Network Camera

User Manual

V1.02

Contents

Disclaimer and Safety Warnings....1
Preface....1
Legal Statement....2
Safety Warnings....3
1 Device Initialization....5
2 Login....6
3 Live View....8
4 Playback....11
5 Photo....14
6 Snapshot....16
7 Configuration....16
7.1 Common....16
7.1.1 Basic Info....16
7.1.2 Local Parameters....17
7.1.3 Network....19
7.1.4 Time....19
7.1.5 OSD....19
7.1.6 Platform Access....19
7.2 System....19
7.2.1 Time....19
7.2.2 User....21
7.2.3 Log....23
7.2.4 Device Info....23
7.3 Network Configuration....24
7.3.1 Basic Setup....24
7.3.2 Service Configuration....30
7.3.3 Platform Access....35
7.4 Security....40
7.4.1 Network Security....40
7.4.2 Video Security....45
7.4.3 Access Policy....45
7.4.4 Certificate Management....46
7.4.5 Registration Info....49
7.5 Image....49
7.5.1 Image Settings....49
7.5.2 OSD Configuration....55
7.5.3 Privacy Mask....57
7.6 Video & Audio....58
7.6.1 Video....58

7.6.2 ROI....59
7.6.3 Snapshot....61
7.6.4 Audio....61
7.6.5 Media Stream....63
7.7 Smart....64
7.7.1 Smart Settings....64
7.7.2 Metadata Analysis....80
7.7.3 Advanced Parameters....80
7.8 Events....81
7.8.1 Common Alarm....81
7.8.2 One-Key Disarming....88
7.9 Storage....89
7.9.1 Storage Management....89
7.9.2 FTP....92
8 Maintenance....93
8.1 Maintenance....93
8.1.1 Maintenance....93
8.1.2 Network Diagnosis....94
Appendix: Initiative for the Proper Use of Video Products....96

Disclaimer and Safety Warnings

Preface

The content of this section is designed to ensure that users use the product correctly to prevent dangers or property loss caused by improper operation. Before using this product, be sure to read this manual carefully. Please keep this manual properly for future reference.

About This Manual

- We recommend that you use this manual under the guidance of a professional.
- This manual is designed for use with multiple product models, and it is not possible to list the appearance and functions of each product individually. Please refer to the actual product for use.
- This manual is intended for multiple software versions, and the illustrations and descriptions in this manual may be different from the actual GUI and functions of the software.
- Despite our best efforts, technical or typographical errors may exist in this manual. Our company cannot be held responsible for any such errors and reserves the right to change the manual without prior notice.
- Users are fully responsible for the damages and losses that arise due to improper operation.
- Our company reserves the right to change any information in this manual without any prior notice or indication. Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.
- This manual will be updated in real time according to the laws and regulations of the relevant regions. For specific details, please refer to the product's paper copy, QR code, or official website. In case of any discrepancy between the paper copy and the electronic version, the electronic version shall prevail.

About This Product

If the product you have chosen is a video product, please strictly adhere to the applicable laws and regulations. You can visit our official website to inquire about the relevant content.

Instructions for Use

- This document serves as a guide for use only. All statements, information, and suggestions contained in this document do not constitute any express or implied warranty.
- We assume no responsibility for any special, incidental, consequential, or indirect damages resulting from the use of this manual or the use of our products, including but not limited to losses due to loss of business profits, data or document loss, and product malfunction or information leakage caused by cyber-attack, hacker attack, and virus infections.
- Due to uncertain factors such as the physical environment, there may be discrepancies between the actual values of some data and the reference values provided in the manual. In case of any questions or disputes, the company's final interpretation shall prevail.

Formatting Conventions

The UI formatting conventions used in this document are as follows:

Format	Meaning
Bold	Bold means UI elements (button names, menu names, window names, etc.), e.g., Click **Save**.
>	Indicate a sequence of actions, e.g., click Device Management > Add Device, which means first click Device Management, and then click Add Device.

Symbol Conventions

This document uses various distinctive symbols to highlight areas that require special attention during the operation process. The meanings of these symbols are as follows:

Symbol	Meaning
	NOTE: Provides tips and additional information related to the operation and use of the product.
	CAUTION: Alerts to matters that requires attention during operation, as improper handling may lead to product damage, data loss, or functional abnormalities.
	WARNING: The annotations following this symbol demand extra attention, as improper handling could potentially cause personal injury.

Legal Statement

Copyright Statement

©2026 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.

The copyright of any part of this document, including text, images, graphics, etc., belongs to Zhejiang Uniview Technologies Co., Ltd (referred to as Uniview, we, us, our company, hereafter). Without our written permission, no organization or individual may copy, reproduce, translate, modify any part or all of the content of this manual without authorization, nor may they disseminate it in any form.

The products described in this manual may contain software copyrighted by us and any potential licensors. Without the permission of the relevant rights holders, no one may copy, distribute, modify, excerpt, decompile, disassemble, decrypt, reverse engineer, rent, transfer, sublicense, or engage in any other actions that infringe upon the software copyright in any form.

Trademark Acknowledgements

UNV uniview are trademarks or registered trademarks of Uniview.

All other trademarks, products, services and companies in this manual or the product described in this manual are the property of their respective owners.

Export Compliance Statement

We comply with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abide by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, we ask you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will we be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. We strongly recommend that users take all necessary measures to enhance the protection of network, device, data and personal information. We disclaim any liability related thereto but will readily provide necessary security related support.
- To the fullest extent permitted by applicable law, in no event shall we, our employees, licensors, or affiliates be liable for any indirect, incidental, special, consequential, or punitive damages, including but not limited to loss of profits, loss of sales or business, loss of data, or costs of procurement of substitute goods or services, arising out of or related to your use or inability to use the product or service, even if advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of liability for personal injury, or of incidental or consequential damages, so the above limitations may not apply to you.
- To the extent allowed by applicable law, in no event shall our total liability to you for all damages for the product described in this manual exceed the amount of money that you have paid for the product.

- When using this product, please strictly adhere to the applicable laws and regulations to avoid infringing upon the rights of third parties, including but not limited to intellectual property rights, data rights, or other privacy rights. You must also not use this product for the purposes of developing or facilitating the use of weapons of mass destruction, biological or chemical weapons, nuclear weapons, or for any other purposes that violate international norms and regulations.

Privacy Protection Reminder

Uniview complies with applicable privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information.

Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Prevent water or other liquids from entering the device. It may cause device damage and risks such as electric shock and fire.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting us first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.
- Warning: Operating this device in a residential environment may cause radio interference.

Power Requirements

- Install and use the device in strict accordance with your local electrical safety regulations.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Battery Safety

Please use batteries properly; otherwise, there is a risk of fire or explosion.

- Warning: Using incorrect battery models can lead to explosion.
- If you need to replace the battery, it is recommended that you go to an authorized service center or have it replaced under professional supervision. We shall not be held responsible for any issues arising from unauthorized battery replacement.

- When replacing the battery, be sure to use a battery of the same type as the original. Using the wrong model for replacement (such as certain types of lithium batteries) may cause safety protection to fail.
- Batteries must not be exposed to overheat environments such as sunlight, fire, as this may lead to fire, explosion, or combustion.
- Do not dispose of batteries in fire or heating appliances. Do not squeeze, bend, or cut batteries, as it may cause explosion.
- Do not expose batteries to extremely high or low temperatures, or to very low-pressure environments, as this may cause explosion or leakage of flammable liquid/gas.
- For products or the included remote control containing a button cell battery: Do not ingest the battery-chemical burn hazard! If swallowed, a button cell battery can cause severe internal burns within 2 hours and may be fatal. Precautions (including but not limited to):
  - Keep new and used batteries away from children.
  - Stop using the product and keep it away from children if the battery compartment is not securely closed.
  - If you suspect that a battery may have been swallowed or inserted inside any part of the body, seek immediate medical attention.

Network Security

Please take all necessary measures to enhance network security for your device.

The following are necessary measures for the network security of your device:

- **Change the default password and set a strong password:** You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.
  - Do not include the account name or the reverse of the account name.
  - Avoid using consecutive characters, such as 123, abc, etc.
  - Do not use overlapping characters, such as 111, aaa, etc.
- **Keep firmware up to date:** It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit our website or contact your local dealer for the latest firmware.

The following are recommendations for enhancing network security of your device:

- **Change password regularly:** Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- **Enable HTTPS/SSL:** Use SSL certificate to encrypt HTTP communications and ensure data security.
- **Enable IP address filtering:** Allow access only from the specified IP addresses.
- **Minimum port mapping:** Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- **Disable the automatic login and save password features:** If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- **Choose username and password discretely:** Avoid using the username and password of your social media, bank, email account, etc., as the username and password of your device, in case your social media, bank and email account information is leaked.
- **Restrict user permissions:** If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- **Disable UPnP:** When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- **SNMP:** Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- **Multicast:** Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- **Check logs:** Check your device logs regularly to detect unauthorized access or abnormal operations.
- **Physical protection:** Keep the device in a locked room or cabinet to prevent unauthorized physical access.

- **Isolate video surveillance network:** Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

You may also obtain security information under Security Response Center at Uniview's official website.

Cleaning and Dust Removal

Regular dust removal significantly prevents overheating risks, extends hardware lifespan, and ensures stable operation. For dusty areas such as factories and warehouses, clean every 1 to 3 months; for normal offices, clean every 6 to 12 months.

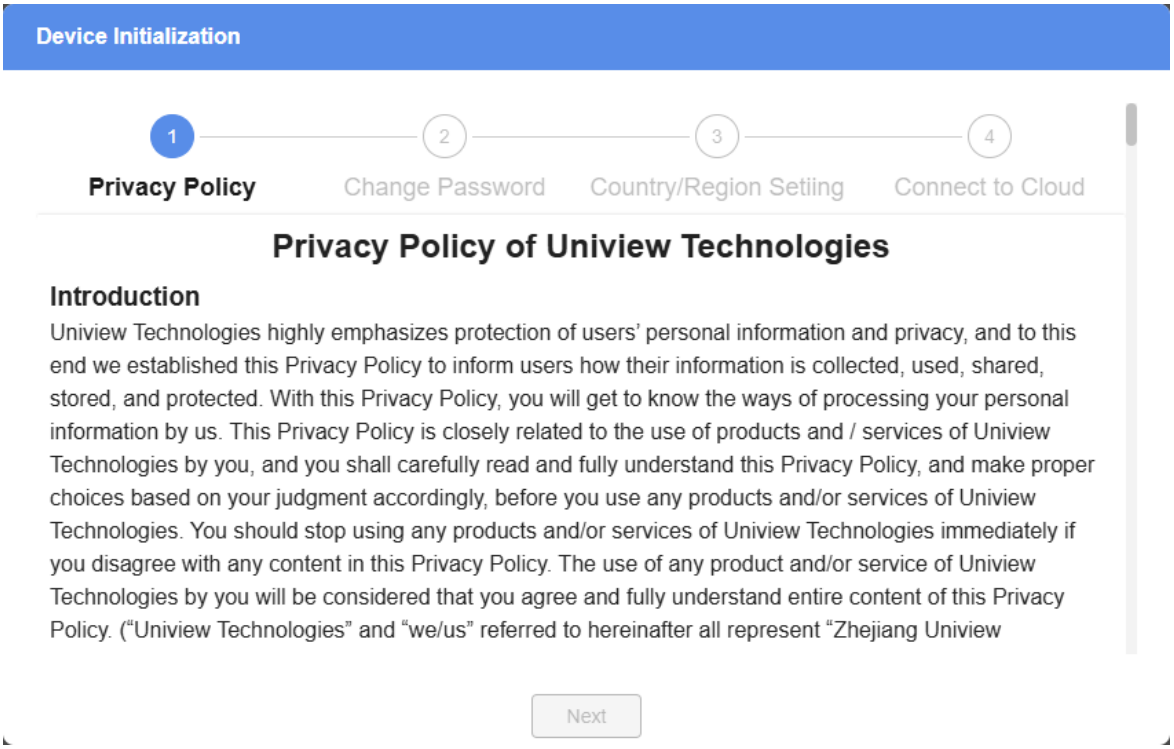
Always power off the device, prevent static discharge, and handle all components gently during operation to avoid equipment damage due to improper operation. After shutting down the device, unplug the power cable to ensure it is completely powered off. It is recommended to allow internal components to cool before cleaning. Please wait at least 5 minutes for devices with fewer than 8 disks, and 15 minutes for devices with 8 or more disks. Pay special attention to cleaning the fan, cooler, internal power supply, etc.

- External cleaning: Use a lightly dampened and well-wrung anti-static cloth to clean dust and stains from the casing. Do not spray alcohol, detergent, or any other liquid directly onto the chassis surface; otherwise, the liquid may cause the interior component corrosion or conductive residue. For stubborn stains, apply a small amount of neutral cleaner to the cloth, wipe the stain, and promptly dry it with a dry cloth.
- Internal cleaning: Wear an anti-static wrist strap or gloves to prevent electrostatic discharge (ESD) damage to electronic components. Use a soft-bristled brush to gently remove accumulated dust from electronic components, fans, and ventilation ports. Stubborn dust may be cleaned using compressed air. Hold the can upright to prevent liquid from spraying out, and keep it at least 10 cm away from components to prevent damage or frost formation caused by rapid temperature change.

1 Device Initialization

Device initialization is a configuration wizard that appears when you log in to the web interface for the first time. It guides you through steps including privacy policy confirmation, changing password, country/region setting, and cloud access configuration to ensure the device is secure and ready to use.

Note: When you log in for the first time, the device initialization wizard is automatically displayed. You must complete all steps before entering the device management interface. The steps may vary depending on the device model and version type, and some steps may not be displayed. Completed initialization steps will not appear again on subsequent logins.



1. After the first login, the device initialization wizard is automatically displayed.
2. (Privacy Policy step) Read the privacy policy content, select "I have read and agree to the above policy", and click **Next**.
3. (Change Password step) Configure the following parameters and click **Next**.

Parameter	Description
Username	The current login username, which cannot be modified.
User Type	The current user type (Admin/Operator/User), which cannot be modified.
Old Password/Admin Password	"Old Password" is displayed for admin users, and "Admin Password" is displayed for non-admin users.
New Password	Set a new password. It must be 9 to 32 characters long and contain uppercase letters, lowercase letters, digits, and special characters.
Confirm	Enter the new password again. It must match the new password.
Email	Used for password reset. It is recommended to fill in this field.
Select Permission	Operators and users can configure the permission scope. Admins have all permissions, which cannot be modified. Users can only select "Live View" and "Playback" permissions.

4. (Country/Region Setting step) Configure the following parameters and click **Next**. After selecting a country/region, the video standard is automatically matched.

Parameter	Description
Region	Select the country or region where the device is located.
Video Standard	PAL or NTSC. It is automatically matched after selecting a country and can be manually modified.

5. (Cloud Access step) Configure the following parameters and click **Finish**.

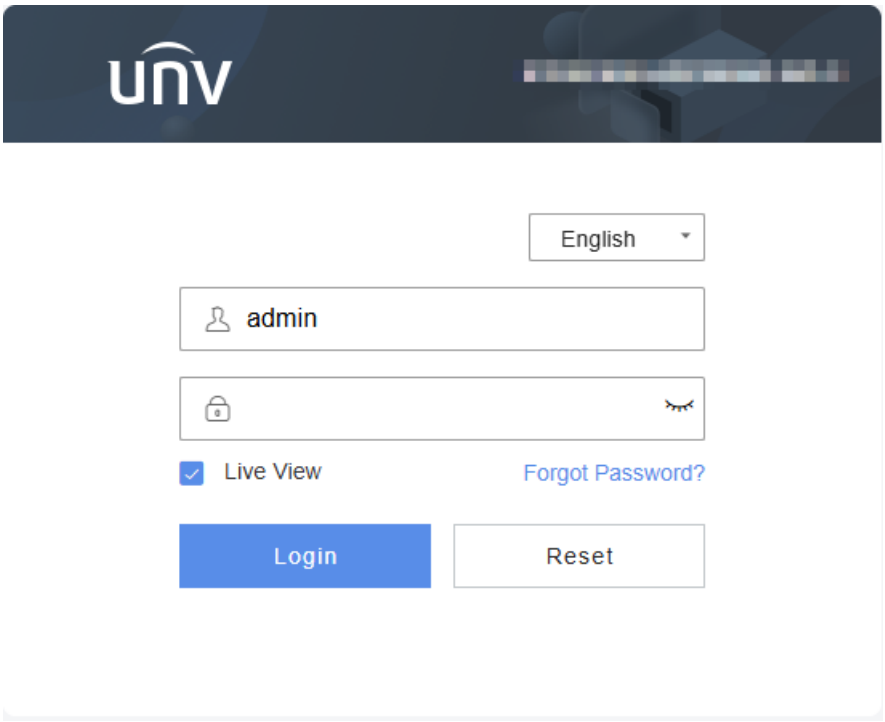
Parameter	Description
EZCloud	Enable or disable the cloud access function. When enabled, the device will connect to the cloud platform. Device information such as IP address and serial number is used only for cloud-based device management. Do not enable this function if you do not agree.
Scan	Displays a QR code. You can add the device by scanning the code with a mobile app.

6. After completing all steps, the page automatically redirects to the live view page.

2 Login

The **Login** page is the entry point to the device web interface. Users authenticate by entering a username and password. After successful authentication, users can access the device management page for configuration and operation.

Note: **Forgot Password?** is unavailable for first-time login. You must change the initial password first. If incorrect passwords are entered beyond the allowed limit, the account will be locked. Wait until the lockout period expires before trying again.



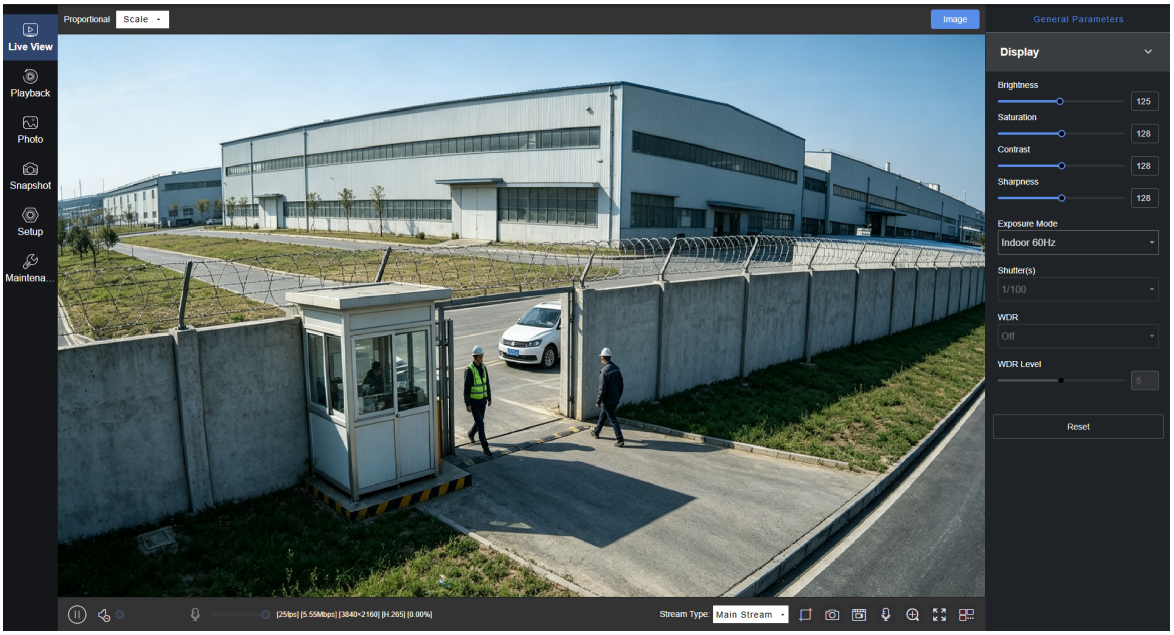
1. Configure the following parameters.

Parameter	Description
Username	The username for logging in to the device. The default username is admin.
Password	The password for logging in to the device. The default password is 123456. Press and hold the icon to view the password.
Language	Select the display language of the page. The available options depend on the languages supported by the device.
Live View	Select this option to automatically play the live view after successful login. For details about the live view feature, see Live View.
Forgot Password?	Click this option when it is not your first login. Scan the QR code to obtain a security code and recover your password.
Reset	Click **Reset** to clear both the **Username** and **Password** text boxes. The **Live View** option will not be reset or cleared.

2. Click **Login** to complete the login.

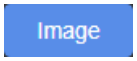
3 Live View

The **Live View** page is used to view the camera video in real time. It supports starting and stopping live view, stream switching, volume adjustment, snapshot, local recording, two-way audio, digital zoom, full screen display, and image parameter adjustment.



Top Toolbar

The top toolbar provides access to **Proportional** and **Image** settings.

Toolbar Button	Description
	Set the display ratio of the video: • **Scale**: Scales the display according to the original aspect ratio of the video. The image is not distorted. • **Stretch**: Stretches the image to fill the entire display area. • **Original**: Displays the video at its original resolution.
	Click to go to the **Image** page and configure parameters such as image adjustment and image scene switch.

Video Window

The video window displays the live view. Double-click the video to display in full screen, and double-click again to exit full screen. When the plugin is not installed, the plugin-free mode is used for playing video.

Bottom Toolbar

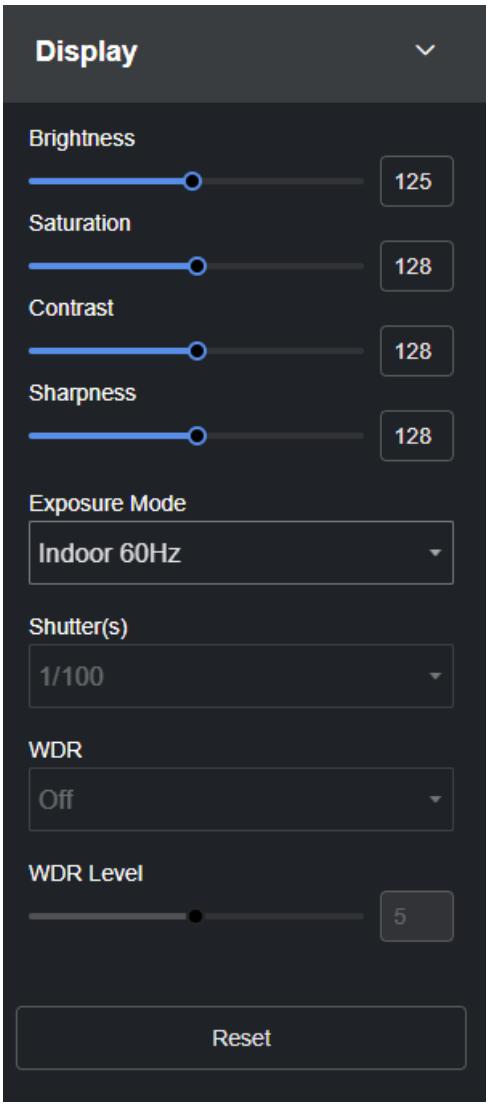
The bottom toolbar provides live view controls and various operation functions.

Toolbar Button	Description
	Start or stop live view.
	Adjust the received volume.
	Adjust the microphone volume during two-way audio.

Toolbar Button	Description
Stream Type: Main Stream	Switch the video stream type: • **Main Stream**: High-quality video stream. • **Sub Stream**: Low-quality video stream that occupies less bandwidth. • **Third Stream**: The third video stream.
	Enable or disable the pixel calculation function, which is used to measure pixel distances on the image.
	Capture the current image and save it to the local device. Available during live view. After the snapshot is completed, a prompt appears. Click **Open** to view the snapshot file.
	Start or stop local recording to record the live view video to the local device.
	Start or stop two-way audio for bidirectional voice communication with the device.
	Enable or disable digital zoom. Draw a box on the image to zoom in on the selected area.
	Switch the video to full screen display.
	Expand or collapse the control panel on the right to adjust image parameters.

Control Panel

After the **Display** panel is expanded, you can adjust image enhancement and exposure parameters.



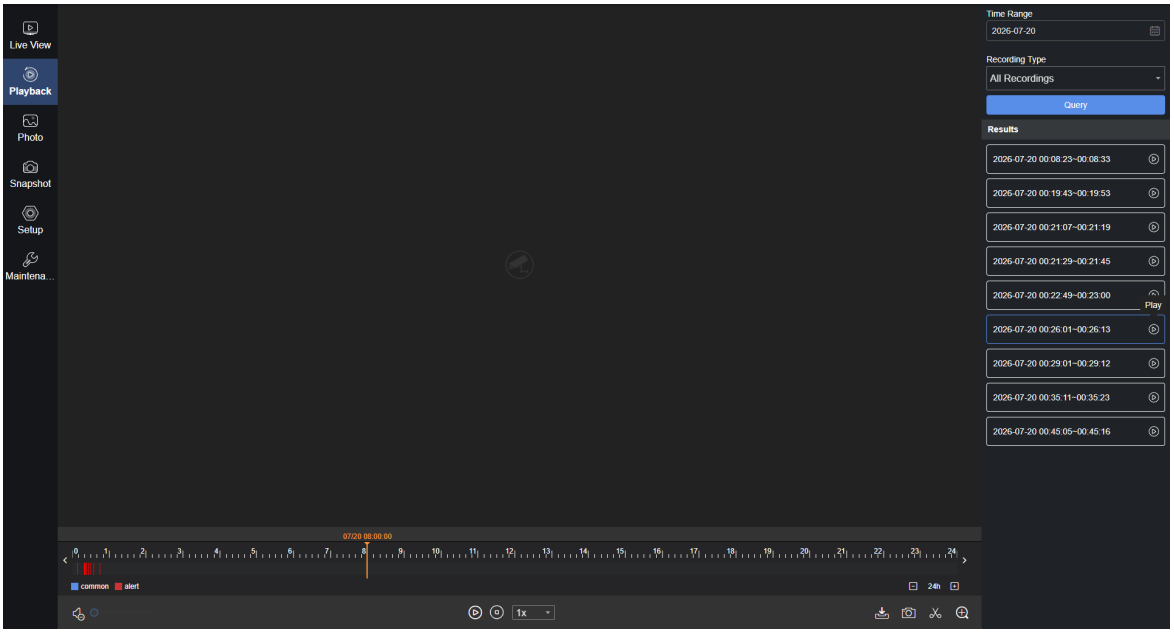
Parameter	Description
Brightness	Adjust the brightness of the image. A larger value indicates a brighter image.
Saturation	Adjust the color saturation. A larger value indicates more vivid colors.
Contrast	Adjust the contrast between light and dark. A larger value indicates stronger contrast.
Sharpness	Adjust the sharpness of the image. A larger value indicates sharper edges.
Exposure Mode	Select the exposure control mode.
Shutter Time	Set the shutter speed. When the unit is microseconds, enter the value directly. When the unit is seconds, select the shutter speed from the dropdown list.
WDR Mode	Select how to enable or disable WDR.
WDR Level	Adjust the WDR intensity. A larger value indicates a stronger WDR effect. This parameter is unavailable when WDR Mode is disabled.
Default	Restore all image enhancement and exposure parameters to factory defaults.

Note:

- When Defog is enabled, WDR Mode is automatically disabled. The two are mutually exclusive.
- If the hard disk space is insufficient during recording, the recording stops automatically.
- Two-way audio requires the device to support the audio intercom function.

4 Playback

The **Playback** page is used to view historical recordings stored on the device. It supports recording search, play/pause/stop playback, speed adjustment, volume adjustment, snapshot, video clipping, recording download, and digital zoom.



Video Window

The video window displays the playback video. Double-click the video to display in full screen, and double-click again to exit full screen. When the plugin is not installed, the plugin-free mode is used for playing video.

Timeline



The timeline displays the recording time segment distribution of the current day. It supports clicking to locate the playback position and scrolling to zoom the time precision. Different colors are used on the timeline to distinguish recording types: normal recording and alarm recording.

Element	Description
Time Scale	Displays the 0–24 hour scale lines. Supports four zoom precision levels: 1h, 6h, 12h, and 24h. Click the zoom in or zoom out icon to switch the precision level.
Recording Segment Color Bar	Displays the recording time segment distribution in the form of color bars. Normal recordings and alarm recordings are distinguished by different colors.
Playback Progress Cursor	Displays the time label and cursor line of the current playback position, which moves in real time as playback progresses.
Page Navigation Buttons	Switch the time offset displayed on the timeline to view the recording distribution of different time periods.
Clip Slider	After entering the clip mode, drag the slider on the timeline to select the start and end time range for clipping.

Bottom Toolbar

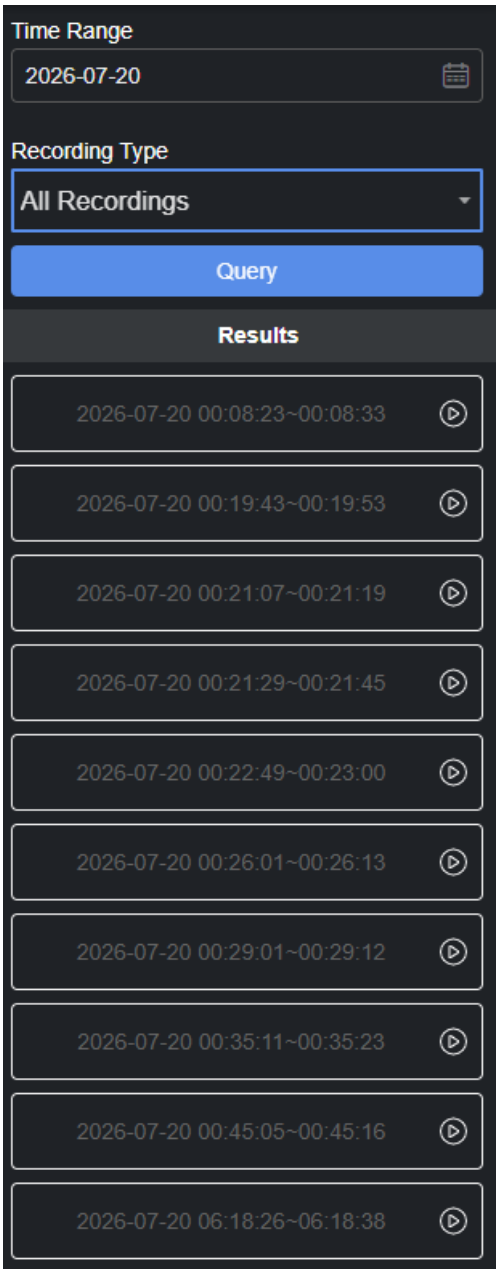
The bottom toolbar provides playback controls and various operation functions.

Toolbar Button	Description
	Start or pause playback.

Toolbar Button	Description
	Stop the current playback and restore the initial state.
	Adjust the playback volume.
	Switch the playback speed.
	Open the recording download dialog box. You can search by conditions and download historical recordings to the local device: • Recording Type: Select the recording type range for download. • Recording Time: Set the time range of the recordings to download. • Alarm Type: When the recording type is alarm recording, select the specific alarm type. • Search: Search for downloadable recording clips by conditions. The search results are displayed in the list. • Recording Download Path: Displays the local save path. Click **Browse** to select the save directory. • Download: After selecting a recording clip, click the **Download** button to save the recording to the local device.
	Capture the current image and save it to the local device. After the snapshot is completed, a prompt appears. Click **Open** to view the snapshot file.
	Enter the clip mode. After selecting a time range on the timeline, click again to open the recording download dialog box and search for and download recording clips within the clip range.
	Enable or disable digital zoom. Draw a box on the image to zoom in on the selected area.

Control Panel

The control panel is used to search recordings and manage playback, including date selection, recording type selection, and search result list.



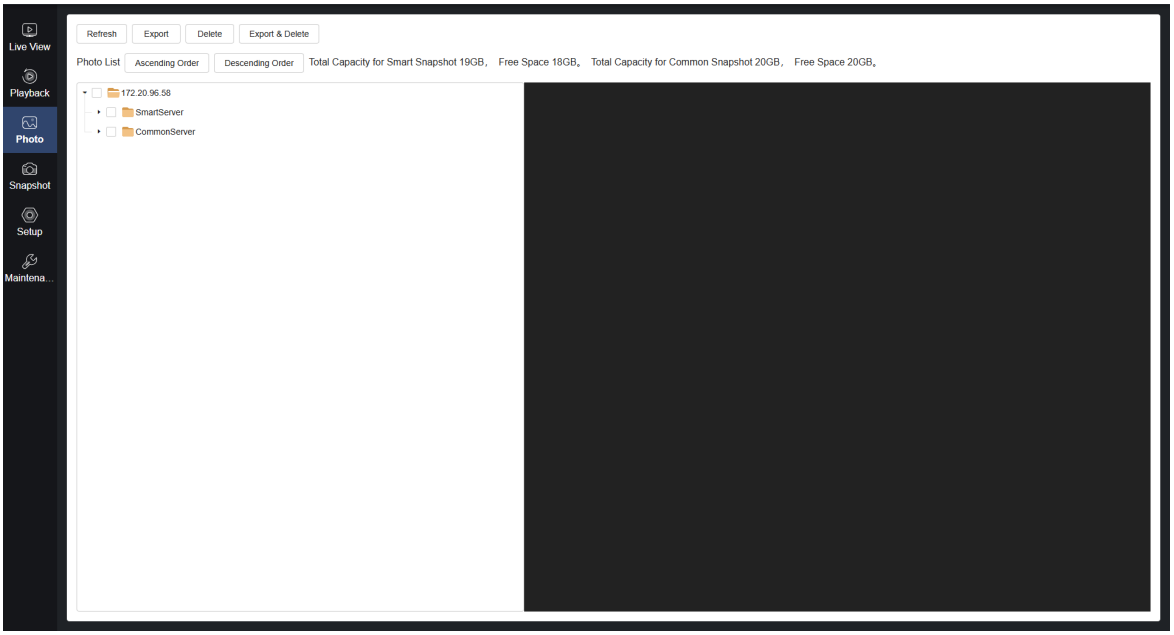
Element	Description
Date Selection	Select the date for searching recordings. Dates with recordings are marked with indicators.
Recording Type	Select the recording type for searching.
Alarm Type	When the recording type is alarm recording, select the specific alarm type, such as motion detection, tampering alarm, cross line detection, enter area, leave area, and intrusion detection. The available options depend on the capability set supported by the device.
Search	Search for recording clips by the selected date and recording type. The search results are displayed in the list.
Search Result List	Displays the recording clips found for the current day. Each clip displays the start and end time. Click the play icon to start playing the recording clip, and click the stop icon to stop playback.

Note:

- The current user must have the recording playback permission.
- Click a recording time segment on the timeline to locate the corresponding position and start playback.
- Digital zoom requires the device to support the digital zoom function.

5 Photo

The **Photo** page is used to view and manage photos stored on the device. It supports browsing photos by directory structure, previewing photos, exporting photos to the local device, deleting photos, and exporting and deleting photos.



Top Toolbar

The top toolbar provides photo management operation buttons.

Button	Description
Refresh	Reload the photo directory tree. After refreshing, the tree restores to the initial expanded state.
Export	Export the selected photos to the local device. You need to select a local save path when exporting.
Delete	Delete the selected photos.
Export & Delete	Export the selected photos to the local device first, and then automatically delete the photos on the device after the export is successful.

List Title Bar

The list title bar displays the photo list title, sort order, and storage capacity information.

Element	Description
Ascending Order	Sort photos in ascending chronological order. Photos taken earlier are displayed first.
Descending Order	Sort photos in descending chronological order. Photos taken later are displayed first.
Total Capacity for Smart Snapshot	Displays the storage space allocated for smart snapshot photos.

Element	Description
Free Space for Smart Snapshot Storage	Displays the available free space for smart snapshot photos.
Total Capacity for Common Snapshot	Displays the storage space allocated for common snapshot photos (page snapshots and alarm-linked snapshots).
Free Space for Common Snapshot Storage	Displays the available free space for common snapshot photos.

Photo Directory Tree

The photo directory tree displays the storage directory of photos on the device in a tree structure. It supports expanding nodes to load subdirectories, clicking leaf nodes to preview photos, and selecting one or more photos via checkboxes.

Element	Description
Directory Node	Displayed as a folder icon. Click to expand and load the subdirectory content.
Photo Node	A leaf node displayed as a photo icon. Click to display the photo in the preview area on the right.
Checkbox	Select photo nodes or directory nodes for multiple selection. After selection, you can perform batch operations such as export and delete.
SmartServer	The smart snapshot photo directory, which stores snapshot images generated by smart analysis.
CommonServer	The common snapshot photo directory, which stores page scheduled snapshot images and alarm-linked snapshot images.

Photo Preview Area

The photo preview area is located on the right side and is used to display the preview of the selected photo.

Note:

- Photo preview on the PC depends on the WebPlugin. The plugin downloads photos to a temporary directory and then displays them.
- A confirmation dialog appears before deleting photos. Proceed with caution, as deleted photos cannot be recovered.
- The Export & Delete operation exports photos first and then deletes them, ensuring data security.

6 Snapshot

The **Snapshot** page displays structured snapshot results reported by smart detection in real time, including snapshot images and metadata of targets such as pedestrians, faces, motor vehicles, and non-motor vehicles.



