HIKVISION

Roadside Parking Terminal

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.
ℹ **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.
- DO NOT touch the bare metal contacts of the inlets after the circuit breaker is turned off. Electricity still exists.
- Ensure correct wiring of the terminals for connection to an AC mains supply.
- An overcurrent protective device confirming to the power supply specification shall be incorporated external to the equipment, not exceeding the specification of the building. Refer to the specification for the detailed power supply requirement.

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.
- The device can only be safely used in the region below 2,000 meters above the sea level.
- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains, etc. The openings shall never be blocked by placing the equipment on a bed, sofa, rug or other similar surface.
- This equipment is suitable for mounting on concrete or other non-combustible surface only.
- Keep body parts away from motors. Disconnect the power source during servicing.

Light Hazard

- DO NOT stare at the light source when the supplement light is working. The light may cause blue light hazard to your retina.
- When you install or maintain the device without protection, stay at the safety range or the area which cannot be irradiated directly by the light source.

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.

Lens

- DO NOT touch the lens with fingers directly in case the acidic sweat of the fingers erodes the surface coating of the lens.
- DO NOT aim the lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the device.

Screen

- Clean the screen with soft and dry cloth or other substitutes to wipe the interior and exterior surface. DO NOT use alkaline detergents. Protect the screen from scratches.
- DO NOT install the device in the position obstructing the driver's sight to prevent it from affecting the normal driving of the vehicle.

Battery

- DO NOT charge the battery continuously more than one week. Overcharging may shorten the battery life.
- Battery will discharge gradually if it is not used for a long time. It must be recharged before using.
- If the device contains dismountable battery, store the device and battery separately if it is not used.
- The battery must be charged and discharged every three months if it is not used, and recharged to 60% to 70% power percentage to store.
- The scrapped battery should be discarded in compliance with the local laws and regulations. If there are no corresponding laws or regulations, throw it in a hazardous trash can.
- DO NOT pierce the battery or shorten the electrodes, or it may cause explosion or fire hazard.
- DO NOT dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- CAUTION: Please use the specific battery supported by the device, or it may cause explosion. If the battery is damaged and needs to be changed, contact the device manufacturer or local distributor.
- If the device contains button battery, keep it far away from children.
- DO NOT expose the battery pack or battery combination to sunlight, fire, or similar overheated environment. DO NOT leave the battery in an extremely high temperature surrounding environment or subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.

- Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children.
- 🔋 identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current.
  - identifies the negative terminal(s) of equipment which is used with, or generates direct current.

Data

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

Laser

⚠ LASER 2 🚫 : The laser radiation emitted from the device can cause eye injuries, burning of skin, or inflammable substances. Before enabling the laser, make sure no human or inflammable substances are in front.

Contents

Chapter 1 Introduction

1.1 Product Introduction

The roadside parking terminal is used to manage roadside parking spaces and other devices. It can be matched with the cloud platform to manage the parking of a city. It also can be matched with a roadside parking capture camera and an intelligent all-in-one parking machine to collect, store and search parking data.

The device can be widely applied in the management of urban roadside parking spaces.

1.2 Key Feature

- Supports to connect a roadside parking capture camera and all-in-one machine to save and manage roadside parking data.
- Supports to connect to cameras to save and manage videos and images.
- Supports multiple network interfaces, and can connect to multiple cameras.
- Supports cabinet alarm and alarm data uploading.
- Supports Web operations.
- Single-sided interface, convenient for construction and installation.

1.3 Running Environment

- Web browser: IE8, IE9, IE10 and IE11 recommended.
- Display 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

Device default information are as follows.

- Default IP address: G1: 192.1.0.64, G2: 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 devices over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website (***https://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.

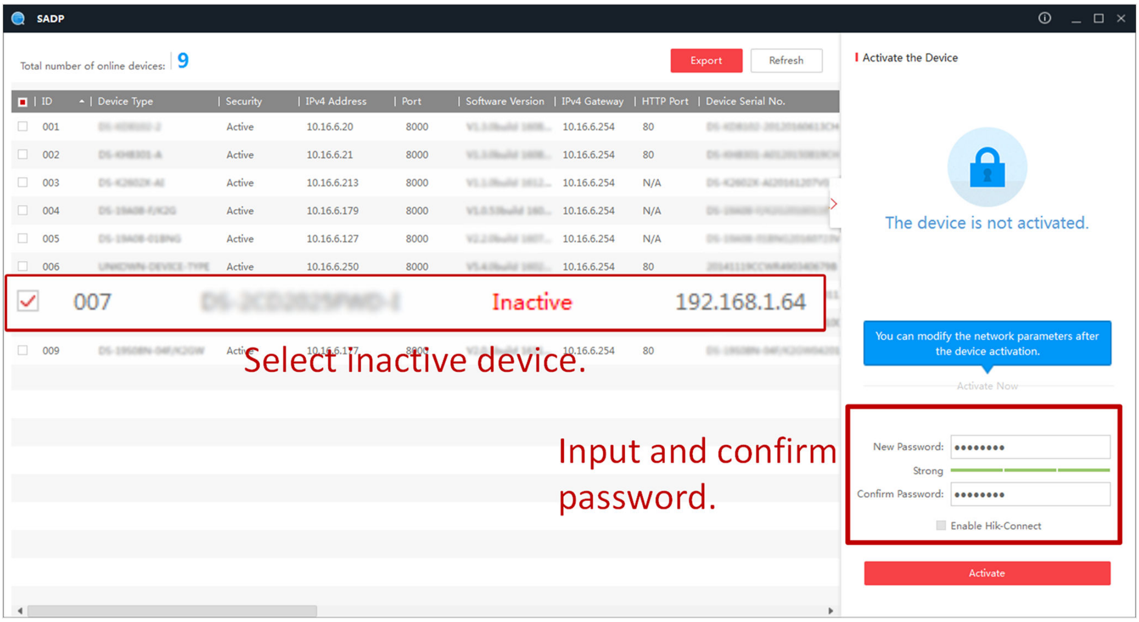
The following steps show how to activate one device and modify its IP address. For batch activation and IP address modification, refer to *User Manual of SADP* for details.

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.



Total number of online devices: 9

☐	ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
☐	001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
☐	002	DS-KH8301-A	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
☐	003	DS-K2602X-AI	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐	004	DS-19A08-F/K2G	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐	005	DS-19A08-01BNG	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐	006	UNKOWN-DEVICE-TYPE	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑	007	[illegible]	Inactive	192.168.1.64					
☐	009	DS-19508N-04F/K2GW	Active	10.16.6.177	8000	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Input and confirm password.

You can modify the network parameters after the device activation.

New Password: ••••••••

Strong

Confirm Password: ••••••••

☐ Enable Hik-Connect

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**.
   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 connect to the same LAN.

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

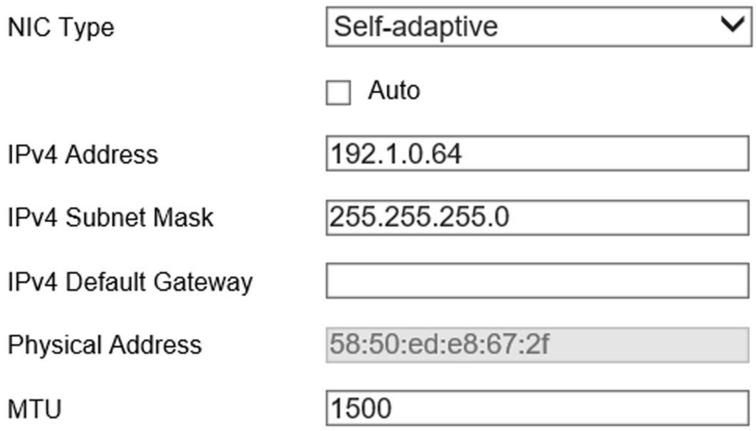
3.1 Set LAN IP Address

3.1.1 Set Internal IP

The internal network is for self-adaptive network interfaces on the device panel. It is mainly used to connect the capture camera, display screen and other devices.

Steps

1. Go to **Param Config → Network → Basic Settings → TCP/IP → Internal Network Settings** .
2. Select **NIC Type** according to the actual network.



NIC Type	Self-adaptive
	□ Auto
IPv4 Address	192.1.0.64
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	
Physical Address	58:50:ed:e8:67:2f
MTU	1500

Figure 3-1 Set Internal IP

3. Set network parameters.
   - Check **Auto** to get the IP address automatically if the network supports distributing the IP address automatically.
   - Manually enter IP address, subnet mask, gateway, MTU, and other parameters.

Note

- The internal IP address and the device on the internal network segment (such as the capture camera) should be set to the same network segment, and it must be set to a different network segment from the external IP address.
- **MTU** stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

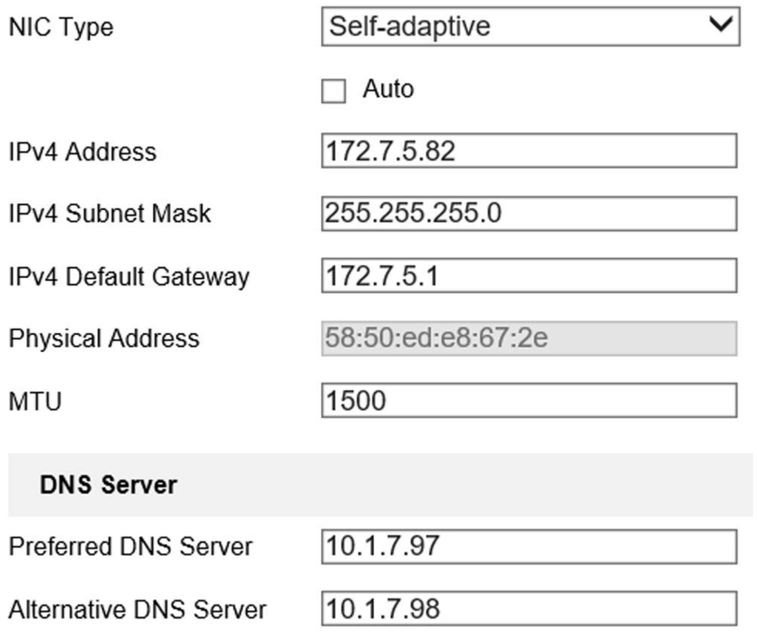
4. Click **Save**.

