



Terminal Server

User Manual

© 2019 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

This Manual is the property of Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as “Hikvision”), and it cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise expressly stated herein, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual, any information contained herein.

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/en/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks Acknowledgement

- **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.

LEGAL 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 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 INSPECTION, 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 LATER 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
 NOTE	Provides additional information to emphasize or supplement important points of the main text.
 WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

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	<ul style="list-style-type: none"> ● 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. ● DO NOT directly touch exposed contacts and components once the device is powered up to avoid electric shock. ● 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. ● DO NOT block the power supply equipment to plug and unplug conveniently. ● Make sure the power supply has been disconnected if the power adapter is idle. ● Make sure the device is connected to the ground firmly.

Transportation, Use, and Storage	<ul style="list-style-type: none"> ● 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. ● Avoid lightning strike for device installation. Install a lightning arrester if necessary. ● Keep the device away from magnetic interference. ● Avoid device installation on vibratory surface or places, and avoid equipment installation on vibratory surface or places subject to shock (ignorance 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.
Maintenance	<ul style="list-style-type: none"> ● 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 is abnormal, contact the store you purchased it or the nearest service center. DO NOT disassemble or modify the device in any way (For the problems caused by unauthorized modification or maintenance, the company shall not take any responsibility). ● Keep all wrappers after unpacking them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage to the device and the company shall not take any responsibility.
Network	<ul style="list-style-type: none"> ● 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. Please contact us when the device might exist network security risks. ● Please understand that you have the responsibility to configure all the passwords and other security settings about the device, and keep your user name and password.
Data	DO NOT disconnect the power during formatting, uploading, and downloading. Or files may be damaged.

Table of Contents

Chapter 1 Introduction	8
1.1 Product Introduction	8
1.2 Key Feature.....	8
1.3 System Requirement.....	8
1.4 Appearance	9
Chapter 2 Getting Started.....	11
2.1 Start Up and Shut Down	11
2.1.1 Start Up	11
2.1.2 Shut Down	11
2.1.3 Reboot.....	11
2.2 Set Admin Password	11
Chapter 3 Configure Network.....	13
3.1 Configure External Network.....	13
3.2 Configure Internal Network	14
3.3 Configure DDNS	14
3.4 Configure PPPoE	15
3.5 Configure Static Router.....	16
3.6 Configure Port	17
3.7 Configure HTTPS.....	18
3.8 Configure Security Service	19
Chapter 4 Live View	20
4.1 Add IP Camera	20
4.1.1 Add IP Camera Manually.....	20
4.1.2 Add IP Camera Quickly.....	20
4.2 Configure Display Settings	20
4.3 Configure Local Parameters	21
4.4 Live View Operations	22
4.5 Playback	24
Chapter 5 Configure Data	26
5.1 Configure Dictionary.....	26
5.1.1 Add Traffic Violation.....	26
5.1.2 Add Evidence Capture	26
5.2 Configure Blocklist and Allowlist	26
5.2.1 Add List.....	26
5.2.2 Delete List	27
5.2.3 Search List.....	27
5.2.4 Export/Import List.....	27
5.3 Configure Segment Speed Detection	28
5.4 Configure Camera Matching	29
5.5 Configure Face Evidence	30
Chapter 6 Configure Camera.....	32

6.1 Configure OSD	32
6.2 Configure Text Overlay.....	32
6.3 Configure Camera Parameter.....	32
6.4 Configure Picture Composition	34
6.5 Configure Composite Overlay	34
6.6 Configure Interaction.....	34
6.7 Configure Other Traffic Settings	35
Chapter 7 Configure Record and Capture	37
7.1 Configure Format HDD.....	37
7.2 Configure Picture Quota	37
7.3 Configure HDD Detection.....	38
7.3.1 S.M.A.R.T Settings.....	38
7.3.2 Bad Sector Detection	38
7.4 Configure Video Parameter.....	39
7.5 Configure Holiday	39
7.6 Configure Record Schedule	40
7.7 Configure Manual Record	42
7.8 Play Back	42
7.9 Configure Data Search	42
7.9.1 Traffic Data Search	42
7.9.2 Traffic Parameters Statistics	43
7.9.3 Real-Time Data	43
Chapter 8 Device Parameters	44
8.1 Device Information	44
8.2 Time Settings.....	44
8.3 DST Settings.....	44
Chapter 9 Serial Port Settings.....	46
9.1 RS-232 Serial Port	46
9.2 RS-485 Serial Port	46
Chapter 10 Configure Backup	48
10.1 Configure USB Backup	48
10.2 Configure Web Backup.....	48
Chapter 11 Uploading Data	50
11.1 Configure Host.....	50
11.2 Configure FTP	51
11.3 Configure Data Uploading.....	52
Chapter 12 Configure Alarm	54
12.1 Alarm Input Settings	54
12.2 Alarm Output.....	55
12.3 Linkage Action	55
12.4 Alarm Exception	56
Chapter 13 Status Information	57
13.1 Server Status	57

13.2 Camera Status	57
Chapter 14 Other Settings	59
14.1 User Management	59
14.1.1 Add a User	59
14.1.2 Edit a User	60
14.1.3 Delete a User	60
14.2 Exception	60
14.3 Maintenance	61
14.3.1 Reboot the Device.....	61
14.3.2 Default Settings.....	62
14.3.3 Restore Database	62
14.3.4 Export/Import Configuration File	62
14.3.5 Remote Upgrade	63

Chapter 1 Introduction

1.1 Product Introduction

Terminal server provides multiply features, including video management, traffic data management, video and audio decoding, picture processing, network transmission, etc. It integrates network ports and fiber ports, effectively meets the demands of distributed storage and accessing to security management platform. It is widely applied in checkpoint, Intersection Violation System, traffic security system, etc.

1.2 Key Feature

- IP camera is connectable.
- Easy-to-dismounting design makes HDD convenient to maintenance.
- Low consumption and lower heat generation.
- Supports GPS time synchronization.
- Supports operation via Web.
- Supports audio alarm and alarm uploading.
- Supports multiple text overlay and picture composition modes.

1.3 System Requirement

Web Browser	Operating System
Internet Explorer 8.0 and above version	Microsoft Windows XP SP1 and above version/Win 7/Win 8/Win 10 (32-bit or 64-bit)
Mozilla Firefox 30-41 version/Google Chrome 31.0-36.0.1985.143	Microsoft Windows XP SP1 and above version/Win 7/Win 8/Win 10 (32-bit only)

1.4 Appearance

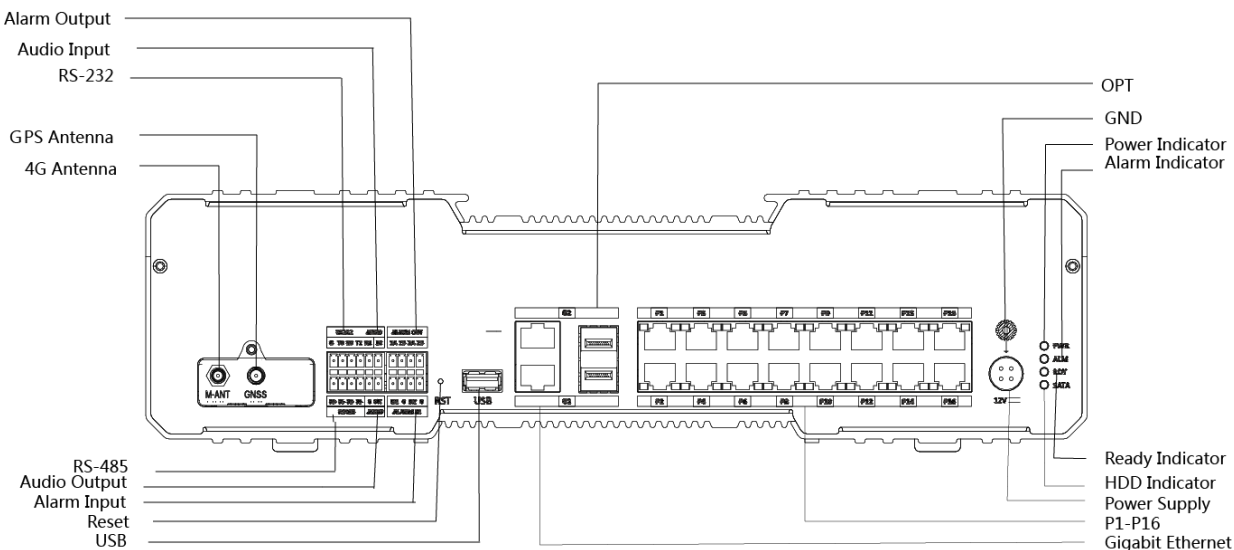


Figure 1-1 Appearance

Table 1-1 Panel Description

Name	Description
Power Indicator	The indicator will be green when the server is powered on.
Alarm Indicator	The indicator will be green when the server triggers alarm.
HDD Indicator	The indicator will be flashing green when the HDD is reading or writing.
Ready Indicator	The indicator will be solid green when the sever is ready.
Power Supply	Power Supply
GND	Ground
P1-P16 (100/1000M)	Gigabit Ethernet is to connect camera by P1-P16 internal network.
Gigabit Ethernet(100/1000M)	G1 is in the same network with P1-P16/P1-P8/P1-P4, optical multiplexing with OPT. G2 is to upload data to platform by external network, independent of G1.

RS-485	RS-485 half-duplex interface.
RS-232	RS-232.
Audio input/output	Audio input/output.
Alarm input/output	Alarm input/output.
USB	USB 3.0.
OPT	Fiber interface of SFP standard.
Reset	Long press for 5 seconds to restore default parameters and reboot.
GPS Antenna	GPS Antenna
4G Antenna	4G Antenna

 **NOTE**

Panel may vary in different models, please refer to actual terminal server.

Chapter 2 Getting Started

2.1 Start Up and Shut Down

Purpose:

Proper startup and shutdown procedures are crucial to expanding the life of the device.

2.1.1 Start Up

Before you start:

- Fix the device in an equipment cabinet.
- Ensure the device is properly grounded.
- Plug the network cable

Plug the power supply to start up.



Make sure the power supply is plugged into an electrical outlet. It is highly recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device.

2.1.2 Shut Down

Unplug the power supply to shut down.

