



Play Box

User Manual



V1.0.1

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 result.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	Updated Foreword, Important Safeguards and Warnings, and Structure.	October 2025
V1.0.0	First release.	August 2025

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.

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.

Transportation Requirements



Transport the device under allowed humidity and temperature conditions.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Installation Requirements



DANGER

Stability Hazard

Possible result: The device might fall down and cause serious personal injury.

Preventive measures (including but not limited to):

- Only use cabinets and brackets specified for the device.
- Only use furniture and structures that can safely support the device.
- Do not place the device on the edge of the furniture or structure that is supporting it.
- Always educate children about the dangers of climbing furniture to reach the device and its controller.
- Carefully arrange the cables connected to the device to avoid people tripping over them and pulling on them.
- Make sure that the device is installed on a stable surface.
- Do not put the device on tall furniture, such as cabinets and bookcases, without first ensuring that the supporting structure is stable enough to bare the device.
- Do not place the device on fabric and other similar material.
- Do not place items, such as toys and remote controls, that may entice children to climb on top of the device or furniture on which the device is placed.



WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- Please follow the electrical requirements to power the device.
 - ◇ Following are the requirements for selecting a power adapter.

- The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
- The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
- When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
- ◇ We recommend using the power adapter provided with the device.
- ◇ When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.



- 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 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



-   The device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

Preventive measures (including but not limited to):

- ◇ Keep new and used batteries out of reach of children.
 - ◇ If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
 - ◇ Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions.

Preventive measures (including but not limited to):

- ◇ Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
- ◇ Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
- ◇ Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
- ◇ Do not leave the batteries in environments with extremely low air pressure to avoid explosions and leakage of flammable liquids or gas.



- Use the box under allowed humidity and temperature conditions. Operating temperature: – 10 °C to +55 °C (14 °F to +113 °F).
- Make sure that the power supply is correct before use.

- Make sure that the device is power off before disassembling wires to avoid personal injury.
- Operate the box within the rated range of power input and output.
- Do not disassemble the box.
- Place the device in a location that children cannot easily access.
- 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.
- Do not disassemble the device without professional instruction.

Maintenance Requirements



Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

Preventive measures (including but not limited to):

- Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
- Dispose of the old batteries as instructed.



- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	II
1 Introduction.....	1
2 Packing List.....	2
3 Structure.....	3
3.1 Dimensions.....	3
3.2 Ports.....	4
4 Basic Operations.....	6
4.1 Starting and Shutting Down.....	6
4.2 Initialization.....	6
4.3 Login.....	11
4.4 Homepage.....	12
4.5 Quick Toolbar.....	12
4.6 Project Release.....	13
4.6.1 Network Release.....	13
4.6.2 Local Release.....	15
4.7 File Manager.....	27
4.8 App Installation.....	28
5 System Configuration.....	29
5.1 Network Settings.....	29
5.2 General Settings.....	31
5.3 System Settings.....	34
Appendix 1 Remote Control.....	36
Appendix 2 Security Commitment and Recommendation.....	38

1 Introduction

The 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.

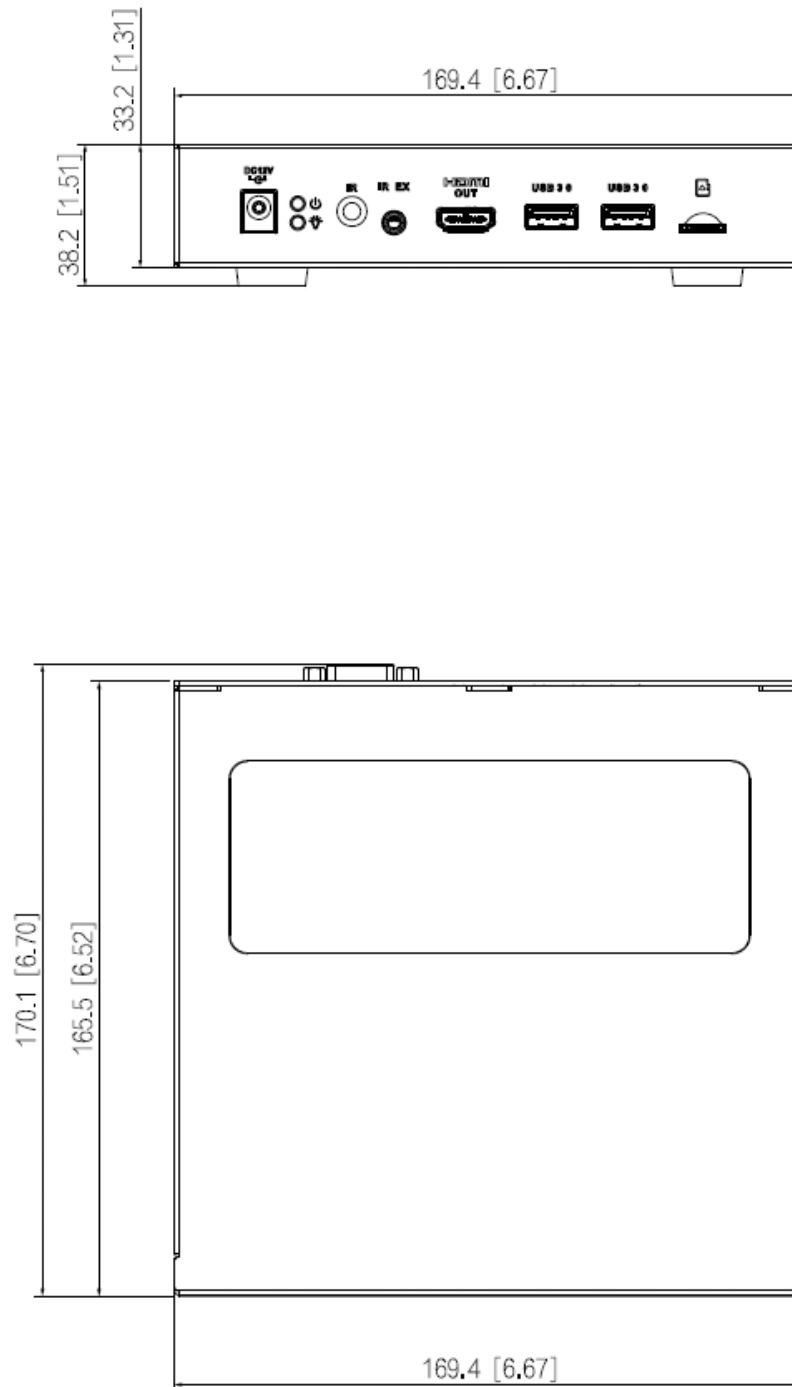
Table 2-1 Packing list

Name	Quantity	Name	Quantity
Play box	1	Power adapter	1
Remote control	1	Fixed base bracket	1
Quick Start Guide	1	—	—

3 Structure

3.1 Dimensions

Figure 3-1 Dimensions (Unit: mm [inch])



3.2 Ports

Figure 3-2 Front port

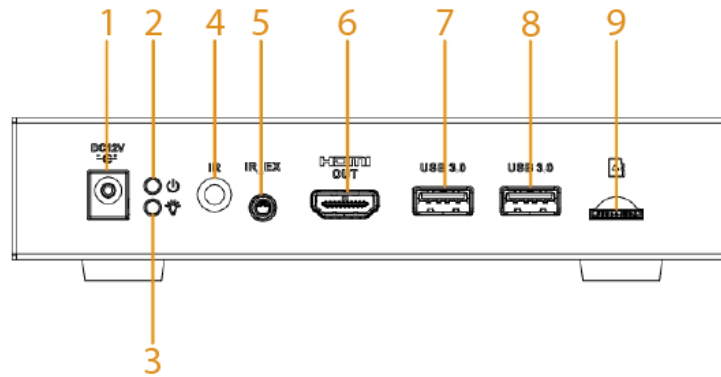


Figure 3-3 Rear port

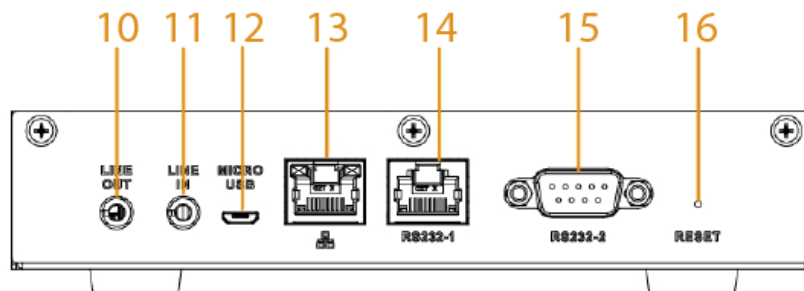


Table 3-1 Port description

No.	Name	Description
1	Power port	Connects to 12 VDC power adapter.
2	Power indicator	Indicates the power-on status, normally the light is red.
3	System indicator	Indicates system working status, the normal light is green.
4	IR port	Infrared remote control signal receiver port.
5	IREX port	Connects to the infrared extension cable.
6	HDMI port	Outputs signals to devices that support HDMI to play projects.
7&8	USB3.0	Connects to mouse, USB storage devices and other devices.

No.	Name	Description
9	TF card slot	Insert a TF card. The TF card is used to provide media for projects.  You cannot use the TF card to store data on the box.
10	LINE OUT	Audio output port.
11	LINE IN	Audio iutput port.
12	MICRO USB	Device debugging port.
13	Network port	Connects to the network cable.
14	RS232-1 serial port	RS232 serial port in the form of RJ45 port, used for serial communication debugging.
15	RS232-2 serial port	RS232 serial port in the form of DB9 port, used for serial communication debugging.
16	Reset button	Used to restore factory settings or reset password. ● Press 3 times to reset password. ● Long press to restore factory settings.

4 Basic Operations

4.1 Starting and Shutting Down



- Before starting the box, check whether the input voltage matches rated voltage of the box.
- To ensure stable operation and long service life of the box and external devices connected to the box, follow national standards and provide a power supply with stable voltage and low ripple interference.

Starting the Box

Plug in the power cable of the box. The box starts.

Shutting down the Box

Unplug the power cable. The box shuts down.

4.2 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.

Procedure

- Step 1 Power on the box.
- Step 2 Select the language, and then click **Next**.

