

Third Generation Indoor Guidance Screen

User Manual



Foreword

This document describes the product structure, installation, and client configuration of the product in details. Read it carefully before using the product. After reading, keep the document properly for future reference.

Symbols

The following symbols might appear in the manual.

Symbol	Description
 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, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.1	Updated IP modification.	November 2024
V1.0.0	First release.	March 2023

Important Safeguards and Warnings

This chapter introduces how to use the product in a proper manner. To prevent hazards and property damage, read the following requirements before you use the product and comply with the requirements when you use the product.

Transportation Requirements



Pack the Illuminator with packaging materials provided by its manufacturer or materials with the same quality before transporting it.

Transport the device under allowed humidity and temperature conditions.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Requirements



- It is strictly forbidden to connect the power adapter to the device after it is powered on. Please connect the power adapter and the device in the power-off state.
- Strictly comply with the local electric safety standards.
- Do not provide two or more than two kinds of power supply modes; otherwise, the device might be damaged or exposed to safety risk.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- When using a laser beam device, avoid exposing the surface of the device to laser beam radiation.



- Personnel working high above the ground must take all necessary safety measures including wearing a helmet.
- Do not place or install the device in a place exposed to direct sunlight or near heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilation of the device.
- Use an adapter or chassis power supply from the manufacturer.

- Make sure the power supply meets the SELV (Safety Extra Low Voltage) requirements and rated voltage conforms to the GB8898 (IEC60065) or GB4943.1 standard (IEC60950-1 or IEC62368-1 complies with Limited Power Source). The requirements of the power supply are subject to the device labels.
- For devices with type-I structure, use a grounded power socket.
- Install the device in a well-ventilated place, and do not block the ventilation of the device.
- Operating temperature: -30 °C to +55 °C (+14 °F to +131 °F).
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 50 mm on the sides and 50 mm on top of the device.
- A safety circuit breaker is designed on power plug of the device to cut the power of the device. Make sure the breaker can be easily operated during installation.

Operation Requirements



This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.



- Make sure that the power supply is correct Front operating the device.
- Do not unplug the power cord on the side of the device when the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into the device.
- Do not disassemble the device without professional instruction.
- Do not aim the device at strong light sources (such as lamplight, and sunlight) when focusing it.
- Do not vibrate, squeeze or immerse the device in liquid during transportation, storage or installation.
- We recommend you use the device with a lightning protection device for stronger protection against lightning. For outdoor scenarios, strictly comply with the lightning protection regulations.
- Ground the function earthing portion of the device to improve its reliability. The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

Maintenance Requirements



- Clean the device with a soft dry cloth or a clean soft cloth dipped in neutral detergent.
- Use the accessories suggested by the manufacturer. Maintenance must be performed by qualified professionals.
- Clean the dust off the circuit board, connectors and the cabinet to avoid the device short circuiting due to dampness.

- Make sure the device is properly grounded to avoid being damaged by static electricity or induced voltage.
- Do not plug in or unplug ports while the power is on to avoid damage to the ports.
- Do not expose the device to heat sources and high temperature environments. Keep the area around the device cabinet well-ventilated.
- Regularly inspect and perform maintenance on the device.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	II
1 Product Overview.....	1
1.1 Introduction	1
1.2 Main Functions.....	1
2 Structure and Installation	2
2.1 Product Appearance	2
2.2 Dimensions.....	2
2.3 Installation	3
2.3.1 Installing the Guidance Screen.....	3
2.3.2 Power on	4
3 Quick Setting.....	6
3.1 Search Setting	6
3.2 Modifying IP	6
3.2.1 Modifying One IP	6
3.2.2 Modifying IP in Batches	7
3.3 Upgrading Devices.....	7
4 Software Configuration Tool	9
4.1 Login	9
4.2 System Settings	9
4.2.1 System Information.....	9
4.2.2 Screen Settings.....	10
4.2.3 Network Configuration.....	11
4.2.4 System Time.....	12
4.2.5 User Management.....	12
4.2.6 System Logs	13
4.2.7 Restoring to Default Configurations.....	13
4.2.8 Auto Maintenance.....	14
4.2.9 Device Test.....	14
Appendix 1 Cybersecurity Recommendations	15

1 Product Overview

1.1 Introduction

Indoor Guidance Screen works with the parking guidance and ANPR system to display the number and location of available parking spaces in real time for vehicle owners to easily find available parking spaces. It is widely used in the entrances, exits and controlled areas of parking lots.

