Red Light Signal Detector

User’s Manual

V1.0.0

Foreword

General

This manual introduces the functions, structure and configuration of the Red Light Signal Detector (hereinafter referred to as "the Device").

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	August 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF

format) cannot be opened.

- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the Device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This chapter introduces the contents covering proper handling of the Device, hazard prevention, and prevention of property damage. Read these contents carefully before using the Device, comply with them when using, and keep the manual well for future reference.

Power Requirements

- Strictly comply with the local electric safety standards.
- Make sure that the power supply is correct before operating the Device.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited Power Source requirement according to IEC60950-1. Note that the power supply requirement is subject to the Device label.
- Install easy-to-use device for power off before installing wiring, which is for emergent power off when necessary.
- Prevent the line cord from being trampled or pressed, especially the plug, power socket and the junction.

Operating Requirements

- Transport, use, and store the Device under allowed humidity and temperature conditions.
- Prevent any liquid from flowing into the Device.
- Do not block the ventilation near the Device.
- Do not press, vibrate or soak the Device during transportation, storage and installation.
- Pack the Device with packaging materials provided by its manufacturer or materials with the same quality before transporting it.
- Do not dissemble the Device.

Table of Contents

1 Product Overview

1.1 Introduction

The red light signal detector is an integrated and intelligent device that collects evidence with greatly improved accuracy and reliability for running red lights.

Using all-in-one design, it is a highly integrated device with a high-performance processor. Focusing on detecting running red lights, the Device has various ports and complete software functions that can apply to different environments and businesses. It can switch to red or green light detection mode. It is compact in structure, and it uploads red/green light status through the network, detects anomaly through up to 20 traffic lights and supports traffic light signal input anomaly detection.

1.2 Functions

- Communicates with camera and sends traffic light status to the camera through the 100M network port when the light status changes.
- Supports 20 channels of traffic light input with each channel linked to up to 5 camera IPs.
- Uploads traffic light status in real time.
- Supports red/green light detection mode.
- Detects traffic light signal input anomaly.
- Connects to other devices through the network to configure parameters and plans, and get information through the config tool.
- Changes account password through the config tool.
- Sets the switch gateway and enable ping.
- Synchronizes time by NTP or with PC.
- Stores logs of operation and red/green signal input anomaly.
- Hardware reset.

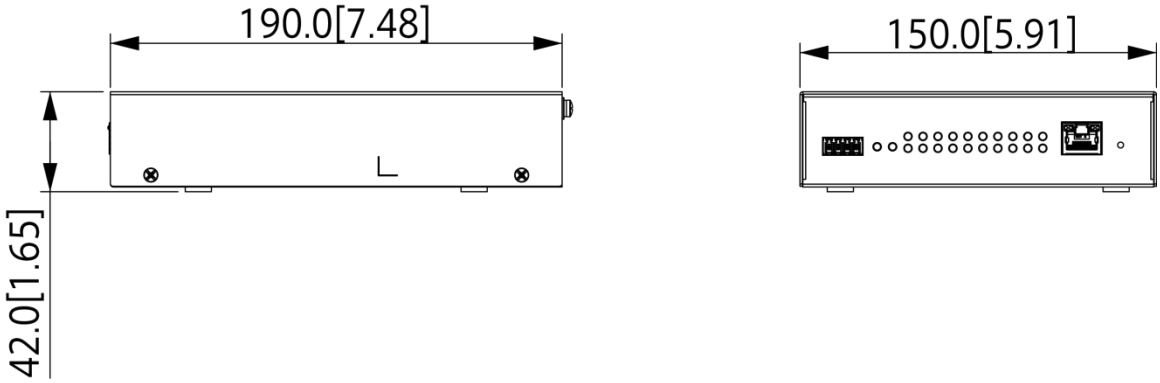
2 Structure

2.1 Appearance

Figure 2-1 Appearance

2.2 Dimensions

Figure 2-2 Dimensions (mm [inch])



2.3 Port

2.3.1 Front Panel Ports

Figure 2-3 Front panel ports

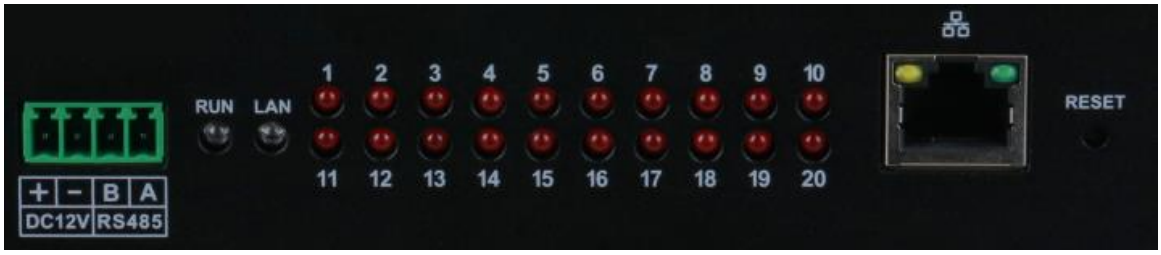
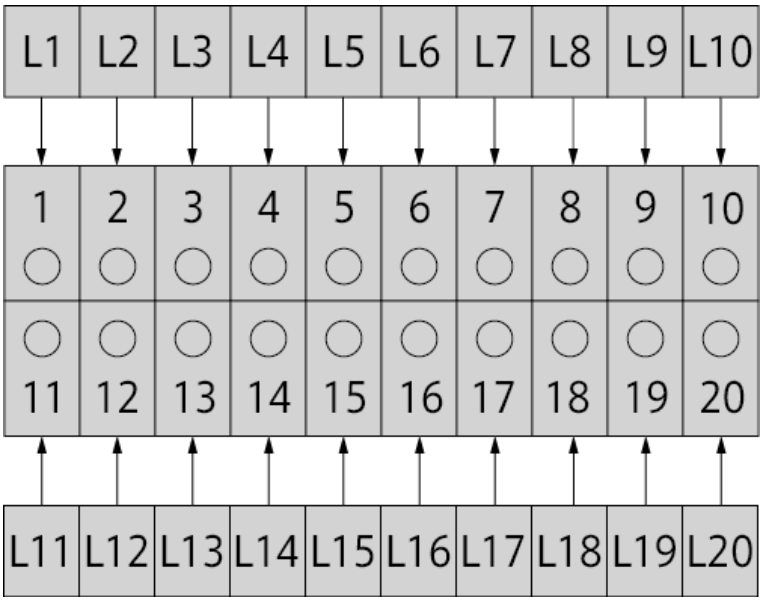


