DS-TP50-12DT Terminal Server

User Manual
User Manual
COPYRIGHT ©2018 Hangzhou Hikvision Digital Technology Co., Ltd.
ALL RIGHTS RESERVED.
Any and all information, including, among others, wordings, pictures, graphs are the properties of
Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be
“Hikvision”). This user manual (hereinafter referred to be “the Manual”) cannot be reproduced,
changed, translated, or distributed, partially or wholly, by any means, without the prior written
permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties,
guarantees or representations, express or implied, regarding to the Manual.
About this Manual
This Manual is applicable to DS-TP50-12DT Terminal Server.
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 in the company website
(http://overseas.hikvision.com/en/).
Please use this user manual under the guidance of professionals.
Trademarks Acknowledgement
Hikvision and other Hikvision’s trademarks and logos are the properties of Hikvision in various
jurisdictions. Other trademarks and logos mentioned below are the properties of their respective
owners.
Legal Disclaimer
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS
HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS,
AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION,
MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND
NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS,
EMPLOYEES, OR AGENTS 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 OR DOCUMENTATION, IN CONNECTION WITH THE
USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH
DAMAGES.
REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY
AT YOUR OWN RISKS. 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.
SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR
JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS
THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS
USED WITH ILLEGITIMATE PURPOSES.
IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER
PREVAILS.
Symbol Conventions

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

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![NOTE]</td>
<td>Provides additional information to emphasize or supplement important points of the main text.</td>
</tr>
<tr>
<td>![WARNING]</td>
<td>Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.</td>
</tr>
<tr>
<td>![DANGER]</td>
<td>Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.</td>
</tr>
</tbody>
</table>
Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Enter voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100 to 240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:

- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
# Table of Contents

Chapter 1 Key Features .........................................................................................6  
Chapter 2 Introduction and Interfaces .................................................................7  
Chapter 3 Getting Started ....................................................................................9  
  3.1 Starting Up and Shutting Down ....................................................................9  
  3.1.1 Start Up .........................................................................................9  
  3.1.2 Shutt Down ....................................................................................9  
  3.1.3 Reboot .........................................................................................9  
  3.2 Environment Requirement ........................................................................10  
  3.3 Set the Admin Password ...........................................................................11  
  3.4 Remote Operation Introduction ..................................................................11  
    3.4.1 Live View Interface .......................................................................11  
    3.4.2 Playback Interface ........................................................................13  
    3.4.3 Traffic Interface ..........................................................................15  
    3.4.4 Log Interface ..............................................................................15  
    3.4.5 Configuration Interface ...............................................................16  
Chapter 4 Network Settings ..............................................................................18  
  4.1 External Network Settings ..........................................................................18  
  4.2 Internal Network Settings ..........................................................................19  
  4.3 DDNS Settings .......................................................................................19  
  4.4 More Settings ..........................................................................................21  
    4.4.1 Port Settings ................................................................................22  
    4.4.2 Remote Access Configuration .....................................................22  
    4.4.3 HTTPS Configuration ..................................................................23  
    4.4.4 Static Router .................................................................................24  
Chapter 5 Device Parameters ...........................................................................26  
  5.1 Device Information ....................................................................................26  
  5.2 Time Settings ..........................................................................................26  
  5.3 DST Settings ..........................................................................................27  
  5.4 Other Traffic Settings ...............................................................................28  
Chapter 6 Camera Management .......................................................................31  
Chapter 7 Camera Settings ..............................................................................33  
  7.1 Display Settings .......................................................................................33  
  7.2 Text Overlay ...........................................................................................33  
  7.3 Monitoring Spot Information Settings .......................................................34  
  7.4 Image Collage Parameters .......................................................................36  
  7.5 Collaged Picture Text Overlay ..................................................................36  
  7.6 Interaction Configuration .........................................................................36  
  7.7 Alarm Output .........................................................................................37  
Chapter 8 Record and Capture Settings ..............................................................39  
  8.1 HDD Initialization .....................................................................................39  
  8.2 Video and Picture Quota ............................................................................39
| Chapter 15 Camera Matching                                                                 | 70   |
| Chapter 14 Blacklist and Whitelist                                                        | 67   |
| Chapter 13 Other Settings                                                                | 60   |
| Chapter 12 Status Information                                                            | 58   |
| Chapter 11 Uploading Data                                                                | 53   |
| Chapter 10 Backup Configuration                                                          | 50   |
| Chapter 9 Serial Port Settings                                                           | 48   |
| Chapter 8 Record Schedule Settings                                                       | 41   |
| Chapter 7 Alarm Input Recording Settings                                                  | 43   |
| Chapter 6 Video Parameter Settings                                                       | 42   |
| Chapter 5 Holiday Settings                                                                | 41   |
| Chapter 4 Bad Sector Detection                                                            | 40   |
| Chapter 3 S.M.A.R.T Settings                                                              | 40   |
| Chapter 2 HDD Detection                                                                  | 40   |
| Chapter 1 Introduction                                                                    | 1    |
Chapter 1 Key Features

