High Performance Event Detection Server

User Manual

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Regulatory Information

FCC Information

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.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

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

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: ***www.recyclethis.info***

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: ***www.recyclethis.info***

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Note	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction

Regulatory Information

This is a class A product and may cause radio interference in which case the user may be required to take adequate measures.

Laws and Regulations

Use of the product must be in strict compliance with the local laws and regulations. Please shut down the device in prohibited area.

Power Supply

- Use of the product must be in strict compliance with the local electrical safety regulations.
- Use the power adapter provided by qualified manufacturer. Refer to the product specification for detailed power requirements.
- It is recommended to provide independent power adapter for each device as adapter overload may cause over-heating or a fire hazard.
- Make sure that the power has been disconnected before you wire, install, or disassemble the device in the authorized way according to the description in the manual.
- To avoid electric shock, DO NOT directly touch exposed contacts and components once the device is powered up.
- DO NOT use damaged power supply devices (e.g., cable, power adapter, etc.) to avoid electric shock, fire hazard, and explosion.
- DO NOT directly cut the power supply to shut down the device. Please shut down the device normally and then unplug the power cord to avoid data loss.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- Make sure the power supply has been disconnected if the power adapter is idle.
- Connect to earth before connecting to the power supply.

Transportation, Use, and Storage

- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- Store the device in dry, well-ventilated, corrosive-gas-free, no direct sunlight, and no heating source environment.
- Avoid fire, water, and explosive environment when using the device.
- Install the device in such a way that lightning strikes can be avoided. Provide a surge suppressor at the inlet opening of the equipment under special conditions such as the mountain top, iron tower, and forest.
- Keep the device away from magnetic interference.
- Avoid device installation on vibratory surfaces or places. Failure to comply with this may cause device damage.
- DO NOT touch the heat dissipation component to avoid burns.

- DO NOT expose the device to extremely hot, cold, or humidity environments. For temperature and humidity requirements, see device specification.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- DO NOT touch the sharp edges or corners.
- To prevent possible hearing damage, DO NOT listen at high volume levels for long periods.

Maintenance

- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.
- If the device cannot work properly, contact the store you purchased it or the nearest service center. DO NOT disassemble or modify the device in the unauthorized way (For the problems caused by unauthorized modification or maintenance, the company shall not take any responsibility).
- Keep all packaging after unpacking them for future use. In case of any failure occurred, you need to return the device to the factory with the original packaging. Transportation without the original packaging may result in damage to the device and the company shall not take any responsibility.

Network

- Please enforce the protection for the personal information and the data security as the device may be confronted with the network security problems when it is connected to the Internet. Contact us if network security risks occur.
- Please understand that you have the responsibility to configure all the passwords and other security settings about the device, and keep your user name and password.

Data

DO NOT disconnect the power during formatting, uploading, and downloading. Or files may be damaged.

Contents

Chapter 1 Introduction

1.1 Production Introduction

Event detection server, the multiple-channel video analysis device, provides multiple functions, including real-time smart detection of events and traffic parameters collection. It can capture the detected events, and recognize license plates. It is widely applied in cities, highways, tunnels, etc.

1.2 Key Feature

- Box cameras and speed domes are connectable to detect traffic events and collect traffic parameters.
- Rack-mounted 1U chassis design, convenient to be placed in the cabinet of machine room.
- Supports multiple events detection, such as congestion, parking, wrong-way driving, etc.
- Supports multiple traffic parameters collection, such as vehicle type, lane flow, speed, space headway, time headway, etc.
- Supports zooming capture of illegal parking and patrol detection of multiple scenes when a speed dome is connected.
- Supports operation via web browser.
- Supports customizing specific events detection.

Note

The supported functions vary with device models. The actual device prevails.

1.3 System Requirement

- Web Browser: IE 9.0 and above versions.
- Resolution: 1024 × 768 and above.

Chapter 2 Activation and Login

2.1 Activation

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. The device supports multiple activation methods, such as activation via SADP software, web browser, and iVMS-4200 Client.

Note

Refer to the user manual of iVMS-4200 Client for the activation via client software.

2.1.1 Default Information

The device default information is shown as below.

- Default IP address: 192.168.1.64
- Default user name: admin

2.1.2 Activate via SADP

SADP is a tool to detect, activate, and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website (***http://www.hikvision.com/***), and install it according to the prompts.
- The device and the computer that runs the SADP tool should belong to the same network segment.

The following steps show how to activate one device and modify its IP address. For batch activation and IP address modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Enter a new password (admin password) and confirm the password.

   Caution

   STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Click **Activate** to start activation.

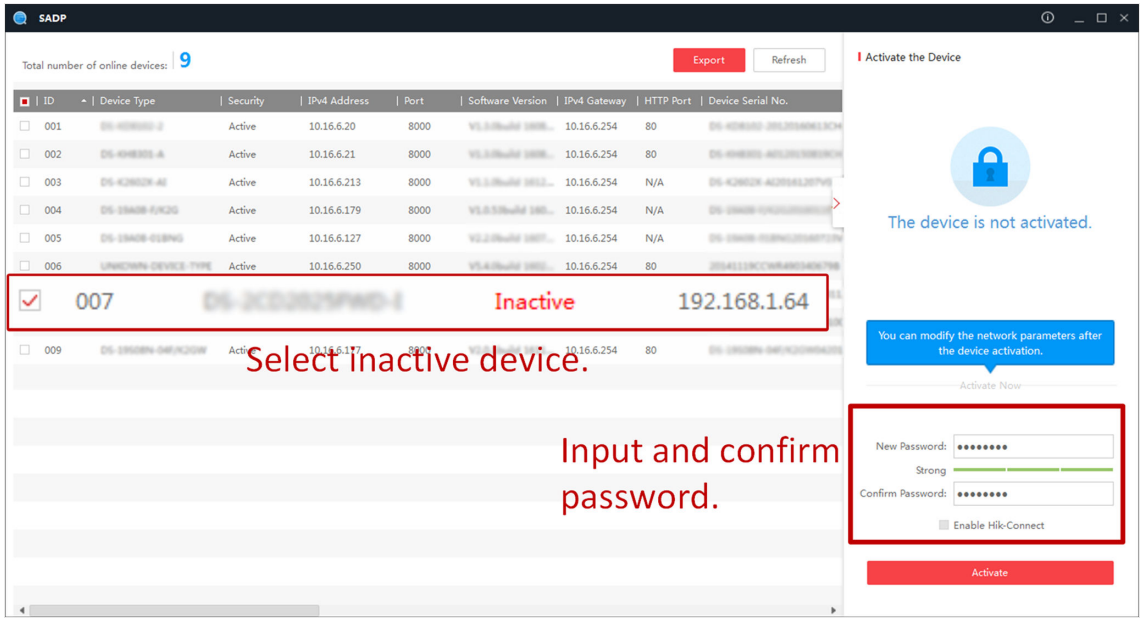

Figure 2-1 Activate via SADP

Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same network segment as your computer by either modifying the IP address manually or checking **Enable DHCP** (Dynamic Host Configuration Protocol).
   3) Enter the admin password and click **Modify** to activate your IP address modification.