Figure 4-1 Select language

Step 1/8

Let's get you setup. Please select your language.

- ☐ 简体中文
Simplified Chinese
- ☒ English
English
- ☐ 繁體中文
Traditional Chinese
- ☐ Italiano
Italian
- ☐ Deutsch
German
- ☐ Français
French
- ☐ Español Europeo

Next

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

Figure 4-2 Private policy

Step 2/8

Privacy Statement

Privacy Policy

Last modified: August 20, 2025

Introduction

Zhejiang Dahua Technology Co., Ltd ("Dahua", "we", "us" or "our") respects your privacy and is committed to protecting it through our compliance with this Privacy Policy (the "Policy"). This Policy describes how we process your personal data when you use the Dahua Information Release Products (the "Product"), or use service(s) as provided by us or our affiliates (the "Service") in connection with the Product. For specific usage or service scenarios, we may release a dedicated privacy policy to describe how to process your personal data and exercise your rights.

Please read this Policy carefully to understand our policies and practices regarding your personal data and how we will treat it. If you have any issues regarding this Policy, please contact us at supportoverseas@dahuatech.com.

Table of contents

1. How We Process Your Personal Data and Purpose of Processing
2. How We Share, Assign and Disclose Your Personal Data
3. Third Party Products and Services
4. How We Protect and Retain Your Personal Data

☐ I agree to all the contents of the above agreement

Previous

Next

Figure 4-3 Software license agreement

Step 3/8

Please read the Software License Agreement

SOFTWARE LICENSE AGREEMENT

Last modified: September 25, 2023

1. PREAMBLE

IMPORTANT NOTICE, PLEASE READ CAREFULLY:

1.1 This Agreement is a Software License Agreement between you and Zhejiang Dahua Technology Co., Ltd. ("Company" or "We"). Please read this software license agreement (hereinafter referred to as "Agreement") carefully before using the Software. By using Company Software, you are deemed to agree to be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, please do not install or use the Software, and click the "disagree" button. If

☐ I agree to all the contents of the above agreement

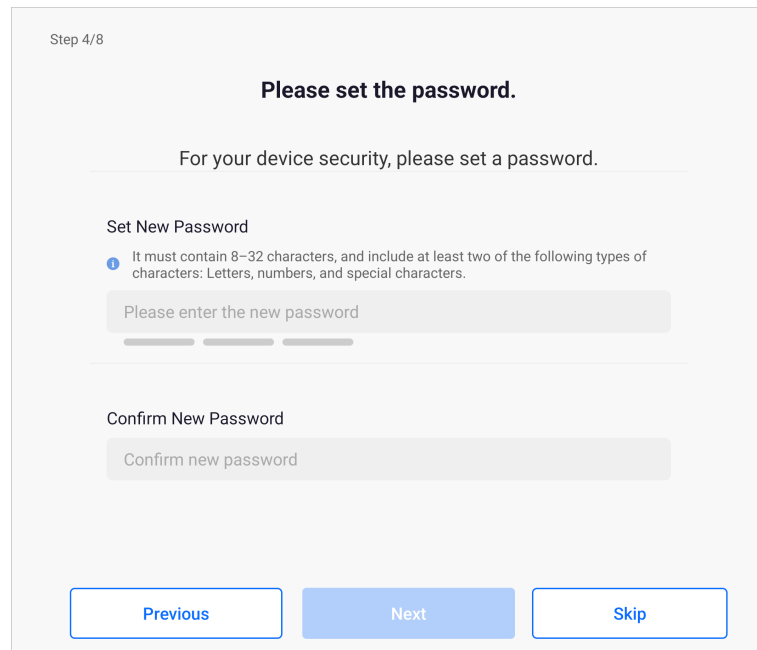
Previous

Next

Step 4 Set a password.

Enter the password and confirm it, and then click **Next**.

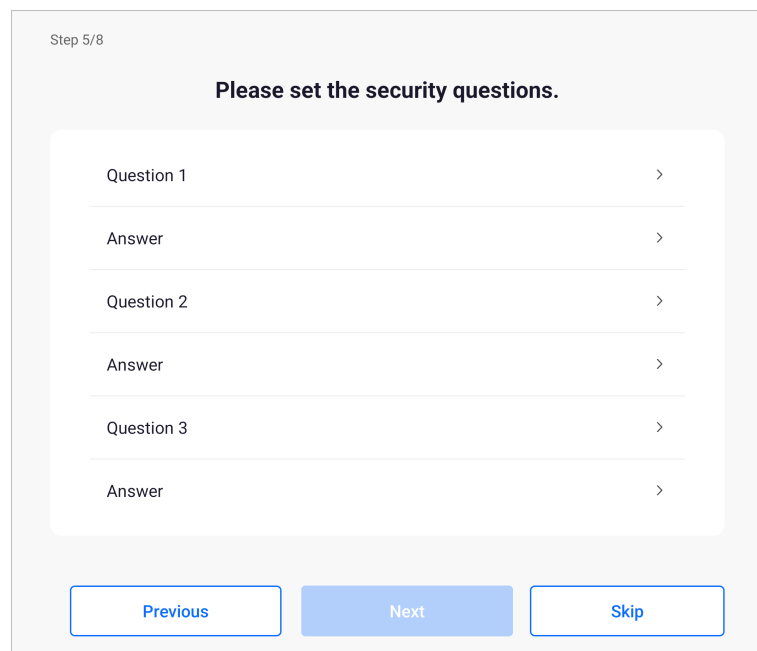
Figure 4-4 Set a password

**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 **Next**.

Figure 4-5 Password protection

**Step 6** Configure network settings.

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

1. Configure the network as required.

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 the password, and then click Connect.  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 **Next**.

Figure 4-6 Configure the wireless network

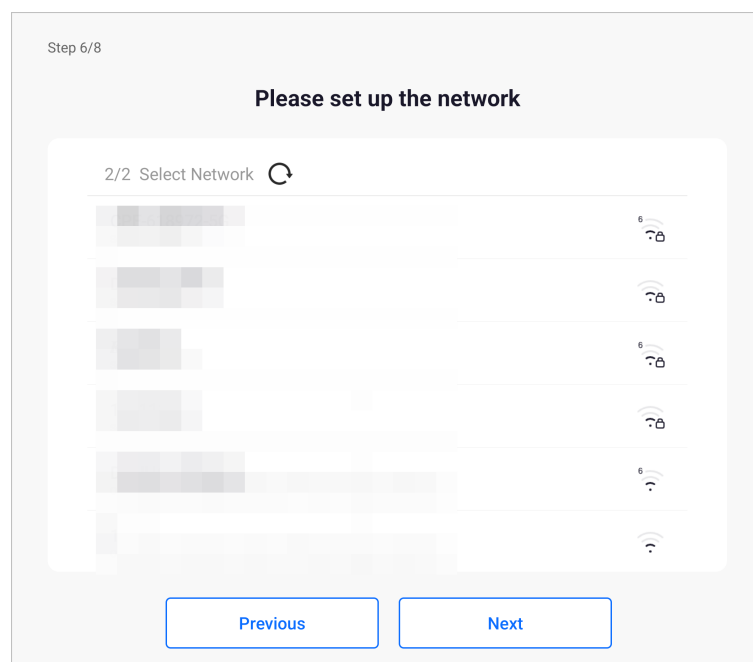


Figure 4-7 Configure the wired network

Step 6/8

Please set up the network

2/2 Configure Wired Network

IP Assignment Auto >

Local Network	Not Connected
IP Address	0.0.0.0
Gateway	0.0.0.0
Subnet Mask	0.0.0.0

[Previous](#) [Next](#)

Step 7 Set device information.

1. Click the device name to set it up.
2. Click **Next**.

Figure 4-8 Configure the device information

Step 7/8

Please check your device information.

Device Name

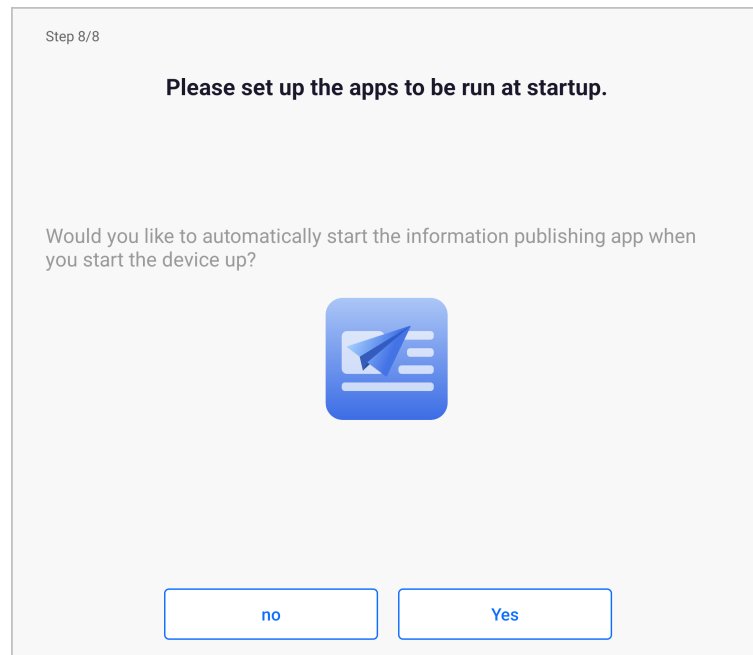
11111111

Device SN	11111111
Motherboard Model	LDM-N(AMPB)
System Version No.	

[Previous](#) [Next](#)

Step 8 Set the apps to be run at startup.

Figure 4-9 Set the apps to be run at startup



4.3 Login

After logging in for the first time, locking the screen manually, or automatically locking the screen, you need to log in to the system before you can perform any operations.

Procedure

Step 1 Click the screen and enter your password.

Step 2 Click **Login**.

The system displays the main page or the page before the lock screen.



If the password is entered incorrectly more than 5 times, you need to restart or try again after 5 minutes.

