



Entrance and Exit LED Screen

User Manual



Foreword

General

This manual introduces the functions and operations of the entrance and exit LED screen (hereinafter referred to as "the Screen").

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

Revision Content	Release Time	Revision Content
V1.0.0	First Release.	October 2025

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited to: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while

using the device.

- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, comply with the guidelines when using it, and keep the manual safe for future reference.

Transportation Requirements



- Transport the device under allowed humidity and temperature conditions.
- Keep the device away from the heavy stress, violent vibration or water splash during transportation.
- Pack the device with standard factory packaging or the equivalent material when transporting the device.

Storage Requirements



- Store the device under allowed humidity and temperature conditions.
- Keep the device away from water or other liquid to avoid damages to the internal components.
- Keep sound ventilation to avoid heat accumulation.
- Store the device away from the heavy stress, violent vibration or water splash.

Installation Requirements



WARNING

- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.



- Ground the grounding holes to enhance the reliability of the device.
- Keep the device away from the heavy stress, violent vibration or water splash during installation.
- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- 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. Please note that the power supply requirement is subject to the device label.
- A readily accessible disconnect device shall be incorporated in the building installation wiring.
- Make sure that the Screen power adapter meets the Screen operating voltage requirement before powering up the device (The material and length of the power cable might influence the device voltage).
- Prevent the power cable from being trampled or pressed, especially the plug, power socket and the junction extruded from the device.

Operation Requirements



- Operate the device together with lightning arrester to improve lightning protection effect.
- Use qualified video transmission cable (RG59 coaxial cable or higher standard) to improve video quality.
- Use standard components or accessories provided by manufacturer and maintain the device by professional engineers.
- Do not expose the surface of the image sensor to the laser beam radiation in an environment where a laser beam device is used.

- Do not provide two or more power supply sources for the device, otherwise it might damage the device.
- Operate the device within the range of allowed humidity and temperature.
- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- When the Screen is in the condition of PoC power supply, do not connect any other device between the Screen and PoC XVR or PoC transceiver including UTC, Balun, optical transceiver, distributor and convertor and so on; otherwise, the device might get burned.
- PoC power supply is with high voltage. Do not dismantle the device during normal operation; otherwise it might cause danger to both device and users due to high voltage.

Maintenance Requirements



- Please do not touch the photosensitive device with your hands. Use an air blower to clean off the dust and filth on the lens.
- Clean the surface of the device with a soft dry cloth or a clean soft cloth dipped in neutral detergent.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.

Table of Contents

Foreword	II
Important Safeguards and Warnings	IV
1 Introduction	1
1.1 Product Overview	1
1.2 Functions	1
2 Structure	2
2.1 Appearance	2
2.2 Dimensions	2
3 Installation	3
3.1 Unpacking and Checking	3
3.2 Installing the Screen	3
3.3 Connecting Cable	4
4 Product Configuration	6
4.1 Configuring Baud Rate	6
4.2 Configuring Network	6
4.2.1 Configuring Screen	6
4.2.2 Configuring Illuminator	1
4.2.3 Configuring Voice Broadcast	2
5 Product Update	4
6 Maintenance	5
7 FAQ	6
Appendix 1 Security Commitment and Recommendation	7

1 Introduction

1.1 Product Overview

The entrance and exit LED screen adopts highlighted display module to meet the requirements of outdoor using. With metal casing and power-sprayed coating, it is a high-end, stylish screen with long service life. The Screen supports voice broadcast with clear sound. Easy debugging, such as display and broadcast configuration, is possible through RS-485. Built-in illuminator makes the Screen free of external light. The Screen is widely used for displaying information of enter/exit vehicles and charging fees on parking lots.

1.2 Functions

- Displays LED screen status, license plate information, time, charge information, remaining parking space, custom information and more.
- Supports self-adaptive adjustment of screen brightness based on different environments, and adjusting it by connecting the camera through RS-485.
- Supports self-adaptive adjustment of illuminator brightness based on different environments, and adjusting it by connecting the camera through RS-485.
- Supports audio broadcast by connecting the camera through audio interface, and setting the output volume, speed, male/female voice.
- Communicates through RS-485, and automatically match baud rate among 9,600 bps, 38,400 bps and 115,200 bps.
- Supports screen bad pixel (abnormal LED) detection.
- Supports online update of program and character library.
- Multiple languages, including Chinese, English, Japanese, Korean, Thai and Arabic are available.

