



# Intelligent Analyzer

User Manual

# TABLE OF CONTENTS

<b>Chapter 1 Introduction.....</b>	<b>7</b>
1.1 Introduction .....	7
1.2 Key Features.....	7
<b>Chapter 2 Start Up Device .....</b>	<b>8</b>
2.1 Activation.....	8
2.1.1 Activate Web Browser.....	8
2.1.2 Activate SADP.....	9
2.1.3 Activate Client Software.....	9
2.2 Log into Device.....	12
<b>Chapter 3 Basic Operations .....</b>	<b>13</b>
3.1 IP Camera Management .....	13
3.1.1 Activate IP Camera .....	13
3.1.2 Add IP Camera.....	13
3.1.3 Edit IP Camera.....	14
3.2 Live View.....	14
3.2.1 Start Live View .....	14
3.2.2 Live View Settings .....	15
3.3 Recording Settings .....	16
3.3.1 Format Storage Media .....	16
3.3.2 Configure Schedule .....	17
3.4 Play Video .....	17
3.4.1 Play Videos by Time.....	17
3.4.2 Play Videos by Event .....	17
3.4.3 Playback Toolbar .....	18
3.5 Backup Video .....	18
3.5.1 Back up Clipped Video .....	18
3.5.2 Download Video .....	18
<b>Chapter 4 Smart Features.....</b>	<b>20</b>
4.1 Driving Behavior Configuration.....	20
4.1.1 Calibrate IPC Position .....	20
4.1.2 Configure Driving Behavior Analysis .....	20
4.2 Configure People Counting .....	20
<b>Chapter 5 Mobile Video Record Features .....</b>	<b>22</b>
5.1 Configure Scheduled Startup/Shutdown .....	22
5.2 Configure Delayed Shutdown .....	23
5.3 Configure Satellite Positioning .....	23
5.4 Configure G-Sensor Alarm .....	24
5.5 Configure Door Settings.....	25
<b>Chapter 6 Network .....</b>	<b>26</b>
6.1 3G/4G Dialing .....	26
6.2 Set Wired Network .....	26

6.3 Remote Access .....	27
6.3.1 Mobile Surveillance Platform.....	27
6.3.2 DDNS Configuration .....	28
6.4 Configure Port.....	28
<b>Chapter 7 Camera Management .....</b>	<b>30</b>
7.1 Configure Video Parameters.....	30
7.2 Set Image Parameters .....	30
7.3 Set OSD Parameters .....	31
7.4 Set Privacy Mask .....	31
<b>Chapter 8 Event Configuration .....</b>	<b>32</b>
8.1 Configure Exception Alarm .....	32
<b>Chapter 9 Security Management.....</b>	<b>33</b>
9.1 User Management .....	33
9.2 HTTPS.....	33
9.3 Whitelist.....	34
9.4 SSH.....	34
<b>Chapter 10 Maintenance.....</b>	<b>35</b>
10.1 View System Information.....	35
10.2 Search Log File .....	35
10.3 Upgrade the System .....	35
10.4 Reboot .....	36
10.5 Restore Default Settings.....	36
10.6 Import/Export Configuration File .....	36
10.6.1 Import Configuration File.....	36
10.6.2 Export Configuration File .....	36
10.7 Time Settings .....	37
10.7.1 Configure DST Settings.....	37
10.7.2 Configure NTP .....	37
10.8 Serial Port Settings.....	38
10.8.1 RS-232 .....	38
10.8.2 RS-485.....	38

## **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 Intelligent Analyzer.

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.

## 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](http://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](http://www.recyclethis.info)

## Applicable Models

This manual is applicable to DS-MP1803.

## Symbol Conventions

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

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

## 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.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 9 to 32 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 unit is installed in a well-ventilated, dust-free environment.
- Keep all liquids away from the device.
- 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.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- 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.

# Chapter 1 Introduction

## 1.1 Introduction

Hikvision DS-MP1803 Intelligent Analyzer, based on deep-learning algorithm, is specially designed for driver behavior supervision and traffic safety protection. The product can detect multiple events such as talking on mobile phone, smoking, fatigue driving, and not looking straight ahead. When abnormal driving behaviors occur, device will warn you by overlaying the warning information on live view image. In addition, the device has other advantages including stable and tiny design, low power consumption, and easy installation and maintenance.

## 1.2 Key Features

- Based on deep-learning algorithm, provides higher object property recognition and detection rate.
- Multiple abnormal behavior detection: using mobile phone, smoking, fatigue driving, and not looking straight ahead.
- Supports accessing via WEB, easy and convenient operation.
- Stores abnormal behavior videos in SD card.
- Wide-range power input (+9 VDC to +32 VDC).
- Aviation plug ensuring stability.



## Chapter 2 Start Up Device

### 2.1 Activation

**Purpose:**

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation.

#### 2.1.1 Activate Web Browser

Step 1 Input the IP address into the address bar of the web browser, and press Enter to enter the activation interface.



- The default IP address of the camera is 192.168.1.64.
- The computer and the device should belong to the same network segment.

Step 2 Enter the same password in **Password** and **Confirm**.



**STRONG PASSWORD RECOMMENDED**—We highly recommend you create a strong password 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. 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.

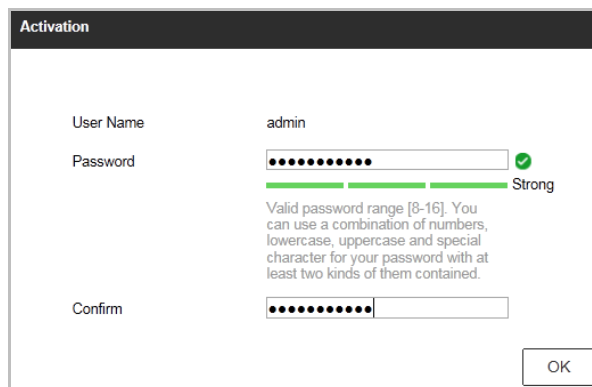
A screenshot of the 'Activation' web interface. It features a title bar 'Activation' and three input fields: 'User Name' with the value 'admin', 'Password' with a masked field and a green checkmark and 'Strong' label, and 'Confirm' with a masked field. A green progress bar is visible below the password field. A note below the password field reads: 'Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.' An 'OK' button is located at the bottom right.

Figure 2-1 Activation

Step 3 Click **OK**.



Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the device.

Step 1 Run the client software and the control panel of the software pops up.

