Entrance & Exit Bullet LPC

User Manual

V1.00

Contents

About This Manual

This manual describes the features and operations of entrance & exit bullet LPC.

Copyright Statement

Applicable Models

This manual is applicable to the following models:

- PKC5601-C4Z-LED44-WH
- PKC5601-C4Z-LED44-IR
- PKC2841-Z28-WH
- PKC2841-Z28-IR

Disclaimer

Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

This manual is for reference only, and all statements, information, and recommendations in this manual are presented without warranty of any kind. The figures, tables, or images in this manual are for reference only and may vary depending on the model.

The symbols in the following table may be found in this manual. Carefully follow the instructions indicated by the symbols to avoid hazardous situations and use the product properly.

Symbo	Description
	NOTE! Indicates useful or supplemental information about the use of product.
	CAUTION! Indicates a situation which, if not avoided, could result in damage, data loss or malfunction to product.
	WARNING! Indicates a hazardous situation which, if not avoided, could result in bodily injury or death.

1 Defaults

Username: admin	Password: 123456
Static IP address: 192.168.1.13	Subnet mask: 255.255.255.0

Note: DHCP (Dynamic Host Configuration Protocol) is enabled by default. If a DHCP server is deployed in the network, the device may be assigned an IP address, and you need to use the assigned IP address to log in.

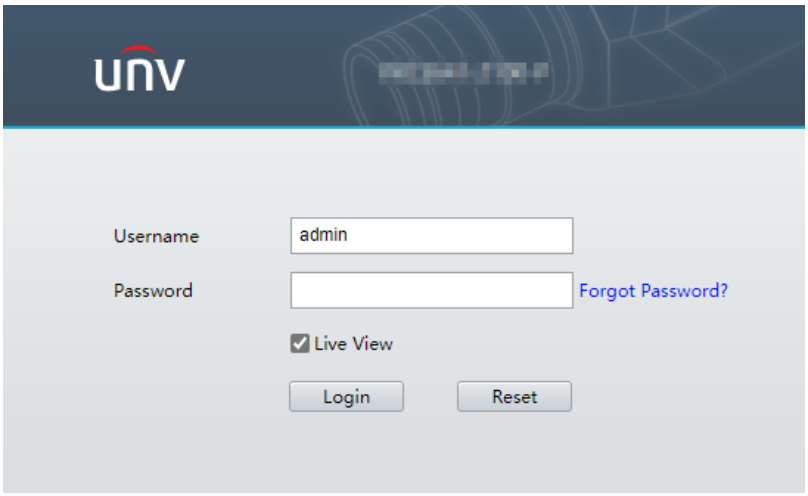
2 Login

Check Before Login

- The device runs normally.
- The client computer (hereinafter referred to as "client") is on the same network segment as the device and is connected to the network.

Log in to Web

1. Open a browser, enter the device's IP address (default: **192.168.1.13**) in the address bar, press **Enter**, and the login page appears.



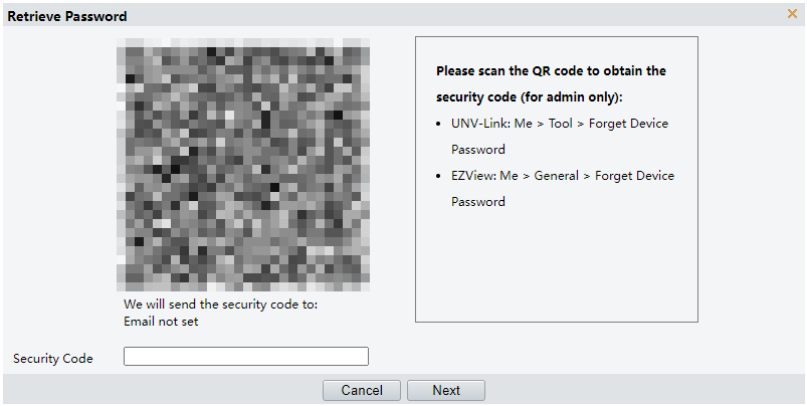
2. Enter the username and password (**admin**/**123456** by default).
3. Click **Login**.
4. (For first-time login) Please follow the on-screen instructions to change the password into a strong one and set your email address, which can receive a security code if you forgot the password. Then, use the new password to log in again.

Forgot Password

If you forgot the password after changing it, you can obtain the security code to reset the password.

Note: To use this function, make sure the device has an email address reserved, otherwise contact the local technical support to reset the password.

1. Click **Forgot Password** on the login page, and the **Retrieve Password** page appears.



2. Follow the on-screen prompt to obtain a security code.
3. Enter the security code, and click **Next** to retrieve the password. Please note this new password.

Logout

Click **Logout** in the upper-right corner of the interface, and click **OK** to log out from the current user.

3 Initial Configuration

After your first login, follow the steps below to complete the basic setup.

1. Change Password

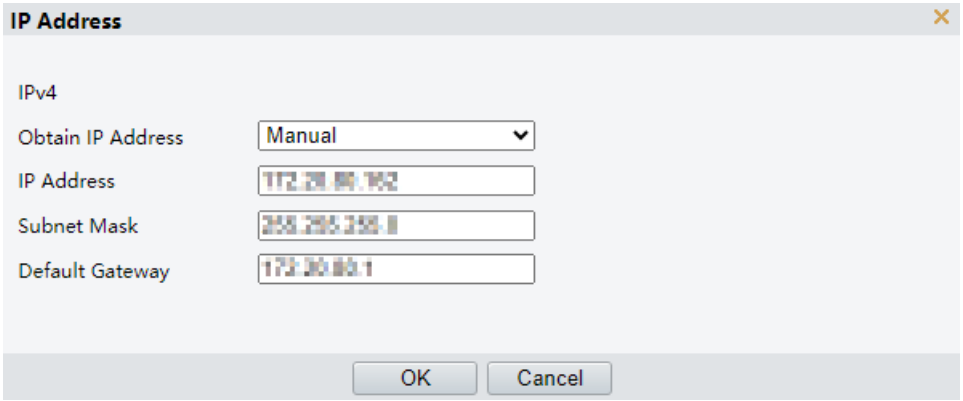
By default, the username is admin and the password is 123456.

After your first login, you are forcibly to change the password into a strong one. Please note the new password.

2. Set IP Address

The IP address is 192.168.1.13 by default. You need to change the IP address to the one you want.

1. On the live view page, click ✎ under the **Basic Config** tab.

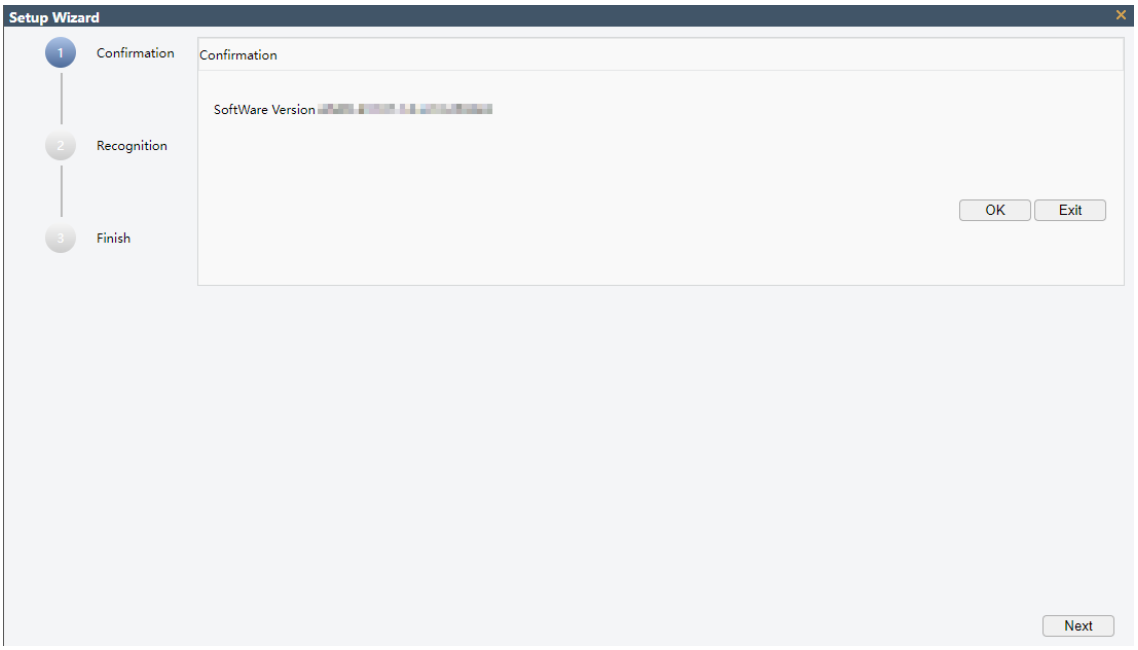


2. Select **Manual** from the **Obtain IP Address** drop-down list.
3. Enter the IP address, subnet mask, and gateway.
4. Click **OK**.

3. Draw Detection Box

After you log in to the camera's web interface for the first time, please follow the on-screen instructions to configure the initial parameters, or click **Setup Wizard** on the live view page.

1. Confirm the version information, and click **OK** or **Next** to proceed.



2. Refer to the example to draw the detection box. The camera takes a snapshot when the vehicle head enters the blue detection area.

   (1) Park a vehicle at the capture point and adjust the camera's shooting angle.

   (2) Click +/- or enter the value in the **Zoom** box to adjust the zoom ratio.

   (3) Click +/- to adjust the focus for clear license plate image.

   (4) Draw a blue detection box. It should be in the lower half of the live view. The top edge of the detection box must be horizontal. The bottom edge should ideally remain horizontal. Both sides must cover the left and right boundaries of the lane. The area should occupy 1/3 of the live view page.

   Click the blue box and drag the vertexes to adjust the size when white rectangles appear at all four corners.

   Click **Save** to save the drawing, or click **Cancel** to reset.

   (5) Move the red detection box. The size must approximate that of a standard license plate.

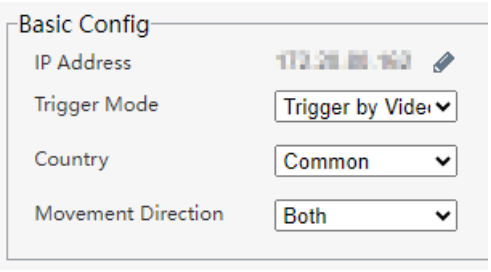
   Click the red box and drag it when white rectangles appear at all four corners.

   (6) (Optional) There is a default angle. You can click **Reset** to restore it.

3. Click **Next** and confirm again.

4. Configure Recognition Parameters

Configure the basic parameters on the live view page.



- Trigger Mode

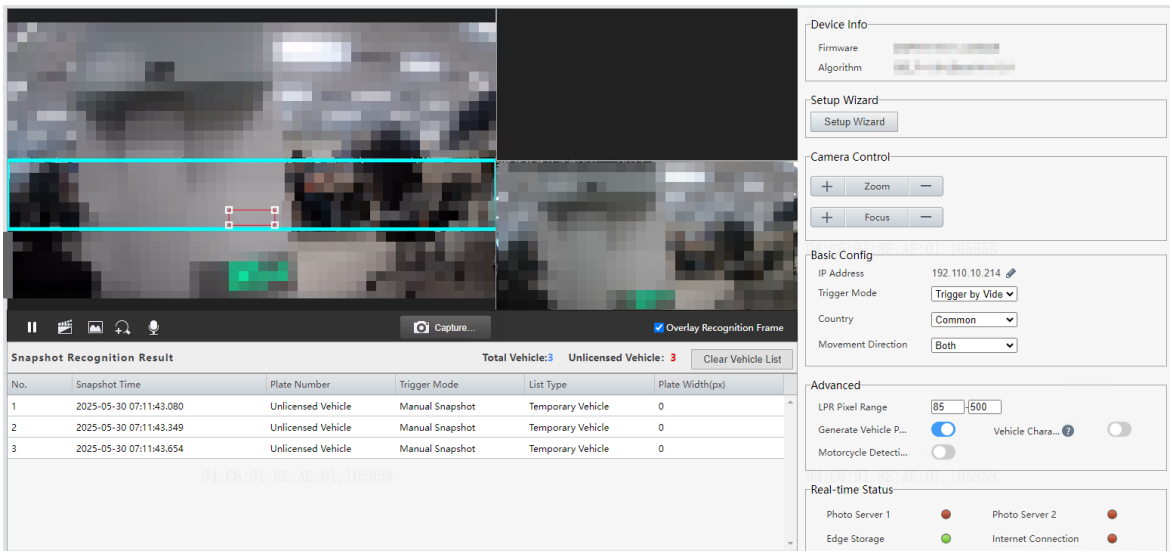
Trigger Mode	Description
Trigger by Video	(Recommended) Used for scenarios without external devices. The camera takes a snapshot when the vehicle head enters the blue detection area.
Trigger by Loop	Used for scenarios with external devices (such as loops, radar). When the external device detects a vehicle, it send signals to the camera for vehicle capture and recognition.

- Country: Change to the country where the camera is located.
- Movement Direction

Direction	Description
Both	(Recommend) Capture vehicles entering the detection area from the top/bottom of the live view.
Upward	Only capture vehicles entering the detection area from the top of the live view.
Downward	Only capture vehicles entering the detection area from the bottom of the live view.

4 Live View

After login, the **Live View** page appears by default.



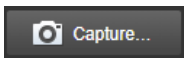
Live View Window

- Left window: Show the live video.
- Upper-right corner window: Show the thumbnail image of the latest captured license plate.

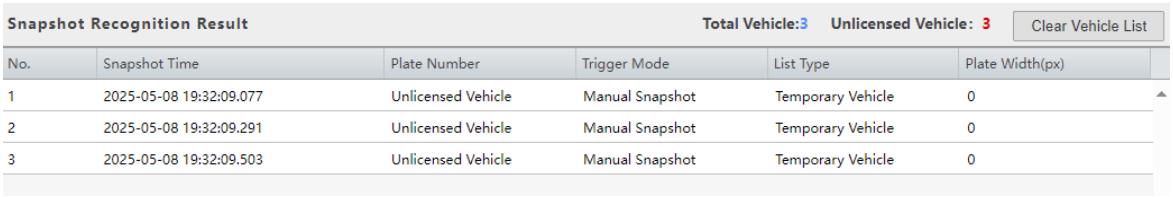
  Note: Please enable **Generate Color Photo** at **Setup** > **Smart** > Intelligent Configuration.
- Lower-right corner window: Show the complete image of the latest captured license plate.

Live View Toolbar

Button	Description
	Start/stop live view.
	Start/stop local recording. See Local Parameters for the path of the saved recordings. **Note:** This feature is not supported when live video is paused.
	Take a snapshot. The recording will be saved to the path set in Local Parameters. **Note:** This feature is not supported when live video is paused.

Button	Description
	Start digital zoom. Click on the area you want to zoom in, then use your scroll wheel to zoom in. Right-click to restore to its original size. Click  to exit digital zoom.
	Click to show  , and you can adjust the output and input volume. **Note:** • To use this function, connect the audio input and output devices to your computer. • If the camera's audio input is enabled, the recording function will be unavailable when the plug-in is not installed. Please disable **Audio Input** at **Setup** > **Video & Audio** > Audio.
	Take a snapshot from the displayed live video. See the snapshot in Photo.
Overlay Recognition Frame	When selected, the live view page will show one detection area. You can adjust the area as needed. See 3. Draw Detection Box for details.

Snapshot Recognition Result



The list shows the captured results in chronological order from top to bottom. The list data will be automatically cleared if you open another page.

Click any result, and the small image and the complete image of the license plate will be displayed on the right windows respectively.

Click **Clear Vehicle List** to clear the snapshot records in the list.

View the historical snapshots in Photo.

The following describes the certain fields:

Parameter	Description
List Type	• If the plate number exists in the allowlist and the vehicle passing time is within the validity period, the list type will be **Allowlist**. • If the plate number exists in the blocklist and the vehicle passing time is within the validity period, the list type will be **Blocklist**. • If the plate number is absent from both allowlist and blocklist, or the vehicle passing time is not within the validity period, the list type will be **Temporary Vehicle**. • If the plate number exists in both allowlist and blocklist and the vehicle passing time is within validity period, the list type will be **Blocklist**. **Note:** You can configure the allowlist and blacklist at **Setup** > Vehicle List.
Plate Width	It is displayed when a vehicle with a plate is captured. **Note:** Please enable **Generate Color Photo** at **Setup** > Intelligent Configuration before use; otherwise, the plate width is 0.

Device Info

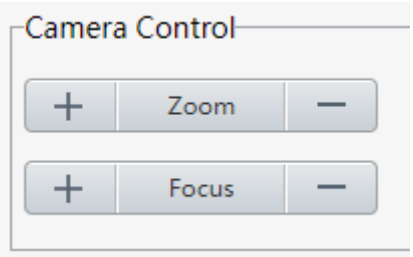
You can view the current software version and algorithm version.

The software version can be upgraded in Maintenance.

Setup Wizard

Click to redraw the detection box. See 3. Draw Detection Box in initial configuration.

Camera Control



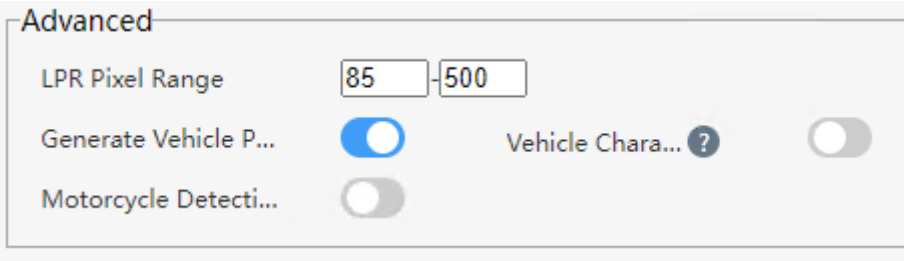
- Zoom: Zoom in or out on images.
- Focus: Focus far or near for clear images.

Basic Config

For IP address setting, see 2. Set IP Address.

For other parameter settings, see 4. Configure Recognition Parameters.

Advanced Config



- LPR Pixel Range: The license plate number can be identified if the plate pixel is within the set range; otherwise, the vehicle will be recognized as a vehicle with no plate.

  The default pixel range is suitable for most scenarios. This range is recommended unless there are specific requirements.

  When the trigger mode is **Trigger by Video**, the detected plate pixels will be displayed on the live video; otherwise, the pixels will not be displayed.
- Generate Vehicle Pass-thru Records Without Recognition: Vehicle passing records are generated directly without identifying vehicles.
- Vehicle Characteristics Recognition: When enabled, the vehicle characteristics will be recognized, including vehicle model, brand, logo, and color, and overlaid on the vehicle's composite photo along with OSD.
- Motorcycle Detection: When enabled, the motorcycles can be recognized.

Indicator Description

Type/ Indicator	🟢	🔴	○
Photo Server 1/2	Please set it in Photo Server.		
	The server is connected and online.	The server is disconnected or offline.	/
Edge Storage	Please set it in Storage.		
	The Micro SD card has been installed and is normal.	/	No Micro SD card is installed.

Type/ Indicator	🟢	🔴	⚪
Internet Connection	The camera is connected to the network.	The camera is disconnected from the network.	/
MQTT Server	The server is connected and online.	The server is disconnected or offline.	/
LED	Enable **Smart Illumination** in Image to turn on the illuminator	/	Illuminator is turned off

Navigation Bar

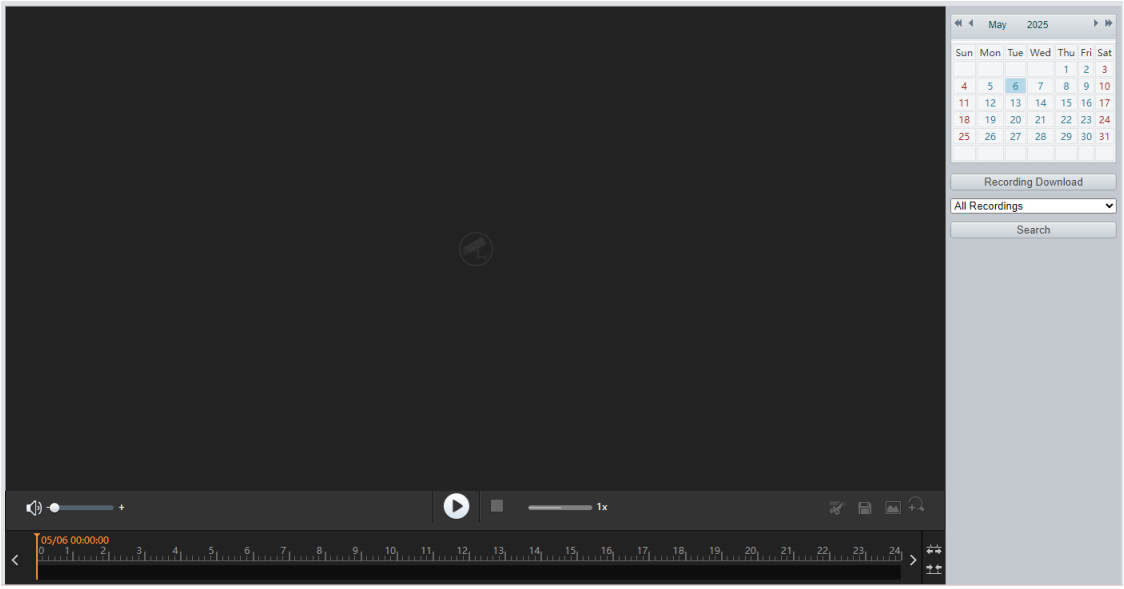
Show the device model. You can download the plug-in or log out from the current user.

5 Playback

Note:

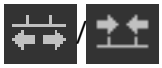
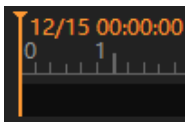
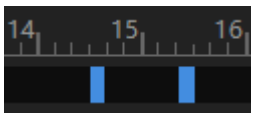
- Edge recordings refer to video recorded on storage media of cameras; local recordings refer to video recorded on a local PC.
- Before you search for edge recordings, make sure that the camera has an installed Micro SD card, and Storage is properly configured.
- Recording playback and download functions are only available on certain models.
- For dual-channel devices, you can set playback parameters for the channels separately.

Enter the playback page.



5.1 Playback Toolbar

Button	Description
	Adjust sound volume. Range: 0 to 100.
	Start playback.

Button	Description
	Pause playback. Click  to resume the playback.
	Exit the playback.
	Start/stop clipping video.
	Save the clipped video.
	Adjust the playback speed. The default speed is 1x. 2x plays faster, and 1/2x plays slower. -2x rewinds fast.
	Take a snapshot. The snapshots are saved locally by default. You can change the storage location in Local Parameters.
	Enable digital zoom. Click on the area you want to zoom in, then use your scroll wheel to zoom in. Right-click to restore to its original size. Click  to exit digital zoom.
	Zoom in/zoom out on the time scale. You can also use the scroll wheel to zoom.
	When the time scale is zoomed in, click to view the previous or next section of the video.
	Playhead. Drag the playhead to skip to any point in the video.
	Playback timeline, including two colors: • Blue: Normal recording. • Red: Alarm recording. To view alarm recordings, you need to configure alarm-triggered recording.

5.2 Search and Playback

Note: Certain cameras support simultaneous playback on two clients.

1. For a multi-channel camera, select the channel first.
2. Select the date on the calendar.
3. Click **All Recordings** in the list and then choose the recording type you want to search.
4. Click **Search**.
5. Choose a recording playback mode.
   - Select a recording for playback: Select the desired recording from the search results and double-click to start playback. The system will automatically play all subsequent recordings in sequence, stopping after the last one completes. To pause playback, click  .

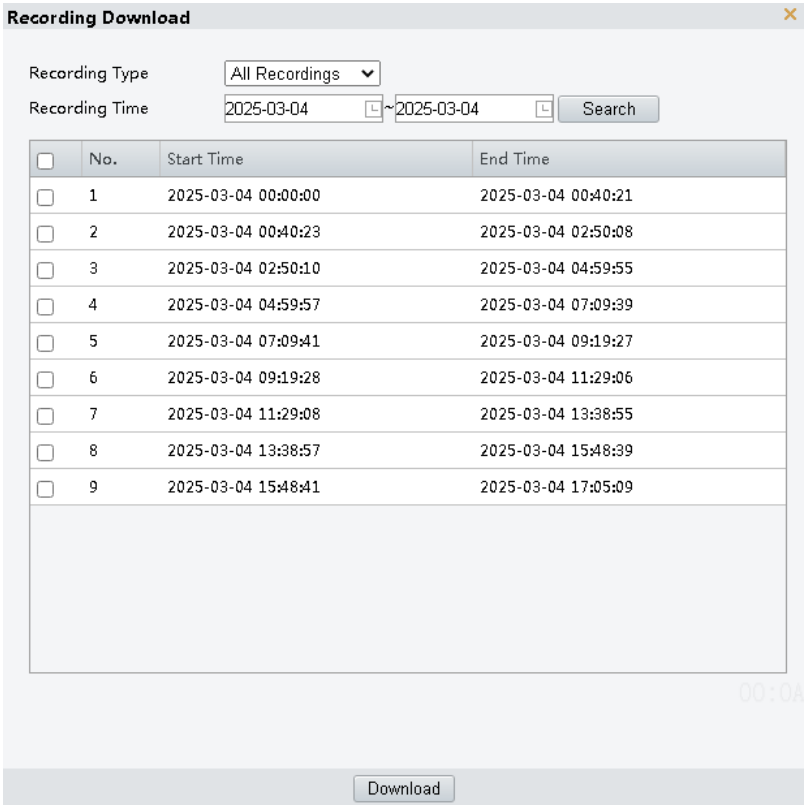
     Note: If the results contain 10 recordings and playback starts from the 3rd recording, and 2 new recordings are added during playback, then the system will then play recordings 3 through 12.
   - Playback from the first recording: Double-click the first recording, and the system will automatically play all the searched recordings in sequence before stopping.

