Terminal Server
User Manual
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.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![i] 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

<table>
<thead>
<tr>
<th>Laws and Regulations</th>
<th>Use of the product must be in strict compliance with the local laws and regulations. Please shut down the device in prohibited area.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply</td>
<td>• Use of the product must be in strict compliance with the local electrical safety regulations.</td>
</tr>
<tr>
<td></td>
<td>• Use the power adapter provided by qualified manufacturer. Refer to the product specification for detailed power requirements.</td>
</tr>
<tr>
<td></td>
<td>• It is recommended to provide independent power adapter for each device as adapter overload may cause over-heating or a fire hazard.</td>
</tr>
<tr>
<td></td>
<td>• Make sure that the power has been disconnected before you wire, install, or disassemble the device.</td>
</tr>
<tr>
<td></td>
<td>• DO NOT directly touch exposed contacts and components once the device is powered up to avoid electric shock.</td>
</tr>
<tr>
<td></td>
<td>• DO NOT use damaged power supply devices (e.g., cable, power adapter, etc.) to avoid electric shock, fire hazard, and explosion.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• DO NOT block the power supply equipment to plug and unplug conveniently.</td>
</tr>
<tr>
<td></td>
<td>• Make sure the power supply has been disconnected if the power adapter is idle.</td>
</tr>
<tr>
<td></td>
<td>• Make sure the device is connected to the ground firmly.</td>
</tr>
<tr>
<td>Table: Transportaion, Use, and Storage</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td></td>
</tr>
<tr>
<td>• To avoid heat accumulation, good ventilation is required for a proper operating environment.</td>
<td></td>
</tr>
<tr>
<td>• Store the device in dry, well-ventilated, corrosive-gas-free, no direct sunlight, and no heating source environment.</td>
<td></td>
</tr>
<tr>
<td>• Avoid fire, water, and explosive environment when using the device.</td>
<td></td>
</tr>
<tr>
<td>• Avoid lightning strike for device installation. Install a lightning arrester if necessary.</td>
<td></td>
</tr>
<tr>
<td>• Keep the device away from magnetic interference.</td>
<td></td>
</tr>
<tr>
<td>• 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).</td>
<td></td>
</tr>
<tr>
<td>• DO NOT touch the heat dissipation component to avoid burns.</td>
<td></td>
</tr>
<tr>
<td>• DO NOT expose the device to extremely hot, cold, or humidity environments. For temperature and humidity requirements, see device specification.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table: Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.</td>
</tr>
<tr>
<td>• 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).</td>
</tr>
<tr>
<td>• 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 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.</td>
</tr>
<tr>
<td>• 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table: Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DO NOT disconnect the power during formatting, uploading, and downloading. Or files may be damaged.</td>
</tr>
</tbody>
</table>