2.1.3 Activate via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use SADP software or client software to activate the device.

Before You Start

Ensure the device and the computer are in the LAN with the same network segment.

Steps

1. Change the IP address of your computer to the same network segment as the device.
2. Open the web browser, and enter the default IP address of the device to enter the activation interface.
3. Create and confirm the admin password.

Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **OK** to complete activation.
5. Go to the network settings interface to modify IP address of the device.

2.2 Login

You can log in to the device via web browser for further operations such as live view and local configuration.

Before You Start

Connect the device to the network directly, or via a switch or a router.

Steps

1. Open the web browser, and enter the IP address of the device to enter the login interface.
2. Enter **User Name** and **Password**.
3. Click **Login**.
4. Download and install appropriate plug-in for your web browser. Follow the installation prompts to install the plug-in.
5. Reopen the web browser after the installation of the plug-in and repeat steps 1 to 3 to login.
6. **Optional:** Click **Logout** on the upper right corner of the interface to log out of the device.

Chapter 3 Basic Operation

3.1 Set LAN IP Address

Different LAN interfaces correspond to different network segments and information transmissions of different function modules.

Steps

1. Go to **Network → Local → Configuration → Network** .
2. Click **LAN/LAN1/LAN2** to set network according to the actual needs.

Note

- LAN is used to access the network and connect to the platform. LAN1 and LAN2 are both load balanced, which are used to connect to a camera and get streams from a device.
- If you need to access the device via a remote domain name, you should configure the DNS server.

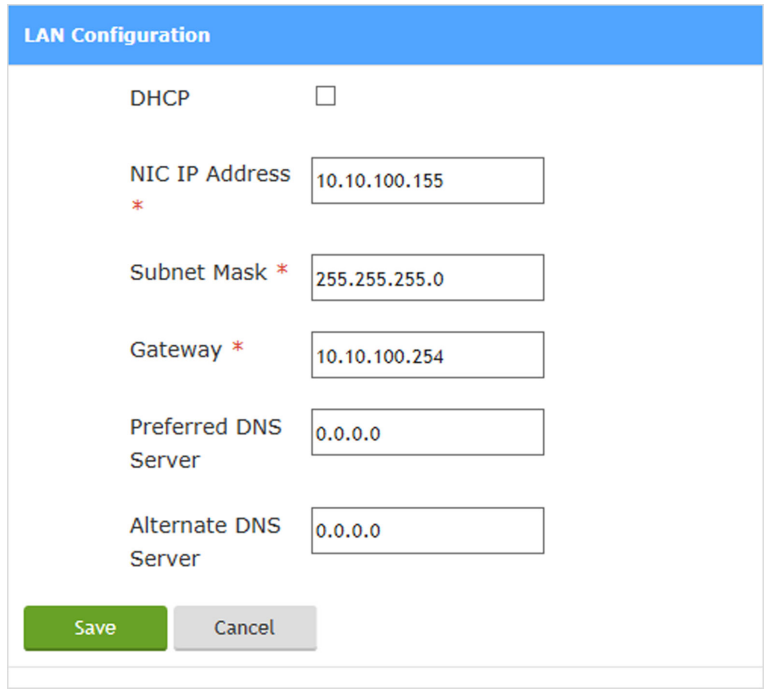

Figure 3-1 LAN Configuration

- If the network supports distributing the IP address automatically, you can check **DHCP** to get **NIC IP Address**, **Subnet Mask**, **Gateway**, etc. automatically. Click **Save** and then click **OK**.
- Enter corresponding parameters manually, and click **Save** and then click **OK**.

3. **Optional:** Go to **Network → Local → Configuration → Basic** to view the basic network information.

3.2 Add IP Camera

Add cameras to the device to facilitate the management and data analysis.

Steps

1. Click **Resources**.
2. Add an IP camera.

Add quickly

a. Click **Add Quickly** to automatically get online cameras in a LAN.
b. Check cameras that need to be added.

Note

The user names should be the same for the cameras added in batch. So do the passwords.

c. Enter **User Name** and **Password**.
d. Click **Add**.

Import in batch

a. Click **Import**.
b. Click **Export Template**, and click **OK** to save the template in the computer.
c. Edit camera information in the template.

Note

You have to edit all the parameters except No. and parent No.

d. Click **Browse** and select the completed template.
e. Click **OK**.

Add one by one

a. Click **Add**.
b. Select **Protocol Type**.
c. Enter **Device Name**, **IP Address**, **Protocol Port**, etc.
d. Click **Save** or **Save and Set**.

Note

- Click **Save** to add the camera to the device.
- Click **Save and Set** to add the device and jump to the parameters settings interface to set the camera parameters.

3. **Optional:** You can also do the following operations.

Modify Check the added camera and click **Modify** to modify the added camera information.

Delete Check the added camera and click **Delete** to delete the added camera.

Export Click **Export** to export the camera list.

Chapter 4 Event Detection

4.1 Set Preset Scene

The position information such as scenes, focal length, focus, etc. can be saved in the preset scene to let the PTZ return to a certain scene quickly, convenient for the event detection in different scenes.

Steps

Note

Only the speed dome supports preset scene configuration.

1. Go to **Parameters → Scene Configuration** .

   Note

   After entering the interface, the PTZ is locked automatically. During the locked period, only the current operator can control the PTZ to prevent the other PTZ movement from interfering the configuration. After the auto lock is released, you can click **Lock** to lock it again.

2. Select the speed dome channel and **Scene**.
3. Click **Preset Scene**.
4. Click the direction buttons and lens control buttons to adjust the live view image to the needed scene.