5.3 Recording Download

You can download videos in batches or clip videos to download.

- Download in batches

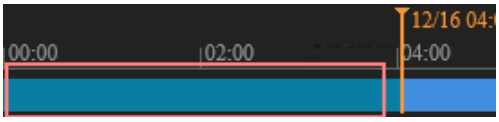
1. Click **Recording Download**.
2. Select the recording type, set the start time and end time, and then click **Search**.
3. Search results are displayed.



4. Click **Browse…** and set the download destination.
5. Select the checkboxes for the recordings you want to download and click **Download**.

- Download video clips
  1. Search for the video to clip. See Search and Playback for details.
  2. On the playback toolbar, click  .
  3. Click 

to specify the clip by setting the start time and end time.
  4. Click  . The clip turns cyan on the timeline.



  5. Click  . The **Recording Download** page appears.

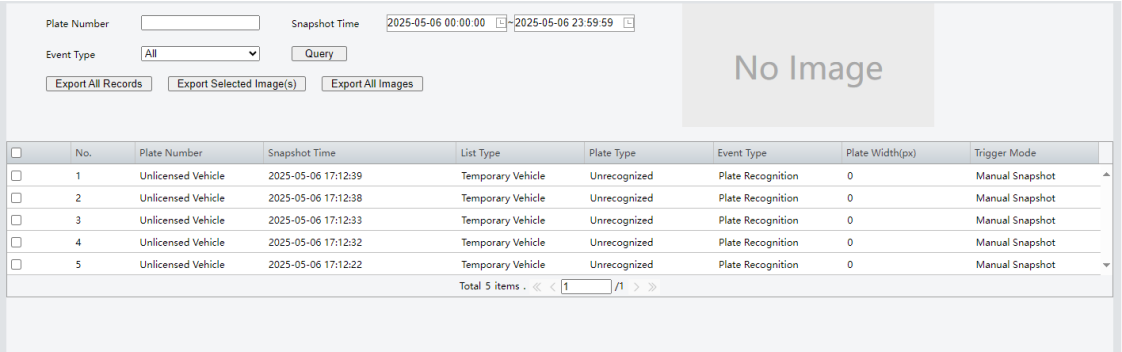
     Note: Recording download functions supported may vary with device model. Please refer to the actual interface.

  6. Download the recording desired. See Download in batches for detailed steps.

6 Photo

Show all the captured license plate information.

Enter the **Photo** page.



Search

You can search for the images according to plate number, snapshot time, and event type.

View Snapshot Image

Click the snapshot record, and the snapshot image will appear on the list above.

Export

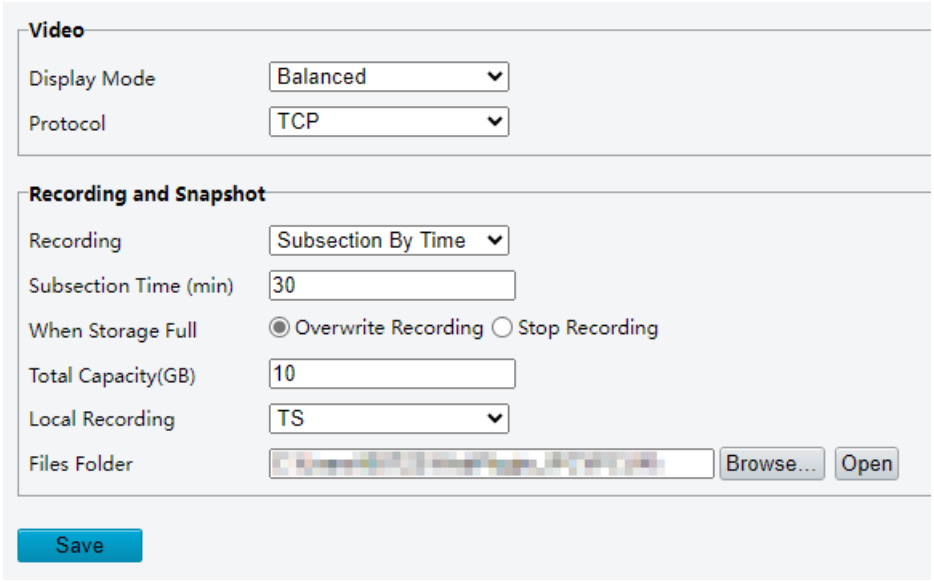
- Export All Records: Click **Export All Records** and click **OK**.
- Export Selected Images: Select the record(s) you want to export, and click **Export Selected Image(s)**.
- Export All Images: Click **Export All Images** and click **OK**.

7 Setup

7.1 Local Parameters

This function appears after the plug-in is installed. Set local parameters for your PC, including video, recording and snapshot.

1. Go to **Setup** > **Local Parameters**.



2. Set local parameters as needed.

Parameter		Description
Video	Display Mode	Set the video display mode according to the network status. • Balanced: Recommended for video playing under good network conditions. • Fluent (default): Recommended for video playing with network delay.

Parameter		Description
		• Min. Delay: Recommended for video playing under poor network conditions.
	Protocol	Set the protocol used to transmit media streams. • UDP: Supports one-to-one, one-to-many, many-to-many, and many-to one communication methods; data can be sent without establishing a logical connection; data security and integrity cannot be guaranteed. • TCP (default): Supports one-to-one communication only; data can only be sent after a logical connection has been established between the receiver and the sender; data transmission is secure and reliable.
Recording and Snapshot	Recording	• Subsection By Time (default): Save recording files of the set subsection time. • Subsection By Size: Save recording files of the set subsection size.
	Subsection Time (min)	Length of each recording file, available when **Recording** is set to **Subsection By Time**. Range: 1 to 60. Default: 30.
	Subsection Size (MB)	Size of each recording file, available when **Recording** is set to **Subsection By Size**. Range: 10 to 1024. Default: 100.
	When Storage Full	The storage policy of the new recording when the local recording capacity reaches the upper limit. • Overwrite Recording (default): When the local recording capacity is full, the oldest recordings are overwritten automatically. • Stop Recording: When the local recording capacity is full, recording stops automatically.
	Total Capacity (GB)	Allocate storage capacity for local recordings and snapshots on the PC. Range: 1 to 1024. Default: 10.
	Files Folder	The location where snapshots and recordings are saved. By default, the snapshots are saved in .jpg or .bmp format. The recordings are saved in .ts format. • Browse: Click to choose the file the storage location. • Open: Click to open the selected folder. **Note:** The maximum length of the directory is 260 bytes. If the limit is exceeded, recording or snapshot during live view will fail and a message will appear.

3. Click **Save**.

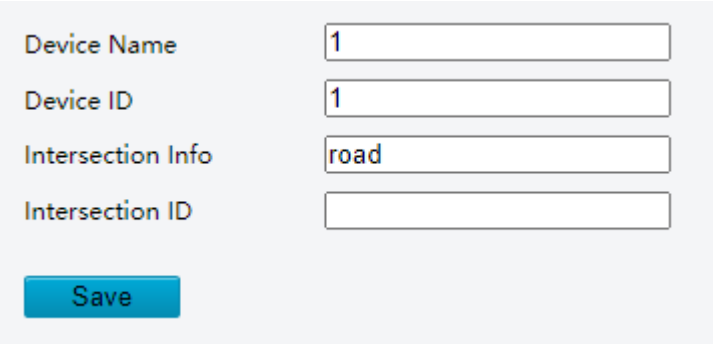
7.2 System

7.2.1 Device Info

Set device information including device name, device ID, location, etc. which can be used in smart FTP, OSD, etc.

Note: The functions supported may vary with device model.

1. Go to **Setup** > **System** > **Device Info**.

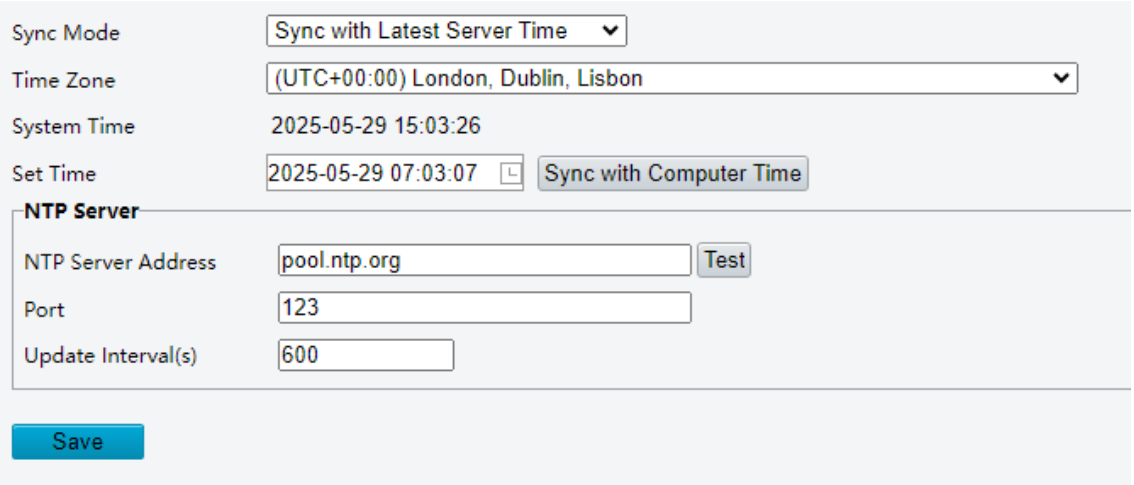


2. Set the device information as needed.
3. Click **Save**.

7.2.2 Time

Set the camera time.

1. Go to **Setup** > **System** > **Time**.

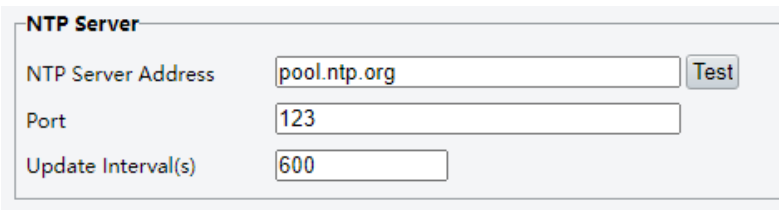


2. You can set the device time manually or sync it with a server.
   - Set manually: Set the system time as needed.

     Note: Make sure **Sync Mode** is set to **Sync with System Configuration**; otherwise, the device time will still sync with other sources after you set it manually.

   - Sync time automatically:

     (1) Select the sync mode.

Parameter	Description
Sync with System Configuration	The device uses the time provided by the camera's built-in time module.
Sync with NTP Server	NTP Server: A server used to sync time with the distributed server and client via NTP protocol. To sync the server time, you need to configure the NTP server address, port, and update interval.  • NTP Server Address: Enter the NTP server address and click **Test** to check the network communication. A message will appear if the NTP is verified successfully.

Parameter	Description
	• Port: Range: 1-65535, integer only, default: 123. • Update Interval (s): Range: 30-3600, integer only, default: 600.
Sync with Management Server(Non-ONVIF)	The camera regularly syncs time with the management server that is not connected via Onvif.
Sync with Management Server(ONVIF)	The camera regularly syncs time with the management server connected via Onvif.
Sync with Latest Server Time	Default sync mode. The camera regularly syncs time with all the connected servers.
Sync with Intelligent Server(LAPI)	The camera regularly syncs time with the management server connected via LAPI.

(2) Set the time zone as needed. The default is **(UTC+00:00) London, Dublin, Lisbon**. You can set it as needed.

(3) Click **Sync with Computer Time**.

3. Click **Save**.

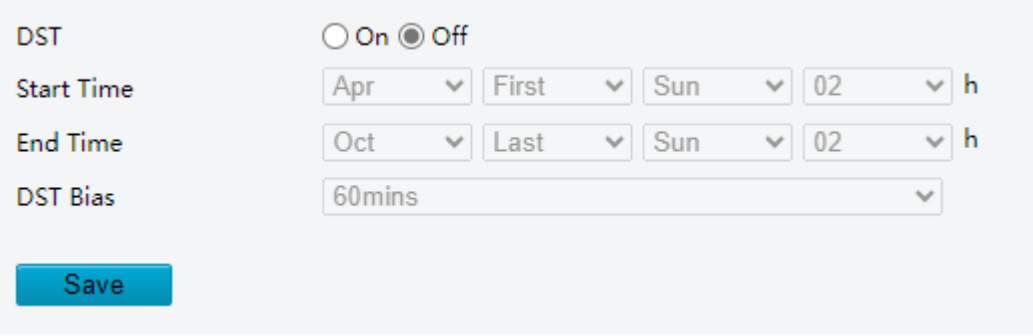
7.2.3 DST

DST (Daylight Saving Time) is a local time system designed to make full use of daytime to save energy, which sets clocks forward by one hour in summer months.

By default, this function is disabled.

Note: DST rules vary in different countries.

1. Go to **Setup** > **System** > **DST**.

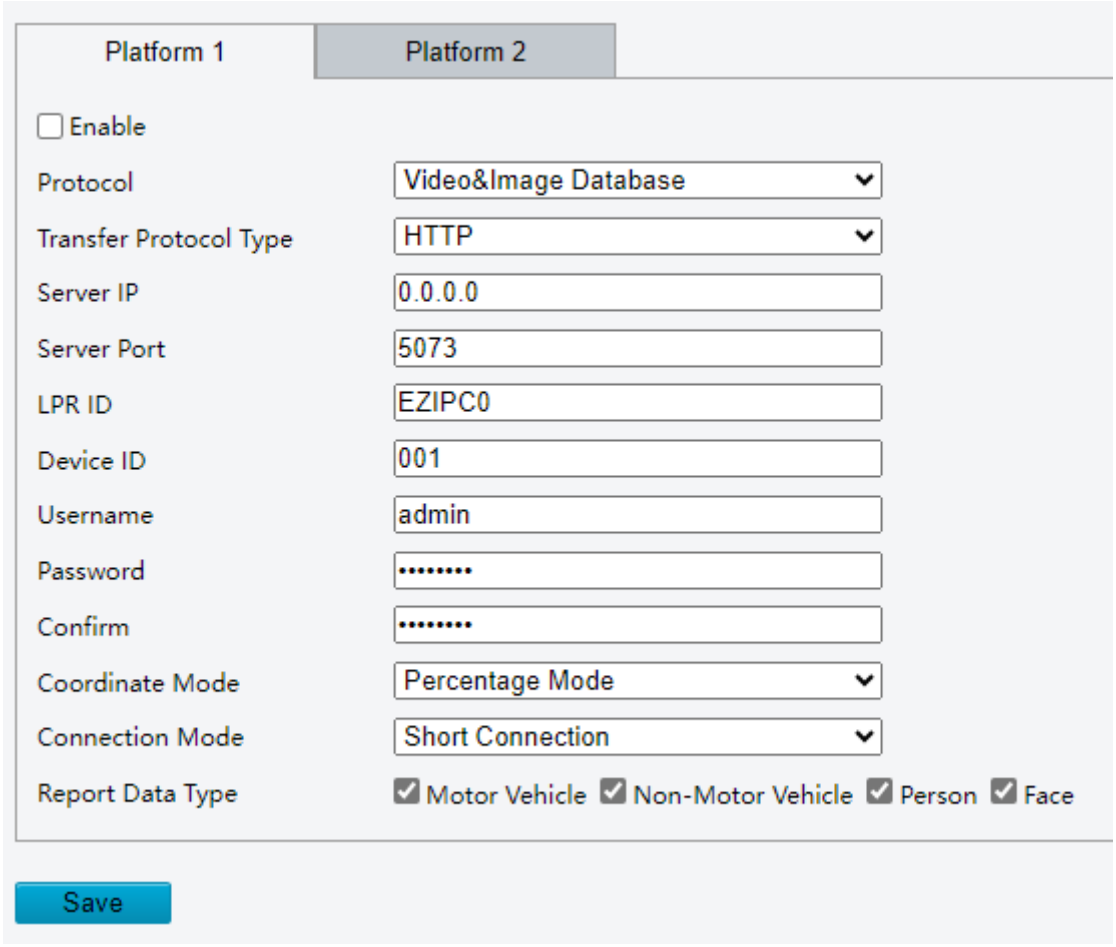


2. Enable **DST**.
3. Set the start time, end time, and DST bias as needed.
4. Click **Save**.

7.2.4 Photo Server

After connected to the photo server, the camera will automatically upload real-time access records and captured images when network connectivity is maintained. A camera can be managed by two photo servers.

1. Go to **Setup** > **System** > **Photo Server**.



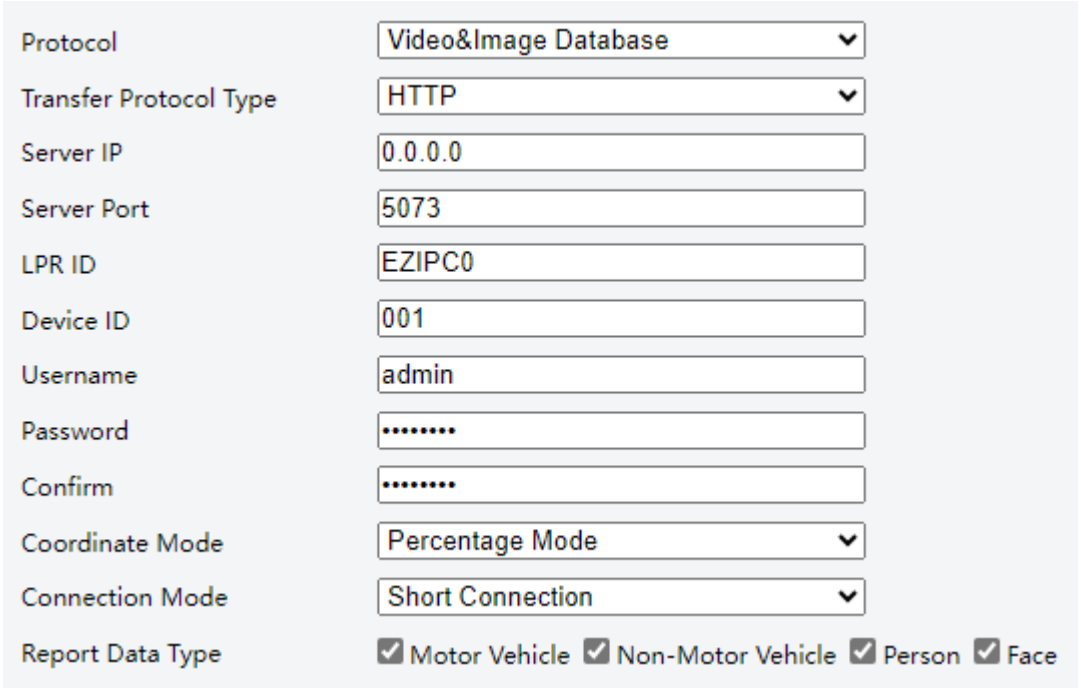
2. Enable **Platform 1**.

   When enabled, the camera can be connected to the platform 1 via the protocol; when disabled, the camera cannot be connected to the platform 1.

   To connect the camera to the platform, add the camera on the platform, and configure the following parameters on the camera.

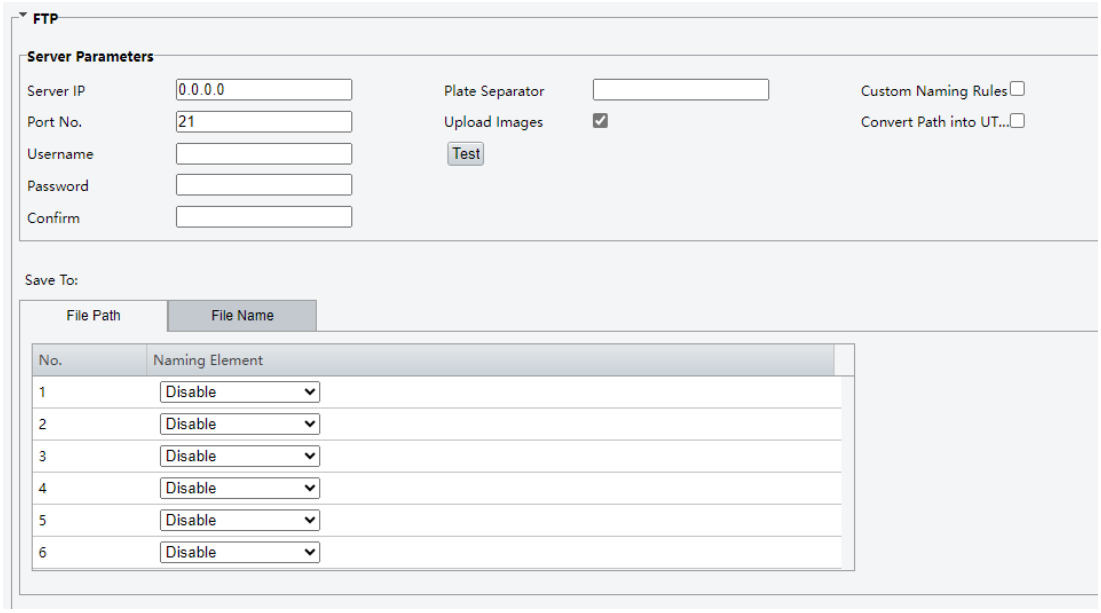
3. Choose a protocol and configure the parameters.

   - Video&Image Database



Parameter	Description
Transfer Protocol Type	• HTTP • HTTPS
Server IP/Port	The server IP address and port of the platform.
LPR ID/Device ID	Use the default.
Username/ Password/Confirm	Username and password used to log in to the VIID server.
Coordinate Mode	Choose **Percentage Mode** (default), **Pixel Mode**, or **Normalized Mode**.
Connection Mode	Choose **Short Connection** (default) or **Standard**.
Report Data Type	Choose **Motor Vehicle**, **Non-Motor Vehicle**, **Person**, or **Face**.

- FTP



Server Parameters

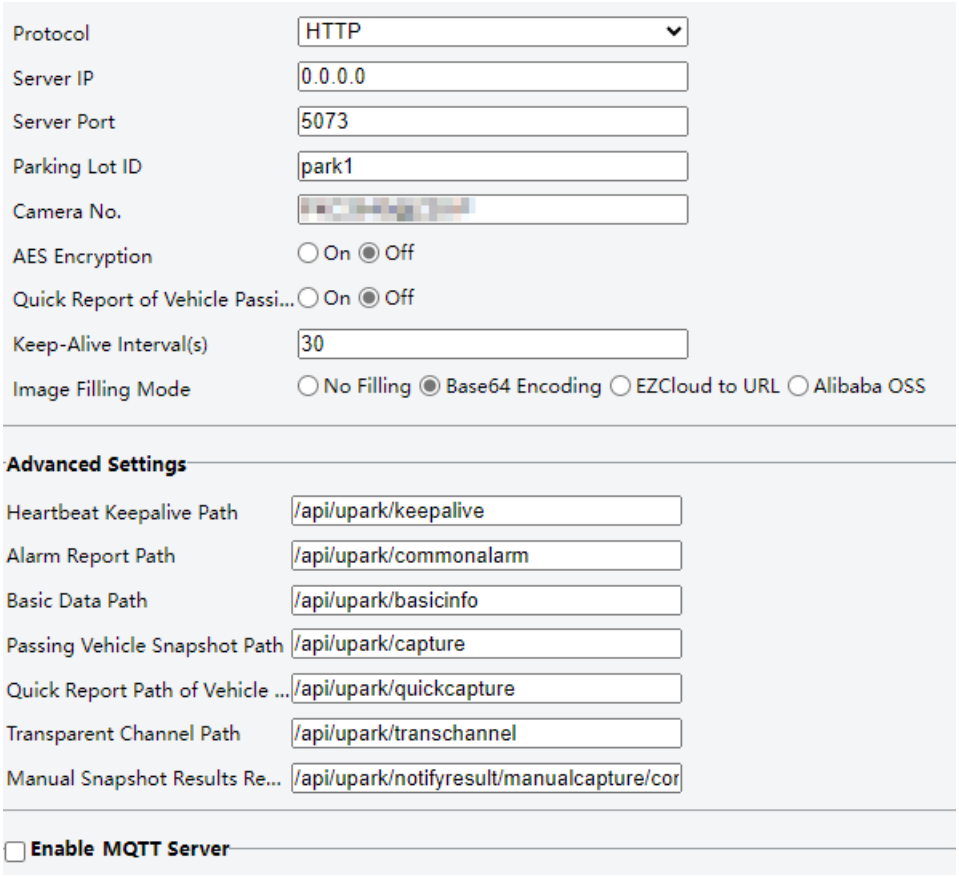
Parameter	Description
Server IP	Set the FTP server address.
Port No.	Use the default 21. You can set it as needed.
Username	Enter the FTP server username.
Password	Enter the FTP server password.
Test	Click to test the connection to the FTP server.
Upload Images	Select the checkbox to enable uploading non-smart snapshots. Overwrite Storage: After the number of photos in the lowest-level folder reaches the set threshold, new photos will overwrite older photos in the folder. For example, the storage path is "\IP\date", the lowest-level folder is the level-2 folder named "date". When the number of photos uploaded on Jan. 4, 2022 reaches 1000 (default value), new photos overwrite old photos in the 20220104 folder. **Note:** To choose **Overwrite Storage**, make sure the last naming element of the files is the image sequence number.
Custom Naming Rule	Select the checkbox, and then you can set the file naming rules as needed.

