



Terminal Server

User Manual

Legal Information

©2022 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

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.

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.

Contents

Chapter 1 Introduction	1
1.1 Product Introduction	1
1.2 Key Feature	1
1.3 Running Environment	1
Chapter 2 Activation and Login	2
2.1 Activation	2
2.1.1 Default Information	2
2.1.2 Activate via SADP	2
2.1.3 Activate via Web Browser	3
2.2 Login	4
Chapter 3 Basic Operation	5
3.1 Set LAN IP Address	5
3.1.1 Set Internal IP	5
3.1.2 Set External IP	6
3.2 Set Static Router	7
3.3 Manage Camera	8
3.3.1 Add IP Camera	8
3.3.2 Set Interaction Parameters	10
3.4 Set Remote Host	10
Chapter 4 Event Detection and Face Recognition	12
4.1 Set Vehicle Arming	12
4.2 Set Event Parameters	13
4.2.1 Set Camera Parameters	13
4.2.2 Set Violation Dictionary	14
Chapter 5 Data Management	15
5.1 View Real-Time Data	15

5.2 Search Data	15
5.3 Enable Traffic Parameters Statistics	15
5.4 View Traffic Statistics	16
5.5 Back up Data	16
5.5.1 Back up to Local	16
5.5.2 Back up to USB	17
Chapter 6 Live View and Local Configuration	18
6.1 Live View	18
6.1.1 Start/Stop Live View	18
6.1.2 Divide Window and Switch Page	18
6.1.3 Select Stream Type	18
6.1.4 Capture Manually	19
6.1.5 Record Manually	19
6.1.6 Enable/Disable Audio	19
6.1.7 Enable Digital Zoom	19
6.1.8 Display in Full Screen	20
6.2 PTZ Control	20
6.2.1 PTZ Control Panel	20
6.2.2 Set Preset	21
6.3 Local Configuration	21
Chapter 7 Network Configuration	24
7.1 Dial	24
7.2 Connect to ISUP Platform	25
7.3 Set DDNS	26
7.4 Set Port	27
7.5 Set SNMP	27
7.6 Set ONVIF	28
Chapter 8 Record and Playback	30

8.1 Set Storage Path	30
8.1.1 Format Disk	30
8.1.2 Set FTP	30
8.1.3 Set Cloud Storage	32
8.2 Set Quota	33
8.3 Record	33
8.3.1 Set Timing Record	33
8.3.2 Set Event Record	34
8.4 Play Back Video	35
8.5 Backup	36
8.5.1 Back up Video	36
8.5.2 Back up Clipped Video	36
Chapter 9 Encoding and Display	38
9.1 Set Video Encoding Parameters	38
9.2 Set Image Parameters	39
9.3 Set OSD	39
Chapter 10 Alarm Congifuration	41
10.1 Set Alarm Input	41
10.2 Set Alarm Output	41
10.3 Set Exception Alarm	42
10.4 Set Record Schedule	43
10.5 Set Holiday	44
10.6 Set Linkage Mode	44
Chapter 11 Safety Management	45
11.1 Manage User	45
11.2 Install Authorized Certificate	45
11.3 Create and Install Self-signed Certificate	46
11.4 Set SSH	46

11.5 Set Session Expired Time	46
Chapter 12 Maintenance	47
12.1 View Device Information	47
12.2 Search Log	47
12.3 Upgrade	47
12.4 Reboot	48
12.5 Restore Parameters	48
12.6 Restore Database	48
12.7 Set RS-485	49
12.8 Set RS-232	49
12.9 Synchronize Camera Time	50
12.10 Synchronize Time	50
12.11 Set DST	51
12.12 Export Parameters	51
12.13 Import Parameters	51
12.14 Detect HDD	52
12.15 Set Working Mode	52
12.16 Reserved Parameters	54
Appendix A. Communication Matrix and Device Command	55

Chapter 1 Introduction

1.1 Product Introduction

Terminal server, as an outdoor network video recorder in the traffic field, integrates multiple functions like storage management, traffic data management, video and audio decoding, picture processing, and network switching. It adopts the embedded, switchable, and hybrid hard disk recording design, which meets the demands for front-end distributed storage and forms a set of security system with the help of the network access platform management center. It is used to receive, store, and process data in the scene of expressway, urban road, tunnel, etc.