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 Blacklist and Whitelist .................................................................................... 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
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Configure OSD</td>
<td>32</td>
</tr>
<tr>
<td>6.2</td>
<td>Configure Text Overlay</td>
<td>32</td>
</tr>
<tr>
<td>6.3</td>
<td>Configure Camera Parameter</td>
<td>32</td>
</tr>
<tr>
<td>6.4</td>
<td>Configure Picture Composition</td>
<td>34</td>
</tr>
<tr>
<td>6.5</td>
<td>Configure Composite Overlay</td>
<td>34</td>
</tr>
<tr>
<td>6.6</td>
<td>Configure Interaction</td>
<td>34</td>
</tr>
<tr>
<td>6.7</td>
<td>Configure Other Traffic Settings</td>
<td>35</td>
</tr>
<tr>
<td>7</td>
<td>Configure Record and Capture</td>
<td>37</td>
</tr>
<tr>
<td>7.1</td>
<td>Configure Format HDD</td>
<td>37</td>
</tr>
<tr>
<td>7.2</td>
<td>Configure Picture Quota</td>
<td>37</td>
</tr>
<tr>
<td>7.3</td>
<td>Configure HDD Detection</td>
<td>38</td>
</tr>
<tr>
<td>7.3.1</td>
<td>S.M.A.R.T Settings</td>
<td>38</td>
</tr>
<tr>
<td>7.3.2</td>
<td>Bad Sector Detection</td>
<td>38</td>
</tr>
<tr>
<td>7.4</td>
<td>Configure Video Parameter</td>
<td>39</td>
</tr>
<tr>
<td>7.5</td>
<td>Configure Holiday</td>
<td>39</td>
</tr>
<tr>
<td>7.6</td>
<td>Configure Record Schedule</td>
<td>40</td>
</tr>
<tr>
<td>7.7</td>
<td>Configure Manual Record</td>
<td>42</td>
</tr>
<tr>
<td>7.8</td>
<td>Play Back</td>
<td>42</td>
</tr>
<tr>
<td>7.9</td>
<td>Configure Data Search</td>
<td>42</td>
</tr>
<tr>
<td>7.9.1</td>
<td>Traffic Data Search</td>
<td>42</td>
</tr>
<tr>
<td>7.9.2</td>
<td>Traffic Parameters Statistics</td>
<td>43</td>
</tr>
<tr>
<td>7.9.3</td>
<td>Real-Time Data</td>
<td>43</td>
</tr>
<tr>
<td>8.1</td>
<td>Device Information</td>
<td>44</td>
</tr>
<tr>
<td>8.2</td>
<td>Time Settings</td>
<td>44</td>
</tr>
<tr>
<td>8.3</td>
<td>DST Settings</td>
<td>44</td>
</tr>
<tr>
<td>9</td>
<td>Serial Port Settings</td>
<td>46</td>
</tr>
<tr>
<td>9.1</td>
<td>RS-232 Serial Port</td>
<td>46</td>
</tr>
<tr>
<td>9.2</td>
<td>RS-485 Serial Port</td>
<td>46</td>
</tr>
<tr>
<td>10</td>
<td>Configure Backup</td>
<td>48</td>
</tr>
<tr>
<td>10.1</td>
<td>Configure USB Backup</td>
<td>48</td>
</tr>
<tr>
<td>10.2</td>
<td>Configure Web Backup</td>
<td>48</td>
</tr>
<tr>
<td>11</td>
<td>Uploading Data</td>
<td>50</td>
</tr>
<tr>
<td>11.1</td>
<td>Configure Host</td>
<td>50</td>
</tr>
<tr>
<td>11.2</td>
<td>Configure FTP</td>
<td>51</td>
</tr>
<tr>
<td>11.3</td>
<td>Configure Data Uploading</td>
<td>52</td>
</tr>
<tr>
<td>12</td>
<td>Configure Alarm</td>
<td>54</td>
</tr>
<tr>
<td>12.1</td>
<td>Alarm Input Settings</td>
<td>54</td>
</tr>
<tr>
<td>12.2</td>
<td>Alarm Output</td>
<td>55</td>
</tr>
<tr>
<td>12.3</td>
<td>Linkage Action</td>
<td>55</td>
</tr>
<tr>
<td>12.4</td>
<td>Alarm Exception</td>
<td>56</td>
</tr>
<tr>
<td>13</td>
<td>Status Information</td>
<td>57</td>
</tr>
<tr>
<td>13.1</td>
<td>Server Status</td>
<td>57</td>
</tr>
</tbody>
</table>
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 surveillance management platform. It is widely applied in checkpoint, Intersection Violation System, traffic surveillance 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