2.1.3 Reboot

For detailed steps, please refer to Reboot the Device.

2.2 Set Admin Password

Purpose:

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. You can also activate the device via Web Browser, SADP or Client Software.

Before you start:

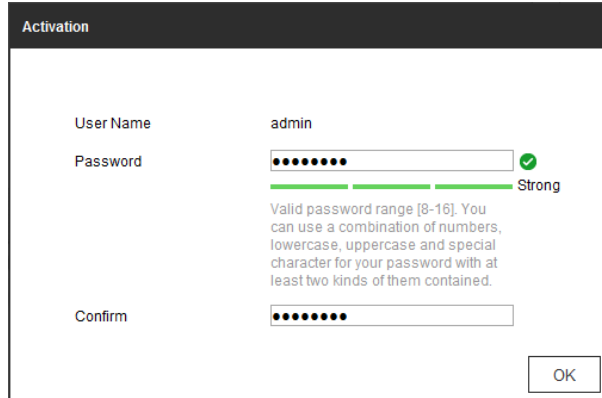
Set the IP address of your computer. Make sure the device is in the same network segment with your computer.

 **NOTE**

- 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.

Step 1 Enter device IP address in address bar of the browser and press **Enter**. Thus the activation interface pops up.

Step 2 Enter the **Admin Password** and **Confirm Password**.



The screenshot shows a web browser window titled "Activation". It contains three input fields: "User Name" with the value "admin", "Password" with a masked field (dots) and a green checkmark, and "Confirm" with a masked field (dots). Below the password field is a strength indicator showing a green bar and the word "Strong". A text box below the strength indicator reads: "Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained." An "OK" button is located at the bottom right of the form.

Figure 2-1 Set Admin Password

 **WARNING**

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.

Step 3 Click **OK** to set the admin password.

Step 4 After successful login, follow the prompt to install the plug-in.

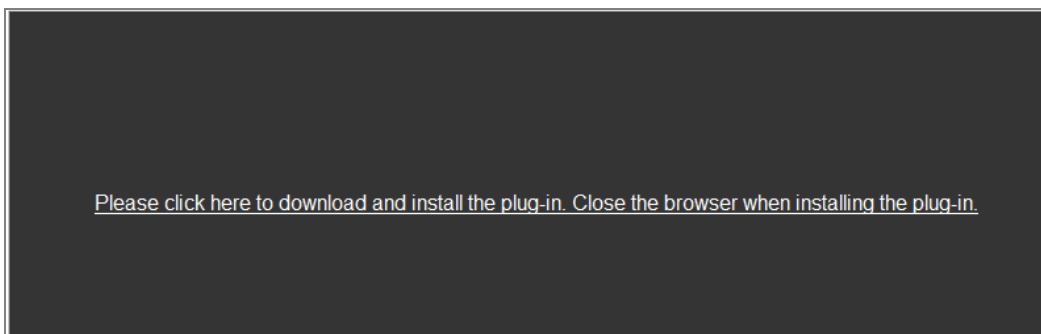


Figure 2-2 Installing Plug-in

Chapter 3 Configure Network

Purpose:

Guarantee the network connection between your computer and the device is correct, thus you can control the device remotely.

3.1 Configure External Network

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

External Network Settings		Internal Network Settings
NIC Type	AUTO	
	<input type="checkbox"/> Auto	
IPv4 Address	10.10.112.68	
IPv4 Subnet Mask	255.255.255.0	
IPv4 Default Gateway	10.10.112.254	
Physical Address	54:c4:15:f1:f0:8b	
MTU	1500	
DNS Server		
Preferred DNS Server		
Alternative DNS Server		
Save		

Figure 3-1 Basic Network Settings

Step 2 Go to **Param Config. > Network > Basic Settings > TCP/IP > External Network Settings.**

- 1) Select the **NIC Type** in the dropdown list.
- 2) Enter **IPv4 Address**, **IPv4 Subnet Mask**, **IPv4 Default Gateway**. Or you can select **DHCP** (Dynamic Host Configuration Protocol) to obtain IPv4 address dynamically.

Step 3 Set the DNS Server.

Enter the Preferred DNS Server and Alternate DNS Server.

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

3.2 Configure Internal Network

Purpose:

You can configure the IP address for the network interfaces. The default IP address is 192.1.0.64.

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

External Network Settings		Internal Network Settings
NIC Type	<input type="text" value="AUTO"/> <input type="checkbox"/> Auto	
IPv4 Address	<input type="text" value="192.1.0.64"/>	
IPv4 Subnet Mask	<input type="text" value="255.255.255.0"/>	
IPv4 Default Gateway	<input type="text"/>	
Physical Address	<input type="text" value="54:c4:15:f1:f0:8c"/>	
MTU	<input type="text" value="1500"/>	
DNS Server		
Preferred DNS Server	<input type="text"/>	
Alternative DNS Server	<input type="text"/>	

Save

Figure 3-2 Basic Network Settings

Step 2 Set the NIC Settings.

- 1) Select the **NIC Type** in the dropdown list.
- 2) Enter **IPv4 Address**, **IPv4 Subnet Mask**, **IPv4 Default Gateway**. Or you can select **DHCP** (Dynamic Host Configuration Protocol) to obtain IPv4 address dynamically.

Step 3 Set the DNS Server.

Enter the Preferred DNS Server and Alternate DNS Server.

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

3.3 Configure DDNS

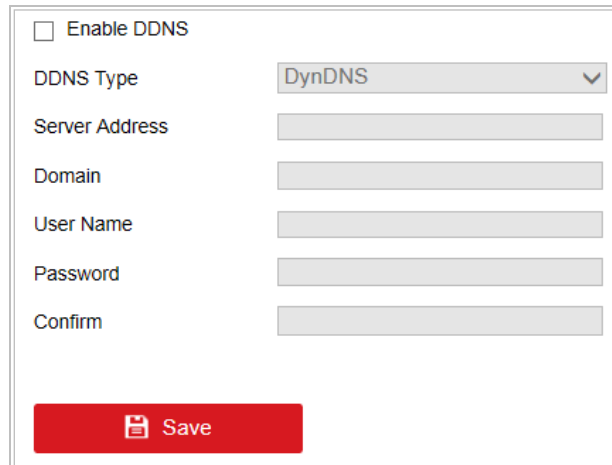
Purpose:

If your device access internet via a dynamic IP address, you may set Dynamic DNS (DDNS) to be used for network access.

Before you start:

Prior registration with your DDNS Provider is required before configuring the system to use DDNS.

Step 1 Go to **Param Config. > Network > Basic Settings > DDNS.**



The screenshot shows a configuration window for DDNS settings. At the top left, there is a checkbox labeled "Enable DDNS". Below it, the "DDNS Type" is set to "DynDNS" in a dropdown menu. There are five text input fields: "Server Address", "Domain", "User Name", "Password", and "Confirm". At the bottom of the window is a red button with a floppy disk icon and the text "Save".

Figure 3-3 DDNS Settings

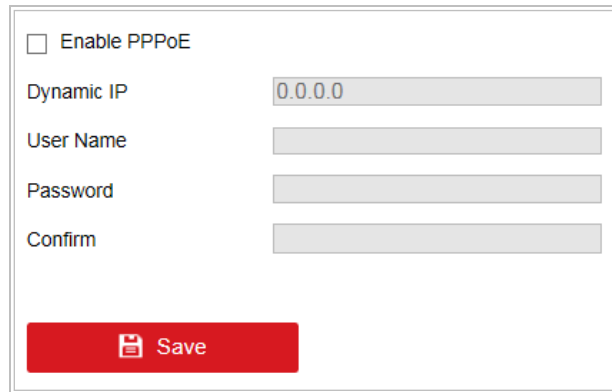
Step 2 Select Enable DDNS.

Step 3 Select the DDNS Type. Three different DDNS types are selectable: DynDNS, PeanutHull, and NO-IP.

- DDNS Type: DynDNS
 - 1) Enter **Server IP** for DynDNS server.
 - 2) In the **Domain** text field, input the domain obtained from the DynDNS website.
 - 3) Enter **User Name** and **Password** registered in the DynDNS website and **Confirm** the password.
 - 4) Click **Save** to save the settings.
- DDNS Type: PeanutHull
 - 1) Enter the **User Name** and **Password** obtained from the PeanutHull website and **Confirm** the password.
 - 2) Click **Save** to save the settings.
- DDNS Type: No-IP
 - 1) Enter **Server IP** address for NO-IP.
 - 2) In the **Domain** text field, enter the domain obtained from the NO-IP website (www.no-ip.com).
 - 3) Enter the **User Name** and **Password** registered in the NO-IP website and **Confirm** the password.
 - 4) Click **Save** to save the settings.

3.4 Configure PPPoE

Step 1 Go to **Param Config. > Network > Basic Settings > PPPoE.**



Enable PPPoE

Dynamic IP

User Name

Password

Confirm


 Save

Figure 3-4 PPPoE Settings

Step 2 Check **Enable PPPoE** to enable this feature.

Step 3 Enter user Name, password, and confirm password for PPPoE access.



The User Name and Password should be assigned by your ISP.



For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

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



A reboot is required for the settings to take effect.

3.5 Configure Static Router

Purpose:

To access different local networks via G1 and G2 network interface, you need to configure static router. If you do not specify a router, the device will visit network via the default G1 gateway.

Step 1 Go to **Param Config. > Network > Basic Settings > Static Router**.

Static Router							Add	Edit	Delete
<input type="checkbox"/>	No.	Target Netwo...	Subnet Mask	Gateway	Net Port	Status			

Figure 3-5 Static Router

Step 2 Click **Add**.

The dialog box titled "Static Router Configuration" contains the following fields:

- Enable
- Target Network Segment:
- Subnet Mask:
- Gateway:
- Net Port:

Buttons: OK, Cancel

Figure 3-6 Add

Step 3 Check **Enable**.

Step 4 Enter **Target Network Segment**, **Subnet Mask**, and **Gateway**.

- **Target Network Segment:** The network segment of target server.
- **Subnet Mask:** subnet mask of target network segment.
- **Gateway:** gateway for the selected network interface.

Step 5 Select **Net Port**.

Step 6 Click **OK** to save the settings.