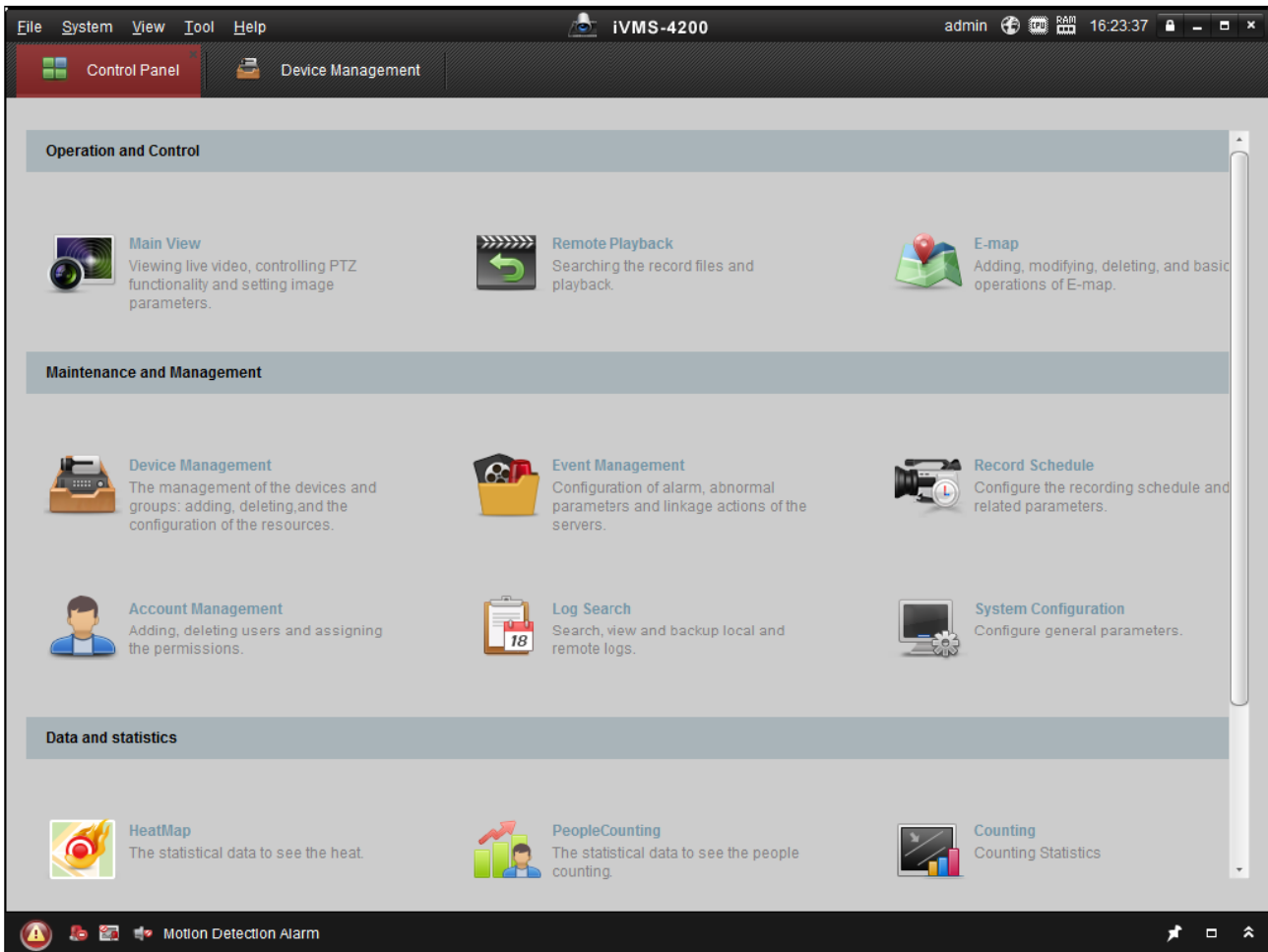


Figure 2-3 Control Panel

Step 2 Click the **Device Management** icon to enter the Device Management interface.

