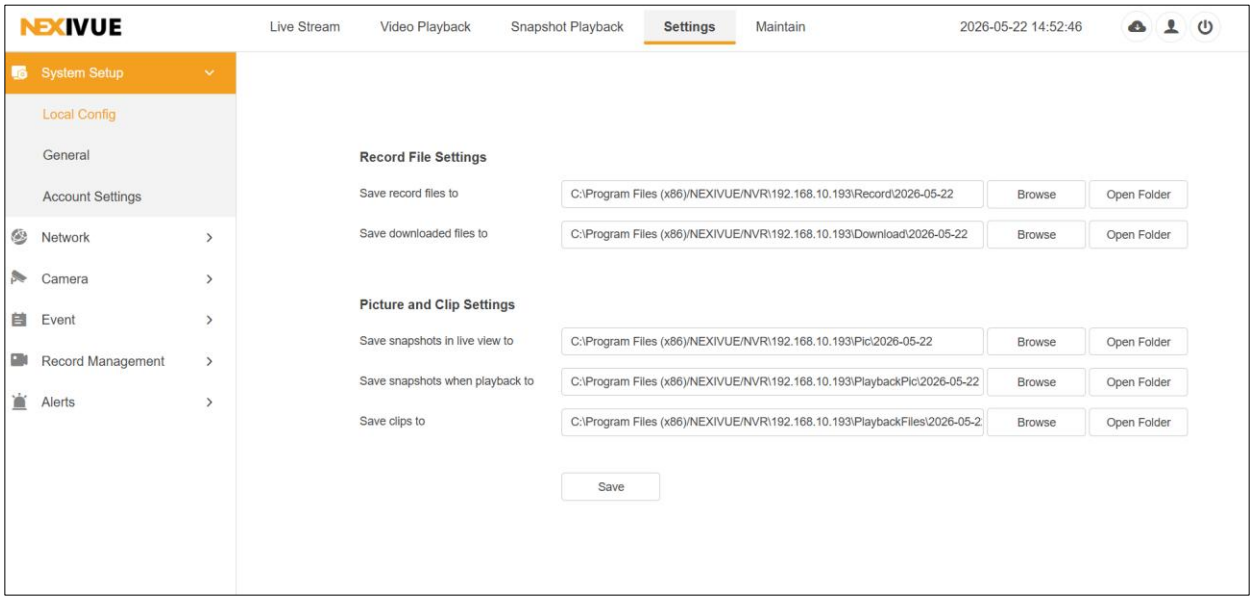


Figure 3-21 Local config

- By default, files are saved to **C:\Users\NEXIVUE\NVR\192.168.10.200**. After downloading and installing the plug-in, the default save path changes to **C:\Program Files (x86)\NEXIVUE\NVR\192.168.10.200**.
- 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 Folder** to directly open the selected folder.

Save downloaded files to:

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

3.5.1.2 General

The General section covers device settings, date settings, daylight saving time, and camera time sync.

Device Settings

Step 1 Navigate to **Settings** > **System Setup** > **General** > **Device Settings**.

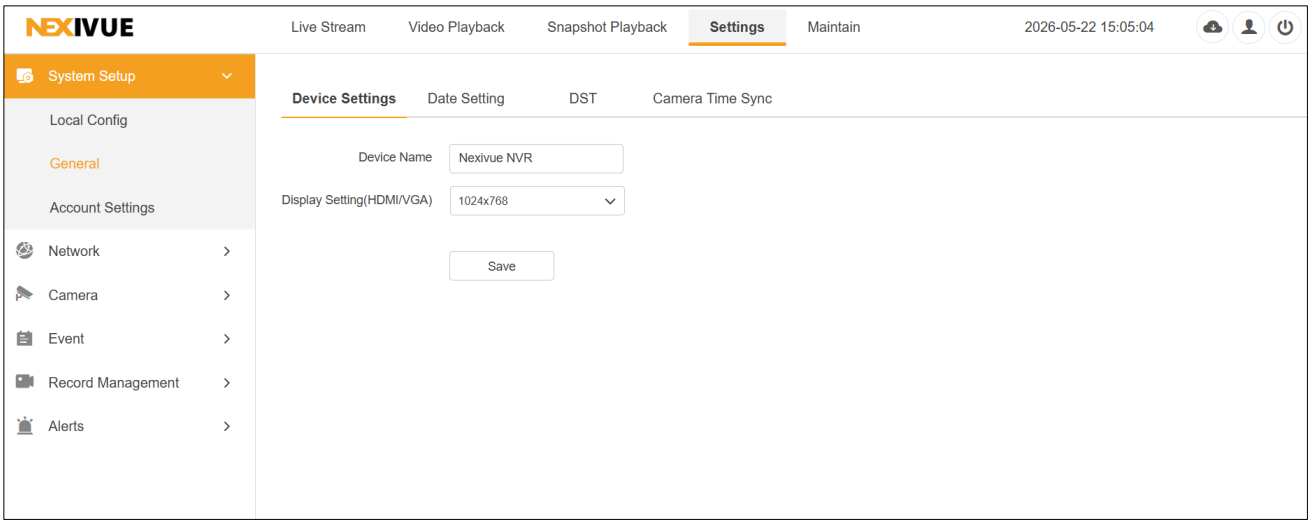


Figure 3-22 Device Settings

Step 2 In the **Device Name** field, enter the desired name for the NVR device.

Step 3 From the **Display Setting (HDMI/VGA)** drop-down list, select the required display resolution.

Step 4 Click **Save** to apply the changes.

Date Setting

Step 1 Navigate to **Settings** > **System Setup** > **General** > **Date Setting**.

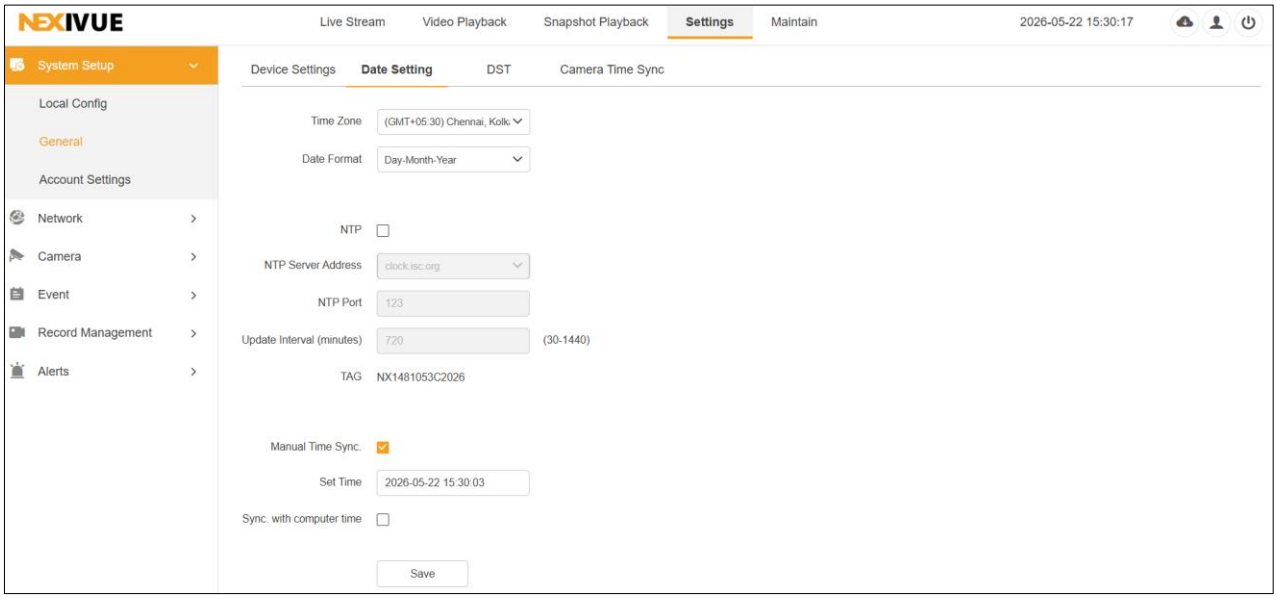


Figure 3-23 Date Settings

Step 2 Configure the settings for date and time parameters.

Parameter	Description
Time Zone	From the **Time Zone** list, select a time zone for the system.
Date Format	From the **Date Format** list, select a date format for the system.
NTP	Enable the NTP function to sync the Device time with the NTP server. ⚠ If NTP is enabled, device time will be automatically synchronized with server.
Server Address	Select the **NTP Server Address**.
NTP Port	Enter the NTP Port. The system supports TCP protocol only, and the default setting is 123.
Update Interval	In the **Update Interval** box, enter the amount of time (in minutes) that you want the Device to sync time with the NTP server. The value ranges from 30 to 1440.

Parameter	Description
Manual Time Sync	Enable the **Manual Time Sync** to set the time manually. You can configure the time using either NTP synchronization or Manual Time Sync. Only one option can be selected at a time.
Set Time	Enter the required date and time. Device Time displays the current time of the device for reference.
Sync. with computer 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.

Table 3-6 Description of date settings

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

Daylight Saving Time

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

Step 1 Navigate to **Settings** > **System Setup** > **General** > **DST**.

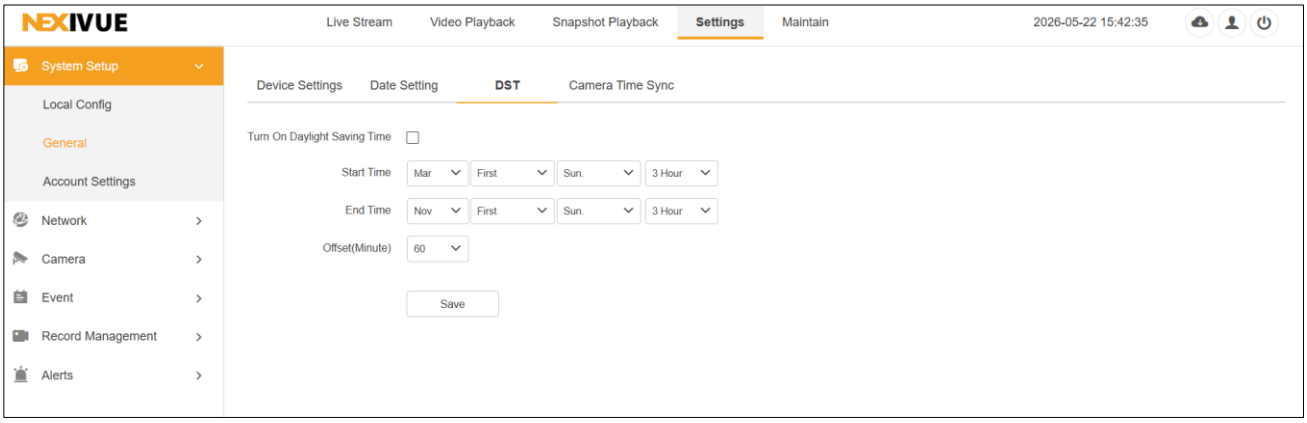


Figure 3-24 Daylight saving time

Step 2 Select the **Turn On Daylight Saving Time** checkbox to enable it.

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

Step 4 Set the **Offset** (in minutes) to define the time offset applied during the daylight saving period.

Step 5 Click **Save** to apply the DST settings.

Camera Time Sync

This section allows you to automatically synchronize the connected camera's date and time with the recorder at the specified interval, ensuring all devices maintain consistent timestamps for accurate recording and playback.

Step 1 Navigate to **Settings** > **System Setup** > **General** > **Camera Time Sync**.

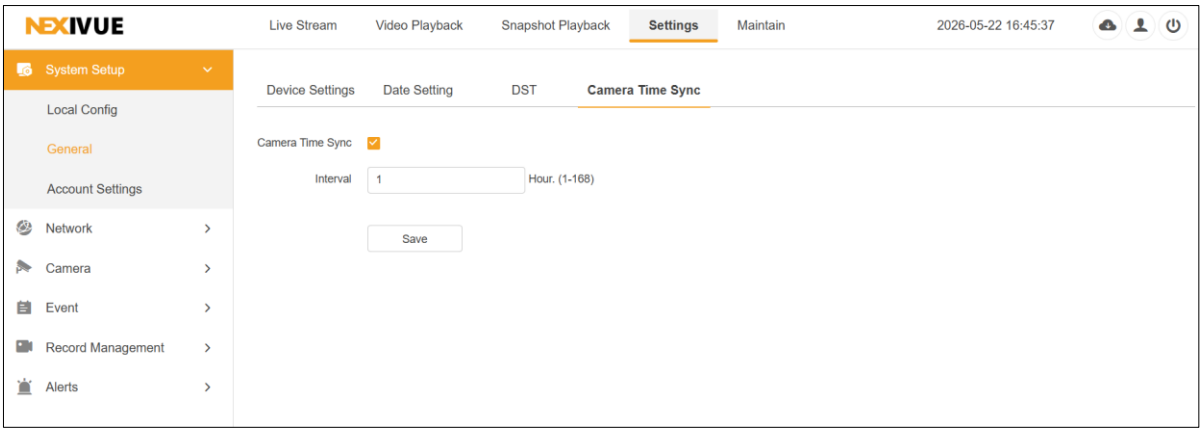


Figure 3-25 Camera time sync

Step 2 Select the **Camera Time Sync** checkbox to enable it.

Step 3 In the **Interval** field, enter the synchronization interval (in hours). The supported range is 1–168 hours.

Step 4 Click **Save** to apply the settings.

3.5.1.3 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** > **System Setup** > **Account Settings** > **User Management**.

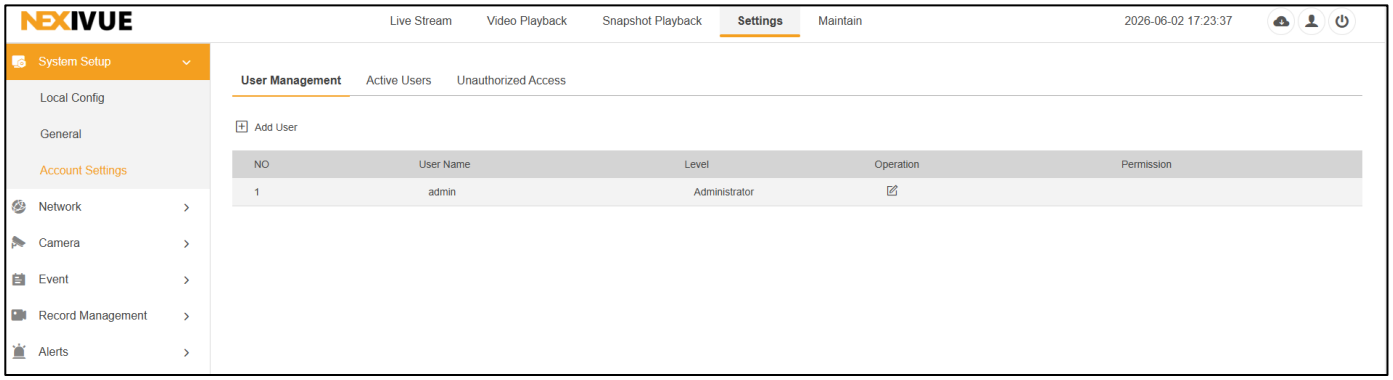


Figure 3-26 User Management

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

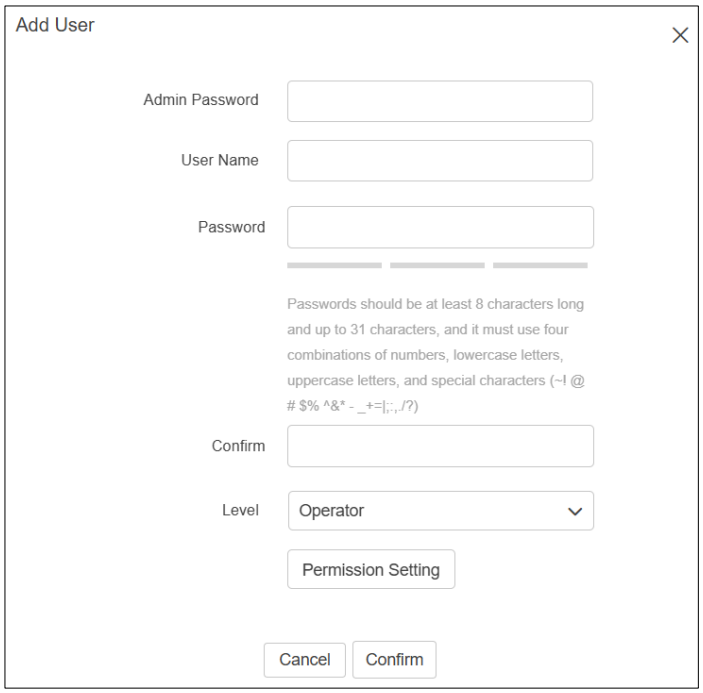


Figure 3-27 Add User

Step 3 Configure the parameters to add a new user account.

Parameter	Description
Admin Password	Enter the administrator's password to authorize adding a new user.
User Name	Enter a unique username for the new user account.
Password	Enter a secure password (8–31 characters with required character combinations).
Confirm	Enter the password again to confirm it.
Level	Select the user role to define the access level. • **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.
Permission Setting	Configure detailed user permissions, including local and remote access, system actions (camera, logs, upgrade, shutdown, and reboot, two-way audio, login), and channel-based rights for live view, playback, backup, and PTZ.

Table 3-7 Description of parameters of adding a user

Step 6 Click **Confirm** 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  to change the password and level of the existing account.

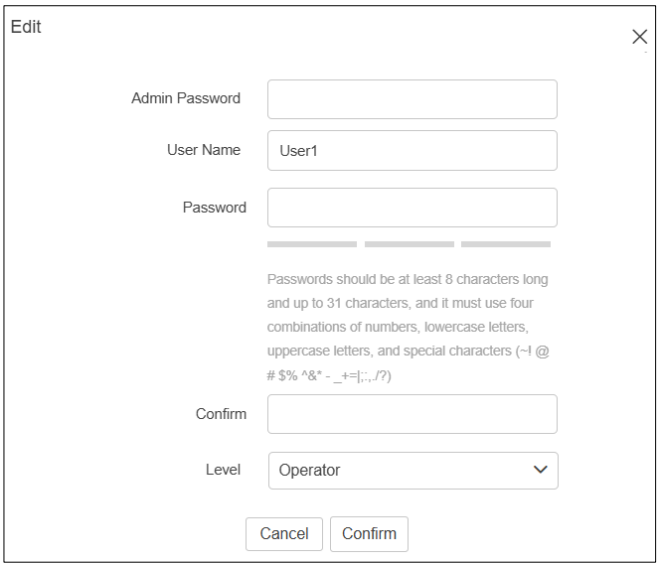


Figure 3-28 Edit User

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

Modify Permissions



- You cannot change the permissions of the admin account.

- Click  to only change the permissions of the user account.

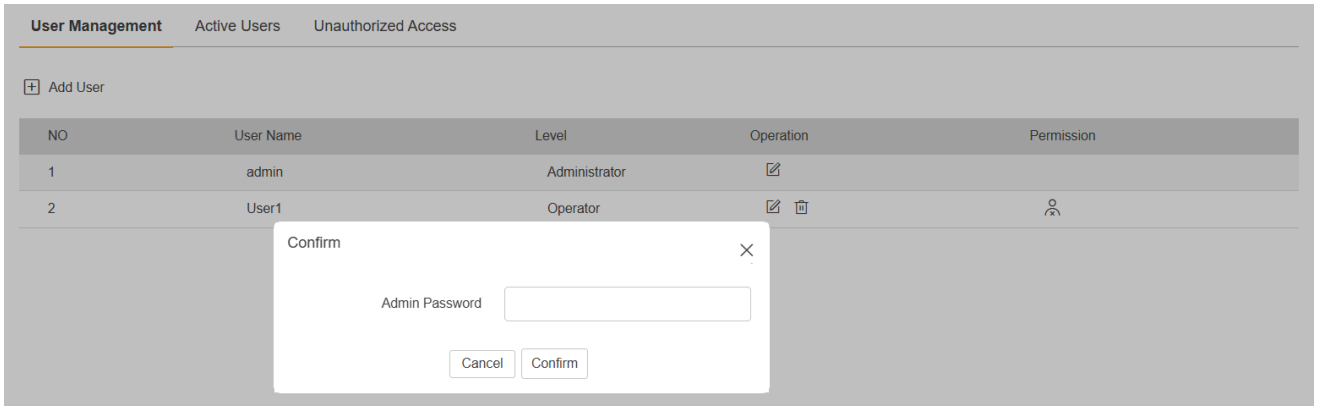


Figure 3-29 Modify level

- Enter the **Admin password** to authorize.
- Configure the user permissions as per the requirement.
- Click **Confirm** to save the user or click **Cancel** to exit without saving.

Delete User

- Admin account cannot be deleted.

- Click to delete the existing user account.

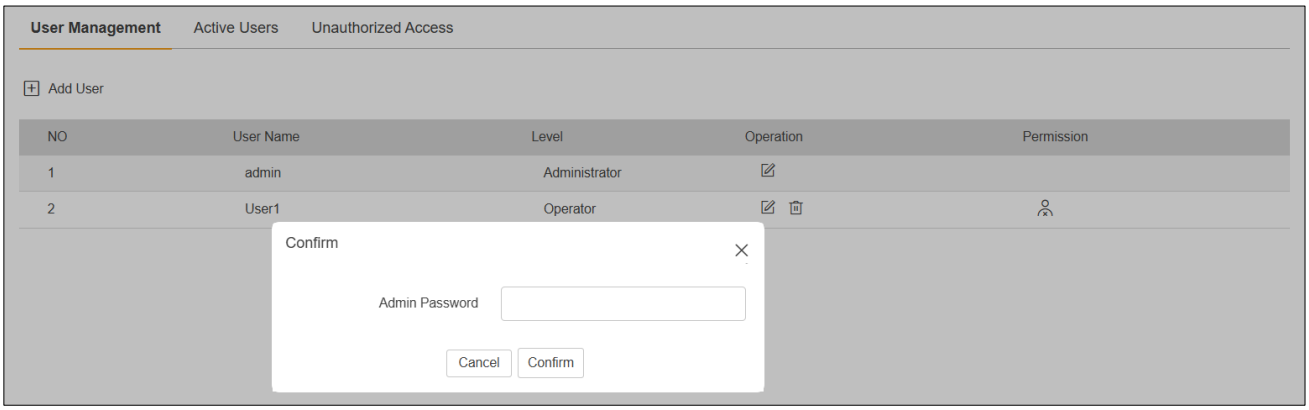


Figure 3-30 Delete user

- Enter the **Admin Password** to authorize and click **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 3-31 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.

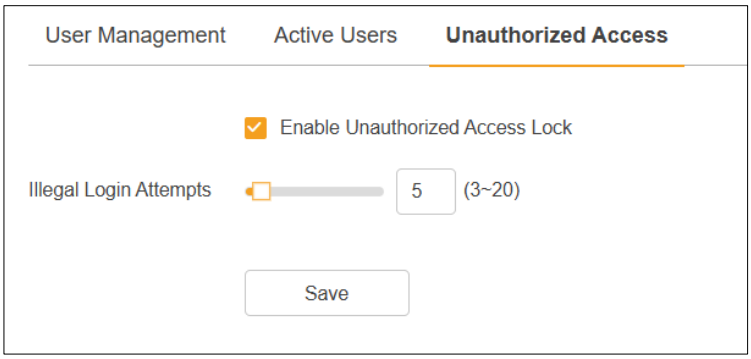


Figure 3-32 Unauthorized access

Step 1 Select the **Enable Unauthorized Access Lock** checkbox to enable it.

Step 2 Set the **Illegal Login Attempts** value using the slider or input box to define the maximum number of failed login attempts allowed. The value ranges from 3 to 20.

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

3.5.2 Network

This section introduces network configuration, including basic network settings, NexiQloud, and email settings.

- The device should be connected to the network.

3.5.2.1 Basic 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, and set DNS servers for network access and streaming.

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

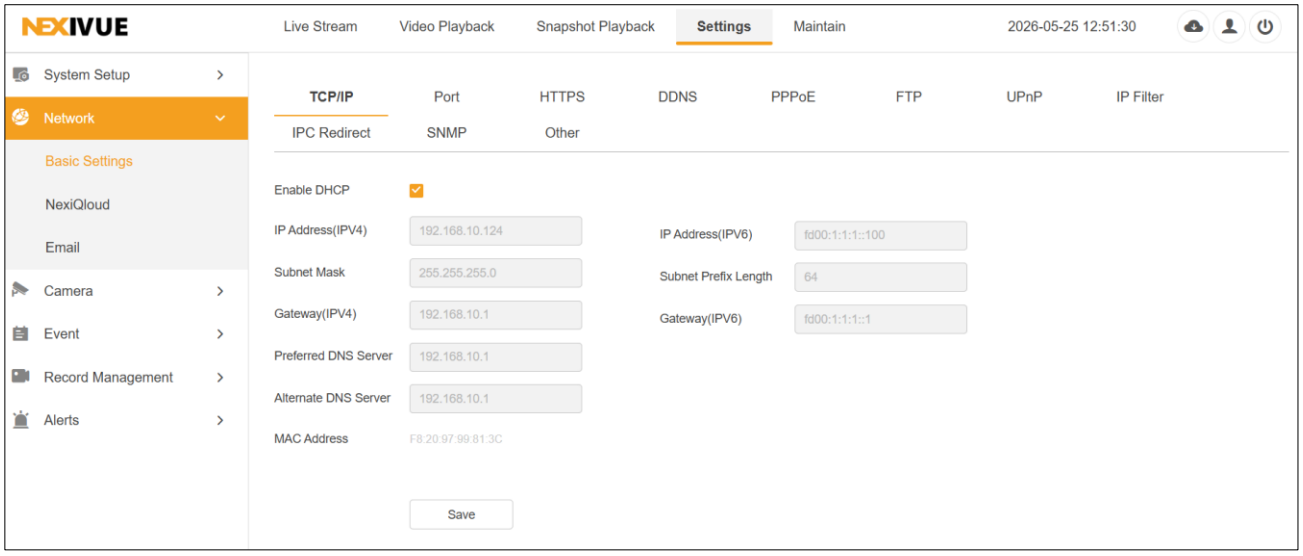


Figure 3-33 TCP/IP

Step 2 Configure TCP/IP parameters.

Parameter	Description
Enable DHCP	When enabled, the device automatically obtains the IPv4 address and related network parameters from the network, and manual IPv4 settings are disabled.
IP Address (IPv4)	Set the device IPv4 address manually when DHCP is disabled.
Subnet Mask	Configure the subnet mask corresponding to the IPv4 address.
Gateway (IPv4)	Configure the default gateway for IPv4 network communication.
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.

MAC Address	Displays the unique hardware address assigned to the network interface of the device.
IP Address (IPv6)	Set the device IPv6 address manually when DHCP is disabled.
Subnet Prefix Length	Enter the network portion of the IPv6 address, similar to the subnet mask in IPv4.
Gateway (IPv6)	Configure the IPv6 default gateway.

Table 3-8 Description of TCP/IP parameters

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

Port

This section allows you to configure the communication ports used by the device for web access, video streaming, and secure network communication

Step 1 Navigate to **Settings** > **Network** > **Basic Settings** > **Port**.

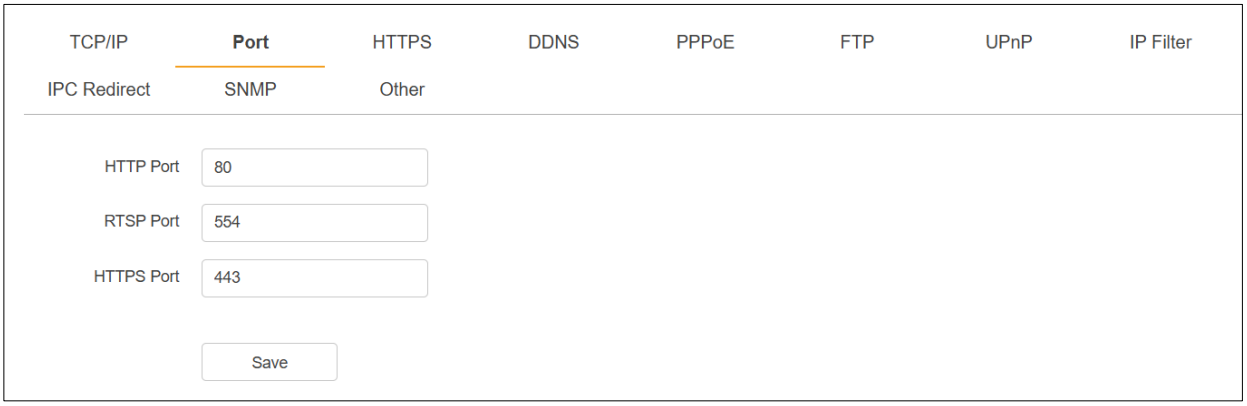


Figure 3-34 Port

Step 2 Configure the port parameters.

Parameter	Description
HTTP Port	Enter the HTTP port number for web access. The default value is 80. HTTP Port number can be configured within the range of 1025 and 65535.
RTSP Port	Change the RTSP port number for real-time video streaming. The default value is 554. If you want to use a different port, you can configure a port number within the range of 1025 to 65535.
HTTPS Port	Change the HTTPS port number for secure web access. The default value is 443. If you want to use a different port, you can configure a port number within the range of 1025 to 65535.

Table 3-9 Description of port parameters

Step 3 Click **Save** to save and apply all configured port parameters.

HTTPS

The HTTPS protocol is a network protocol constructed by combining the SSL and HTTP protocols, which can perform encrypted transmission and identity authentication, thereby improving the security of web access.

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

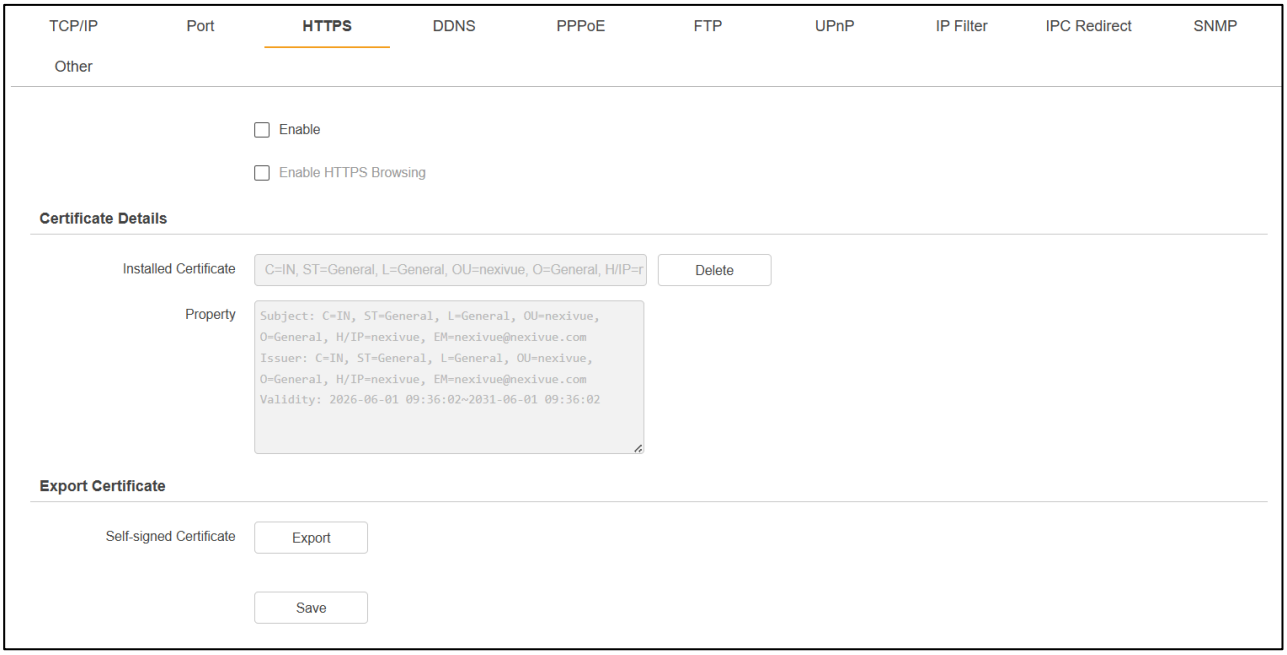


Figure 3-35 HTTPS

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.