1.2 Key Feature

- Supports connecting to various types of cameras.
- Solid, compact, fan-free, and small-sized, applicable to various scenarios such as roadside cabinet and pole mounted cabinet.
- Interfaces designed on a single panel, which makes it easy for constructions and operations.
- Supports large-capacity storage.
- Supports web operations and SDK.

1.3 Running Environment

- Browser: IE 8.0 and above versions recommended.
- 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: The default IP address for G1 network interface is 192.1.0.64. The default IP address for G2 network interface is 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

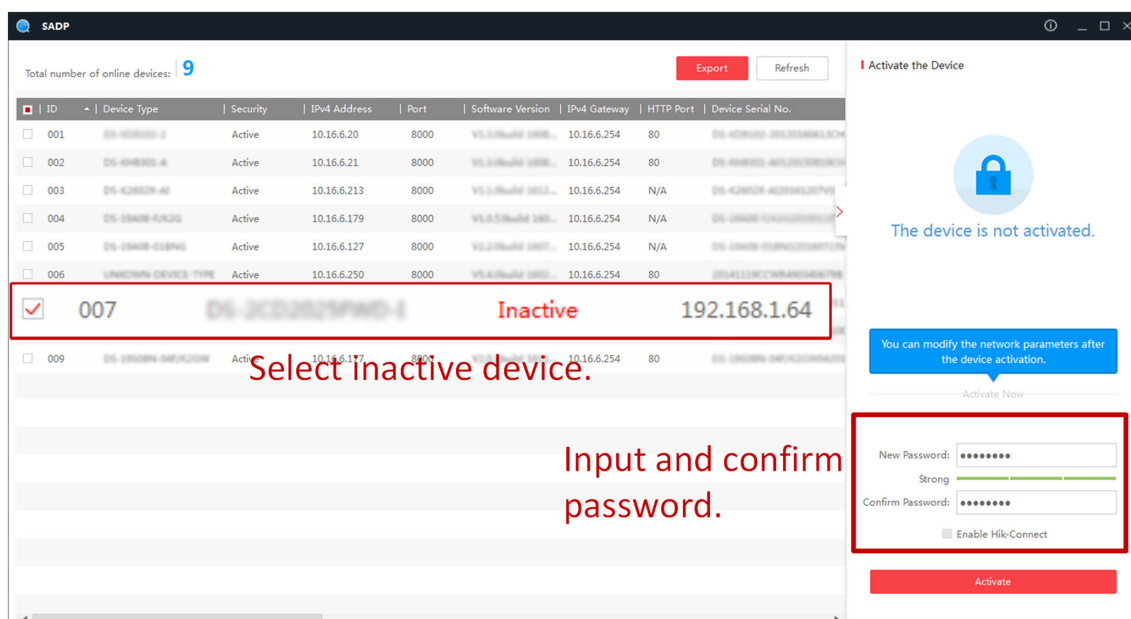


Figure 2-1 Activate via SADP

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



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

Complete connections before setting networks.