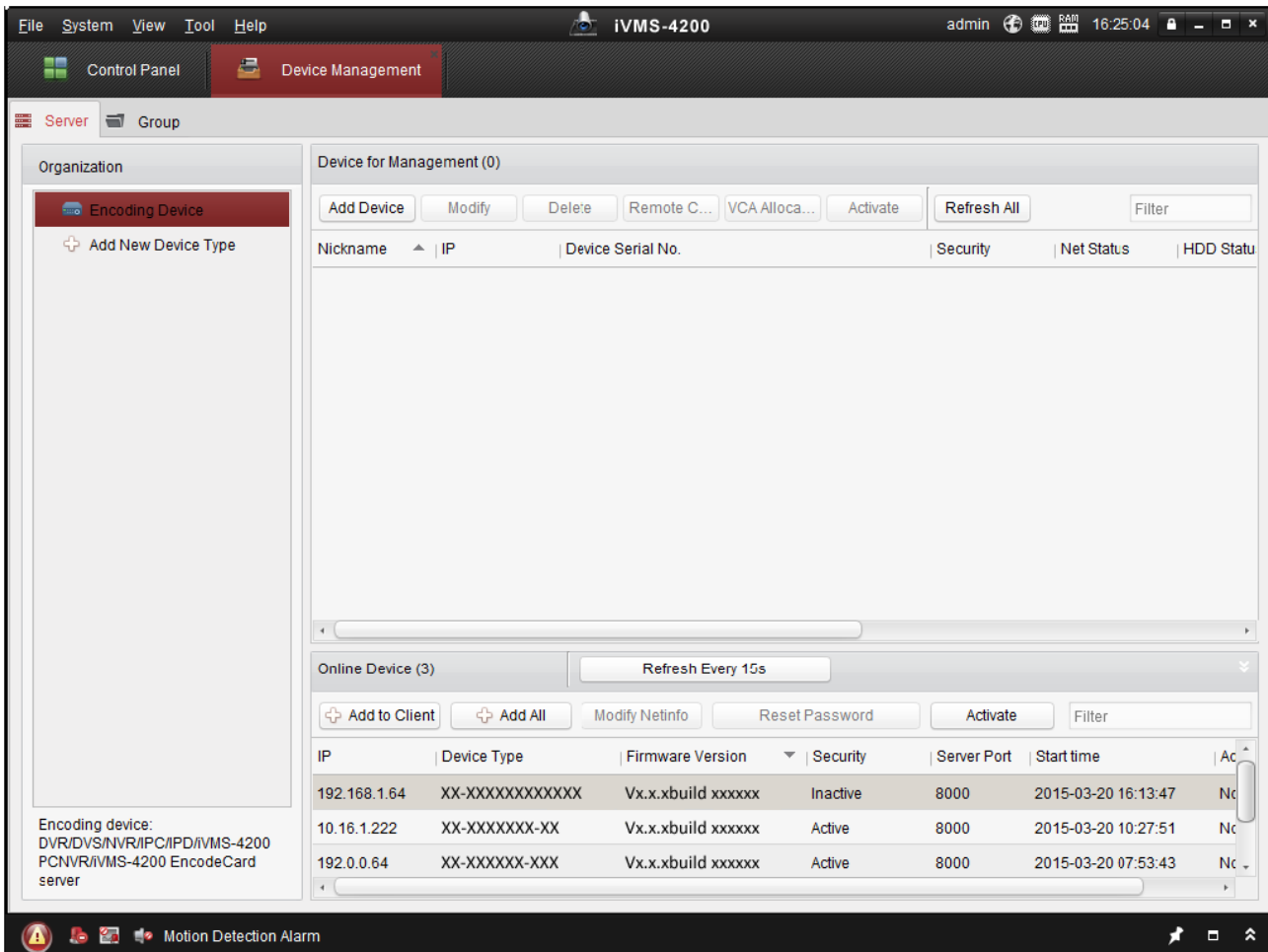


Figure 2-4 Device Management Interface

Step 3 Check the device status from the device list, and select an inactive device.

Step 4 Click the **Activate** button to pop up the Activation interface.

Step 5 Create a password and input the password in the password field, 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 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. 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.

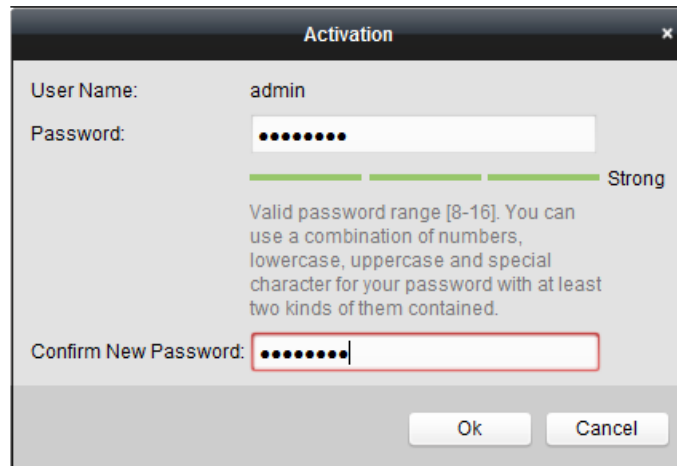


Figure 2-5 Activation

Step 6 Click **OK**.

## 2.2 Log into Device

### **Purpose:**

Get access to the device via web browser.

Step 1 Open web browser, input the IP address of the device and then press Enter.

Step 2 Enter the user name and password in the login interface and click **Login**.

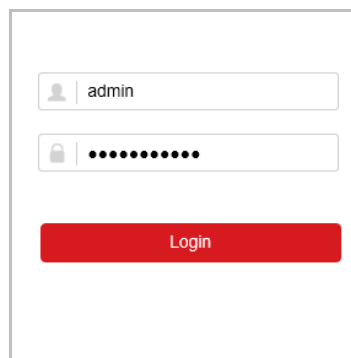


Figure 2-6 Login

Step 3 Install the plug-in before viewing the live video and managing the camera. Please follow the installation prompts to install the plug-in.

## Chapter 3 Basic Operations

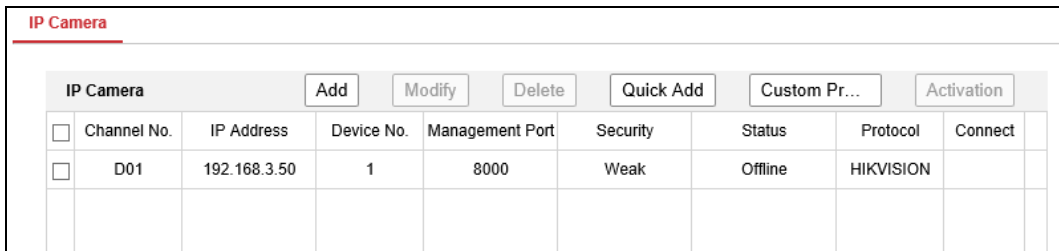
### 3.1 IP Camera Management

#### 3.1.1 Activate IP Camera

**Purpose:**

Before adding an IP camera, activate it by setting a password for it.

Step 1 Go to **Configuration > System > Camera Management**.



IP Camera								Add	Modify	Delete	Quick Add	Custom Pr...	Activation
<input type="checkbox"/>	Channel No.	IP Address	Device No.	Management Port	Security	Status	Protocol	Connect					
<input type="checkbox"/>	D01	192.168.3.50	1	8000	Weak	Offline	HIKVISION						

Figure 3-1 IP Camera

Step 2 Select an inactivated IP camera.

Step 3 Click **Activation**.

Step 4 Enter the same password in **New Password** and **Confirm**.



**WARNING**

**STRONG PASSWORD RECOMMENDED** – We highly recommend you create a strong password 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. 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 5 Click **OK**.

#### 3.1.2 Add IP Camera

**Purpose:**

You can add the activated IP cameras. Ensure the device and IP cameras are in the same network segment.

Step 1 Go to **Configuration > System > Camera Management**.

Step 2 Add IP camera.

- Quick Add:
  - 1) If the passwords of analyzer and IP camera are the same, check the online IP camera and click **Quick Add**.
- Manual Add:
  - 2) Click **Add**.
  - 3) Edit the required IP camera information, including the **IP Address, Protocol, Management Port, User Name, and Password**.
  - 4) Click **OK**.

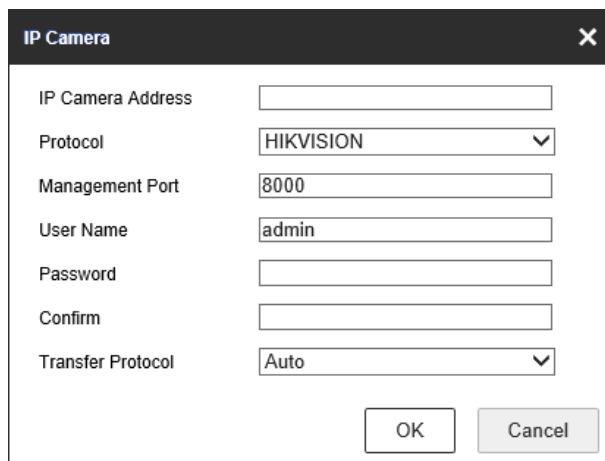


Figure 3-2 Add IP Camera

### 3.1.3 Edit IP Camera

Step 1 Select an added IP camera and click **Modify**.

Step 2 Edit the parameters.

Step 3 Enter **Password**. The password must be correct.

Step 4 Click **OK**.

## 3.2 Live View








### 3.2.1 Start Live View

Step 1 Go to **Live View**.

