4MP AI Enforcement Camera

Web Operation Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.2

Foreword

General

This manual introduces the web operations of the 4MP AI enforcement camera (hereinafter referred to as the "Camera").

Models

DHI-ITC431-RW1F-L, DHI-ITC431-RW1F-IRL8

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.2	Changed some images.	December 2021
V1.0.1	Updated model information and cybersecurity recommendations.	September 2021
V1.0.0	First release.	September 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by

implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

1 Web Introduction

After mounting the Camera (see details in the user's manual of the all-in-one enforcement camera), power on the Camera, connect it to the network and configure its settings, then you can get the desired detection results.

The actual page might vary depending on the model you purchased and the version of software. The figures in this manual are only for reference, and might differ from the actual page.

1.1 First-time Login

The Camera is delivered in the uninitialized status. You need to initialize the Camera and modify its default password before it can be used.

Step 1 Connect the Camera to the network.

1) Connect the Camera to PC over the Ethernet cable.
2) Keep the IP address of the PC and the camera on the same network segment.
   The network segment can be set to 192.168.1.X, but cannot be the same as the factory default IP of the Camera (192.168.1.108).
3) Execute ping ***.***. ***. *** (device IP) command on PC to check the network connection.

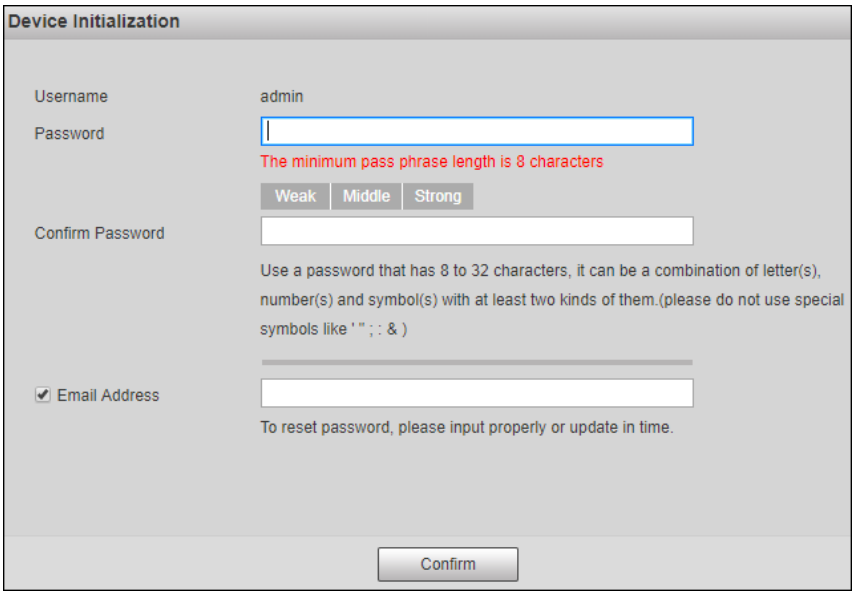
Step 2 Enter the IP address of the Camera (192.168.1.108) in the browser address bar, and press the Enter key to log in to the web page of the Camera.

Step 3 On the **Device Initialization** page, enter your new password.

Step 4 Select the **Email Address** checkbox, and then enter your email address. This helps you reset your password when your password is lost or forgotten.

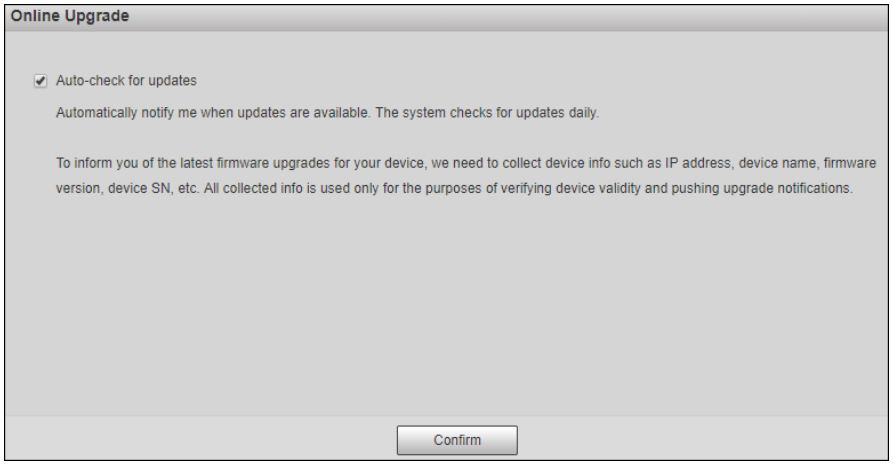
Step 5 Click **Confirm**.

Figure 1-1 Device initialization



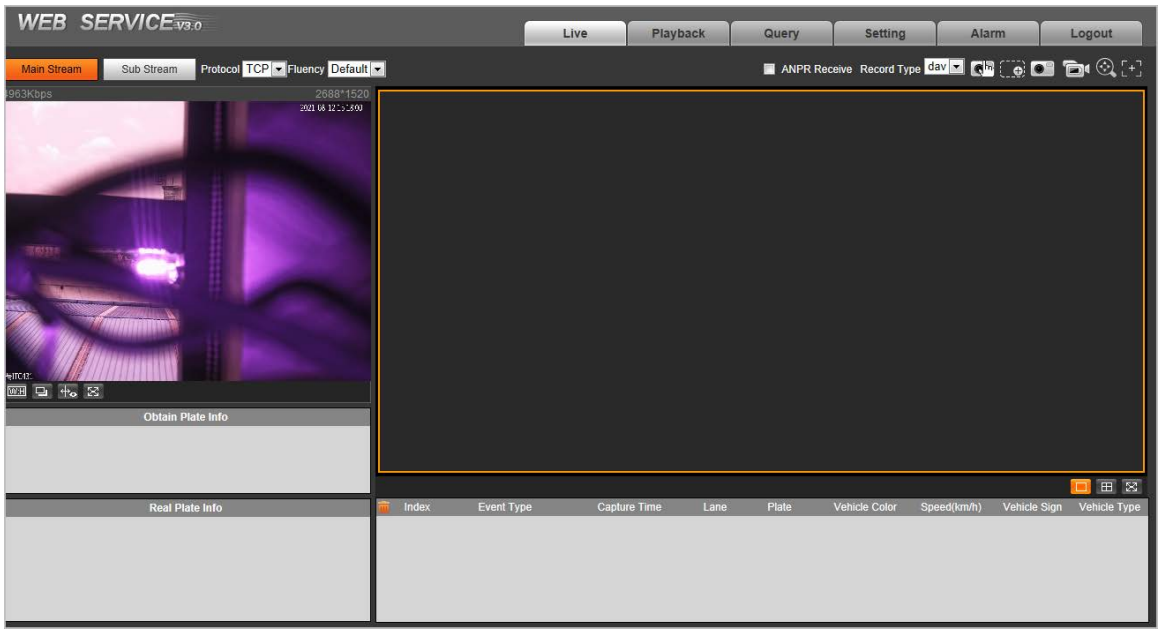
Step 6 On the **Online Upgrade** page, select **Auto-check for updates** and then click **Confirm**.

Figure 1-2 Login



Step 7 On the login page, enter the username (admin) and the password that you set, and then click **Login**.

Figure 1-3 Live page



Step 8 For first-time login, click **Please click here to download and install the plug-in**, and then install the plug-in.

Before installing the plug-in, make sure that **ActiveX controls** (in Internet Explorer) from **Tools > Internet Options > Security > Custom Level** is enabled.

After successfully installing the plug-in, the live view of the Camera is displayed.

If there is no operation for a long time, the system prompts **Authorized failed. Please login again!** In this case, you need to log in again.

1.2 Login

You can log in to the web by following the steps below. For first-time login, see "1.1 First-time Login".

Step 1 Enter the IP address of the Camera in the browser address bar, and press Enter.

Step 2 Enter username and password on the displayed page, and then click **Login**.

- A box pops up when the username or password is incorrect. See Figure 1-4.
- If you enter an invalid username or password five times, the account will be locked for five minutes.

Figure 1-4 Invalid username or password

1.3 Logout

Click **Logout** at the upper-right corner of the web page to log out.

You can enter the username and password to log in again.

1.4 Password Reset

You can reset your password through email when it is lost or forgotten. Make sure that your email is correctly entered during initialization (see "1.1 First-time Login"). Email address of admin user can be modified from **Setting > System > Account > Account > Username**.

Step 1 Enter the IP address of the Camera in the browser address bar, and press Enter.

Step 2 On the login page, click **Forgot password?**.

Step 3 In the pop-up dialog box, click **OK**.

Step 4 Scan the QR code according to the page prompt, and send the scanning result to the designated email to acquire security code.

Scan the actual QR code. Do not scan the QR code in this manual.

Step 5 Enter the security code that you received in the text box of **Security code**.

Figure 1-5 Reset password

Step 6 Click **Next**.

Step 7 Set **Password**, and enter your new password again in **Confirm Password**.

- The new password must consist of 8–32 characters, and contain at least two types from upper cases, lower cases, numbers and special characters (excluding ' " ; : and &).
- The new password must be the same as the **Confirm Password**. Follow the password security notice to set a high-security password.

Step 8 Click **Yes**.

1.5 Web Functions

You can view real-time video captured by the Camera, set detection rules of number plate recognition and traffic violations, and play back video recordings and snapshots to trace back events (if any). Here introduces the overview of each function button on the **Live** page.

Figure 1-6 Web function bar

Table 1-1 Web functions

Operation	Description
Live	Displays real-time video and picture. You can record video and capture images, and configure video play and picture settings. See "2 Live".
Playback	You can play back manual video recordings and videos related to traffic violations to trace back events (if any). See "3 Playback".

Operation	Description
Query	You can search for images, traffic flow information, and records on this page. See "4 Query".
Setting	You can configure the way that the Camera works, the rules for detecting violations, and the internet protocol for camera network connection. You can also view version and system information of the Camera. See "5 Settings".
Alarm	You can configure how the Camera responds when alarms occur. See "6 Alarm".
Logout	Log out the web page. See "1.3 Logout".

2 Live

The **Live** page is displayed after you successfully log in to web. On this page, you can view the live video image and the captured number plate, take snapshots, view event details, and more.

Figure 2-1 Live

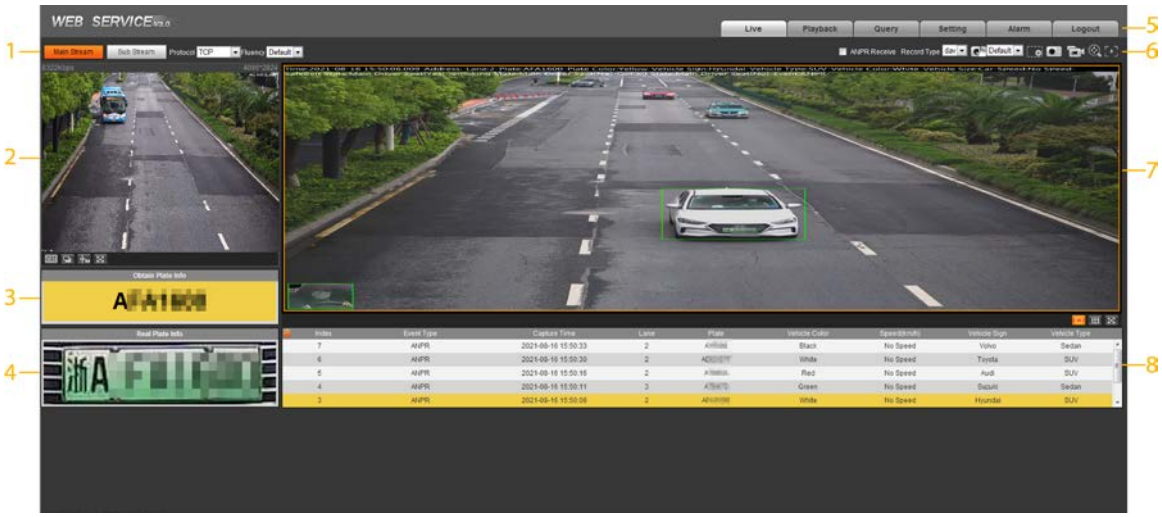


Table 2-1 Description of live page

No.	Description	No.	Description
1	Video stream	5	System functions
2	Live view	6	Functions of Live page
3	Logged plate number	7	Vehicle snapshot
4	Plate snapshot	8	Event list

2.1 Video Stream

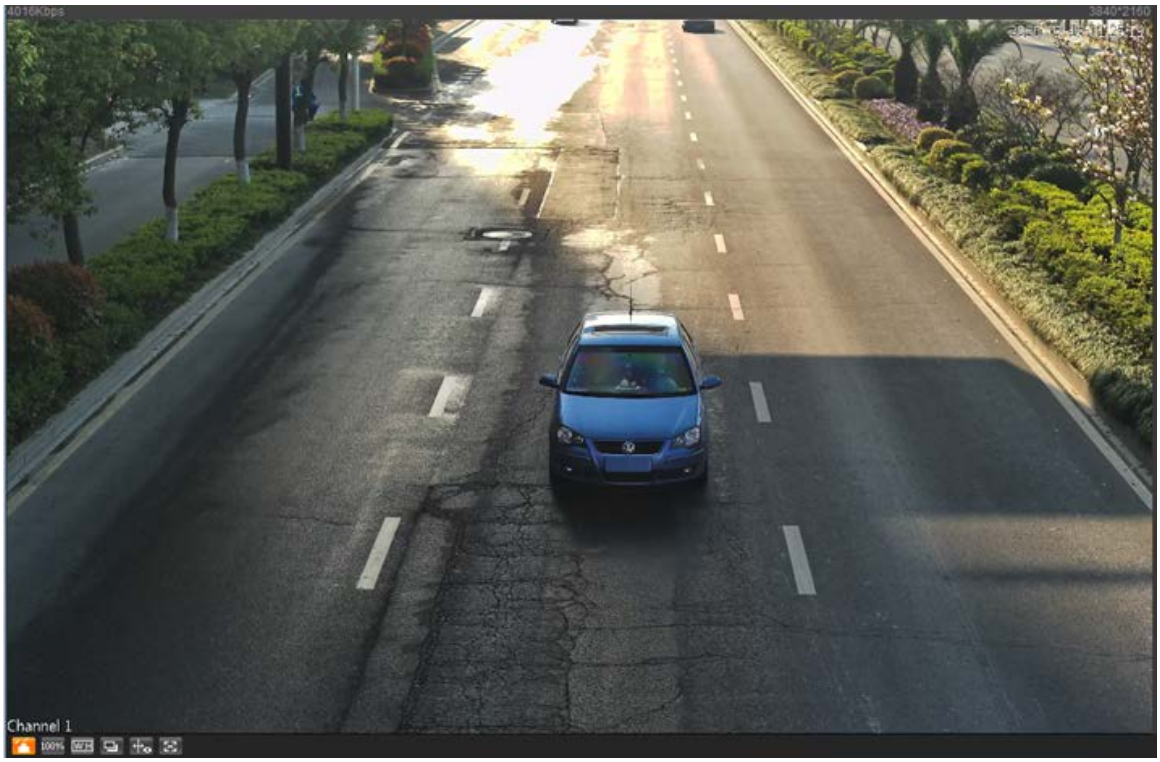
- **Main Stream**: Make sure that the Camera can record videos and carry out network surveillance when the network is normal. You can configure main stream resolution within the supported range of the Camera.
- **Sub Stream**: Replaces main stream to make network surveillance and reduce the network bandwidth usage when network bandwidth is insufficient.
- **Protocol**: Video surveillance protocol. Currently it only supports **TCP**.
- **Fluency**: Fluency of viewing the live video. The fluency can be set to **High**, **Middle**, **Low** and **Default** (recommended).

2.2 Live View

Displays the live video captured by the Camera. You can also click the icons to change the display mode of live view.

-  : Adjust the image to original size or appropriate window.
-  : Click it to switch to big window. Click it again to exit big window.

Figure 2-2 Big window



  - ◇  : Click it to open image adjustment window on the right, meanwhile the button turns to  . Click  to close the image adjustment window.
  - ◇  : Click it and the image is displayed at 100%, and the button turns to  . Click  to switch back to original size.
-  : Click it to enable smart track detection. Number plate, vehicle bounding box, and other smart tracking information will be displayed in the video image.
-  : Click it and the window is displayed in full screen; double-click or right-click to exit full screen.

Table 2-2 Image adjustment

Icon	Name	Description
	Brightness	Adjust the overall image brightness. Change the value when the image is too bright or too dark. The range is from 0 to 128 (64 by default).
	Contrast	Change the value when the image brightness is suitable, but contrast is not enough. The range is from 0 to 128 (64 by default).
	Hue	Adjust the image hue. For example, change red into blue. The default value is made by the light sensor and normally it does not have to be adjusted. The range is from 0 to 128 (64 by default).
	Saturation	Adjust the vividness of the colors, without influencing the overall brightness of the image. The range is from 0 to 128 (64 by default).
	—	Click it to restore brightness, contrast, saturation, and hue to their default values.

In this image adjustment window, you can only adjust image brightness, contrast, hue, and saturation of local web. To adjust system brightness, contrast, hue and saturation, go to **Setting > Camera > Camera Attribute > General**.

2.3 Plate Number Recognition

Displays the plate number recognized by the Camera in real-time when a vehicle passes.

2.4 Plate Snapshot

Displays the snapshot of a license plate when a vehicle passes.

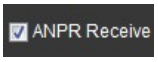
2.5 System Functions

Click the icons to set system functions, which include playback, video recording and snapshot query, intelligent rules setting, alarm event setting, and system logout. See more details in the following chapters.

2.6 Functions on the Live Interface

Set functions on the **Live** page, and then the system will display the desired information on the **Live** page.

Table 2-3 Function description of the Live page

Icon	Name	Description
	ANPR Receive	Select the checkbox, and the Camera automatically receives vehicle snapshots and detects event information triggered by sources such as radar or video detection, and displays such snapshots and information at the lower part of the page. The snapshots are saved in the storage path defined by **Setting > Storage > Destination > Save Path**.
	Record Type	Select the format of video recordings (**dav** by default).
	Manual Snapshot	Click it, and the Camera takes a snapshot when a vehicle passes. The snapshot is saved in the storage path. ● Enable **ANPR Receive** first. ● To change the storage path of snapshots, go to **Setting > Storage > Destination > Save Path**.
	Snapshot	Click it, and a snapshot is taken, even when there is no vehicle passing. The snapshot is saved in the path defined by **Setting > Storage > Destination > Save Path**.
	Digital Zoom	Click and drag to select any area in the video window, and then the area will be zoomed into. In any area of the video window, click  or right-click to exit.
	Video Recording	Click it to start recording. Click  again to stop recording and the recorded video will be saved to the set path. The Camera will keep recording until the web page is closed or you log out if the recording is not manually stopped.
	Easy Focus	Click it to start auto focus, local focus, and license plate check for the monitoring image. **ANPR Receive** and **Plate Check** cannot be enabled at the same time.

2.7 Vehicle Snapshot

Select **ANPR Receive**, and then snapshots will be displayed when vehicles pass.

2.8 Event List

Select **ANPR Receive**, and the event information will be displayed, including number, event types, capture time, lanes, plates, vehicle color, speed, vehicle signs, and vehicle types.

3 Playback

Click the **Playback** tab, and then you can play back video recordings stored on the TF card of the Camera.

To set the record strategies, see "5.6.6 Record Control".

Figure 3-1 Playback

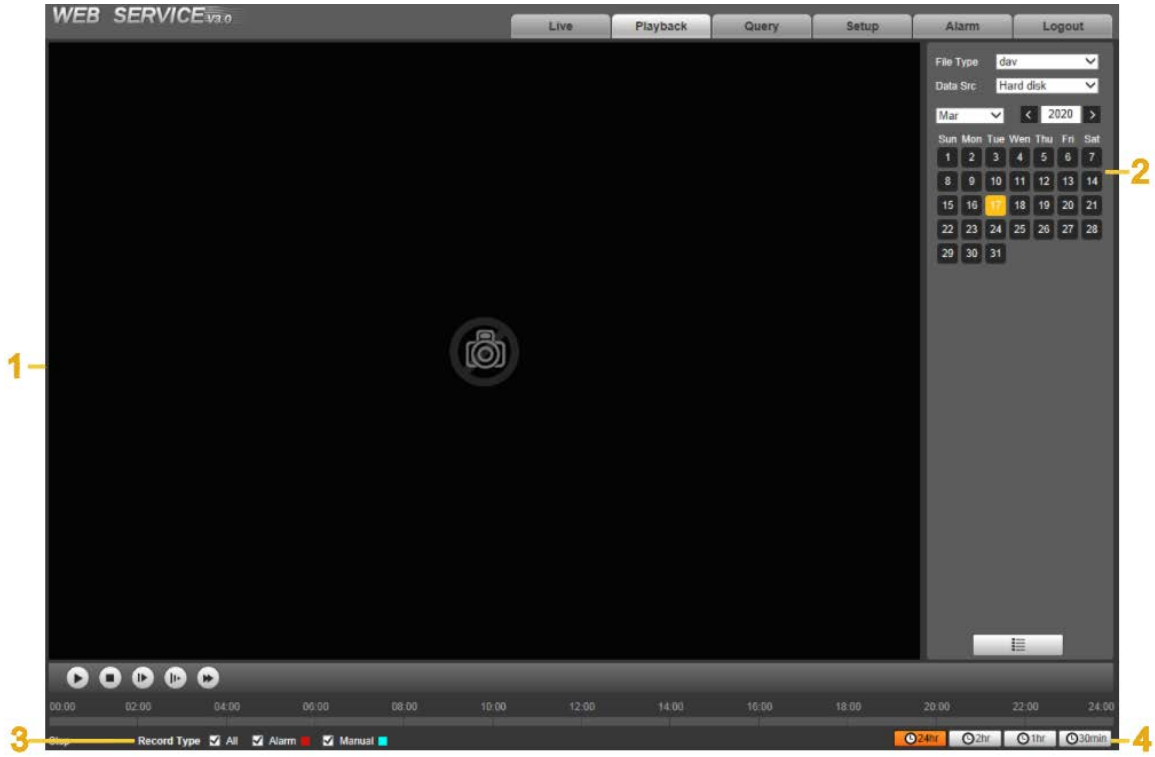


Table 3-1 Functions

No.	Description	No.	Description
1	Video playback	3	Record type
2	Playback file	4	Time format

3.1 Video Playback

When playing back video recordings, you can control the video playing status with the following icons.

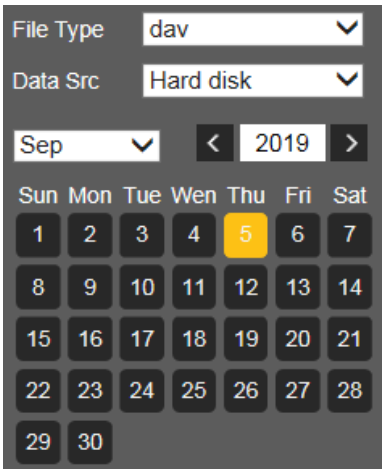
Table 3-2 Video playing description

Icon	Function	Description
	Play and pause	• : The video is paused or not being played. • : The video starts playing.
	Stop	Stop playing video.
	Play by frame	Play by frame.
	Slow	Slow down.
	Fast	Speed up.

3.2 Viewing Recordings

You can view recordings by following the steps below.

Figure 3-2 Playback file



Step 1 Set **File Type** and data source (**Data Src**), and set record time.

The data source is **Hard disk** (here referred to as TF card) by default. No video will be played if there are no videos stored on the TF card.

Step 2 Click a day with blue shading, and a colored progress bar is displayed on the timeline.

Date with blue shading means there are recordings on this day.

- Point to this day, and the color turns to orange.
- Select this day, and the color turns to green.

Step 3 Click any time on the progress bar, and the system plays back videos starting from that time.

Figure 3-3 Timeline

Step 4 Click , and videos recorded on a selected day will be displayed in a list.

Figure 3-4 Playback file

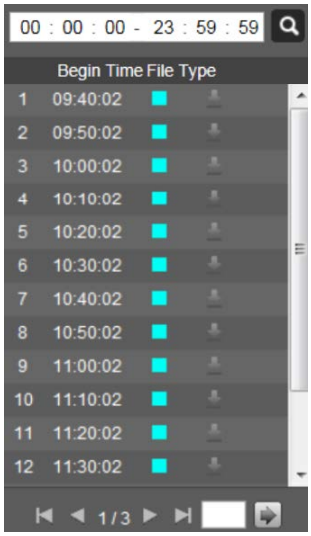


Table 3-3 Playback file description

Parameter	Description
	Search for all the video files within the selected period.
	Click it to download files to local.
	Click it to go back to the calendar page, where you can search and play back videos of other periods.

Step 5 Double-click a file in the list, and the file will be played with information displayed such as the file size, start time, and end time.

3.3 Record Type

Select a record type, and then only files of the selected types will be displayed on timeline and in the file list.

Figure 3-5 Record type

3.4 Time Format

Displays time in different formats. You can click each time format to play back the videos in 24-hour mode, 2-hour mode, 1-hour mode, and 30-minute mode respectively.

Figure 3-6 Time format

4 Query

You can search for snapshots, vehicle flow, and video recordings on the **Query** page.

4.1 Image Search

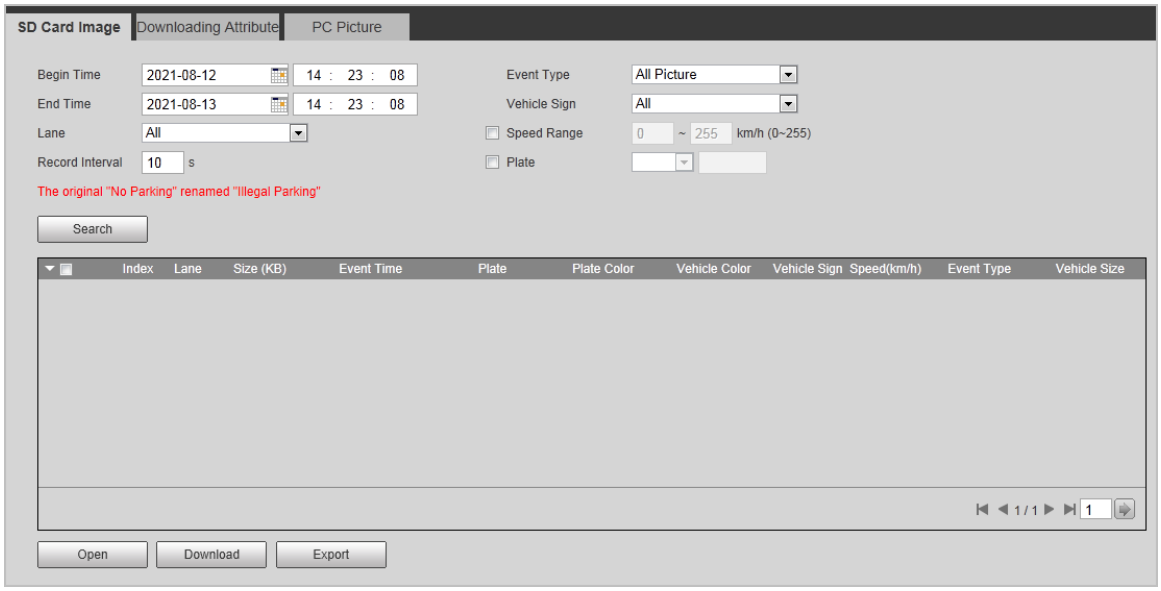
4.1.1 Searching for SD Card Image

On the **SD Card Image** page, you can search for and download the images stored in the TF card of the Camera.

