



Entrance and Exit LED Screen

User's 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.	March 2021

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 regions. For detailed information, see 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, please refer to our 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 occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

Electrical Safety

- All installation and operation should conform to your local electrical safety codes.
- 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.
- We assume no liability or responsibility for all the fires or electrical shock caused by improper handling or installation.

Environment

- Transport, use and store the device within the range of allowed humidity and temperature.
- Keep the Screen away from water or other liquid to avoid damages to the internal components.
- Keep sound ventilation to avoid heat accumulation.
- Heavy stress, violent vibration or water splash are not allowed during transportation, storage and installation.
- Pack the device with standard factory packaging or the equivalent material when transporting the device.
- It is recommended to use the device together with lightning arrester to improve lightning protection effect.
- It is recommended to get the grounding holes to be grounded to enhance the reliability of the device.
- It is recommended to use qualified video transmission cable to improve video quality. It is recommended to use RG59 coaxial cable or higher standard.
- Use standard components or accessories provided by manufacturer and make sure the device is installed and maintained by professional engineers.
- The surface of the image sensor should not be exposed to 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.
- 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.

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	7
4.2.2 Configuring Illuminator	1
4.2.3 Configuring Voice Broadcast	2
4.2.3.1 Configuring Voice Broadcast	2
5 Product Update	4
6 Maintenance	5
7 FAQ	6
Appendix 1 Cybersecurity Recommendations.....	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.

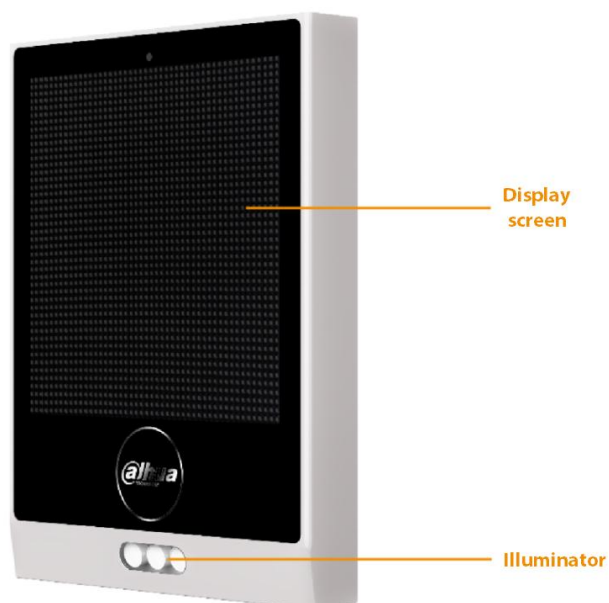
1.2 Functions

- 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

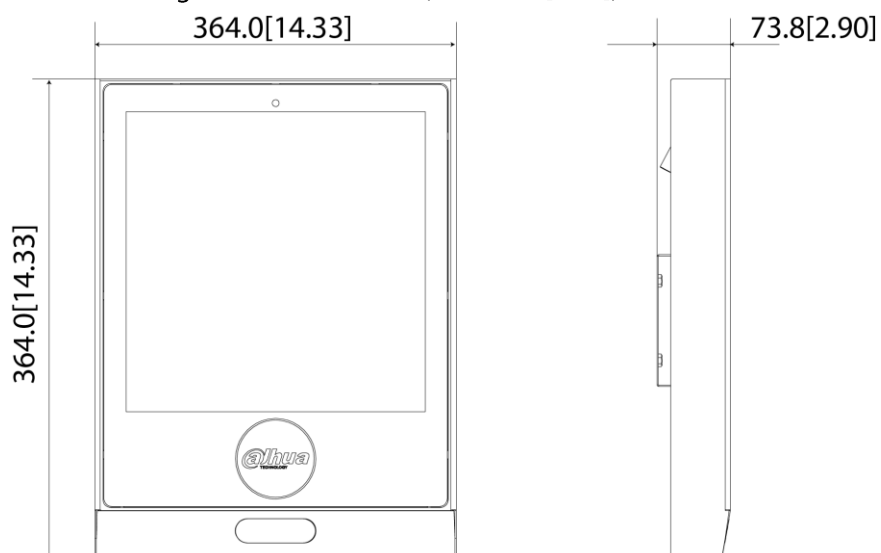
2.1 Appearance

Figure 2-1 LED Screen



2.2 Dimensions

Figure 2-2 Dimensions (Unit: mm [inch])