Designed with an RJ-45 port, the screen is highly compatible and can display text including Chinese characters, English letters, numbers and arrows. The color of the text can be configured to automatically change based on the number of available parking spaces. The screen can also display notices and advertisements for easy management of parking lots.

1.2 Main Functions

Display with LED High Brightness

The screen supports red, green and yellow LED highlighting.

Customizable Arrow

Customized the arrow direction, you can set the direction, position and scrolling.

Customizable Color

Supports setting the color to red, green and yellow according to the number of available parking spaces.

Customizable Text

Displays English letters, Chinese characters, numbers and arrows, allowing you to customize the text. You can set the scroll and color of the display text.

Easy for Commissioning

Single network port configuration, simple debugging, the device can be tested by software screen bad points and IP display.

2 Structure and Installation

2.1 Product Appearance

Figure 2-1 One-way guidance screen appearance



Figure 2-2 Two-way guidance screen appearance



Figure 2-3 Three-way guidance screen appearance



2.2 Dimensions

Figure 2-4 One-way guidance screen dimensions (Unit: mm [inch])

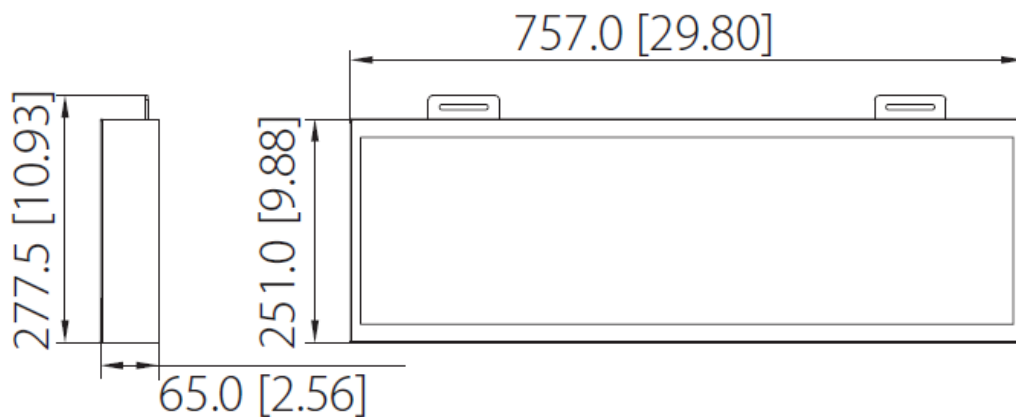


Figure 2-5 Two-way guidance screen dimensions (Unit: mm [inch])

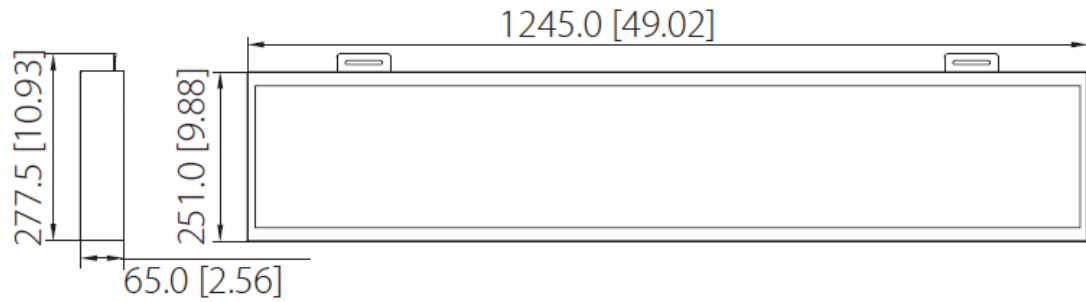
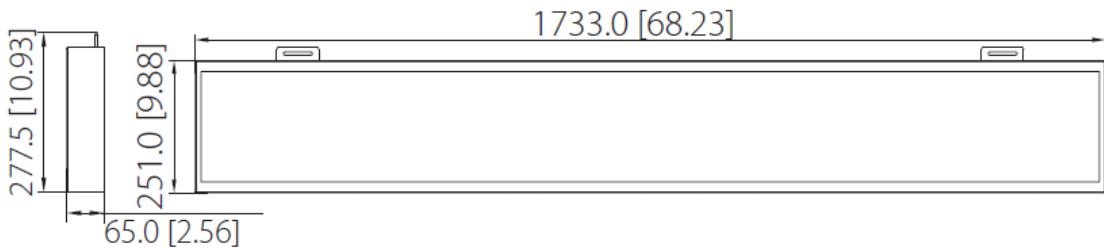


Figure 2-6 Three-way guidance screen dimensions (Unit: mm [inch])



2.3 Installation



The installation diagram is for reference only, please install according to the actual situation.