Make sure the TF card is inserted into the Camera; otherwise, there might be no results.

Step 1 Select **Query > Image Search > SD Card Image**.

Figure 4-1 SD card image



Step 2 Configure the parameters, and then click **Search**.

Table 4-1 SD picture parameters

Parameter	Description
Begin Time	Set the begin time and the end time to define a period, and then you can search for images stored on the TF card within this period.
End Time	
Event Type	● **All Picture**: Search for all snapshots. ● **Mix Events**: Search for snapshots related to events, which include but are not limited to **ANPR**, **Cross Solid White Line**, and **Wrong-way Driving**.
Vehicle Sign	Search for snapshots by the selected vehicle sign. You can select **All**, **Unknown** or a specific vehicle sign.
Lane	Select the capture lane.

Parameter	Description
Speed Range	Select the **Speed Range** checkbox, and set the speed range to search for images of vehicles within the defined speed range.
Record Interval	The length of a recorded video associated with the snapshot that you want to save.
Plate	Select the **Plate** checkbox, and then enter the plate number to search for images related to this plate.
	This icon is displayed next to the traffic violation snapshot when **Related Record** is enabled in **Advanced Parameter** (except **ANPR**) under **Setting > Event > ANPR Snap > Rule Config**).

Step 3 Select the images that you need, and click **Open** to view the images in photo viewer.

Step 4 Select the images that you want to download, and then click **Download**.

Step 5 Select the path to save the images, and the system starts downloading the images to your PC.

4.1.2 Downloading Attribute

You can configure the image information.

Step 1 Select **Query > Image Search > Downloading Attribute**.

Step 2 Set **Download Snapshot by** to download snapshots based on their **Creation Time** or **Capture Time**.

Step 3 Select Download Mode.

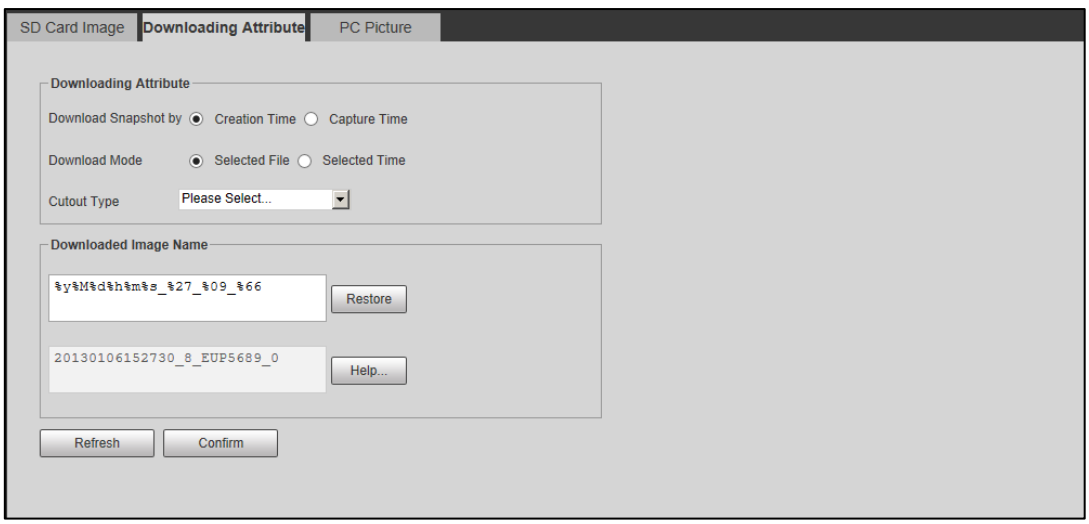
- **Selected File**: Download the selected snapshots.
- **Selected Time**: Download all images captured during the set time period. You can set the time in the **SD Card Image** tab.

Step 4 Select cutouts that you want to download from **All**, **Plate Cutout**, **Binarized Plate**, **Assistant Driver Face** (cutout of front-seat passenger's face), **Driver Face**, and **Vehicle Body Matting**.

Step 5 Name the snapshots. Click **Help…** to view the image naming rule. Click **Restore** to go back to default.

Step 6 Click **Confirm**.

Figure 4-2 Downloading attribute



4.1.3 PC Picture

You can view images saved on your PC and verify whether the image contains a watermark.

To view or set the save path of images on your PC, go to **Setting > Storage > Destination > Save Path**.

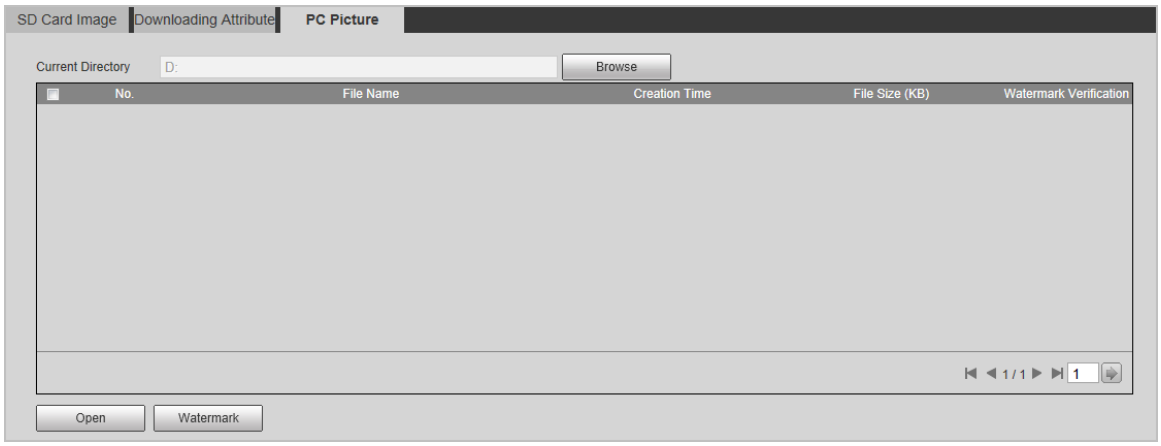
Step 1 Select **Query > Image Search > PC Picture**.

Step 2 Click **Browse** to select the file that includes the picture to be verified.

Step 3 Select the picture to be verified, and then click **Watermark**.

Step 4 Select a picture and click **Open**, or double-click a picture to view the picture in a photo viewer.

Figure 4-3 PC picture



4.2 Flow Query

You can search for traffic flow and pedestrian flow within the defined period.

- The function is available on select models, and might differ from the actual product.
- This section uses **Traffic Flow Query** as an example.

Step 1 Select **Query > Flow Query > Traffic Flow Query** (select **Pedestrian Flow Query** if you want to search for pedestrian flow).

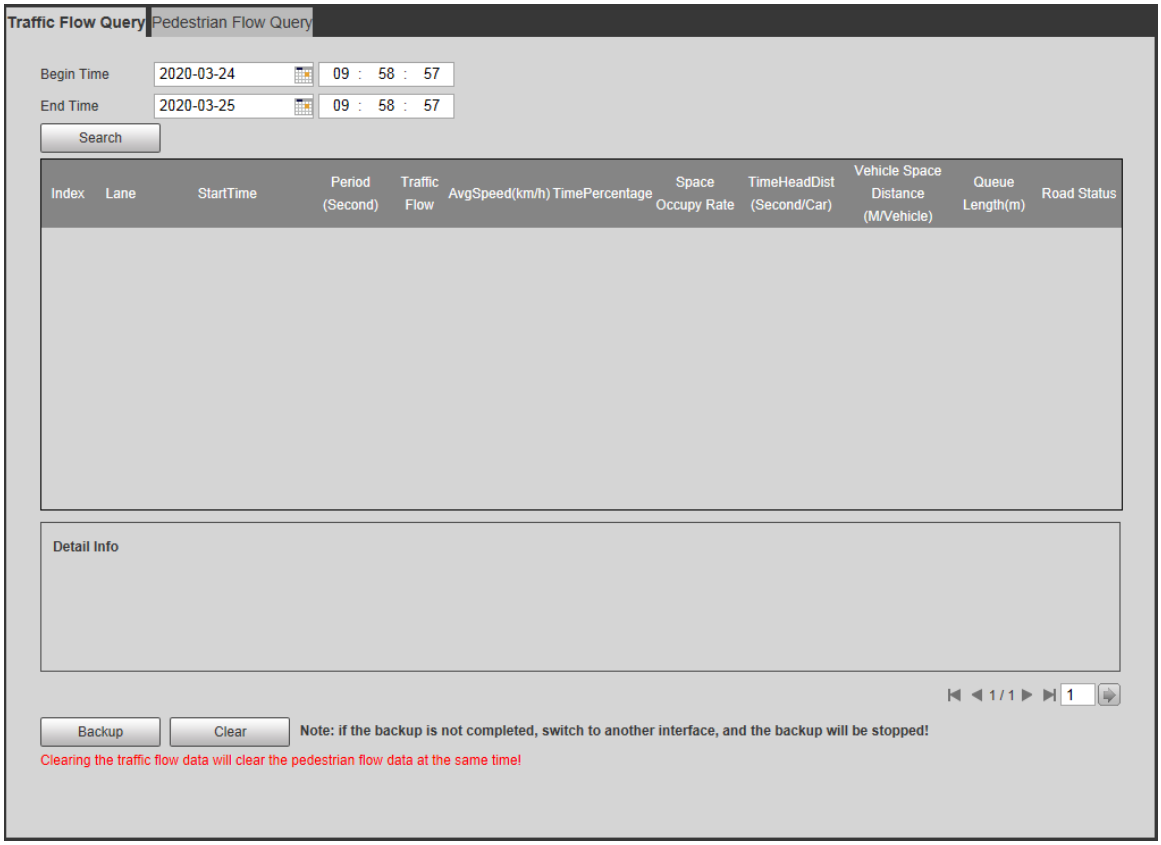
Step 2 Set **Begin Time** and **End Time** of your search.

Step 3 Click **Search**.

Step 4 Select search results, and click **Backup** to save the results to PC.

Step 5 Click **Clear** to delete all the current results.

Figure 4-4 Traffic flow query



4.3 Recording Search

Search for the video recordings stored on your PC to trace back abnormal events (if any).

4.3.1 Recording

You can search for a recorded video on your PC and play back the video.

- Click on the **Live** page, and the Camera starts recording. The recorded video is saved on the path defined in **Setting > Storage > Destination > Save Path**.
- The function is available on select models, and might differ from the actual product.

Step 1 Select **Query > Recording Search > Recording**.

Step 2 Click **Browse** to select the recorded video on your PC, and then you can play back the video.

Figure 4-5 Record

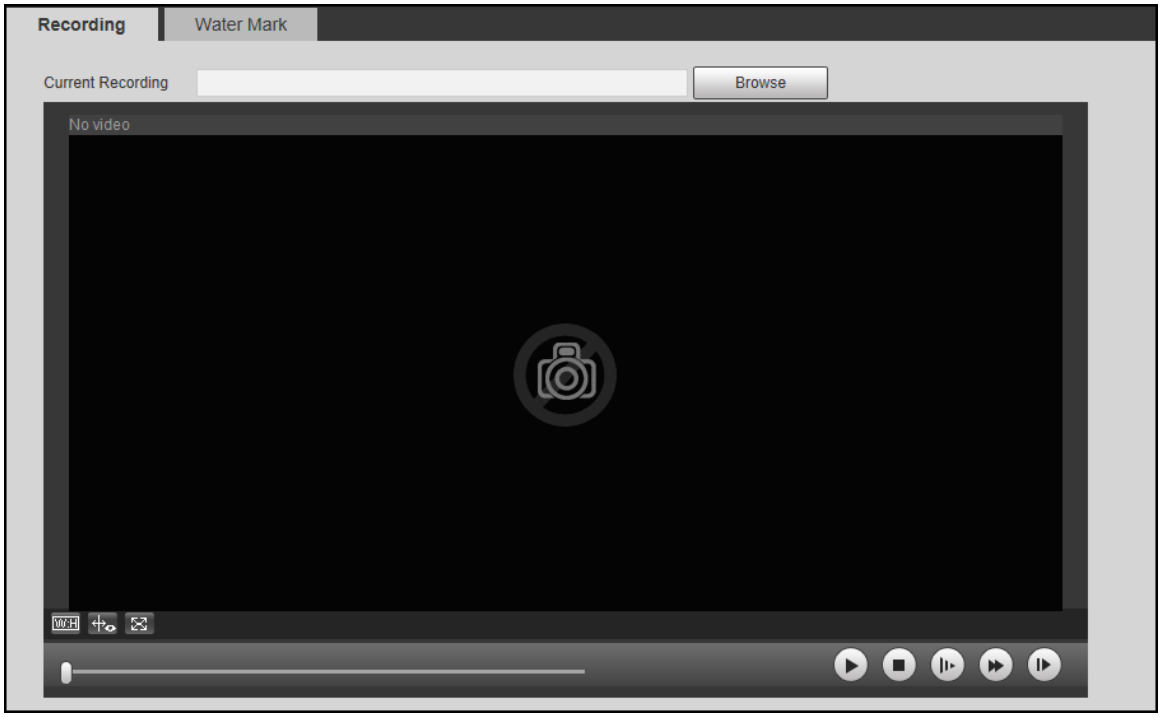


Table 4-2 Play parameters

Icon	Description
	Click it to select **Original** or **Adpative** playback.
	Click it to enable smart track detection. Number plate, vehicle bounding box, and other smart tracking information will be displayed on the video image.
	Click it to enter full screen. Double-click the video image or press Esc to exit.
	Click it to play back the video. Click to pause.
	Click it to stop playing back the current video.
	Click it to slow down the video to play at× (1/2), × (1/4) or× (1/8). Click to restore to normal playing speed.
	Click it to speed up the video to play at× 2, × 4, or× 8. Click to restore to normal playing speed.
	Click it to play back the next frame.

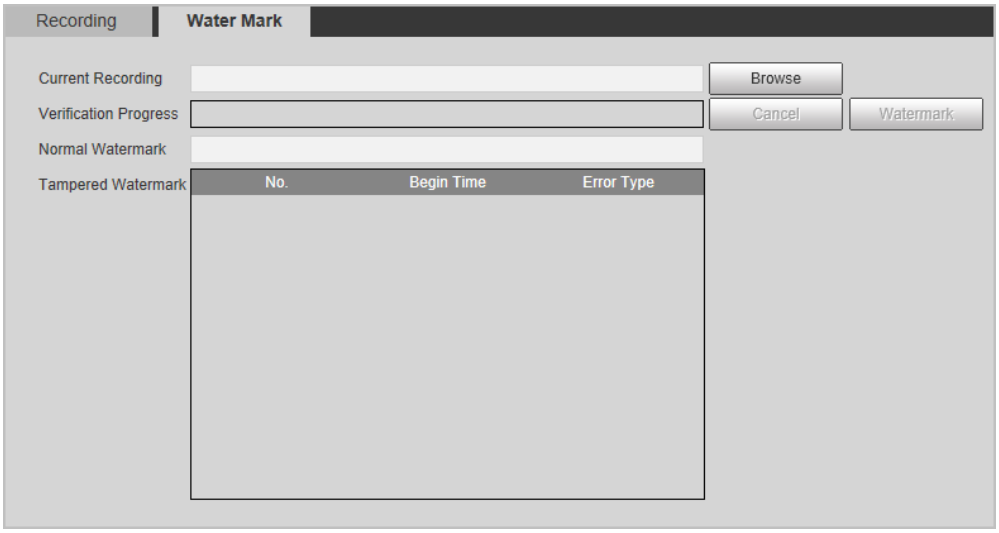
4.3.2 Watermark

Verify the watermark of selected video recordings. Only .dav recording is supported.

Before verifying the watermark, you need to select **Watermark Settings** and configure **Watermark Character** from **Setting > Camera > Video > Video > Main Stream**. The watermark character is **DigitalCCTV** by default.

Step 1 Select **Query > Record Query > Water Mark**.

Figure 4-6 Watermark



Step 2 Click **Browse** to select a recording.

Step 3 Click **Watermark**. The system will display the verification progress and normal watermark information.

5 Settings

You can configure camera attributes to make the Camera clearly display the monitoring image of the scenario, set the detection rules to make the Camera detect violations (such as running a red light, not yielding to pedestrians, and speeding, and more), set the network parameters of the Camera, and view device and system information.

5.1 Camera

You can configure camera attributes such as brightness, contrast, shutter, metering zone and focus.

5.1.1 Attributes

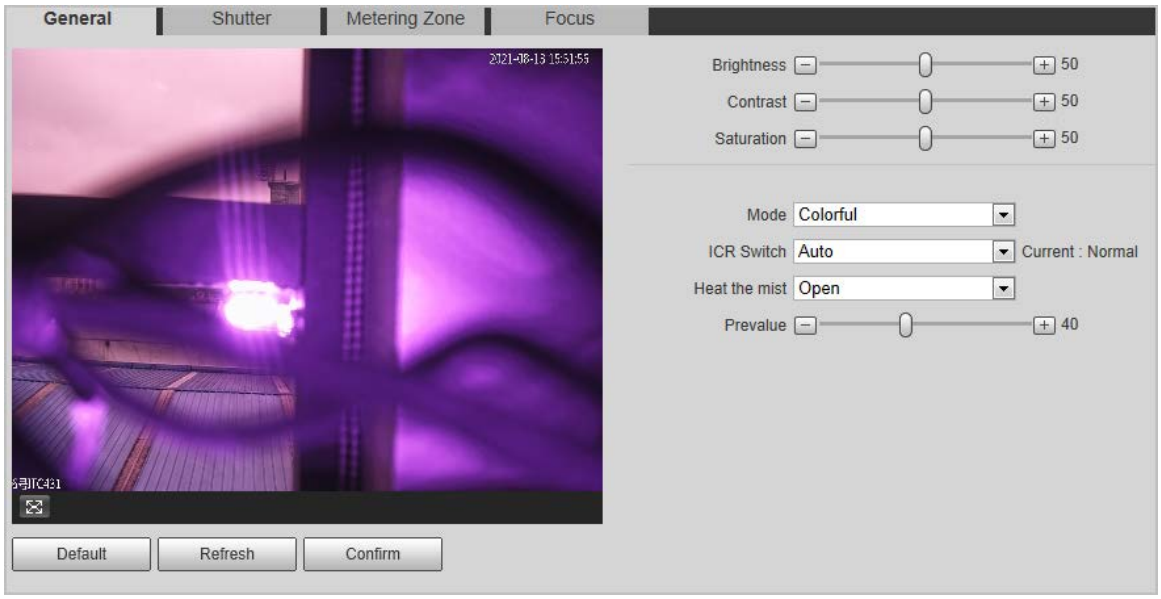
After connecting the Camera to the network and viewing the live video on its web page, you can adjust the image parameters of the Camera when necessary to get clear images.

5.1.1.1 Configuring General Parameters

You can configure the brightness, contrast, saturation, mode, and other properties of the Camera.

Step 1 Select **Setting > Camera > Camera Attribute > General**.

Figure 5-1 General



Step 2 Configure the parameters.

Table 5-1 General parameters

Parameter	Description
Brightness	• Both the darker areas and the brighter areas will be changed together when adjusting the brightness. The image might become blurry when the value gets bigger. The recommended range is 40–60, and the available range is 0–100. • It is 50 by default. The larger the value, the brighter the image.
Contrast	• The larger the value, the darker the dark area, and the more exposed the bright area. • The image might become blurry when the value gets smaller. The recommended range is 40–60, and the available range is 0–100. • It is 50 by default. The larger the value, the stronger the contrast.
Saturation	• Saturation value does not change the overall image brightness. • The larger the value, the more saturated the image. • It is 50 by default. The smaller the value, the more unsaturated the image. The recommended range is 40–60, and the available range is 0–100.
Mode	• **Colorful**: The image is always colored. • **Auto Switch by Brightness**: When the brightness is higher than the threshold, the image automatically changes to color; when it is below the threshold, the image changes to black and white. • **B/W**: The image is always black and white.
ICR Switch	• **Auto**: You need to pre-set the brightness in this mode. When the ambient brightness is higher than the pre-set value, the CPL will start to work. • **IR** (for IR models) or **Normal** (for white light models): Applicable to scenarios with low brightness.

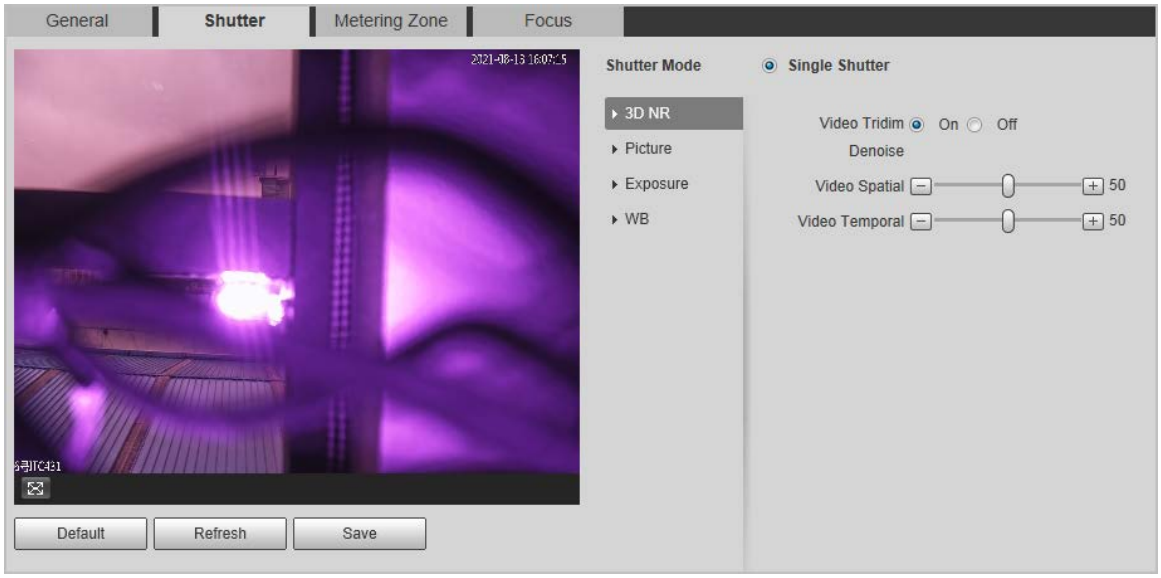
Step 3 Click **Confirm**.

5.1.1.2 Configuring Shutter

You can configure shutter mode, exposure mode, and gain mode.

Step 1 Select **Setting > Camera > Camera Attribute > Shutter**.

Figure 5-2 Shutter



Step 2 Click **Video Shutter**, **Snap Shutter**, or **Recognition Shutter** to show the parameters related to the shutter. To configure the parameters, refer to the table below.

Recognition Shutter is only available in **Three Shutter** mode.

Table 5-2 Shutter parameters

Parameter	Description
Shutter Mode	
Single Shutter	Video and snapshot share the same exposure mode.
Double Shutter	• **Video Shutter** and **Snap Shutter** can be separately configured. • **Half FPS**: Video and snapshot take half of the frame respectively. • **Full FPS**: Snapshot takes 1frame, and video takes the rest of the frames.
Three Shutter	**Video Shutter** and **Snap Shutter** can be separately configured, and a **Recognition Shutter** is added. **Three Shutter** mode is available only when **Common Mode** is selected as **Snap Match Mode** from **Setting > Event > ANPR Snap > Other Settings**.
3D NR	
Video Tridim Denoise	When it is **On**, 3D NR is enabled to reduce noise of video/snapshot.
Video Spatial	Spatial video denoising. The higher the value, the less noise there is.
Video Temporal	Temporal video denoising. The higher the value, the fewer the flicker noise.
Picture	
Scene	You can change the scene and adjust the sharpness of the corresponding scene. Scenes available: **Dawn/Dusk**, **Daytime**, and **Night**.
Sharpness	You can set the sharpness of the corresponding scene. The higher the value, the clearer the image. But there will be noise if the sharpness is too high.
WDR	Select **On** to enable WDR (wide dynamic range), which helps provide clear video images in bright and dark light.
Exposure	
Mode	• In **Auto** mode, only **Manual** iris type is available. • In **Force** mode, several iris types are available, and you also need to configure the **Iris Adjust Mode**, which includes: **Auto** and **Manual**. If **Manual** is selected, you can manually drag the slider to adjust the value.
Iris Type	Displays the detected iris type.
Mode	Select the way of adjusting exposure mode. You can select from **Manual** and **Auto**.
Shutter	You can select the shutter value, or select **Customized Range**, and then set the shutter range. You need to configure shutter when **Mode** is set to **Manual**.

Parameter	Description
Shutter Scope	Set the time range of shutter. You need to configure shutter when **Shutter** is set to **Customized Range**.
Gain Scope	Set the value range of gain. You need to configure gain scope when **Mode** is set to **Manual**.
WB	
Mode	Set scene mode to adjust the image to its best status.

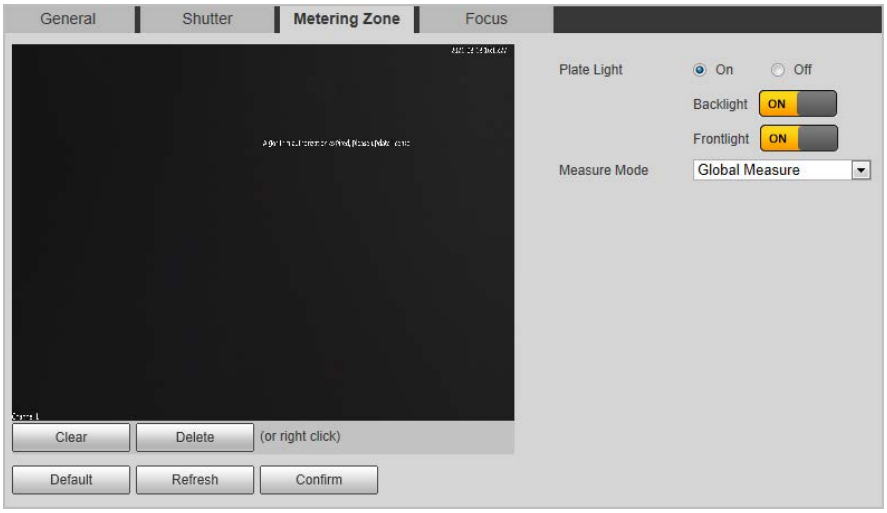
Step 3 Click **OK**.

5.1.1.3 Configuring Metering Zone

This section provides guidance on setting the measure mode of metering zone.

Step 1 Select **Setting > Camera > Camera Attribute > Metering Zone**.

Figure 5-3 Metering zone



Step 2 Configure the parameters.