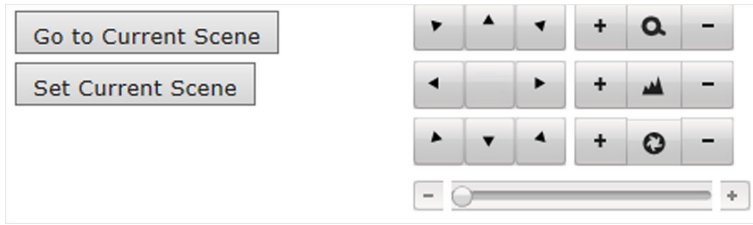

Figure 4-1 PTZ Control

5. Click **Set Current Scene** to set the current scene as the preset scene.
6. **Optional:** Repeat the steps above to set more preset scenes.

   Note

   When the device lens deviates from the preset scene, you can click **Go to Current Scene** to return to the preset scene quickly.

4.2 Set Camera Location Parameters

When you need to capture pictures, set the camera location parameters.

Steps

1. Go to **Parameters → Camera Location** .

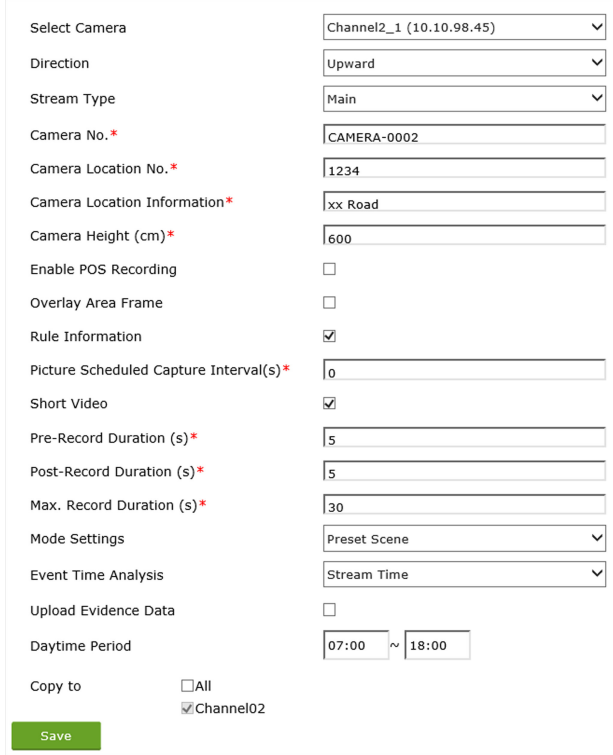

Figure 4-2 Set Camera Location Parameters

2. Select the camera to set.
3. Set the camera location parameters according to the actual conditions.

Direction

It refers to the driving direction of the vehicle, depending on which the installation direction of the device lens can be inferred. **Upward** represents the direction in which the vehicle is driving away from the lens. **Downward** represents the direction in which the vehicle is driving towards the lens.

Note

For the speed dome, go to **Parameters → Scene Configuration → Preset Scene** to select the direction.

Stream Type

Select the main stream to get the high-quality image when the network condition is good, and select the sub-stream to get the fluent image when the network condition is not good enough.

Scene Reset Delay

It refers to the time since the device deviates from the preset scene till the device returns to the preset scene to continue the event detection. After the device deviates from the preset scene, event detection will stop.

Note

Scene reset delay is only applicable to the speed dome.

Enable POS Recording

Check it to enable POS recording for convenient video collection for the event detection analysis.

Overlay Area Frame

Check it to overlay the area or lane where the corresponding event occurred on the captured picture.

Rule Information

Check it, and the target vehicle and pedestrian will be marked by frames on the live view image.

Picture Scheduled Capture Interval

Pictures will be captured every set interval.

Short Video

Check it to record the event enforcement process.

Pre-Record Duration

The record duration before the short video starts.

Post-Record Duration

The record duration after the short video ends.

Max. Record Duration

The max. length of the short video.

Mode Settings

Select **Preset Scene** to set the area and lane manually or select **Scene Auto-Switch** to automatically set the area and lane.

4. **Optional:** Check the other channel(s) to copy the settings.
5. Click **Save**.

4.3 Set Scene

Set the scene capture parameters.

Before You Start

If the channel is a speed dome, set the preset scene first.

Steps

1. Go to **Parameters → Scene Configuration** .
2. Select the channel and scene.

   Note

   Scene is only available for the speed dome.

3. Set the scene name.
   1) Click **Event Rule**.
   2) Select **Scene Mode** according to actual needs.
   3) Enter **Scene Name**.
   4) Click **Save**.
4. **Optional:** For the speed dome channel, set the basic scene parameters.
   1) Click **Preset Scene**.
   2) Check **Enable This Scene**.
   3) Select the direction according to the actual driving direction.
   4) **Optional:** Check the copying mode and the channel(s) to copy the configuration.

      All

      Check it to copy the parameters of **Event Rule**, **Preset Scene**, and **Draw Area**.

      Copy Event Rule Parameters

      Check it to copy the parameters of **Event Rule** and **Preset Scene**.
   5) Click **Save**.

4.4 Set Violation Event

The device supports multiple violation events detection. After the event rule configuration, the device will detect and capture the events according to the set rules automatically.

Before You Start

Set the scene first.

Steps

1. Go to **Parameters → Scene Configuration** .
2. Select the channel and scene.

   Note

   Scene is only available for the speed dome.

3. Click **Event Rule**.
4. Select **Scene Mode**.
5. Enter **Scene Name**.
6. **Optional:** Check **Longitude and Latitude Calibration**, and enter the longitudes and latitudes of the four calibration area vertexes to calibrate the coordinates.

Note

The longitudes and latitudes information can only be uploaded via the SDK protocol. Relevant parameters need to be set through the path **System → Settings → Basic Configuration** before uploading.

7. Check the event(s) to be detected.

Note

- The supported events vary with different scene modes. The actual device prevails.
- **Congestion** and **Congestion (Area)** cannot be enabled at the same time. Select **Congestion** when you need to detect the congestion event of the whole road. Select **Congestion (Area)** when you need to detect the congestion event of an area.

8. Set the event parameters.

Note

The supported parameters vary with different models. The actual device prevails.

Long Range Target Frame

When the vehicle with violation event is far away from the lens, the target frame will appear on the live view image to mark the vehicle position.

Duration

When the vehicle stays at the detection area or lane line for a time period longer than the set duration, the vehicle will be judged as a vehicle with violation event.

