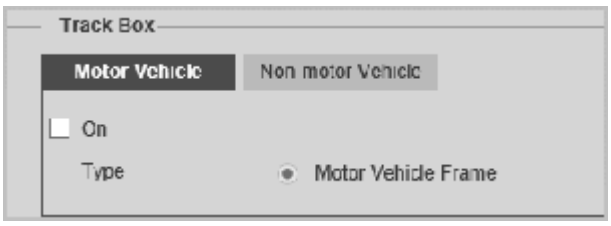
Step 4 In the **Track Box** section, select **On** to enable bounding box of vehicles.

Step 5 Select the bounding box type.

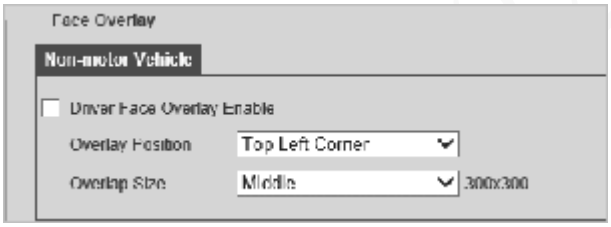
- For motor vehicles, you can overlay the bounding box only on the **Motor Vehicle Frame**.
- For non-motor vehicle, select overlaying bounding box on the **Whole** body or only **Face** of the driver.

Figure 4-65 Track box (2)



Step 6 In the **Face Overlay** section, select whether to enable face overlay and then select the overlay position and size of driver faces.

Figure 4-66 Face overlay (2)



Step 7 Click **Confirm**.

4.7.4.4 Device Direction

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

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

4.7.5 Alarm

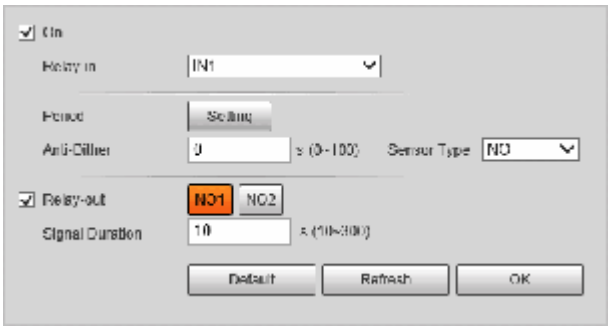
You can configure how the Camera responds when alarms occur.

4.7.5.1 Setting Relay Activation

Set the input and output channel of alarms on the Camera, and then when an alarm is triggered, the Camera outputs the signal to the external device connected to the corresponding output channel, such as a buzzer.

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

Figure 4-67 Relay activation



Step 2 Select **On** to enable the relay-in for the current channel.

Step 3 Select the relay-in channel.

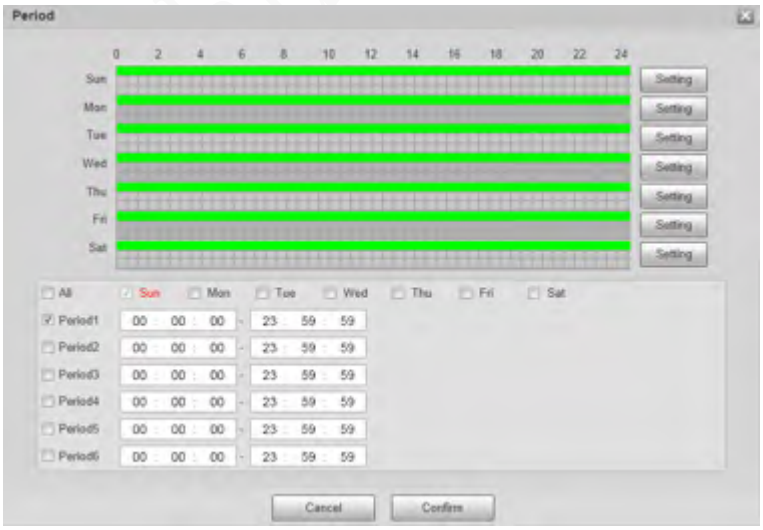
The settings in the subsequent steps are based on the current channel number. They will take effect after you click **Confirm**. If you switch the channel number before clicking **Confirm**, all settings for the current channel will not be effective.

Step 4 Set the relay-in arming and disarming periods.

The Camera outputs alarm signals during armed periods.

1) Click **Setting**.
2) Set the arming and disarming periods.
   - Method 1: Press and hold the left mouse button, and directly drag to set the period on the timeline corresponding to Sunday to Saturday.
   - Method 2: Click **Setting** corresponding to Sunday to Saturday, and then select and set the arming and disarming periods. You can set up to six periods.

Figure 4-68 Period



3) Repeat the earlier steps to set the periods corresponding to other days.
4) Click **Confirm**.

Step 5 Set other parameters.

Table 4-35 Relay activation parameters

Parameter	Description
Anti-Dither	Set the anti-dither duration to filter out false alarms.

Parameter	Description
Sensor Type	Select sensor type according to the connected relay-in device. ● Normally open: Effective for low level. ● Normally closed: Effective for high level.
Relay-out	Optocoupler output. When enabled, the corresponding external device can be activated after an alarm goes off.
Signal Duration	Set the duration of the output signal.

Step 6 Click **Confirm**.

4.7.5.2 Relay-out

You can simulate to trigger alarm output signal.

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

Step 2 Click **NO1** or **NO2** 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 4-69 Relay-out

4.7.6 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.
- **Traffic Light Fault**: Alarm will be triggered when the Camera detects traffic light fault.

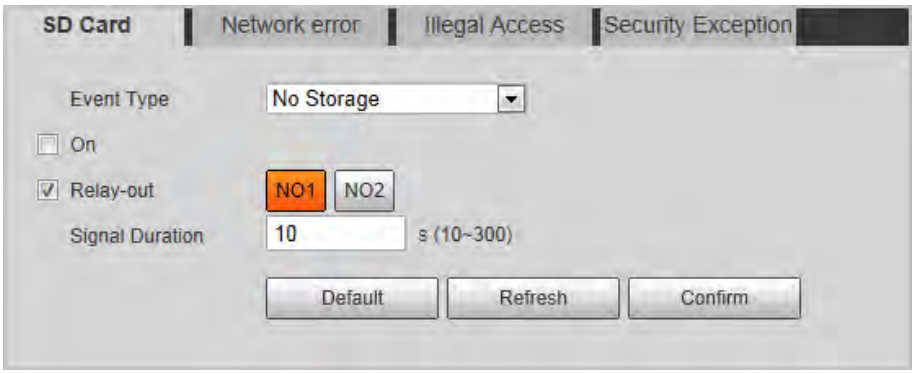
- You can set the alarm tone by selecting **Alarm** at the upper-right side of the Camera's web page.
- **Traffic Light Fault** is only available in **E-Police** mode.

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

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

Step 2 Configure the parameters.