Table 5-3 Metering zone parameter description

Parameter	Description
Plate Light	When selecting **On**, you can turn on backlight and frontlight according to scene requirements to improve the backlight and frontlight image brightness.
Backlight	
Frontlight	
Measure Mode	• **Global Measure**: Measure the brightness of the whole image area and intelligently adjust the overall image brightness. • **Partial Measure**: Measure the brightness of sensitive areas and intelligently adjust the overall image brightness. If the measured area becomes bright, then the whole area becomes dark, and vice versa. Drag the mouse to select the measured area and a yellow box displays over the video image. Drag the box to a proper location, and then click **Confirm** to complete configuration.

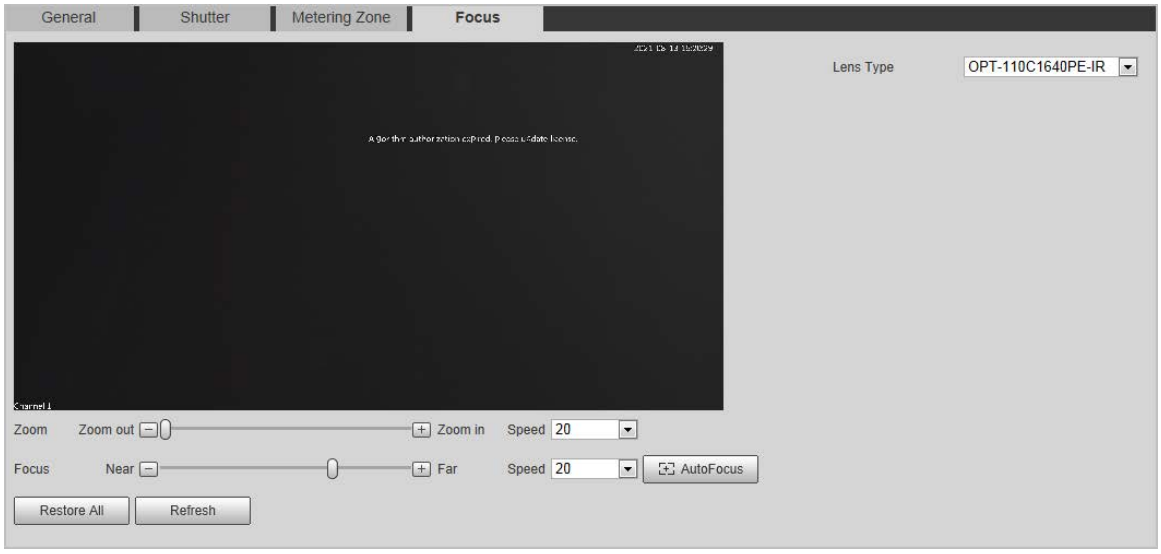
Step 3 Click **Confirm**.

5.1.1.4 Configuring Focus

Adjust the focus of the Camera.

Step 1 Select **Setting > Camera > Camera Attribute > Focus**.

Figure 5-4 Focus



Step 2 Configure the parameters.

Table 5-4 Description of focus parameters

Parameter	Description
Lens Type	The type of the Camera lens. Select **Manual** to restart the Camera when the lens is not standard.
Zoom	Drag the slider to zoom in or out the video image at the selected speed.
Focus	Drag the slider to adjust the camera focus at the selected speed.
Speed	Set the speed of adjusting the value of zoom in/out and focus.
Auto Focus	Automatically adjusts the camera focus to get clear images.

Step 3 Click **Confirm**.

5.1.2 Video

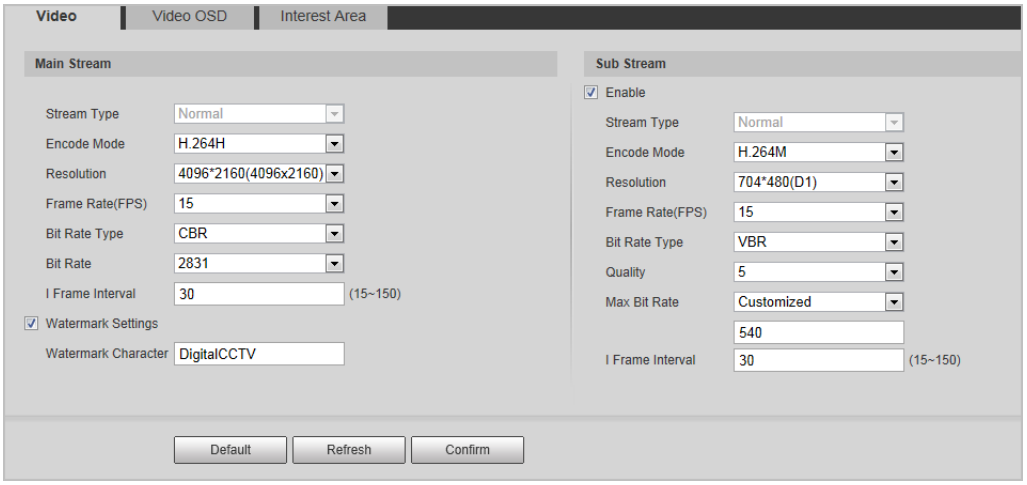
After connecting the Camera to the network and viewing the live video on its web page, you can configure encoding parameters when necessary to get clear and smooth video image.

5.1.2.1 Configuring Video Parameter

Configure the parameters of video stream.

Step 1 Select **Setting > Camera > Video > Video**.

Figure 5-5 Video stream



Step 2 Configure the parameters.

Table 5-5 Video stream parameter

Parameter	Description
Encode Mode	Modes of H.264M, H.264H, MJPEG, and H.265 can be selected.
Resolution	The higher the value, the clearer the overall image. For each resolution, the recommended bit stream value is different. The resolution of sub stream cannot be greater than that of main stream.
Frame Rate (FPS)	The higher the value, the smoother the video image. The frame rate might vary due to different resolutions.
Bit Rate Type	You can select from **VBR** (variable bitrate) and **CBR** (constant bitrate). ● **VBR**: Gives the best balance between quality and file size as the bitrate can be altered depending on the video. ● **CBR** keeps the bitrate the same during encoding, and it is more advantageous to use when the network connection is limited to performing at, for example, 320 Kbps.
Quality	6 quality levels are available. The higher the value, the better the quality. You need to configure the image quality when **VBR** is set to **Bit Rate Type**.
Bit Rate	Higher bit rate signifies greater image or video quality, but also occupies more storage space. You need to configure the bit rate when **CBR** is set to **Bit Rate Type**.
Max. Bit Rate	It is the upper limit of stream in VBR. In CBR, the value is fixed.
I Frame Interval	The number of P-frame between two I-frames. The number varies according to the bit rate. The range is 25–150. We recommend configuring the value to be twice the amount of the bit rate.

Parameter	Description
Watermark Settings	You can verify the watermark to check whether the video has been tampered. Select the **Watermark Settings** checkbox to enable watermark verification. The watermark character is **DigitalCCTV** by default. Watermark character consists of up to 85 characters with numbers, letters and underlines.
Enable	Enable sub stream when your network bandwidth is insufficient or other conditions that influence the video smoothness in main stream.

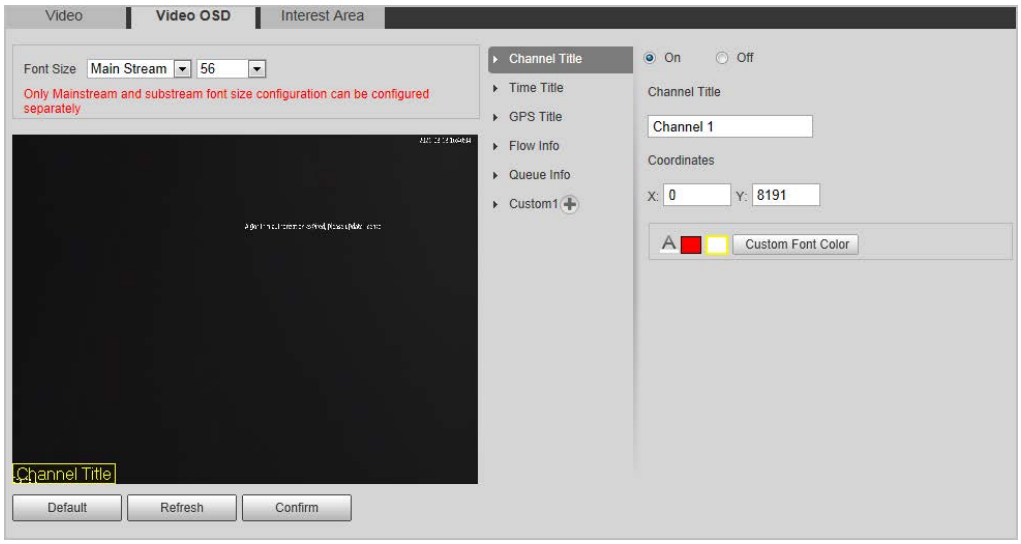
Step 3 Click **Confirm**.

5.1.2.2 Configuring Video OSD

Configure the OSD information of videos.

Step 1 Select **Setting > Camera > Video > Video OSD**.

Figure 5-6 Video OSD



Step 2 Configure parameters.

Table 5-6 Description of video OSD parameters

Parameter	Description
Font Size	Set the font size of **Main Stream** or **Sub Stream**.
Channel Title	Enable the function and set the channel title, coordinates and font color (can be customized) of channel information OSD.
Time Title	Enable the function and set the coordinates and font color (can be customized) of time information OSD. You can select **Display Week Info** to display week information on the video image.
GPS Title	Enable the function and set the coordinates and font color (can be customized) of channel information OSD.
Flow Info	Enable the function and set the coordinates and font color (can be customized) of flow information OSD.
Queue Info	Enable the function and set the font color (can be customized) of queue information OSD.

Parameter	Description
Custom	Enable the function and set the coordinates, custom title and font color (can be customized) of custom information OSD. You can add up to 5 custom titles.

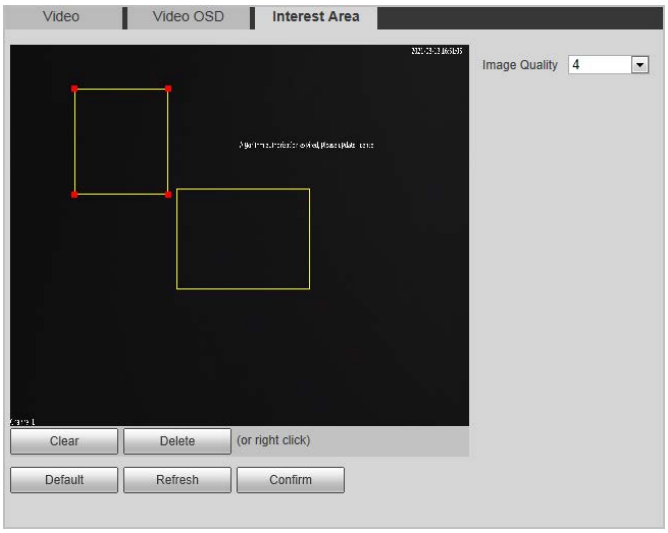
Step 3 Click **Confirm**.

5.1.2.3 Interest Area

Set the region of interest in the video image, and then the selected image will be displayed with the configured quality.

Step 1 Select **Setting > Camera > Video > Interest Area**.

Figure 5-7 Interest area



Step 2 Drag anywhere in the video image to draw the region of interest. You can draw more than one region when necessary.

You can click **Clear** to delete all the regions of interest, or click **Delete** or right-click on the video image to delete the most recently drawn area.

Step 3 Set the image quality of the regions of interest. 6 quality levels are available. The higher the value, the better the quality.

Step 4 Click **Confirm**.

5.2 Network

You can configure network parameters such as IP address, subnet mask, default gateway, and more.

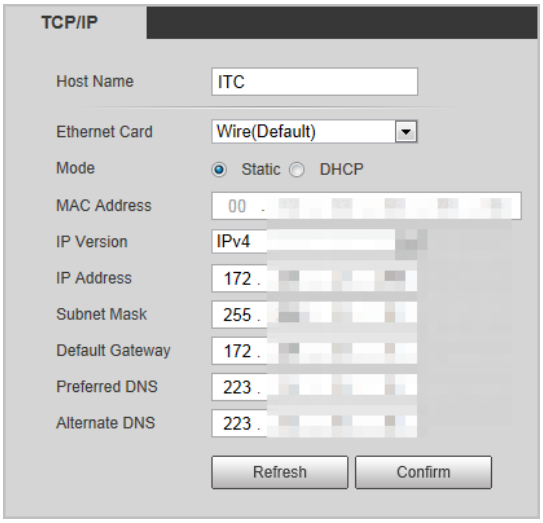
5.2.1 Configuring TCP/IP

You can configure host name, IP address, and more.

Step 1 Select **Setting > Network > TCP/IP**.

Some models are designed with two network ports. Do not configure the ports to be on the same network segment; otherwise, the network might fail.

Figure 5-8 TCP/IP



Step 2 Configure the parameters.

Table 5-7 TCP/IP parameters

Parameter	Description
Host Name	Configure the host name (not exceeding 32 characters).
Ethernet Card	Supports wired network only.
Mode	● **DHCP**: The camera automatically searches IP. In this case, the **IP Address**, **Subnet Mask**, and **Default Gateway** cannot be configured. ● **Static**: The **IP Address**, **Subnet Mask**, and **Default Gateway** need to be manually configured.
MAC Address	Displays host MAC address.
IP Version	IPv4 and IPv6 are available. Both IP versions can be accessed.
IP Address	IP address of the Camera.
Subnet Mask	The subnet mask that masks the IP address of the Camera.
Default Gateway	The default gateway corresponding to IP address of the Camera.
Preferred DNS	IP address of preferred DNS.
Alternate DNS	IP address of alternate DNS.

Step 3 Click **Confirm**.

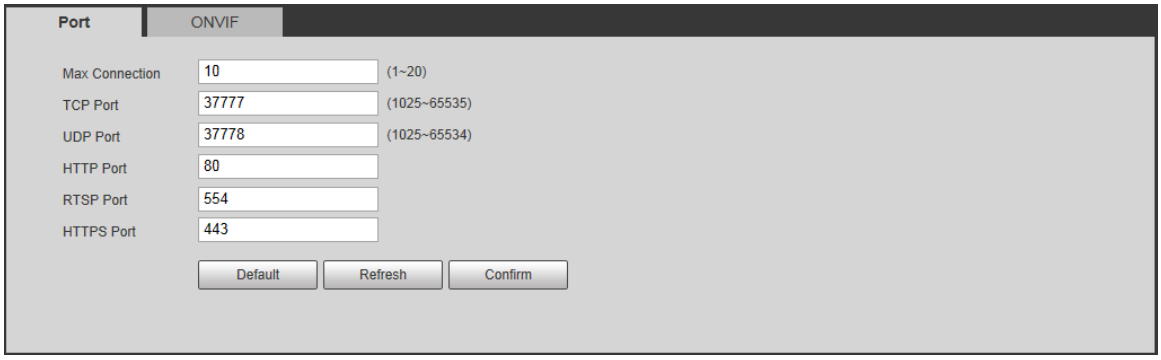
5.2.2 Port

5.2.2.1 Configuring Port

You can set the port information, so you can access the Camera through different protocols or configuration tools.

Step 1 Select **Setting > Network > Port > Port**.

Figure 5-9 Port



Step 2 Configure the port number of the Camera for each protocol.

Table 5-8 Port parameters description

Parameter	Description
Max Connection	The maximum number of clients (such as web client and platform client) that is allowed to access the Camera simultaneously. It is 10 by default.
TCP Port	TCP protocol communication port. It is 37777 by default.
UDP Port	User data packet protocol port. It is 37778 by default.
HTTP Port	HTTP communication port. It is 80 by default.
RTSP Port	Media streaming control port. It is 554 by default.
HTTPS Port	HTTPS communication port. It is 443 by default.

Step 3 Click **Confirm**.

5.2.2.2 Configuring ONVIF

Open Network Video Interface Forum (ONVIF) is an open industry forum with the goal of providing and promoting standardized pages for interoperability of physical IP-based security products, such as IP camera, and network recorder, and more.

Select **Setting > Network > Port > ONVIF**.

Verification of username and password will be required for logging in to ONVIF when ONVIF authentication is turned on. If it is turned off, then no verification is required.

Figure 5-10 ONVIF

5.2.3 Configuring Auto Registration

When the Camera is connected to the network, it will automatically report its location to the server specified by the user. This helps client software to access the Camera through the server for viewing and monitoring the live video.

Step 1 Select **Setting > Network > Auto Register**.

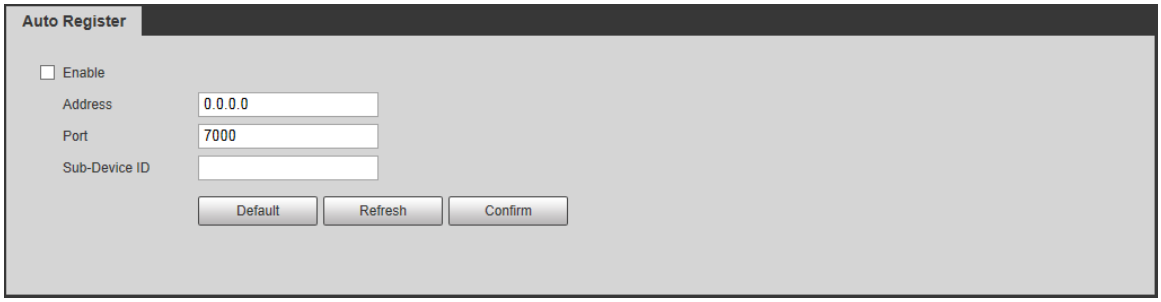
Step 2 Select the **On** checkbox to enable auto registration function.

Step 3 Enter the IP address of server that needs to be registered, and also the port for auto registration.

Step 4 Enter the **Sub-Device ID**, meaning the device ID assigned by the server for auto registration. Make sure that there are no repeated device IPs.

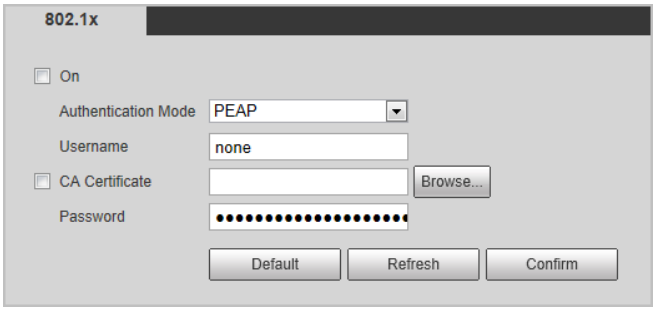
Step 5 Click **Confirm**.

Figure 5-11 Auto register



5.2.4 Configuring 802.1x

Figure 5-12 802.1x



5.3 Remote Device

Remote device (such as enforcement camera or IP camera) information will be displayed on the **Remote Device** page if any of such devices is in use. You can enable the remote device to work with the Camera to capture events. Currently, only events of crossing the stop line and running a red light can be captured by combining the Camera and remote device.

This function is available only in **E-Police** mode.

Step 1 Select **Setting > Remote Device > Remote Config**.

Step 2 Select a remote device, and then click .

Step 3 Select **Remote Device Enable** to enable using the remote device, and modify other device information, such as name, IP address, login username and password.

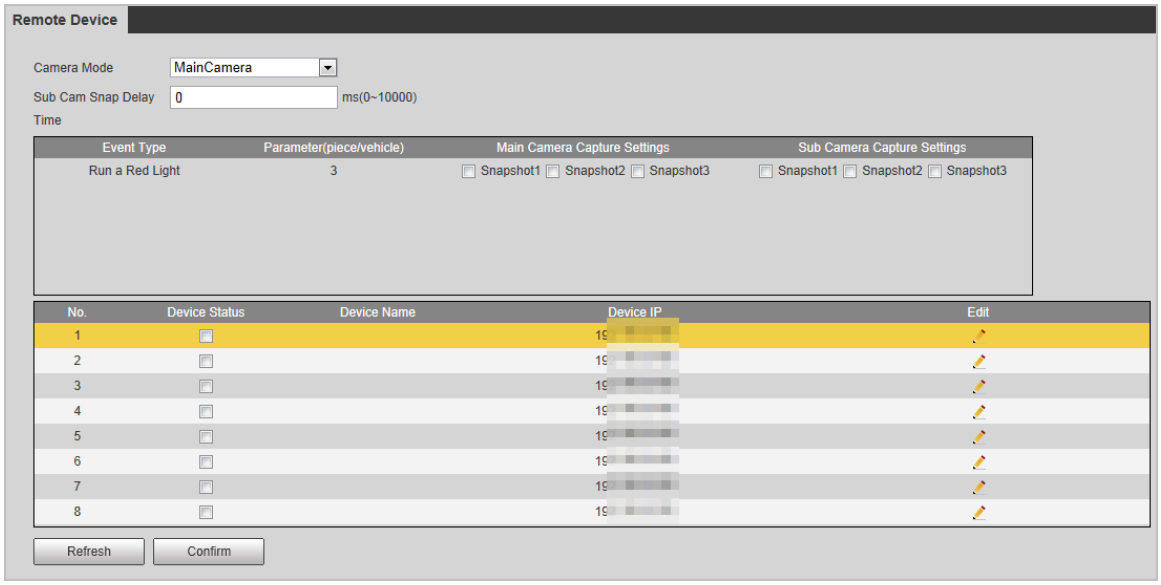
Step 4 Select **Rear Capture Enable** to enable snapshot by the Camera.

Step 5 Select the snapshots from the Rear Camera Capture Settings and Front Camera Capture Settings columns.

- Rear camera refers to the Camera, and it captures feature images, such as face, license plate. Front camera refers to the remote device, and it captures event images.
- When IP camera is connected, you can select at most 3 and 2 snapshots respectively from the **Rear Camera Capture Settings** and **Front Camera Capture Settings** columns; if enforcement camera is camera is connected, you can select at most 3 and 1 snapshots respectively.
- If a storage device is used, the snapshots captured by the Camera and the remote device will be composited, and saved to the storage device. If no, the snapshots will be saved to the storage path defined on the web page of each device.

Step 6 Click **Confirm**.

Figure 5-13 Remote device



5.4 Event

You can configure how the Camera responds when alarms or abnormal events occur.

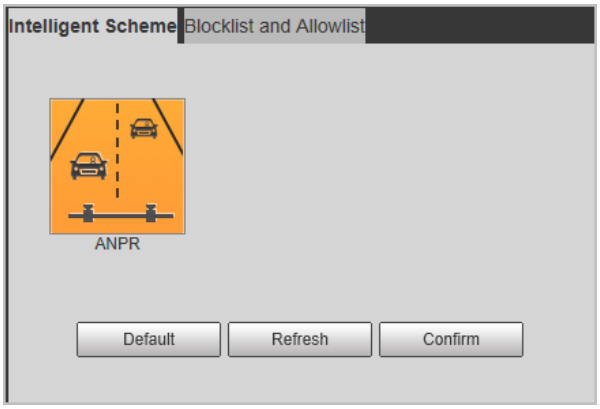
5.4.1 Intelligent Scheme

5.4.1.1 Switching between E-police and ANPR

ANPR is applicable to road sections without signal lights to detect violations such as speeding, driving slow, not wearing seat belt, calling while driving, and more. See "5.4.2 Configuring ANPR Snap".

Select **Setting > Event > Intelligent Scheme > Intelligent Scheme**.

Figure 5-14 Select a working mode



5.4.1.2 Configuring and Searching Blocklist and Allowlist

An alarm is triggered when a vehicle is detected in the blocklist. A vehicle in the allowlist will not be captured.

5.4.1.2.1 Fuzzy Matching

You can enable fuzzy matching for allowlist. In this way, if the fuzzy matching result shows that the number plate of a vehicle is in the allowlist, the vehicle will not be captured and there will be no alarm.

Step 1 Select **Setting > Event > Intelligent Scheme > Blocklist and Allowlist > Fuzzy Matching**.

Step 2 Select **On** to enable the allowlist.

Step 3 Select **Fuzzy Matching** to enable fuzzy matching.

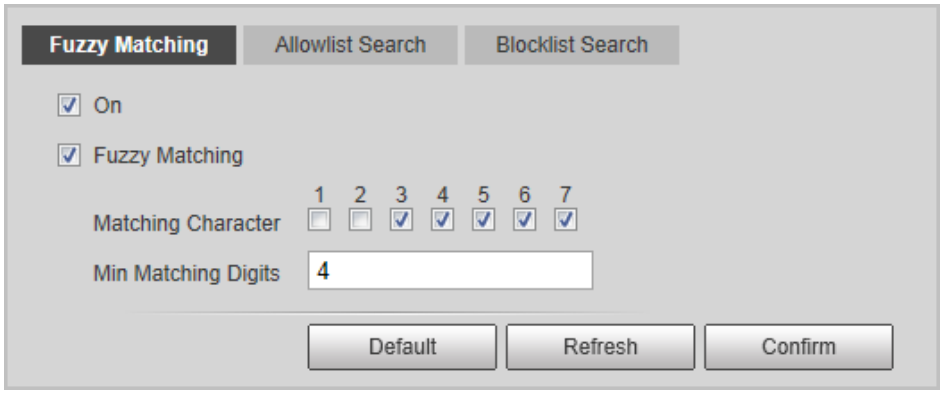
Step 4 Configure matching rule.

- **Matching Character**: The specific digit(s) that should be exactly matched.
- **Min Matching Digits**: The minimum number of digits that should be exactly matched.

For example, if you select 1, 2 and 4 for **Matching Character** and enter 2 for **Min Matching Digits**, the system will successfully recognize a vehicle when any two among Digit 1, 2, and 4 are exactly matched.

Step 5 Click **Confirm**.

Figure 5-15 Set fuzzy matching



5.4.1.2.2 Allowlist Search

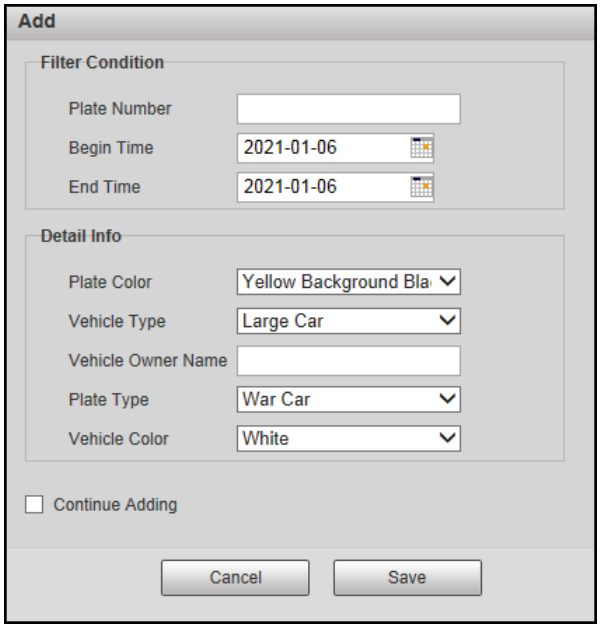
You can search to see whether a plate number is included in the allowlist, or you can import or export plate numbers in the allowlist.