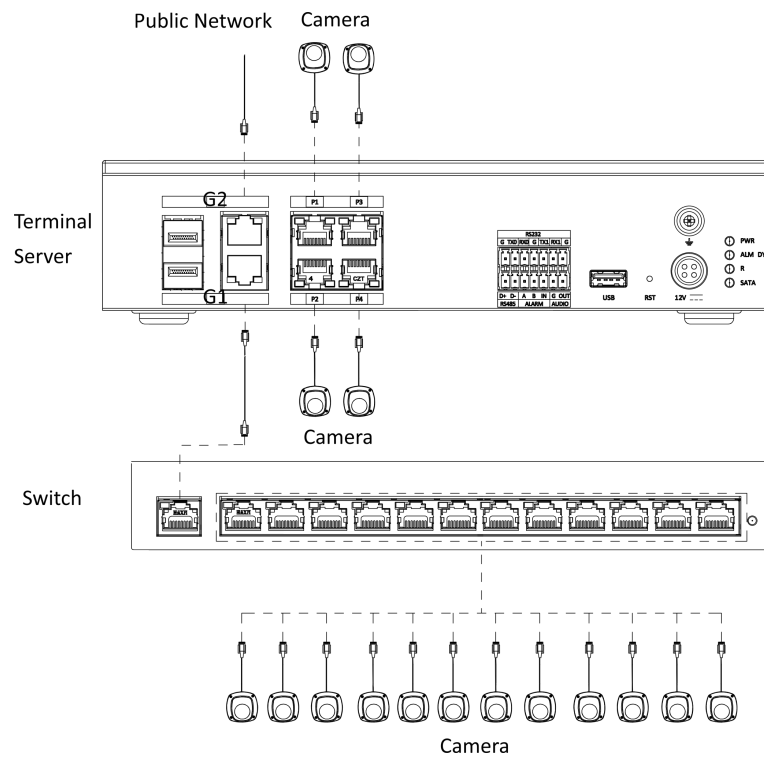


Figure 3-1 Connection Sample

3.1.1 Set Internal IP

The internal network is set for the IP of the G1 network interface on the device panel, and it is mainly used to connect to the camera.

Steps

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

NIC Type	Self-adaptive ▼ ☐ Auto
IPv4 Address	192.1.0.64
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	
IPv6 Address	fd01::c001:40
IPv6 Prefix Length	64
IPv6 Default Gateway	::
Physical Address	58:50:ed:e1:a0:39
MTU	1500

Figure 3-2 Set Internal IP

2. Select **NIC Type** according to the actual network.
3. Set relevant network parameters.
 - Check **Auto** to get the IPv4 and IPv6 addresses automatically if the network supports distributing the IP addresses automatically.
 - Manually enter the IPv4 and IPv6 parameters and the MTU according to the actual network conditions.

 Note

- The internal IP address and the camera should be set to the same network segment, and it must be set to a different network segment from that of the external IP address.
- **MTU** stands for the maximum transmission unit in the network.

-
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	10.10.99.168
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.10.99.254
IPv6 Address	fd00::c0a8:140
IPv6 Prefix Length	64
IPv6 Default Gateway	::
Physical Address	58:50:ed:e1:a0:38
MTU	1500

Figure 3-3 Set External IP

2. Select **NIC Type** according to the actual network.
3. Set relevant network parameters.
 - Check **Auto** to get the IPv4 and IPv6 addresses automatically if the network supports distributing the IP addresses automatically.
 - Manually enter the IPv4 and IPv6 parameters and the MTU according to the actual network conditions.

 Note

- The network segment of external IP address should be different from that of the internal IP address.
- **MTU** stands for the maximum transmission unit in the network.
- Set **DNS Server** if remote domain name access is needed.

-
4. Click **Save**.

3.2 Set Static Router

Set a static router for access across network segments. The device will transmit data 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

Figure 3-4 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

The device supports deleting or editing 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 3-5 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:** In this mode, you can know the camera status via the camera's stream, and you can record and preview images and receive image data via the server.
 - **Data Receiving Mode:** In this mode, you can only receive image data via the server, but you cannot record or preview the images.
4. 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 a remote host.



Note

The supported number of remote hosts varies with different devices. The actual interface prevails.

3. 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.
4. 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.
5. Click the enter box behind **Data Type** to check the upload data type and select specific upload data.



Note

For access via the remote host, **Upload Strategy** needs to be set first. Parameters may be different under different protocols. The actual interface prevails.

6. Select the **License Plate Color**.
7. Set the upload types to be enabled (for example, **Upload History Data**, **Upload No-Plate Data**, **Upload Blocklist Data**, **Upload Allowlist Data**, and **Upload by Time**) according to your needs, and set other parameters.

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**.
 - 1) Select **Upload Mode**, **Start Time**, **End Time**, and **Data Type**.
 - 2) Click **OK**.
9. **Optional**: Check **Enable Cloud Storage** to set the picture server ID, 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. **Optional**: Repeat the above steps if you need to set another remote host.
11. Click **Save**.

Chapter 4 Event Detection and Face Recognition

4.1 Set Vehicle Arming

The device supports setting vehicle arming to manage special license plates.