4.4 Homepage

Figure 4-10 Homepage

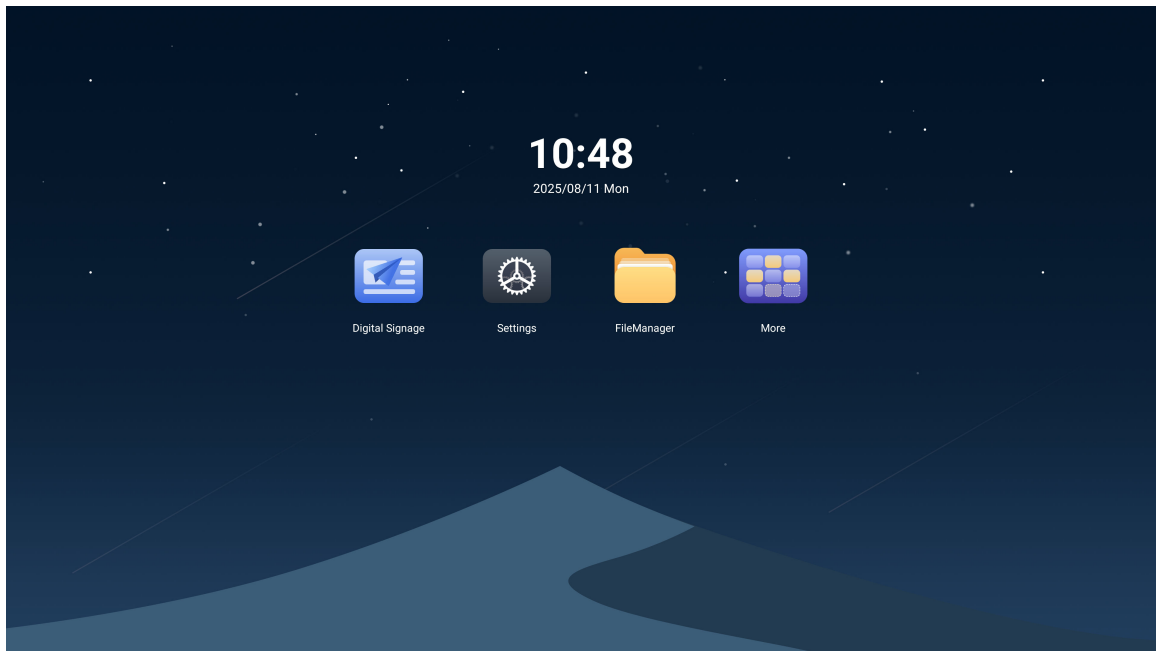


Table 4-2 Homepage description

Feature	Description
Digital Signage	Distribute content either by pushing it from the platform or publishing it locally.
Settings	System configuration, including adjusting network and general settings, and viewing system information.
FileManager	File management for access local files, such as images, videos, documents, and APK packages.
More	Browse or install apps. - Click an existing app icon to open it. - Click Install App, select an APK package, and install other applications.

4.5 Quick Toolbar

The quick toolbar can help to improve your operation efficiency.

Figure 4-11 Quick toolbar



Table 4-3 Description of quick toolbar

Icon	Description
	Go to the home page.
	Return to the previous level.
	Manual lock screen.
	Adjust volume.
	Open file manager.

4.6 Project Release

4.6.1 Network Release

If you want to release projects through the platform for the first time, the Device must be registered in the accompanying media publishing system. For detailed operations of the media publishing system, refer to its user manual.

4.6.1.1 Configuration Flow

Complete the configuration flow to release projects via the network.

Figure 4-12 Configuration flow of network release



Table 4-4 Configuration flow (network release)

Operation	Description
Log in	Log in and configure the Device.
Configure network	Connects the Device to the network.
Register the Device to the platform	After registering the Device to the platform, you can release projects and operate the Device through the platform.
Release project through the platform	After adding media and configuring project plans on the platform, the project can be played on the Device. For details, see the user's manual of the platform.

4.6.1.2 Connecting the Device to Network

Connect the Device to a wired or wireless network.

For detailed operations, see "5.1 Network Settings".

4.6.1.3 Registering the Device to the Platform

After being registered to the platform, the Device can release projects issued by the platform.

Prerequisites

- The Device and the platform are connected to the same network.
- The platform's IP address has been added on the Device.

Procedure

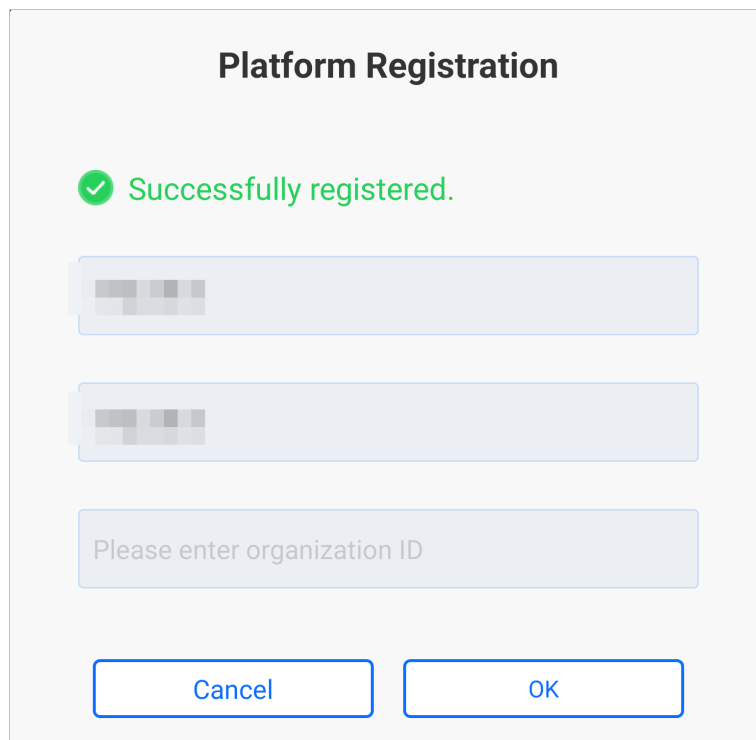
Step 1 Click **Network Release** to set the platform server's IP address or domain name, port number, and organization ID.

The department ID is the terminal group ID on the platform. After registration, only users associated with the department can manage the terminal device.



The department ID on the Device side can be left blank. When the Device is manually moved to a group on the platform, the department ID will be automatically assigned to the Device. Platform users can only manage devices associated with their own department.

Figure 4-13 Platform registration settings



Step 2 Click **OK**.



After successful registration, the icon would be shown as .

Step 3 Click **Network Release**.

Projects issued by the platform are available for being released.

4.6.2 Local Release

Add videos or pictures to projects, and release projects locally through **General Template** or **Industry Template**.

4.6.2.1 Configuration Flow

Figure 4-14 Local release (general template)

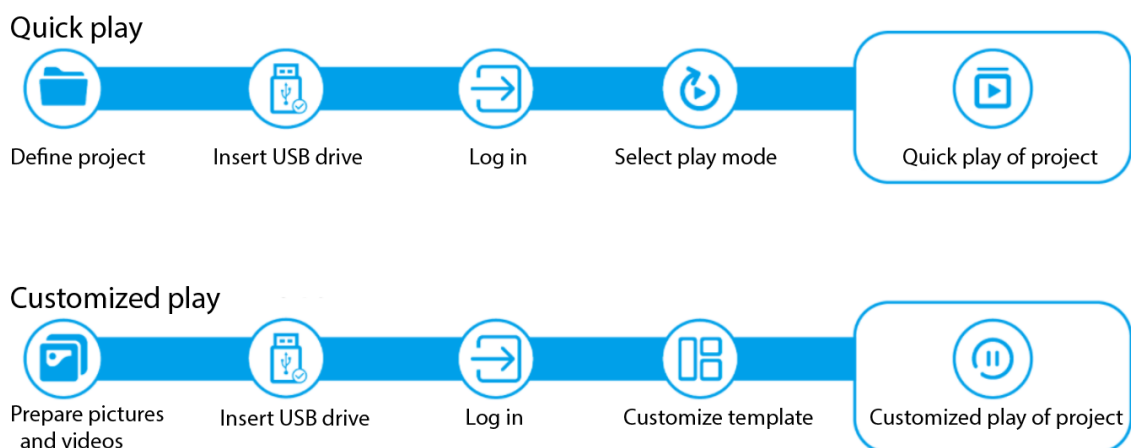
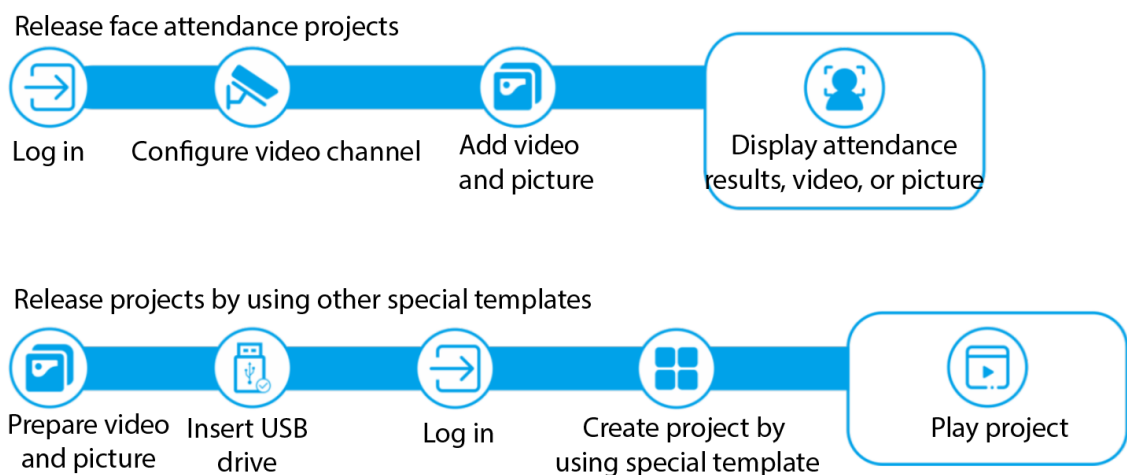


Figure 4-15 Local release (industry template)



4.6.2.2 Releasing Projects by General Templates

4.6.2.2.1 Quick Play

Use the given templates to quickly release projects.