Parameter	Description
Covert Path into UTF8	Select the checkbox, and the path will be converted into UTF8 format.

Save Path

Parameter	Description
File Path	Six levels are allowed. If not set, the default path "\IP\Date\Common" will be used, where "Common”"means non-smart snapshots.
File Name	Up to 20 fields are allowed. If not set, sequence numbers will be used as file names, for example, "1, 2, 3", etc.

- HTTP



Parameter	Description
Server IP	Set the HTTP server address.
Server Port/ Parking Lot ID/ Camera No.	Use the defaults.
AES Encryption	When enabled, the data security can be protected effectively, preventing unauthorized access and tampering.
Advanced Settings	Storage paths for different data. Use the defaults.
Enable MQTT Server	MQTT server can receive, store, and forward messages. Cameras can publish messages to specific topics for information sharing. Other devices may subscribe to these topics to receive relevant messages. When enabled, please configure the MQTT server address, port, login information, request topic, and response topic.

4. If you need to manage the camera via two photo servers, enable Platform 2 and configure the server parameters (only supports VIID and FTP protocols).

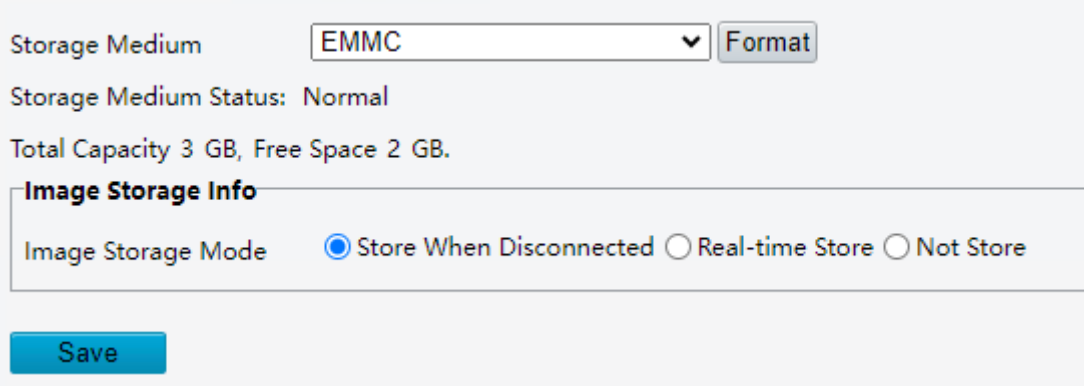
5. Click **Save**.

7.2.5 Storage

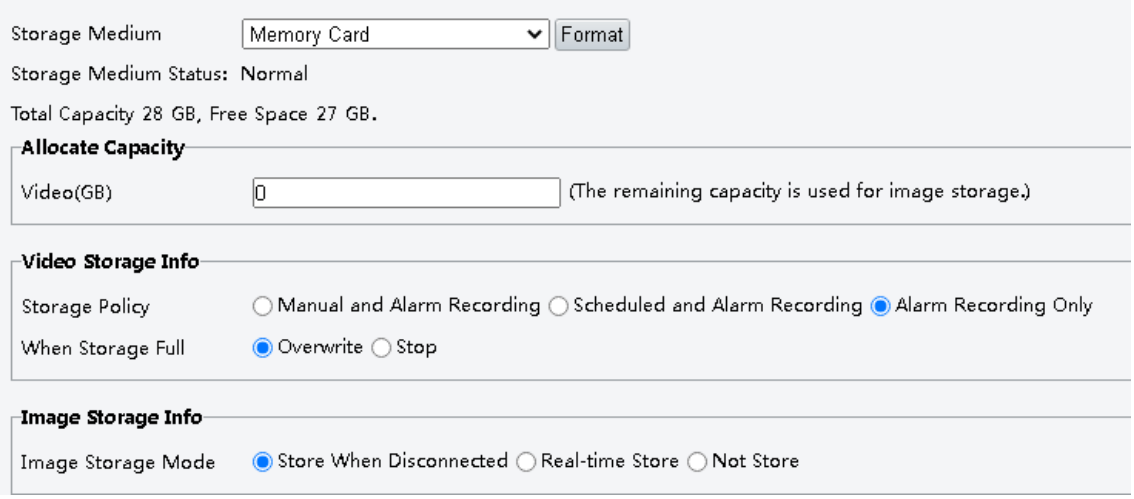
After inserting a micro SD card and the camera connecting to the Photo Server, you can then configure whether to store images on the camera's memory card.

Go to **Setup** > **System** > **Storage**.

- The **Storage Medium** is **EMMC** by default, which stores images only.



- When a Micro SD card is inserted, the storage medium will switch to **Memory Card**, allowing the camera to store recordings and images. The images previously stored in eMMC are unavailable.



Configure the parameters, and click **Save**.

Parameter	Description
Storage Medium	It is **EMMC** by default and switches to **Memory Card** when a Micro SD card is inserted. Then, the eMMC becomes ineffective. • Format: Click to format the Micro SD card. • Storage Medium Status: Show the actual status of the memory card. • Total Capacity: Show the total capacity and remaining space of the memory card.

Image Storage Info	**Note:** The following configurations apply only to the photo server 1. For the photo server 2, the image storage mode is **Store When Disconnected** by default.
	• Store When Disconnected: This mode is recommended.
	  • Photo server offline: The images are stored on the Micro SD card.
	  • Photo server online: The images are uploaded to the photo server without local storage on the Micro SD card.
	• Real-time Store: It requires significant storage space.
	  • Photo server offline: The images are stored on the Micro SD card.

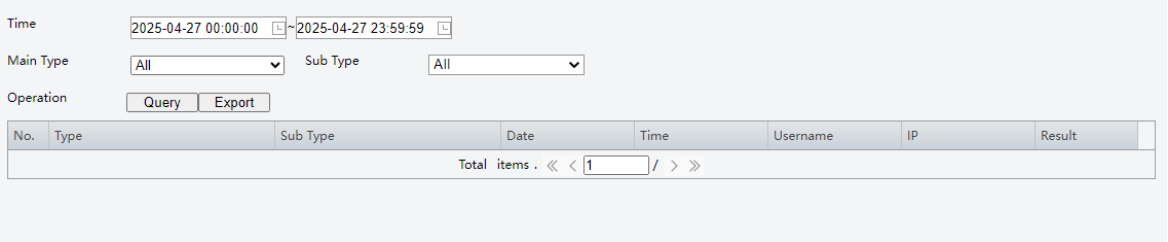
Parameter	Description
	• Photo server online: The images are uploaded to the photo server and will be also stored on the Micro SD card. • Not Store: Images are never stored on the Micro SD card.
Video	Allocate video storage capacity without exceeding total available storage capacity. The remaining capacity after allocation is used for image storage. **Note:** When the allocated storage capacity exceeds remaining capacity, some historical images will be deleted from the Micro SD card.

Video Storage Info	• Storage Policy
	  • Manual and Alarm Recording: Store manual recordings and alarm recordings.
	  • Alarm Recording Only: Store alarm recordings only.
	• Stream: Main Stream by default.
	• When Storage Full
	  • Overwrite: When space is used up on the memory card, new data overwrites old data.
	  • Stop: When space is used up on the memory card, the camera stops saving new data.

7.2.6 Log

Search operation logs that configure alarm and network parameters.

Go to **Setup** > **System** > **Log**.



Search

1. Set the time range, main type, and sub type.
2. Click **Search**, and the desired logs will be displayed in the list below.

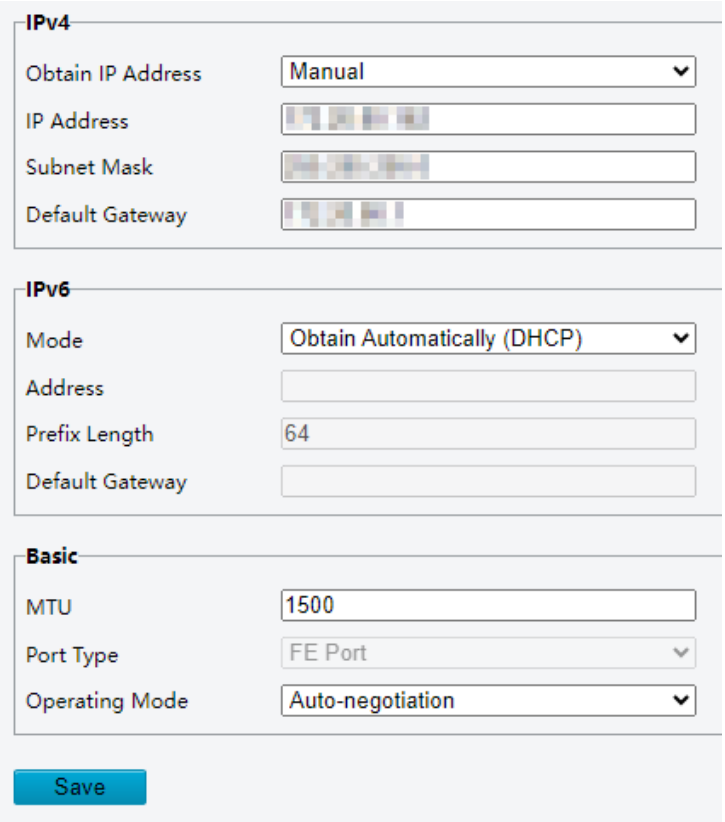
Export

Click **Export** to save search results as a file named **operation .csv**.

7.3 Network

7.3.1 Wired Network

1. Go to **Setup** > **Network** > **Wired Network**.



2. Configure the network parameters.

Note: Some devices have two network interfaces, allowing separate configurations for interface 1 and interface 2.

- IPv4
  - Manual

    (1) Select **Manual** from the **Obtain IP Address** drop-down list.

    (2) Enter the IP address, subnet mask, and default gateway. Make sure that the IP address of the camera is unique in the network.

    (3) Click **Save**.
  - PPPoE

    Configure PPPoE to assign a dynamic IP address.

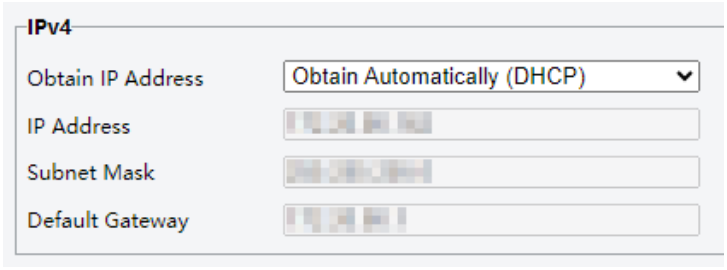
    (1) Select **PPPoE** from the **Obtain IP Address** drop-down list.

    (2) Enter the username and password provided by your ISP (Internet Service Provider), click **Save**, then the camera will be assigned an IP address.
  - **Obtain Automatically (DHCP)**

    DHCP (Dynamic Host Configuration Protocol) is enabled by default. If a DHCP server is deployed in the network, the camera can automatically obtain an IP address from the DHCP server.

    (1) Select **Obtain Automatically (DHCP)** from the **Obtain IP Address** drop-down list.

    (2) Complete the settings as shown below.



- IPv6

- **Obtain Automatically (DHCP)**

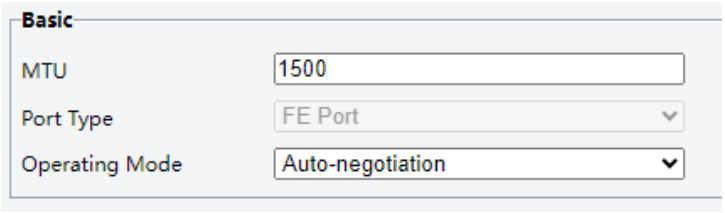
  The default mode is **Obtain Automatically(DHCP)**. In this mode, the IP address is assigned by the DHCP server.

- Manual

  (1) Select **Manual** from the **Mode** drop-down list.

  (2) Enter the IPv6 address, prefix length, and default gateway. Make sure that the IPv6 address is unique in the network.

3. Set the basic parameters.
   - MTU: Set the maximum packet size supported by the network in bytes. The greater the value, the higher the communication efficiency, the higher the transmission delay.
   - Port Type: **FE Port** by default.
   - Operating Mode: **Auto-negotiation** by default.



4. Click **Save**.

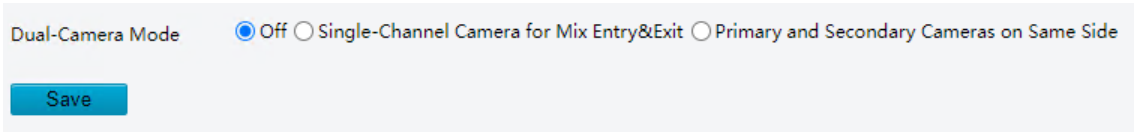
7.3.2 Dual-Camera Parameters

To use primary and secondary camera mode and single-channel camera for mix entry&exit mode, you should complete the relevant configurations on the cameras for inter-camera communication.

Note:

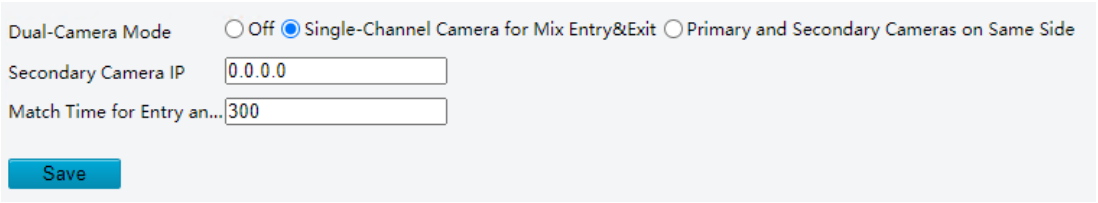
- The two modes cannot be enabled simultaneously on the camera.
- The two camera versions must be consistent when using the two modes.
- When an LED display is required, both cameras must use the same display style, with each LED screen configured as a 4-row × 4-character matrix.

1. Go to **Setup** > **Network** > **Dual-Camera Parameters**.

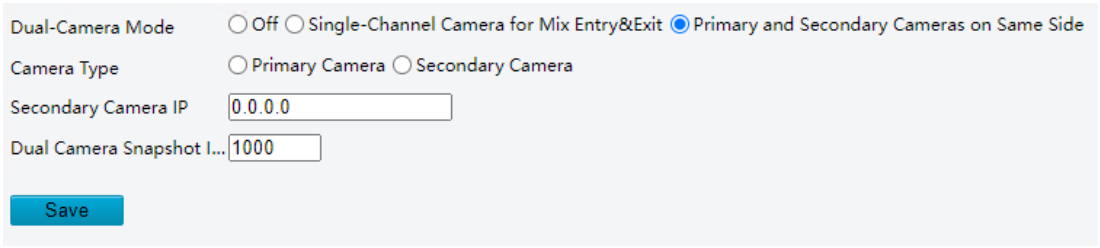


2. Choose a dual-camera mode and configure the parameters.
   - Off: This function is disabled.
   - Single-Channel Camera for Mix Entry&Exit: Applicable to mixed entry and exit scenarios. Both cameras must select this mode.

     Secondary Camera IP: The IP address of the other camera.



   - Primary and Secondary Camera on Same Side: When a single camera cannot capture all passing vehicles at one exit/entrance, you can install two cameras with the same mode and enable **Primary and Secondary Camera on Same Side** to capture all passing vehicles.



- Function Introduction: For example, there are two cameras. Camera A is the primary camera, with a recognition result of a, while Camera B is the secondary camera, with a recognition result of b. Camera B transmits its recognition results to Camera A. Camera A then compares both results (A and B) and uploads the optimal results to the server. If the time difference exceeds the specified threshold during capture, the system directly reports the first record.
- Extended Function-LED Display: After the primary camera and secondary camera have been configured, connect the LED displays to the cameras respectively. The primary camera will then sync the received LED display information with the secondary camera to output synced content.
- Configuration Description:

  (1) Enter the **Dual-Camera Parameters** page of the camera A, set **Dual-Camera Mode** to **Primary and Secondary Camera on Same Side**, set **Camera Type** to **Primary Camera**, enter the IP address of the secondary camera B, and click **Save**.

  (2) Enter the **Dual-Camera Parameters** page of the camera B, set **Dual-Camera Mode** to **Primary and Secondary Camera on Same Side**, set **Camera Type** to **Secondary Camera**, enter the IP address of the secondary camera A, and click **Save**.

Note:

- When the primary and secondary cameras are connected to LED displays, the display type and protocol must be the same.
- When **Primary and Secondary Camera on Same Side** is enabled, **Quick Report of Vehicle Passing Through** for HTTP protocol in the server photo is unavailable and will be forcibly disabled during data upload.
- Once the primary camera is configured, all settings will automatically sync to the secondary camera without requiring manual setup.
- After primary and secondary cameras configuration are complete, the secondary camera time will automatically sync with the primary camera time.
- When the two cameras run different versions, it is recommended to upgrade both to the latest version before primary camera and secondary camera configuration.
- When the two cameras are different models, contact the technical support for primary camera and secondary camera configuration.

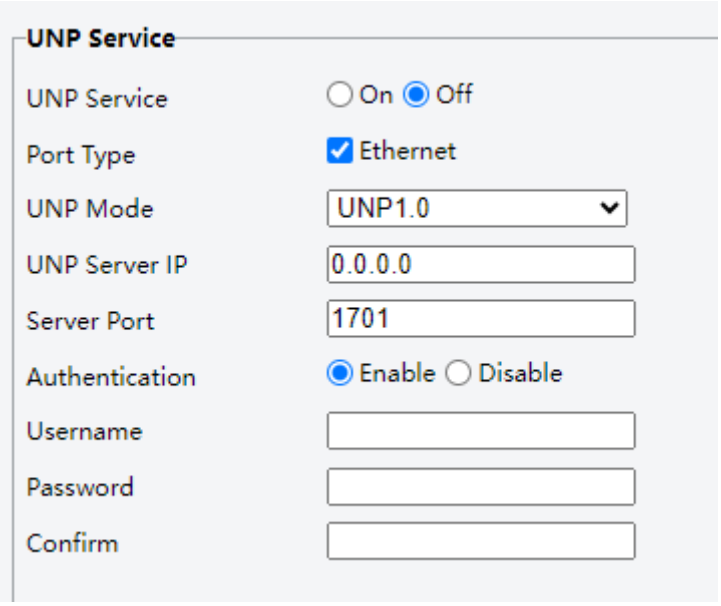
3. Click **Save**.

7.3.3 Network Protocol

Go to **Setup** > **Network** > **Network Protocol**. Configure the parameters, and click **Save**.

UNP Service

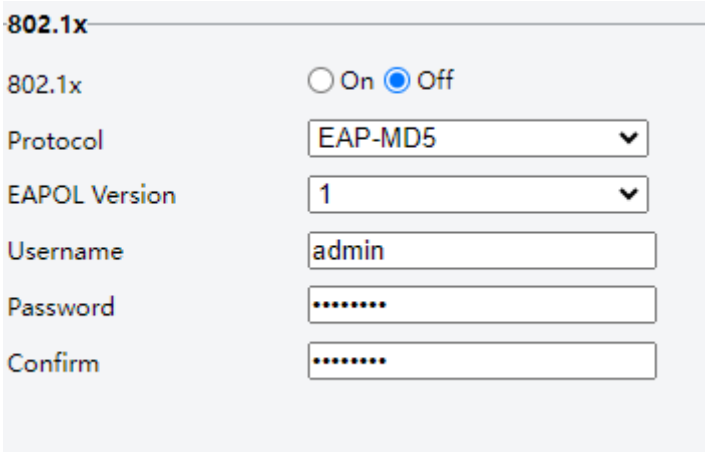
If the network environment has a data diode or firewall, you can connect the camera to the network via a UNP(Universal Network Passport).



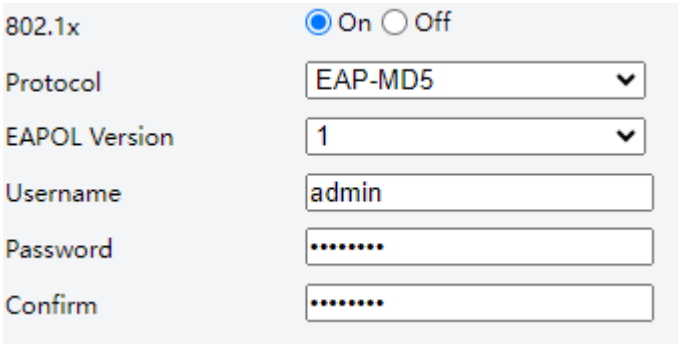
1. Enable **UNP Service**.
2. Select the port type as needed.
3. Enter the UNP server address.
4. If the UNP server requires authentication, enable **Authentication** and enter the UNP username and password, and confirm the password.
5. Click **Save**.

802.1x

802.1x is a client/server-based access control and authentication protocol. When the device functions as an 802.1x client, only imported certificates and CA certificates can pass server authentication. The network connection will fail if the self-signed certificate and the default certificate are unable to pass authentication.



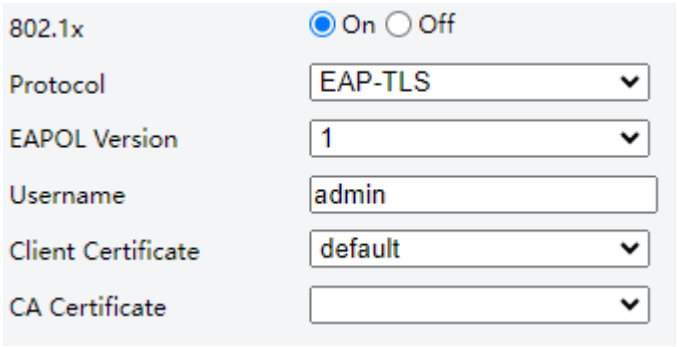
1. Enable **802.1x**.
2. Select a protocol. The camera can establish network communication only after successful protocol authentication.
   - EAP-MD5



(1) Choose the EAPOL version according to the protocol version on the network switch.

(2) Enter the device username and password, and confirm the password.

- EAP-TLS



(1) Choose the EAPOL version according to the protocol version on the network switch.

(2) Enter the username.

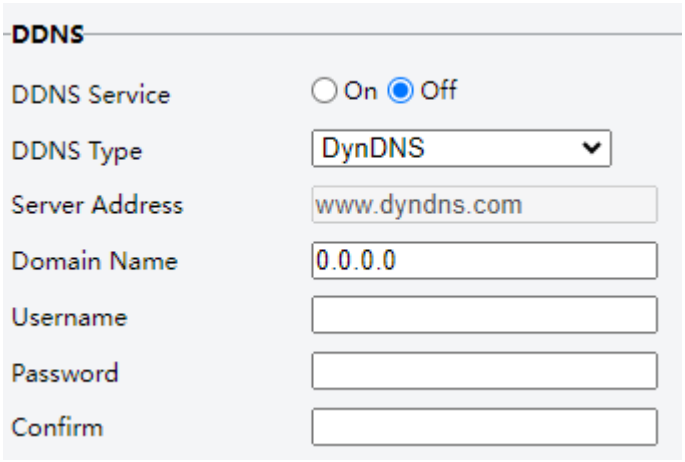
(3) Click ⌄ to select the client certificate and CA certificate. See Certificate Management for detailed certificate settings.