Steps

1. Go to **Param Config → Advanced Settings → Vehicle Arming → Arming Management**.
2. Check **Blocklist Arming** or **Allowlist Arming**.
3. **Optional:** Check **Blocklist Time Period Arm** or **Allowlist Time Period Arm** to set specific arming time periods.



Note

After checking these two functions, you can set the arming time period while adding an item, and the arming will be performed within the set time period. Otherwise, the arming will be performed all day long.

Example

If you check **Blocklist Time Period Arming** and set the arming time period between 8 AM and 9 AM, the arming would be performed between the set time period. If you don't check **Blocklist Time Period Arming**, the arming would be performed all day long by default even though you set the time period while adding the item.

4. Add arming data.

- Batch Import**
- a. Download the import template and fill in relevant information.
 - b. Click **Import** to select the file with the relevant information.
 - c. Click **Import**.

- Manually Add**
- a. Select **Arming Type**.
 - b. Click **Add**.
 - c. Enter **License Plate Number**, and set the specific date and time.
 - d. Click **OK**.

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

- Search Data** Click **Search** after selecting the arming type or entering the license plate number to view relevant data.

- Edit Data** Check the item to be edited and click **Edit** to edit this item.

- Delete Data** Check the item to be deleted and click **Delete** to delete this item.

- Export Data** Check the item to be exported and click **Export** to export the item to the designated path.

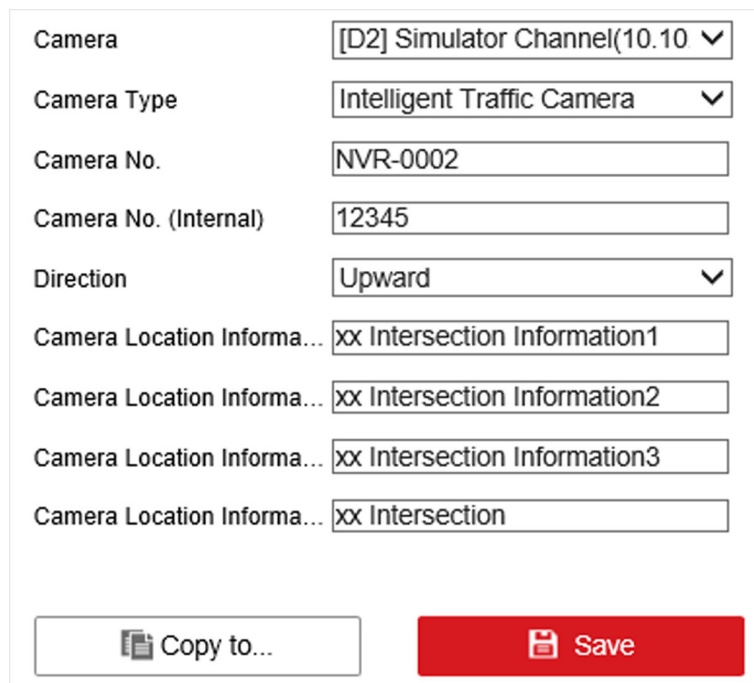
4.2 Set Event Parameters

4.2.1 Set Camera Parameters

You can set camera parameters for easy management.

Steps

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



Camera	[D2] Simulator Channel(10.10 ▾)
Camera Type	Intelligent Traffic Camera ▾
Camera No.	NVR-0002
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

 Copy to...
 Save

Figure 4-1 Set Camera Parameters

2. Select a camera.
3. Select **Camera Type**.

Note

The camera types vary with different models. The actual device prevails.

- **Camera for Video Surveillance:** Terminal server won't receive capture pictures.
- **Intelligent Traffic Camera:** Terminal server will receive capture pictures.

4. Set **Camera No.**, **Camera No. (Internal)**, and **Camera Location Information**.
5. Select **Direction** according to the vehicle passing direction.
6. **Optional:** Click **Copy to...** to copy the settings to other channels.
7. Click **Save**.

4.2.2 Set Violation Dictionary

Violation dictionary defines corresponding codes of violation types, and it is convenient for violation recognition.