3.6 Configure Port

Step 1 Go to **Param Config. > Network > Basic Settings > Port**.

The form contains the following fields:

- HTTP Port:
- RTSP Port:
- HTTPS Port:
- Server Port:

Buttons: Save

Figure 3-7 Network Port Settings

Step 2 Edit the HTTP Port, RTSP Port and HTTPS Port and Server Port.

- **RTSP Port:** Port for getting stream from IP camera.

- **HTTP Port:** Port for browser to access the device.
- **HTTPS Port:** Port for browser to access the device.
- **Server Port:** Port for other devices or platform to access the device.

Step 3 Click **Save** to save the settings.



Reboot the device to activate the new settings.

3.7 Configure HTTPS

Purpose:

HTTPS provides authentication of the web site and associated web server that one is communicating with, which protects against Man-in-the-middle attacks. Perform the following steps to set the port number of https.

Example:

If you set the port number as 443 and the IP address is 192.0.0.64, you may access the device by inputting `https://192.0.0.64:443` via the web browser.

Step 1 Go to **Param Config. > Network > Basic Settings > Port.**

Step 2 Create the self-signed certificate or authorized certificate.

Figure 3-8 HTTPS Settings

- **Option 1:** Create the self-signed certificate
 - 1) Select the radio of **Create Self-Signed Certificate.**
 - 2) Click the **Create** button to pop up the following dialog box.
 - 3) Enter the **Country/Region, Hostname/IP, Validity,** and other information.
 - 4) Click **OK** to create the certificate.
- **Option 2:** Install available certificate

- 1) Select the radio of **Signed certificate is available, Start the installation direction.**
 - 2) Click **Browse** and import the certificate to the device and install it.
- **Option 3:** Create the authorized certificate
 - 1) Select the radio of **Create the certificate request first and continue the installation.**
 - 2) Click the **Create** button to create the certificate request.
 - 3) Download the certificate request and submit it to the trusted certificate authority for signature.
 - 4) After receiving the signed valid certificate, import the certificate to the device and install it.

Step 3 There will be the certificate information after you successfully create and install the certificate.

Step 4 Check **Enable** to enable HTTPS function.

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

3.8 Configure Security Service

Purpose:

SSH (Secure Shell) as a security protocol ensures network security for the remote accessing and other network service. It prevents information leakage issues during remote management.

Step 1 Go to **Param Config. > System > Security > Security Service.**



Figure 3-9 Remote Access Settings

Step 2 Enable **SSH**.

Step 3 Click **Save** to enable it.

Chapter 4 Live View

4.1 Add IP Camera

Before you start:

The IP camera has accessed to terminal server.

4.1.1 Add IP Camera Manually

Add IP Camera Manually when terminal server password is different from IP camera.

Step 1 Go to **Param Config. > System > Camera Management > IP Camera.**

Step 2 Check required IP camera, and click **Add.**

Step 3 Set IP camera parameters.

Step 4 Click **OK** to save the settings.

4.1.2 Add IP Camera Quickly

IP Cameras can be quickly added when there are multiple IP cameras.

Step 1 Go to **Param Config. > System > Camera Management > IP Camera.**

Step 2 Check required IP camera, and click **Quick Add.**

Step 3 Set IP camera parameters.

Step 4 Click **OK** to save the settings.

4.2 Configure Display Settings

Purpose:

You can configure display settings menu.

Step 1 Go to **Param Config. > Image > Display Settings.**

Step 2 Select camera to configure.

Step 3 Configure brightness, contrast, saturation and hue according to need.

Step 4 Optionally, you can click "" and select cameras you want to copy above settings to.

Step 5 Click **OK** to save the settings.

4.3 Configure Local Parameters

Purpose:

The local settings refers to the parameters of the live view, record files and captured pictures. The record files and captured pictures are the ones you record and capture using the web browser and thus the saving paths of them are on the PC running the browser.

Step 1 Go to **Param Config. > Local.**

Live View Parameters			
Protocol Type	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP	
Stream Type	<input checked="" type="radio"/> Main Stream	<input type="radio"/> Sub Stream	
Play Performance	<input type="radio"/> Shortest Delay	<input checked="" type="radio"/> Balanced	<input type="radio"/> Fluent
Rules	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
Display POS Information	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
Image Size	<input checked="" type="radio"/> Auto-fill	<input type="radio"/> 4:3	<input type="radio"/> 16:9
Auto Start Live View	<input type="radio"/> Yes	<input checked="" type="radio"/> No	
Image Format	<input checked="" type="radio"/> JPEG	<input type="radio"/> BMP	
Record File			
Record File Size	<input type="radio"/> 256M	<input checked="" type="radio"/> 512M	<input type="radio"/> 1G
Save record files to	<input type="text" value="C:\Users\wangyuqian\MT Web\RecordFiles"/>	<input type="button" value="Browse"/>	
Save downloaded files when playb...	<input type="text" value="C:\Users\wangyuqian\MT Web\DownloadFiles"/>	<input type="button" value="Browse"/>	
Capture and Clip Settings			
Save snapshots in live view to	<input type="text" value="C:\Users\wangyuqian\MT Web\CaptureFiles"/>	<input type="button" value="Browse"/>	
Save snapshots when playback to	<input type="text" value="C:\Users\wangyuqian\MT Web\PlaybackPics"/>	<input type="button" value="Browse"/>	
Save clips when playback to	<input type="text" value="C:\Users\wangyuqian\MT Web\PlaybackFiles"/>	<input type="button" value="Browse"/>	

Figure 4-1 Local Settings Interface

Step 2 Configure the following settings:

- Protocol: TCP, UDP, and MULTICAST are selectable.
 - TCP: Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected.
 - UDP: Provides real-time audio and video streams.
 - MULTICAST: It is recommended to select MCAST type when using the Multicast function.
 - Play Performance: Set the play performance to Shortest Delay, Balanced, or Fluency.
 - Rules: It refers to the rules on your local browser, select enable or disable to display or not display the colored marks when event is triggered. E.g., enabled as the rules are, and

the face detection is enabled as well, when a face is detected, it will be marked with a green rectangle on the live view.

- Image Format: Choose the image format for picture capture.
- Record File Settings: Set the saving path of the recorded video files. Valid for the record files you recorded with the web browser.
 - Record File Size: Select the packed size of the manually recorded and downloaded video files to 256M, 512M or 1G. After the selection, the maximum record file size is the value you selected.
 - Save record files to: Set the saving path for the manually recorded video files.
 - Save downloaded files to: Set the saving path for the downloaded video files in playback mode.
- Capture and Clip Settings: Set the saving paths of the captured pictures and clipped video files. Valid for the pictures you capture with the web browser.
 - 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 of the captured pictures in playback mode.
 - Save clips to: Set the saving path of the clipped video files in playback mode.

**NOTE**

You can click **Browse** to change the directory for saving the clips and pictures, and click **Open** to open the set folder of clips and picture saving.

Step 3 Click **Save** to save the settings.

4.4 Live View Operations

Purpose:

The live view interface provides following functions:

- Display live view image of analog cameras and IP cameras.
- Adjust the speed dome image by rotating it to a certain view, and configuring zoom, focus, and iris parameters.
- Capture and recording.

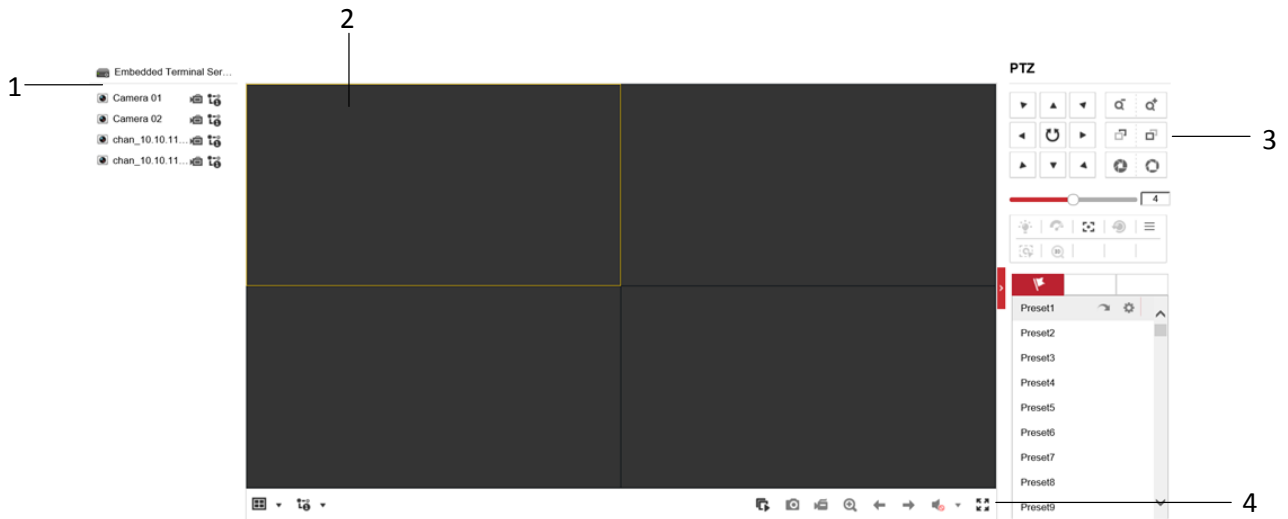










Figure 4-2 Live View

Table 4-1 Live View Description

No.	Name	Description
1	Camera List	List the analog cameras and added IP cameras.
2	Live View Window	Display the live view image of the cameras.
3	PTZ Control Panel	PTZ control panel for rotating speed dome.
4	Live View Control Bar	Live view control is provided.

Table 4-2 Live View Control Bar Description

Icon	Description	Icon	Description
	Split the live view window into 1 window, 4 windows or 9 windows.		Turn to previous page
	Start live view for all the cameras		Turn to next page.
	Capture pictures for the selected camera.	 / 	Disable / Enable audio.
	Start recording for all the cameras		

4.5 Playback

Purpose:

You can play back the record files of a specified day.