3.1.2 Set External IP

The external network is set for the IP of the G2 network interface on the device panel, and it mainly communicates with the external network (platform, remote host, etc.).

Steps

1. Go to **Param Config → Network → Basic Settings → TCP/IP → External Network Settings** .



NIC Type	Self-adaptive
	□ Auto
IPv4 Address	172.7.5.82
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	172.7.5.1
Physical Address	58:50:ed:e8:67:2e
MTU	1500
DNS Server	
Preferred DNS Server	10.1.7.97
Alternative DNS Server	10.1.7.98

Figure 3-2 Set External IP

2. Select NIC type according to the actual network.
3. Set network information.
   - Check **Auto** to get the IP address automatically if the network supports distributing the IP address automatically.
   - Manually enter IP address, subnet mask, gateway, and other parameters.

Note

- The network segment of external IP address should be different from that of the internal IP address.
- **MTU** stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.
- Set the DNS server if you need to visit the device with domain access.

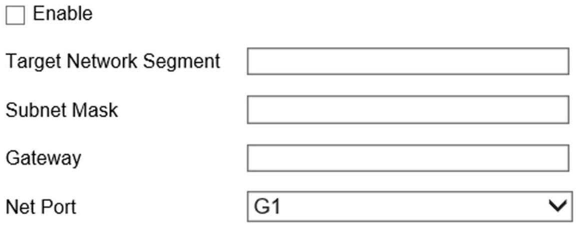
4. Click **Save**.

3.2 Set Static Router

Set a static router to access across network segments. The device will transmit as a router.

Steps

1. Go to **Param Config → Network → Basic Settings → Static Router** .
2. Click **Add** to add a static router.



□ Enable

Target Network Segment

Subnet Mask

Gateway

Net Port G1

Figure 3-3 Set Static Router

3. Check **Enable**.
4. Enter **Target Network Segment**, **Subnet Mask** and **Gateway**.

Note

Set the gateway according to the selected network interface.

5. Select the network interface that needs external communication for routing.
   - When you need other network segments to access the connected camera through the G1, set the G1 as a static router, and the internal IP address will serve as the gateway.
   - When you need to upload data to other network segments through the G2, set the G2 as a static router, and the external IP address will serve as the gateway.
6. Click **OK**.

Note

You can delete or edit the added router.

3.3 Manage Camera

3.3.1 Add IP Camera

Add cameras before managing and analyzing data.

Quick Add

If cameras need to be added via the parameters such as the default protocol and the port, it is recommended to use quick add.

Before You Start
Connect the device to the camera via the network interface.

Steps

1. Go to **Param Config → System → Camera Management → IP Camera** .
2. Click **Quick Add**.
3. Check the camera that need to be added, enter the corresponding user name and password, and click **OK**.

   Note

   You can check cameras that have the same user name and password to add in batch.
4. **Optional:** You can also do the following operations.

Edit	Edit the added camera IP address.
Delete	Delete the added camera.
Reboot	Reboot the online camera.
Access Directly	Access the online camera.

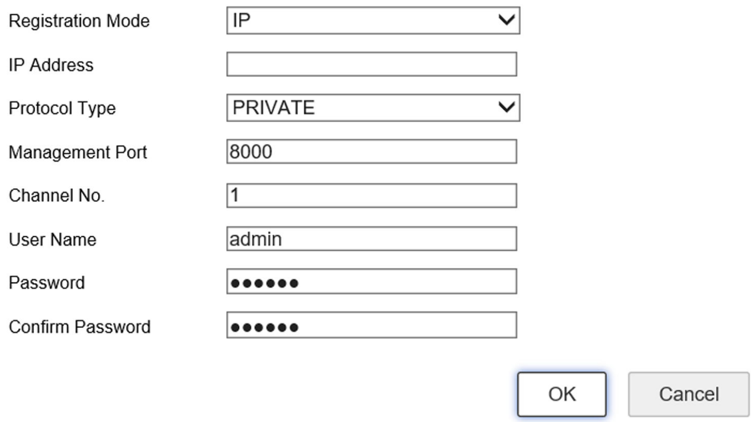
Manual Add

Add manually if you need to customize the access protocol or port.

Before You Start
Connect the device to the camera via the network interface.

Steps

1. Go to **Param Config → System → Camera Management → IP Camera** .
2. Click **Add**.



Registration Mode	IP
IP Address	
Protocol Type	PRIVATE
Management Port	8000
Channel No.	1
User Name	admin
Password	●●●●●●
Confirm Password	●●●●●●

Figure 3-4 Manual Add

3. Select **Registration Mode**.
4. Select **Protocol Type** of the added camera.

Note

The device and the camera should both support the selected protocol type.

5. Enter the camera IP address/domain name, port, user name, password, and other information.

Note

Channel No. is only used to select the access channel when multiple channel devices are accessed. For example, if you want to access the Channel 5 device, you can choose Channel 2 as a network camera to access, then enter 2 at **Channel No.**.

6. Click **OK**.
7. **Optional:** You can also do the following operations.

Edit	Edit the added camera IP address.
Delete	Delete the added camera.
Reboot	Reboot the online camera.
Access Directly	Access the online camera.

3.3.2 Set Interaction Parameters

Set interaction parameters to control the interaction data between the camera and the device.

Before You Start

Add the camera.

Steps

1. Go to **Param Config → System → Camera Management → Interactive Settings** .
2. Select a camera.

3. Select an interaction mode.
   - Normal mode: the server can tell the camera status via the camera's stream, and it can record and live view images and receive image data.
   - Data receiving mode: the server only can receive image data, but it cannot record or live view the camera.
4. **Optional:** You can click **Copy to...** and check channels to copy the set parameters to those selected channels.
5. Click **Save**.

3.4 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 **Param Config → Platform Settings → Remote Host** .
2. Select the remote host.

   Note

   The supported number of remote hosts varies with different devices. The actual interface prevails.
3. Click **Data Upload Config**.
4. Select **Platform Access Mode** according to the actual communication protocol.
   - **Remote Host**: select this mode when communicating via remote host protocol.
   - **Http Host**: select this mode when communicating via HTTP protocol.
5. Set access parameters.
   1) For access via the remote host, please select **Upload Protocol**. For access via Http host, please enter **URL** and select **Address Type**.
   2) Enter host IP address and port.
6. Click **Data Type** to check the upload data type and select specific upload parameters.
7. Enable **Upload History Data**, **Upload No-Plate Data** and **Upload by Time**.

   Interval

   The interval between 2 data uploads.

   Timeout

   When the upload time of a single piece of data exceeds the set time, the data will be automatically saved as history data and uploaded according to history data rule.
8. Click **Data Upload Config** to select the specific time for data to upload.
9. **Optional:** Check **Enable Cloud Storage** to set the address and port of the cloud storage server, and upload the remote host data to the cloud.

Note

Only certain devices in specific protocol support cloud storage settings. The actual interface prevails.

10. Click **Save**.

Chapter 4 Event Detection

4.1 Set Parking Space Information

Set the parking space information if you need to link the parking space to the license plate.

Steps

1. Go to **Param Config → Advanced Settings → List Management → List Management** .
2. Add a list.

Add one by one	a. Click **Add**. b. Enable **Allowlist Arming**. c. Enter **Parking Space No.**, **License Plate Number**, and other basic parameters. d. Click **OK**.
Import in batch	a. Click **Import**. b. Click **Download Import Template** to download according to the prompt. c. Fill all the information in the template. d. Click **Browse** to select the filled template. e. Click **Import**.

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

Export list	Click **Export** to export list to the local.
Delete list	Check the list, and click **Delete** to delete the selected list. Click **Delete All** to clear the existing list information.
Search list	Enter **Parking Space No.**, **License Plate Number** and click **Search** to search the list information.

4.2 Set Occupation Alarm

After linked the parking space with the license plate, set the parking space occupation alarm then it will trigger alarm when the parking space mismatches the vehicle.

Steps

1. Go to **Param Config → Advanced Settings → List Management → Parking Space Occupation Alarm** .
2. Select **Camera**.
3. Enable **Illegal Occupation Alarm**.
4. **Optional:** If you need to upload alarm information to the platform, you can enable **Upload Event to Platform**.
5. Click **Save**.