Pedestrian/Face/Motor Vehicle/Non-Motor Vehicle Area

Element	Description
Thumbnail	Displays snapshot thumbnails, arranged in chronological order of reporting.
Snapshot Detail Dialog	Double-click any snapshot thumbnail to open the corresponding detection detail dialog. The left side of the dialog displays the snapshot image and snapshot time, and the right side displays the thumbnail and metadata list (visible only when metadata display is enabled).

Live Video Area

Located in the middle of the page, playing the real-time video. When the device reports a smart detection event, snapshot data is received in real time via WebSocket and rendered in the corresponding area.

Other Operations

Element	Description
Open Image Folder	Open the local snapshot image storage path.
Clear All Records	Clear the snapshot image list on the current page.

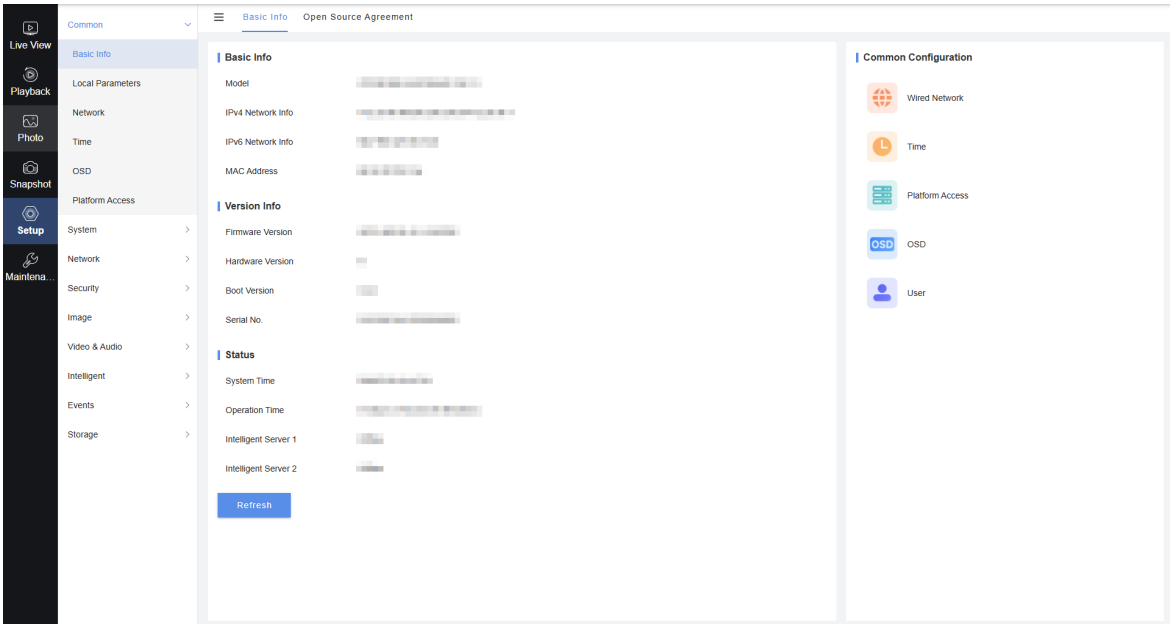
7 Configuration

7.1 Common

7.1.1 Basic Info

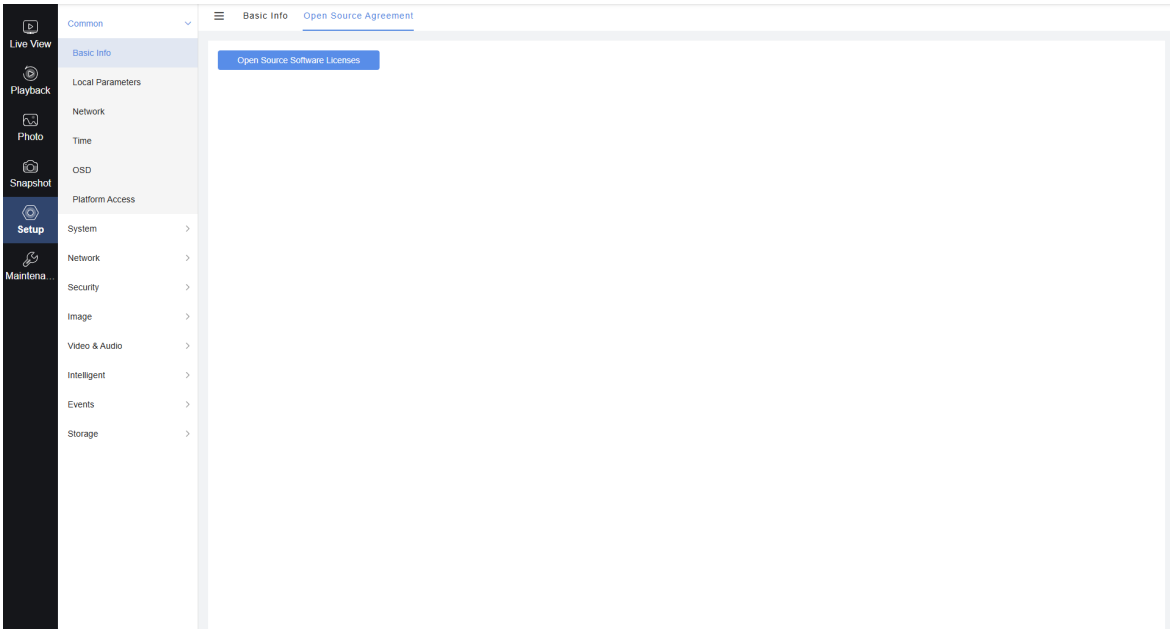
7.1.1.1 Basic Info

This page displays basic info, version info, running status, and common configuration entries.



7.1.1.2 Open Source Agreement

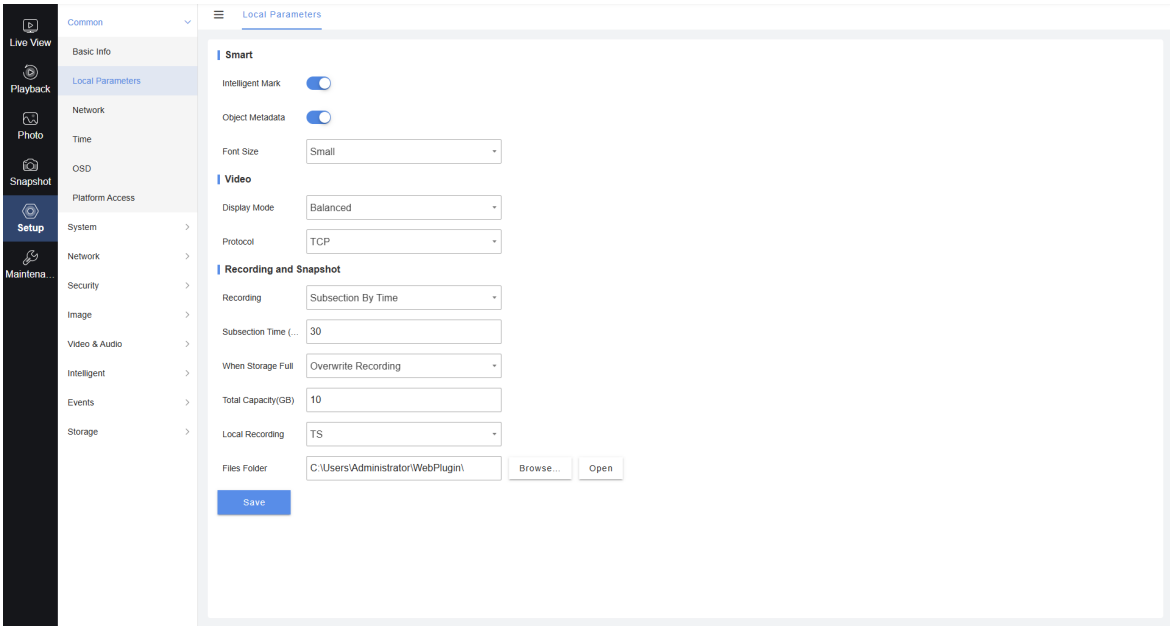
This page displays open source software licenses.



7.1.2 Local Parameters

Local parameters are used to configure client-side live view, recording, and smart display parameters. You need to install the web plugin before operation. The configuration takes effect only on the local client.

Note: Install the plugin before configuring local parameters. Parameters cannot be saved without the plugin. When the streaming protocol is switched to a non-TCP protocol, if the stream adaptive function is enabled on the device, it will be automatically disabled.



Configure the following parameters as needed.

Smart

Parameter	Description
Intelligent Mark	Enable or disable the intelligent mark function. After it is enabled, smart detection results will be overlaid on the live view image.
Target Attribute	Enable or disable target attribute display. After it is enabled, target attribute information will be overlaid on the live view image.
Font Size	Set the font size for target attributes.

Video

Parameter	Description
Display Mode	Select the live view display mode. Options: • **Balanced**: Balances smoothness and latency. • **Fluent**: Prioritizes playback smoothness. • **Minimum Latency**: Prioritizes reducing playback latency. • **Custom**: Manually set the buffer frame count. After selecting this mode, set the custom frame count. A larger value provides smoother live view but increases latency.
Streaming Protocol	Select the streaming protocol for live view. Options: • **UDP**: Transmits via UDP. • **TCP**: Transmits via TCP. When switching to a non-TCP protocol, if the stream adaptive function is enabled on the device, it will be automatically disabled.

Recording & Snapshot

Parameter	Description
Segment Type	Select the segment method for local recording. Options: • **By Duration**: Segments recordings by a specified duration. You need to set the segment duration.

Parameter	Description
	• **By File Size**: Segments recordings by a specified file size. You need to set the segment size.
Overwrite Policy	Select the action when storage space is full. Options: • **Overwrite**: Automatically overwrites the earliest recording files when storage space is full. • **Stop Recording**: Stops recording when storage space is full.
Total Capacity	Set the storage capacity limit for local recording.
Local Recording Format	Select the file format for local recording.
File Path	Displays the save path for local recordings and snapshots. Click **Browse** to change the save path, or click **Open** to open the selected path.

7.1.3 Network

See Wired Port

7.1.4 Time

For details, see Time.

7.1.5 OSD

For details, see OSD.

7.1.6 Platform Access

For details, see Platform Access

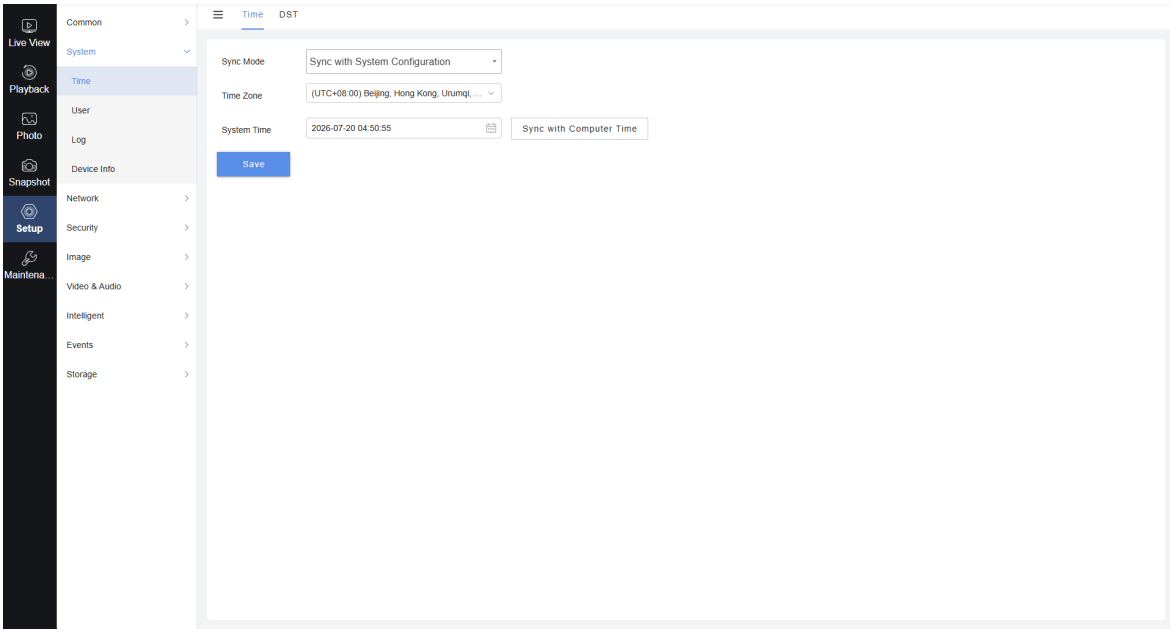
7.2 System

7.2.1 Time

7.2.1.1 Time

By configuring the system time, you can ensure that the device time stays consistent with the actual time. Manual setting and NTP server automatic synchronization are supported to meet time calibration requirements in different scenarios.

Note: The NTP server address supports the IP address or domain name format. The first segment of the IP address ranges from 1 to 223, and 127.x.x.x is not allowed. The domain name must comply with the URL format.



Manual Configuration

Manually set the time zone and system time of the device. This applies to scenarios where network time synchronization is not required.

1. From the Sync Mode dropdown list, select a manual sync mode.
   - **Sync with System Configuration**: Keeps the time consistent with the system configuration time.
   - **Sync with ONVIF Access Time**: Keeps the time consistent with the ONVIF access device time.
   - **Sync with Cloud Server**: Keeps the time consistent with the cloud server time (not supported by some devices).
   - **Sync with Management Platform**: Keeps the time consistent with the management platform time (device support required).
   - **Sync with Photo Server**: Keeps the time consistent with the photo server time (device support required).
2. From the Time Zone dropdown list, select the time zone where the device is located (GMT-12 to GMT+13, including half-hour time zones).
3. In System Time, set the date and time (Format: yyyy-MM-dd HH:mm:ss. Maximum: 2036-12-31 23:59:59).
4. For quick synchronization, click **Sync with Computer Time**. The device time will automatically be consistent with the current computer time.
5. Click **Save** to complete the configuration.

NTP Synchronization

Automatically calibrate the device time through an NTP server. This applies to scenarios that require precise time synchronization.

1. From the Sync Mode dropdown list, select an NTP sync mode.
   - **Sync with NTP Server**: Synchronizes with the specified NTP server time.
   - **Sync with Latest Server Time**: Automatically obtains the latest time from all available servers and displays the NTP configuration area.
2. From the Time Zone dropdown list, select the time zone where the device is located (GMT-12 to GMT+13, including half-hour time zones).
3. Configure the following parameters.

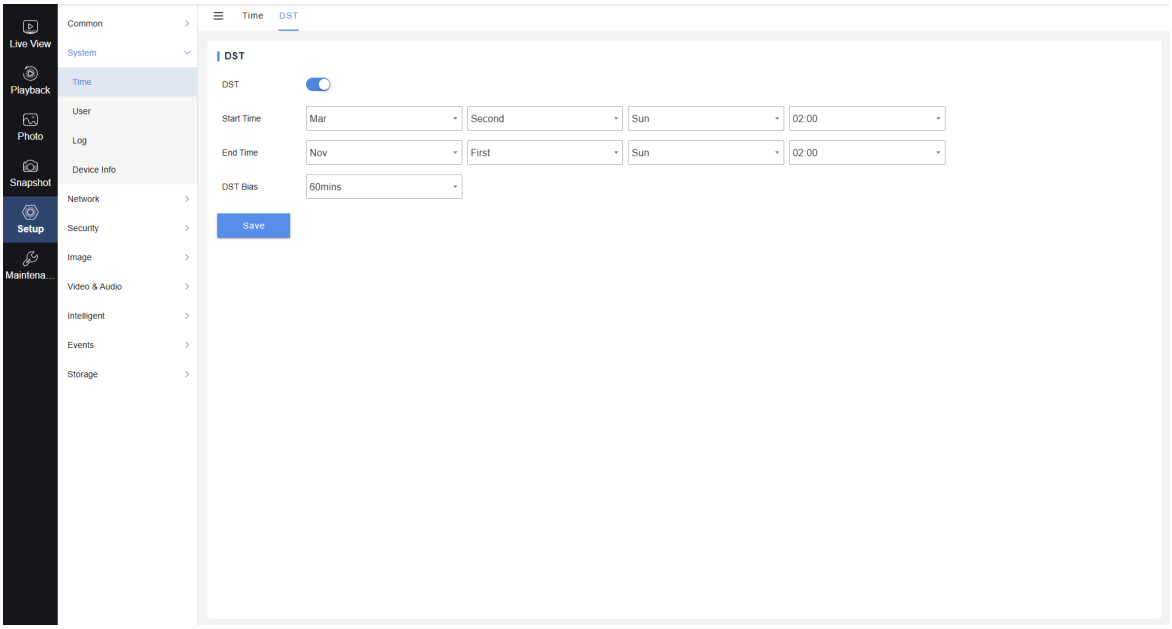
Parameter	Description
NTP Server Address	Enter the IP address or domain name of the NTP server. Click **Test** to verify the connectivity to the server.

Parameter	Description
Port	Enter the NTP server port number.
Update Interval (s)	Enter the update interval for NTP time synchronization.

4. Click **Save** to complete the configuration.

7.2.1.2 DST

By configuring the DST start time, end time, and bias, the device can automatically adjust the system time during the DST period to adapt to time changes in regions that observe DST.



Note: The DST start and end months cannot be the same.

1. Click to enable DST.
2. Configure the following parameters.

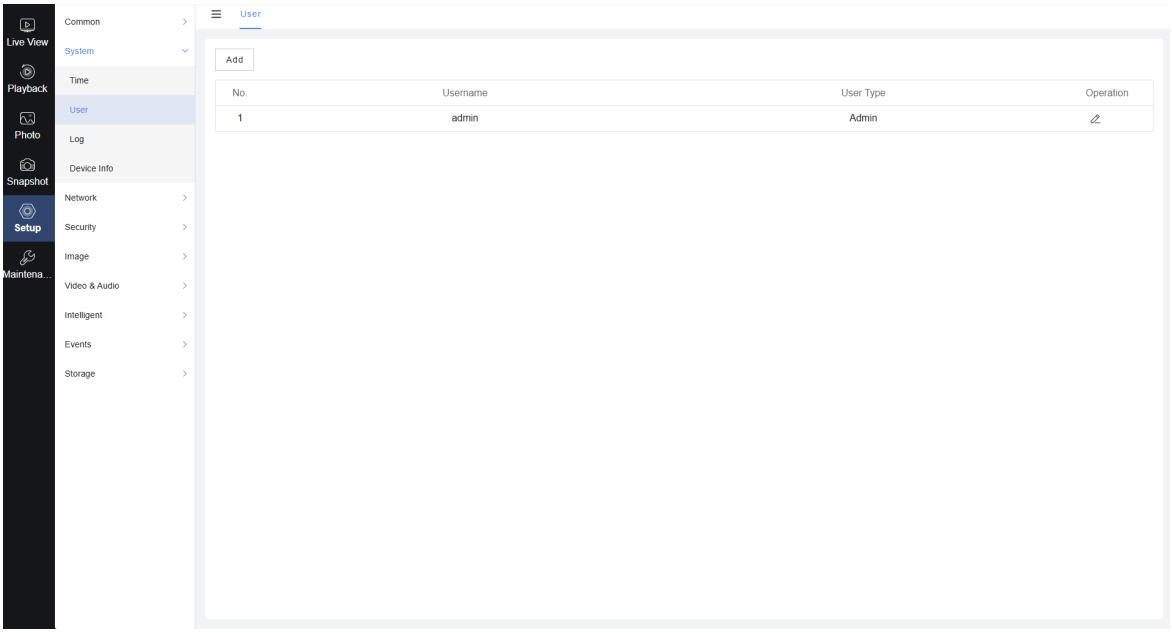
Parameter	Description
Start Time	Set the DST start time, including month, week, day of the week, and hour. • Month: January through December. • Week: First, Second, Third, Fourth, or Last. • Day of the Week: Monday through Sunday. • Hour: 00:00 through 23:00.
End Time	Set the DST end time. The parameters are the same as those for Start Time.
DST Bias	Set the time offset during the DST period. Options: 30 minutes, 60 minutes, 90 minutes, and 120 minutes.

3. Click **Save** to complete the configuration.

7.2.2 User

User management is used to manage device user accounts. By adding, editing, and deleting users and assigning corresponding permissions, differentiated operation control for different roles is achieved, ensuring secure access to the device.

Note: Admin accounts cannot be deleted.



Add User

1. Click **Add** to go to the user configuration page.
2. Configure the user parameters. The parameters are described as follows.

Parameter	Description
Username	Enter a username. The username cannot be the same as an existing username.
User Type	Select a user type. The options are as follows: • Operator: All permissions are available. • Common User: Only live view and playback permissions are available. Admin cannot be added. Anonymous User and Extended User are built-in types and cannot be added manually.
Password	Set a user password. In some scenarios, a strong password is required (9 to 32 characters, which must contain letters, digits, and special characters).
Confirm	Enter the password again. It must be the same as the password.
Select Permission	Select the permissions to be assigned to the user. The permission items vary by user type. Admin has all permissions by default and they cannot be modified. Operator can select permissions as needed. Common User only displays live view and playback permissions, and live view is selected by default when adding.

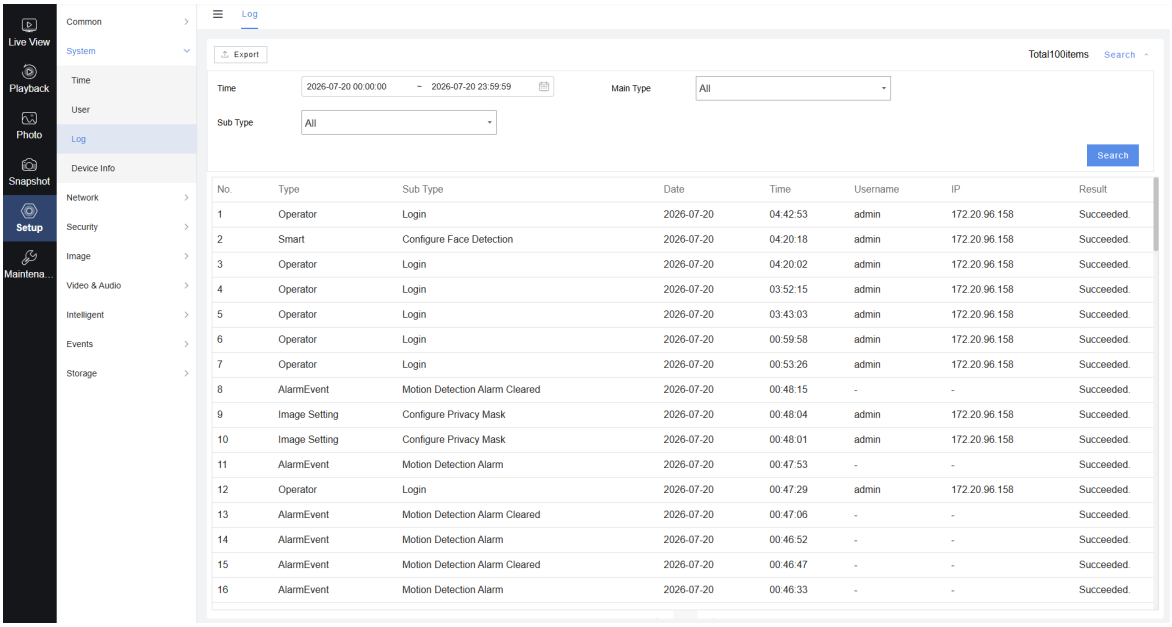
3. Click **OK** to complete adding the user.

Manage User

- Edit a user. In the user list, click of the target entry, modify the parameters, and then click **OK**. The username and user type cannot be modified during editing. For an Admin user, the old password must be entered. For a non-Admin user, the Admin password must be entered. If the password is not modified, no password input is required. If the password of the currently logged-in user is modified, the user will be automatically logged out after the modification is successful.
- Delete a user. In the user list, click of the target entry and confirm to delete it. Admin accounts cannot be deleted.

7.2.3 Log

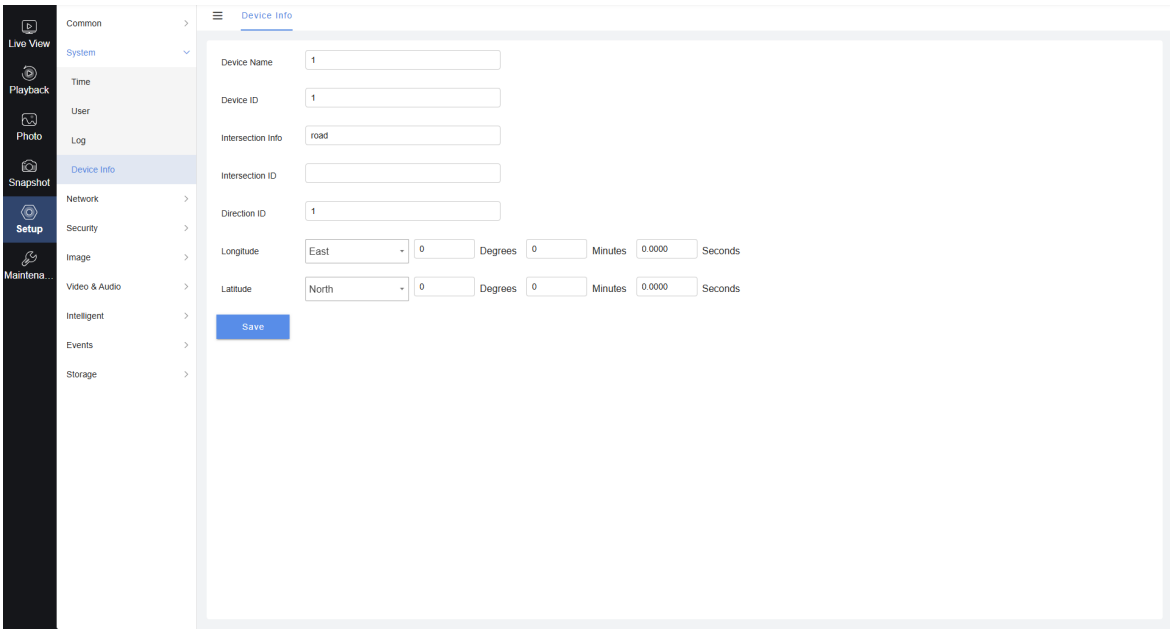
You can view or export device usage status and alarm information by start time, end time, main log type, and sub log type.



7.2.4 Device Info

Device info is used to configure the device identity (device name, ID, and intersection info) and geographic location (latitude and longitude coordinates). It applies to scenarios that require identifying the device deployment location and precise positioning. After configuration, the device location information can be displayed in OSD and on the platform.

Note: Latitude and longitude coordinates and direction ID are displayed only when the device supports the GPS function.



1. Configure the device info parameters.

Parameter	Description
Device Name	The name identifier of the device.
Device ID	The unique ID of the device.
Intersection Info	The name of the intersection where the device is deployed.

Parameter	Description
Intersection ID	The ID of the intersection where the device is deployed.
Forward Direction ID	The ID identifier of the device facing direction.

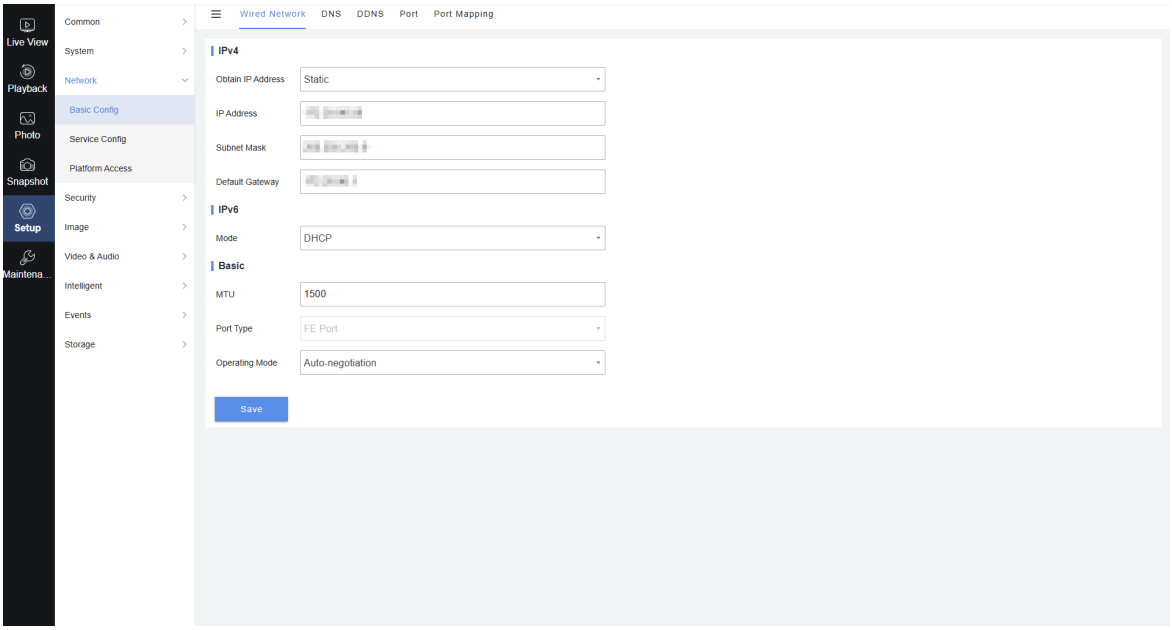
2. Configure the latitude and longitude coordinate parameters. Enter the latitude and longitude in degrees, minutes, and seconds (DMS) format.
3. Click **Save** to complete the configuration.

7.3 Network Configuration

7.3.1 Basic Setup

7.3.1.1 Wired Network

By configuring the wired network port parameters, the device can connect to a wired network and communicate with external devices. Two protocol stack configurations are supported: IPv4 (Static/PPPoE/DHCP) and IPv6.



Note:

- Changing network settings may cause network disconnection. Confirm the configuration before saving.
- After changing the static IP address, the system will automatically attempt to reconnect. If the connection fails, use the new IP address to access the device again.
- In PPPoE mode, the password is encrypted and transmitted using RSA.

IPv4

Configure the IPv4 protocol stack parameters. Select different configuration modes based on the IP obtain method.

1. Select the IP obtain method.

   Select an IP address obtain method based on the network environment. Different methods require different parameters.

   - **Static**: Manually specify the IP address, subnet mask, and default gateway.
   - **PPPoE**: Obtain the IP address through PPPoE dial-up. Enter the username and password provided by the ISP.
   - **Obtain Automatically (DHCP)**: The IP address is automatically assigned by the DHCP server. No manual configuration is required.

Static

Manually specify the IPv4 address, subnet mask, and default gateway. This is applicable to network environments with fixed IP addresses.

1. Set the IP obtain method to **Static**.
2. Configure the following parameters.

Parameter	Description
IP Address	Enter the IPv4 address of the device. The first octet ranges from 1 to 223 (excluding 127). The IP address cannot be the same as the default gateway, and the IP address and the default gateway must be in the same network segment.
Subnet Mask	Enter the subnet mask. In binary form, the mask must consist of all 1s followed by all 0s. The bitwise AND result of the IP address and the mask cannot be a network address or a broadcast address.
Default Gateway	Enter the default gateway address. The first octet ranges from 1 to 223 (excluding 127). The gateway cannot be the same as the IP address and must be in the same network segment. If left blank, the system defaults to 0.0.0.0.

3. Click **Save** to complete the configuration.

PPPoE

Obtain the IP address from the ISP through PPPoE dial-up. This is applicable to broadband dial-up network environments.

1. Set the IP obtain method to **PPPoE**.
2. Configure the following parameters.

Parameter	Description
IP Address	Automatically obtained and displayed by the device after PPPoE dial-up succeeds. No manual configuration is required.
Username	Enter the PPPoE dial-up username. ASCII printable characters are supported.
Password	Enter the PPPoE dial-up password. ASCII printable characters are supported. The password is encrypted and transmitted using RSA.
Confirm	Enter the password again, which must be consistent with the password.

3. Click **Save** to complete the configuration. A success prompt will be displayed after the dial-up succeeds.

Obtain Automatically (DHCP)

The IP address is automatically assigned by the DHCP server. No manual IPv4 configuration is required. This is applicable to DHCP network environments.

1. Set the IP obtain method to **Obtain Automatically (DHCP)**.
2. Click **Save** to complete the configuration. The device will automatically obtain the IP address from the DHCP server.

IPv6

Configure the IPv6 protocol stack parameters. This configuration area is displayed only when the device supports IPv6.

1. Select the mode.

   Select the IPv6 address configuration mode based on the network environment.

   - **Manual**: Manually specify the IPv6 address, subnet prefix length, and default gateway.
   - **Obtain Automatically (DHCP)**: The IPv6 address is automatically assigned by the DHCPv6 server.

Manual (IPv6)

Manually specify the IPv6 address, subnet prefix length, and default gateway. This is applicable to network environments with fixed IPv6 addresses.

1. Set the mode to **Manual**.
2. Configure the following parameters.

Parameter	Description
IPv6 Address	Enter the IPv6 address of the device. The :: abbreviation format is supported. The first segment cannot be ff** or fe8*/fe9*/fea*/feb*, the address cannot be all zeros or ::1 only, and the address cannot be the same as the default gateway.
Prefix Length	Enter the subnet prefix length.
Default Gateway	Enter the IPv6 default gateway address. The first segment cannot be ff** or fe8*/fe9*/fea*/feb*, the address cannot be all zeros or ::1 only, and the address cannot be the same as the IPv6 address.

3. Click **Save** to complete the configuration.

Obtain Automatically (DHCPv6)

The IPv6 address is automatically assigned by the DHCPv6 server. No manual IPv6 configuration is required.

1. Set the mode to **Obtain Automatically (DHCP)**.
2. Click **Save** to complete the configuration. The device will automatically obtain the IPv6 address from the DHCPv6 server.

Basic Parameters

Configure the basic parameters of the network port, including MTU, port type, and operating mode.

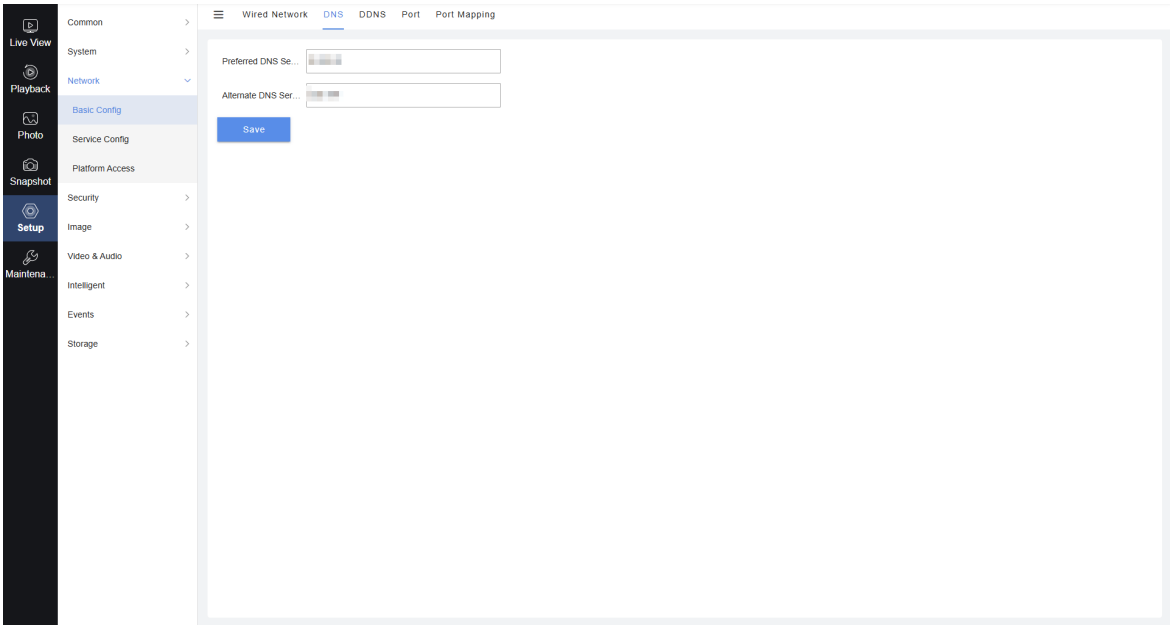
1. Configure the following parameters.

Parameter	Description
MTU	Enter the maximum transmission unit value. This is displayed only in Static or DHCP mode.
Port Type	Displays the physical type of the current network port, determined by the device capability set and not editable. Options: • **RJ45 Port**: RJ45 electrical port • **SFP Port**: SFP fiber port • **EPON Port**: EPON fiber port
Operating Mode	Select the operating mode of the network port.

2. Click **Save** to complete the configuration.

7.3.1.2 DNS

DNS resolves domain names into IP addresses. By configuring the preferred and alternate DNS server addresses, the device can resolve domain names into corresponding IP addresses to properly access network resources.