2 Structure

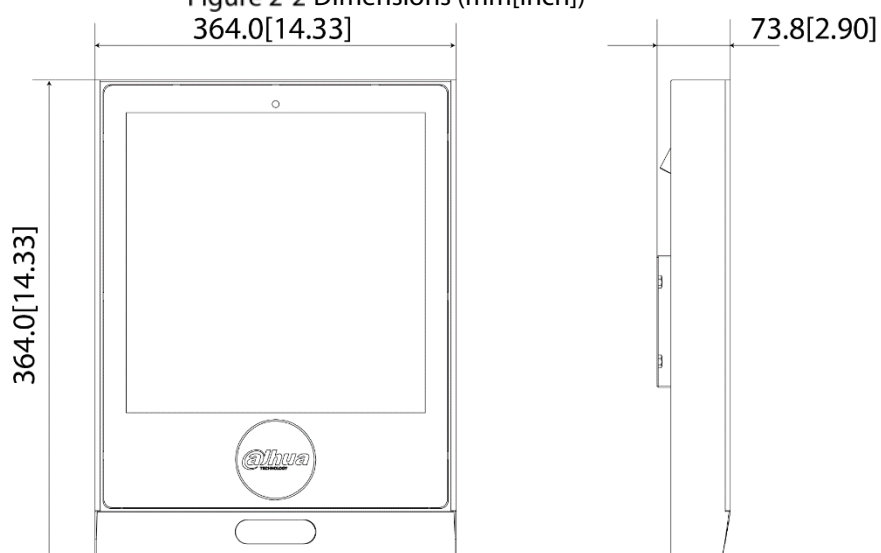
2.1 Appearance

Figure 2-1 LED screen



2.2 Dimensions

Figure 2-2 Dimensions (mm[inch])



3 Installation

3.1 Unpacking and Checking

Table 3-1 Packing list

Item	Quantity
Screen	1
Pole mount bracket	1
Cable	1
M6 screw	4
User Manual	1

3.2 Installing the Screen

There are screw holes on the bottom or back of the Screen which fixes it onto the pole.



- The Screen is equipped with metal casing and power-sprayed coating. Do not crash or press it.
- The inside of the Screen is not waterproof. Pay extra attention during installation and maintenance.

Step 1 Use pole mount bracket and 16 M6 hexagon cup head combination screws to fix the Screen onto the pole at proper height.

Step 2 Put the corrugated pipe with cables inside through the cable-entering hole of the pole, and then connect them with the camera cable and power cable at the cable-connecting operation window.

Figure 3-1 Installation

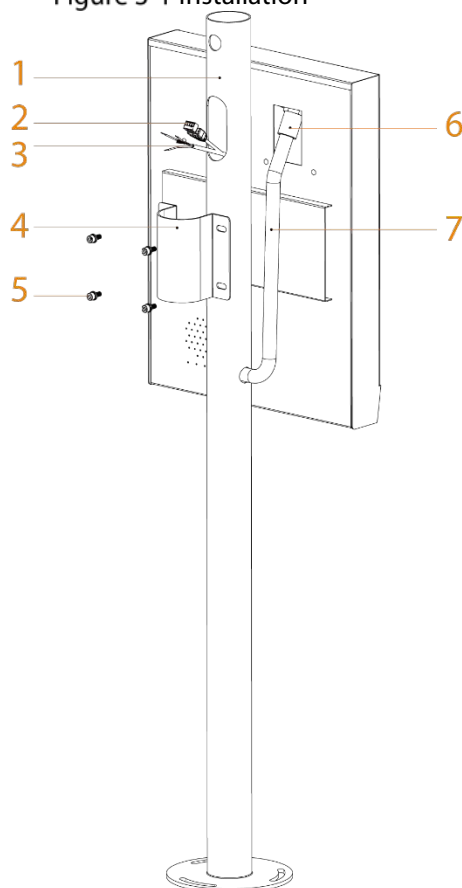


Table 3-2 Parameter description

No.	Description
1	Pole
2	4-core signal cable
3	3-core power cable
4	Pole mount bracket
5	16 × M6 hexagon cup head combination screw
6	Corrugated pipe joint AD18.5–M20 × 1.5
7	Corrugated pipe

3.3 Connecting Cable

- Power cable: Directly connect to supply power.
- Signal cable: Connect the RS-485 cable of both the Screen and the camera.
- Audio cable: Connect the audio cable of both the Screen and the camera.