Step 1 Select **Setting > Event > Intelligent Scheme > Blocklist and Allowlist > Allowlist Search**.

Step 2 Add a number plate.

1) Click **Add**.

Figure 5-16 Add



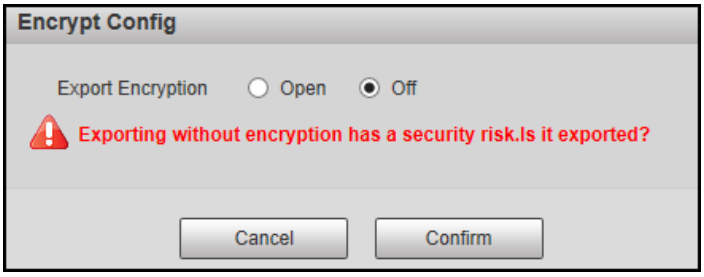
2) Enter the entire plate number.
3) Set the start time and end time to add the plate number in the allowlist. The plate number will be outside of the allowlist beyond this time period.
4) Select the plate color, vehicle type, plate type and vehicle color. Enter the owner of vehicle.
5) Click **Save**.
   To save and add more, select **Continue Adding** before clicking **Save**.

You can also:

- Search for a plate number: Enter the plate number (or part of it) that you want to search for, and then click **Search** to check whether it is in the allowlist.

- Modify plate information: Click **Modify** to modify detailed information of the corresponding plate number. Click **Confirm** to save the settings.
- Delete a plate number: Click **Delete** to delete the corresponding plate number.
- Delete plate number in batches: Click **Clear All**, and then click **Confirm** in the pop-up box to delete all the information in the allowlist.
- Import allowlist plates in batches: Click **Browse**, and then select the path to import the file to. Click **Import** to import the allowlist information to the system.
- Export allowlist plates in batches: Click **Export**, and then select the path to save the file to. Click **Export** to export the allowlist information to the system.
- You can encrypt the file when importing and exporting the allowlist, depending on your actual needs.

Figure 5-17 Encrypt config



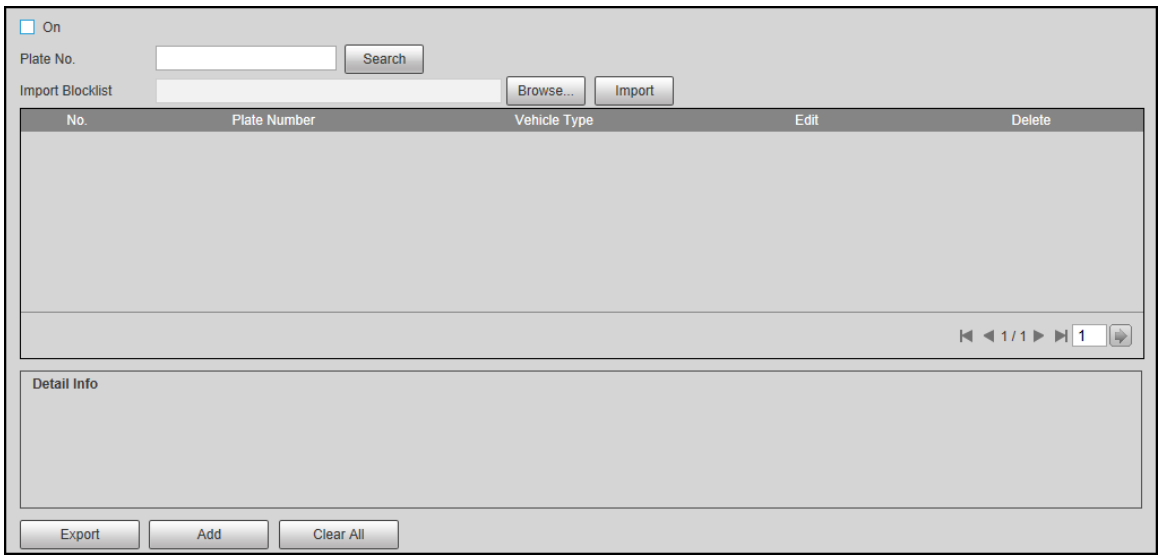
5.4.1.2.3 Blocklist Search

An alarm will be triggered when a vehicle in the blocklist is detected.

Select **Setting > Event > Intelligent Scheme > Blocklist and Allowlist > Blocklist Search**, and then select **On** to enable the blocklist function.

The search, import, and export of blocklist are similar to that of allowlist. See "5.4.1.2.2 Allowlist Search".

Figure 5-18 Blocklist search



5.4.2 Configuring ANPR Snapshot

Configure ANPR parameters.

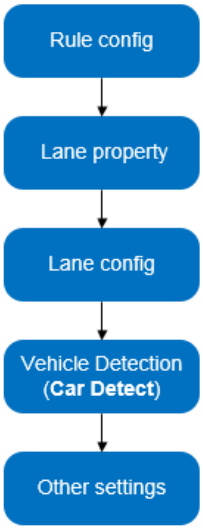
Make sure that you have set **Intelligence Scheme** to **ANPR**. For details, see "5.4.1.1 Switching between E-police and ANPR".

5.4.2.1 Configuring Violation Capture

Configure the video detection parameters for detecting traffic violations.

Follow this order to configure violation capture: Rule config > lane property > lane config > vehicle detection (**Car Detect**) > other settings. This is described separately in the configuration order below.

Figure 5-19 Configuration order for violation capture

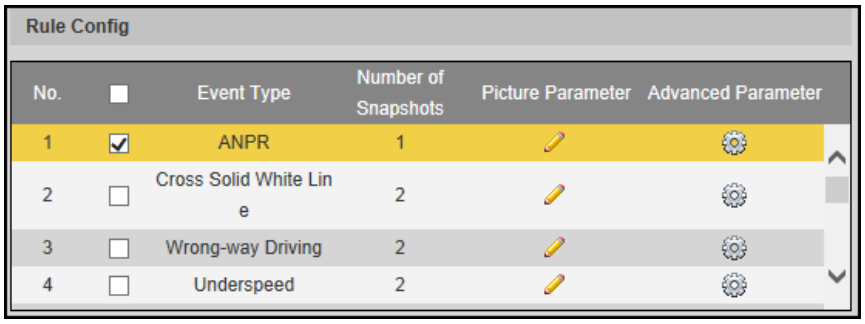


5.4.2.1.1 Rule Configuration

You can select the traffic violation types and configure the corresponding parameters of the images of the offending vehicle.

Step 1 Select **Setting > Event > ANPR Snap > Illegal Capture > Rule Config**.

Figure 5-20 Rule config



Step 2 Click , and then configure picture parameters.

The parameter table describes the parameters involved in all event types, and might differ from the actual page.

Figure 5-21 Configure picture parameter

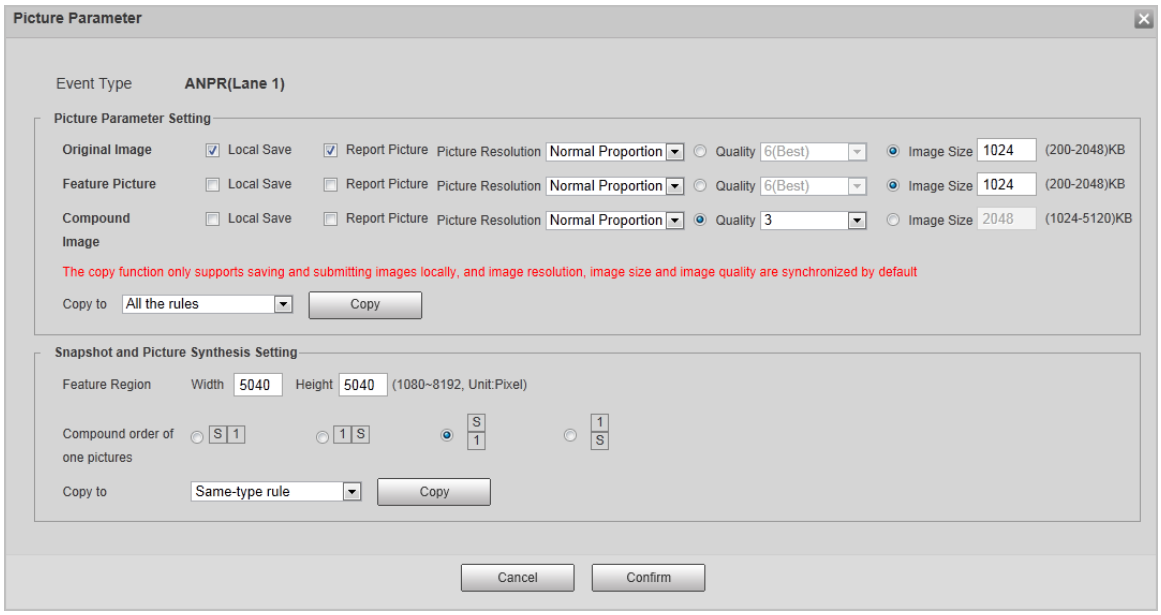


Table 5-9 Picture parameter

Category	Name	Description
Picture Parameter Setting	Original Image	The original picture of the vehicle that is violating traffic rules.
	Compound Image	The compound picture of several sequential images of the vehicle violating the traffic rules.
	Feature Picture	The close-up of the offending vehicle.
	Local Save	Save the vehicle picture locally when an offending vehicle is captured.
	Report Picture	Upload the vehicle picture to the upper-level device or platform when a vehicle is captured.
	Picture Resolution	Select picture resolution.
	Quality	Select the level of picture quality.
	Image Size	Limit the size the picture.
	Copy to	Copy the current picture parameter setting to the same-type rules or all the rules. After selecting an option from **Copy to**, click **Copy**.

Category	Name	Description
Snapshot and Picture Synthesis Setting	Feature Region	Centering on the vehicle, enter the height and width of the close-up of the vehicle.
	Compound order of one pictures	Select the layout of the compound picture. The picture consists of 1 original image proving the vehicle offending traffic rule and one close-up of the vehicle. ● **S**: Close-up ● **1**: Original images

Step 3 Click **Confirm**.

Step 4 Click , and then configure advanced parameters.

The parameter table describes the parameters involved in all event types, and might differ from the actual page.

Figure 5-22 Advanced parameters

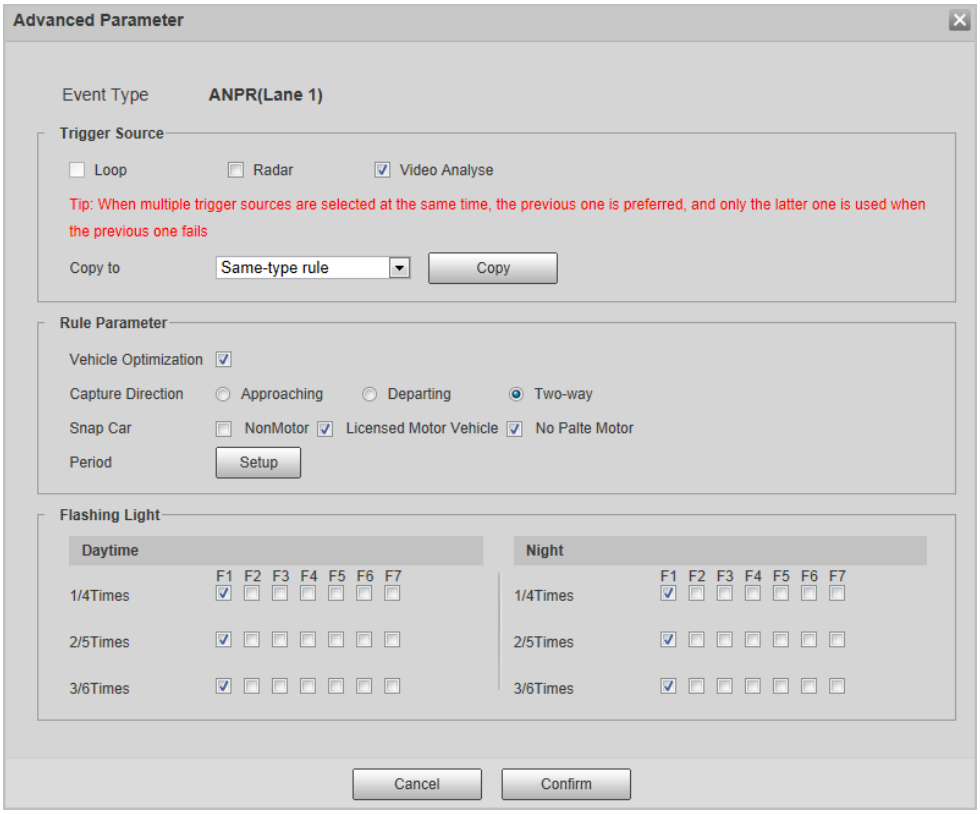


Table 5-10 Advanced parameter description

Category	Name	Description
Trigger Source (The way to trigger vehicle capture)	Loop	Unavailable
	Radar	The system captures offending vehicles upon the radar detecting a violation.
	Video Analyse	The system analyzes the real time video to detect traffic violations. Once a violation is detected, the system automatically captures images of the offending vehicle.

Category	Name	Description
	Copy to	Copy the current setting to the same-type rules or all the rules. After selecting an option from **Copy to**, click **Copy**.
Rule Parameter	Capture Direction	Vehicle driving direction to the camera
	Period	The period during which the alarm is valid. To set time, you can click **Setting**, and then drag your cursor over the time table or select days and enter hours in the entry fields.
	Snap Car	The vehicle types to snap.
Flashing Light	Daytime	Select which flashing light flashes when snapshots are taken during daytime or night. A snapshot can be associated with up to 5 flashing lights. For example, select **F1** from the **1/4Times** section, meaning flashing light F1 flashes when taking the 1st and 4th snapshots.
	Night	

Step 5 Click **Confirm**.

5.4.2.1.2 Lane Property

Step 1 Select **Setting > Event > ANPR Snap > Illegal Capture > Lane Property**.

Step 2 Configure lane parameters.

Figure 5-23 Lane property

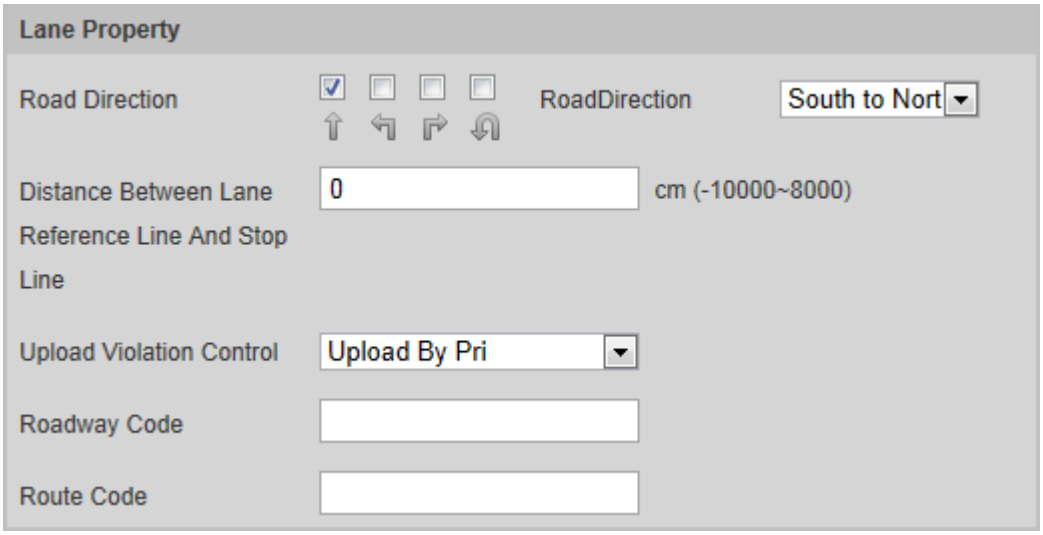


Table 5-11 Lane property description

Parameter	Description
Road Direction	The direction of the lane.
RoadDirection	The geographical direction of the lane.

Parameter	Description
Distance Between Lane Reference Line And Stop Line	The distance between the bottom of the video image and the stop line (where the traffic post is).
Roadway Code	The code of the roadway and route.
Route Code	

Step 3 Click **Confirm**.

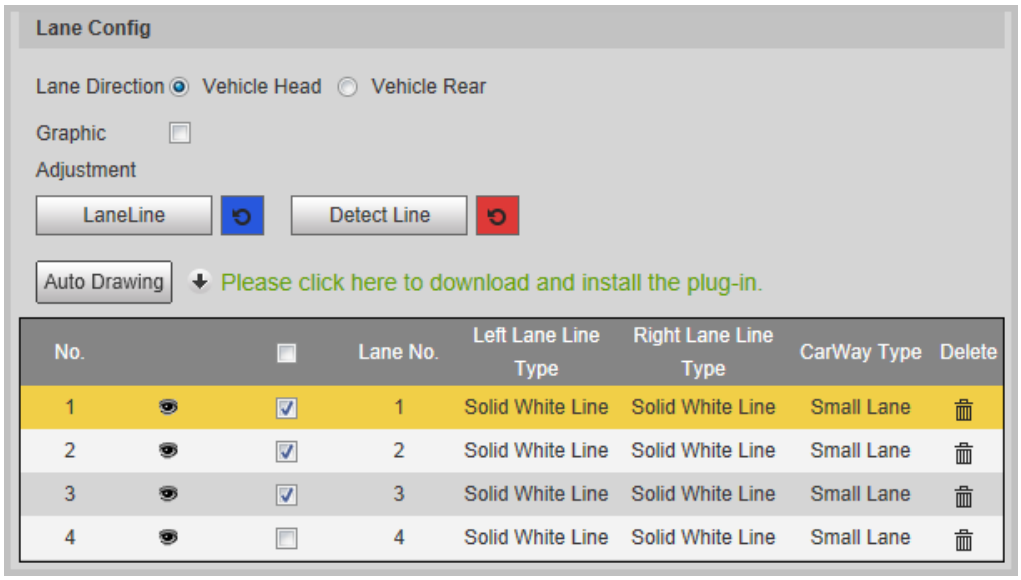
5.4.2.1.3 Lane Parameters

Configure lane information and events that you desire the Camera to detect.

Step 1 Select **Setting > Event > ANPR Snap > Illegal Capture > Lane Config**.

Step 2 Configure lane parameters.

Figure 5-24 Lane config



Click to select a lane and then all configurations on the **Illegal Capture** are for this lane.

Table 5-12 Lane config parameters

Parameter	Description
Lane Direction	The arrow direction of the lane line needs to be the same as that of the travelling vehicle. • **Vehicle Rear**: Lane line arrow is upward. • **Vehicle Head**: Lane line arrow is downward.
Graphic Adjustment	Select the checkbox to enable the function, and then you can adjust the lane lines by dragging the corners on the image.

Step 3 Click a line type, and then draw the lane lines on the image.

To clear the lane lines or regions that you have drawn, click .

Table 5-13 Lane line description

Parameter	Description
LaneLine	Each lane needs to have two lane lines, shown as blue lines with arrows indicating the direction in which the vehicles travel. The drawn lines should go along the actual lane line.
Detect Line	The line that will trigger vehicle capture if reached. The detect line is red.
Auto Drawing	Install the plug-in before using the **Auto Drawing** function. Click **Auto Drawing**, and then the system automatically draws lane lines. You can adjust the auto lines as needed.

Step 4 Click to select and show a lane on the video image.

Step 5 Click **Confirm**.

5.4.2.1.4 Car Detect

Step 1 Select **Setting > Event > ANPR Snap > Illegal Capture > Car Detect**.

Step 2 Click the line or region type, and then draw on the video image.

- To draw a line, click the line type and then drag your mouse cursor on the image.
- To draw a region, click the region type, and then draw the lines by dragging your cursor on the image and make them form a closed region.

To clear the lines that you have drawn, click .

Figure 5-25 Line or region types

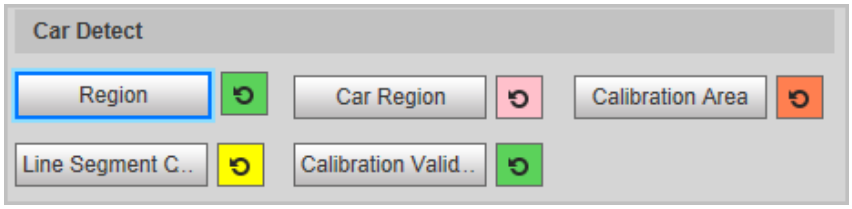


Table 5-14 Car detect description

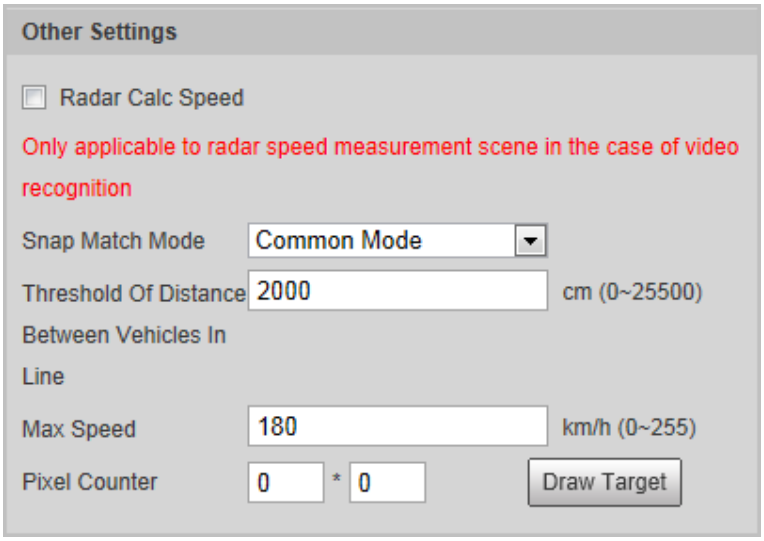
Parameter	Description
Region	The region of detection.
Car Region	The region for detecting vehicle volume.
Calibration Area	The region for analyzing vehicle traffic.
Line Segment Calibration	Used to verify the accuracy of calibration results. Click **Line Segment Calibration** to draw the calibration segment in the calibration area, enter the actual length of the calibration segment in the pop-up page, and then click **Calibration Validation**.
Calibration Validation	Used to verify the accuracy of calibration results.

Step 3 Click **Confirm**.

5.4.2.1.5 Other Settings

Step 1 Select **Setting > Event > ANPR Snap > Illegal Capture > Other Settings**.

Figure 5-26 Other settings



Step 2 Configure parameters.

Table 5-15 Other settings description

Parameter	Description
Radar Calc Speed	Use radar to measure vehicle speed.
Snap Match Mode	• **Common Mode**: Recommended for the ANPR snap mode. • **Priority Mode**: Recommended for the e-police mode.
Threshold Of Distance Between Vehicles In Line	Set the distance between vehicles when waiting in a line.
Max Speed	When the travelling speed exceeds this value, the system automatically changes the vehicle speed to a random value in the normal range.
Pixel Counter	Click **Draw Target**, and then draw a rectangular area on the image to show the pixel size of that area.

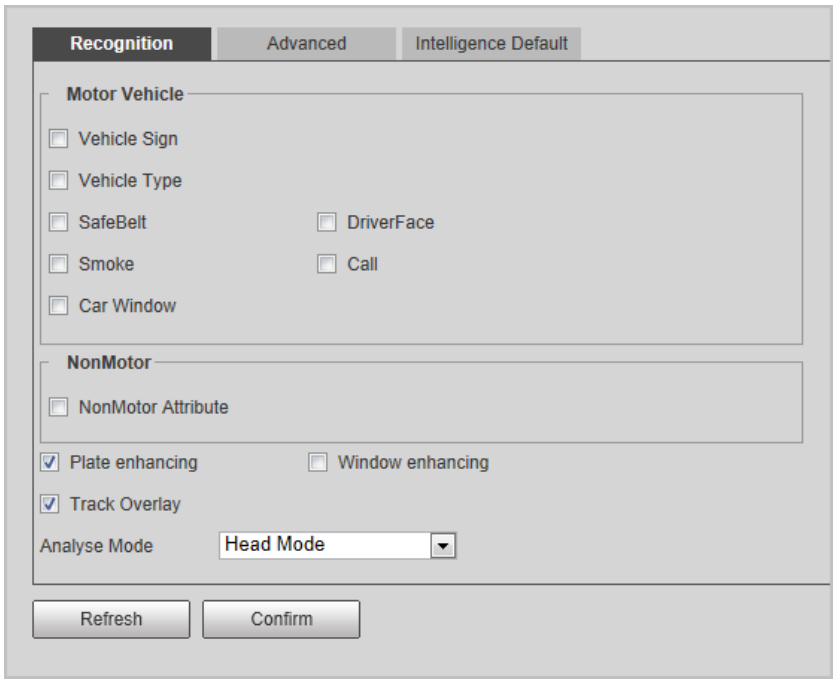
Step 3 Click **Confirm**.

5.4.2.2 Configuring Intelligent Analysis

5.4.2.2.1 Recognition

Step 1 Select **Setting > Event > ANPR Snap > Intelligent Analysis > Recognition**.

Figure 5-27 Recognition



Step 2 Configure parameters.

Table 5-16 Recognition parameters

Parameter	Description
Motor Vehicle	Identify motor vehicle characteristics, driver characteristics, and window objects
NonMotor	Identify non-motor vehicle attributes such as type, helmet, and rider number.
Plate enhancing	Enhance number plate image effect.
Window enhancing	Enhance vehicle window image effect.
Track Overlay	Enable **Track Overlay**, click  on the left side of the **Live** page, and then you can see each vehicle is covered by a green frame, which means each vehicle is traced.
Analyse Mode	The vehicle plate recognition mode. ● **Head Mode**: Recognize and snap the number plate on the vehicle head. ● **Tail Mode**: Recognize and snap the number plate on the vehicle rear. ● **Head Prior Mode**: Head plate has the priority. ● **Tail Prior Mode**: Rear plate has the priority.

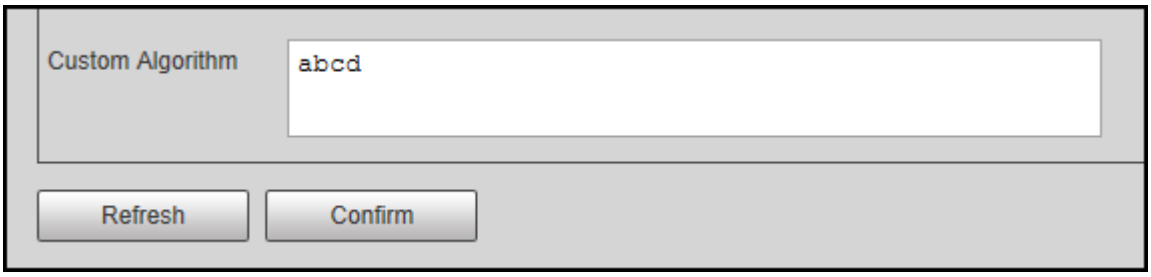
Step 3 Click **Confirm**.

5.4.2.2.2 Advanced

You can make a custom algorithm.

Step 1 Select **Setting > Event > ANPR Snap > Intelligent Analysis > Advanced**.

Figure 5-28 Custom algorithm



Step 2 Configure custom algorithm.