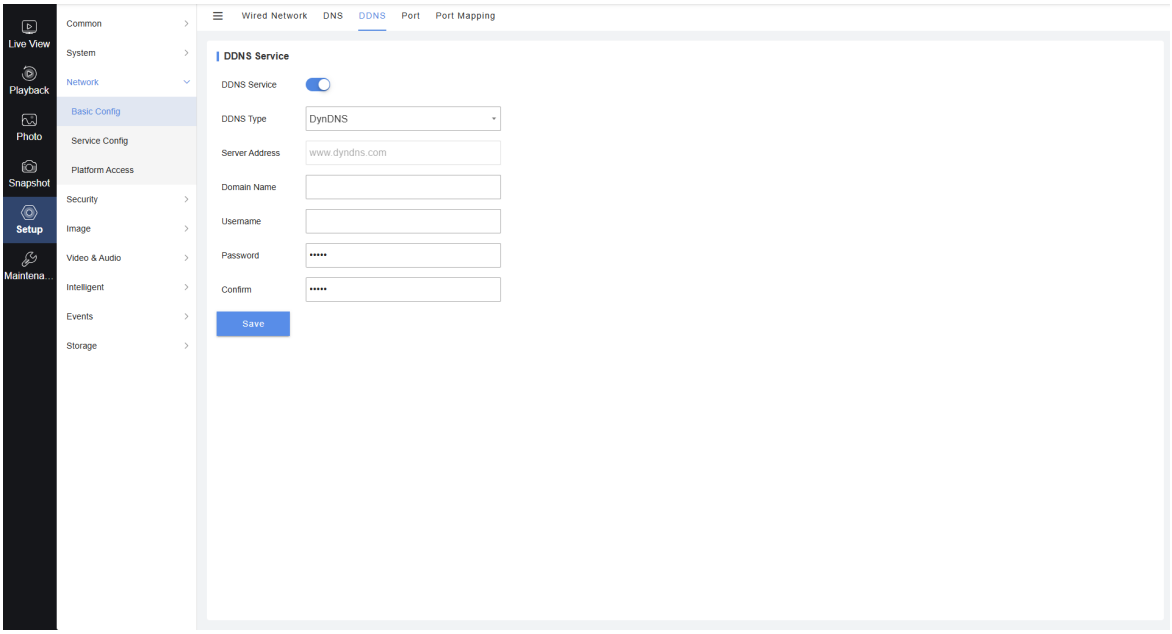
1. Configure the following parameters.

Parameter	Description
Preferred DNS Server	Enter the IP address of the preferred DNS server. The address must be a valid IPv4 address, with the first octet ranging from 1 to 223 (excluding 127).
Alternate DNS Server	Enter the IP address of the alternate DNS server, which is used when the preferred DNS server is unavailable. The format requirements are the same as those for the preferred DNS server.

2. Click **Save** to complete the configuration.

7.3.1.3 DDNS

By configuring the DDNS service, the device can be accessed remotely through a fixed domain name when the public IP address changes.



DynDNS

Configure DynDNS type DDNS. You need to set the domain name, username, and password. The server address is automatically filled in and cannot be modified.

1. Click the switch to enable DDNS Service.
2. Select the DDNS type as **DynDNS**.
3. Configure the following parameters.

Parameter	Description
Server Address	The DynDNS server address, automatically filled in as www.dyndns.com and not editable.
Domain Name	Enter the domain name, which must comply with the URL format requirements.
Username	Enter the username registered with the DDNS service.
Password	Enter the password registered with the DDNS service.
Confirm	Enter the password again, which must be consistent with the password.

4. Click **Save** to complete the configuration.

NO-IP

Configure NO-IP type DDNS. You need to set the domain name, username, and password. The server address is automatically filled in and cannot be modified.

1. Click the switch to enable DDNS Service.
2. Select the DDNS type as **NO-IP**.
3. Configure the following parameters.

Parameter	Description
Server Address	The NO-IP server address, automatically filled in as www.noip.com and not editable.
Domain Name	Enter the domain name, which must comply with the URL format requirements.
Username	Enter the username registered with the DDNS service.
Password	Enter the password registered with the DDNS service.
Confirm	Enter the password again, which must be consistent with the password.

4. Click **Save** to complete the configuration.

EZDDNS

Configure the private DDNS type. Only the domain name needs to be set. Domain name availability testing is supported, and the device access address is automatically generated by the system.

1. Click the switch to enable DDNS Service.
2. Select the DDNS type as **EZDDNS**.
3. Configure the following parameters.

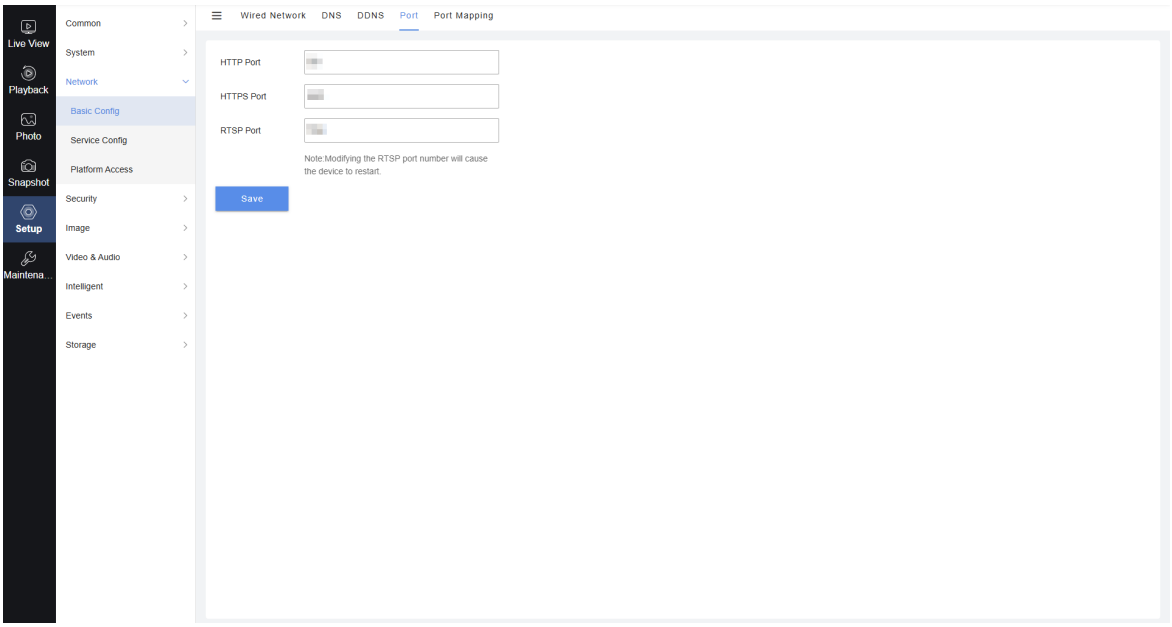
Parameter	Description
Server Address	The EZDDNS server address, automatically filled in and not editable.
Domain Name	Enter the domain name.
Test	Click **Test** to verify whether the domain name is available. If the verification passes, "Valid domain name" is prompted; otherwise, "Invalid domain name" is prompted.
Device Address	The device access address, in the format "Server Address/Domain Name", automatically generated based on the domain name input and not editable.

4. Click **Save** to complete the configuration.

7.3.1.4 Port

Configure the HTTP, HTTPS, and RTSP network service ports of the device so that clients can access the web management interface and video streams of the device through the specified ports. Modifying the RTSP port number will cause the device to restart.

Note: The three port numbers cannot be the same. Some ports (such as 23, 81, 82, 85, 3260, and 49152) are system reserved ports and cannot be used.

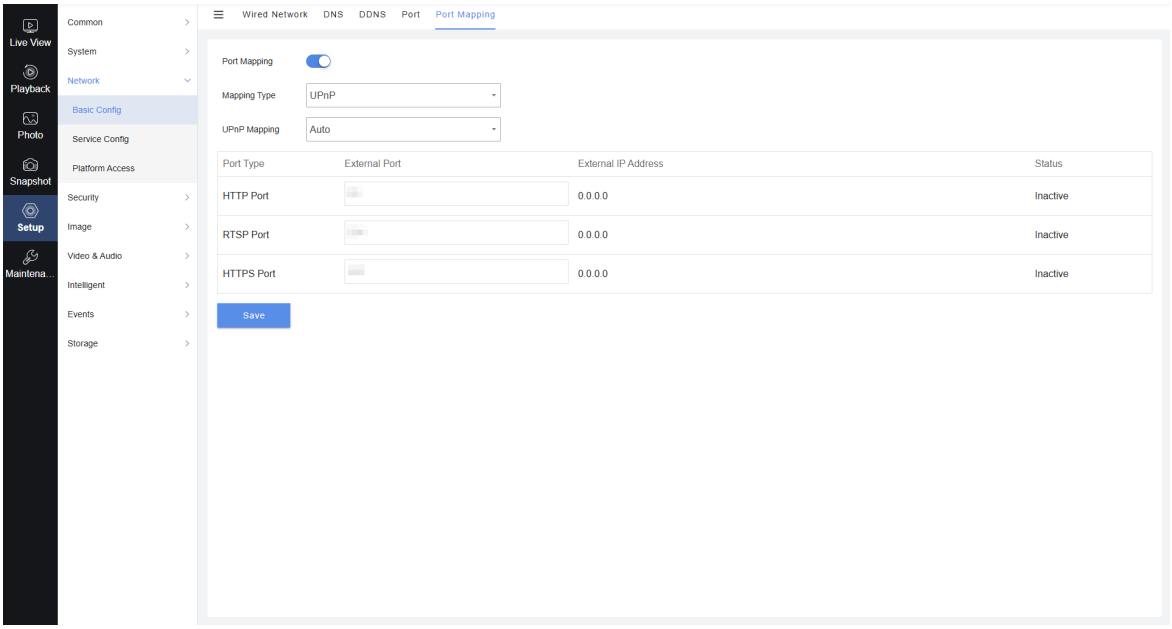


7.3.1.5 Port Mapping

By configuring port mapping, internal service ports of the device are mapped to external network ports, allowing the external network to access the services provided by the device. Two mapping methods are supported: Manual and UPnP.

Note:

- Port mapping requires router support. If the router does not support port mapping or UPnP, the mapping status will be displayed as "Inactive".
- UPnP mapping requires the router to have UPnP enabled.
- Changing port mapping settings may interrupt the current connection. Proceed with caution.



Manual

Manually specify the mapping port numbers for each service protocol to map the internal ports of the device to externally accessible ports.

1. Set the mapping type to **Manual**.
2. Configure the related parameters.
3. Click **Save** to complete the configuration.

UPnP Mapping

Automatically create port mappings on the router through the UPnP protocol. No manual port configuration is required.

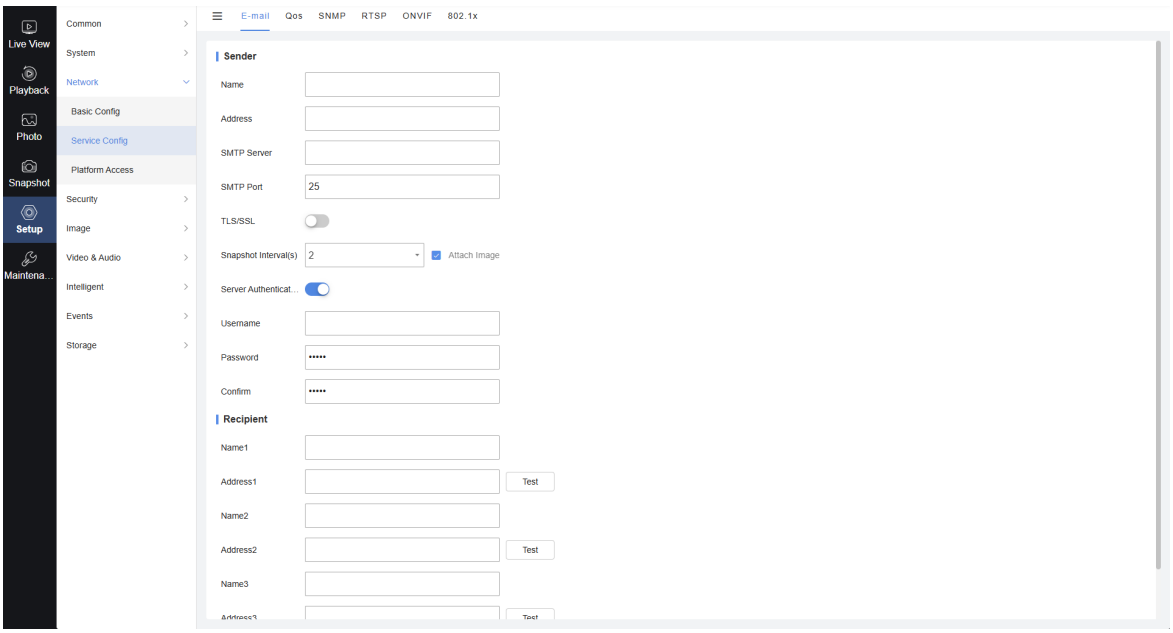
1. Set the mapping type to **UPnP**.
2. Select the UPnP mapping type.
   - **Auto-negotiation:** Enable the router's UPnP function to open ports, enabling communication between the internal and external networks. When disabled, the NAT gateway releases the ports.
   - **Specified Port:** The NAT gateway opens a fixed port. The mapping relationship persists regardless of connection status. Enter the mapping port number to open the port.
3. Click **Save** to complete the configuration.

7.3.2 Service Configuration

7.3.2.1 E-mail

By configuring the sender and recipient information of the email server, the device can send captured images or alarm information to specified email addresses upon event triggers. This is applicable to remote monitoring and event notification scenarios.

Note: The device supports up to 3 recipients. After server authentication is enabled, a username and password are required. After Attach Image is enabled, the snapshot interval can be set.



1. Configure the sender parameters.

Parameter	Description
Name	The sender name.
Address	The sender email address.
SMTP Server	The IP address or domain name of the SMTP server.

Parameter	Description
SMTP Port	The port number of the SMTP server.
TLS/SSL	Click to use a TLS/SSL encrypted connection for communication with the email server.
Attach Image	Click to attach captured images when sending emails.
Snapshot Interval(s)	The time interval for attaching captured images when sending emails. This parameter is available only after Attach Image is enabled.
Server Authentication	Click to require a username and password for SMTP server authentication.
Username	The username for logging in to the SMTP server, which must be in email format. This parameter is available only after Server Authentication is enabled.
Password	The password for logging in to the SMTP server. This parameter is available only after Server Authentication is enabled.
Confirm	Enter the password again, which must be consistent with the password. This parameter is available only after Server Authentication is enabled.

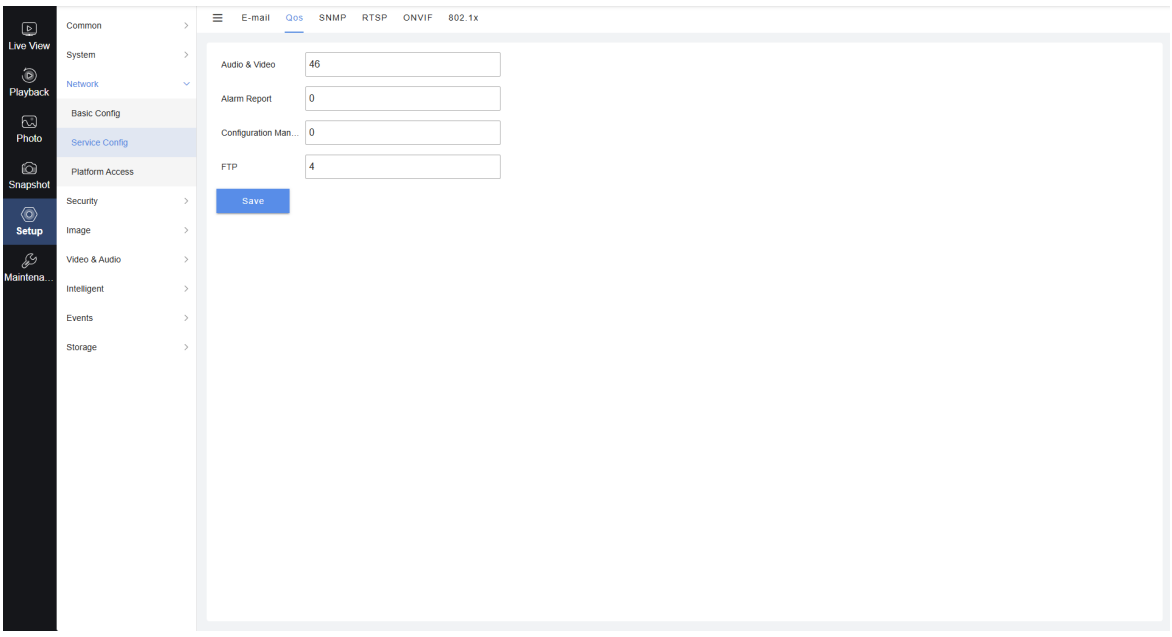
2. Configure the recipient parameters.

Parameter	Description
Name 1–3	The recipient name.
Address 1–3	The recipient email address, which must be in a valid email format. Click **Test** to verify the email connectivity.

3. Click **Save** to complete the configuration.

7.3.2.2 QoS

QoS (Quality of Service) is used to set DSCP priority tags for different types of network traffic. By assigning different DSCP values to traffic such as audio and video, alarm reporting, configuration management, and FTP, network devices can perform differentiated processing based on these tags, thereby ensuring the network transmission quality of critical services.



1. Configure the following parameters.

Parameter	Description
Audio & Video	Set the DSCP priority value for the audio and video stream. The default value is 46 (corresponding to EF Expedited Forwarding, which is applicable to latency-sensitive traffic such as real-time audio and video).

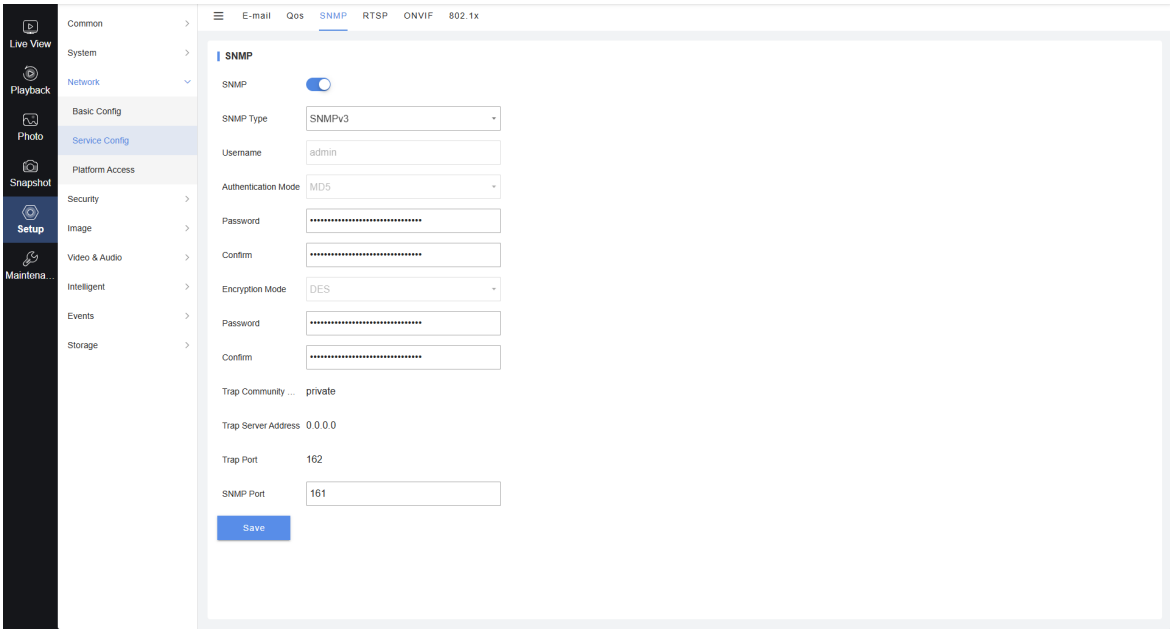
Parameter	Description
Alarm Report	Set the DSCP priority value for the alarm report stream.
Configuration Management	Set the DSCP priority value for the configuration management stream.
FTP	Set the DSCP priority value for the FTP stream.

2. Click **Save** to complete the configuration.

7.3.2.3 SNMP

By configuring the SNMP service, the network management system can remotely monitor and manage the device. Two protocol versions are supported: SNMPv2 and SNMPv3.

Note: SNMPv2 has security risks. When you save the SNMPv2 configuration, the system will prompt a risk confirmation. It is recommended to use SNMPv3.



SNMPv2

Through the SNMPv2 protocol, the network management system can use community names to perform basic remote monitoring and management of the device.

1. Click to enable SNMP.
2. Select the SNMP type as **SNMPv2**. A security risk confirmation prompt appears. Click **OK**.
3. Configure the following parameters.

Parameter	Description
Read Community	The read-only access community name for SNMPv2.
Read/Write Community	The read/write access community name for SNMPv2, generated by the system and not editable.
Trap Community	The community name for SNMPv2 trap alarms, generated by the system and not editable.
Trap Server IP	The IP address of the server that receives trap alarms, generated by the system and not editable.
Trap Port	The port number for receiving trap alarms, generated by the system and not editable.
SNMP Port	The listening port of the SNMP service.

4. Click **Save** to complete the configuration.

SNMPv3

Through the SNMPv3 protocol, the network management system can use usernames, authentication, and encryption mechanisms to perform secure remote monitoring and management of the device.

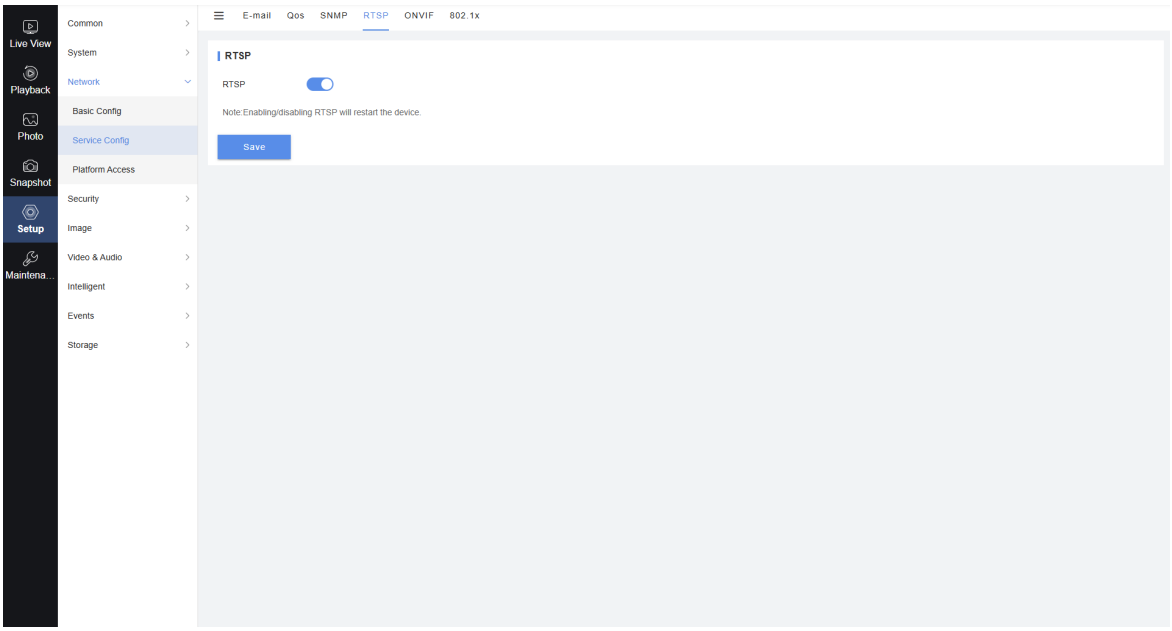
1. Click to enable SNMP.
2. Select the SNMP type as **SNMPv3**.
3. Configure the following parameters.

Parameter	Description
Username	The username for SNMPv3, not editable.
Authentication Mode	The authentication algorithm for SNMPv3, not editable.
Password	The authentication password for SNMPv3.
Confirm	Enter the authentication password again, which must be consistent with the authentication password.
Encryption Mode	The encryption algorithm for SNMPv3, not editable.
Password	The encryption password for SNMPv3.
Confirm	Enter the encryption password again, which must be consistent with the encryption password.
Trap Community	The community name for SNMPv3 trap alarms, generated by the system and not editable.
Trap Server IP	The IP address of the server that receives trap alarms, generated by the system and not editable.
Trap Port	The port number for receiving trap alarms, generated by the system and not editable.
SNMP Port	The listening port of the SNMP service.

4. Click **Save** to complete the configuration.

7.3.2.4 RTSP

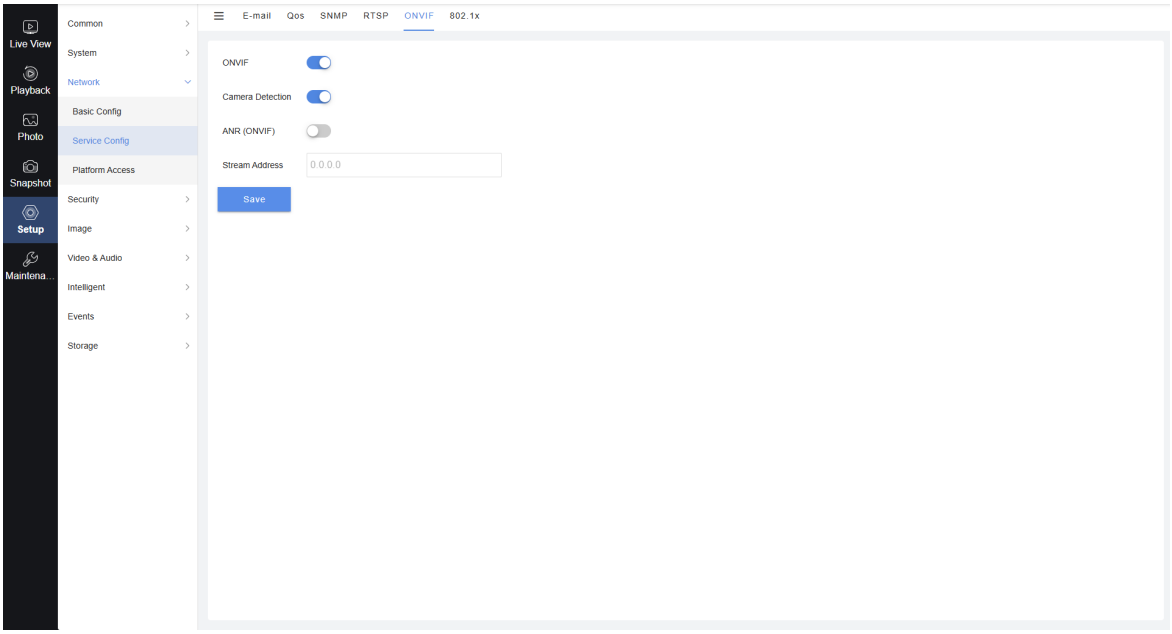
Configure the RTSP service of the device. RTSP provides remote control capabilities such as start, pause, fast-forward, and stop for media streams, but does not transmit data itself.



1. Click to enable **RTSP**. When disabled, the live view page will not display video.
2. Click **Save** to complete the configuration.

7.3.2.5 ONVIF

ONVIF is a standard protocol for network video surveillance. By enabling the ONVIF feature, the device can be automatically discovered and connected by third-party NVRs or clients. ONVIF ANR is also supported to ensure that video data is not lost during network interruptions.



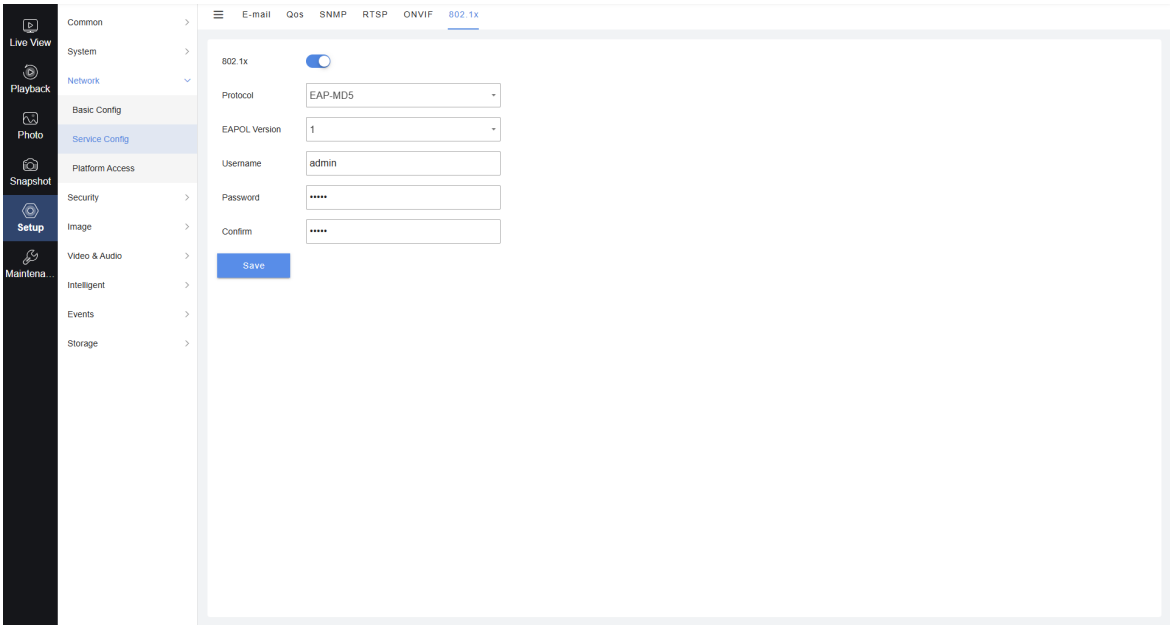
1. Click to enable ONVIF.
2. Click to enable Camera Detection, allowing the device to be discovered by other clients on the network.
3. Click to enable ANR (ONVIF).
4. Configure the stream address. Set the server IP address for receiving the ANR video stream. The IP address must be valid (first octet 1–223, excluding 127) and can be left empty. This parameter is available only after ANR (ONVIF) is enabled.
5. Click **Save** to complete the configuration.

7.3.2.6 802.1x

Configure the 802.1x authentication feature to authenticate devices accessing the network. EAP-MD5 and EAP-TLS authentication protocols are supported.

Note:

- Before using EAP-TLS authentication, install the client certificate and CA certificate in Certificate Management.
- The password is encrypted and transmitted using RSA to ensure authentication information security.



EAP-MD5

Authentication is performed using username and password.

1. Click to enable 802.1x authentication.
2. Configure the following parameters.

Parameter	Description
Protocol	Select **EAP-MD5** to authenticate using username and password.
EAPOL Version	Select the EAPOL protocol version.
Username	Enter the authentication username.
Password	Enter the authentication password.
Confirm	Enter the password again. The two passwords must match.

3. Click **Save** to complete the configuration.

EAP-TLS

Authentication is performed using digital certificates.

1. Click to enable 802.1x authentication.
2. Configure the following parameters.

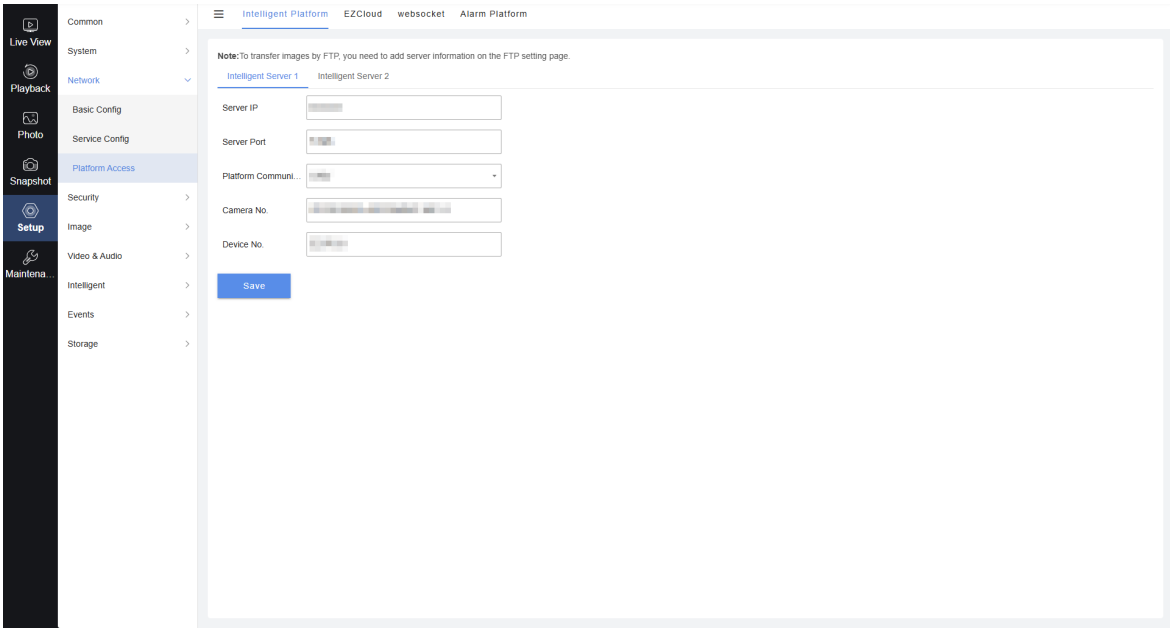
Parameter	Description
Protocol	Select **EAP-TLS** to authenticate using digital certificates.
EAPOL Version	Select the EAPOL protocol version.
Username	Enter the authentication username.
Client Certificate	Select a certificate for authentication from the installed client certificates.
CA Certificate	Select a certificate for server verification from the installed CA certificates.

3. Click **Save** to complete the configuration.

7.3.3 Platform Access

7.3.3.1 Intelligent Platform

By configuring the intelligent platform access parameters, the device can connect to an intelligent analysis server or an upper-level platform for intelligent data reporting and service integration.



GA/T1400 Access

1. Select **GA/T1400** as the platform communication type.
2. Configure the protocol parameters.

Parameter	Description
Protocol Version	Select the version.
Device ID	Set an ID that meets the interface prompt requirements and keep it consistent with the platform side.
Username	Enter the authentication username for the device-to-platform connection. The device and the platform must have the same configuration.
Password	Enter the authentication password for the device-to-platform connection. The device and the platform must have the same configuration.
Confirm Platform Access Code	Enter the authentication password again.
Coordinate Mode	Used to locate the position of structured information in the image. This must be consistent with the coordinate mode used by the platform to read structured information. Options: ten-thousandth coordinate, pixel coordinate, normalized coordinate.
Connection Mode	Options: Short Connection and Standard Mode. Short Connection is sufficient for general use.
Report Data Type	Select the report data types.

3. Click <Save> to complete the configuration.

UNV Persistent Connection Access

1. Set the protocol parameters.

Parameter	Description
Camera ID	Must be consistent with the device ID on the management platform. If the management platform is accessed through the IMOS protocol, the camera ID is the device ID on the management platform plus "_1".

Parameter	Description
Device Code	Custom device code.

2. Click <Save> to complete the configuration.

FTP Access

1. Click  to enable.
2. Click **Configure FTP** to enter the [Configure FTP] page.
3. Configure the protocol parameters.

Parameter	Description
Server Address	The FTP server IP address.
Port	Use the default port 21.
Username	Enter the username for logging in to the FTP server.
Password	Enter the password for logging in to the FTP server.
Test	Click to test whether the device and the server are connected successfully.
Upload Images	Select to upload images captured by intelligent functions. Overwrite Storage: When the number of photos in the lowest-level folder reaches the set threshold, the stored photos will be overwritten to continue storage. For example, if the save path is "\IP\Date", the lowest level is the second-level "Date". When the photos uploaded on January 4, 2022 exceed 1000, the photos already stored in the folder named "20220104" will be overwritten to continue storage. **Note:** • When Overwrite Storage is selected, ensure that the last naming element of the file name is the photo number. • Overwrite threshold (photos): Default 1000, maximum 100,000.
Custom Naming	Select to customize file naming rules. For naming rules, see step 6 "Configure Save Path".
Convert Path into UTF8 Format	Select to convert the path format to UTF8 format.