- Analog camera and IP camera are connectable, including 2 HD (High-Definition) TVI cameras.
- BNC interface and video loop interface for video output.
- Powers external device like external HDD with 12 VDC power output.
- Easy-to-dismounting design makes HDD convenient to maintenance.
- Low consumption and lower heat generation
- GPS time synchronization and speed test within a section are supported.
- Operable via Web.
Chapter 2 Introduction and Interfaces

**Purpose:**

DS-TP50-12DT as a traffic dedicated terminal server provides multiple features, including video management, traffic data management, video and audio decoding, picture processing, network transmission, etc. It integrates 16 network ports and 2 fiber ports, effectively meets the demands of distributed storage and accessing to surveillance management platform. Owning to the above features, DS-TP50-12DT series is widely applied in checkpoint, E-police, traffic surveillance system, etc.

The front panel view is shown below:

![Figure 2-1 Front Panel View](image)
<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RS-485</td>
<td>4 × RS-485 half-duplex interface.</td>
</tr>
<tr>
<td></td>
<td>RS-232</td>
<td>1 × RS-232.</td>
</tr>
<tr>
<td></td>
<td>Audio input/output</td>
<td>1 × audio input/output.</td>
</tr>
<tr>
<td></td>
<td>Alarm input/output</td>
<td>4 × alarm input/output.</td>
</tr>
<tr>
<td>2</td>
<td>Power output</td>
<td>12/5 VDC (Consumption of 12 VDC ≤ 15 W. 5 VDC ≤ 5 W)</td>
</tr>
<tr>
<td>3</td>
<td>Analog Video Input/output</td>
<td>2 × HD-TVI video input. 2 × HD-TVI loop output.</td>
</tr>
<tr>
<td>4</td>
<td>ANT</td>
<td>Antenna interface.</td>
</tr>
<tr>
<td>5</td>
<td>CVBS</td>
<td>CVBS output interface.</td>
</tr>
<tr>
<td>6</td>
<td>VGA</td>
<td>VGA interface.</td>
</tr>
<tr>
<td>7</td>
<td>HDMI</td>
<td>HDMI interface.</td>
</tr>
<tr>
<td>8</td>
<td>eSATA</td>
<td>eSATA interface.</td>
</tr>
<tr>
<td>9</td>
<td>USB</td>
<td>2 × USB 2.0.</td>
</tr>
<tr>
<td>10</td>
<td>Indicators</td>
<td>5 × status indicator: power indicator, alarm indicator, HDD indicator, ready indicator, and backup indicator.</td>
</tr>
<tr>
<td>11</td>
<td>OPT</td>
<td>Fiber interface of SFP standard.</td>
</tr>
<tr>
<td>12</td>
<td>G1 and G2</td>
<td>100/1000 M Ethernet interfaces.</td>
</tr>
<tr>
<td>13</td>
<td>P1 to P16</td>
<td>10/100 M Ethernet interfaces</td>
</tr>
<tr>
<td>14</td>
<td>Ground</td>
<td>Ground terminal</td>
</tr>
<tr>
<td></td>
<td>12 VDC</td>
<td>Power supply</td>
</tr>
<tr>
<td>15</td>
<td>Reset</td>
<td>Long press for 5 seconds to restore to factory.</td>
</tr>
</tbody>
</table>
Chapter 3 Getting Started

3.1 Starting Up and Shutting Down

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

3.1.1 Start Up

Before you start:
1. Fix the device in an equipment cabinet.
2. Ensure the device is properly grounded.
3. Plug the network cable

Step 1 Plug the power supply to start up.

NOTE
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.

3.1.2 Shutt Down

Unplug the power supply to shut down.

3.1.3 Reboot

For detailed steps, please refer to 13.3.1 Rebooting the Device.

3.2 Environment Requirement

Purpose:
Requirements on web browser and operation system are as follows:

- **Web Browser**: Internet Explorer 8.0 and above version/Mozilla Firefox 30-52 version/Google Chrome 31.0-45.0.2454.85.
- **Operating System**: Windows 7/Windows 8/Windows 10 (32-bit or 64-bit).
For Windows 10 operation system, to access the terminal server via Internet Explorer 10, you need to Run IE10 as an Administrator.

### 3.3 Set the 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 192.168.1.2.
- The default IP address for G2 network interface is 192.0.0.64.

**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**.

![Figure 3-1 Setting Admin Password](image)

**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.
3.4 Remote Operation Introduction

*Purpose:*

Embedded WEB feature enables the device to be operable via internet explorer. After successful login, you can see five items are list in the menu bar, including **Live View**, **Playback**, **Traffic**, **Log** and **Configuration**. This section will introduce the contents provided by the five menus.