Table 2-1 Description of front panel ports

Port	Description
DC 12V+, DC 12V-	DC 12V power port, 1A.
RS-485_A, RS-485_B	Debugging serial ports.
RUN	Device activity indicator. ● Blue flashes every 0.5s: Device working. ● Solid blue: Device failure.
LAN	Network status indicator. ● Solid blue: Ping not enabled or ping failed. ● Blue flashes: Ping succeeded.
Indicator 1–20	Input status indicators that show input signal status. Indicator number corresponds with input port number L1–20. See Figure 2-4. ● Solid red: 220V signal input detected. ● Light off: Input signal not detected or channel not configured.
	RJ45 100M Ethernet port, through which the Device uploads traffic light status.
RESET	Resets all configurations except device ID, board SN number and MAC address.

Figure 2-4 Indicator light number corresponds with input port number



2.3.2 Rear Panel Ports

Figure 2-5 Rear panel ports

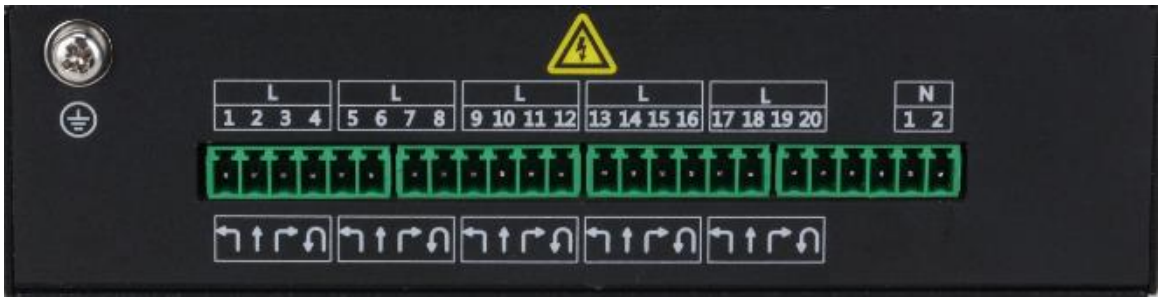


Table 2-2 Port descriptions of rear panel

Port	Description
⏚	Grounding end.
L	L1–20: 20 channels of red light input ports connected to the live wires of traffic lights.
N	● N1 and N2: 2 channels of red light input ports connected to the neutral wires of traffic lights. Connect the live and neutral wires of the red light of each entrance direction. You can connect up to 5 entrance directions, each including a set of entrance types. For example, from left to right, L1–4 represent turning left, going straight, turning right and making a U-turn. 📖 ● When different entrance types of the same entrance direction share one red light signal (for example, the **N to S** (north to south) going straight and turning right share one red light signal), you can: 1. Connect the live wire of the red light to the going straight or turning right

Port	Description
	channel and connect the neutral wire normally; 2. Open the config tool, go to **Detection Parameter > Detector** and select both **Straight** and **Right Turn** for that channel in the **Entrance Type** section. ● You can also connect the live and neutral wires of green lights. Open the config tool and switch to **Green Light Detection** mode. See Figure 4–2.

3 Web Configuration

Before configuring the Device, you need to configure the camera to be bound to the Device.

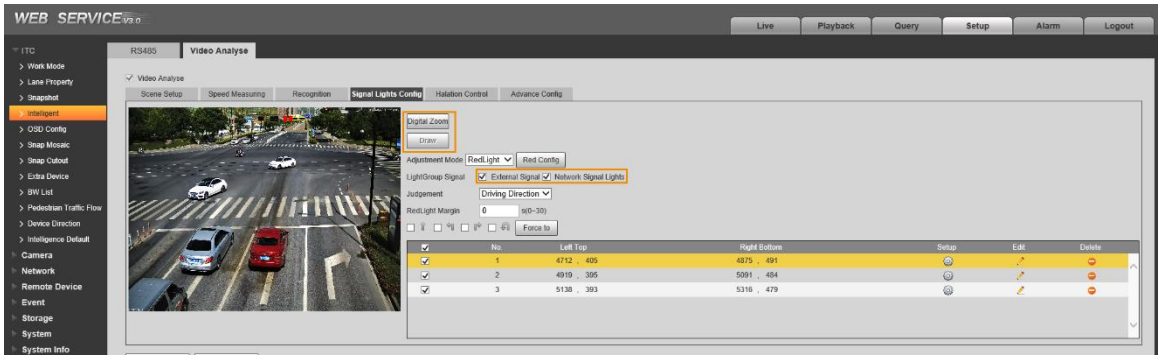
Step 1 Power on the Device. Check the status indicator. Flashing means the Device is working properly.

Step 2 Log in to the web interface of the camera. Select **Setup > ITC > Work Mode**. Set **Business Type** as **E-Police**.

Figure 3-1 Work mode

Step 3 Select **Setup > ITC > Intelligent > Video Analyse > Signal Lights Config**.