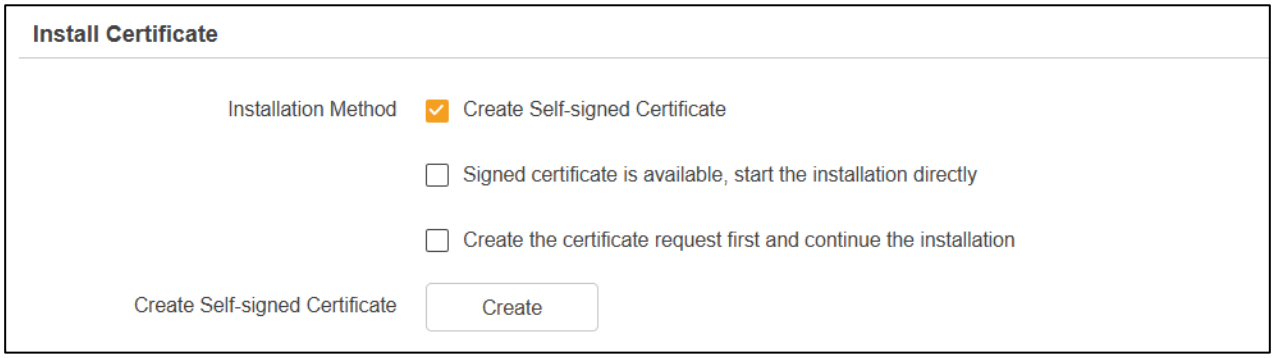


Figure 3-36 Install Certificate

- For creating a self-signed certificate:

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

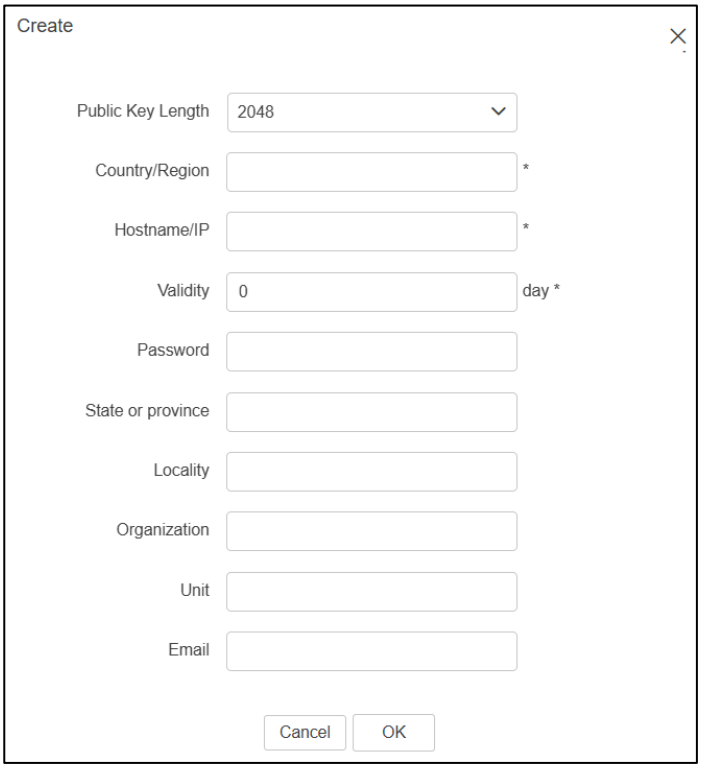


Figure 3-37 Create dialog box

  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 3-38 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 **Browse** to select the signed certificate key.

Step 4 Click **Install**, then click **Save**.

- For creating a certificate request:



Figure 3-39 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 **Browse** to select the signed certificate key.

Step 8 Click **Install**, then click **Save**.

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

DDNS

When the IP address of the Device changes frequently, the DDNS function can dynamically refresh the correspondence between the domain in DNS and the IP address. You can access the Device by using the domain.

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

- Check the type of DNS server supported by the device.
- 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 device must be connected to the Internet.

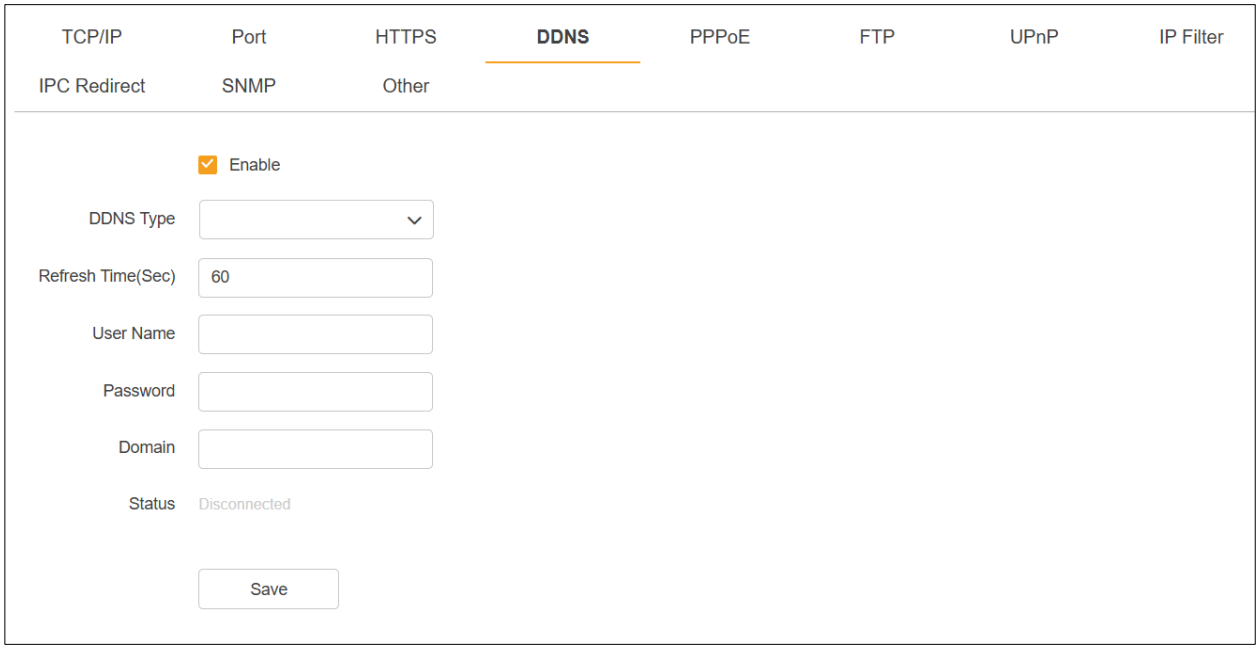


Figure 3-40 DDNS

Step 2 Enable the DDNS function 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 • DYN DDNS web address: members.dyndns.org
Refresh Time (Sec)	Enter the refresh time at which the device updates its IP address information to the DDNS server.

User Name Password	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.
Domain	Enter the domain name that you registered on the website of the DDNS Service Provider.
Status	Displays the current DDNS connection status (for example, login successful, failed, or disconnected).

Table 3-10 Description of DDNS parameters

Step 3 Click **Save** to save and apply all configured DDNS parameters.

PPPoE

PPPoE is another way for the Device to access the network. You can establish a network connection by configuring PPPoE settings to give the Device an IP address on the WAN.

Prerequisites

To use this function, first obtain the username and password from the Internet Service Provider.

Step 1 Navigate to **Settings** > **Network** > **Basic Settings** > **PPPoE**.

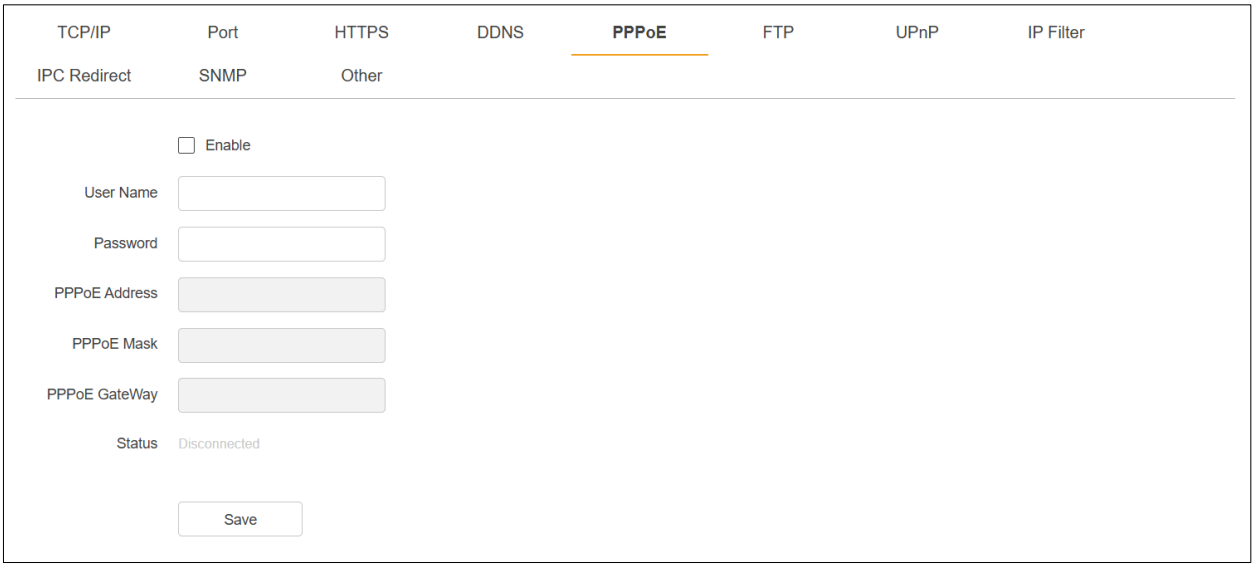


Figure 3-41 PPPoE

Step 2 Enable the PPPoE function and configure the parameters.

Parameter	Description
User Name	Enter the username provided by your Internet Service Provider (ISP)
Password	Enter the password associated with the PPPoE account.
PPPoE Address	Displays the IP address assigned through the PPPoE connection.
PPPoE Mask	Displays the subnet mask assigned for the PPPoE connection.
PPPoE Gateway	Displays the gateway address assigned through the PPPoE connection.
Status	Displays the current PPPoE connection status.

Table 3-11 Description of PPPoE parameters

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

- When the PPPoE function is enabled, the IP address on the TCP/IP page cannot be modified.

FTP

This section enables you to configure FTP/SFTP settings for uploading snapshots or alarm files to a remote server for storage and backup. FTP can be enabled only when it is selected as a destination path.

Prerequisites

Purchase or download an FTP (File Transfer Protocol) server and install it on your PC.

- For the created FTP user, you need to set the write permission; otherwise, the upload of captured snapshots will be failed.

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

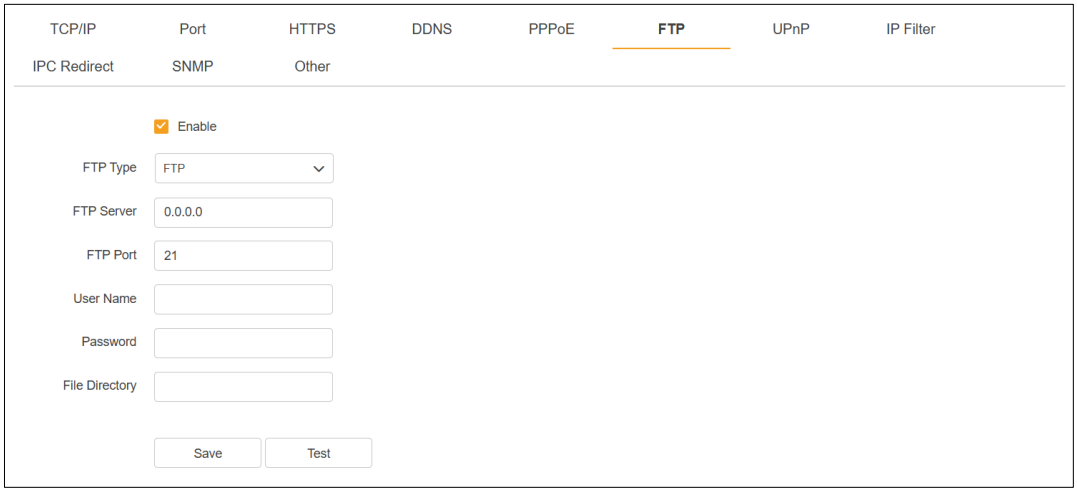


Figure 3-42 FTP

Step 2 Enable the FTP function and configure the FTP parameters.

Parameter	Description
FTP Type	Select FTP type. • FTP: Plaintext transmission. • SFTP: Encrypted transmission (recommended).
FTP Server	The IP address of the FTP/SFTP server where files will be uploaded.
FTP Port	Specifies the communication port number of the FTP/SFTP server. By default, the FTP port number is 21, and the SFTP port number is 22.
User Name	The username to log in to the FTP/SFTP server.
Password	The password to log in to the FTP/SFTP server.
File Directory	Create a folder on the FTP server. • If you do not enter the name of the remote directory, the system automatically creates the folders according to the IP and time. • If you enter the name of a remote directory, the system creates the folder with the entered name under the FTP root directory first, and then automatically creates the folders according to the IP and time.
Test	Verifies the connectivity between the device and the FTP/SFTP server.

Table 3-12 Description of FTP parameters

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

UPnP

You can map the relationship between the LAN and the WAN to access the Device on the LAN through the IP address on the WAN. After enabling UPnP, the Internet service port of the device will be mapped to the Extranet.

Step 1 Navigate to **Settings** > **Network** > **Basic Settings** > **UPnP**.

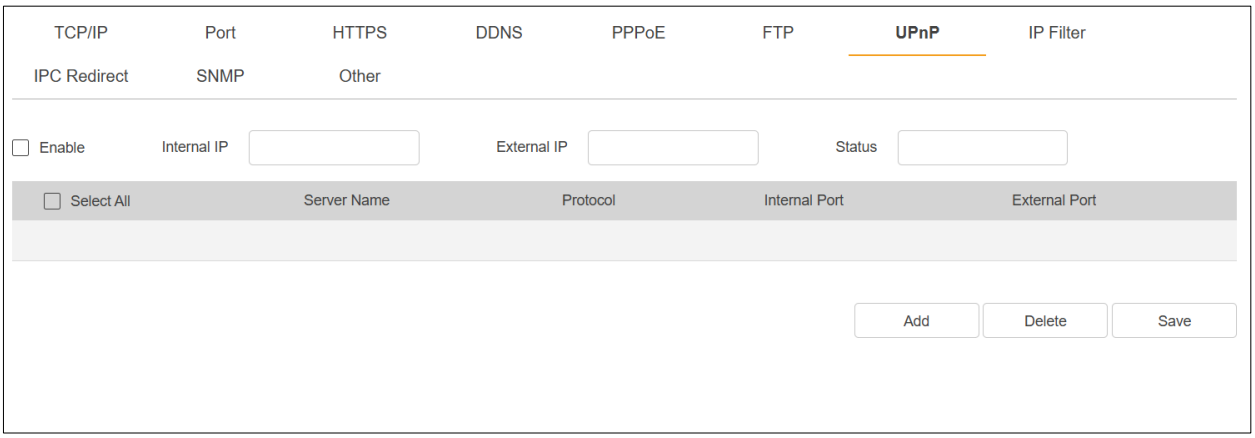


Figure 3-43 UPnP

Step 2 Enable the UPnP function.

Parameter	Description
Status	Indicates the status of the UPnP function. • Offline: Failed. • Online: Succeeded.
Internal IP	Enter the IP address of the router on the LAN. After mapping succeeds, the system obtains IP address automatically.
External IP	Enter the IP address of the router on the WAN. After mapping succeeds, the system obtains IP address automatically.

Table 3-13 Description of UPnP parameters

Step 3 Click **Add** to add port information.

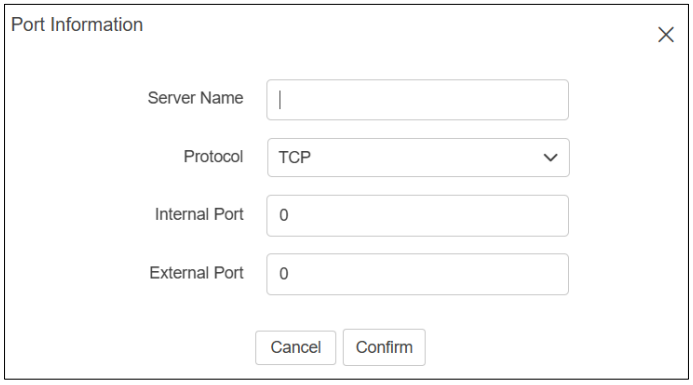


Figure 3-44 Port information

Parameter	Description
Server Name	Enter the server name to identify the port mapping entry. This can be any descriptive name (for example, HTTPS or FTP).
Protocol	Select the protocol to be used for communication.
Internal Port	Enter the internal port number of the device on the local network where the service is running.
External Port	Enter the external port number that will be accessible from the internet and mapped to the internal port.

Table 3-14 Description of port information parameters

Step 4 Click **Confirm** to add the port information.

IP Filter

You can configure the hosts that are allowed or prohibited from accessing the device.

Step 1 Navigate to **Settings** > **Network** > **Basic Settings** > **IP Filter**.

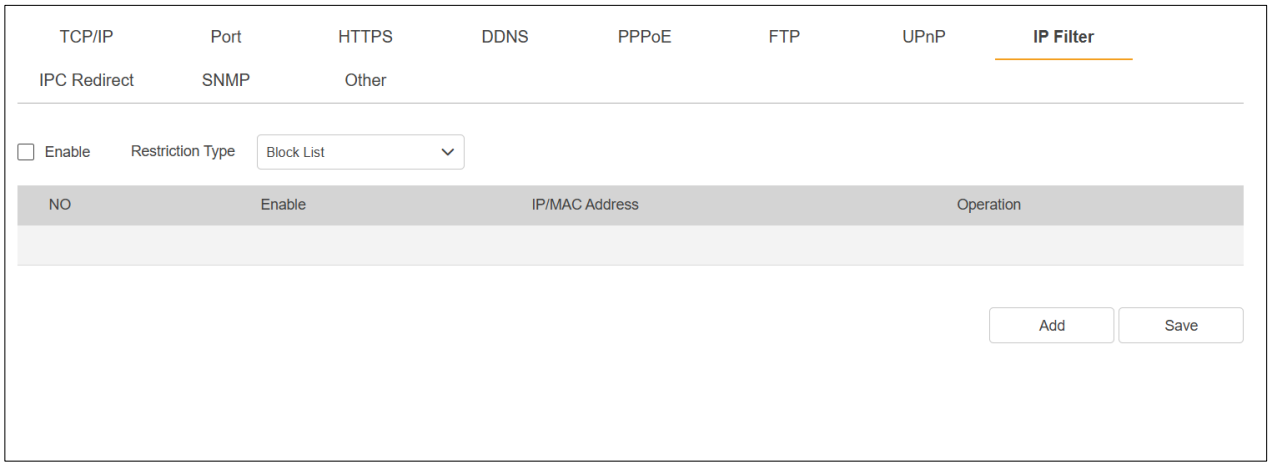


Figure 3-45 IP Filter

Step 2 Enable the IP Filter function.

Step 3 Select a restriction type.

- **Allow List**: The hosts on the allow list can access the Device.
- **Block List**: The hosts on the block list are prohibited from accessing the Device.

Step 4 Click **Add** and then select a type for the allowlist or blocklist.

You can allow or prohibit hosts through a specific IP address or a MAC address.

- **IP address:** Enter the IP address and then click **Save**.
- **MAC address:** Enter the MAC address, and then click **OK**.

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

IPC Redirect

IPC Redirect is a feature that allows the device to map and redirect ports for connected IP cameras, enabling remote web access and video streaming through assigned HTTP and RTSP ports.

Step 1 Navigate to **Settings** > **Network** > **Basic Settings** > **IPC Redirect**.

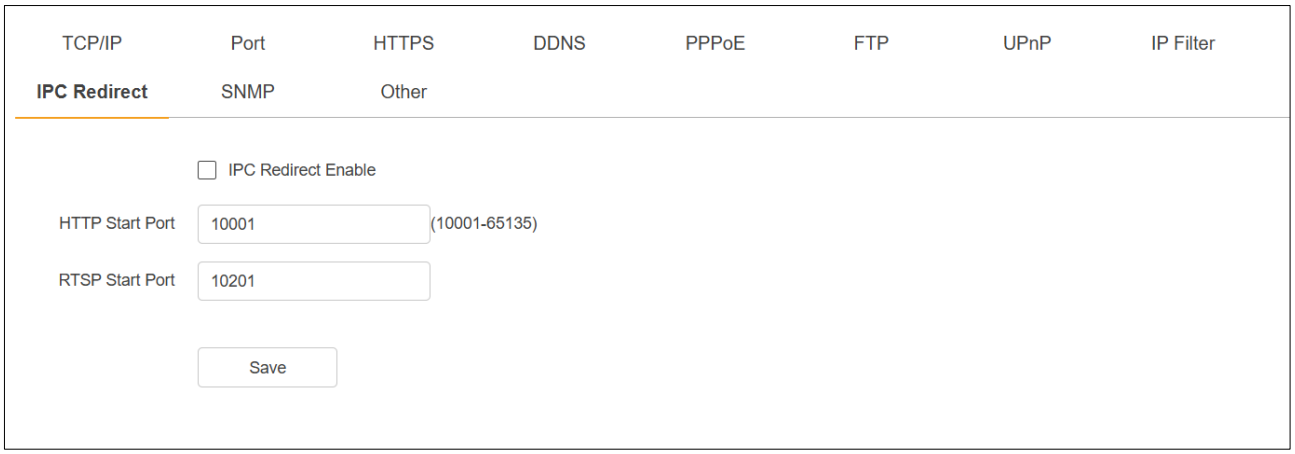


Figure 3-46 IPC redirect

Step 2 Enable the IPC Redirect function.

Step 3 Enter a valid **HTTP Start Port** number. The value ranges from 10001 to 65135.

Step 4 Enter a valid **RTSP Start Port** number.

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

SNMP

You can connect the Device to software to manage and control it.

Step 1 Navigate to **Settings** > **Network** > **Basic Settings** > **SNMP**.

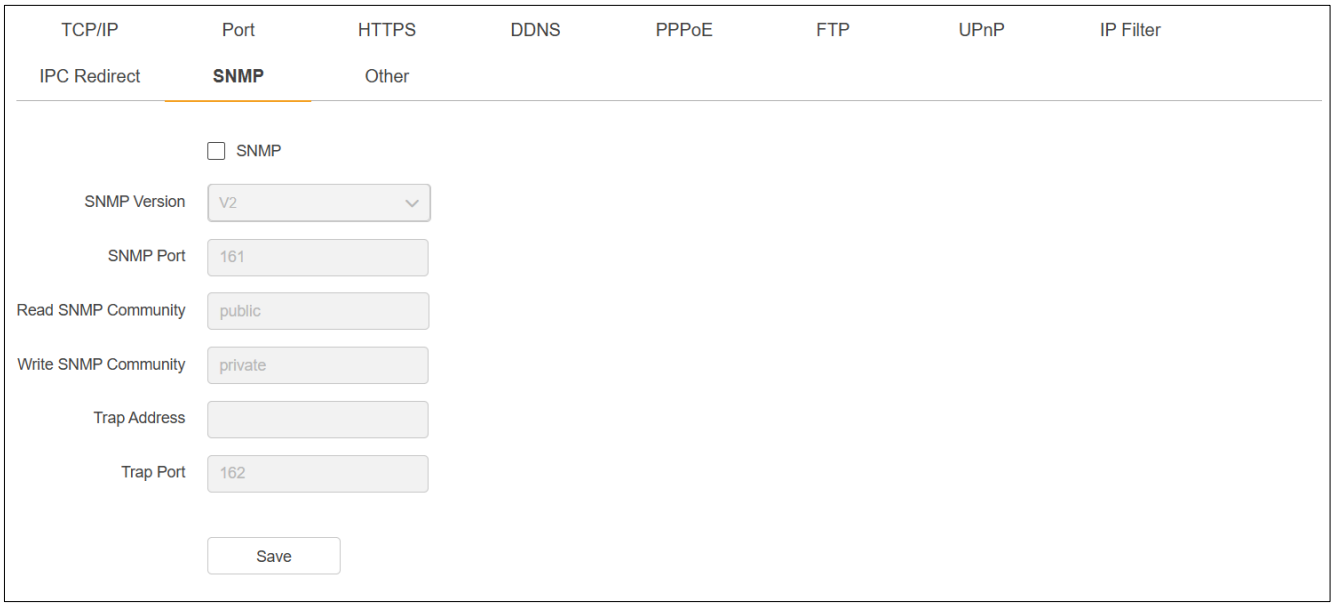


Figure 3-47 SNMP

Step 2 Enable the SNMP function.

Step 3 Configure the SNMP parameters.

Parameter	Description
SNMP Version	Select the SNMP version that you are using. The default version is V2.
SNMP Port	Enter the monitoring port on the agent program.
Read SNMP Community	Enter the read and write strings supported by the agent program.
Write SNMP Community	
Trap Address	Enter the destination address for the agent program to send the Trap information.
Trap Port	Enter the destination port for the agent program to send the Trap information.

Table 3-15 Description of SNMP parameters

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

Other

This section provides SSH configuration exclusively for debugging and diagnostic purposes. SSH access is restricted to authorized technical support personnel and is not available for general user operations.

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

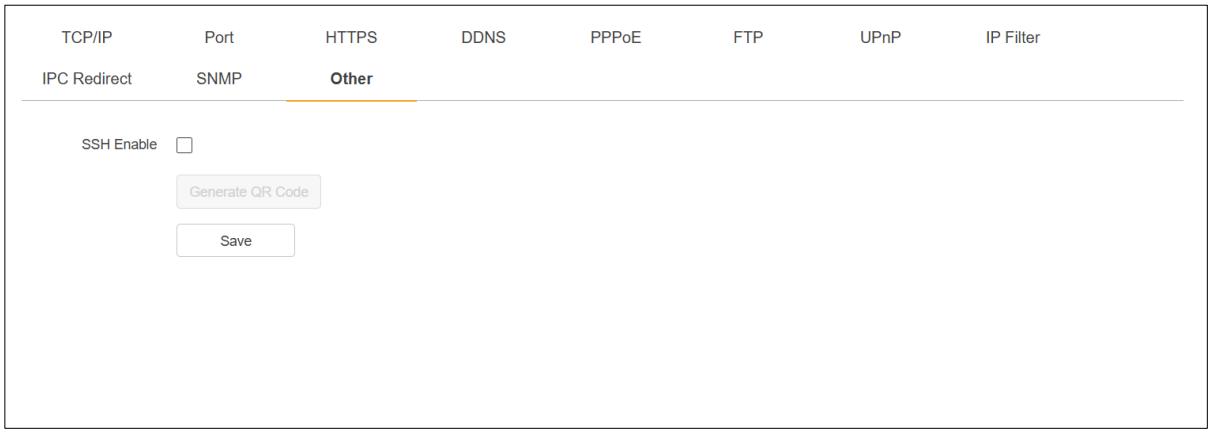


Figure 3-48 Other network services

Step 2 Enable the SSH function for advanced maintenance and troubleshooting, and click **Generate QR code**.

Step 3 Scan the generated QR code for quick and secure configuration or access to the device.

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

3.5.2.2 NexiQloud

NexiQloud allows you to access your device remotely in a secure way. Activating NexiQloud will synchronize all your device information, such as Device Model Number, Device Serial Number, MAC Address, and IP address, to the NexiQloud server.

- Before using the NexiQloud function, make sure the NVR is connected to the WAN.
- All the information collected will only be used to make your device accessible remotely.

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

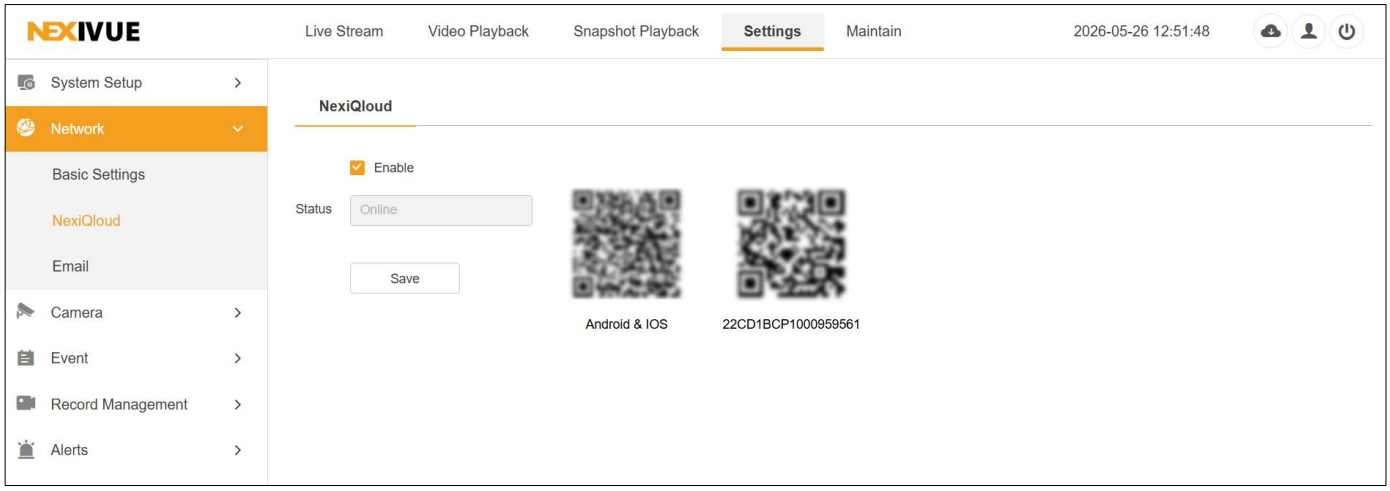


Figure 3-49 NexiQloud

Step 2 Enable the NexiQloud function.

- After you enable the NexiQloud function and connect to the Internet, the system will collect information such as your email address and MAC address for remote access.

Step 3 Click **Save** to save the changes.

The NexiQloud function is enabled. You can use your phone to scan the QR code under Android & IOS to download and install the mobile client. After that, you can use the mobile client to scan the QR code under NexiQloud ID to add the Device for remote management.

3.5.2.3 Email

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

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

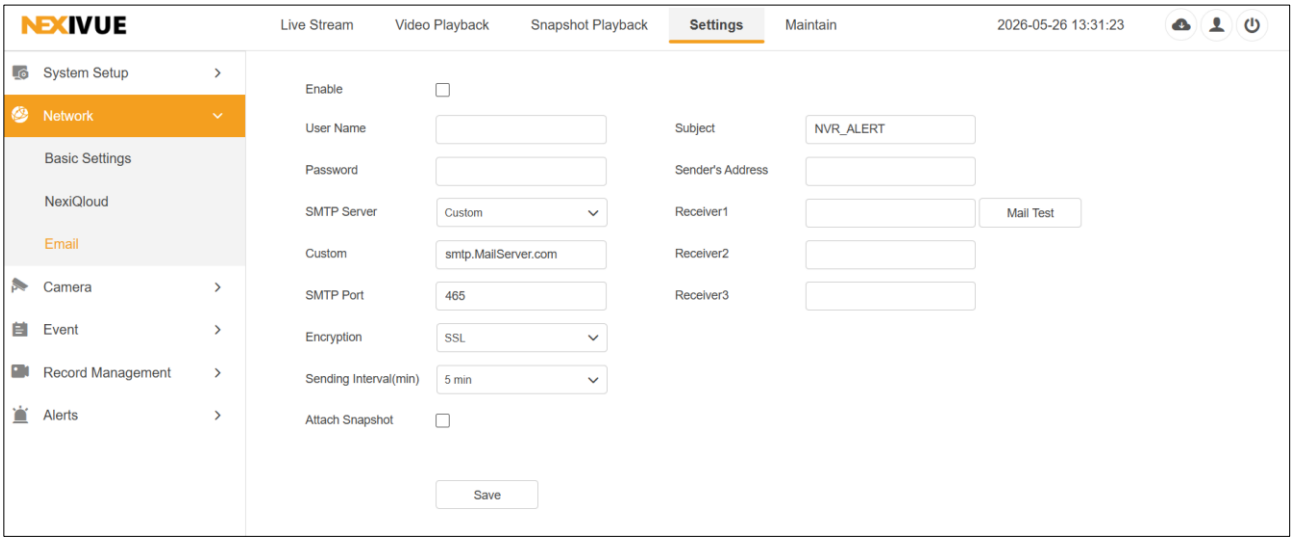


Figure 3-50 Email

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

Step 3 Configure the email parameters.

