Distributed Play Box

Quick Start Guide



V1.0.2

Foreword

General

This manual introduces the installation, functions and operations of the distributed play box (hereinafter referred to as "the box"). Read carefully before using the box, and keep the manual safe for future reference.

Safety Instructions

The following signal words 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, 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 Time
V1.0.2	Updated basic operations.	August 2022
V1.0.1	Updated Important Safeguards and Warnings.	April 2022
V1.0.0	First release.	April 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, 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 box, hazard prevention, and prevention of property damage. Read carefully before using the box, and comply with the guidelines when using it.

Installation Requirements

 DANGER

- Improper use of the battery might result in a fire or explosion.
- Make sure to use the same model when replacing the battery.
- Use the standard power adapter. We will assume no responsibility for any problems caused by the use of a nonstandard power adapter.
- Use the power cords that are recommended for the region and conform to the rated power specifications.



- Do not place the box in a place exposed to sunlight or near heat sources.
- Keep the box away from dampness, dust, and soot.
- Install the box on a stable surface to prevent it from falling.
- Put the box in a well-ventilated place, and do not block its ventilation.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- 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.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it.

Operation Requirements



- Do not drop or splash liquid onto the box, and make sure that there is no object filled with liquid on the box to prevent liquid from flowing into it.
- Operate the box within the rated range of power input and output.
- Do not disassemble the box.
- Use the box under allowed humidity and temperature conditions. Operating temperature: –10 °C to +55 °C (14 °F to 113 °F).

Table of Contents

Foreword I

Important Safeguards and Warnings III

1 Introduction 1

2 Packing List 2

3 Structure 3

3.1 Dimensions 3

3.2 Ports 3

4 Initialization 5

5 Login 7

6 Quick Toolbar 8

Appendix 1 Cybersecurity Recommendations 9

1 Introduction

The play box is a new generation of smart cloud information terminal integrated with multimedia information release, advertisement release, and network access. Based on an industrial design scheme, it is paired with the information release management platform that features B/S architecture. The box can play images, videos, and scroll captions in both full screen or split screen. You can set multiple play modes on the platform such as loop, timed playing, inter-cut and idle-time playing for multidimensional and flexible control over the time videos are played, their sequence, content and position.

The box is highly suitable for use in residential communities, factories, schools, and more. It can also be used in various industries such as elevator, finance, catering, media, hotel, transportation, and education.

2 Packing List

Check whether there is any obvious damage to the package box. Unpack the box and check whether the components are complete according to the packing list.