Steps

1. Go to **Param Config → Dictionary Settings** .
2. Select a violation type.
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 data and click **Delete** to delete the data.



Note

The default data in the dictionary cannot be deleted.

Reset Click **Reset** to restore the dictionary to the factory settings, and all the custom data will be cleared.

Chapter 5 Data Management

5.1 View Real-Time Data

The device supports viewing captured violation information in real time.

Steps

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

View the vehicle violation detailed information

Check the data row, and the left side of the interface will display the vehicle violation detailed information.

View the vehicle violation picture information

Click **Picture** to view the vehicle violation picture information.

5.2 Search Data

You can search the traffic data of the connected cameras by searching data.

Steps

1. Click **Data Search** → **Traffic Data Search**.
2. Set **Start Time** and **End Time**.



Note

The time span between the start time and the end time cannot exceed 7 days.

3. Set the search conditions.
4. Click **Search**.
The searched result will be displayed.
5. Click **Details** after the data to view detailed information, pictures, video clips, etc.
6. **Optional:** After the data has been searched, click **Export** to export the selected data information to the set path.



Note

Make sure the IP of the camera has been added as a trusted site before exporting the data.

5.3 Enable Traffic Parameters Statistics

After enabling the traffic parameters statistics, the device will receive and store the traffic statistics of the camera.

Steps

1. Go to **Param Config → Advanced Settings → Other Settings → Traffic Parameters Statistics** .
2. Check **Traffic Parameter Statistics**.
3. Click **Save**.

5.4 View Traffic Statistics

You can view the traffic statistics of the specific time period via data search.

Steps

1. Go to **Data Search → Traffic Parameters Statistics** .
2. Set **Start Time** and **End Time**.
3. Select **Statistics Cycle** according to the actual needs.
4. Select a camera.
5. Click **Statistics**.
6. **Optional:** After the data has been searched, click **Export** to export the selected data information to the set path.

5.5 Back up Data

5.5.1 Back up 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 data export rule.
 - 1) Go to **Param Config → Backup Settings → Web Backup** .
 - 2) Enter the name, saving path, and other information of the picture and video.



Note

After the random number digits have been set, 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

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

5.5.2 Back up to USB

The device supports automatically backing 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. Enable USB backup.
4. Select **Backup Period** and **Start Time**.
 - **Real-Time Backup**: Automatically back up the data only once after the data have been saved at the set time.
 - **Backup Every Day**: Automatically back up the data once a day at the set time.
5. Select **Data Type** to backup.
6. Enter the picture backup naming rule and saving path.
7. Click **Save**.

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

Chapter 6 Live View and Local Configuration

6.1 Live View

6.1.1 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.

6.1.2 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 page and view the camera live view of all pages.

6.1.3 Select Stream Type

The device supports the dual-stream technology, including a main stream and a sub-stream. The main stream stands for a high-resolution and high bit rate stream, mainly used for storing

recordings. The sub-stream stands for a low-resolution and low bit rate stream, mainly used for bandwidth-saving network transmission.

Click  /  in the channel list to select the stream type.

6.1.4 Capture Manually

Capture live view pictures and save them to your computer.

Steps

1. Click **Live View**.
2. Double click the channel name on the left to enable live view.
3. Click .
4. Name and save the captured pictures.



Note

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

6.1.5 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.

6.1.6 Enable/Disable Audio

Enable the audio if necessary after relevant configuration of a connected audio input device.

Click  to enable and adjust the audio. Click the icon again to mute the audio.

6.1.7 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.

6.1.8 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.

6.2 PTZ Control

6.2.1 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 device supports power-down memory. After PTZ device suddenly loses power or reboots, it can automatically go back to the former position.

Table 6-1 Buttons Description

Icon	Description	Icon	Description
	Direction buttons		Auto-scan button
	Zoom -		Zoom +
	Focus +		Focus -
	Iris +		Iris -
	Display the PTZ control panel		Hide the PTZ control panel
	Control the PTZ speed		Auxiliary focus
	Menu		/

Note

Other functions are reserved.

6.2.2 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 .