The device should be installed to avoid wet locations or locations that will produce dripping water, such as below the air conditioner and wet walls.

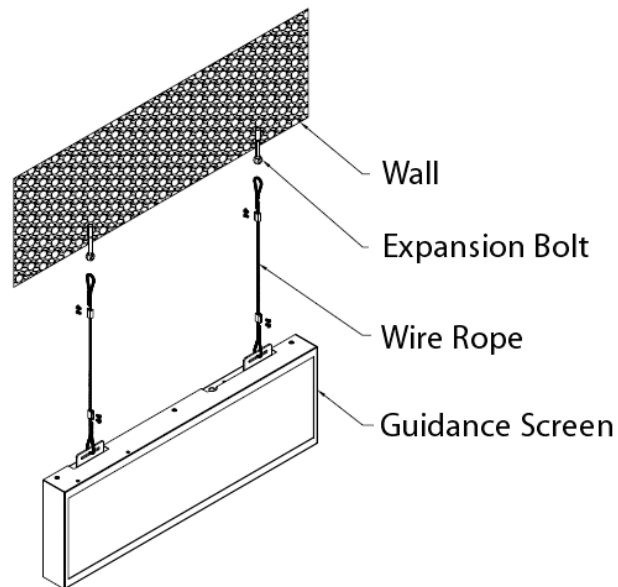
2.3.1 Installing the Guidance Screen

The device supports wire rope lifting and wire rod lifting.

Wire Rope Lifting

- Step 1** Connect the wire rope to the guidance screen firmly with the rope lock and tighten the screws.
- Step 2** Fix the expansion screws of the rings to the required position, and tighten the expansion screws.
- Step 3** Adjust the length of the wire rope according to the required height, fix the wire rope with the expansion bolt of the rings with a rope lock, and then tighten the screws.

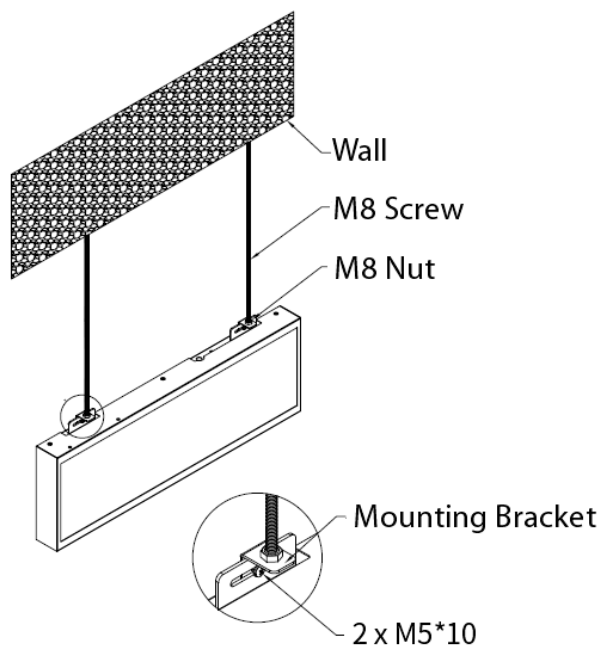
Figure 2-7 Install the guidance screen (wire rope lifting)



Wire Rod Lifting

- Step 1** Fasten the 2 mounting brackets to the screw by locking them with two M8 nuts.
- Step 2** Install the M5 bolts and nuts on the mounting ears of guidance screen.
- Step 3** Hang the induction screen on the M5 bolt and lock the M5 nut.

Figure 2-8 Installing the guidance screen (Wire rod lifting)



2.3.2 Power on

Connect the device to the network and power it on.

- Power supply: 1 pc, 100–240 VAC.
- Network interface: 1 pc, 10 M/100 M Ethernet port (RJ-45).



The total length of the network cable of a single port cannot exceed 50 m, otherwise, signals might be attenuated.

3 Quick Setting

You can use quick configuration tool to search for the current IP address of the device, modify the IP address, and upgrade the device system.

3.1 Search Setting

Step 1 Open ConfigTool.

Step 2 Click **Search Setting**.

Step 3 Select search method, login username and password.