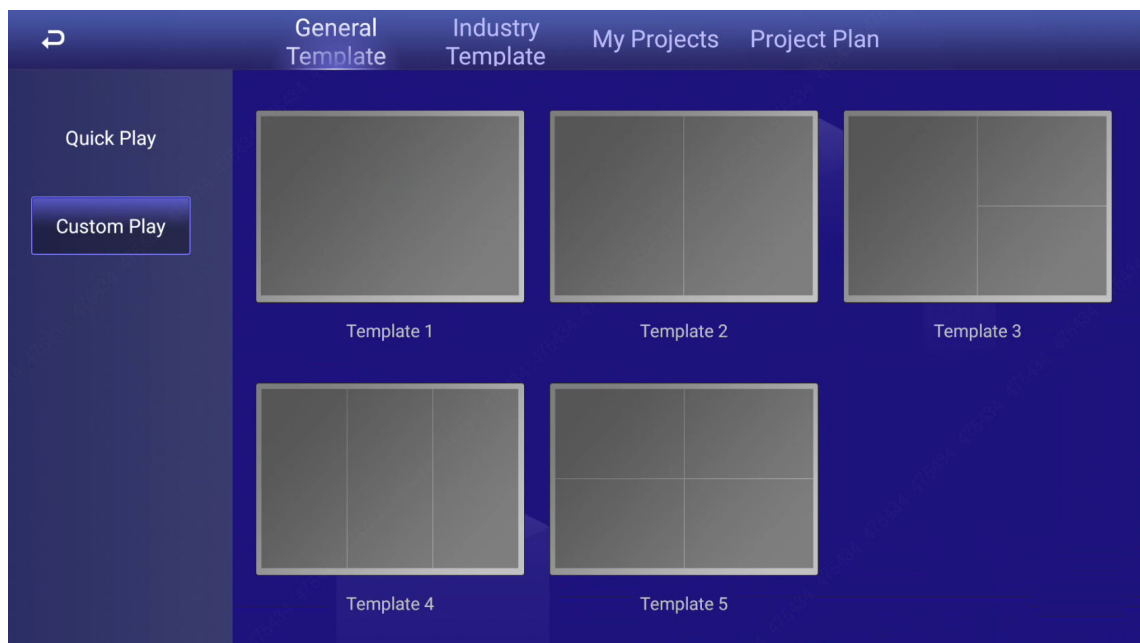
Prerequisites

- The USBPLAY folder is created on the USB drive.
- Insert the USB drive with media to be played into the Device. Make sure that the pictures and videos are saved in the root directory of the USBPLAY folder.

Procedure

Step 1 On the main page, select **Local Release** > **General** > **Quick Play**.

Figure 4-16 Quick play



Step 2 Select a template.

The system will display pictures and videos according to their layout in the template. A picture is displayed for 10 seconds by default and a video to the end.

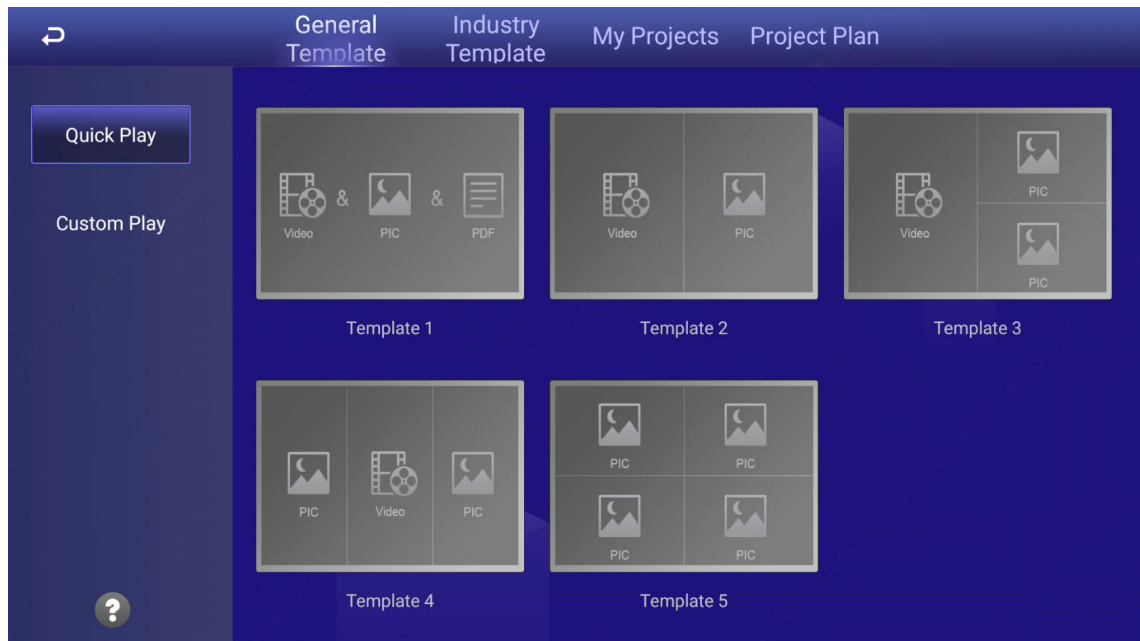
4.6.2.2.2 Custom Play

Define your own templates to release information.

Procedure

Step 1 On the main page, select **Local Release** > **General** > **Custom Play**.

Figure 4-17 Customized play

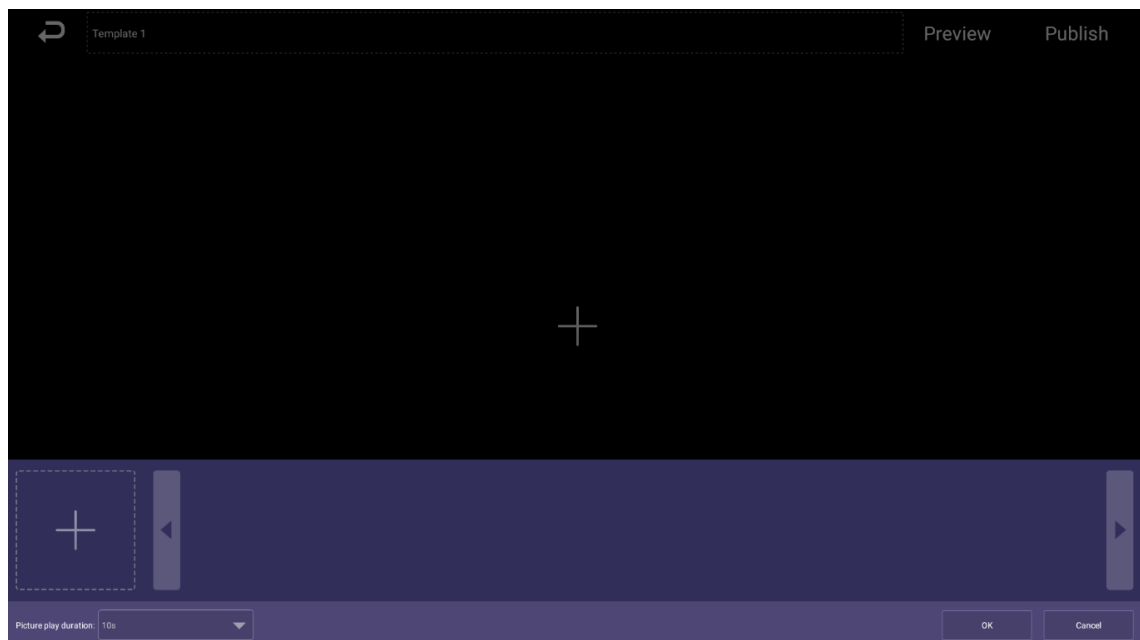


Step 2 Click a template that you want to define.

Step 3 Define the template.

1. Click  to configure this region's display sequence and content.

Figure 4-18 Add media



2. Click .
3. Select a picture or a video, and configure the picture play duration as needed.



- Pictures are displayed for 10 seconds by default and videos to the end.
- You can repeat the following steps to upload multiple pictures or videos. After adding the media (pictures and videos), you can drag the media to sort them.

- Click  to delete the picture/video.

4. Click **OK**.

If there are multiple regions in your template, to make the template effective, you need to add projects to other regions.

Step 4 (Optional) Click **Preview** to preview the project to be played.

Step 5 Click **Publish** to play your project immediately.

4.6.2.3 Releasing Projects by Industry Templates

Industry templates include face attendance template, advertising templates and video surveillance templates. Templates of the media publishing platform are supported to be imported.

4.6.2.3.1 Configuring Face Attendance Template

Add a camera channel to the Device, and then the face information captured by the camera will be displayed, such as the similarity between the faces captured and faces saved in the database, and capture time.

Prerequisites

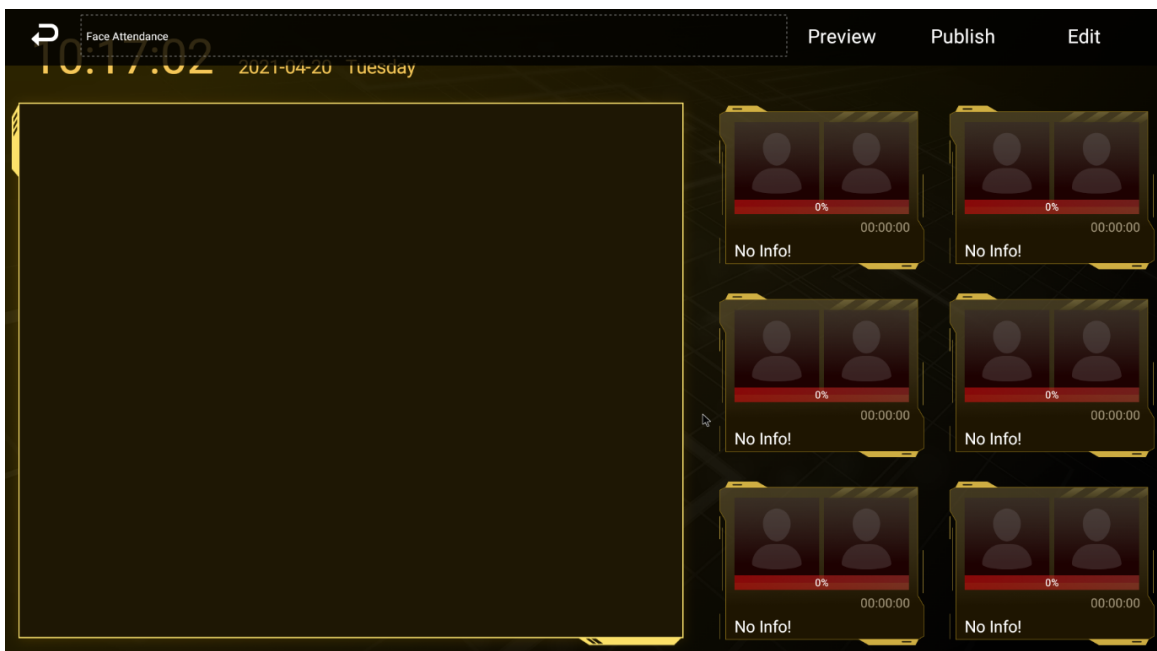
- The Device, your camera, and the platform are connected to the same LAN (Local Area Network).
- Your camera supports face detection and face comparison, and face database is configured.