3. Click **Save**.

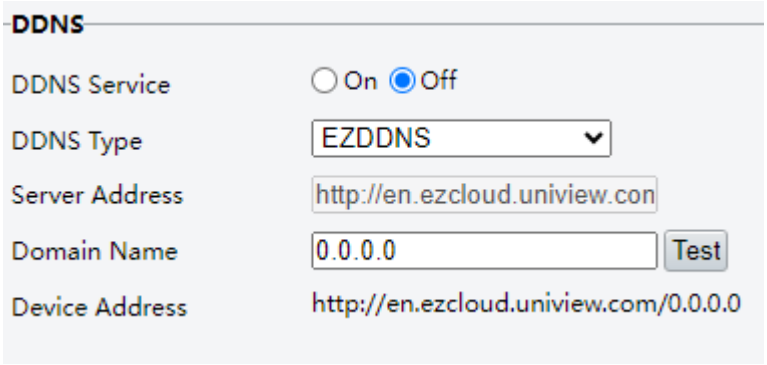
DDNS

DDNS (Dynamic Domain Name System) automatically updates the DNS server with the device's dynamic IP address to enable remote Internet access to the device on the network. With DDNS, users can access the private network device for remote control with the public IP address.

1. Enable **DDNS Service**.



2. Select the DDNS type.
   - DynDNS/NO-IP: Third-party DDNS service provider, enter the domain name registered with the DDNS provider.
   - EZDDNS: Uniview's DDNS service, enter a domain name for your camera.



Note: If your server is located domestically, it is recommended to select a domestic DDNS service provider, as overseas DDNS servers may be blocked by the national firewall.

3. Click **Save**.

SNMP

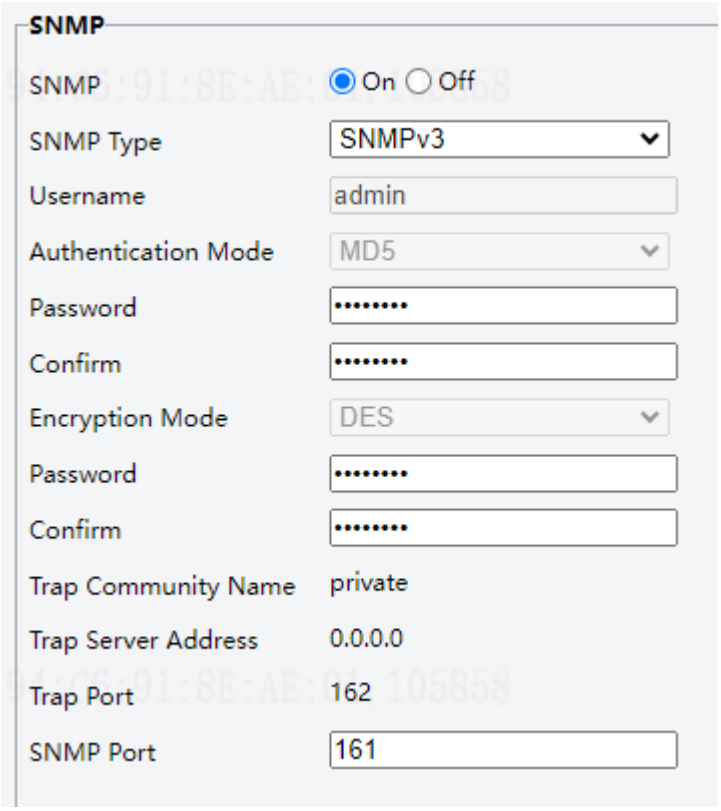
SNMP is required for the camera to share configuration information to servers.

1. Go to **Setup** > **Network** > **Network Protocol** > **SNMP**.
2. Enable **SNMP**.

   Note: If SNMP is enabled by default, this occurs due to backward compatibility requirements after upgrading the camera to the latest firmware version. This behavior is expected and normal.

3. Set SNMP parameters.
   - SNMPv3

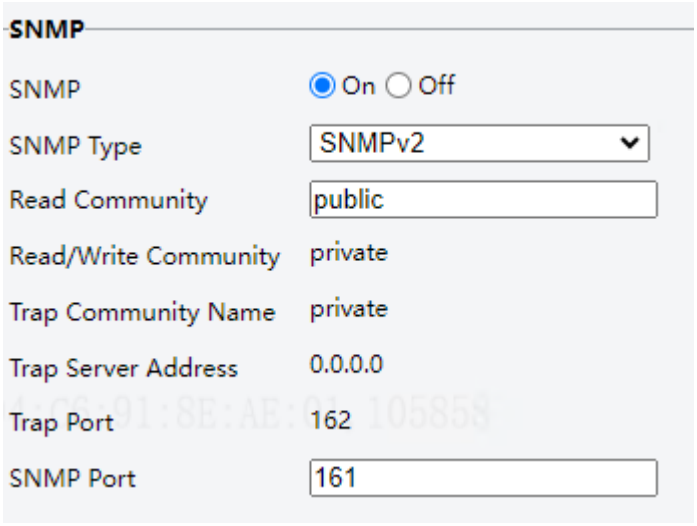
     Note: Before you enable SNMPv3, make sure that it is supported both on your camera and the server.



Item	Description
SNMP Type	**SNMPv3** by default.
Password	Set a password for authentication.
Confirm	Confirm the password by entering it again.

Item	Description
Password	Set a password for data encryption.
Confirm	Confirm the password by entering it again.
Trap Server Address	It is automatically filled after the management platform configuration is completed .
SNMP Port	The default is 161. You may change is as needed.

- SNMPv2



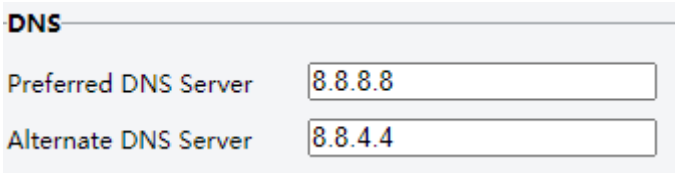
Item	Description
SNMP Type	Select **SNMPv2**. After you select SNMPv2, a message pops up to remind you of potential risks and ask if you want to continue. Click **OK**.
Read Community	The default read community name is public, and you may change it as needed. Make sure the read community names of the server and camera are the same, otherwise the two-way authentication will fail.
SNMP Port	The default is 161. You may change is as needed.

4. Click **Save**.

DNS

DNS (Domain Name System) is a globally distributed service that translates human readable domain names into numeric IP addresses, facilitating devices to access external servers or hosts through domain names.

Enter the preferred and alternate DNS server addresses. The camera will use the preferred IP address as the DNS server address. If the preferred DNS server is unavailable, the alternate DNS server will be activated.

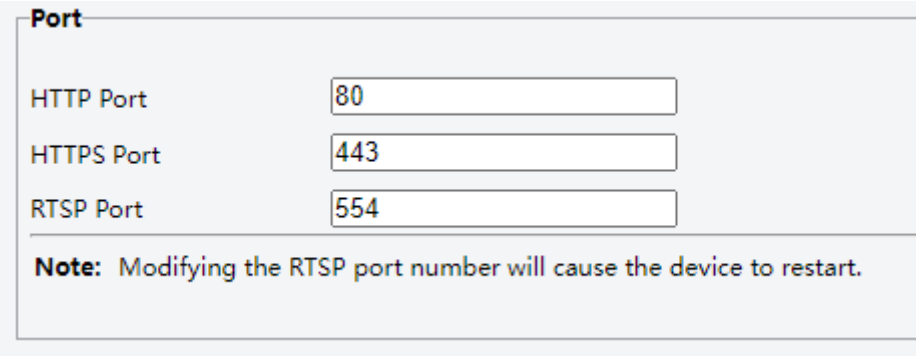


7.3.4 Network Port

Go to **Setup** > **Network** > **Network Port**.

Port

Set HTTP, HTTPS, and RTSP ports. Set the ports as needed when you visit the camera via the network.



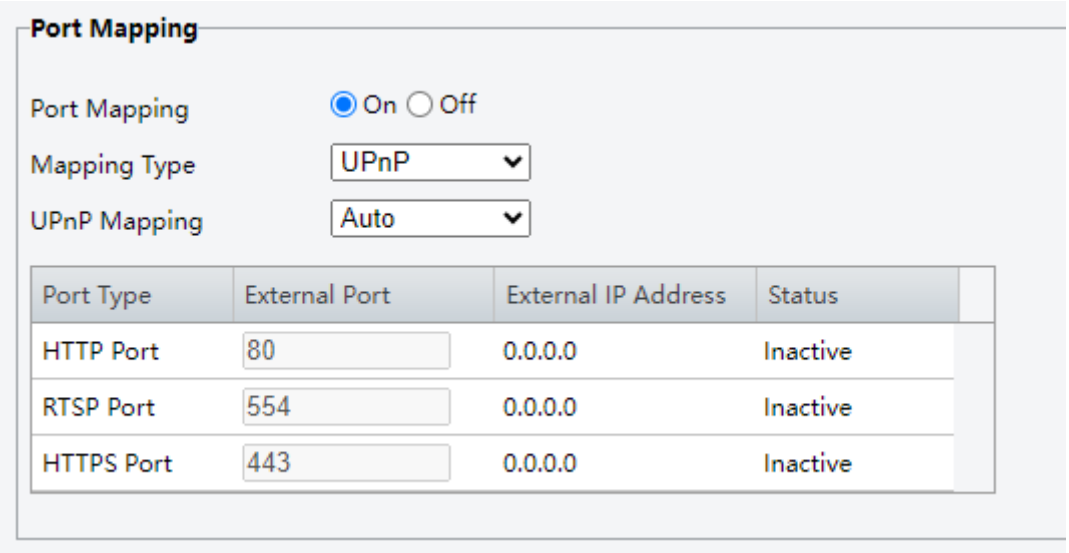
1. You can use the defaults or change them in case of port conflicts.

   Note: If the HTTP port number you entered has been used, a message "Port conflicts. Please try again." will appear. 23, 81, 82, 85, 3260, and 49152 have been assigned for other purposes and cannot be used. In addition to the above port numbers, the system can also dynamically detect other port numbers that are already in use.

   - HTTP/HTTPS Port: If you change the HTTP/HTTPS port number, then you need to add the new port number after the IP address when logging in. For example, if the HTTP port number is set to 88, you need to use http://192.168.1.13:88 to log in to the device.
   - RTSP Port: Real-Time Streaming Protocol port, enter an available port number.

2. Click **Save**.

Port Mapping

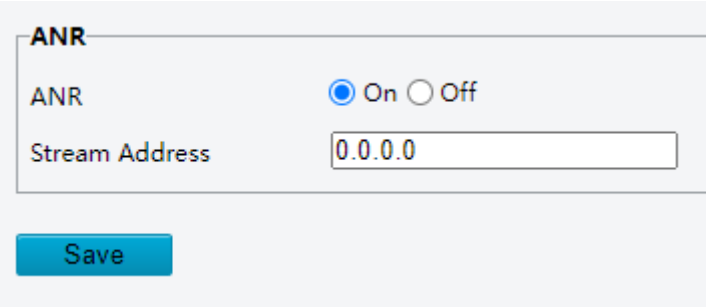


1. Enable **Port Mapping**.
2. Set the mapping type.
   - Auto: The external port numbers and external IP address are assigned automatically.
   - Manual: The external port numbers need to be set manually.
3. Click **Save**.

7.3.5 ONVIF

If the network connection between the device and the peer (stream receiving address) is disconnected, the device can store videos according to the configured recording schedule; and after the network connection is restored, the device can retransfer the video stored during the interruption period to the stream receiving address on the request of the peer.

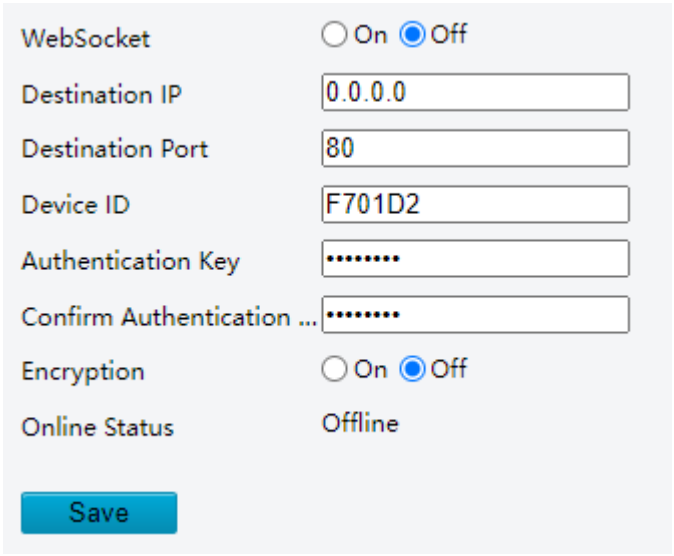
Go to **Setup** > **Network** > **ONVIF**.



7.3.6 WebSocket

WebSocket can connect your camera to a third-party platform and enable remote management of the camera from the third-party platform, including viewing device version and capabilities, control PTZ, and receive alarms.

1. Go to **Setup** > **Network** > **WebSocket**.



2. Configure the parameters.

Item	Description
WebSocket	Click **On**/**Off** to enable/disable WebSocket.
Destination IP	Enter the IP address of the third-party platform.
Destination Port	Enter the listener port of the third-party platform.
Device ID	It is the device's serial number by default. You can set it as required by following the rules prompt on the interface.
Authentication Key	Enter the authentication key used to connect the camera to a third-party platform. Make sure the authentication key configured on the camera and the third-party platform is the same.
Encryption	Encrypt via the SSL protocol. Enable encryption to enhance the security of data transmission. **Note:** If you first choose not to enable Encryption and then enable it after the camera is connected to the platform, encryption does not take effect immediately; it will take effect when the next time the camera is successfully connected to the platform.
Confirm Authentication	Confirm the password by entering it again.
Online Status	Check whether the device is successfully connected to the third-party platform.

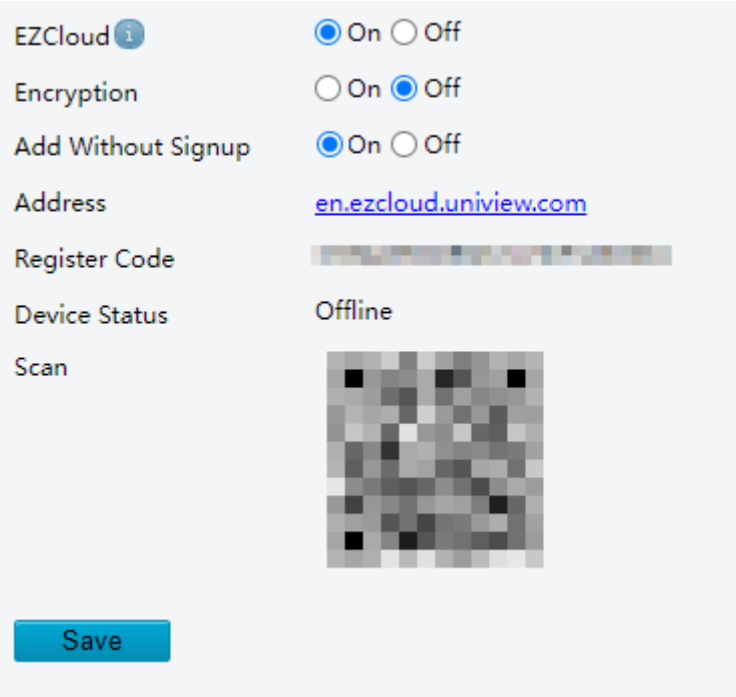
3. Click **Save**.

7.3.7 EZCloud

Add the camera to EZCloud so you can remotely access, monitor, and manage the camera.

You can add the device to EZCloud via the following methods.

Go to **Setup** > **Network** > **EZCloud**, and enable **EZCloud**.



Option 1: Add device on the UNV-Link app

1. Scan the QR code on the EZCloud page or search UNV-Link in the app stores to download and install the app.
2. Register an account and log in to the app.
3. Tap **Add Device** on the home screen.
4. Scan the register code on the camera or on the Quick Guide, and then tap **OK**.
5. Select a connection method according to the actual situation.
6. Follow the on-screen instructions to add the device.

Note: The actual operations may be slightly different, please follow the instructions in the app.

Method 2: Add device on the EZCloud website

1. Visit en.ezcloud.uniview.com using a web browser, and the login page appears.
2. Click **Sign Up** and follow the on-screen instructions to create an account.
3. Log in to the EZCloud.
4. Go to **Device Management** > **My Cloud Devices,** and click **Add**.

   The parameter description is shown below:

Item	Description
Device Name	Enter the device name as needed.
Register Code	Enter the register code.
Organization	Select an organization for your device. By default, the root organization is selected. You may add or delete organizations at **Organization Management** > **My Cloud Organizations**.

5. Click **OK**.
6. Click **Save**.

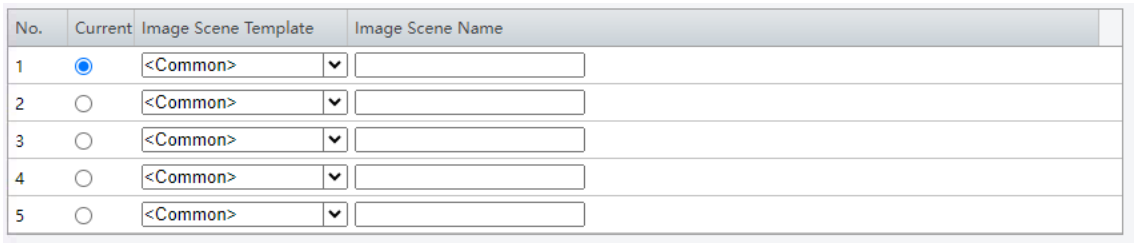
7. Check the device status.
   - EZCloud website: Check the device status at **Device Management** > **My Cloud Devices**.
   - Device Web: Check the device status at **Setup** > **Network** > **EZCloud**.

7.4 Video & Audio

7.4.1 Image

You need to complete scene configuration first, and then configure image parameters (image enhancement, exposure, smart illumination, focus, white balance). The image settings are saved automatically.

1. Go to **Setup** > **Video & Audio** > **Image**.
2. Configure scene parameters. Each scene corresponds to each image parameters. Up to 5 scenes are allowed to meet various scene requirements.

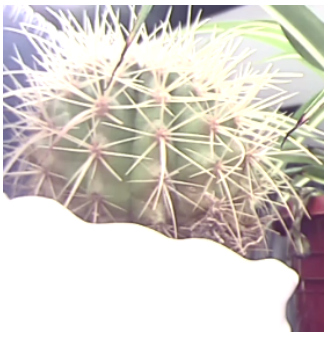
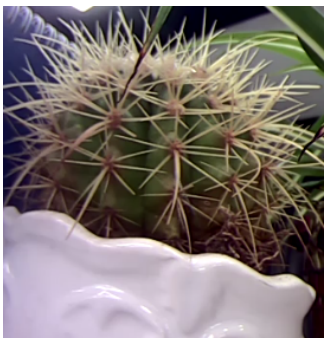
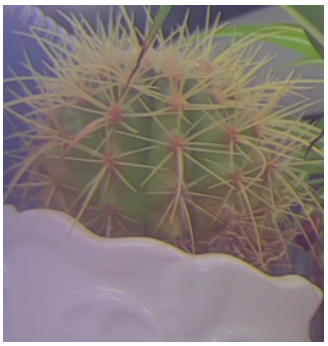
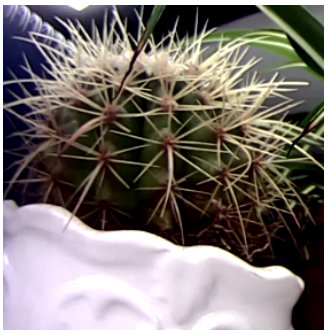
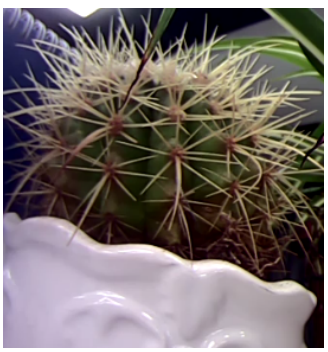


(1) ◉ means the scene is currently in use. To switch scenes when **Enable Auto Switch** is disabled, click ○ before the scene name, and the image settings will also switch to the corresponding image settings configured for the scene.

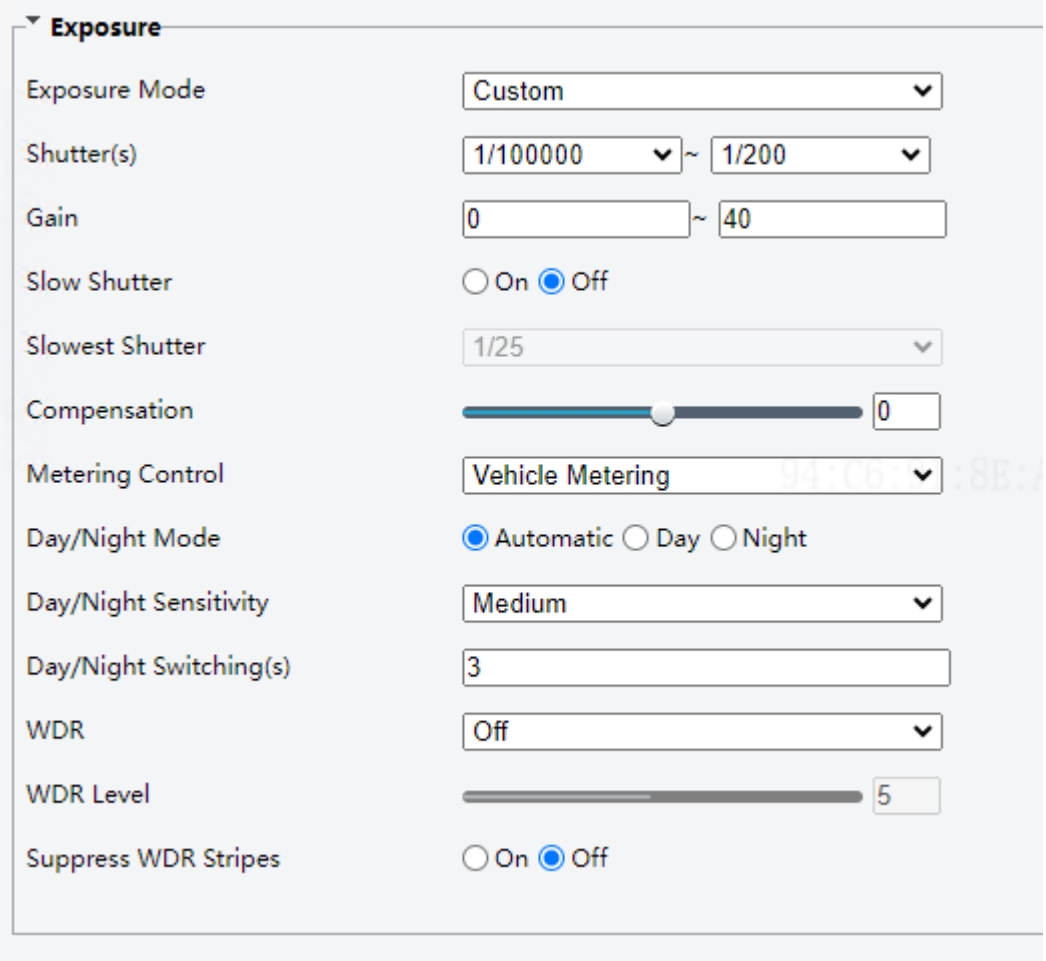
(2) Set the scene name. The device provides several predefined scene modes for different scenarios. After a scene mode is selected, image parameters are automatically switched, you can also adjust the parameters as needed.
   - Common: Recommended for outdoor scenes.
   - Road Highlight Compensation: Apply brightness compensation to the road scene to enhance the image, thereby improving the recognition accuracy that may be compromised by overly dark images.
   - Custom: Set a scene as needed.

3. Go to the **Image Enhancement** tab to configure the parameters. You can click **Default** in the upper-right corner to restore the default factory settings.

Parameter	Description
Brightness	The overall lightness or darkness of the image.

Parameter	Description
	 Low brightness  High brightness
Saturation	The intensity or vividness of colors in the image.  Low saturation  High saturation
Contrast	The black-to-white ratio in the image, that is, the gradient of color from black to white.  Low contrast  High contrast
Sharpness	The definition of edges in the image.  Low sharpness  High sharpness
2D Noise Reduction	Reduce noise by individually analyzing each frame, which may cause image blur.
3D Noise Reduction	Reduce noise by analyzing the difference between successive frames, which may cause image smearing or ghosting.

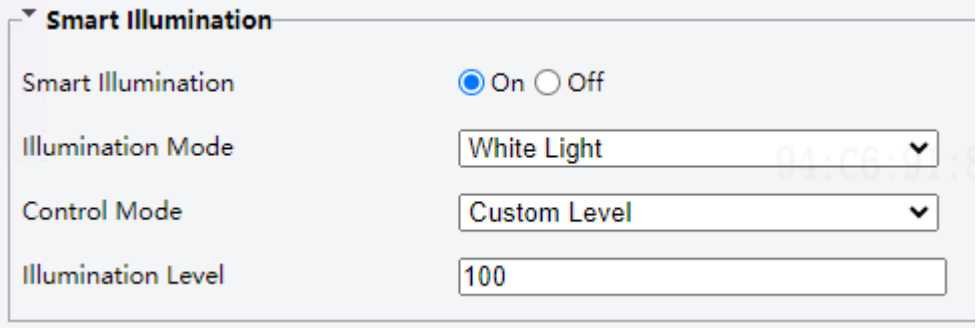
4. Go to the **Exposure** tab to configure the parameters. You can click **Default** in the upper-right corner to restore default factory settings.