Figure 3-2 Signal lights config

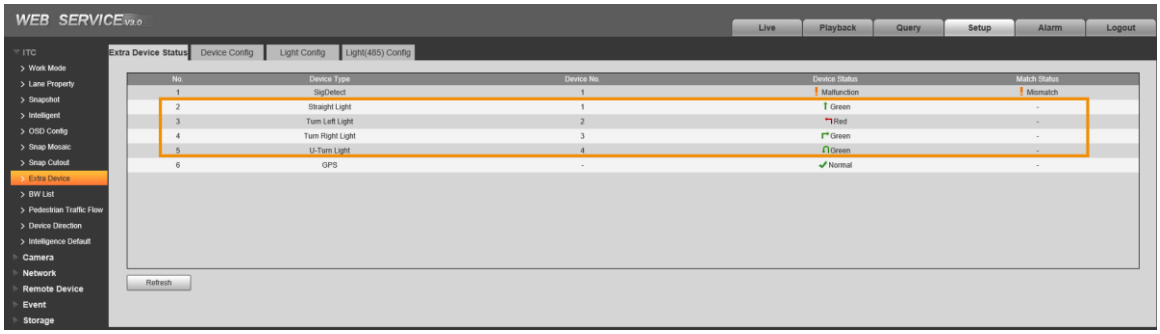


Step 4 Configure signal lights parameters.

1) Click **Digital Zoom** and draw a selection box on the video to zoom in on the traffic light. Then click **Draw** to draw the area of the traffic light to be detected.
2) Select both **External Signal** and **Network Signal Lights** under **LightGroup Signal**.
3) Click **Confirm**.

Step 5 Select **Setup > ITC > Extra Device > Extra Device Status** to check device status.

Figure 3-3 Extra device status



Click **Refresh** to get latest status.

4 Config Tool

Through the traffic light detector config tool, you can configure parameters and get status, search for logs, find help document and more.

4.1 Logging In

Step 1 Make sure that the Device is connected to the network, and the 20 channels of traffic light signal input ports are connected to 220V signal. Power on the Device.

Step 2 Open the config tool 

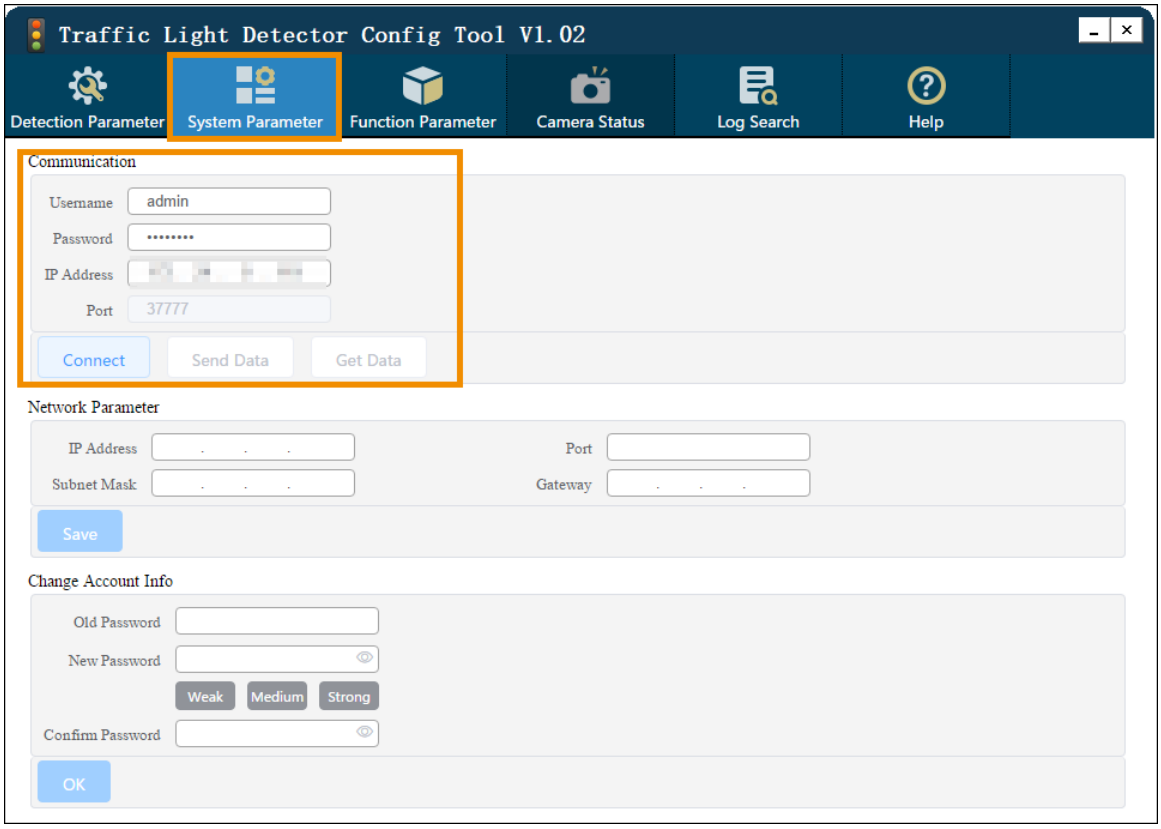
.

Please contact technical support to get the installation package.

Step 3 Click **System Parameter**.

Step 4 In the **Communication** section, enter the **Username**, **Password**, **IP Address**, and click **Connect**.