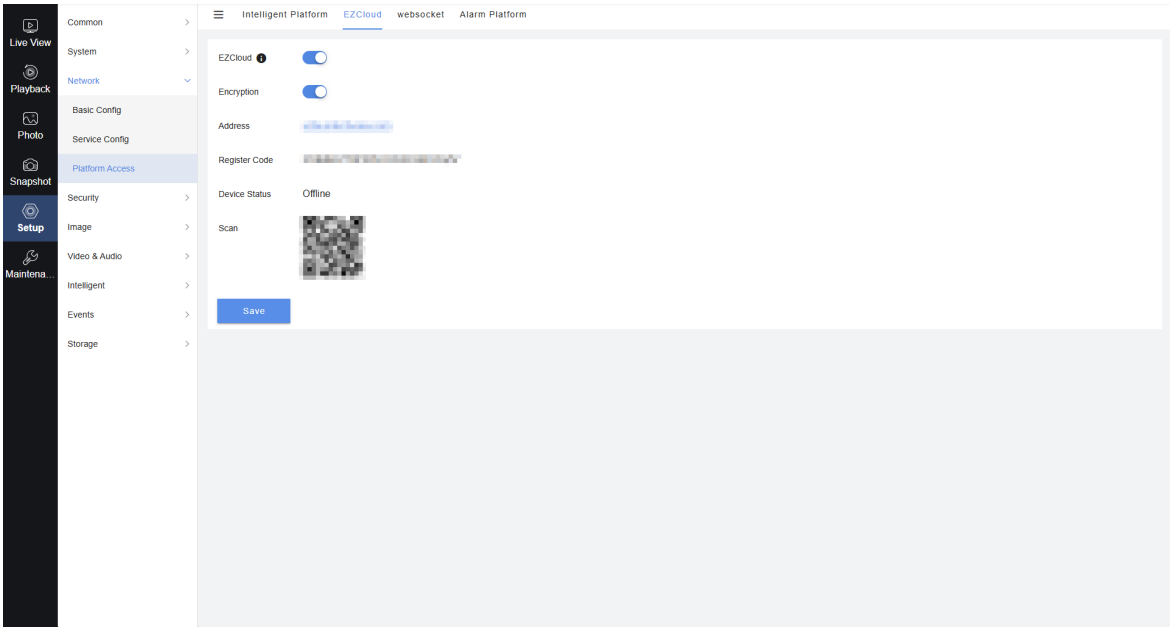
4. Configure the save path and file name.

Parameter	Description
File Path	Up to 6 levels can be set. If not set, the default is "\IP\Date\Intelligent", where "Intelligent" indicates that the image is captured by an intelligent function.
File Name	Naming elements: Up to 20 fields can be set. If not set, the default is a sequential number, such as "1", "2", "3", and so on.
	Naming rule: Prefix<(front padding character) front length%total length (rear padding character)> Suffix.

5. Click <Save> to complete the configuration.

7.3.3.2 EZCloud

Add the device to EZCloud. Scan the QR code with a mobile client to add the device and complete the binding and pairing between the device and the app.

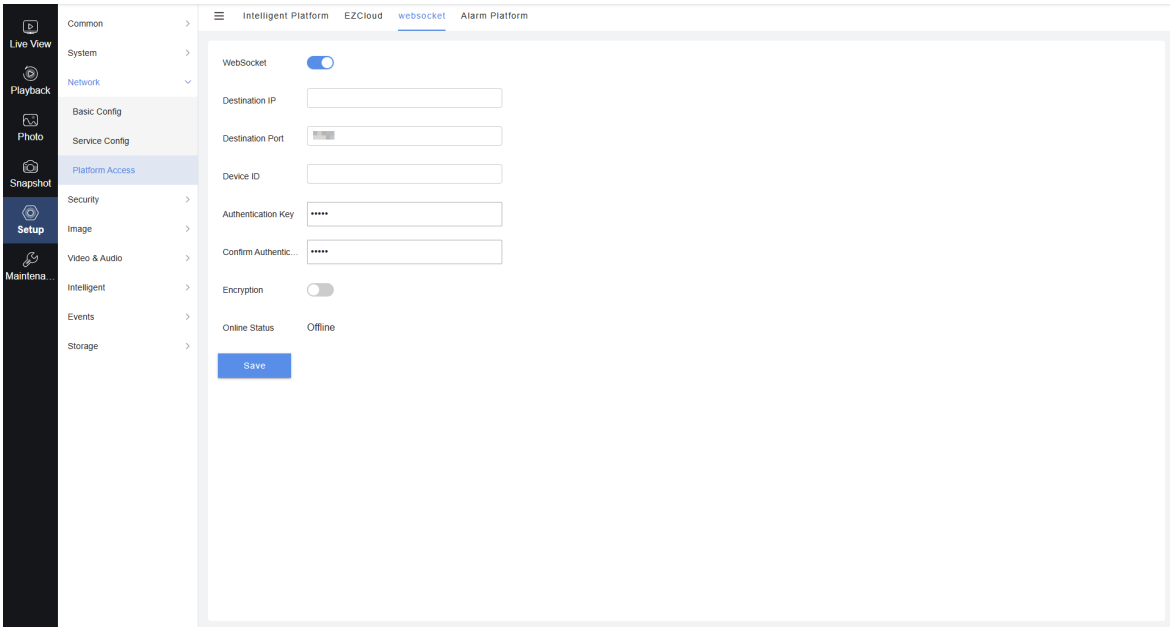


1. Click to enable EZCloud. Scan the QR code on the page to download the mobile client. For more details, see the user manual in the app.
2. Click **Save** to complete the configuration.

7.3.3.3 WebSocket

By configuring WebSocket parameters, the device can establish a WebSocket persistent connection with the upstream server for real-time communication and data reporting between the device and the platform.

Note: WebSocket and EZCloud are mutually exclusive. Disable the cloud platform before enabling WebSocket.



1. Click to enable the WebSocket function.
2. Configure the following parameters.

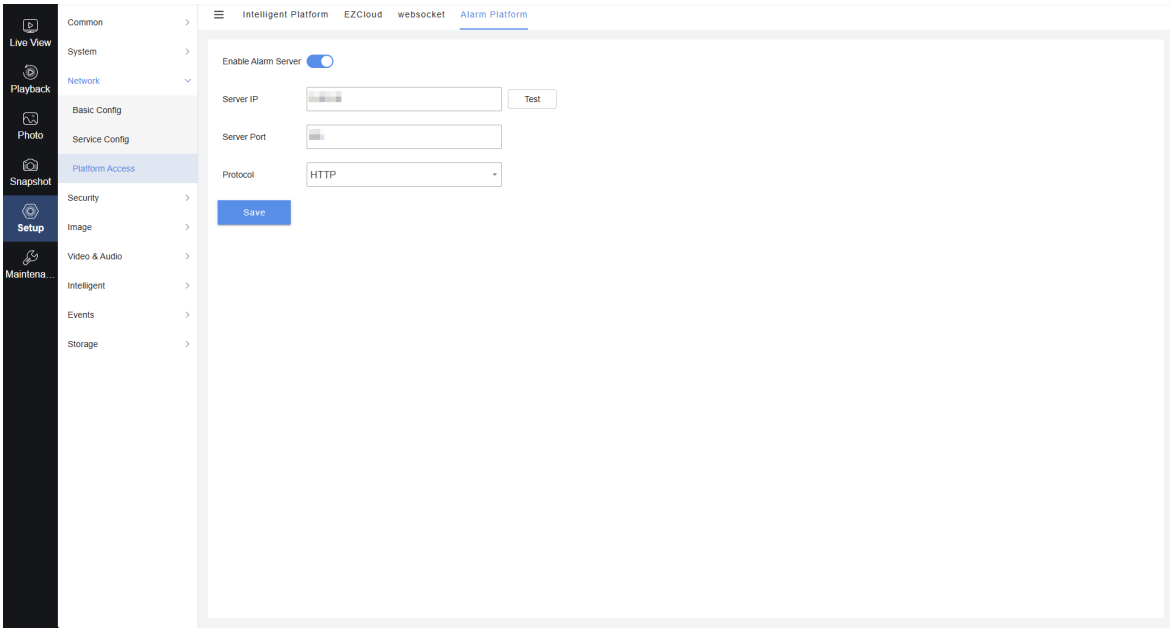
Parameter	Description
Destination Address	Set the address of the upstream WebSocket server. IPv4 addresses (first octet 1–223, excluding 127), IPv6 addresses, and URL domain names are supported.

Parameter	Description
Destination Port	Set the port number of the upstream WebSocket server.
Device ID	Set the device identifier, which is used by the upstream server to identify the device.
Authentication Key	Set the authentication key for the device to connect to the upstream server. After modification, the key is transmitted using RSA encryption.
Confirm Authentication Key	Enter the authentication key again. It must be identical to the authentication key.
Encryption	When enabled, the communication data between the device and the upstream server will be encrypted during transmission.
Online Status	Displays the current connection status between the device and the upstream server, including Online and Offline. This parameter is read-only.

3. Click **Save** to complete the configuration.

7.3.3.4 Alarm Platform

After configuring the alarm platform, the device can send alarm information to the specified alarm server, thereby enabling centralized management and coordinated response for alarm information.



1. Click  to enable Alarm Server.
2. Configure the following parameters.

Parameter	Description
Server Address	Enter the IP address or domain name of the alarm server. IPv4, IPv6 addresses and domain names are supported.
Server Port	Enter the port number of the alarm server.
Protocol	Select the protocol for communicating with the alarm server.

3. Click **Test** to verify the connectivity to the alarm server.
4. Click **Save** to complete the configuration.

7.4 Security

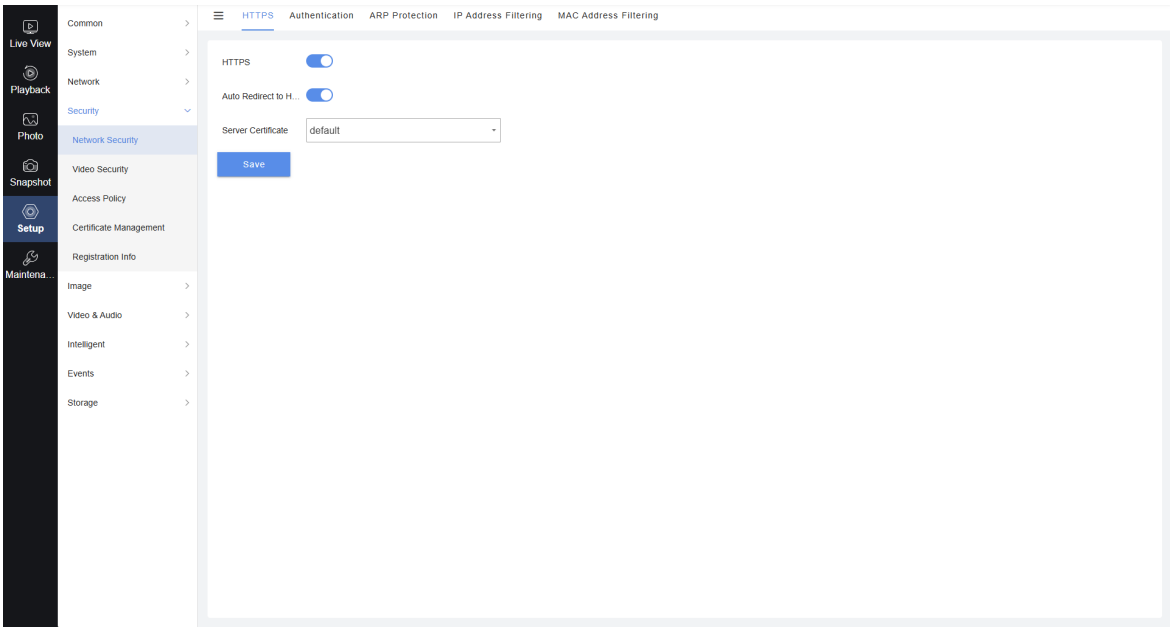
7.4.1 Network Security

Configure network security features of the device, including HTTPS, authentication, ARP protection, IP address filtering, and MAC address filtering.

7.4.1.1 HTTPS

By enabling HTTPS, the communication between the device and the client uses encrypted transmission to prevent data from being intercepted or tampered with. After auto redirect is enabled, all HTTP requests are automatically redirected to HTTPS, ensuring secure access.

Note: After HTTPS is disabled, the current page automatically switches to HTTP protocol access.



1. Click to enable HTTPS.
2. Configure the following parameters.

Parameter	Description
Auto Redirect to HTTPS	After it is enabled, all HTTP requests are automatically redirected to HTTPS for encrypted access.
Server Certificate	Select the server certificate used for HTTPS encrypted communication. The certificate must be uploaded in Certificate Management in advance. Only server-type certificates are displayed here.

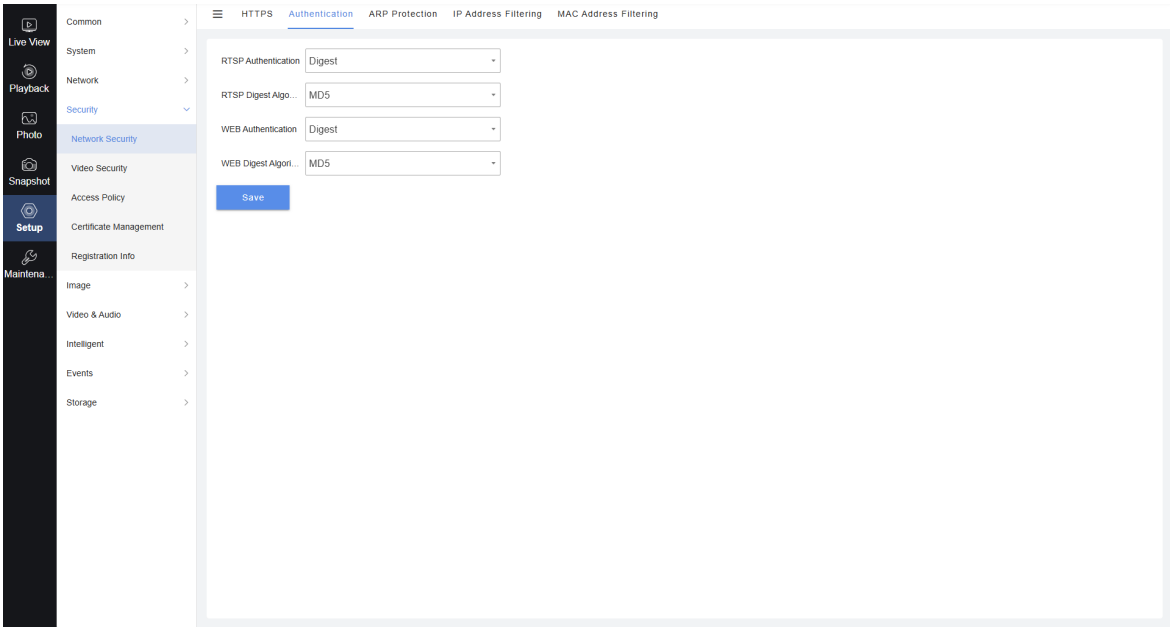
3. Click the **Save** button to complete the configuration.

7.4.1.2 Authentication

By configuring authentication modes, you can control the authentication mode and digest algorithm for RTSP and WEB protocols, ensuring identity verification security when clients access the device.

Note:

- Disabling WEB authentication will cause user permissions to become invalid. Proceed with caution.
- RTSP Basic authentication transmits credentials in plaintext, which provides lower security. Digest authentication is recommended.



RTSP Authentication

Configure the authentication mode and digest algorithm for the RTSP protocol.

1. Configure the following parameters.

Parameter	Description
RTSP Authentication	Select the authentication mode for the RTSP protocol. • **None**: No authentication is performed. Any client can access the device. • **Basic**: Uses basic authentication. Credentials are transmitted in plaintext, which provides lower security. • **Digest**: Uses digest authentication. Credentials are encrypted before transmission, which provides higher security.
RTSP Digest Algorithm	This is displayed when **Digest** is selected for RTSP Authentication. Select the hash algorithm used for digest authentication. • **MD5**: Uses the MD5 algorithm. • **SHA256**: Uses the SHA-256 algorithm. • **MD5/SHA256**: Supports both MD5 and SHA-256 algorithms. The client can select either algorithm.

2. Click **Save** to complete the configuration.

WEB Authentication

Configure the authentication mode and digest algorithm for the WEB (HTTP) protocol.

1. Configure the following parameters.

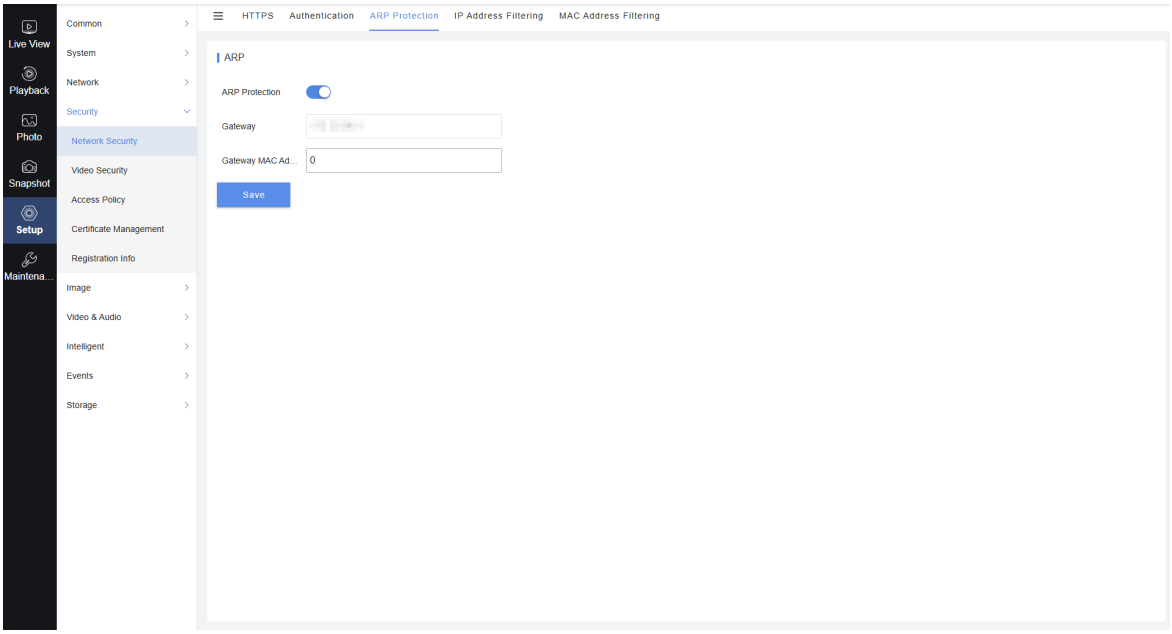
Parameter	Description
WEB Authentication	Select the authentication mode for the WEB protocol. • **None**: No authentication is performed. Disabling WEB authentication will cause user permissions to become invalid. • **Digest**: Uses digest authentication. Credentials are encrypted before transmission, which provides higher security.
WEB Digest Algorithm	This is displayed when **Digest** is selected for WEB Authentication. Select the hash algorithm used for digest authentication. • **MD5**: Uses the MD5 algorithm.

Parameter	Description
	• **SHA256**: Uses the SHA-256 algorithm. • **MD5/SHA256**: Supports both MD5 and SHA-256 algorithms. The client can select either algorithm.

2. Click **Save** to complete the configuration.

7.4.1.3 ARP Protection

ARP resolves an IP address to the corresponding MAC address. Attackers can launch attacks by forging ARP responses. By enabling ARP Protection, the device verifies the physical address of the access source, thereby preventing ARP attacks.



Note: After ARP Protection is enabled, the gateway MAC address is required. The gateway IP address is automatically obtained by the device and cannot be manually modified.

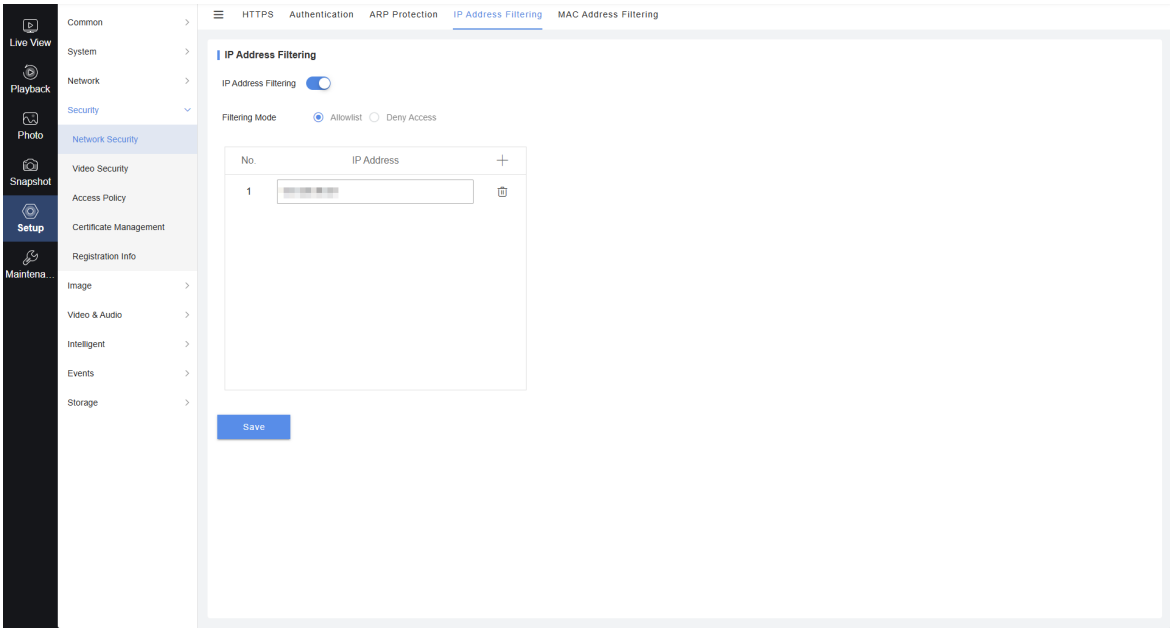
1. Click to enable ARP Protection.
2. Configure the following parameters.

Parameter	Description
Gateway	Displays the IP address of the current gateway. This parameter cannot be edited.
Gateway MAC Address	Enter the MAC address of the gateway. The format is XX:XX:XX:XX:XX:XX, for example, 00:1A:2B:3C:4D:5E. This parameter is required after ARP Protection is enabled.

3. Click **Save** to complete the configuration.

7.4.1.4 IP Address Filtering

By configuring IP address filtering rules, you can restrict or allow access to the device from specific IP addresses, thereby enhancing network security of the device.



Configure IP Address Filtering

1. Click to enable IP Address Filtering.
2. Select a filtering mode.
   - **Allowlist**: Only IP addresses in the list can access the device, and all other IP addresses are denied access.
   - **Deny Access**: IP addresses in the list are denied access to the device, and all other IP addresses can access the device normally.
3. Add an IP address. Click + and enter the IP address to be filtered. Requirements:
   - 0.0.0.0, 127.0.0.1, 255.255.255.255, and 224.0.0.1 are not supported.
   - The first segment ranges from 1 to 223.
   - The fourth segment cannot be 0.
   - IP addresses cannot be duplicated.
   - A maximum of 32 IP addresses can be added.
4. Click **Save** to complete the configuration.

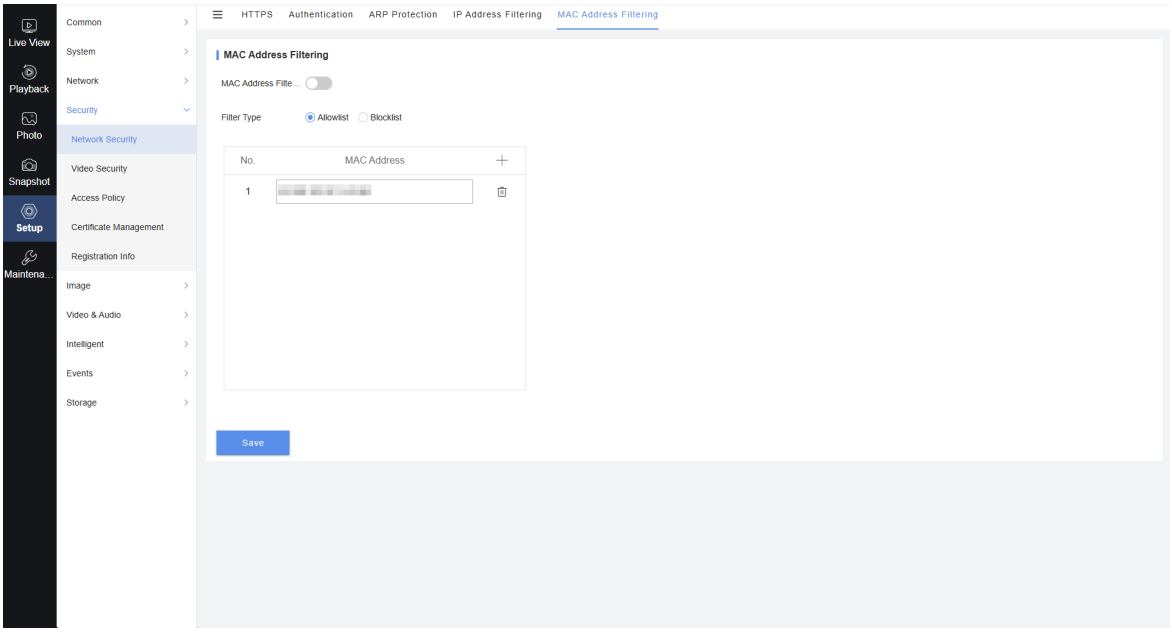
Manage IP Addresses

Delete an IP address. In the IP address list, click 🗑 of the corresponding entry to delete the IP address.

7.4.1.5 MAC Address Filtering

By configuring MAC address filtering rules, you can restrict or allow access to the device from devices with specific MAC addresses, thereby enhancing network security of the device.

Note: After enabling Allowlist, make sure that the MAC addresses of your client and gateway have been added to the allowlist. Otherwise, you cannot access the device.



Configure MAC Address Filtering

1. Click  to enable MAC Address Filtering.
2. Select a filter type.
   - **Allowlist**: Only MAC addresses in the list can access the device.
   - **Blocklist**: MAC addresses in the list are denied access to the device.
3. Click + and enter a MAC address in the MAC address list. The MAC address format is six groups of two-digit hexadecimal numbers separated by colons, for example, AA:BB:CC:DD:EE:FF.
4. Click **Save** to complete the configuration.

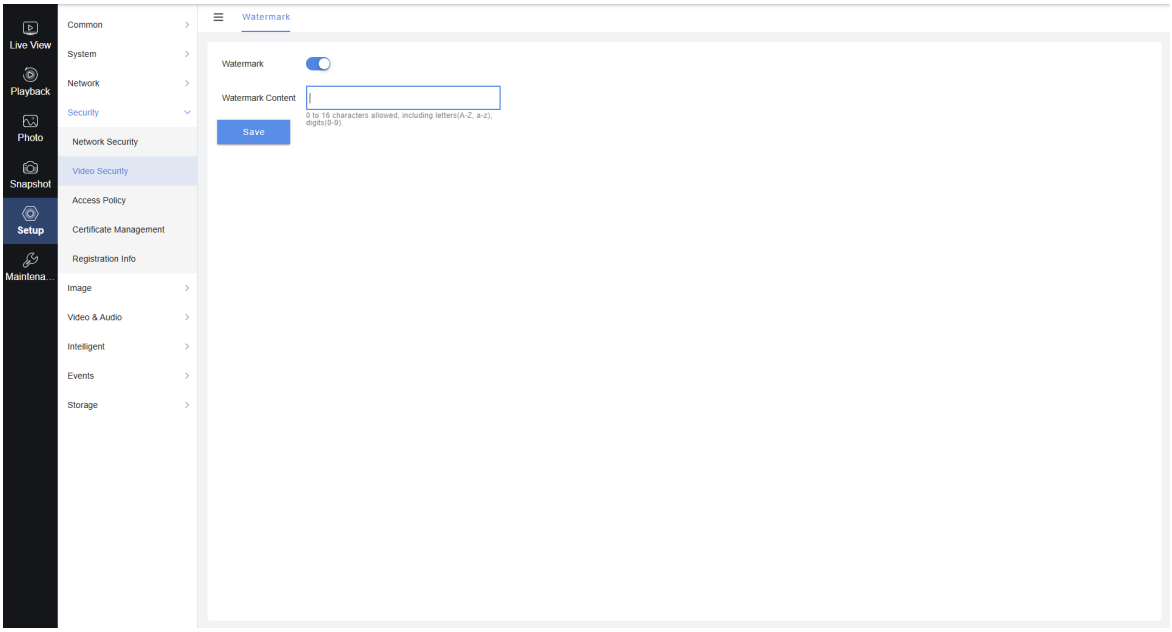
Manage MAC Addresses

Delete a MAC address. In the MAC address list, click 🗑 of the corresponding entry to delete the MAC address.

7.4.2 Video Security

7.4.2.1 Watermark

The Watermark feature overlays text watermarks on the video image to identify the video source or prevent unauthorized use of the video.

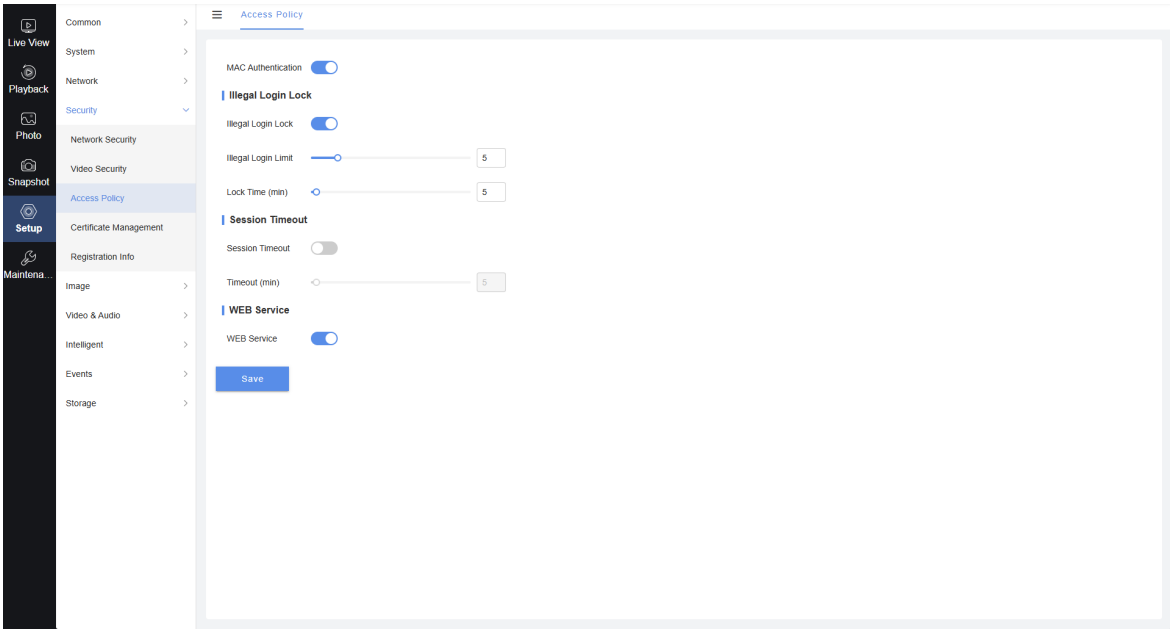


1. Click  to enable the watermark.
2. In **Watermark Content**, enter the text to be overlaid.
3. Click **Save** to submit the configuration.

Note: The watermark content only supports uppercase and lowercase English letters and digits. Chinese characters and special characters are not supported.

7.4.3 Access Policy

By configuring policies such as MAC Authentication, Illegal Login Lock, and Session Timeout, you can apply security control to web access to the device, thereby preventing unauthorized access and brute-force attacks.



MAC Authentication

When enabled, the device validates the format of MAC addresses entered in the MAC address filtering list, and checks whether the MAC address is empty or duplicates an existing entry. This ensures that only valid MAC addresses can be added to the allowlist or blocklist.

Illegal Login Lock

Parameter	Description
Illegal Login Lock	When enabled, if consecutive login failures from the same IP address reach the specified limit, the login permission of that IP address will be locked. During the lock period, the IP address cannot log in to the device.
Illegal Login Limit	The upper limit of consecutive login failures allowed.
Lock Time (min)	The duration for which the IP address remains locked.

Session Timeout

Parameter	Description
Session Timeout	When enabled, if no operation is performed within the specified time, the device automatically logs out the current session.
Timeout (min)	The idle timeout period for the session.

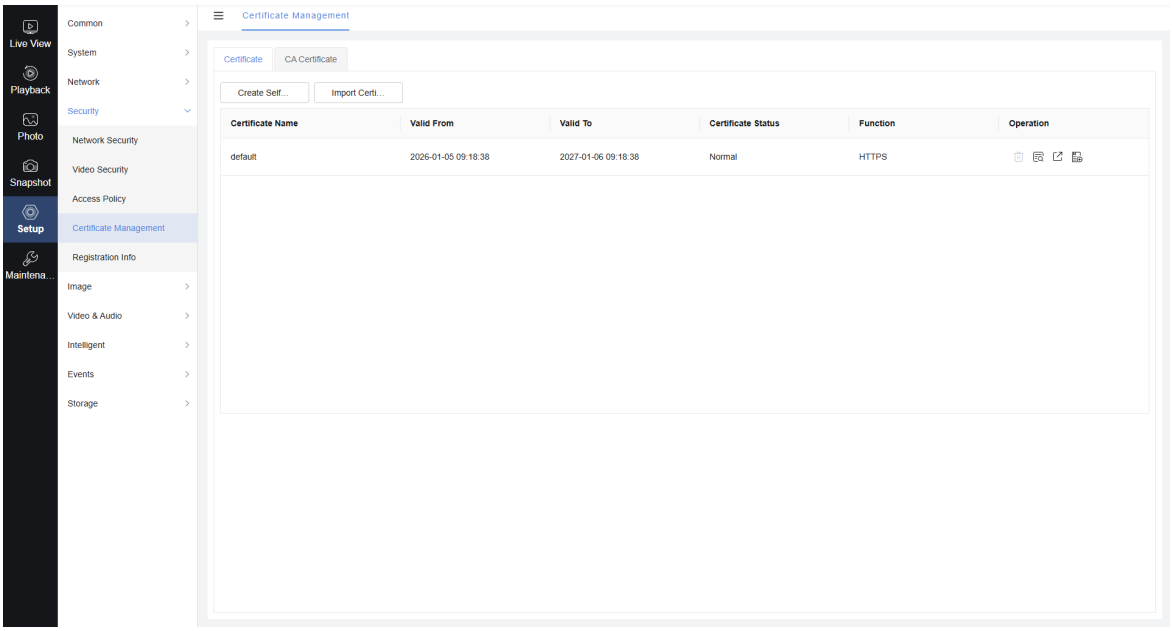
WEB Service

When the WEB Service is disabled, the device cannot be accessed through a web browser.

7.4.4 Certificate Management

Certificate Management manages device digital certificates and CA certificates. It supports creating self-signed certificates, importing certificates, and creating certificate signing requests, providing certificate authentication for features such as HTTPS, interconnection services, and IEEE 802.1x.

Note: A certificate that is being referenced by a feature (HTTPS, interconnection service, or IEEE 802.1x) cannot be deleted. You must cancel the reference in the corresponding feature before deleting the certificate. After creating a self-signed certificate, wait for the process to complete. Do not repeat the operation. The default device certificate cannot be edited or deleted.



The **Certificate Management** page consists of the **Certificate** and **CA Certificate** tabs. The **Certificate** tab manages device certificates and supports creating self-signed certificates, importing certificates, exporting certificates, and creating certificate signing requests. The **CA Certificate** tab manages CA certificates and only supports importing.

Certificate

1. Create a self-signed certificate.

   (1) On the **Certificate** tab, click **Create Self-Signed Certificate**.

   (2) Configure the self-signed certificate parameters. Parameter descriptions are as follows.

Parameter	Description
Certificate Name	Enter a certificate name.
Public Key	Select the RSA public key length. Options: • **2048**: Default value, providing higher security. • **1024**: Better compatibility, lower security.
Country	Enter a two-letter country code in uppercase, such as CN or US.
Domain Name/IP	Enter a valid IP address or domain name.
Valid Period(day)	Enter the number of days the certificate is valid.
Province	Enter a province name.
City	Enter a city name.
Organization	Enter an organization name.
Organizational Unit	Enter an organizational unit name.
Email	Enter a valid email address.

   (3) Click **OK**. The device starts creating the self-signed certificate. Wait until the creation is complete and the list refreshes automatically.

2. Create a certificate signing request.

   (1) On the **Certificate** tab, in the certificate list, click **Create Certificate Signing Request** in the operation column of the target certificate.

   (2) Configure the certificate signing request parameters. Parameter descriptions are as follows.

Parameter	Description
Country	Enter a two-letter country code in uppercase, such as CN or US.
Domain Name/IP	Enter a valid IP address or domain name.
Province	Enter a province name.
City	Enter a city name.
Organization	Enter an organization name.
Organizational Unit	Enter an organizational unit name.
Email	Enter a valid email address.

   (3) Click **OK**. The device generates the CSR data and displays it in a pop-up window. Review the data and close the window.

   (1) Import a certificate.

      1. On the **Certificate** tab, click **Import Certificate**.
      2. Select an import format. Parameter descriptions for different formats are as follows.

Parameter	Description
Import Format	Select the certificate import format. Options: • **PEM Format**: Requires uploading the certificate file and private key file separately. • **PKCS#12**: Upload a .p12 or .pfx file. A password is required. • **Other Format**: Only the certificate file needs to be uploaded.

Parameter	Description
Certificate Name	Enter a certificate name.
Certificate	Select a certificate file. PEM format supports .pem/.crt/.cer/.der files; PKCS#12 format supports .p12/.pfx files; other formats support .pem/.crt/.cer/.der files.
Private Key	Select a private key file. Supported file types are .pem and .key. This is required only for PEM format.
Private Key Password	Enter the private key password. This is displayed only for PEM format.
Password	Enter the password for the PKCS#12 file. This is displayed only for PKCS#12 format.