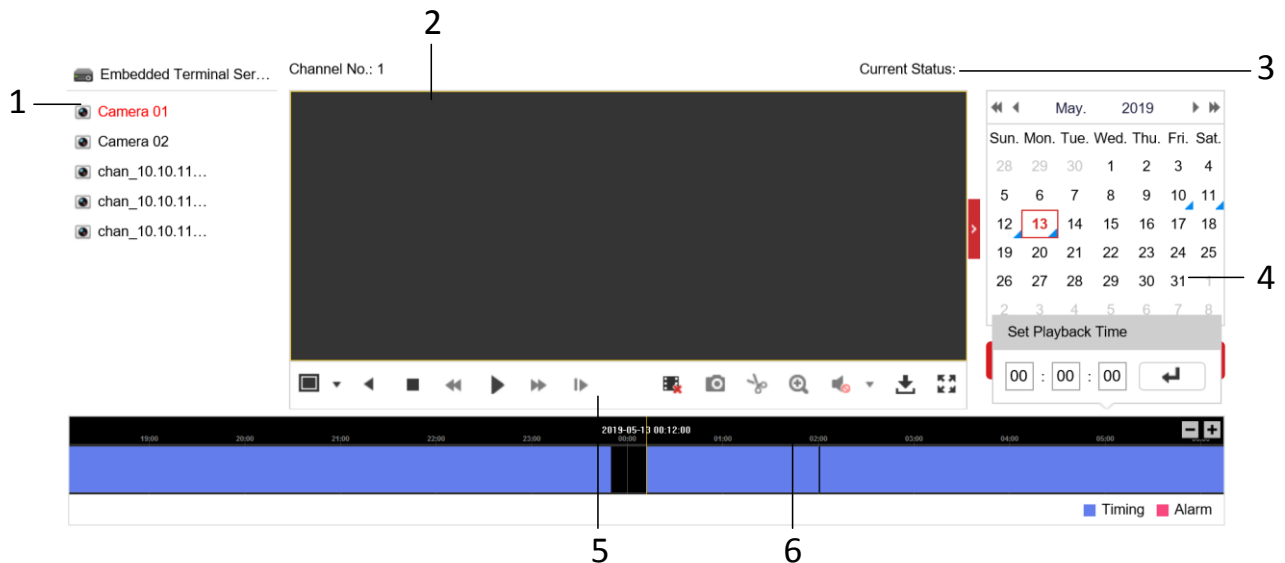













Figure 4-3 Playback Interface

Table 4-3 Playback Description

No.	Name	Description
1	Camera List	List the enabled analog cameras and added IP cameras.
2	Playback Window	Display the playback image.
3	Playback Status	Show the playback status, including playback camera No. and playback speed.
4	Calendar	Select a day to play back record files.
5	Playback Control Bar	Playback control is provided.
6	Time Bar	4 types of record file are marked with 4 colors.

Table 4-4 Playback Control Bar Description

Icon	Description	Icon	Description
	Split the playback window into 1 window, 4 windows or 9 windows.		Stop playback for all cameras.
	Start/pause playback for selected camera.		Capture pictures for the selected camera.
	Stop playback for selected camera.		Download record files.
	Slow forward.		Clip.
	Fast forward.		Audio.
	Start single frame playback.		

Chapter 5 Configure Data

5.1 Configure Dictionary

Purpose:

Configure dictionary parameters to recognize the violation vehicle acts.

5.1.1 Add Traffic Violation

Step 1 Go to **Param Config. >Dictionary Settings >Traffic Violation.**

Step 2 Click **Add.**

Step 3 Enter violation and violation code.

Step 4 Click **OK** to save the settings.

5.1.2 Add Evidence Capture

Step 1 Go to **Param Config. >Dictionary Settings > Evidence Capture.**

Step 2 Click **Add.**

Step 3 Enter evidence capture and evidence capture code.

Step 4 Click **OK** to save the settings.

5.2 Configure Blocklist and Allowlist

Purpose:

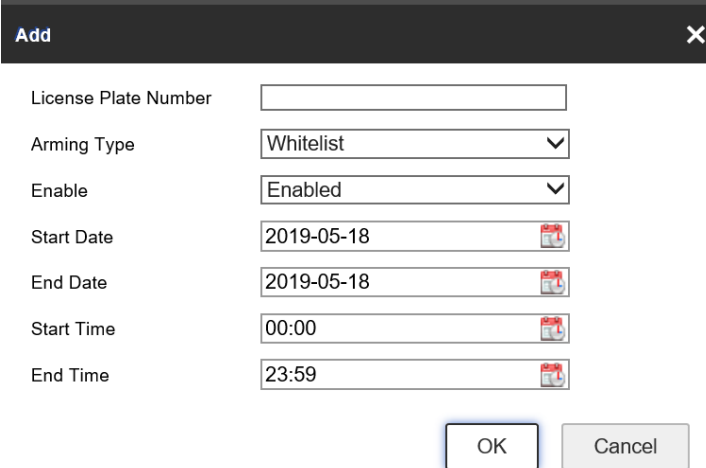
To manage special license plate numbers, you can add them into blocklist or allowlist.

Enter blocklist/allowlist interface.

5.2.1 Add List

Step 1 Go to **Param Config. > Advanced Settings > Vehicle Arming > Arming Management.**

Step 2 Click **Add.**



The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- License Plate Number: A text input field.
- Arming Type: A dropdown menu with "Whitelist" selected.
- Enable: A dropdown menu with "Enabled" selected.
- Start Date: A date picker showing "2019-05-18".
- End Date: A date picker showing "2019-05-18".
- Start Time: A time picker showing "00:00".
- End Time: A time picker showing "23:59".

At the bottom of the dialog are two buttons: "OK" and "Cancel".

Figure 5-1 Adding Blocklist/Allowlist

Step 3 Select **Arming Type** as **Blocklist** or **Allowlist**.

Step 4 Enter **License Plate No.**

Step 5 Select **Enable** as **Enabled** to enable the function.

Step 6 Set arming time.

Step 7 Click **OK** to add the license plate number.

5.2.2 Delete List

Step 1 Check the checkboxes of blocklists and allowlists to delete.

Step 2 Click **Delete** to delete them.

5.2.3 Search List

Purpose:

You can search added license plate numbers in blocklist/allowlist.

Step 1 Select **Arming Type** as **Blocklist** or **Allowlist** in drop-down list.

Step 2 Click **Search** to start searching.

5.2.4 Export/Import List

Export List

Purpose:

You can export all the license plate numbers in blocklist and allowlist to a local path.

Step 1 Click **Export**.

Step 2 Click **Browse** to select a local path and click **Export** to start export.



License plate numbers will be exported in an Excel file.

- Arming Type: 0 refers to Allowlist. 1 refers to Blocklist.
- Status: 0 refers to disabled. 1 refers to enabled.

Table 5-1 Exported Excel Content

License Plate Number	Arming Type	Status
HUA123	2	1

Import List

Purpose:

You can import license plate numbers to blocklist or allowlist in batch.

Step 3 Click **Download Import Template** to download the Excel template.

Step 4 Fill in license plate number, list type, and status in an Excel template.



- Arming Type can only be 1 or 2. 0: allowlist. 1: blocklist.
- Status can only be 0 or 1. 0: disabled. 1: enabled.

Step 5 Click **Import**.

Step 6 Click **Browse** to select a local path and click **Import** to start import.

5.3 Configure Segment Speed Detection

Purpose:

Calculate vehicle average speed within a road segment. There should be no fork with the road segment.

Step 1 Go to **Param Config. > Advanced Settings> Segment Speed Detection**.

Step 2 Check **Enable** to enable average speed detection feature.

Step 3 Click **Add**.

Parameter Configuration		Entrance/Exit Channel			
Enable Segment Speed...	<input checked="" type="checkbox"/>	Camera No.	Entrance Channel	Exit Channel	Deselect
Segment Name	<input type="text"/>	1(10.10.112.37)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Segment Length	<input type="text"/> (m)	2(10.10.112.37)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Segment Scene	Highway Mode <input type="button" value="v"/>				
Marked Speed Limit for L...	<input type="text"/> (km/h)				
Speed Limit for Large-Siz...	<input type="text"/> (km/h)				
Speed Limit for Large-Siz...	<input type="text"/> (km/h)				
Marked Speed Limit for S...	<input type="text"/> (km/h)				
Speed Limit for Small-Siz...	<input type="text"/> (km/h)				
Speed Limit for Small-Siz...	<input type="text"/> (km/h)				

Figure 5-2 Section Settings

Step 4 Check **Enable**.

Step 5 Configure section parameters and vehicle speeding parameters.

- **Segment Name:** Enter **Segment Name**.
- **Segment Length:** Enter **Segment Length** according to actuality.
- **Segment Scene:** Select **Segment Scene** as **Highway Mode** or **City Mode** according to actuality.
- **Entrance/ Exit Channel:** The selected channels must be traffic cameras.
- **Marked Speed Limit for Large-Sized Vehicle:** The actual speed limit value. Enter the value according to actuality.
- **Speed Limit for Large-Sized Vehicle:** The value cannot be smaller than Large-Size Vehicle Speeding Percentage.
- **Speed Limit for Large-Sized Vehicle Exception:** The value must be larger than both Large-Size Vehicle Speeding Percentage and Large-Size Vehicle Speed Limit.
- **Marked Speed Limit for Small-Sized Vehicle:** The actual speed limit value. Enter the value according to actuality.
- **Speed Limit for Small-Sized Vehicle:** The value cannot be smaller than Small-Size Vehicle Speeding Percentage.
- **Speed Limit for Small-Sized Vehicle Exception:** The value must be larger than both Small-Size Vehicle Speeding Percentage and Small -Size Vehicle Speed Limit.

Step 6 Click **OK**.

5.4 Configure Camera Matching

Purpose:

Compose the two picture of vehicles. Configure the following parameters according to your actual camera type.

Step 1 Go to **Param Config. > Advanced Settings > Camera Matching**.

Step 2 Check **Enable** to enable camera match.

Step 3 Click **Add**.

Camera Matching			
Parameter Configuration		Main/Sub Channel	
<input checked="" type="checkbox"/> Enable			
Linkage Action	<input type="text" value="Coil Linkage"/>		
Camera No.	Main Channel	Sub Channel	Deselect
1(10.10.112.37)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2(10.10.112.37)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 5-3 Camera Matching

Step 4 Check **Enable**.

Step 5 Select **Camera No.** to configure.