Figure 3-2 Cable

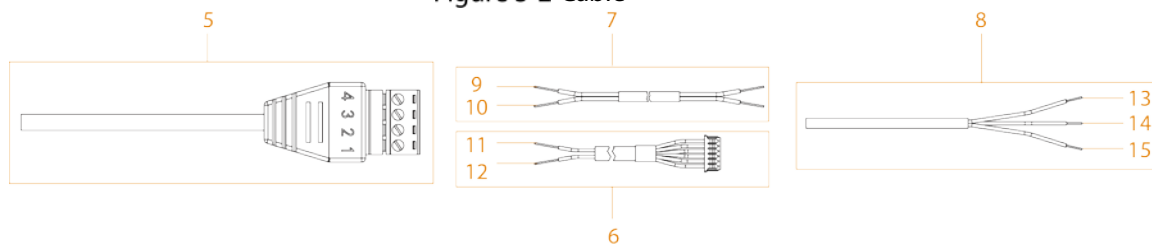


Table 3-3 Cable description

No.	Description
1	Audio +
2	Audio –
3	RS-485A
4	RS-485B
5	4-core signal cable
6	Audio cable
7	RS-485 cable
8	3-core power cable
9	RS-485A (red)
10	RS-485B (black)
11	Audio – (black)
12	Audio + (red)
13	Fire (brown)
14	Neutral (blue)
15	Ground (yellow and green)

4 Product Configuration

4.1 Configuring Baud Rate

You can configure RS-485 communicating baud rate through the DIP (dual in-line package) switch on the control card. The Screen shows the corresponding DIP value.

Figure 4-1 DIP switch

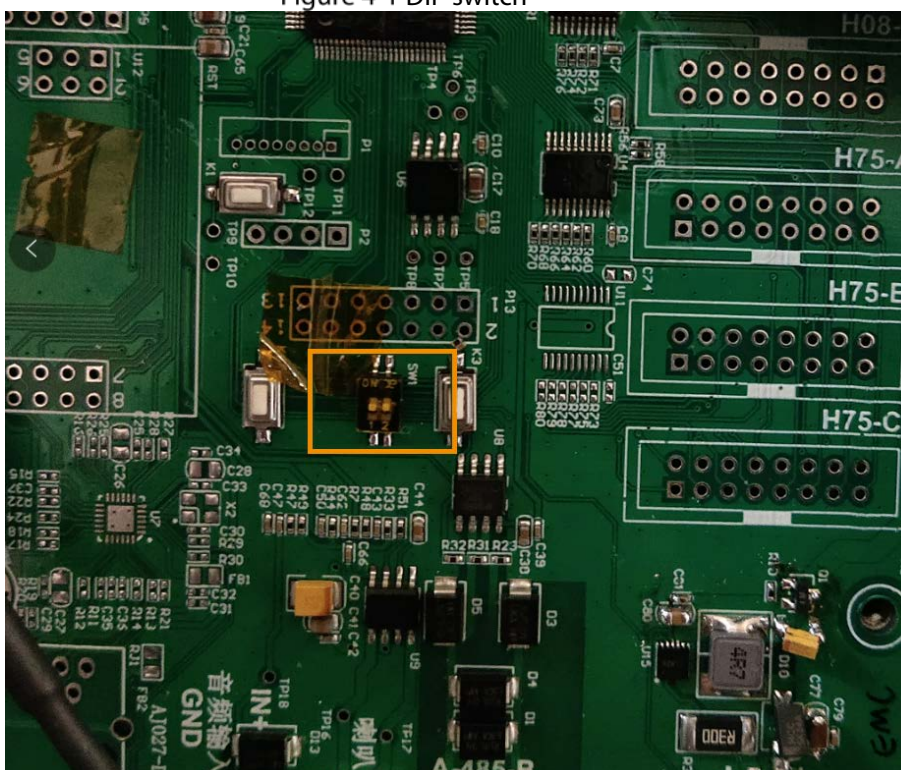


Table 4-1 Baud rate configuration

DIP value	RS-485 baud rate
00	Self-adaptive (default)
01	9,600 bps
10	38,400 bps
11	115,200 bps

4.2 Configuring Network

The Screen supports configuring related parameters on the camera web interface.



- The configuration interface is for reference only, and might differ from the actual models.
- This document introduces operations of the Screen. For the camera details, see the camera manual.

4.2.1 Configuring Screen

You can configure the Screen control mode, display content, character color, display action, screen brightness and scroll speed. Device status is also available to view.