- Current segment search: Search for devices on the same network segment with the computer.
- Other segment search: Search devices according to the start IP and end IP.



- After the initialization is completed, the system automatically generates a default user name admin, and the password is set by the user.
- For devices need to be initialized, you need to initialize them before use.

Figure 3-1 Settings

Step 4 Click **OK** to start the search, the searched devices are displayed.

3.2 Modifying IP

3.2.1 Modifying One IP



For details on how to modify the IP address on the Client, see “4.2.3 Network Configuration”.

Step 1 Open ConfigTool.

Step 2 Click  **Modify IP**.

Step 3 Click **Search Settings** to search for the device for which you want to modify the IP address, see “3.1 Search Setting” for details of the search procedure.

Step 4 Select the device for which you want to modify IP address, and then click **Edit**.

Step 5 Select the mode of IP address according to actual requirements.

- DHCP (Dynamic Host Configuration Protocol) mode: When there is DHCP server in the network, set **Mode** as **DHCP**, and then the device can automatically acquire IP address from DHCP server.
- Manual mode: Set **Mode** as **Static**, and enter **Target IP**, **Subnet Mask** and **Gateway**, and then IP address of devices can automatically acquire IP address from DHCP server.

Figure 3-2 Modify one IP

The dialog box titled "Modify IP Address" has a close button (X) in the top right corner. It contains a "Mode" section with two radio buttons: "Static" (selected) and "DHCP". Below this are three input fields: "Target IP", "Subnet Mask", and "Gateway", each with a numeric keypad icon. A blue "OK" button is positioned below the input fields. At the bottom of the dialog, it says "Selected number of devices: 1".

Step 6 Click OK.

3.2.2 Modifying IP in Batches

Step 1 Open ConfigTool.

Step 2 Click **Modify IP**.

Step 3 Click **Search Settings** to search for the device for which you want to modify the IP address, see "3.1 Search Setting" for details of the search procedure.

Step 4 Select the devices for which you want to modify IP address, click **Batch Modify IP**.

Step 5 Select the mode of IP address according to actual requirements.

- DHCP mode: When there is DHCP server in the network, set **Mode** as **DHCP**, and then the device can automatically acquire IP address from DHCP server.
- Manual mode: Set **Mode** as **Static**, and enter **Target IP**, **Subnet Mask** and **Gateway**, and then IP address of devices can automatically acquire IP address from DHCP server.



Select **Same IP** and set the same IP for selected devices.

Figure 3-3 Modify IP in batches

The dialog box titled "Modify IP Address" has a close button (X) in the top right corner. It contains a "Mode" section with two radio buttons: "Static" (selected) and "DHCP". Below this are three input fields: "Start IP", "Subnet Mask", and "Gateway", each with a numeric keypad icon. To the right of the "Start IP" field is a checkbox labeled "Same IP". A blue "OK" button is positioned below the input fields. At the bottom of the dialog, it says "Selected number of devices: 2".

Step 6 Click OK.

3.3 Upgrading Devices

You can upgrade a device at a time or upgrade devices in a batch.

Step 1 Open ConfigTool.

Step 2 Click **Device Upgrade**.

Step 3 Select the devices you want to upgrade.

- Upgrade one device: Click next to the device that you want to upgrade. Select the specific file that needs to be upgraded, and then click **Open**.

- Upgrade devices in batches: Select the devices that need to be upgraded, and click **Batch Upgrade**.

Step 4 Upgrade the devices.

- Upgrade one device: Click  to start upgrading.
- Upgrade devices in batches: Click **Browse** to select the files that need to be upgraded. Click **OK**.

4 Software Configuration Tool

The device is equipped with a dedicated configuration tool that supports personalized settings, such as arrows, color of available parking spaces, customized display text, and screen brightness. Contact technical support for software configuration tool.