Step 6 Select **Main Channel** and **Sub-Channel**.

Step 7 Select **Linkage Action** according to selected main channel and sub-channel.

- **Coil Linkage:** One of main channel and sub-channel must be a panorama camera, the other is a capture camera. Device will collage the captured pictures of main channel and sub-channel.
- **Video Linkage:** Main channel and sub-channel must support license plate recognition feature. When the recognized license plate number of main channel and sub-channel matches, device will collage the captured pictures of main channel and sub-channel.

Step 8 Click **OK**.

5.5 Configure Face Evidence

Purpose:

Compose pictures of E-Police and checkpoint according to license plate recognition. It provides evidence of vehicle violation acts.



NOTE

Segment speed detection, camera matching and face evidence cannot be supported at the same time.

Step 1 Go to **Param Config. > Advanced Settings > Face Evidence**.

Step 2 Check **Face Evidence**.

Step 3 Check **Compose**, and configure parameters.

Face Evidence

Parameter Config Channel Linkage Real-Time Matching Status

Notice: You need to disable picture composition if you want to enable this function.

Face Evidence

Compose

3 Captured Pictures

4 Captured Pictures

Maximum Size of Picture(...)

Original Picture Zoom Mu... ▼

Matching Retrospect Tim...

Matching Delay Time (s)

Data Type

Figure 5-4 Camera Matching

- Matching Retrospect Time: Retrospect time from first E-Police picture, to match forward checkpoint pictures.
- Matching Delay Time: Delay time from first E-Police picture, to match checkpoint pictures.

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

Step 5 Go to Channel Linkage, add required linked groups.

Chapter 6 Configure Camera

6.1 Configure OSD


Purpose:

You can configure parameters of OSD (On Screen Display) menu.

Step 1 Go to **Param Config. > Image > OSD Settings.**

Step 2 Select camera to configure.

Step 3 Configure parameters according to your need, including **Camera Name, Display Name, Display Date, Display Week, Time Format, Date Format.**

Step 4 Optionally, you can click “” and select cameras you want to copy above settings to.

Step 5 Click **OK** to save the settings.

6.2 Configure Text Overlay

Purpose:

You can overlay 8 text contents onto the video.

Step 1 Go to **Param Config. > Image > OSD Settings.**

Step 2 Select camera to configure in **Select Camera** dropdown list.

Step 3 Enter contents in the text content.

Step 4 Check the checkbox of text content you want to display.

Step 5 Click **Save** to show the contents.

6.3 Configure Camera Parameter

Purpose:

You can configure camera parameter settings.

Step 1 Go to **Param Config. > System > Camera Management > Camera Parameter.**

Camera	<input type="text" value="[D1] chan(10.10.112.37)"/>
Camera Type	<input type="text" value="Intelligent Traffic Camera"/>
Camera No.	<input type="text" value="NVR-0001"/>
Camera No. (Internal)	<input type="text" value="1234"/>
Direction	<input type="text" value="Upward"/>
Camera Location Informa...	<input type="text" value="Camera Location Information 1"/>
Camera Location Informa...	<input type="text" value="Camera Location Information 2"/>
Camera Location Informa...	<input type="text" value="Camera Location Information 3"/>
Camera Location Informa...	<input type="text" value="Camera Location Information"/>

 Save

Figure 6-1 Monitoring Spot Information

Step 2 Select camera to configure in **Camera** dropdown list.

Step 3 Select **Camera Type** as **Camera for Video Security (No Capture)** or **Intelligent Traffic Camera**.

- **Camera for Video Security** : Terminal server stores camera video files. Camera picture files won't be stored.
- **Intelligent Traffic Camera**: Terminal server stores both camera video files and picture files.

Step 4 Enter **Camera No.** and **Camera No. (Internal)**.

- **Camera No.**: Used to distinguish traffic cameras from each other. Enter an exclusive No. for each camera. It only supports letter and number in 30 bytes.
- **Camera No. (internal)**: Used to distinguish traffic cameras in different checkpoints. Enter an exclusive No. for each camera. It only supports number no bigger than 4,294,967,295.

Step 5 Select **Direction** according to actual installation.

Step 6 Enter detailed information for camera in the four text contents, including Camera Location Information 1, Camera Location Information 2, Camera Location Information 3, and Camera Location Information 4.

 **NOTE**

- Camera Location Information 1: No more than 120 characters.
- Camera Location Information 2: No more than 40 characters.
- Camera Location Information 3: No more than 30 characters.
- Camera Location Information 4: No more than 120 characters.

Step 7 Click **Save** to save the settings.

6.4 Configure Picture Composition

Purpose:

Configure image collage layout and other parameters.

Step 1 Go to **Param Config. > Picture Settings > Picture Composition.**

Step 2 Select camera to configure.

Step 3 Set Compose as **Enable.**

Step 4 Select layout for **2 Captured Pictures** and **3 Captured Pictures.**

Step 5 Configure picture Composition parameters.

Step 6 Click **Save** to save the settings.

6.5 Configure Composite Overlay

Purpose:

Overlay text on composite pictures.

Step 1 Go to **Param Config. >Picture Settings >Composite Overlay.**

Step 2 Select camera to configure.

Step 3 Select **Text Overlay Method.**

Step 4 Select **content.**

Step 5 Set text parameters including **Initial Top Margin, Initial Left Margin, Character Size, Font Color, Background Color, Space Number, and Position Percentage of Line Break.**

- **Initial Top Margin:** Text position from top margin.
- **Initial Left Margin:** Text position from left margin.
- **Position Percentage of Line Break:** Text will switch to next line when the percentage between text length and picture width reaches the set value.

Step 6 Click **Save** to save the settings.

6.6 Configure Interaction

Purpose:

Configure the Interaction Mode between terminal server and traffic cameras.

Step 1 Go to **Param Config. > System > Camera Management > Interaction Settings.**

The screenshot shows a configuration window with two dropdown menus. The first dropdown is labeled 'Camera' and has the selected value '[D2] Camera 01(10.99.107.31)'. The second dropdown is labeled 'Interaction Mode' and has the selected value 'Normal Mode'. Below the dropdowns are two buttons: a white button with a document icon and the text 'Copy to...' and a red button with a floppy disk icon and the text 'Save'.

Figure 6-2 Interaction Settings

Step 2 Select camera to configure in **Select Camera** dropdown list.

Step 3 Select Interaction Mode as **Normal Mode** or **Data Receiving Mode**. The default one is Normal Mode.

- **Normal Mode:** Device can record videos, live view, and receive pictures from the selected camera.
- **Data Receiving Mode:** Device can only receive pictures from the selected camera. Recording videos and live view are not supported.

Step 4 Click “▼” and select camera(s). Thus to configure the same parameters to selected camera(s).

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

6.7 Configure Other Traffic Settings

Purpose:

Configure other traffic settings for device.

Step 1 Go to **Param Config. > Advanced Settings > Other Settings**.

The screenshot shows a configuration window with several settings. The first four are dropdown menus: 'Traffic Camera Connectio...' set to 'Arming Mode', 'Arming Level' set to 'Level 1', 'Traffic Data Matching Str...' set to 'Single Channel Matching', and 'Camera Time Synchroniz...' set to 'Enable'. The next three are sliders with numeric input boxes: 'Pre-record (s)' set to 4, 'Post-record (s)' set to 6, and 'Longest Recording Time (s)' set to 60. The last two are text input fields: 'Cabinet Door Name' set to 'Equipment Cabinet Door' and 'Cabinet Door No.' set to '12345'. At the bottom is a red 'Save' button.

Figure 6-3 Other Settings

Step 2 Select **Traffic Camera Connection Mode**: as **Arming Mode** or **Listening Mode**. The default mode is **Arming Mode**.

- **Arming Mode**: Terminal server takes pictures from traffic cameras. Terminal server is the active device.
- **Listening Mode**: Traffic cameras upload pictures to terminal server. Terminal server is the passive device.

Step 3 Select **Arming Level**: as **Level 1**, **Level 2**, or **Level 3**. The default **Arming Level** is **Level 1**.

- **Level 1**: The terminal server has the highest priority to receive pictures from connected traffic cameras. Ensures no picture loss.
- **Level 2**: Two terminal servers can receive pictures from one traffic camera. They are equal to cameras.
- **Level 3**: Three terminal servers can receive pictures from one traffic camera. They are equal to cameras.

Step 4 Select **Camera Time Synchronization** as **Enable** or **Disable**.

Enable: Terminal server synchronizes the connected traffic cameras' time.

Step 5 Drag the sliders to set **Pre-record (s)**, **Post-record (s)**, or **Longest Recording Time (s)**: for violation videos.

- **Pre-record (s)**: The time you set to record before the violation. For example, when a violation occurs at 10:00, if you set the pre-record time as 4 seconds, the camera records it at 9:59:56.
- **Post-record (s)**: The time you set to record after the violation. For example, when a violation ends at 11:00, if you set the post-record time as 6 seconds, it records till 11:00:06.
- **Longest Recording Time (s)**: The longest time for a violation video.



NOTE

When you search the violation pictures, you can view the violation video as while. In order to keep the violation video completeness, set the all-day record schedule for cameras.

Step 6 Enter **Cabinet Door Name** and **Cabinet Door No.** according to actual installation.

Step 7 Click **Save** to save the settings.

Chapter 7 Configure Record and Capture

7.1 Configure Format HDD

Purpose:

Initialize the HDD before you use it.



- HDD amount varies according to different models. You can refer to specification for details.
- Format HDD will cause HDD blocklist data lost. Export and save the blocklist before you format HDD, and import it after formatting.

Step 1 Go to **Param Config. > Storage > Storage Management > HDD Management.**

Step 2 Check the checkbox of **HDD** to format.

Step 3 Click **Format.**

Step 4 Click **OK** to save the settings.

HDD Management									Set	Format
<input type="checkbox"/>	HDD No.	Capacity	Free space	Status	Database Status	Type	Property	Progress		
<input type="checkbox"/>	1	2794.52GB	2067.00GB	Normal	Normal	Local	R/W			
<input type="checkbox"/>	2	2794.52GB	2786.00GB	Normal	Normal	Local	R/W			

Figure 7-1 HDD Management

7.2 Configure Picture Quota

Purpose:

You can set the maximum capacity for saving picture.