Figure 4-70 SD card event



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

Table 4-36 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**.

4.7.7 Peripheral

4.7.7.1 Extra Device Status

Select **Setting** > **Peripheral** > **Peripheral** > **Extra Device Status**, and then you can view the information of the connected external devices.

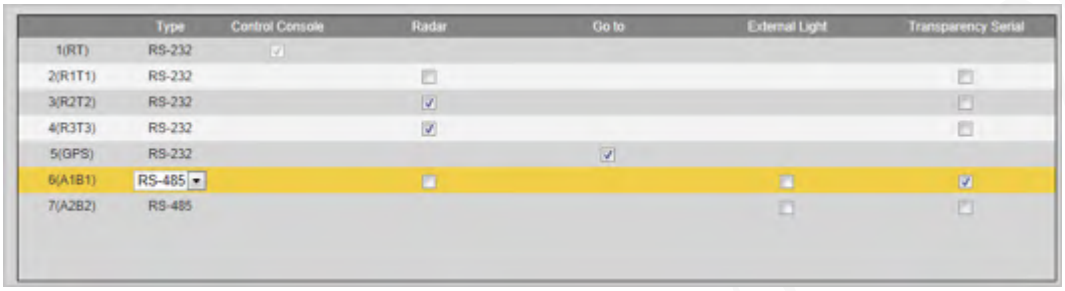
4.7.7.2 Serial Port Settings

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**.

Step 2 Configure external devices.

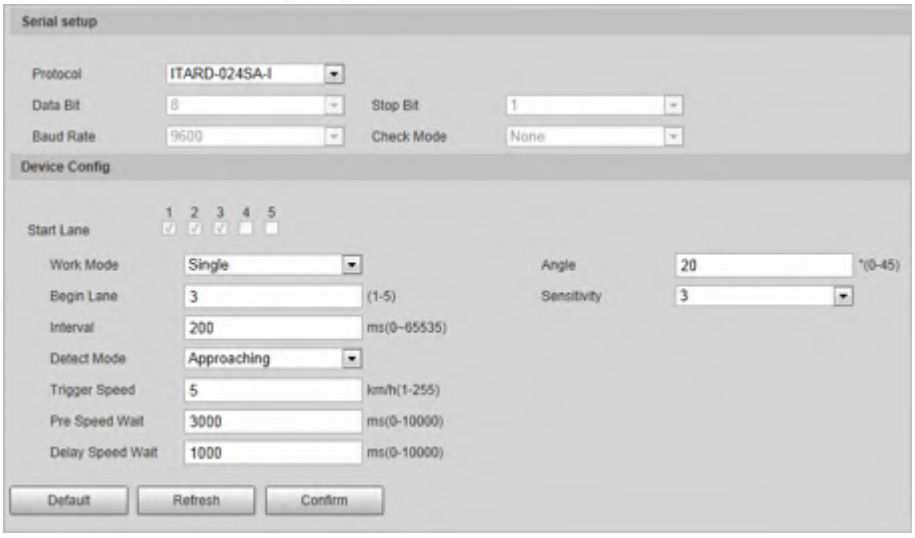
Figure 4-71 Serial port settings



- One serial port can only enable one external device.
- RS-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 4-72 Radar configuration (single lane)



2) Configure radar parameters.

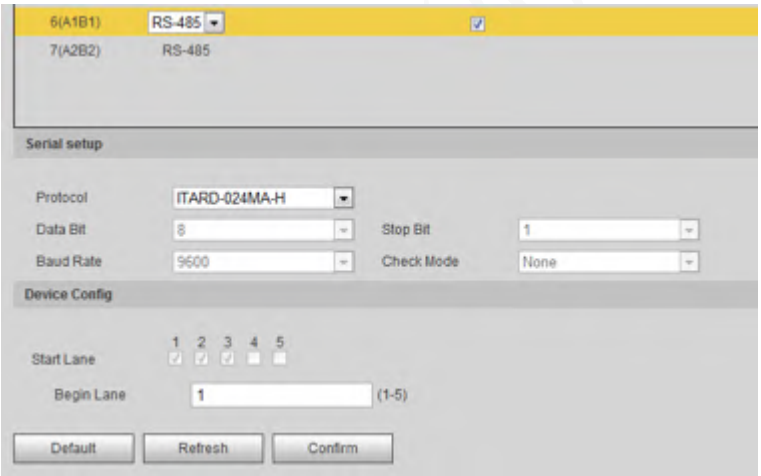
Table 4-37 Description of important parameters of the radar

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**.

Parameter	Description
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.
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 4-73 Radar configuration (multiple lanes)

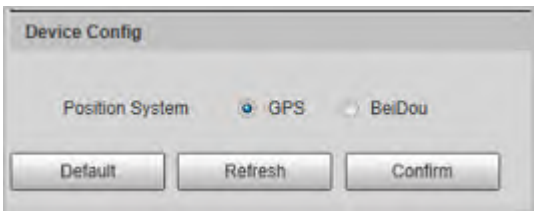


4) Click **Confirm**.

- Positioning

1) Select **Go to**.

Figure 4-74 Positioning configuration



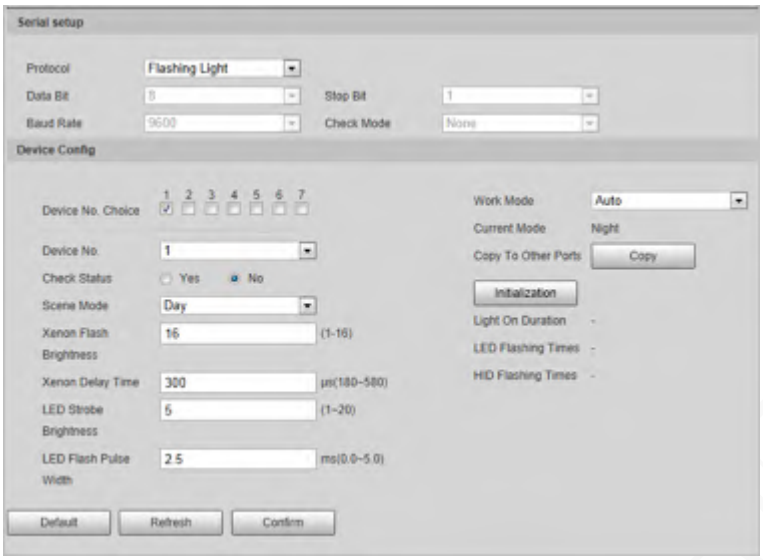
2) Select the positioning method from **GPS** and **BeiDou** as needed.

3) Click **Confirm**.

- External Light

1) Select **External Light**.

Figure 4-75 External light configuration



2) Configure external light parameters.

