Outdoor LED Screen

User's Manual

V1.0.0

Foreword

This manual introduces the configuration and operations of the Outdoor LED Screen (hereinafter referred to as the "Screen"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

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

Signal Words	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
V1.0.0	First release.	November 2024

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: 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's 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

⚠

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

⚠ WARNING

- 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

⚠ WARNING

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 dissemble 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 RS-232, RS-485, and other 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

1 Product Overview

1.1 Introduction

The Screen is a complementary product for parking guidance and entrance and exit systems. It is primarily installed at the entrance and exit of parking lots to display the number of available parking spaces in real time.

2 Configuration and Troubleshooting

2.1 Device Configuration

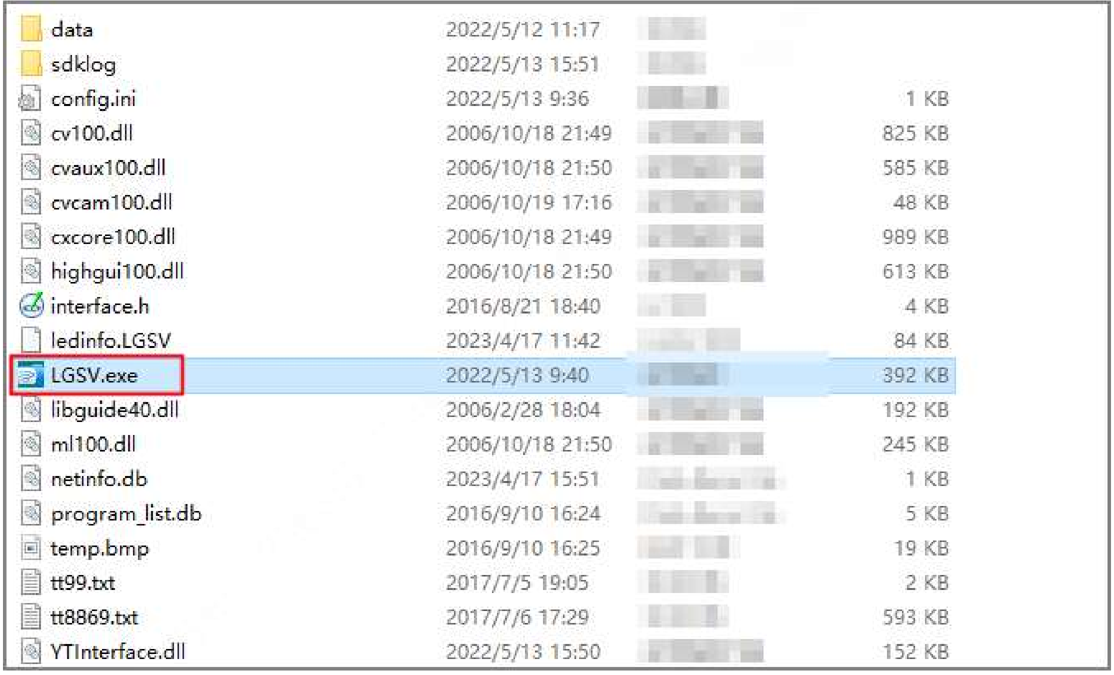
This manual is only applicable to specific models. For the commissioning software LGSV, log in to the Support platform or contact the technical support.

Procedure

Step 1 Run the LGSV system.

- For first-time use, direct connection through a single card is recommended.
- The default IP address is 192.168.1.222. Make sure the IP addresses of the computer and screen are on the same network segment.