Step 1 Go to **Param Config. > Storage > Storage Management > Picture Quota.**

Total Disk Capacity (GB):

Used Capacity for Picture...

Picture Quota (GB)

Save

Figure 7-2 Advanced Settings

Step 2 Enter the **Picture Quota** in the text field. The other HDD capacity is for video files.

Step 3 Click **OK** to save the settings.

7.3 Configure HDD Detection

Purpose:

The device provides the HDD detection function such as the adopting of the S.M.A.R.T and the Bad Sector Detection technique. The S.M.A.R.T (Self-Monitoring, Analysis and Reporting Technology) is a monitoring system for HDD to detect and report on various indicators of reliability in the hopes of anticipating failures.

7.3.1 S.M.A.R.T Settings

Step 1 Go to **Param Config. > Storage > Storage Management > HDD Detection > S.M.A.R.T Detection.**

Step 2 Select the HDD to view its S.M.A.R.T information.

The related information of the S.M.A.R.T. is shown on the interface.

Step 3 Choose the **Self-Test Type** as **Short Test**, **Expanded Test** or the **Conveyance Test**.

Step 4 Click **Start** to start the S.M.A.R.T. HDD self-evaluation.

S.M.A.R.T Information							
ID	Attribute Name	Status	Flags	Threshold	Value	Worst	Raw Value

Figure 7-3 S.M.A.R.T Settings Interface

7.3.2 Bad Sector Detection

Step 1 Go to **Param Config. > Storage > Storage Management > HDD Detection > Bad Sector Test.**

Step 2 Select the **HDD No.** in the drop-down.

Step 3 Choose **Test Type** as **Full Detection** or **Key Area Detection**.

Step 4 Click **Start Detect** to start the detection. You can pause or cancel the detection.

7.4 Configure Video Parameter

Purpose:

You can define the parameters that affect the image quality, such as the transmission stream type, the resolution and so on.

Step 1 Go to **Param Config. > Video & Audio > Video.**

Camera	[A1] Camera 01	▼
Video Input Resolution	NO VIDEO	
Stream Type	Main Stream(Normal)	▼
Video Type	Video	▼
Resolution	352*240	▼
Bitrate Type	Variable Bitrate	▼
Image Quality	Low	▼
Frame Rate	Full Frame Rate	▼ fps
Max. Bitrate	512	Kbps
Video Encoding	H.264	▼

Figure 7-4 Video Settings

Step 2 Select the camera.

Step 3 Select stream to configure as **Main Stream (Normal)**, **Sub-stream**, or **Main Stream (Event)**.

- **Main Stream (Normal):** Stream for normal recording.
- **Sub-stream:** Stream for network transmission.
- **Main Stream (Event):** Stream for event recording.

Step 4 Configure Encoding Parameters. You can configure the stream type, resolution, and other parameters on your demand.

Step 5 Optionally, click “▼” and select cameras to copy the above parameters to.

Step 6 Click **OK** to save the settings.

7.5 Configure Holiday

Purpose:

You may want to have different recording schedule on holiday or special days. Follow the steps to specify holiday date.

Step 1 Go to **Param Config. > Storage > Advanced Settings > Holiday.**









Holiday Settings				The periods of holiday cannot be overlapped		
Enable	No.	Holiday Name	Type	Start Date	End Date	Edit
<input type="checkbox"/>	1	Holiday1	By Month	1.Jan	1.Jan	
<input type="checkbox"/>	2	Holiday2	By Month	1.Jan	1.Jan	
<input type="checkbox"/>	3	Holiday3	By Month	1.Jan	1.Jan	
<input type="checkbox"/>	4	Holiday4	By Month	1.Jan	1.Jan	
<input type="checkbox"/>	5	Holiday5	By Month	1.Jan	1.Jan	
<input type="checkbox"/>	6	Holiday6	By Month	1.Jan	1.Jan	
<input type="checkbox"/>	7	Holiday7	By Month	1.Jan	1.Jan	

Figure 7-5 Holiday Settings

Step 2 Click “” to edit the holiday.



NOTE

Up to 32 holidays can be configured.

Edit
✕

Holiday Name

Type

Start Date

End Date

Figure 7-6 Edit Holiday

Step 3 Edit the Holiday Name.

Step 4 Check the Enable Holiday checkbox.

Step 5 Select holiday Type as By Date, By Week or By Month.

Step 6 Enter Start Date and End Date.

Step 7 Click OK to save the settings.

7.6 Configure Record Schedule

Purpose:

Set the record schedule as timing recording or alarm triggered recording, and then the camera automatically starts/stops recording according to the configured schedule.

Step 1 Go to **Param Config. > Storage > Schedule Settings > Recording Schedule.**

Camera [A1] Camera 01

Enable

Timing Delete Delete All

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

■ Timing
■ Alarm

Figure 7-7 Recording Schedule Interface

Step 2 Check **Enable** to enable scheduled recording.

Step 3 Click **Advanced** to set the camera record parameters.


- **Pre-record:** The time you set to start recording before the scheduled time or the event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record at 9:59:55.
The Pre-record time can be configured as No Pre-record, 5s, 10s, 15s, 20s, 25s, 30s, or not limited.
- **Post-record:** The time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.
The Post-record time can be configured as 5s, 10s, 30s, 1 min, 2 min, 5 min or 10 min.
- **Stream Type:** Select the stream type for recording.

Step 4 Select a record type. The record type can be **Timing** or **Alarm**.

- **Timing**
The video will be recorded automatically according to the time of the schedule.
- **Alarm**
The video will be recorded when the alarm is triggered via the external alarm input channels.

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

7.7 Configure Manual Record

Go to **Live View**, click “” to start record.

7.8 Play Back

Purpose:











You can play back the record files of a specified day.

Step 1 Go to **Playback**.

Step 2 Select the camera, and file date.

Step 3 Click Search to play back the file.

Table 7-1 Playback Control Bar Description

Icon	Description	Icon	Description
	Split the playback window into 1 window, 4 windows or 9 windows.		Stop playback for all cameras.
	Start/pause playback for selected camera.		Capture pictures for the selected camera.
	Stop playback for selected camera.		Download record files.
	Slow forward.		Clip.
	Fast forward.		Enable/disable audio.

7.9 Configure Data Search

7.9.1 Traffic Data Search

Purpose:

You can search traffic data of cameras.

Step 1 Go to **Data Search > Traffic Data Search**.

Step 2 Set **Start Time** and **End Time**.



NOTE

There must be less than 7 days between start time and end time.


Step 3 Set search conditions.

Step 4 Click **Search** to view information.

Step 5 (Optional) Click **Details** to view details.

Step 6 (Optional) Click **Export** to export data information to specified directory.



If you use IE browser, before you export data first time, Click “” > **Internet Option** > **Security** > **Trusted Sites**, and click **Sites** to add this website to your trusted sites. Click **OK** and restart the browser.

7.9.2 Traffic Parameters Statistics

Purpose:

You can search traffic statistics to view traffic situation.

Step 1 Go to **Data Search** > **Traffic Parameters Statistics**.

Step 2 Set **Start Time** and **End Time**.

Step 3 Set statistics conditions.

Step 4 Click **Statistics** to view information.

Step 5 (Optional) Click **Export** to export data information to specified directory.

7.9.3 Real-Time Data

Go to **Real-Time Data** to view violation vehicle information.

Chapter 8 Device Parameters

8.1 Device Information

Purpose:

You can enter Device Information interface to view the basic information of device.

Go to **Param Config. > System > System Settings > Basic Information**, you can view the basic information.

8.2 Time Settings

Purpose:

You can synchronize the date and time of the device manually or automatically.

Step 1 Go to **Param Config. > System > System Settings > Time Settings**.

Step 2 Select **Time Zone** from the dropdown list.

Step 3 Select required synchronization mode.

- NTP Time Sync.
Enter Server Address, NTP Port and Interval.
- Manual Time Sync.
Enter the device time and set time. Or you can select **Sync. with computer time**.
- GPS Time Sync.
- SDK Time Sync.
Select remote host and set IP address.
- Ehome Time Sync.

8.3 DST Settings

Purpose:

DST (Daylight Saving Time) is the practice of advancing clocks during summer months by specified hours so that evening daylight lasts specified hours longer while sacrificing normal sunrise times.

Step 1 Go to **Param Config. > System > System Settings > DST**.

DST

Enable DST

Start Time Apr. First Sun. 02

End Time Oct. First Sun. 02

Bias Time 30min

Figure 8-1 DST Settings Interface

Step 2 Check **Enable DST**.

Step 3 Set **Start Time**, **End Time**, and **DST Bias**.

Step 4 Or you can manually check **Enable DST**, and then you choose the date of the DST period.

Chapter 9 Serial Port Settings

Purpose:

Configure RS-232 serial port and RS-485 serial port.

9.1 RS-232 Serial Port

Purpose:

Connect the RS-232 serial interface in device rear panel with the one on computer. Thus device can communicate with computer.

Step 1 Go to **Param Config. > System > System Settings > Serial Port.**

RS232						
No.	Baud Rate	Data Bit	Stop Bit	Verification	Flow Control	Control Mode
1	115200	8	1	None	None	Control Panel(By...
2	115200	8	1	None	None	Transparent Cha...

Figure 9-1 RS-232 Settings

Step 2 Configure the parameter, including **Baud Rate, Data Bit, Stop Bit, Verification, Flow Control** and **Control Mode.**



NOTE

Make sure the parameters are exactly the same with the computer parameters.

Step 3 Click **Save** to save the settings.

9.2 RS-485 Serial Port

Step 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
2	9600	8	2	None	None
3	9600	8	2	None	None
4	9600	8	2	None	None

Figure 9-2 RS-485 Settings

Step 2 Configure the parameter, including **Baud Rate, Data Bit, Stop Bit, Verification, Flow Control** and **Control Mode.**



NOTE

Make sure the parameters are exactly the same with the connected device.

Step 3 Click **Save** to save the settings.

Chapter 10 Configure Backup

10.1 Configure USB Backup

Purpose:

You can export data to USB backup device.

Before you start:

Plug a USB backup device into the USB interface in rear panel.