Step 3 Click **Confirm**.

5.4.2.2.3 Intelligence Default

Step 1 Select **Setting > Event > ANPR Snap > Intelligent Analysis > Intelligence Default**.

Step 2 Click **Default** to restore settings including lane property, violation capture and intelligent business to default.

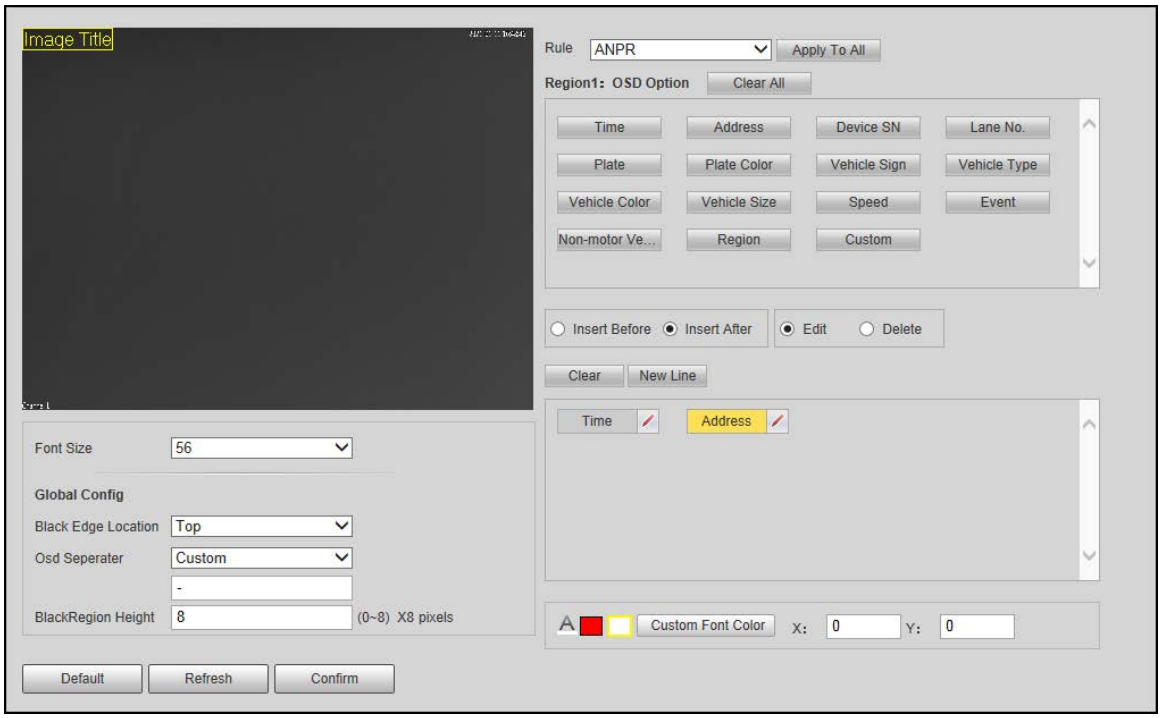
5.4.3 Configuring OSD

5.4.3.1 Configuring Snapshot OSD

Configure OSD content, style and position for captured image.

Step 1 Select **Setting > Event > ANPR Snap >Snapshot OSD**.

Figure 5-29 Snapshot OSD



Step 2 Configure OSD black edge position, black region height, OSD separator, and front size.

Step 3 Select a rule type.

Step 4 Configure OSD parameters.

Table 5-17 Snapshot OSD description

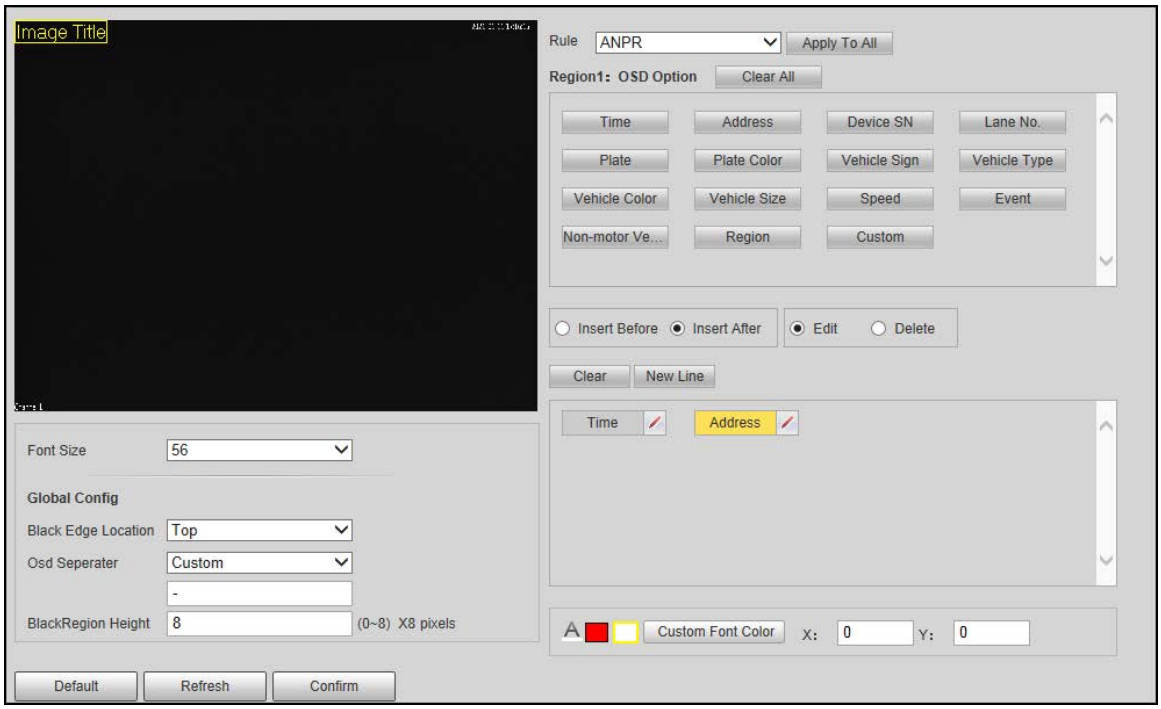
Parameter	Description
Insert Before	Select an OSD option, click **Insert Before**, and then select another OSD option. The new OSD option will be inserted before the original one.
Insert After	Select an OSD option, click **Insert After**, and then select another OSD option. The new OSD option will be inserted after the original one.
Edit	Click **Edit**, and then is displayed next to all the selected OSD options. To edit an OSD option, click the corresponding .
Delete	Click **Clear**, and then is displayed next to all the selected OSD options. To delete an option, click the corresponding
Clear	Delete all the selected OSD options.
New Line	To start a new line after a certain OSD option, click the OSD option, and then click **New Line**.

Step 5 Click **Confirm**.

5.4.3.2 Configuring Merge OSD

Step 1 Select **Setting > Event > ANPR Snap > Merge OSD**.

Figure 5-30 Configuring merge OSD



Step 2 Configure parameters. For details, see Table 5-17.

Step 3 Click **Confirm**.

5.4.4 Configuring Traffic Flow Analysis

5.4.4.1 Traffic Data

You can configure the lane and the period of traffic flow statistics, and then the flow data will be displayed in the **Traffic Flow Data** and **Pedestrian Flow Data** tabs.

Step 1 Select **Setting > Event > ANPR Snap > Traffic Flow > Flow Data**.

Step 2 Select the **Pedestrian Flow Enable** checkbox to enable statistics of pedestrian flow as needed.

Step 3 Set the **Period** and **Flow Upper Limit** of making statistics.

Step 4 Select the lane that you want to make flow statistics.

Step 5 Click **Confirm**.

5.4.4.2 Traffic Flow Data

After enabling traffic flow statistics, you can view the traffic flow data of the defined lane within the defined period by clicking the **Traffic Flow Data** tab. The flow data will automatically update when a period ends.

- Click  to clear the flow information.
- Click **Export** to export the flow information to local PC.

5.4.4.3 Pedestrian Flow Data

After enabling pedestrian flow statistics, you can view the pedestrian flow data of the defined lane within the defined period by clicking the **Pedestrian Flow Data** tab. The flow data will automatically update when a period ends.

- Click  to clear the flow information.
- Click **Export** to export the flow information to local PC.

5.4.5 Cutout

5.4.5.1 Snapshot Cutout

The Camera can recognize and crop snapshots, and save the cutouts.

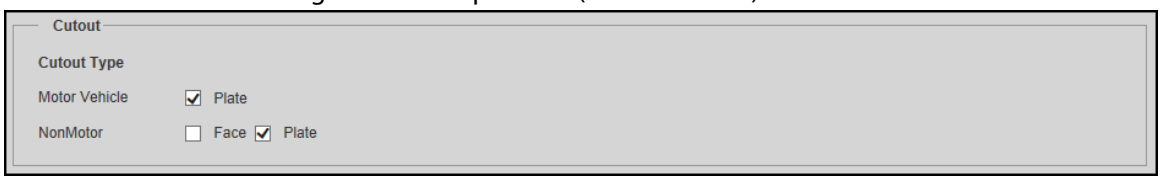
The page and function might vary in **ANPR**, and **E-Police**, and might differ from the actual page and function.

Step 1 Select **Setting > Event > ANPR Snap > Cutout > Cutout**.

Step 2 Select the cutout type.

Step 3 Click **Confirm**.

Figure 5-31 Snap cutout (E-Police mode)



5.4.5.2 Face Overlap

Configure whether to enable overlapping face picture on the snapshots. If overlap is enabled, you can configure the overlap position and size of driver face and front-seat passenger face.

Step 1 Select **Setting > Event > ANPR Snap > Cutout > Face Overlap**.

Step 2 Select **Driver Face Overlap Enable** to enable face overlay of the driver.

Step 3 Configure the overlay position and size of driver face and front-seat passenger face.

Step 4 Click **Confirm**.

5.4.5.3 Track Box

Set whether to overlay track box on the driver of non-motor vehicles.

Step 1 Select **Setting > Event > ANPR Snap > Cutout > Track Box**.

Step 2 Select **On** to enable the overlaying track box.

Step 3 For non-motor vehicle, select overlaying track box on the **Whole** body or only **Face** of the non-motor vehicle driver.

Step 4 Click **Confirm**.

5.4.6 Device Direction

You can view the device position information, such as its longitude and latitude.

Select **Setting > Event > Device Direction**.

5.4.7 Alarm

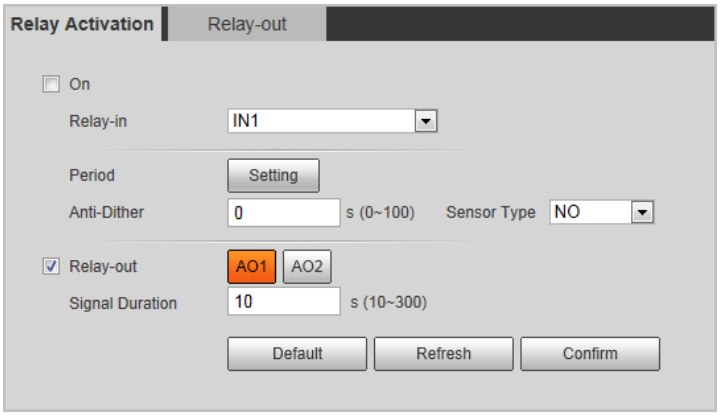
You can configure how the Camera responds when alarms occur.

5.4.7.1 Relay Activation

You can connect the alarm output device to corresponding I/O port.

Step 1 Select **Setting > Event > Alarm> Relay Activation**.

Figure 5-32 Relay activation



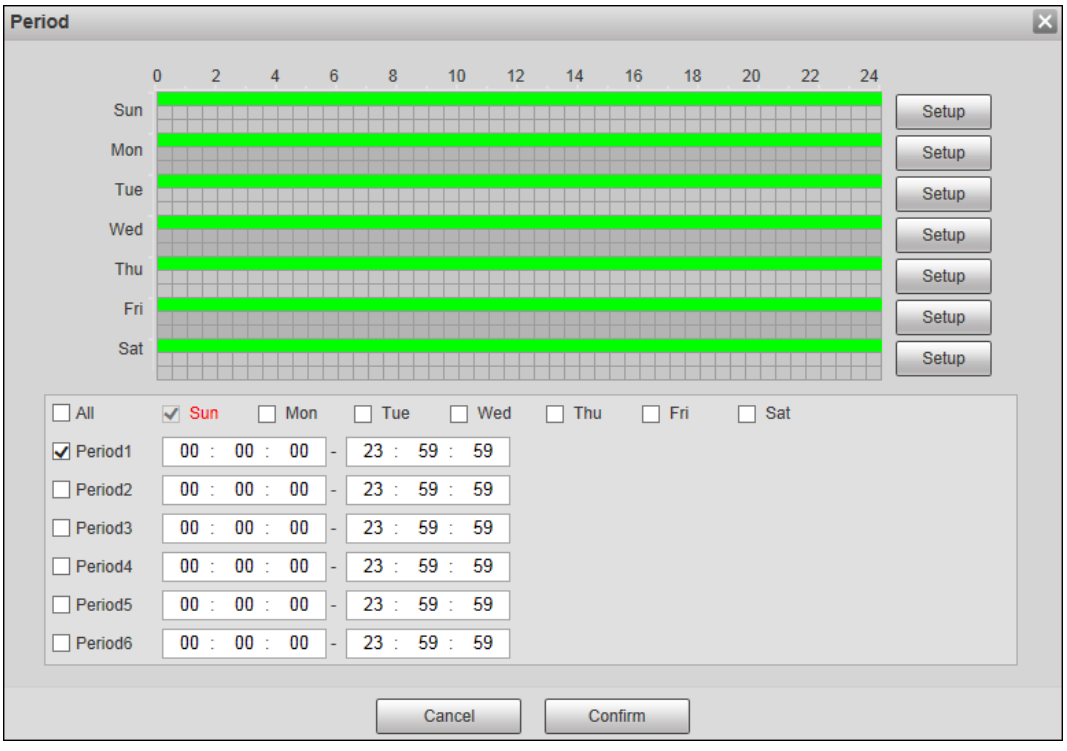
Step 2 Select the **Enable** checkbox to enable alarm input.

Step 3 Configure the parameters.

Table 5-18 Relay activation parameters

Parameter	Description
Relay-in	Currently, only 4 channels support alarm input.
Period	Configure the time of arming and disarming. Click **Setting**, and the **Period** page is displayed. See Figure 5-33. Configure the day and period of arming. Click **Confirm** to save the period settings.
Anti-Dither	The system records only one alarm event within the defined time, and the time range is 0 s–100 s.
Sensor Type	**NO** (normally open) and **NC** (normally closed) are available.
Relay-out	Select the alarm output port.
Signal Duration	The alarm linkage keeps running for the defined time after alarm ends. The time range is 10 s–300 s.

Figure 5-33 Period setting



Step 4 Click **Confirm**.

5.4.7.2 Relay-out

You can simulate to trigger alarm output signal.

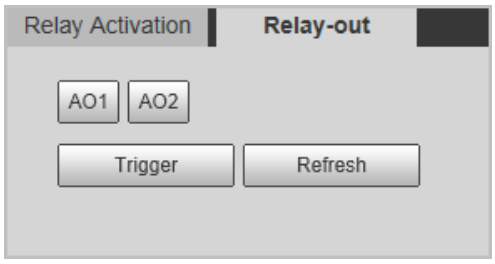
Step 1 Select **Setting > Event > Alarm> Relay-out**.

Step 2 Click **AO1** or **AO2** to configure one-channel alarm output.

Step 3 Click **Trigger** to trigger alarm output.

Step 4 Click **Refresh** to view the status of alarm output.

Figure 5-34 Relay-out



5.4.8 Abnormality

An alarm will be triggered when an abnormal event occurs. The event types include:

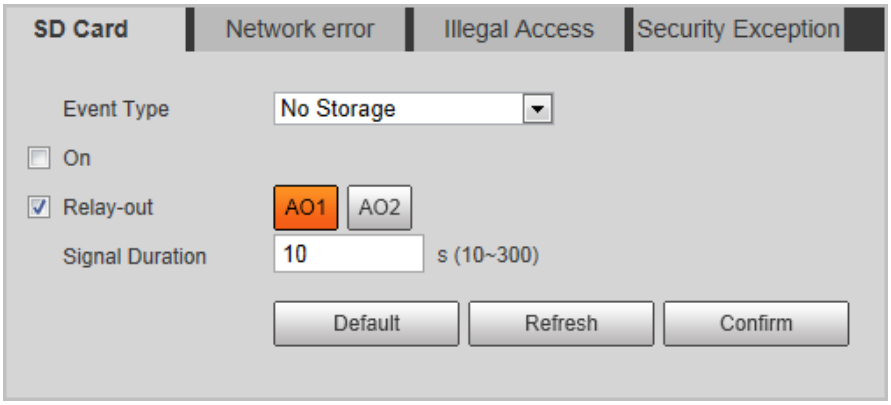
- **SD Card**: Alarm will be triggered when there is **No Storage**, **Storage Error**, or **Scarcity of Storage Space** (no enough storage space).
- **Network Error**: Alarm will be triggered when there is **Off-line Event** (the Camera is offline) or **IP Conflict**.
- **Illegal Access**: Alarm will be triggered when unauthorized access is detected by the system.
- **Security Exception**: Alarm will be triggered when security problem occurs.

You can set the alarm tone by selecting **Alarm** at the upper-right side of the Camera's web page.

Step 1 Select **Setting > Event > Abnormality**.

The following figure uses **SD Card** as an example. For other events, refer to the actual page.

Figure 5-35 SD card event



Step 2 Configure the parameters.

Refer to the actual page to view the parameters that you need to configure for each abnormality.

Table 5-19 Parameters of abnormality events

Parameter	Description
Enable	Select it to enable alarm of abnormality event. Select **Alarm Enable** for **Traffic Light Fault** event in **E-Police** mode.
Relay-out	Select it to enable the corresponding alarm output of event, and select the corresponding port.
Signal Duration	The alarm linkage keeps running for the defined time after alarm ends. The time range is 10 s–300 s.
Capacity Limit	Configure the storage available for triggering abnormality.
Ethernet Card1, Ethernet Card2	Select the Ethernet card that triggers alarm output.
Max Switch Time Value	Configure the maximum time that traffic light remains unchanged. This parameter is required only for **Traffic Light Fault** in **E-Police** mode.
Login Error	Configure the number of login errors allowed. The range is 3–10 times.
Rollover Angel Threshold	Configure the threshold of rollover angle.
Pitch Angle Threshold	Configure the threshold of pitch angle.
Acceleration Threshold	Configure the threshold of acceleration.

Step 3 Click **Confirm**.

5.5 Peripheral

5.5.1 Extra Device Status

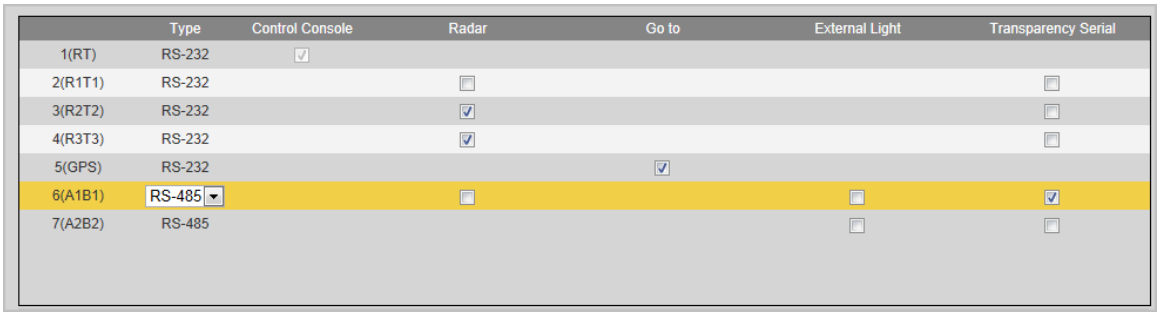
Select **Setting > Peripheral > Extra Device Status**, and then you can view the information related to the external device.

5.5.2 Serial Port Settings

This section displays all serial ports of the Camera, and integrates all devices which can be connected so you can configure them on one page. At present, the Camera supports configuring radar, positioning method, external light and transparency serial.

Step 1 Select **Setting > Peripheral > Serial Port Settings**.

Figure 5-36 Serial port settings

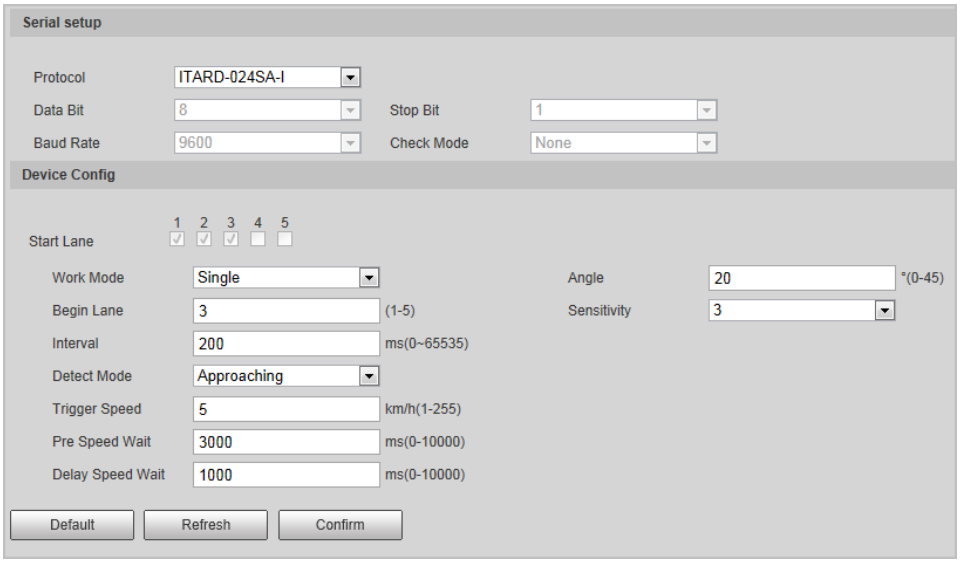


Step 2 Configure external devices.

- One serial port can only enable one external device.
- RA-485 and RS-232 ports are supported.
  - ◇ RS-232 port can enable radar for single lane, and RS-485 enables radar for multiple lanes.
  - ◇ You cannot enable single lane and multiple lanes at the same time.
- Only one external device can be enabled for one port at the same time.
- Radar

1) Select **Radar**.

Figure 5-37 Radar configuration (single lane)



2) Configure radar parameters.

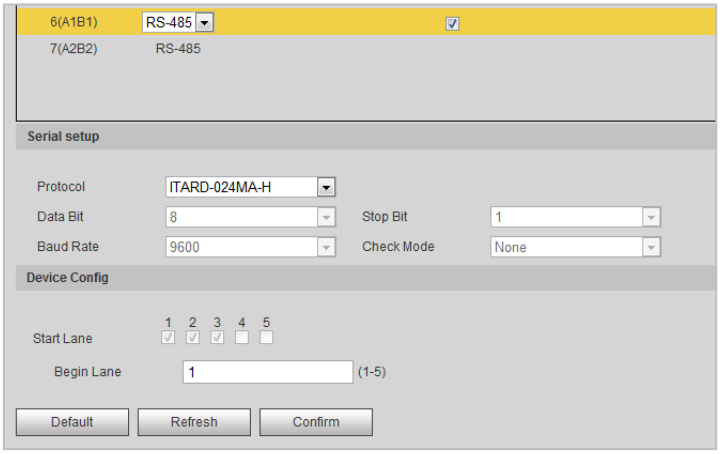
Table 5-20 Description of important parameters of the radar

Parameter	Description
Start Lane	The number of lanes on which the radar has been enabled.
Work Mode	Select the work mode of the radar from **Speed Measure Mode**, **Calculate Mode**, **Single**, **Continuous** and **Manual**.
Begin Lane	The lane number on which the radar starts detecting.
Interval	During the interval, the radar only detects one object. This function works together with a special program.

Parameter	Description
Detect Mode	The direction of radar detection.
Trigger Speed	The low speed limit that triggers the radar to send a capture signal to the Camera. Once the vehicle exceeds the limit, the Camera takes a snapshot.
Pre Speed Wait	During the speed wait, if the Camera reads the speed from the radar, it is the vehicle speed; Otherwise, the displayed vehicle speed is a random value within the speed limit.
Delay Speed Wait	
Angle	The angle between the radar beam and vehicle driving direction.
Sensitivity	Supports adjusting the sensitivity of the radar capture. 5 is the most sensitive.

3) Select **RS-485** to enable multi-lane radar detection.

Figure 5-38 Radar configuration (multiple lanes)

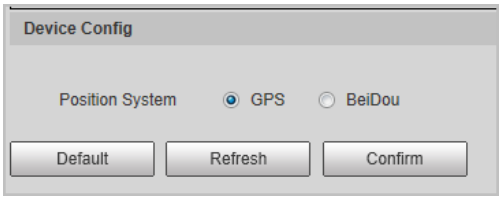


4) Click **Confirm**.

- Positioning

1) Select **Go to**.

Figure 5-39 Positioning configuration



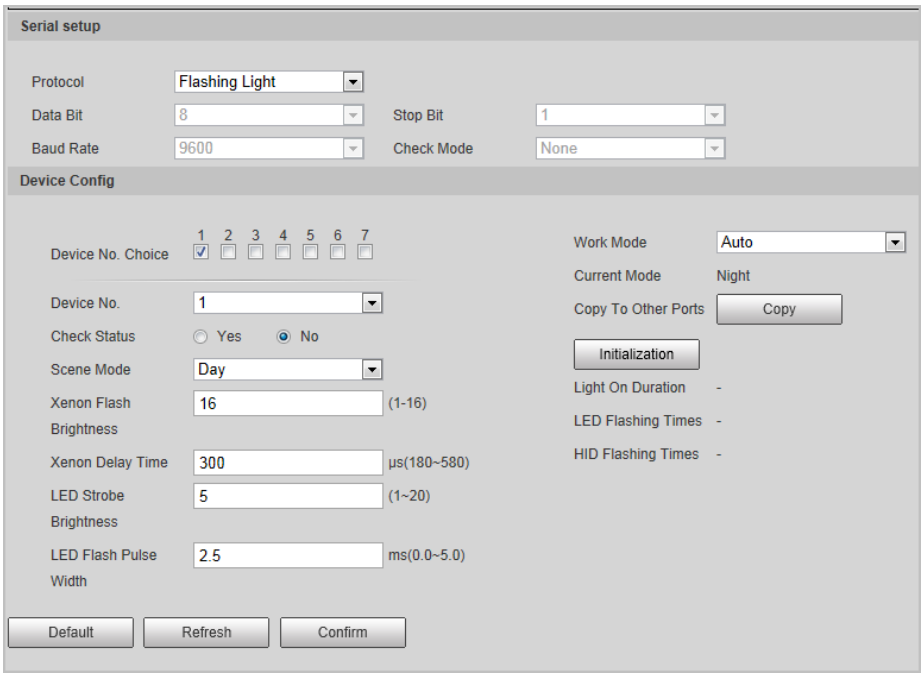
2) Select the positioning method from **GPS** and **BeiDou** as needed.