Parameter	Description
Exposure Mode	Select the exposure mode from the drop-down list to achieve the desired exposure effect. • Automatic: The device automatically adjusts the exposure parameters based on the environment. • Custom: User can set exposure parameters as needed.
Shutter(s)	Shutter is used to control the light that comes into the lens. A fast shutter speed is ideal for scenes in quick motion. A slow shutter speed is ideal for scenes that change slowly. The default range is 1/100000 to 1/25. **Note:** • This parameter is configurable when **Exposure Mode** is set to **Custom**. • If **Slow Shutter** is disabled, the reciprocal of the shutter speed must be greater than the frame rate.
Gain	Control image signals so that the device can output standard video signals in different light conditions. **Note:** This parameter is configurable when **Exposure Mode** is set to **Custom**.
Slow Shutter	When enabled, the device can improve image brightness in low light conditions.
Slowest Shutter	Set the slowest shutter speed for exposure.
Compensation	Adjust the compensation value as required to achieve the desired image effect.

Parameter	Description
Metering Control	Set how the device measures the intensity of light. The default is **Center-Weighted Average Metering**. You can choose the mode as needed. • Center-Weighted Average Metering: Measure light mainly in the central part of the image. • Evaluative Metering: Measure light in the specified area of the image, suitable for scenes where the target and the background contrast widely. • Vehicle Metering: Applicable to vehicle driving scenarios. **Note:** This parameter is configurable when **Exposure Mode** is not set to **Manual**.
Day/night mode	• Automatic: The device automatically switches between day mode and night mode according to the ambient lighting condition to output optimum images. • Day: The device outputs high-quality images in daylight conditions. • Night: The device outputs high-quality images in low-light conditions.
Day/Night Sensitivity	Light threshold for switching between day mode and night mode. A higher sensitivity value means that the device is more sensitive to the change of light and is therefore more easily to switch between day mode and night mode. **Note:** This parameter is configurable when **Day/Night Mode** is set to **Automatic**.
Day/Night Switching(s)	Set the length of time before the camera switches between day mode and night mode after the switching conditions are met. **Note:** This parameter is configurable when **Day/Night Mode** is set to **Automatic**.
WDR	• On: The bright and dark areas on the image can be distinguished simultaneously. You need to set the WDR level manually. • Off: The camera displays the original image. **Note:** • Typical WDR scenes include: backlighting scenes with significant contrast (such as halls with insufficient lighting); counter-lighting scenes (such as toll booths); scenes with intense light sources. etc. • This parameter is configurable when **Exposure Mode** is set to **Automatic**.
WDR Level	When WDR is enabled, you can adjust the WDR level to improve image quality.
Suppress WDR Stripes	Suppress the stripes in the image caused by the flickering light in WDR mode. When enabled, the camera automatically adjusts the shutter and frequency to minimize stripes.

5. Go to the **Smart Illumination** tab to configure the parameters. You can click **Default** in the upper-right corner to restore the default factory settings.



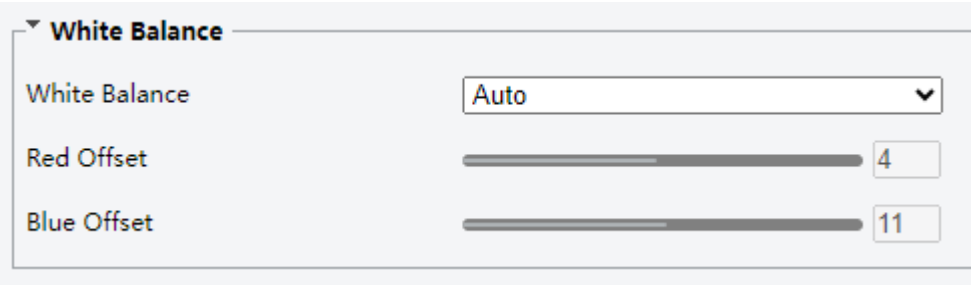
Parameter	Description
Illumination Mode	Use the default.

Control Mode	• Infrared
	  • Global Mode: The camera automatically adjusts illumination, and the illumination level cannot be adjusted.
	  • Overexposure Restrain: The illuminator is controlled by the day/night mode. The camera automatically adjusts illumination, and the illumination level cannot be adjusted.
	  • Custom Level: Default. The illuminator is controlled by the day/night mode.
	• White Light
	  • Custom Level: The illuminator is controlled by the day/night mode. The illumination level can be adjusted manually.
	  • Custom Level(Always On): The illuminator is not controlled by the day/night mode, but by the high/low beam settings of the headlights.

Illumination Level	The greater the value, the higher the intensity. 0 is off.

6. Go to the **White Balance** tab to configure the parameters. You can click **Default** in the upper-right corner to restore the default factory settings.

   White Balance is used to adjust red gain and blue gain of the entire image under different color temperatures so as to output images that best suit human eyes.



Parameter	Description
White Balance	• Auto/Auto 2: The device automatically adjusts the red and blue gains according to the lighting conditions. If there are still color casts in **Auto** mode, try **Auto 2** mode. • Outdoor: Recommended for outdoor scenes where the color temperature varies widely. • Fine Tune: Allows user to manually adjust red and blue offsets. • Sodium Lamp: Automatically adjust the red and blue gains for optimal color reproduction in sodium light sources. • Locked: Keep the current color temperature.
Red Offset	When **White Balance** is set to **Fine Tune**, drag the slider or set the value to adjust the red offset.
Blue Offset	When **White Balance** is set to **Fine Tune**, drag the slider or set the value to adjust the blue offset.

7. Repeat the previous steps to complete all scene parameters and corresponding image settings.

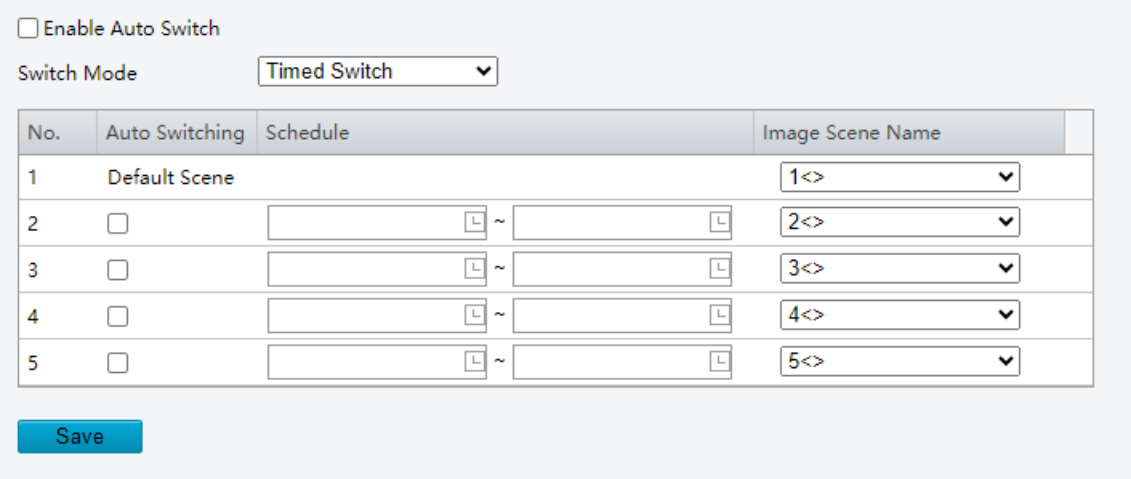
7.4.2 Image Scene Switch

Select whether to add the scene to the auto switching list (include the default scene). When enabled, if the conditions for switching to a non-default scene are met, the camera will automatically switch to the scene; otherwise, the camera uses the default scene. When disabled, the camera uses the currently selected scene.

Note:

- If multiple non-default scenes meet the switching condition at the same time, the device will switch to the scene with the smallest number (starting from 1 to 5).
- When **Auto Switch** is enabled, all the scene parameters cannot be configured.
- When **Auto Switch** is enabled, the current scene will be automatically switched based on the settings.

1. Go to **Setup** > **Video & Audio** > **Image Scene Switch**.



2. Select the **Enable Auto Switch** checkbox.
3. Return to the **Scenes** tab on the **Image** page.
4. Select ☐ before the desired scene to add it to the auto switching list.
5. Set the schedule. Up to 4 periods are allowed, and the periods must not overlap. If both the start time and end time are 0, the settings do not take effect.
6. Select the corresponding number for each scene to be enabled.

7.4.3 Video Encoding

1. Go to **Setup** > **Video & Audio** > **Video Encoding**.

2. Select a capture mode for your camera.

   After you change the capture mode, the encoding settings will be reset to defaults and some models of cameras will restart.

3. Set stream parameters.

   At present, up to 3 streams are supported for each channel, and the streams are independent of each other and can be set with different resolutions, frame rates, video compression formats, etc. Only the main stream supports full resolution.

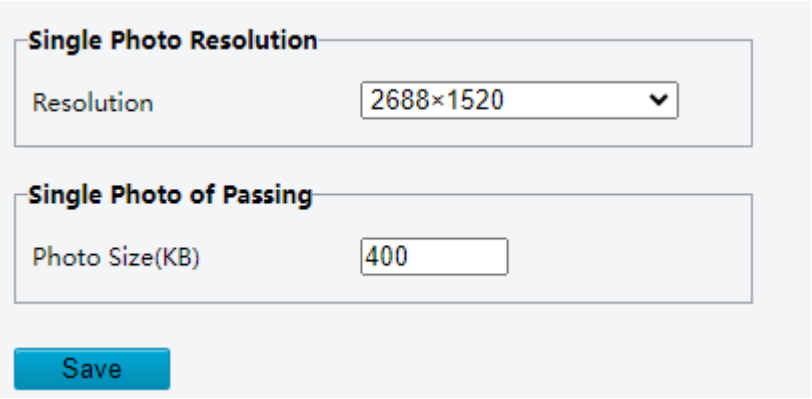
Item	Description
Video Compression	Select a video compression standard for your camera: H.265 or H.264. The bit rate restores to the default when you switch between H.264 and H.265.
Resolution	Select a video resolution for your camera. The higher the resolution, the clearer the image.
Frame Rate(fps)	The number of frames per second. Choose a frame rate from the drop-down list. **Note:** To ensure image quality, the frame rate shall not be greater than the reciprocal of the shutter speed.
Bit Rate(Kbps)	Set the bit rate. Range: 128 to 16384, integer only. **Note:** The bitrate range may vary with camera model.
Bitrate Type	Select the bitrate type. • CBR: The device keeps a specific bit rate by varying the quality of video streams. • VBR: The device keeps the quality of video streams as constant as possible by varying the bit rate.
Image Quality	Adjust the image quality by dragging the slider. It is configurable when **Bitrate Type** is set to **VBR**. The closer the slider is to **Quality**, the higher the bit rate, and the higher the image quality. The closer the slider is to **Bit Rate**, the lower the bit rate, and the image quality will be affected.
I Frame Interval	Set the number of frames between I-frames. A shorter interval presents better image quality but consumes more bandwidth and storage.
GOP	Group of Pictures, defines the basic pattern of the video stream encoded with I and P frames.
Smoothing	Set the smoothness of the video stream. Drag the slider to choose whether smoothness or clarity takes precedence. **Note:** Smoothing is recommended for fluent video in a poor network environment.
U-Code Smart Encoding	Select the U-Code mode, including **Off**, **Basic Mode**, and **Advanced Mode**. • Basic Mode: The bit rate is reduced by about 25%. • Advanced Mode: The bit rate is reduced by about 50%.

4. (Optional) Set other streams as needed. To enable third stream, please enable sub stream first. Set stream parameters settings for details.
5. Click **Save**.

7.4.4 Image Encoding

Set the snapshot parameters, and then set the scheduled snapshot as needed.

1. Go to **Setup** > **Video & Audio** > **Image Encoding**.



2. Set the resolution and maximum photo size. The greater the value, the higher the image quality.
3. Click **Save**.

7.4.5 ROI

When enabled, the system ensures image quality for the specified areas on the image first at low bit rate.

1. Go to **Setup** > **Video & Audio** > **ROI**.

2. Set ROI areas.

   (1) Click + to add an ROI area. The area is a rectangle by default. Up to 8 areas are allowed.

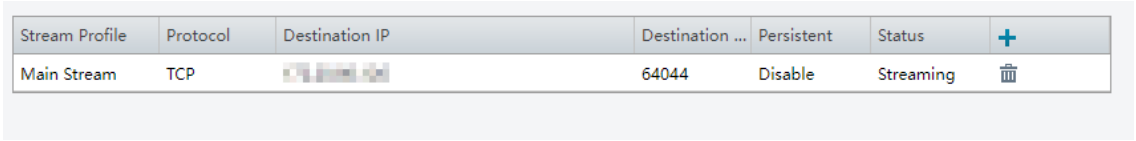
   (2) Adjust the area as needed.

   - To redraw the detection area, click on the image and drag to draw a new one.
   - To adjust the size and position of the area, point to a handle of the area and drag to resize it. Point to any position of the area and drag it to the desired position.

7.4.6 Media Stream

Media streams are a type of media that transmit audio and video content in real-time via data streams. The media stream page displays third-party clients, such as a PCs or other servers, that are currently receiving data transmitted from the camera. After the media stream is added, the camera can transmit the collected images, audio, or video to a designated IP address or port using the specific transmission protocol.

1. Go to **Setup** > **Video & Audio** > **Media Stream**.



2. Click + to add a media stream.
3. Complete the media stream settings.

Item	Description
Stream Profile	Choose main stream, sub stream, or third stream. The device will transmit media contents to a third-party client.
Destination IP	Enter the IP address of the device receiving media streams.
Protocol	The default protocol is RTMP. The device transmits data to a third-party client through the specific protocol.
Persistent	Set whether to automatically establish the configured media stream after restart.

4. Click **OK**.

7.4.7 RTSP Multicast Address

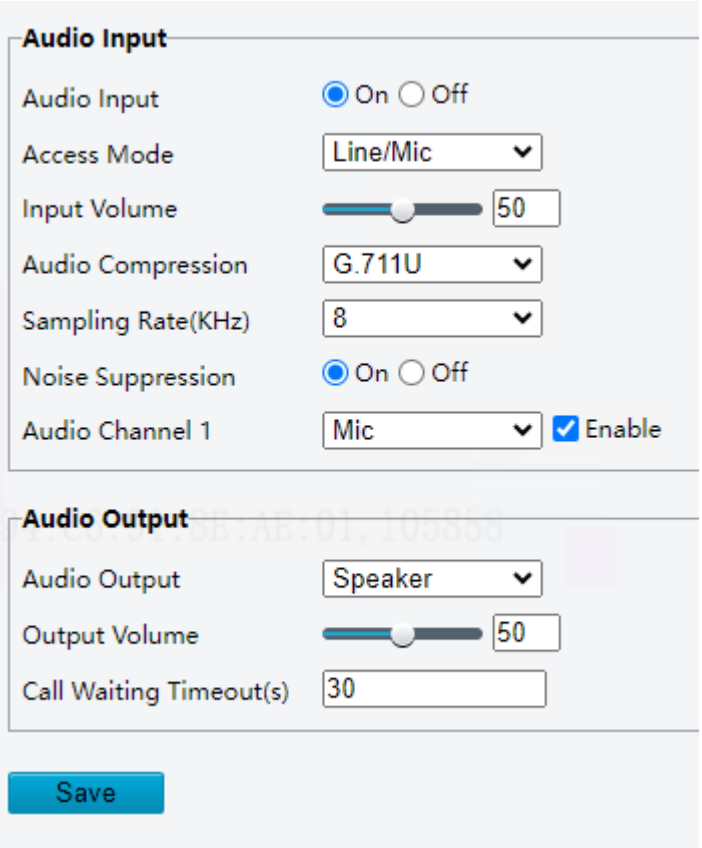
RTSP multicast allows third-party players to request RTSP multicast media streams from the camera through the RTSP protocol.

1. Go to **Setup** > **Video & Audio** > **RTSP Multicast Address**.

2. Set the multicast address and port number (multicast address range: 224.0.1.0 to 239.255.255.255, port number range: 0 to 65535).
3. Click **Save**.

7.4.8 Audio

1. Go to **Setup** > **Video & Audio** > **Audio**.



2. Set audio input parameters.

Item	Description
Audio Input	Enable **Audio Input**. **Note:** If audio is not needed, it is recommended to turn it off to improve camera performance.
Access Mode	Select the audio input mode, including **Line/Mic** and **RS485**. Some cameras connect to a sound pickup via a RS485 cable. You need to set the access mode to sound pickup.
Input Volume	Drag the slider or input a value to set the input volume.
Audio Compression	Choose the audio compression format: **G.711U**, **G.711A**, or **AAC-LC**.
Sampling Rate(kHz)	Choose a sampling rate: **8kHz** and **16kHz**. The higher the sampling rate, the better the sound quality.
Noise Suppression	Reduce noise in audio to improve audio output quality.
Audio Channel 1	Select the **Enable** checkbox to enable audio input for the channel.

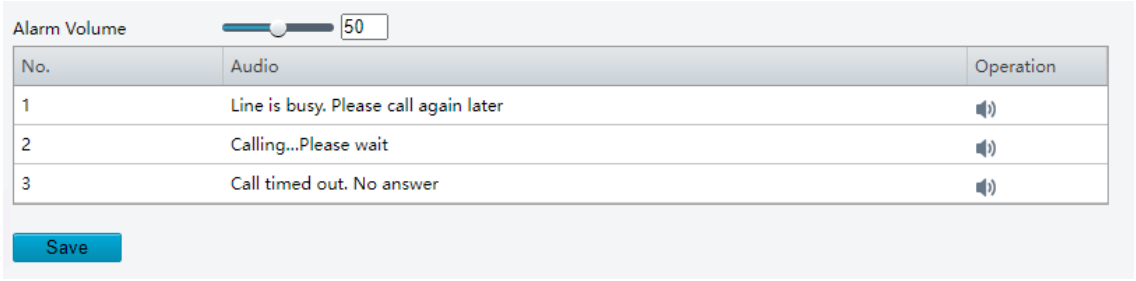
3. Set audio output parameters.

Item	Description
Audio Output	A speaker or an earphone needs to be connected.
Output Volume	Drag the slider or input a value to set the output volume.

4. Click **Save**.

7.4.9 Audio File

1. Go to **Setup** > **Video & Audio** > **Audio File**.



2. Set audio file parameters.

Item	Description
Alarm Volume	Drag the slider or input a value to set alarm volume.
Alarm Audio File	There are 3 system audio files. Click to play the audio. **Note:** Built-in audio files may vary depending on the smart functions supported by the device.

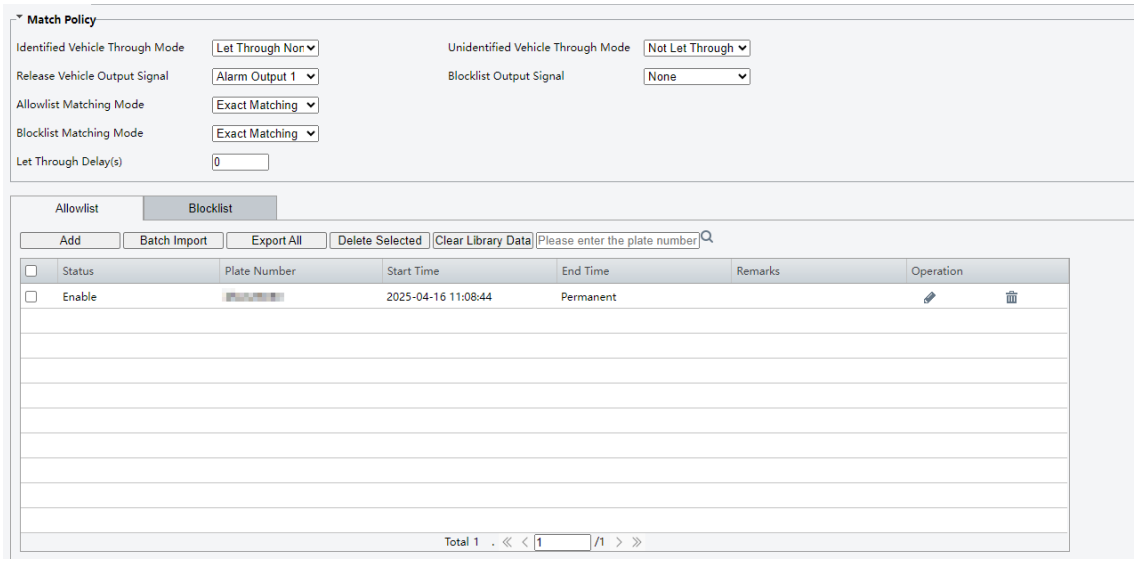
3. Click **Save**.

7.5 Vehicle List

Configure the vehicle list and entry policy if there are restrictions on automatic vehicle entry.

When the camera is operating independently, it determines whether to automatically let vehicles through based on the vehicle list and release strategy on the camera end. When the camera connects to the server, both the camera and the server can control vehicle release.

1. Go to **Setup** > **Vehicle List**.



2. Set the match policy. You can control which vehicles are automatically released.

- Identified Vehicle Through Mode: The vehicle through modes for different list types are shown below. They are applied when the camera is running independently, the camera is offline after connecting to the server and **Let Through Allowlist List When Offline** is disabled on the server, or different through modes are configured for identified vehicles.

  Note:

  - The camera allows all vehicles to pass when it is connected to the server and is offline, and **Let Through Allowlist List When Offline** is enabled on the server.
  - The vehicles on the allowlist can pass when the camera-connected server via HTTP protocol is effective and the camera is offline.

Vehicle/Match Policy	Let Through All	Let Through Allowlist List	Let Through Allowlist List When Offline	Let Through Blocklist List
Allowlist List	Let Through	Let Through	Let Through	Let Through
Blocklist List	Let Through	Not Let Through	Not Let Through	Not Let Through
Not in Allowlist/ Blocklist	Let Through	Not Let Through	Not Let Through	Let Through

- Unidentified Vehicle Through Mode

Mode	Policy
Let Through	The unlicensed vehicles identified by the camera will be automatically allowed to pass.
Not Let Through	The unlicensed vehicles identified by the camera will be denied access

- Output Signal: By default, the alarm output 1 controls the gate to open and the alarm output 2 controls the gate to close. Therefore, **Release Vehicle Output Signal** is **Alarm Output 1** and **Blocklist Output Signal** is **Alarm Output 2** by default. Please keep the defaults. The two items are available only when the camera controls vehicle access.
- Allowlist Matching Mode/Blocklist Matching Mode

Parameter	Description
Exact Matching	Default option. In this mode, the vehicle can only be recognized as a listed vehicle when the captured plate number matches exactly with that in the allowlist or blocklist.
Matching	Allowed mismatched character count: Three options: 0, 1, and 2, corresponding to the number of digits allowed to be mismatched in the license plate. The captured plates within this range are all recognized as vehicles in the whitelist or blocklist.

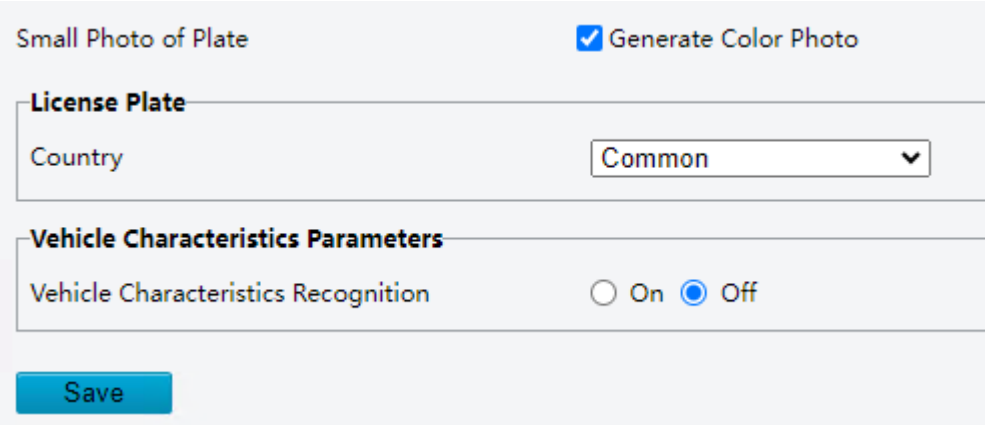
- Let Through Delay (s): It is 0 by default and is effective when the camera runs independently. It must be 0 unless there is a delay in opening the gate.