Step 2 Click an IP camera in IP camera list to start live view of the camera.

Or click  in toolbar to start live view of all IP camera.

Table 3-1 Icon Description

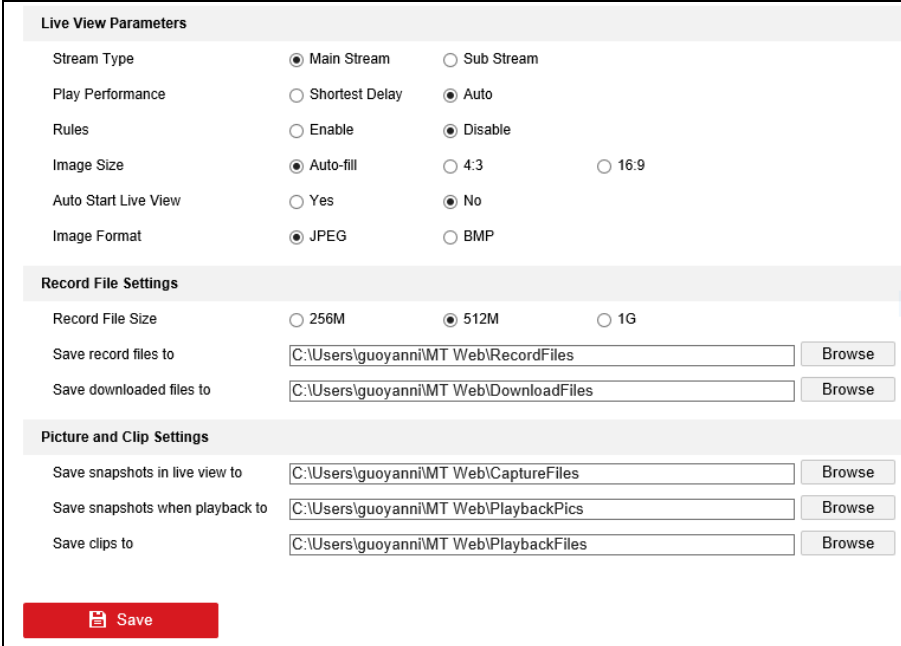
Icon	Description
	Start/stop live view of all IP cameras.
	Select live view window division.
	Select live view stream as main stream or sub-stream.
	Click it to capture one picture. Go to <b>Configuration &gt; Local &gt; Picture and Clip Settings</b> for the saving path captured pictures.
	Click it to start recording. Go to <b>Configuration &gt; Local &gt; Record File Settings</b> for the saving path recorded videos.
	Turn on/off audio.
	Full screen live view.

### 3.2.2 Live View Settings

**Purpose:**

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

Step 1 1. Enter the Local Configuration interface: **Configuration > Local**.



**Live View Parameters**

Stream Type  Main Stream  Sub Stream

Play Performance  Shortest Delay  Auto

Rules  Enable  Disable

Image Size  Auto-fill  4:3  16:9

Auto Start Live View  Yes  No

Image Format  JPEG  BMP

**Record File Settings**

Record File Size  256M  512M  1G

Save record files to

Save downloaded files to

**Picture and Clip Settings**

Save snapshots in live view to

Save snapshots when playback to

Save clips to

Figure 3-3 Live View Parameters

Step 2 Configure the following settings:



- **Live View Parameters:** Set live view performance.
  - **Stream Type:** Main stream and sub-stream are selectable.
  - **Play Performance:** Set the play performance to **Shortest Delay** or **Auto**.
  - **Rules:** Reserved.
  - **Image Size:** Auto-fill, 4:3, and 16:9 are selectable.
  - **Auto Start Live View:** Select it as **Enable** to start live view automatically.
  - **Image Format:** Choose the image format for picture capture.
- **Record File Settings:** Set the saving path of videos. Valid for the videos recorded via the web browser.
  - **Record File Size:** Select the maximum size for the manually recorded and downloaded videos to 256M, 512M or 1G.
  - **Save record files to:** Set the saving path for the manually recorded videos.
  - **Save downloaded files to:** Set the saving path for the downloaded videos in playback mode.
- **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped videos.
  - **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 videos in playback mode.

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

## 3.3 Recording Settings

### 3.3.1 Format Storage Media

**Purpose:**

A newly installed storage media must be initialized before it can be used.

Step 1 Go to **Configuration > Storage > HDD Management**.

HDD Management							Set	Format
<input type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress	
<input type="checkbox"/>	1	29.86GB	0.00GB	normal	SD Card	R/W		

Figure 3-4 Storage Management

Step 2 Check the storage media to format.

Step 3 Click **Format**.

### 3.3.2 Configure Schedule

Step 1 Go to **Configuration > Storage > Schedule Settings**.

Step 2 Check the checkbox of **Enable** to enable scheduled recording.

Step 3 Click **Advanced** to set the 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 device 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 device 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.

Step 1 Select a **Record Type**. The record type can be Continuous.

- **Continuous:** The video will be recorded automatically according to the time of the schedule.

Step 2 Select the record type, and click-and-drag the mouse on the time bar to set the record schedule.

Step 3 Click **Save**.

## 3.4 Play Video

### ***Purpose:***

View the remotely recorded videos stored in storage media.

### 3.4.1 Play Videos by Time

Step 1 Go to **Playback**.

Step 2 Click **Search** above the calendar.

Step 3 Select camera and date.

Step 4 Click **Search**.

Step 5 Click  to play the founded videos.

### 3.4.2 Play Videos by Event

Step 1 Go to **Playback**.

Step 2 Click **Search by Event** above the calendar.











Step 3 Set **Event Type**, **Event Sub Type**, **video Start Time**, and **video End Time**.

Step 4 Click **Search**.

Step 5 Click  to play the founded videos.

### 3.4.3 Playback Toolbar

Table 3-2 Toolbar Description

Icon	Description	Icon	Description
	Pause.		Play reverse.
	Stop.		Slow down.
	Speed up.		Single frame playback.
	Stop all playback.		Full screen playback.
	Capture		Turn on audio.


## 3.5 Backup Video

### 3.5.1 Back up Clipped Video

Step 1 Go to **Playback**.

Step 2 Start playback. For details, refer to 3.4.1 Play Videos by Time or 3.4.2 Play Videos by Event.

Step 3 Click  to start clipping.

Step 4 Click  to stop clipping. For the saving path of clipped video, refer to **Configuration > Local > Save clips to**.

### 3.5.2 Download Video

Step 1 Go to **Playback**.

Step 2 Click .

Step 3 Set Search Conditions.

Step 4 Click **Search**.

Step 5 Check videos to download and click **Download**. For the saving path of downloaded video, refer to **Configuration > Local > Save downloaded files to**.