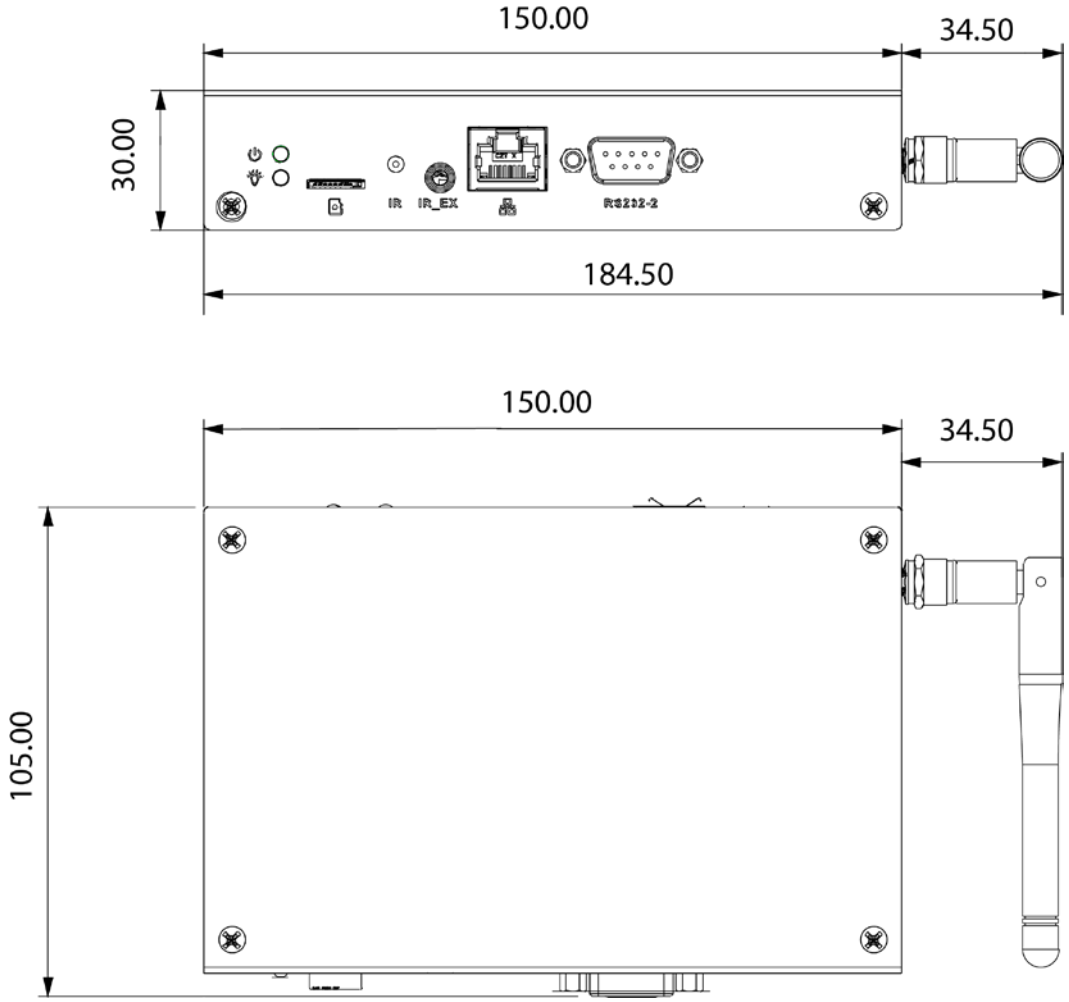
Table 2-1 Packing list

Name	Quantity	Name	Quantity
Distributed play box	1	Power adapter	1
Remote control	1	Fixed base bracket	1
Wi-Fi antenna	1	Quick Start Guide	1

3 Structure

3.1 Dimensions

Figure 3-1 Dimensions (mm [inch])



3.2 Ports

Figure 3-2 Ports (1)

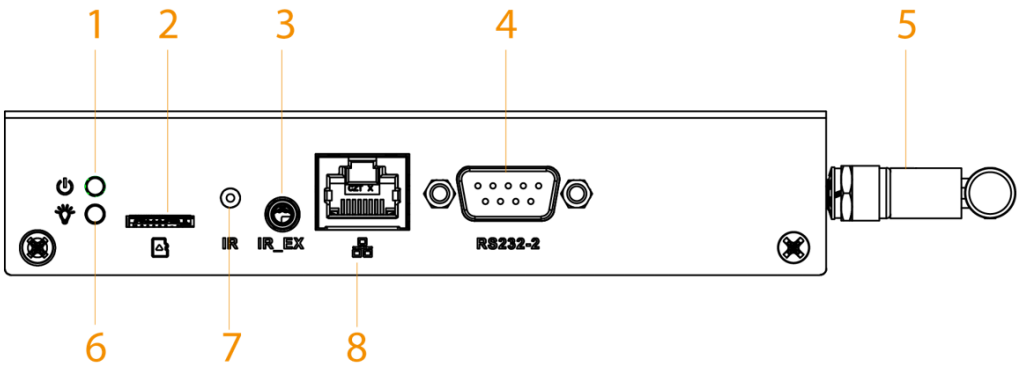


Figure 3-3 Ports (2)