Table 4-38 Important external light parameters description

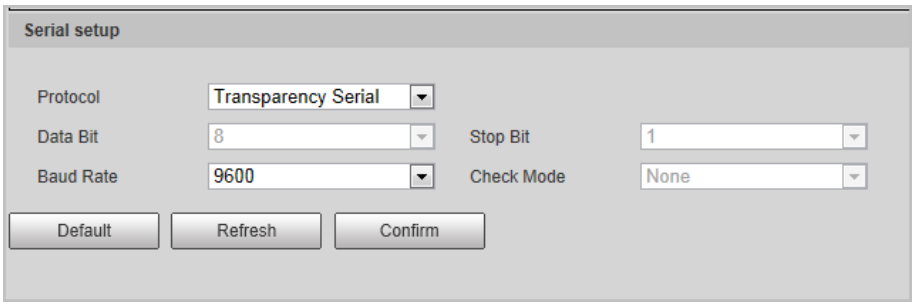
Parameter	Description
Protocol	Select from Flashing Light, Strobe and Continuous Light.
Device No. Choice	Select device number as needed.
Device No.	Select external light number based on the selected device number.
Check Status	Select **Yes** to enable external light status check.
Scene Mode	Select the 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 4-76 Transparency serial



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

4.7.7.3 Light Configuration

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

Step 1 Select **Setting** > **Peripheral** > **Peripheral** > **Light Config**.

Figure 4-77 Light config

Step 2 Configure parameters.

Table 4-39 Illuminator parameter description

Parameter		Description
F1/2/3/4/5/6/7		Select the light type connected to each port. The light type must be the same as the actual connected light type. Otherwise, the light might be damaged.
Flashing Light	Work Mode	• **Forbidden**: The light is normally off. • **Always**: The light is normally on. • **Default**: Configure the preset value of brightness. If the ambient brightness is lower, the light automatically turns on; if higher, the light automatically turns off.
	Scene Mode	Select the scene mode for the flashing light from **Dawn/Dusk**, **Daytime** and **Night**, indicating different brightness of the light which suits the environment the best.
	Pulse Width	Configure the pulse width of flashing light. The higher the value, the brighter the light.

Parameter		Description
	Delay Time	Configure the delay time of the light to keep the snapshot in sync with the flash.
	Burst Mode	You can select the level that triggers the flashing light. Currently, only **Low** level is supported.
	Prevalue	When setting **Work Mode** to **Default**, you need to set the brightness prevalue.
Strobe	Output Mode	Same as **Work Mode** of flashing light.
	Frequency	Set the frequency of the strobe.

Step 3 Click **OK**.

The light type in this section is for reference only, and might differ from the actual model.

4.7.8 Storage

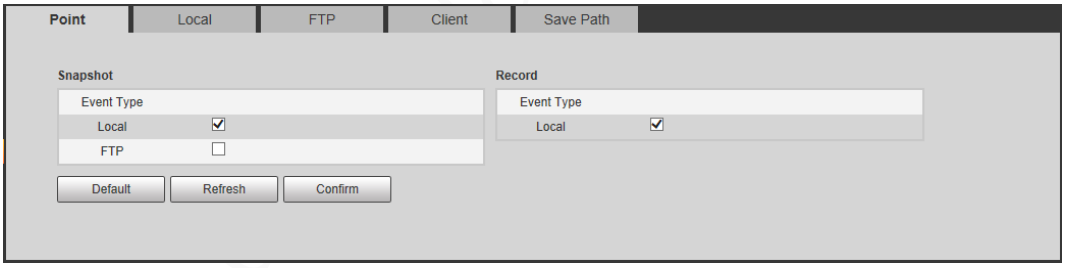
You can configure the storage path of snapshots and video records.

4.7.8.1 Point

Set the storage path of snapshots and video recordings.

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

Figure 4-78 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**.