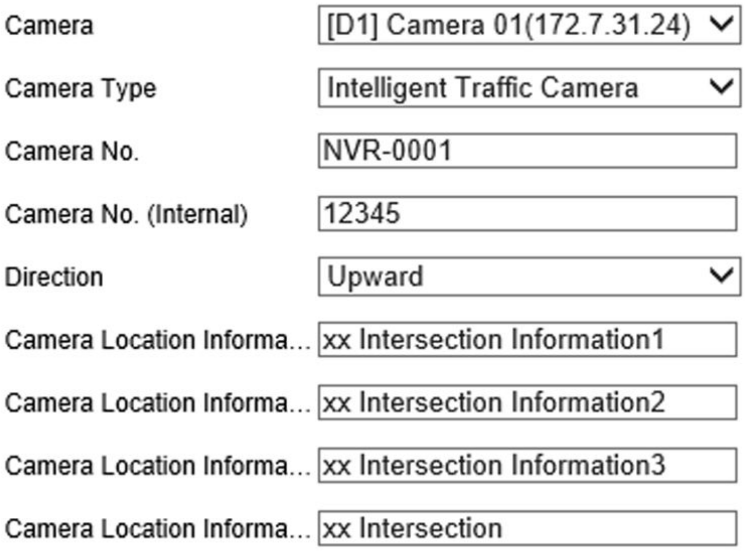
4.3 Set Event Parameters

4.3.1 Set Camera Parameters

To facilitate channel management, please set the camera location parameters.

Steps

1. Go to **Param Config → System → Camera Management → Camera Parameter** .



Camera	[D1] Camera 01(172.7.31.24)
Camera Type	Intelligent Traffic Camera
Camera No.	NVR-0001
Camera No. (Internal)	12345
Direction	Upward
Camera Location Informa...	xx Intersection Information1
Camera Location Informa...	xx Intersection Information2
Camera Location Informa...	xx Intersection Information3
Camera Location Informa...	xx Intersection

Figure 4-1 Set Camera Parameters

2. Select a camera.
3. Select the camera type.
   - If you do not need to capture, please select **Camera for Video Surveillance**.
   - If you need to capture, please select **Intelligent Traffic Camera**.

   Note

   The camera type depends on the model, the actual device prevails.
4. Customize the camera No., the internal camera No., camera location information and description.
5. Select the direction of the camera location according to the driving direction.
6. Click **Save**.

4.3.2 Set Violation Dictionary

Violation dictionary defines corresponding codes of violation types.

Steps

1. Go to **Param Config → Dictionary Settings** .
2. Select **Traffic Violation**/**Evidence Capture**.
3. Check the data, and click **Edit** to edit the code.
4. **Optional:** You can also do the following operations.

Add	Click **Add** to add custom acts and codes.
Delete	Check the added custom data, and click **Delete** to delete the data. **Note** The default data in the dictionary can not be deleted.
Reset	Click **Reset** to restore the dictionary to the factory settings, and the custom data will be cleared.

Chapter 5 Peripheral Device Linkage

5.1 Control Parking Lock

Connect the device to the parking lock, then you can view the parking lock status and remotely control the parking lock.

Before You Start

Connect the device to the platform. Connect the ANPR camera to the device. Connect the parking lock to the ANPR camera. Communication is normal.

Steps

1. Click **Parking Space Status**.
2. Select the connected parking video pole in the list, and view the parking lock status at the bottom right corner.
3. Click **Unlock** or **Lock** to remotely control the parking lock.

Chapter 6 Data Management

6.1 View Real-Time Data

You can view the real-time vehicle violation information.

Steps

1. Click **Real-Time Data**.
2. View the data.

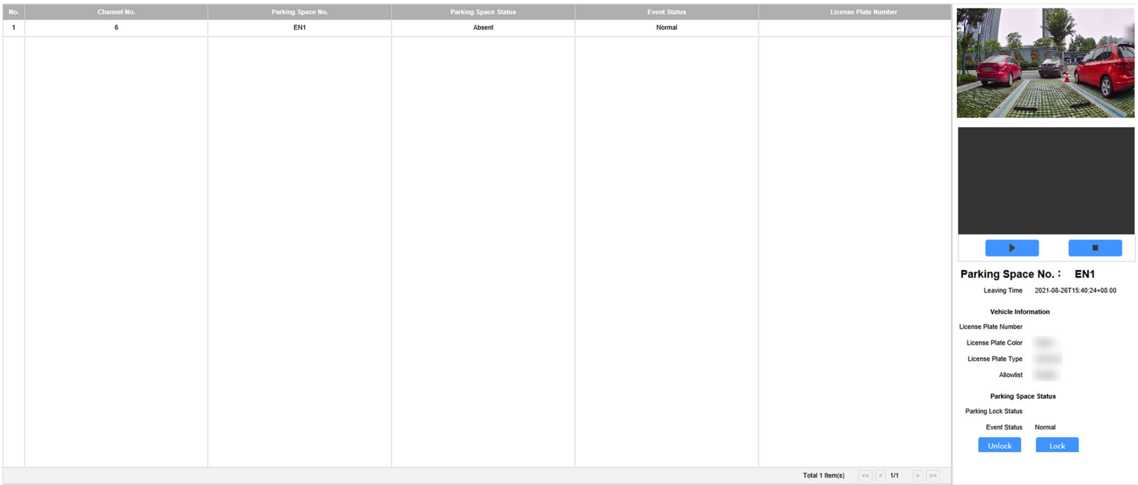
View the vehicle violation detailed information	Check the data row, the left side of the interface will display the vehicle violation detailed information.
View the vehicle violation picture	Click **Picture** to view the vehicle violation picture information.

6.2 View Parking Space Status

You can view the parking space status, parking space picture and event video of all the parking cameras connected to the device.

Steps

1. Click **Parking Space Status**.



No.	Channel No.	Parking Space No.	Parking Space Status	Event Status	License Plate Number
1	6	EN1	Absent	Normal	

Total 1 Item(s) << < 1/1 > >>

Parking Space No.： EN1

Leaving Time 2021-08-26T15:40:24+08:00

Vehicle Information

License Plate Number

License Plate Color

License Plate Type

Allowlist

Parking Space Status

Parking Lock Status

Event Status Normal

Figure 6-1 View Parking Space Status

Note

The parking status information will refresh automatically.

2. View the parking space No., parking space status, event status and other information in the list.
3. **Optional:** You can also do the following operations.

View the parking space picture
Select a piece of information to view the enlarged parking space picture on the upper right corner of the interface.

View the detailed information
Select a piece of information to view the detailed information of the vehicle and parking space on the lower right corner of the interface.

View the event video
Select a piece of information to view the event video on the middle right side of the interface, and click ▶ / ■ to start/stop recording.

6.3 Search Data

You can search the traffic data according to the camera channel.

Steps

1. Go to **Data Search → Traffic Data Search** .
2. Select time and other search conditions.

   Note

   There must be less than 7 days between start time and end time.
3. Click **Search**.

   The device will display the search result.
4. Click **Details** to view details, pictures and videos.
5. **Optional:** After searched the data, click **Export** to export the selected data information to the specified path.

   Note

   If the exporting failed, please add the IP address of the channel as a trusted site in the browser.

6.4 Data Backup

Enter a short description of your concept here (optional).

This is the start of your concept.

6.4.1 Backup to Local

You can back up the data of the device to your computer.

Before You Start
Search the data to back up.

Steps

1. Set the picture export rule.

1) Go to **Param Config → Backup Settings → Web Backup Settings** .
2) Enter the name, path and other information of the picture and video.

Note

After set the random number digits, pictures with the same name will be automatically numbered. The upper limit of the number is the maximum number of the random number digits.

3) Click **Save**.

2. Set the device IP address as a trusted site in the security settings of the browser.
3. Search the data, refer to "Search Data" for details.
4. Click **Export** to select export type and export the data to your computer.

Result

Pictures will be backed up as the set name in the set path.

6.4.2 Backup to USB

You can set the device to automatically back up the data to the USB.

Before You Start

Connect a USB to the device.

Steps

1. Go to **Param Config → Backup Settings → Local Backup → USB Backup Settings** .
2. Click **USB Backup Settings**.
3. Select **Enable USB Backup** as **Enable**.
4. Select backup strategy and time.
    - **Real-Time Backup**: Automatically back up the data only once after it saved at the set time.
    - **Backup Every Day**: Automatically back up the data once a day at the set time.
5. Select the **Data Type** to backup.
6. Set **Saving Path and File Name**.

    Pictures will be backed up as the set name in the set path.
7. Click **Save**.
8. **Optional:** Click **USB Backup Status** to view the backup status.

Chapter 7 Live View and Local Configuration

7.1 Live View

7.1.1 Start/Stop Live View

Start/stop the live view of cameras.

Start Live View

Click the camera list on the left side of the live view interface to start a camera live view.

Note

If you want to display a camera live view in a specific split window, please select the split window first, and then click the camera to start live view. The display window is only set for once, and you need to set it again when you start live view next time.

Click ▶ to start all live view.

Stop Live View

When the camera starts live view, click the camera list on the left side of the live view interface to stop live view.
Click ■ to stop all live view.

7.1.2 Divide Window and Switch Page

Select window division if you need to switch the single or multi-window live view mode, and view the camera live view of all pages via switching the page.

Divide Window

Click ⊞▾ to select the live view window division mode according to the actual needs.

Switch Page

When the number of divided windows is less than the cameras, click ← and → to switch the page and view the camera live view of all pages.

7.1.3 Select Stream Type

Click ① / ② to select the stream type. It is recommended to 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.

7.1.4 Capture Manually

Capture live view pictures and save them to your computer.

Steps

1. Click **Live View**.
2. Start live view of a camera.
3. Click 📷 .
4. View captured pictures.

Note

Go to **Param Config → Local** for the saving path of snapshots in live view.

7.1.5 Record Manually

You can record videos manually on the live view image and save them to the computer.

Steps

1. Click ▶ to start live view.
2. Click 🎥 to start recording.
3. Click 🎥 to stop recording.
4. **Optional:** Go to **Param Config → Local** to view the saving path of record files.