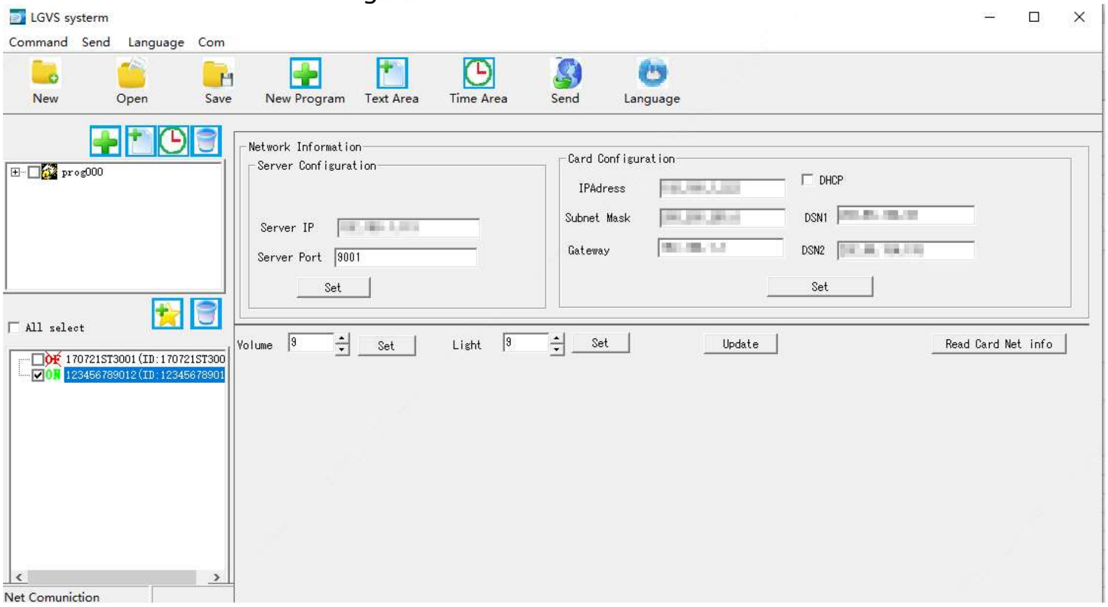
Figure 2-1 Run the LGSV system



data	2022/5/12 11:17	[illegible]	
sdklog	2022/5/13 15:51	[illegible]	
config.ini	2022/5/13 9:36	[illegible]	1 KB
cv100.dll	2006/10/18 21:49	[illegible]	825 KB
cvaux100.dll	2006/10/18 21:50	[illegible]	585 KB
cvcam100.dll	2006/10/19 17:16	[illegible]	48 KB
cxcore100.dll	2006/10/18 21:49	[illegible]	989 KB
highgui100.dll	2006/10/18 21:50	[illegible]	613 KB
interface.h	2016/8/21 18:40	[illegible]	4 KB
ledinfo.LGSV	2023/4/17 11:42	[illegible]	84 KB
LGSV.exe	2022/5/13 9:40	[illegible]	392 KB
libguide40.dll	2006/2/28 18:04	[illegible]	192 KB
ml100.dll	2006/10/18 21:50	[illegible]	245 KB
netinfo.db	2023/4/17 15:51	[illegible]	1 KB
program_list.db	2016/9/10 16:24	[illegible]	5 KB
temp.bmp	2016/9/10 16:25	[illegible]	19 KB
tt99.txt	2017/7/5 19:05	[illegible]	2 KB
tt8869.txt	2017/7/6 17:29	[illegible]	593 KB
YTInterface.dll	2022/5/13 15:50	[illegible]	152 KB

Step 2 Check the status of the device. If the network is connected, the device will be displayed as online on the lower-left box of the page.

Figure 2-2 Check the status



prog000

Server IP [redacted]
Server Port 9001

IPAdress [redacted]
Subnet Mask [redacted]
Gateway [redacted]
□ DHCP
DSN1 [redacted]
DSN2 [redacted]