<table>
<thead>
<tr>
<th>Web Browser</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 8.0 and above version</td>
<td>Microsoft Windows XP SP1 and above version/Win 7/Win 8/Win 10 (32-bit or 64-bit)</td>
</tr>
<tr>
<td>Mozilla Firefox 30-41 version/Google Chrome 31.0-36.0.1985.143</td>
<td>Microsoft Windows XP SP1 and above version/Win 7/Win 8/Win 10 (32-bit only)</td>
</tr>
</tbody>
</table>
1.4 Appearance

Table 1-1 Panel Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Indicator</td>
<td>The indicator will be green when the server is powered on.</td>
</tr>
<tr>
<td>Alarm Indicator</td>
<td>The indicator will be green when the server triggers alarm.</td>
</tr>
<tr>
<td>HDD Indicator</td>
<td>The indicator will be flashing green when the HDD is reading or writing.</td>
</tr>
<tr>
<td>Ready Indicator</td>
<td>The indicator will be solid green when the sever is ready.</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Power Supply</td>
</tr>
<tr>
<td>GND</td>
<td>Ground</td>
</tr>
<tr>
<td>P1-P16 (100/1000M)</td>
<td>Gigabit Ethernet is to connect camera by P1-P16 internal network.</td>
</tr>
<tr>
<td>Gigabit Ethernet(100/1000M)</td>
<td>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.</td>
</tr>
<tr>
<td>RS-485</td>
<td>RS-485 half-duplex interface.</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Audio input/output</td>
<td>Audio input/output.</td>
</tr>
<tr>
<td>Alarm input/output</td>
<td>Alarm input/output.</td>
</tr>
<tr>
<td>USB</td>
<td>USB 3.0.</td>
</tr>
<tr>
<td>OPT</td>
<td>Fiber interface of SFP standard.</td>
</tr>
<tr>
<td>Reset</td>
<td>Long press for 5 seconds to restore default parameters and reboot.</td>
</tr>
<tr>
<td>GPS Antenna</td>
<td>GPS Antenna</td>
</tr>
<tr>
<td>4G Antenna</td>
<td>4G Antenna</td>
</tr>
</tbody>
</table>

**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.

**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.

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.
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**.

![Figure 2-1 Set 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.

![Figure 2-2 Installing Plug-in](image)
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](image)

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

**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.**

<table>
<thead>
<tr>
<th>NIC Type</th>
<th>AUTO</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Address</td>
<td>192.1.0.64</td>
</tr>
<tr>
<td>IPv4 Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>IPv4 Default Gateway</td>
<td></td>
</tr>
<tr>
<td>Physical Address</td>
<td>54:c4:15:11:0:8c</td>
</tr>
<tr>
<td>MTU</td>
<td>1500</td>
</tr>
</tbody>
</table>

![Figure 3-2 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.

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.**

![Figure 3-3 DDNS Settings](image)

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

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

**NOTE**

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

**WARNING**

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.

**NOTE**

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.**
Step 2 Click **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**.

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.

![NOTE]

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**, **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.**

![Security Service](image)

**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 refer 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.**

<table>
<thead>
<tr>
<th>Live View Parameters</th>
<th>TCP</th>
<th>UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stream Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Play Performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display POS Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Image Size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Start Live View</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Image Format</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Record File          |     |     |
| Record File Size     | 250M | 512M | 1G |
| Save record files to | C:\Users\wanyuqian\MT.Web\RecordFiles | | | Browse |
| Save downloaded files when playbl | C:\Users\wanyuqian\MT.Web\DownloadFiles | | | Browse |

| Capture and Clip Settings |     |     |
| Save snapshots in live view to | C:\Users\wanyuqian\MT.Web\CaptureFiles | | | Browse |
| Save snapshots when playback to | C:\Users\wanyuqian\MT.Web\PlaybackPics | | | Browse |
| Save clips when playback to | C:\Users\wanyuqian\MT.Web\PlaybackFiles | | | 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.
## Table 4-1 Live View 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>Live View Control Bar</td>
<td>Live view control is provided.</td>
</tr>
</tbody>
</table>
Table 4-2 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>![icon]</td>
<td>Split the live view window into 1 window, 4 windows or 9 windows.</td>
<td>←</td>
<td>Turn to previous page</td>
</tr>
<tr>
<td>![icon]</td>
<td>Start live view for all the cameras</td>
<td>→</td>
<td>Turn to next page.</td>
</tr>
<tr>
<td>![icon]</td>
<td>Capture pictures for the selected camera.</td>
<td>sound/mute</td>
<td>Disable / Enable audio.</td>
</tr>
<tr>
<td>![icon]</td>
<td>Start recording for all the cameras</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4.5 Playback

**Purpose:**

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

![Playback Interface]