Step 1 Go to **Param Config. > Backup Settings > Local Backup > USB Backup Settings.**

Figure 10-1 USB Backup Settings

Step 2 Select **Enable USB Backup** as **Enable**.

Step 3 Set **Backup Period**.

- 1) Select **Backup Period** as **Real-Time Backup** or **Backup Every Day**. The recommend one is Real-time Backup.
 - Real-Time Backup: Export pictures and video files immediately to USB backup device, once terminal server receives any data.
 - Backup Every Day: Export last day's pictures and video files in every 0 a.m.
- 2) Set the **Backup Start Time** to export historical files.

Step 4 Select the **Data Type** to backup.

Step 5 Set **Saving Path and File Name**.

Step 6 Click **Save** to save the settings.

10.2 Configure Web Backup

Purpose:

In Traffic interface, you can export traffic information. And you can set the file name and directory for the backup files, including license plate pictures and traffic violation pictures and videos.

Step 1 Go to **Param Config. > Backup Settings > Web Backup Settings.**

Step 2 Edit the parameters.

Step 3 Click **Save** to save the settings.

Chapter 11 Uploading Data



NOTE

When gateways of G1 and G2 are configured, you should also configure static route when uploading data to platform or FTP.

11.1 Configure Host

Purpose:

Configure the Remote Host settings to upload data to Remote Host.

Step 1 Go to **Param Config. > Platform Settings > Remote Host.**

Remote Host 1		Remote Host 2			
Parameter Configuration		Data Upload Configuration			
Host Name	Enable	Network Status	Real-time Data Time	History Data Time	Information
Remote Host 1	Disabled				

Figure 11-1 Host Settings

Step 2 Select **Remote Host.**



NOTE

You can configure both the two Remote Hosts. Files can be uploaded to the two Remote Hosts.

Step 3 Click **Param Config.**

Step 4 Select Upload Protocol as **SDK Protocol** or **Private Protocol**. The default Upload Protocol is SDK Protocol.

iVMS-8600 whose version is V2.3 or above supports both SDK Protocol and Private Protocol. Other versions only support Private Protocol.

Step 5 Enter selected Remote Host **IP Address** and **Port**.

The default Port for SDK Protocol and Private Protocol are 5650 and 5682 separated.

Step 6 Select **Data Type** to upload in the dropdown list.

Step 7 You can select **Upload Historical Data** and **Upload No-Plate Data** as **Enable** to upload historical data and No-plate data.

Upload Historical Data: Upload historical data in HDD.

Step 8 Enable the **Upload by Time** and set the **Uploading Start Time** and **Uploading End Time**. Up to 2 periods can be set. Device only uploads data during the start time and end time.

Step 9 Enter **Upload Interval (ms)** and **Upload Timeout Interval (ms)**.

Step 10 Optionally, set the Enable Cloud Storage settings. Thus the data are saved in Cloud Storage device.

- 1) Check **Enable Cloud Storage** checkbox.
- 2) Enter cloud storage **Management Server IP Address, Command Port, User Name, and Password**.
- 3) Enter **Normal Vehicle Picture and Record File Pool ID** and **Traffic Violation Picture and Record File Pool ID**.

Step 11 Click **Save** to save the settings.

11.2 Configure FTP

Purpose:

Device provides two FTP servers. Configure the parameters, thus to upload data to the two FTP servers.

Step 1 Go to **Param Config. > Platform Settings > FTP Upload Settings > Param Config..**

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

Figure 11-2 Custom Settings

Step 2 Select **FTP Server 1** tab or **FTP Server 2** tab. You can enable both of them or one of them. The Custom Parameters interface is reserved.

Step 3 Click **Param Config.**

Step 4 Select **Enable** in **FTP** dropdown list.

Step 5 Enter **FTP Server Address, FTP Port, FTP User Name, and FTP Password**.

Step 6 You can select **Upload Historical Data** and **Upload No-Plate Data** as **Enable** to upload historical data and No-plate data.

Step 7 Enable the **Upload by Time** and set the **Uploading Start Time** and **Uploading End Time**. Up to 2 periods can be set.

Step 8 Select **Data Type**.

- 1) Click on text field to pop up Data Type items.
- 2) Check the checkbox (es) of item (s) to upload.
- 3) Click **OK** to save the settings and go back to upper level.

Step 9 Edit uploading file name and saving path.

Step 10 Click **OK** to save the settings.

11.3 Configure Data Uploading

Purpose:

Set parameters for uploading historical files and re-uploading files to Remote Host.

Before you start:

- To upload data to remote host, enable the **Upload Historical Data** function in Host settings first.
- To upload data to FTP server, enable the **Upload Historical Data** function in FTP settings first.

Step 1 Go to **Param Config. > Platform Settings > FTP Upload Settings > Data Upload Settings.**



Configure the four host's parameters before selecting Remote Host as any of them. For detailed steps, please refer to Configure Host and Configure FTP

Step 2 Click **Data Upload Settings.**

Figure 11-3 Data Retransmission

Step 3 Select Data Uploading.

- **Data Retransmission:** Resends files to Remote Host.
- **Upload Historical Data First:** Sends historical files first. Otherwise terminal server sends historical files when free.
- **Disable:** Terminal server won't upload historical data when free.

Step 4 Enter **Start Time** and **End Time**, thus to specify the start time and end time of uploaded file.

Step 5 Select uploading **Data Type** in dropdown list.

Step 6 Click **Save** to save the settings.

Chapter 12 Configure Alarm

12.1 Alarm Input Settings

Purpose:

Follow the steps to configure the alarm input recording schedule and alarm responding actions.

Step 1 Go to **Param Config. > Event > Basic Event > Alarm Input.**

Alarm Input No. IP Address

Alarm Type Alarm Name

Enable Alarm Input Handling

Arming Schedule Linkage Action

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

Figure 12-1 Alarm Input Settings

Step 2 Select **Alarm Input No.**

Step 3 Select Alarm Type.

- **Normal Open:** Alarm linking method and alarm recording are triggered when the alarm input is closed.
- **Normal Closed:** Alarm linking method and alarm recording are triggered when the alarm input is opened.

Step 4 Enter **Alarm Name.**

Step 5 Select the time period.

Step 6 (Optional) Click **Delete** to delete the current arming schedule, or click Save to save the settings.

Step 7 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.

Step 8 Click **Linkage Action** to configure linking action.

Step 9 Set **Alarm Linking**, **Trigger Alarm Output**, **Alarm Linked Recording**, and **PTZ Linking** according to your needs. Once an alarm occurs, the selected linking method will be triggered.

Step 10 Configure the alarm record schedule.

Step 11 Click **Save** to save the settings.

12.2 Alarm Output

Purpose:

You can configure the delay time, arming time, and alarm output name.

Step 1 Go to **Param Config. > Event > Basic Event > Alarm Output**.

The screenshot shows the 'Alarm Output' configuration page. At the top, there are several configuration fields: 'Alarm Output No.' set to 'A->1', 'IP Address' set to 'Local', 'Default Status' set to 'High Level', 'Triggering Status' set to 'High Level', 'Delay' set to '5s', 'Alarm Name' (disabled with '(cannot copy)'), and 'Alarm Status' set to 'OFF' (disabled with '(cannot copy)'). Below these fields is a section titled 'Arming Schedule' with a red border. It contains two buttons: 'Delete' (with a red 'X' icon) and 'Delete All' (with a trash can icon). Underneath is a 24-hour timeline for four days: Mon, Tue, Wed, and Thu. Each day's timeline has a blue bar spanning from 0 to 24, indicating that the alarm output is armed for the entire duration of each day.

Figure 12-2 Alarm Output

Step 2 Select **Alarm Output No.**.

Step 3 Select the **Delay Time**. Thus the device sends out alarm output signal for the set time.

Step 4 Enter **Alarm Name**.

Step 5 Configure the arming time. The alarm output signal is only available in arming time.

Step 6 Click **Save** to save the settings.

12.3 Linkage Action

Purpose:

You can set required linkage action of event.

Normal Linkage

- Select **Audio Warning** when beep is required in event alarm.
- Select **Notify Surveillance Center** when prompt alarm image is required in display.
- Select **Full Screen Monitor** when full screen display is required.

Trigger Alarm Output

Check **Trigger Alarm Output** when trigger alarm output is required once event occurs.

Trigger Recording

Check **Trigger Recording** when trigger recording is required once event occurs.

12.4 Alarm Exception

Purpose:

Set exception alarm of HDD full, HDD error, network cable disconnected, IP address conflicted, illegal login, video signal exception, input/output video standard mismatch, record/capture exception.

Step 1 Go to **Param Config. > Event > Basic Event > Exception**.

- **HDD Full:** Alarm when HDD is full, and content is not input into HDD.
- **HDD Error:** Alarm when there is HDD error.
- **Network Cable Disconnected:** Alarm when network cable is disconnected.
- **IP Address Conflicted:** Alarm when IP Address is conflicted. You need to edit IP address
- **Illegal Login:** Alarm when wrong password is entered.
- **Video Signal Exception:** Alarm when there is video signal exception
- **Input/ Output Video Standard Mismatch:** Alarm when input video standard mismatches output video standard.
- **Record/Capture exception:** Alarm when there is record/capture exception

Step 2 Configure linkage action.

Step 3 Click **Save** to save the settings.

Chapter 13 Status Information

13.1 Server Status

Purpose:

You can view the network status, server working status, and network uploading status.

Step 1 Go to **Param Config. > System Status > Server Status > Working Status.**

Working Status	Network Status
System Time	2018-02-28 14:01:00 +08:00
Working Time	11hours 59minutes 53seconds
Mainboard Temperature	42 °C
Terminal	0-Normal
Equipment Cabinet Door	0-Normal
GPS Device Status	GPS time synchronization is disabled.

Figure 13-1 Status

Step 2 Click Network Status or Working Status to view system status.

- **Network Status:** Shows all network interfaces status.
- **Working Status:** Displays the system working status.

13.2 Camera Status

Purpose:

You can view the Traffic Flow Statistic information, Front-end Device Status, and Camera Status. The function is only available when the connected camera supports traffic flow statistics.

Before you start:

Select the Camera Type.