3 Installation

3.1 Unpacking and Checking

Table 3-1 Packing list

Item	Number
Screen	1
Pole mount bracket	1
Cable	1
M6 screw	4
User's 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

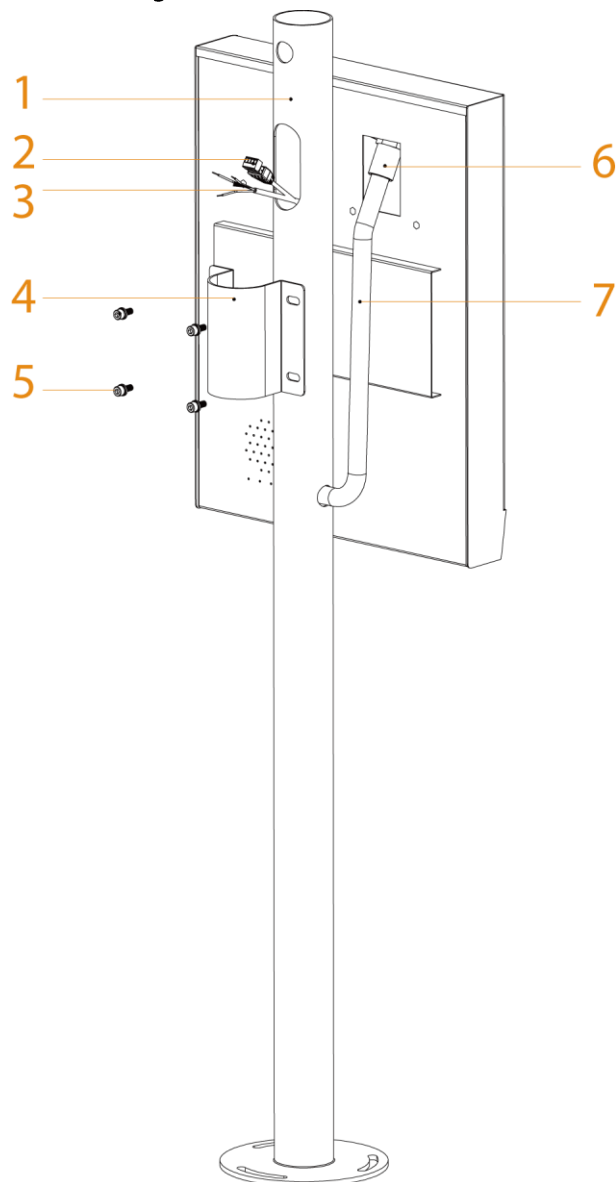


Table 3-2 Parameter Description

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

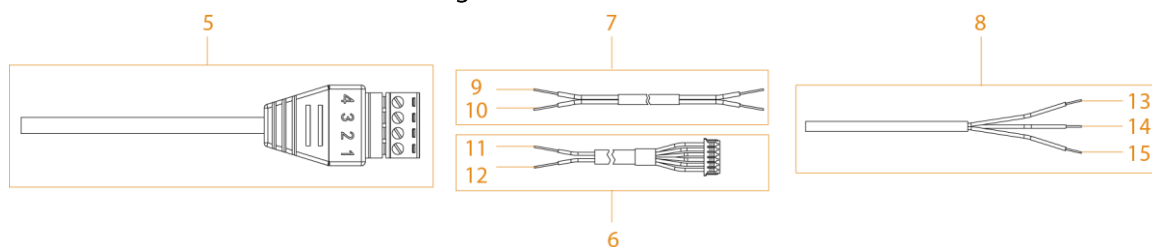