Procedure

Step 1 On the main page, select **Local Release** > **Industry Template**.

Step 2 Click the **Face Attendance** template.

Figure 4-19 Configure face attendance template



Step 3 Click **Edit** on the upper-right corner.



- You can add video channels, video recordings and pictures to the template.
- Only one kind of media can be played at the same time.

Step 4 Add a monitoring device, and then configure other parameters.

Figure 4-20 Setting



Step 5 Click **Add**, and then configure the parameters of the monitoring device.

Figure 4-21 Add monitoring device

Add Monitoring Device

IP Address

Username

Password

Port No.

Channel No.

Bit Rate

OK
Cancel

Table 4-5 Description of adding monitoring device

Parameter	Description
IP Address	The IP address of the Device, the platform, or the client. If you select Acquisition as the protocol, enter the IP address of the IP camera or the IVSS.

Parameter	Description
Username	If you select Acquisition as the protocol, configure the username and password for logging into the camera or platform. - When adding an IP camera, enter the username and password for logging into the camera. - When adding an IVSS, enter the username and password for logging into the IVSS.
Password	
Port No.	Port for logging in to an IP camera or the platform. If you select Acquisition as the protocol, enter the port number for logging into the IP camera, with the default number of 37777.
Channel No.	If you select Acquisition as the protocol, configure the remote channel number to connect. - When adding an IP camera, set the channel number to 1. - When adding an IVSS, set it to the channel number displayed on the IVSS.
Bit Rate	Select Main Stream , Sub Stream1 or Sub Stream2 .

Step 6 Click **Confirm**, and then configure other parameters.

Table 4-6 Description of other parameters

Parameter	Description
Display Video Image	Screen s plit: You can view the video image of the added channels by 1, 2, 3, or 4 splits. Switching time (seconds) : Switch to play video of another added channel after the defined time. Channel selection : Select the channel to be played in each screen split.
Play Media	Click  to add media (video or picture).  - Select media, and then click  to delete it. - Drag the media to sort them. - Pictures are displayed for 10 seconds by default and videos to the end. - Only one kind of media can be played at a time.

Parameter	Description
Display Comparison Results	Enable or disable voice broadcast and display face comparison results. • Voice broadcast: Click  to enable voice broadcast. It supports setting the broadcast content as Name+result, Result or None. • Broadcast now: After it is enabled, if the broadcasts overlap, the current broadcast will be directly overwritten and the next one will be announced immediately. • Display successful comparison results: Click , and then select the item to be displayed when face comparison succeeds. • Display failed comparison results: Click , and then select the item to be displayed when face comparison fails. • Supports the broadcast of credential numbers and temperature.
Display LOGO	Click  to add a picture.  The image uploaded must not exceed 430 pixels in width and 80 pixels in height.

Step 7 Click **Preview** on the upper-right corner to preview the project to be played.

Step 8 Click **Publish** on the upper-right corner to play your project immediately.

4.6.2.3.2 Configuring Video Surveillance Templates

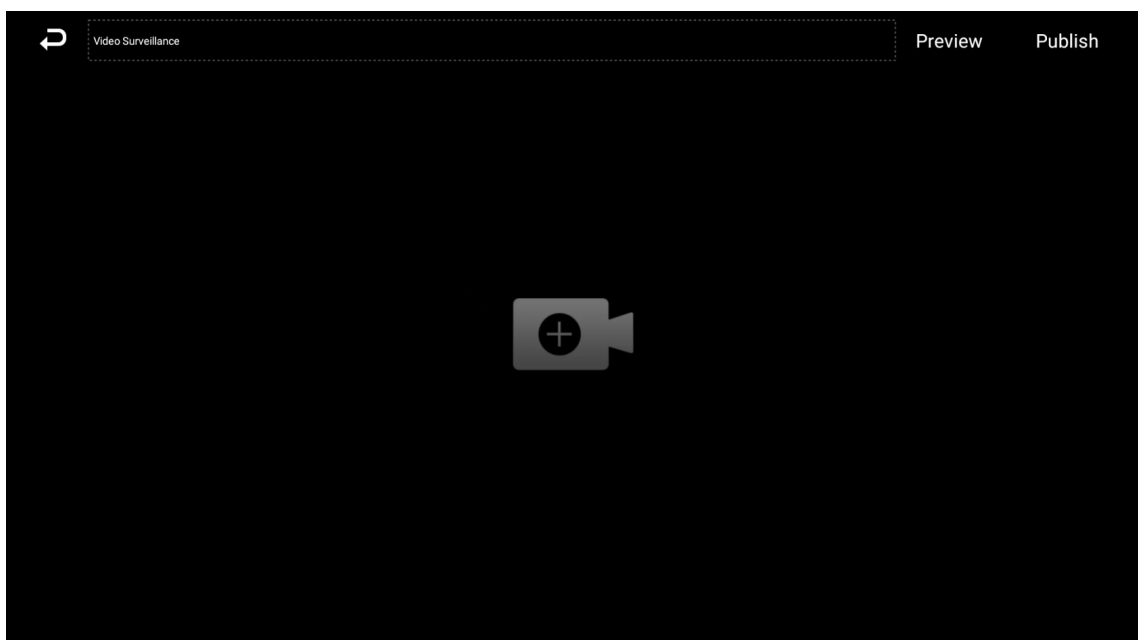
Surveillance templates include the advertising template, video surveillance template, and the people counting template. This section introduces the configuration of the video surveillance template as an example.

Procedure

Step 1 On the main page, select **Local Release** > **Industry Template**.

Step 2 Click **Video Surveillance Template**.

Figure 4-22 Video Surveillance Template



Step 3 Click  to add a monitoring device.

Figure 4-23 Add monitoring device

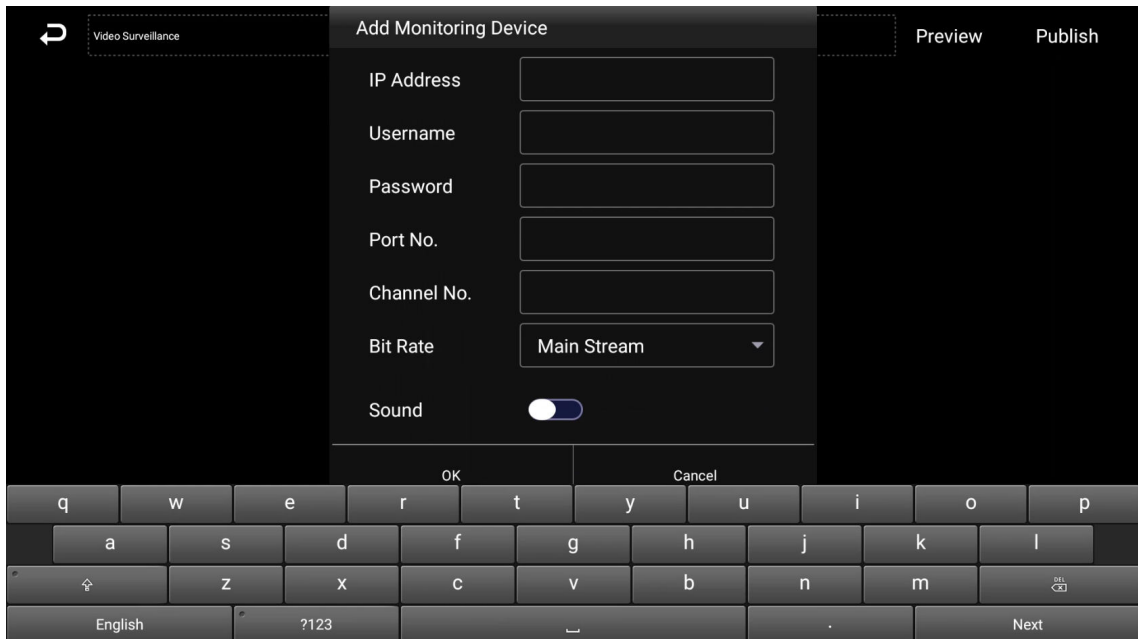


Table 4-7 Monitoring device parameters

Parameter	Description
IP Address	The IP address of the monitoring device.
Username	The username and password for logging into the monitoring device or the associated platform.
Password	
Port No.	The port number for logging into the monitoring device or the associated platform.
Channel No.	The remote channel number connected to the monitoring device.
Bit Rate	Select Main Stream , Sub Stream1 or Sub Stream2 .
Sound	When enabled, it plays the real-time audio captured by the monitoring device.  This feature is not available for the video surveillance and advertising templates.
People Counting	● Max Number: Set the maximum number of people to be counted. If this number is exceeded, the screen will alarm (red light on). ● Warning Number: Set the warning threshold for the number of people. If this number is exceeded, the screen will alert (yellow light on). ● Presumed Number: Set the default value for the number of people. ● Enter/Exit: When enabled, it counts the number of people entering and exiting separately.  This feature is only available for the people counting template.

- Step 4 Click **OK**.
- Step 5 Click **Preview** to preview the project to be played.
- Step 6 Click **Publish** to play your project immediately.

4.6.2.3.3 Importing Templates from the Platform

Import templates created by the platform to quickly release projects. Supports to import the media at the same times.