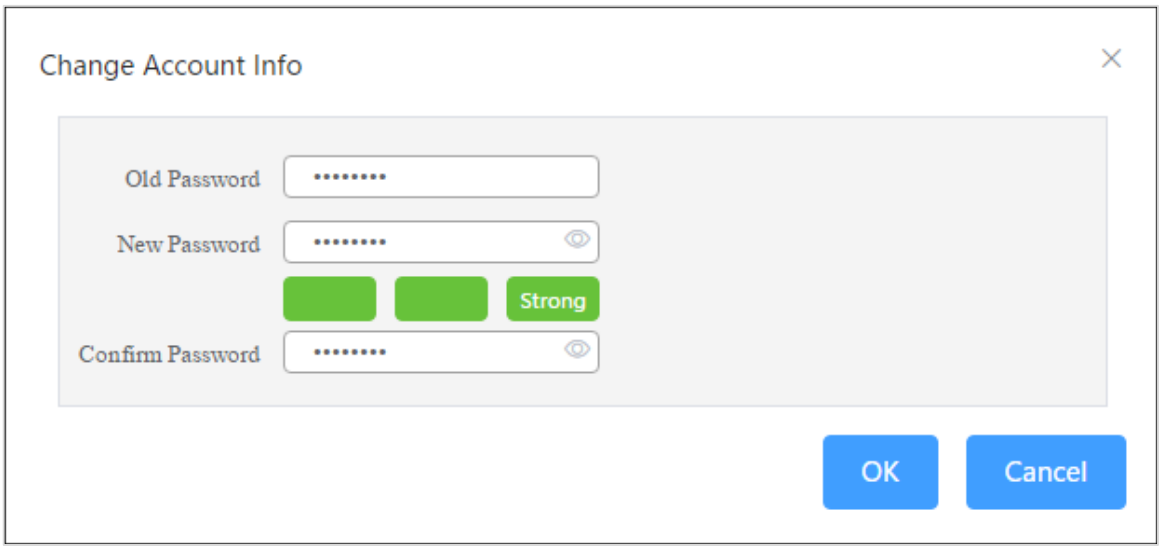
Figure 4-1 Communication



Step 5 Change password.

You can also click **Cancel** and change it later in the **Change Account Info** section. See "4.3 Changing Password."

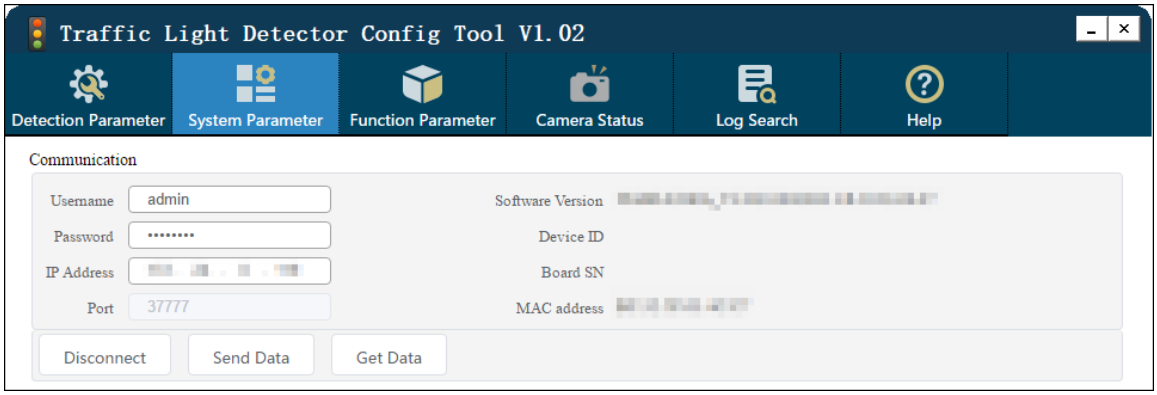
Figure 4-2 Change password



Step 6 Click **OK** to connect the client and the Device. You can check the Device information, including **Software Version**, **Device ID**, **Board SN** and **MAC address**.

The default IP address is 192.168.1.108. The default username and password are "admin" and "admin123" respectively.

Figure 4-3 Successfully connected



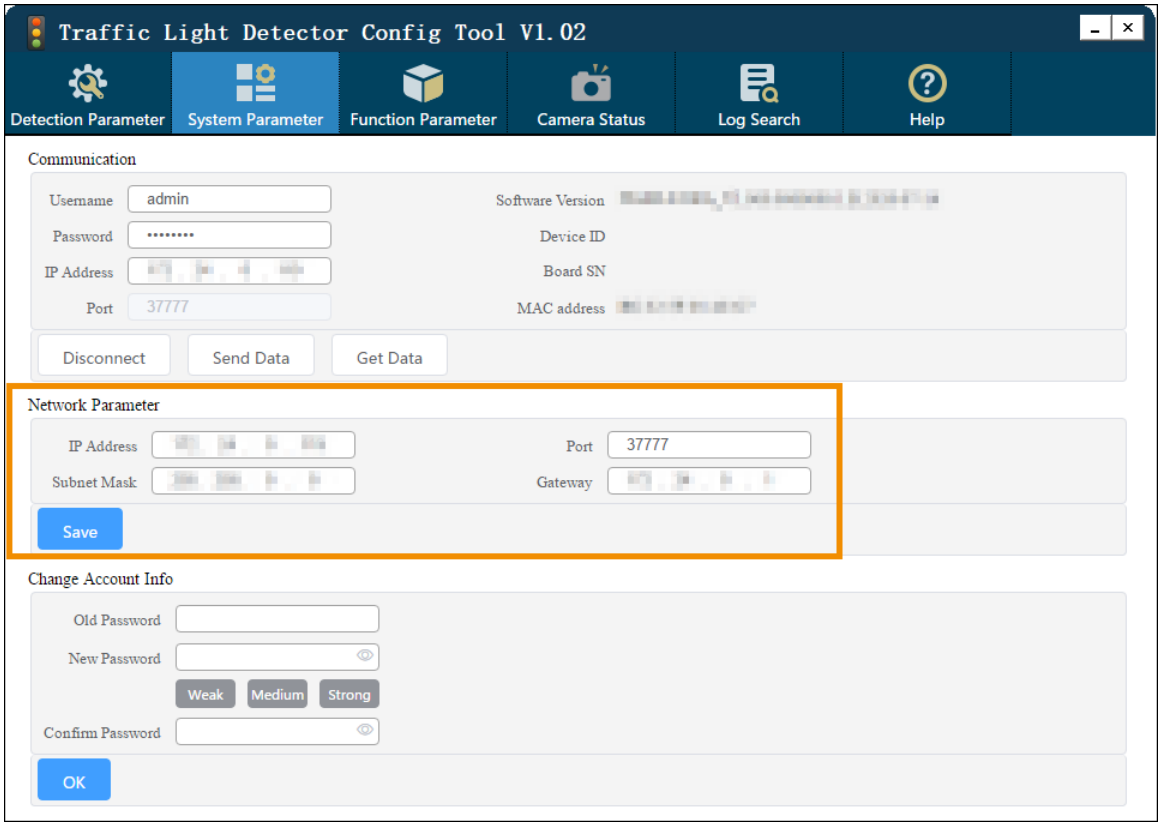
4.2 Changing IP Address

Step 1 Open the config tool and connect to the Device.