Step 1 Go to **Param Config. > System Status > Status.**

Traffic Flow Statistics	Front-End Device Status	Camera Management Status
Camera	[D1] chan(10.10.112.37)	▼
Log in or not	Yes	
Arm or not	Yes	
Arming Level	Lv.1	
Arming Heartbeat	2019-05-21 16:09:11	

Figure 13-2 Camera Status

Step 2 Select the **Traffic Flow Statistics**, **Front-End Device Status**, or **Camera Management Status** to view camera status.

- **Traffic Flow Statistics:** Shows the Average Speed, Traffic Flow, Lane Occupancy, and Time Interval of Vehicle Head information.
- **Front-End Device Status:** Shows the camera, vehicle detector, or signal lamp detector working status.
- **Camera Management Status:** Shows the Camera Version, Camera Serial No., Login Status, and Arming Status.

Chapter 14 Other Settings

14.1 User Management

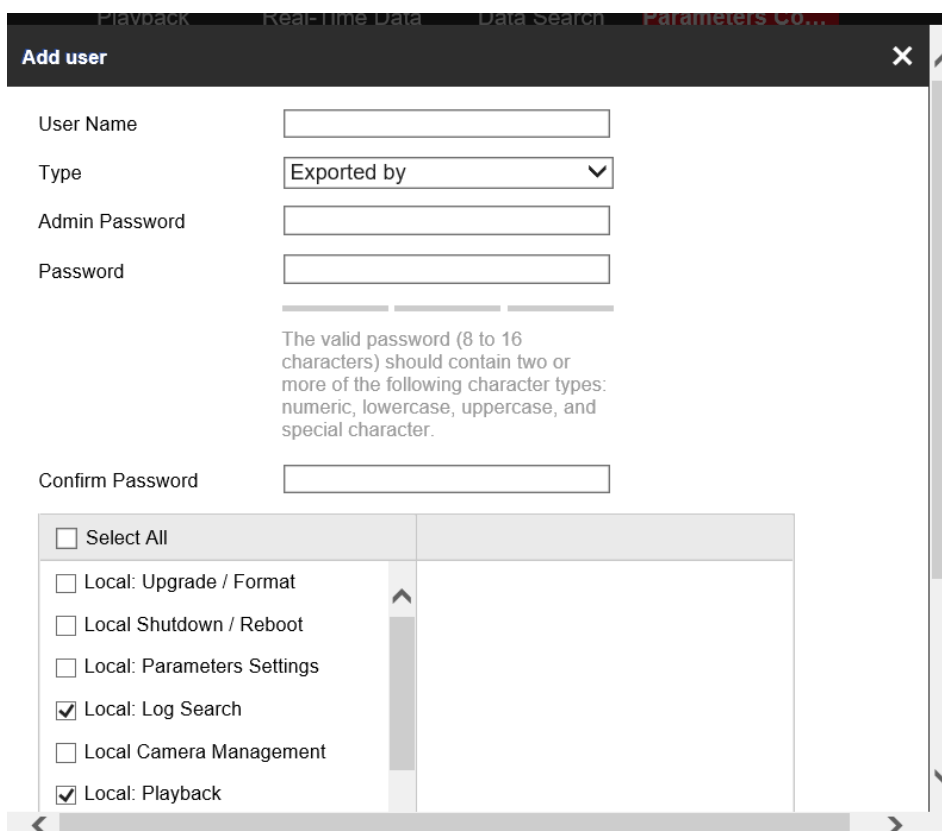
Purpose:

You can add, edit, and delete users.

14.1.1 Add a User

Step 1 Go to **Param Config. > System > User Management.**

Step 2 Click **Add** to enter the Add user interface.



The screenshot shows the 'Add user' dialog box. At the top, there are navigation tabs: Playback, Real-time Data, Data Search, and Parameters Co. The dialog has a title bar 'Add user' with a close button (X) and a scroll bar on the right. The form contains the following fields and elements:

- User Name: [Text input field]
- Type: [Dropdown menu with 'Exported by' selected]
- Admin Password: [Text input field]
- Password: [Text input field]
- Confirm Password: [Text input field]
- A note: "The valid password (8 to 16 characters) should contain two or more of the following character types: numeric, lowercase, uppercase, and special character."
- A list of checkboxes:
 - Select All
 - Local: Upgrade / Format
 - Local: Shutdown / Reboot
 - Local: Parameters Settings
 - Local: Log Search
 - Local: Camera Management
 - Local: Playback

Figure 14-1 Add User

Step 3 Enter the **User Name** and **Password**, and confirm the password.



WARNING

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.

Step 4 Select type.

Step 5 Configure the user permissions for the created user account.

Step 6 Click **OK** to add the user.

14.1.2 Edit a User



NOTE

You need the admin password to edit the admin user.

Step 1 Select a user account.

Step 2 Click **Edit** to enter the setting interface.

Step 3 Modify the **User Name**, and **Password**.



WARNING

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.

Step 4 Configure the user permission for the user.

Step 5 Click **OK** to save the settings.

14.1.3 Delete a User

Step 1 Select a user account from the list on the User Information interface to be deleted.

Step 2 Click **Delete**.

Step 3 Click **OK** to delete the selected user account.

14.2 Exception

Purpose:

You can specify the linkage action and triggered alarm output for nine exception types.

- **HDD Full:** The HDD is full.
- **HDD Error:** Writing HDD error or unformatted HDD.
- **Network Disconnected:** Disconnected network cable.
- **IP Conflicted:** Duplicated IP address.
- **Violation Access:** Incorrect user ID or password.

- **Video Standard Mismatch:** I/O video standards do not match.
- **Video Signal Exception:** Unstable video signal.
- **Record/Capture Exception:** Unable to recording or capture.

Step 1 Go to **Param Config. > Event > Basic Event.**

Exception Type	
HDD Full	
<input type="checkbox"/> Normal Linkage	<input type="checkbox"/> Trigger Alarm Output
<input type="checkbox"/> Audible Warning	<input type="checkbox"/> A->1
<input type="checkbox"/> Notify Surveillance Center	<input type="checkbox"/> A->2
	<input type="checkbox"/> A->3
	<input type="checkbox"/> A->4

Figure 14-2 Exception

Step 2 Select the **Exception Type** in the dropdown list.

Step 3 Select **Normal Linkage** and **Trigger Alarm Output**.

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

14.3 Maintenance

Purpose:

You can restart, restore default, repair database index, export/import configuration file, and upgrade device.

14.3.1 Reboot the Device

Go to **Param Config. > System > System Maintenance.**

- Click **Reboot** to reboot the device.
- Optionally, check **Auto-Reboot** checkbox. Then the device reboots automatically 2 a.m. every day.
- Optionally, check **Reboot without HDD** checkbox. Then the device reboots automatically when no HDD is detected.

Reboot	
<input type="button" value="Reboot"/>	Reboot the device.
<input type="checkbox"/> Reboot	Auto-reboot in every 0 a.m.
<input type="checkbox"/> Reboot Without HDD	Reboot when no HDD is detected.

Figure 14-3 Reboot

14.3.2 Default Settings

Step 1 Select the restoring type as **Restore** or **Default**.

- **Restore:** Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.
- **Default:** Restore all parameters to the factory default settings.

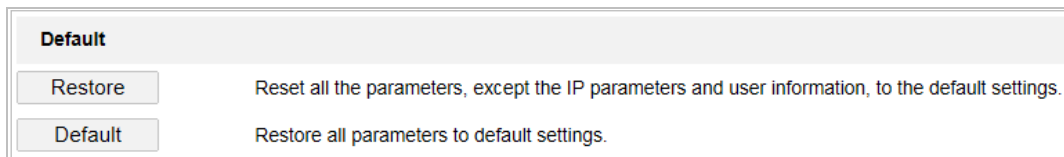


Figure 14-4 Default

14.3.3 Restore Database

Purpose:

When errors happen, such as searching data failed, uploading data failed, etc., repairing database function is one of the method to recover the errors.

Step 1 Click **Restore** to restore database.

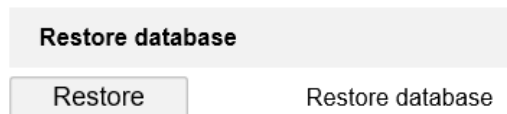


Figure 14-5 Restoring Database Index

14.3.4 Export/Import Configuration File

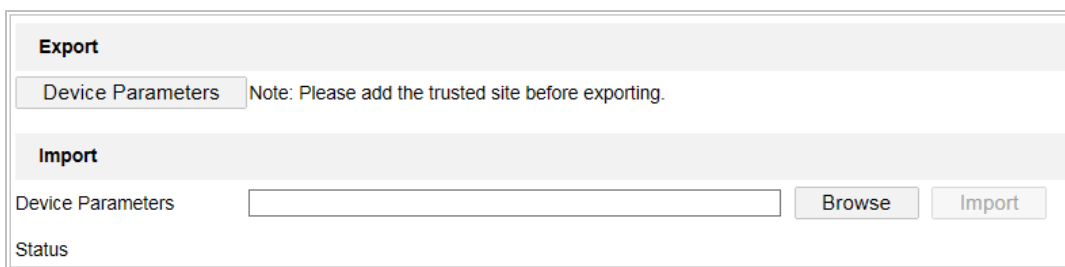


Figure 14-6 Importing/Exporting Configuration File

- Import configuration file.
 - 1) Click **Browser**.
 - 2) Select configuration file path.
 - 3) Click **Import** to import the selected file.
- Export configuration file.
 - 1) Click **Export**.
 - 2) Select exporting path.

3) Click **Save** to save the configuration file.

14.3.5 Remote Upgrade

Step 1 Click **Browse**.

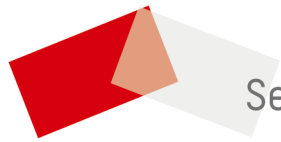
Step 2 Select upgrade file.

Step 3 Click **Upgrade** to upgrade.



The screenshot shows a web-based interface for upgrading a device. At the top, there is a header bar with the title "Upgrade". Below this, there is a row containing a dropdown menu currently set to "Firmware", an empty text input field, and two buttons labeled "Browse" and "Upgrade". Underneath this row is a section labeled "Status" which contains a note: "Note: The upgrading process will be 1 to 10 minutes, please don't disconnect power to the device during the process. The device reboots automatically after upgrading."

Figure 14-7 Remote Upgrade



See Far, Go Further