### 3.4.1 Live View Interface

*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 3-4 Live View Interface
Table 3-1 Live View Interface Description

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Camera List</td>
<td>List the analog cameras and added IP cameras.</td>
</tr>
<tr>
<td>2</td>
<td>Live View Window</td>
<td>Display the live view image of the cameras.</td>
</tr>
<tr>
<td>3</td>
<td>PTZ Control Panel</td>
<td>PTZ control panel for rotating speed dome.</td>
</tr>
<tr>
<td>4</td>
<td>Video Parameters</td>
<td>Configure value of brightness, contrast, saturation and hue for the selected camera.</td>
</tr>
<tr>
<td>5</td>
<td>Live View Control Bar</td>
<td>Live view control is provided. For details, please refer to Table 3-2 Live View Control Bar.</td>
</tr>
</tbody>
</table>

Table 3-2 Live View Control Bar Description

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>Split the live view window into 1 window, 4 windows or 9 windows.</td>
<td><img src="image2" alt="Icon" /></td>
<td>Turn to previous page</td>
</tr>
<tr>
<td><img src="image3" alt="Icon" /></td>
<td>Start live view for all the cameras</td>
<td><img src="image4" alt="Icon" /></td>
<td>Turn to next page.</td>
</tr>
<tr>
<td><img src="image5" alt="Icon" /></td>
<td>Capture pictures for the selected camera.</td>
<td><img src="image6" alt="Icon" /></td>
<td>Enable / disable audio.</td>
</tr>
<tr>
<td><img src="image7" alt="Icon" /></td>
<td>Start recording for all the cameras</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.4.2 Playback Interface

*Purpose:*

You can play back the record files of a specified day.
Table 3-3 Playback Interface Description

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Camera List</td>
<td>List the enabled analog cameras and added IP cameras.</td>
</tr>
<tr>
<td>2</td>
<td>Playback Window</td>
<td>Display the playback image.</td>
</tr>
<tr>
<td>3</td>
<td>Playback Status</td>
<td>Show the playback status, including playback camera No. and playback speed.</td>
</tr>
<tr>
<td>4</td>
<td>Calendar</td>
<td>Select a day to play back record files.</td>
</tr>
<tr>
<td>5</td>
<td>Playback Control Bar</td>
<td>Playback control is provided. For details, please refer to Figure 3-4 Live View Interface.</td>
</tr>
<tr>
<td>6</td>
<td>Time Bar</td>
<td>4 types of record file are marked with 4 colors.</td>
</tr>
</tbody>
</table>
Table 3-4 Playback Control Bar Description

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Image" alt="Icon" /></td>
<td>Split the playback window into 1 window, 4 windows or 9 windows.</td>
<td><img src="Image" alt="Icon" /></td>
<td>Stop playback for all cameras.</td>
</tr>
<tr>
<td><img src="Image" alt="Icon" /></td>
<td>Start/pause playback for selected camera.</td>
<td><img src="Image" alt="Icon" /></td>
<td>Capture pictures for the selected camera.</td>
</tr>
<tr>
<td><img src="Image" alt="Icon" /></td>
<td>Stop playback for selected camera.</td>
<td><img src="Image" alt="Icon" /></td>
<td>Download record files.</td>
</tr>
<tr>
<td><img src="Image" alt="Icon" /></td>
<td>Slow forward.</td>
<td><img src="Image" alt="Icon" /></td>
<td>Start/stop clipping.</td>
</tr>
<tr>
<td><img src="Image" alt="Icon" /></td>
<td>Fast forward.</td>
<td><img src="Image" alt="Icon" /></td>
<td>Enable/disable audio.</td>
</tr>
<tr>
<td><img src="Image" alt="Icon" /></td>
<td>Start single frame playback.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.4.3 Traffic Interface

**Purpose:**

Specify search condition to search traffic data.

![Figure 3-6 Traffic Interface](Image)

Table 3-5 Traffic Interface Description

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Search Results</td>
<td>Display traffic data search results.</td>
</tr>
<tr>
<td>2</td>
<td>Search Conditions</td>
<td>Configure traffic data search conditions.</td>
</tr>
</tbody>
</table>

3.4.4 Log Interface

**Purpose:**
You can review the device status of a certain period by searching logs.

![Figure 3-7 Log Interface](image)

### Table 3-6 Log Interface Description

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Search Results</td>
<td>Display the log search results.</td>
</tr>
<tr>
<td>2</td>
<td>Search Conditions</td>
<td>Configure log search conditions.</td>
</tr>
</tbody>
</table>

### 3.4.5 Configuration Interface

**Purpose:**

You can configure the device parameters here, including adding IP cameras, enabling record schedule, setting the alarm parameters, etc.

![Figure 3-8 Configuration Interface](image)
<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Menu List</td>
<td>Display the main menu and sub-menu.</td>
</tr>
<tr>
<td>2</td>
<td>Parameter Area</td>
<td>Shown or configure parameters of a certain menu.</td>
</tr>
</tbody>
</table>
Chapter 4 Network Settings

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

### 4.1 External Network Settings

**Step 1** Go to Configuration > Remote Configuration > Network Settings > External Network Settings.

![Figure 4-1 Basic Network Settings](image)

**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.
4.2 Internal Network Settings

Purpose:
You can configure the IP address for the network interfaces. The default IP address is 192.0.0.64.