Figure 4-3 Playback Interface
### Table 4-3 Playback 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.</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 4-4 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="Split" /></td>
<td>Split the playback window into 1 window, 4 windows or 9 windows.</td>
<td><img src="image" alt="Stop" /></td>
<td>Stop playback for all cameras.</td>
</tr>
<tr>
<td><img src="image" alt="Start/Pause" /></td>
<td>Start/pause playback for selected camera.</td>
<td><img src="image" alt="Capture" /></td>
<td>Capture pictures for the selected camera.</td>
</tr>
<tr>
<td><img src="image" alt="Stop" /></td>
<td>Stop playback for selected camera.</td>
<td><img src="image" alt="Download" /></td>
<td>Download record files.</td>
</tr>
<tr>
<td><img src="image" alt="Slow Forward" /></td>
<td>Slow forward.</td>
<td><img src="image" alt="Clip" /></td>
<td>Clip.</td>
</tr>
<tr>
<td><img src="image" alt="Fast Forward" /></td>
<td>Fast forward.</td>
<td><img src="image" alt="Audio" /></td>
<td>Audio.</td>
</tr>
<tr>
<td><img src="image" alt="Start Single Frame" /></td>
<td>Start single frame playback.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 Blacklist and Whitelist

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

Enter blacklist/whitelist interface.

5.2.1 Add List
Step 1 Go to **Param Config. > Advanced Settings > Vehicle Arming > Arming Management.**
Step 2 Click **Add.**
Step 3 Select **Arming Type** as **Black List** or **White List**.

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 blacklists and whitelists to delete.

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

### 5.2.3 Search List

*Purpose:*

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

Step 1 Select **Arming Type** as **Black List** or **White List** 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 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.
License plate numbers will be exported in an Excel file.

- Arming Type: 0 refers to Whitelist. 1 refers to Blacklist.
- Status: 0 refers to disabled. 1 refers to enabled.

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

**Import List**

*Purpose:*

You can import license plate numbers to blacklist or whitelist 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.

**NOTE**

- Arming Type can only be 1 or 2. 0: whitelist. 1: blacklist.
- 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**.
Step 4 Check **Enable**.

Step 5 Configure section parameters and vehicle speeding parameters.

- **Segment Name**: Enter **Segment Name** according to actuality.
- **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**.

<table>
<thead>
<tr>
<th>Parameter Configuration</th>
<th>Camera Matching</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ Enable</td>
<td></td>
</tr>
<tr>
<td>Linkage Action</td>
<td>Coil Linkage</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mains/Sub Channel</th>
<th>Camera No.</th>
<th>Main Channel</th>
<th>Sub Channel</th>
<th>Deselect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1(10.10.112.37)</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>2(10.10.112.37)</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
</tbody>
</table>

![Figure 5-3 Camera Matching](image)

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

<table>
<thead>
<tr>
<th>Parameter Config</th>
<th>Channel Linkage</th>
<th>Real-Time Matching Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice: You need to disable picture composition if you want to enable this function.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>☑ Face Evidence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>☑ Compose</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Captured Pictures</td>
<td>303(3)</td>
<td></td>
</tr>
<tr>
<td>4 Captured Pictures</td>
<td>601(7)</td>
<td></td>
</tr>
<tr>
<td>Maximum Size of Picture(…)</td>
<td>4096</td>
<td></td>
</tr>
<tr>
<td>Original Picture Zoom Multiplier</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Matching Retrospect Time(s)</td>
<td>90</td>
<td></td>
</tr>
<tr>
<td>Matching Delay Time(s)</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Data Type</td>
<td>2 Selected, Total 36</td>
<td></td>
</tr>
</tbody>
</table>

#### 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 “

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**.

Step 2 Select camera to configure in Camera dropdown list.

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

- **Camera for Video Surveillance**: 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.
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.
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.

NOTE

- HDD amount varies according to different models. You can refer to specification for details.
- Format HDD will cause HDD blacklist data lost. Export and save the blacklist 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.

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): 3726
Used Capacity for Picture... 256
Picture Quota (GB) 256

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.