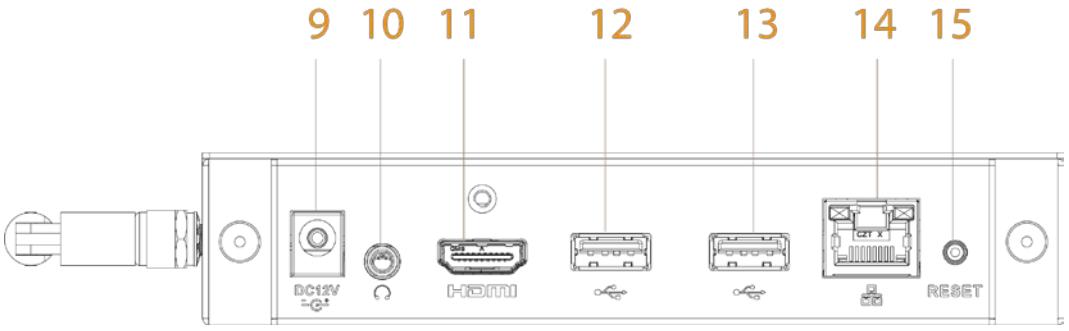


Table 3-1 Port description

No.	Name	Description
1	Power indicator light	The light turns on when the box is powered on.
2	TF card slot	Insert a TF card. The TF card is used to force update the Android OS or provide media for projects. A force update is needed when the Android OS restarts repeatedly or the box cannot be started. • You cannot use the TF card to store data on the box. • Contact the technical support if your box needs a force update.
3	IREX port	Connects to the infrared extension cable.
4	RS-232 port	DB9 RS-232 serial port for communication and debugging.
5	Wi-Fi antenna	Receives Wi-Fi signals.
6	Operation status indicator light	• The light turns on when the box runs normally. • The light flashes when the box malfunctions.
7	IR port	Receives IR signals from the remote control.
8	RS-232 port	RJ-45 RS-232 serial port for communication and debugging.
9	Power port	Connects to 12 VDC power adapter.
10	Audio jack	Connects to a 3.5 mm headphone to output audio signals.
11	HDMI port	Outputs signals to devices that support HDMI to play projects.
12	USB 2.0/OTG	Connects to the mouse, USB storage devices and other types of devices. You can switch the USB mode to OTG.
13	USB 2.0	Connects to mouse, USB storage devices and other devices.
14	Network port	Connects to the network cable.
15	Reset button	Contact customer service to use the button to restore the box to its factory settings or reset the password.

4 Initialization

When you log in for the first time or after you restore the factory settings, you need to initialize the box. After that, you can configure and operate the box.

Step 1 Power on the box.

Step 2 Select the language, and then click **Save and Next**.

Step 3 Read the software license agreement, and then click **Next**.

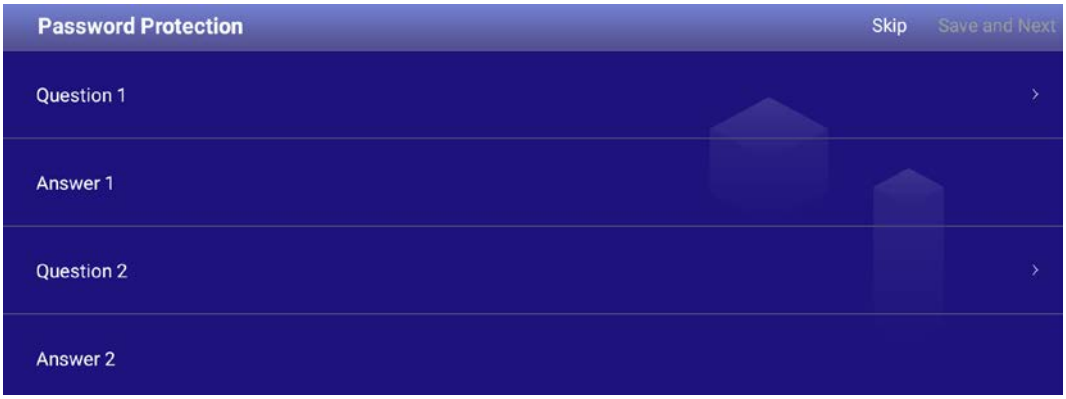
Step 4 Enter and confirm the password, and then click **OK**.

Step 5 Set your security questions.

Click **Skip** if you do not want to configure the security questions.

1. Select the security questions and then configure the corresponding answers.
2. Click **Save and Next**.

Figure 4-1 Password protection



Step 6 Set the device name.

1. Click to set the device name.
2. Click **Save and Next**.

Step 7 Configure network settings.

Click **Skip** if you do not want to configure the network settings.

1. Select a network type and then configure network settings.

Table 4-1 Network settings

Network type	Description
WLAN	Click when Wi-Fi is available near the box. ● Auto search: Click a Wi-Fi network, enter its password, and then click **Connect**. ● Connect to the Wi-Fi manually: Click , and then on the **Add network** page, enter network SSID, select a security option, and then click **Save**. We recommend you choose a secure authentication method to connect to the Wi-Fi.
Ethernet	Connect the box to the network by Ethernet. There are 2 methods to set the IP address of the box. ● DHCP: When there is a DHCP server on the network, select **DHCP** to allow the box to get an IP address from the DHCP server automatically. ● Static IP: After you select **Static IP**, configure **IP Address**, **Gateway**, and **Netmask** according to your network plan.