Prerequisites

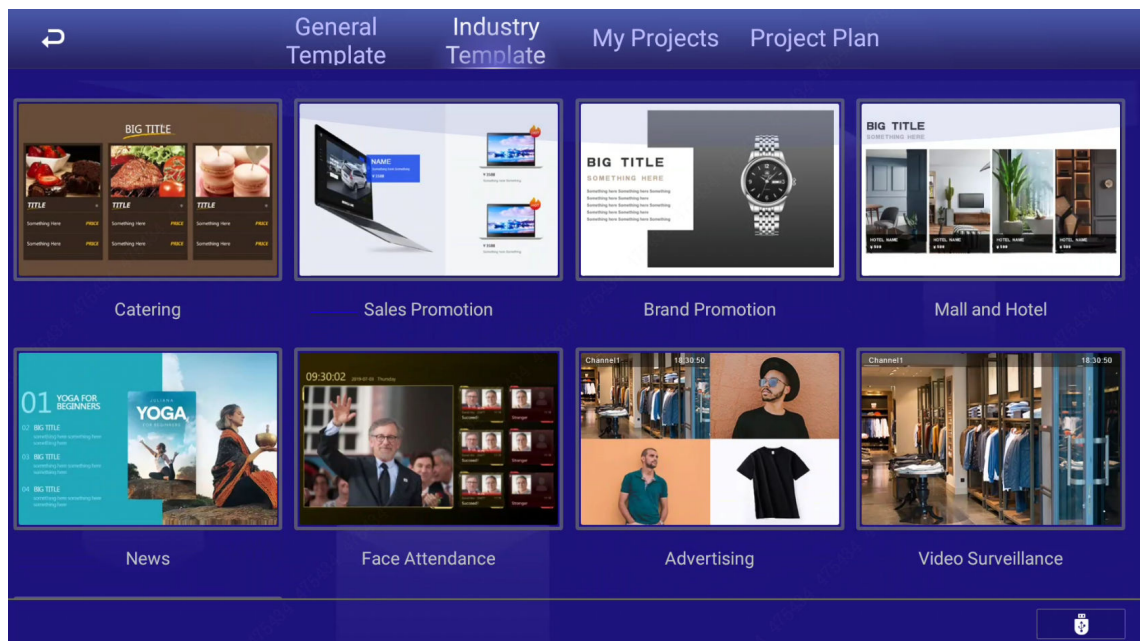
Already exported the template from the platform. If you choose to export media at the same time when exporting a template, the exported file contains both the template and media.

Procedure

- Step 1 Import the template created by the platform.
1. Create a new folder named **TEMPLATE** on the USB drive.
 2. Copy the files exported from the platform to the **TEMPLATE** folder.
 3. Select **Local Release** > **Industry Template**, and then click  on the lower-right corner.
 4. On the pop-up page, click **Confirm**. The Device starts to importing the platform.
- Step 2 Click the imported template, and then edit it.

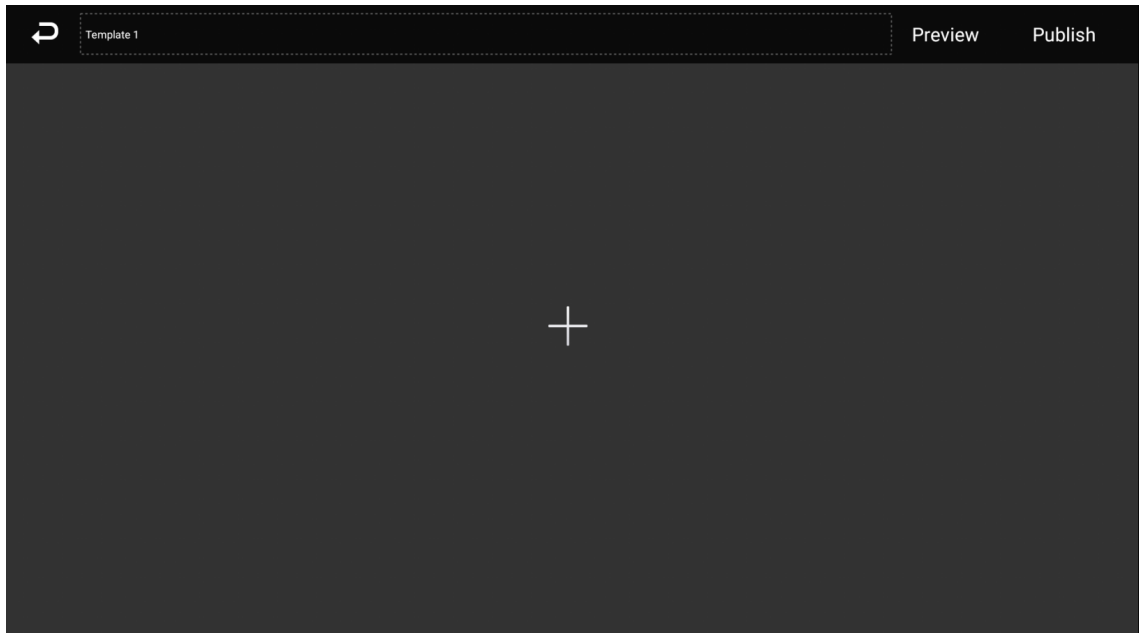
The imported template shows  on the upper-right corner.

Figure 4-24 Templates imported from the platform



Supports to modify the name of the template. Click  to add more media.

Figure 4-25 Edit the template



Step 3 Click **Preview** to preview the added media.

Step 4 Click **Publish**, the system displays the configured project.

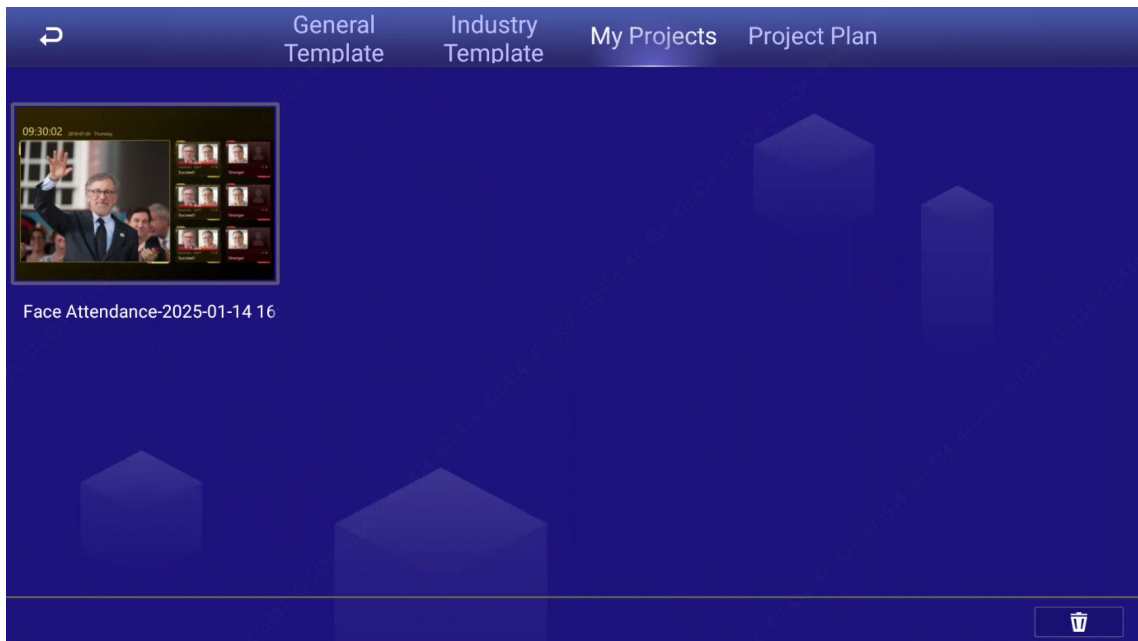
4.6.2.4 Managing My Project

On the main page, select **Local Release** > **My Project**, and then you can view projects that have been played and the templates you have saved.

You can also:

- View played projects and saved templates.
- Click a project to play it.
- Click , and then select a project to delete this project.

Figure 4-26 My project



4.6.2.5 Scheduled Project

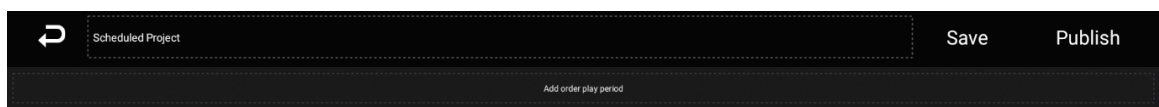
4.6.2.5.1 Customizing Scheduled Project

Configure which and when projects will be played.

Procedure

- Step 1** On the main page, select **Local Release** > **Scheduled Project**.
- Step 2** Click , and then on the page displayed, click **Add order play period**.

Figure 4-27 Add order play period



- Step 3** Set time period, and then click .

Figure 4-28 Add order play period

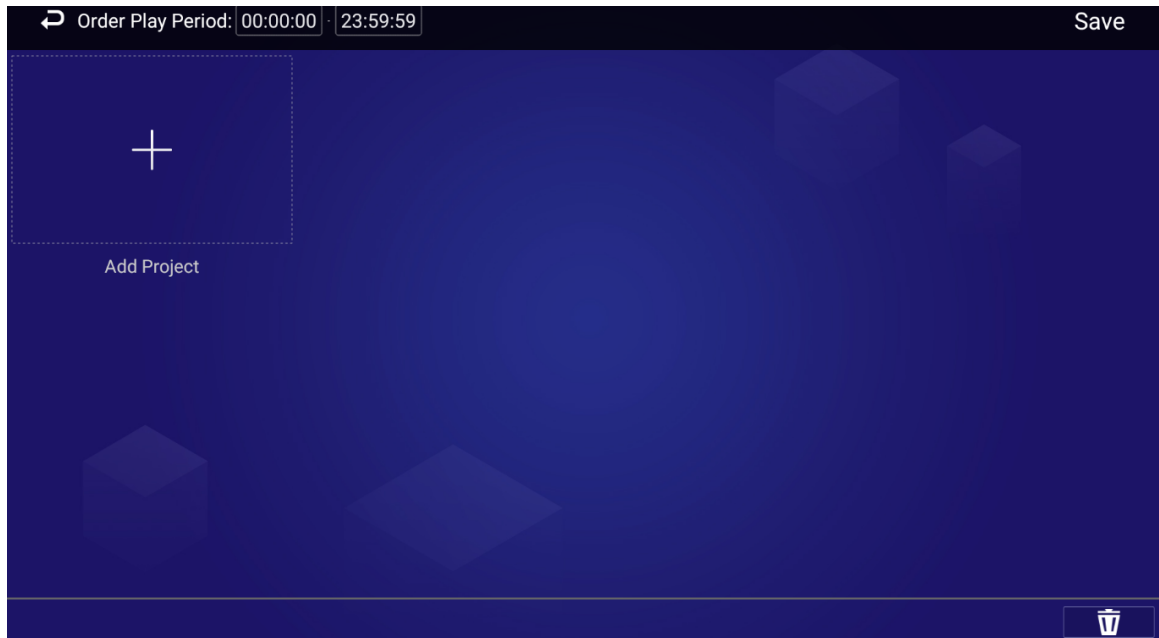


- Step 4** Click , select a project, and then click **OK**.
The system goes back to the **Add Project** page.