Table 3-3 Description

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

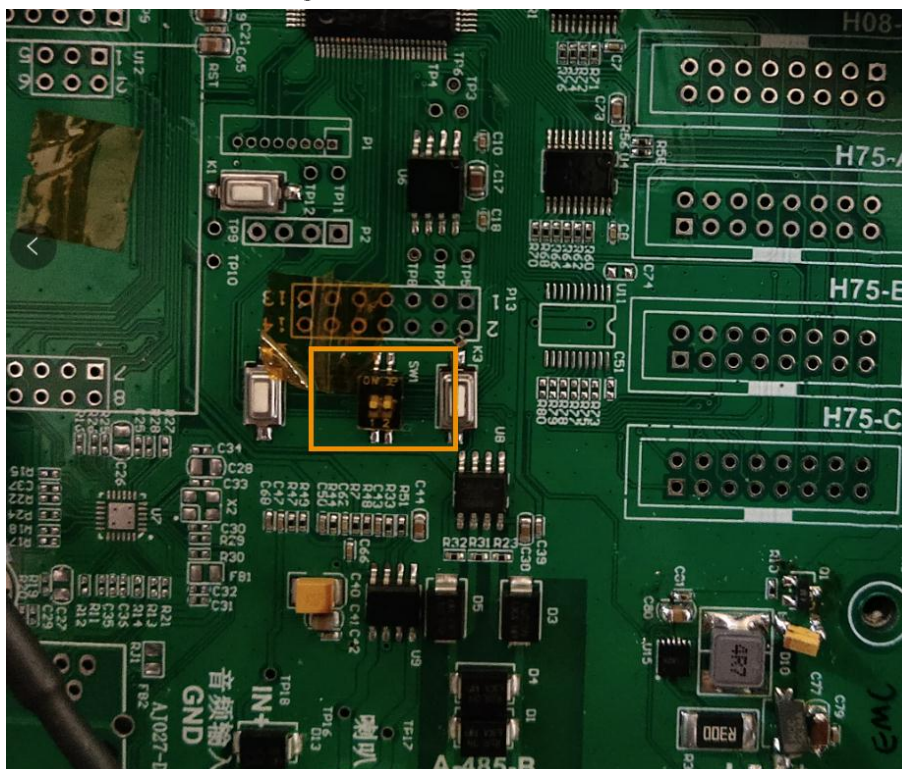


Table 4-1 Baud rate configuration

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**.

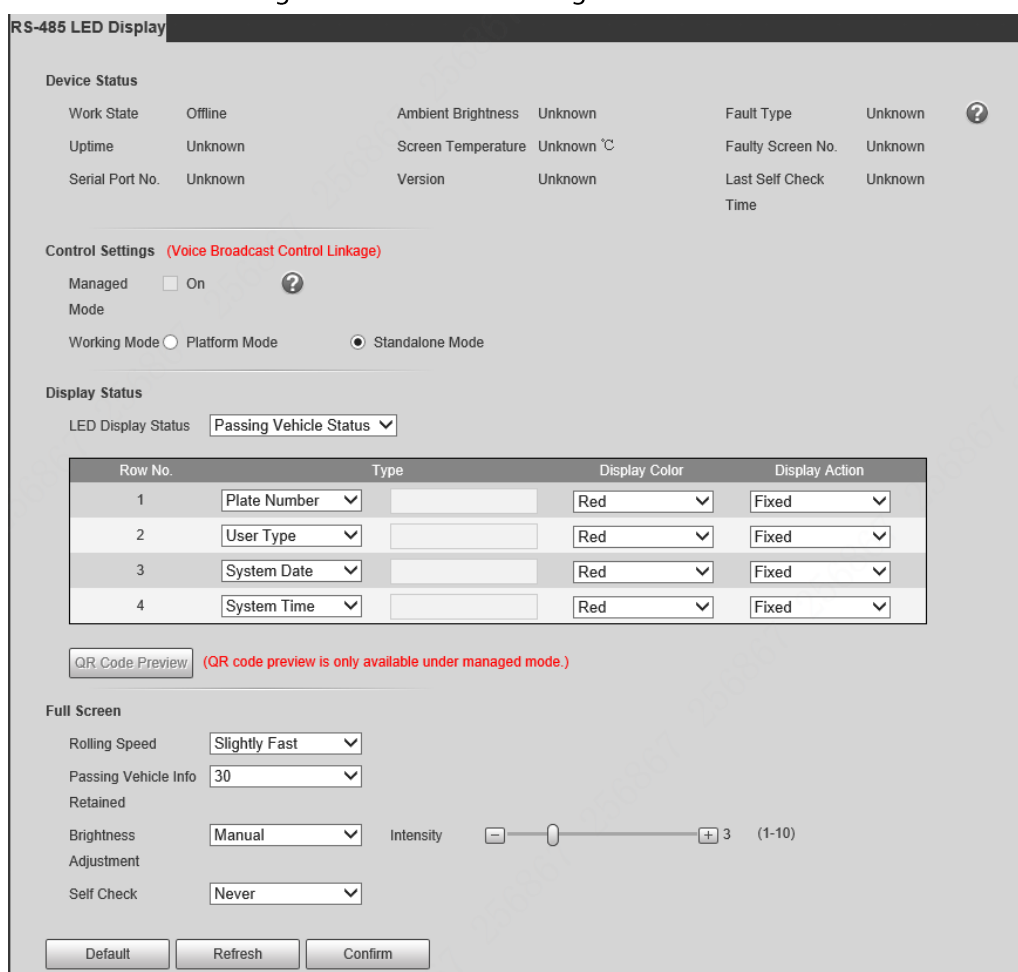
Step 2 Check whether the Screen works properly. Configure related parameters when the Screen is under normal status..