Filtering Time

The violation capture during the set filtering time will be judged as the violation capture of the same target. In this case, only one captured picture will be uploaded.

Linked Congestion Threshold

When the vehicle density in the detection area or lane line exceeds the set threshold, no picture will be captured or uploaded.

Sensitivity

The higher the sensitivity is, the more possible it is for the detection target to be recognized as the vehicle with violation events. If the value is too high, detection mistakes may occur. If the value is too low, detection loopholes may occur. Therefore, it's recommended that the value should be set reasonably according to the actual conditions.

Capturing Target

Select the capturing target type according to actual needs.

Congestion Upper/Lower Limit

It is used to evaluate the traffic flow congestion status. If the vehicle density is higher than the set upper limit, the traffic flow status is congestion. If the vehicle density falls between

the set lower limit and the set upper limit, the traffic flow status is slow running. If the vehicle density is lower than the set lower limit, the traffic flow status is fluent running.

Traffic Jam Length

When the low-speed vehicle density exceeds the set value, the current traffic condition is considered as congestion.

Duplicate Alarm Before Cancelling Congestion

Check it to enable repeated alarm data reporting until the vehicle evacuation is achieved.

Statistics Time

The camera data statistics and uploading will be done every the set time.

Flow Margin

It refers to the distance from the flow trigger line 1 to flow trigger line 2, which is used to calculate the average speed.

Alarm in Construction

Check it to enable traffic accident or vehicle failure alarm in construction events.

9. **Optional:** If the channel is a speed dome, and the illegal parking event has been enabled, you can set the illegal parking evidence capture of the current scene.
   1) Click **Preset Scene**.
   2) Check **Capture No Plate Vehicle** when you need to capture the vehicles without license plates.

   Note

   The function is only available for the captured close view pictures. When you set all the captured pictures as distant view ones, no matter you check it or not, the vehicles without license plates will be detected.

   3) Set the parameters below.

   Number of Captured Picture

   The number of the captured pictures for illegal parking detection.

   Single Picture Capture Timeout

   It refers to the max. time of one picture capture. If the time exceeds the value, one picture of the current scene will be captured as the evidence picture.

   Plate Matching Ratio

   When the plate matching ratio of vehicles exceeds the set value, the vehicles with the license plates will be judged as the same one, and the violation of the vehicle will only be captured once.

   4) Click **Picture Detailed Configuration** to set the capture interval and picture type.

   Capture Interval

   The time interval between two captured pictures.

   Picture Type

In order to guarantee the license plate recognition result, set at least one close view picture.

5) Click **Save**.

When the illegal parking is detected, the device will capture pictures according to the set picture No. and interval.

10. Check **Area Linkage** or **Lane Linkage**.
11. Draw the rule areas or lane lines according to the actual needs.

Operation	Reference
Draw lane lines	***Draw Lane Line***
Draw flow triggering lines	***Draw Flow Triggering Line***
Draw rule area	***Draw Rule Area***
Draw shielded area	***Draw Shielded Area***
Draw calibration area	***Draw Longitude and Latitude Calibration Area***

12. **Optional:** Check the copying mode and the channel(s) to copy the event rule configuration.

All

Check it to copy the parameters of **Event Rule**, **Preset Scene**, and **Draw Area**.

Copy Event Rule Parameters

Check it to copy the parameters of **Event Rule** and **Preset Scene**.

13. Click **Save**.

4.5 Set Evidence Code

Evidence codes define various violation types. Through setting evidence codes, different captured evidences can be easily managed.

Steps

1. Go to **System → Settings → Evidence Code** .
2. Select the captured evidence(s) according to your needs or edit the captured evidence and the corresponding evidence code after clicking the captured evidence.
3. **Optional:** Click **Reset** to restore to defaults.

4.6 Set Picture Composition

You can composite the captured multiple pictures to one picture to upload and store.

Steps

1. Go to **Parameters → Picture Composition** .

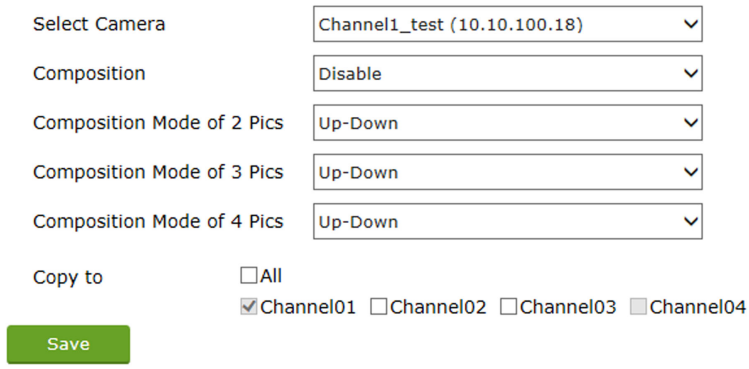

Figure 4-3 Set Picture Composition

2. Select the channel.
3. Enable picture composition.
4. Select the composition mode of two/three/four pictures.
5. **Optional:** Check the channel(s) to set the same settings.
6. Click **Save**.

4.7 Set Text Overlay

You can overlay the information such as the intersection, lane No., license plate number, etc. on the captured pictures.

Steps

1. Go to **Parameters → Text Overlay** .

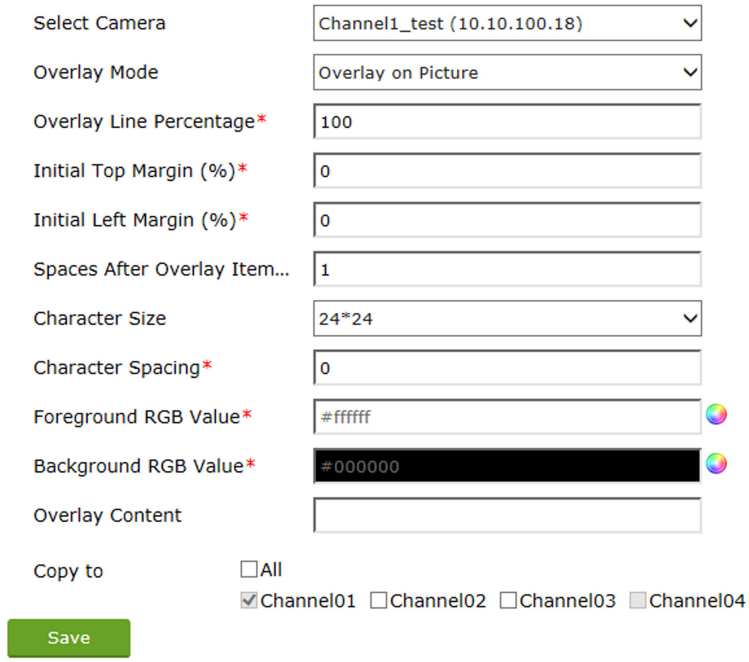

Figure 4-4 Set Text Overlay

2. Select the channel.
3. Set the text overlay parameters.

Overlay Mode

Overlay on Picture

The text will be overlaid within the picture.