Step 1 Go to Configuration > Remote Configuration > Network Settings > Internal Network Settings.

![Image of 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.

4.3 DDNS Settings

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 Configuration > Remote Configuration > Network Settings > 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.

### 4.4 More Settings

**Purpose:**

Optionally, you can configure the device network ports. And SSH (Secure Shell) function is provided. SSH is an encrypted network protocol to ensure the remote visit security.
4.4.1 Port Settings

Step 1 Go to Configuration > Remote Configuration > Network Settings > Network Port Settings.

![Network Port Configuration](image)

**Step 2** Edit the SDK Port, RTSP Port and HTTP Port.

- **SDK Port**: Port for platform to communicate with the device.
- **RTSP Port**: Port for getting stream from IP camera.
- **HTTP Port**: Port for browser to access the device.

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

![NOTE](image)

Restart the device to activate the new settings.

### 4.4.2 Remote Access Configuration

**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 Configuration > Remote Configuration > Network Settings > Remote Access Configuration.

![Remote Access Configuration](image)

**Step 2** Check the checkbox of **SSH**.

**Step 3** Click **Save** to enable it.
4.4.3 HTTPS Configuration

*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 **Configuration > Remote Configuration > Network Settings > HTTPS.**

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

![HTTPS Settings](image)

**Figure 4-9 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.

![Create Self-signed Certificate](image)

**Figure 4-10 Create Self-signed Certificate**

  3) Enter the **Country**, **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.

![Figure 4-11 Installed Certificate Property](image)

**Step 4** Check the checkbox to enable the HTTPS function.

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

### 4.4.4 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 **Configuration > Remote Configuration > Network Settings > Static Router.**

![Figure 4-12 Static Router](image)

**Step 2** Click the **Add** button.
Step 3 Check Enable checkbox.

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 **Network Interface**.

Step 6 Click **OK** to save the settings.
Chapter 5 Device Parameters

5.1 Device Information

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

Step 1 Go to Configuration > Remote Configuration > Device Parameters > Device Information.

![Device Information](image)

Figure 5-1 Device Information

5.2 Time Settings

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

Step 1 Go to Configuration > Remote Configuration > Device Parameters > Time Settings.
Step 2 Select **Time Zone** from the dropdown list.

Step 3 Select the clock synchronization mode as **NTP**, **Manual Time Synchronization** or **GPS Time Synchronization**.

- **NTP**
  Enter NTP Server, NTP Port and Interval time.

- **Manual Time Synchronization**
  Enter the time and date in **Set Time**. Or you can select **Synchronize with computer time**.

### 5.3 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 **Configuration** > **Remote Configuration** > **Device Parameters** > **Time Settings**.
Step 2 Check the checkbox of **Enable DST**.

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

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

### 5.4 Other Traffic Settings

**Purpose:**
Configure other traffic settings for device.

Step 1 Go to **Configuration > Remote Configuration > Device Parameters > Other Settings**.

![Other Settings](image)

**Figure 5-4 Other Settings**

Step 2 Configure following parameters according to your needs.

- **Traffic Camera Connection Mode:**
  - **Arming Mode:** Link between terminal server and traffic cameras is a long-period link. Terminal server takes pictures from traffic cameras. Terminal server is the active device.
  - **Listening Mode:** Link between terminal server and traffic cameras is a short-period link. Traffic cameras upload pictures to terminal server. Terminal server is the passive device.

- **Arming Level** (only available for Arming Mode):
  - **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.

- **Checkpoint Video Linkage:**
  - **Enable:** When searching traffic data in Traffic interface, you can play and export checkpoint linked video.

- **Secondary Picture Recognition:**
  - **Enable:** Device will analyze the pictures that have been recognized as unknown by traffic camera.

- **Traffic Camera Time Synchronization:**
  - **Enable:** Terminal server synchronizes the connected traffic cameras’ time.

- **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.

- **Mark Picture with:** Add *Time Synchronization Mark* or add *Security Code* to pictures. The two items are written in binary code and they are invisible.

Step 3 Enter **Cabinet Door Name** and **Cabinet Door No.** according to actual installation.

Step 4 Click **Save** to save the settings.
Chapter 6 Camera Management

Purpose:
Up to 12 smart IP cameras can be added to the device. This makes managing 12 lanes possible.

Step 1 Go to Configuration > Remote Configuration > Camera Management > IP Camera.

Step 2 Add IP cameras. Manual add and quick-scan are provided.

- **Option 1**: Manual Add
  1) Click the Add button.
  2) Select Registration Mode as IP or Normal Domain.
  3) Enter IP Address / Domain.
  4) Select Protocol.
  5) Enter Management Port, Channel No., User Name, Admin Password and Password Confirm.
  6) Click OK to add it.

  ![Figure 6-1 Manually Add IP Camera](image)

- **Option 2**: Quick-Scan
  1) Click the Quick-Scan button. The online IP cameras will be listed.
  2) Select the IP cameras you want to add.
  3) Click OK to add them.

**NOTE**

All the input parameter above should be the same with the IP camera itself.
IP cameras have the same password with the device can be connected successfully.