Move the mouse to 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 Retained 30

Brightness Adjustment Manual Intensity  3 (1-10)

Self Check Never

Default Refresh Confirm

Table 4-2 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 4-3 Configure external light

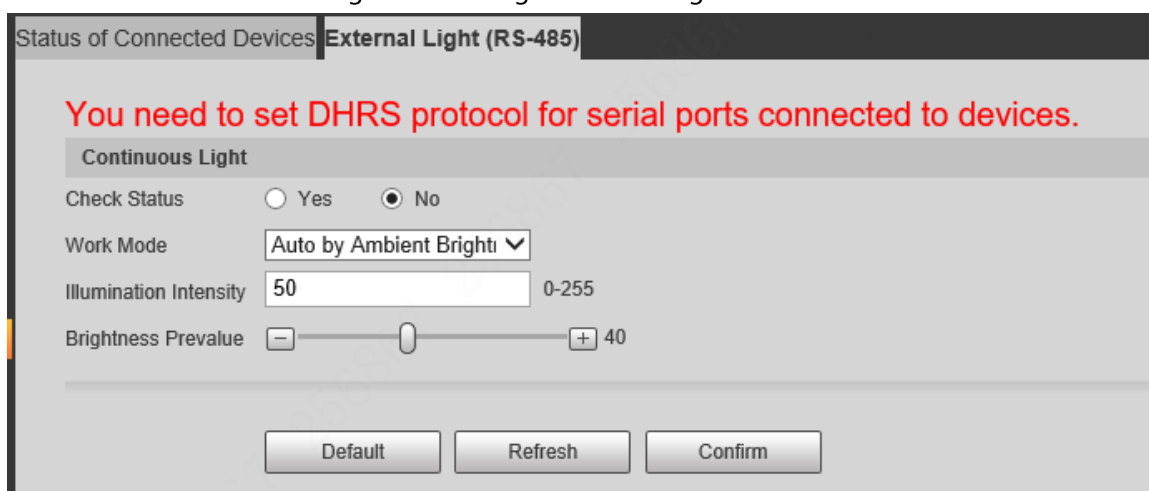


Table 4-3 External light parameter description

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.

4.2.3.1 Configuring Voice Broadcast

You can configure the content of voice broadcast to play when vehicles passing.

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 4-4 Configuring voice broadcast option