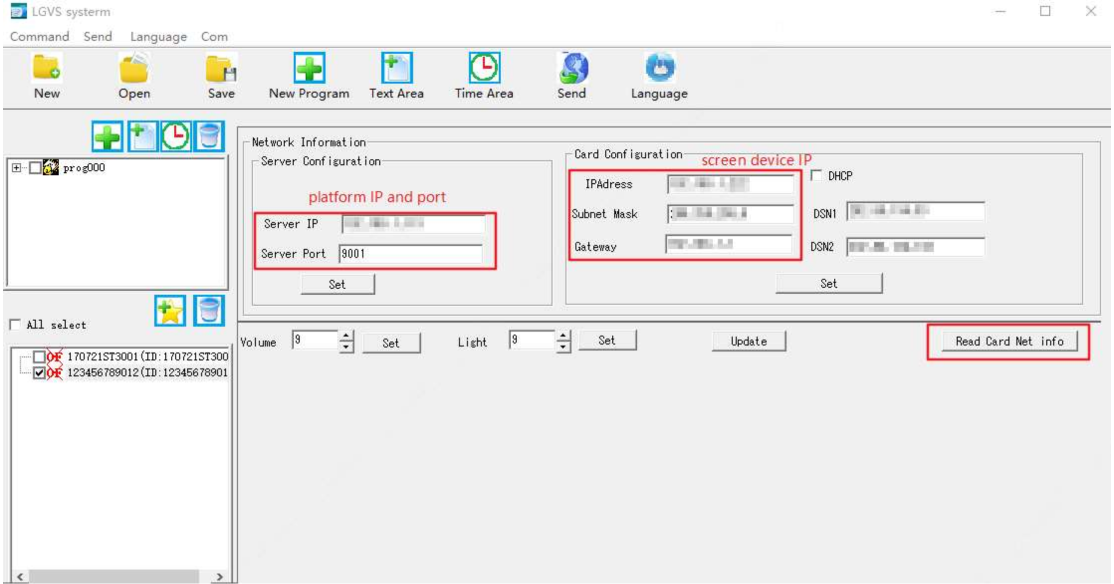
Volume 9
Light 9

□ OFF 170721ST3001(ID:170721ST300
☑ ON 123456789012(ID:12345678901

Step 3 Select the online device, read the network information of the control card, and then set the platform server and control card.

The default port is 9001.

Figure 2-3 Set the platform server and control card



prog000

Server IP [redacted]
Server Port 9001

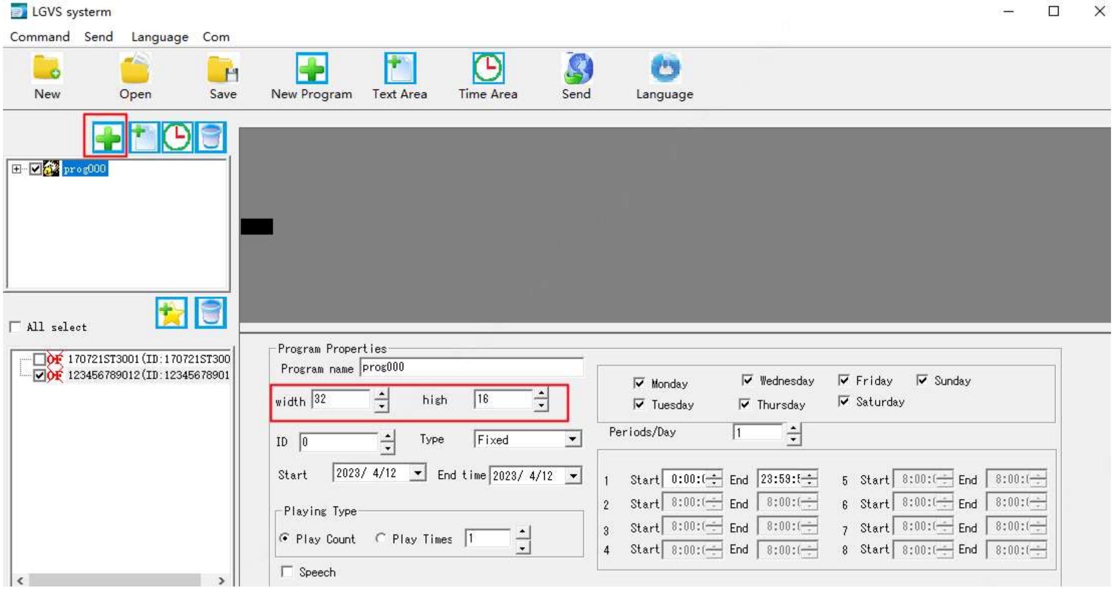
IPAdress [redacted]
Subnet Mask [redacted]
Gateway [redacted]
□ DHCP
DSN1 [redacted]
DSN2 [redacted]

Volume 9
Light 9

□ OFF 170721ST3001(ID:170721ST300
☑ OFF 123456789012(ID:12345678901

Step 4 Click ✚ to add programs. Set the program width to 32 and the height to 16. The program width and height should be identical with those of the device.

Figure 2-4 Add a program


LGVS systerm
Command Send Language Com
New
Open
Save
New Program
Text Area
Time Area
Send
Language
prog000
All select
170721ST3001 (ID:170721ST300
123456789012 (ID:12345678901