Figure 6-2 Quick-Scan

Step 3 Optionally, you can click to select an added IP camera, and click Modify, Delete or Reboot to perform corresponding actions.
Chapter 7 Camera Settings

7.1 Display Settings

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

*Step 1* Go to *Configuration > Remote Configuration > Camera Settings > Display Settings.*

![Figure 7-1 Display Settings](image)

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** and **OSD Display**.

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

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

7.2 Text Overlay

*Purpose:* You can overlay four text contents onto the video.

*Step 1* Go to *Configuration > Remote Configuration > Camera Settings > Text Overlay.*
Step 2 Select camera to configure in Select Camera dropdown list.

Step 3 Enter contents in the four Text Contents.

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

Step 5 Click Save to show the contents.

### 7.3 Monitoring Spot Information Settings

**Purpose:**

You can configure monitoring spot settings.

Step 1 Go to Configuration > Remote Configuration > Camera Settings > Monitoring Spot Information.
Step 2 Select camera to configure in **Select Camera** dropdown list.

Step 3 Select **Camera Type** as **Video Surveillance Camera** or **Intelligent Traffic Camera**. The default Camera Type is Video Surveillance Camera.

- **Video Surveillance Camera**: 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 **Monitoring Spot 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.
- **Monitor Spot 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 monitoring spots in the four text contents, including **Monitoring Spot Information 1**, **Monitoring Spot Information 2**, **Monitoring Spot Information 3**, and **Monitoring Spot Information 4**:

- Valid **Monitoring Spot Information 1**: No more than 120 characters.
- Valid **Monitoring Spot Information 2**: No more than 40 characters.
- Valid **Monitoring Spot Information 3**: No more than 30 characters.
- Valid **Monitoring Spot Information 4**: No more than 24 characters.

Step 7 Click **Save** to save the settings.
7.4 Image Collage Parameters

*Purpose:*
Configure image collage layout and other parameters.

Step 1 Go to Configuration > Remote Configuration > Camera Settings > Image Collage Parameters.

Step 2 Select camera to configure.

Step 3 Set Image Collaging as Enable.

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

Step 5 Configure Maximum Size of Picture (KB) and Original Picture Zoom Multiple.
- **Maximum Size of Picture (KB):** The maximum size of collaged pictures.
- **Original Picture Zoom Multiple:** The zoom in times for pictures to collage.

Step 6 Click Save.

7.5 Collaged Picture Text Overlay

*Purpose:*
Overlay text on collaged pictures.

Step 1 Go to Configuration > Remote Configuration > Camera Settings > Collaged Picture Text Overlay.

Step 2 Select camera to configure.

Step 3 Select Text Overlay Position.

Step 4 Select Text Overlay Type.

Step 5 Set text parameters including Initial Top Margin, Initial Left Margin, Character Size, Character Color, Background Color, Space, 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.

7.6 Interaction Configuration

*Purpose:*
Configure the Interaction Mode between terminal server and traffic cameras.

**Step 1** Go to **Configuration > Remote Configuration > Camera Settings > Interaction Configuration**.

![Interaction Configuration](image)

**Figure 7-4 Interaction Configuration**

**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.

### 7.7 Alarm Output

**Purpose:**

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

**Step 1** Go to **Configuration > Remote Configuration > Alarm Settings > Alarm Output**.
Step 2 Select **Alarm Output** No. in the dropdown list.

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

Step 4 Enter **Alarm Name**.

Step 5 Click the **Edit** button to configure the arming time. The alarm output signal is only available in arming time.

For detailed steps, turn to step 5 to 8 in 8.7 Alarm Input Recording Settings.

Step 6 Click **Save** to save the settings.
Chapter 8 Record and Capture Settings

8.1 HDD Initialization

*Purpose:* Initialize the HDD before you use it.

**NOTE**
HDD amount varies according to different models. You can refer to specification for details.

Step 1 Go to **Configuration > Remote Configuration > HDD Management > Basic Settings.**
Step 2 Check the checkbox of **HDD** to initialize.
Step 3 Click **Init** to initiate it.

![HDD Management](image1)

Figure 8-1 HDD Management

8.2 Video and Picture Quota

*Purpose:* You can set the maximum capacity for saving picture.

Step 1 Go to **Configuration > Remote Configuration > HDD Management > Advanced Settings.**

![Advanced Settings](image2)

Figure 8-2 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.

### 8.3 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.

#### 8.3.1 S.M.A.R.T Settings

Step 1 Go to **Configuration > Remote Configuration > HDD Management > S.M.A.R.T.**

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 the **Start** button to start the S.M.A.R.T. HDD self-evaluation.

![Figure 8-3 S.M.A.R.T Settings Interface](image)

#### 8.3.2 Bad Sector Detection

Step 1 Go to **Configuration > Remote Configuration > HDD Management > S.M.A.R.T.**
Step 2 Select the HDD No. in the drop-down.

Step 3 Choose Detection Type as Detect All or Key Area Detection.