Step 2 Click **System Parameter**.

Step 3 In the **Network Parameter** section, enter the **IP Address**, **Subnet Mask** and **Gateway**.

Figure 4-4 Network parameter



Step 4 Click **Save**, restart the Device and the configuration takes effect.

4.3 Changing Password

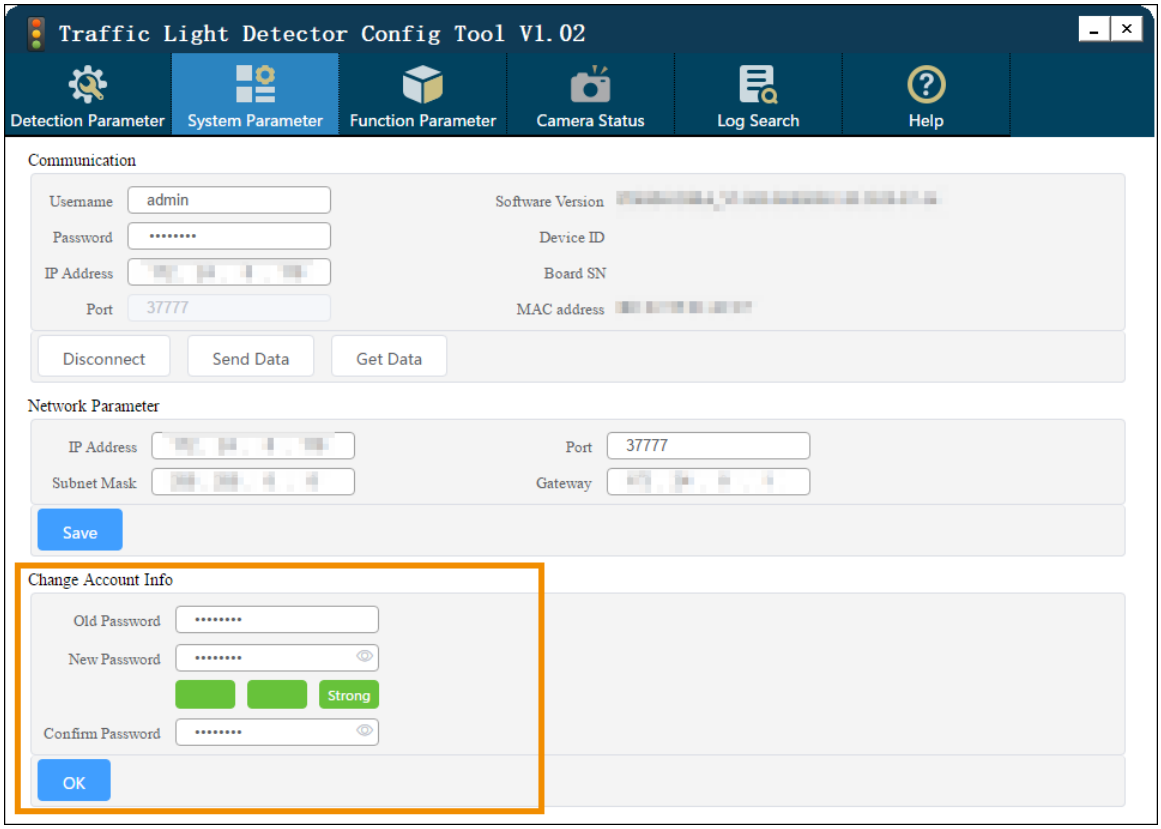
You can change the password used to connect to the Device.

Step 1 Open the config tool and connect to the Device.

Step 2 Click **System Parameter**.

Step 3 In the **Change Account Info** section, enter **Old Password**, **New Password** and **Confirm Password**.

Figure 4-5 Change account info



Step 4 Click **OK**, the change takes effect immediately and the new password is automatically filled in in the **Communication** section.

4.4 Configuring Detection Parameter

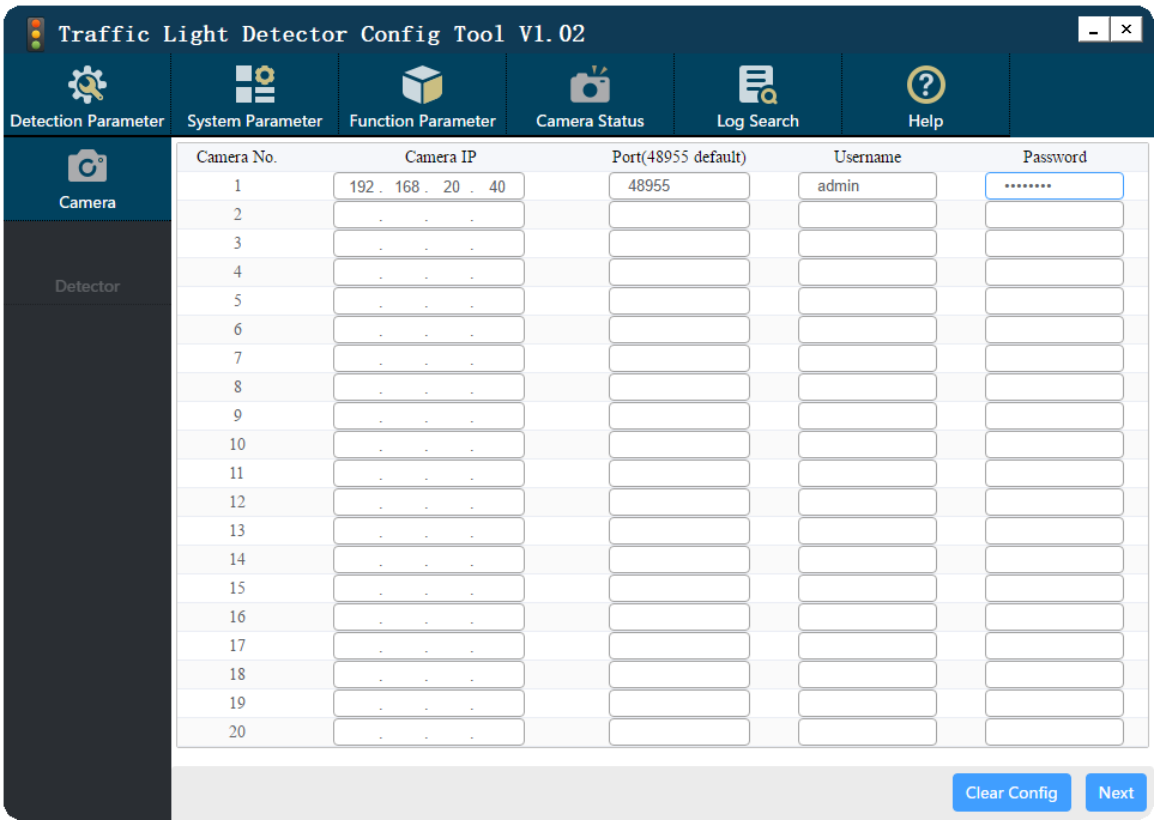
You can bind multiple cameras to the Device and configure parameters to monitor the traffic light status from these cameras.