Parameter	Description
User Name	Username for SMTP server authentication, usually the sender's email address.
Password	Password corresponding to the SMTP user account.
SMTP Server	Select the address of the SMTP server of the sender's email account.
Custom	Enter the custom address of the SMTP server of the sender's email account. You need to select **SMTP Server** as **Custom** to add the custom address.
SMTP Port	Enter the port of the SMTP server. The default value is 465.
Encryption	Select the encryption type from NONE, SSL, TLS, or STARTTLS. For the SMTP server, the default encryption type is SSL.
Sending Interval (min)	Set the interval at which the system sends an email for the same type of alarm event to avoid excessive pileup of emails caused by frequent alarm events. The value ranges from 1 to 30 minutes.
Subject	Enter the email subject.
Sender's Address	Email address used by the device to send notification emails.
Receiver's Address 1	Email address to receive alarm or event notifications.

Receiver's Address 2	
Receiver's Address 3	
Mail Test	Sends a test email to verify the email configuration.
Attach Snapshot	Enable the attach snapshot function. When there is an alarm event, the system can attach snapshots as an attachment to the email.

Table 3-16 Description of email parameters

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

3.5.3 Camera

This section provides comprehensive camera configuration options, including camera management, stream type selection, video encoding settings, OSD customization, image parameter adjustment, and privacy mask configuration.

3.5.3.1 Camera Management

This page allows you to search, add, and manage IP cameras connected to the system. You can view device details, configure connection settings, and monitor the status of each added camera from this section.

Adding Cameras

Add remote devices to the NVR to receive, store, and manage the video streams of the remote devices.



- Before adding the remote devices, make sure that the devices have been initialized.

Adding Cameras from Search

Search for remote cameras on the same network as the device and then add the remote cameras from the search results.

Step 1 Navigate to **Settings** > **Camera** > **Camera Management**.

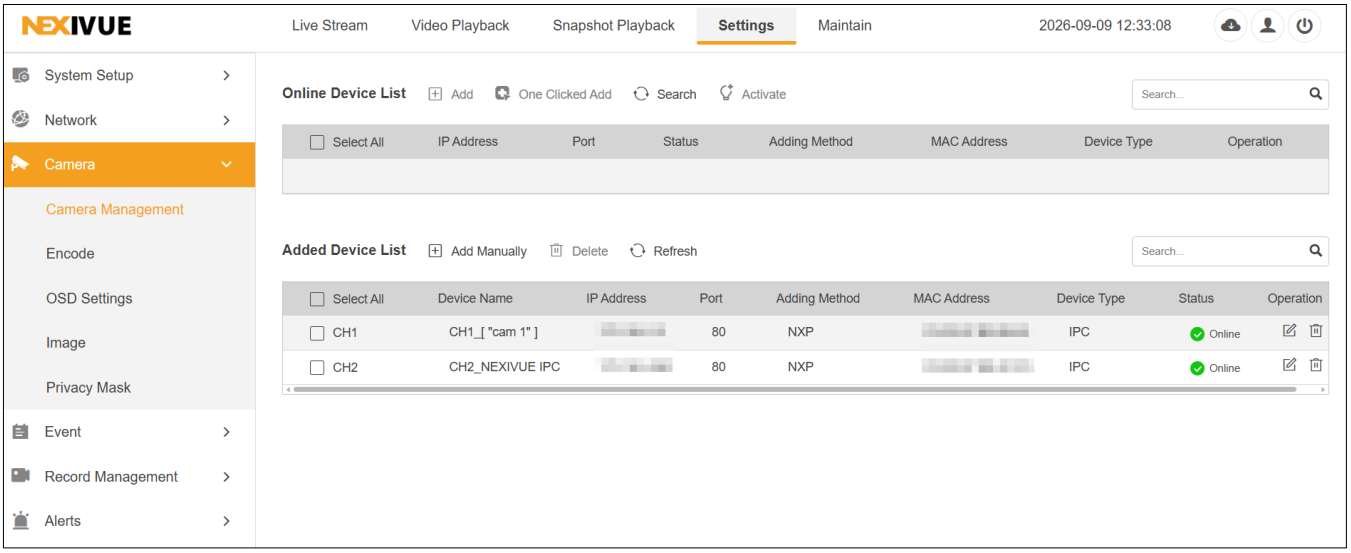


Figure 3-51 Camera Management

Step 2 Click **Search**.

The remote devices found are displayed under the **Online Device List**. Devices already added are not included in the search results.

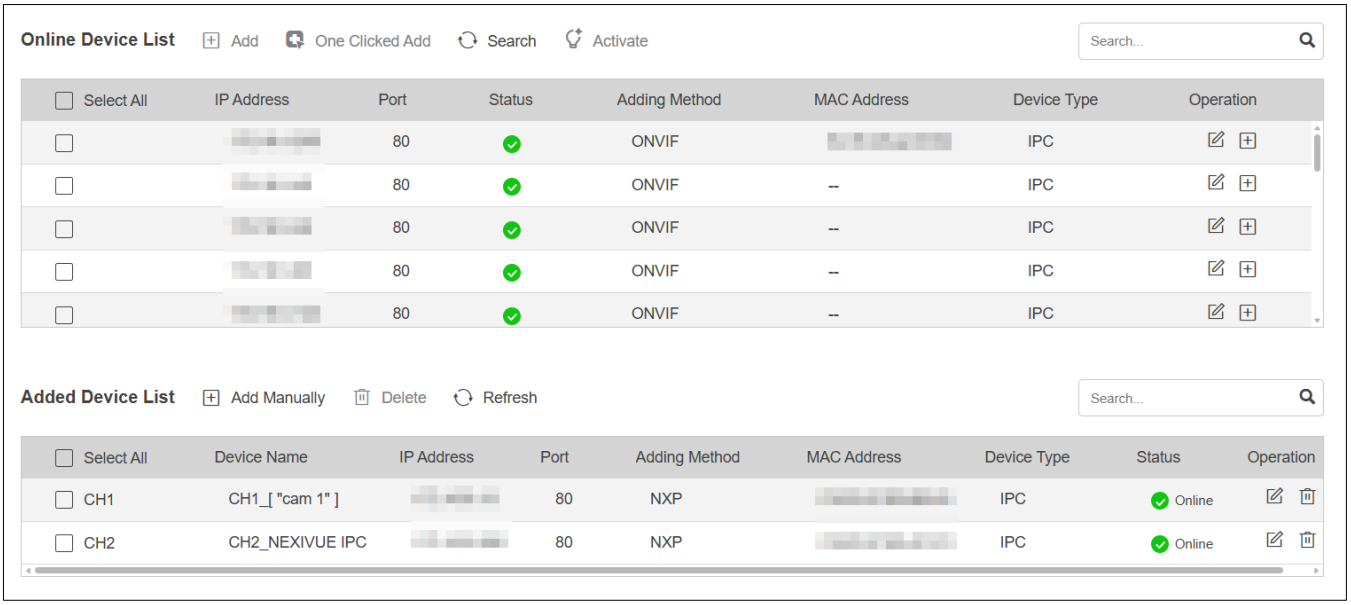


Figure 3-52 Search device

- To filter the remote devices, you can enter all or part of the device name in the **Search** box.

Step 3 Click ⊞ icon for the device you want to register to the **Added Device** list.

Related Operations

- Edit camera information.
  - On the **Online Device** list, click to change the IP address, username, password and other information.
- Add cameras in batches
  - Select one or more cameras, and then click **Add** to add the cameras.
- Delete cameras.
  - Delete one by one.
    - Click to delete the corresponding camera.
  - Delete in batches.
    - Select one or more cameras, and then click **Delete**.

Adding Cameras Manually

Background Information

Configure the IP address, username, password and other information of the remote device manually and add it to the NVR.

- We recommend this method when you want to add only a few remote devices and know their IP addresses, usernames and passwords.

Step 1 On the home page, navigate to **Settings** > **Camera** > **Camera Management**.

Step 2 Click **Add Manually**.

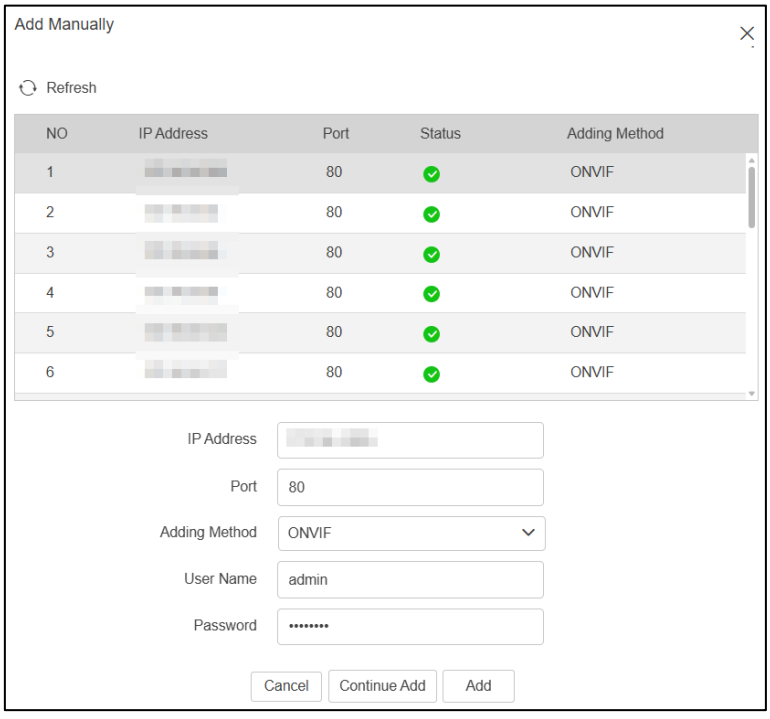


Figure 3-53 Add manually

Step 3 Click **Refresh** to search and display the available cameras on the network.

Step 4 Select the camera that you want to add to the device.

- If the camera is not available in the search results, manually enter its details to add it to the device.

Step 5 Verify the **IP Address** and **Port** number of the remote device.

Step 6 Select the **Adding Method** from the drop-down list (for example, NXP, ONVIF, or RTSP).

Step 7 Enter the username of the remote device.

Step 8 Enter the corresponding Password.

Step 9 Click **Add** to add the selected camera to the device.

Step 10 (Optional) Click **Continue Add** to add multiple cameras one after another.

Initializing Cameras

This section allows you to initialize the detected network devices via the NVR.

- You can activate multiple uninitialized cameras simultaneously.

Step 1 Navigate to **Settings** > **Camera** > **Camera Management**.

Step 2 Under the **Online Device List** tab, select the device with the status of **Not Activate** and click **Activate**.

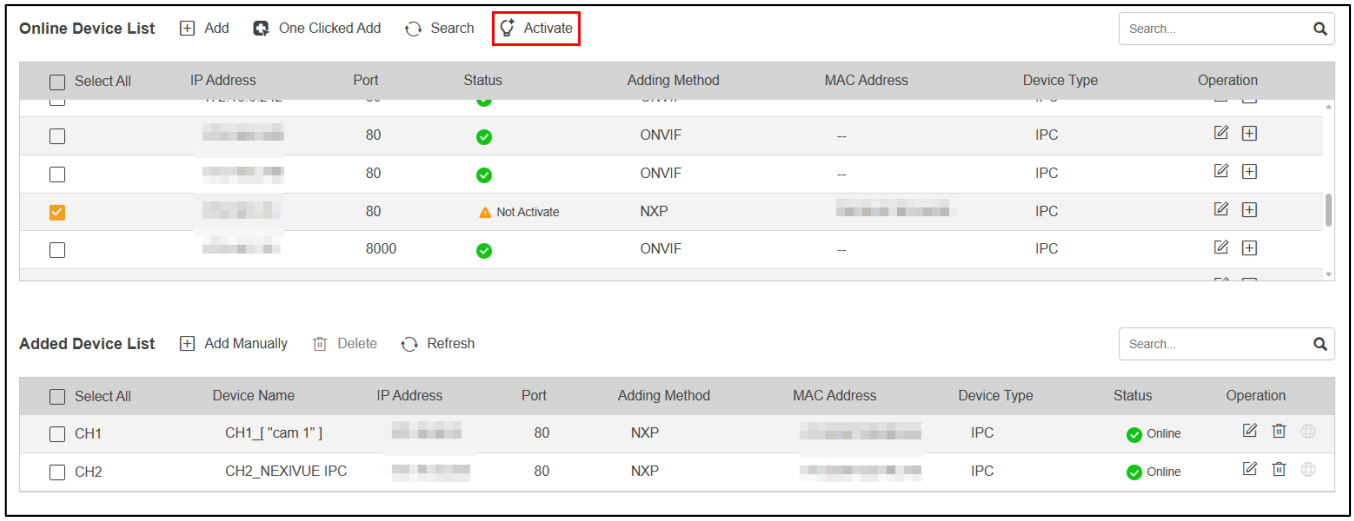


Figure 3-54 Activate

Step 3 Click **Confirm** to synchronize the NVR administrator password, security questions, and phone number to the camera.

The device is activated successfully.

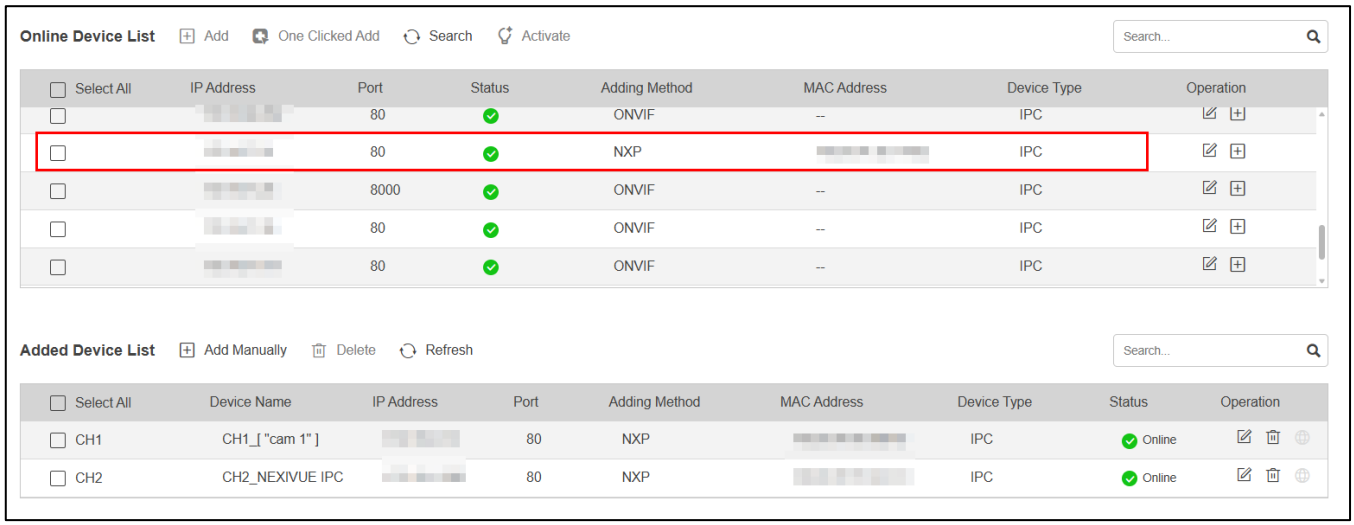


Figure 3-55 Activated device

Modifying the IP Address of a Detected Network Device

This section includes the process of editing the IP address of detected network devices.

Step 1 Navigate to **Settings > Camera > Camera Management**.

Step 2 Under the **Online Device List** tab, click on  for the active camera whose IP address you want to modify.

Step 3 Enter the network device username and password, then configure the IP address.



Figure 3-56 Edit IP address

Step 4 Click **Confirm** to save the changes.

Changing the Device for a Particular Channel

This section covers the process of replacing or updating the device for a designated channel.

Step 1 Navigate to **Settings > Camera > Camera Management**.

Step 2 Under the **Added Device List** tab, click on for the active camera.

Step 3 Replace the IP address, port number, username, and password of the new device that you want to add to that channel.

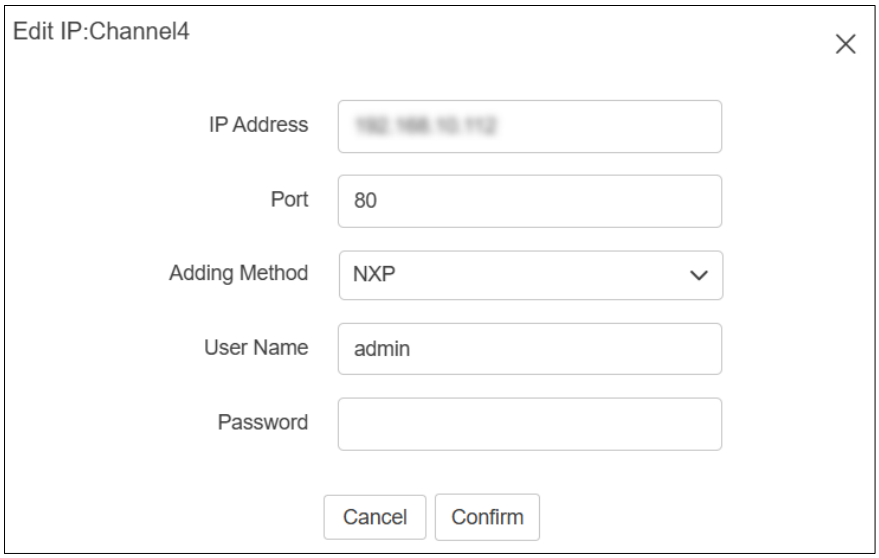


Figure 3-57 Change the device details for a particular channel

Step 4 Click **Confirm** to save the changes.

3.5.3.2 Encode

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

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

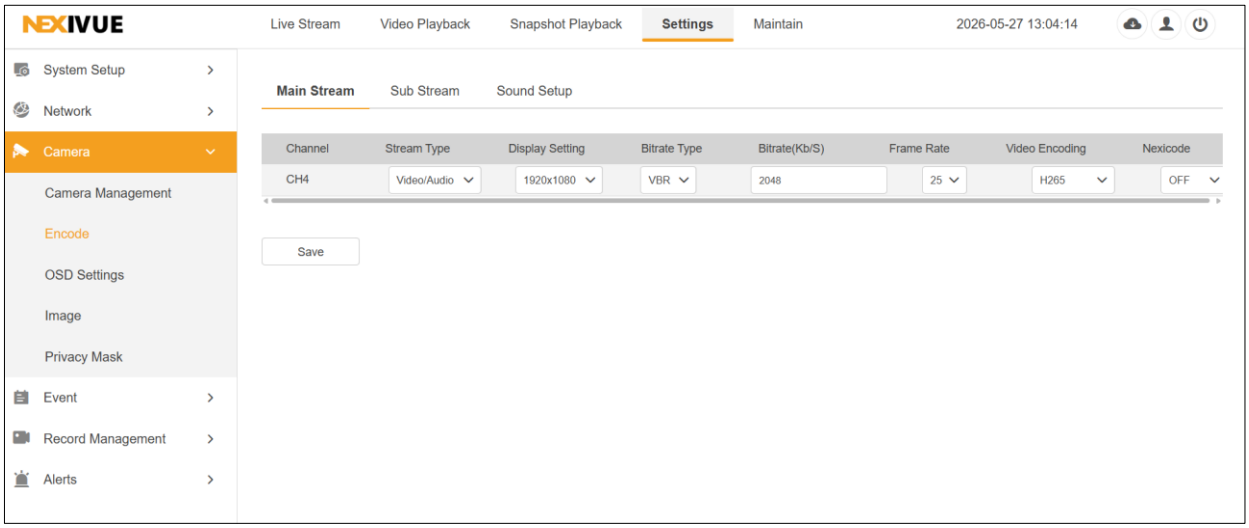


Figure 3-58 Encode

Step 2 Configure the encoding settings as required for both mainstream and sub-stream video quality, bandwidth, and storage.

- The parameters for the mainstream and the sub stream will differ.

Parameter	Description
Stream Type	Select the video stream type: • **Video/Audio:** Transmit both video and audio streams from the camera, allowing live viewing and recording with sound. • **Video:** Transmit only the video stream from the camera, without audio. This option reduces bandwidth and storage usage when audio recording is not required.
Display Setting	Sets the output video resolution; higher resolution provides clearer images but uses more bandwidth.
Bitrate Type	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**.
Bit Rate (Kb/S)	Specifies the amount of data used for video transmission; a higher bit rate improves quality but increases bandwidth usage.
Frame Rate	Configure the frames per second for the video. The higher the value is, the clearer and smoother the image will become.
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.
Nexicode	Enables or disables advanced encoding optimization to improve compression efficiency when supported.

Table 3-17 Description of encoding parameters

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

Sound Setup

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

Step 1 Navigate to **Settings** > **Camera > Encode** > **Sound Setup**.

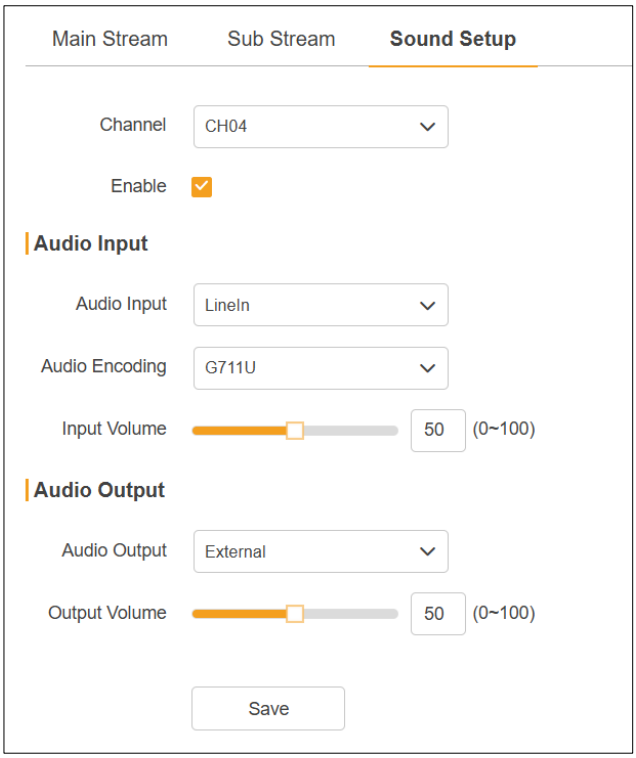


Figure 3-59 Sound Setup

Step 2 Select the channel for which you want to configure the audio settings.

Step 3 Enable the sound setup function.

Step 4 Configure the audio settings based on the connected audio devices and required audio quality.

Parameter	Description
Audio Input	Selects the audio input source. By default, **LineIn** is selected for external audio input devices.
Audio Encoding	Defines 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. • To get recorded files with audio from the Nexivue IPC, set the audio compression format to **AAC** in the IPC audio settings. Play the recorded files using **Windows Media Player** for proper audio playback.
Input Volume	The gain control value of the audio input source; the user can adjust 0-100 according to the actual volume demand.
Audio Output	Selects 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 0-100 according to the actual volume demand.

Table 3-18 Description of sound setup parameters

3.5.3.3 OSD Settings

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 set the OSD on the live screen to the position you want (top left or 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** > **Camera** > **OSD Settings**.

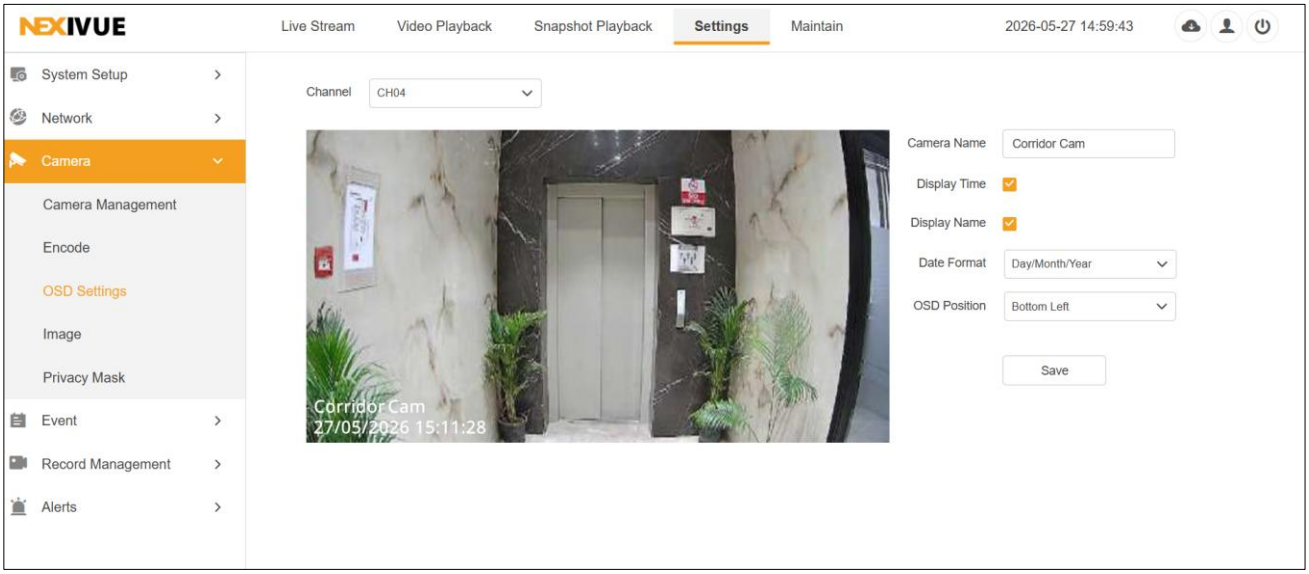


Figure 3-60 OSD settings

Step 2 Select the channel and configure OSD parameters as per requirements.

Parameter	Description
Camera Name	Edit the camera name as per the requirement.
Display Time	Enable or disable the display of the current date and time on the video.
Display Name	Enable or disable the display of the camera name on the video.
Date Format	Sets the format of the displayed date. Options include **Date/Month/Year**, **Month/Date/Year**, and **Year/Month/Date**.
OSD Position	Selects the position of the OSD on the video. Options include **Bottom Left** and **Top Left**.

Table 3-19 Description of OSD parameters

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

3.5.3.4 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** > **Camera** > **Image**.

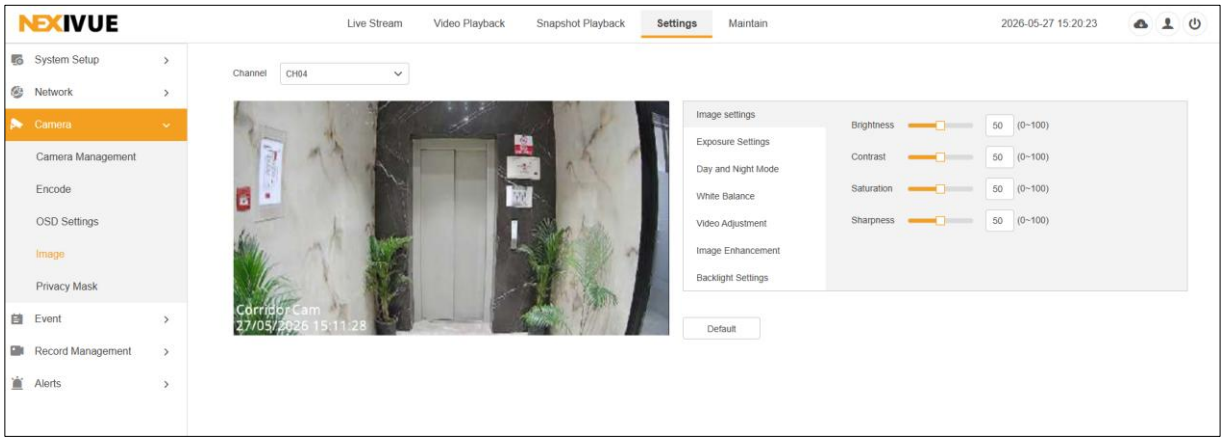


Figure 3-61 Image settings

Step 2 Select the required channel from the channel dropdown list.

Step 3 Configure different image controls as per the requirements.

Image settings

You can configure the image adjustment parameters as needed.

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

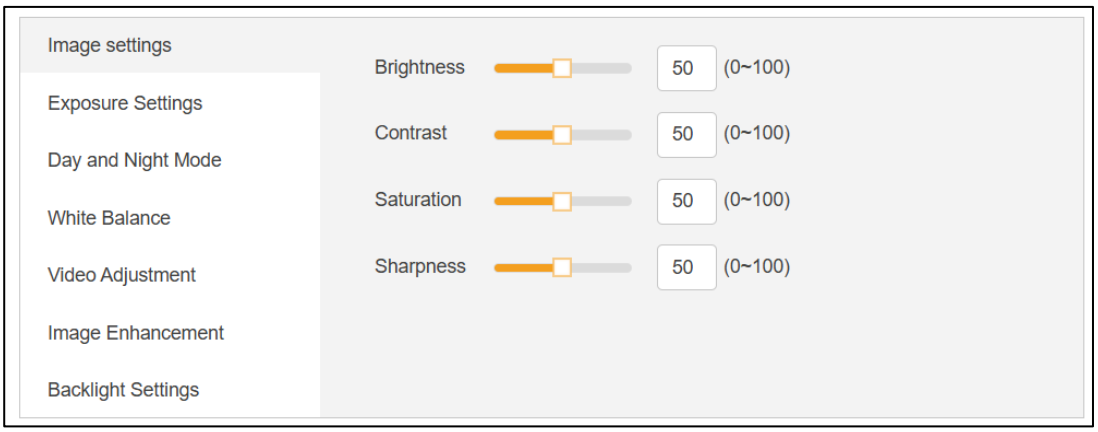


Figure 3-62 Image settings

Step 2 Configure image setting 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, the greater the contrast between bright and dark areas; the lower the value, the less contrast there is. If the value is set too high, the dark areas would be too dark, and the bright areas would be more likely to overexpose. The picture might be hazy if the value is set too small.
Saturation	Makes the color deeper or lighter. The higher the value, the deeper the color will be, and the lower the value, the lighter the color will be.
Sharpness	Changes the sharpness of picture edges. The higher the value, the clearer the picture edges will be; if the value is set too high, picture noise is more likely to appear.

Table 3-20 Description of image setting parameters

Exposure Settings

You can configure the exposure parameters as needed.

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

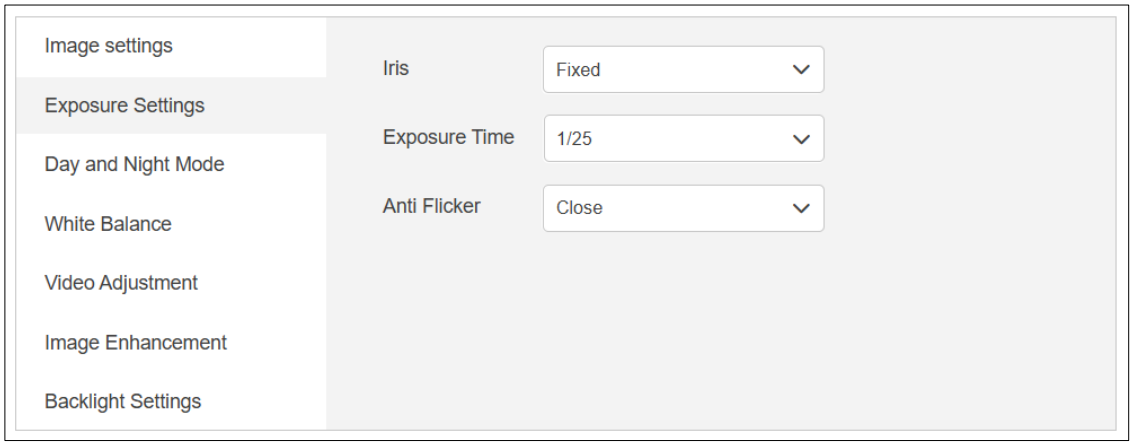


Figure 3-63 Exposure settings

Step 2 Configure the exposure setting parameters as needed.