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

8.4 Video Parameter Settings

*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 Configuration > Remote Configuration > Camera Settings > Video Settings.
Step 2 Select the camera to configure from the Select Camera dropdown list.

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.

Only analog cameras can copy parameters to each other.

Step 6 Click OK to save the settings.

### 8.5 Holiday Settings

**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 Configuration > Remote Configuration > Camera Settings > Holiday Settings.
Step 2 Click the icon after a holiday to enter Edit Holiday interface.

**NOTE**

Up to 32 holidays can be configured.

Step 3 Edit 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 holiday and go back to upper menu.

### 8.6 Record Schedule Settings

**Purpose:**

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

Step 1 Go to Configuration > Remote Configuration > Camera Settings > Record Schedule.
Step 2 Select camera to configure in the **Select Camera** dropdown list.

Step 3 Check the checkbox of **Enable Schedule**.

Step 4 Click ![Edit](Image) to configure record schedule.

Step 5 Select a day in a week to configure.

Step 6 Check **All Day** record schedule or **Segment Record** schedule checkbox.

- **All Day**: Device records video for the whole day in the selected record type. Select Record Type as Normal or Alarm.
- **Normal**: Continuous recording.
• **Alarm**: Alarm triggered recording.

• **Segment Record**: Up to 8 time segments can be set in a day. Device records only in set time segments.
  1) Set the **Start Time**, **End Time**, and **Record Type** for a time segment.
  2) Optionally, repeat step 1) to configure more time segments.

Step 7 Select day(s) in **Copy to Week** and click **Copy**, thus to copy the schedule to other days. Or repeat the step 5 and 6 to configure.

Step 8 Click **OK** to go back to previous menu.

Step 9 Optionally, click **Advanced** to set Advanced Settings.

• **Pre-Record**: The time you set to record before the scheduled time or event. For example, when an alarm triggered the recording at 10:00, if you set the pre-record time as 5 seconds, the camera records it at 9:59:55.

• **Post-Record**: The time you set to record after the scheduled time or the event. For example, when an alarm triggered the recording ends at 11:00, if you set the post-record time as 5 seconds, it records till 11:00:05.

• **Redundant Record**: Enabling redundant record or capture means you save the record and captured picture in the redundant HDD.

• **Record Audio**: Check the checkbox to enable or disable audio recording.

• **Expired Time**: The expired time is the longest time for a record file to be kept in the HDD, if the deadline is reached, the file will be deleted. You can set the expired time to 0, and then the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

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

### 8.7 Alarm Input Recording Settings

*Purpose:*

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

Step 1 Go to **Configuration > Remote Configuration > Alarm Settings > Alarm Input.**
Step 2 Select **Alarm Input No.** in the dropdown list.

Step 3 Select Alarm Type as **NO** (normally open) or **NC** (normally closed) for alarm type.

![NOTE]

- **NO**: Alarm linking method and alarm recording are triggered when the alarm input is closed.
- **NC**: Alarm linking method and alarm recording are triggered when the alarm input is opened.

Step 4 Enter alarm input **Name** in the text field.

Step 5 Click **Arming Time** to configure arming time. Linking method is only available in the arming time.
1) Select a day in a week to configure.
2) Up to 8 time segments are provided. Set the Start Time and End Time for one or more time segments.
3) Select day(s) in Copy to Week and click Copy, thus to copy the schedule to other days. Or repeat the step 1) and 2) to configure arming time for other days.

Step 6 Click Linking Method to configure linking method.

Step 7 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 8 Configure the alarm record schedule. For detailed steps, please refer to 8.4 Video Parameter Settings.

Step 9 Click Save to save the settings.
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 **Configuration > Remote Configuration > Serial Port Settings > RS-232 Serial Port.**

![RS-232 Settings](image)

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

**i** **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 **Configuration > Remote Configuration > Serial Port Settings > RS-485 Serial Port.**
Step 2 Select Serial Port No., Baud Rate, Data Bit, Stop Bit, Parity and Flow Control.

![NOTE]

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

Step 3 Click **Save** to save the settings.
Chapter 10 Backup Configuration

10.1 USB Backup Settings

**Purpose:**
You can export data to USB backup device.

**Before you start:**
Insert a USB backup device into the USB interface in rear panel.

Step 1 Go to Configuration > Remote Configuration > Backup Configuration > USB Backup Settings.

![USB Backup Settings](image)

Figure 10-1 USB Backup Settings

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

Step 3 Set **Backup Mode**.

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 pictures and video files of last day in every 0 a.m.

2) Set **Backup Start Time** to export historical files.

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

Step 5 Set **Saving Path and File Name**. We take setting the file name and directory for backing up license plate picture as an example.

3) Click the text field after the **License Plate Picture Name**. The following menu pops up.
4) Click to select contents. The selected contents are list in the text filed. And the text filed is the license plate picture name.

![NOTE]

If you want to add other contents that is not provided in the list, you can input the contents in the textfield.

5) Optionally, click **Backspace** in keyboard to delete contents.

6) Click **OK** to save the contents and go back to upper level.