Step 1 Open the config tool and connect to the Device. Click **Detection Parameter**.

Step 2 Enter **Camera IP**, **Port**, **Username** and **Password**.

The Device can bind to 20 cameras at most.

Figure 4-6 Camera



Step 3 Click **Next** to configure **Detector** parameters.

Figure 4-7 Detector

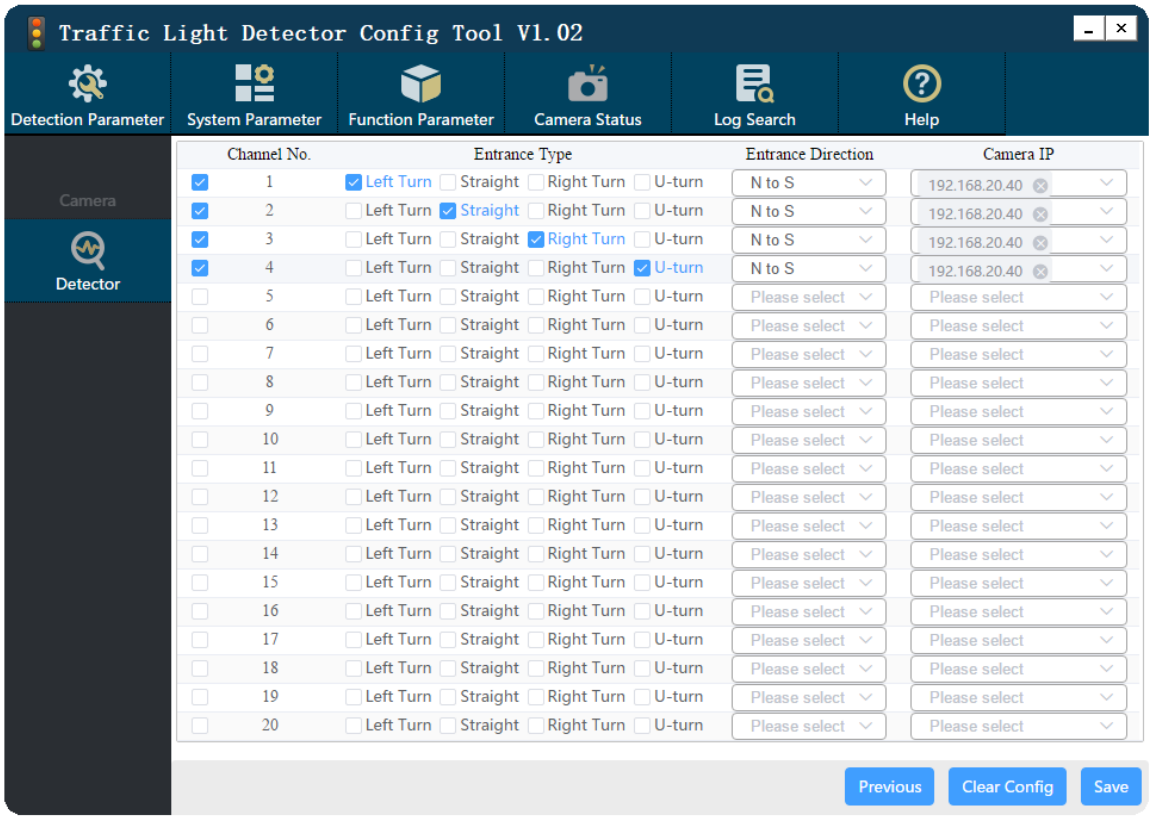


Table 4-1 Detection parameters

Parameter	Description
Entrance Type	Select the entrance type(s) for the channel, including **Left Turn**, **Straight**, **Right Turn** and **U-turn**. ● You can select more than one entrance types for one channel. ● If you select the same camera IP for different channels, their entrance types cannot be overlapped.
Entrance Direction	Select **Entrance Direction** for each channel, including north to south (**N to S**), northeast to southwest (**NE to SW**), east to west (**E to W**), southeast to northwest (**SE to NW**), south to north (**S to N**), southwest to northeast (**SW to NE**), west to east (**W to E**) and northwest to southeast (**NW to SE**).
Camera IP	Select the camera IP address. Up to 5 camera IPs can be bound to 1 channel.

Step 4 Click **Save**.