## Chapter 4 Smart Features

### 4.1 Driving Behavior Configuration

**Purpose:**

Driving behavior detection is on by default. Configure driving behavior detection parameters to achieve best analysis effect.

#### 4.1.1 Calibrate IPC Position

**Purpose:**

Calibrate IPC position before enabling driving behavior detection.

Step 1 Go to **Configuration > VCA > Driving Behaviors > IPC Position Calibration**.

Step 2 Adjust IPC position to make the driver face image appear in red frame.

#### 4.1.2 Configure Driving Behavior Analysis

Step 1 Go to **Configuration > VCA > Driving Behaviors > Driving Behaviors**.

Step 2 Select **Camera No.**

Step 3 Check behaviors to analyze and configure **Alarm Time** and **Confidence Interval**.

- **Alarm Time:** Device alarms when the corresponding driving behavior lasts for the set time.
- **Confidence Interval:** Available for on-the-phone detection and smoking detection. You are recommended to use the default value.
- **Stop Detections when Driving in Low-Speed:** The feature is valid when GPS positioning succeeded.
- **Voice Alarm:** When it is checked, device will send out voice alarm when a checked behavior is detected.

Step 4 Click **Save**.

### 4.2 Configure People Counting


Step 1 Go to **Configuration > VCA > People Counting**.

Step 2 Select **Camera No.**

Step 3 Adjust the counting area (red frame) position and size.

Step 4 Set detection line (orange line) position and direction. Device counts people that passing the detection line along the set direction.

5) Drag detection line to vehicle door

6) Click  to adjust detection direction. The arrow detection is the entry direction.

Step 5 Set OSD (On Screen Display) parameters. People counting result will be displayed in OSD.

7) Check **Display OSD**.

8) Adjust OSD (yellow frame) position.

9) Select **OSD Type**.

Step 6 Click **Save**.

## Chapter 5 Mobile Video Record Features

### 5.1 Configure Scheduled Startup/Shutdown

**Purpose:**

Set the scheduled startup/shutdown. The device will automatically start up/shut down according the schedule.

**Before you start:**

Wire power cord. For details, refer to quick start guide.

Step 1 Go to **Configuration > Vehicle > Basic Settings > Start**.

Step 2 Select **Auto Work Type** as **Auto Working**.

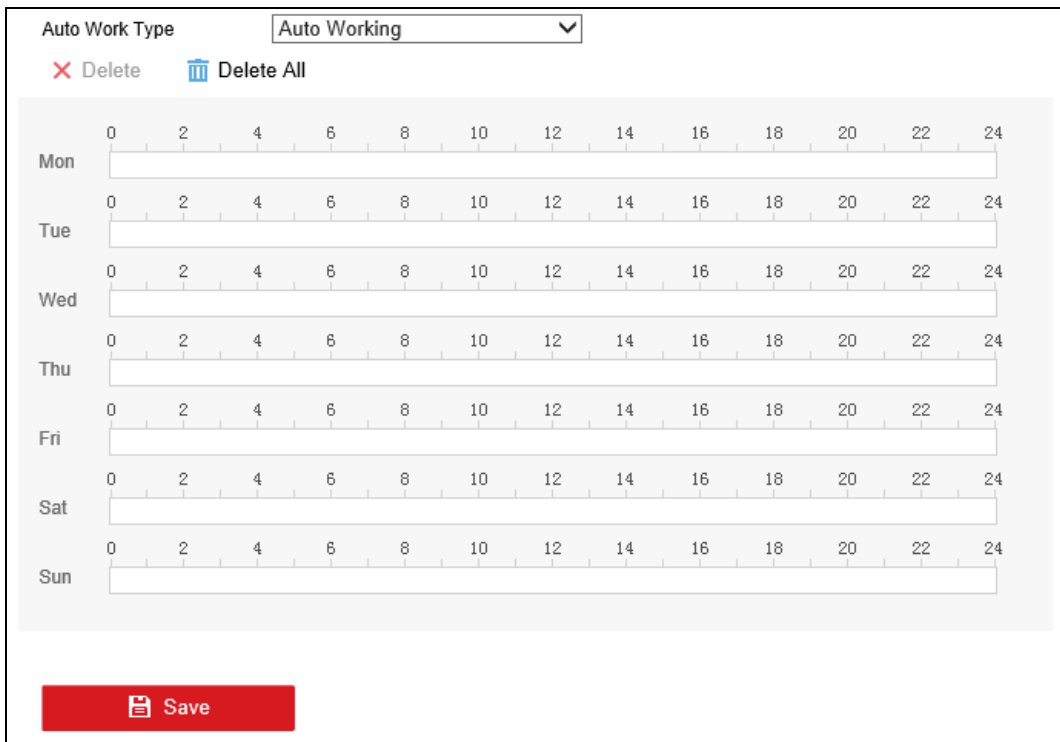


Figure 5-1 Auto Working

Step 3 Select a data and drag on the time bar to set the schedule. During the period, device is on. In other periods, device is off.

 **NOTE**

- Two periods can be configured for each day.
- The time periods cannot be overlapped each other.

Step 4 Click **Save**.

## 5.2 Configure Delayed Shutdown

### **Purpose:**

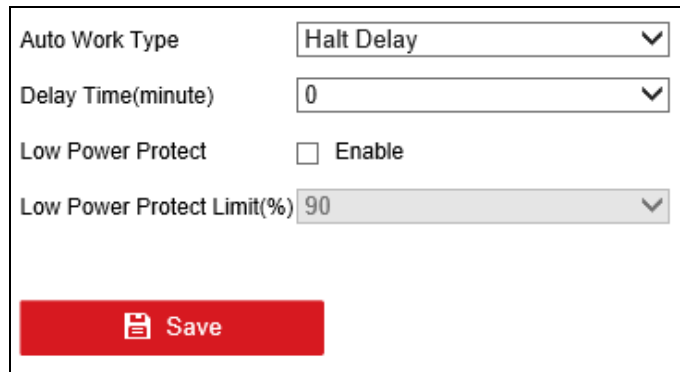
You can set the shutdown delay time (Vehicle Ignition Startup and Shutdown) for the device.

### **Before you start:**

Wire power cord. For details, refer to quick start guide.

Step 1 Go to **Configuration > Vehicle > Basic Settings > Start**.

Step 2 Select **Auto Work Type** as **Halt Delay**.



Auto Work Type	Halt Delay
Delay Time(minute)	0
Low Power Protect	<input type="checkbox"/> Enable
Low Power Protect Limit(%)	90

**Save**

Figure 5-2 Halt Delay

Step 3 Select **Delay Time**. The delay time ranges from 0 to 6 hours.