7.1.6 Enable/Disable Audio

Enable the audio if necessary after connecting an audio input device under the audio & video stream. Click 🔇 to enable and adjust it. Click the icon again to disable this function.

7.1.7 Enable Digital Zoom

You can enable digital zoom to zoom in a certain part of the live view image.

Steps

1. Click ▶ to start live view.
2. Click 🔍 to enable digital zoom.
3. Place the cursor on the live view image position which needs to be zoomed in. Drag the mouse rightwards and downwards to draw an area.

   The area will be zoomed in.
4. Click any position of the image to restore to normal image.
5. Click 🔍 to disable digital zoom.

7.1.8 Display in Full Screen

You can display the live view image in full screen.

On **Live View** interface, click ⛶ to display the live view image in full screen.

Press **esc** on the keyboard to exit the full screen mode.

7.2 PTZ Control

7.2.1 PTZ Control Panel

Click **Live View** and control PTZ cameras via PTZ control panel.

Note

- PTZ control panels may vary with recorder models. The actual device prevails.
- PTZ supports power-down memory. After PTZ suddenly loses power or reboot, it can automatically go back to the former position.

Table 7-1 Buttons Description

Icon	Description	Icon	Description
◤ ▲ ◥ ◀ ↻ ▶ ◣ ▼ ◢	Direction buttons	↻	Auto-scan button
🔍	Zoom -	🔍	Zoom +
⧉	Focus +	⧉	Focus -
○	Iris +	●	Iris -
💡	Turn on/off light	⌒	Start/stop wiper
‹	Display the PTZ control panel.	›	Hide the PTZ control panel.

7.2.2 Set Preset

A preset is a predefined image position. For the defined preset, you can call the preset No. to view the position.

Steps

1. Click ⚑ .

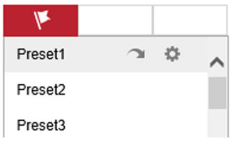


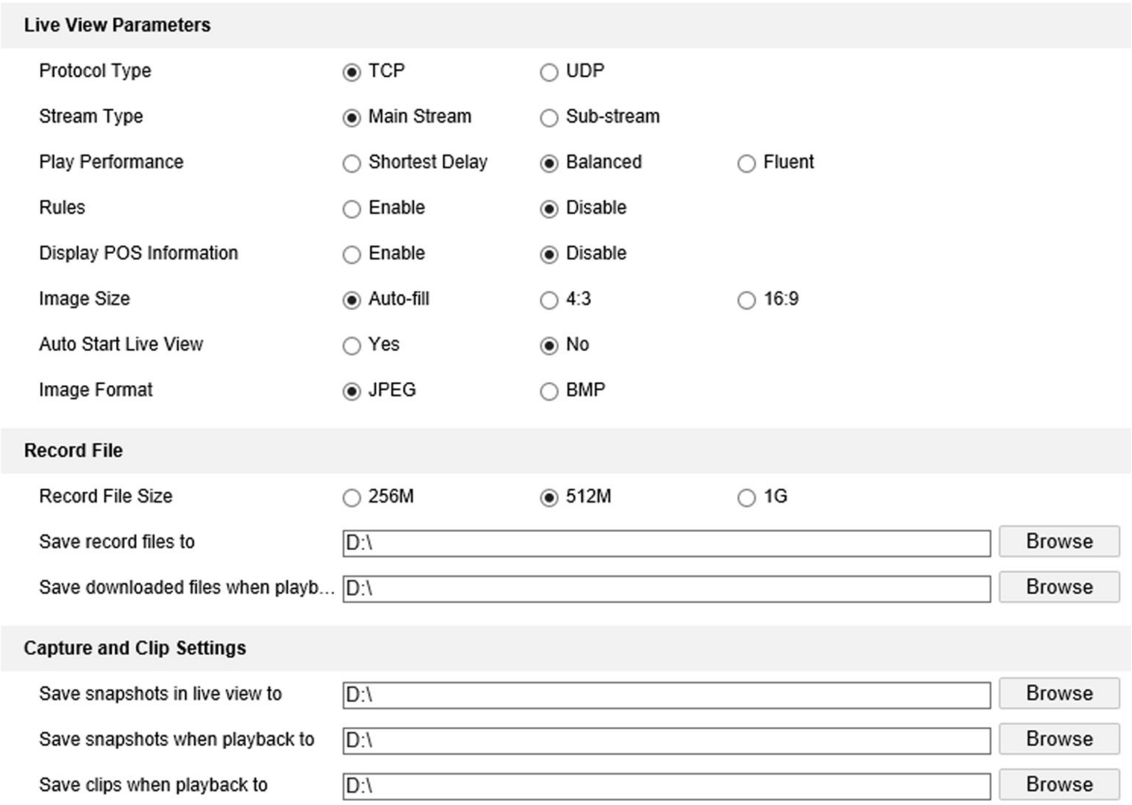
Figure 7-1 Set Preset

2. Operate the direction buttons of PTZ control to adjust PTZ to the desired position, and adjust the focus, zoom, etc., to get the desired scene.
3. Select the preset to set.
4. **Optional:** You can also do the following operations.

Click ⚙	Set preset according to prompt.
Click ↷	Call the preset, then PTZ will turn to the set direction.

7.3 Local Configuration

Go to **Param Config → Local** to set the live view parameters.



Live View Parameters

Protocol Type ● TCP ○ UDP

Stream Type ● Main Stream ○ Sub-stream

Play Performance ○ Shortest Delay ● Balanced ○ Fluent

Rules ○ Enable ● Disable

Display POS Information ○ Enable ● Disable

Image Size ● Auto-fill ○ 4:3 ○ 16:9

Auto Start Live View ○ Yes ● No

Image Format ● JPEG ○ BMP

Record File

Record File Size ○ 256M ● 512M ○ 1G

Save record files to D:\ Browse

Save downloaded files when playb... D:\ Browse

Capture and Clip Settings

Save snapshots in live view to D:\ Browse

Save snapshots when playback to D:\ Browse

Save clips when playback to D:\ Browse

Figure 7-2 Local Configuration

Protocol Type

TCP

Ensures completely delivery of streaming data and better video quality, yet the real-time transmission will be affected.

UDP

Provides real-time audio and video streams.

Stream Type

The stream type decides the definition of live view image.

Main Stream

Provides the best resolution and frame rate the device can do.

Sub-stream

Provides comparatively low resolution options.

Play Performance

Shortest Delay

The video is real-time, but the video fluency may be affected.

Balanced

Balanced mode considers both the real time and fluency of the video.

Fluent

When the network condition is good, the video is fluent.

Rules

If you select **Enable**, set rule information will be displayed on the live view interface.

Display POS Information

If you select **Enable**, the POS information of the capture camera will be displayed on the live view interface.

Image Size

Select according to your needs.

Auto Start Live View

If you select **Yes**, you can view the camera live view image after login the browser. If you select **No**, you need to start live view manually after login the device.

Image Format

Set the saving format of captured pictures.

JPEG

The picture will be compressed.

BMP

The picture will not be compressed.

Record File Size

Select the packed size of the manually recorded video files. After the selection, the max. record file size is the value you selected.

Save record files to

Set the saving path for the manually recorded video files in live view interface.

Save downloaded files when playback to

Set the saving path for the downloaded files in playback mode.

Save snapshots in live view to

Set the saving path of the manually captured pictures in live view mode.

Save snapshots when playback to

Set the saving path for the manually captured pictures in playback mode.

Save clips when playback to

Set the saving path for the clips in playback mode.

Chapter 8 Network Configuration

8.1 Connect to Platform

8.1.1 Connect to ISUP Platform

ISUP (EHome) is a platform access protocol. The device can be remotely accessed via this platform.

Before You Start

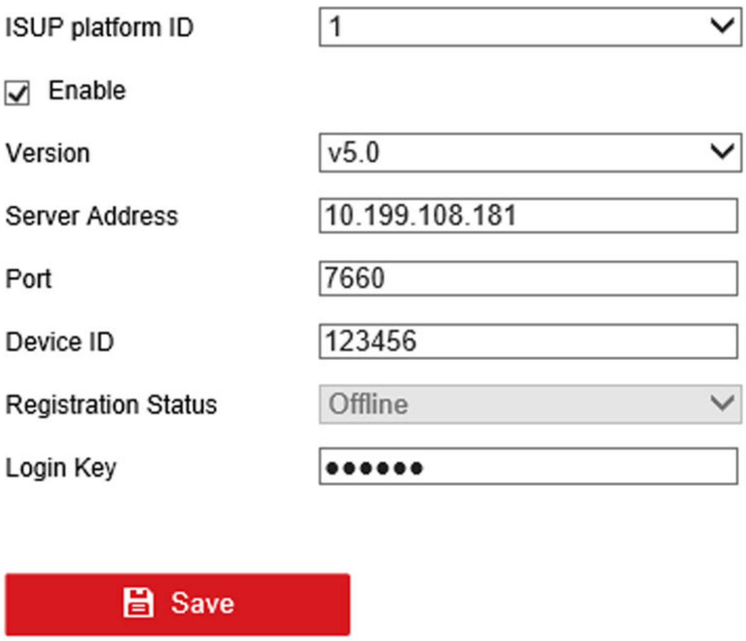
- Create the device ID on ISUP platform.
- Ensure the device can communicate with the platform normally.

Steps

Note

This function varies with different models. The actual device prevails.