<table>
<thead>
<tr>
<th>S.M.A.R.T. Detection</th>
<th>Bad Sector Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDD No.</td>
<td>1</td>
</tr>
<tr>
<td>Self-test Status</td>
<td>Not tested.</td>
</tr>
<tr>
<td>Self-test Type</td>
<td>Short Test</td>
</tr>
<tr>
<td>S.M.A.R.T.</td>
<td>Start Detecting</td>
</tr>
<tr>
<td>Temperature</td>
<td>43°C</td>
</tr>
<tr>
<td>Used Time</td>
<td>1760 Day(s)</td>
</tr>
<tr>
<td>Self-evaluation</td>
<td>Approved</td>
</tr>
<tr>
<td>All-evaluation</td>
<td>Functional</td>
</tr>
</tbody>
</table>

**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.**

![Video Settings](image)

**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.**
Step 2 Click “📝” to edit the holiday.

![NOTE]

Up to 32 holidays can be configured.

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.**
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>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Split" /></td>
<td>Split the playback window into 1 window, 4 windows or 9 windows.</td>
<td><img src="image2" alt="Stop" /></td>
<td>Stop playback for all cameras.</td>
</tr>
<tr>
<td><img src="image3" alt="Start/Pause" /></td>
<td>Start/pause playback for selected camera.</td>
<td><img src="image4" alt="Capture" /></td>
<td>Capture pictures for the selected camera.</td>
</tr>
<tr>
<td><img src="image5" alt="Stop" /></td>
<td>Stop playback for selected camera.</td>
<td><img src="image6" alt="Download" /></td>
<td>Download record files.</td>
</tr>
<tr>
<td><img src="image7" alt="Slow Forward" /></td>
<td>Slow forward.</td>
<td><img src="image8" alt="Clip" /></td>
<td>Clip.</td>
</tr>
<tr>
<td><img src="image9" alt="Fast Forward" /></td>
<td>Fast forward.</td>
<td><img src="image10" alt="Audio" /></td>
<td>Enable/disable audio.</td>
</tr>
</tbody>
</table>

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.

**NOTE**

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.
  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**.
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.

<table>
<thead>
<tr>
<th>RS232</th>
<th>Baud Rate</th>
<th>Data Bit</th>
<th>Stop Bit</th>
<th>Verification</th>
<th>Flow Control</th>
<th>Control Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>115200</td>
<td>8</td>
<td>1</td>
<td>None</td>
<td>None</td>
<td>Control Panel(By...)</td>
</tr>
<tr>
<td>2</td>
<td>115200</td>
<td>8</td>
<td>1</td>
<td>None</td>
<td>None</td>
<td>Transparent Cha...</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>RS485</th>
<th>Baud Rate</th>
<th>Data Bit</th>
<th>Stop Bit</th>
<th>Verification</th>
<th>Flow Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9600</td>
<td>8</td>
<td>2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>2</td>
<td>9600</td>
<td>8</td>
<td>2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>3</td>
<td>9600</td>
<td>8</td>
<td>2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>4</td>
<td>9600</td>
<td>8</td>
<td>2</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

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.

![USB Backup Settings](image)

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.

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.


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.**

<table>
<thead>
<tr>
<th>FTP 1</th>
<th>FTP 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter Configuration</strong></td>
<td><strong>Data Upload Configuration</strong></td>
</tr>
<tr>
<td>Host Name</td>
<td>Enable</td>
</tr>
<tr>
<td>FTP Uploading Server 1</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

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.**

![NOTE]
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.**

- Select **Alarm Input No.**
- 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.
- Enter **Alarm Name.**
- Select the time period.
- (Optional) Click **Delete** to delete the current arming schedule, or click **Save** to save the settings.

![Figure 12-1 Alarm Input Settings](image)

**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**.

![Figure 12-2 Alarm Output](image)

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 surveillance 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
- 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.

![Figure 13-1 Status](image)

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.
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.

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

![Add User Interface](image)

**Figure 14-1 Add User**

**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.
- **NetworkDisconnected:** 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](image)

**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](image)

**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](image)

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](image)

14.3.4 Export/Import 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.

![Remote Upgrade Interface](image)

**Figure 14-7 Remote Upgrade**