3) Click **Confirm**.

- External Light

1) Select **External Light**.

Figure 5-40 External light configuration



2) Configure external light parameters.

Table 5-21 Important external light parameters description

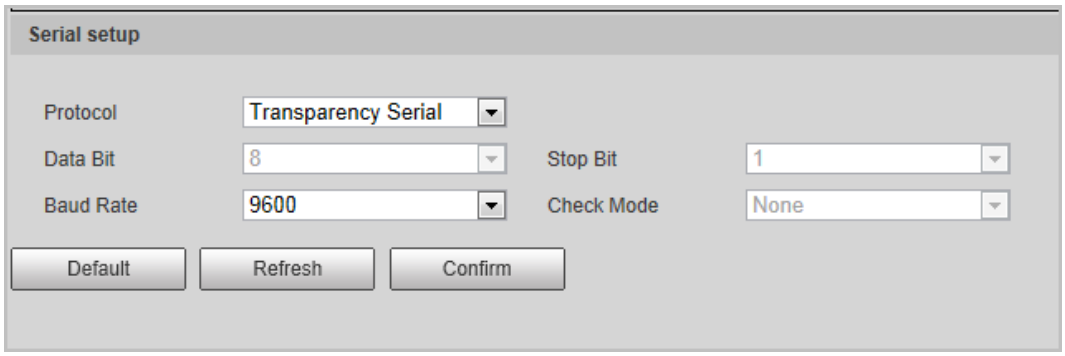
Parameter	Description
Protocol	Select from **Flashing Light**, **Strobe** and **Continuous Light**.
Device No. Choice	Select device number as needed.
Device No.	Select external light number based on the selected device number.
Check Status	Select **Yes** to enable external light status check.
Scene Mode	Select the working environment of the external light.
Xenon Flash Brightness	Set as needed.
Xenon Delay Time	
LED Strobe Brightness	
LED Flash Pulse Width	
Work Mode	Select the work mode of the external light from **Force Infrared**, **Force White** and **Auto**.
Copy to Other Ports	Click **Copy** to copy the configuration of the current light to other ports.
Initialization	Click **Initialization** to restore the RS-485 address of the external light to default.

3) Click **Confirm**.

- Transparency Serial

1) Select **Transparency Serial**.

Figure 5-41 Transparency serial



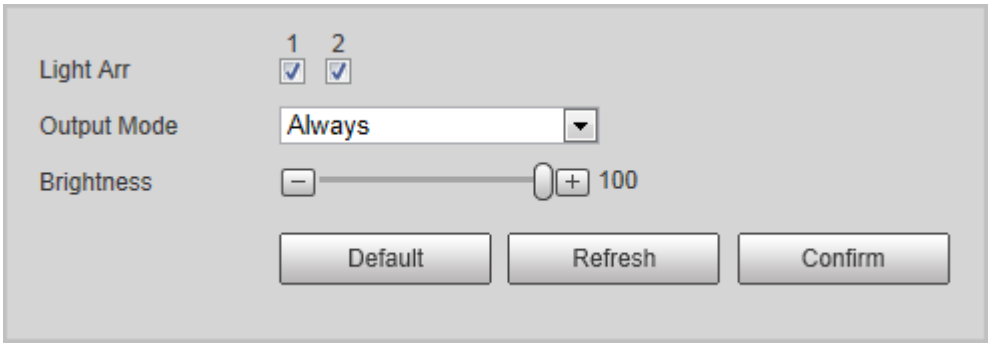
2) Set **Transparency Serial** as Protocol, and configure **Baud Rate** as needed.
3) Click **Confirm**.

5.5.3 Spotlight

You can configure the work mode of the flashing lights and strobes connected through RS-485 to the Camera in this section.

Step 1 Select **Setting > Peripheral > Spotlight**.

Figure 5-42 Light config



- **Light Arr**: Select **1** or **2** (each number controls 2 LEDs on the Camera) to turn on or off the illuminators.
- **Output Mode**:
  - ◇ **Always**: The spotlight is always on.
  - ◇ **Off**: The spotlight is always off.
  - ◇ **Auto**: The spotlight turns on or off according to the ambient brightness.

Step 2 Click **Confirm**.

5.6 Storage

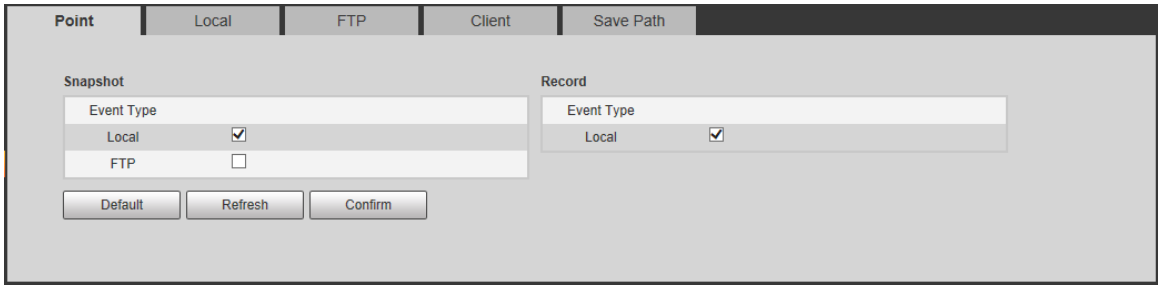
You can configure the storage path of snapshots and video records.

5.6.1 Point

Set the storage path of snapshots and video recordings.

Step 1 Select **Setting > Storage > Destination > Point**.

Figure 5-43 Point



Step 2 Select storage path as needed.

- **Local**: Store in the TF card, which has a limited capacity but offers continuous access to its storage, even during network failure. Videos can only be stored in TF card.
- **FTP**: Store in the FTP server, which offers a greater capacity but it will stop storing when the network fails.

Step 3 Click **Confirm**.

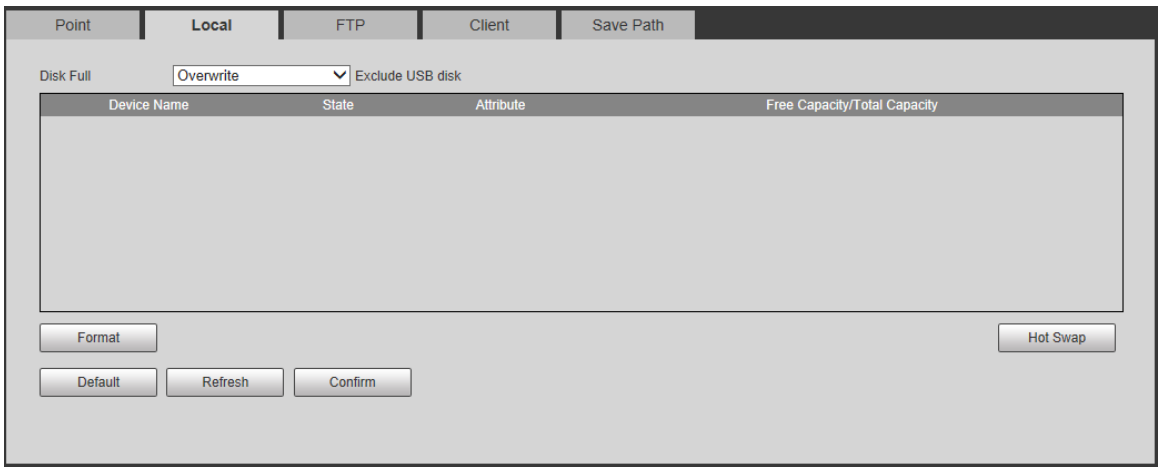
5.6.2 Local

Select **Setting > Storage > Destination > Local**, and the page displays the information of the TF card.

You can **Format** or **Hot Swap** the TF card, or select to **Overwrite** or **Stop** storage when the disk is full. Click **Confirm** after these operations.

Make sure that a TF card is inserted; otherwise, no card information will be displayed on the **Local** page.

Figure 5-44 Local

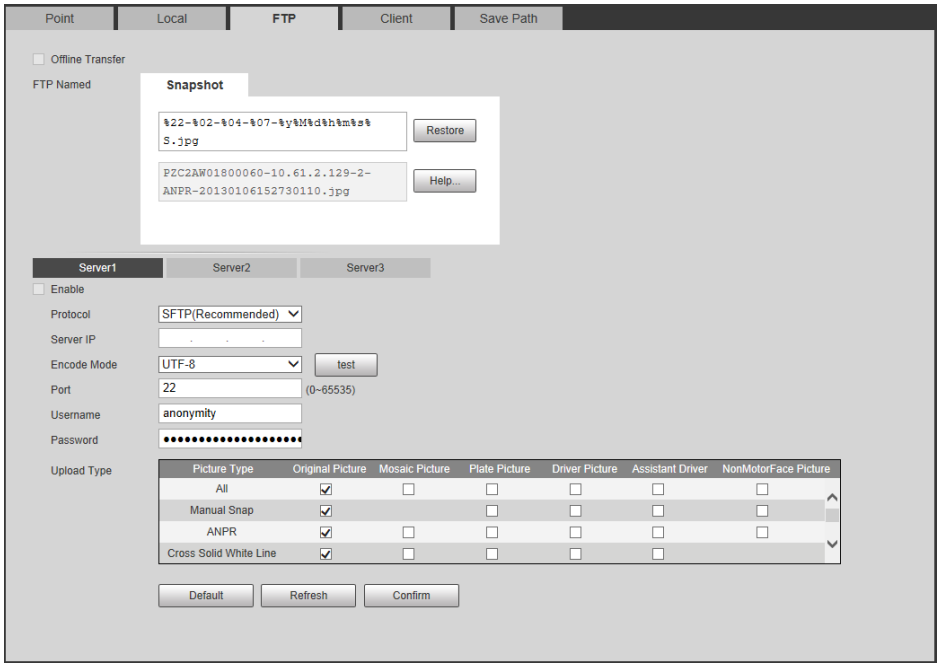


5.6.3 FTP

FTP function can be enabled only when TF card is inserted and FTP server is enabled. Only snapshots can be saved to the FTP server.

Step 1 Select **Setting > Storage > Destination > FTP**.

Figure 5-45 FTP



Step 2 Configure the parameters.

Table 5-22 FTP parameters

Parameter	Description
Offline Transfer	When the network disconnects or fails, snapshots will be stored in TF card. After the network is restored, the snapshots will be uploaded from the TF card to FTP or client. Make sure that TF card is inserted in the Camera; otherwise, the offline transfer function cannot be enabled.
FTP Named	Set the naming rule of snapshots to be saved in FTP server. You can click **Help…** to view the **Picture Naming Help**, or click **Restore** to restore the default naming rule.
Server1, Server2, Server3	Supports uploading to multiple servers. You can save different types of snapshots to different servers. Select the snapshot types from **Upload Type**.
Enable	Enable FTP server storage.
Protocol	• **SFTP (Recommended)**: Secure File Transfer Protocol, a network protocol allows file access and transfer over a secure data stream. • **FTP**: File Transfer Protocol, a network protocol implemented to exchange files over a TCP/IP network. Anonymous user access is also available through an FTP server.
Server IP	The IP address of FTP server.
Encode Mode	Refers to the encode mode of Chinese characters when naming images. Two modes are available: **UTF-8** and **GB2312**. After configuring **Server IP** and **Port**, click **test** to check whether the FTP server works.
Port	The port number of FTP server.
Username, Password	The username and password of FTP server.

Parameter	Description
Upload Type	Select event(s) and picture type(s) to be uploaded to each FTP server. Different modes (**ANPR**, **E-Police**, and **Yield to Pedestrians**) support different events, and might differ from the actual page.

Step 3 Click **Confirm**.

5.6.4 Client

You can set the parameters of storing to the client, which generally refers to the platform.

You need to install and log in to platform first before you can store snapshots to platform server.

Step 1 Select **Setting > Storage > Destination > Client**.

Figure 5-46 Client

Step 2 Configure the parameters.

Table 5-23 Client parameters

Parameter	Description
Offline Transfer	When the network is disconnected or fails, the Camera stores the snapshots to its TF card (when TF card is inserted), and it will automatically upload the stored snapshots to platform server after the network resumes. When selecting **Offline Transfer**, **Manual Upload** option will be displayed, and then you can configure **Begin Time** and **End Time** of upload, and select the server to upload to.
Type	Select connection type with platform server. ● **IP**: Connect to platform server through IP address. ● **MAC**: Connect to platform server through MAC address.
Server	Select the server, which includes **Server1** and **Server2**.
Server IP	● When **Type** is set to **IP**, enter the server's IP address. ● When **Type** is set to **MAC**, enter the server's MAC address.

Step 3 Click **Confirm**.

5.6.5 Save Path

You can configure the names and storage paths of snapshots and video recordings.

Step 1 Select **Setting > Storage > Destination >Save Path**.

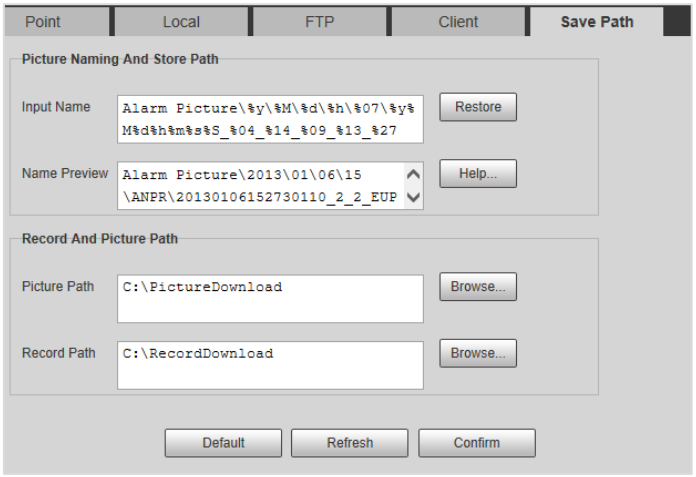
Step 2 Name the snapshots in the **Input Name** section. You can click **Help…** to view the **Picture Naming Help**, or click **Restore** to restore the naming rule to the default.

After setting the naming rule, you can preview an example of the name in the **Name Preview** section.

Step 3 Click **Browse…** to set the save paths of snapshots and video recordings respectively.

Step 4 Click **Confirm**.

Table 5-24 Save path



5.6.6 Record Control

You can set how to record the videos and the stream for recording the videos.

Step 1 Select **Setting > Storage > Record Control**.

Step 2 Select the record mode.

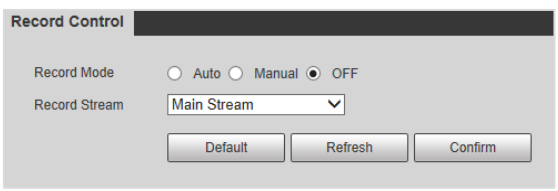
- **Auto**: Record videos only when a traffic violation event is detected.

  After enabling auto recording, go to **Setting > Event > ANPR Snap > Rule Config**, under Advanced Parameter, select a lane (**Event Type** is not **ANPR**) and then enable **Related Record** to automatically record the corresponding lanes. In addition, select **Local** from **Setting > Storage > Destination > Point**.
- **Manual**: Record videos continuously.
- **Off**: Do not record videos.

Step 3 Select the record stream. You can select from **Main Stream** and **Sub Stream**.

Step 4 Click **Confirm**.

Figure 5-47 Record control



5.7 System

You can configure system information, add users, restore to factory settings, import and export system configuration files, and more.

5.7.1 General

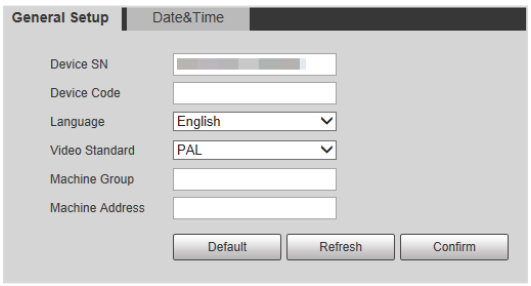
You can configure display language, video standard, and also set the time and time zone of the Camera.

5.7.1.1 General Settings

You can configure the device code, system, video standard, and more.

Step 1 Select **Setting > System > General Setup > General Setup**.

Figure 5-48 General



Step 2 Configure the parameters.

Table 5-25 General setting parameters

Parameter	Description
Device SN	The device serial number consisting of letters, numbers, underlines and strikethroughs.
Device Code	Number of the Camera. The device code cannot be overlaid with OSD information.
Language	Language of web browser page. You need to log in again when switching to another language. Currently, only **English** is supported.
Video Standard	**PAL** and **NTSC** are available. ● **PAL**: Much more common around the world, and can be found in most of Western Europe, Australia, China, and elsewhere. ● **NTSC**: Mostly limited to North America, parts of South America, Japan, and the Philippines.
Machine Group	The group or entity that uses the Camera.
Machine Address	The locations where snapshots were taken by the Camera.

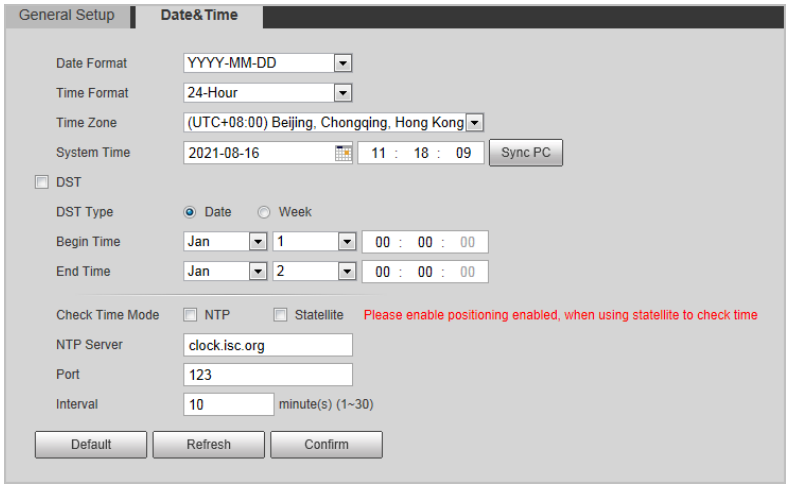
Step 3 Click **Confirm**.

5.7.1.2 Date & Time

You can configure date, time, time zone, and more for the Camera.

Step 1 Select **Setting > System > General Setup > Date&Time**.

Figure 5-49 Date & time



Step 2 Configure the parameters.

Table 5-26 Date & time parameters

Parameter	Description
Date Format	Select the date format. Three formats are available: **YYYY-MM-DD**, **MM-DD-YYYY** and **DD-MM-YYYY**.
Time Format	Select the time format. Two formats are available: **24-Hour** and **12-Hour**.
Time Zone	The time zone where the Camera is located.
System Time	The current time of the Camera.
Sync PC	Synchronize the time of the Camera to that of the PC. Click **Sync PC**, and the settings will immediately take effect.
DST	Select the **DST** (means daylight saving time) checkbox, set the **DST Type** by **Date** or by **Week**, and then configure the **Start Time** and **End Time** of DST.
Check Time Mode	Time synchronization mode. You can select **NTP** (network time protocol) or **Satellite**.
NTP Server	The IP address and the port number of NTP server. Required when **NTP** is set to **Check Time Mode**.
Port	
Interval	The time synchronization interval of the Camera and the NTP or satellite.

Step 3 Click **Confirm**.

5.7.2 Account Management

You can add or delete users and user groups, assign permissions to new users and user groups, modify passwords, and manage users and user groups.

5.7.2.1 Account

Management Rules

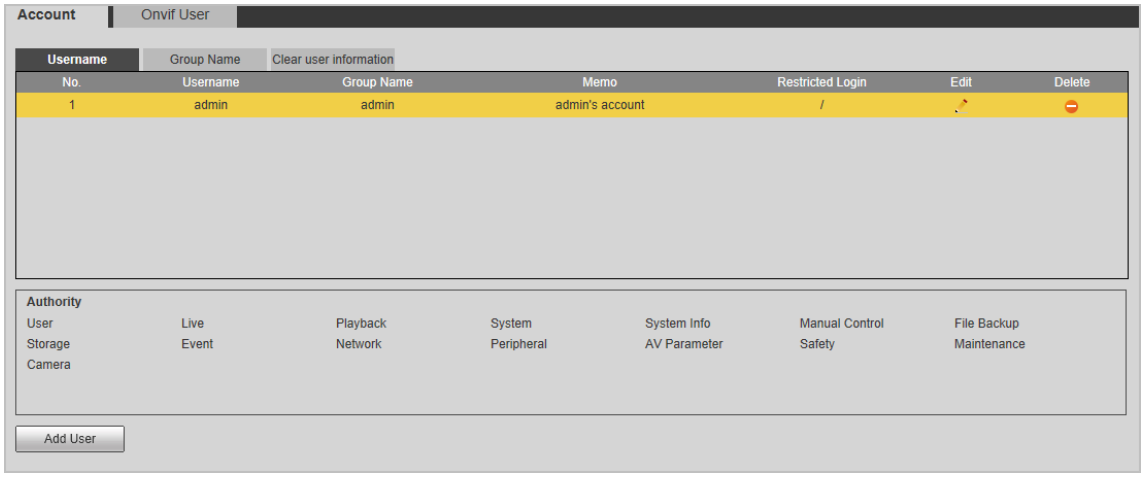
- The system manages both users and user groups. You can set up to 8 user groups and 18 users. The factory settings cover two groups: User and admin.
- Group name cannot be repeated, so is the username. Each user must be placed in a group, and can only belong to one group. You can add or delete user group(s).
- The username can be 31 characters at most, consisting of letters, numbers, "_", "@" and ".".
- The name of the user group can be 15 characters at most, consisting of at least two of the following types of characters: Letters, numbers, underlines, and hyphens.
- The default username and password are both admin. There is one admin user by default which has the highest authority.
- We recommend giving fewer authorities to normal users than premium users.

User Management

You can view user information, add or delete user(s), change user password, assign user permissions, restrict user login, and more.

Step 1 Select **Setting > System > Account > Account > Username**.

Figure 5-50 Account



Step 2 Add a user.

1) Click **Add User**.
2) On the **Add User** page, configure user information including username, password, group name, memo, and operation permissions (see Figure 5-51).
3) Set login restrictions (if necessary), and then the restricted IP address will be unable to log in to the Camera during the restricted period (see Figure 5-52).
4) Click **Save** to save the settings.

Figure 5-51 Add user

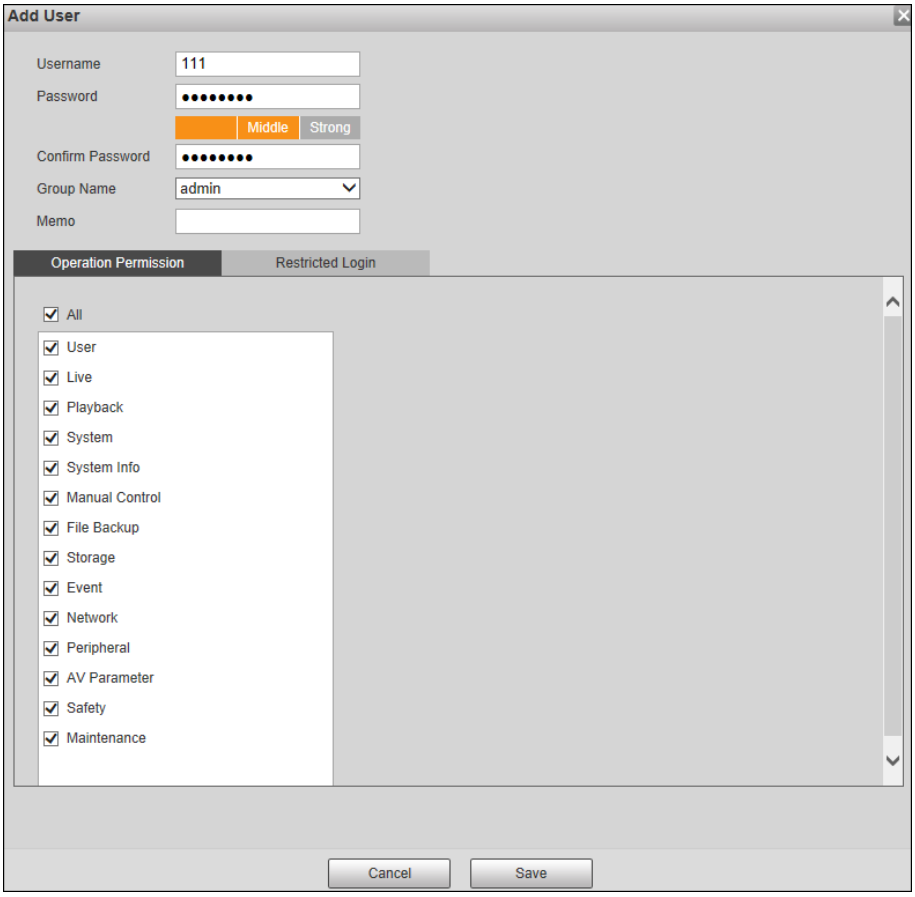
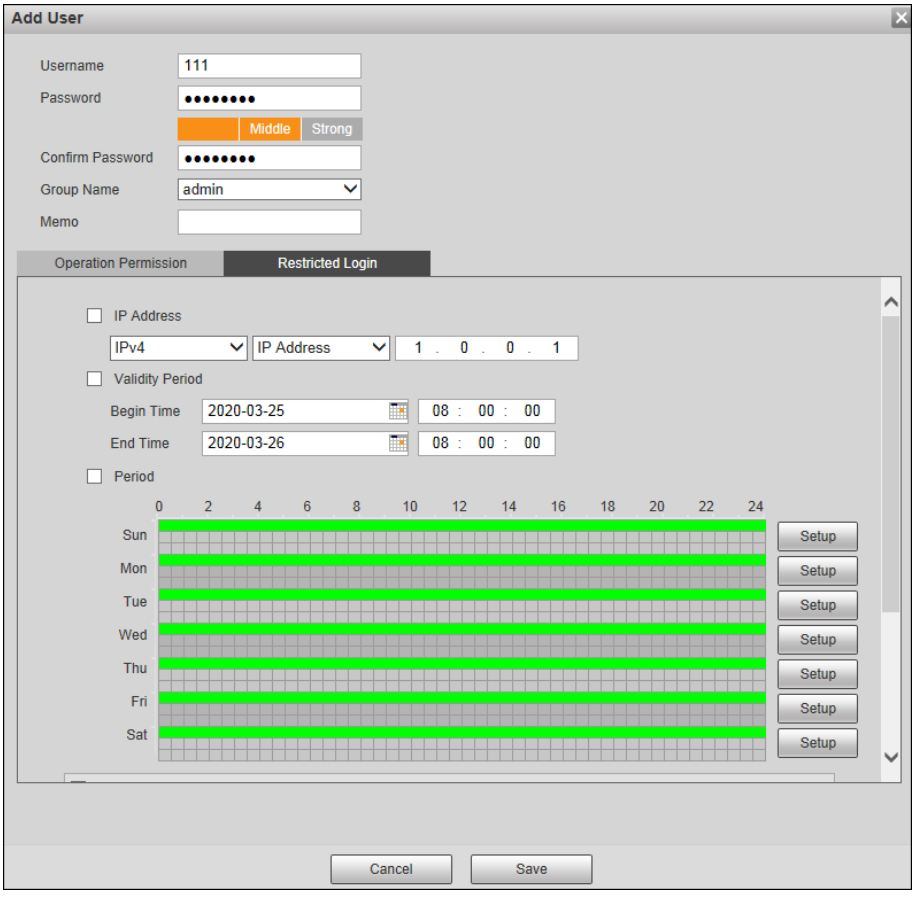


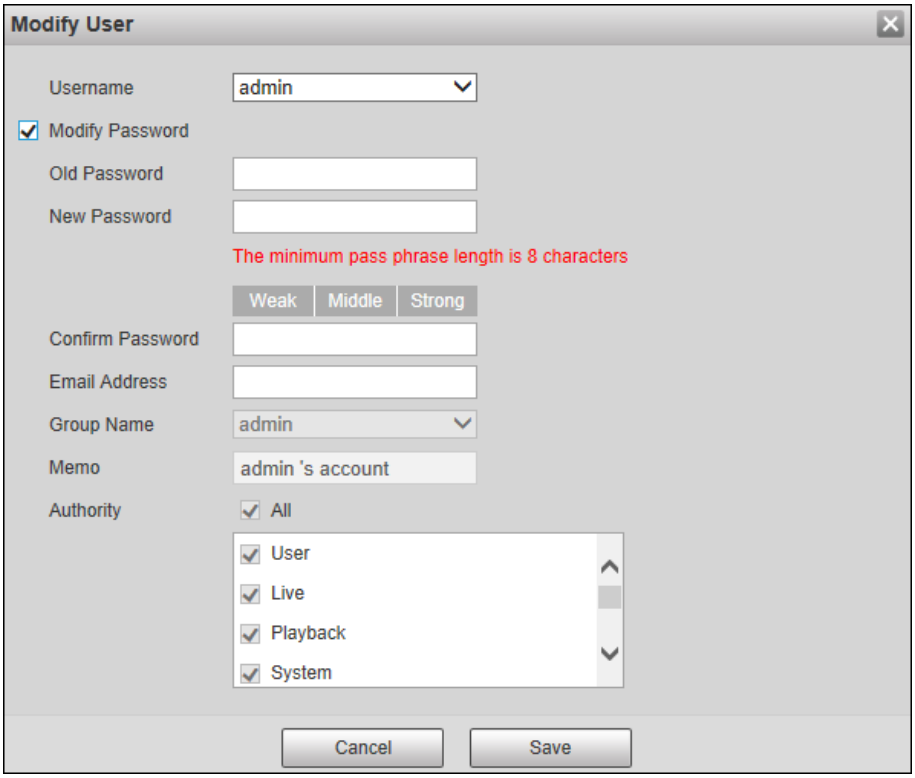
Figure 5-52 Set log restriction



You can also:

- Delete a user: Click to delete the corresponding user.
- Modify user information: Click corresponding to the user. You can modify information such as username, password, email address, group name, and memo. Click **Save** to save the settings.