Step 4 Optionally, check **Low Power Protect** and select **Low Power Protect Limit**. If the voltage of the device reaches the selected percentage, the device will shut down automatically.

Step 5 Click **OK**.

## 5.3 Configure Satellite Positioning

### **Purpose:**

The built-in GNSS module supports GPS (Global Positioning System), enabling device positioning and speed limit alarm.

Step 1 Go to **Configuration > Vehicle > Basic Settings > Position Settings**.



Position Module	Built-In
Satellite Timing	<input type="checkbox"/> Enable
Speed Units	<input checked="" type="radio"/> Kilometers Per Hour <input type="radio"/> Miles Per Hour
Speed Limit of Alarm	100
The superimposed chann...	<input type="checkbox"/> Select All <input type="checkbox"/> D1
<input checked="" type="checkbox"/> Normal Linkage	<input checked="" type="checkbox"/> Trigger Alarm Output
<input checked="" type="checkbox"/> Audible Warning	

Figure 5-3 Position Settings

Step 2 Select **Positioning Module**.

- **Access of RS-232:** Obtain data from the connected RS-232 device.
- **Access of RS-485:** Obtain data from the connected RS-485 device.
- **Built-in:** Obtain data from the satellite positioning module built in the device.
- **Intelligent Display Terminal:** Obtain data from display terminal.

Step 3 Optionally, check **Satellite Timing** to synchronize device time with satellite time.

Step 4 Select **Speed Unit** and input **Speed Limit of Alarm**. If vehicle speed exceeds the set value, device will alarm.

Step 5 Set the linkage action for speeding alarm, including **Audible Warning** and **Alarm Output**.

Step 6 Select **The Superimposed Channel of Position**. The device positioning information will be displayed on the selected channels.

Step 7 Click **Save**.

## 5.4 Configure G-Sensor Alarm

### **Purpose:**

G-Sensor detects and records acceleration information in 3-axial (X, Y, Z) directions.

### **Before you start:**

Connect an external sensor to the device for obtaining and providing the acceleration speed in 3-axial directions.

Step 1 Go to **Configuration > Vehicle > Basic Settings > G-Sensor**.

Step 2 Select G-sensor module as **External**.

- **External:** The G-sensor is connected to the device through RS-232/RS-485 interface.
- **Built-in:** The G-sensor is a built-in module of the device.

Step 3 Set the limit value for acceleration alarm in X, Y and Z directions.



X, Y and Z represent the direction of acceleration and the unit of alarm value is G ( $G=9.8 \text{ m/s}^2$ ).

Step 4 Set the linkage actions for acceleration alarm, including **Audible Warning** and **Alarm Output**.

Step 5 Click **Save**.

## 5.5 Configure Door Settings

### **Purpose:**

Configure door settings to obtain door status via alarm input.

Step 1 Go to **Configuration > Vehicle > Basic Settings > Door Settings**.

Figure 5-4 Door Settings

Step 2 Select **Alarm Input Single Type** for both front door and rear door.

Step 3 Click **Save**.



When the detected door status is open, device will turn off driving behavior detection and turn on people counting.

## Chapter 6 Network

### 6.1 3G/4G Dialing

**Before you start:**

Install a 3G/4G SIM card on the device.

Step 1 Go to **Configuration > Network > Basic Settings > 3G/4G**.

Step 2 Check **Enable**.

Step 3 Configure the 3G/4G VPDN (Virtual Private Dialup Network) settings. Please consult the local operator for the network parameters of the VPDN.

- 10) Click **Set** of **More Settings**.
- 11) Select **Bearing Mode**.
- 12) Enter **APN** (Access Point Name), **Dial Number**, **User Name**, and **Password**.
- 13) Select **Verification Protocol**.
- 14) Click **OK**.

Step 4 Click **OK** and reboot the device to activate the new settings.

### 6.2 Set Wired Network

Step 1 Go to **Configuration > Network > Basic Settings > TCP/IP**.


NIC Type	Auto
IPv4 Address	10.16.112.60
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.16.112.254
Mac Address	a4:14:37:8c:6e:67
MTU	1500
<b>DNS Server</b>	
Preferred DNS Server	0.0.0.0
Alternate DNS Server	0.0.0.0
	

Figure 6-1 TCP/IP Settings

Step 2 Enter the device **IP Address**, **Subnet Mask**, **Default Gateway**, **DNS Server Address**, and **Download Server IP**.

Step 3 Click **Save**.

## 6.3 Remote Access

### 6.3.1 Mobile Surveillance Platform

#### **Purpose:**

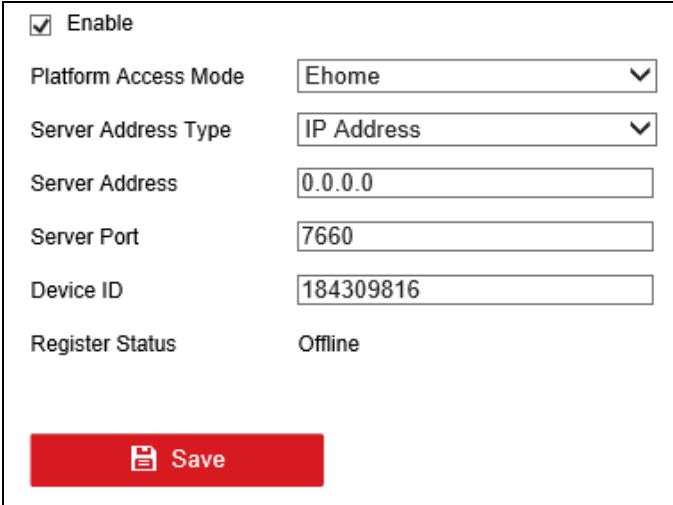
The device can be remotely accessed via mobile surveillance platform. For details of platform configuration, you can refer to platform user manual.

When your device and mobile surveillance platform are not in the same network segment, network priority: 3G/4G network > Wi-Fi > wired network.

#### **Before you start:**

Create the device ID on the mobile surveillance platform.

Step 1 Go to **Configuration > Network > Advanced Settings > Platform**.



<input checked="" type="checkbox"/> Enable	
Platform Access Mode	Ehome
Server Address Type	IP Address
Server Address	0.0.0.0
Server Port	7660
Device ID	184309816
Register Status	Offline

Save

Figure 6-2 Platform Access

Step 2 Check **Enable**.

Step 3 Select **Platform Access Mode** as **Ehome**.

Step 4 Configure the following parameters.

- **Server Address Type:** **IP Address** and **Domain Name** are selectable.
- **Server Address:** Enter the static IP address of iVMS server.
- **Port No.:** The default value for mobile surveillance platform is 7660.
- **Device ID:** The ID of the device registered on the iVMS server. If you leave it empty, device logs in to the platform with serial No.