3. Click **OK** to complete the certificate import.

CA Certificate

1. Switch to the **CA Certificate** tab and click **Import Certificate**.
2. Configure the CA certificate parameters. Parameter descriptions are as follows.

Parameter	Description
Certificate Name	Enter a CA certificate name (1 to 32 letters or digits).
Certificate	Select a CA certificate file. Supported formats are .pem/.crt/.cer/.der.

3. Click **OK** to complete the CA certificate import.

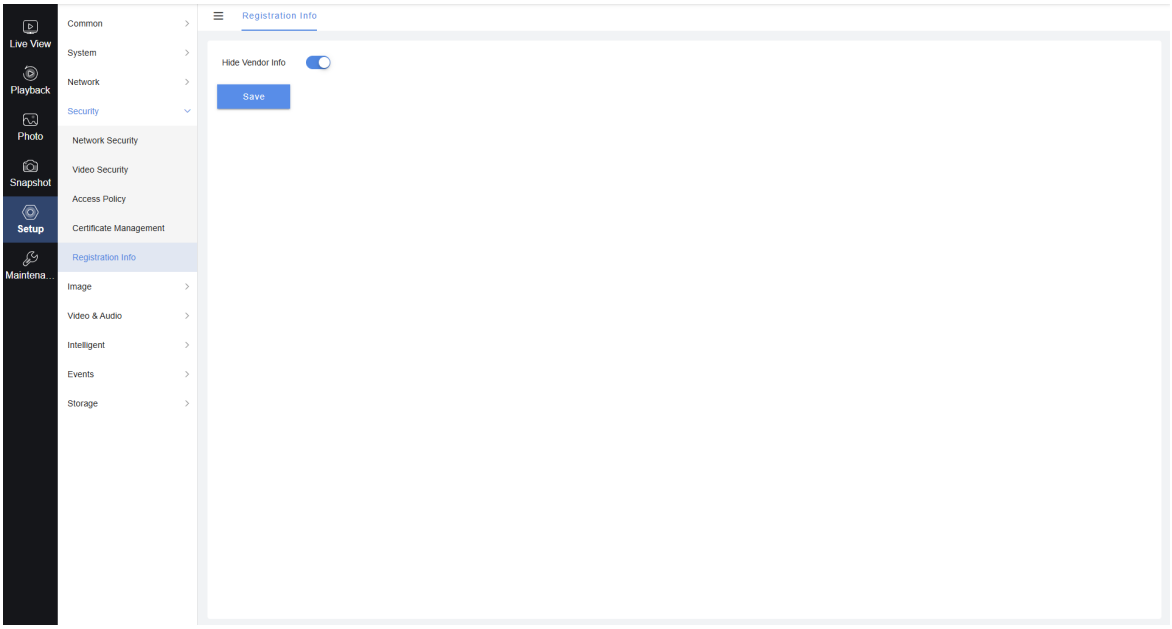
Manage Certificates

- View certificate properties. In the certificate list, click in the operation column of the target certificate to view the certificate properties and holder information.
- Export a certificate. On the **Certificate** tab, in the certificate list, click in the operation column of the target certificate to download the certificate file (.pem format) to the local device.
- Delete a certificate. In the certificate list, click in the operation column of the target certificate, and then confirm to delete the certificate.

  Note: When a certificate is being referenced by a feature, the delete button is unavailable. You must cancel the certificate reference in the corresponding feature before deleting the certificate.

7.4.5 Registration Info

Configure whether the device hides the manufacturer brand identifier from external display.



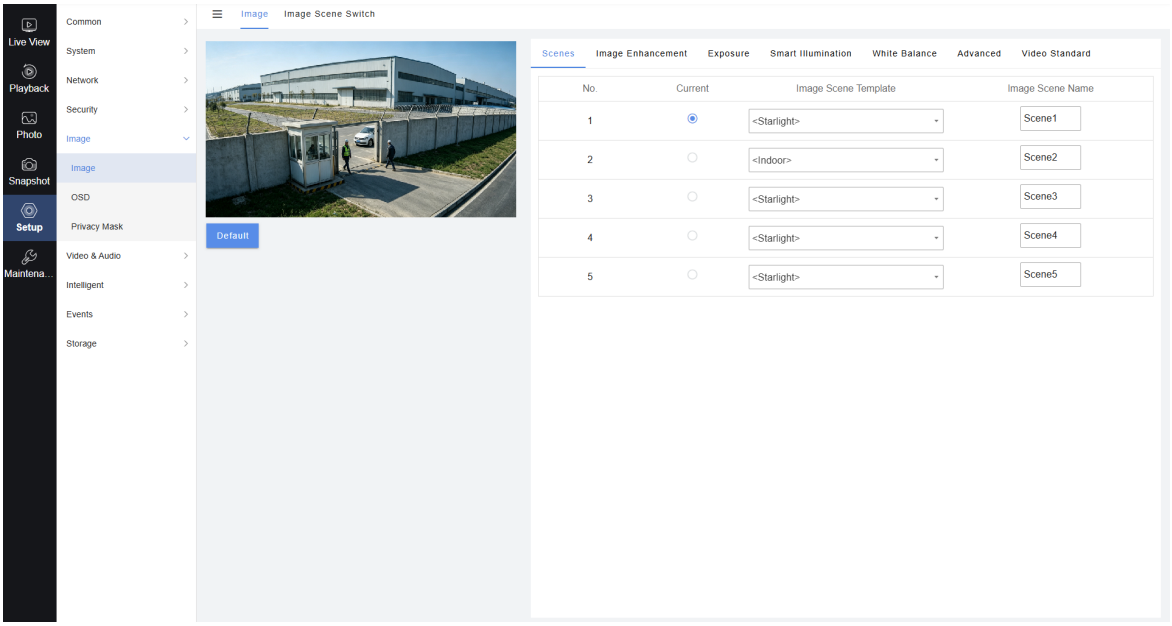
Click  to enhance device information security.

7.5 Image

7.5.1 Image Settings

7.5.1.1 Image Tuning

Image Tuning is used to configure the image display effect of the camera. You can adjust various parameters according to the actual monitoring environment to obtain the optimal image quality.



Scenes

Scenes is used to manage the camera scene configuration. It supports creating multiple scenes.

1. Select the active scene. In the scene list, select the radio button in the row of a scene to set it as the current running scene.
2. Configure the scene template and scene name:

Parameter	Description
Image Scene Template	Select the scene type. Available options are dynamically displayed based on the device capability set: • **Custom**: Custom scene type. You need to enter a custom name after selecting it. • **Adaptive Mode**: The device automatically adjusts the image parameters based on ambient light changes. • **Indoor**: Suitable for indoor environments. • **Common**: Suitable for outdoor environments. • **License Plate**: Suitable for license plate recognition scenarios. • **Starlight**: Suitable for low-illumination environments. • **Test**: Suitable for objective evaluation scenarios. • **High Photographic**: Suitable for campus scenarios. • **Road Highlight Compensation(HLC)**: Suitable for road highlight environments. • **WDR**: Suitable for WDR scenarios. • **Standard**: Standard scene mode. • **Bright**: Bright scene mode. • **Vivid**: Vivid scene mode. • **Face**: Suitable for face recognition scenarios. • **Clarity**: Clarity scene mode. • **Person And Vehicle**: Suitable for mixed vehicle and pedestrian scenarios. • **Intrusion Prevention**: Suitable for perimeter prevention scenarios.
Image Scene Name	Enter the scene name.

Note: When switching the scene template, a confirmation dialog box appears. After confirmation, the scene parameters will be reset.

Image Enhancement

Image Enhancement is used to adjust display effect parameters such as brightness, saturation, contrast, sharpness, and noise reduction of the image.

Parameter	Description
Brightness	Adjust the overall image brightness. A larger value indicates a brighter image.
Saturation	Adjust the color saturation of the image. A larger value indicates more vivid colors.
Contrast	Adjust the contrast between light and dark areas of the image. A larger value indicates a more noticeable contrast.
Sharpness	Adjust the edge sharpness of the image. A larger value indicates sharper edges.
2D Noise Reduction	Adjust the 2D spatial noise reduction intensity. A larger value indicates stronger noise reduction, but may result in loss of detail.
3D Noise Reduction	Adjust the 3D temporal noise reduction intensity. A larger value indicates stronger noise reduction, but may cause motion blur. **Note:** 3D noise reduction is supported only when the video standard is 25 fps or lower.

Parameter	Description
Image Rotation	Set the image rotation mode. Available options are dynamically displayed based on the device capability set: • **Normal**: No rotation is applied. • **Flip Vertical**: Flip the image vertically. • **Flip Horizontal**: Flip the image horizontally. • **180°**: Rotate the image by 180°. • **90° Clockwise (Corridor Mode)**: Rotate the image 90° clockwise to display in portrait mode. This is suitable for narrow and long scenarios such as corridors. • **90° Anti-clockwise (Corridor Mode)**: Rotate the image 90° anti-clockwise to display in portrait mode. This is suitable for narrow and long scenarios such as corridors.

Exposure

Exposure is used to configure the exposure mode and related parameters of the camera, which affect the brightness and visual effect of the image.

Parameter	Description
Exposure Mode	Select the exposure mode. Available options are dynamically displayed based on the device capability set: • **Automatic**: The device automatically adjusts the shutter and gain. Exposure compensation and metering control are available. • **Custom**: Manually set the shutter and gain ranges. Exposure compensation and metering control are available. • **Indoor 50Hz**: Suitable for indoor environments with 50Hz power frequency. • **Indoor 60Hz**: Suitable for indoor environments with 60Hz power frequency. • **Manual**: Manually set the shutter, gain, and iris. Exposure compensation and metering control are unavailable. • **Low Motion Blur**: Suitable for fast-moving scenarios.
Shutter(us)	Set the exposure shutter time. Two unit options are supported: microsecond input and reciprocal second selection. The display method is determined by the device capability set. In Custom exposure mode, the shutter range can be set.
Gain	Set the image signal gain value. In Custom exposure mode, the gain range can be set.
Slow Shutter	Enable or disable the slow shutter function. When it is enabled, the slowest shutter time can be set. **Note:** When it is enabled, the shutter exposure time is extended, which may cause image trails and a decrease in the frame rate.
Exposure Compensation	Adjust the exposure compensation value. It is unavailable in Manual exposure mode.
Linear Stripe Suppression	Adjust the linear stripe suppression level.
Metering Control	Select the metering mode. Available options are dynamically displayed based on the device capability set: • **Center-Weighted Average Metering**: Meters primarily based on the central area of the image. • **Evaluative Metering (BLC)**: Draw a metering area rectangle on the preview image. Metering is primarily based on this area.

Parameter	Description
	• **Face Metering**: Meters primarily based on the face area. The face brightness and minimum duration can be set. • **Spot Metering**: Draw a metering spot area on the preview image. Metering is primarily based on this spot.
Day/Night Mode	Select the day/night switching mode: • **Auto**: The device automatically switches between day and night modes based on ambient light. The sensitivity and switching time can be set. • **Day**: Always stays in color mode. • **Night**: Always stays in black-and-white mode. • **Input Boolean**: Controls day/night switching through an external digital input signal. Day/Night sensitivity options: Ultra-low, Low, Medium, and High. These are available only in Auto mode.
Day/Night Switching(s)	Select the switching time.
WDR	Select the WDR mode: • **Off**: Disables WDR. • **On**: Enables WDR. The WDR level and stripe suppression can be set. • **Auto**: The device automatically determines whether to enable WDR. The on/off sensitivity can be set. • **Smart**: The device intelligently adjusts the WDR parameters. **Note:** WDR is unavailable when Defog is enabled; Defog is grayed out and cannot be operated when WDR is enabled. WDR is unavailable in Road Highlight Compensation(HLC) and Park Highlight Compensation(HLC) scenes.
WDR Level	After WDR is enabled, adjust this parameter to improve the image effect. A larger value indicates a stronger WDR effect.
Suppress WDR Stripes	Enable or disable the WDR stripe suppression function. When it is enabled, stripe interference generated by WDR can be suppressed.
WDR On/Off Sensitivity	Set the WDR switching sensitivity.

Smart Illumination

Smart Illumination is used to configure the illuminator parameters of the camera. It supports multiple illuminator types and illumination control modes.

Parameter	Description
Smart Illumination	Enable or disable the Smart Illumination function.
Illumination Mode	Select the illuminator type. Available options are dynamically displayed based on the device capability set: • **White Light**: Uses the white light illuminator. • **Smart White Light**: Uses the smart white light illumination. • **Infrared**: Uses the IR illuminator. This is suitable for dark environments at night. • **Dual Light**: Intelligently switches between white light and IR illumination. The illumination mode is automatically selected based on the environment. • **Mixed Lights**: Uses a combination of white light and IR illumination.
Control Mode	Select the illumination control mode. Available options are dynamically displayed based on the device capability set: • **Global Mode**: Balances the overall image brightness.

Parameter	Description
	• **Overexposure Restrain**: Suppresses overexposed areas in the image. • **Custom Level**: Manually set the brightness level of each illuminator group.

White Balance

White Balance is used to configure the white balance mode of the camera and adjust the color reproduction effect of the image.

Parameter	Description
White Balance	Select the white balance mode. Available options are dynamically displayed based on the device capability set: • **Auto**: The device automatically adjusts the white balance. • **Fine Tune**: Manually adjust the R/B offset values. • **Outdoor**: Suitable for outdoor natural light environments. • **Locked**: Locks the current white balance parameters. • **Auto 2**: Auto white balance mode 2. • **Area White Balance**: Draw a white balance area rectangle on the preview image. The white balance is adjusted based on this area as a reference.
Red Offset	Adjust the red channel offset. It can be edited only in Fine Tune, Fine Tune (based on night mode), and night Auto modes.
Blue Offset	Adjust the blue channel offset. It can be edited only in Fine Tune, Fine Tune (based on night mode), and night Auto modes.

Note: In Area White Balance mode, a white balance area rectangle is displayed on the preview image. You can drag to adjust its position, and the coordinates are automatically updated when changed.

Advanced

Advanced parameters are used to configure the Defog and Dewarping functions.

Parameter	Description
Defog	Select the Defog mode: • **Off**: Disables Defog. • **On**: Enables Defog. The Defog level can be set. • **Auto**: The device automatically determines whether to enable Defog. The Defog level can be set. **Note:** Defog and WDR are mutually exclusive. WDR is unavailable when Defog is enabled, and Defog cannot be operated when WDR is enabled.
Dewarping	Select the Dewarping mode: • **Off**: Disables Dewarping. • **On**: Enables Dewarping. The dewarping level can be set.

Video Standard

Video Standard is used to configure the video system parameters of the device.

Parameter	Description
Region	Select the country or region where the device is located. This is displayed only during the first login. The region determines the default video standard.

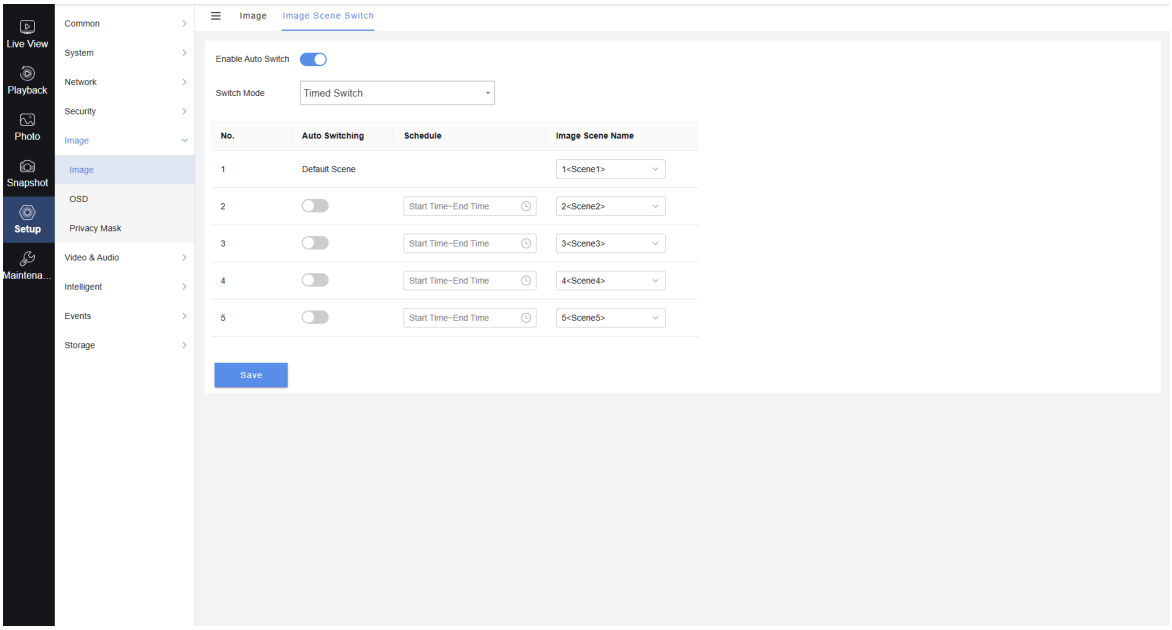
Parameter	Description
Video Standard	Select the video system: • **PAL**: PAL system, 25 fps. • **NTSC**: NTSC system, 30 fps.

Note: For first-time login, select the region first. The region determines the default video standard. For subsequent logins, only the video standard can be modified.

7.5.1.2 Image Scene Switch

Image Scene Switch is used to automatically switch the image scene of the device according to a preset schedule or preset. When different image parameters are required for different time periods, enabling this function allows the device to automatically switch to the corresponding scene mode at the specified time without manual operation.

Note: After the auto switching function is disabled, all auto switching schedules become ineffective, but the configuration information is retained.



1. Click the switch to enable the auto switching function.
2. Select a switch mode and configure the corresponding parameters.

Parameter	Description
Switch Mode	Timed Switch: Automatically switch scenes according to a schedule. You need to configure the start time, end time, and corresponding scene for each time period in the scene switching schedule table.

3. In the scene switching schedule table, configure the scene and time for each time period.

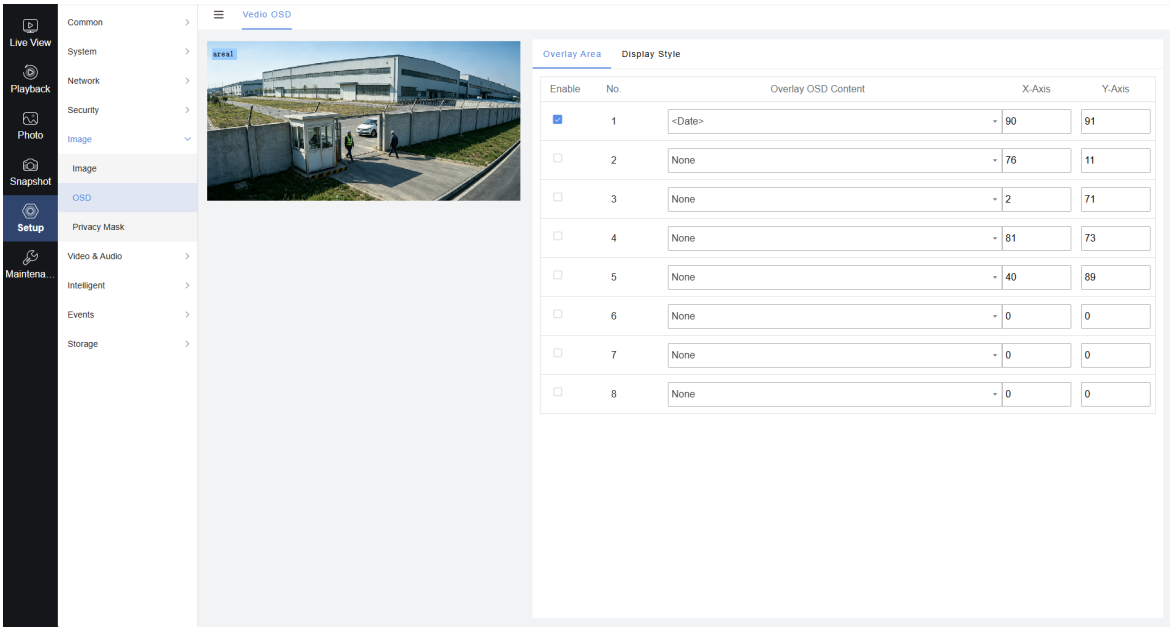
Parameter	Description
Default Scene	Select the default image scene used when no scheduled time period is active. The default scene row cannot be deleted.
Auto Switching	After it is enabled, the time period is added to the auto switching schedule.
Schedule	Set the time period for auto switching. Time periods cannot overlap.
Image Scene Name	Select the target image scene to switch to during the time period.

4. Click **Save** to complete the configuration.

7.5.2 OSD Configuration

7.5.2.1 Video OSD

Overlay OSD information (such as date and time, custom text, and pictures) on the video image. The overlay area position and content display style can be configured.



The Video OSD function supports overlaying multiple types of information on the live video image, including date and time, custom text, and pictures. The page adopts a left-right split layout. The left side is the video preview area, where you can view the OSD overlay effect in real time and drag to adjust the area position. The right side is the configuration panel, which contains the **Overlay Area** and **Display Style** tabs.

Configuring the Overlay Area

1. Select a video channel.
2. On the **Overlay Area** tab, select an area and the overlay OSD content type:

Overlay Content Type	Description
Custom	Enter custom text.
Date & Time	Overlay both date and time information.
Time	Overlay time information only.
Date	Overlay date information only.
PTZ Coordinates	Display the P/T/Z coordinates of the PTZ.
Zoom	Display the zoom information.
Preset	Display the current preset information.
Alarm	Overlay alarm information.
Serial Port	Overlay information reported by the serial port.
Direction	Overlay the PTZ direction information.
People Counting	Overlay people counting information.
Network Port	Overlay network port information. Confirm the security risk before selecting this option.
Sensing	Overlay intelligent sensing information, which needs to be selected from the sensing list.

Overlay Content Type	Description
Battery Status	Overlay battery level information.
Picture Overlay	Overlay pictures. BMP and PNG formats are supported, and the transparency can be set.
Vehicle Flow	Overlay vehicle flow statistics information.
Non-Motor Vehicle Flow	Overlay non-motor vehicle flow statistics information.
Pedestrian Flow	Overlay pedestrian flow statistics information.
Motor Vehicle&Non-Motor Vehicle&Pedestrian Count	Comprehensively overlay the flow statistics information of motor vehicles, non-motor vehicles, and pedestrians.
Scene Name	Overlay the scene name.
Temperature	Overlay temperature information.
Device Latitude and Longitude Coordinates	Overlay GPS positioning information.
Mobile Network	Overlay mobile network status information.
Vehicle Plate Info	Overlay the license plate number.
Parking Space	Overlay the parking space status.
Vehicle Passing Record	Overlay vehicle passing record information.
Gate Status	Overlay the barrier gate open/close status.

Note: The available overlay content types depend on the device capability.

3. Drag the area on the video image to adjust the position, or click the edit icon to configure the area parameters in the pop-up dialog box:

Parameter	Description
X-Axis	The horizontal coordinate of the upper-left corner of the area.
Y-Axis	The vertical coordinate of the upper-left corner of the area.
Alignment Mode	The alignment mode of the OSD content.
Upload Picture	This can be set only when the overlay content is Picture Overlay. Select and upload a picture file.

4. Use the **Move Up** and **Move Down** buttons to adjust the OSD order.
5. Click **Save** to complete the overlay area configuration.

Configuring the Display Style

1. Switch to the **Display Style** tab.
2. Configure the OSD display style:

Parameter	Description
Effect	Set the font display effect. The available options are subject to the device capability.
Font Size	Set the OSD font size. The available options are subject to the device capability.
Font Color	Set the OSD font color. This can be configured only when the device supports custom colors.
Min. Margin	Set the minimum margin between the OSD and the image edge. The available options are subject to the device capability.

Parameter	Description
Date Format	Select the date display format.
Time Format	Select the time display format.

3. (Optional) Click **GA/T751 Mode** to switch the OSD configuration to the GA/T751 industry standard configuration with one click. After it is enabled, the system automatically sets the font effect to Normal, the font size to Medium, the date format and time format to standard values, and the minimum margin to one character width. Meanwhile, the OSD overlay information is reassigned to each area according to the GA/T751 standard.
4. Click **Save** to complete the display style configuration.

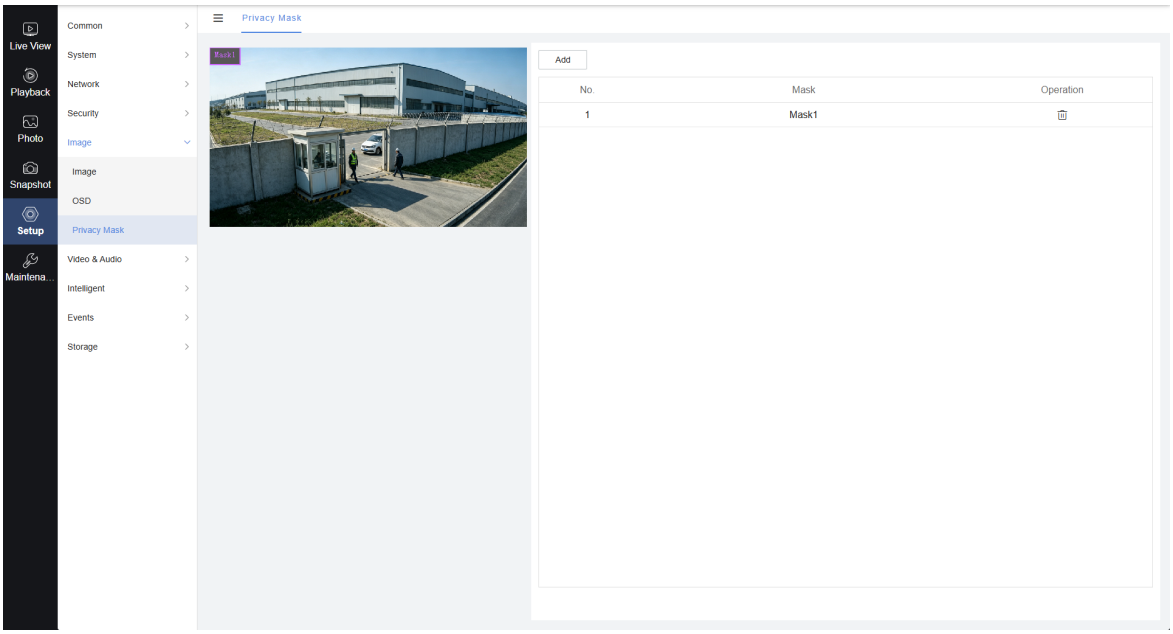
Managing OSD Configurations

Operation	Description
Edit	Click the edit icon in the overlay area list to modify parameters such as coordinates and alignment mode of the area.
Move Up/Move Down	Click the Move Up or Move Down button to adjust the order of OSD overlay content in the list.
Enable/Disable	In the overlay area list, select or clear the enable checkbox to quickly enable or disable a single OSD overlay area.

7.5.3 Privacy Mask

Privacy Mask is used to draw rectangular mask areas on the video image to cover sensitive information (such as private areas and password keypads), preventing those areas from being exposed in live view and recordings.

Note: The maximum number of mask areas supported by each channel depends on the device capability. Once the limit is reached, no more mask areas can be added. After modifying the position of a mask area, the change takes effect immediately without additional save operations.



Adding a Mask Area

1. Click **Add**, and the system adds a mask area that covers the upper-left corner by default.
2. Drag the mask frame on the video preview image to adjust the position and size of the mask area. The parameters are described below.

Parameter	Description
No.	The sequence number of the mask area, which increments automatically starting from 1.
Mask	The name of the mask area, in the format "Mask + No." (e.g., Mask 1, Mask 2), which is automatically generated by the system.

Managing Mask Areas

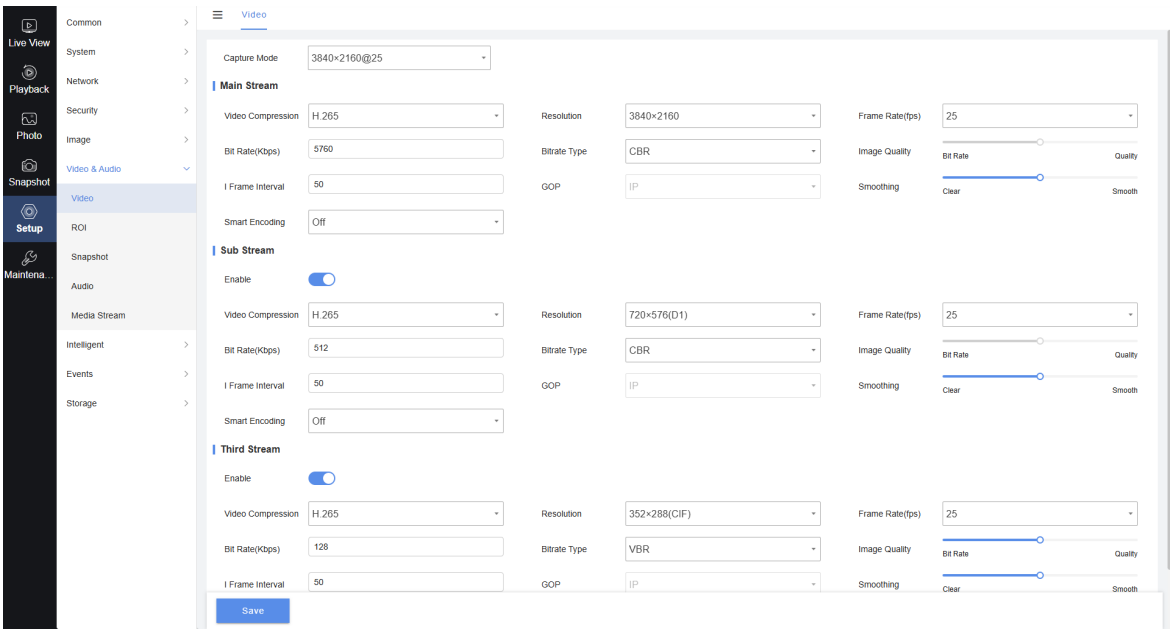
- Select a mask area. In the overlay area list, click the corresponding entry or click the mask frame on the video image to select the mask area. Once selected, you can drag it on the video image to adjust its position and size.
- Delete a mask area. In the overlay area list, click the icon of the corresponding entry to delete the mask area.

7.6 Video & Audio

7.6.1 Video

Video configuration is used to set the video encoding parameters of the IPC device, including capture mode and multi-stream encoding parameters. Proper encoding configuration can effectively save storage space and network bandwidth while ensuring image quality.

Note: Changing the capture mode will reset the encoding parameters to default. For some models, the device will also restart.



1. Select a capture mode. The capture mode options are combinations of resolutions and frame rates supported by the device.
2. Configure the stream encoding parameters. The device supports multiple streams, and each stream can be configured independently. The main stream is enabled by default and cannot be disabled.

Parameter	Description
Enable	Enable or disable this stream. The sub stream and above can be turned on or off.
Video Compression	Select a video compression format. The available options are limited by the device capability set: • **MJPEG**: Motion JPEG encoding. When selected, Bit Rate, I Frame Interval, U-Code, and Smoothing are unavailable, and the bitrate type is forced to VBR. • **H.264**: H.264 encoding.

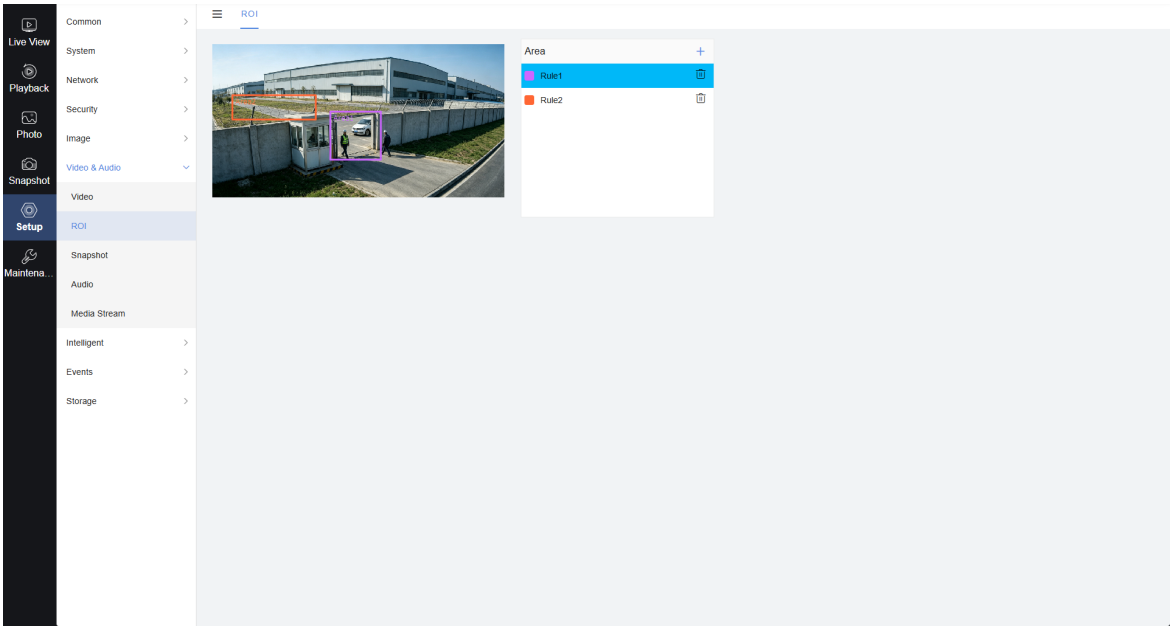
Parameter	Description
	• **H.265**: H.265 encoding. The bitrate is approximately 50% to 70% of H.264 at the same image quality.
Resolution	Select a video resolution. The sub stream resolution cannot exceed the main stream resolution. The options change dynamically based on the capture mode and encoding capability.
Frame Rate(fps)	Select a video frame rate. The options change dynamically based on the resolution and capture mode. The maximum value is limited by the resolution and capture mode frame rate.
Bit Rate(Kbps)	Set the video bit rate.
Bitrate Type	Select a bitrate control mode: • **CBR**: The bit rate remains constant, and the network bandwidth usage is stable. • **VBR**: Used together with image quality. The bit rate is dynamically adjusted based on image complexity and fluctuates below the set upper limit.
Image Quality	In VBR mode, drag the slider to adjust the image quality.
I Frame Interval	Set the I frame interval. This parameter is unavailable when MJPEG is selected.
GOP	Select a GOP structure type. The available options are limited by the device capability set, including IP, IBP, IBBP, and I types.
Smoothing	Drag the slider to adjust the stream smoothing. This parameter is unavailable when MJPEG is selected.
Smart Encoding	Select a smart encoding mode. Device support is required. The available options are limited by the device capability set: • **Off**: Smart encoding is not used. • **Basic Mode**: Basic smart encoding. • **Advanced Mode**: Advanced smart encoding with higher encoding efficiency. • **Super H.265**: Enhanced smart encoding based on H.265, which provides higher encoding efficiency and a lower bit rate at the same image quality. It is available only when the encoding format is set to H.265.

3. Click **Save** to complete the configuration.

7.6.2 ROI

Region of Interest (ROI) is used to define key areas on the video image and improve the encoding quality of those areas. It applies to scenarios that require focusing on local details (such as license plates and faces) in the image, allowing key areas to achieve clearer image quality under a limited bitrate.

Note: Area coordinates are automatically saved after being changed. You do not need to click the Save button manually. When the number of areas reaches the limit, no more areas can be added.



Add Area

1. Click ＋, and the system automatically adds a rectangular area on the video image and selects it.
2. Drag the rectangular frame on the video image to adjust the area position and size. The area is automatically saved after you release. The area parameters are described as follows.

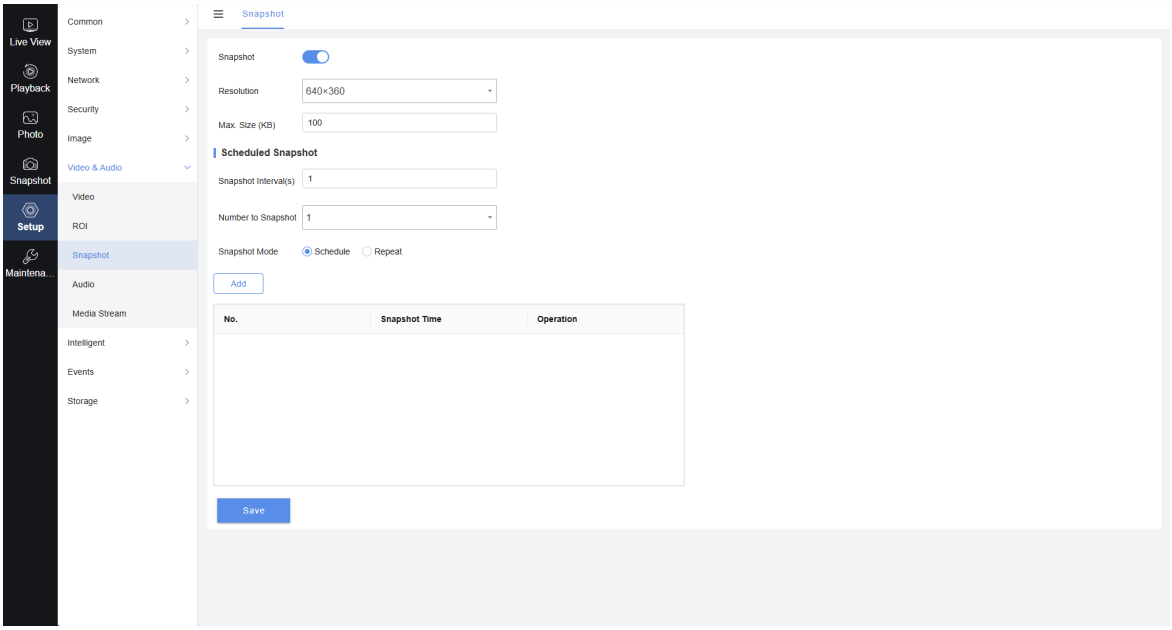
Parameter	Description
Area ID	Automatically assigned in the format "Rule 1–Rule 8". Each area has a different color identifier.
Area Position	Adjusted by dragging the rectangular frame.
Max. Areas	Determined by the device capability set.