Parameter	Description
Iris	The iris value is set to a fixed value, and the device adjusts the shutter value then. If the image brightness is insufficient and the shutter value has reached its upper or lower limit, the system automatically adjusts the gain to ensure the image is at an ideal brightness.
Exposure Time	The camera's 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 close. 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 3-21 Description of exposure settings

Day and Night Mode

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

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

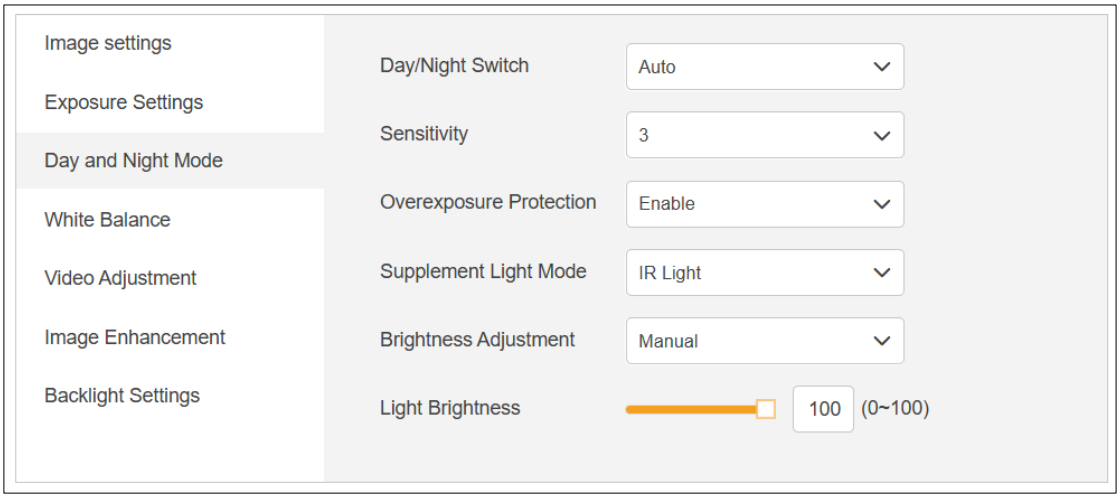


Figure 3-64 Day and Night Mode

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

Parameter	Description
Day/Night Switch	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 switch the supplement lighting mode for a specified period. Configure the Start Time and End Time to define the active duration. During this period, the camera operates in the selected supplement light mode, such as **IR Light**, **White Light**, or **Intelligent** mode. Outside the specified time range, the camera automatically reverts to its default lighting 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.
Overexposure Protection	Enable or disable protection against excessive light exposure to improve image visibility in bright areas.
Supplement Light Mode	You can select **IR Light**, **White Light**, and **Intelligent,** depending on the camera; light mode options will vary accordingly.
Brightness Adjustment	Choose whether the brightness level is adjusted automatically or manually. • **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 3-22 Description of day and night parameters

White Balance

You can configure the white balance parameters as needed.

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

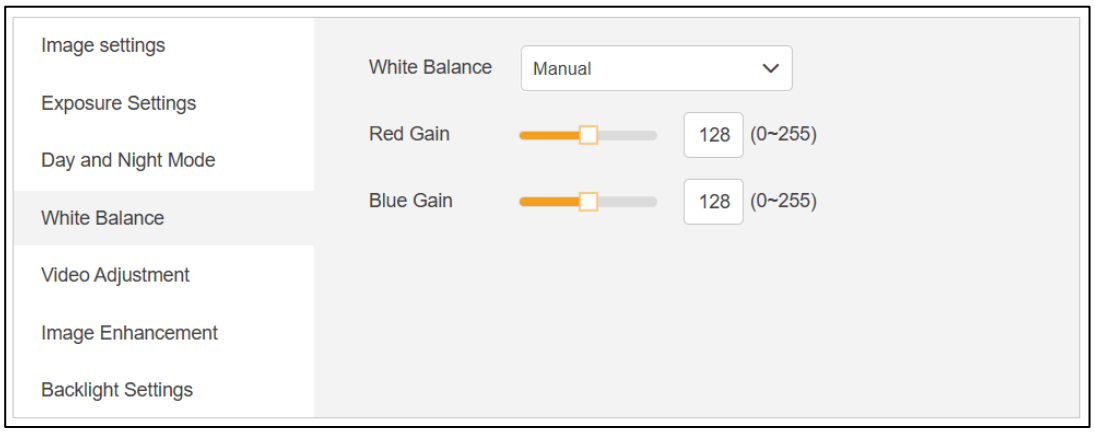


Figure 3-65 White balance

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, corridor mode, and video format.

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

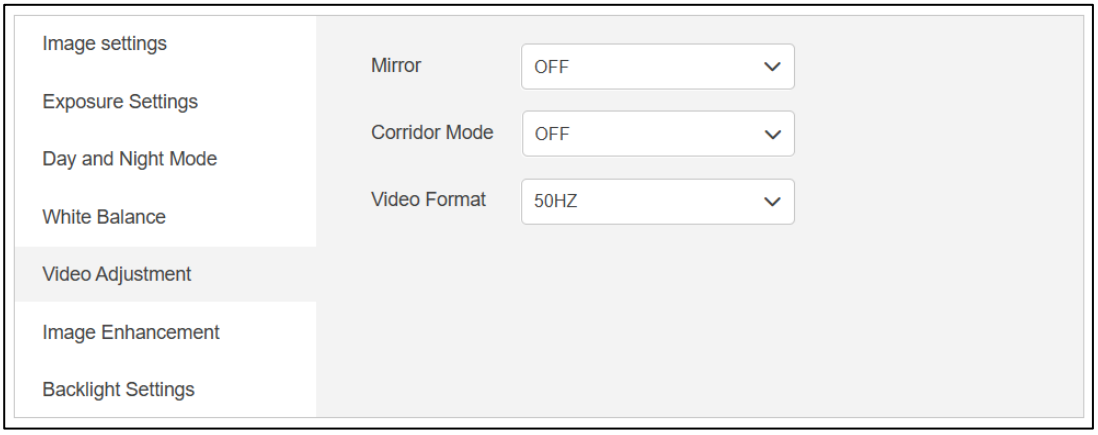


Figure 3-66 Video Adjustment

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.
Corridor Mode	Select **OFF**, **90°**, 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 no stripes appear. • **60HZ:** When the electric supply is 60HZ, the system adjusts the exposure according to ambient light automatically to ensure that no stripes appear.

Table 3-23 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** > **Camera** > **Image** > **Image Enhancement**.

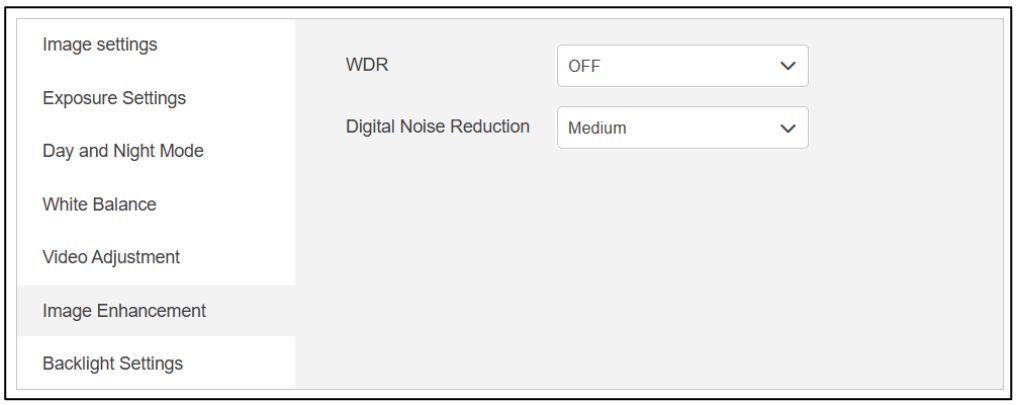


Figure 3-67 Image Enhancement

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 3-24 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** > **Camera** > **Image** > **Backlight Settings**.

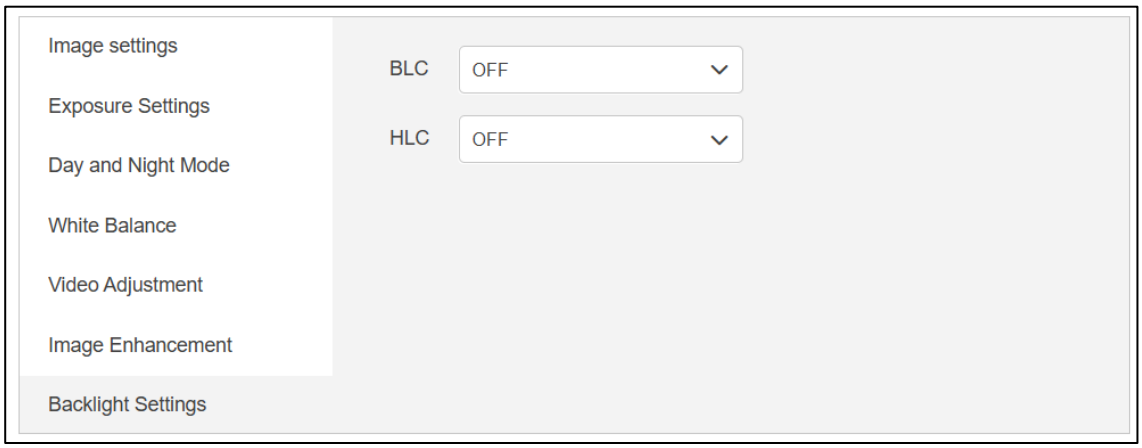


Figure 3-68 Backlight Settings

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 **HLC Intensity** and **Dark Area Boost Strength** by dragging the progress bar as per the requirement. The value ranges from 0 to 255.

Table 3-25 Description of backlight setting parameters

3.5.3.5 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** > **Camera** > **Privacy Mask**.

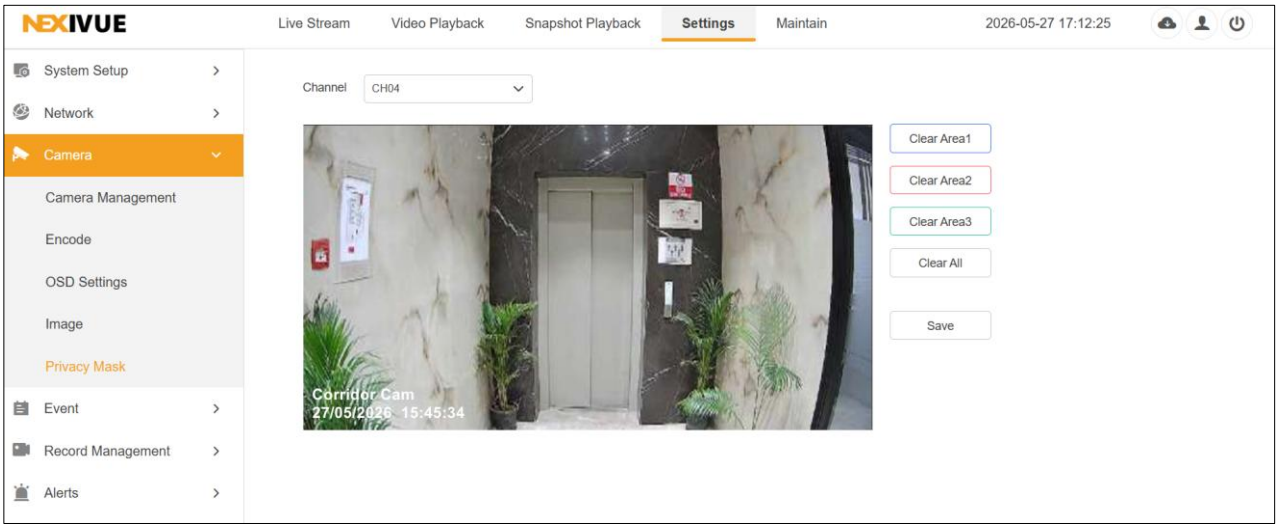


Figure 3-69 Privacy masking

Step 2 Select the required channel from the channel dropdown list.

Step 3 Hold the left mouse button and drag it to select the area. You can choose up to three blocking areas here.

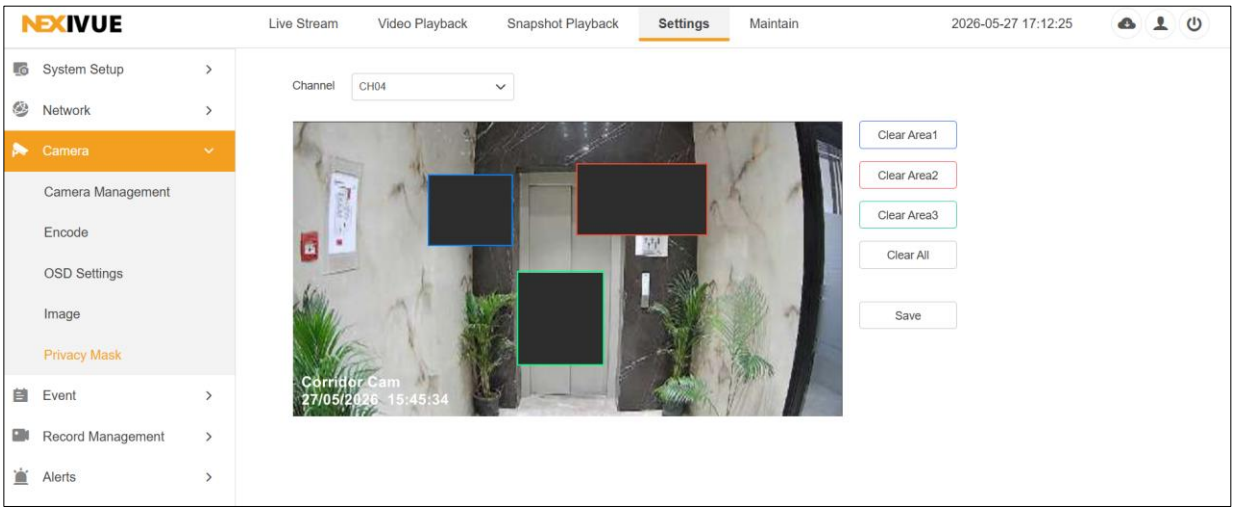


Figure 3-70 Privacy masking regions

Step 4 Click **Clear Area1**, **Clear Area2**, or **Clear Area3** to delete the respective blocking area.

Step 5 (Optional) Click **Clear All** to delete all the blocking areas.

Step 6 Click **Save** after completing the settings.

3.5.4 Event

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

3.5.4.1 Normal Event

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** > **Normal Event > Motion**.

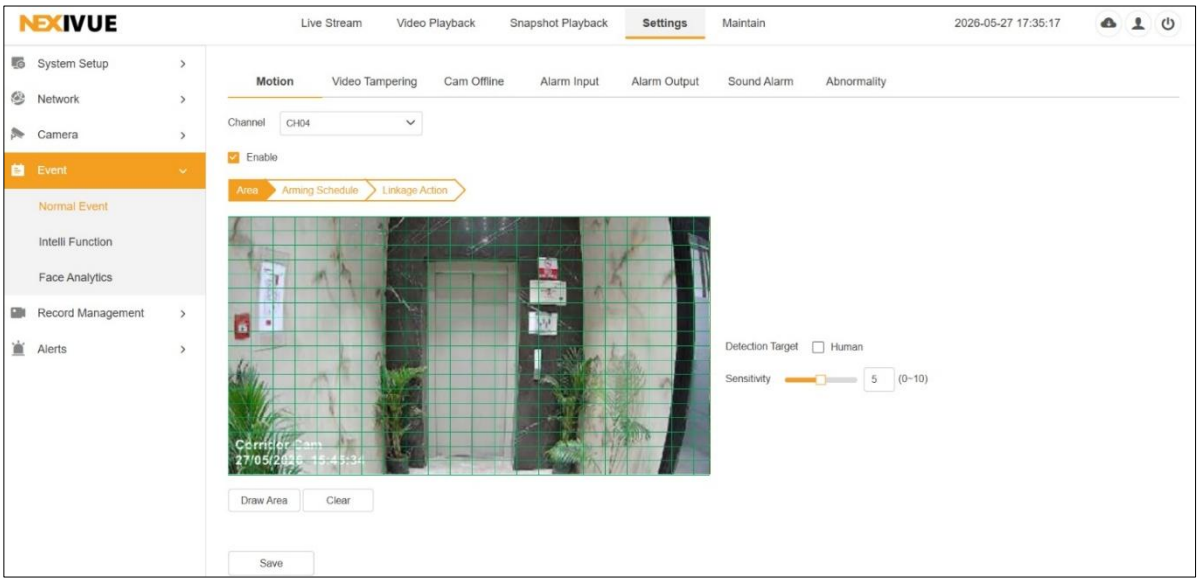


Figure 3-71 Motion detection

Step 2 Select the required channel from the channel dropdown list.

Step 3 Enable the motion detection function.

Step 4 (Optional) Enable **Human** to reduce false alarms caused by non-human motion.

Step 5 Select the area and set the sensitivity of motion detection.

- Set the area for motion detection.
  - Click **Draw Area** and move the mouse to the live screen, click the left mouse button to select the area range of motion detection, and release the left mouse button to complete the area drawing. Again, click **Draw Area** to exit drawing mode.
  - Click **Clear** 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 6 Set arming schedule.

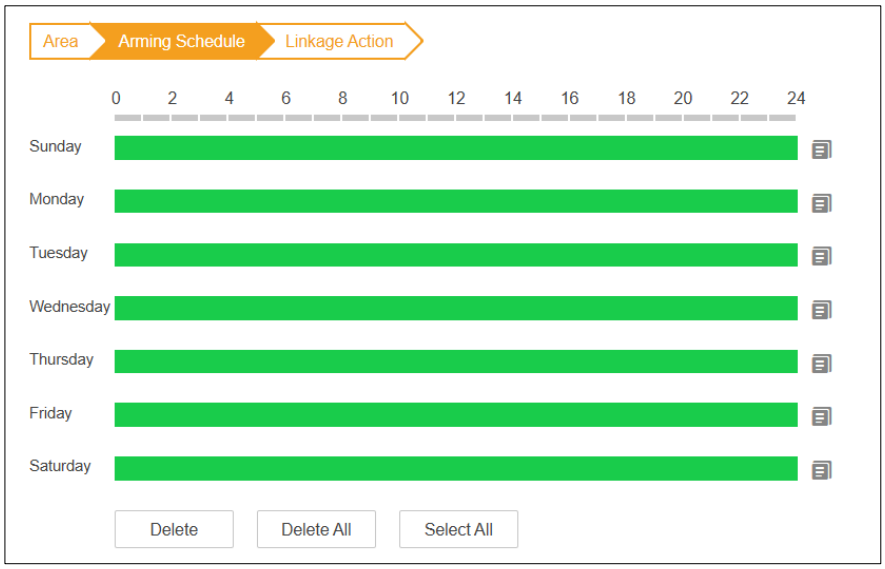


Figure 3-72 Arming schedule

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 want to delete the time period, click **Delete** button to reset the time 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 7 Set the linkage method.

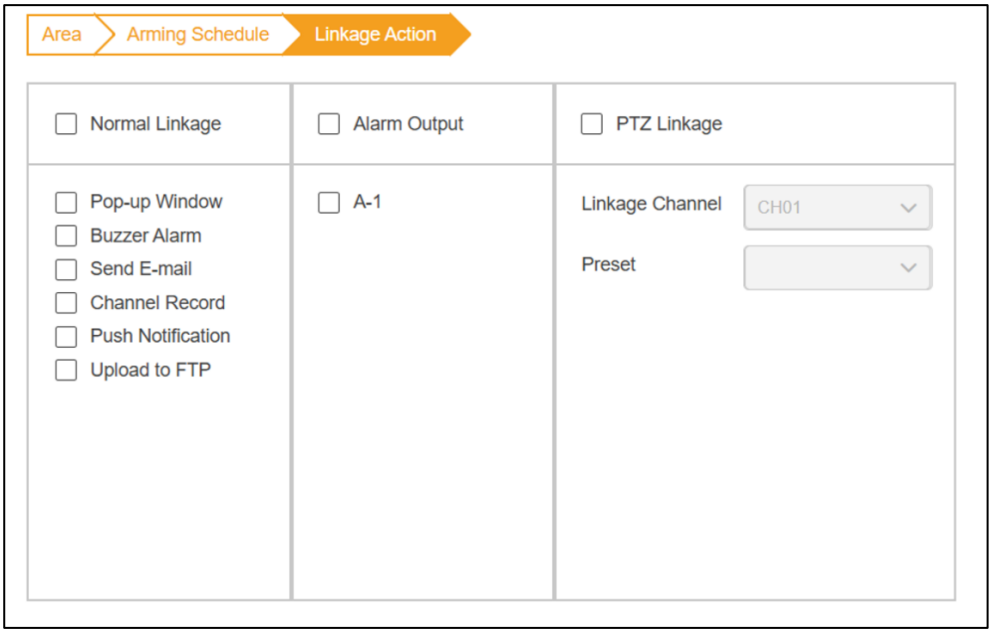


Figure 3-73 Linkage method

- 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	Configure the linkage actions to be triggered when an event occurs. • **Pop-up Window**: Display a pop-up window on the monitor screen. • **Buzzer Alarm**: Activate the device buzzer during the event. • **Send E-mail**: Send an email notification for the event. • **Channel Record**: Start recording on the selected channel. • **Push Notification**: Send a notification to the connected mobile application. • **Upload to FTP**: Upload snapshots to the configured FTP server.
Alarm Output	Configure the alarm output action for the event. **A-1**: Activate the selected alarm output channel during the event.
PTZ Linkage	Configure PTZ actions to be triggered during the event. • **Linkage Channel**: Select the PTZ camera channel for linkage action. • **Preset**: Select the preset position to which the PTZ camera will move when the event is triggered.

Table 3-26 Description of linkage method parameters

- Click **Save** to save the configured 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 to **Settings** > **Event** > **Normal Event** > **Video Tampering**.

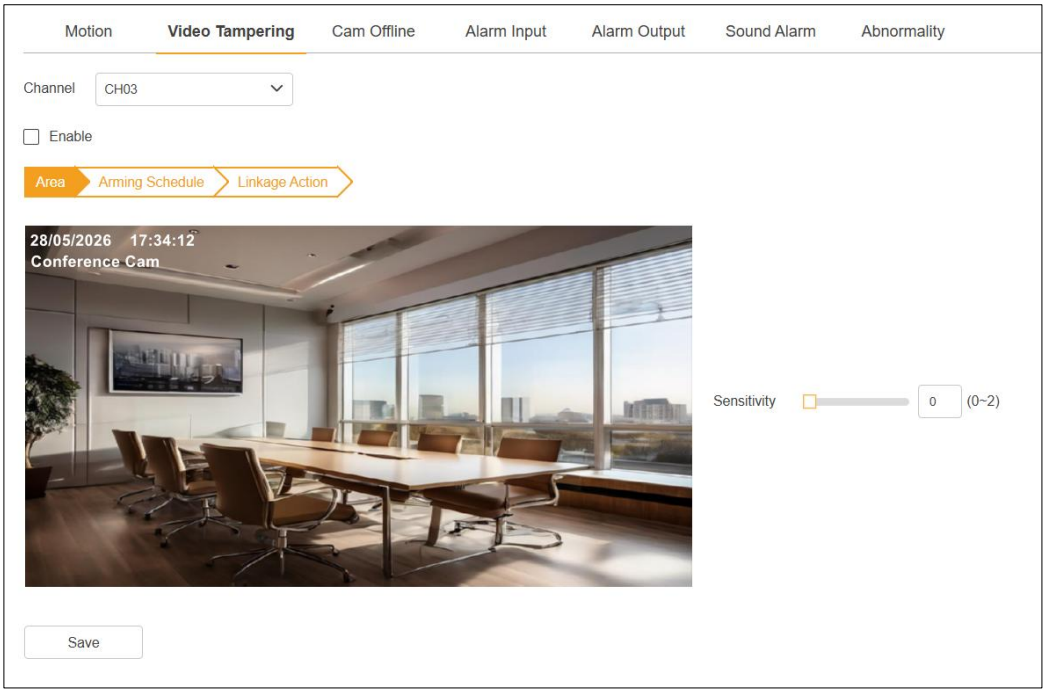


Figure 3-74 Video tampering

Step 2 Select the required channel from the channel dropdown list.

Step 3 Enable the video tampering function.

Step 4 Set the sensitivity of the video tampering and click **Save** to complete the setting.

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

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

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

Cam Offline

You can configure event detection and linkage actions when a camera disconnects or loses communication with the NVR.

Step 1 Navigate to **Settings** > **Event** > **Normal Event** > **Cam Offline**.

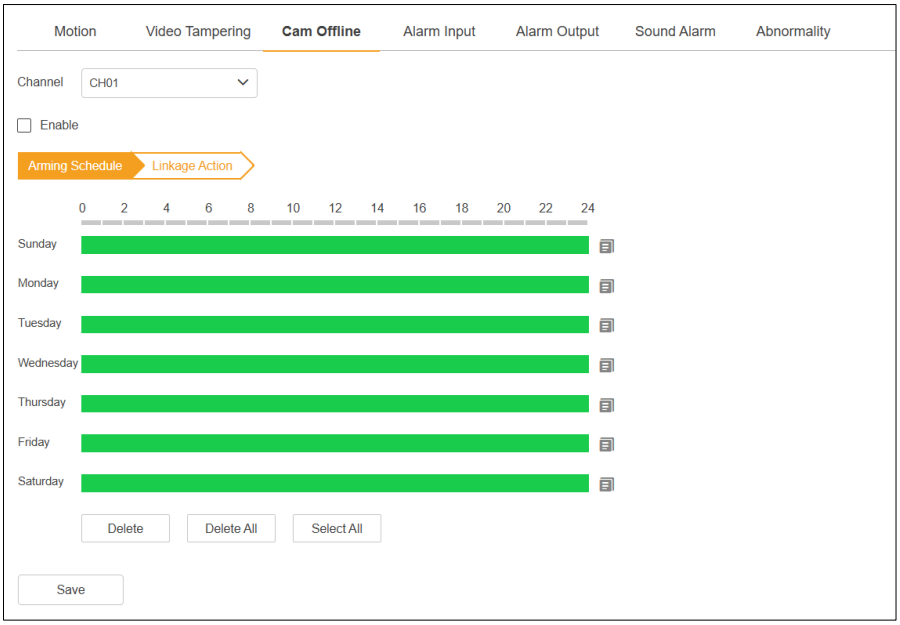


Figure 3-75 Cam Offline

Step 2 Select the required channel from the channel dropdown list.

Step 3 Enable the Cam Offline function.

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

Step 5 Set the linkage method.

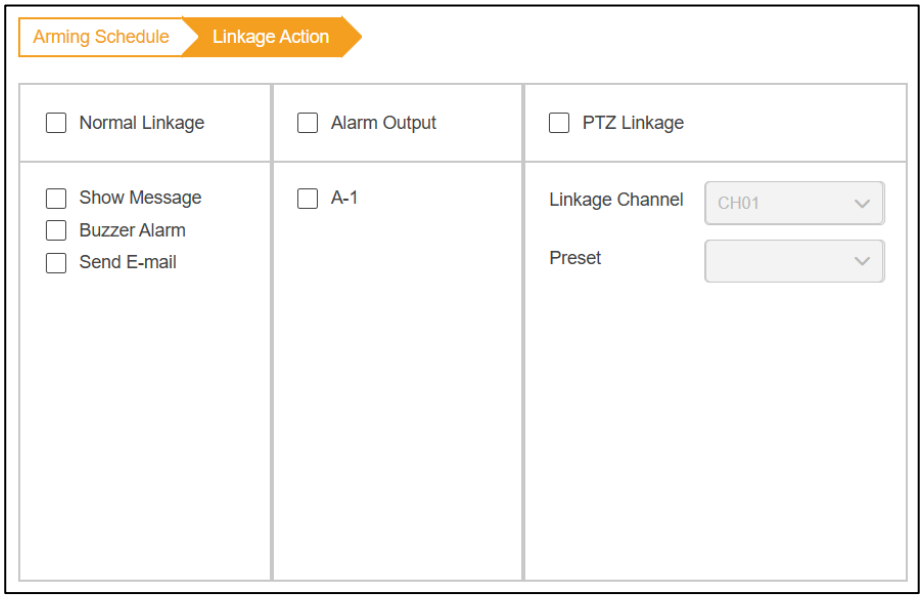


Figure 3-76 Linkage method

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

Parameter	Description
Normal Linkage	Configure the linkage actions to be triggered when an event occurs. • **Show Message:** Display an on-screen message when an abnormal event occurs. • **Buzzer Alarm**: Activate the device buzzer during the event. • **Send E-mail**: Send an email notification for the event.
Alarm Output	Configure the alarm output action for the event. • **A-1**: Activate the selected alarm output channel during the event.
PTZ Linkage	Configure PTZ actions to be triggered during the event. • **Linkage Channel**: Select the PTZ camera channel for linkage action. • **Preset**: Select the preset position to which the PTZ camera will move when the event is triggered.

Table 3-27 Description of linkage method parameters

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** > **Normal Event** > **Alarm Input**.

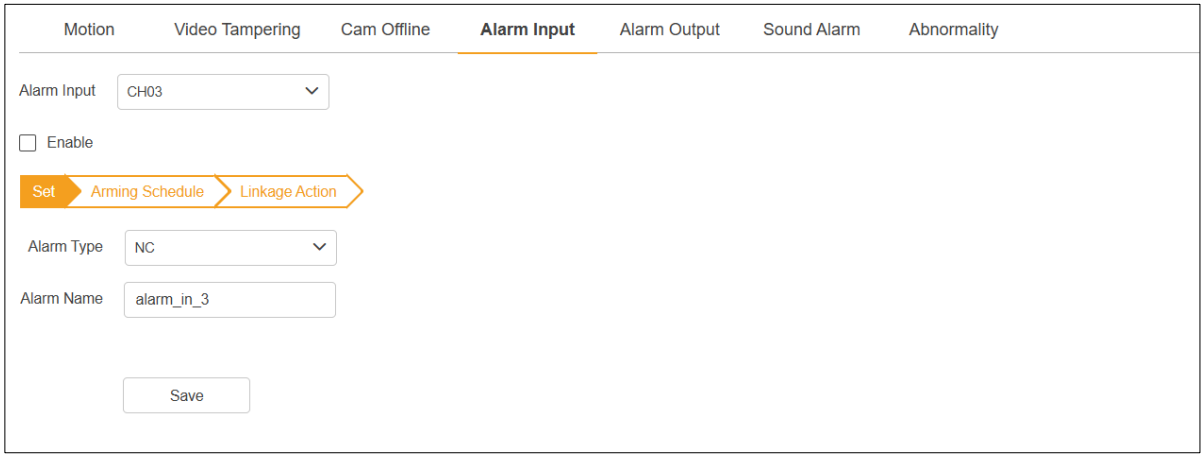


Figure 3-77 Alarm Input

Step 2 Select the required channel from the alarm input dropdown list.

Step 3 Enable the alarm input function.

Step 4 Select the **Alarm Type**: Normally Open (**NO**) or Normally Closed (**NC**).

Step 5 Enter the **Alarm Name** as required.

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

Step 7 Set the linkage action settings.

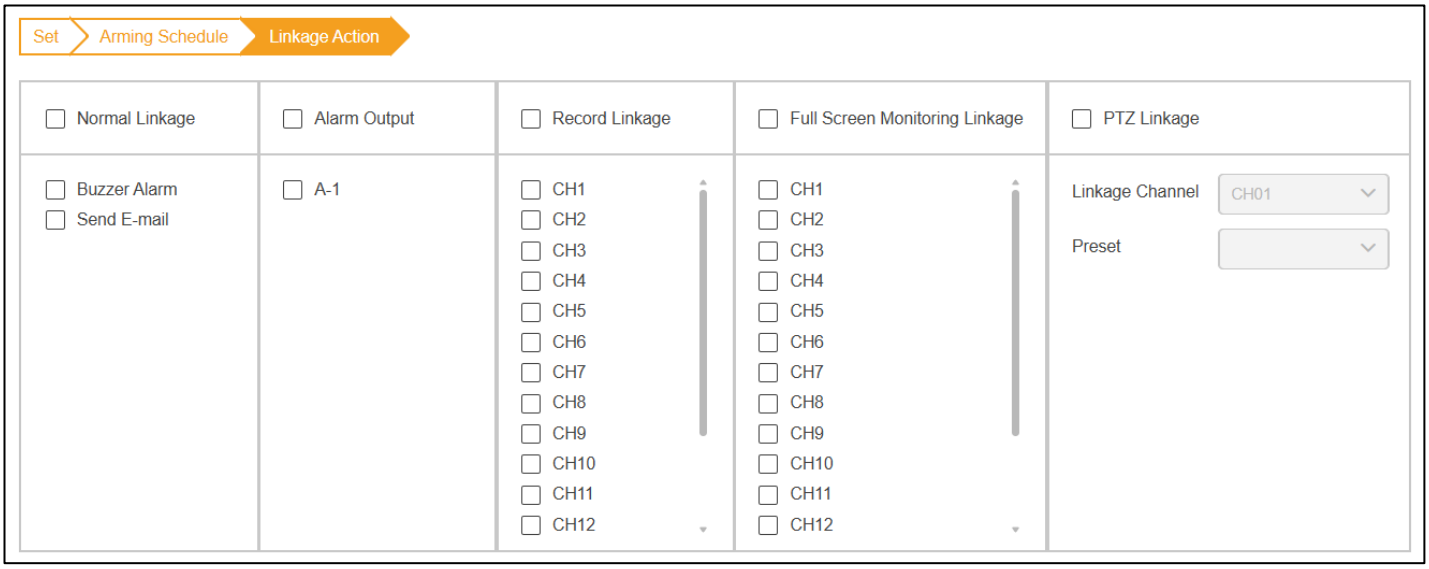


Figure 3-78 Linkage action for alarm input

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

Parameter	Description
Normal Linkage	Configure the linkage actions to be triggered when an event occurs. • **Pop-up Window**: Display a pop-up window on the monitor screen. • **Buzzer Alarm**: Activate the device buzzer during the event. • **Send E-mail**: Send an email notification for the event.
Alarm Output	Configure the alarm output action for the event. **A-1**: Activate the selected alarm output channel during the event.
Record Linkage	Select the channel(s) that will automatically start recording when the event is detected.
Full Screen Monitoring Linkage	Select the channel(s) to be displayed in full-screen mode on the monitor when the event occurs, allowing immediate viewing of the associated camera.