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

### 10.2 Web Backup Settings

**Purpose:**

In Traffic interface, you can export traffic information. And you can set the file name and directory for the backup files, including pictures and videos of license plate, traffic violation, event, and evidence. Event file configuration is only available for traffic incident detection server. Evidence file is only available for enforcement speed dome.

We take setting the file name and directory for backing up license plate picture as an example.

**Step 1** Go to **Configuration > Remote Configuration > Backup Configuration > Web Backup Settings.**
Step 2 Click the text field after the **License Plate Picture Name**. The following menu pops up.

![License Plate Picture Name](image)

**Figure 10-4 License Plate Picture Name**

Step 3 Edit the saving path and file name. We can turn to Step 5 in 10.1 USB Backup Settings for reference.

Step 4 Click **Save** to save the settings.
Chapter 11 Uploading Data

11.1 Host Settings

Purpose:
Configure the Remote Host settings to upload data to Remote Host, including iVMS-8600 and third-party platforms.

Step 1 Go to Configuration > Remote Configuration > Remote Host > Host Settings.

Step 2 Select Remote Host as Remote Host 1 or Remote Host 2 in Select dropdown list.

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


- iVMS-8600 whose version is V2.3 or above supports both SDK Protocol and Private Protocol. Other versions only support Private Protocol.
- If set Upload Protocol as EHome Protocol, you need to register the device in Ehome platform first.

Step 4 Enter selected Remote Host IP Address and Port.
The default Port for SDK Protocol and Private Protocol are 5650 and 5682 separated.

Step 5 Select **Data Type** to upload in the dropdown list.

Step 6 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 7 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 8 Enter **Upload Interval (ms)** and **Upload Timeout Interval (ms)**.

Step 9 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**.

![Figure 11-2 Cloud Storage](image)

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

11.2 FTP Settings

**Purpose:**

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

**Step 1** Go to **Configuration > Remote Configuration > 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 Select **Enable** in **FTP** dropdown list.

Step 4 Enter **FTP Server Address**, **FTP Port**, **FTP User Name**, and **FTP Password**.

Step 5 You can select **Upload Historical Data** and **Upload No-Plate Data** as **Enable** to upload historical data and No-plate data.

Step 6 Enable the **Upload by Time** and set the **Uploading Start Time** and **Uploading End Time**. Up to 2 periods can be set.

Step 7 Select **Data Type**.

1) Click **6 items are selected,total 9 items** 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 8 Edit uploading file name and saving path. For detailed steps, please refer to step 5 of 10.1 **USB Backup Settings**.
11.3 Data Uploading Configuration

*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. For details, refer to *Step 6 of 11.1 Host Settings*.
- To upload data to FTP server, enable the **Upload Historical Data** function in FTP settings first. For details, refer to *Step 5 of 11.2 FTP Settings*.

**Step 1** Go to **Configuration > Remote Configuration > Remote Host > Data Uploading Configuration**.

**Step 2** Select Data Uploading Mode as **Data Retransmission**, **Upload Historical Data First**, or **Disable**.
- **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 3 Select uploading Remote Host as Remote Host 1, Remote Host 2, FTP Uploading Host 1, or FTP Uploading Host 2.

**NOTE**

Configure the four host’s parameters before selecting Remote Host as any of them. For detailed steps, please refer to 11.1 Host Settings and 11.2 FTP Settings.

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 Status Information

12.1 Server Status

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

Step 1 Go to **Configuration > Remote Configuration > Status Information > Server Status.**

![Server Status Table]

Step 2 Click Network Status, Working Status, and Network Uploading Status to view system status.

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

12.2 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 as Intelligent Traffic Camera. For details, please refer to **7.3 Monitoring Spot Information Settings.**

Step 1 Go to **Configuration > Remote Configuration > Status Information > Camera Status.**
Step 2 Select camera to view status in **Select Camera** dropdown list.

Step 3 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 13 Other Settings

13.1 User Management

*Purpose:*
You can add, edit, and delete users.

**Step 1** Go to **Configuration > Remote Configuration > User Management.**

![Figure 13-1 User Management](image)

### 13.1.1 Adding a User

**Step 1** Click **Add** to enter the Add user interface.

![Figure 13-2 Add User](image)

**Step 2** 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 3 Select the Level to Operator or User.

- **Operator**: The *Operator* user level has permission of Local Log Search in Local Configuration, Remote Log Search and Two-way Audio in Remote Configuration and all operating permission in Camera Configuration.
- **User**: The Guest user has permission of Local Log Search in Local Configuration, Remote Log Search in Remote Configuration and only has the local/remote playback in the Camera Configuration.

Step 4 Configure the user permissions for the created user account, including the **Basic Permission** and **Camera Operation**.

Step 5 Click **OK** to add the user.

### 13.1.2 Modifying a User

**NOTE**

You need the admin password to modify the admin user.

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

![Figure 13-3 Select a User](image)

Step 2 Click **Modify** to enter the setting interface.
Step 3 Modify the User Name, Password, and then select User Type.

**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, including the Basic Permission and Camera Operation.

Step 5 Click OK to finish the user modification.