Step 5 Click **Save** and reboot the device to activate the new settings.

 **NOTE**

- You can download mobile surveillance platform to your computer by visiting our official website and going to Home > VMS > Support > Download > iVMS-5200 Mobile Surveillance. Official website: <http://www.hikvision.com/en/>
- You can download iVMS-5260M to your mobile phone by search it in app store/google play or scan QR code below.



Figure 6-3 iOS



Figure 6-4 Android

## 6.3.2 DDNS Configuration

**Purpose:**

If your device is set to use PPPoE as its default network connection, you can use the Dynamic DNS (DDNS) for network access.

**Before you start:**

Register your device on the DDNS server.

Step 1 Go to **Configuration > Network > Basic Settings > DDNS**.

Step 2 Check **Enable DDNS**.

Step 3 Select **DDNS Type**.

Step 4 Enter **Server** information.

Step 5 Click **Save** and reboot the device to take effect the settings.

## 6.4 Configure Port

**Purpose:**

You can set the port No. of the device.

Step 1 Go to **Configuration > Network > Basic Settings > Port**.

HTTP Port	<input type="text" value="80"/>
RTSP Port	<input type="text" value="554"/>
HTTPS Port	<input type="text" value="443"/>
Server Port	<input type="text" value="8000"/>


 Save

Figure 6-5 Port Settings

Step 2 Set the HTTP port, RTSP port, HTTPS port, and server port.

- **HTTP Port:** The default port number is 80, and it can be changed to any port No. which is not occupied.
- **RTSP Port:** The default port number is 554 and it can be changed to any port No. ranges from 1 to 65535.
- **HTTPS Port:** The default port number is 443, and it can be changed to any port No. which is not occupied.
- **Server Port:** The default server port number is 8000, and it can be changed to any port No. ranges from 2000 to 65535.

Step 3 Click **Save** and reboot the device to take effect the settings.

## Chapter 7 Camera Management

### 7.1 Configure Video Parameters

**Purpose:**

Configure the transmission stream type, the resolution, frame rate, etc.

Step 1 Go to **Configuration > Video/Audio**.

Step 2 Select **Channel No.**

Step 3 Configure the video parameters.

- **Stream Type**

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

- **Video Type**

Video and Video & Audio are selectable.

- **Bitrate Type**

- **Variable** and **Constant** are selectable.
- **Variable:** The video quality is configurable.
- **Constant:** The video quality is set as Medium and cannot be edited.

- **Video Quality**

Bitrate type is variable, you can set the video quality as Highest, Higher, Medium, Low, Lower, or Lowest.

- **Frame Rate**

Frame rate refers to the frequency of the image frame after compression. With other parameters constant, reduce the video frame rate, and you can lower the maximum bitrate to some extent.

- **Max. Bitrate(Kbps)**

Select the fixed value provided by the system or customize the maximum bitrate as desired.

Step 4 Click **Save**.

### 7.2 Set Image Parameters

Step 1 Go to **Configuration > Image > Display Settings**.

Step 2 Adjust the image parameters.

## 7.3 Set OSD Parameters

***Purpose:***

Configure the camera name, OSD (On Screen Display) settings, etc.

Step 1 Go to **Configuration > Image > OSD Settings**.

Step 2 Select **Channel No.**

Step 3 Edit parameters as your desire.

Step 4 Click **Save**.

## 7.4 Set Privacy Mask

***Purpose:***

The privacy mask can be used to protect personal privacy by concealing parts of the image from view or recording with a masked area.

Step 1 Go to **Configuration > Image > Privacy Mask**.

Step 2 Select **Channel No.**

Step 3 Check **Enable Private Mask**.

Step 4 Draw areas in live view window.

Step 5 Click **Save**.



## Chapter 8 Event Configuration

### 8.1 Configure Exception Alarm

**Purpose:**

Configure alarms which are triggered by exceptions to take necessary actions in time.

Exception types include:

- **HDD Full:** Storage media is full.
- **HDD Error:** Writing storage media error, unformatted storage media, etc.
- **Network Disconnected:** Network cable is disconnected.
- **IP Address Conflicted:** Duplicated IP address.
- **Illegal Login:** Incorrect user ID or password.
- **Record/Capture Exception:** Recording or capture exception.

Step 1 Go to **Configuration > Event > Basic Event > Exception**.

The screenshot shows a configuration window for an exception type. At the top, 'Exception Type' is set to 'HDD Full'. Below this, there are two columns of options. The left column contains three unchecked checkboxes: 'Normal Linkage', 'Audible Warning', and 'Notify Surveillance Center'. The right column contains one checked checkbox: 'Trigger Alarm Output'. At the bottom of the window is a red 'Save' button with a document icon.

Figure 8-1 Exception

Step 2 Select **Exception Type** and set corresponding alarm linkage actions, including audible warning and alarm output.

Step 3 Click **Save**.

## Chapter 9 Security Management

### 9.1 User Management

**Purpose:**

Add and delete users, and modify the password and permission of users.

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

User List			Add	Modify	Delete
No.	User Name	Level			
1	admin	Administrator			

Figure 9-1 User Management

Step 2 Click **Add**.

Step 3 Enter **User Name** and **Password** and enter the same password in **Confirm**.

Step 4 Select the user permission level.

- **Operator:** The operator has permissions for Preview, Playback, Backup, Log Search and Parameters Settings.
- **Guest:** The Guest has permissions for Preview, Playback, Backup and Log Search.

Step 5 Select user permission as needed.

Step 6 Click **OK**.

### 9.2 HTTPS

**Purpose:**

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

E.g., If you set the port number as 443 and the IP address is 192.168.1.64, you may access the device by inputting https://192.168.1.64:443 via the web browser.

Step 1 Go to **Configuration > Network > Advanced Settings > HTTPS**.

Step 2 Check **Enable**.

Step 3 Create the self-signed certificate or authorized certificate.

- Create the self-signed certificate
  - 1) Select **Create Self-signed Certificate** as the Installation Method.

- 2) Click **Create** button to enter the creation interface.
- 3) Enter country, host name/IP, validity and other information.
- 4) Click **OK**.



**NOTE**

If you already had a certificate installed, the Create Self-signed Certificate is grayed out.

- Create the authorized certificate
  - 1) Select Create the certificate request first and continue the installation as the Installation Method.
  - 2) Click Create button to create the certificate request. Fill in the required information in the popup window.
  - 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.

Step 4 There will be the certificate information after your successfully creating and installing the certificate.

Step 5 Click **Save**.

## 9.3 Whitelist

***Purpose:***

The device provides software-based firewall to protect the device against the threats from the public network. A white list can be set, and only the trusted IP addresses on the white list can access the device via the network.