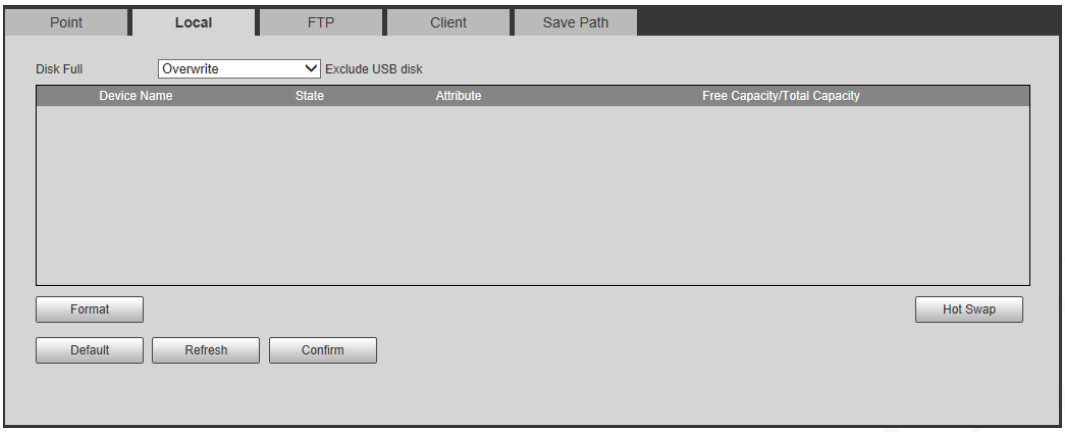
4.7.8.2 Local

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 4-79 Local

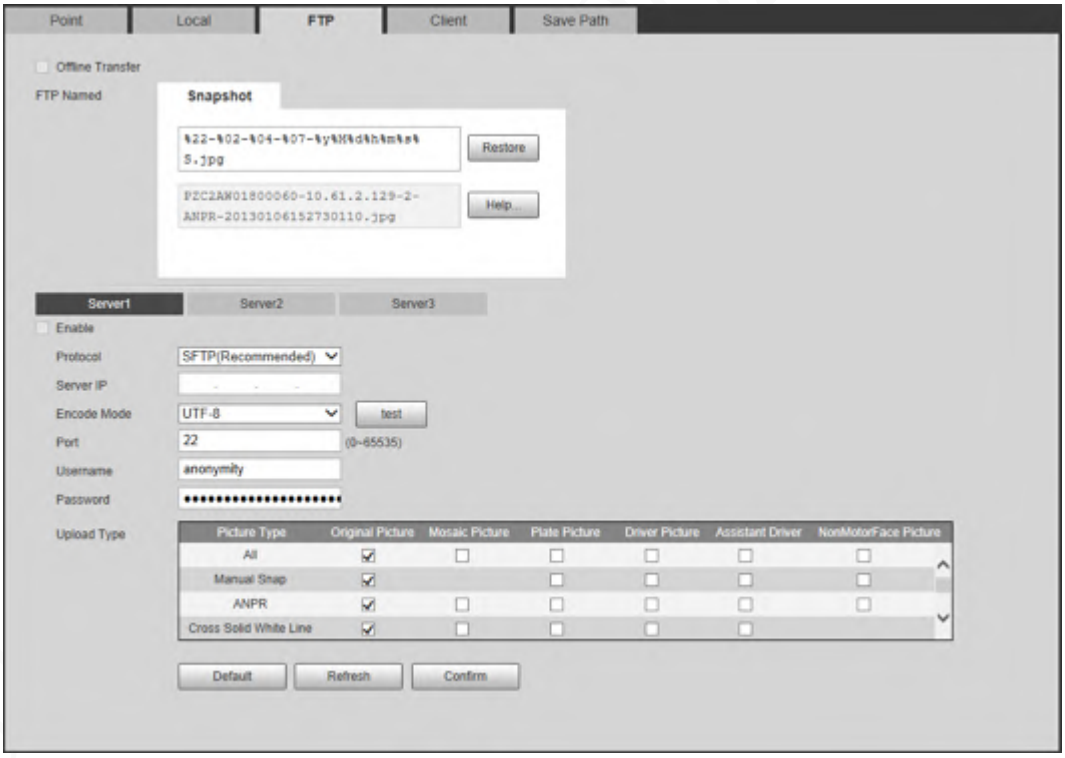


4.7.8.3 FTP

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 4-80 FTP



Step 2 Configure the parameters.

Table 4-40 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.

Parameter	Description
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.
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.

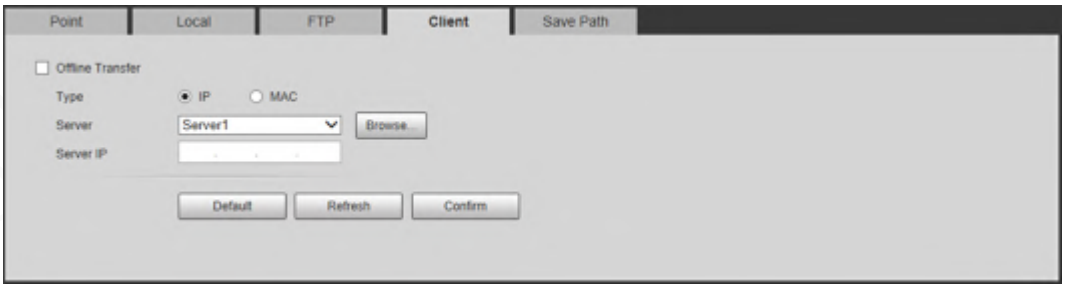
Step 3 Click **Confirm**.

4.7.8.4 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 4-81 Client



Step 2 Configure the parameters.

Step 3 Click **Confirm**.

4.7.8.5 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**

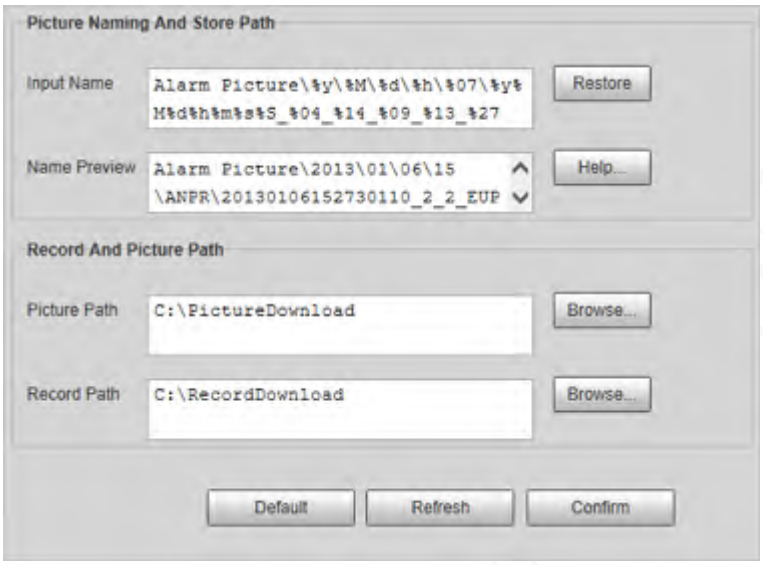
Naming Help, or click **Restore** to restore the naming rule to the default.

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**.

Figure 4-82 Save path



4.7.8.6 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.

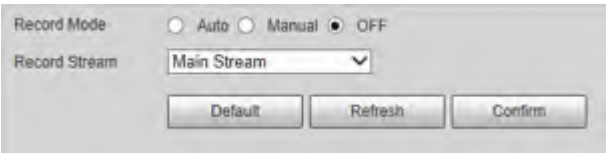
- **Auto**: Record videos only when a traffic violation event is detected.

  After enabling auto recording, go to **Setting** > **Event** > **ANPR Snap**, in the **Rule Config** section, 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 4-83 Record control



4.7.9 System

4.7.9.1 General

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

4.7.9.1.1 General Settings

You can configure the Camera No., video standard, and more.

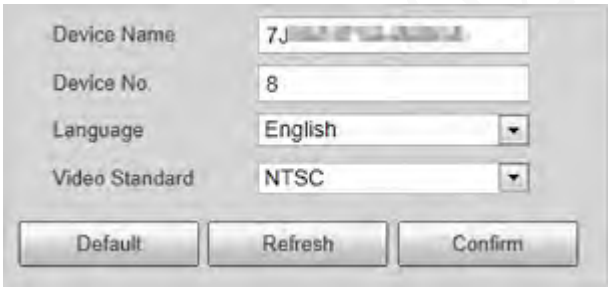
Step 1 Select **Setting** > **System** > **General Setup** > **General Setup**.

Step 2 Configure the parameters.

For **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, the Philippines.

Figure 4-84 General



Step 3 Click **Confirm**.

4.7.9.1.2 Date & Time

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

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

Step 2 Configure the parameters.

Figure 4-85 Date & time

Table 4-41 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	Only **24-Hour** is available.
Time Zone	The time zone where the Camera locates.
System Time	The current time of the Camera.
Sync PC	Sync the time of the Camera with the time of the computer. Click **Sync PC**, and settings will immediately take effect.
DST	Select the **DST** (Daylight Saving Time) checkbox, set the **DST Type** by **Date** or by **Week**, and then configure the **Start Time** and **End Time** of DST.
Enable	Select **GPS** or **BeiDou** positioning system.
Check Time Mode	Select time synchronization mode. ● **NTP**: Select the checkbox to enable **NTP** (network time protocol) time synchronization. In this case, you need to set the NTP server IP address, port, and time synchronization interval. ● **Satellite**: Synchronize the time according to the positioning. In this case, you need to enable **GPS** or **BeiDou** positioning first.

Step 3 Click **Confirm**.

4.7.9.2 Account Management

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

4.7.9.2.1 Managing Users

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

- After the Camera is initialized, the admin user generated by default has the highest permission. The admin user cannot be deleted, and its permissions cannot be changed.
- Users with **User** permission can change its own password, and change the password of other users.
- Users who have logged in cannot be deleted.