Program Properties

Program name prog000

width 32 high 16

ID 0 Type Fixed

Start 2023/ 4/12 End time 2023/ 4/12

Playing Type

● Play Count ○ Play Times 1

☐ Speech

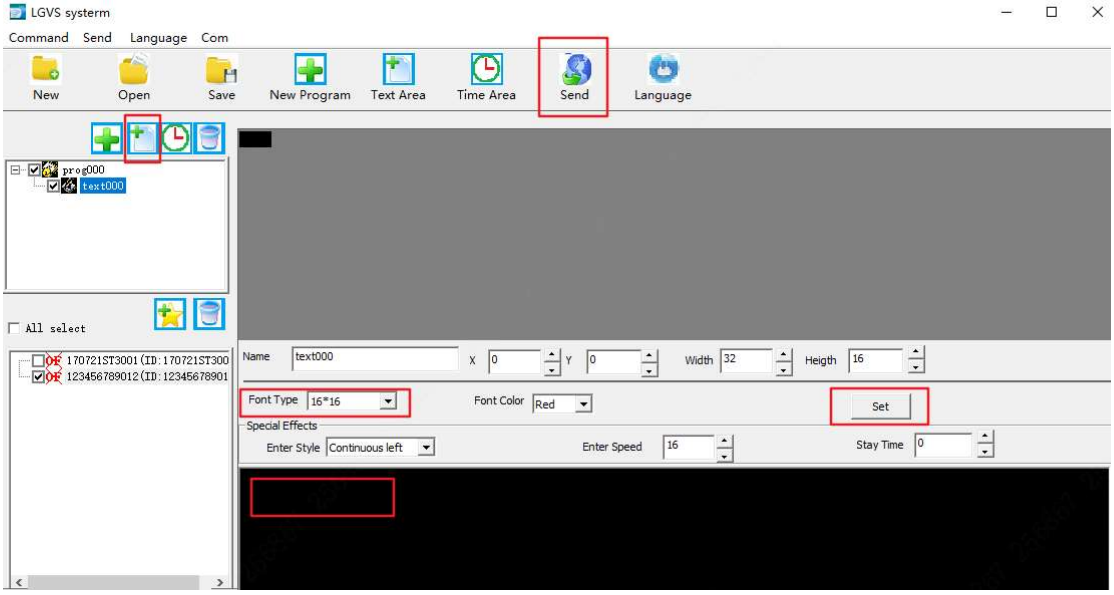
☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Periods/Day 1

1	Start	0:00:(	End	23:59:5	5	Start	8:00:(	End	8:00:(
2	Start	8:00:(	End	8:00:(	6	Start	8:00:(	End	8:00:(
3	Start	8:00:(	End	8:00:(	7	Start	8:00:(	End	8:00:(
4	Start	8:00:(	End	8:00:(	8	Start	8:00:(	End	8:00:(

Step 5 Click the icon to add text. Set the **Font Type** to **16*16**, enter the content in the box, and then click **Set**. You can click **Send** to check if the screen can display the content.

Figure 2-5 Add a text



Name text000 X 0 Y 0 Width 32 Heigth 16

Font Type 16*16 Font Color Red

Special Effects

Enter Style Continuous left Enter Speed 16 Stay Time 0

2.2 Device Connection to the Platform

This section uses DSS Pro is used as an example. Before adding the device to the platform, close the LGSV first. If the system is installed with a firewall, you should either disable the firewall or add LGSV to the firewall allowlist.