PTZ Linkage	Configure PTZ actions to be triggered during the event. • **Linkage Channel**: Select the PTZ camera channel for linkage action. • **Preset**: Select the preset position to which the PTZ camera will move when the event is triggered.

Table 3-28 Description of linkage method parameters

Step 8 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 to **Settings** > **Event** > **Normal Event** > **Alarm Output**.

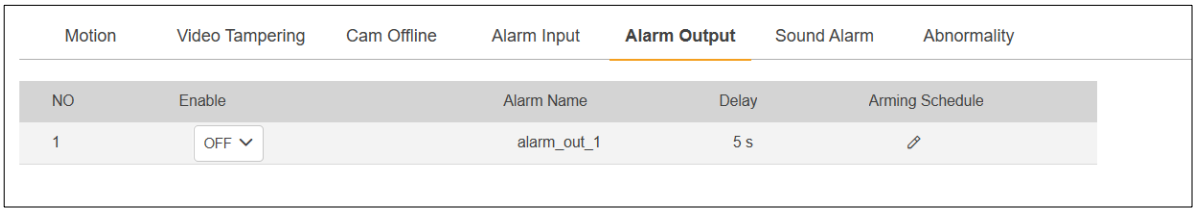


Figure 3-79 Alarm Output

Step 2 Enable the alarm output function.

Step 3 Click  to configure the alarm output settings.

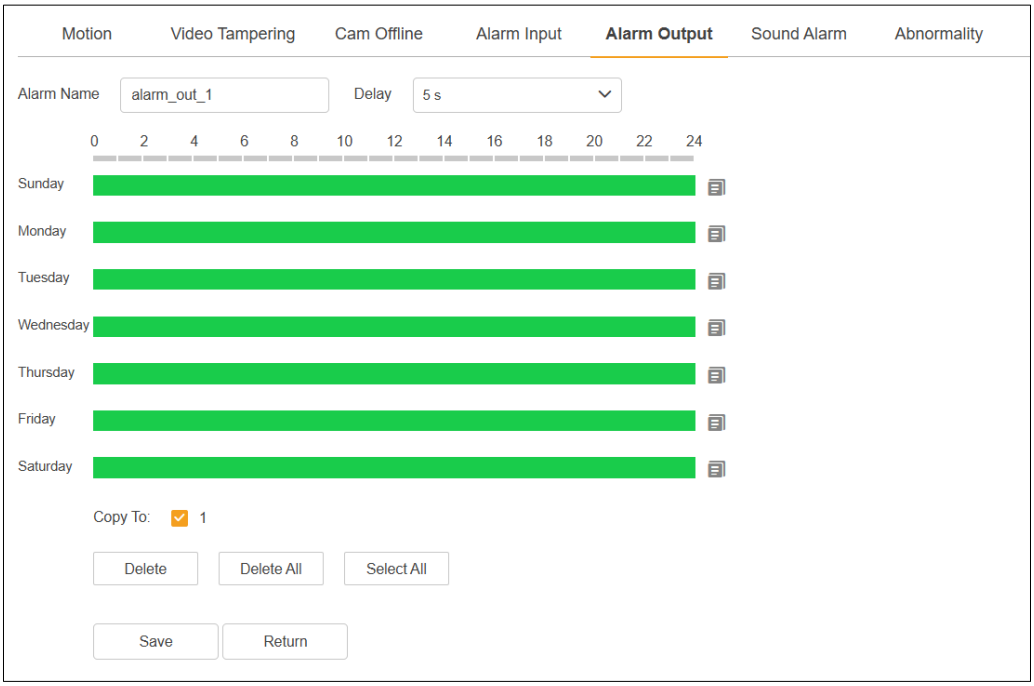


Figure 3-80 Alarm output settings

Step 4 Enter the **Alarm Name** as required.

Step 5 Set the alarm output **Delay**.

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

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

Sound Alarm

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

Step 1 Navigate to **Settings** > **Event** > **Normal Event** > **Sound Alarm**.

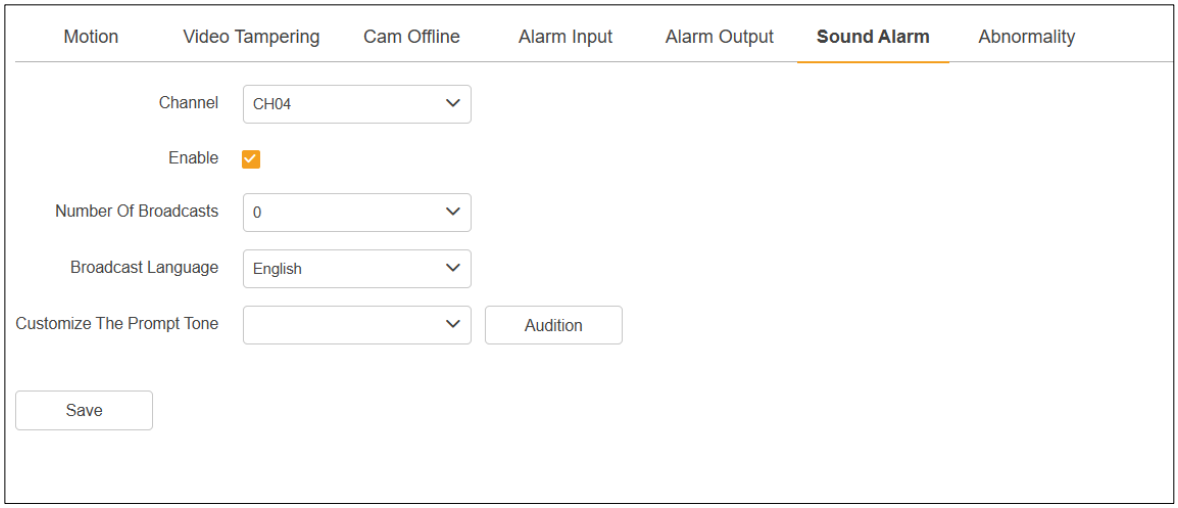


Figure 3-81 Sound Alarm

Step 2 Select the required channel.

Step 3 Enable the sound alarm function.

Step 4 Configure the sound alarm parameters.

Parameter	Description
Number Of Broadcasts	Select the number of times the alarm message should be broadcast during an alarm event.
Broadcast Language	Select the language used for the voice broadcast or prompt tone.
Customize The Prompt Tone	Select the customized prompt tone to be played during the alarm event.
Audition	Plays the selected sound through the camera speaker for preview before saving the configuration.

Table 3-29 Description of sound alarm parameters

Step 5 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 HDD issues. By setting exception types and corresponding responses, the device can promptly notify users or trigger alarms to ensure system reliability.

Step 1 Navigate to **Settings** > **Event** > **Normal Event** > **Abnormality**.

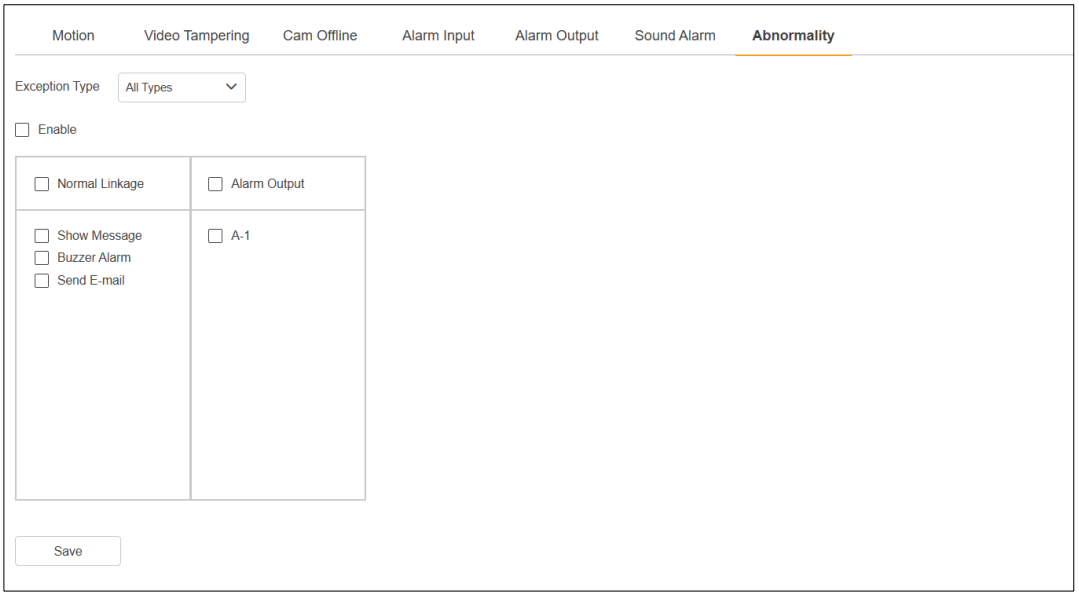


Figure 3-82 Abnormality

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

- No HDD
- HDD Error
- Network Disconnected
- IP Conflicted
- HDD Full

Step 3 Enable the abnormality function.

Step 4 Enable the required response options based on your needs.

Option	Description
Normal Linkage	Configure the linkage actions to be triggered during an abnormal event. • **Show Message:** Display an on-screen message when an abnormal event occurs. • **Buzzer Alarm:** Activate the buzzer alarm during an abnormal event. • **Send E-mail:** Send an email notification when an abnormal event occurs.
Alarm Output	Configure the alarm output actions for the abnormal event. • **A-1:** Select the alarm output channel to be activated during the abnormal event.

Table 3-30 Description of abnormality response options

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

3.5.4.2 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 the video setting area, and the alarm will be linked according to the judgment result.

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

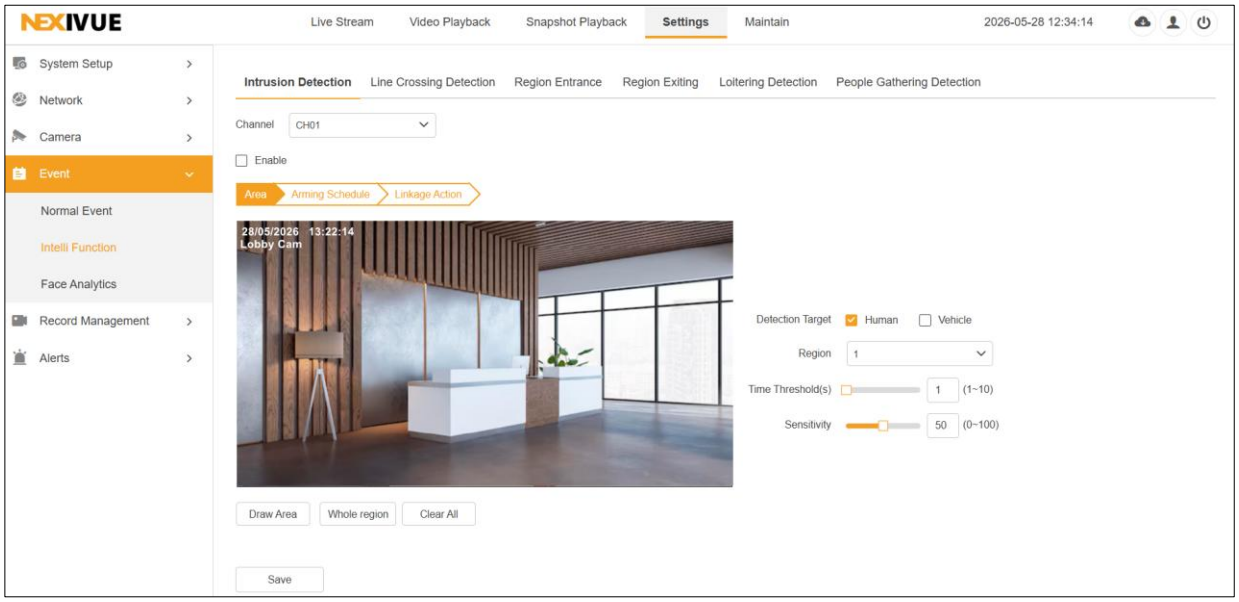


Figure 3-83 Intrusion detection

Step 2 Select the required channel.

Step 3 Enable the intrusion detection function.

Step 4 Select the detection target:

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

Step 5 Select the **Region**. The system supports setting up to 4 warning regions. After selecting a warning region, you need to make the following settings.

Step 6 Configure the intrusion detection parameters.

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. Again, click **Draw Area** to exit drawing mode.
Whole region	Selects the entire camera view as the intrusion detection area.
Clear All	Clears all previously drawn intrusion detection areas from the screen.
Time 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 1 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 3-31 Description of intrusion detection parameters

Step 7 Set the arming time (For details, please refer to the motion detection arming time setting).

Step 8 Set the linkage method.

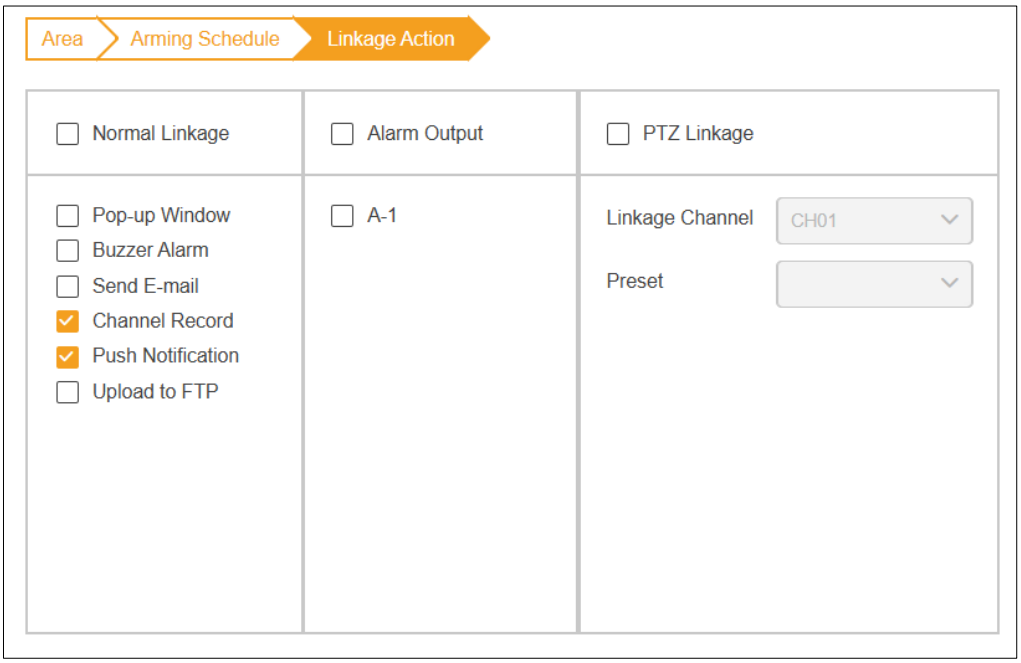


Figure 3-84 Linkage action

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

Parameter	Description
Normal Linkage	Configure the linkage actions to be triggered when an event occurs. • **Pop-up Window**: Display a pop-up window on the monitor screen. • **Buzzer Alarm**: Activate the device buzzer during the event. • **Send E-mail**: Send an email notification for the event. • **Channel Record**: Start recording on the selected channel. • **Push Notification**: Send a notification to the connected mobile application. • **Upload to FTP**: Upload snapshots to the configured FTP server.
Alarm Output	Configure the alarm output action for the event. • **A-1**: Activate the selected alarm output channel during the event.
PTZ Linkage	Configure PTZ actions to be triggered during the event. • **Linkage Channel**: Select the PTZ camera channel for linkage action. • **Preset**: Select the preset position to which the PTZ camera will move when the event is triggered.

Table 3-32 Description of linkage method parameters

Step 9 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 line, and link the alarm according to the judgment result.

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

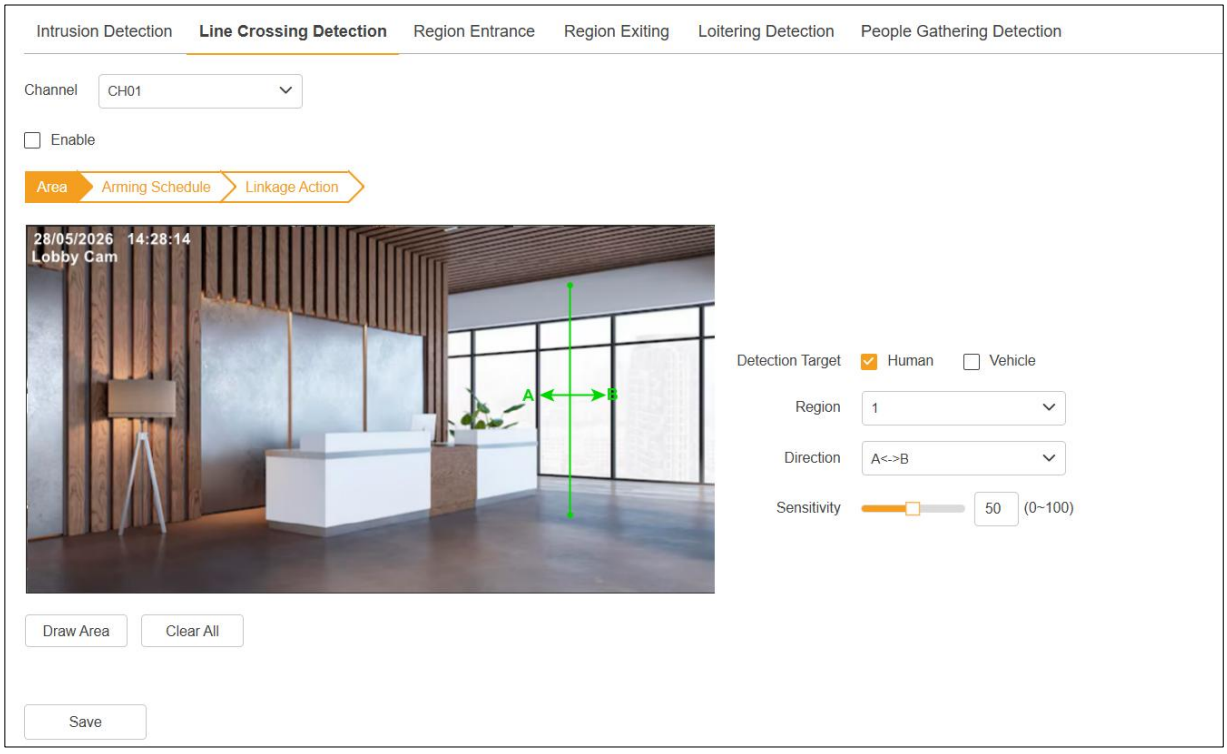


Figure 3-85 Line crossing detection

Step 2 Select the required channel.

Step 3 Enable the line crossing detection function.

Step 4 Select the detection target type:

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

Step 5 Select the **Region**. The system supports setting up to 4 warning regions. After selecting a warning region, you need to make the following settings.

Step 6 Configure the line crossing detection parameters.

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 an alarm triggering.

Table 3-33 Description of line crossing detection parameters

Step 7 Set the arming time (For details, please refer to the motion detection arming time setting).

Step 8 Set the linkage method (For details, please refer to the intrusion detection linkage method setting).

Step 9 Click **Save** to save the configured settings.

Region Entrance Detection

Region entrance detection is used to detect whether an object enters the configured detection area in the video and trigger the linked alarm action based on the detection result.

- This intelligent event function depends on the camera model; please refer to the actual camera.

Step 1 Navigate to **Settings** > **Event** > **Intelli Function** > **Region Entrance**.

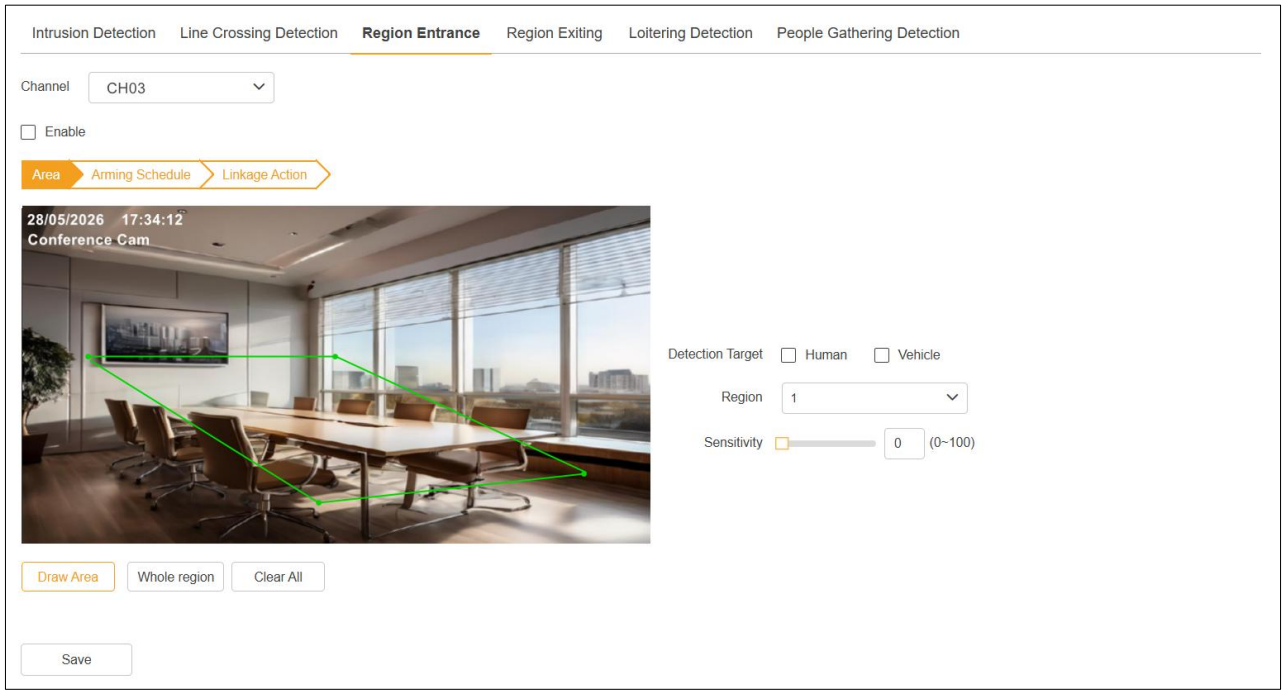


Figure 3-86 Region Entrance

Step 2 Select the required channel.

Step 3 Enable the region entrance detection function.

Step 4 Select the detection target type:

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

Step 5 Select the **Region**. The system supports setting up to 4 warning regions. After selecting a warning region, you need to make the following settings.

Step 6 Configure the region entrance parameters.

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. Again, click **Draw Area** to exit drawing mode.
Whole region	Selects the entire camera view as the region entrance detection area.
Clear All	Clears all previously drawn region entrance detection areas from the screen.
Sensitivity	Sets the sensitivity of detecting the entrance; 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 3-34 Description of region entrance detection parameters

Step 7 Set the arming time (For details, please refer to the motion detection arming time setting).

Step 8 Set the linkage method (For details, please refer to the intrusion detection linkage method setting).

Step 9 Click **Save** to save the configured settings.

Region Exiting Detection

Region exiting detection is used to detect whether an object exits the configured detection area in the video and trigger the linked alarm action based on the detection result.

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

Step 1 Navigate to **Settings** > **Event** > **Intelli Function** > **Region Exiting**.

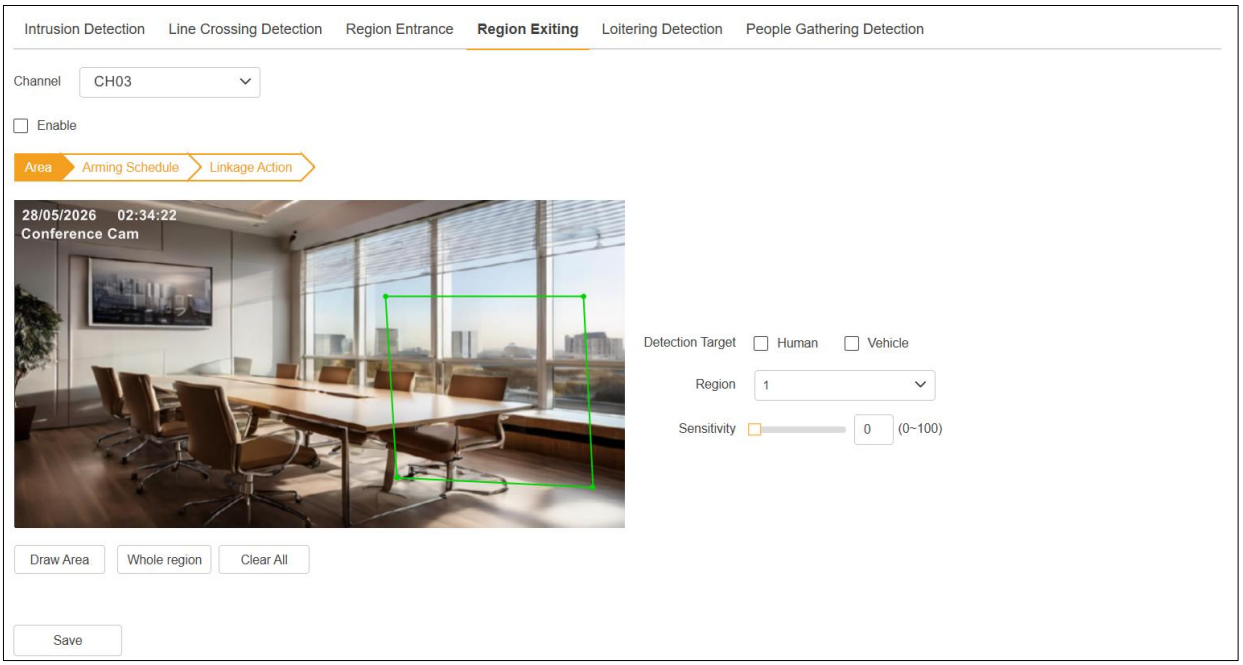


Figure 3-87 Region Exiting

Step 2 Select the required channel.

Step 3 Enable the region's exiting detection function.

Step 4 Select the detection target type:

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

Step 5 Select the **Region**. The system supports setting up to 4 warning regions. After selecting a warning region, you need to make the following settings.

Step 6 Configure the region exiting parameters.

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. Again, click **Draw Area** to exit drawing mode.
Whole region	Select the entire camera view as the region exiting detection area.
Clear All	Clear all previously drawn region exiting detection areas from the screen.
Sensitivity	Set the sensitivity of detecting the exiting; 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 3-35 Description of region exiting detection parameters

Step 7 Set the arming time (For details, please refer to the motion detection arming time setting).

Step 8 Set the linkage method (For details, please refer to the intrusion detection linkage method setting).

Step 9 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 to **Settings** > **Event** > **Intelli Function** > **Loitering Detection**.

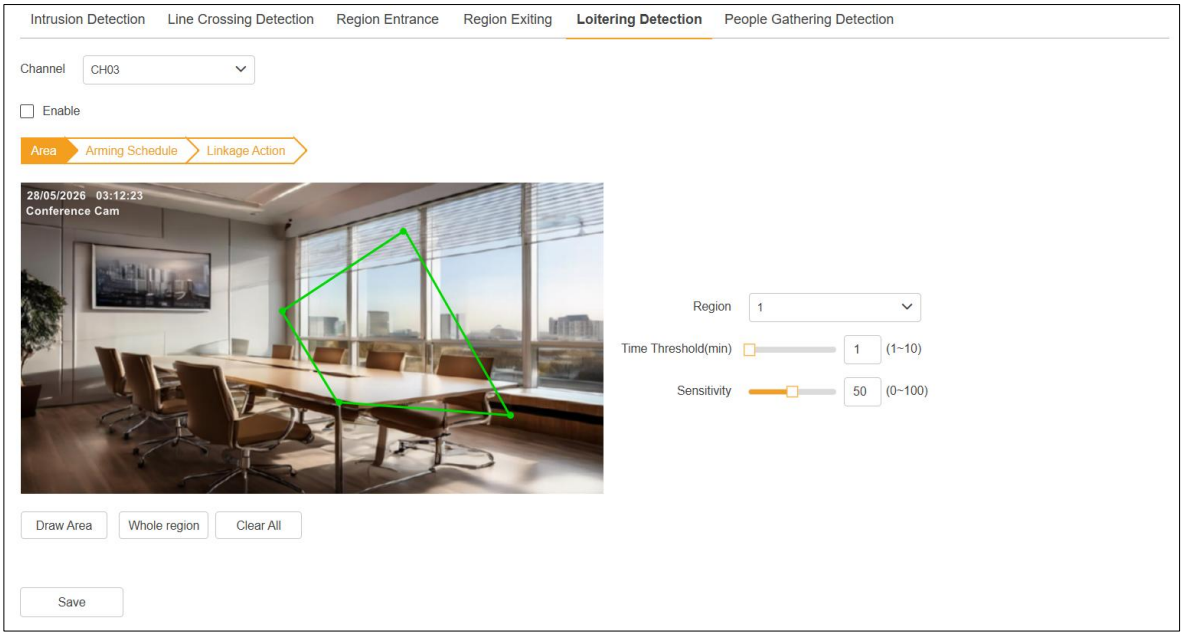


Figure 3-88 Loitering detection

Step 2 Select the required channel.

Step 3 Enable the loitering detection function.

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.

Step 5 Configure the loitering detection parameters.

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. Again, click **Draw Area** to exit drawing mode.
Clear All	Clear all previously drawn loitering detection areas from the screen.
Whole region	Select the entire camera view as the loitering detection area.
Time Threshold (min)	Set how long a person must stay inside the selected region continuously before the system considers it as loitering and generates an alarm. The default value is 1. Its value ranges from 1 to 10.

Sensitivity	Set 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 3-36 Description of loitering detection parameters

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

Step 7 Set the linkage method (For details, please refer to the intrusion detection linkage method setting).

Step 8 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 camera model; please refer to the actual camera.

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

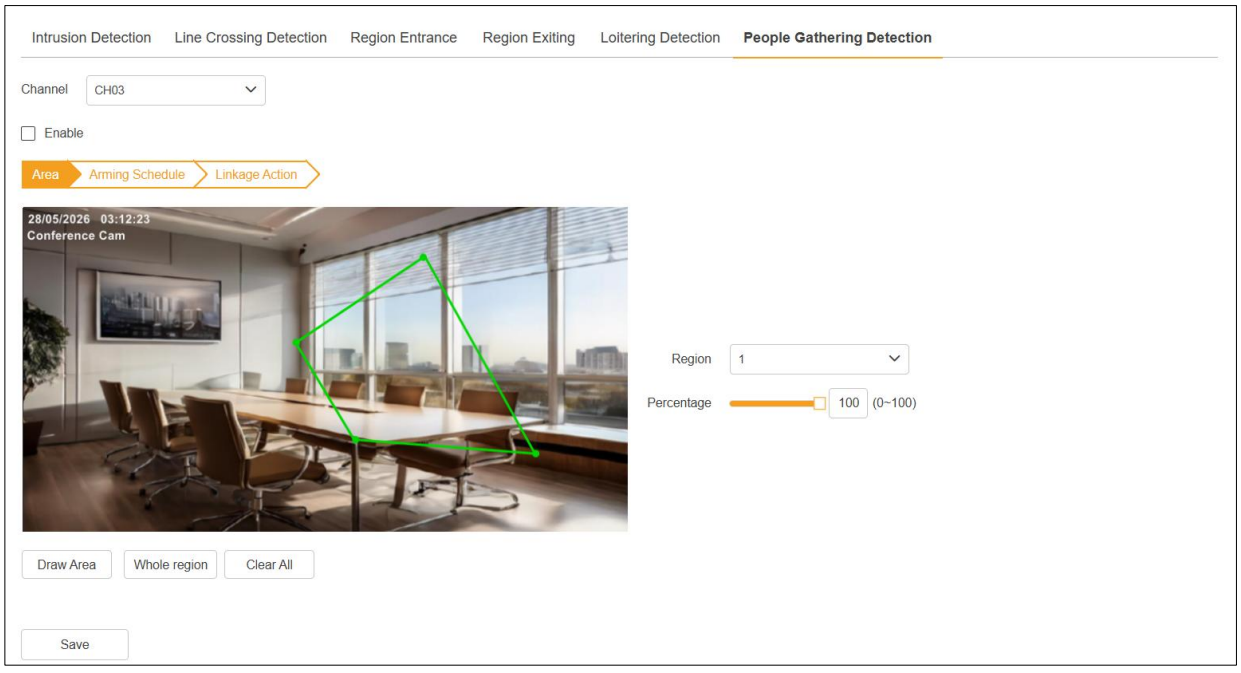


Figure 3-89 People gathering detection

Step 2 Select the required channel.