- Step 1** Log in to web and select **Setting > ITC > RS-485 LED Display**.
- Step 2** Check whether the Screen works properly. Configure related parameters when the Screen is under normal status.



Hover over the  to view the detailed information.

- Step 3** Set LED screen parameters.

Figure 4-2 LED screen configuration

RS-485 LED Display

Device Status

Work State	Offline	Ambient Brightness	Unknown	Fault Type	Unknown
Uptime	Unknown	Screen Temperature	Unknown °C	Faulty Screen No.	Unknown
Serial Port No.	Unknown	Version	Unknown	Last Self Check Time	Unknown

Control Settings (Voice Broadcast Control Linkage)

Managed ☐ On

Mode

Working Mode ☐ Platform Mode ☒ Standalone Mode

Display Status

LED Display Status Passing Vehicle Status

Row No.	Type	Display Color	Display Action
1	Plate Number	Red	Fixed
2	User Type	Red	Fixed
3	System Date	Red	Fixed
4	System Time	Red	Fixed

QR Code Preview

(QR code preview is only available under managed mode.)

Full Screen

Rolling Speed Slightly Fast

Passing Vehicle Info 30

Retained

Brightness Adjustment Manual

Intensity 3 (1-10)

Self Check Never

Default

Refresh

Confirm

Figure 4-3 Parameter description

Parameter		Description
Control Settings	Managed Mode	Select On to enable managed mode, under which all operations of content display and change are controlled by the platform.  • The managed mode needs the new protocol be supported by the platform. • Under managed mode, you cannot configure broadcast content. • Move the mouse to  to view the detailed information.
	Working Mode	• Platform Mode: The platform controls the display content.  Platform mode is enabled by default under managed mode. • Standalone Mode: Display content can only be configured on the Screen.
Display Status		Configure the display content type, display color and action under different status. • General Status: The Screen status when no vehicles passing. • Vehicle Passing Status: The Screen status when vehicles passing.
Full Screen	Rolling Speed	The displaying speed of information on LED screen.
	Passing Vehicle Info Retained	The period (second as unit) of vehicles passing information displayed on the screen.
	Brightness Adjustment	• Manual: Adjusts brightness manually. • Auto: Adjusts brightness according to the environment automatically.
	Self Check	• Auto: Set the specific time for the Screen to self-check the screen status. • Never: Disable self check.

Step 4 Click **Confirm**.

4.2.2 Configuring Illuminator

You can configure the work mode, illumination intensity and brightness prevalue of the external lights connected through RS-485.

Step 1 Log in to web and select **Setting > ITC > RS-485 External**.

Step 2 Configure external lights parameters.

Figure 4-4 Configure external light

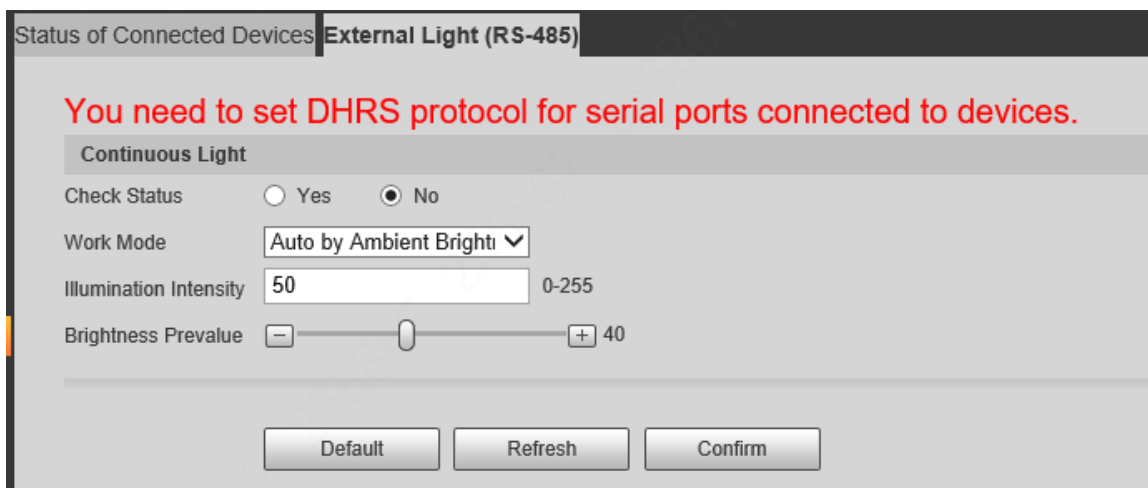


Table 4-1 External light parameter description

Parameter	Description
Check Status	Select Yes or No to enable or disable the function of detecting the continuous light status. The external light status can only be obtained after enabling the function.
Working Mode	Select the work mode of the continuous light as needed. ● Always Off: The continuous light is always off. ● Always On: The continuous light is always on. ● Auto by Time: Set the period during which the continuous is on. ● Auto by Ambient Brightness: Set environment brightness prevalue. The continuous light is on when environmental brightness is lower than the prevalue and when it is higher, the light is off.
Illumination Intensity	Set the light beam intensity of the continuous light during work. The larger the value is, the higher the brightness will be.