Up to 30 projects can be added to each time period.

Figure 4-29 Add project



Step 5 Click **Save**.

The system goes back to the **Add order play period** page.



Up to 30 periods can be added.

Step 6 Click **Save**.



You can also click **Publish** to play the project immediately.

4.6.2.5.2 Importing Project from the Platform

Prerequisites

Already exported projects from the platform.

Procedure

- Step 1** Create a new folder named **DAILYPLAN** on the USB drive.
- Step 2** Copy the project exported from the platform to the **DAILYPLAN** folder.
- Step 3** Insert the USB drive to the Device, and then import the project.
- Step 4** Click the imported project to check the information.

The imported project shows  on the upper-right corner.

- If the imported project is expired, the project details cannot be viewed.
- If the current time is within the scheduled time, the Device jumps to the network release page to display the specific project.
- If the current time is not in the scheduled time, the Device jumps to the network release page, but no project will be displayed.

4.7 File Manager

Used for managing local files and USB-drive files.

On the homepage, click **FileManager** to open an interface that displays local files, images, documents, etc. Below **Local File**, you'll see how much storage is used and how much remains.

Figure 4-30 FileManager

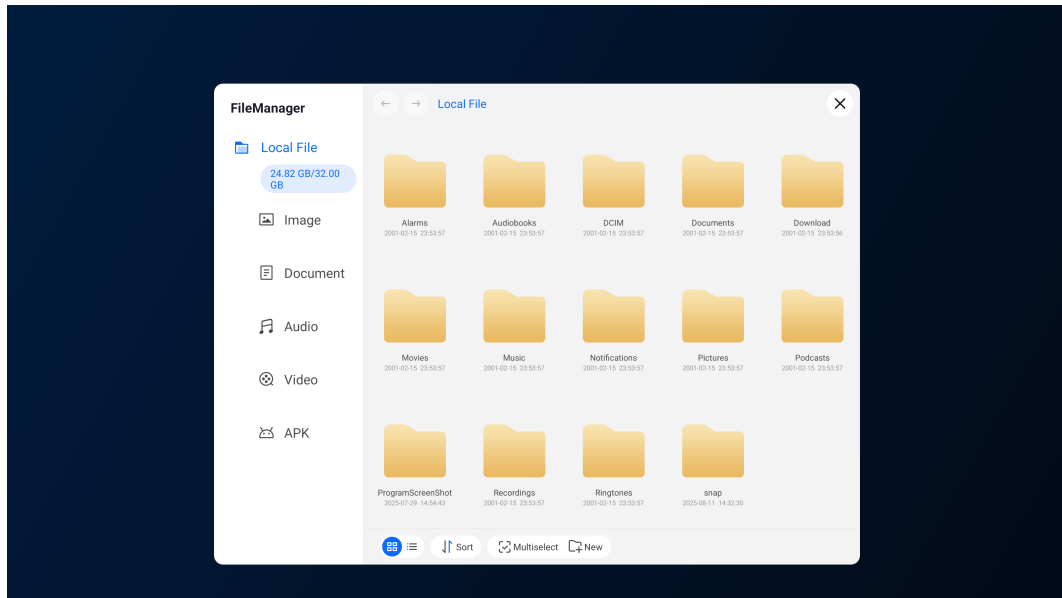


Table 4-8 Description of FileManager icons

Icon	Description
	View the previous or next page of local files.
	
	Switch between icon view and list view.
	
Sort	Arrange files by name, size, or time in ascending or descending order.
Multiselect	Select multiple or all files.
Select All	
New	Create a new folder.
Copy	After selecting files or folders, click Copy or Cut , and then click Paste to place them in the desired location.
Paste	
Cut	
Delete	Remove selected files or folders.
Rename	Rename a file or folder. File extensions cannot be changed.

Icon	Description
Send	Transfer files to another Bluetooth-enabled device via Bluetooth  Bluetooth must be turned on when you are using this feature.

4.8 App Installation

Prerequisites

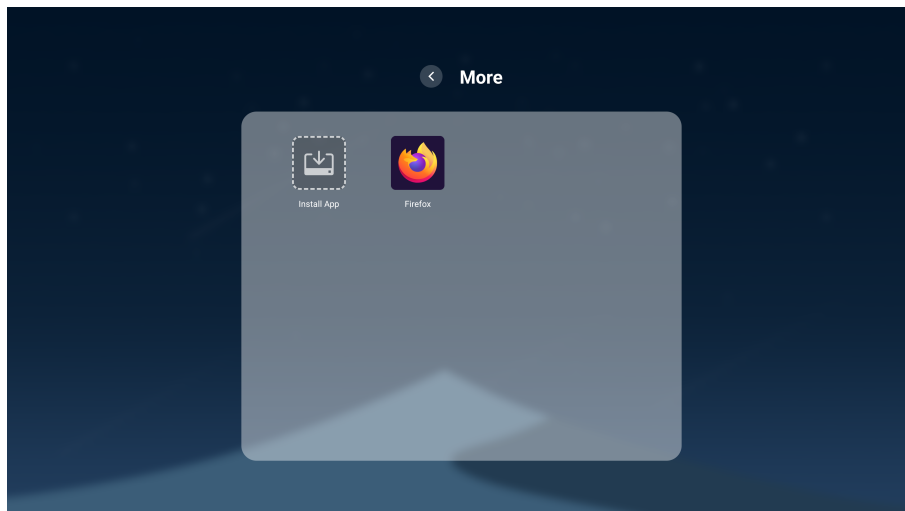
Insert a USB drive containing the installation package (.apk) into the Device.

Procedure

Step 1 On the homepage, click **More**.

Step 2 Click **Install App**.

Figure 4-31 Install app



Step 3 Select the installation package.

Step 4 Click **OK**.

Once the installation is complete, view and use the app in **More**.

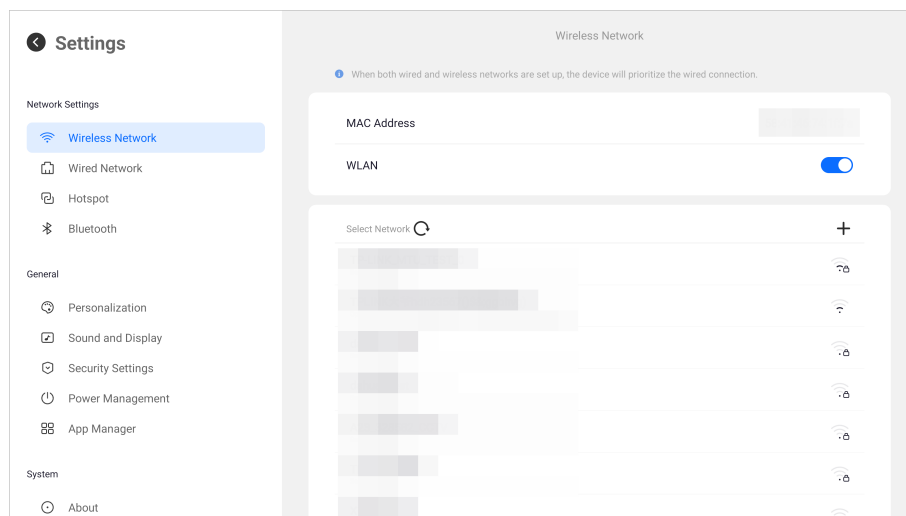
5 System Configuration

5.1 Network Settings

Wireless Network

On the homepage, select **Settings** > **Network Settings** > **Wireless Network**.

Figure 5-1 Configuring the wireless network



- Connect to an existing network: Click the network in the list, enter the password, and then connect.
- Add network manually: Click **+**, enter the network's SSID, select the encryption type, and then enter the password.



- When you select **Encryption Method** as **none**, no password is required.



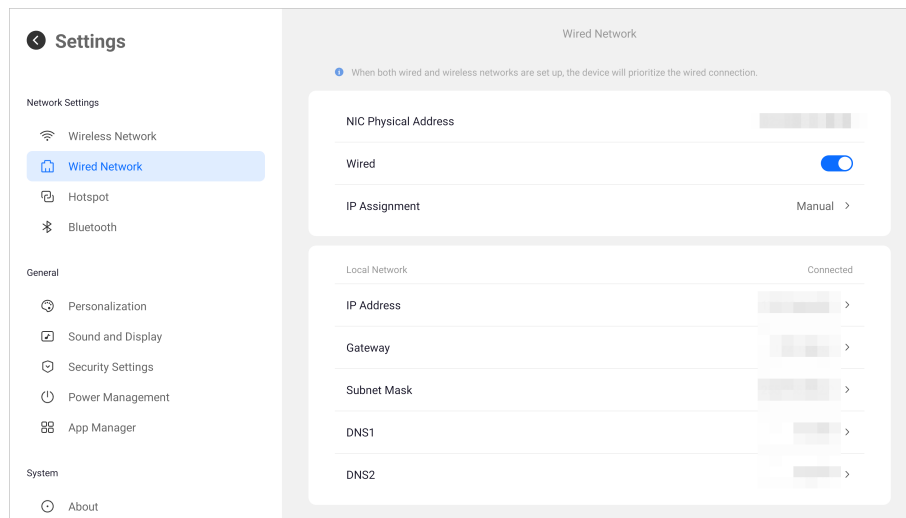
The insecure encryption method may leave the device vulnerable to attacks.