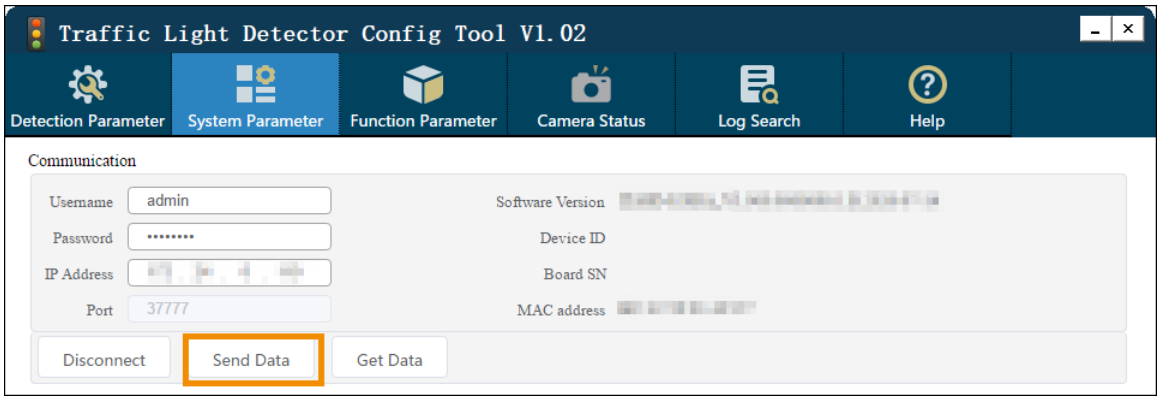
- Click **Clear Config** to clear all configurations of the current interface.
- Click **Previous** to return to **Camera** and modify the configurations.

Step 5 Send data to the Device.

1) Click **System Parameter**.
2) In the **Communication** section, click **Send Data**.

Click **Get Data** to get configurations of the connected Device.

Figure 4-8 Send data



4.5 Configuring Function Parameter

You can switch to red/green light detection mode, sync time, enable ping and more.

Step 1 Open the config tool and connect to the Device. Click **Function Parameter**.

Step 2 Configure the parameters as needed.

Figure 4-9 Function parameter

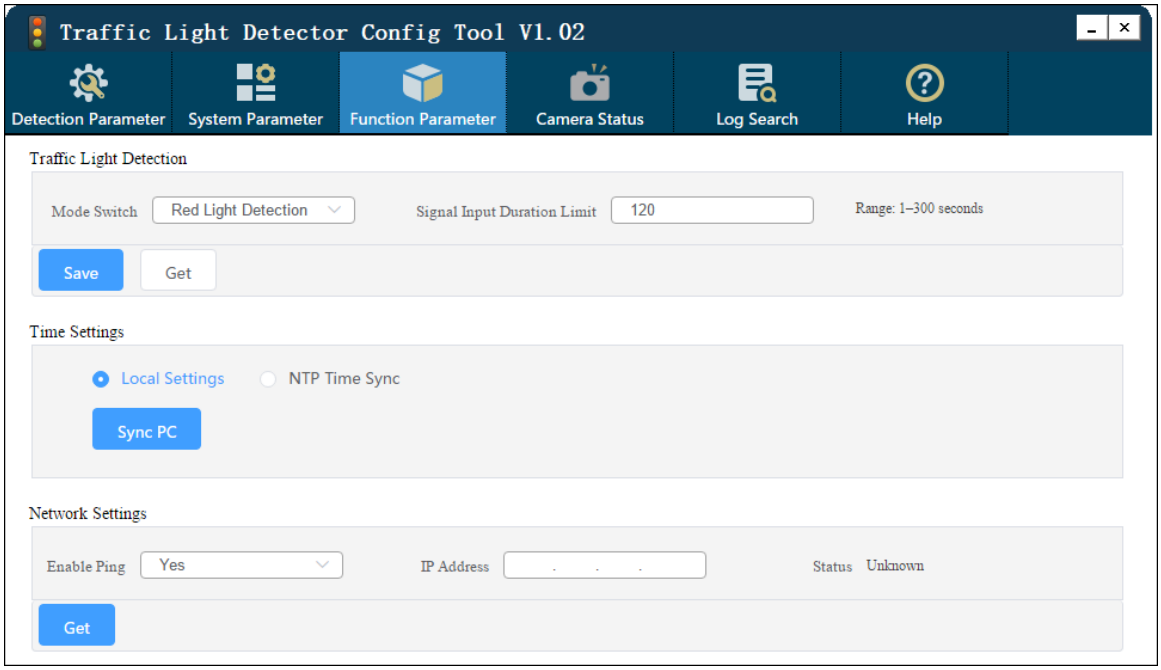


Table 4-2 Parameters descriptions

Parameter		Description
Traffic Light Detection	Mode Switch	Select **Red Light Detection** (default setting) or **Green Light Detection**.
	Signal Input Duration Limit	When traffic light signal input duration is longer than the predefined **Signal Input Duration Limit**, it is detected as a signal input exception and logged. You can click **Log Search**, and click **Search** to check. The value ranges from 1 to 300 seconds, and the default value is 120 seconds.
	Save	Save the current configurations.
	Get	Get configurations of the connected Device.
Time Settings	Local Settings	Select **Local Settings** and click **Sync PC** to synchronize time with the current PC.
	NTP Time Sync	Select **NTP Time Sync**, enter the IP address of the **NTP Server**, **Update Period**, **Port** and **Zone**, the Device will synchronize time with the NTP server automatically, ● Click **Save** to save the current NTP time sync configurations. ● Click **Get** to get NTP time sync configurations of the connected Device.
Network Settings	Enable Ping	Select whether to enable Ping. ● Select **Yes**, enter **IP Address** and click **Get** to check ping results. ● Select **No** to disable ping, which will take effect immediately. You can also enter the switch IP address to monitor the

Parameter		Description
		network status.

4.6 Camera Status

You can check camera status and traffic light status of the bound channels.