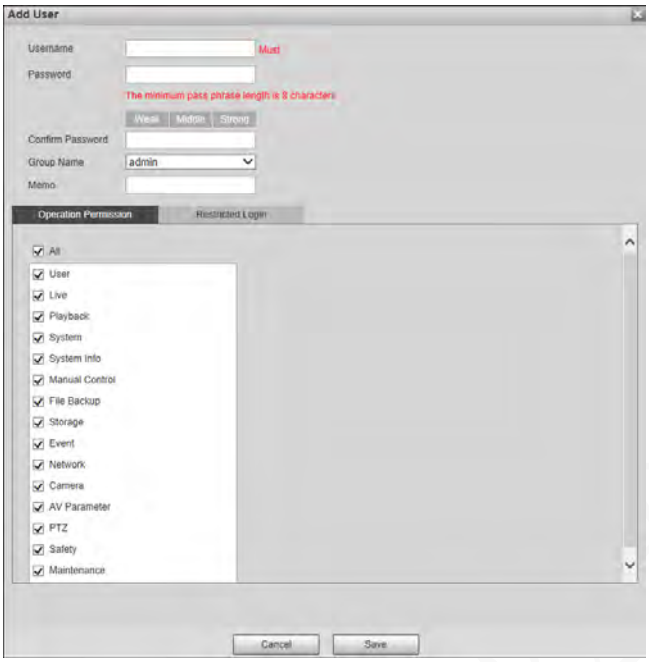
Procedure

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

Step 2 Click **Add User**.

Step 3 Configure the user information including username, password, group name, memo, and operation permissions.

Figure 4-86 Add user



Step 4 Set login restrictions (if necessary), and then the restricted IP addresses or IP within the defined segment will be allowed to log in to the Camera during the defined validity period and time.

Figure 4-87 Configure login restriction

Step 5 Click **Save**.

Related Operations

- Click to delete the corresponding user. Admin user cannot be deleted.
- Click corresponding to the user. You can edit the information such as username, password, email address, group name, and memo. Click **Save** to save the settings.
- Click to edit the restricted login settings of the user account.
- Select **Setting** > **System** > **Account** > **Account** > **Clear user information** to clear all user information.

4.7.9.2.2 Managing User Groups

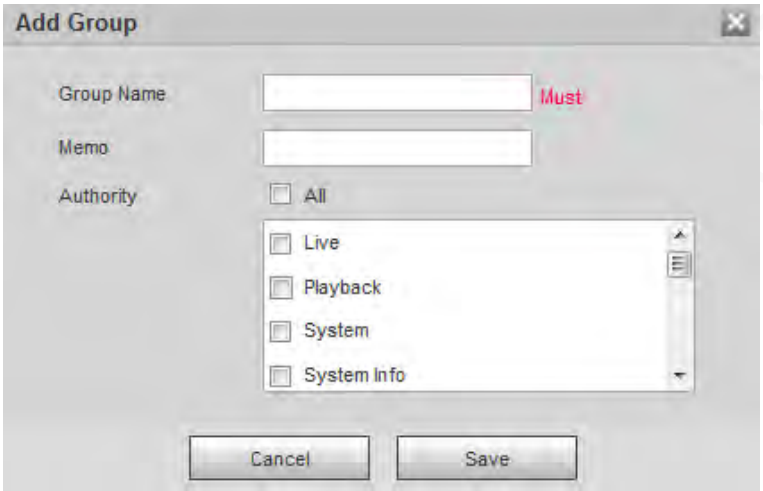
After the Camera is initialized, two user groups, admin and user, are generated by default. You can also add or delete user group(s), and change user group password and permissions.

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

Step 2 Add, modify, and delete user groups.

- Add a user group
  1. Click **Add Group**.
  2. Configure the **Group Name** and **Authority** of the group.

Figure 4-88 Add user group



  3. Click **Save**.

  Click an added user group, and then you can view its permissions.

- Modify a user group
  1. Click .
  2. Modify the memo and permissions of the group.

  Permission of admin user group cannot be deleted.

  3. Click **Save**.
- Delete a user group

  Click to delete the selected user group. Admin and user groups cannot be deleted.

4.7.9.2.3 ONVIF User

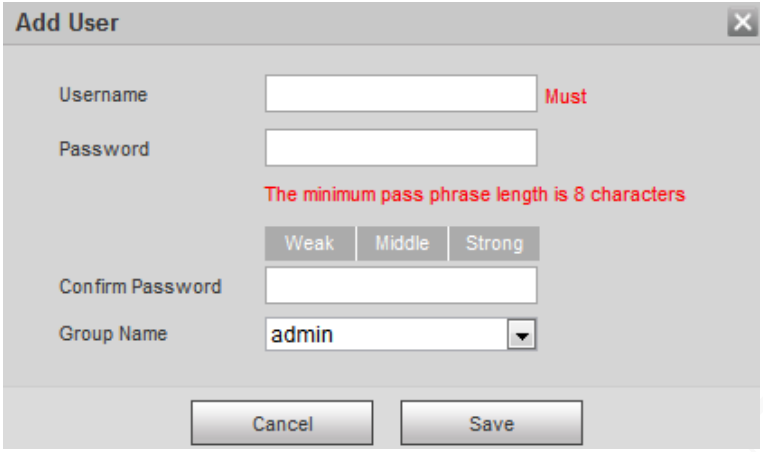
You can view ONVIF user information, add or delete ONVIF users, and change ONVIF user passwords.

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

Step 2 Add, modify, and delete an ONVIF user.

- Add user
  1. Click **Add User**.
  2. Configure user information such as username, password, and group name.

Figure 4-89 Add user



3. Click **Save**.

- Modify user

  Click  to modify the information such as username, password, and group name. Group of admin user cannot be modified.

- Delete user

  Click  to delete the added user. Admin user cannot be deleted.

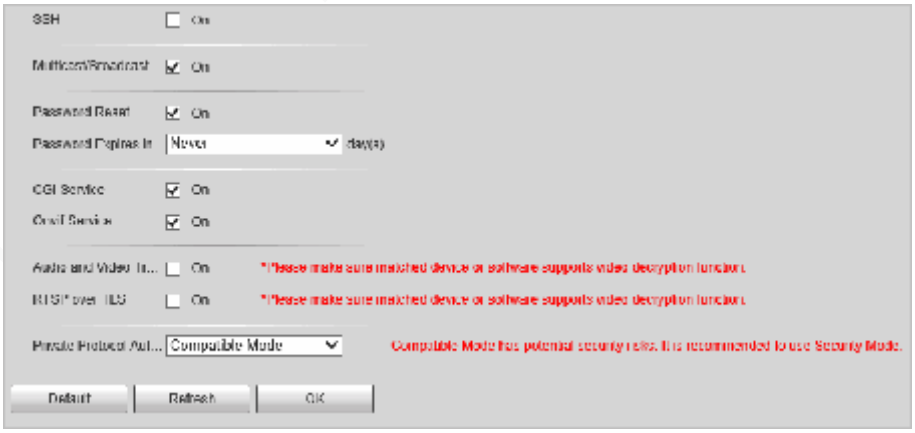
4.7.9.3 Safety

4.7.9.3.1 System Service

You can enable multiple system services to secure network safety.