Manage Area

- Select an area. Click the target area in the area list, or click the rectangular frame on the video image. After selection, the rectangular frame is highlighted.
- Adjust the area. Drag the rectangular frame on the video image to adjust the area position and size. The area is automatically saved after you release.
- Delete an area. In the area list, click 🗑 on the right of the target area. The configuration is automatically saved after deletion. After the currently selected area is deleted, the system automatically selects the first enabled area.

7.6.3 Snapshot

The snapshot function is used to automatically capture images from the surveillance screen according to a configured schedule. The captured images can be uploaded to a storage device or server at a specified resolution and size for later review and evidence collection.



1. Click to enable the snapshot function.
2. Configure the following parameters.

Parameter	Description
Resolution	Select the image resolution for snapshots. The options vary by device model.
Max. Size (KB)	The maximum file size of a snapshot image. The value range changes dynamically based on the resolution.

3. Configure the scheduled snapshot parameters.

Parameter	Description
Snapshot Interval(s)	The time interval between two consecutive snapshots.
Number to Snapshot	The number of snapshots captured per trigger.
Snapshot Mode	Select a snapshot time mode: • **Schedule**: Captures images at specified time points. Click **Add**, select the snapshot time, and then click **OK**. • **Repeat**: Captures images periodically at a configured interval. Enter the interval and configure the scheduled snapshot plan.

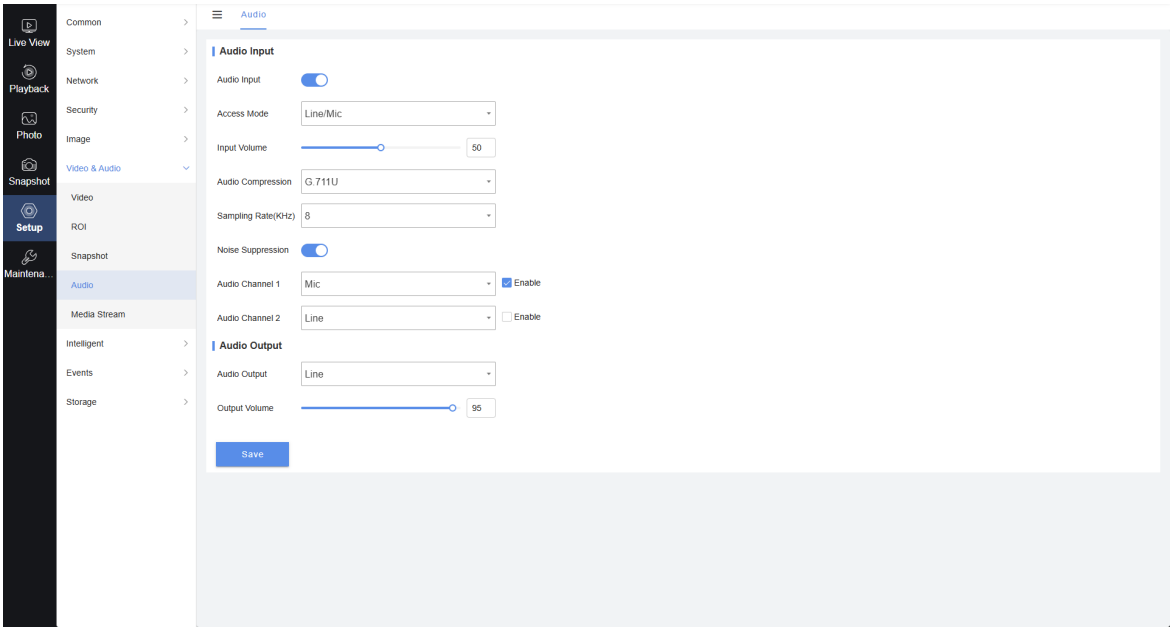
4. Click **Save** to complete the configuration.

7.6.4 Audio

7.6.4.1 Audio

Configure audio input and audio output parameters to set the audio capture mode, audio compression, volume, and audio output mode of the device, thereby enabling the device to capture and play audio.

Note: When the audio compression is AAC-LC and the sampling rate is 8KHz, AAC audio plays poorly in Firefox 58 and later. It is recommended to use other browsers. When the audio input is not muted, at least one audio channel must be enabled.



1. Configure audio input parameters.

Parameter	Description
Audio Input	Enable or disable audio input. When enabled, the device captures surrounding sounds.
Access Mode	Line/Mic: Input via line or microphone.
Input Volume	Set the audio input volume.
Audio Compression	Select the audio compression format.
Sampling Rate	Select the audio sampling rate.
Noise Suppression	Enable or disable noise suppression to reduce background noise.
Audio Channel 1	Set the input mode and enable status of Audio Channel 1.
Audio Channel 2	Set the input mode and enable status of Audio Channel 2.

2. Configure audio output parameters.

Parameter	Description
Audio Output	Select the audio output mode.
Output Volume	Set the audio output volume.
Call Waiting Timeout(s)	Set the call waiting timeout for two-way audio.

3. Click **Save** to complete the configuration.

7.6.4.2 Audio File

The **Audio File** page is used to manage alarm audio files on the device. You can set the alarm volume and upload custom audio files as alarm tones. You can also play, rename, and delete uploaded audio files.

Note: Built-in audio files cannot be modified or deleted.

Configuring Audio Files

1. Set the alarm volume. Drag the alarm volume slider to set the output volume of the alarm audio. A larger value indicates a higher volume.
2. Upload an audio file. Click **Import** and select a local audio file to upload.
3. Click **Save** to complete the audio file configuration.

Managing Audio Files

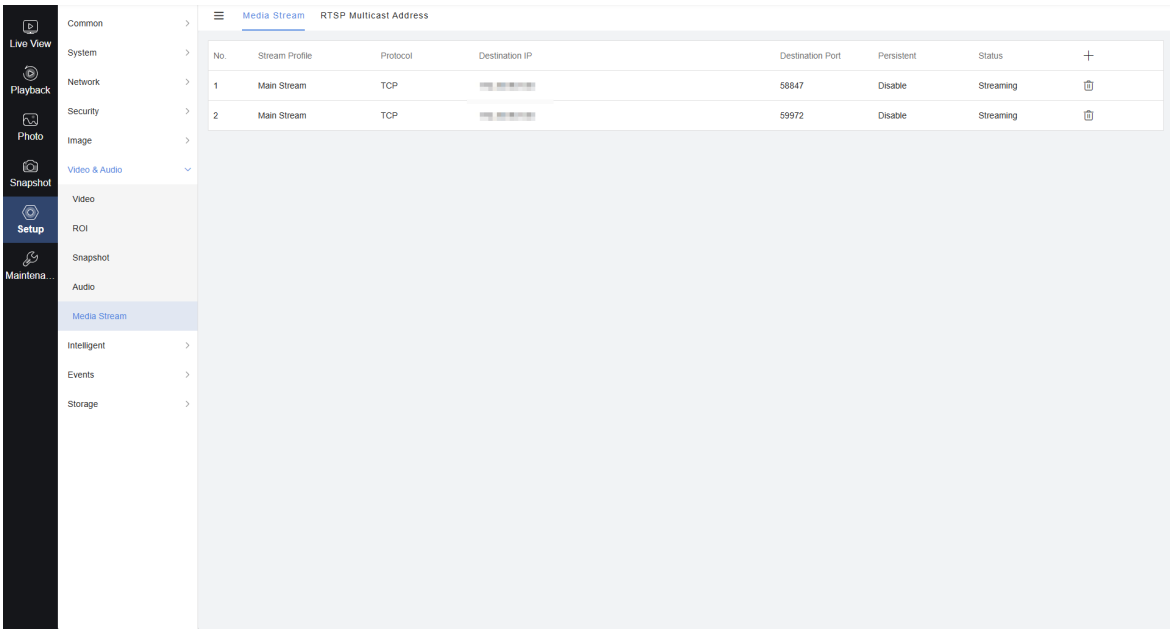
- Play audio. In the audio file list, click of the corresponding entry to play the audio.
- Rename audio. In the audio file list, click of the user-imported entry, enter a new name, and click **OK**.
- Delete audio. In the audio file list, click of the user-imported entry and confirm to delete the audio file. Audio files in use cannot be deleted.

7.6.5 Media Stream

7.6.5.1 Media Stream

Media Stream is used to manage media stream forwarding sessions on the device, pushing the device video stream to a specified destination address for remote forwarding and distribution of the video stream.

Note: The number of media streams that can be added has a limit. When the limit is reached, no more media streams can be added.



Add Media Stream

1. Click + to go to the **Add Media Stream** configuration page.
2. Configure the media stream parameters. The parameters are described as follows.

Parameter	Description
Stream Profile	Select the video stream type to be forwarded.
Destination IP	Enter the destination address for pushing the media stream.
Protocol	RTMP: Real-Time Messaging Protocol. The destination address must start with rtmp://.
Persistent	When enabled, the media stream session is automatically restored after the device restarts.

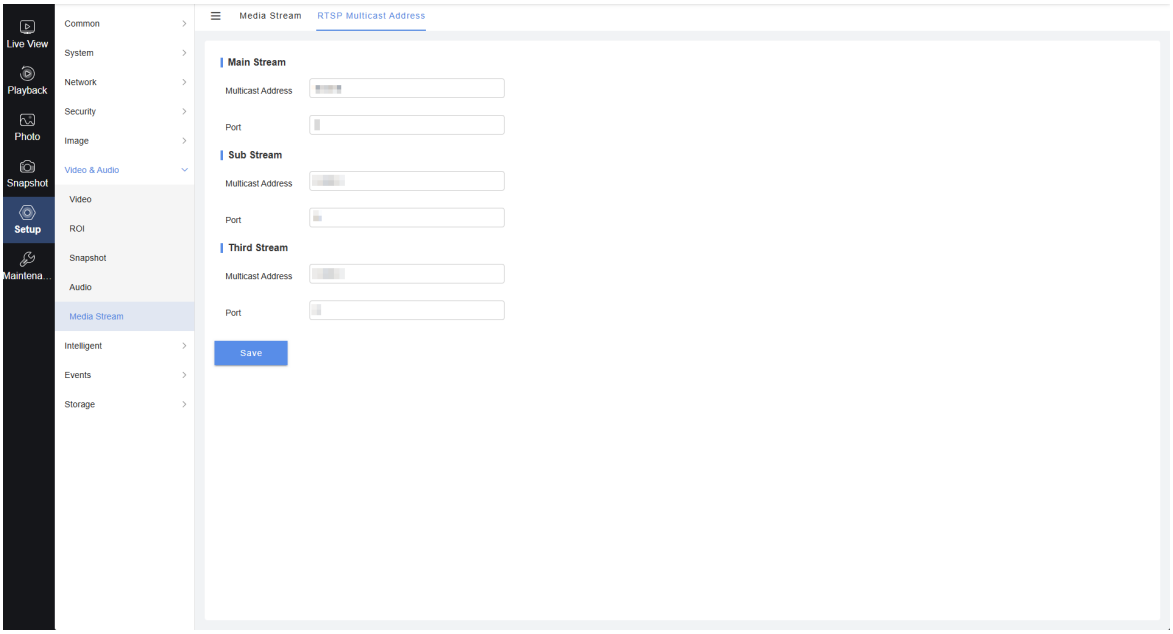
3. Click **OK** to complete adding the media stream.

Manage Media Stream

In the media stream list, click of the target entry and confirm to delete it.

7.6.5.2 RTSP Multicast

By configuring the RTSP multicast address and port for each stream, the device distributes video streams via multicast over the network. Clients can receive video streams through the multicast address, thereby reducing network bandwidth consumption.



1. Configure the multicast address and port for each stream.

Parameter	Description
Multicast Address	Enter the RTSP multicast address. Entering 0.0.0.0 indicates that multicast is disabled for this stream.
Port	Enter the multicast port number.

2. Click **Save** to complete the configuration.

7.7 Smart

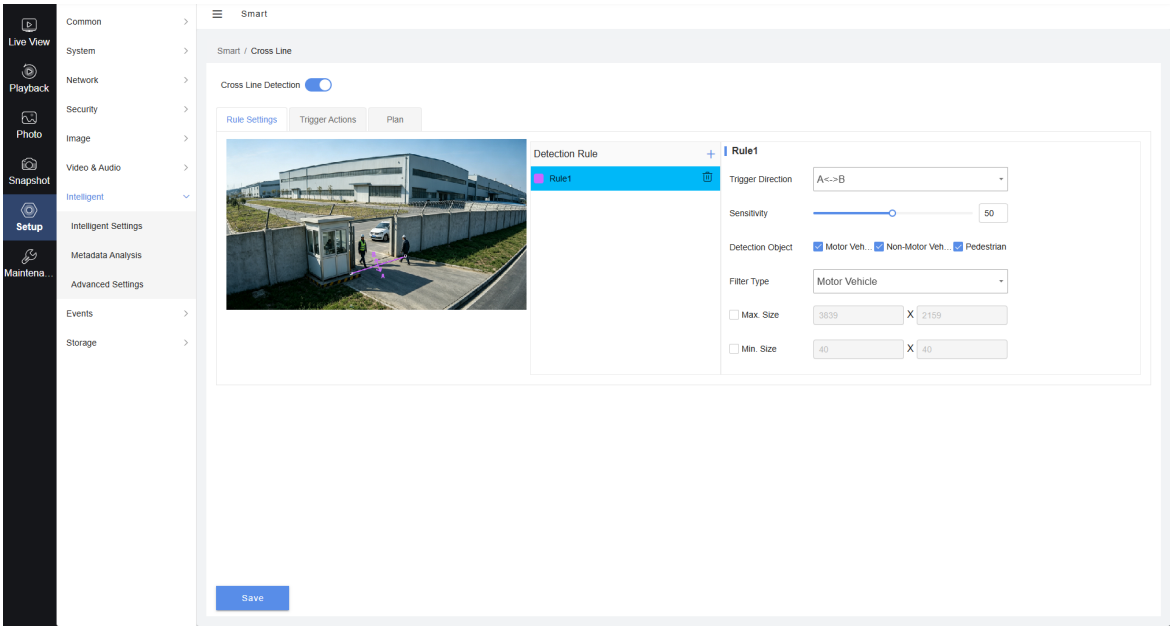
7.7.1 Smart Settings

7.7.1.1 Smart Service

7.7.1.1.1 Perimeter Protection

7.7.1.1.1.1 Cross Line

Draw a detection line on the video image and set the trigger direction. When a target crosses the detection line in the specified direction, alarm linkage is triggered.



1. Find **Cross Line** on the **Smart** page and enable it.
2. Click the icon to go to the **Cross Line** configuration page.

   Note: If other smart detection functions are already enabled and are mutually exclusive with **Cross Line**, a confirmation dialog box is displayed when you enable it. After confirmation, the device automatically disables the conflicting smart functions.

3. On the **Rule Settings** tab, click + to add a detection rule, draw a detection line on the video image, and configure the rule parameters:

Parameter	Description
Detection Line	Draw a detection line on the video image. The line position is determined by two endpoints. Drag the endpoints to adjust the position and angle of the detection line.
Trigger Direction	• **A<->B**: Bidirectional trigger. An alarm is triggered when a target crosses the detection line from either direction • **A->B**: An alarm is triggered only when a target crosses the detection line from end A to end B • **B->A**: An alarm is triggered only when a target crosses the detection line from end B to end A
Sensitivity	Set the detection sensitivity. A larger value indicates higher sensitivity. Higher sensitivity makes alarms easier to trigger but may increase the false alarm rate. Adjust the settings based on the actual scenario to determine the optimal configuration.
Detection Object	Displayed when the device supports deep intelligence. Select the target types to detect: • **Motor Vehicle**: Detects motor vehicle targets • **Non-Motor Vehicle**: Detects non-motor vehicle targets • **Pedestrian**: Detects pedestrian targets Select at least one detection object.

Parameter	Description
Filter by Object Size	Displayed when the device supports deep intelligence. After you select the checkbox to enable it, draw rectangles on the video image to set the target size range: • **Max. Size**: Width × height. Targets larger than this size will be filtered out • **Min. Size**: Width × height. Targets smaller than this size will be filtered out The max. size must be greater than the min. size.

Note: Up to 4 detection rules can be added. Each rule corresponds to one detection line, and parameters such as sensitivity and trigger direction can be configured independently for each rule.

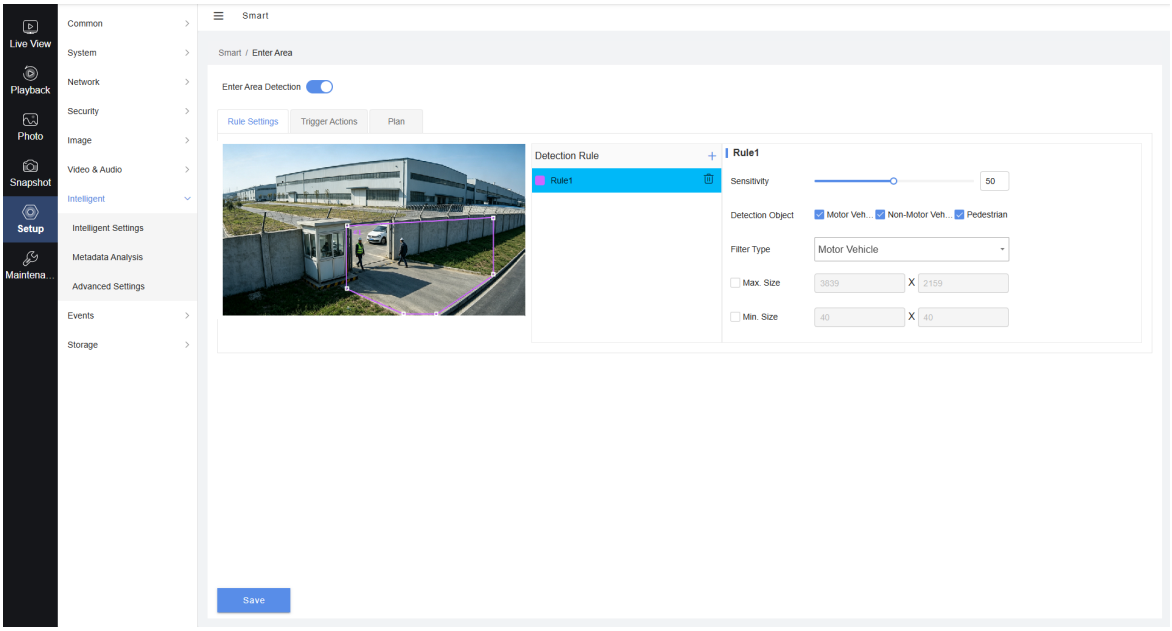
4. (Optional) Configure trigger actions on the **Trigger Actions** tab.

Trigger Action	Description
Conventional	• **Send E-mail**: After you select the checkbox, an alarm email is sent when an alarm is triggered. Before using this function, complete the sender and recipient configuration in E-mail • **Attribute Collection**: After you select the checkbox, target attribute information is collected when an alarm is triggered • **Upload Image(Original)**: After you select the checkbox, full-view snapshots are uploaded when an alarm is triggered. Requires the device to support deep intelligence
Alarm Output	• **A->1**: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered • **Alarm Sound**: After you select the checkbox, an audio alarm is activated when an alarm is triggered. The alert tone and the number of alarm repetitions can be configured • **Flashing Light**: After you select the checkbox, the light flashes when an alarm is triggered. The flashing duration can be configured
Storage	• **Recording Edge Storage**: After you select the checkbox, videos are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **Image Edge Storage**: After you select the checkbox, snapshots are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **FTP Video Storage**: After you select the checkbox, videos are stored to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP

5. (Optional) Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and **Cross Line** takes effect only during the arming periods.
6. Click **Save** to complete the configuration.

7.7.1.1.1.2 Enter Area

Draw a detection area on the video image. When a target is detected entering the area, alarm linkage is triggered.



1. Find **Enter Area** on the **Smart** page and enable it.
2. Click the icon to go to the **Enter Area** page.

   Note: If other smart detection functions are already enabled and are mutually exclusive with **Enter Area**, a confirmation dialog box is displayed when you enable it. After confirmation, the device automatically disables the conflicting smart functions.

3. On the **Rule Settings** tab, click + to add a detection rule, draw a detection area on the video image, and configure the rule parameters:

Parameter	Description
Detection Area	Draw a polygon detection area on the video image. Drag the vertices to adjust the shape and position of the area.
Sensitivity	Set the detection sensitivity. A larger value indicates higher sensitivity. Higher sensitivity makes alarms easier to trigger but may increase the false alarm rate. Adjust the settings based on the actual scenario to determine the optimal configuration.
Detection Object	Select the target types to detect: • **Motor Vehicle**: Detects motor vehicle targets • **Non-Motor Vehicle**: Detects non-motor vehicle targets • **Pedestrian**: Detects pedestrian targets Select at least one detection object.
Filter by Object Size	After you select the checkbox to enable it, draw rectangles on the video image to set the target size range: • **Max. Size**: Width × height. Targets larger than this size will be filtered out • **Min. Size**: Width × height. Targets smaller than this size will be filtered out The max. size must be greater than the min. size.

   Note: Up to 4 detection rules can be added. Each rule corresponds to one detection area, and parameters such as sensitivity and detection object can be configured independently for each rule.

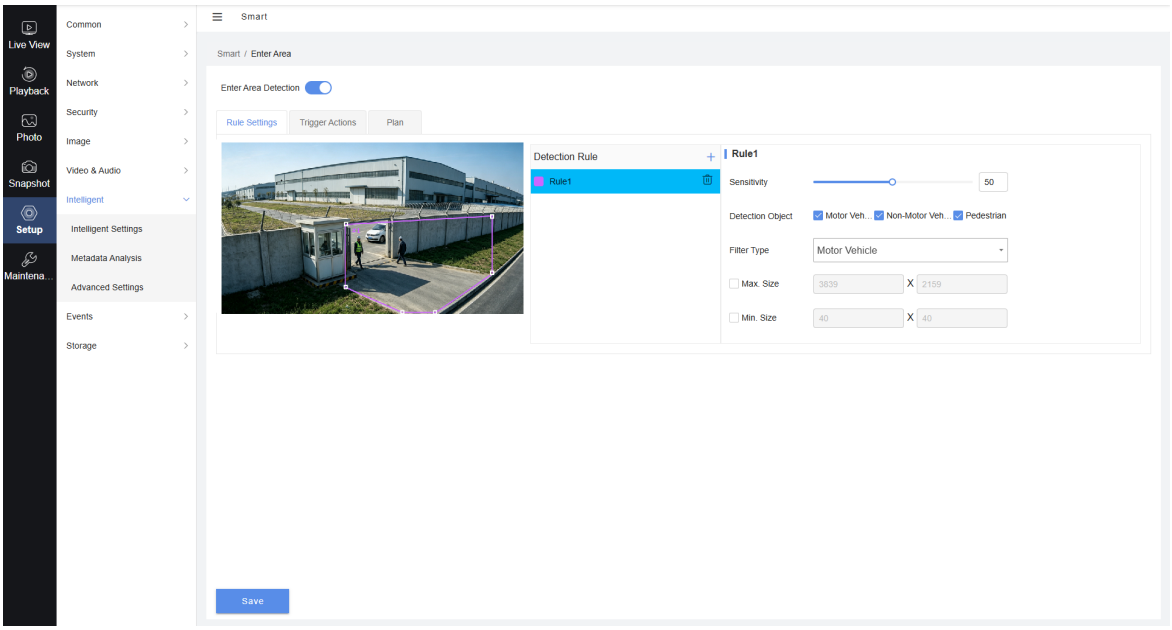
4. (Optional) Configure trigger actions on the **Trigger Actions** tab.

Trigger Action	Description
Conventional	• **Send E-mail**: After you select the checkbox, an alarm email is sent when an alarm is triggered. Before using this function, complete the sender and recipient configuration in E-mail • **Attribute Collection**: After you select the checkbox, target attribute information is collected when an alarm is triggered • **Upload Image(Original)**: After you select the checkbox, full-view snapshots are uploaded when an alarm is triggered. Requires the device to support deep intelligence
Alarm Output	• **A->1**: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered • **Alarm Sound**: After you select the checkbox, an audio alarm is activated when an alarm is triggered. The alert tone and the number of alarm repetitions can be configured • **Flashing Light**: After you select the checkbox, the light flashes when an alarm is triggered. The flashing duration can be configured
Storage	• **Recording Edge Storage**: After you select the checkbox, videos are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **Image Edge Storage**: After you select the checkbox, snapshots are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **FTP Video Storage**: After you select the checkbox, videos are stored to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP

5. (Optional) Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and **Enter Area** detection takes effect only during the arming periods.
6. Click **Save** to complete the configuration.

7.7.1.1.1.3 Leave Area

Draw a detection area on the video image. When a target is detected leaving the area, alarm linkage is triggered.



1. Find **Leave Area** on the **Smart** page and enable it.
2. Click the icon to go to the **Leave Area** page.

   Note: If other smart detection functions are already enabled and are mutually exclusive with **Leave Area**, a confirmation dialog box is displayed when you enable it. After confirmation, the device automatically disables the conflicting smart functions.

3. On the **Rule Settings** tab, click + to add a detection rule, draw a detection area on the video image, and configure the rule parameters:

Parameter	Description
Detection Area	Draw a polygon detection area on the video image. Drag the vertices to adjust the shape and position of the area.
Sensitivity	Set the detection sensitivity. A larger value indicates higher sensitivity. Higher sensitivity makes alarms easier to trigger but may increase the false alarm rate. Adjust the settings based on the actual scenario to determine the optimal configuration.
Detection Object	Select the target types to detect: • **Motor Vehicle**: Detects motor vehicle targets • **Non-Motor Vehicle**: Detects non-motor vehicle targets • **Pedestrian**: Detects pedestrian targets Select at least one detection object.
Filter by Object Size	After you select the checkbox to enable it, draw rectangles on the video image to set the target size range: • **Max. Size**: Width × height. Targets larger than this size will be filtered out • **Min. Size**: Width × height. Targets smaller than this size will be filtered out The max. size must be greater than the min. size.

   Note: Up to 4 detection rules can be added. Each rule corresponds to one detection area, and parameters such as sensitivity and detection object can be configured independently for each rule.

4. (Optional) Configure trigger actions on the **Trigger Actions** tab.

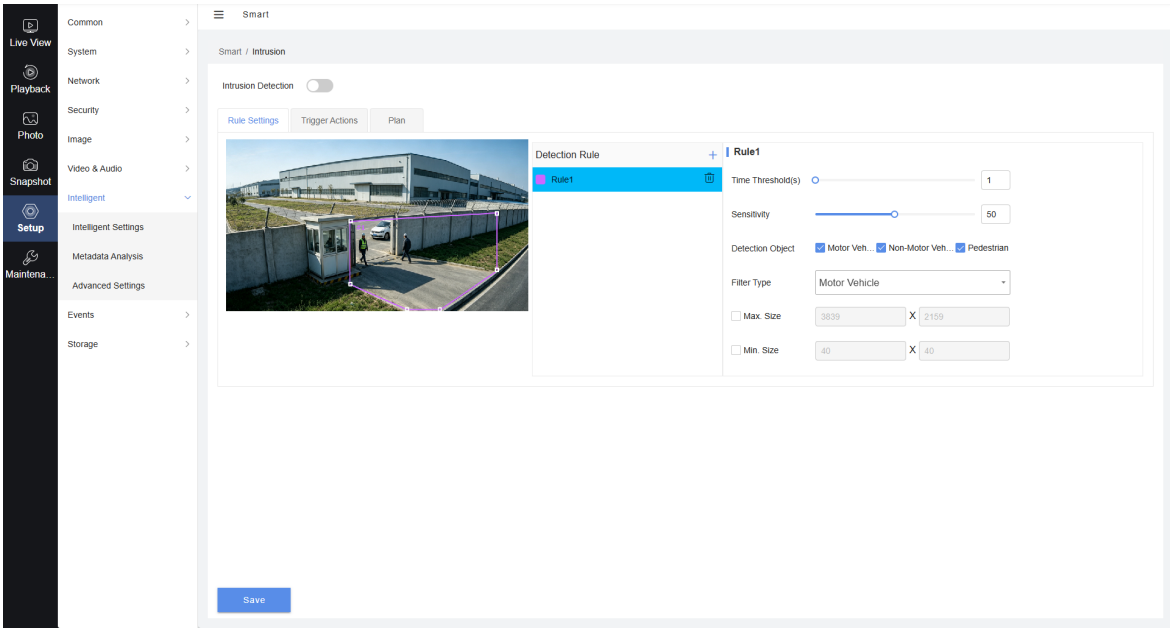
Trigger Action	Description
Conventional	• **Send E-mail**: After you select the checkbox, an alarm email is sent when an alarm is triggered. Before using this function, complete the sender and recipient configuration in E-mail • **Attribute Collection**: After you select the checkbox, target attribute information is collected when an alarm is triggered • **Upload Image(Original)**: After you select the checkbox, full-view snapshots are uploaded when an alarm is triggered. Requires the device to support deep intelligence
Alarm Output	• **A->1**: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered • **Alarm Sound**: After you select the checkbox, an audio alarm is activated when an alarm is triggered. The alert tone and the number of alarm repetitions can be configured • **Flashing Light**: After you select the checkbox, the light flashes when an alarm is triggered. The flashing duration can be configured
Storage	• **Recording Edge Storage**: After you select the checkbox, videos are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management

Trigger Action	Description
	• **Image Edge Storage**: After you select the checkbox, snapshots are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **FTP Video Storage**: After you select the checkbox, videos are stored to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP

5. (Optional) Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and **Leave Area** detection takes effect only during the arming periods.
6. Click **Save** to complete the configuration.

7.7.1.1.1.4 Intrusion

Draw a detection area on the video image. When a target is detected staying in the area for longer than the specified time, alarm linkage is triggered.



1. Find **Intrusion** on the **Smart** page and enable it.
2. Click the icon to go to the **Intrusion** page.

   Note: If other smart detection functions are already enabled and are mutually exclusive with **Intrusion**, a confirmation dialog box is displayed when you enable it. After confirmation, the device automatically disables the conflicting smart functions.

3. On the **Rule Settings** tab, click + to add a detection rule, draw a detection area on the video image, and configure the rule parameters:

Parameter	Description
Detection Area	Draw a polygon detection area on the video image. Drag the vertices to adjust the shape and position of the area.
Time Threshold(s)	Set the minimum time a target must stay in the detection area before an alarm is triggered. An alarm is triggered only after the target stays in the area for longer than this threshold.
Sensitivity	Set the detection sensitivity. A larger value indicates higher sensitivity. Higher sensitivity makes alarms easier to trigger but may increase the false alarm rate. Adjust the settings based on the actual scenario to determine the optimal configuration.

Parameter	Description
Detection Object	Select the target types to detect: • **Motor Vehicle**: Detects motor vehicle targets • **Non-Motor Vehicle**: Detects non-motor vehicle targets • **Pedestrian**: Detects pedestrian targets Select at least one detection object.
Filter by Object Size	After you select the checkbox to enable it, draw rectangles on the video image to set the target size range: • **Max. Size**: Width × height. Targets larger than this size will be filtered out • **Min. Size**: Width × height. Targets smaller than this size will be filtered out The max. size must be greater than the min. size.

Note: Up to 4 detection rules can be added. Each rule corresponds to one detection area, and parameters such as time threshold and sensitivity can be configured independently for each rule.

4. (Optional) Configure trigger actions on the **Trigger Actions** tab.

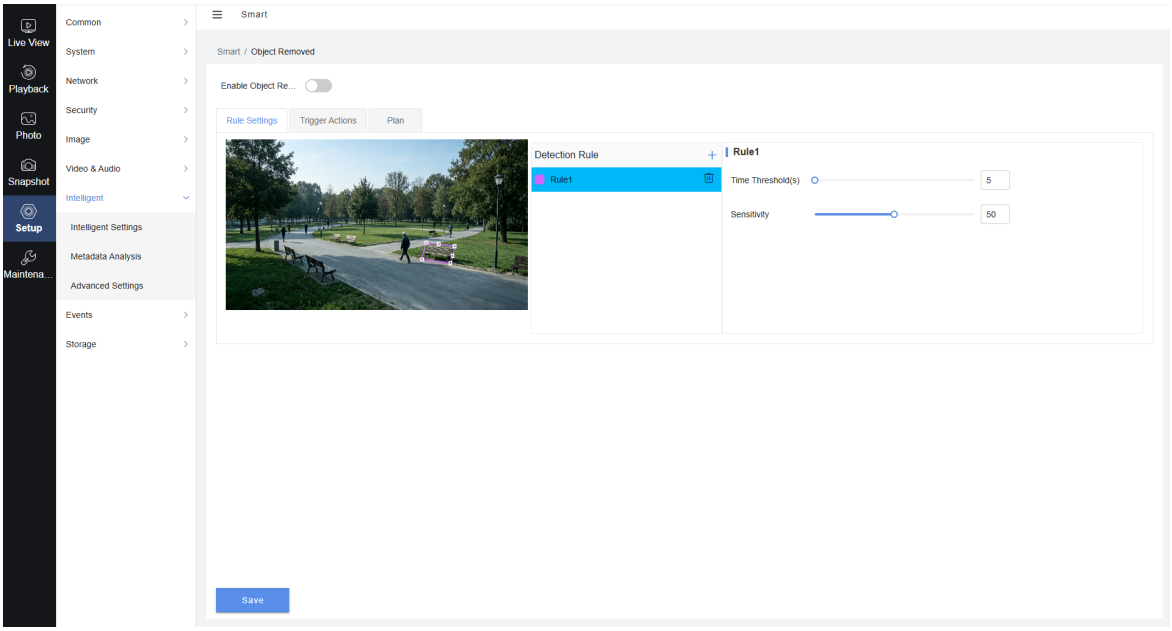
Trigger Action	Description
Conventional	• **Send E-mail**: After you select the checkbox, an alarm email is sent when an alarm is triggered. Before using this function, complete the sender and recipient configuration in E-mail • **Attribute Collection**: After you select the checkbox, target attribute information is collected when an alarm is triggered • **Upload Image(Original)**: After you select the checkbox, full-view snapshots are uploaded when an alarm is triggered. Requires the device to support deep intelligence
Alarm Output	• **A->1**: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered • **Alarm Sound**: After you select the checkbox, an audio alarm is activated when an alarm is triggered. The alert tone and the number of alarm repetitions can be configured • **Flashing Light**: After you select the checkbox, the light flashes when an alarm is triggered. The flashing duration can be configured
Storage	• **Recording Edge Storage**: After you select the checkbox, videos are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **Image Edge Storage**: After you select the checkbox, snapshots are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **FTP Video Storage**: After you select the checkbox, videos are stored to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP

5. (Optional) Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and **Intrusion** detection takes effect only during the arming periods.
6. Click **Save** to complete the configuration.

7.7.1.1.2 Scene Detection

7.7.1.1.2.1 Object Removed

Draw a detection area on the video image. When an object in the area is detected being removed and the duration exceeds the time threshold, alarm linkage is triggered.



1. Find **Object Removed** on the **Smart** page and enable it.
2. Click the icon to go to the **Object Removed** page.

   Note: If other smart detection functions are already enabled and are mutually exclusive with **Object Removed**, a confirmation dialog box is displayed when you enable it. After confirmation, the device automatically disables the conflicting smart functions.

3. On the **Rule Settings** tab, click + to add a detection rule, draw a detection area on the video image, and configure the rule parameters:

Parameter	Description
Detection Area	Draw a polygon detection area on the video image. Drag the vertices to adjust the shape and position of the area.
Time Threshold(s)	Set the duration after an object is removed before an alarm is triggered. An alarm is triggered only after the object is removed and the duration exceeds this threshold.
Sensitivity	Set the detection sensitivity. A larger value indicates higher sensitivity. Higher sensitivity makes alarms easier to trigger but may increase the false alarm rate. Adjust the settings based on the actual scenario to determine the optimal configuration.

   Note: Up to 4 detection rules can be added. Each rule corresponds to one detection area, and the time threshold and sensitivity can be configured independently for each rule.