Figure 5-53 Modify user



- Change password: On the **Modify User** page, select the **Modify Password** checkbox. Enter the old and new passwords, and confirm password. Click **Save** after configuration. Configure the password according to the password strength prompt. The new password must be 8–32 characters and contain at least two of the following types of characters: Numbers, upper case letters, lower case letters and special characters (excluding ' " ; : &).

Password strength prompts will be made according to the points obtained from password length, letters, numbers, characters, and combination. See the table below.

Table 5-27 Password strength evaluation

Item	Evaluation
Length	• 5 points: Not more than 4 characters. • 10 points: 5–7 characters. • 25 points: 8 characters or more.
Letter	• 0: No letter. • 10 points: Only upper or lower case letters. • 20 points: A combination of upper and lower case letters.

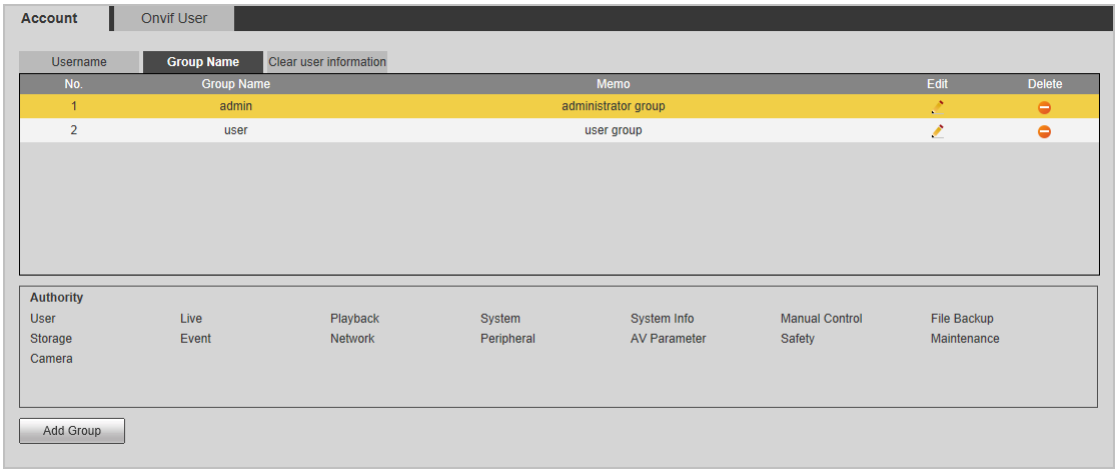
Item	Evaluation
Number	● 0: No number. ● 10 points: 1 number. ● 20 points: 3 numbers or more.
Special character	● 0: No special characters. ● 10 points: 1 special character. ● 25 points: More than 1 special character.
Combination	Categories: Upper case letters, lower case letters, numbers and special characters. ● 2 points: A combination of two categories. ● 3 points: A combination of three categories. ● 5 points: A combination of four categories.
Strength	● ≥ 70 points: Strong. ● ≥ 50 points: Medium. ● ≥ 0 points: Weak.

User Group Management

You can view user group information, add or delete user groups, and modify the password of user groups.

Step 1 Select **Setting > System > Account > Account > Group Name**.

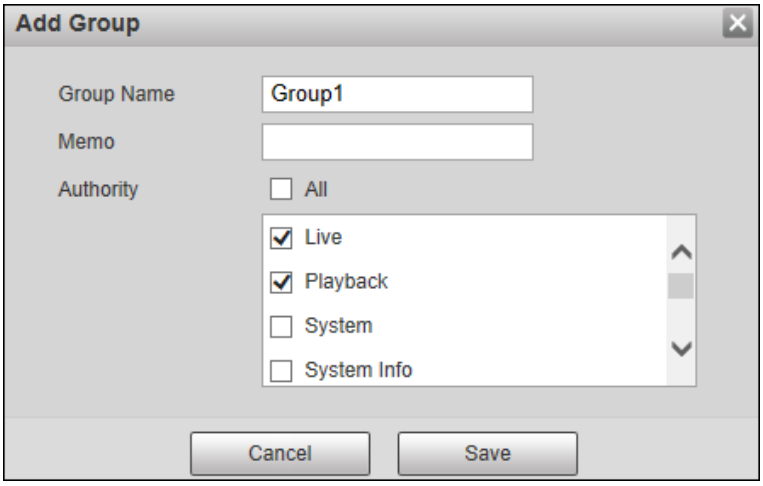
Figure 5-54 User group



Step 2 Manage groups.

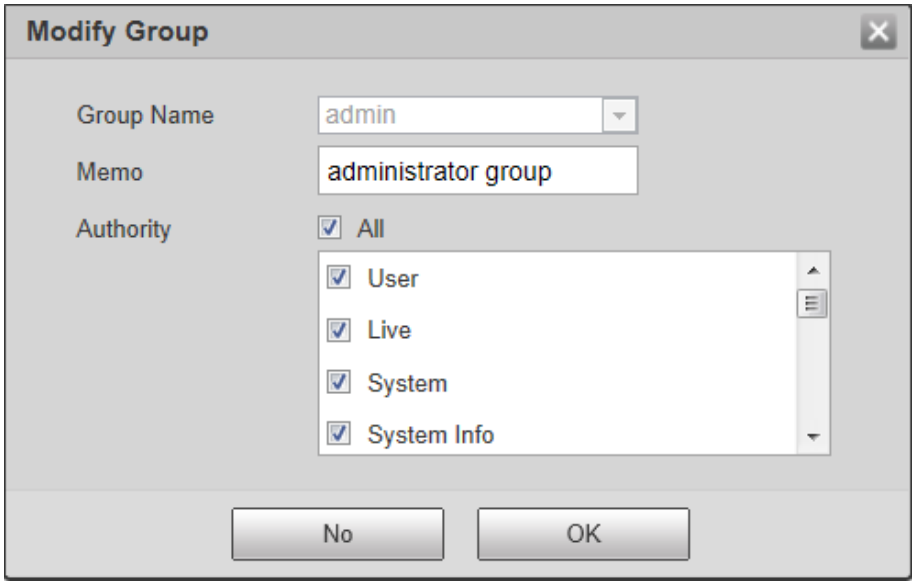
- Add a group: Click **Add Group**, and then configure the **Group Name** and **Authority** of the group. Click **Save** after configuration.

Figure 5-55 Add group



- Delete a group: Click to delete the corresponding group.
- Modify group information: Click corresponding to the group, and then you can modify the memo and authority of the group. Click **OK** after configuration.

Figure 5-56 Modify group



- The admin and user groups cannot be deleted.
- A group cannot be deleted if there is any user in the group.

Clear User Information

You can clear all user information by clicking **Clear user** under **Setting > System > Account > Account > Clear user information**.

5.7.2.2 ONVIF User

ONVIF users can be separately managed with account users and user groups.

Management Rules

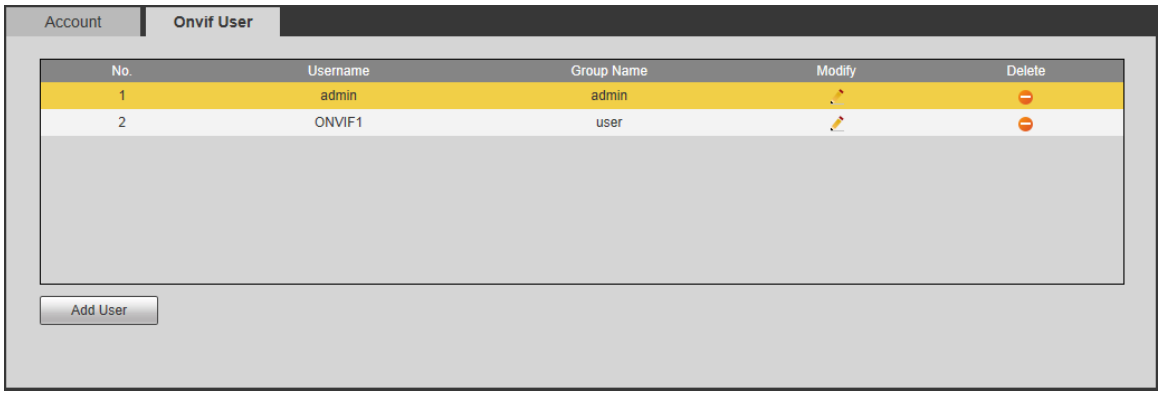
- The system manages both ONVIF users and user groups. The factory settings cover one group: admin. You can set up to 18 ONVIF users.
- ONVIF username cannot be repeated. Each ONVIF user must belong to a group, and can only belong to one group. The username can be 31 characters at most, consisting of letters, numbers, "_", "@" and ".".
- The default ONVIF username and password are both admin. There is one admin by default which has the highest authority.

ONVIF User Management

You can view ONVIF user information, add or delete user(s), and modify user password.

Step 1 Select **Setting > System > Account > Onvif User**.

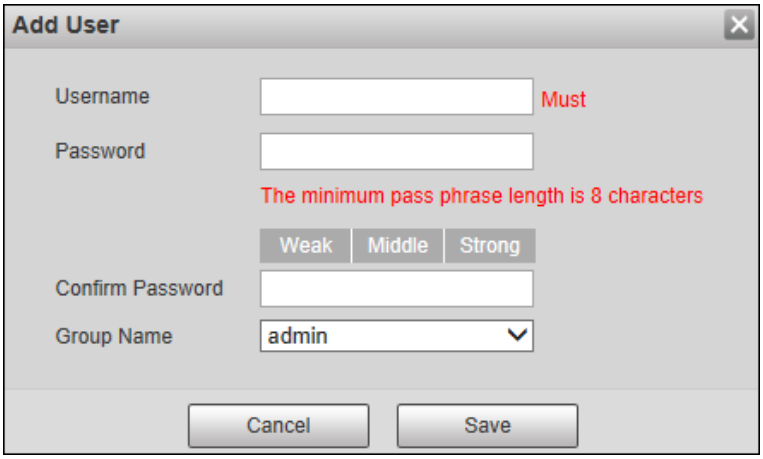
Figure 5-57 Onvif user



Step 2 Manage ONVIF users.

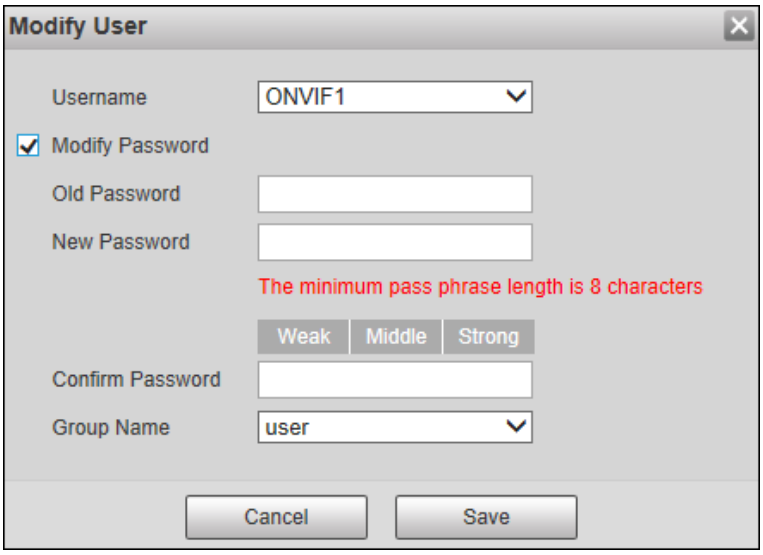
- Add ONVIF user: Click **Add User**, and then you can configure user information such as username, password, and group name. Click **Save** after configuration.

Figure 5-58 Add User



- Modify user information: Click corresponding to the user, and then you can modify information such as username, password, and group name. Click **Save** after configuration.

Figure 5-59 Modify user



- Modify password: On the **Modify User** page, select the **Modify Password** checkbox. Enter the old and new passwords, and confirm password. Click **Save** after configuration. Configure the password according to the password strength prompt. The new password must be 8–32 characters and contain at least two of the following types of characters: Numbers, upper case letters, lower case letters and special characters (excluding ' " ; : &).

  For password strength evaluation, see Table 5-27.

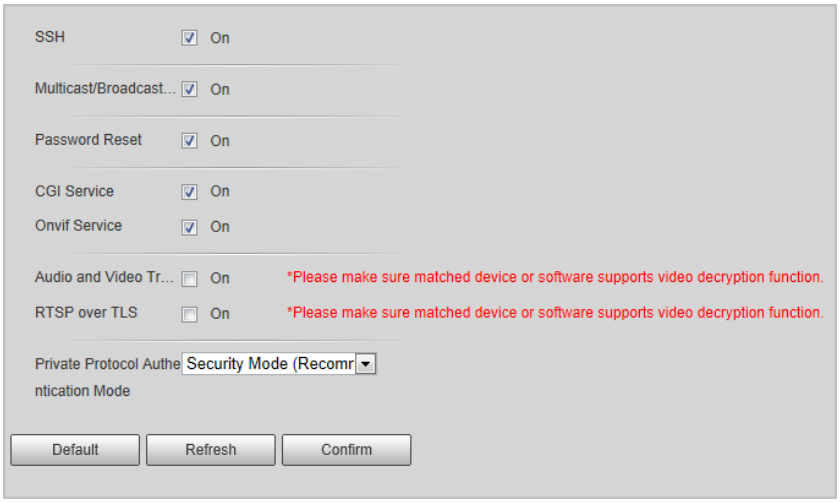
5.7.3 Safety

5.7.3.1 System Service

You can enable multiple system services to secure network safety.

Step 1 Select **Setting > System > Safety > System Service**.

Figure 5-60 System service



Step 2 Enable the service(s).

Table 5-28 System service

Parameter	Description
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecure network. It is a method for secure remote login, providing secure access for users.
Multicast/Broadcast Search	Multicast identifies logical groups of computers group members. This allows a single message to be sent to the group. Broadcast allows all devices on the same network segment to see the same message.
Password Reset	Enable it so that you can reset the password.
CGI Service	Select the **Enable** checkbox to enable Common Gateway Interface (CGI) service.
Onvif Service	Select the **Enable** checkbox to enable Open Network Video Interface Forum (ONVIF) service.
Audio and Video Transmission Encryption	Enable this function to encrypt stream transmitted through private protocol. ● Make sure that the matched device or software supports the video decryption function. ● We recommend enabling the encryption service to avoid data leak.
RTSP over TLS	Enable this function to encrypt stream transmitted through standard protocol. ● Make sure that the matched device or software supports video decryption function. ● We recommend enabling the encryption service to avoid data leak.
Private Protocol Authentication Mode	Leave it as default.

Step 3 Click **Confirm**.

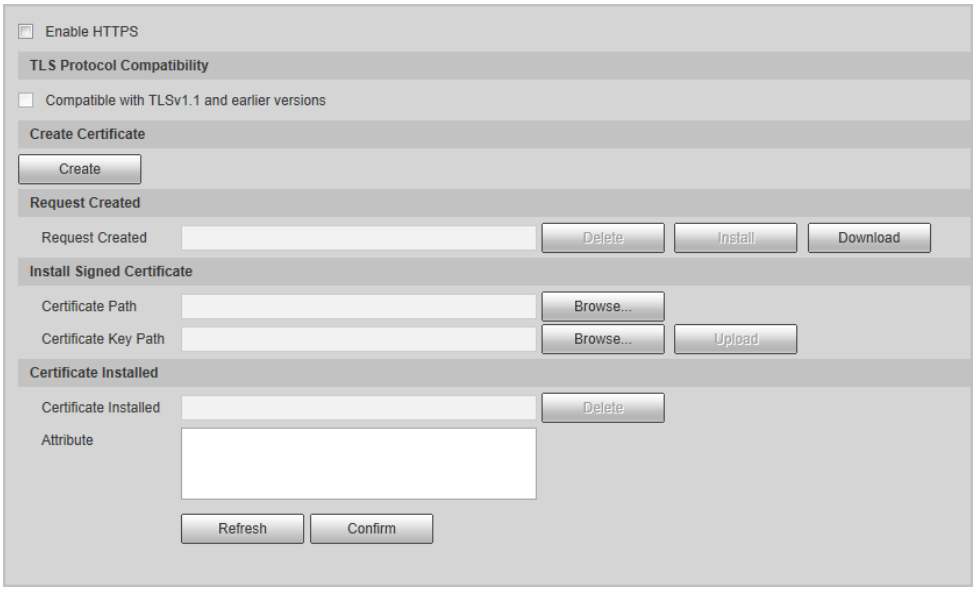
5.7.3.2 HTTPS

On the **HTTPS** page, you can create certificates or install signed certificates, so that you can log in to the web page by HTTPS. This helps ensure the security of data and the Camera.

Creating Certificate

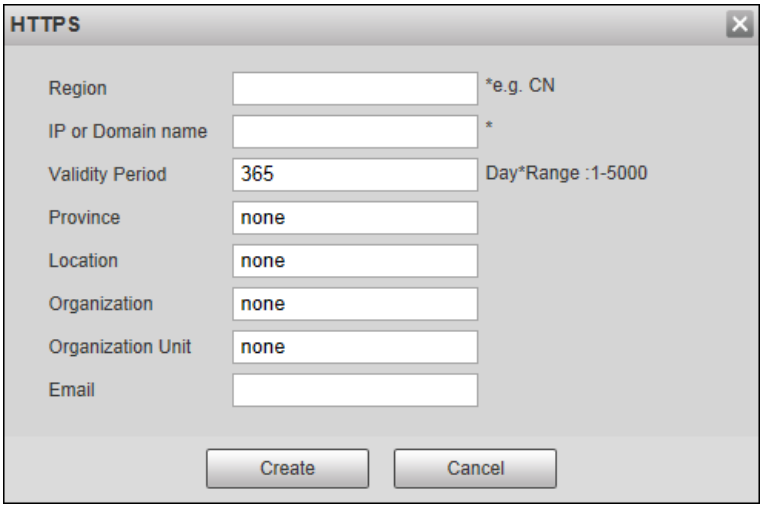
Step 1 Select **Setting** > **System** > **Safety** > **HTTPS**.

Figure 5-61 HTTPS



Step 2 Click **Create**.

Figure 5-62 HTTPS setting

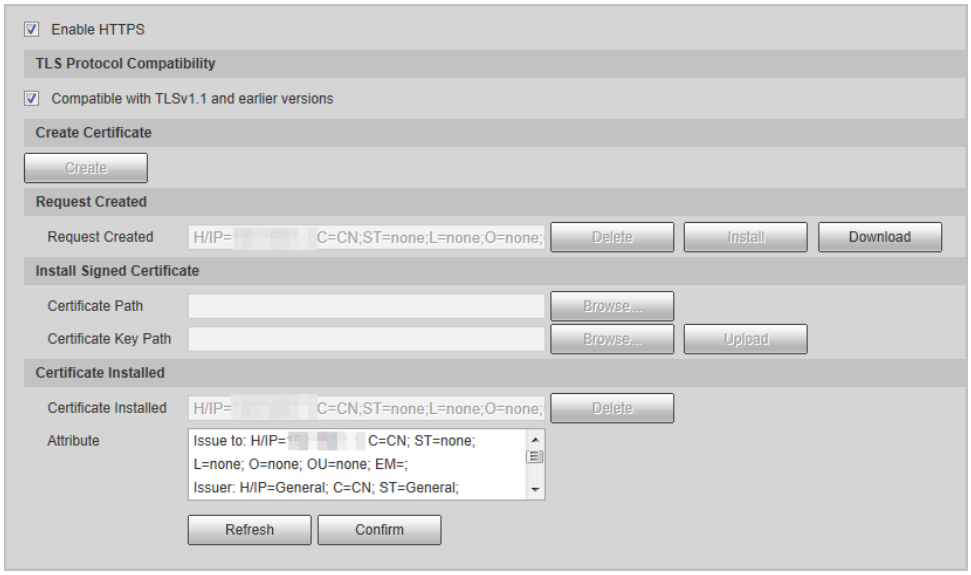


Step 3 Configure the region, and IP address or domain name of the Camera, and then click **Create**. The system prompts **Operation succeeded!** when it is done.

Step 4 Click **Install** to install the certificate.

The system prompts **Operation succeeded!** after installation, and the information of the HTTPS certificate will be displayed in **Attribute**.

Figure 5-63 Certificate installation



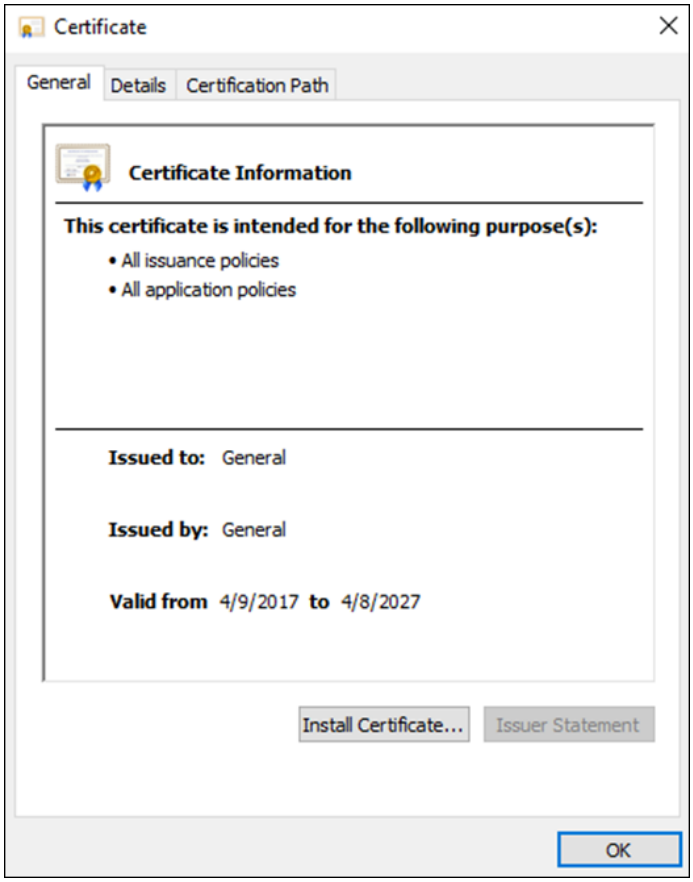
Step 5 Click **Download**, and then select the path to save the certificate.

Step 6 Import the certificate to the browser.

- The following steps use Internet Explorer as the example.
- The method for importing certificates might differ depending on the browser.

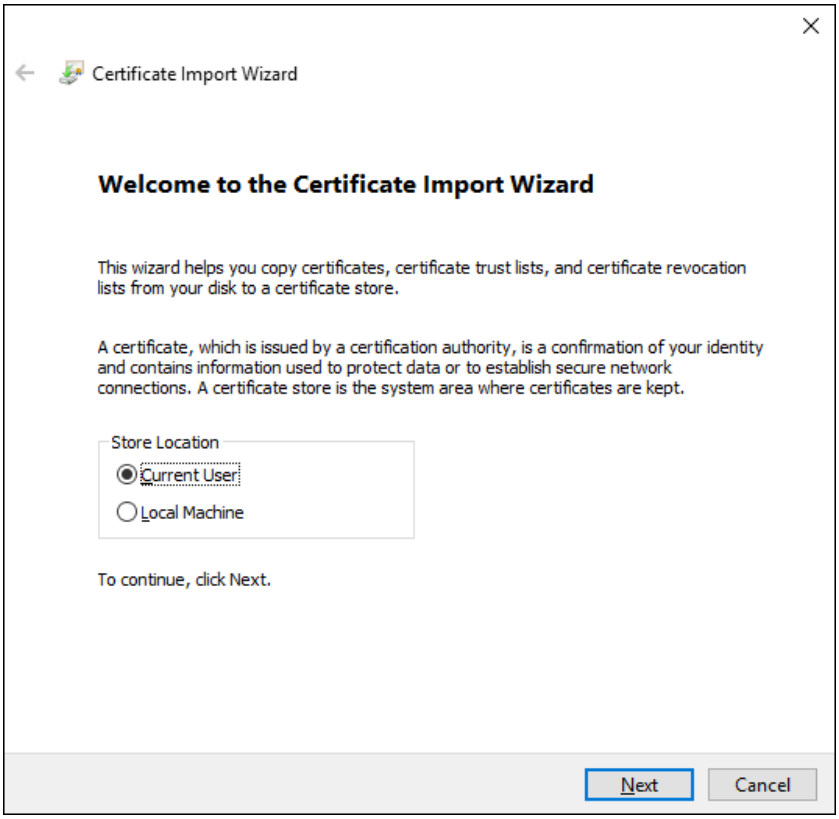
1) Go to the save path of the certificate, and then double-click the certificate.