Step 3 Enable the people gathering detection function.

Step 4 Configure the people gathering detection parameters.

Parameter	Description
Region	Select the Region. The system supports setting up to 4 warning regions.
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. Again, click **Draw Area** to exit drawing mode.
Clear All	Clear all previously drawn people gathering areas from the screen.
Whole region	Select the entire camera view as the people gathering 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 3-37 Description of people gathering 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 intrusion detection linkage method setting).

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

3.5.4.3 Face Analytics

This section includes the face detection feature, which detects human faces in the video stream for monitoring purposes.

Face Detection

Face detection is used to detect whether a human face appears in the video and trigger the linked alarm action based on the detection result.

Step 1 Navigate to **Settings** > **Event** > **Face Analytics** > **Face Detection**.

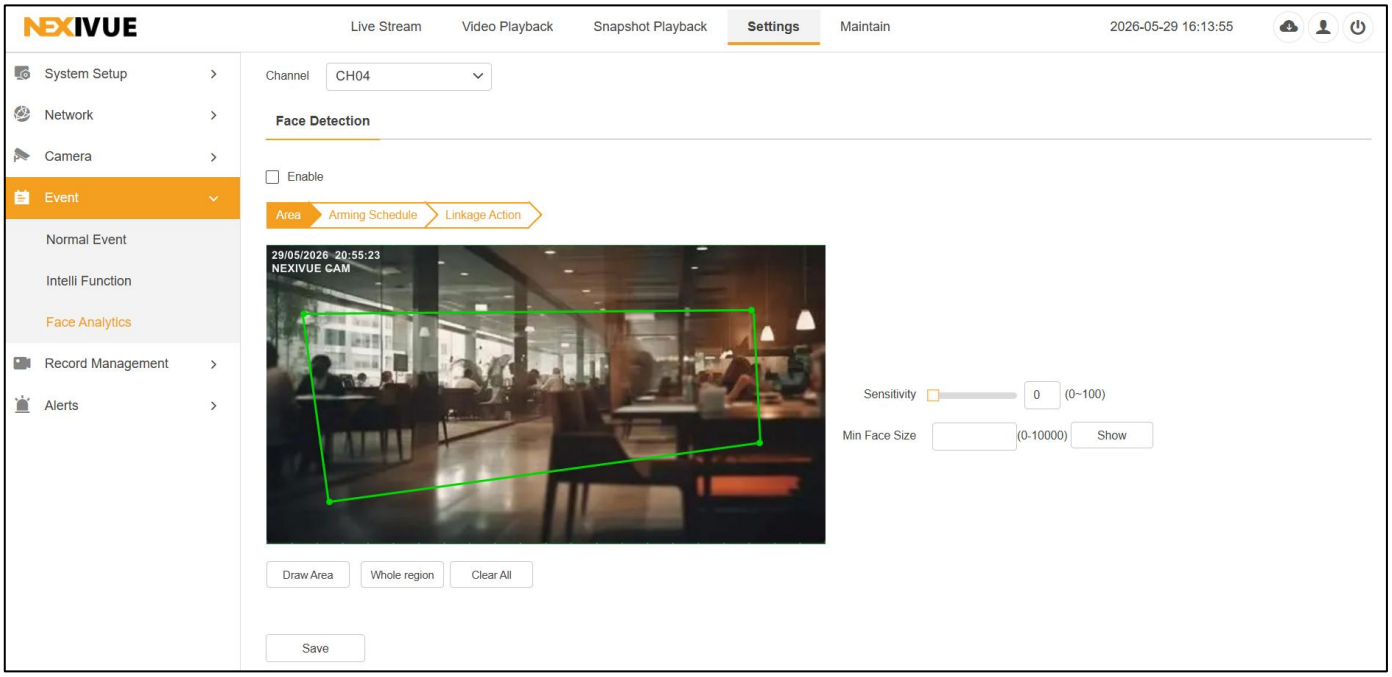


Figure 3-90 Face detection

Step 2 Select the required channel.

Step 3 Enable the face detection function.

Step 4 Configure the face detection parameters.

Parameter	Description
Region	Select the **Region**. The system supports setting up to 4 warning regions.
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. Again, click **Draw Area** to exit drawing mode.
Clear All	Clears all previously drawn face detection areas from the screen.
Whole region	Selects the entire camera view as the face detection area.

Sensitivity	Sets the sensitivity level for face 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.
Min Face Size	Adjust the face size value. The value ranges from 0 to 1000. Click **Show** to review the face size.

Table 3-38 Description of face 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 intrusion detection linkage method setting).

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

3.5.5 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.

3.5.5.1 Schedule

This part allows users to define specific time periods for video recordings. 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.

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

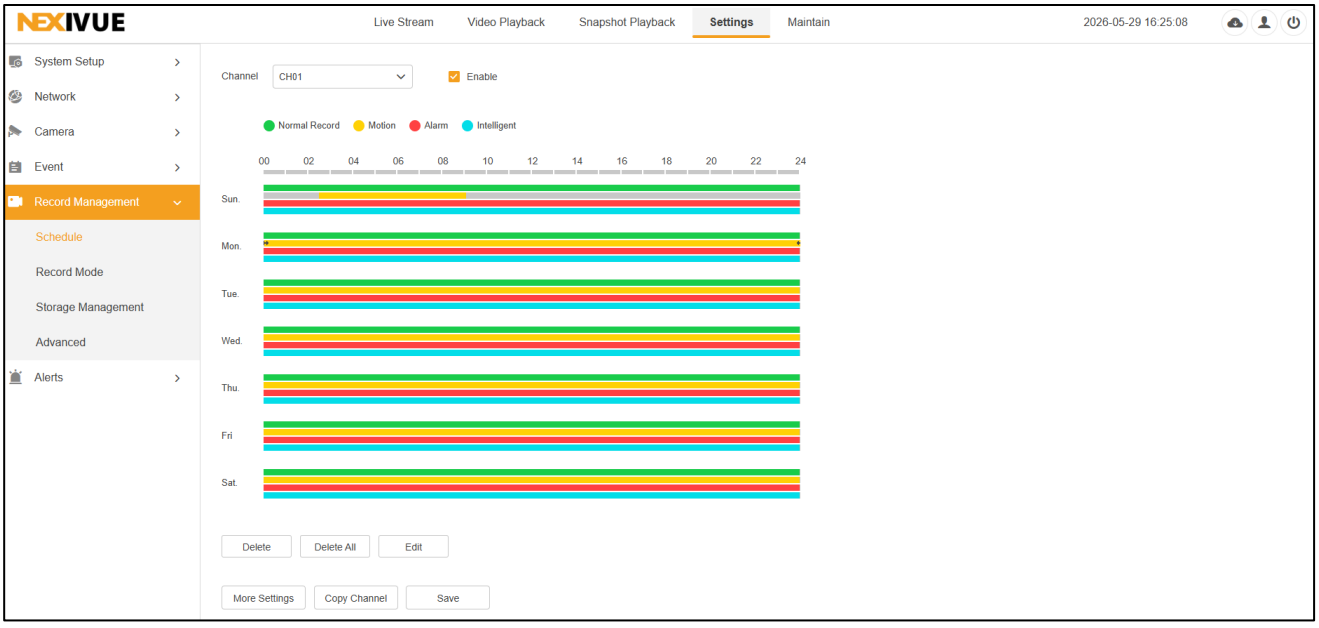


Figure 3-91 Record Schedule

Step 2 Select a channel to record a video.

Step 3 Enable the schedule function to activate the recording schedule.

Step 4 Set the arming time for recording.

- Multiple time periods can be set on the timeline of the same day, supporting up to 8 time periods.
- When the arming time is set, there can be no overlapping time between any two time periods.

- **Method 1:** Click on the event timeline as per their color 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, select the event type, and click **Save** after setting. If you need to delete the time period, click **Delete** button to reset the time period.
- **Method 3:** Click **Edit** and configure the time period and event type, and then click **Save**.

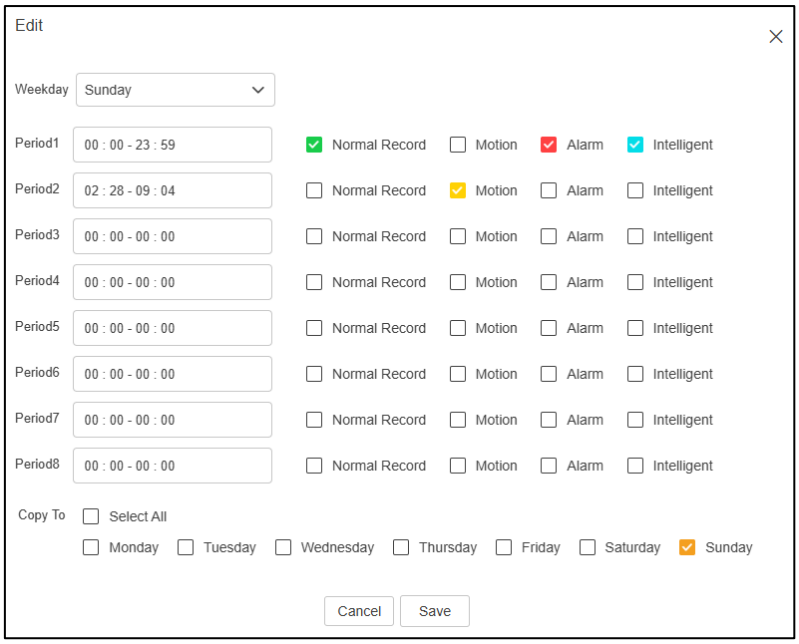


Figure 3-92 Edit record schedule

Step 5 Configure other required recording parameters.

Parameter	Description
More Settings	Click **More Settings** and then enter the amount of time that you want the pre-recording to last. A recording will be made before the event.
Copy Channel	Copy the schedule of a particular channel to other channels.
Delete	Select a particular type of event timeline and click **Delete** to delete it.
Delete All	Removes the entire week's schedule.

Table 3-39 Description of record schedule parameters

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

3.5.5.2 Record Mode

This section allows you to configure record mode settings, including setting the stream type and channel for recording.

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

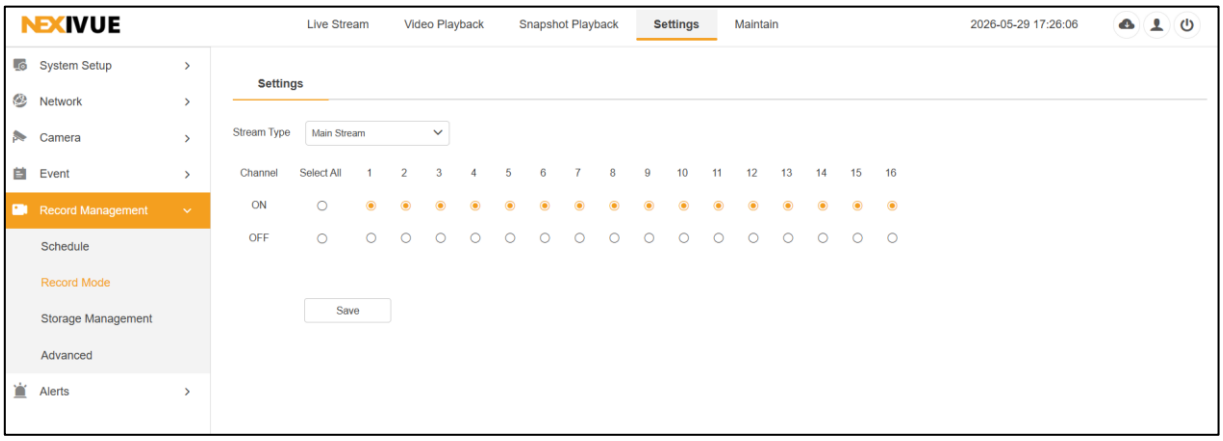


Figure 3-93 Record mode settings

Step 2 Select the stream type:

- **Main stream:** It has a large bit of 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.

Step 3 Select the channels whose recording you want to On/Off.

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

3.5.5.3 Storage Management

This section allows you to monitor and manage the storage devices connected to the NVR. From this page, you can view disk health and capacity, monitor available storage space, format storage devices when required, and configure cloud storage settings for secure remote backup and data retention.

Disk Management

Disk Management allows you to monitor and manage the storage drives installed in the NVR.

Step 1 Navigate to **Settings** > **Record Management** > **Storage Management** > **Disk Management**.

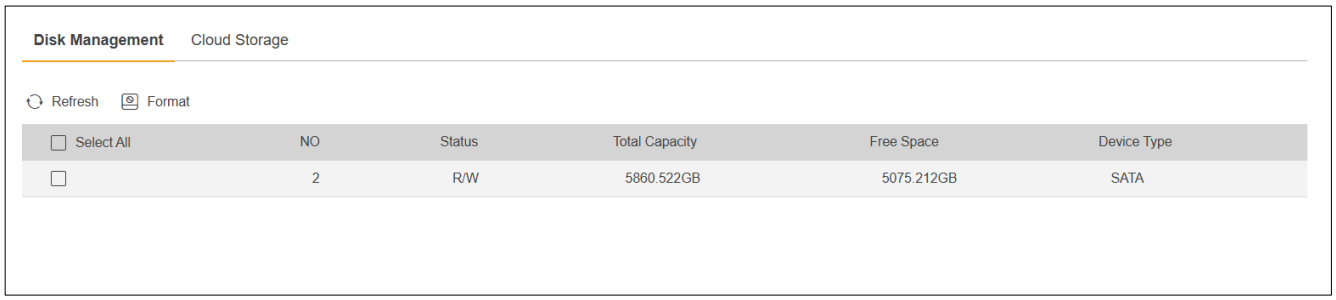


Figure 3-94 Disk Management

Step 2 Configure the disk management parameters.

Parameter	Description
Select All	Select all available storage devices for management operations.
No	Displays the disk number assigned by the NVR.
Status	Displays the current operating status of the disk, such as Read/Write (R/W).
Total Capacity	Displays the total storage capacity of the disk.
Free Space	Displays the remaining available storage space.
Device Type	Displays the storage interface type of the connected disk, such as SATA.
Refresh	Update and display the latest storage information.
Format	Format the selected storage device and erase all stored data.

Table 3-40 Description of disk management parameters

Cloud Storage

This section allows you to connect the NVR to a supported cloud storage service for automatic upload and backup of event snapshots, providing an additional layer of data protection and remote accessibility.

Step 1 Navigate to **Settings** > **Record Management** > **Storage Management** > **Cloud Storage**.

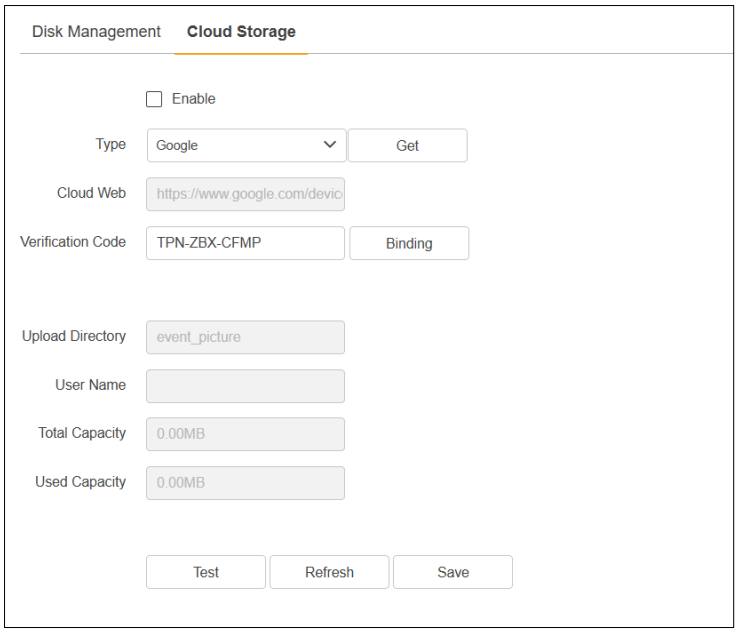


Figure 3-95 Cloud Storage

Step 2 Enable the cloud storage function.

Step 3 Configure the cloud storage parameters.

Parameter	Description
Type	Select the cloud storage service to be used for data upload and backup.
Get	Generate the cloud authorization information required for account binding.
Cloud Web	Displays the web address used to authorize and link the cloud storage account.
Verification Code	Enter or view the verification code required to complete cloud account authorization.
Binding	Bind the NVR to the authorized cloud storage account.
Upload Directory	Specify the cloud directory where you want to upload files.
User Name	Displays the username of the connected cloud storage account.
Total Capacity	Displays the total storage capacity available in the cloud account.
Used Capacity	Displays the amount of cloud storage space currently in use.

Test	Verify the connectivity and accessibility of the configured cloud storage account.
Refresh	Update and display the latest cloud storage information.

Table 3-41 Description of cloud storage parameters

Step 4 Click **Save** to apply the cloud storage configuration settings.

3.5.5.4 Advanced Settings

This section allows you to configure storage management policies, including how the NVR handles recordings when the hard disk becomes full and whether old recordings should be automatically deleted.

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

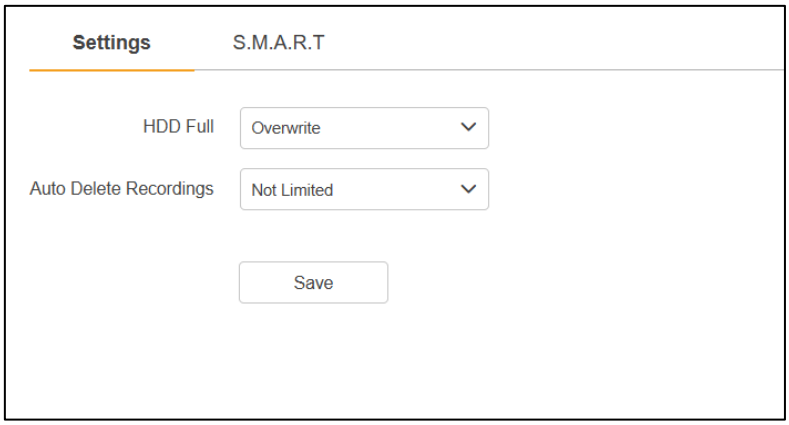


Figure 3-96 Advanced settings

Step 2 From the **HDD Full** drop-down list, select the desired option:

- **Overwrite:** The newest files overwrite the oldest ones.
- **Do Not Overwrite:** The newest files do not overwrite the oldest ones.

Step 3 Configure the **Auto Delete Recordings** period as required.

Step 4 Click **Save** to apply the settings.

S.M.A.R.T Settings

The S.M.A.R.T (Self-Monitoring, Analysis, and Reporting Technology) section provides detailed health and diagnostic information for installed hard drives. It helps monitor disk performance, identify potential issues, and evaluate the overall condition of the storage device.

Step 1 Navigate to **Settings** > **Record Management** > **Advanced** > **S.M.A.R.T**.

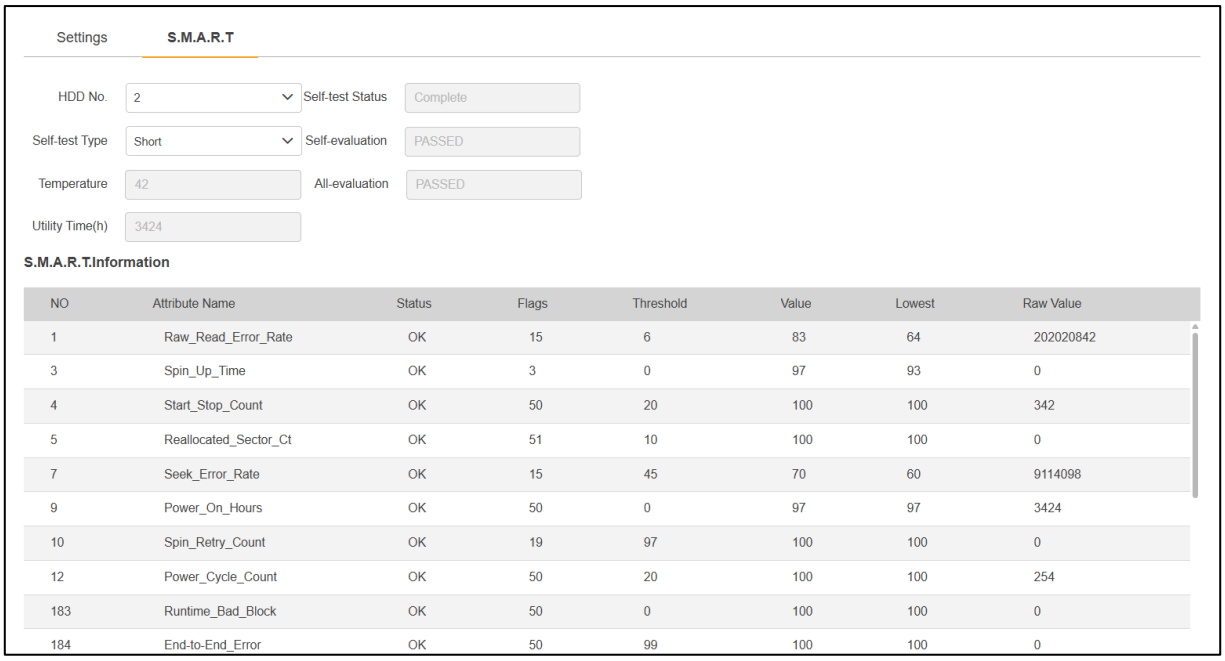


Figure 3-97 S.M.A.R.T Recordings

Step 2 Configure the S.M.A.R.T parameters.

Parameter	Description
HDD No.	Select the hard drive whose S.M.A.R.T information will be displayed.
Self-test Type	Select the type of diagnostic test to perform on the hard drive.
Self-test Status	Displays the current status of the selected self-test.
Self-evaluation	Displays the result of the drive's self-assessment.
All-evaluation	Displays the overall health evaluation of the hard drive.
Temperature	Displays the current operating temperature of the hard drive.
Utility Time (h)	Displays the total number of hours the hard drive has been in operation.
S.M.A.R.T Information	Displays detailed drive health attributes, including attribute name, status, threshold, current value, lowest recorded value, and raw value for monitoring hard drive reliability and performance.

Table 3-42 Description of S.M.A.R.T parameters

3.5.6 Alerts

This section allows you to configure audible notification settings for system events and alarms. It helps ensure that important events are promptly brought to the attention of operators through buzzer notifications.

3.5.6.1 Buzzer

This section allows you to enable and customize audible alarm notifications that are triggered by specific system events, helping operators quickly identify and respond to alerts.

Step 1 Navigate to **Settings** > **Alerts** > **Buzzer**.

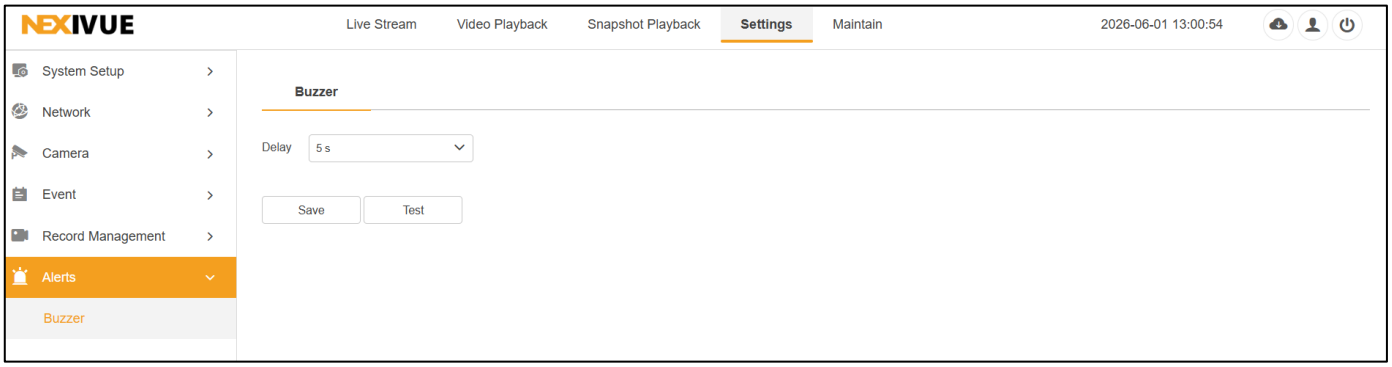


Figure 3-98 Buzzer

Step 2 Set the buzzer delay (in seconds) for which the buzzer remains active after an alarm is triggered.

Step 3 Click **Test** to verify the connectivity and duration of alarming.

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

3.6 Video Playback

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

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

3.6.1 Video Playback Interface

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

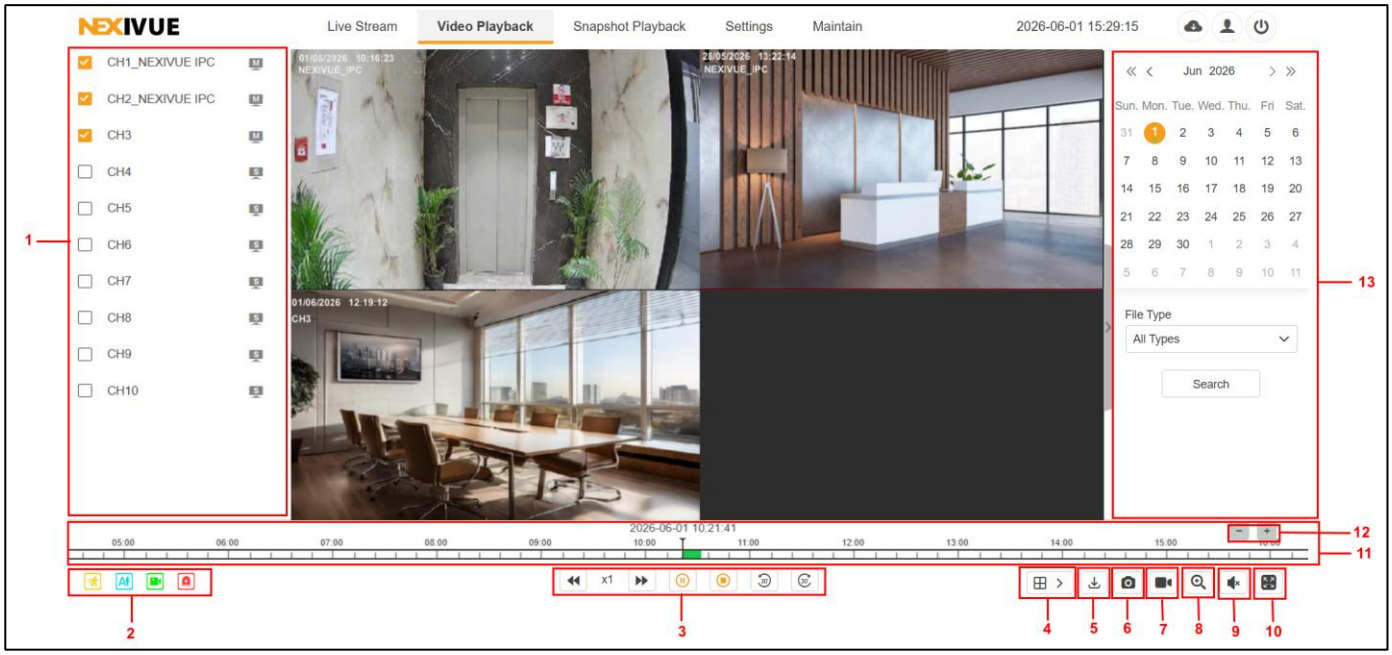


Figure 3-99 Video playback

No.	Function	Description
1	Channel List	In the connected channel list, select one or more channels that you want to play back.
2	Record Type Indicators	Different colors icons indicate various recording types: • : Indicates the **Normal Record** recording type • : Indicates the **Motion Detection** recording type • : Indicates the **Alarm** recording type • : Indicates the **Intelligent** recording type.

3	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 pause playing back recorded video. •  : Click the icon to jump back 30 seconds backward. •  : Click the icon to jump 30 seconds forward. •  : Click the icon to slow down the playing back video speed. •  : Click the icon to increase the speed of playing back video.
4	Window Layout	Select the layout according to the playback channel selection.
5	Download	Click this icon and recorded playback video list will be displayed according to different time slots. You can select the **Channel** and **File Type** according to the requirement and download the recorded videos.
6	Snapshot	Captures and saves a snapshot image from the playback video. The path to save the captured images can be viewed at **C:\Program Files (x86)\NEXIVUE\NVR\192.168.10.200\PlaybackPic\2026-06-01**  • The IP address included in the path refers to the assigned IP address of the device. • Captured snapshots are automatically saved in a date-wise folder.
7	Record	Start and Stop playback video recording. The path of local video recording can be viewed at **C:\Program Files (x86)\NEXIVUE\NVR\192.168.10.200\PlaybackFiles\2026-06-01**  • The IP address included in the path refers to the assigned IP address of the device. • Captured snapshots are automatically saved in a date-
8	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.
9	Audio control	Allows you to enable or disable audio during video playback.

10	Full Screen	Expands the playback video screen to full-screen mode for a larger and clearer view, hiding other interface elements. Press **Esc** to exit the full screen view.
11	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 its relations in Record Type Indicators.
12	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.
13	Search Panel	• Select a date from the calendar. • Choose the **File Type**, including All, Normal Record, Motion, Alarm, and Intelligent. • 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.

Table 3-43 Description of video playback interface

3.7 Snapshot Playback

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

3.7.1 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 HDD.

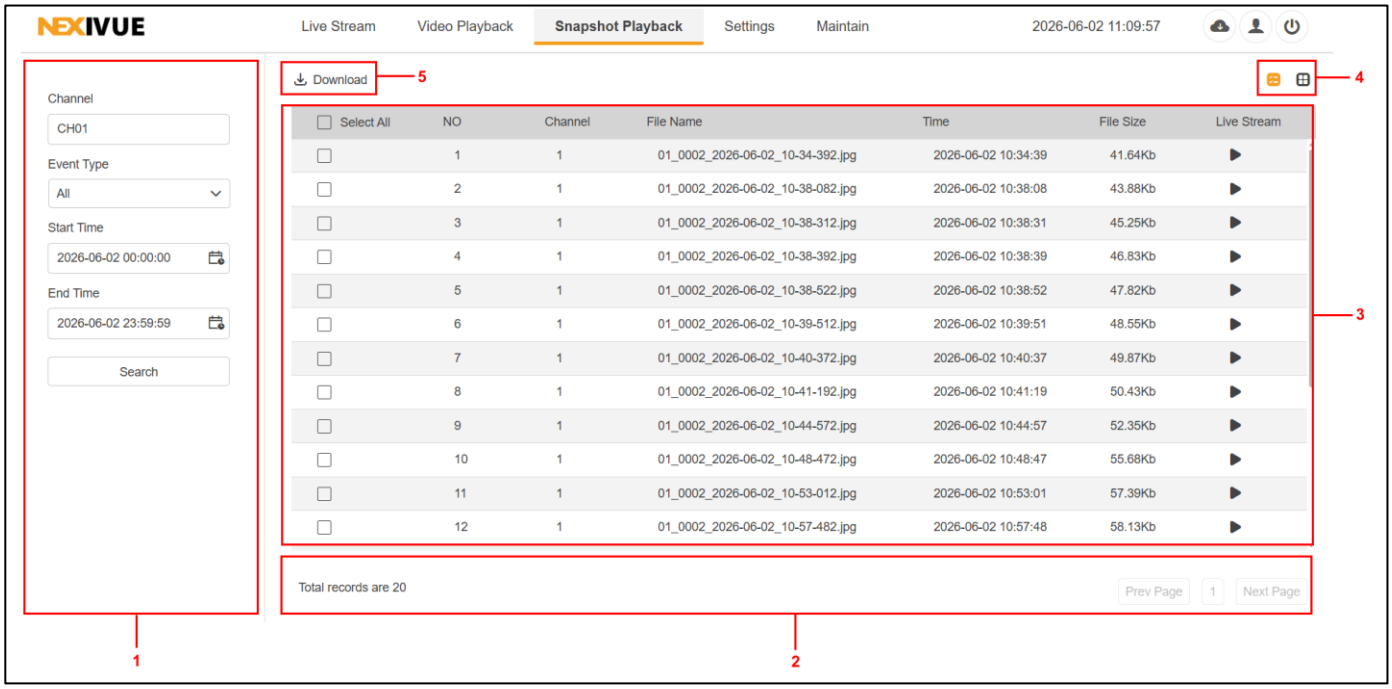


Figure 3-100 Snapshot Playback

No.	Function	Description
1	Search Panel	• Select the **Channel** in which you want to search for the snapshot. • Choose the **Event Type**, including All, Manual, Motion, Pedestrian, Vehicle, Region Entrance, Region Exiting, Line Crossing Detection, Intrusion Detection, Loitering Detection, People Gathering Detection, and Face Detection. • 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.**, **Channel**, **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 3-44 Description of snapshot playback interface

3.8 Maintain

This section provides system management and maintenance options, including firmware upgrades, factory reset, automatic maintenance, configuration backup and restore, channel information, system logs, and diagnostic information.