3. Set the allowlist.
   - Add: Click **Add** to add the lists on by one or click **Batch Import** to import lists.

     Note: If you do not set the start time and end time for the added allowlist, the plate list will fail to import.
   - Edit: Click to edit the plate information except the plate number.
   - Click to delete a list; or select the list(s) you want to delete and click **Delete Selected**.
   - Clear: Click **Clear Library Data** to delete all data from the list.
4. See the operations above to set the blocklist.

7.6 Intelligent Configuration

1. Go to **Setup** > **Smart** > **Intelligent Configuration**.



2. (Optional) Disable **Generate Color Photo**. It is recommended to enable this feature. When enabled, a closeup image of the license plate will be automatically generated upon a snapshot is captured, and displayed in the top-right corner of the live view page. If the platform subscribes to the messages, the closeup image will also be pushed to the platform.
3. Choose the country where the license plate is applicable.
4. Enable/disable **Vehicle Characteristics Recognition** according to the actual on-site requirements. When enabled, the vehicle characteristics can be recognized, including vehicle model, brand, logo, and color, and overlaid on the vehicle's composite photo along with OSD.
5. Click **Save**.

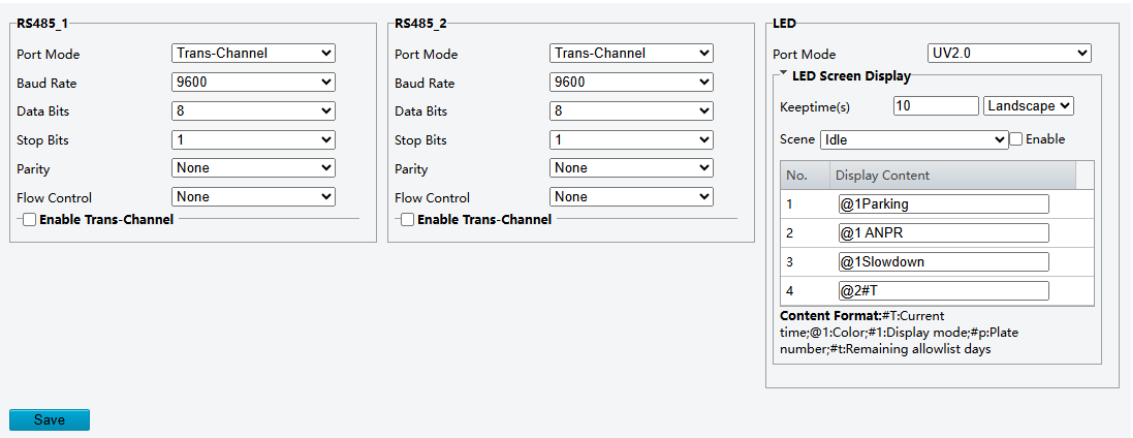
7.7 External Device

7.7.1 Serial Port

Set RS485 serial port and LED screen display parameters.

- RS485 serial port: Enable transparent data transmission and OSD overlay with third-party devices. The serial port parameters must match those of the connected serial device.
- LED Screen Display: This function is available on devices that support LED screen connection.

1. Go to **Setup** > **External Device** > **Serial Port**.



2. Set RS485_1 parameters.

Item	Description
Baud Rate	Data transmission speed (unit: bits per second). The greater the value, the faster the transmission speed, and the shorter the transmission distance. Usually the default value is applicable.
Data Bits	The actual number of data bits in a group of data packets. Usually the default value is applicable.
Stop Bits	Indicates the end of transmission of a group of data. Usually the default value is applicable.

Item	Description
Parity	Used to check whether the received data bits are erroneous. You can choose **None**, **Odd-Parity Check**, or **Even-Parity Check**.
Flow Control	Used to control data transmission to prevent data loss.
Enable Trans-Channel	Optional. The camera establishes transparent data transmission with third-party device via the RS485 serial port. Enter the destination IP address and port number (i.e., the IP address and port number of the third-party device for transparent channel connection).

3. Set RS485_2 parameters by referring to the steps above.
4. Set LED parameters.

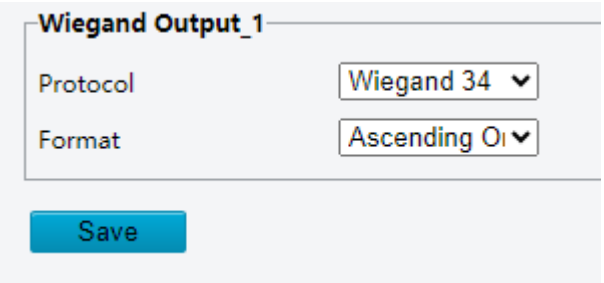
Item	Description
Port Mode	Default: UV2.0
Keeptime(s)	Display duration of recognized license plate information.
Scene	5 scenes are available, including **Idle**, **Allowlist Vehicle Passing**, **Blocklist Vehicle Passing**, **Temporary Vehicle**, and **Unlicensed Vehicle**. The LED display will show the preset information when entering the corresponding scene. (1) Select a scene. (2) Select the **Enable** checkbox; otherwise, the content display will fail in corresponding scene. (3) Configure the display parameters. See the description below for content format. (4) Follow the first three steps to complete display content configuration for all scenes.

5. Click **Save**.

7.7.2 Wiegand Interface

The Wiegand interface can be used to connect external IC or CPU card readers.

1. Go to **Setup** > **External Device** > **Wiegand Interface**.



2. Set Wiegand port parameters.

Parameter	Description
Protocol	Choose Wiegand 26 or Wiegand 34. Default: Wiegand 34. • Wiegand 26: Reads 3-byte card numbers. • Wiegand 34: Reads 4-byte card numbers. None: Disable the Wiegand card reading function.
Format	The card number read by our card readers is in ascending order. Two options are available: • Ascending Order (default): Used when the sequence of card number read by the external card reader is the same as the sequence of card number read by our card readers.

Parameter	Description
	• Descending Order: Used when the sequence of card number read by the external card reader is opposite to the sequence of card number read by our card readers.

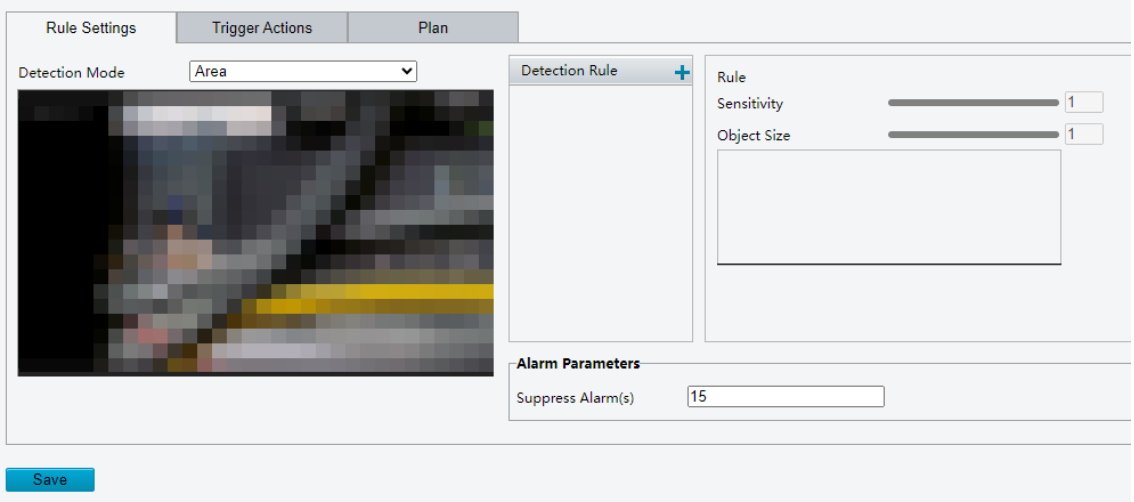
3. Click **Save**.

7.8 Events

7.8.1 Motion Detection

Motion detection detects motions in specified grids on the image. An alarm is reported when detection rules are triggered.

1. Go to **Setup** > **Events** > **Motion Detection**.

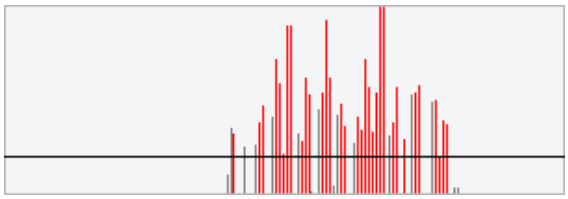


2. Choose the detection mode.
   - Area Detection
     (1) Click + to add a detection rule. A default rectangle detection appears on the image. Up to 4 detection rules are allowed.

     (2) Adjust the detection box as needed.
       - To adjust the size and position of the area, point to a handle of the area and drag to resize it. Point to any position of the area and drag it to the desired position.
       - Click anywhere on the image, and then drag to draw a new area.

     (3) Set detection rules.

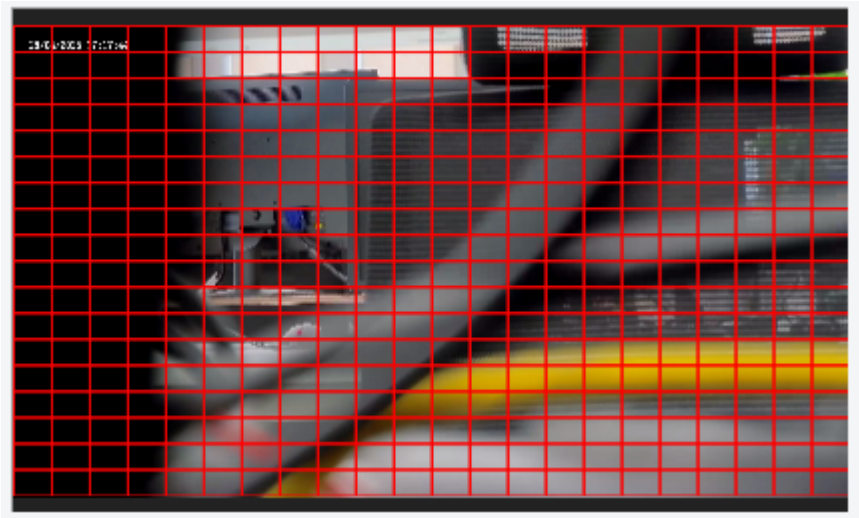
Item	Description
Sensitivity	Set the sensitivity by dragging the slider.

Item	Description
	The higher the sensitivity, the higher the detection rate, and the more likely false alarms will occur. Set based on the scene and your actual needs.
Object Size	Drag the slider to set object size. • The ratio of the size of the detected object to the size of the detection area. An alarm is triggered when the ratio reaches the set value. To detect motion of small objects, you need to draw a small detection area separately. • Motion detection results of the current detection area are shown below in real time. The red means motions that have triggered a motion detection alarm. The height of the lines indicates the extent of motion. The density of the lines indicates the frequency of motion. The higher a line, the greater the extent. The denser the lines, the higher the frequency. 

(4) Set alarm parameters. Set **Suppress Alarm** to avoid receiving the same alarms within a certain length of time (alarm suppression time). For example, alarm suppression time is set to 5s, after an alarm is reported:

- If no motion is detected within the next 5s, new alarms can be reported after 5s when the alarm suppression time (5s) is over.
- If motion is detected within the next 5s, the alarm suppression time recounts from the time of the last alarm, and new alarms can be reported when the alarm suppressions time (5s) is over.

- Grid Detection



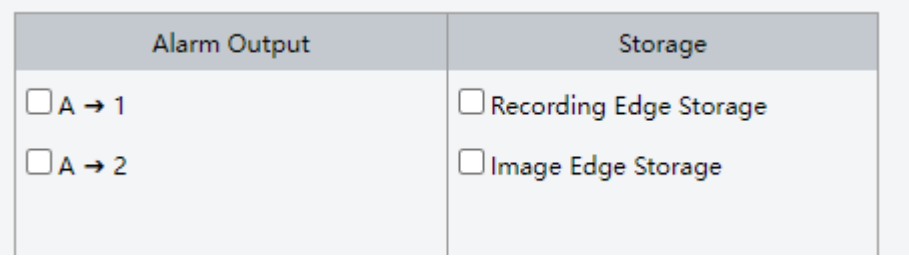
(1) Set grid detection areas.

(2) Adjust grid detection areas as needed.

- Click to clear the grid; or click and drag on grid areas to erase grids.
- Redraw:
  - Click on a grid vertex and drag to clear grids.
  - Click to draw a grid  ; click for multiple times to form irregular detection areas; or click and drag the draw the rectangle grid area.

(3) Set the sensitivity and alarm parameters. See the description in area detection.

3. Enter the **Trigger Actions** page. Configure alarm actions triggered by the detection rule to alert user or the specified people.



- Alarm Output: Connect the external alarm output devices, such as alarm lights and alarm bells, etc., to the camera's ALARM OUT interfaces. The camera triggers alarm output devices when an event occurs.

  A→1: A refers to the ALARM OUT interfaces on the camera, 1 means the first ALARM OUT interface. Likewise, A→2 means the second ALARM OUT interface on the camera. The number of ALARM OUT interfaces may vary with camera model. See the device datasheet for specifications.

  Please set Alarm Output first, and enable the alarm interface as needed.

- Storage
  - Recording Edge Storage: When an alarm is triggered, the camera automatically saves recordings to the preset path.
  - Image Edge Storage: When an alarm is triggered, the camera automatically saves images to the preset path.

4. Enter the **Plan** page. The default arming schedule is 24/7. The following two ways are available.

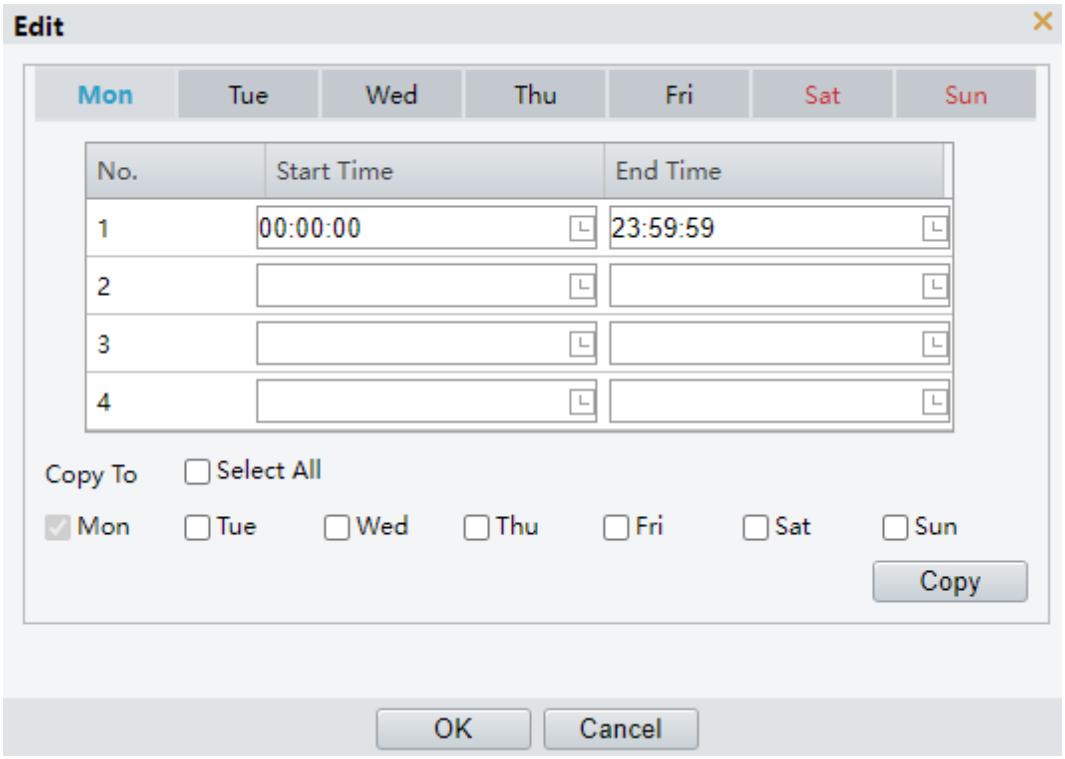
- Use the blue and white grids

  Click **Unarmed**, and click on the blue time grids to disable arming.

  Click **Armed**, and click on the white time grids to enable arming.

- Use the **Edit** button

  (1) Click **Edit**. The **Edit** page appears.



  (2) Set the time periods for the current day. Up to 4 time periods are allowed and periods cannot overlap.

  (3) Repeat the above steps and complete the settings for other six days. To apply the current settings to other days, select the check box(es) for the days and then click **Copy**.

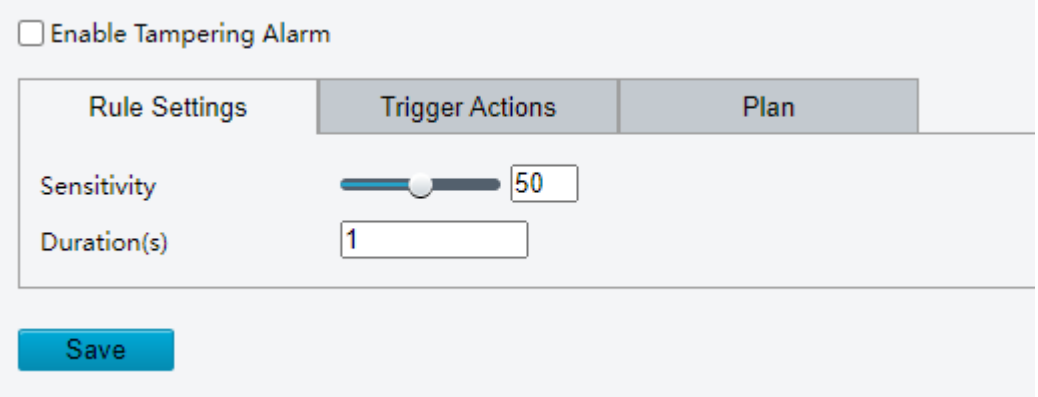
  (4) Click **OK** to save the arming schedule; click **Cancel** to exit the arming schedule settings.

5. Click **Save**.

7.8.2 Tampering Alarm

The camera triggers a tampering alarm after the lens is blocked for a certain length of time.

1. Go to **Setup** > **Events** > **Tampering Alarm**.

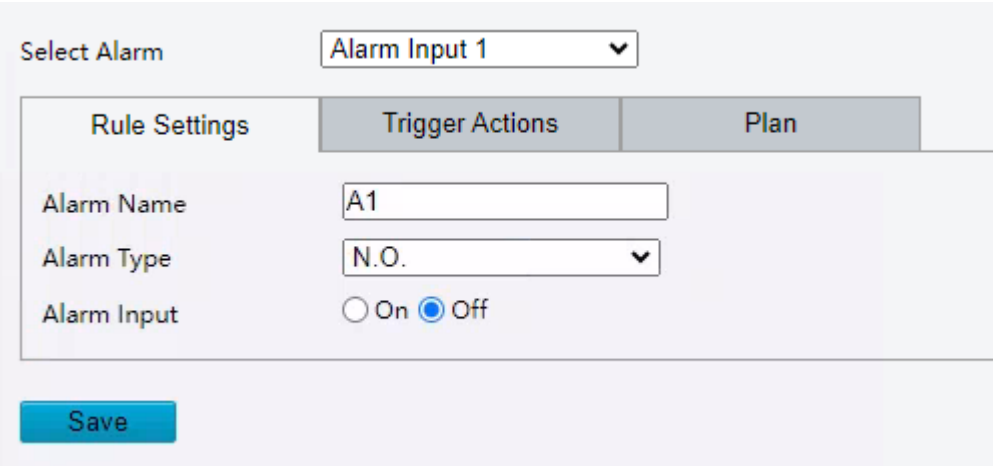


2. Select the **Enable Tampering Alarm** checkbox.
3. Drag the slider to adjust the sensitivity. The higher the sensitivity level, the higher the detection rate, and the higher the false alarm rate. Set based on the scene and your actual needs.
4. Set the duration of lens blocking. The camera reports an alarm when the duration of lens blocking exceeds the set value.
5. Set the alarm-triggered actions and arming schedule. See Motion Detection for details.
6. Click **Save**.

7.8.3 Alarm Input

The corresponding actions will be triggered when the alarm input is detected.

1. Go to **Setup** > **Events** > **Alarm Input**.



2. Choose an alarm input port from the drop-down list.

   The number of alarm inputs available may vary with camera model. For example, if the camera has two alarm inputs on the tail cable, you can configure alarm input 1 and alarm input 2 separately.

3. Set alarm input parameters.

Item	Description
Alarm Name	Set as needed.
Alarm Type	Set the alarm type according to the alarm input device. • If the alarm input device is normally open (N.O.), choose **N.C.**. • If the alarm input device is normally closed (N.C.), choose **N.O.**.

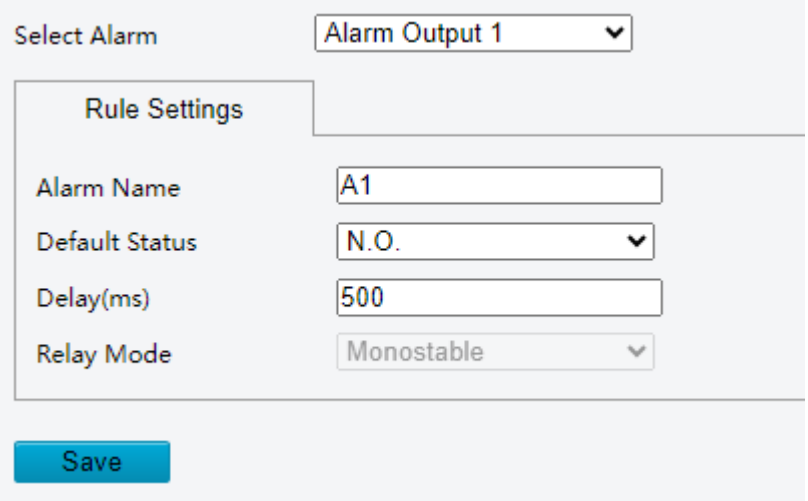
Item	Description
Alarm Input	Enable **Alarm Input**.

4. Drag the slider to adjust detection sensitivity. The higher the sensitivity, the higher the detection rate, and the more likely false alarms will occur. Set based on the scene and your actual needs.
5. Set the alarm-triggered actions and arming schedule. See Motion Detection for details.
6. Click **Save**.

7.8.4 Alarm Output

The corresponding actions will be triggered when the alarm output is detected.

1. Go to **Setup** > **Events** > **Alarm Output**.



2. Choose an alarm output port from the drop-down list. The number of alarm outputs available may vary with camera model.
3. Set alarm output parameters.

Item	Description
Alarm Name	The default name is the alarm output channel ID. You can rename it as needed.
Default Status	Choose the default status. The default is **N.O.**. • If the external alarm device is normally open (N.O.), choose **N.O.**. • If the external alarm device is normally closed (N.C.), choose **N.C.**.
Delay(s)	The duration of alarm output after the alarm is triggered. Set it as needed.
Relay Mode	Choose the relay mode. The default is **Monostable**. • Monostable: The circuit can only remain in one stable state. When a trigger pulse is applied, the circuit switches to another state, and then automatically switches back to the original stable state. The circuit will repeat the same actions when the next trigger pulse arrives. • Bistable: The circuit can remain in two stable states. When a trigger pulse is applied, the circuit switches to another state, and remains in this state after the trigger pulse is removed. When the next trigger pulse is applied, the circuit switches back to the other stable state and remains in that state. **Note:** Set relay mode to better adapt to third-party alarm devices such as alarm lights. Please set the relay mode according to the trigger mode of the third-party alarm device.

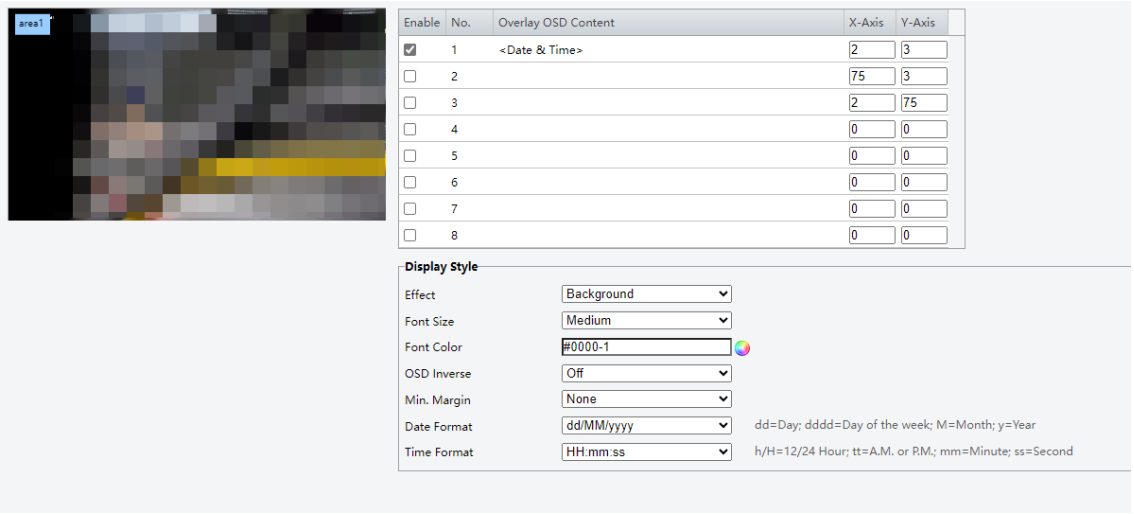
4. Click **Save**.