Overlay Above Picture

The text will be overlaid on the top of the picture outside.

Overlay Below Picture

The text will be overlaid on the bottom of the picture outside.

Overlay Line Percentage

It is the percentage that the overlaid information occupies on the picture. For example, if you set the percentage to 50, the overlaid information in a row will occupy up to half of the image width, and the excess content will be overlaid from a new line.

Initial Top Margin

Set the top coordinate from which the text begins to overlay.

Initial Left Margin

Set the left coordinate from which the text begins to overlay.

Spaces After Overlay Items

Set the number of space after between two overlaid items. For example, if you set it as 1, the adjacent overlaid items will be separated with one space.

Character Spacing

Set the distance between characters.

Overlay Content

Click the text filed to check the overlaid information, and click **Save**.

Note

If the overlaid information exceeds the overlay area, the excess content will not be displayed.

4. **Optional:** Check the channel(s) to set the same settings.
5. Click **Save**.

4.8 Set Event Record

The device supports event recording function when detecting relevant events.

Steps

1. Go to **Parameters → Camera Location** .
2. Check **Short Video**.
3. Set recording parameters according to actual needs.

Pre-Record Duration

The record duration before the short video starts.

Post-Record Duration

The record duration after the short video ends.

Max. Record Duration

The max. length of the short video.

4. Click **Save**.

4.9 Set Scene Patrol

You can set the scene patrol schedule to make the device monitor the preset scene in patrol during the set period.

Before You Start

Only the speed dome supports scene patrol. Ensure at least two preset scenes have been set.

Steps

1. Go to **Parameters → Scene Patrol** .

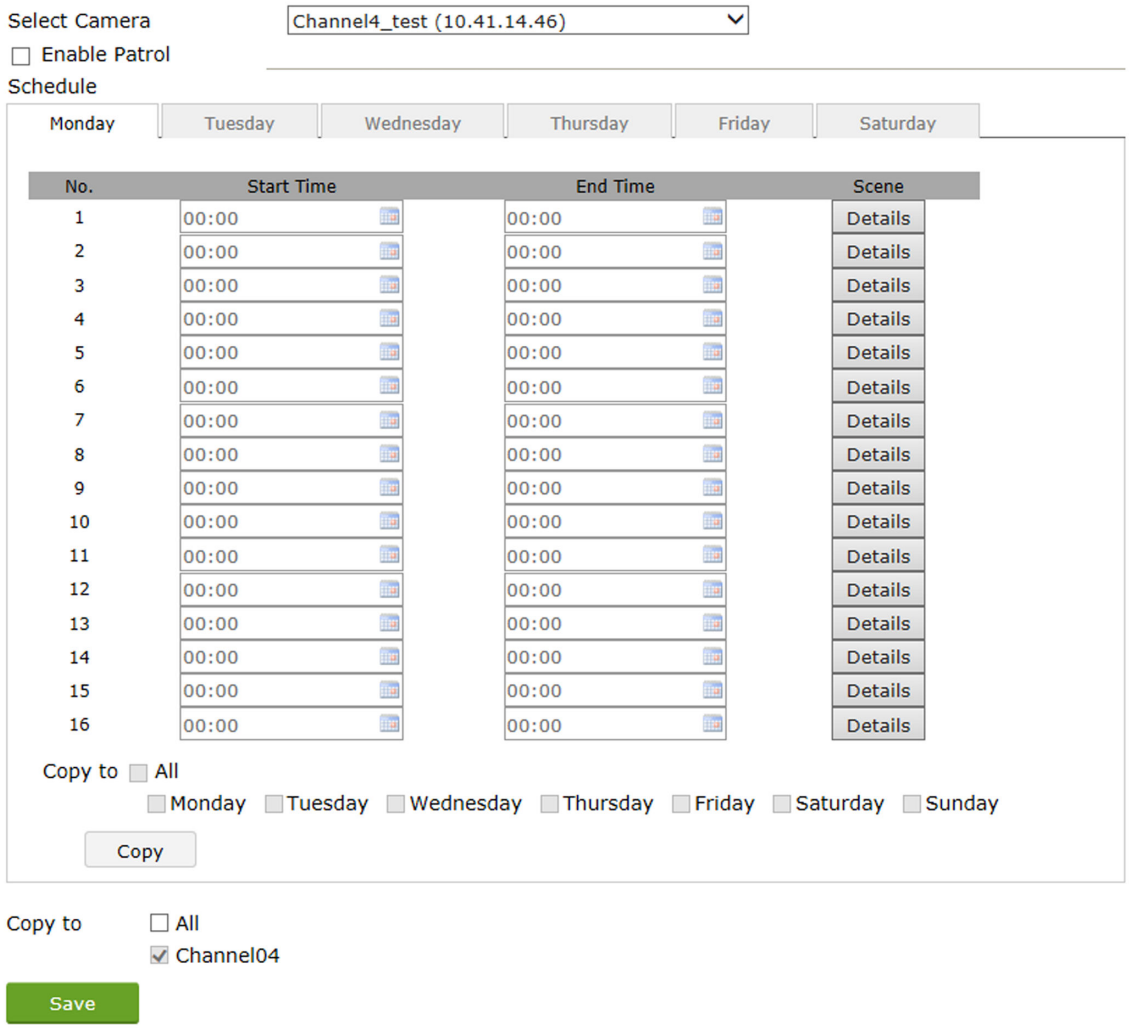

Figure 4-5 Set Scene Patrol

2. Select the channel.
3. Check **Enable Patrol Schedule**.
4. Select the day to set the schedule.
5. Set the start and end time of the period.
6. Set the scene patrol.
   1) Click **Details**.
   2) Click **Add New Rule** to add the scene.
   3) Select **Scene** and set **Dwell Time**.
   4) **Optional:** Click ↑ ↓ to adjust the scene sequence.
   5) Click **OK**.
7. **Optional:** Check the channel(s) to set the same settings.
8. Click **Save**.