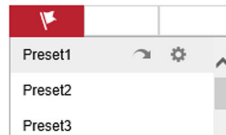


Figure 6-1 Set Preset

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.

6.3 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 6-2 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 7 Network Configuration

7.1 Dial

Set the dial-up parameters if you want to connect the device to the network via a SIM card.

Before You Start

The device has a dial-up module and a SIM card has been installed.

Steps



Note

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

1. Go to **Param Config → Network-Advanced Settings → Wireless Communication Configuration** .

☒ Enable	
APN	
Dial Number	
User Name	
Password	
Security Mode	AUTO ▼
Network Mode	Auto-Switch ▼
MTU	0
Dial-up Mode	Self-adaptive ▼

Figure 7-1 Set Dial-up Parameters

2. Check **Enable**.
3. Set dial-up parameters.
 - When you connect the device to the private network, set the dial number, user name, password and APN information according to the SIM card information.
 - When you connect the device to the normal network, you do not need to set the dial-up parameters.
4. Select **Security Mode** and **Network Mode** according to the actual needs.

Auto-Switch

The device will switch the network mode automatically after connected to the Internet.

3G Only/4G Only

Connecting the device via 3G/4G.

5. Set **MTU**.



Note

The MTU is the maximum payload length for a particular transmission media.

6. Select **Dial-up Mode** according to the actual needs.

7. Click **Save**.

8. **Optional:** You can go to **Param Config → System Status → Server Status → Wireless Network Status** to view results.

7.2 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

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

ISUP platform ID	1
☒ Enable	
Version	v5.0
Server Address	0.0.0.0
Port	7660
Device ID	123456
Registration Status	Offline
Login Key	••••••

Figure 7-2 Connect to ISUP Platform

2. Select **ISUP platform ID**.

3. Check **Enable**.

4. Select **Version**.

5. Enter **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 is online, you can add or manage the device via the platform software. Refer to its corresponding manual for details.

7.3 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. Refer to "Set IP Address" for details.
- 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 7-3 Set DDNS

2. Check **Enable DDNS**.

3. Enter the server address and other information.

4. Click **Save**.

What to do next

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

7.4 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 finishing 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.

Server 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.
-

7.5 Set SNMP

Set the SNMP to obtain or receive exceptions or alarms that occur during the transmission.

Before You Start

Deploy the SNMP server and make sure corresponding parameters are set. Make sure the server can work normally.

Steps

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

SNMP v1/v2
☐ Enable SNMP v1c
☐ Enable SNMP v2c
Read SNMP Community
Write SNMP Community
Trap Address
Trap Port
Trap Community

SNMP v3
☐ Enable SNMP v3c
Security Name of Reading
Security Level
Authentication Algorithm ☒ MD5 ☐ SHA
The Authentication Code
Private Algorithm ☒ DES ☐ AES
Private Password
Safe Name of Writing
Security Level
Authentication Algorithm ☒ MD5 ☐ SHA
The Authentication Code
Private Algorithm ☒ DES ☐ AES
Private Password

Other configuration of SNMP
SNMP Port

Figure 7-4 Set SNMP

2. Check the SNMP version according to the protocol version of the SNMP server.

 Note

It is recommended to use **SNMP v3** in order to enhance the security level.

3. Click **Save**.

7.6 Set ONVIF

If you want to use the device as an ONVIF server, you should enable this function.

Steps

1. Go to **Param Config → Network → Advanced Settings-Integration Protocol** .
2. Enable ONVIF.
3. Click **Save**.

Chapter 8 Record and Playback

8.1 Set Storage Path

8.1.1 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**.

8.1.2 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** .

The screenshot shows the 'Data Upload Config' window with the 'Param Config' tab selected. The 'FTP' section is expanded, showing various configuration options. The 'Host Name' is 'FTP Uploading Server 1' and 'Enable' is 'Disabled'. The 'FTP' dropdown is set to 'Disable'. The 'FTP Server Address' is '127.0.0.1', 'FTP Port' is '21', 'FTP User Name' is 'admin', and 'FTP Password' is masked with dots. The 'Upload Historical Data', 'Upload Allowlist Data', 'Upload Blocklist Data', 'Upload by Time', 'Data Type', 'License Plate Color', and 'Upload No-Plate Data' are all set to 'Enable'. The 'Data Type' dropdown shows '86 Selected, Total 92'.