Step 3 Click **Confirm**.

4.2.3 Configuring Voice Broadcast

You can configure the voice broadcast content, volume and encoding.

Step 1 Log in to the camera web interface and then select **Setting** > **ITC** > **Voice Broadcast** > **Broadcast Content**.

Step 2 Configure the voice broadcast options as needed. Position adjustment of options is available.

Figure 4-5 Configuring voice broadcast option

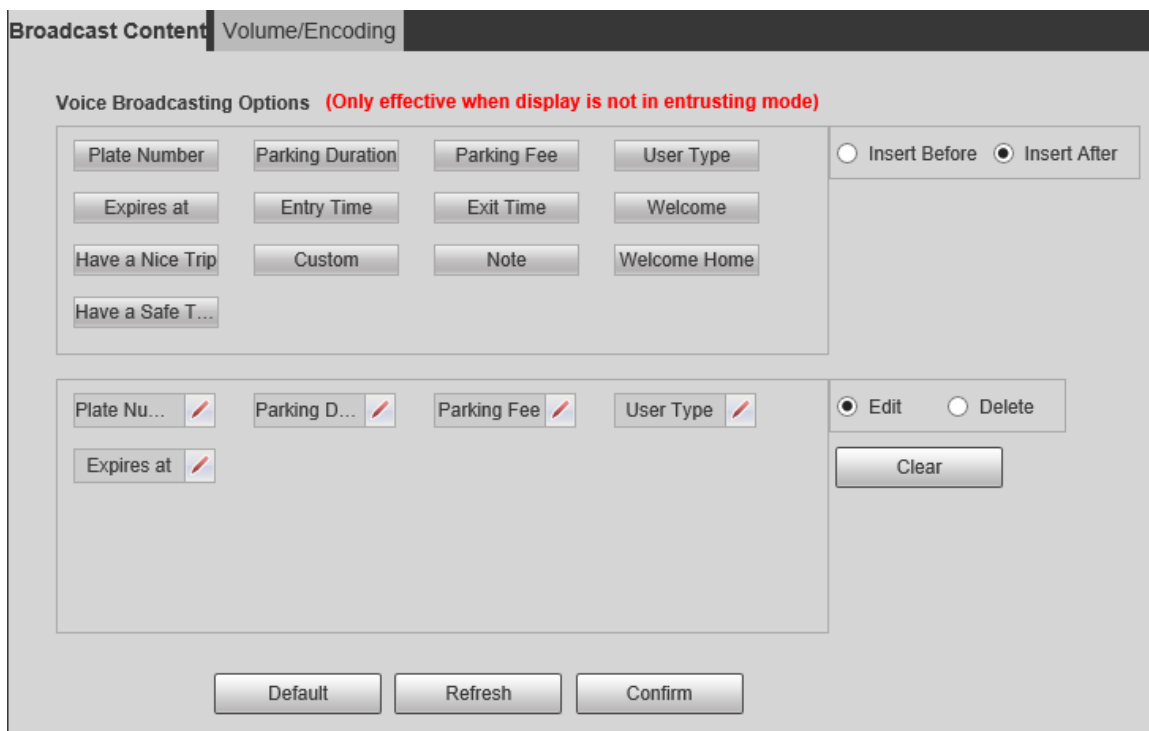


Table 4-2 Description of content options

Parameter	Description
Insert Before	Select Insert Before , click a selected option and then click a new option. The new option will be inserted before the selected one.
Insert After	Select Insert After , click a selected option and then click a new option. The new option will be inserted after the selected one.
Edit	Select Edit , and then click  next to selected options to edit the content.
Delete	Select Delete , and then click  next to selected options to delete the option.
Clear	Delete all selected voice broadcast options.

Step 3 Click **Confirm**.

5 Product Update

You can import the update file to update the control card program and character library by connecting the camera through RS-485 protocol.