4.10 Draw Line and Area

Steps

1. Go to **Parameters → Scene Configuration** .
2. Select the channel and scene.

Note

Scene is only available for the speed dome.

3. Click **Event Rule**.
4. Click **Draw Area**.

Figure 4-6 Draw Line and Area

4.10.1 Draw Lane Line

You need to set lane lines for event detection. Draw two lane lines for each real lane, and up to six lanes can be set for each scene.

Steps

1. Go to **Draw Area → Draw Lane Line** .
2. Select **Number of Lane**.
3. Click **Left Line** and **Right Line**, and click the left button of the mouse to locate the two ends of the line to draw the lane line according to the actual lane location.

Note

The adjacent lane areas cannot be overlapped.

4. **Optional:** Click **Clear** to clear all the lane lines.

5. Set the lane parameters such as **Lane Type**, **Lane Direction**, etc.
6. Click **OK**.

4.10.2 Draw Flow Triggering Line

Draw flow triggering lines for the congestion or traffic flow detection.

Steps

1. Go to **Draw Area → Draw Triggering Line** .
2. Select the flow triggering line to draw.
3. Click the left button of the mouse to locate the two ends of the line to draw the triggering line at the location needing to detect the traffic flow.

   Note

   The flow triggering line must be crossed with the lane line.
4. **Optional:** Click **Clear** to clear all the triggering lines.
5. Click **OK**.

4.10.3 Draw Rule Area

Draw the rule areas to detect the events in the areas.

Steps

1. Go to **Draw Area → Draw Area** .
2. Select the area to draw.
3. Click **Draw Area**.
4. Click the left button of the mouse to draw a rectangular or polygonal frame, and then click the right button of the mouse to save the area.

   Note

   The areas of different events can be overlapped.
5. **Optional:** Click **Delete Area** to delete the current area.
6. Click **OK**.

4.10.4 Draw Shielded Area

The shielded area is an area in which the events will not be detected. Interference can be greatly reduced when the shielded area is drawn.

Steps

1. Go to **Draw Area → Draw Shielded Area** .
2. Select the shielded area to draw.

3. Click **Draw Shielded Area**.
4. Click the left button of the mouse to draw a rectangular or polygonal frame, and then click the right button of the mouse to save the area.

Note

The shielded areas can be overlapped.

5. **Optional:** Click **Delete Area** to delete the current area.
6. Click **OK**.

4.10.5 Draw Longitude and Latitude Calibration Area

Draw the longitude and latitude calibration area to calibrate the coordinates of the area vertexes.

Before You Start

Enable **Longitude and Latitude Calibration** in event rule settings.

Steps

1. Go to **Draw Area → Draw Longitude and Latitude Calibration Area** .
2. Click **Draw Longitude and Latitude Calibration Area**.
3. Click the left button of the mouse to draw a rectangular frame, and then click the right button of the mouse to save the area.
4. **Optional:** Click **Delete Area** to delete the current area.
5. Click **OK**.

Chapter 5 Data Management

5.1 Search Data

You can search and export the event detection and violation capture data of the connected cameras, or the traffic parameters statistics of the cameras.

Steps

1. Click **Data Search**.
2. Search the event detection and violation capture data.
   1) Click **Data Search**.
   2) Set **Start Time** and **End Time**.
   3) Select **Device ID**, **Data Type**, and **Violation Type**.
   4) Click **Search**.

      The searched result will be listed on the right.
   5) **Optional:** Select the data you want to export, and click **Export** to export the data to your computer.
3. Search the traffic parameters statistics of the cameras.
   1) Click **Parameters Statistics**.
   2) Set **Start Time** and **End Time**.
   3) Select **Device ID**.
   4) **Optional:** Set **Lane No.**
   5) Click **Search**.

      The searched result will be listed on the right.
   6) **Optional:** Select the data you want to export, and click **Export** to export the data to your computer.

5.2 Set Upload Data Type

The device supports setting upload data type to meet various data uploading needs.

Steps

1. Go to **System → Settings → Upload Arming Data Type** .
2. Click the input box behind **Upload Data Type** to check the data type(s) to be uploaded.
3. Click **Save**.

5.3 Back up Data

The device supports backing up data to your computer.

Before You Start

The data search has been made.

Steps

1. Set the rules for exporting pictures and videos.
   1) Go to **System → Settings → Web Backup** .
   2) Enter the naming rules and saving paths of the pictures and videos.
   3) Click **Save**.
2. Add the IP address of this device as the trusted site in the safety settings of your browser.
3. Refer to ***Search Data*** to search data.
4. Click **Export** to select the file type(s).
5. Click **OK**.

Result

The pictures and videos will be backed up according to the set naming rules in the set saving paths.

Chapter 6 Storage

6.1 Set Storage Path

6.1.1 Format Disk

Format the disk when the storage is abnormal or a new disk is installed.

Steps

Caution

Formatting the disk will cause the disk data loss. Back up the data first.

1. Go to **System → Settings → Format Disk** .
2. Click **Format Disk**.
3. Click **OK** on the popup window.

6.1.2 Set FTP

Set FTP parameters if you want to upload the captured pictures or videos to the FTP server.

Before You Start

Set the FTP server, and ensure the device can communicate normally with the server.

Steps

1. Go to **System → FTP Upload** .

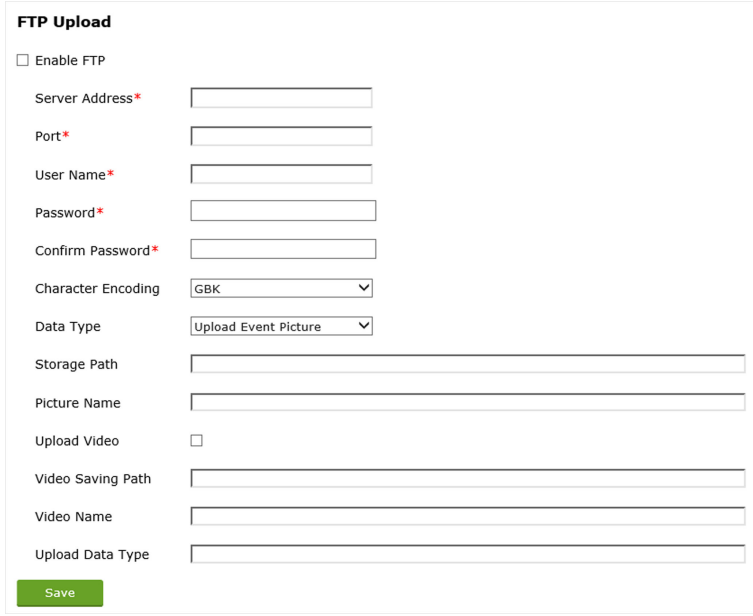

Figure 6-1 Set FTP

2. Check **Enable FTP**.
3. Enter **Sever Address**, **Port**, **User Name**, **Password**, and confirm the password.
4. Set the character encoding format.
5. Select **Data Type**.