Host Name	Enable	Network Status	Real-time Data Time	History Data Time	Information
FTP Uploading Server 1	Disabled				

Param Config	
FTP	Disable
FTP Server Address	127.0.0.1
FTP Port	21
FTP User Name	admin
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 8-1 Set FTP

2. Select a FTP server.
3. Set FTP parameters.

- 1) Enable the FTP.
- 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 be uploaded due to network disconnection or congestion. After this function has been enabled, historical data will be uploaded again.

Upload Allowlist Data

Upload the information of vehicles that are set in the allowlist through **Param Config → Advance Settings → Vehicle Arming**.

Upload Blocklist Data

Upload the information of vehicles that are set in the blocklist through **Param Config → Advance Settings → Vehicle Arming**.

Upload by Time

After this function has been enabled, data will be uploaded within the time period between the set uploading start time and the set uploading end time.

Upload No-Plate Data

Upload data of vehicles without license plates to the FTP server.

5. Select **License Plate Color** and **Data Type**.
6. Edit other relevant parameters according to the actual needs.
7. Click **Data Upload Settings** to set relevant parameters.

Upload Mode: Data Retransmission

Start Time: 2022-02-15 00:00:00

End Time: 2022-02-15 23:59:59

Data Type: All

Data Retransmission: Turn the status of the history data into the To Be Uploaded status, and upload the history data only once.

OK Cancel

Figure 8-2 Set Data Upload

- 1) Select **Upload Mode**.

Data Retransmission

Turn the status of the history data into the To Be Uploaded status, and upload the history data only once.

History Data Priority

Upload the history data in the To Be Uploaded first.

Disable

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

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

8. Optional: Repeat the above steps to set another FTP.

9. Click **Save**.

8.1.3 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	0.0.0.0
Port	8000
Cloud Storage Server Parameters	
Protocol Version	V1.0
Central Management Port	6120
User Name	
Password	
Storage Pool ID	0
	

Figure 8-3 Set Cloud Storage

2. Select **Cloud Storage**.
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

The 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**.

8.2 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**.

8.3 Record

8.3.1 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 ▼ Delete Delete All Advanced

Mon. 0 2 4 6 8 10 12 14 16 18 20 22 24

Tues. 0 2 4 6 8 10 12 14 16 18 20 22 24

Wed. 0 2 4 6 8 10 12 14 16 18 20 22 24

Thur. 0 2 4 6 8 10 12 14 16 18 20 22 24

Fri. 0 2 4 6 8 10 12 14 16 18 20 22 24

Sat. 0 2 4 6 8 10 12 14 16 18 20 22 24

Sun. 0 2 4 6 8 10 12 14 16 18 20 22 24

Copy to... Save

■ CMR ■ ALARM

Figure 8-4 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.

8.3.2 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 ▼ ✕ Delete 🗑️ Delete All Advanced

Mon. 0 2 4 6 8 10 12 14 16 18 20 22 24

Tues. 0 2 4 6 8 10 12 14 16 18 20 22 24

Wed. 0 2 4 6 8 10 12 14 16 18 20 22 24

Thur. 0 2 4 6 8 10 12 14 16 18 20 22 24

Fri. 0 2 4 6 8 10 12 14 16 18 20 22 24

Sat. 0 2 4 6 8 10 12 14 16 18 20 22 24

Sun. 0 2 4 6 8 10 12 14 16 18 20 22 24

Legend: ■ CMR ■ ALARM

📄 Copy to... 💾 Save

Figure 8-5 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.

8.4 Play Back Video

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

Steps

1. Click **Playback**.
2. Select a 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.
5. **Optional:** You can also do the following operations.

	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.
	Reversed.		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.

8.5 Backup

8.5.1 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** .

8.5.2 Back up Clipped Video

Clip videos and save them to a local path.

Steps

1. Click **Playback**.
2. Select a 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. Go to **Param Config** → **Local** to view the saving path of video clips.

Chapter 9 Encoding and Display

9.1 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. Select a camera.
3. 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.