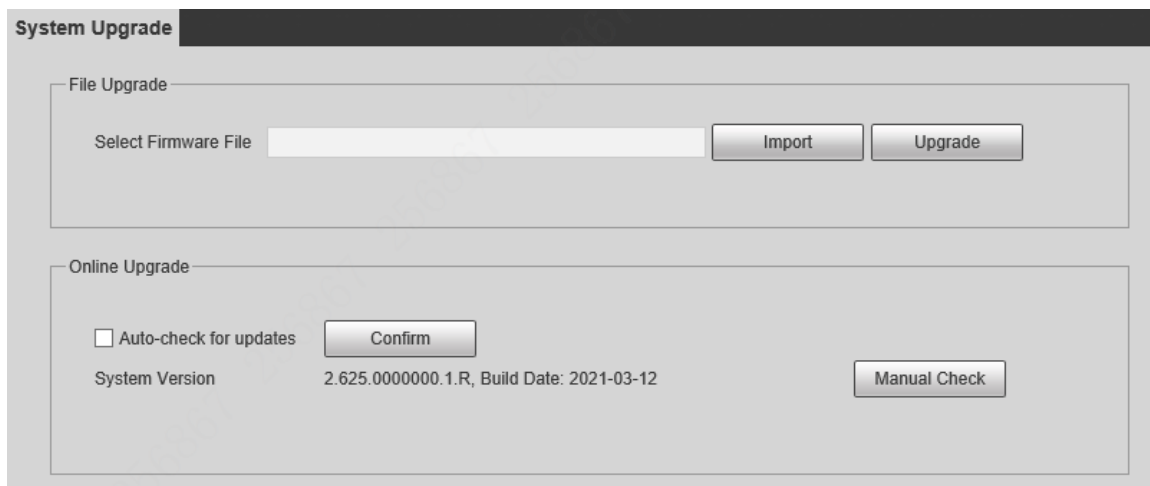
- Incorrect update programs may result in the Screen unable to work.
- During update, make sure that the device is not disconnected from power and network, and restart or shut down the Web.

Step 1 Select **Setting > System > Upgrade**.

Step 2 Update the program. Only file update is available.

1. Click **Import** to import update files. The update file extension name is **2.6XX.0000000.X.R.YYMMDD.bin**.
2. Click **Upgrade**. The update takes about 2 to 5 minutes.

Figure 5-1 System update



System Upgrade

File Upgrade

Select Firmware File

Online Upgrade

☐ Auto-check for updates

System Version 2.625.0000000.1.R, Build Date: 2021-03-12

6 Maintenance

- Keep the Screen and the voice output port clean.
- Do not store the Screen outdoors with no power.
- We recommend using the Screen every half month and keep it powered on for 4 hours.

7 FAQ

Table 7-1 FAQ

FAQ	Solutions
Black screen.	● Check whether the air switch and 220 V power supply are properly connected. ● Check whether the 220 V input and 5 V output power cables are loose. ● Check whether the FPC (Flexible Printed Circuit) and power cable of LED module are loose.
Speaker has no sound or has noise.	● Check whether the audio cable between the camera and the control card is in poor contact. ● Check whether the audio cable between the speaker and the control card is in poor contact. ● Change speaker. ● Change control card.
Screen display exception.	● Check whether the FPC between the control card and the screen is loose. ● Change LED module.
Illuminator does not light up.	● Check whether the cable between the control card and the illuminator is in poor contact. ● Change the illuminator board. ● Change control card.
The screen brightness does not change along with the environment.	● Check whether the cable between the control card and the light sensor is in poor contact. ● Change light sensor.

Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua's official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

1. Account Management

1.1 Use complex 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: 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 repeating characters, such as 111, aaa, etc.

1.2 Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

1.3 Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

1.4 Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

1.5 Set and update password reset information in a timely manner

Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

2. Service Configuration

2.1 Enable HTTPS

It is recommended that you enable HTTPS to access Web services through secure channels.

2.2 Encrypted transmission of audio and video

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

2.3 Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

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

2.4 Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

3. Network Configuration

3.1 Enable Allow list

It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.

3.2 MAC address binding

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3.3 Build a secure network environment

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;

According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;

Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

4. Security auditing

4.1 Check online users

It is recommended to check online users regularly to identify illegal users.

4.2 Check device log

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

4.3 Configure network log

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

5. Software Security

5.1 Update firmware in time

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

5.2 Update client software in time

We recommend you to download and use the latest client software.

6. Physical protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188