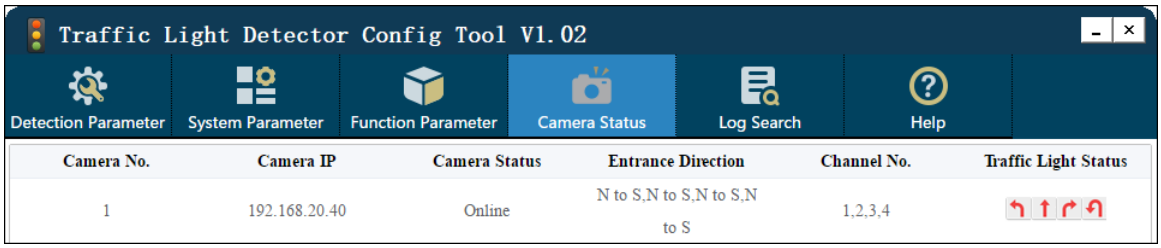
Step 1 Open the config tool and connect to the Device. Click **Camera Status**.

Step 2 You can check camera status and traffic light status of the bound channels.

- If set to **Red Light Detection** mode, but the Device detects no red light signal input, traffic light status will show as green.
- If set to **Green Light Detection** mode, but the Device detects no green light signal input, traffic light status will show as red.

All statuses are refreshed every 5 seconds.

Figure 4-10 Camera status



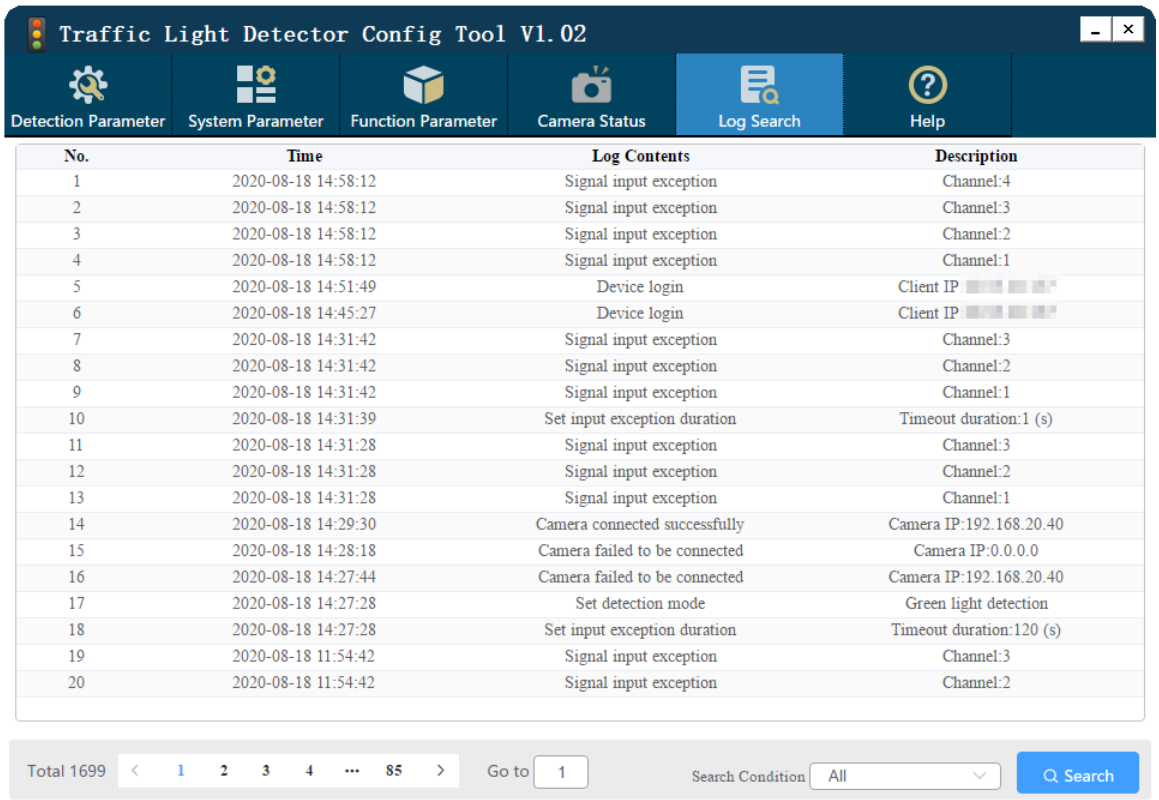
4.7 Checking Logs

You can check different kinds of operation logs.

Step 1 Open the config tool and connect to the Device. Click **Log Search**.

Step 2 On the lower-right corner, select a **Search Condition** and click **Search** to check all related logs.

Figure 4-11 Checking logs



No.	Time	Log Contents	Description
1	2020-08-18 14:58:12	Signal input exception	Channel:4
2	2020-08-18 14:58:12	Signal input exception	Channel:3
3	2020-08-18 14:58:12	Signal input exception	Channel:2
4	2020-08-18 14:58:12	Signal input exception	Channel:1
5	2020-08-18 14:51:49	Device login	Client IP
6	2020-08-18 14:45:27	Device login	Client IP
7	2020-08-18 14:31:42	Signal input exception	Channel:3
8	2020-08-18 14:31:42	Signal input exception	Channel:2
9	2020-08-18 14:31:42	Signal input exception	Channel:1
10	2020-08-18 14:31:39	Set input exception duration	Timeout duration:1 (s)
11	2020-08-18 14:31:28	Signal input exception	Channel:3
12	2020-08-18 14:31:28	Signal input exception	Channel:2
13	2020-08-18 14:31:28	Signal input exception	Channel:1
14	2020-08-18 14:29:30	Camera connected successfully	Camera IP:192.168.20.40
15	2020-08-18 14:28:18	Camera failed to be connected	Camera IP:0.0.0.0
16	2020-08-18 14:27:44	Camera failed to be connected	Camera IP:192.168.20.40
17	2020-08-18 14:27:28	Set detection mode	Green light detection
18	2020-08-18 14:27:28	Set input exception duration	Timeout duration:120 (s)
19	2020-08-18 11:54:42	Signal input exception	Channel:3
20	2020-08-18 11:54:42	Signal input exception	Channel:2

4.8 Help

Open the config tool and connect to the Device. Click **Help** to get the manual on using the config tool.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.