4. Optional: Click **Copy to** to copy the settings to other channels.

5. Click **Save**.

9.2 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 the parameters to obtain clear images.

Brightness

The brightness of the image.

Contrast

The contrast of the image. Set it to adjust the levels and permeability of the image.

Saturation

The colorfulness of the image color.

Hue

Select the range to adapt to the display.

4. Optional: Click **Restore Default Settings** to restore parameters to the default status.

9.3 Set OSD

You can customize OSD information on the live view.

Steps



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

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 10 Alarm Configuration

10.1 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**.

10.2 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. IP Address

Default Status Triggering Status

Delay Alarm Name

Alarm Status (cannot copy)

Arming Schedule

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon.													
Tues.													
Wed.													
Thur.													
Fri.													
Sat.													
Sun.													

Figure 10-1 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**.

10.3 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.

Vehicle Blocklist

When vehicles in blocklist detected, alarm will be triggered.

Vehicle Allowlist

When vehicles in allowlist detected, alarm will be triggered.

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

4. Click **Save**.

10.4 Set Record Schedule

Set the valid time of the device tasks.

Steps

1. Click on the time bar and drag the mouse to select the time period.
2. 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.

3. **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.

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

10.5 Set Holiday

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

Steps

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

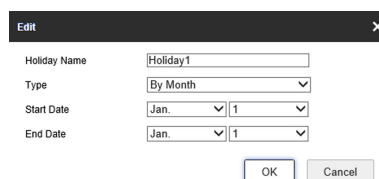


Figure 10-2 Set Holiday

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**.

10.6 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 11 Safety Management

11.1 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 recommended to 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. Set the user name, password and other information in the popup window.
4. Click **OK**.
5. **Optional:** You can also do the following operations.

Delete the User Select the added user and click **Delete** to delete the user.

Edit the User Information Select the added user and click **Edit** to edit the user information.

11.2 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/Region, Domain Name/IP, Password**, 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 **Setup** to import the certificate to the device.
- Select **Signed certificate is available, start the installation directly..** Click **Browse** to select the certificate and click **Setup** to import the certificate to the device.

7. Click **Save**.

11.3 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/Region, Domain Name/IP, Effective Period**, and other parameters.
5. Click **OK**.
6. Click **Save**.

11.4 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**.

11.5 Set Session Expired Time

If you log out of the device or the device is disconnected, and then log in to the device within the set session expired time, you will enter into the page which you logged out from the last time automatically.

Steps

1. Go to **Param Config → System → Security → Security Enhancement** .
2. Enter **Session Expired Time**.
3. Click **Save**.

Chapter 12 Maintenance

12.1 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.** It is recommended to reserve the default value.

Device Status

Go to **Param Config → System Status** to view the server status and other statuses.

12.2 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.

12.3 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.

12.4 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 → Reboot** .
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 when no HDD is detected.

12.5 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**.

12.6 Restore Database

When an exception occurs, you can restore the database if you have backed up the database before.

Before You Start

Make sure you have backed up the database before.

Steps

1. Go to **Param Config → System → System Maintenance → Upgrade & Maintenance → Restore Database** .
2. Click **Restore**.
3. Click **OK**.

12.7 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 12-1 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**.

12.8 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**.

12.9 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.

12.10 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**.

12.11 Set DST

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

Steps

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

12.12 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**.

12.13 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.

12.14 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.

12.15 Set Working Mode

You can set the device under the 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 12-2 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 under 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. Enter the name and No. of the cabinet door.
7. Select **Positioning Module** according to the connected positioning module type of the device.
8. Click **Save**.
9. **Optional:** Click **Data Search** and select search conditions to search relevant violation recordings.

12.16 Reserved Parameters

The reserved parameters are for technical personnel debugging only.

Appendix A. Communication Matrix and Device Command

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

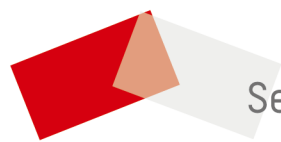


Figure A-1 Communication Matrix

Scan the QR code below to get the device command.



Figure A-2 Device Command



See Far, Go Further