Step 1 Go to **Configuration > System > Security > White List**.

Step 2 Check **Enable White List**.

Step 3 Click **Add**.

Step 4 Enter **IP Address** of the computer that needs to visit the device and click **OK**.

## 9.4 SSH

***Purpose:***

Disable SSH to improve network security. The feature is designed for professionals to debug device.

Step 1 Go to **Configuration > System > Security > Security Service**.

Step 2 Check/Uncheck **Enable SSH**.

Step 3 Click **Save**.

## Chapter 10 Maintenance

### 10.1 View System Information

Go to **Configuration > System > System Settings > Basic Information** to view device information.

### 10.2 Search Log File

**Purpose:**

The operation, alarm, exception and information of the device can be stored in log files, which can be viewed and exported at any time.

Step 1 Go to **Configuration > System > Maintenance > Log**.

The screenshot displays a web interface for searching log files. At the top, there are two dropdown menus for 'Major Type' and 'Minor Type', both set to 'All Types'. Below these are two date-time input fields: 'Start Time' (2018-06-06 00:00:00) and 'End Time' (2018-06-06 23:59:59), each with a calendar icon. A 'Search' button is located to the right of the 'End Time' field. Below the search filters is a 'Log List' section with an 'Export' button. The log list is a table with the following columns: No., Time, Major Type, Minor Type, Channel No., Local/Remote User, and Remote Host IP. The table is currently empty. At the bottom right of the table area, it shows 'Total 0 Items' and navigation controls: '<<', '<', '0/0', '>', and '>>'.

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
-----	------	------------	------------	-------------	-------------------	----------------

Figure 10-1 Log

Step 2 Select log **Major Type** and **Minor Type**.

Step 3 Specify log **Start Time** and **End Time**.

Step 4 Click **Search**.

### 10.3 Upgrade the System

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance**.

Step 2 Click **Browser** and select upgrade file.



Figure 10-2 Upgrade

Step 3 Click **Upgrade** to start upgrading and reboot the device to activate the new settings.

## 10.4 Reboot

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance**.

Step 2 Click **Reboot** and click **OK** on popup dialog box to reboot the device.

## 10.5 Restore Default Settings

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance**.

Step 2 Click to select the restoring type from the following two options.

- **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.

Step 3 Click **OK** on popup dialog box.

## 10.6 Import/Export Configuration File

### 10.6.1 Import Configuration File

**Purpose:**

The configuration files of one device can be imported to multiple device devices if they are to be configured with the same parameters.

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance**.

Step 2 Click **Browser** of **Import Config. File** section frame and select configuration file to import.

Step 3 Click **Import**.

Step 4 Click **OK** on confirmation dialog box.

### 10.6.2 Export Configuration File

**Purpose:**

The configuration files of the device can be exported to local path for backup.

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance**.

Step 2 Click **Device Parameters** of **Export** section frame and select the local path to save the configuration file.

## 10.7 Time Settings

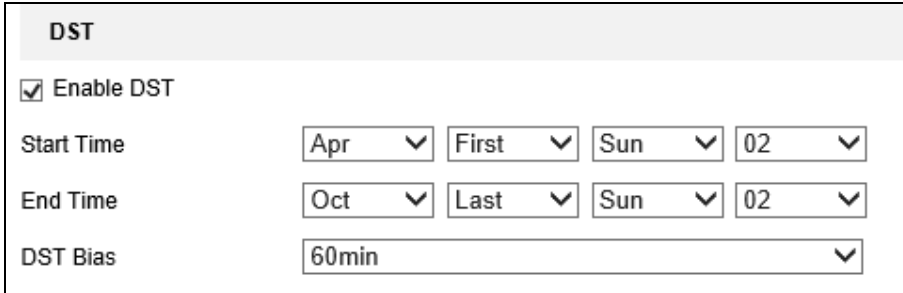
### 10.7.1 Configure DST Settings

**Purpose:**

Configure DST (Daylight Saving Time) settings for the system.

Step 1 Go to **Configuration > System > System Settings > Time Settings**.

Step 2 Check **Enable DST**.



DST			
<input checked="" type="checkbox"/> Enable DST			
Start Time	Apr	First	Sun 02
End Time	Oct	Last	Sun 02
DST Bias	60min		

Figure 10-3 DST

Step 3 Set **Start Time** and **End Time** for DST.

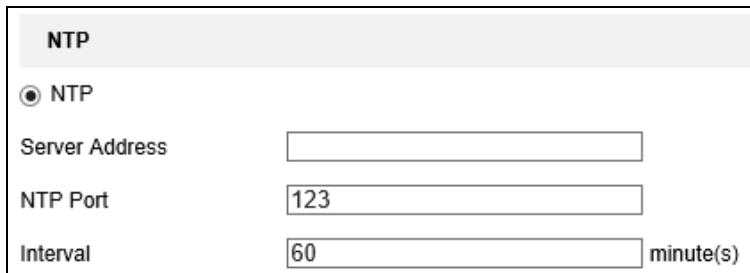
Step 4 Select **DST Bias**.

Step 5 Click **Save**.

### 10.7.2 Configure NTP

Step 1 Go to **Configuration > System > System Settings > Time Settings**.

Step 2 Select **NTP**.



NTP	
<input checked="" type="radio"/> NTP	
Server Address	
NTP Port	123
Interval	60 minute(s)

Figure 10-4 NTP Settings

Step 3 Enter NTP **Server address** and **NTP Port**.

Step 4 Enter time synchronization **Interval**.

Step 5 Click **Save**.

## 10.8 Serial Port Settings

### ***Purpose:***

Two types of serial ports are provided: RS-232 and RS-485.

### 10.8.1 RS-232

The RS-232 port can be used in two ways:

- **Console:** Connect a computer to the device through the computer serial port. Device parameters can be configured by using software such as HyperTerminal. The serial port parameters must be the same as of the device when connecting with the computer serial port.
- **Transparent Channel:** Connect a serial device directly to the device. The serial device will be controlled remotely by the PC through the network and the protocol of the serial device. If alarm button is connected, select RS-232 usage as Transparent Channel.

Step 1 Go to **Configuration > System > System Settings > RS-232**.

Step 2 Edit parameters as required.

Step 3 Click **Save**.

### 10.8.2 RS-485

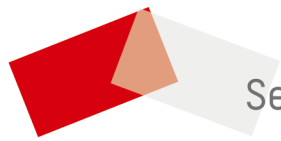
### ***Purpose:***

Configure the RS-485 parameters the same with RS-485 device connected to the device.

Step 1 Go to **Configuration > System > System Settings > RS-485**.

Step 2 Edit parameters as required.

Step 3 Click **Save**.



See Far, Go Further