1. Go to **Param Config → Network → Advanced Settings → ISUP** .



ISUP platform ID	1
☑ Enable	
Version	v5.0
Server Address	10.199.108.181
Port	7660
Device ID	123456
Registration Status	Offline
Login Key	••••••

Figure 8-1 Connect to ISUP Platform

2. Select **ISUP Platform ID**.
3. Check **Enable**.
4. Select protocol **Version**.

Note

Functions vary with different protocol versions.

5. Enter ISUP **Server Address**, **Port**, and **Device ID**.

Note

The device ID should be the same with the added one on the ISUP platform.

6. **Optional:** Enter **Login Key** if you select **v5.0**.
7. Click **Save**.
8. **Optional:** View **Registration Status**.

Note

When the registration status shows online, you can add or manage the device via the platform software. Refer to its corresponding manual for details.

8.1.2 Connect to Guarding Vision

You can set the function to realize network access via the Guarding Vision.

Before You Start

- Connect the device to the public network via dial or network cable.
- Set the device LAN IP address, subnet mask, gateway, and DNS server parameters.

Steps

1. Go to **Param Config → Network → Advanced Settings → Guarding Vision** .
2. Check **Enable**.
3. Customize the verification code. Adding device on the Guarding Vision needs to enter this verification code.

Note

6 to 12 characters allowed, including digits, uppercase letters, and lowercase letters. You are recommended to use a combination of no less than 8 letters or digits.

4. Click **Save**.
5. Access the Guarding Vision platform.
   - Use computer browser to access ***http://www.guardingvision.com*** .
   - Search "Guarding Vision" in the mobile App store.
6. Register the user name and password, and log in.
7. Add the device serial No. and verification code.
8. Start live view to view the device image.

8.2 Set DDNS

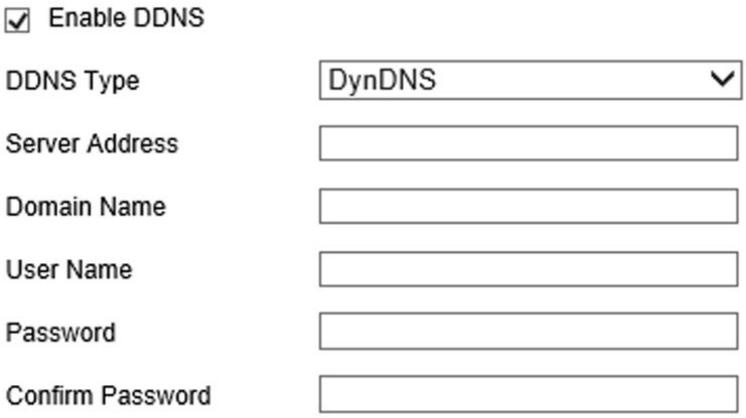
You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start

- Register the domain name on the DDNS server.
- Set the LAN IP address, subnet mask, gateway, and DNS server parameters.
- Complete port mapping. The default ports are 80, 8000, and 554.

Steps

1. Go to **Param Config → Network → Basic Settings → DDNS** .



☑ Enable DDNS

DDNS Type: DynDNS

Server Address

Domain Name

User Name

Password

Confirm Password

Figure 8-2 Set DDNS

2. Select **DDNS Type** according to the registered type.
3. Enter the server information and **Domain Name**.
4. Click **Save**.

What to do next

Enter the domain name in the browser to access the device.

8.3 Set Port

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

Caution

Do not modify the default port parameters at will, otherwise the device may be inaccessible.

Go to **Param Config → Network → Basic Settings → Port** for port settings. Click **Save** after finished settings.

HTTP Port

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser for login.

RTSP Port

It refers to the port of real-time streaming protocol.

HTTPS Port

It refers to the port of encrypted transmission and identity authentication protocol.

Service Port

It refers to the port to connect to client for obtain network protocol control and set device parameters.

Note

- Certain ports need to reboot after edited to take the new settings into effect.
- When the device cannot edit the port No. via access Web due to port conflicts, you can connect the device to your computer and edit via SADP software.

Chapter 9 Record and Playback

9.1 Set Storage Path

9.1.1 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 **Param Config → Storage → Storage Management → HDD Management** .
2. Check the HDD No. needs to be formatted.
3. Click **Format**.

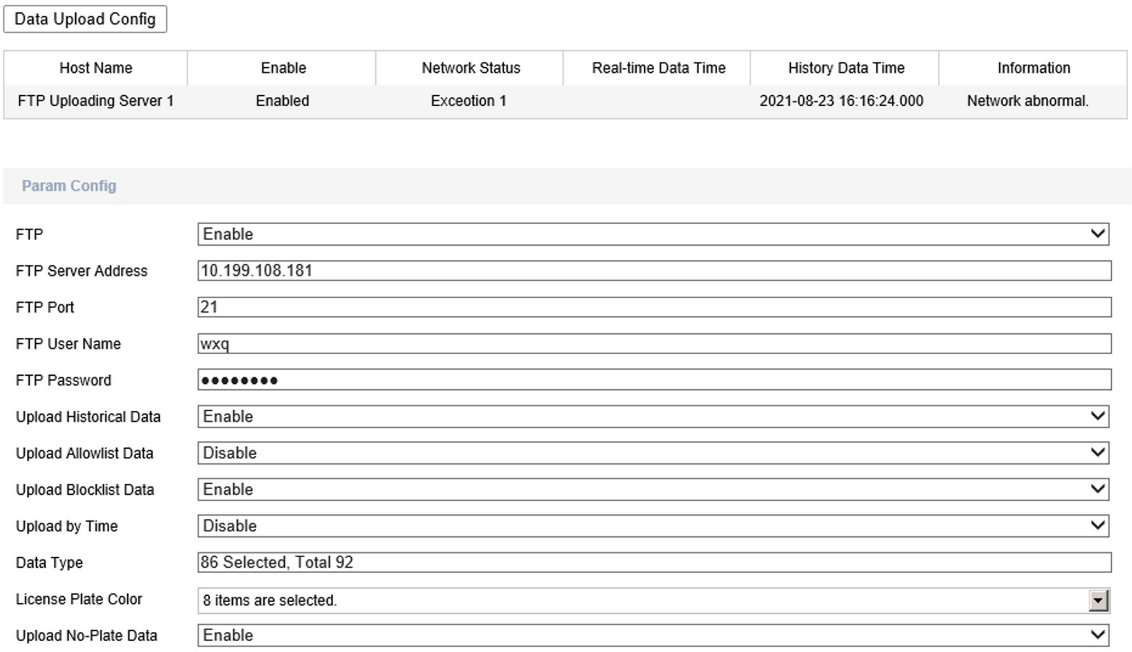
9.1.2 Set FTP

Set FTP parameters if you want to upload the captured pictures or recordings 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 **Param Config → Platform Settings → FTP Upload Settings** .



Data Upload Config

Host Name	Enable	Network Status	Real-time Data Time	History Data Time	Information
FTP Uploading Server 1	Enabled	Exceotion 1		2021-08-23 16:16:24.000	Network abnormal.

Param Config

FTP	Enable
FTP Server Address	10.199.108.181
FTP Port	21
FTP User Name	wxq
FTP Password	●●●●●●●●
Upload Historical Data	Enable
Upload Allowlist Data	Disable
Upload Blocklist Data	Enable
Upload by Time	Disable
Data Type	86 Selected, Total 92
License Plate Color	8 items are selected.
Upload No-Plate Data	Enable

Figure 9-1 Set FTP

2. Select a FTP server.

3. Set the upload address.

1) Select **Enable** in **FTP** dropdown list.

2) Enter **FTP Server Address**, **FTP Port**, **FTP User Name**, and **FTP Password**.

4. Set upload parameters.

Upload Historical Data

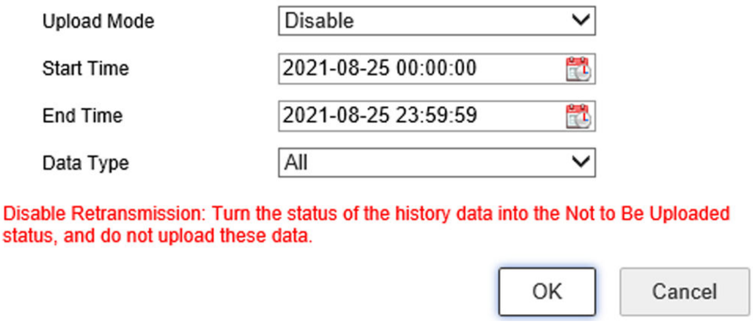
Historical data refers to the data failed to upload due to network disconnection or congestion. After enabled, historical data will upload again.

Upload No-Plate Data

Upload no-plate vehicle data to the FTP server.

5. Edit uploading file name and saving path according to the actual needs.

6. Click **Data Upload Config** to set parameters



Upload Mode	Disable
Start Time	2021-08-25 00:00:00
End Time	2021-08-25 23:59:59
Data Type	All

Disable Retransmission: Turn the status of the history data into the Not to Be Uploaded status, and do not upload these data.

Figure 9-2 Set Data Upload

1) Select **Upload Mode**.

   Data Retransmission

   Resends files to Remote Host.

   History Data Priority

   Sends historical files first. Otherwise terminal server sends historical files when free.

   Disable

   Terminal server won't upload historical data when free.

2) Select **Start Time** and **End Time**.
3) Select uploading **Data Type** in dropdown list.
4) Click **OK**.