4.1 Login

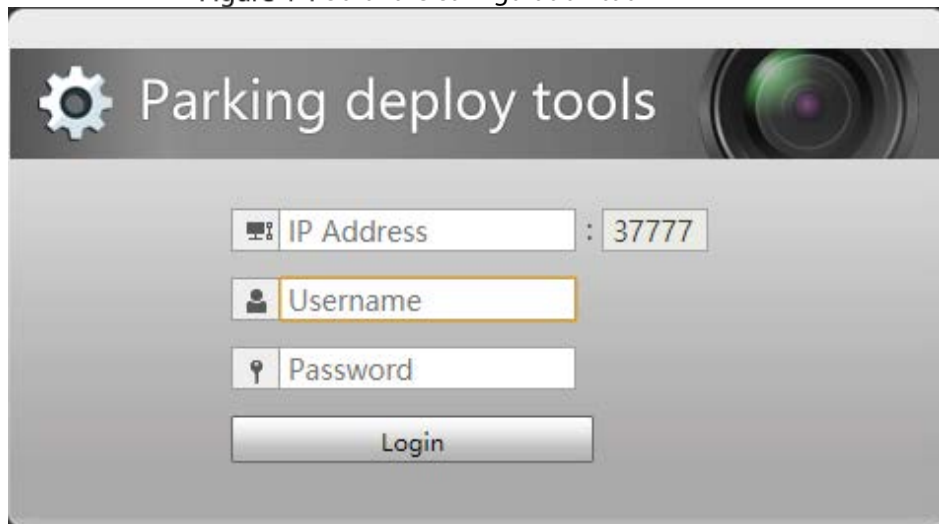
The system supports the configuration of the guidance screen through the Parking deploy tools on the computer. Before configuration, make sure that the computer can communicate with the guidance screen.

Step 1 Double-click the client configuration software and install the Parking deploy tools on the computer as prompted.

After the installation is complete, the shortcut of **Parking deploy tools** is displayed on the desktop.

Step 2 Double-click  to run the software configuration tool.

Figure 4-1 Software configuration tool



Step 3 Enter the IP address, username and password, and then click **Login**.



- The default username and password are admin and admin123 respectively. Modify your password for first-time login.
- To modify the password, go to **System Setup > User Management**.

4.2 System Settings

The system supports configuration of system information, screen settings, network settings and system time on the software configuration tool.

4.2.1 System Information

View information about the device type, software version, client version, software build time and SN of the guidance screen.

Select **System Setup > System Info**, the **System Info** page is displayed. You can view the device system information.

Figure 4-2 System information

Device Type	IPMPGI-1032
Software Version	3.000.00000000.0.0.0, build: Feb 23 2023
Client Version	1.0
Soft Build Time	Feb 23 2023 14:50:12
SN	000-001
Security Baseline Version	V2.3

Copyright 2023, all rights reserved

4.2.2 Screen Settings

Support personalized configuration of the screen display for the device.

Step 1 Select **System Setup > Screen Info**.

Step 2 Configure the screen settings parameters.

Figure 4-3 Screen settings

Arrow Position	Left ▼	
Screen1	Screen2	
Arrow Direction	Right ▼	Arrow Direction Top Right ▼
☐ Scroll	☐ Scroll	
☐ Color Settings for Available Parking Spaces		
☐ Custom Settings for Display		
		
Screen Brightness	High ▼	
Default Refresh Save		

Table 4-1 Screen setting parameters description

Parameter	Description
Arrow Position	Set the position of number of available parking spaces and arrows. For example, if you select Left , the arrow is on the left and the number of available parking spaces is on the right.
Arrow Direction	Set the arrow direction for each screen, up, right, left, top right and top left are optional.
Scroll	After the selection, the arrow direction is displayed by scrolling.
Color Settings for Available Parking Spaces	After the selection, set the color of the available parking spaces.

Parameter	Description
Custom Settings for Display	After the selection, enter the fixed content to be displayed.
Screen Brightness	Set the brightness of the screen, high, medium and low are optional.

Color Settings for Available Parking Spaces

Step 1 Select the check box.

Step 2 Enter the number range corresponding to the color. If you need 0 to display red, 1 to 9 to display yellow, and 10 to 999 to display green, enter the following:

Figure 4-4 Color Settings for available parking spaces

Custom Settings for Display

Step 1 Select the check box.

Step 2 In the display content input box, enter the text to be displayed, support English letters, Chinese characters and numbers. If you need to display arrows, select arrows.

Step 3 (Optional) If you want the displayed content to scroll, select the checkbox before **Scroll**.

Step 4 (Optional) Click the color drop-down list to select red, green, or yellow.

Figure 4-5 Color settings for available parking spaces

4.2.3 Network Configuration

Configure the IP address and MAC address of the device so that the device can be connected to other devices in the network.

Step 1 Select **System Setup > Network Config**.

Step 2 Configure the network configuration parameters.

Figure 4-6 Network configuration

Table 4-2 Network parameters description

Parameter	Description
MAC address	Indicates the device MAC address, which cannot be modified.