Note

Some types of devices support uploading one data type only. The actual interface prevails.

6. Set **Storage Path** and **Picture Name**.
7. **Optional:** Upload the event enforcement videos to the FTP server.
   1) Check **Upload Video**.
   2) Set **Video Saving Path**, **Video Name**, and **Upload Data Type**.
8. Click **Save**.

6.1.3 Set SDK Listening

The SDK listening can be used to receive the arming alarm information uploaded by the device.

Before You Start

The listening service has been enabled for the listening host, and the network communication between the listening host and the device is normal.

Steps

1. Go to **System → Settings → Basic Configuration → NIC Parameters** .

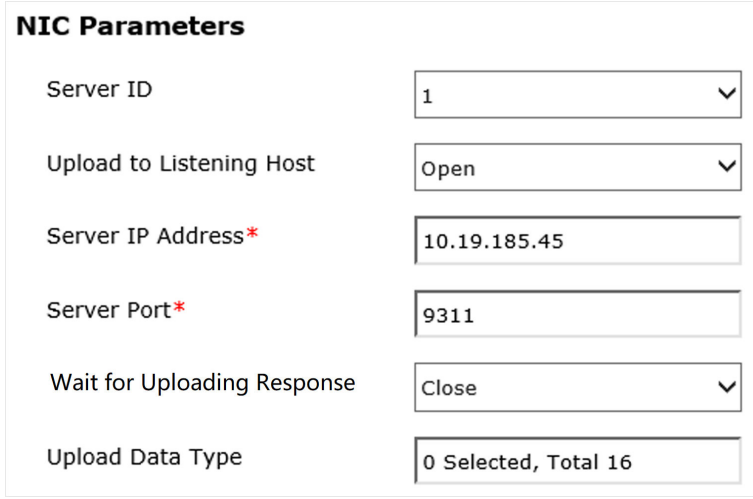

Figure 6-2 Set Listening Host

2. Select **Server ID**.
3. Enable **Upload to Listening Host**.
4. Set **Server IP Address** and **Server Port**.
5. **Optional:** Enable **Wait for Uploading Response**.

Note

- This function is for professionals use only.
- This function is only available when the platform that receives the data supports uploading response.

The platform will send a response to the device after receiving the uploaded data from the device. If the device does not receive the response from the platform, it means that uploading failed.

6. Click the input box behind **Upload Data Type** to check the data type(s) to be uploaded.
7. Click **Save**.

6.1.4 Set Cloud Storage

Cloud storage is a kind of network storage. It can be used as the extended storage to save the captured pictures.

Before You Start

Arrange the cloud storage server.

Steps

1. Go to **System → Basic Configuration → Cloud Storage** .
2. Check **Cloud Storage**.
3. Set the server parameters.

1) Enter Server IP Address, Port No., and other parameters.
2) Enter **accessKey** and **secretKey**.

4. Click **Save**.

6.2 Set Capture Interval

Set capture interval to enable picture capturing at a set time interval.

Steps

1. Go to **Parameters → Camera Location** .
2. Set **Picture Scheduled Capture Interval** according to the actual needs.
3. Click **Save**.

Chapter 7 Network

7.1 Set Remote Host

Set remote host when the device needs to transmit data to the central control platform.

Before You Start

Set the remote host, and ensure the device can communicate normally with the remote host.

Steps

1. Go to **System → Settings → Remote Host** .
2. Select **Upload Protocol**.

   HTTP

   The device communicates with the remote host via HTTP.
3. Enable **Upload**.
4. Set **URL**, **Address Type**, **IP Address**, and **Port** of the remote host.
5. Select **Data Type**.
6. Click the input box behind **Upload Data Type** to select the data type(s) to be uploaded.
7. Click **Save**.

7.2 Set Port

The device port can be modified when the device cannot access the network due to port conflicts.

Steps

1. Go to **System → Settings → Basic Configuration → Port** .
2. Set **SDK Port** according to the actual needs.
3. Click **Save**.

Chapter 8 Live View and Manual Evidence Capture

8.1 Live View

Click **Live View**, and double click the channel in the channel list to start live view.

8.2 Set Manual Evidence Capture Parameters

For the speed dome, you can set the manual evidence capture parameters. Then when you capture the evidence pictures on the live view interface, the device will capture pictures according to the set rules.

Steps

1. Go to **Parameters → Manual Evidence Capture** .

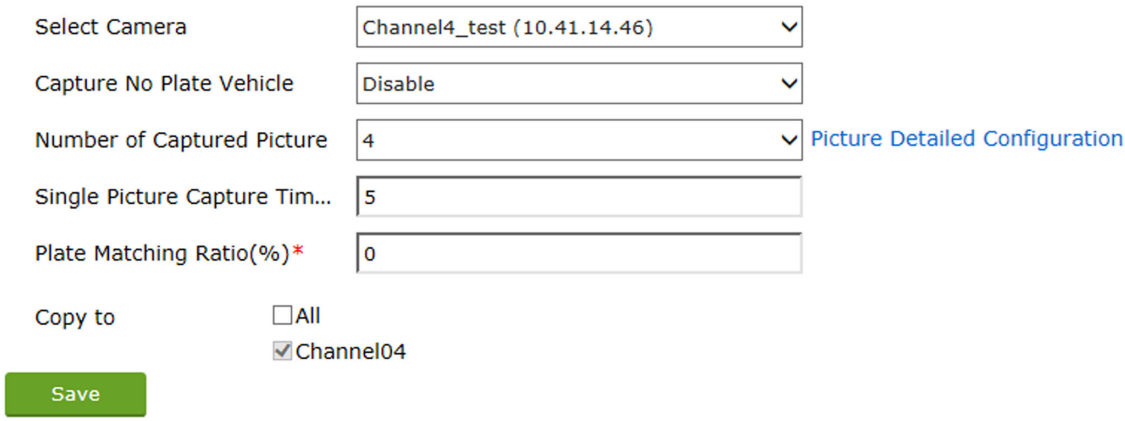

Figure 8-1 Set Manual Evidence Capture Parameters

2. Select the channel.
3. Set the parameters below.

Capture No Plate Vehicle

If you enable the function, the vehicles without license plates will be captured.