3.8.1 Version

This part provides comprehensive device information, including Device Name, Device Type, Firmware Version, Web Version, Release Date, Plugin Version, Channel Count, MAC Address, and Serial Number (S/N). These details help in device identification, compatibility verification, firmware management, network configuration, and technical support reference.

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

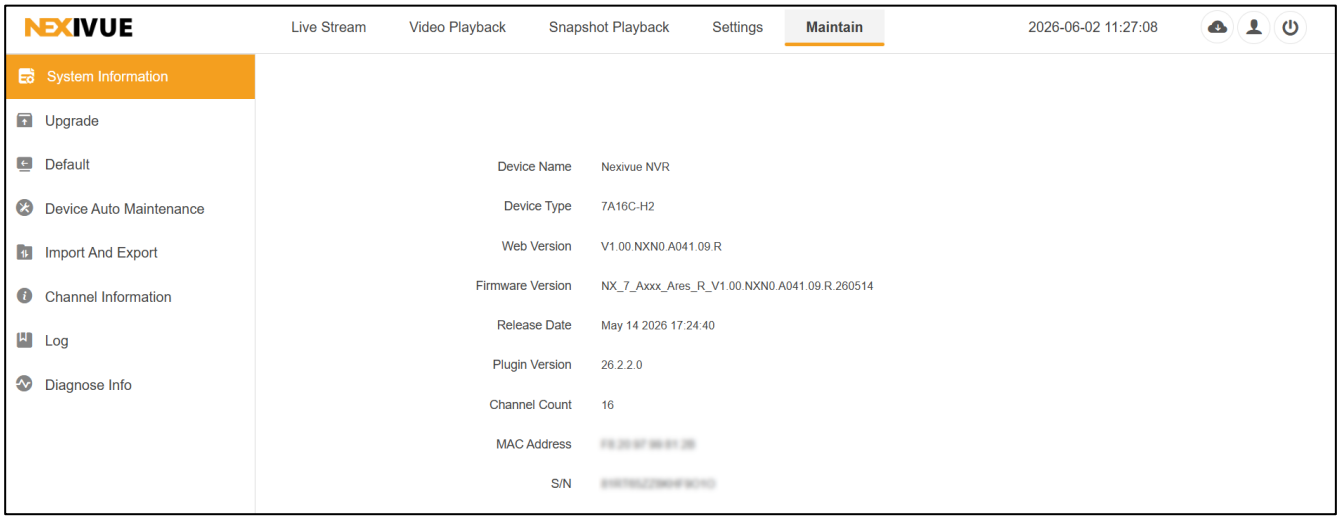


Figure 3-101 System Information

3.8.2 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**.

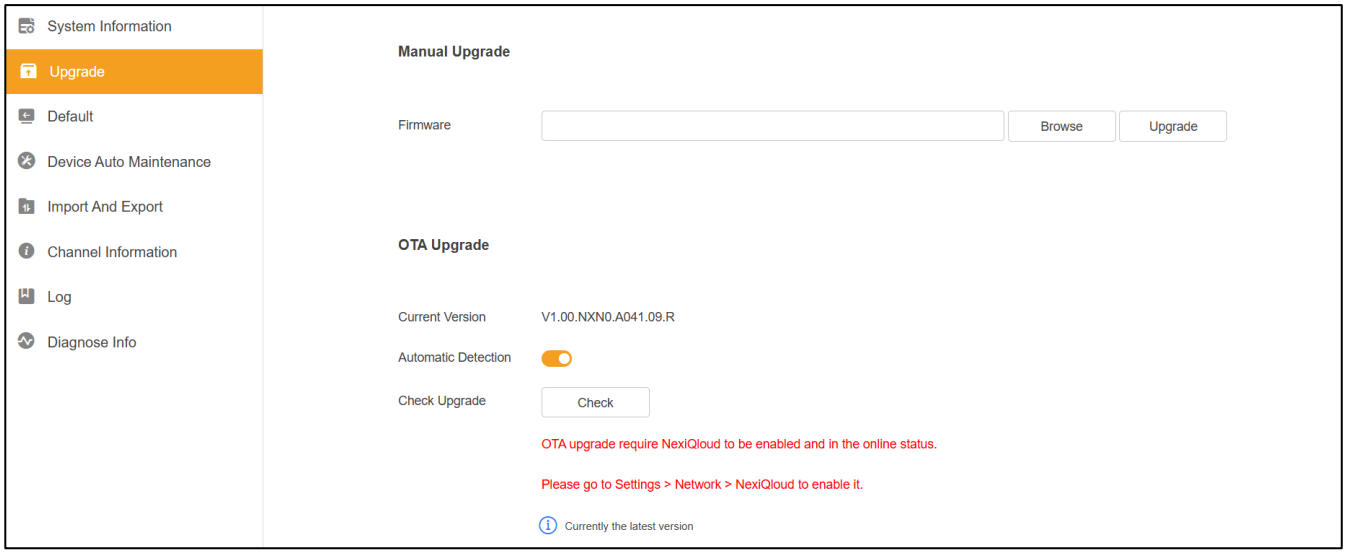


Figure 3-102 Upgrade

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 Upgrade**. If an update is available, it will be displayed.
  2. Enable the **Automatic Detection** option to automatically check for updates.

- OTA upgrade requires NexiQloud to be enabled. To enable NexiQloud, go to **Settings** > **Network** > **NexiQloud**.

3.8.3 Default

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

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

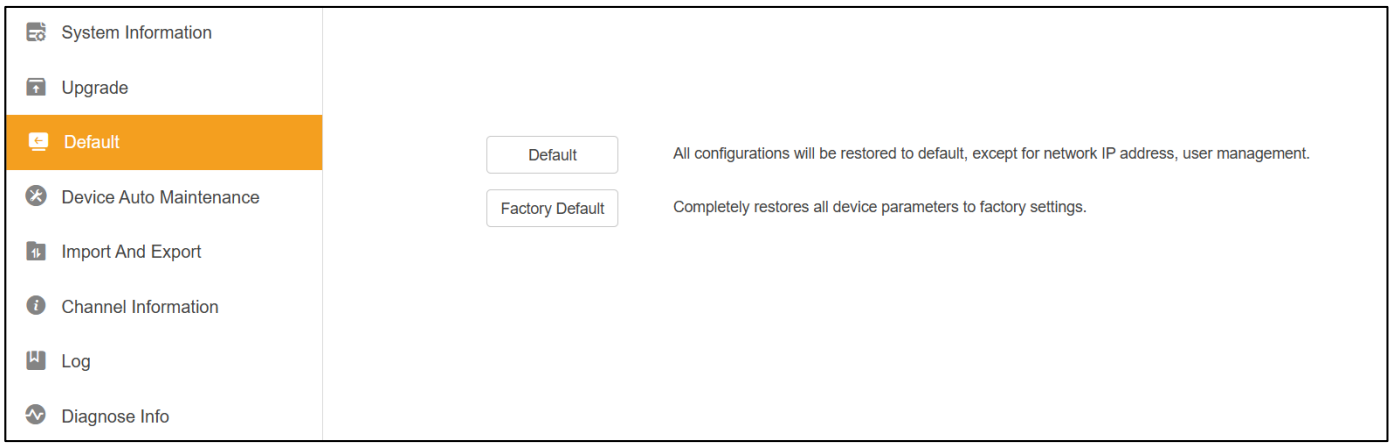


Figure 3-103 Default

Step 2 Select the reset method according to your needs.

- After clicking **Default**, all parameters of the device will be automatically restored to the factory default settings, except the network IP address and user management parameters.
- After clicking **Factory Default**, all parameters of the device will be automatically restored to the factory default settings.

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

3.8.4 Device Auto 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** > **Device Auto Maintenance**.

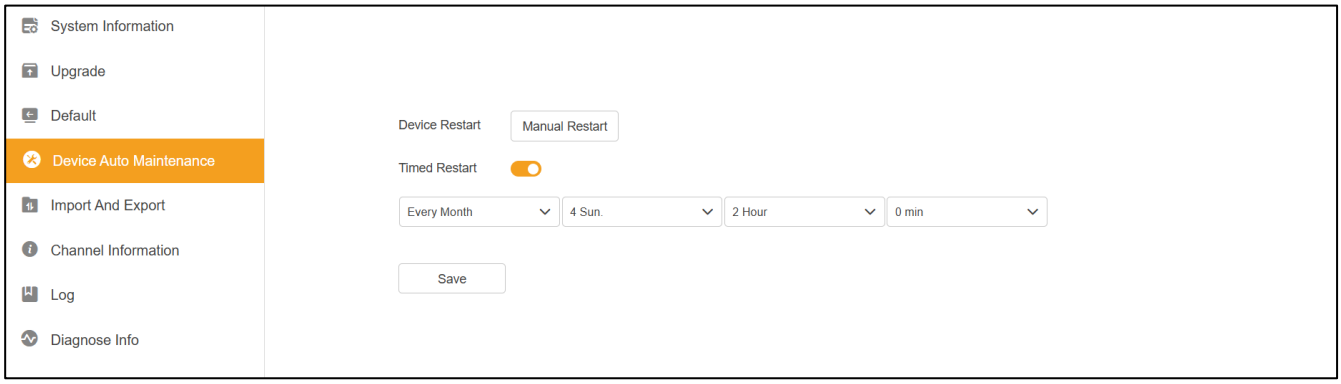


Figure 3-104 Device Auto Maintenance

Step 2 Configure device auto 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.

3.8.5 Import and Export

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

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

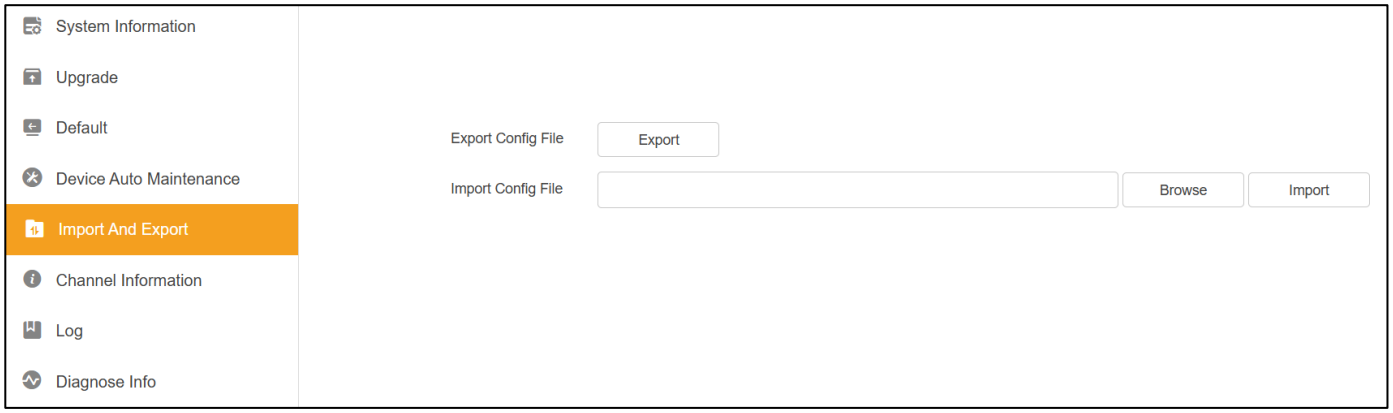


Figure 3-105 Import and export

Step 2 Click **Export** to export the config file of the device and save it to the local computer.

Step 3 Click **Browse**, select the storage path of the device config file, and click **Import**. This is used to import the exported config file into the device.

3.8.6 Channel Information

This section displays the connected channel information, including channel no., camera name, resolution, and IPC version.

Step 1 Navigate to **Maintain** > **Channel Information**.

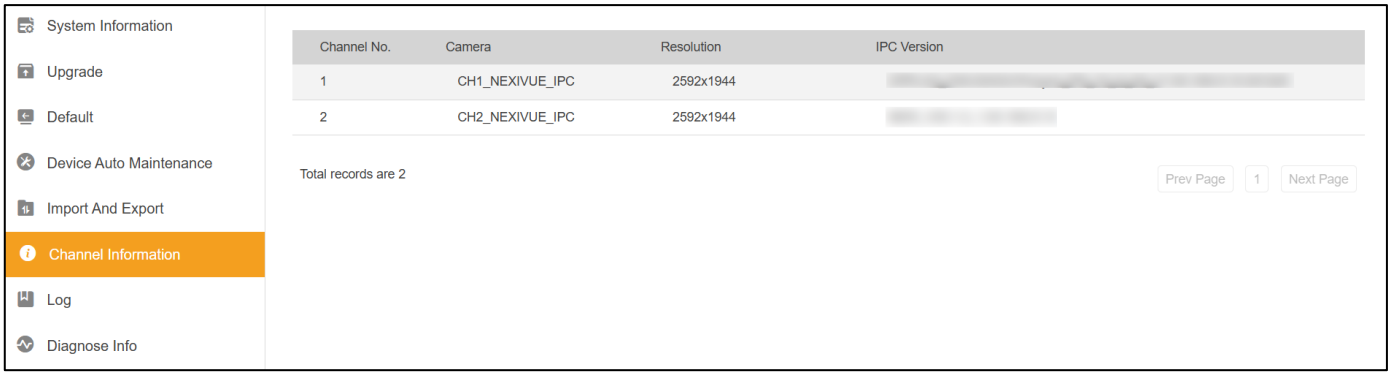


Figure 3-106 Channel Information

3.8.7 Log

The log interface allows querying, displaying and exporting log information that is effectively saved in the HDD.

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

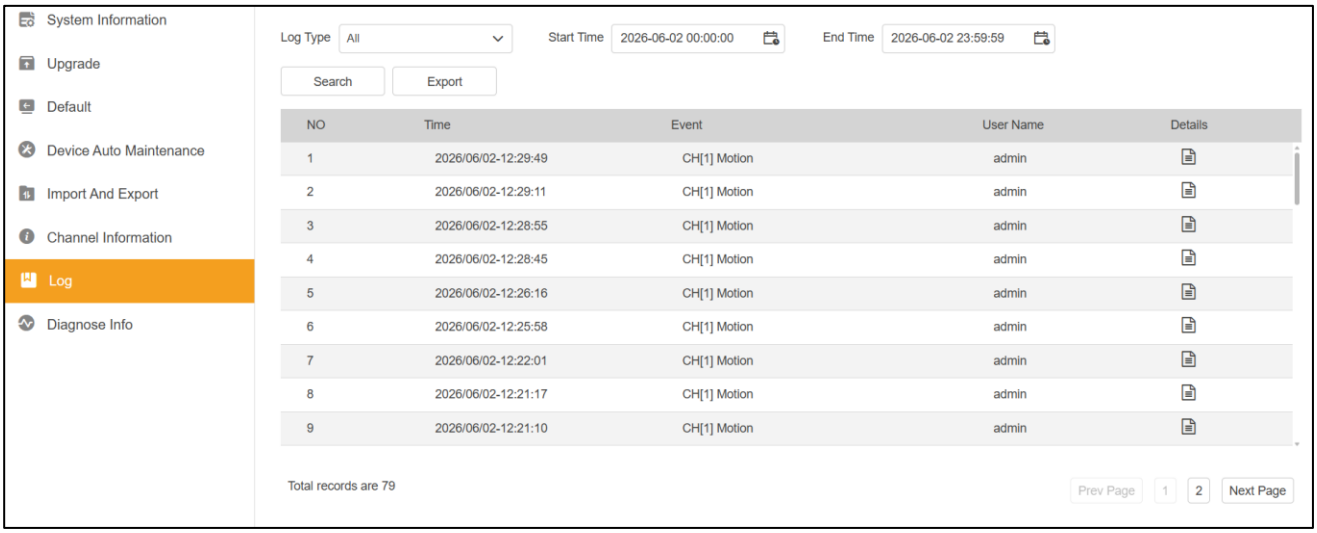


Figure 3-107 Log

Step 2 Select the **Log Type**, including **All**, **Alarm**, **Exception**, **Operation**, and **Parameter Configuration**.

Step 3 Enter the **Start Time** and **End Time** to define the log period you want to view.

Step 4 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.

Step 5 Click **Export** to download the displayed logs for backup or analysis.

3.8.8 Diagnose Info

The Diagnose Info section allows you to view, search, and export diagnostic log packages generated by the device. These diagnostic files contain system information and operational data that can be used for troubleshooting, maintenance, and technical support purposes.

Step 1 Navigate to **Maintain** > **Diagnose Info**.

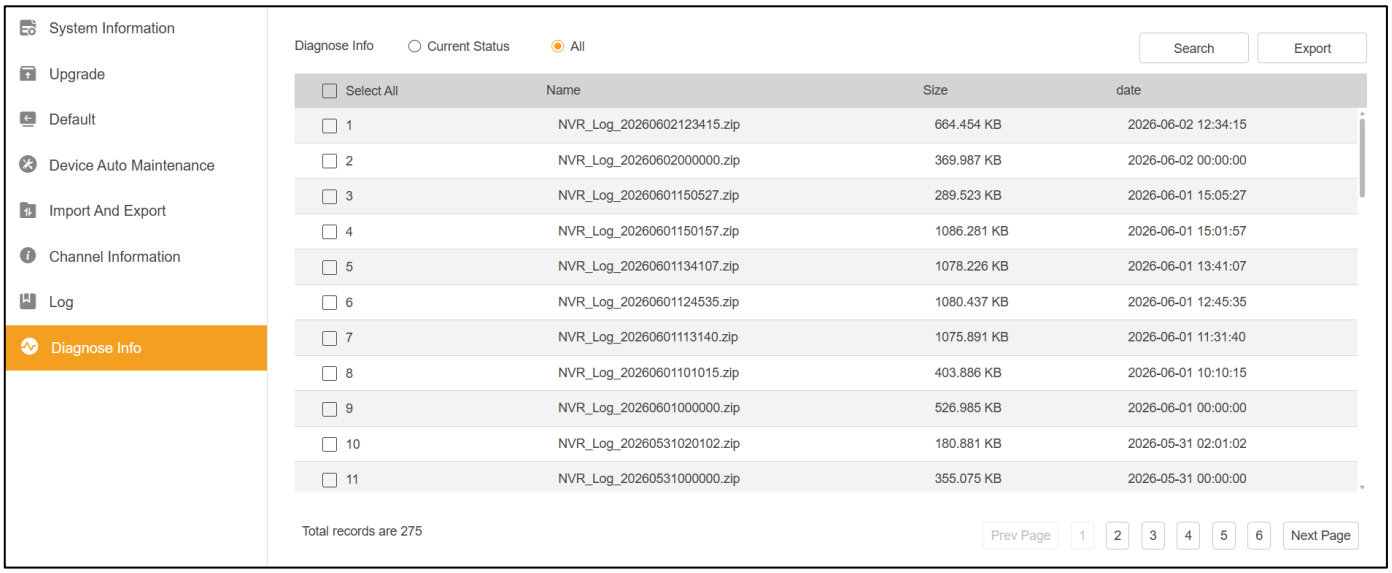


Figure 3-108 Diagnose info

Step 2 Select the diagnosis info type:

- **Current Status:** To view the latest diagnostic package.
- **All:** To display all available diagnostic packages.

Step 3 Click Search to retrieve diagnostic records.

Step 4 Select the diagnostic package and click **Export** to download the selected diagnostic package(s).

4. Local Operations

4.1 Local Login

Log in to the Device to perform local operations.

- If you have configured an unlock pattern, the unlock pattern login window is displayed. Click **Forgot Pattern** to switch to password login.
- If you did not configure an unlock pattern, the password login window is displayed.

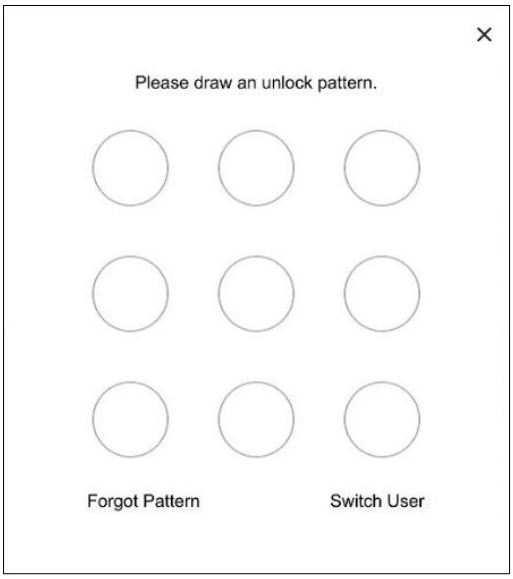


Figure 4-1 Unlock pattern login



Figure 4-2 Password login

Draw the unlock pattern or enter your password and click **Login** to access the local interface of the device.

You can reset the password using the security questions, a reserved email address, or a mobile number if you forget the admin account password. For details, see 3.2 Resetting Password section.

4.2 Main Menu

After logging in, right-click the live page and click **Exit Full Screen** to open the main menu page.

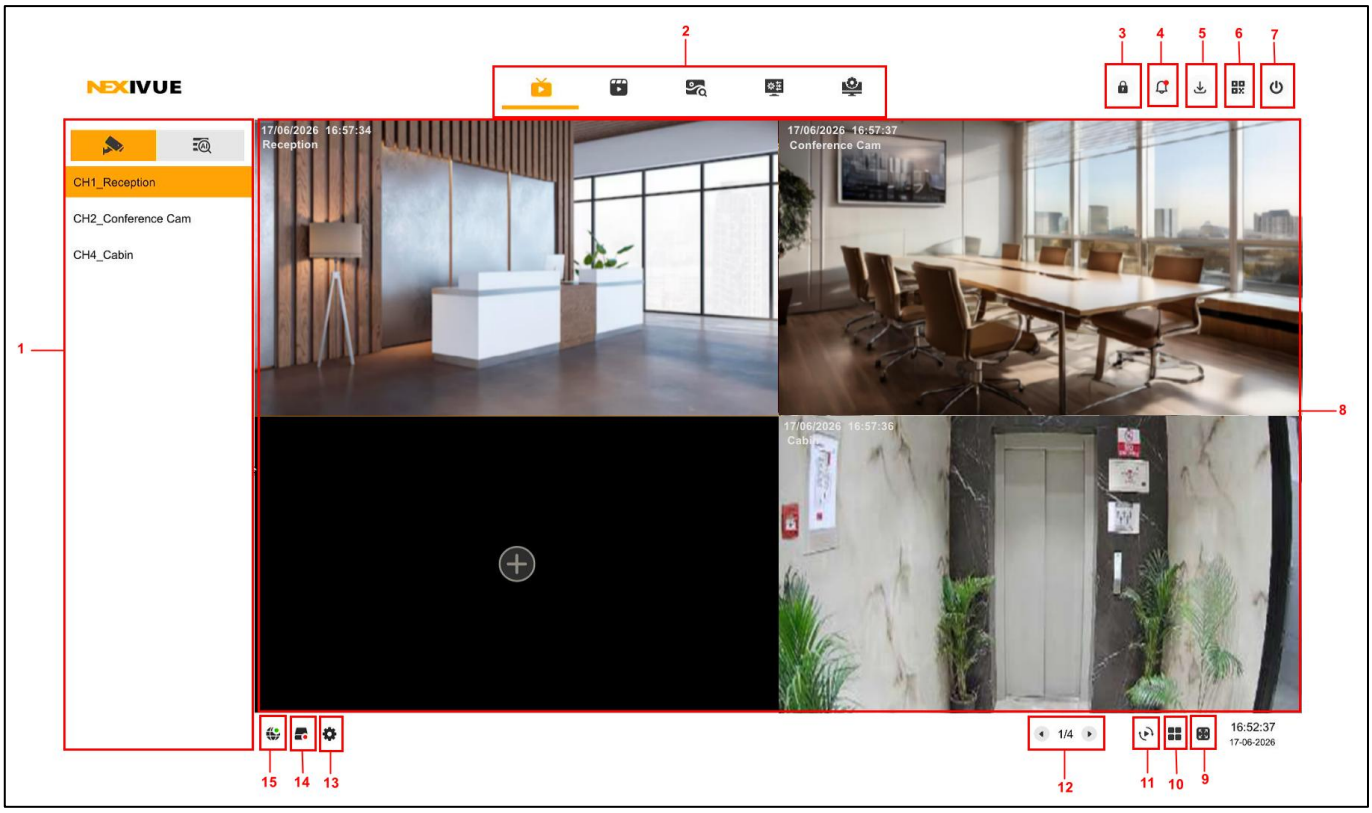


Figure 4-3 Main menu page

No.	Option	Description
1	Live Stream & Target Detection	• Displays the list of cameras connected to the device. • Click to select the target for detection in the live view, including, human detection, vehicle detection and face detection.
2	Configuration Options	Configure the settings of Live view, Playback, Backup, Settings, and Maintenance.
3	Lock Screen	Locks the current user session to prevent unauthorized access. A password is required to unlock the screen.
4	Alerts	Displays active alarms, event notifications, system warnings, and other alert messages generated by the NVR.
5	Download	Indicates the status of the active download, including the download progress and completion state of the file.
6	QR Code	Displays a QR code that can be scanned using the Nexivue mobile application for device addition, remote access, or configuration purposes.
7	Power	Provides power management options, including logout, reboot, and shutdown of the NVR.

8	Live View Layout	Displays the live view screens as per the selection of the window split.
9	Full Screen	Expands the live view display to occupy the entire monitor screen for improved monitoring.
10	Window Split	Divides the live view screen into multiple windows, enabling simultaneous monitoring of multiple camera channels.
11	Start sequence	Automatically switches between selected camera channels or view layouts at predefined intervals.
12	Page Change option	Switches between different pages of camera channels when the number of channels exceeds the current display layout.
13	System Information	Displays detailed information about the system, including device name, firmware version, device type, protocol and web version, channel information and record information.
14	HDD Status	Displays the operational status, capacity, and health information of the installed hard disk drives.
15	Network Status	Displays current network information, including NexiQloud connection status, IP address details etc.

Table 4-1 Description of main menu parameters

4.3 Live View

After you log in, the system goes to multiple-channel live view mode by default. You can view the live video of each channel.

The number of window splits might vary depending on the model you are using.

4.3.1 Live View Control Bar

Hover the cursor over the live video of any channel to display the live view control bar at the bottom center of the video.

If the mouse remains in this area without any operation, the control bar automatically hides.

- The live view control bar is different depending on the model.

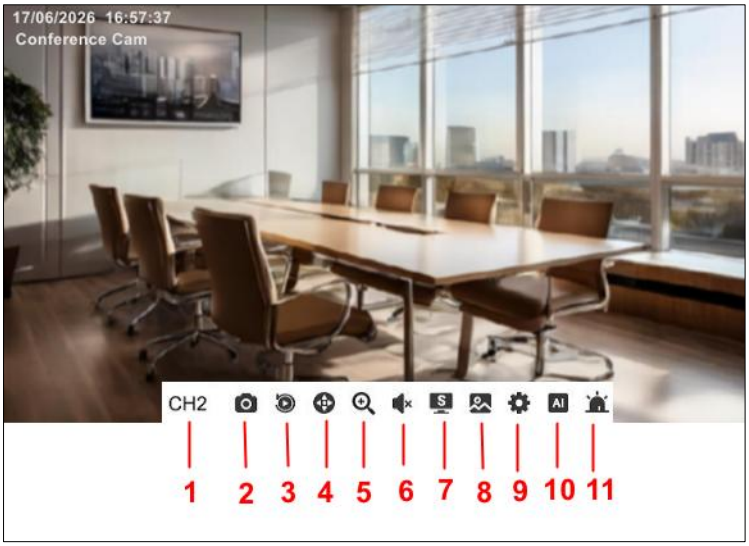


Figure 4-4 Live view control bar

No.	Option	Description
1	Channel No.	Displays the current channel number.
2	Snapshot	Captures an instant snapshot of the current live view.
3	Instant Playback	You can play recordings from the previous 5 minutes of the current channel. • Move the slider to manage the instant playback. • You can pause and close the instant playback. • The information, such as the channel name shielded during instant playback and will not display until you exit playback. • During playback, the screen split layout switch is not allowed.
4	PTZ	Displays PTZ control panel to perform operations such as directing the camera in eight directions, adjusting zoom, focus and iris settings, and quick positioning.

5	Digital Zoom	You can zoom in on a specified zone of the current channel to view details. Click  to zoom in. • Left-click and scroll the mouse to the area where you want to see the zoom-in view. • You can move the red box shown in the mini-view to the area where you want to see the zoom-in view.
6	Audio	Enable or disable the audio of the live video and adjust it accordingly.
7	Stream Switch	Click  to switch the bit stream type of the main stream and sub stream according to the current network bandwidth. • M (main stream): Its bit streams are big, and the definition is high. It occupies a large network bandwidth suitable for video wall surveillance, storage and more. • S (sub stream): Its definition is low, but it occupies a small network bandwidth. It is suitable for general surveillance, remote connection and more.
8	Image Manage	Displays the image configuration panel to configure image parameters, including Brightness, Contrast, Saturation, Sharpness, WDR, Mirror, Corridor mode, Video format, and Day/Night.
9	Preview Policy	Allows you to select a preview policy, including **Real Time**, **Smooth**, and **Balance**.
10	Intelli Rule	Displays the AI rules in the live view page. This function is available on selected models.
11	Alerts	After Alert activation, a preset warning sound and light alarm will be emitted.

Table 4-2 Description of live view control bar parameters

4.3.2 Shortcut Menu

Right-click the live view page to bring up the shortcut menu. You can go to full screen, playback videos, configure view split, and configure the settings of PTZ, image, and more.

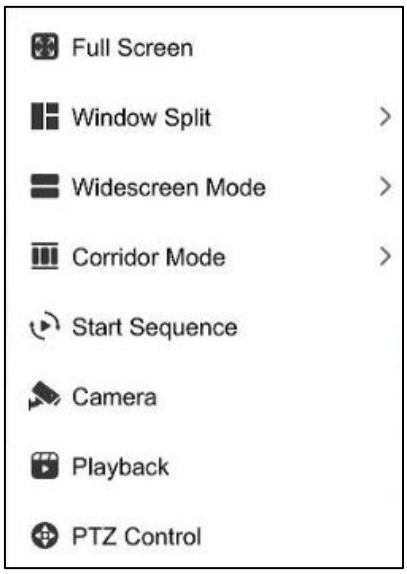


Figure 4-5 Shortcut menu

Option	Description
Full Screen	Displays the selected live view layout in full-screen mode, hiding menus and toolbars for maximum viewing area.
Window Split	Changes the screen layout by dividing the live view into multiple windows (for example, 1, 4, 8, 9, 16, or more channels) to monitor multiple cameras simultaneously.
Widescreen Mode	Adjusts the display layout to fit widescreen monitors, providing an optimized viewing experience and better screen utilization.
Corridor Mode	Selects a corridor-view display layout optimized for cameras installed in vertical scenes such as hallways, aisles, staircases, and passages. You can choose different corridor layouts (1, 3, 4, 5, 7, 9, 10, 12, or 16 windows) to display one or more corridor-mode camera channels efficiently.
Start Sequence	Starts automatic channel switching according to the configured sequence settings, allowing cameras to be displayed one after another at a specified interval.
Camera	Provides quick access to camera-related functions and settings, such as image adjustment, camera information, and other supported camera operations. For details, see 4.6.3 Camera Settings.
Playback	Opens the playback interface to search, review, and manage recorded video footage from the selected camera or channel. For details, see 4.4 Video Playback.
PTZ Control	Opens the PTZ (Pan-Tilt-Zoom) control panel, allowing you to control camera movement, zoom, focus, presets, patrols, and other PTZ functions. For details, see 3.4.1.3 PTZ Panel.