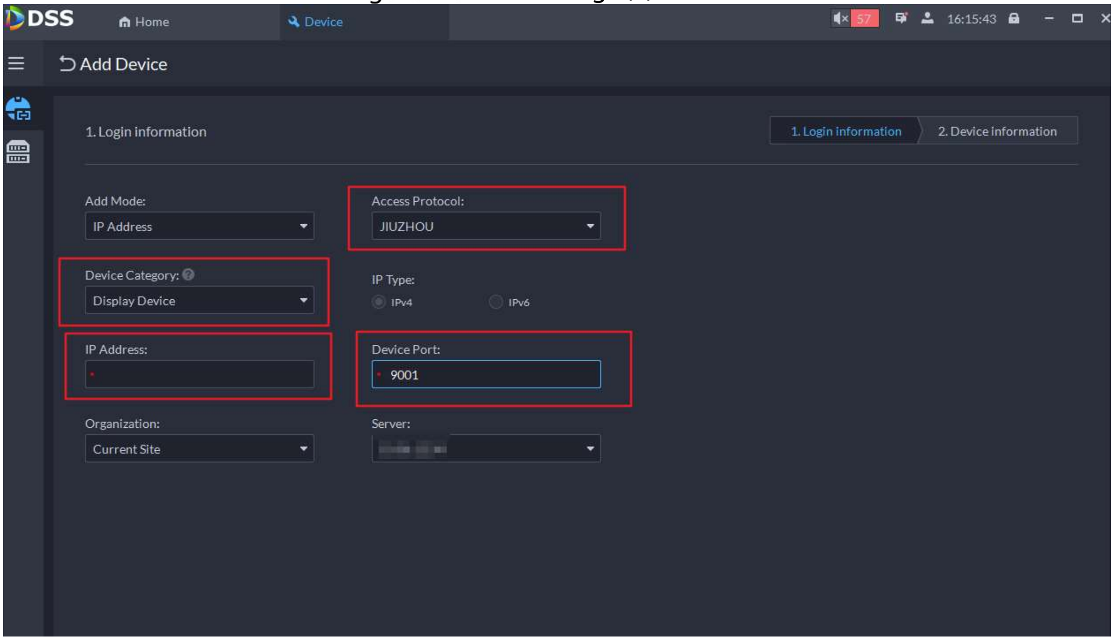
Procedure

Step 1 Log in to the DSS platform, and then go to the **Add Device** page.

Step 2 Set the **Access Protocol** to **JIUZHOU**, the **Device Category** to **Display Device**, and then enter the IP address and device port.

The default port is 9001.

Figure 2-6 DSS settings (1)



1. Login information

Add Mode: IP Address

Access Protocol: JIUZHOU

Device Category: Display Device

IP Type: ● IPv4 ○ IPv6

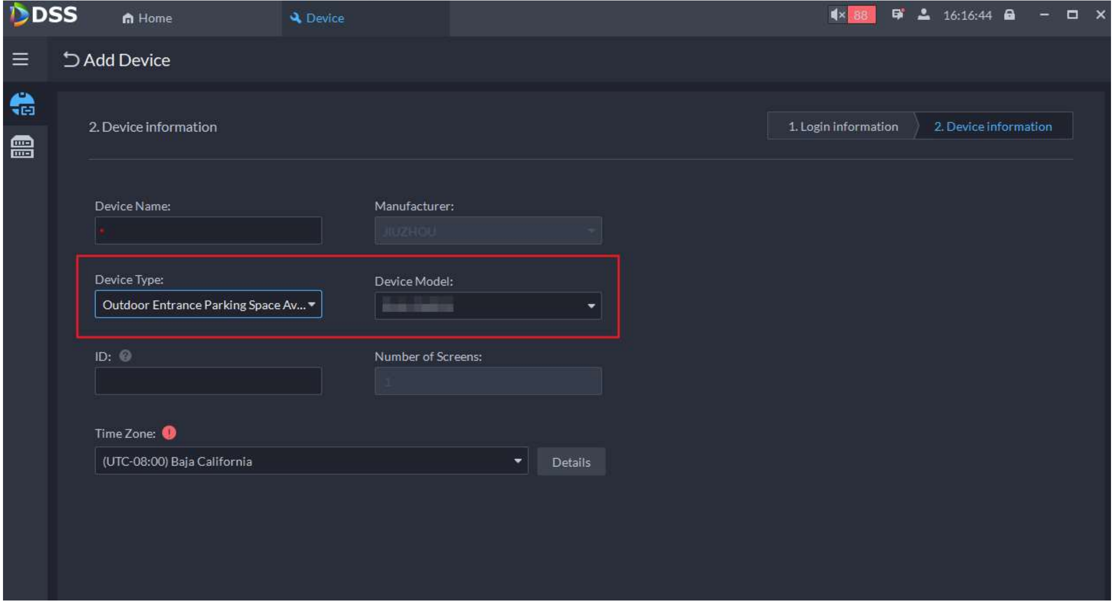
IP Address: *

Device Port: * 9001

Organization: Current Site

Server: [redacted]

Figure 2-7 DSS settings (2)



2. Device information

Device Name: *

Manufacturer: JIUZHOU

Device Type: Outdoor Entrance Parking Space Av...

Device Model: [redacted]

ID:

Number of Screens: 1

Time Zone: (UTC-08:00) Baja California

Details

2.3 Troubleshooting for Communication Anomaly

- If the system is installed with a firewall, you should either disable the firewall or add LGSV to the firewall allowlist.
- For multi-NIC servers, disable other NICs, or check the parameter in config.ini. Change the parameter isbindlocal=0 to isbindlocal=1, and change localIPaddr= to localIPaddr=XXX.XXX.XXX.XXX, which is the IP address of the NIC connected to the control card. Then restart the configuration software.
- For servers with virtual machines, disable the virtual machine NICs.

Appendix 1 Cybersecurity Recommendations

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

Our 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.
- stablish 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

It is recommended 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).