Figure 5-64 Certificate



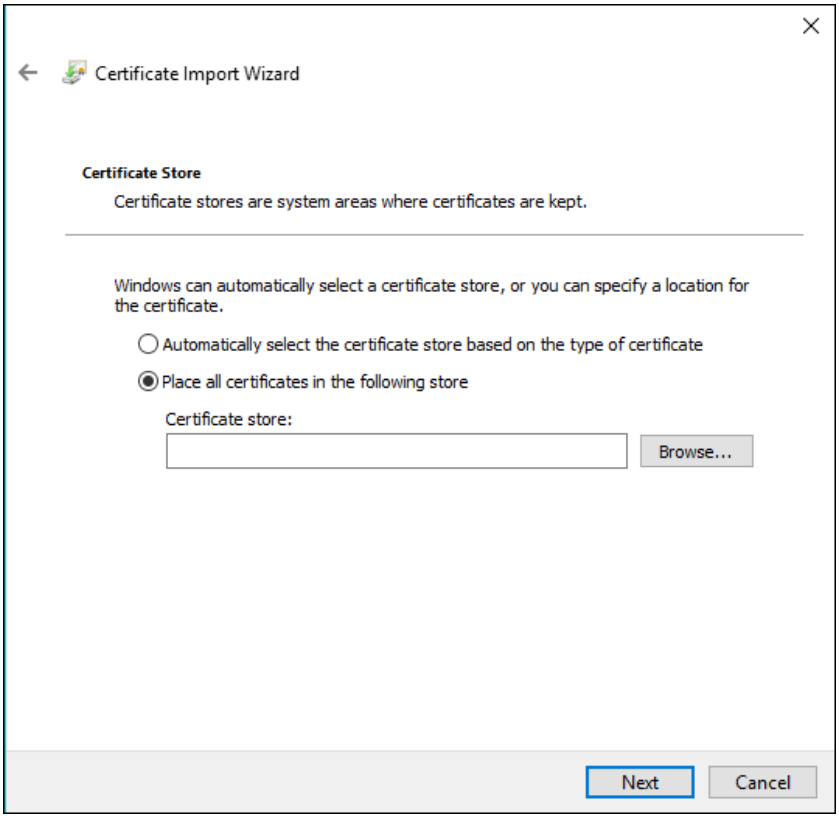
2) Click **Install Certificate…**, and then click **OK**.

Figure 5-65 Certificate import wizard



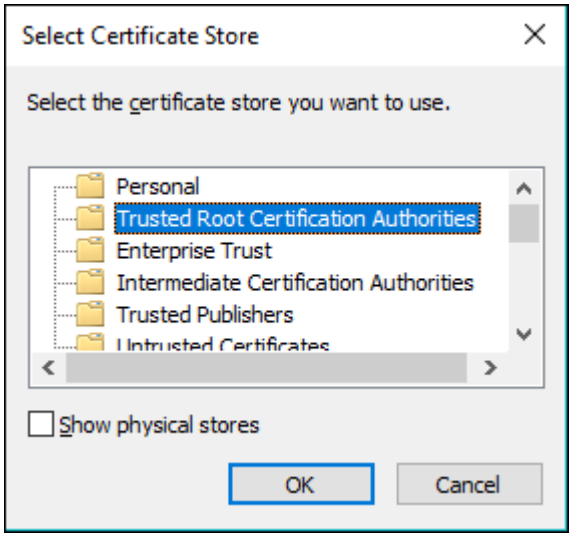
3) Click **Next**.

Figure 5-66 Certificate store



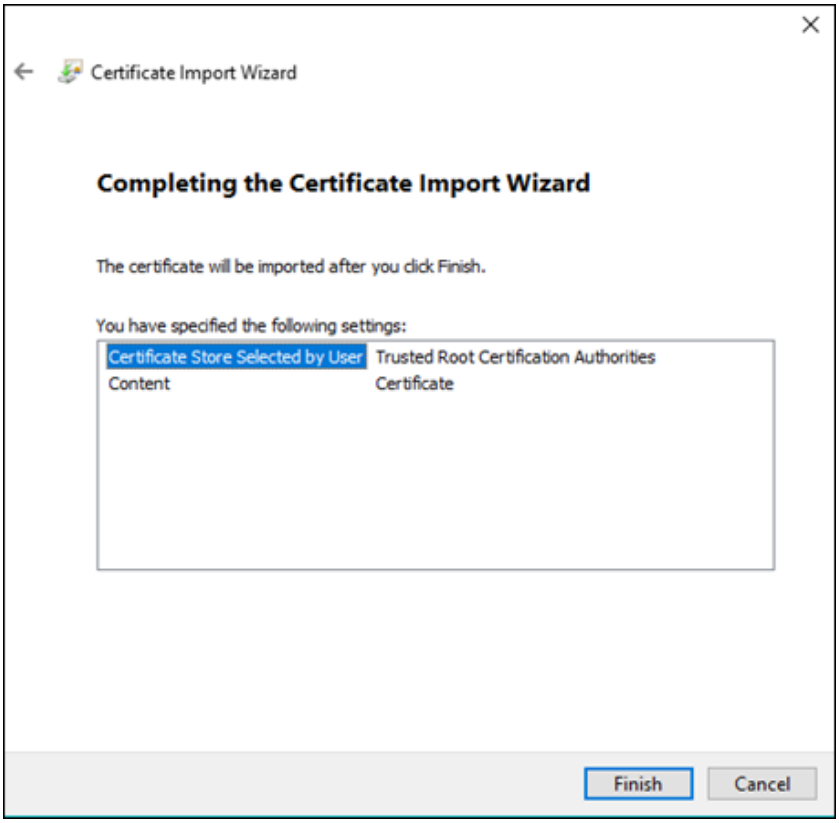
4) Click **Next**.

Figure 5-67 Select certificate store



5) Select **Trusted Root Certification Authorities**, and then click **OK**.

Figure 5-68 Completing the certificate import wizard



6) Click **Finish**, and then it prompts **The import was successful**.

7) Click **OK**.

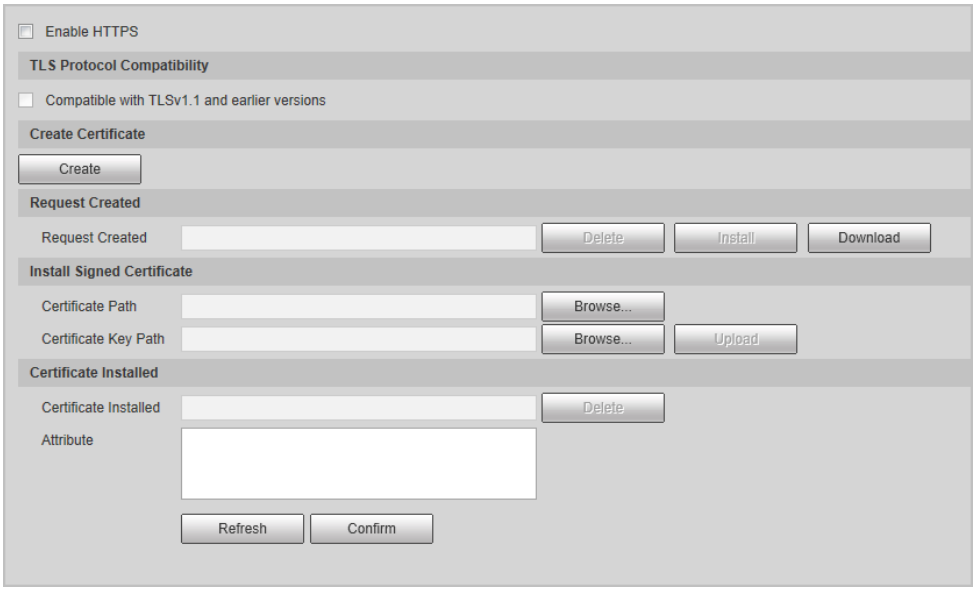
Step 7 Select the **Enable HTTPS** checkbox, and then click **OK**.

The Camera will restart. Wait for a few minutes, and then log in again.

Installing Signed Certificate

Step 1 Select **Setting > System > Safety > HTTPS**.

Figure 5-69 HTTPS



Step 2 Click **Browse** corresponding to **Certificate Path** to select the signed certificate.

Step 3 Click **Browse** corresponding to **Certificate Key Path** to select the private key file of the certificate.

Step 4 Install the root certificate. For details, see Step 6 of "Creating Certificate."

Step 5 Select the **Enable HTTPS** checkbox, and then click **OK**.

Step 6 Wait for a few minutes for the Camera to restart, and then log in again.

5.7.3.3 Firewall

Set the security rules to protect the safety of your camera system.

Step 1 Select **Setting > System > Safety > Firewall**.

Figure 5-70 Firewall

Step 2 Select Rule Type.

- **Network Access**: Add the IP address to allowlist or blocklist to allow or restrict it from accessing the corresponding ports of the device.
- **PING Prohibited**: IP address of your camera is prohibited from ping. This helps to prevent unauthorized attempts at accessing your network system.
- **Prevent Semijoin**: Prevents half-open SYN attacks.

Step 3 Select **Enable** to enable the rule type that you selected.

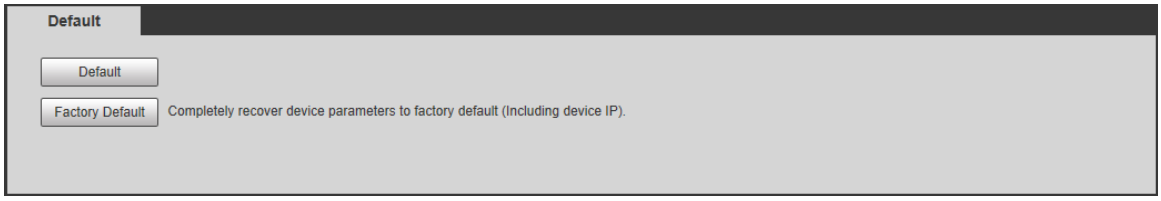
Step 4 Click **Confirm**.

5.7.4 Default

Select **Setting > System > Default**, and then you can:

- Click **Default** to restore most configurations of the Camera to default settings (except information such as IP address, account, and log).
- Click **Factory Default** to restore all configurations of the Camera to default settings, including IP address.

Figure 5-71 Default

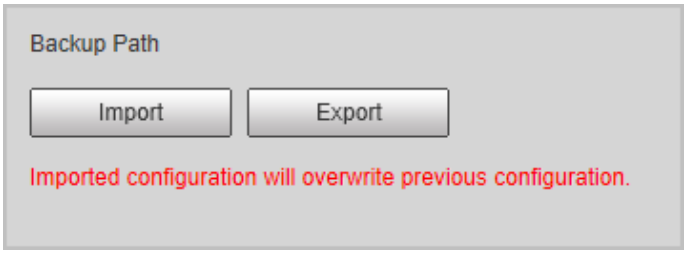


5.7.5 Import/Export

The system supports exporting the configurations from the web to local PC, and importing the configuration files from local backup.

Step 1 Select **Setting > System > Import/Export**.

Figure 5-72 Import/Export



Step 2 Click **Import** or **Export**.

- **Import**: Import the configuration files from local backup.
- **Export**: Export the configuration from the web page to local PC.

The imported and exported files should be in the format of .backup.

Step 3 Select the path of the file to import, or the path of the file to export.

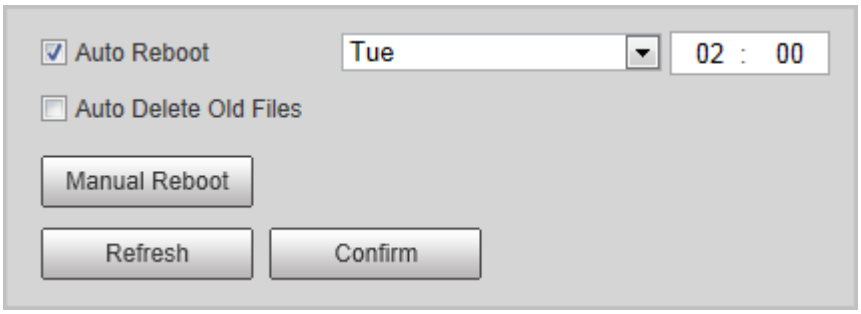
5.7.6 Configuring Auto Maintain

You can select to either automatically restart the Camera at the defined day and time, or manually restart the Camera to solve problems such as stuck images.

5.7.6.1 Auto Maintain

Step 1 Select **Setting > System > Auto Maintain > Auto Maintain**.

Figure 5-73 Auto maintain



Step 2 Select the restart mode.

- **Auto Reboot**: Select the **Auto Reboot** checkbox, and then configure the day and time. The system will automatically restart at the defined day and time.
- **Manual Reboot**: Click it to manually restart the Camera.

Step 3 Select the **Auto Delete Old File** checkbox, and the system will automatically delete the old files.

Step 4 Click **Confirm**.

5.7.6.2 Emergency Maintenance

Step 1 Select **Setting > System > Auto Maintain > Emergency Maintenance**.

Step 2 Select **On** to enable emergency maintenance.

Step 3 Click **Save**.

5.7.7 System Upgrade

You need to update the firmware to the latest version to make the Camera run properly.

Import the update file in the format of .bin to the system, and then update the system.

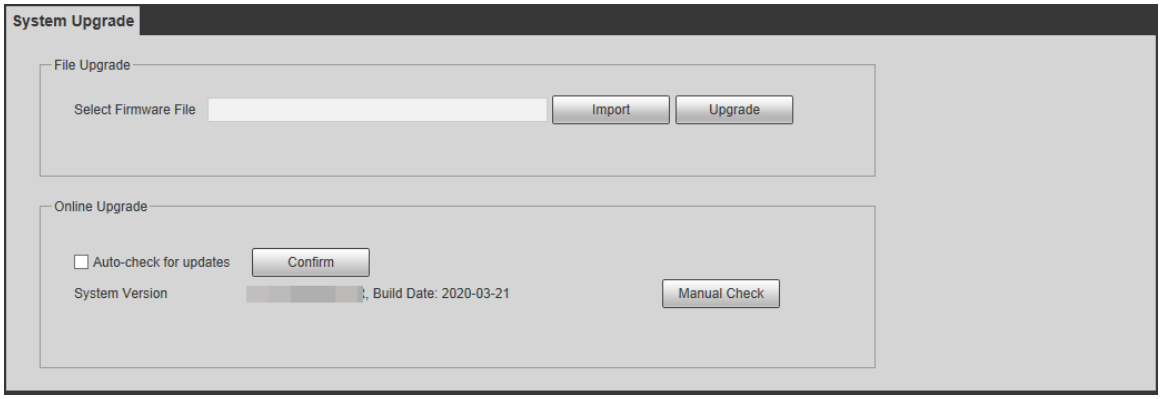
- **Online Upgrade** function is currently not available.
- Do not disconnect the power or network, or restart or shut down the Camera during update. Incorrect update programs might result in the Camera being unable to work.

Step 1 Select **Setting > System > System Upgrade**.

Step 2 Click **Import** to select the firmware update file (.bin).

Step 3 Click **Upgrade** to update the firmware.

Figure 5-74 Upgrade



5.8 System Information

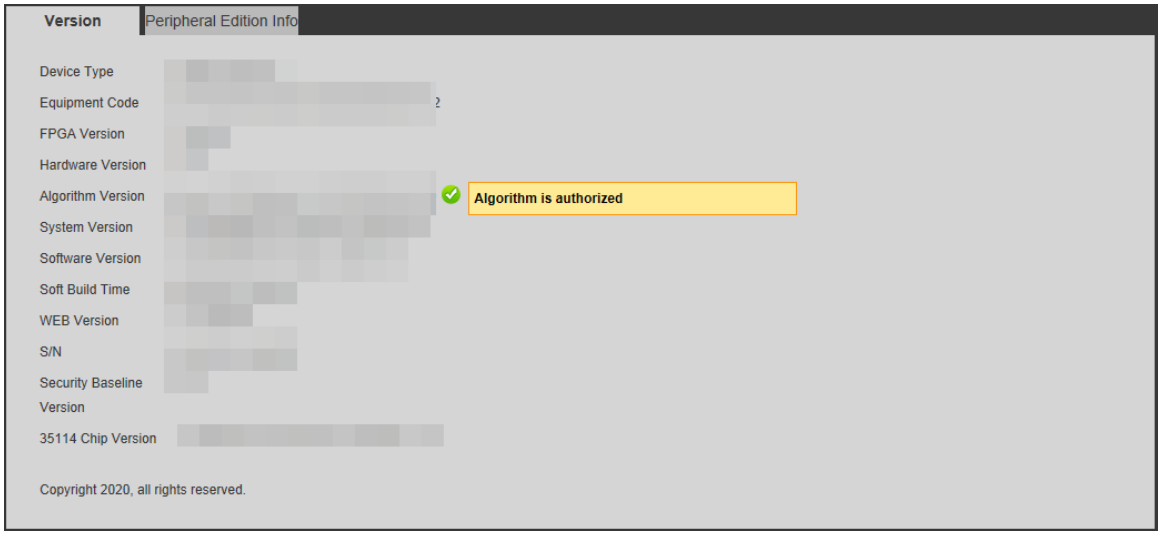
You can view information such as version, log, online user, and work status.

5.8.1 Version Information

- Select **Setting > System Info > Version** to view information such as device model, and the version of the hardware, system, and software.
- Select **Setting > System Info > Peripheral Edition Info** to view version information of the external device, such as radar and flashing light.

Version might differ depending on the device model.

Figure 5-75 Version



5.8.2 Log

5.8.2.1 System Log

You can search for and view logs by the time and type, and backup the logs. The log type includes **All**, **System**, **Setting**, **Data**, **Event**, **Record**, **Account**, and **Safety**.

Step 1 Select **Setting > System Info > Log > Log**.

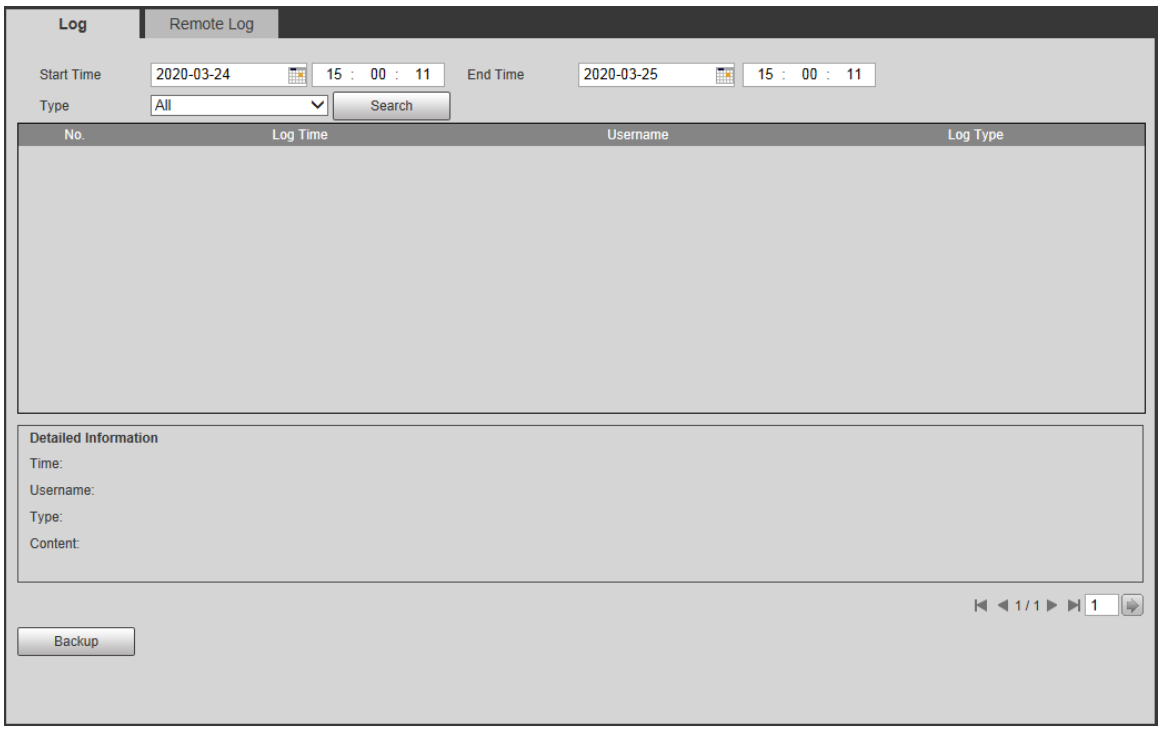
Step 2 Configure **Start Time** and **End Time**, and then select log type.

Step 3 Click **Search**.

Step 4 View and backup the search results.

You can save the search results to your PC in a .txt file.

Figure 5-76 Log



5.8.2.2 Remote log

Critical logs can be saved to the log server. This helps provide important clues to the source of security incidents. The log server needs to be deployed in advance by a professional or system administrator.

Step 1 Select **Setting > System Info > Log > Remote Log**.

Step 2 Select **Enable** to enable **Remote Log**.

Step 3 Configure the IP address, port and device number.

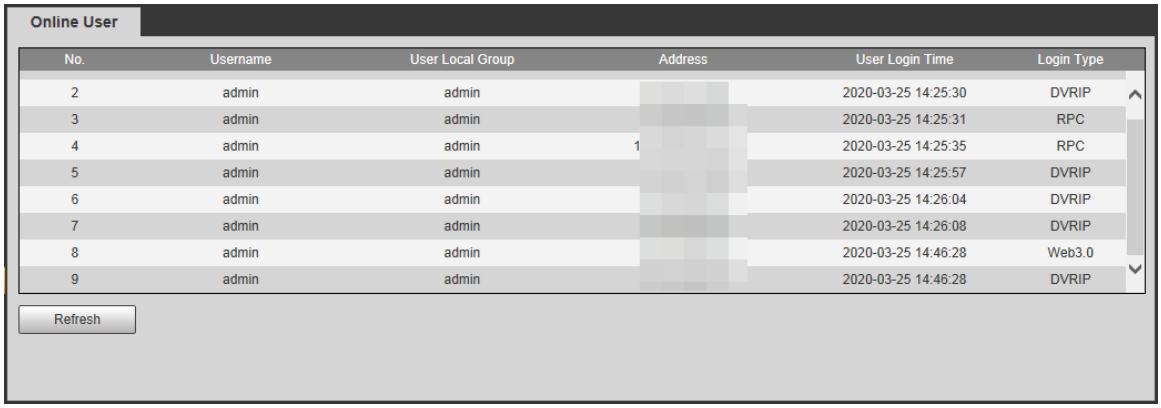
Step 4 Click **Confirm**.

Figure 5-77 Remote log

5.8.3 Online User

Select **Setting >System Info > Online User**, and then you can view online users' information, such as username, user local group, IP address, and user login time.

Figure 5-78 Online user



5.8.4 Work Status

Select **Setting >System Info > Work State**, and then you can view device work status, including CPU used, memory used, and temperature.

Figure 5-79 Work state

5.8.5 Legal Information

Select **Setting >System Info > Open Source Software Notice** to check the legal information.

6 Alarm

Select **Alarm** at the upper-right corner of the web page, and then you can select the event type to trigger an alarm, and also configure the sound of the alarm.

The alarm type might differ depending on the device model.

Figure 6-1 Alarm (ANPR)

Table 6-1 Alarm parameters

Name	Parameter	Description
Alarm Type	Storage Full	Alarm is triggered when storage is full.
	Storage Error	Alarm is triggered when storage error occurs.
	External Alarm	Alarm is triggered by alarm input device.
	No Storage	Alarm is triggered when there is no storage space available.
	Blocklist	Alarm is triggered when a license plate in the blocklist is detected.
	Illegal Access	Alarm is triggered when illegal access is detected.
	Security Exception	Alarm is triggered when a network security problem is detected, such as session hijacking.
Operation	Listen Alarm	When an alarm is triggered, the Camera will inform users on the web page.
Alarm Tone	Play Alarm Tone	Select the **Play Alarm Tone** checkbox, and then click **Choose** to select the alarm tone. The system will play the defined alarm tone when an alarm is triggered.
	Tone Path	

7 FAQ

Table 7-1 FAQ

Question	Solution
Device error, unable to start or operate normally	Press and hold the Reset button for 5 seconds to restore the Camera to factory settings.
TF card hot swapping	Stop recording and image capturing, and then wait for at least 15 seconds before removing the TF card. This helps ensure data integrity and avoid losing all the data on the card.
TF card read/write limit	Do not set the TF card as the storage media for pre-set recording. It might damage the TF card.
TF card cannot be used as storage media	When the TF card hibernates or its capacity is full, format the card through the web first.
Recommended TF card	We recommended using TF card of 16 GB or above. This helps to avoid data loss due to insufficient capacity.

Appendix 1 Allowlist Format

- Fields in the allowlist include start time, time of cancellation, owner's name, license plate color, license plate number, license plate type, vehicle color, type, and more.

Appendix Figure 1-1 Allowlist format template

Begin Time	Cancel Time	Owner Of Car	Plate Color	Plate Number	Plate Type	Vehicle Color	Vehicle Type

- The license plate number must not exceed 12 characters, and the vehicle owner's name must not exceed 30 characters. The start time and end time format must be in strict accordance with the "yy-mm-dd hh:mm:ss" format, and the start time must be earlier than the end time. See the range of values for each time parameter in the table below.

Appendix Table 1-1 Time parameter range

Time Parameter	Value Range
Year	[2000, 2037]
Month	[1, 12]
Day	[1, 31]
Hour	[0, 23]
Minute	[0, 59]
Second	[0, 59]

- In the format template, you need to fill in the number information corresponding to the various attributes of the vehicle. Refer to the tables below for the plate color number, plate type number, model number, vehicle color number, and arm type number.

Appendix Table 1-2 Plate color number

Plate Color	Number
Yellow plate with black text	1
Blue plate with white text	2
Black plate with white text	3
White plate with black text	4

Appendix Table 1-3 Plate type number

Plate Type	Number
Business	1
Private	2

Appendix Table 1-4 Vehicle type number

Vehicle Type	Number
Business	1
Private	2

Appendix Table 1-5 Vehicle color number

Vehicle Color	Number
White	A
Gray	B
Yellow	C
Pink	D
Red	E
Purple	F

Vehicle Color	Number
Green	G
Blue	H
Brown	I
Black	J
Other	Z

Appendix Table 1-6 Arm type number

Arm Type	Number
Annual inspection overdue	1
Stolen & robbed vehicle	2
Hit and run vehicle	3
Traffic violation	4
Other	5

- After filling in the information and creating the excel template file, save the file in .csv format with the file name TrafficAllowList.

Appendix 2 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords.

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

2. **Update Firmware and Client Software in Time**

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

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

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

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

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

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

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers

between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883