7. Click **Save**.

9.1.3 Set Cloud Storage

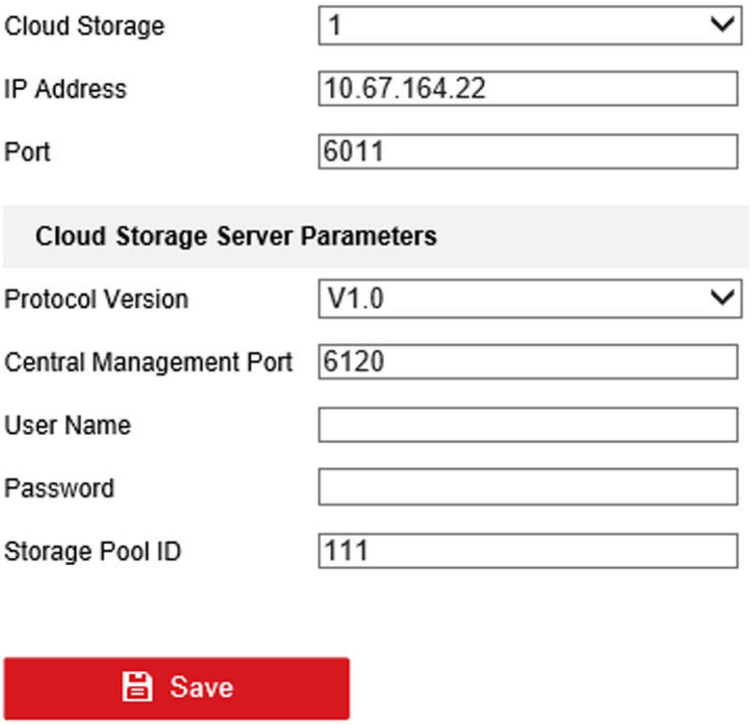
Cloud storage is a kind of network storage. It can be used as the extended storage to save the captured pictures.

Before You Start

Arrange the cloud storage server.

Steps

1. Go to **Param Config → Network → Advanced Settings → Cloud Storage** .



Cloud Storage: 1

IP Address: 10.67.164.22

Port: 6011

Cloud Storage Server Parameters

Protocol Version: V1.0

Central Management Port: 6120

User Name:

Password:

Storage Pool ID: 111

Figure 9-3 Set Cloud Storage

2. Select **Cloud Storage** server.
3. Enter **IP Address** and **Port** of the cloud storage server.
4. Set cloud storage server parameters.

Protocol Version

Protocol version of the cloud storage server.

Note

Cloud storage server parameters vary with different protocol versions. The actual interface prevails.

Central Management Port

Central management HTTP port of the cloud storage server.

Storage Pool ID

Storage pool ID of uploaded files on the cloud storage server.

User Name and Password

User name and password of the cloud storage server.

access_key

Key to access the cloud storage server.

secret_key

Key to encrypt the data uploaded to the cloud storage server.

5. Click **Save**.

9.2 Set Quota

Set the picture ratio in the storage.

Steps

1. Go to **Param Config → Storage → Storage Management → Picture Quota** .
2. Set the capacity for saving picture according to the actual needs.
3. Click **Save**.

9.3 Record

9.3.1 Set Timing Record

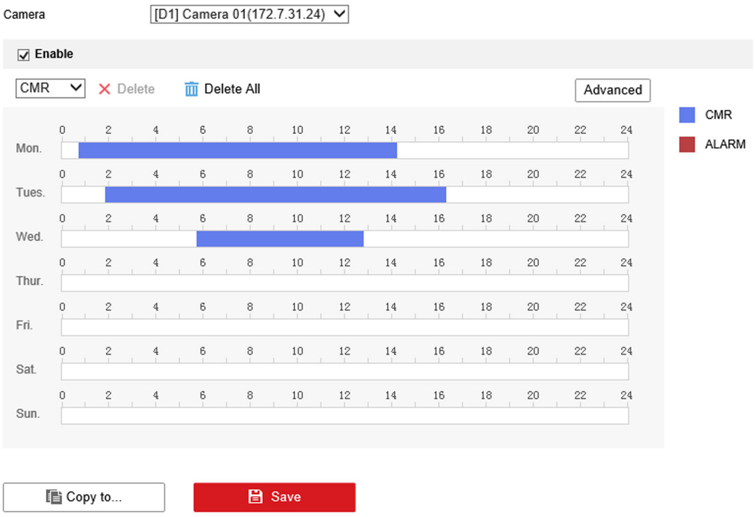
Set timing record if you need the camera to record automatically according to the set schedule.

Before You Start

Install and format the storage media (like HDD).

Steps

1. Go to **Param Config → Storage → Schedule Settings → Recording Schedule** .



Camera [D1] Camera 01(172.7.31.24)

☑ Enable

CMR

Figure 9-4 Set Timing Record

2. Select camera.
3. Check **Enable**, and select record type as **CMR**.
4. **Optional:** Click **Advanced** to set the camera record parameters.

- **Pre-record Time**: The time you set to start recording before the scheduled time.
- **Post-record**: The time you set to stop recording after the scheduled time.
- **Video Expiry Date**: Automatically delete video files after the scheduled time. **0** means that video files won't be deleted, but will be automatically overwritten after enabled overwritten record.

5. Set record time, refer to ***Set Record Schedule*** for details.
6. **Optional:** Click **Copy to...**, check the camera, and click **OK**.
7. Click **Save** to save the settings.

9.3.2 Set Event Record

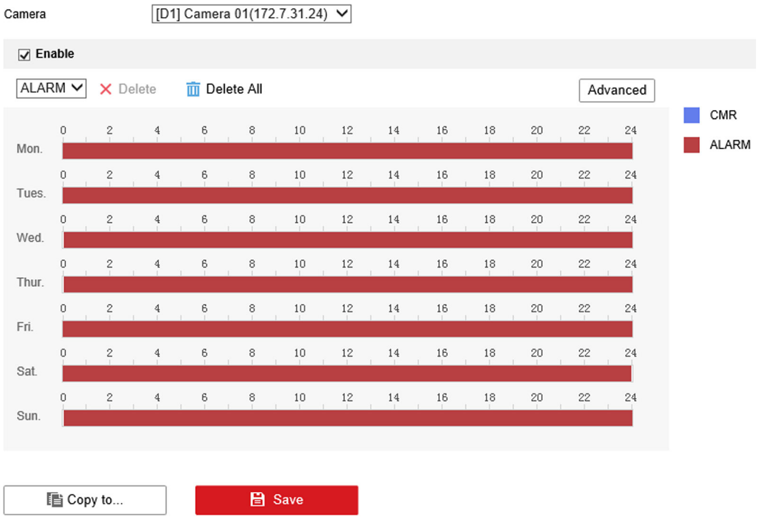
Set event record if you need the camera to record when event occurs.

Before You Start

- Install and format the storage media.
- Refer to event chapter for details of event settings.

Steps

1. Go to **Param Config → Storage → Schedule Settings → Recording Schedule** .



Camera [D1] Camera 01(172.7.31.24)

☑ Enable

ALARM

Figure 9-5 Set Event Record

2. Select camera.
3. Check **Enable**, and select record type as **Alarm**.
4. **Optional:** Click **Advanced** to set pre-record, post-record, video expiry date and stream type.
   - **Pre-record Time**: The time you set to start recording before the event.
   - **Post-record**: The time you set to stop recording after the event.
   - **Video Expiry Date**: Automatically delete video files after the event. **0** means that video files won't be deleted, but will be automatically overwritten after enabled overwritten record.
5. Set record time, refer to ***Set Record Schedule*** for details.

6. **Optional:** Click **Copy to...**, check the camera, and click **OK**.
7. Click **Save** to save the settings.

9.4 Play Back Video

You can play back the record files saved in the storage media (HDD, etc.).

Steps

1. Click **Playback**.
2. Select the camera.
3. Select the file date, and click **Search**.
   - Drag time bar and put the yellow line at the time point that you need.
   - Enter the specific time at **Set Playback Time**.
4. Click ▶ to play back the file.

⏸	Pause	⏵	Start playback for selected camera.
⊞ ▾	Split the playback window, and play back multiple cameras simultaneously.	■	Stop playback for selected camera.
⏩	Fast forward.	⏪	Slow forward.
⊠	Stop playback for all cameras.	📷	Capture pictures.
◂	Reverse.	🔇	Enable/disable audio.
⛶	Full screen.	-	-

Note

- For the captured picture of playback saving path, refer to **Save snapshots when playback to** in **Param Config → Local** .
- Operations and buttons vary with different models. The actual device prevails.

9.5 Backup

9.5.1 Back up Video

Download videos to a local path.

Steps

1. Click **Playback**.
2. Click ⤓ .

3. Select **Camera**.
4. Select download type.
   - If you need to search video by date, select **Download by Date**, and select the date.
   - If you need to search video by file type, select **Download by File**, and select file type and search time.
5. Select **File Type**.
6. Click **Search**.
7. Check videos to download and click **Download**.
8. For the video saving path, refer to **Save downloaded files when playback to** in **Param Config → Local** .

9.5.2 Back up Clipped Video

Clip videos and save them to a local path.

Steps

1. Click **Playback**.
2. Select playback **Camera** and date.
3. Click **Search**.
4. Play the video.
5. Drag time bar to the clip start time and click ✂ to start clipping.
6. Drag time bar to the clip end time and click ✂ to stop clipping.
7. For clipped video saving path, refer to **Save clips to** in **Configuration → Local** .

Chapter 10 Encoding and Display

10.1 Set Video Encoding Parameters

Set video encoding parameters to adjust the live view and recording effect.