4. (Optional) Configure trigger actions on the **Trigger Actions** tab.

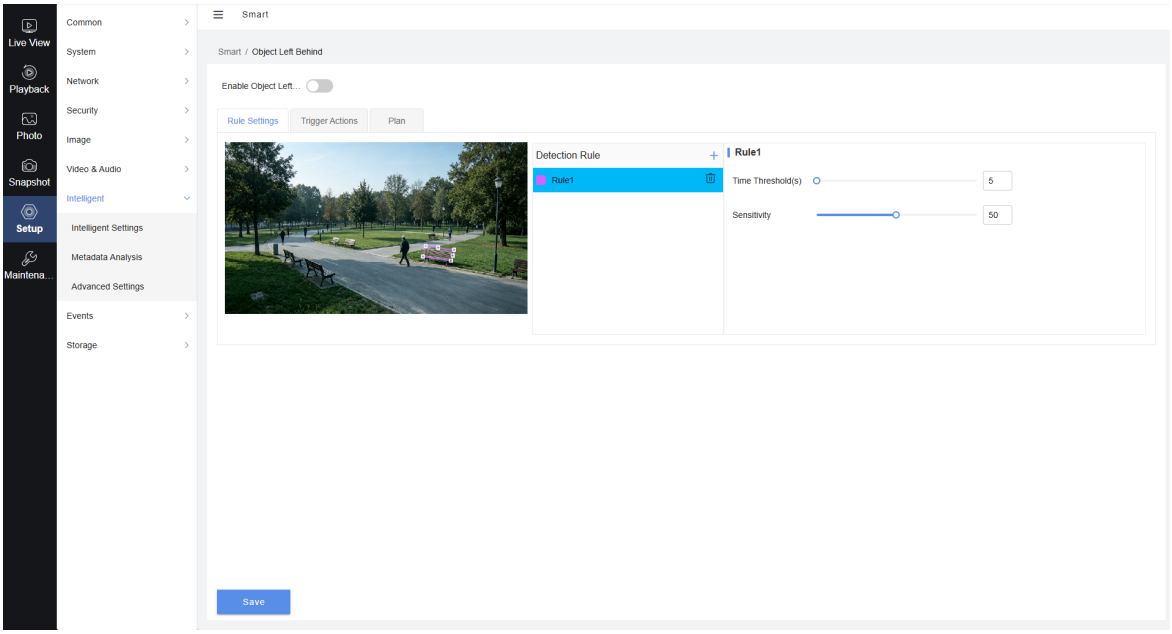
Trigger Action	Description
Conventional	• **Upload to FTP**: After you select the checkbox, snapshots are uploaded to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP • **Send E-mail**: After you select the checkbox, an alarm email is sent when an alarm is triggered. Before using this function, complete the sender and recipient configuration in E-mail
Alarm Output	**A->1**: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered

Trigger Action	Description
Storage	• **Recording Edge Storage**: After you select the checkbox, videos are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **Image Edge Storage**: After you select the checkbox, snapshots are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **FTP Video Storage**: After you select the checkbox, videos are stored to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP

5. (Optional) Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and **Object Removed** detection takes effect only during the arming periods.
6. Click **Save** to complete the configuration.

7.7.1.1.2.2 Object Left Behind

Draw a detection area on the video image. When an object is detected left behind in the area and the duration exceeds the time threshold, alarm linkage is triggered.



1. Find **Object Left Behind** on the **Smart** page and enable it.
2. Click the icon to go to the **Object Left Behind** page.

   Note: If other smart detection functions are already enabled and are mutually exclusive with **Object Left Behind**, a confirmation dialog box is displayed when you enable it. After confirmation, the device automatically disables the conflicting smart functions.

3. On the **Rule Settings** tab, click + to add a detection rule, draw a detection area on the video image, and configure the rule parameters:

Parameter	Description
Detection Area	Draw a polygon detection area on the video image. Drag the vertices to adjust the shape and position of the area.
Time Threshold(s)	Set the time threshold for an object staying in the detection area. An alarm is triggered only after the object is left behind and the duration exceeds this threshold.

Parameter	Description
Sensitivity	Set the detection sensitivity. A larger value indicates higher sensitivity. Higher sensitivity makes alarms easier to trigger but may increase the false alarm rate. Adjust the settings based on the actual scenario to determine the optimal configuration.

Note: Up to 4 detection rules can be added. Each rule corresponds to one detection area, and the time threshold and sensitivity can be configured independently for each rule.

4. (Optional) Configure trigger actions on the **Trigger Actions** tab.

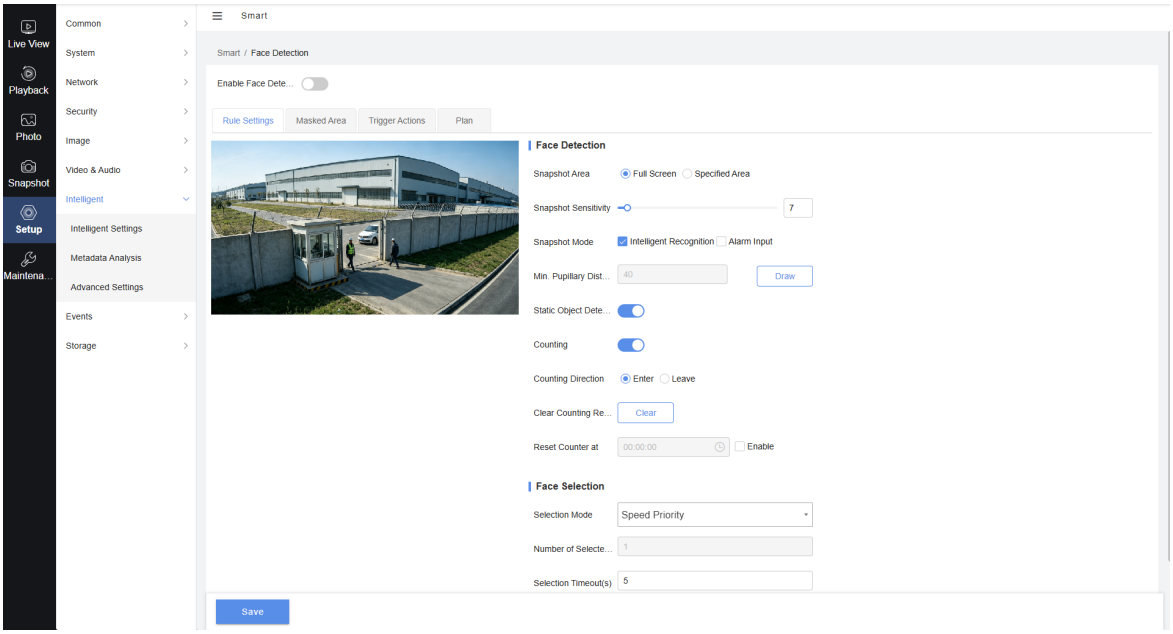
Trigger Action	Description
Conventional	• **Upload to FTP**: After you select the checkbox, snapshots are uploaded to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP • **Send E-mail**: After you select the checkbox, an alarm email is sent when an alarm is triggered. Before using this function, complete the sender and recipient configuration in E-mail
Alarm Output	**A->1**: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered
Storage	• **Recording Edge Storage**: After you select the checkbox, videos are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **Image Edge Storage**: After you select the checkbox, snapshots are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **FTP Video Storage**: After you select the checkbox, videos are stored to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP

5. (Optional) Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and **Object Left Behind** detection takes effect only during the arming periods.
6. Click **Save** to complete the configuration.

7.7.1.1.3 Object Detection

7.7.1.1.3.1 Face Detection

Face detection detects face targets in the video image. When a face is detected, snapshot capture and alarm linkage are triggered.



Before enabling this function, confirm that the device supports face detection. Face Detection is mutually exclusive with some smart functions, and mutual exclusion is automatically checked when it is enabled.

Configure Face Detection

1. Find **Face Detection** on the **Smart** page and enable it.

   Note: If other smart detection functions are already enabled and are mutually exclusive with **Face Detection**, a confirmation dialog box is displayed when you enable it. After confirmation, the device automatically disables the conflicting smart functions.

2. Click the icon to go to the **Face Detection** page.
3. On the **Rule Settings** tab, configure the face detection parameters:

Parameter	Description
Snapshot Area	• **Full Screen**: Detects faces within the full screen of the video image • **Specified Area**: Draw a polygon detection area on the video image, and faces are detected only within the area. Drag the vertices to adjust the shape and position of the area.
Snapshot Sensitivity	Set the detection sensitivity. A larger value indicates higher sensitivity. Higher sensitivity makes alarms easier to trigger but may increase the false alarm rate. Adjust the settings based on the actual scenario to determine the optimal configuration.
Snapshot Mode	• **Intelligent Recognition**: The device's intelligent algorithm automatically captures faces • **Alarm Input**: Face capture is triggered by an external alarm input. Requires the device to support alarm input. Both modes can be selected at the same time.
Min. Pupillary Distance	Set the minimum pupillary distance (in pixels) for a detectable face. The pupillary distance is determined by the device capability set and the current resolution. You can draw a rectangle on the video image to visually adjust the pupillary distance.
Static Object Detection	After it is enabled, stationary face and body targets can be detected. Requires the device to support this function.

Parameter	Description
Counting	After it is enabled, the number of detected faces is counted. The counting direction can be set: • **Enter**: Counts the number of faces entering the detection area • **Leave**: Counts the number of faces leaving the detection area

4. Configure the clear mode:

Parameter	Description
Clear	Click **Clear** to immediately reset the current face counting data to zero.
Reset Counter at	After you select the checkbox to enable it, set the daily automatic reset time. At the specified time, the system automatically resets the count to zero.

5. Configure the face selection parameters:

Parameter	Description
Selection Mode	• **Effect Priority**: Prioritizes selecting the face snapshot with the highest quality • **Speed Priority**: Prioritizes quickly outputting the capture result. The selection timeout can be set • **Periodic Selection**: Outputs the capture result at fixed time intervals. The selection period can be set
Number of Selected Photos	Set the number of selected photos output per capture. Displayed only in Effect Priority or Speed Priority mode.
Selection Timeout	Set the timeout in Speed Priority mode. Displayed only in Speed Priority mode.
Upload Original Image	After it is enabled, in Periodic Selection mode, the device periodically uploads full-view images containing face targets to the backend according to the configured selection period. When it is disabled, only face thumbnails (small images) are uploaded, without the full-view image. Displayed only in Periodic Selection mode.
Filter by Angle	After it is enabled, faces that do not meet the angle requirements are filtered out. The angle thresholds for each direction can be set: • **Roll**: Left and right tilt angle threshold • **Yaw**: Left and right rotation angle threshold • **Pitch**: Up and down tilt angle threshold Faces outside the configured angle range will be filtered out. Requires the device to support angle filtering.

6. On the **Masked Area** tab, manage the masked areas. Face detection is not performed within masked areas.

Operation	Description
Add Area	Click  , draw a polygon masked area on the video image, and drag the vertices to adjust the shape and position of the area.
Delete Area	Select an area and click  to delete the masked area.
Select Area	Click an area in the area list to select it. The corresponding area is highlighted on the video image, and its shape can be edited.

Note: The number of masked areas is limited, depending on the device capabilities. The **Masked Area** tab is displayed only when the device supports this function.

7. (Optional) Configure trigger actions on the **Trigger Actions** tab.

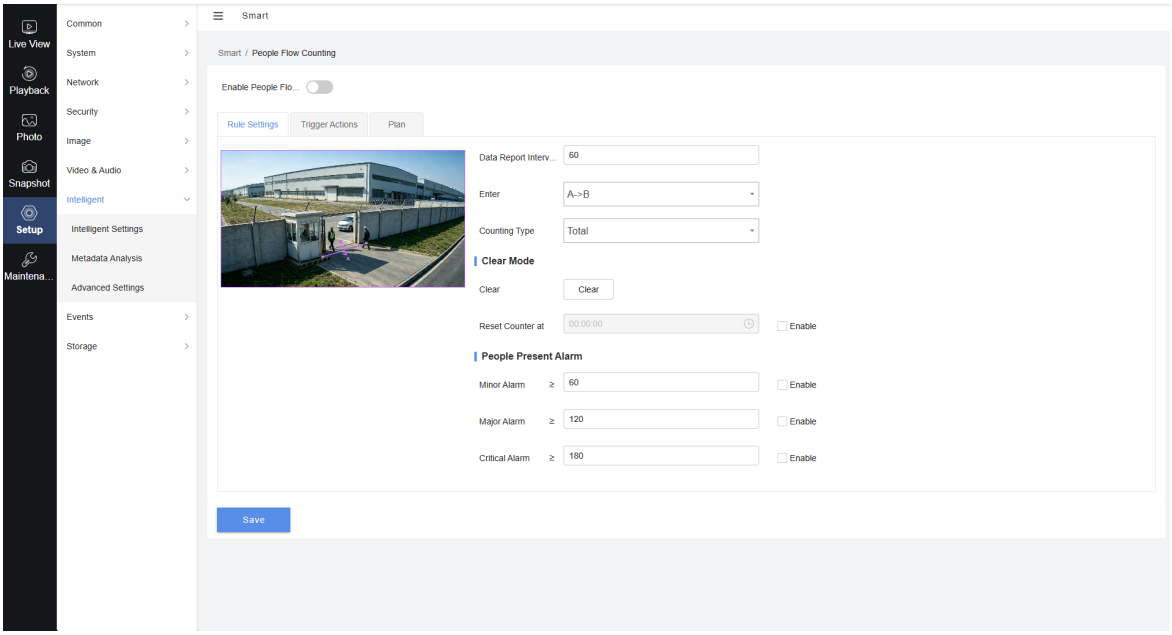
Trigger Action	Description
Conventional	• **Upload Image(Original)**: After you select the checkbox, full-view snapshots are uploaded when an alarm is triggered • **Upload Image(Target)**: After you select the checkbox, face thumbnails are uploaded when an alarm is triggered
Alarm Output	**A->1**: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered

8. (Optional) Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and **Face Detection** takes effect only during the arming periods.
9. Click **Save** to complete the configuration.

7.7.1.1.4 People Counting

7.7.1.1.4.1 People Flow Counting

Draw a detection line on the video image, and counting is performed when people are detected crossing the detection line. If the people present alarm is enabled, alarm linkage is triggered when the number of people present reaches the alarm threshold.



1. Find **People Flow Counting** on the **Smart** page and enable it.
2. Click the icon to go to the **People Flow Counting** page.
3. On the **Rule Settings** tab, draw a detection line on the video image and configure the rule parameters:

Parameter	Description
Data Report Interval(s)	Set the interval at which statistical data is reported.
Enter	Set the direction determined as entering: • B→A: The direction from end B to end A is determined as entering • A→B: The direction from end A to end B is determined as entering
Counting Type	Select the counting method: • Total: Counts the total number of people who entered and exited • People Entered: Counts only the number of people in the entering direction • People Exited: Counts only the number of people in the exiting direction

Parameter	Description
	Note: After the minor alarm is enabled, the counting type cannot be changed.

4. Configure the clear mode:

Parameter	Description
Clear	Click **Clear** to immediately reset the current people flow count to zero.
Reset Counter at	After you select the checkbox to enable it, set the daily automatic reset time. At the specified time, the system automatically resets the count to zero.

5. Configure and enable the people present alarm. The three alarm levels have a cascading linkage relationship, and the thresholds must meet: critical alarm > major alarm > minor alarm.

Parameter	Description
Minor Alarm	Set the minor alarm threshold for the number of people present. A minor alarm is triggered when the number of people present is ≥ this threshold.
Major Alarm	Set the major alarm threshold for the number of people present. It must be greater than the minor alarm threshold. A major alarm is triggered when the number of people present is ≥ this threshold.
Critical Alarm	Set the critical alarm threshold for the number of people present. It must be greater than the major alarm threshold. A critical alarm is triggered when the number of people present is ≥ this threshold.

Note: Cascading rule for the three alarm levels: enabling a higher-level alarm automatically enables the lower-level alarms; disabling a lower-level alarm automatically disables the higher-level alarms. For example, enabling the critical alarm also enables the major and minor alarms, and disabling the minor alarm also disables the major and critical alarms.

6. (Optional) Configure alarm trigger actions on the **Trigger Actions** tab. Each of the three alarm levels has its own trigger action configuration:
   - People Present Minor Alarm trigger actions: trigger actions performed when a minor alarm is triggered
   - People Present Major Alarm trigger actions: trigger actions performed when a major alarm is triggered
   - People Present Critical Alarm trigger actions: trigger actions performed when a critical alarm is triggered

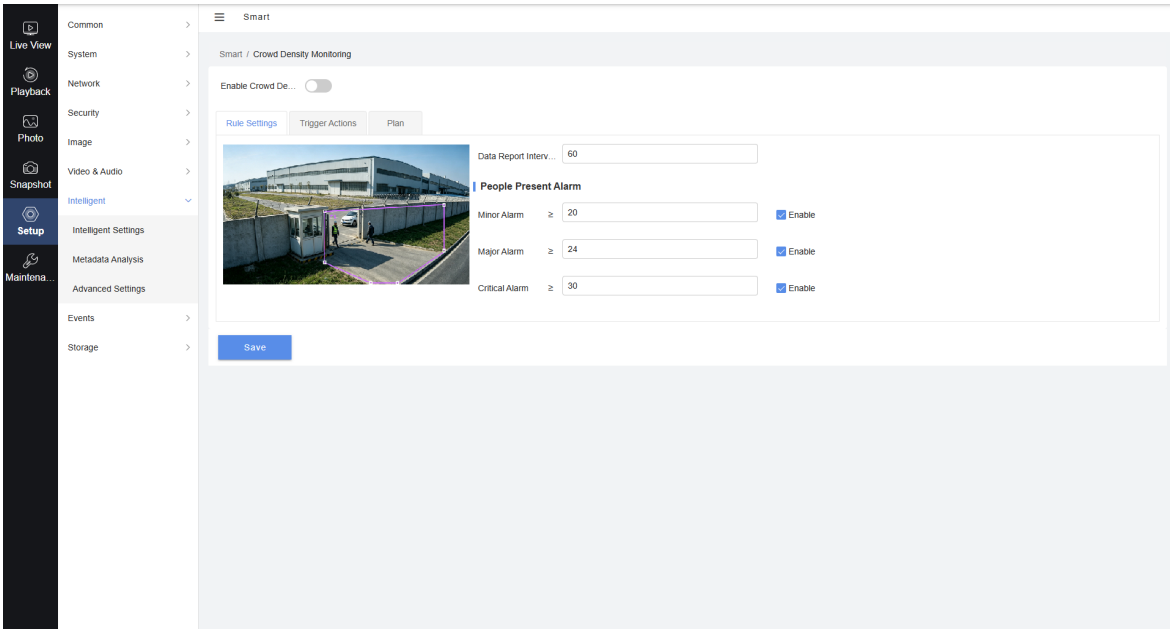
Trigger Action	Description
Alarm Output	• **A->1**: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered • **Alarm Sound**: After you select the checkbox, an audio alarm is activated when an alarm is triggered. The alert tone and the number of alarm repetitions can be configured • **Flashing Light**: After you select the checkbox, the light flashes when an alarm is triggered. The flashing duration can be configured

Note: The **Trigger Actions** tab is displayed only when the device supports alarm sound, light alarm, or alarm output capabilities.

7. (Optional) Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and **People Flow Counting** takes effect only during the arming periods.
8. Click **Save** to complete the configuration.

7.7.1.1.4.2 Crowd Density Monitoring

Draw a detection area on the video image. When the number of people in the area reaches the configured alarm threshold, alarm linkage of the corresponding level is triggered.



1. Find **Crowd Density Monitoring** on the **Smart** page and enable it.
2. Click the icon to go to the **Crowd Density Monitoring** page.
3. On the **Rule Settings** tab, draw a detection area on the video image and configure the data report interval.
4. Configure the people present alarm. The three alarm levels have a cascading linkage relationship, and the thresholds must meet: critical alarm > major alarm > minor alarm.

Parameter	Description
Minor Alarm	Set the minor alarm threshold for the number of people present. A minor alarm is triggered when the number of people in the area is ≥ this threshold. It takes effect after you select the checkbox to enable it, and it is enabled by default.
Major Alarm	Set the major alarm threshold for the number of people present. It must be greater than the minor alarm threshold. A major alarm is triggered when the number of people in the area is ≥ this threshold. It takes effect after you select the checkbox to enable it.
Critical Alarm	Set the critical alarm threshold for the number of people present. It must be greater than the major alarm threshold. A critical alarm is triggered when the number of people in the area is ≥ this threshold. It takes effect after you select the checkbox to enable it, and it is disabled by default.

Note: Cascading rule for the three alarm levels: enabling a higher-level alarm automatically enables the lower-level alarms; disabling a lower-level alarm automatically disables the higher-level alarms. For example, enabling the critical alarm also enables the major and minor alarms, and disabling the minor alarm also disables the major and critical alarms.

5. (Optional) Configure alarm trigger actions on the **Trigger Actions** tab. Each of the three alarm levels has its own trigger action configuration:
   - Crowd Density Minor Alarm trigger actions: trigger actions performed when a minor alarm is triggered
   - Crowd Density Major Alarm trigger actions: trigger actions performed when a major alarm is triggered
   - Crowd Density Critical Alarm trigger actions: trigger actions performed when a critical alarm is triggered

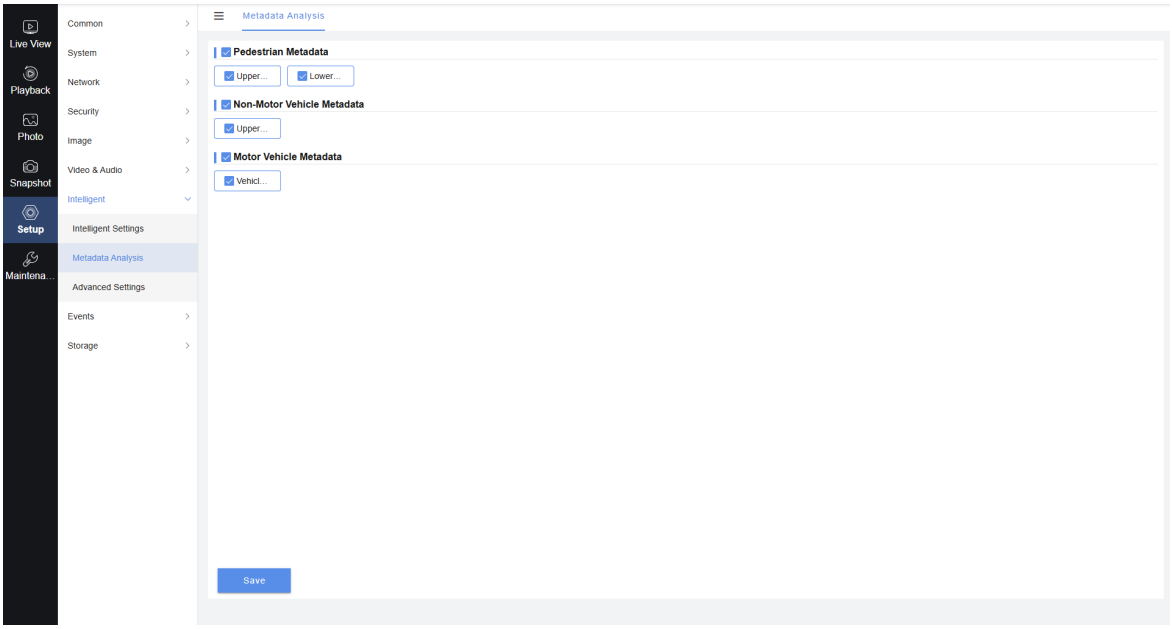
Trigger Action	Description
Conventional	After you select the checkbox, an alarm email is sent when an alarm is triggered. Before using this function, complete the sender and recipient configuration in E-mail.
Alarm Output	• **A->1**: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered • **Alarm Sound**: After you select the checkbox, an audio alarm is activated when an alarm is triggered. The alert tone and the number of alarm repetitions can be configured • **Flashing Light**: After you select the checkbox, the light flashes when an alarm is triggered. The flashing duration can be configured

Note: The Trigger Actions tab is displayed only when the device supports e-mail, alarm output, alarm sound, or light alarm capabilities.

6. (Optional) Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and **Crowd Density Monitoring** takes effect only during the arming periods.
7. Click **Save** to complete the configuration.

7.7.2 Metadata Analysis

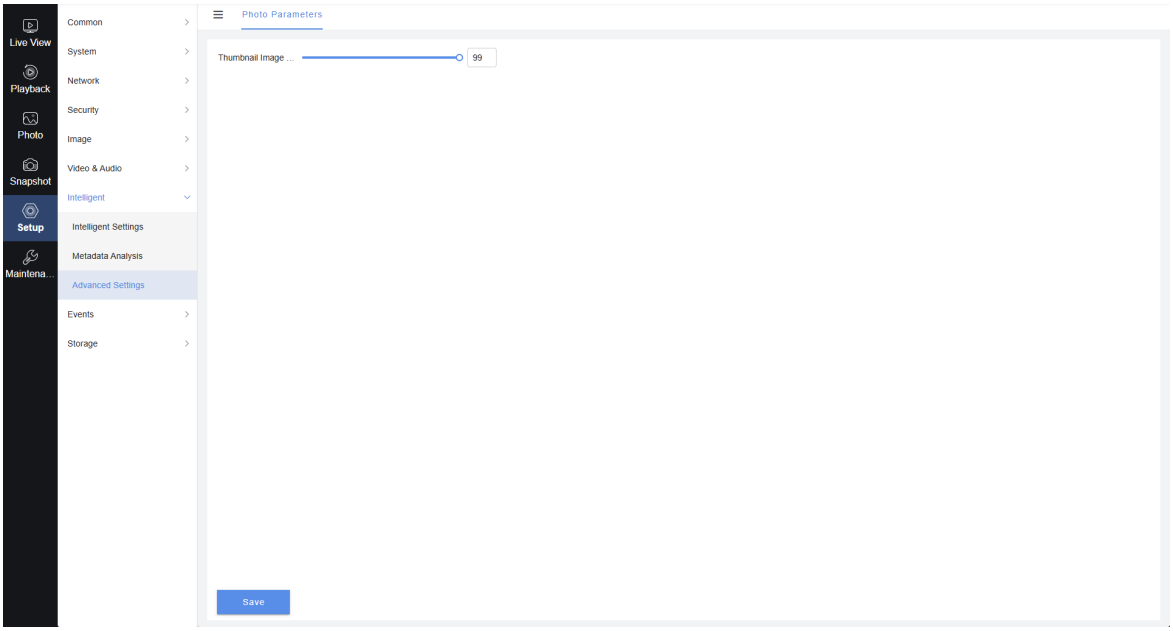
Enable the device's metadata extraction capability for detected objects as needed. After it is selected, the device outputs the corresponding metadata information during smart snapshot capture.



7.7.3 Advanced Parameters

7.7.3.1 Photo Parameters

Configure the output quality of smart snapshot photos. A larger value produces clearer photos.

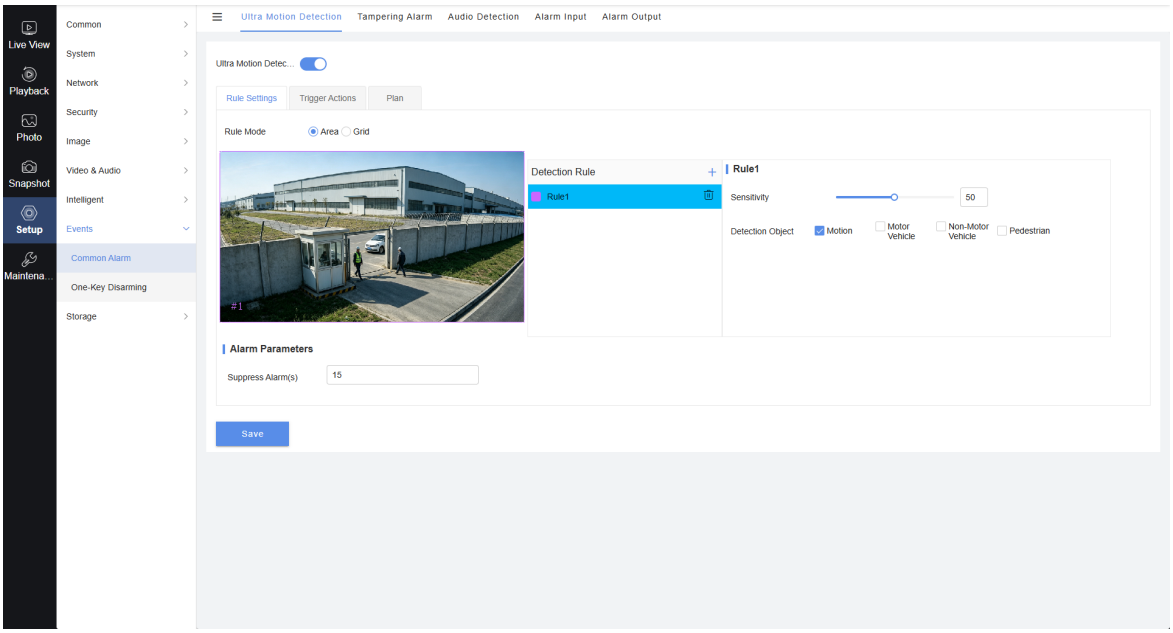


7.8 Events

7.8.1 Common Alarm

7.8.1.1 Ultra Motion Detection

Draw a detection area or grid on the video image. When target activity is detected in the area, alarm linkage is triggered.



Configure Ultra Motion Detection

1. Click to enable Ultra Motion Detection.
2. On the **Rule Settings** tab, select a rule mode:

- **Area**: Draw a detection area on the video image (Ultra Motion Detection mode supports polygon areas, and motion detection mode supports rectangular areas). It is suitable for scenarios where the detection range needs to be precisely defined.
- **Grid**: Select the detection area as a grid on the video image. It is suitable for scenarios where an irregular detection range needs to be quickly defined.

3. Click + to draw a detection area. On the video image, press and hold the left mouse button and drag to draw the first two vertices of the polygon, then release and click in sequence to add the subsequent vertices. At least 3 vertices are required. Click the first vertex or double-click to close the area and form a polygon detection area. Up to 6 vertices are supported.
4. Configure the detection rules:

Parameter	Description
Sensitivity	Set the detection sensitivity. A larger value indicates higher sensitivity. Higher sensitivity makes alarms easier to trigger but may increase the false alarm rate. Adjust the settings based on the actual scenario to determine the optimal configuration.
Detection Object	Select the target types to detect. • **Motor Vehicle**: Detects motor vehicles • **Non-Motor Vehicle**: Detects non-motor vehicles • **Pedestrian**: Detects pedestrians • **Motion**: Detects motion changes in the image Select at least one detection object.

5. Configure the alarm suppression time. Set the minimum interval between two alarms. During the suppression time, alarms will not be repeatedly reported.
6. Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and **Ultra Motion Detection** takes effect only during the arming periods.
7. Configure trigger actions on the **Trigger Actions** tab.

Trigger Action	Description
Conventional	• **Send E-mail**: After you select the checkbox, an alarm email is sent when an alarm is triggered. Before using this function, complete the sender and recipient configuration in E-mail • **Attribute Collection**: After you select the checkbox, target attribute information is collected when an alarm is triggered • **Upload to FTP**: After you select the checkbox, snapshots are uploaded to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP
Alarm Output	• **A->1**: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered • **Alarm Sound**: After you select the checkbox, an audio alarm is activated when an alarm is triggered. The alert tone and the number of alarm repetitions can be configured • **Flashing Light**: After you select the checkbox, the light flashes to raise an alarm when an alarm is triggered. The flashing duration can be configured
Storage	• **Recording Edge Storage**: After you select the checkbox, videos are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **Image Edge Storage**: After you select the checkbox, snapshots are stored to the edge storage device when an alarm is triggered. Before using

Trigger Action	Description
	this function, complete the storage resource configuration in Storage Management • **FTP Video Storage**: After you select the checkbox, videos are stored to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP

8. Click **Save** to complete the configuration.

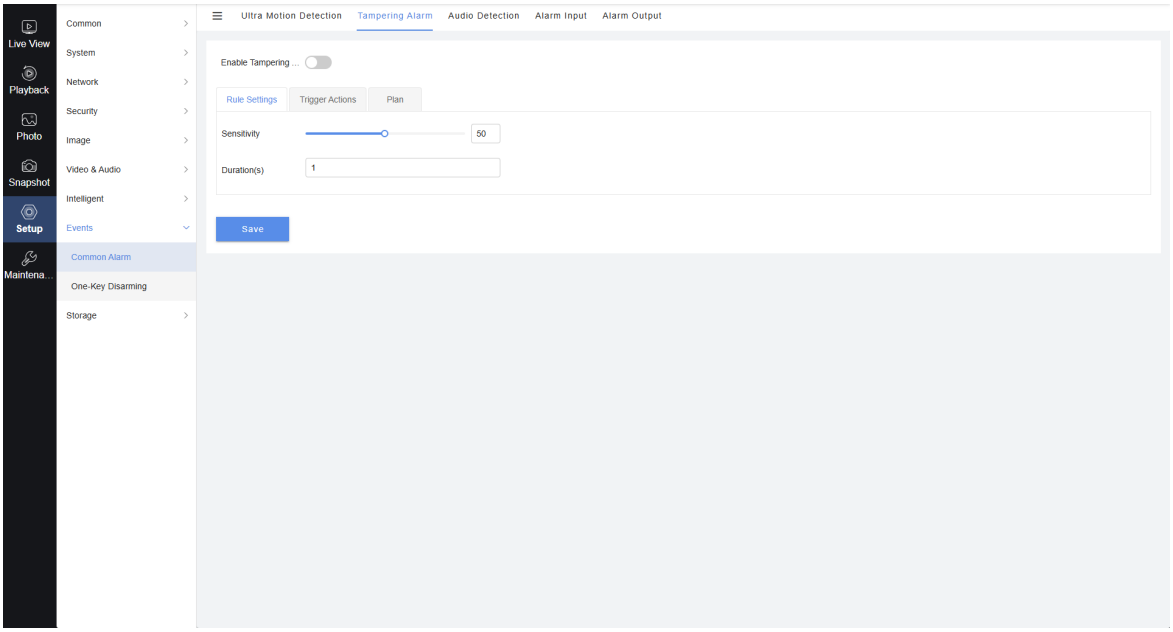
Note: When Ultra Motion Detection is enabled, the system performs a mutual exclusion check. Ultra Motion Detection may be mutually exclusive with other smart functions.

Manage Detection Rules

Operation	Description
Select Area	Click the target area in the detection rule list. The area is highlighted on the image, and its parameter configuration is displayed accordingly.
Delete Area	Click in the detection rule list to delete the corresponding detection area.
Draw Grid	In Grid mode, click or drag on the video image to select the grids to detect.

7.8.1.2 Tampering Alarm

After Tampering Alarm is enabled, alarm linkage is triggered when the lens is blocked and the duration reaches the specified time. The detection results can be viewed in event search and channel alarms.



1. Click to enable Tampering Alarm.
2. On the **Rule Settings** tab, configure the detection parameters:

Parameter	Description
Sensitivity	Set the detection sensitivity. A larger value indicates higher sensitivity. Higher sensitivity makes alarms easier to trigger but may increase the false alarm rate. Adjust the settings based on the actual scenario to determine the optimal configuration.
Duration (s)	Set how long the blockage must last before an alarm is triggered.

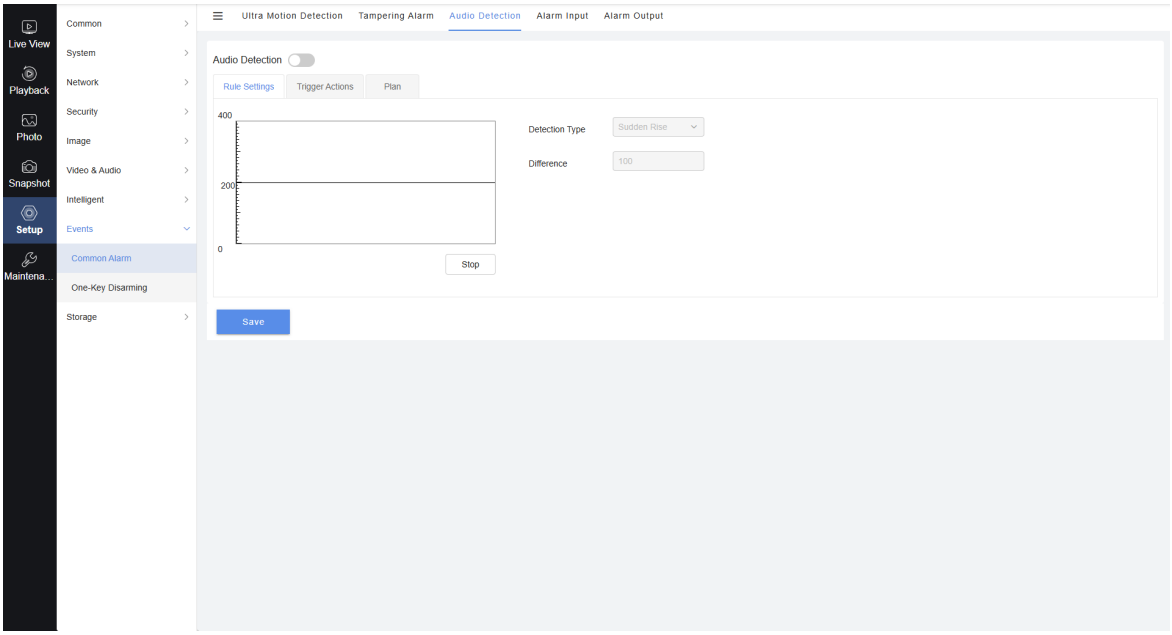
3. Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and Tampering Alarm takes effect only during the arming periods.
4. Configure trigger actions on the **Trigger Actions** tab.