7.9 OSD

7.9.1 Live View

On Screen Display (OSD) refers to characters overlaid on live video, allowing date, time, or other customized contents.

1. Go to **Setup** > **OSD** > **Live View**.



2. Configure OSD displayed on the live video. Up to 8 OSDs are allowed.

   (1) Select the checkboxes in the **Enable** column to overlay the corresponding OSD contents on live video.

   (2) Select OSD content you want to overlay from the **Overlay OSD Content** column.

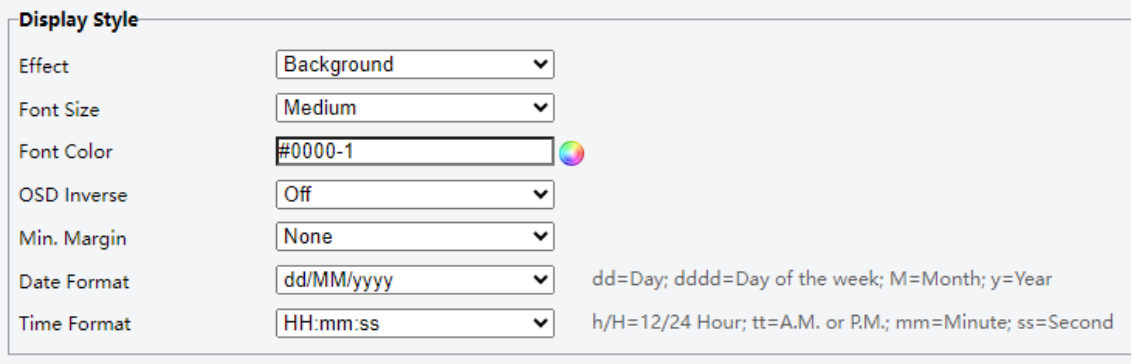
   - Custom: Customizes the OSD contents.
   - Date & Time: Displays the current date and time of the camera according to the set format (content style), for example, Thursday, 25 August, 2022 20:04.
   - Zoom: Displays the zoom information of the PTZ, for example, Z: 1.00X.
   - Time: Displays the current time of the device.
   - Date: Displays the current date of the device.
   - License Plate: Displays the pass-thru plate number and its pixel data in real time.

   (3) Set the exact position of the OSD.

   The top left corner of the image is the origin (0, 0), the horizontal axis is the X-axis, and the vertical axis is the Y-axis. Enter the X and Y coordinates to set the horizontal and vertical axis individually.

3. Set the OSD display style.

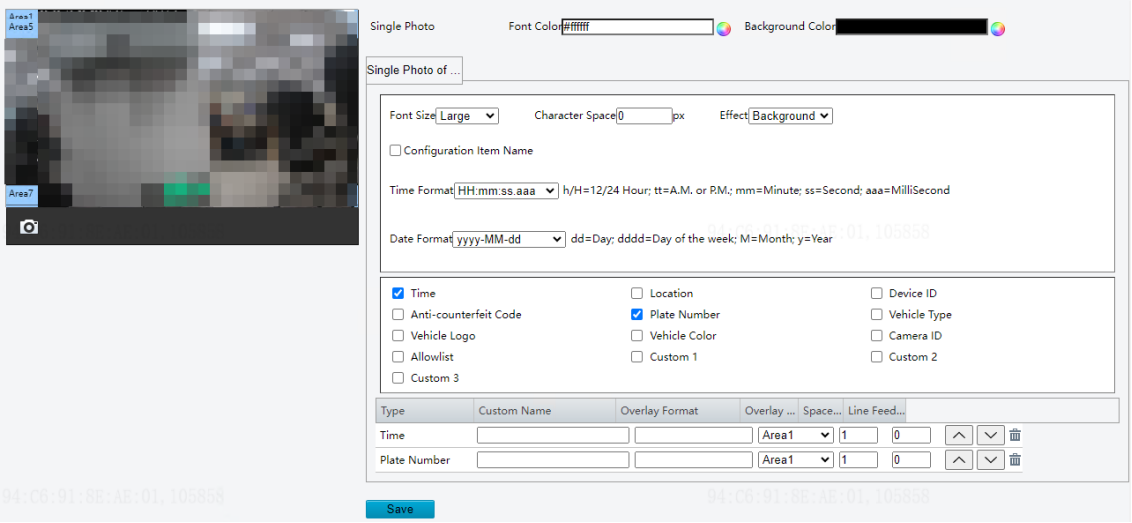


4. Complete the other OSD configurations.

7.9.2 Photo

Configure OSD displayed on the photo.

1. Go to **Setup** > **OSD** > **Photo**.

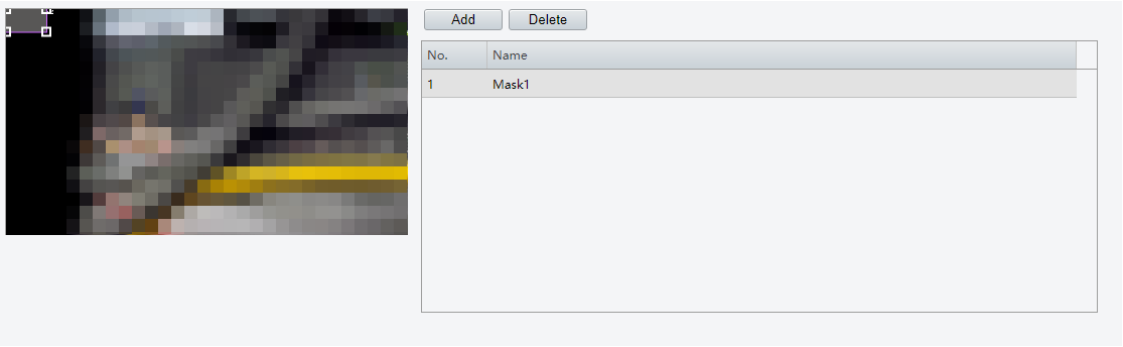


2. Set the font color, background color, font size, character space, etc.
3. Select the information to be overlaid on the photo. **Time** and **Plate Number** are enabled by default. The following takes **Device ID** as an example.
   (1) Select the **Device ID** checkbox.
   (2) (Optional) Set the custom name and overlay format.
   (3) Choose the overlay area. Up to 8 OSDs are allowed, corresponding to Area 1 to Area 8.
   You can drag the area name on the left live view page to adjust the OSD position.
   (4) Set **Space Count** and **Line Feed Count**. 0 means no line break.
   (5) You can click  to rearrange the order of OSDs if multiple OSDs are overlaid on the same area.
   (6) To delete an OSD, click  or clear the corresponding checkbox.
4. Click **Save**.

7.9.3 Privacy Mask

Privacy mask is used to cover certain areas on the image for privacy, for example, ATM keyboard. When a PTZ camera rotates and zooms, the privacy mask moves and zooms with the camera and the masked area is always covered.

1. Go to **Setup** > **OSD** > **Privacy Mask**.



2. Click **Add** to add a privacy mask. The privacy mask is a rectangle by default.
3. Adjust the mask as needed.
   - To adjust the size and position of the area, point to a handle of the area and drag to resize it. Point to any position of the area and drag it to the desired position.

- Click any position on the left live view page and drag to draw an area.

8 Maintenance

8.1 Maintenance

8.1.1 Maintenance

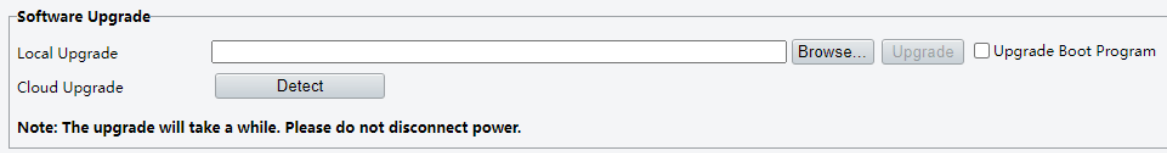
Note:

- Software upgrade, device restart, restoration to defaults, configuration import, or person library import will restart the camera.
- Restarting the camera will interrupt the ongoing services. Please handle with caution.

Go to **Maintenance** > **Maintenance** > **Maintenance**.

Software Upgrade

Local upgrade and cloud upgrade are available.



Note:

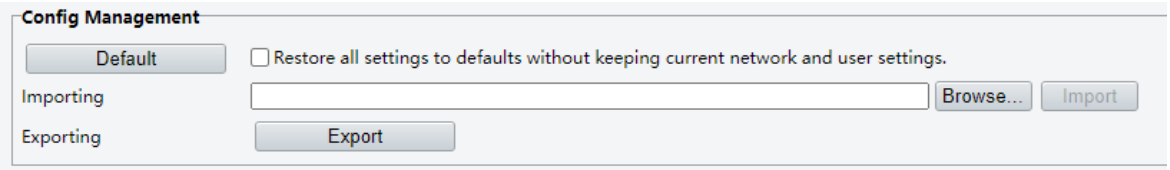
- Make sure the upgrade file matches the device; otherwise, unexpected problems may occur.
- The version file is a .zip file that includes all the upgrade files.
- Power must be connected throughout the upgrade.

- Local Upgrade
  1. Click **Browse**, and locate the upgrade file.

     (If applicable) select **Upgrade Boot Program** to upgrade the boot program.
  2. Click **Upgrade**. The camera will restart automatically after the upgrade is completed and the login page will appear.
- Cloud Upgrade: Click **Detect** to check for new versions. You can perform a cloud upgrade if a new version is available on the cloud server.

System Configuration

You can export the current configurations of the camera to the computer or an external storage device for backup, so when necessary, you can restore camera configurations by importing the backup file.



- Click **Default**, and the system will restore all settings to factory defaults except current network and user settings, and the camera will restart automatically.

  When **Restore all settings to defaults without keeping current network and user settings** is enabled, the camera will reset to factory settings. If a Micro SD card is installed, its capacity allocation will restore to default settings, and any data may be cleared.
- Import Configuration

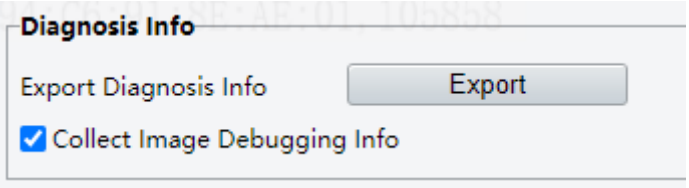
  Note: Before you import a configuration file, make sure the file matches the camera model; otherwise, unexpected results may occur.

1. Click **Browse**.
2. Select the configuration data, and then click **Import**.
3. Click **OK**. The camera will restart after importing the configuration file.

- Export Configuration: Click **Export**.

Diagnosis Info

You can export the image debugging information for troubleshooting.

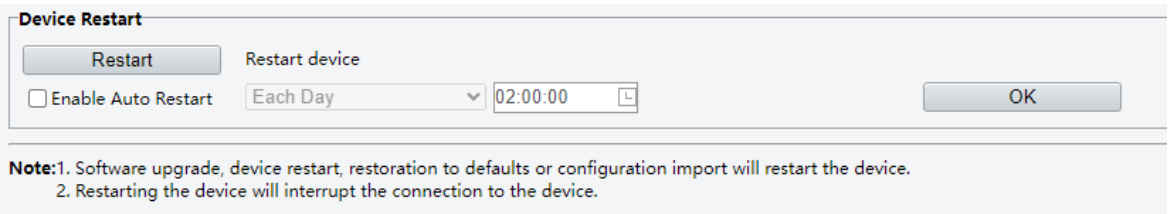


Collect Image Debugging Info: Export the video and debugging information.

Device Restart

You can restart the camera either immediately or at the set time.

Note: Restarting the camera will interrupt the ongoing services. Please handle with caution.

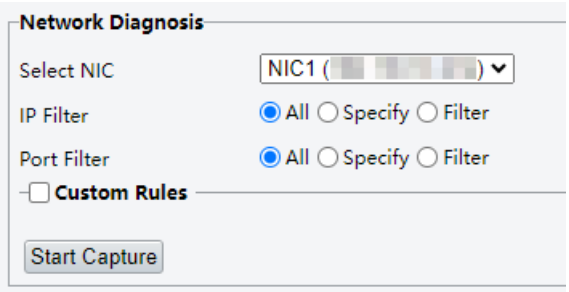


- Restart immediately: Click **Restart**, and click **OK** to restart the camera.
- Restart automatically:
  1. Select **Enable Auto Restart**, and set the restart time.
  2. Click **OK**, and the camera will restart based on the set time.

8.1.2 Network Diagnosis

Go to **Maintenance** > **Maintenance** > **Network Diagnosis**.

Network Diagnosis

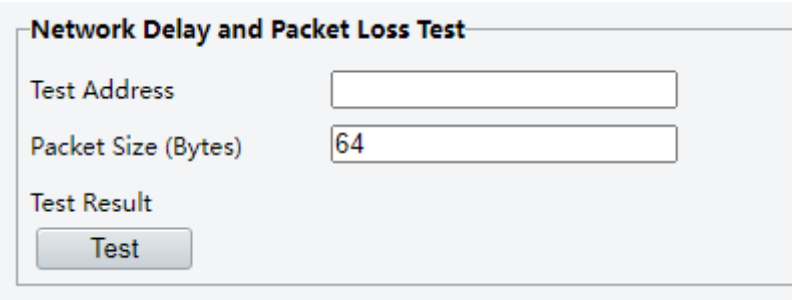


1. Select an NIC.
2. Select an IP and port filter mode.
   - All: Capture packets of all the ports and IPs.
   - Specify: Capture packets of the specified port and IP.
   - Filter: Capture packets except that of the specified port and IP.
3. (Optional) Set the custom rules according to description.
4. Click **Start Capture** to start capturing packets.

5. Click **Stop Capture**, and the captured data are saved to the custom directory.

Network Delay and Packet Loss Test

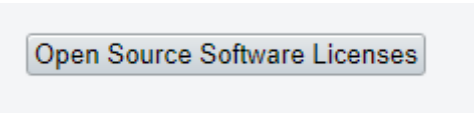
The system can send test packets multiple times, and check if the operation is normal and network is smooth based on average delay and packet loss, which can help users to find the cause of network failures. The average delay refers to the average length of time from test packets are sent till responses are received. The packet loss rate refers to the ratio of lost packets to the sent packets.



1. Enter the test address.
2. Enter the options based on instructions.
3. Click **Test**. The results will appear after the test is complete.

8.1.3 About

Go to **Maintenance** > **Maintenance** > **About**.



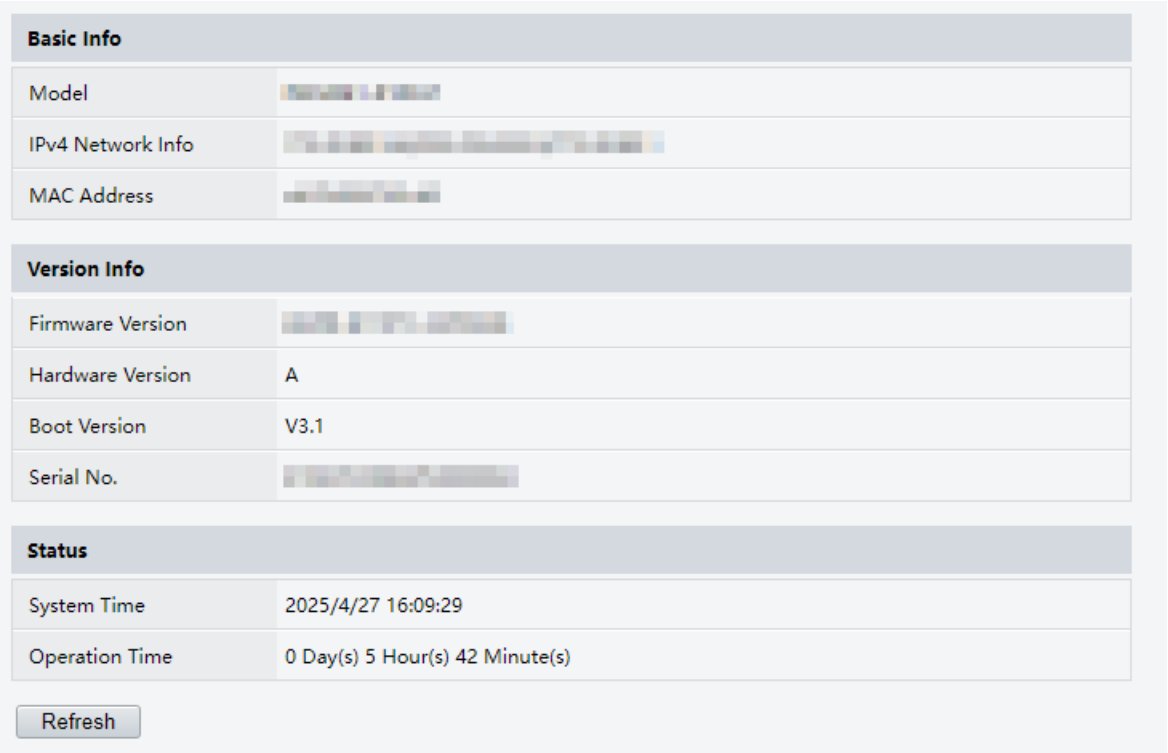
Click **Open Source Software Licenses** to view details.

8.2 Device Status

View the basic information and operation status of the device.

You can view the camera's basic parameters and view the real-time operation status, thereby improving the camera's maintainability.

Go to **Maintenance** > **Device Status**.



- Basic Info: View the device model, firmware version, hardware version, etc.
- Status: View the system time and device operation time. Click **Refresh** to update the data.

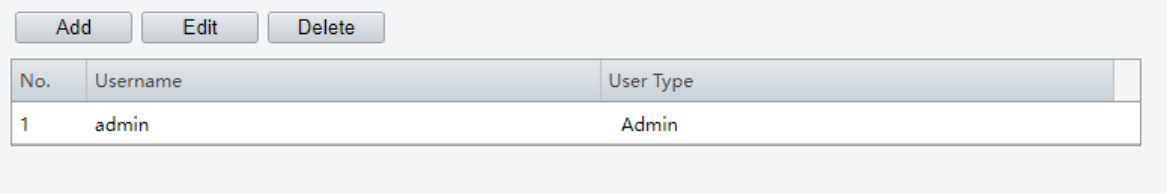
8.3 Security

8.3.1 User

User Type

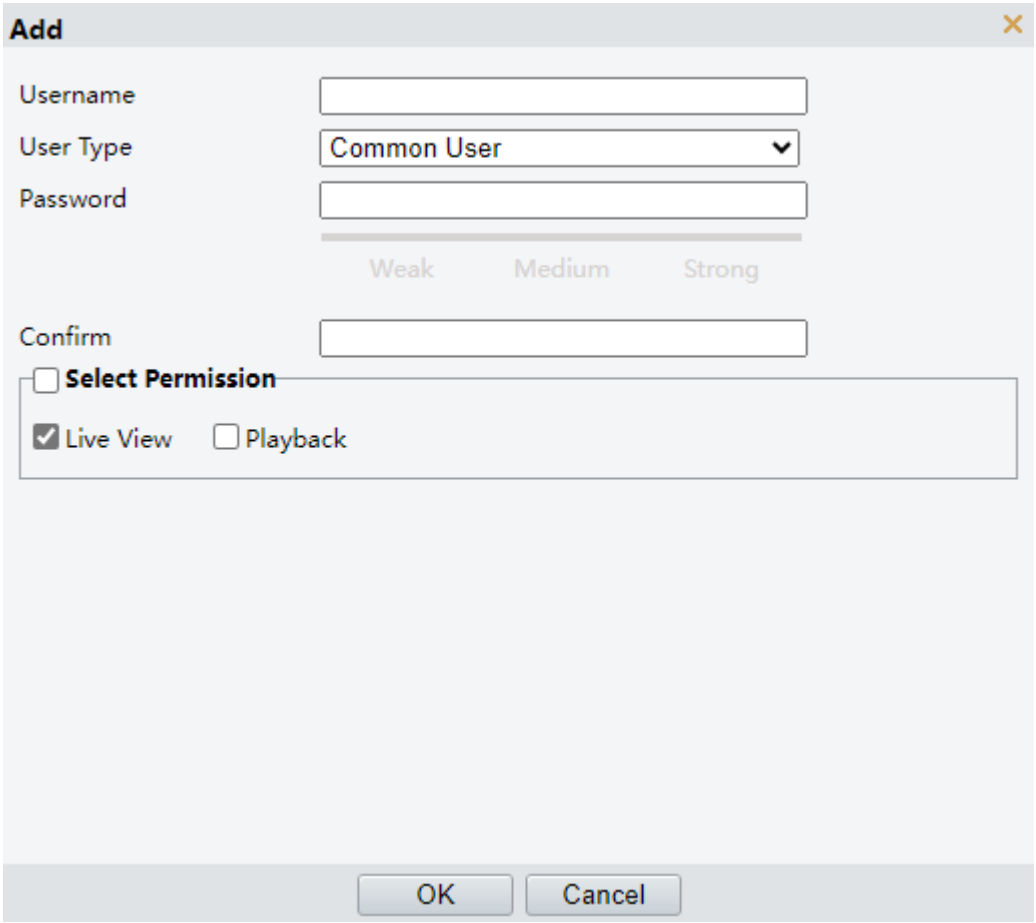
- Admin: Has the maximum permissions. Only 1 admin user is allowed.
- Operator: Has all permissions for managing the device and common users.
- Common User: Only has live view and playback permissions. Up to 32 common users are allowed.

Go to **Maintenance** > **Security** > **User**.



Add

1. Log in to the camera's web interface using the admin account.
2. Go to **Maintenance** > **Security** > **User**.
3. Click **Add**.



4. Configure the parameters.

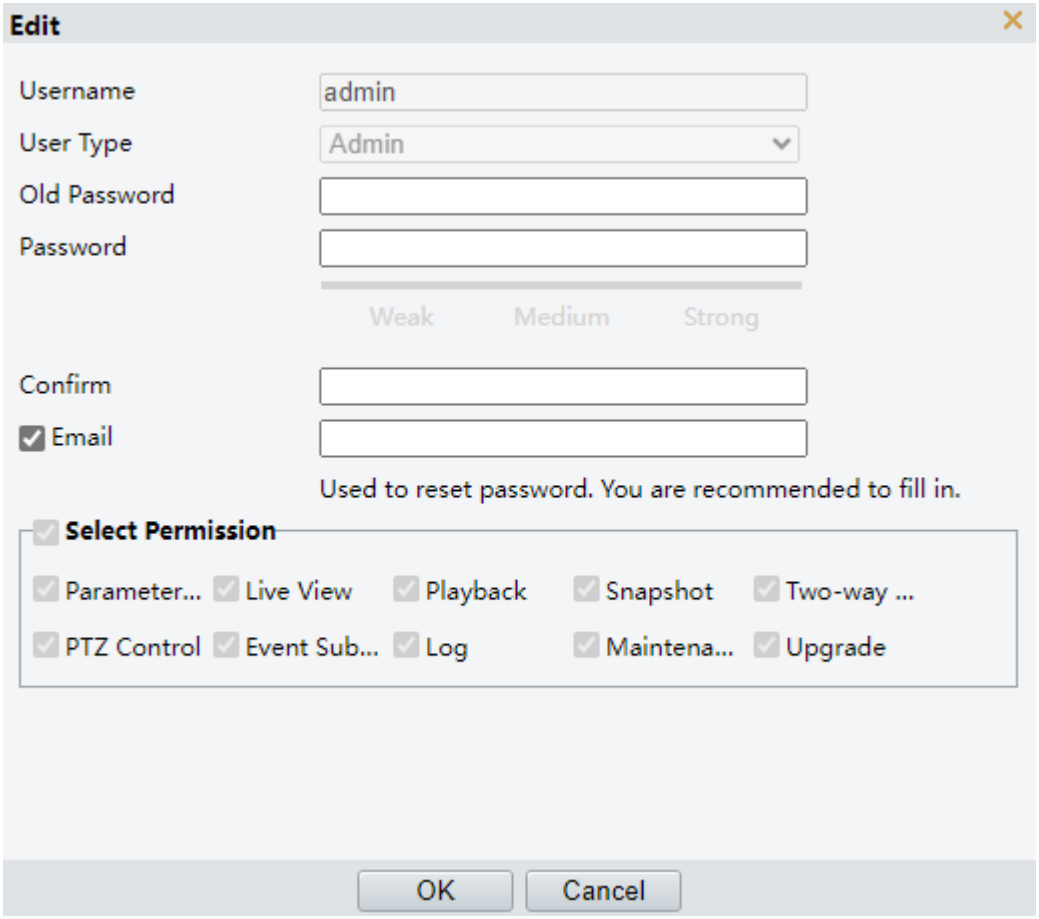
Parameter	Description
Username	Enter the username. 1 to 32 characters are allowed, including uppercase and lowercase letters, digits, underscores, hyphens, dots, and plus signs.
User Type	Choose **Operator** or **Common User**.
Password	The more complex the password, the more secure the system. The password shall be 8 to 32 characters consisting at least three of the following elements: digits, lowercase letters, uppercase letters, underscores, and hyphens.
Confirm	Enter the password again.
Select Permission	Select permissions you want to assign to the user.