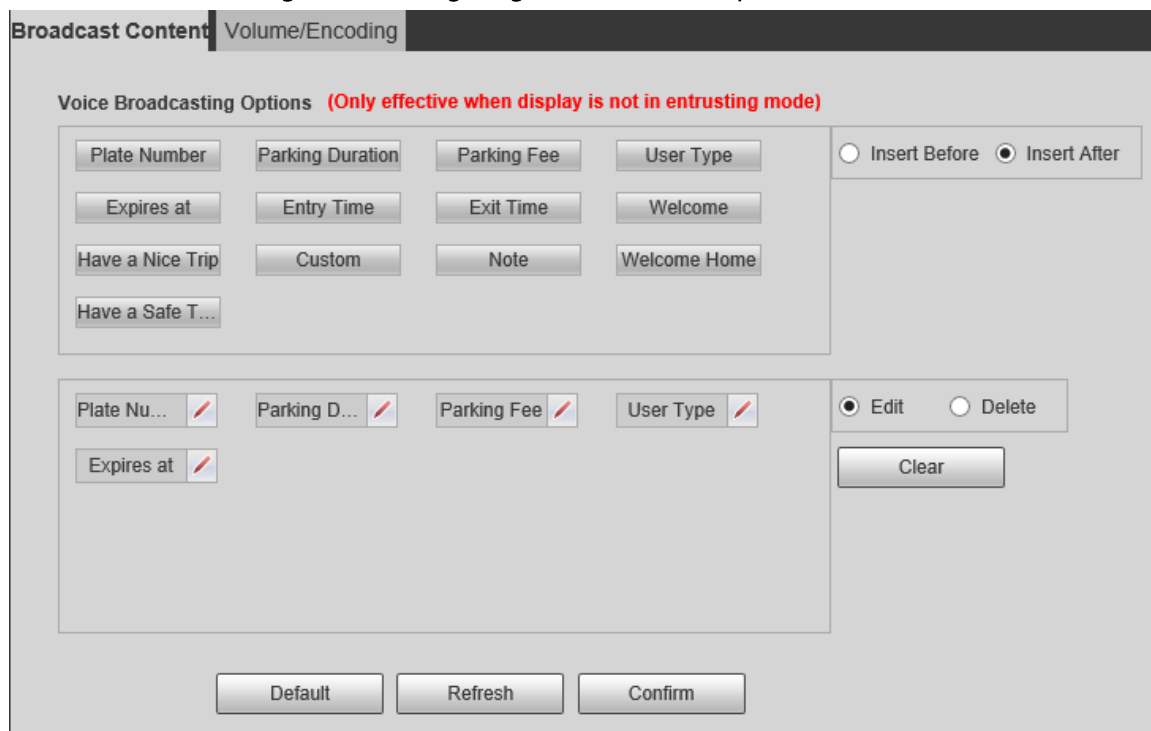


Table 4-4 Description of content options

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.



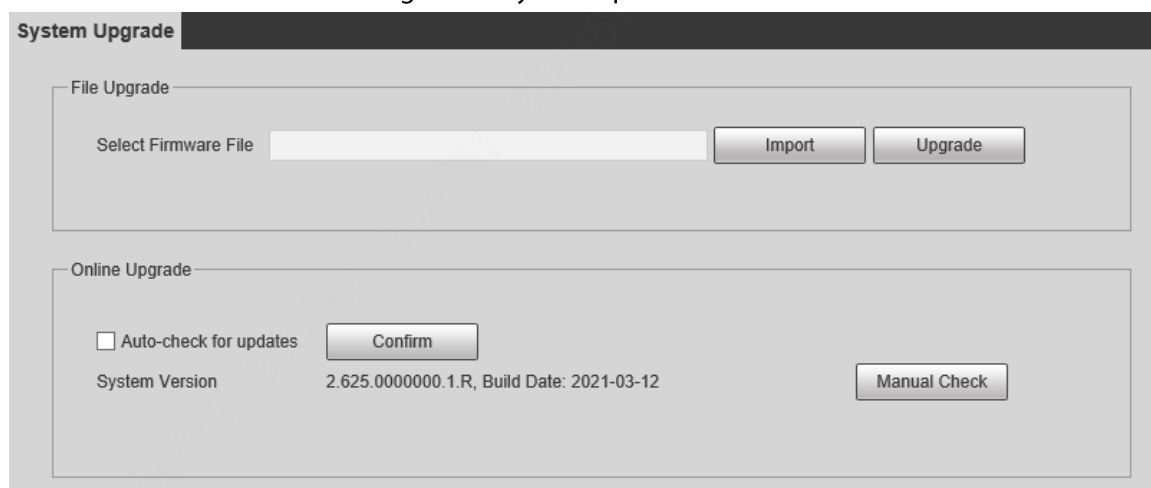
- Incorrect update programs may result in the Screen unable to work.
- During update, make sure that the device is not disconnected from power and network, and restart or shut down the Web.

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 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 equipment 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 equipment (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 equipment 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 equipment network security:

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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 equipment, 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 equipment 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 equipment, 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 equipment 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.

ENABLING A SAFER SOCIETY AND SMARTER LIVING