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

Figure 4-90 System service



Step 2 Enable the services as needed.

Table 4-42 Description of system service parameters

Parameter	Description
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. It is a method for secure remote login, providing secure access for users.

Parameter	Description
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 you can reset the password when you forgot your password. You can also set the validity of the password in **Password Expires in xx day(s)**.
CGI Service	The service is enabled by default. CGI is the interface between external applications and the web server, and devices can be accessed through this protocol.
Onvif Service	The service is enabled by default. It allows network video products produced by different manufacturers to communicate with each other.
Audio and Video Transmission Encryption	Select the **Enable** checkbox to enable encryption during audio and video transmission. Make sure that the matched device or software supports video decryption function; otherwise, do not enable it.
RTSP over TLS	Enable this function to encrypt stream transmitted through standard protocol. We recommend you keep the function on.
Private Protocol Authentication Mode	Leave it as default.

Step 3 Click **OK**.

4.7.9.3.2 HTTPS

Prerequisites

- For first-time use of HTTPS or after changing device IP address, you need to create server certificate, and install root certificate.
- After creating server certificate, and installing root certificate, if you change a computer to log in to the web client, then you need to download and install the root certificate again on the new computer or copy the downloaded root certificate on the new computer, and install it.

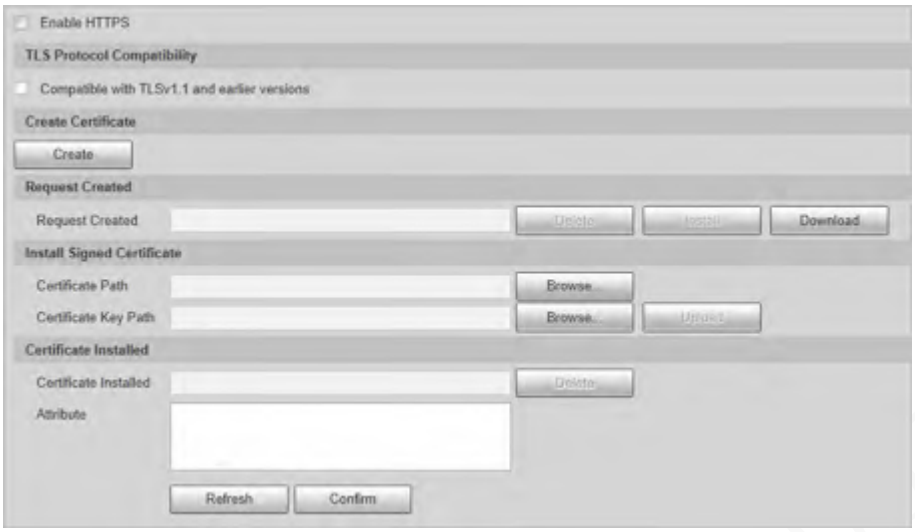
On the **HTTPS** page, users can make computer log in normally through HTTPS by creating certificate or uploading authenticated certificate. It can ensure security of communication data, and provide guarantee for user information, and device safety through reliable and stable technical approach.

Procedure

Step 1 Create certificate or upload the authenticated certificate.

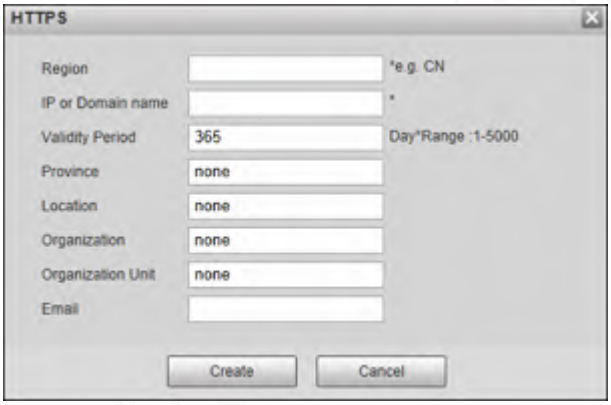
- Create a certificate.
  1. Select **Setting** > **System** > **Safety** > **HTTPS**.

Figure 4-91 HTTPS



2. Click **Create**.

Figure 4-92 HTTPS



3. Enter the required information such as region, IP or domain name, and then click **Create**.

   The entered **IP or Domain name** must be the same as the IP or domain name of the Camera.

4. Click **Install** under **Request Created**, and then click **Download** to download root certificate.

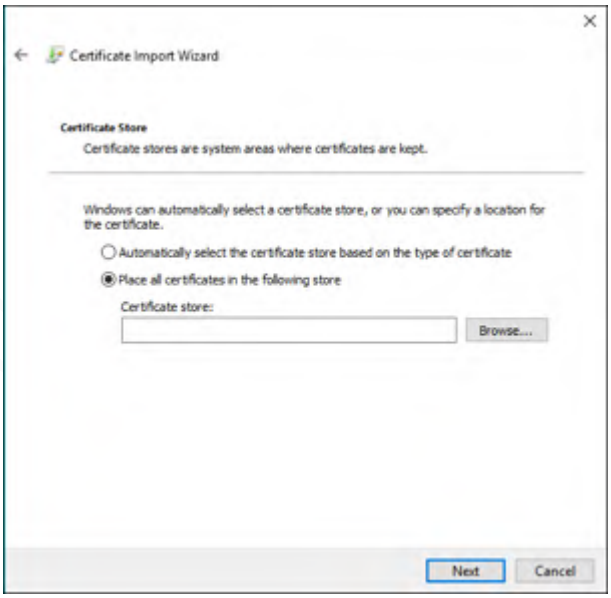
   The system pops up **Save As** dialog box, select storage path, and then click **Save**.

5. Double-click the RootCert.cer icon.
6. Click **Install Certificate…**.

Figure 4-93 Install certificate

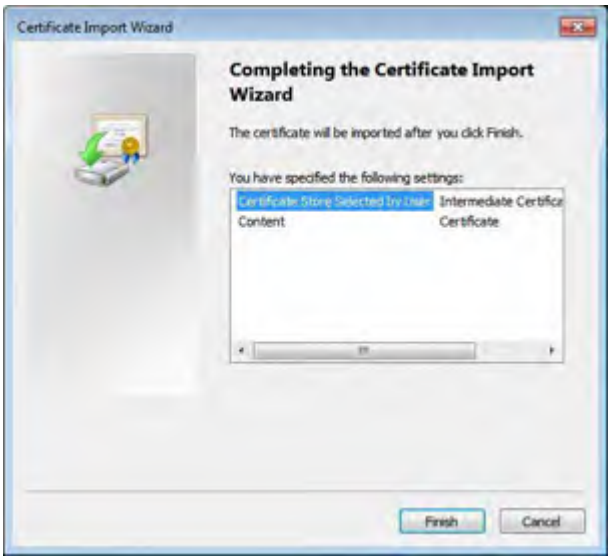
7. Click **Next**.