- When the network signal is good and the speed is fast, you can set high resolution and bitrate to raise the image quality.
- When the network signal is bad and the speed is slow, you can set low resolution, bitrate, and frame rate to guarantee the image fluency.
- When the network signal is bad, but the resolution should be guaranteed, you can set low bitrate and frame rate to guarantee the image fluency.
- Main stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission. Sub-stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space. Third stream is offered for customized usage.

Steps

1. Go to **Param Config → Video & Audio → Video** .
2. Set the parameters for different streams.

   Stream Type

   Main stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission. Sub-stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space.

   Video Type

   Select the video type to video & audio when you need taping while recording. Select video when you only need record.

   Note

   The device only supports audio can select video & audio. The actual device prevails.

   Resolution

   The higher the resolution is, the clearer the image will be. Meanwhile, the network bandwidth requirement is higher.

   Bitrate Type and Max. Bitrate

   Select the bitrate type to constant or variable. Constant bitrate means that the stream is compressed and transmitted at a comparatively fixed bitrate. Variable bitrate means that the device automatically adjust the bitrate under the set **Max. Bitrate**.

Image Quality

When bitrate type is variable, you can select video quality according to actual needs. The higher the video quality is, the higher requirements of the network bandwidth.

Frame Rate

It is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Video Encoding

The device supports multiple video encoding types. Supported encoding types for different stream types may differ. H.265 is a new encoding technology. Compared with H.264, it reduces the transmission bitrate under the same resolution, frame rate, and image quality.

10.2 Set Image Parameters

Set image parameters to adjust brightness and contrast.

Steps

1. Go to **Param Config → Image → Display Settings** .
2. Select a camera.
3. Set **Brightness**, **Contrast**, and **Saturation** to obtain clear images.
4. **Optional:** Click **Restore Default Settings** to restore parameters to the default status.

10.3 Set OSD

You can customize OSD information on the live view.

Steps

1. Go to **Param Config → Image → OSD Settings** .
2. Select a camera.
3. Enter **Camera Name** and select **Time Format** and **Date Format**.
4. Check **Display Name**, **Display Date**, and **Display Week** according to actual needs.
5. **Optional:** Check the text overlay No. and enter contents according to your needs.
6. Drag the red frame overlaid on the live view image to adjust the OSD information positions.
7. Click **Save**.

Result

The set OSD will be displayed in live view image and recorded videos.

Chapter 11 Alarm Configuration

11.1 Set Alarm Input

Alarm signal from the external device triggers the corresponding actions of the current device.

Before You Start
Make sure the external alarm device is connected. See *Quick Start Guide* for cable connection.

Steps

1. Go to **Param Config → Event → Basic Event → Alarm Input** .
2. Select **Alarm Input No.** and edit **Alarm Name**.

   Note

   If you select **Alarm Input No.** as **A<-1(Cabinet Door Alarm)** or **A<-2(Cabinet Door Alarm)** (options vary with different models), please go to **Param Config → Advanced Settings → Other Settings** to set **Cabinet Door Name** and **Cabinet Door No.**.
3. Select **Alarm Type** according to the alarm device type.
4. Check **Enable Alarm Input Handling**.
5. Refer to ***Set Record Schedule*** for setting **Arming Schedule**.
6. Refer to ***Set Linkage Mode*** for setting **Linkage Action**.
7. **Optional:** Click **Copy to...** to copy the settings to other alarm input channels.
8. Click **Save**.

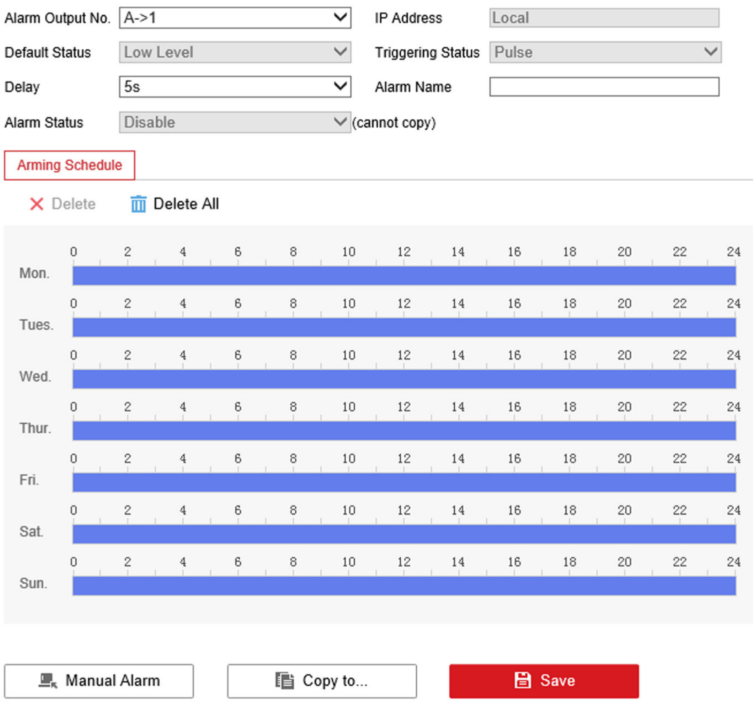
11.2 Set Alarm Output

Set alarm output to realize linkage alarm via external alarm device when the event occurs.

Before You Start
Make sure the external alarm device is connected. See *Quick Start Guide* for cable connection.

Steps

1. Go to **Param Config → Event → Basic Event → Alarm Output** .



Alarm Output No. A->1

IP Address Local

Default Status Low Level

Triggering Status Pulse

Delay 5s

Alarm Name

Alarm Status Disable (cannot copy)

Figure 11-1 Set Alarm Output

2. Select **Alarm Output No.** and edit **Alarm Name**.
3. Select **Delay**.

   The device will send out alarm output signal for the set time.
4. Refer to ***Set Record Schedule*** for setting **Arming Schedule**.
5. Click **Manual Alarm** to enable manual alarm output. Set according to the actual needs.
6. **Optional:** Click **Copy to...** to copy the settings to other alarm input channels.
7. Click **Save**.

11.3 Set Exception Alarm

Set exception alarm when the network is disconnected, the IP address is conflicted, etc.

Steps

1. Go to **Param Config → Event → Basic Event → Exception** .
2. Select **Exception Type**.

   HDD Full

   The HDD storage is full.

   HDD Error

   Error occurs in HDD.

   Network Cable Disconnected

The device is offline.

IP Address conflicted.

The IP address of current device is same as that of other device in the network.

Illegal Login

Incorrect user name or password is entered.

Record/Capture Exception

Exception occurs in record/capture.

3. Refer to ***Set Linkage Mode*** for setting linkage method.
4. Click **Save**.

11.4 Set Record Schedule

Set the valid time of the device tasks.

Steps

1. Click **Arming Schedule** to edit the arming schedule.
2. Click on the time bar and drag the mouse to select the time period.
3. Adjust the time period.
   - Click on the selected time period, and enter the desired value. Click **Save**.
   - Click on the selected time period. Drag the both ends to adjust the time period.

Note

- Click **Delete All** to delete all the set schedules.
- Up to 8 periods can be configured for one day.

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

Copy the same settings to other days	Move the mouse to the end of each day, a copy dialogue box pops up, and you can copy the current settings to other days.
Copy the same settings to other cameras	Click **Copy to...** to copy the same settings to other days. **Note** This function varies with different devices. The actual interface prevails.

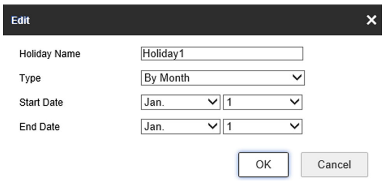
5. Click **Save** to save the settings.

11.5 Set Holiday

Set holiday for special days that alarms will not be triggered.

Steps

1. Go to **Param Config → Storage → Advanced Settings → Holiday** .



Holiday Name: Holiday1

Type: By Month

Start Date: Jan. 1

End Date: Jan. 1

Figure 11-2 Set Holiday

2. Check the holiday date to set.
3. Set the holiday parameters.
   1) Click ✎ .
   2) Set **Holiday Name**, **Type**, **Start Date** and **End Date**.
   3) Click **OK**.
4. **Optional:** Repeat the previous step to set other holidays.
5. Click **Save**.

11.6 Set Linkage Mode

Check the linkage actions as needed, and save the settings.

Note

Available linkage modes may vary with different events. The actual interface prevails.

Notify Surveillance Center

Upload the alarm information to the surveillance center.

Full Screen Monitoring

Display the image from the alarm channel in full screen.

Chapter 12 Safety Management

12.1 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

⚠ **Caution**

It is highly recommend you create a strong password of your own choosing in order to increase the security of your product.

1. Go to **Param Config → System → User Management** .
2. Click **Add**.
3. Enter the user name, password and other information in the popup window.
4. Click **OK**.

Delete the User	Select a user and click **Delete** to delete the user.
Edit the User Information	Click the user name of the added user and click **Edit** to edit the user information.

12.1.1 Install Authorized Certificate

If the demand for external access security is high, you can create and install authorized certificate via HTTPS protocol to ensure the data transmission security.

Steps

1. Go to **Param Config → Network → Advanced Settings → HTTPS** .
2. Select **Create the certificate request first and continue the installation.** and click **Create**.
3. Follow the prompt to enter **Country**, **Domain Name/IP**, **Effective Period**, and other parameters.
4. Click **OK**
5. Click **Download** to download the certificate request and submit it to the trusted authority for signature.

   Note

   Certification of certificates issued by Certification Authority may incur costs.
6. Import certificate to the device.
   - Click **Browse** to select the certificate and click **Install** to import the certificate to the device.