Table 4-3 Description of Shortcut menu options

4.4 Video Playback

On the home page, click the **Playback** icon or right-click live view and select **Playback** to open the Playback page.

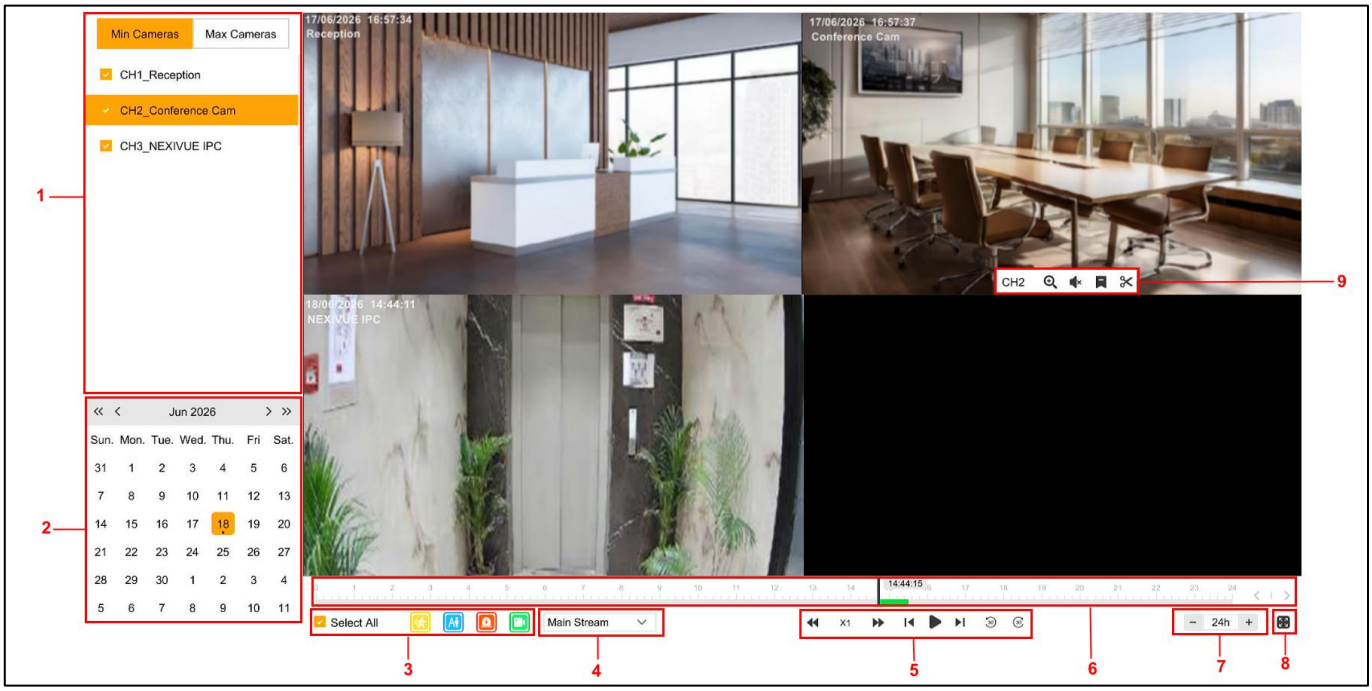


Figure 4-6 Video playback

No.	Option	Description
1.	Camera List Panel	Displays all available camera channels. Select one or multiple cameras to view and search recorded video. The **Min Cameras** tab allows you to select each camera individually, and the **Max Cameras** tab allows you to select all the cameras at once so that you can filter cameras based on the required criteria.
2.	Calendar Panel	Allows users to select a specific date for playback. • Dates marked with orange dots indicate the availability of video playback recordings, regardless of the recording type.
3.	Record Type Indicator	Different-colored icons indicate various recording types. Select the recording type according to the requirement or click **Select All** to select all the types of recording: • : Indicates the **Normal Record** recording type • : Indicates the **Motion Detection** recording type • : Indicates the **Alarm** recording type

		• : Indicates the **Intelligent** recording type.
4.	Stream Type Selection	Allows users to choose the recording stream for playback, such as **Main Stream** or **Sub Stream**, depending on the required video quality and bandwidth.
5.	Playback Control Bar	Contains playback controls such as fast rewind, slow playback, play, pause, stop, fast forward, frame-by-frame playback, and other playback navigation functions.
6.	Timeline Bar	Displays the recording timeline for the selected cameras. Users can drag the time cursor or click a specific time segment to begin playback from that point. Different colors indicate different recording types.
7.	Timeline Zoom Controls	Allows users to zoom in or out of the timeline scale to view recordings in greater detail or over a broader time range.
8.	Full Screen	Expands the playback video screen to full-screen mode for a larger and clearer view, hiding other interface elements.
9.	Channel Quick Action Toolbar	Provides quick access to channel-specific playback functions, including channel identification, digital zoom, audio enable/disable, add tag, and video clipping for efficient review and analysis of recorded footage.

Table 4-4 Description of video playback parameters

4.5 Backup

This section enables you to search and retrieve backed-up videos and snapshots based on selected record types and search criteria. Supported search categories include Video Recordings, Snapshots, Events, Human Detection, Vehicle Detection, and Face Detection records, allowing you to quickly locate and review specific footage.

Step 1 On the home page, click the **Backup** icon to open the backup page.

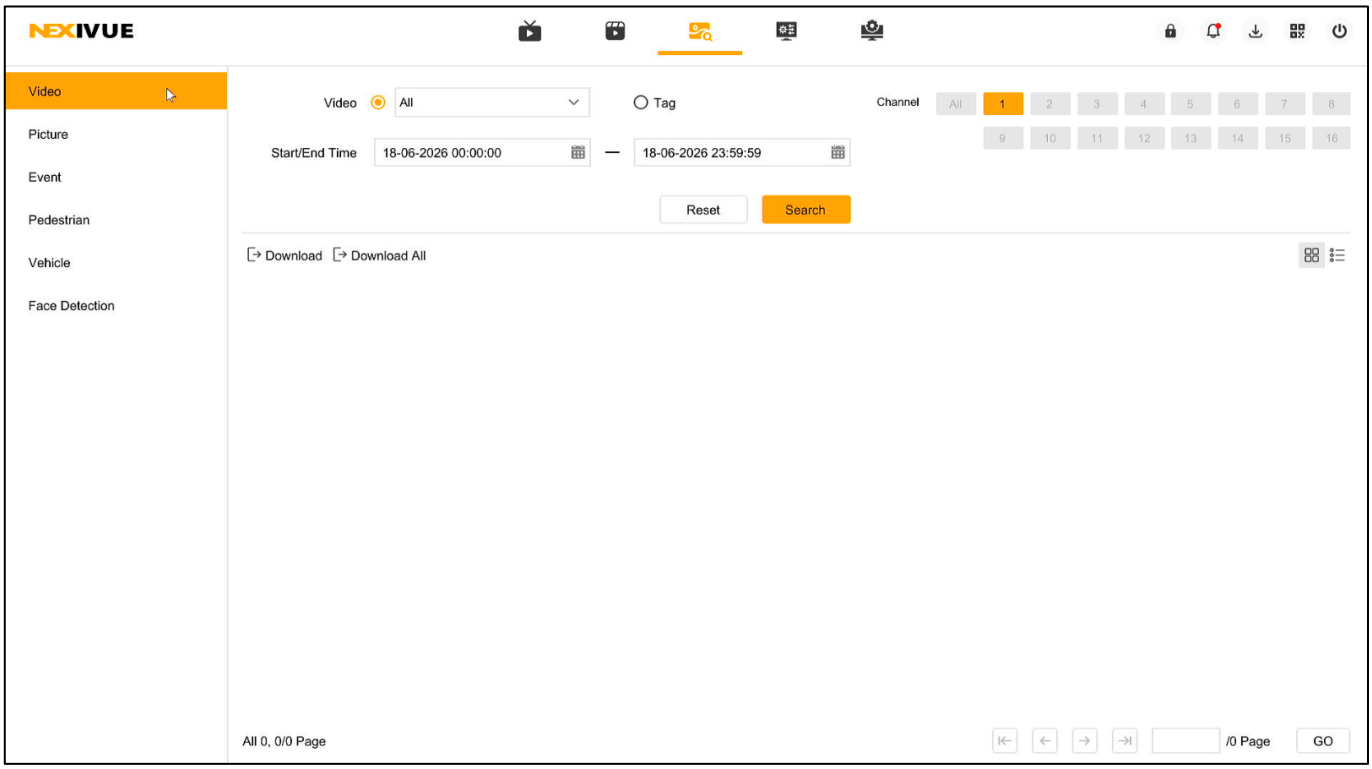


Figure 4-7 Video backup

Step 2 From the left navigation pane, select **Video**.

Step 3 Choose the desired **Video Type** from the drop-down list, such as Motion, Region Entrance, Region Exiting, Intrusion Detection, Line Crossing Detection, or All.

Step 4 Specify the **Start Time** and **End Time** for the search.

Step 5 Select the desired Channel(s) to search recordings from.

Step 6 (Optional) Select **Tag** to display the videos that contain any tag.

Step 7 Click **Search** to display the matching video records.

Step 8 Click **Download** to download the selected recording or click **Download All** to download all search results.

- The search procedure for **Picture**, **Event**, **Pedestrian**, **Vehicle**, and **Face Detection** records is similar. Select the corresponding category from the left navigation pane and configure the available search criteria before clicking **Search**.

4.6 Settings

This section allows you to configure and manage various system settings, including system setup, network configuration, camera settings, event management, recording parameters, and alert notifications.

On the home page, click the **Settings** icon to open the settings page.

4.6.1 System Setup

You can configure general system settings, manage display tour options, and set up user accounts and access permissions.

4.6.1.1 General Settings

To configure general settings parameters, refer to 3.5.1.2 General section.

4.6.1.2 Display Tour

This feature allows the NVR to automatically cycle through selected camera channels in a predefined split-screen layout. This enables continuous monitoring of multiple cameras without requiring manual channel switching.

Sequence

Step 1 On the home page, navigate to **Settings** > **System Setup** > **Display Tour > Sequence**.

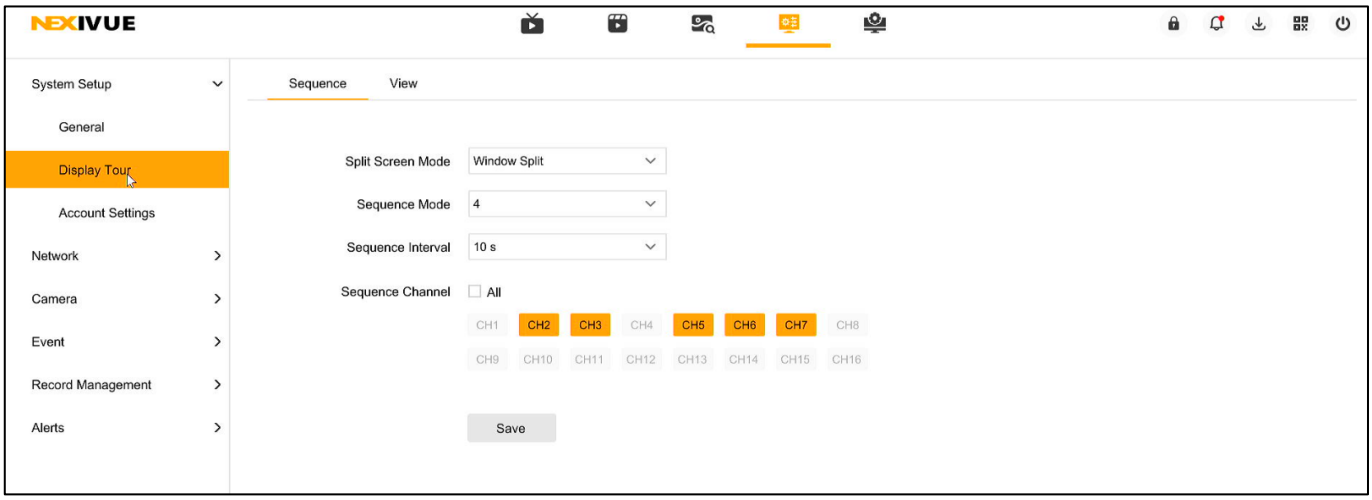


Figure 4-8 Display tour

Step 2 Configure the display tour parameters.

Parameter	Description
Split Screen Mode	Select the display layout used during the tour sequence. The selected layout determines how many camera channels are displayed simultaneously on the screen. The options include **Window Split**, **Widescreen Mode**, and **Corridor Mode**.
Sequence Mode	Specifies the screen division mode for the display tour, such as 1-window, 4-window, 8-window, or other supported layouts.

Sequence Interval	Defines the amount of time each set of channels is displayed before the system automatically switches to the next set in the sequence.
Sequence Channel	Select the camera channels to be included in the display tour. Only the selected channels will participate in the automatic channel rotation. Select **All** to select all available channels for inclusion in the display tour sequence.

Table 4-5 Description of display tour parameters

Step 3 Click **Save** to apply the current display tour configuration settings.

View

Step 1 On the home page, navigate to **Settings** > **System Setup** > **Display Tour > View**.

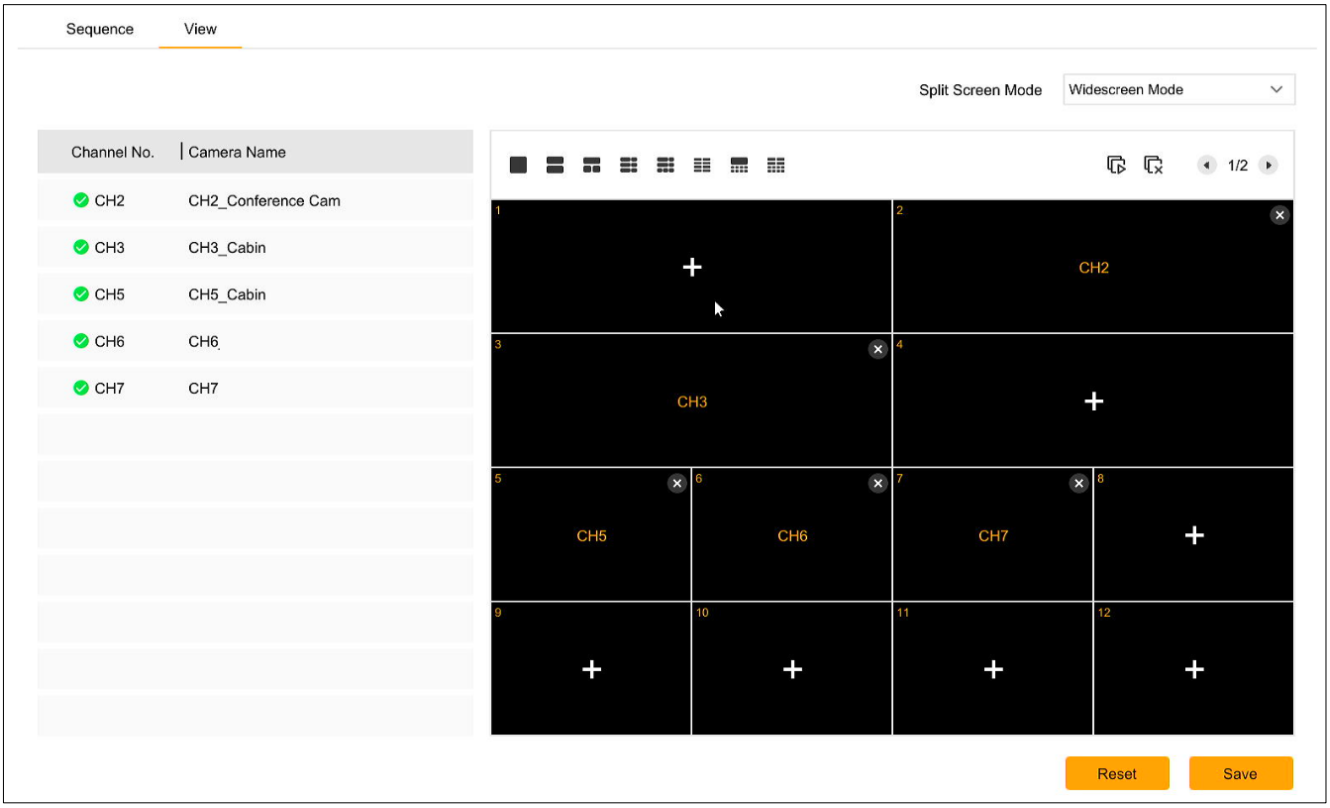


Figure 4-9 View

Step 2 Select the Split Screen Mode (**Window Split**, **Widescreen Mode**, and **Corridor Mode**) and check the layout based on the mode.

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

4.6.1.3 Account Settings

To configure account settings, refer to the 3.5.1.3 Account Settings section.

- Admin password authentication is required before adding or editing an account.

4.6.2 Network Settings

This section introduces network configuration, including basic network settings, NexiQloud, and email settings.

- The device should be connected to the network.
- Certain options and settings may differ based on the web interface version and operational configuration.

To configure the network settings, refer to the 3.5.2 Network section.

4.6.3 Camera Settings

This section allows you to configure and manage camera settings, including adding and upgrading cameras, adjusting network parameters, managing storage, and other related system settings.

4.6.3.1 Camera Management

This page allows you to search, add, and manage IP cameras connected to the system. You can view device details, configure connection settings, and monitor the status of each added camera from this section.

Adding Cameras

Add remote devices to the NVR to receive, store, and manage the video streams of the remote devices.

- Before adding the remote devices, make sure that the devices have been initialized.

Adding Cameras from Search

Search for remote cameras on the same network as the device and then add the remote cameras from the search results.

- Before adding the remote devices, make sure that the devices have been initialized.

Step 1 Navigate to **Settings** > **Camera** > **Camera Management**.

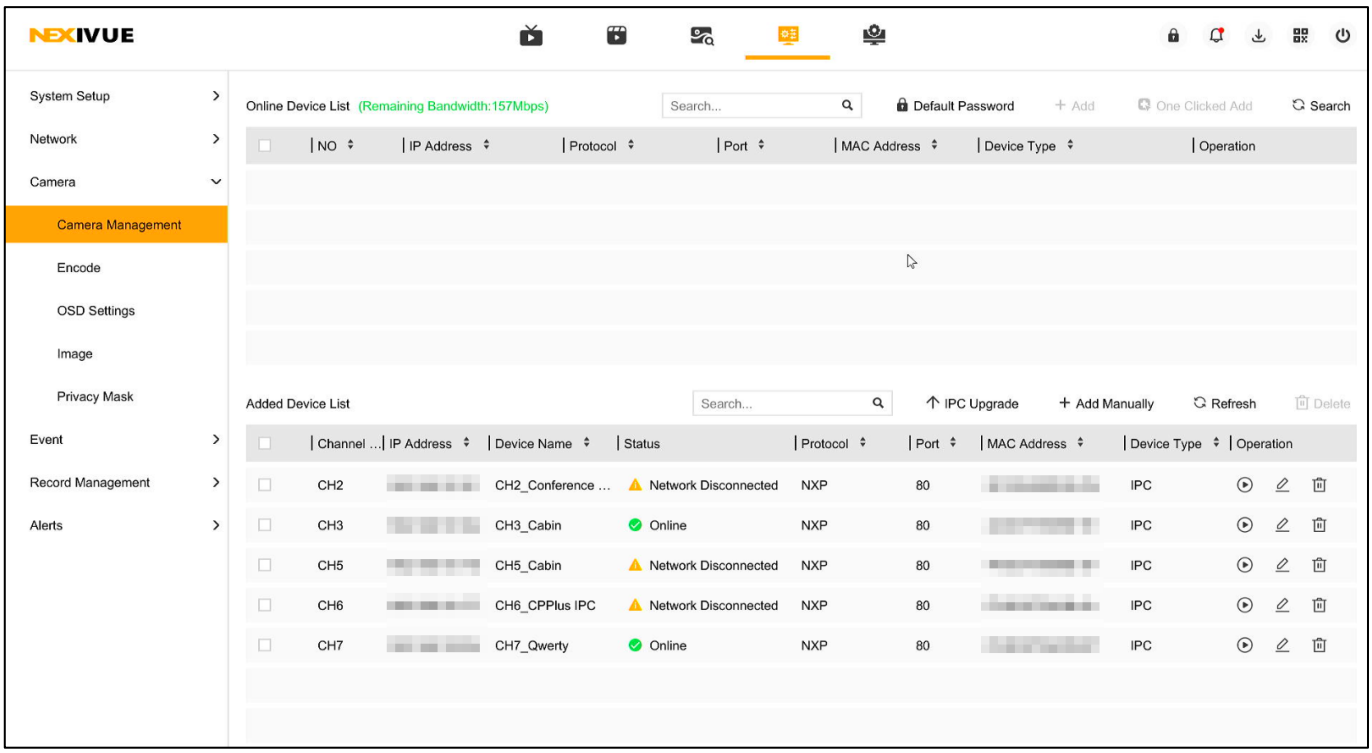


Figure 4-10 Camera Management

Step 2 You can configure a default password so that cameras using this password are automatically added to the **Added Device List** without requiring manual password entry for each device.

a. Click **Default Password**.
b. Enter the admin password for confirmation.
c. Enter the default password. You can keep the default password the same as that of the device password.



Figure 4-11 Default password

d. Click **Confirm** to save the password.

Step 3 Click **Search**.

The remote devices found are displayed under the **Online Device List**. Devices already added are not included in the search results.

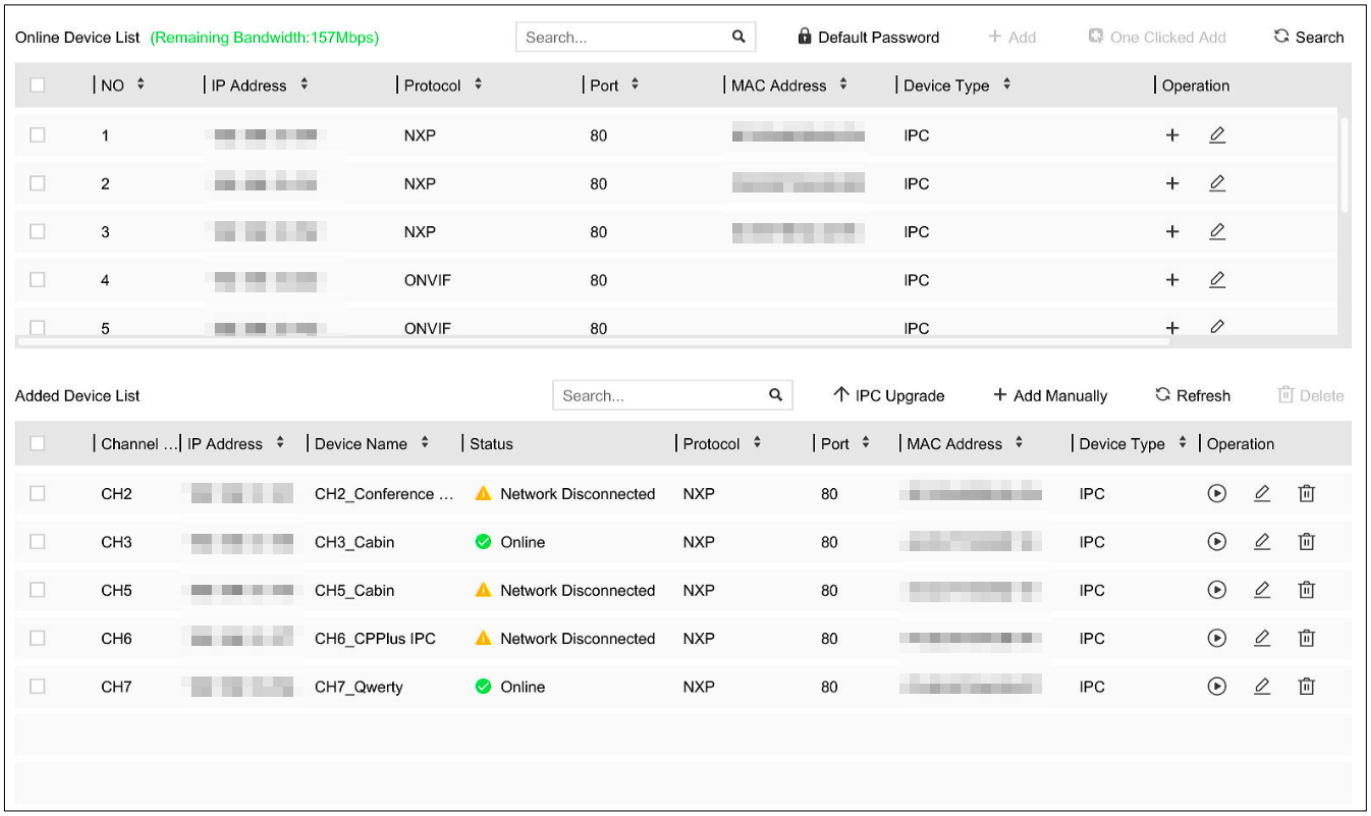


Figure 4-12 Search device

- To filter the remote devices, you can enter all or part of the device name in the **Search** box.

Step 4 Click + icon for the device you want to register to the **Added Device** list.

Related Operations

- Add cameras in batches
  - Select one or more cameras, and then click **Add** to add the cameras.
- Delete cameras.
  - Delete one by one.
    - Click 🗑 to delete the corresponding camera.
  - Delete in batches.
    - Select one or more cameras, and then click **Delete**.
- IPC Upgrade
  1. From the **Added Device List**, select the device that you want to upgrade.
  2. Click **IPC Upgrade**.
  3. From the **Device Name** drop-down list, select the storage device (USB drive) containing the firmware file.
  4. Select the firmware version available on the selected storage device.
  5. Click **Next** to proceed with the firmware upgrade.
  6. Select the channel(s) to be upgraded. If multiple cameras of the same model are connected, you can choose the specific channel(s) as required.
  7. Click **Upgrade** to start the upgrade process.

Adding Cameras Manually

Background Information

Configure the IP address, username, password and other information of the remote device manually and add it to the NVR.

- We recommend this method when you want to add only a few remote devices and know their IP addresses, usernames and passwords.

Step 1 On the home page, navigate to **Settings** > **Camera** > **Camera Management**.

Step 2 Click **Add Manually**.

Step 3 Click **Refresh** to search and display the available cameras on the network.

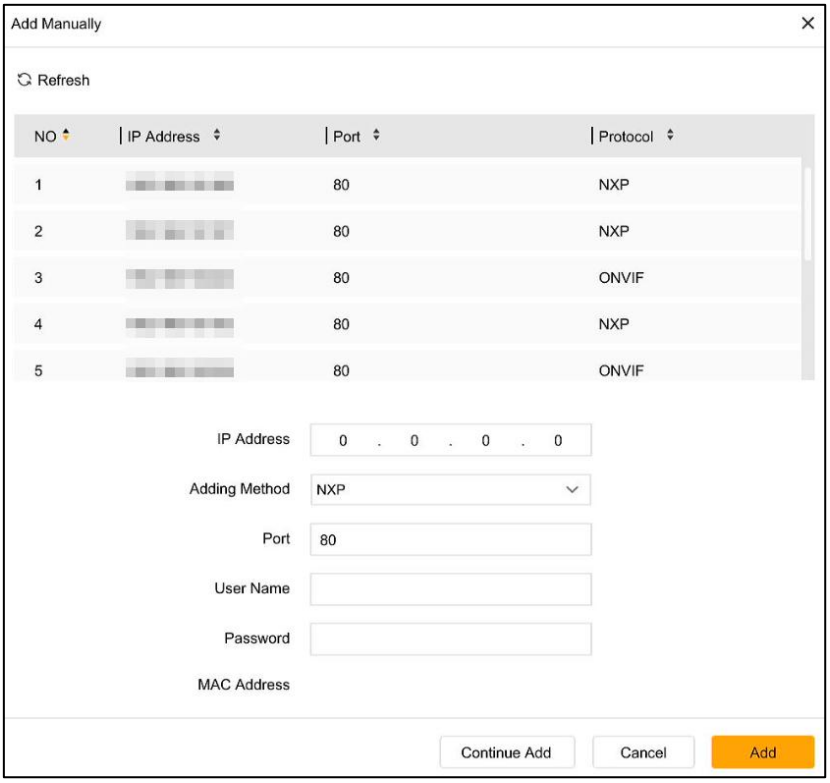


Figure 4-13 Add manually

Step 4 Select the camera that you want to add to the device.

Step 5 Verify the **IP Address** and **Port** number of the remote device.

- If the camera is not available in the search results, manually enter its details to add it to the device.

Step 6 Select the **Adding Method** from the drop-down list (for example, ONVIF, RTSP, or NXP).

Step 7 Enter the user name of the remote device.

Step 8 Enter the corresponding password.

Step 9 Click **Add** to add the selected camera to the device.

Step 10 (Optional) Click **Continue Add** to add multiple cameras one after another.

Modifying the IP Address of a Detected Network Device

This section covers editing the IP address of detected network devices.

Step 1 Navigate to **Settings > Camera > Camera Management**.

Step 2 Under the **Online Device List** tab, click on for the active camera whose IP address you want to modify.

Step 3 Enter username and password of the network device, and then configure the IP address.



Figure 4-14 Edit IP address

Step 4 Click **Confirm** to save the changes.

Changing the Device for a Particular Channel

This section covers the process of replacing or updating the device for a designated channel.

Step 1 Navigate to **Settings > Camera > Camera Management**.

Step 2 Under the **Added Device List** tab, click on for the active camera.

Step 3 Replace the IP address, port number, username, and password of the new device that you want to add to that channel.

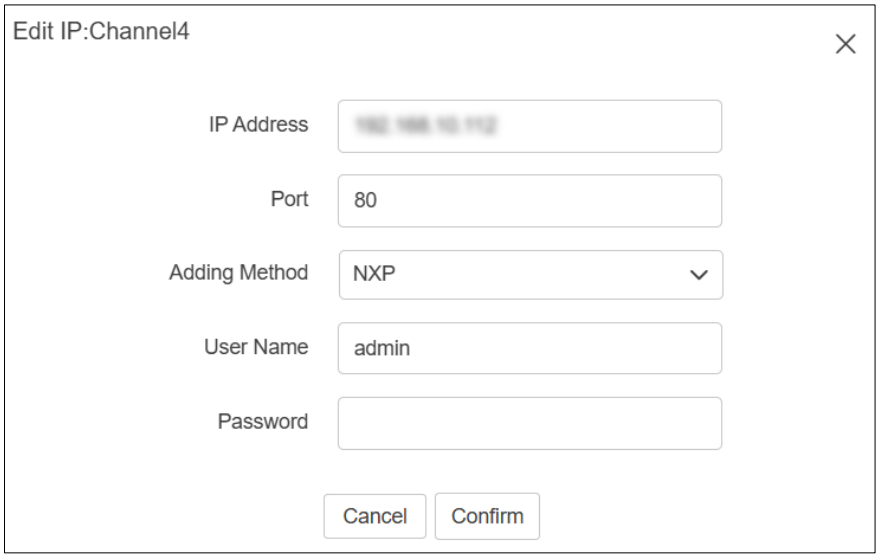


Figure 4-15 Change the device details for a particular channel

Step 4 Click **Confirm** to save the changes.

4.6.3.2 Encode Settings

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

To configure the encode settings, refer to the 3.5.3.2 Encode section.

4.6.3.3 OSD Settings

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 set the OSD on the live screen to the position you want (top left or bottom left). You can also modify the format of the OSD text, time, and date displayed on the preview screen. For more information, refer to the 3.5.3.3 OSD Settings section.

4.6.3.4 Image Settings

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

To configure the image settings, refer to the 3.5.3.4 Image Settings section.

4.6.3.5 Privacy Mask Settings

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.

To configure privacy mask settings, refer to the 3.5.3.5 Privacy Masking section.

4.6.4 Event Settings

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

To configure the event settings, refer to the 3.5.4 Event section.

4.6.5 Record Management Settings

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.

To configure the record management settings, refer to the 3.5.5 Record Management section.

4.6.6 Alert Settings

This section allows you to configure audible notification settings for system events and alarms on supported devices. It helps ensure that important events are promptly brought to the attention of operators through buzzer notifications.

To configure the alert settings, refer to the 3.5.6 Alerts section.

4.7 Maintain

This section provides system management and maintenance options, including firmware upgrades, factory reset, automatic maintenance, configuration backup and restore, channel information, system logs, and diagnostic tools.

On the home page, click **Maintain**  icon, to configure the maintenance settings. For more details, refer to the 3.8 Maintain section.

5. 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 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 on 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 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 to 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 the web service through a secure communication channel.

7) MAC Address Binding

We recommend that you 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