Figure 4-94 Certificate store



8. Click **Next**.

Figure 4-95 Completing certificate import wizard



9. Click **Finish**.

Figure 4-96 Security warning

10. Click **Yes**, and then click **OK** on the pop-up window.

- Install a signed certificate.
  1. Select **Setting Safety** > **System** > **Safety** > **HTTPS**.
  2. Select **Enable HTTPS**, and **Compatible with TLSv1.1 and earlier versions**.
  3. Click **Browse** to upload the signed certificate, and certificate key, and then click **Upload**.
  4. To install the root certificate, see operation steps from 4 to 10 in **Create Certificate**.

Step 2 Select **Enable HTTPS**, and click **Confirm**.

The configuration takes effect until the Camera restarts.

Step 3 Use HTTPS to log in to the Camera.

1. Enter https://*xx.xx.xx.xx* in the browser.

   xx.xx.xx.xx is the Camera IP address or domain name.

2. Enter the username, and password to log in to the Camera.

4.7.9.3.3 Firewall

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

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

Figure 4-97 Firewall

Step 2 Select **Rule Type**.

- **Network Access**: Add the IP address to allowlist or blocklist to allow or restrict it to access corresponding ports of the Camera.
- **PING Prohibited**: IP address of your camera is prohibited from ping. This helps prevent attempt of accessing your network system without permission.
- **Prevent Semijoin**: Prevents half-open SYN attacks.

Step 3 Select **On** to enable the selected rule type.

Step 4 Click **Confirm**.

4.7.9.4 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**, and then enter the correct login password in the pop-up box to restore all configurations of the Camera to default settings, including IP address.

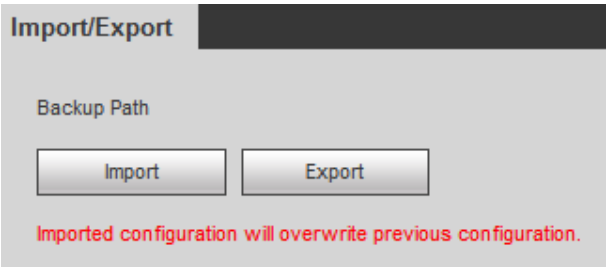
Figure 4-98 Default

4.7.9.5 Import/Export

The system supports exporting the configurations on web to local computer for backup, and importing the configuration files from local backup for quick configuration or restoration.

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

Figure 4-99 Import/Export



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

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

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

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

4.7.9.6 Auto Maintain

The system automatically restarts at 02:00 every day by default. You can also select to automatically restart the Camera at the defined day and time, or manually restart the Device to solve problems such as stuck images.

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

Figure 4-100 Auto maintain

Step 2 Select **Auto Reboot**, and then set the restart time.

Step 3 Select **Auto Delete Old Files**, and then set a time point, and all the old files before this time will be deleted.

Step 4 (Optional) Click **Manual Reboot** can restart the Camera immediately.

Step 5 Click **Confirm**.

Step 6 Select **Emergency Maintenance**, and then select **On** to enable the function.

Step 7 Click **Save**.

4.7.9.7 System Upgrade

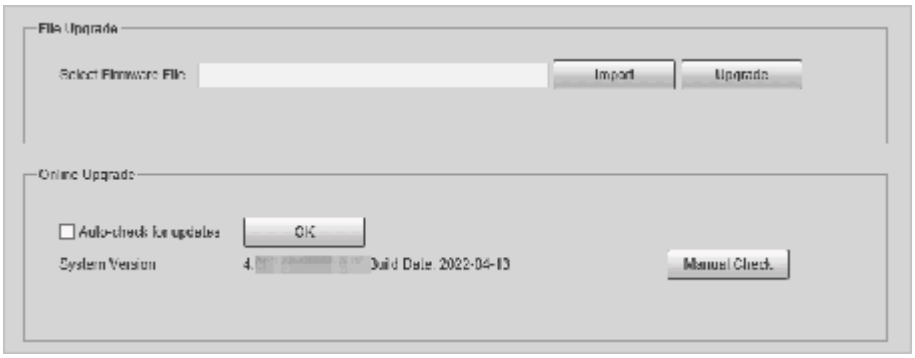
You need to update the system to the latest version to make the Camera run properly.

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

Step 2 Upgrade the system through file upgrade or online upgrade.

- File Upgrade
  1. Click **Import**, and then select the upgrade file in the pop-up dialog box.
  2. Click **Upgrade** to start system upgrading.
- Online Upgrade
  - Select **Auto-check for updates**, and then click **Confirm**. When a new version is detected, click **Upgrade Now**, the system starts upgrading.
  - Click **Manual Check**, and when a new version is detected, click **Upgrade Now**, the system starts upgrading.

Figure 4-101 System upgrade



4.7.10 System Information

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

4.7.10.1 Version Information

Select **Setting** > **System Info** > **Version**, and then click **Version** or **Peripheral Edition Info** to view information such as device type, software version, web version, and version of the radar and flashlight.

Versions might vary depending on the different devices.

4.7.10.2 Log

4.7.10.2.1 System Log

You can search for and view logs by the time and type, and backup the logs.

After the number of log records reaches a certain number, the earliest log records will be overwritten. To prevent critical logs from being overwritten, the system performs log overwriting in three levels: Low, medium, and high.

- Low: When the log records reach 896, the earliest log records will be overwritten.
- Medium: When the log records reach 256, the earliest log records will be overwritten.
- High: When the log records reach 640, the earliest log records will be overwritten.

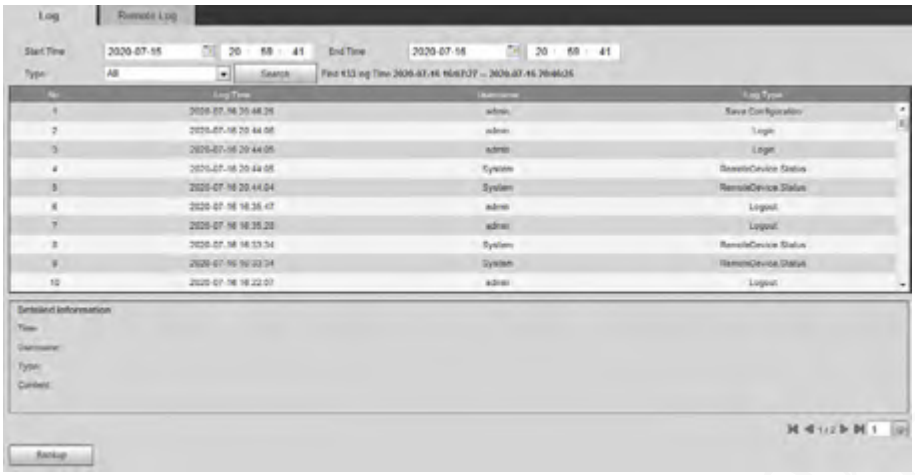
Step 1 Select **Setting** > **System Info** > **Log** > **Log**.