5. Click **OK**.

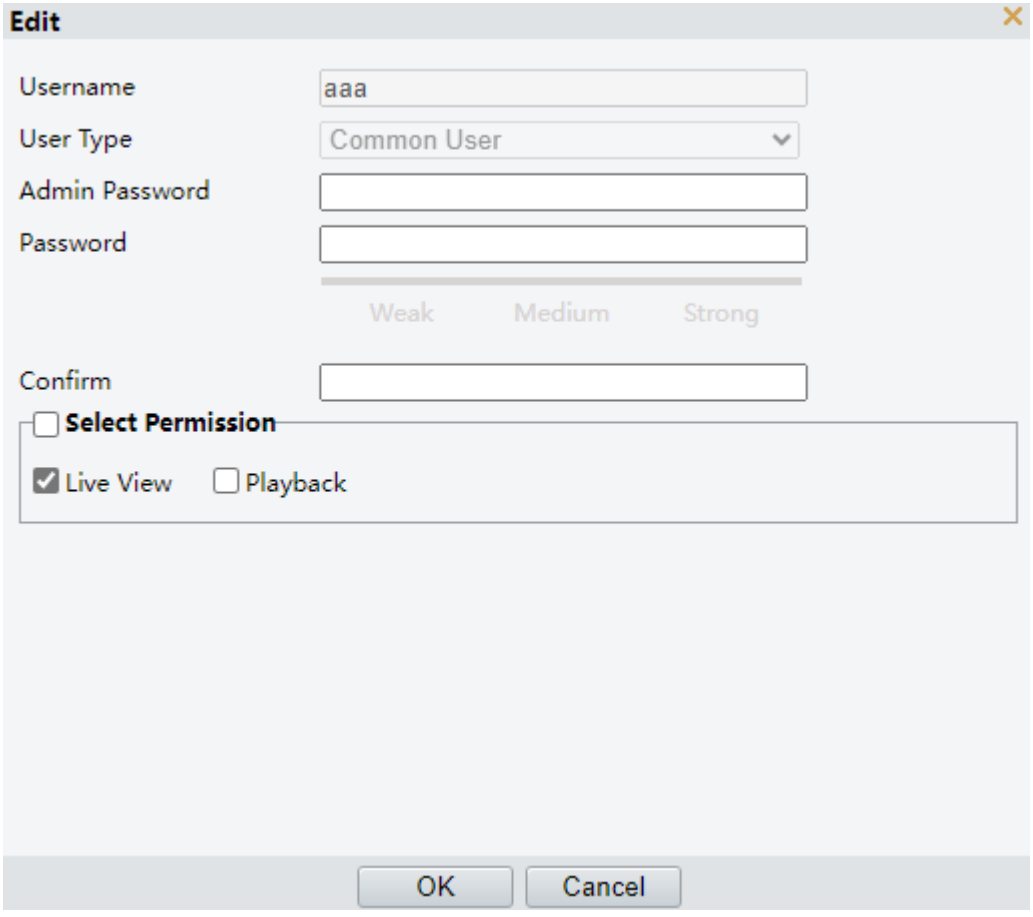
Edit User

Change the password (admin password is required) or permissions.

1. Log in to the camera's web interface using the admin account.
2. Go to **Maintenance** > **Security** > **User**.
3. Click the user you want to edit, and click **Edit**.
   - Change Admin Info



- Change Common User/Operator Info



4. Enter the old password (for admin) or the admin password (for common users).
5. Enter the new password, and confirm the new password.

6. (Optional) Change the email reserved.

Note:

- Only admin can change the reserved email, which is used to receive the security code so as to retrieve the password.
- To change the email reserved, you must also reset the admin password; otherwise, the email update will not be applied.

7. Click **OK**.

Delete

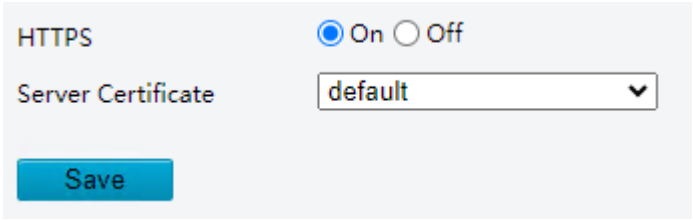
Note: The admin user cannot be deleted.

1. Log in to the camera's web interface using the admin account.
2. Go to **Maintenance** > **Security** > **User**.
3. Click the user you want to delete, click **Delete**, and then click **OK** to confirm.

8.3.2 HTTPS

HTTPS is a secure version of the HTTP protocol that uses SSL protocol to authenticate both a client and a server, and encrypt data during transmission to prevent data from being stolen or altered, enhancing data security.

1. Go to **Maintenance** > **Security** > **HTTPS**.

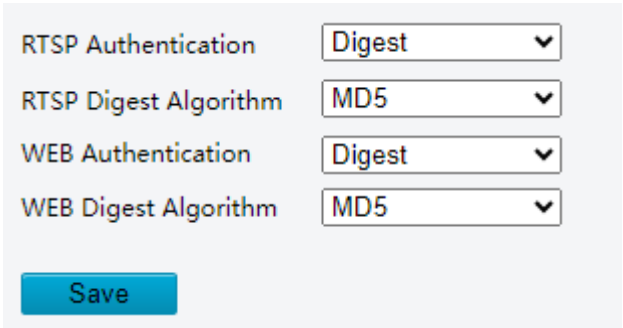


2. Enable **HTTPS**.
3. Click **Save**.

8.3.3 Authentication

Configure RTSP authentication and WEB authentication to improve the security of network transmission. Only after successful authentication can data such as videos, audios, texts, and images be transferred on the network.

1. Go to **Maintenance** > **Security** > **Authentication**.



2. Choose an authentication mode.

Parameter	Description
RTSP	• None: Transmits data without authentication. • Basic: Authentication information is transferred in plaintext without encryption, which imposes serious security risks. • Digest: Authentication information is encrypted to provide higher security. • Digest MD5: Digest authentication, which uses MD5 to protect the username, password, and domain of the requester, not transferred on network in plaintext and provides higher security.

Parameter	Description
	• Digest SHA256: Digest authentication, which uses SHA256 for authentication and provides higher security than Digest MD5. • Digest MD5/ SHA256: Supports MD5 or SHA256 algorithm adaption.

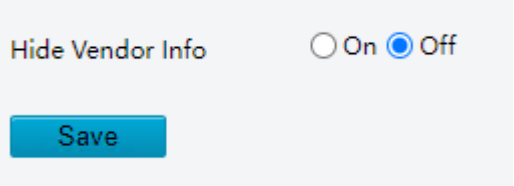
WEB	• None: Transmits data without authentication.
	• Digest: Authentication information is encrypted to provide higher security.
	  • Digest MD5: Digest authentication, which uses MD5 to protect the username, password, and domain of the requester, not transferred on network in plaintext and provides higher security.
	  • Digest SHA256: Digest authentication, which uses SHA256 for authentication and provides higher security than Digest MD5.
	  • Digest MD5/ SHA256: Supports MD5 or SHA256 algorithm adaption.

3. Click **Save**.

8.3.4 Registration Info

The manufacturer information is provided on the management platform.

1. Go to **Maintenance** > **Security** > **Registration Info**.



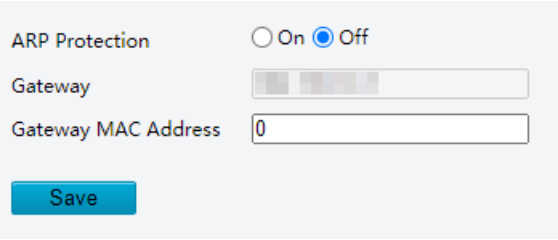
2. Enable or disable **Hide Vendor Info** as needed.
3. Click **Save**.

8.3.5 ARP Protection

ARP attack mainly exists in local area network, which forges IP address and physical address (MAC address) to achieve ARP spoofing, causing communication failures among devices within the local area network.

Configure ARP protection, and the device will verify the physical address (MAC address) of the access source, so as to avoid ARP spoofing attacks.

1. Go to **Maintenance** > **Security** > **ARP Protection**.



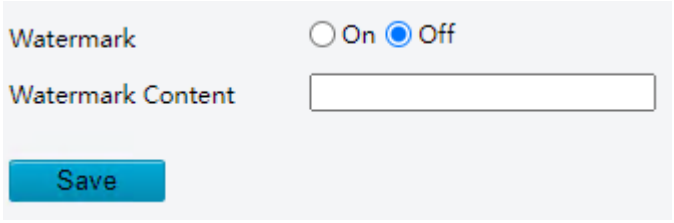
2. Enable **ARP Protection**.
3. Enter the gateway's physical address (legal MAC address).
4. Click **Save**.

8.3.6 Watermark

Use the watermark function to encrypt custom information into video contents to prevent video tampering.

You can view the watermark effect of the video player on the EZPlayer website.

1. Go to **Maintenance** > **Security** > **Watermark**.

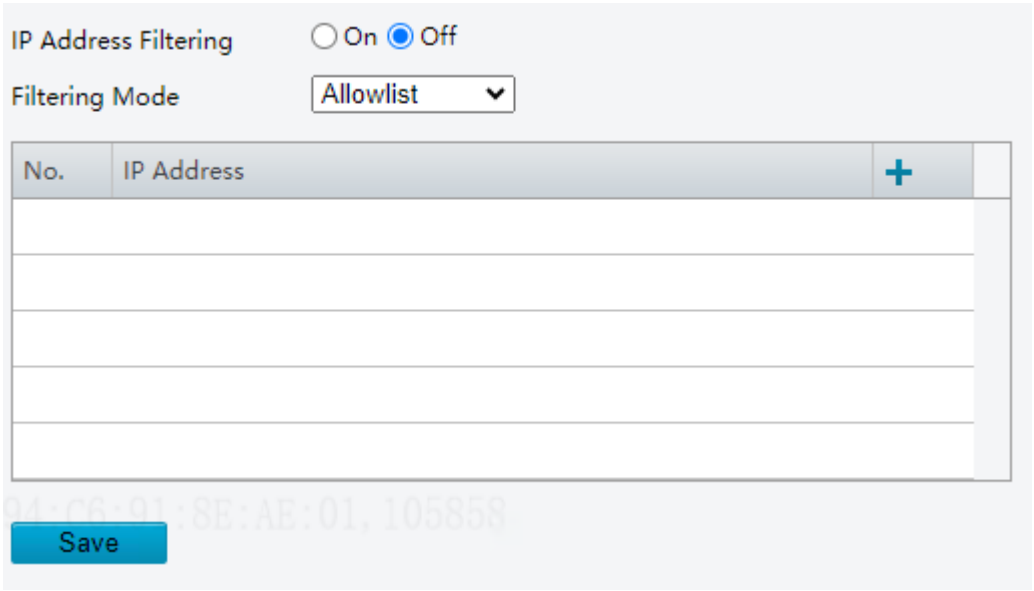


2. Enable **Watermark**.
3. Set the watermark content, with 0 to 16 characters, including lowercase and uppercase letters, and digits.
4. Click **Save**.

8.3.7 IP Address Filtering

Use IP address filtering to allow or forbid access from specified IP addresses.

1. Go to **Maintenance** > **Security** > **IP Address Filtering**.



2. Enable **IP Address Filtering**.
3. Set the filtering mode to **Allowlist** or **Deny Access**. If **Allowlist** is selected, only the added IP addresses are allowed to access the device. If **Deny Access** is selected, only the added IP addresses cannot access the device.
4. Click **+**, and enter IP address(es).
   - Up to 32 IP addresses can be added. Duplicate addresses are not allowed.
   - The first byte of the IP must be 1-233, and the fourth byte cannot be 0. Invalid IP addresses such as 0.0.0.0, 127.0.0.1, 255.255.255.255, and 224.0.0.1 are not allowed.
5. Click **Save**.

8.3.8 Access Policy

Access policies are used to prevent unauthorized access and operation from the network.

1. Go to **Maintenance** > **Security** > **Access Policy**.

2. Configure the parameters.

- MAC address refers to the hardware address written into the hardware during manufacturing. It can be used to identify the device's location during data transmission at the lower layers of the network.

  Enable **MAC Authentication**.

- Illegal Login Lock

  Note: When enabled, if the maximum number of illegal access attempts reaches, the camera is locked and unavailable. When disabled, the number of illegal access attempts is unlimited.

Item	Description
Illegal Login Lock	If the client IP address is not on the blocklist, the input username is correct, but the input password is wrong, it is an illegal access attempt. **Note:** • The user can unlock the account by disconnecting power and rebooting the camera. • When an account is locked, information including the username, IP address, etc., is logged by the system.
Illegal Access Limit	• Set the maximum number of illegal access attempts allowed. • When the same user accesses the camera using different client IP address, the illegal access limit is determined by the most recent configuration.
Lock Time (min)	Integer within the range of 1-120.

  Example: User A tries to log in from the client IP address 192.168.1.33 and is locked. Then user A cannot log in within the lock time, but user B is not affected and can still log in from the same IP address.

- Session Timeout: A session is the connection established between the client (Web browser) and the server (camera). When enabled, the device will log out if there is no user activity (such as clicking or syncing configuration) within the specified time. You will need to log in again from the login page once logged out.

  Note: Only admin can enable or disable this feature.

Item	Description
Session Timeout	Click **On**/**Off** to enable/disable **Session Timeout**. Sessions are counted as follows. Take one device as an example. • If the session is established using one web browser from one client IP, there is one session.

Item	Description
	• If sessions are established using one web browser from one client IP, there are two sessions. • If sessions are established using two web browsers from two client IPs (two browsers from each IP), there are four sessions. **Note:** Up to 36 sessions are allowed at the same time.
Timeout (min)	Enter an integer within the range of 1 to 120. **Note:** The timer restarts when the session is re-established after a reboot.

Note:

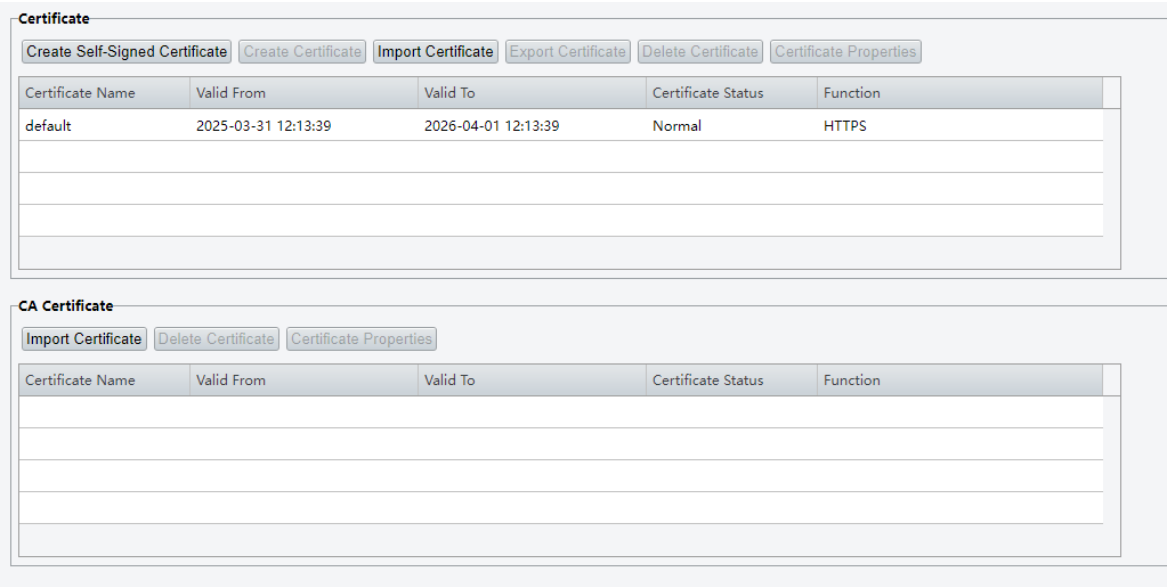
- The friendly password function is available on certain models.
- When **Friendly Password** is enabled, the camera's web interface can be used normally. When **Friendly Password** is disabled and a user logs in to the camera's web interface with a weak password, the password change page will appear and forcibly ask the user to change the password into a strong one.

3. Click **Save**.

8.3.9 Certificate Management

A certificate is an electronic file that uniquely represents individuals and resources on the Internet and enables secure and confidential communications between the two entities. On the **Certificate Management** page, you can set different servers, create CA certificates, view certificate properties, etc.

Go to **Maintenance** > **Security** > **Certificate Management**.

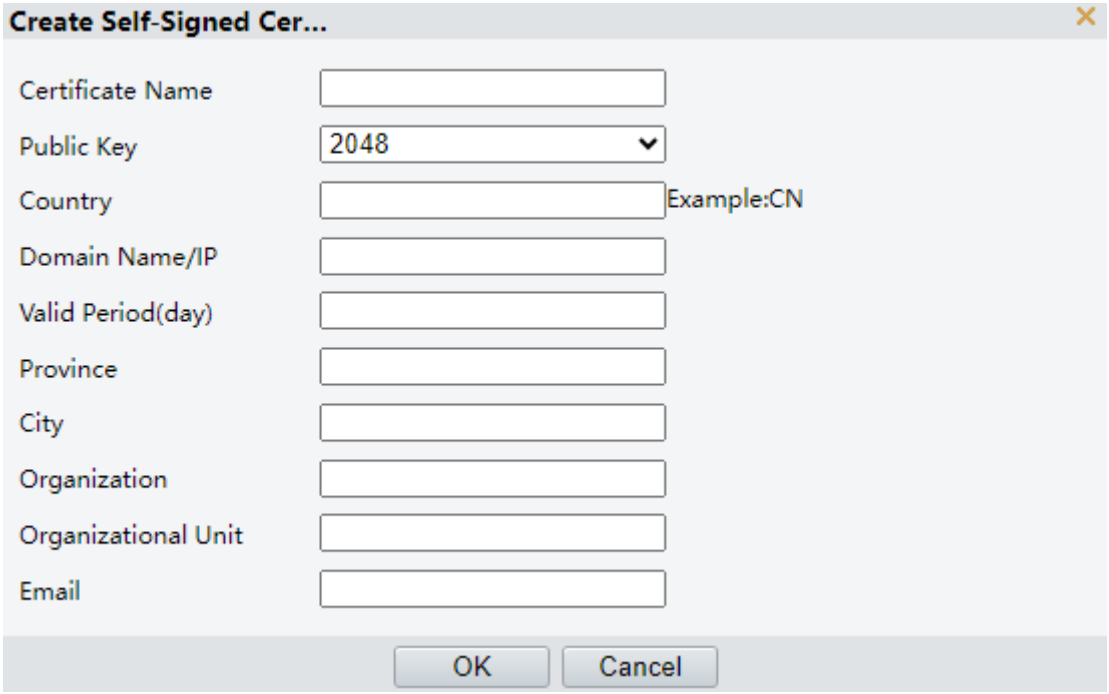


8.3.9.1 Certificate

Create Certificate

Create a self-signed certificate or import a certificate.

- Create a self-signed certificate for application scenarios with low-security requirements. It is a digital certificate issued by an untrusted CA (Certificate Authority), such as a company or software developer.

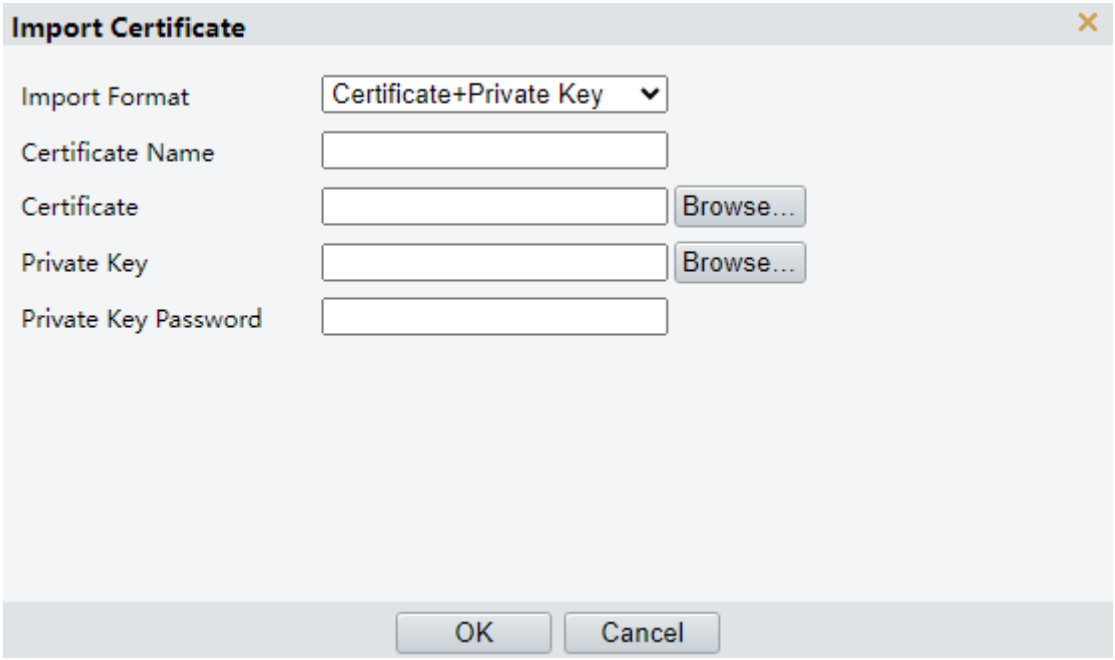


1. Click **Create Self-Signed Certificate**.
2. Configure the parameters.

Item	Description
Certificate Name	Set as needed.
Public Key	Choose a length for the public key: 2048 or 1024. Default: 2048.
Country	Enter the two-character country code, for example, CN for China.
Domain Name/IP	Enter the device's IP address or domain name.
Valid Period(day)	Enter the validity period of the certificate.
Province	Enter the complete province name.
City	Enter the complete city name.
Organization	Enter the organization name.
Organizational Unit	Enter the organizational unit name.
Email	Enter a valid email address.

3. Click **OK**.

- Import a non-CA certificate.



1. Click **Import Certificate**.
2. Configure the parameters.

Item	Description
Import Format	You may choose **Certificate+Private Key**, **PKCS#12**, or **Self-Signed Request Certificate**.
Certificate Name	Enter the certificate name.
Certificate	Click **Browse** and locate the certificate.
Private Key	Click **Browse** and locate the private key.
Private Key Password	Enter the private key password.

3. Click **OK**.

- (Optional) Create a certificate request to obtain a trusted signed certificate for application scenarios with high-security requirements.
  1. After creating or importing a certificate, select the certificate, and click **Create Certificate Request**.
  2. Configure the parameters.
  3. Click **OK**.

     Note: After the certificate request is created, export the certificate request file. After the certificate authority (CA) signs and issues a certificate in accordance with the request, import the certificate into the device.

Export Certificate

Click **Export Certificate** to save the certificate to your computer.

Delete Certificate

Select a certificate and delete it. A certificate that is in use cannot be deleted.

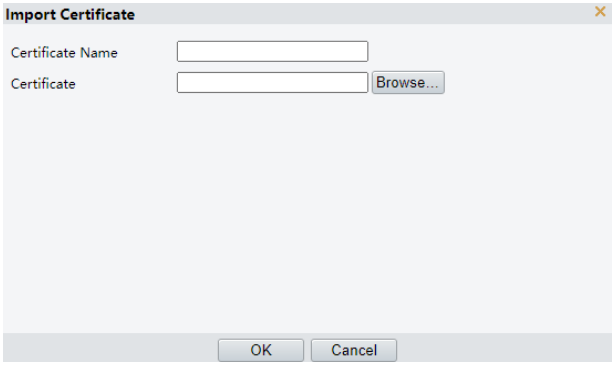
Certificate Properties

Select the certificate to view its properties.

8.3.9.2 CA Certificate

CA is an authority that issues certificates. It can sign and issue certificates, and manage certificates issued. A CA certificate is a self-signed certificate issued by an untrusted certificate authority (CA) and thus is more secure and reliable.

1. Click **Import Certificate**.
2. Enter the certificate name, and select the certificate.



3. Click **OK**.
   - Delete Certificate

     Select a certificate and delete it. A certificate that is in use cannot be deleted.
   - Certificate Properties

     Select the certificate to view its properties.