Number of Captured Picture

The number of the captured pictures when you click on the live view interface.

Single Picture Capture Timeout

When the capture and uploading time of one picture exceeds the set time, a new picture will be captured and uploaded.

Plate Matching Ratio

When the plate matching ratio exceeds the set value, the vehicles with the license plates will be judged as the same one, and the events of the vehicle will only be captured once.

4. Click **Picture Detailed Configuration** to set the capture interval and picture type.

   Capture Interval

   The time interval between two captured pictures.

   Picture Type

   In order to guarantee the license plate recognition result, set at least one close-up picture.
5. **Optional:** Check the channel(s) to set the same settings.
6. Click **Save**.

8.3 Capture Picture

Note

Only the speed dome supports manual capture.

Click **Live View**. Click , and the device will capture pictures.

Chapter 9 Safety Management

9.1 Manage User

The administrator can add, modify, or delete other accounts, and grant different permissions to different user levels.

Before You Start
Set the administrator password when you first use the device to ensure a normal working.

Steps
1. Go to **System → Settings → User Configuration** .
2. Add a user.
   1) Click **Add**.
   2) Enter **User Name**, **Password**, and confirm the password.

   Caution

   To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

   3) Click **Save**.
3. **Optional:** Click the user name of the added user to edit the user information.
4. **Optional:** Select a user and click **Delete** to delete the user.

9.2 Set SSH

To improve network security, it is recommended to disable the SSH service. The service is especially saved for the professionals to debug the device.

Steps
1. Go to **System → Settings → Security Service** .
2. Check **Enable SSH**.
3. Set **SSH Port**.
4. Click **Save**.

Chapter 10 Maintenance

10.1 Synchronize Time

Synchronize the device time when it is inconsistent with the actual time.

Steps

1. Go to **System → Settings → Time Configuration** .
2. Select the time synchronization mode.
   - If an NTP server is available, select **NTP** and enter NTP server information to synchronize the device time with that of the NTP server.
   - Select **Manual Time Sync.** and set time to customize the device time.
   - Select **Manual Time Sync.** and check **Sync. with computer time** to synchronize the device time with that of the computer.
3. Click **Save**.

Note

The time synchronization modes vary with different models. The actual device prevails.

10.2 Synchronize Camera Time

It is recommended to synchronize the camera time when the camera time is inconsistent with the device time.

Steps

Note

The settings are only applicable to SDK protocol cameras.

1. Go to **System → Settings → Camera Time Sync.**
2. Check **Enable Camera Time Sync.**
3. Set **Interval**.
4. Click **Save**.

Result

The device will synchronize the camera time at the set interval to ensure its time is consistent with the device time.

10.3 Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

Steps

1. Go to **System → Settings → DST** .
2. Check **Enable DST**.
3. Set **Start Time**, **End Time**, and **Bias Time**.
4. Click **Save**.

10.4 View Device Information

View Device Basic Information

Go to **System → Version** to view device versions and plugin information.

View Device Performance

Go to **Network → Local → Performance** to view **CPU Usage Rate**, **Network IO**, and **Temperature**.

View System Status

Go to **System → Settings → System Status** to view system statuses.

10.5 Search Log

The device supports viewing and exporting alarm logs and operation logs.

Steps

1. Go to **System → Log** .
2. Select a log type.
3. Set **Start Time** and **End Time**.
4. Click **Search**.
5. **Optional:** Export logs.
   1) Click **Export**.
   2) Click **OK** on the popup window.
   3) Open the log file directly or select a saving path, set the file name, and save it.

10.6 Reboot

When the device needs to be rebooted, reboot it via the software instead of cutting off the power directly.

Steps

1. Go to **System → Settings → Maintenance → Reboot** .
2. Click **Reboot**.
3. Click **OK** to reboot the device.

10.7 Upgrade

Upgrade the system when you need to update the device version.

Before You Start

Prepare the upgrade file.

Steps

1. Go to **System → Settings → Maintenance → Upgrade** .
2. Click **Browse** to select the upgrade file.
3. Click **OK** on the popup window.

Note

The upgrade process will take 1 to 10 minutes. Do not cut off the power supply.

Result

The device will upgrade and reboot automatically.

10.8 Restore Parameters

When the device is abnormal caused by the incorrect set parameters, you can restore the parameters.

Steps

1. Go to **System → Settings → Maintenance → Restore Parameters** .
2. Select the restoration mode.
   - Click **Default** to restore the parameters except the IP address, subnet mask, gateway, port, etc. to the default settings.
   - Click **Factory** to restore all the parameters to the factory settings.
3. Click **OK**.

10.9 Export Parameters

You can export the parameters of one device, and import them to another device to set the two devices with the same parameters.

Steps

1. Go to **System → Settings → Maintenance → Export Parameters** .

2. Click **Export**.
3. Select the saving path.
4. Click **Save**.

10.10 Import Parameters

Import the configuration file of another device to the current device to set the same parameters.

Before You Start
Save the configuration file to the computer.

Steps

Caution
Importing configuration file is only available to the devices of the same model and same version.

1. Go to **System → Settings → Maintenance → Import Parameters** .
2. Click **Browse** to select the configuration file.
3. Click **Import**.
4. Click **OK** on the popup window.

Result

The parameters will be imported, and the device will reboot.

10.11 Set Reserved Parameters

Go to **System → Settings → Custom Interface** . This function is for professional personnel debugging only.

10.12 Set UID Indicator

Click **Network** and enable **UID Indicator** according to the actual needs to locate the server quickly.

10.13 Export Debug Log

The device supports exporting debug log to your computer.

Steps
1. Go to **System → Settings → Maintenance → Export** .
2. Click **Export Log**.
3. Click **OK**.

Result

The debug log will be exported to your computer.

Appendix A. Communication Matrix and Device Command

Scan the QR code below to get the communication matrix of the device.

Figure A-1 Communication Matrix

Scan the QR code below to get the device command.

Figure A-2 Device Command


See Far, Go Further