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

Step 3 Click **Search**. You can stop searching according to your need.

- View: Click a log to view its details.
- Back up: Click **Backup** to back up the log to local computer in .txt format.

Figure 4-102 System log



4.7.10.2.2 Remote Log

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

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

Figure 4-103 Remote log

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

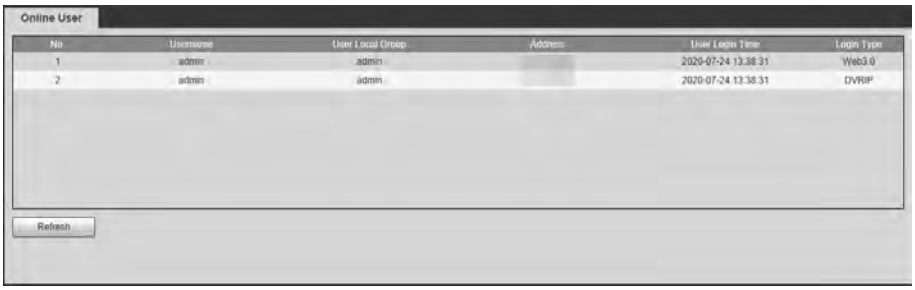
Step 3 Configure the IP address, port, and device number of remote device.

Step 4 Click **Confirm**.

4.7.10.3 Online User

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

Figure 4-104 Online user



4.7.10.4 Work Status

Select **Setting** > **System Info** > **Work State**, and then you can view device work status, including

CPU, memory and temperature.

4.7.10.5 Legal Information

Select **Setting** > **System Info** > **Legal Info** to view the Open Source Software Notice.

4.8 Alarm

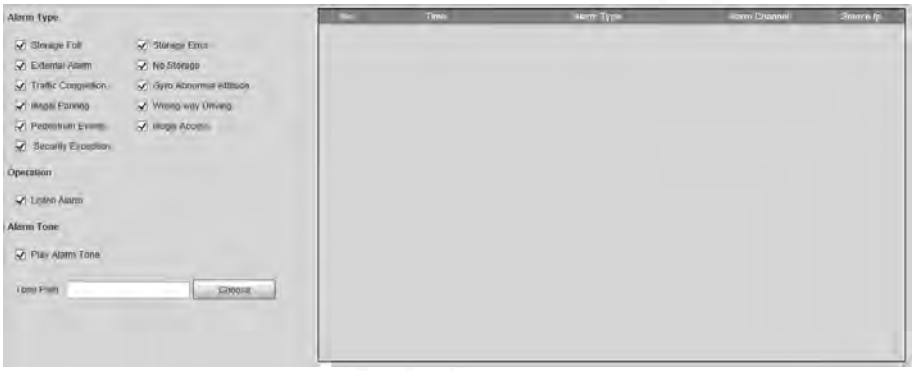
You can select the event type that triggers an alarm, and also configure how to sound the alarm.

Step 1 Select **Alarm** at the upper-right side of web.

Step 2 Select alarm type as needed.

When alarms are triggered, information of the selected alarm type will be displayed at the right side.

Figure 4-105 Alarm



Step 3 Configure alarm operation and alarm tone.

Table 4-43 Description of alarm parameters

Parameter	Description
Operation	Select **Listen Alarm**, and when an alarm is triggered and you are not viewing the alarm page, will be displayed on the alarm menu bar, and the alarm information will be automatically recorded. When you click the alarm menu bar, the icon disappears. If you are viewing the alarm page when an alarm is triggered, the alarm icon will not appear, but alarm information will be recorded in the alarm list on the right.
Alarm Tone	Select **Play Alarm Tone** to enable playing alarm tone, and then click **Choose** to select the audio file. When an alarm is triggered, the system plays the selected audio. Currently, only **.wav** audio file is supported.

4.9 Logout

Click **Logout** at the upper-right side of the web page to log out. You can enter the username and

password to log in again.

Appendix 1 Reference for Filling in Allowlist and Blocklist Template

Appendix Table 1-1 Plate color number

Plate Color	Plate Color No.
Yellow Plate with Black Text	1
Blue Plate with White Text	2
Black Plate with White Text	3
White Plate with Black Text	4
Black	5
Blue	6
Cyan	7
Red	8
Gradient Green	9
White	10
Yellow and Green	11
Yellow	12

Appendix Table 1-2 Vehicle color number

Vehicle Color	Vehicle Color No.
White	A
Black	B
Red	C
Yellow	D
Gray	E
Green	F
Blue	G
Pink	H
Purple	I
Brown	J
Yellow Green	K
Cyan	L
Dark Blue	M
Dark Brown	N
Dark Cyan	O
Dark Golden	P
Dark Green	Q

Vehicle Color	Vehicle Color No.
Dark Olive	R
Dark Orange	S
Dark Pink	T
Dark Purple	U
Dark Red	V
Dull Purple	W
Dark Yellow	X
Deep Sky Blue	Y
Others	Z
Dark Gray	a
Forest Green	b
Golden	c
Green Yellow	d
Chestnut	e
Light Rosy	f
Olive	g
Orange	h
Ocean Green	i
Silver Gray	j
Tomato Red	k
White Smoke	l

Appendix Table 1-3 Vehicle type number

Vehicle Type	Vehicle Type No.
Large Vehicle	1
Small Vehicle	2
Tractor	14
Bus	23
Heavy Truck	24
MPV	25
Light Truck	26
Van	27
Medium Bus	28
Medium Truck	29
Minicar	30
Two-wheeled Vehicle	31
Tank Truck	32

Vehicle Type	Vehicle Type No.
Public Bus	33
Pickup	34
SUV	35
Sedan	36
SUV-MPV	37
Taxi	38
Tricycle	39
Unknown	40
Ambulance	41
Mixer Truck	42
Construction Truck	43
Fire Truck	44
General	45
Engineering Truck	46
Fuel Tank Truck	47
Police Car	48
Pulverized Material Vehicle	49
Tank Truck	50
Sewage Suction Truck	51
Hazardous Chemicals Truck	52
Sanitation Truck	53

Appendix 2 Cybersecurity Recommendations

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.
14. Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two

conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

If the distance from the product to the human body is greater than 20cm, the following warning is required (this requirement is not required for micro-power SRD devices).

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.