- Select **Signed certificate is available, start the installation directly.**. Click **Browse** to select the certificate and click **Install** to import the certificate to the device.

7. Click **Save**.

12.1.2 Create and Install Self-signed Certificate

HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Param Config → Network → Advanced Settings → HTTPS** .
2. Select **Create Self-signed Certificate**.
3. Click **Create**.
4. Follow the prompt to enter **Country**, **Domain Name/IP**, **Effective Period**, and other parameters.
5. Click **OK**.
6. Click **Save**.

12.1.3 Set SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

Steps

1. Go to **Param Config → System → Security → Security Service** .
2. Uncheck **Enable SSH**.
3. Click **Save**.

Chapter 13 Maintenance

13.1 View Device Information

Basic Information

Go to **Param Config → System → System Settings → Basic Information** to view the device basic information.
You can edit **Device Name** and **Device No.** The device No. is used to control the device. It is recommended to reserve the default value.

Device Status

Go to **Param Config → System Status** to view the sever status.

13.2 Search Log

You can search logs to troubleshoot problems.

Steps

1. Go to **Param Config → System → System Maintenance → Log Search** .
2. Set the search conditions.
3. Click **Search**.

   The log information will be displayed in the list.
4. **Optional:** Click **Export** to export the logs to the computer.

13.3 Upgrade

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

Before You Start
Prepare the upgrade file.

Steps

1. Go to **Param Config → System → System Maintenance → Upgrade & Maintenance → Upgrade** .
2. Click **Browse** and select the upgrade file.
3. Click **Upgrade**.
4. Click **OK** in the popup window.

Note

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

Result

The device will reboot automatically after upgrade.

13.4 Reboot

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

Steps

1. Go to **Param Config → System → System Maintenance → Upgrade & Maintenance** .
2. Click **Reboot**.
3. Click **OK** to reboot the device.

   Reboot

   The device will reboot automatically in every 2 a.m.

   Reboot without HDD

   The device will reboot after no HDD is detected.

13.5 Restore Parameters

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

Steps

1. Go to **Param Config → System → System Maintenance → Upgrade & Maintenance → Restore Default Settings** .
2. Select the restoration mode.
   - Click **Restore** to restore the parameters except the IP parameters and platform parameters to the default settings.
   - Click **Default** to restore all the parameters to the factory settings.
3. Click **OK**.

13.6 Set RS-485

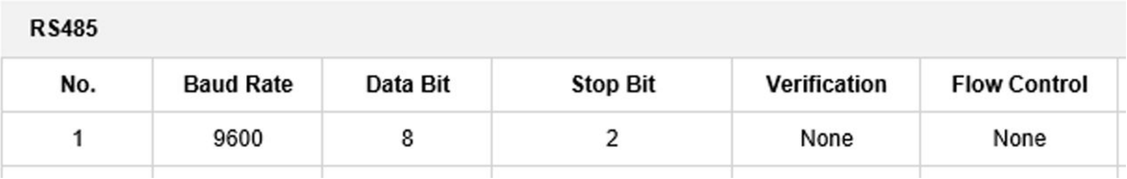
Set RS-485 parameters if the device has been connected to a vehicle detector or other RS-485 devices.

Before You Start

The corresponding device has been connected via the RS-485 serial port.

Steps

1. Go to **Param Config → System → System Settings → Serial Port** .



RS485

No.	Baud Rate	Data Bit	Stop Bit	Verification	Flow Control
1	9600	8	2	None	None

Figure 13-1 Set RS-485

2. Set **Baud Rate**, **Data Bit**, **Stop Bit**, **Verification** and **Flow Control**.

Note

- Flow control can control the process of data transmission and avoid data loss.
- When you select hardware flow control, you need to ensure the cable connection. It is recommended to select software flow control if the cable connection is restricted.

3. Click **Save**.

13.7 Set RS-232

Set RS-232 parameters if you need to debug the device via RS-232 serial port, or peripheral devices have been connected.

Before You Start

The corresponding device has been connected via the RS-232 serial port.

Steps

1. Go to **Param Config → System → System Settings → Serial Port** .
2. Select COM port according to the connected peripheral devices.

Note

Do not need to select COM port if the device only has one RS-232.

3. **Optional:** Edit **Baud Rate**, **Data Bit** and **Stop Bit**.
4. Select **Control Mode**.

   Transparent Channel

   For the data transmission of peripheral devices.

   Control Panel(By Parameter)

   For the serial port debugging of the device.
5. Click **Save**.

13.8 Synchronize Time

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

Steps

Note

Time sync. mode varies with different models. The actual interface prevails.

1. Go to **Param Config → System → System Settings → Time Settings** .
2. Select **Time Zone**.
3. Select the time sync. mode.

   NTP Time Sync.

   Select it to synchronize the device time with that of the NTP server. Set **Server Address**, **NTP Port**, and **Interval**. Click **NTP Test** to test if the connection between the device and the server is normal.

   Note

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

   Manual Time Sync.

   Select it to synchronize the device time with that of the computer. Set time manually, or check **Sync. with computer time**.

   GPS Time Sync.

   Select it to synchronize the device time with that of the GPS. It is high-efficiency and less error.

   SDK Time Sync.

   If the remote host has been set for the device, select it to synchronize time via the remote host.

   EHome Time Sync

   Select it to synchronize the device time with that of the EHome platform.
4. Click **Save**.

13.9 Synchronize Camera Time

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

Steps

1. Go to **Param Config → Advanced Settings → Other Settings → Other Settings** .
2. Select **Camera Time Synchronization** as **Enable**.
3. Set the 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.

13.10 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 **Param Config → System → System Maintenance → Upgrade & Maintenance → Export Parameters** .
2. Click **Device Parameters**.
3. Select the saving path and enter the file name.
4. Click **Save**.

13.11 Import Parameters

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

Before You Start
Save the file that needs to be imported to the computer.

Steps

Note

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

1. Go to **Param Config System System Maintenance Upgrade & Maintenance Import Parameters**.
2. Click **Browse** to import the configuration file.
3. Click **Import**.

Result

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

13.12 Detect HDD

Detect HDD regularly to avoid data loss due to HDD damage.

Steps

1. Go to **Param Config → Storage → Storage Management → HDD Detection** .

S.M.A.R.T. Detection Detect and report on various indicators of reliability in the hopes of anticipating failures.

Bad Sector Test	Detect the block capacity of the HDD.

2. Select **HDD No.** and **Self-test Type**, and click **Start Detecting**.

Result

Decide whether to use the HDD any more according to the detection result. If there are too many bad sectors, change the HDD in time.

13.13 Set Working Mode

You can set the device as listening mode or arming mode.

Before You Start

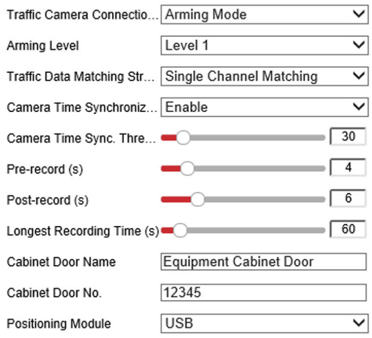
Ensure the connected camera supports violation capture function.

Steps

Note

Traffic Data Matching Strategy is a reserved function.

1. Go to **Param Config → Advanced Settings → Other Settings → Other Settings** .



Traffic Camera Connectio...	Arming Mode
Arming Level	Level 1
Traffic Data Matching Str...	Single Channel Matching
Camera Time Synchroniz...	Enable
Camera Time Sync. Thre...	30
Pre-record (s)	4
Post-record (s)	6
Longest Recording Time (s)	60
Cabinet Door Name	Equipment Cabinet Door
Cabinet Door No.	12345
Positioning Module	USB

Figure 13-2 Set Working Mode

2. Select **Traffic Camera Connection Mode**.

   Arming Mode

   The device actively connects to the camera and receives images after logging in to the camera.

   Listening Mode

   You need to connect the camera to the device. After set the camera as listening mode, the device can receive the data uploaded from the camera.

3. Select **Arming Level**.

Note

- Level 1 arming can only connect 1 client or web. Level 2 arming can connect 3 clients or webs. Level 3 arming can connect 5 clients or webs.
- The device supports to set level 1, level 2 and level 3 arming simultaneously. The level 1 arming uploads first.

4. Select **Camera Time Synchronization**.
5. Set record time parameters.

   Pre-record

   The time to record before the violation recording start time.

   Post-record

   The time to record after the violation recording end time.

   Longest Recording Time

   The longest recording time of violation recording.
6. Click **Save**.
7. **Optional:** Click **Data Search** and select search conditions to search relevant violation recordings.

13.14 Reserved Parameters

The reserved parameters are only for technical personnel to debug.

Face picture collection, segment speed detection and channel matching are reserved functions. The actual device prevails.

Appendix A. Communication Matrix and Device Command

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

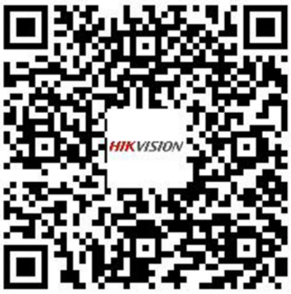


Figure A-1 Communication Matrix

Scan the QR code below to get the device command.

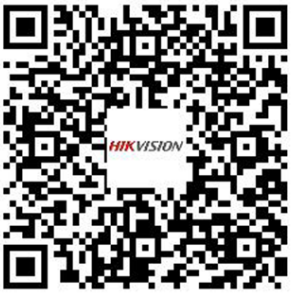


Figure A-2 Device Command

See Far, Go Further