Trigger Action	Description
Conventional	• **Send E-mail**: After you select the checkbox, an alarm email is sent when an alarm is triggered. Before using this function, complete the sender and recipient configuration in E-mail • **Upload to FTP**: After you select the checkbox, snapshots are uploaded to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP
Alarm Output	A->1: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered
Storage	• **Recording Edge Storage**: After you select the checkbox, videos are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **Image Edge Storage**: After you select the checkbox, snapshots are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **FTP Video Storage**: After you select the checkbox, videos are stored to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP

5. Click **Save** to complete the configuration.

7.8.1.3 Audio Detection

After Audio Detection is enabled, alarm linkage is triggered when the sound volume captured by the device meets the configured detection conditions.



1. Click to enable Audio Detection.
2. On the **Rule Settings** tab, configure the detection parameters:

Parameter	Description
Detection Type	Select the trigger method of audio detection: • **Sudden Rise**: An alarm is triggered when the volume suddenly increases and exceeds the configured difference. • **Sudden Fall**: An alarm is triggered when the volume suddenly decreases and exceeds the configured difference.

Parameter	Description
	• **Sudden Change**: An alarm is triggered when the volume changes suddenly and the change exceeds the configured difference. • **Threshold**: An alarm is triggered when the volume exceeds the configured threshold.
Difference	Displayed when the detection type is Sudden Rise, Sudden Fall, or Sudden Change. Set the volume change difference. An alarm is triggered when the volume change exceeds this difference.
Threshold	Displayed when the detection type is Threshold. Set the volume threshold. An alarm is triggered when the volume exceeds this threshold.

Note: The left side of the Rule Settings tab is the real-time sound waveform visualization area, which displays the current volume in a bar chart. Red indicates abnormal volume, and gray indicates normal volume. You can drag the threshold line to adjust the reference value, and click the **Start**/**Pause** buttons to control waveform capture.

3. Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and **Audio Detection** takes effect only during the arming periods.
4. Configure trigger actions on the **Trigger Actions** tab.

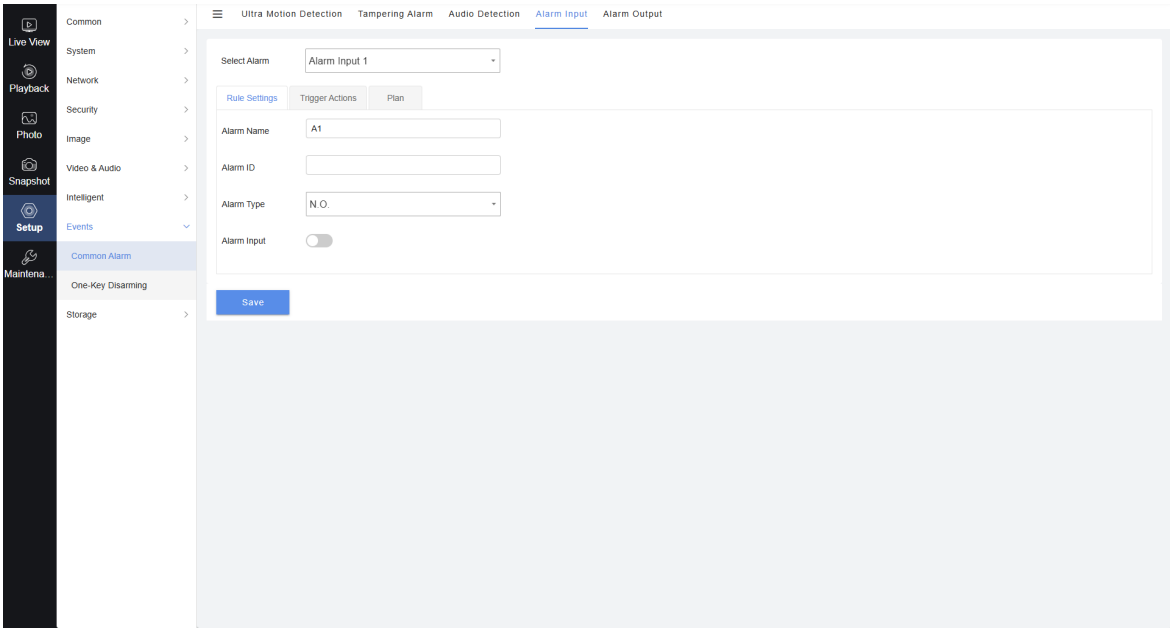
   Note: The **Trigger Actions** tab is displayed only when the device supports linkage output.

Trigger Action	Description
Conventional	• **Send E-mail**: After you select the checkbox, an alarm email is sent when an alarm is triggered. Before using this function, complete the sender and recipient configuration in E-mail. • **Upload to FTP**: After you select the checkbox, snapshots are uploaded to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP.
Alarm Output	A->1: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered
Storage	• **Recording Edge Storage**: After you select the checkbox, videos are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **Image Edge Storage**: After you select the checkbox, snapshots are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **FTP Video Storage**: After you select the checkbox, videos are stored to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP

5. Click **Save** to complete the configuration.

7.8.1.4 Alarm Input

Configure the basic parameters and alarm type of the alarm input channel. When an alarm input signal is triggered, trigger actions are performed.



1. Select the alarm input channel to configure from the **Select Alarm** dropdown list.
2. On the **Rule Settings** tab, configure the alarm input parameters:

Parameter	Description
Alarm Name	Enter the name of the alarm input channel.
Alarm ID	Enter the ID of the alarm input channel.
Alarm Type	• **N.O.**: The alarm input port is open (open circuit) under normal conditions, and an alarm is triggered when the port is closed. • **N.C.**: The alarm input port is closed (short circuit) under normal conditions, and an alarm is triggered when the port is open.
Alarm Input	Enable or disable the detection function of this alarm input channel.

3. Configure the periods during which detection takes effect on the **Plan** tab. The periods are divided by day of week (Monday through Sunday), and **Alarm Input** detection takes effect only during the arming periods.
4. Configure trigger actions on the **Trigger Actions** tab.

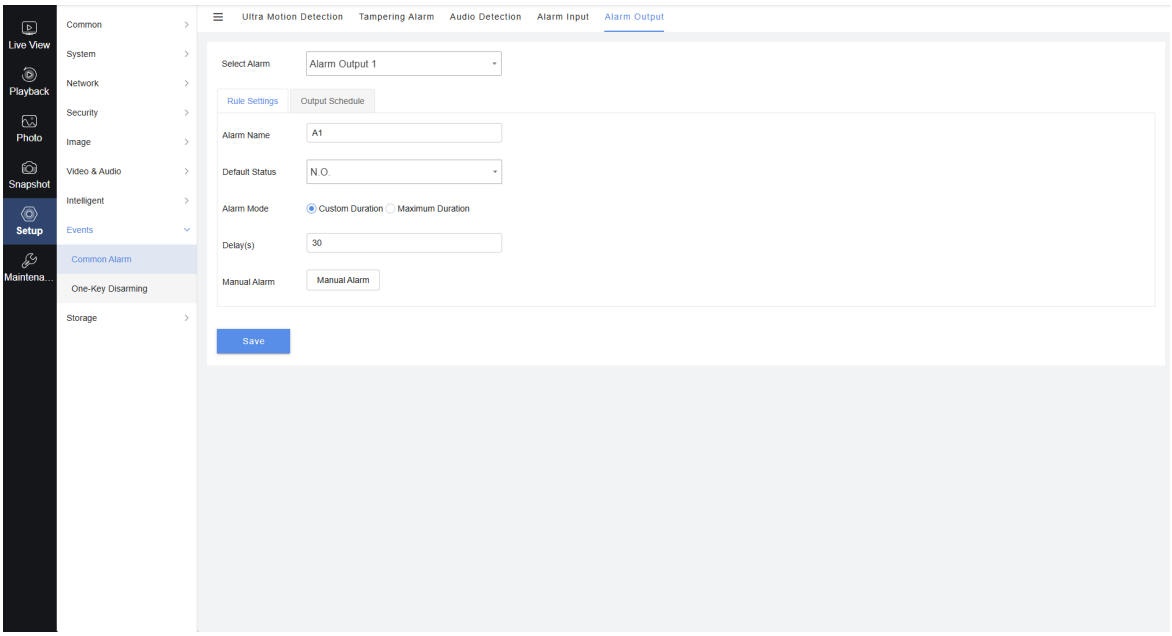
Trigger Action	Description
Conventional	• **Send E-mail**: After you select the checkbox, an alarm email is sent when an alarm is triggered. Before using this function, complete the sender and recipient configuration in E-mail • **Upload to FTP**: After you select the checkbox, snapshots are uploaded to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP
Alarm Output	A->1: After you select the checkbox, alarm output channel 1 is activated when an alarm is triggered
Storage	• **Recording Edge Storage**: After you select the checkbox, videos are stored to the edge storage device when an alarm is triggered. Before using this function, complete the storage resource configuration in Storage Management • **Image Edge Storage**: After you select the checkbox, snapshots are stored to the edge storage device when an alarm is triggered. Before using

Trigger Action	Description
	this function, complete the storage resource configuration in Storage Management • **FTP Video Storage**: After you select the checkbox, videos are stored to the FTP server when an alarm is triggered. Before using this function, complete the FTP server configuration in FTP

5. Click **Save** to complete the configuration.

7.8.1.5 Alarm Output

Alarm output serves as a trigger action and takes effect when other detection functions trigger alarm output.



1. Select the alarm output channel to configure from the **Select Alarm** dropdown list. Only when the device supports multiple alarm outputs can you select Alarm Output 1 or Alarm Output 2.
2. On the **Rule Settings** tab, configure the alarm output parameters:

Parameter	Description
Alarm Name	Enter the name of the alarm output channel.
Default Status	• **N.O.**: The relay is open under normal conditions and closed when an alarm occurs • **N.C.**: The relay is closed under normal conditions and open when an alarm occurs
Alarm Mode	• **Custom Duration**: The alarm output automatically clears after the specified duration • **Maximum Duration**: The alarm output continues until it is manually cleared
Duration	Set the duration of the alarm output. It can be configured only in Custom Duration mode.
Manual Alarm	Manually trigger the alarm output or clear the current alarm. The button text is displayed dynamically based on the current alarm status: **Manual Alarm** is displayed when no alarm is present, and **Clear Alarm** is displayed during an alarm.

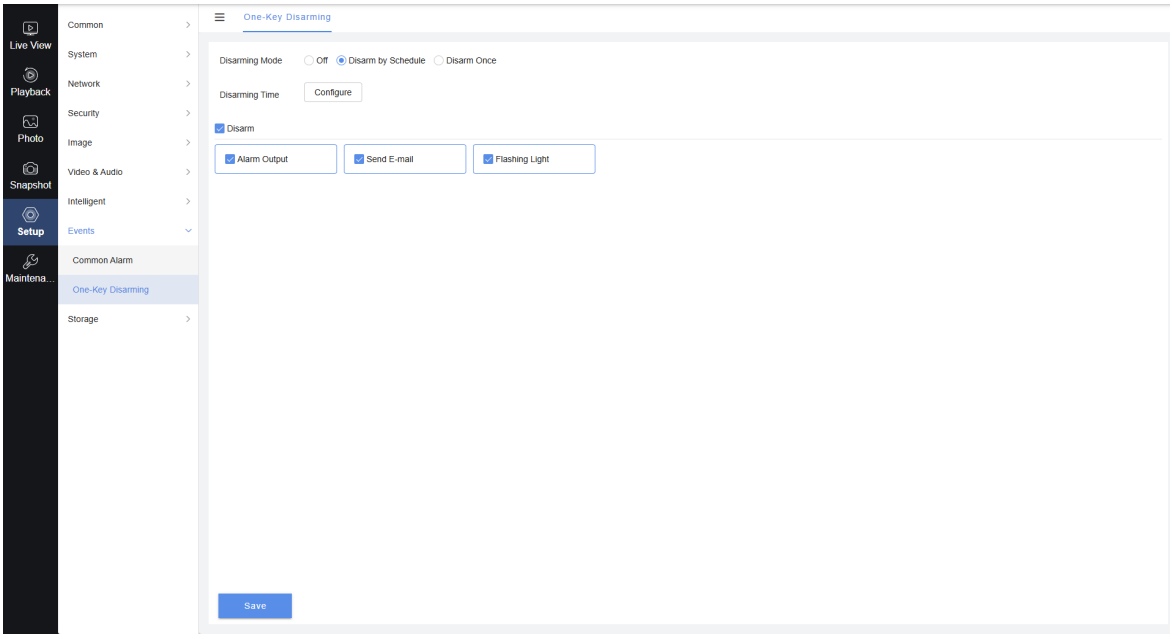
3. Configure the periods during which alarm output takes effect on the **Output Schedule** tab. The periods are divided by day of week (Monday through Sunday), and **Alarm Output** takes effect only during the arming periods.
4. Click **Save** to complete the configuration.

7.8.2 One-Key Disarming

The one-key disarming function allows you to block alarm services and smart service trigger action rules during a specified time period, preventing unnecessary alarm notifications and ensuring quiet system operation during maintenance or special periods.

Note:

- The availability of disarming action items depends on device capability. Unavailable action items are not displayed.
- When selecting **Disarm by Schedule** or **Disarm Once** mode, at least one disarming action item must be selected. Otherwise, the disarming does not take effect.



Do Not Disarm

In Off mode, the device responds to all alarm services and trigger action rules normally without any blocking.

1. Select the disarming mode as **Off**.
2. Click **Save** to complete the configuration.

Disarm by Schedule

In Disarm by Schedule mode, the device automatically performs disarming according to the configured weekly schedule. This mode is suitable for recurring disarming requirements.

1. Select the disarming mode as **Disarm by Schedule**.
2. Configure the disarming time. Click **Settings**, and in the displayed schedule template, set the daily disarming time periods.

Parameter	Description
Day	Select the days for which to set disarming time periods. Monday to Sunday are supported.
Time Period	Set the start and end time of daily disarming. Up to 4 time periods can be configured per day.

3. Select the required disarming action items.

Parameter	Description
Alarm Output	Block the alarm output trigger action. The device does not perform the alarm output action when an alarm is triggered.

Parameter	Description
Send E-mail	Block the Send E-mail trigger action. The device does not send alarm emails when an alarm is triggered.
Flashing Light	Block the flashing light trigger action. The device does not perform the flashing light action when an alarm is triggered.

4. Click **Save** to complete the configuration.

Disarm Once

In Disarm Once mode, the device performs disarming within the specified start and end time range. After the period expires, the device automatically returns to the normal alarm state. This mode is suitable for temporary disarming requirements.

1. Select the disarming mode as **Disarm Once**.
2. Configure the disarming time. Set the start and end date and time for disarming.

Parameter	Description
Start Time	Set the start date and time for disarming.
End Time	Set the end date and time for disarming. After the period expires, the device automatically returns to the normal alarm state.

3. Select the required disarming action items.

Parameter	Description
Alarm Output	Block the alarm output trigger action. The device does not perform the alarm output action when an alarm is triggered.
Send E-mail	Block the Send E-mail trigger action. The device does not send alarm emails when an alarm is triggered.
Flashing Light	Block the flashing light trigger action. The device does not perform the flashing light action when an alarm is triggered.

4. Click **Save** to complete the configuration.

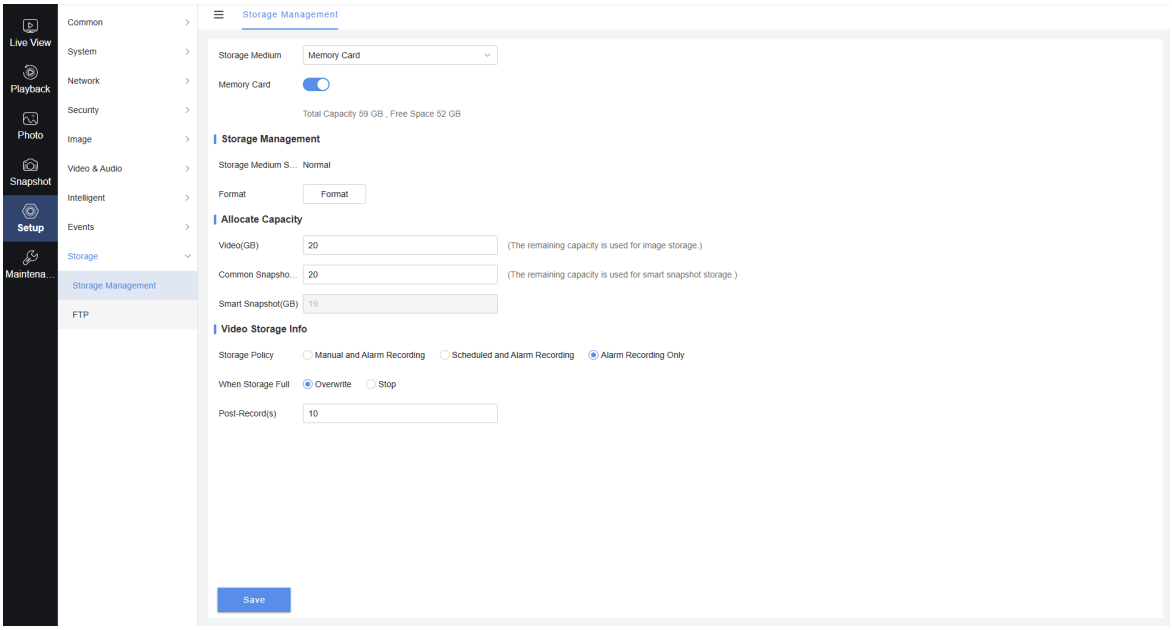
7.9 Storage

7.9.1 Storage Management

Through the Storage Management function, configure the storage medium and storage policy of the device. It supports two storage medium types: memory card and NAS, enabling local storage and capacity allocation for data such as videos and snapshots.

Note:

- If the memory card is abnormal, an error message is displayed on the interface. Format the memory card.
- In NAS mode, if the server address or path is not configured, the configuration items for capacity allocation and storage policy are grayed out and unavailable.
- The device will restart after the memory card is formatted. Confirm that no recording tasks are in progress before formatting.



Memory Card

Select the memory card as the storage medium to store data such as videos and snapshots on the device's SD card.

1. Select **Storage Medium** as **Memory Card**.
2. Click  to enable the memory card function.
3. (Optional) Click **Format** to format the memory card. The device will restart automatically after formatting.
4. Configure capacity allocation parameters.

Parameter	Description
Video	Displays the total capacity available for video storage.
Common Snapshot	Sets the capacity allocated for common snapshot storage.
Smart Snapshot	Automatically calculated by subtracting the video capacity and common snapshot capacity from the total capacity. The remaining capacity is used for smart snapshot storage.

5. Configure video storage parameters.

Parameter	Description
Storage Policy	Select a recording storage policy. Options: • **Manual and Alarm Recording**: Manually start and stop recording, and record alarm videos simultaneously. • **Scheduled and Alarm Recording**: Automatically record according to the storage schedule, and record alarm videos simultaneously. • **Alarm Recording Only**: Only save recordings triggered by alarms.
Stream	Select the stream type for recording storage. Options: **Main Stream** or **Sub Stream**. Manual recording and scheduled recording can be configured with different stream types.
When Storage Full	Select the action when the storage space is full. Options: **Overwrite** (cyclically overwrite the earliest recordings) or **Stop Recording** (stop writing).
Post-Record(s)	Set the duration to continue recording after an alarm event ends.

6. (Optional) When the storage policy is set to **Scheduled and Alarm Recording**, configure the arming schedule in the storage schedule area.
7. Click **Save** to complete the configuration.

NAS

Select NAS as the storage medium to store data such as videos and snapshots on a network storage server.

1. Select **Storage Medium** as **NAS**.
2. Configure NAS server connection parameters.

Parameter	Description
Server Address	Enter the IP address or domain name of the NAS server.
Path	Enter the storage path on the NAS server.

3. (Optional) Click **NAS Test** to test the connectivity with the NAS server.
4. After confirming that the NAS connection is successful, check the storage medium status, total capacity, and remaining capacity.
5. Configure capacity allocation parameters.

Parameter	Description
Video	Displays the total capacity available for video storage.
Common Snapshot	Sets the capacity allocated for common snapshot storage.
Smart Snapshot	Automatically calculated by subtracting the video capacity and common snapshot capacity from the total capacity. The remaining capacity is used for smart snapshot storage.

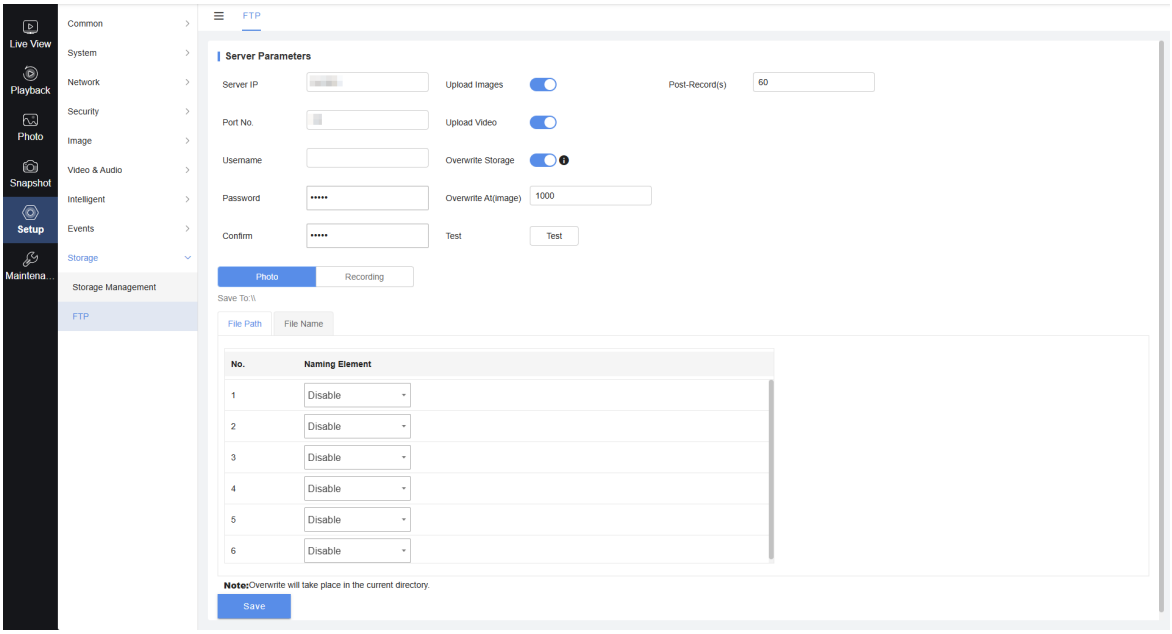
6. Configure video storage parameters.

Parameter	Description
Storage Policy	Select a recording storage policy. Options: • **Manual and Alarm Recording**: Manually start and stop recording, and record alarm videos simultaneously. • **Scheduled and Alarm Recording**: Automatically record according to the storage schedule, and record alarm videos simultaneously. • **Alarm Recording Only**: Only save recordings triggered by alarms.
Stream	Select the stream type for recording storage. Options: **Main Stream** or **Sub Stream**. Manual recording and scheduled recording can be configured with different stream types.
When Storage Full	Select the action when the storage space is full. Options: **Overwrite** (cyclically overwrite the earliest recordings) or **Stop Recording** (stop writing).
Post-Record(s)	Set the duration to continue recording after an alarm event ends.

7. Click **Save** to complete the configuration.

7.9.2 FTP

By configuring the FTP upload function, the device can upload captured images and recordings to a remote server via FTP, enabling remote storage and centralized management of data.



Note: After overwrite is enabled, the last naming element of the file name must be "Image Serial Number"; otherwise, the configuration cannot be saved.

1. Configure server parameters.

Parameter	Description
Server IP	IP address or domain name of the FTP server.
Port	Port number of the FTP server.
Username	Username for logging in to the FTP server.
Password	Password for logging in to the FTP server.
Confirm Password	Enter the password again. It must be consistent with the password.

2. Click to enable the image upload function; click to enable the recording upload function. Both can be enabled simultaneously.

3. (Optional) Click to enable the overwrite function, and configure the overwrite threshold.

Parameter	Description
Overwrite	After it is enabled, when the number of stored images reaches the overwrite threshold, the earliest files are automatically overwritten. Overwrite is performed in the current directory.
Overwrite Threshold (Images)	The image quantity threshold that triggers overwrite.

4. (Optional) Configure the post-record duration, that is, the duration to continue recording after an alarm occurs.

5. Configure the file path and file name.

Parameter	Description
File Path	Configure the storage path rule for uploaded files, which consists of multiple path naming elements.
File Name	Configure the naming rule for uploaded files, which consists of multiple naming elements.
Separator	The separator between naming elements in the file name.

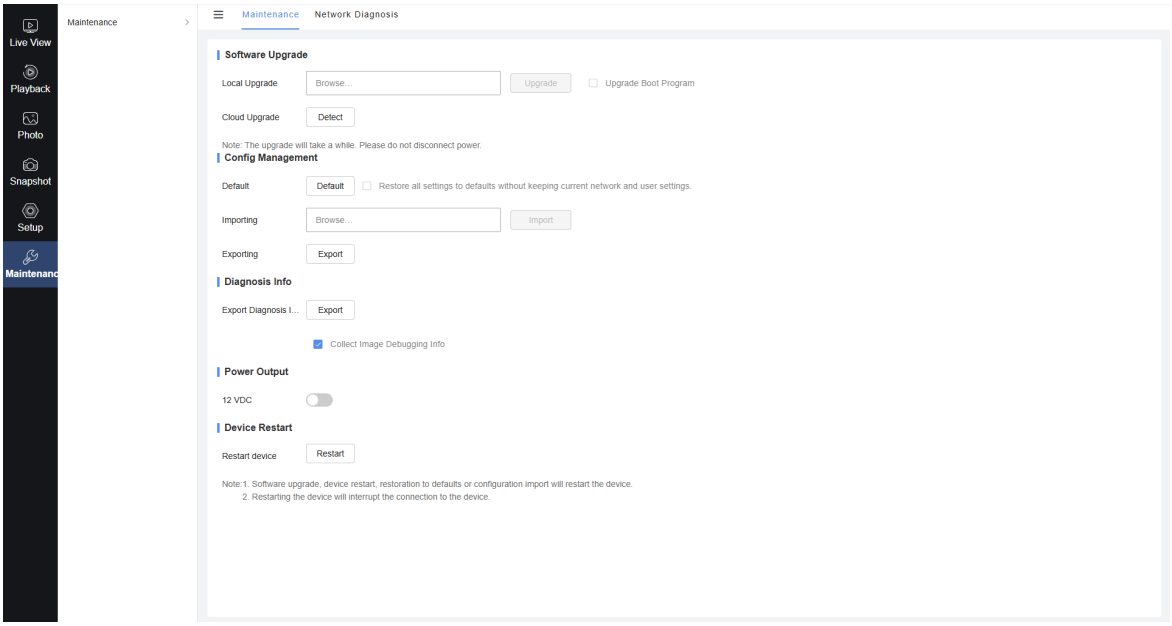
6. (Optional) Click **Test** to test the connectivity with the FTP server.
7. Click **Save** to complete the configuration.

8 Maintenance

8.1 Maintenance

8.1.1 Maintenance

The **Maintenance** page provides device maintenance functions such as software upgrade, config management, diagnosis info export, power output, and device restart, helping users perform daily maintenance and management operations on the device.



Software Upgrade

Software Upgrade provides local upgrade and cloud upgrade methods for updating the device firmware version.

Note: The upgrade takes a long time. Do not turn off the power.

1. Click the box after the local upgrade field and select a local upgrade file (supports .zip, .cst, and .patch formats).
2. Click **Upgrade** and confirm. The device starts upgrading.
   The device will automatically restart during the upgrade. After the upgrade is complete, you need to log in to the device again.

The cloud upgrade steps are as follows:

1. Click **Detect**. The system automatically checks for a new version.
2. After a new version is detected, click **Cloud Upgrade** and confirm. The device starts upgrading.

Config Management

Config Management provides the Default, Import, and Export functions for managing device configuration information.

1. Restore default configuration. Click **Default**. To fully restore factory settings, select **Do not retain network and user configurations. Fully restore to factory settings**.
   After confirmation, the device will restore the default configuration and automatically restart.

2. Import configuration. Click the box after the import configuration field, select a configuration file, and click **Import**. In the **File Decryption** dialog box that appears, enter and confirm the password. After the verification is passed, the configuration file is imported to the device.
   The device will automatically restart after the configuration is imported.
3. Export configuration. Click **Export**. In the file encryption dialog box that appears, enter and confirm the password. After the verification is passed, the configuration file is automatically downloaded to the local device.

Diagnosis Info

Diagnosis Info provides the functions of collecting image debug info and exporting diagnosis info for device troubleshooting.

1. To collect image debug info, select **Collect Image Debug Info**.
2. To export diagnosis info, click **Export**. The device will package the diagnosis info and automatically download it to the local device.

Power Output

Power Output is used to control the DC12V power output switch of the device.

1. Click to enable the DC12V power output function.

Device Restart

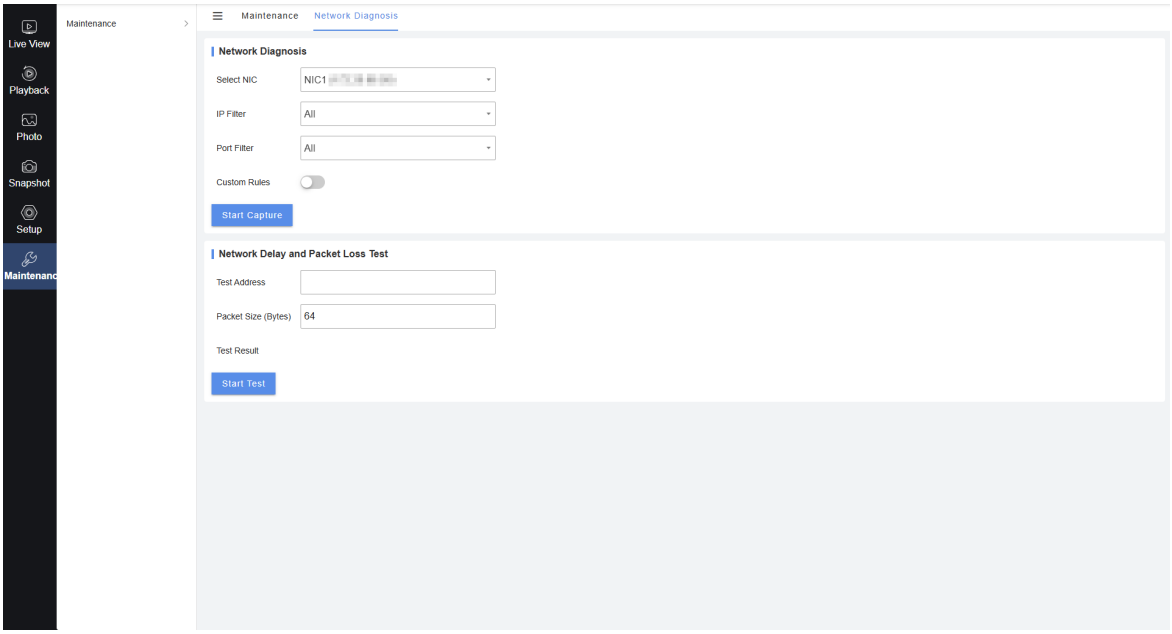
Click **Restart** and confirm. The device restarts immediately.

(Optional) After auto restart is enabled, the device can be automatically restarted at a configured time. The configuration steps are as follows:

1. Click to enable auto restart.
2. Select a restart mode:
   - **Each Day**: The device automatically restarts at the configured time every day.
   - **Every Monday through Sunday**: The device automatically restarts at the configured time on the specified day of the week.
3. Set the restart time.
4. Click **Confirm** to save the configuration.

8.1.2 Network Diagnosis

The **Network Diagnosis** page provides packet capture, network delay, and packet loss test functions to help troubleshoot network communication issues.



Network Diagnosis

Note: Configuration parameters cannot be modified while packet capture is in progress.

1. In the network diagnosis area, select a NIC and configure filter parameters.

Parameter	Description
Select NIC	Select a NIC for packet capture, including: • **All NICs**: Capture packets on all NICs. • **NIC N (IP)**: Capture packets on the specified NIC only, displayed as the NIC number and corresponding IP address.
IP Filter	Select an IP filter mode, including: • **All**: No IP filtering is applied. Packets of all IP addresses are captured. • **Specify**: Capture packets of the specified IP address only. • **Filter**: Filter out packets of the specified IP address.
IP Address	Displayed when IP Filter is set to Specify or Filter. Enter the IP address for filtering.
Port Filter	Select a port filter mode, including: • **All**: No port filtering is applied. Packets of all ports are captured. • **Specify**: Capture packets of the specified port only. • **Filter**: Filter out packets of the specified port.
Port	Displayed when Port Filter is set to Specify or Filter. Enter the port number for filtering.
Custom Rules	Click to enable the custom rules function. After it is enabled, IP Filter and Port Filter are automatically reset to All and disabled. You need to enter a filter rule that complies with the pcap filter syntax in the text box.

2. Click **Start Capture**. The device starts capturing packets.
3. After packet capture is complete, click **Stop Capture**. The device generates a .pcap file and automatically downloads it to the local device.

Network Delay and Packet Loss Test

1. In the network delay and packet loss test area, configure the following parameters.

Parameter	Description
Test Address	Enter the IP address or domain name of the test target.
Packet Size (Bytes)	Enter the size of the test packet.

2. Click **Start Test**. The device starts performing the Ping test.
3. After the test is complete, view the results in the test result area.
   - Test succeeded: The average delay and packet loss rate are displayed.
   - Destination unreachable: "The destination is unreachable." is displayed.

Appendix: Initiative for the Proper Use of Video Products

Thank you for choosing our products.

As technology advances, its applications have a profound impact on every aspect of our lives. As a high-tech company, we have an increasingly deep understanding of the contributions of technology in enhancing efficiency and improving the quality of life. At the same time, we are also aware that the misuse of technology can cause harm. For instance, video surveillance products, due to their ability to record real, complete, and clear images, have significant value in tracing and reconstructing facts. However, improper dissemination, use, and processing of image records can also lead to issues that infringe upon the legitimate rights and interests of others. To continuously promote technology for good, we advocate that every user should use technology and video products responsibly. This includes not only adhering to legal and regulatory requirements but also following the constraints of moral customs, to jointly establish and maintain a positive social environment and atmosphere.

Please read the following proposals carefully:

- Everyone has a reasonable expectation of privacy, and the installation of video products should not violate the reasonable privacy expectations of an individual. When installing video surveillance products in public places, it should be done in a reasonable and effective manner with clear indications of the surveillance area. When installing video products in non-public places, one should not infringe upon the rights and interests of others, including but not limited to not installing video surveillance products without the consent of the stakeholders, or installing highly covert video surveillance products.
- During the use of video products, real activities within specific time and space frames will be recorded under certain conditions. Users should reasonably define the rights they have within that specific range to avoid infringing upon the portrait, privacy, or other legal rights of others.
- During the use of video products, a continuous stream of video image data originating from real-life scenes, including a large amount of biometric data (such as facial data), will be generated. This data can be applied or further processed for various purposes. The video products themselves are not capable of distinguishing between good and bad uses of data. The outcomes of data usage depend on the actions of the data controllers, their intentions, and purposes. Data controllers should adhere to legal requirements and norms, as well as respect international conventions, local customs, societal ethics, public order, and moral standards - all non-mandatory regulations. It is essential for data controllers to respect individuals' privacy, likeness, and other rights during data usage.
- Considering the ongoing generation of video image data by video products, which carries the rights protection requirements, value claims, or other demands of various stakeholders, it is crucial to ensure the security of the product and its data. Users of the product and data controllers should take reasonable and necessary measures to ensure network and data security, to prevent data leaks or improper use. This includes, but is not limited to, carefully allocating the use and management permissions of the product, and establishing and continuously optimizing the security systems of various networks, such as the Internet and local area networks, that the product connects to, in conjunction with the product's usage scenarios.
- Video products have made significant contributions to enhancing societal security, and we believe these products will continue to play a positive role in more aspects of social life. Any use of these products to infringe upon human rights or engage in illegal activities is contrary to the original intent of technological innovation and product development. Therefore, we encourage every user to establish an assessment and tracking mechanism to ensure that the product is used properly, reasonably, and in good faith.