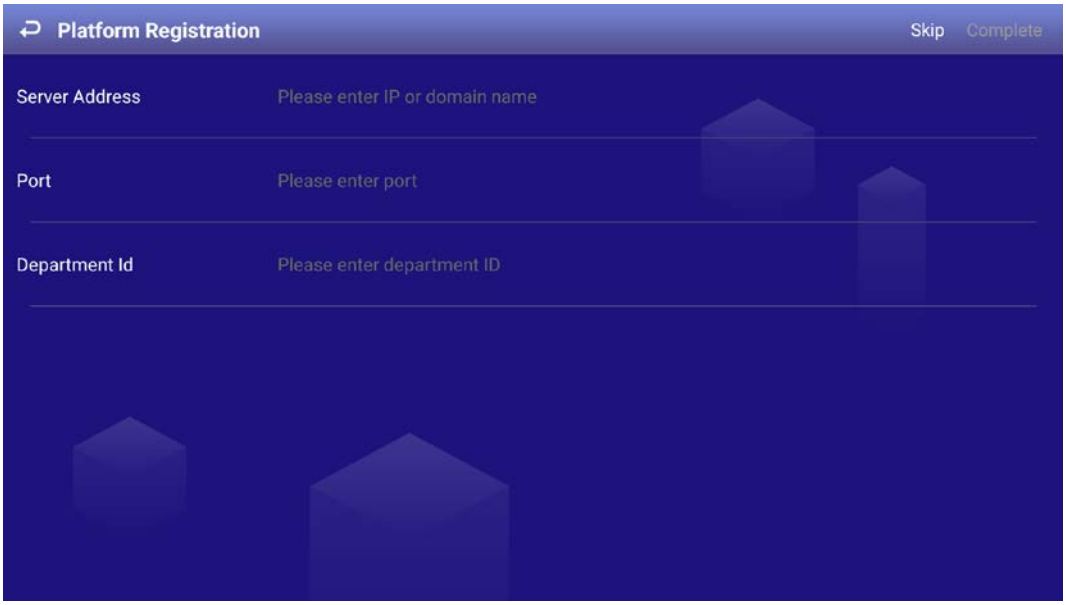
2. Click **Save and Next**.

Step 8 Register the box to the platform.

Click **Skip** to skip platform registration.

1. Enter the IP address or domain name, port of the platform (MPS or ICC), and the department ID.

Figure 4-2 Platform registration



2. Click **Complete**.

5 Login

You need to log in to the system to perform operations when any of the following situations occurs.

- It is your first-time use after initialization.
- You locked the screen manually.
- The screen locked the screen automatically after a long period of inactivity.

Step 1 Click any position on the screen.

Step 2 Enter the password, and then click **OK**.

The home page or the page that was open before the screen is locked is displayed.



After 5 consecutive failed login attempts, the system will prompt **Account locked, restart or try again 5 minutes later**.

6 Quick Toolbar

The quick toolbar can help to improve your operation efficiency.

Point to the bottom of the page, and then the quick toolbar is displayed.

Figure 6-1 Quick toolbar

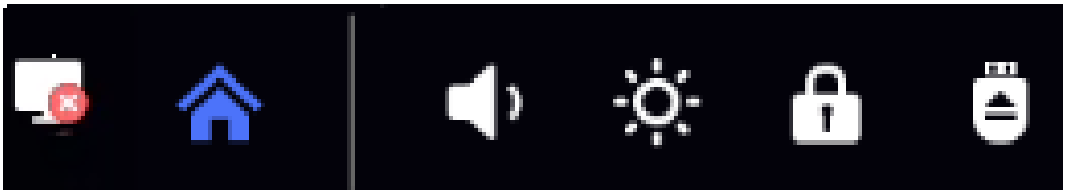


Table 6-1 Description of quick toolbar

Icon	Description
	Indicates whether the box is registered to the platform.
	Go to the home page.
	Adjust volume.
	Adjust backlight brightness.
	Lock the screen.
	Disconnect your USB drive from the box.

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.