13.1.3 Deleting a User

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

Step 2 Click Delete, and an information box will pop up.

Step 3 Click OK to delete the selected user account.

13.2 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.
- **Illegal Access**: Incorrect user ID or password.
- **Video Standard Dismatch**: 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 **Configuration > Remote Configuration > Exception**.

![Figure 13-5 Exception](image)

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

**Step 3** Select **Alarm Linking** and **Trigger Alarm Output**.

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

### 13.3 Maintenance

**Purpose:**

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

**Step 1** Go to **Configuration > Remote Configuration > Maintenance**.
13.3.1 Rebooting the Device

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

13.3.2 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.
13.3.3 Repairing 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 **Repair** to repair database.

13.3.4 Exporting/Importing 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.

13.3.5 Remote Upgrade

Step 1 Click **Browse**.

Step 2 Select upgrade file.

Step 3 Click **Upgrade** to upgrade.
Figure 13-11 Remote Upgrade
Chapter 14 Blacklist and Whitelist

Purpose:
To manage special license plate numbers, you can add them into blacklist or whitelist.

Go to Configuration > Remote Configuration > Blacklist/Whitelist.

Step 1 Click Add.

Step 2 Select List Type as Blacklist or Whitelist.
Step 3 Enter License Plate Number.
Step 4 Select Whether to Enable as Yes to enable the function.
Step 5 Click OK to add the license plate number.
14.2 Deleting List

Step 1 Check the checkboxes of blacklists and whitelists to delete.
Step 2 Click **Delete** to delete them.

14.3 Searching List

*Purpose:*
You can search added license plate numbers in blacklist/whitelist.

Step 1 Select **List Type** as **Blacklist** or **Whitelist** in drop-down list.
Step 2 Click **Search** to start searching.

![Figure 14-3 Search](image)

14.4 Exporting/Importing List

14.4.1 Exporting List

*Purpose:*
You can export all the license plate numbers in blacklist and whitelist to a local path.

Step 1 Click **Export**.
Step 2 Click **Browse** to select a local path and click **Export** to start export.

![Figure 14-4 Export](image)

License plate numbers will be exported in an Excel file. The Excel contents are shown in *Figure 14-1*. 
• Arming Type: 1 refers to Whitelist. 2 refers to Blacklist.
• Status: 0 refers to disabled. 1 refers to enabled.

Table 14-1 Exported Excel Content.

<table>
<thead>
<tr>
<th>License Plate Number</th>
<th>List Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>HUA123</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

14.4.2 Importing List

*Purpose:*

You can import license plate numbers to blacklist or whitelist in batch.

Step 1 Click **Download Import Template** to download the Excel template.

Step 2 Fill in license plate number, list type, and status in an Excel template.

**NOTE**

• Arming Type can only be 1 or 2. 1: whitelist. 2: blacklist.
• Status can only be 0 or 1. 0: disabled. 1: enabled.

Step 3 Click **Import**.

Step 4 Click **Browse** to select a local path and click **Import** to start import.
Chapter 15 Camera Matching

15.1 Section Configuration

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

Step 1 Go to Configuration > Remote Configuration > Camera Matching > Section Configuration.

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

Step 3 Click **Add**.

![Figure 15-1 Section Configuration](image)

Step 4 Check **Enable**.

Step 5 Configure section parameters and vehicle speeding parameters.

- **Section Number**: Select road segment number to configure. 6 segments are selectable.
- **Section Name**: Enter **Section Name**.
- **Section Length**: Enter **Section Length** according to actuality.
- **Section Scene**: Select **Section Scene** as **High Speed Mode** or **City Mode** according to actuality.
- **Entrance Channel** and **Exit Channel**: The selected channels must be traffic cameras.
- **Large-Size Vehicle Speeding Percentage**: The actual speed limit value. Enter the value according to actuality.
- **Large-Size Vehicle Speed Limit**: The value cannot be smaller than Large-Size Vehicle Speeding Percentage.
- **Large-Size Vehicle Exception Speeding Limit**: The value must be larger than both Large-Size Vehicle Speeding Percentage and Large-Size Vehicle Speed Limit.
- **Small-Size Vehicle Speeding Percentage**: The actual speed limit value. Enter the value according to actuality.
- **Small-Size Vehicle Speed Limit**: The value cannot be smaller than Small-Size Vehicle Speeding Percentage.
- **Small-Size Vehicle Exception Speeding Limit**: The value must be larger than both Small-Size Vehicle Speeding Percentage and Small-Size Vehicle Speed Limit.

Step 6 Click **OK**.

### 15.2 Camera Matching

**Purpose:**
Collage the two picture of vehicles. Configure the following parameters according to your actual camera type.

Step 1 Go to **Configuration > Remote Configuration > Camera Matching > Camera Matching**.

Step 2 Check **Enable Channel Match**.

Step 3 Click **Add**.

![Camera Matching](image.png)

**Figure 15-2 Camera Matching**

Step 4 Check **Enable**.

Step 5 Select **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.
See Far, Go Further