Parameter	Description
IP address	Enter the IP address of the device.
Subnet Mask	Set the subnet mask according to actual conditions. The subnet prefix is a number in the range of 1 to 255. The subnet prefix identifies a specific network link, and usually contains a hierarchical structure.
Default Gateway	Configure the default gateway according to the actual condition, and it must be in the same network segment with the IP address.

Step 3 Click **Save**.

4.2.4 System Time

Set the time format and system time of the guidance screen.

Step 1 Select **System Setup > System Time**.

Step 2 Configure the system time parameters.

Figure 4-7 System time

Table 4-3 System time parameters description

Parameter	Description
Time Format	Select the time format, only the 24-hour system is supported.
System Time	The current system time of the device.
Sync time	Modify the device system time to the PC system time.

Step 3 Click **Save**.

4.2.5 User Management

On the user management page, you can modify user password.



We recommend you modify the password after the first-time login to ensure device security.

Step 1 Select **System Setup > User Log**.

Step 2 Click  to modify the username.

Step 3 Enter the old password and the new password as required. The new password must be 8–32 characters in length and contain at least 2 categories of the following characters: numbers, upper-case letters, lower-case letters, and special characters, excluding quotation marks (', "), semicolons (;), colons (:), and ampersands (&).

Step 4 Set the password update period and click **Setting** to save it.

Figure 4-8 Password changing

The 'Modify User' dialog box contains the following fields and controls:

- Username:** A text field containing 'admin'.
- Old Password:** An empty password field.
- New Password:** An empty password field.
- Confirm Password:** An empty password field.
- password update period:** A dropdown menu set to 'Never' and a 'Setting' button.
- Instructions:** A text block stating: '* The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding spaces and ' ' ; &).'.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.

Step 5 Click OK.

4.2.6 System Logs

Search the operation logs of the software configuration tool by time, displaying up to 7 logs per page.

Step 1 Select **System Setup > System Log**.

Figure 4-9 System logs

The 'System Log' interface includes the following elements:

- Search Filters:** 'Start Time' (2023-03-15 15:25:47) and 'End Time' (2023-03-16 15:25:47) with calendar and clock icons, and a 'Search' button.
- Table:** A table with columns 'No.', 'Log time', 'User', and 'Type'. It displays 'No data' with a folder icon.
- System Log Info:** A section with labels for 'Log Time:', 'User:', 'Type:', and 'Content:'.
- Buttons:** 'Backup' and 'Clear log' buttons at the bottom.

Step 2 Enter the **Start Time** and **End Time**.

Step 3 Click **Search**, the search can be stopped as needed.

Step 4 Check the searching result, backup or clear log.

- **Clear log:** Clear all logs recorded by the system. Clearing logs by classification is not supported.
- **Backup:** Backup the search results to local in a .txt file.

4.2.7 Restoring to Default Configurations

Select **System Setup > Restore to Defaults**, the **Restore to Defaults** page is displayed.

Figure 4-10 Restore to defaults

Default	Restores to the default settings of the display, device access and auto maintenance.
Restore Factory	All the parameters will be restored to their factory default settings (including the device IP).

Select the recovery mode as needed.

- **Default:** Restore the default settings of screen, device access, and automatic maintenance.
- **Restore Factory:** The function is equivalent to the Reset button of the device. All configured information of the camera, including the IP address, can be restored to factory defaults. After clicking **Restore Factory**, enter the password of admin user on the pop-up window. The device can be restored to factory defaults only after the system confirms that the password is correct.

4.2.8 Auto Maintenance

You can set automatic device restart. If you select **Automatic device restart**, the frequency and time need to be set.

Step 1 Select **System Setup > Auto Maintenance**.

Figure 4-11 Automatic device restart

☐ Automatic device restart
Reboot Device
Refresh Save

Step 2 Set the device restart mode.

- Automatic restart the device.
 1. Select **Automatic device restart**.
 2. Set the restart interval, default to 02:00 every day.
- Manual restart the device: Click **Reboot Device** and manually restart the device.

Step 3 Click **OK**.

4.2.9 Device Test

Test the screen for bad spots and display IP.

Step 1 Select **System Setup > Device Test**.

Figure 4-12 Device test

Display IP
Program version
Red Full Screen
Green Full Screen
Yellow Full
Exit

Step 2 Click a test item to test it as required.

Step 3 Click **Exit** after the test is completed.

Appendix 1 Cybersecurity Recommendations

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.