- When the static IP feature is enabled, the Device will connect to Wi-Fi using a static IP address. You must configure the IP address, subnet mask, gateway, and DNS addresses.

Wired Network

On the homepage, select **Settings** > **Network Settings** > **Wired Network**.

Figure 5-2 Configuring the wired network



Configure the IP assignment method. You can select **Auto** or **Manual**.

- **Auto**: The device automatically receives an IP address from the DHCP server.
- **Manual**: Enter the IP Address, the gateway, the subnet mask and the DNS of your network plan.

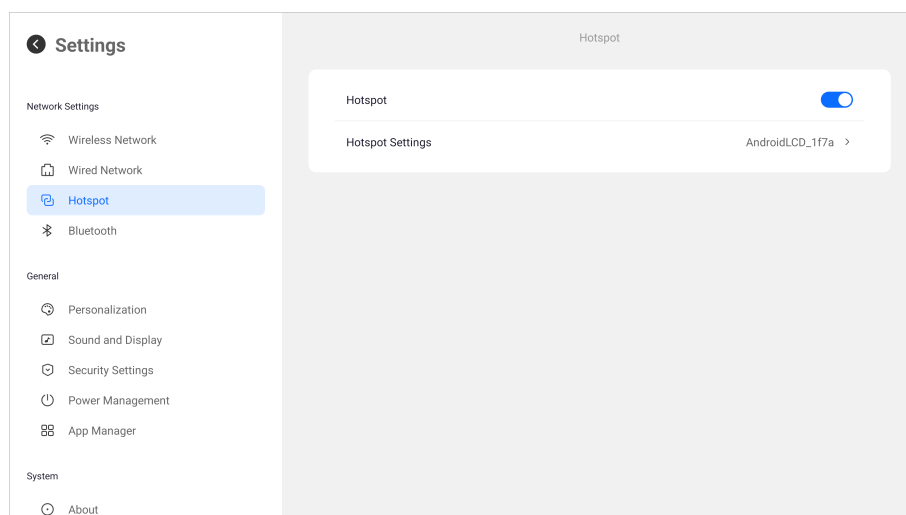
Hotspot

On the homepage, select **Settings** > **Network Settings** > **Hotspot**.

Enable **Hotspot**.

Click **Hotspot Settings** to configure the SSID, the encryption method, the password and the frequency band of your hotspot.

Figure 5-3 Configuring the hotspot



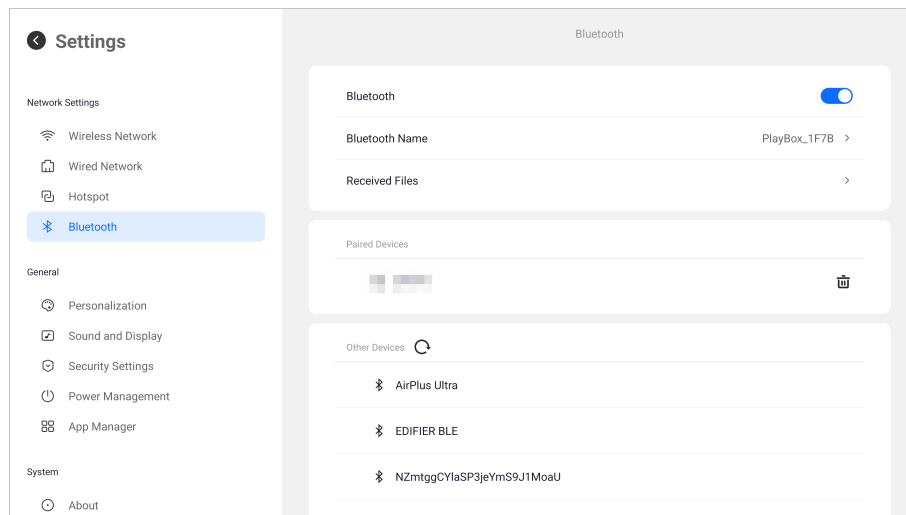
When **Hide SSID** is enabled, other devices will no longer detect the network; connections must be established by manually adding.

Bluetooth

On the homepage, select **Settings** > **Network Settings** > **Bluetooth**.

Enable **Bluetooth**. Click **Bluetooth Name** to modify the name of your Bluetooth.

Figure 5-4 Configuring the Bluetooth



Pair with other devices

1. Click a Bluetooth device in the list to pair.
2. Click **Confirm**; once pairing is complete, view the device under **Paired Devices**. Click  to remove the paired devices.

5.2 General Settings

Personalization

On the homepage, select **Settings** > **General** > **Personalization**.

Table 5-1 Description of personalization settings

Feature	Description
Wallpaper	Set the background image displayed on the home screen. • The system provides 8 wallpapers by default. • You can upload the desired wallpaper. The 16:9 ratio or the 9:16 ratio is recommended.
Startup Logo	Set the startup logo. Click Custom in any view to modify its corresponding logo image.

Sound and Display

On the homepage, select **Settings** > **General** > **Sound and Display**.

Table 5-2 Description of sound and display settings

Feature	Description
Volume settings	Adjust the Device's volume. - Default volume: Manually set the volume; except any volume plans, this level is used. - Volume Plan: When the feature is enabled, click  and set start/end times; and the volume during these periods can still be adjusted manually.  Up to 5 schedules are supported.
Screen rotation	Configure the screen orientation. The default option is Horizontal (0 °), and other options include: - Horizontal (0 °) - Vertical (90 °) - Horizontal (180 °) - Vertical (270 °)
Output resolution	Configure the output resolution. The default value is auto, and other options include: - auto 720P 60Hz 1080P 50Hz 1080P 60Hz 2160P 50Hz 2160P 60Hz  - The actual options depend on the connected display. - The Device only supports 16:9 or 9:16 aspect ratios; other ratios may cause image distortion or black bars.

Security Settings

On the homepage, select **Settings** > **General** > **Security Settings**.

Table 5-3 Description of security settings

Feature	Description
Screen lock time	Set the screen-lock time, with the options of 1 min , 3 min, 10 min, or never.  When the screen lock time is configured as never, the device can be operated without logging in. Please be aware of the security risks.
Password	To change the device password, click Password , enter the old password, set a new one, confirm it, and then click Confirm.

Feature	Description
Security question	Set or update security questions. For example, click Question 1 to select a question, click Answer, enter your answer, and then click Confirm. After completing all questions, click Confirm again.  Password recovery is only possible after security questions are configured.
Password validity period	Change the password validity period; the default option is Always Valid, with other options of 180 Days and 30 Days.  When the password is about to expire, you'll be prompted to change it at login.
Use password to verify installation	When the feature is enabled, a password is required to install any application.
Allowlist	Once the feature is enabled, only IP addresses in the allowlist can connect to the Device. - Click  to add an IP address. - Click  to remove an IP address.
Disable external storage	When the feature is enabled, the Device will not recognize external storage devices (e.g., USB drives, TF cards); USB peripherals like mice remain unaffected.
Device management app	Adjust advanced permissions for installed applications.

Power Management

On the homepage, select **Settings** > **General** > **Power Management**.



Plan priority: Custom (cross day) > custom (current day) > by week.

Table 5-4 Description of power management

Feature	Description
Auto turn on/off display	Configure weekly or custom plans. Custom plans include Custom (Current Day) and Custom (Cross Day) Click  to set the on/off times and the days when the plan applies.
Auto turn on/off power	
Auto restart	Create a restart plan by setting the restart time and the days it should run.
Restart	Click Restart ; after confirmation, the Device will restart immediately.

App Manager

On the homepage, select **Settings** > **General** > **App Manager**.

Table 5-5 Description of app manager

Feature	Description
Run at start up	Configure apps that run automatically at startup. By default, no app runs automatically at startup.
Desktop management	Configure the apps shown on the desktop—the desktop supports up to 8 apps.
Installed apps	View or uninstall installed applications.

5.3 System Settings

About

On the homepage, select **Settings** > **System** > **About**.

Click **Device Name** to modify the device name.

Date and Time

On the homepage, select **Settings** > **System** > **Date and Time**.

Table 5-6 Description of date and time

Feature	Description
Date	Set the date display of the Device.
Time	Set the time display of the Device.
Use 24-Hour Format	Enable it to display the time in 24-hour format.
Time Zone	Set the time zone of the Device.
IPC Time Sync	When the feature is enabled, the Device synchronizes time with the IPC at the specified interval. The default interval is 24 hours.
NTP Time Sync	After you enable the feature and configure an NTP server, the Device synchronizes time at the specified interval. The default interval is 1 minute.

Language

On the homepage, select **Settings** > **System** > **Language**, and then modify the device language; with 14 available languages including Simplified Chinese, English, Traditional Chinese, Italian, German, and French.

Maintenance and Update

On the homepage, select **Settings** > **System** > **Maintenance and Update**.

Table 5-7 Description of maintenance and update

Feature	Description
Restore factory defaults	Enter the password to restore the Device to factory defaults.  When you finish this operation, all the configuration of the device would be restored to the default. Be cautious with this operation.
System update	Update the system by selecting a package from the upgrade list.
SCM update	Update the microcontroller.
Documents	Scan the QR code to view product documents.

Upgrade methods



Please be advised that downgrading to a lower version will make the whiteboard vulnerable to security attacks.

- USB drive upgrade

1. Copy the update.zip package to the root directory of a USB drive.
2. Insert the USB drive into the USB port of the Device.



Use a USB drive formatted as FAT32; otherwise, the upgrade may fail.

3. When the Device detects the upgrade file, an upgrade prompt appears.
 4. Click **Confirm**. The system begins upgrading; and the Device will restart automatically when finished.
- Online upgrade: See the user manual of the media publishing platform.

Appendix 1 Remote Control

For Device of specified models, you can use remote control to operate them.



- The remote control supports limited operations: You can use the remote control to turn on or off the screen, turn on, turn off, or restart the box, adjust the volume and go back to the home page.
- Refer to the packing list to see whether the remote control comes with the box. If not, you need to purchase it separately.

Appendix Figure 1-1 Remote control appearance



Appendix Table 1-1 Buttons description

Operation Item	Buttons Needed
Power on/off the box	Press  . In the pop-up dialog box, select Power off . Press the button again to power on the box.
Screen on/off the box	Press  . In the pop-up dialog box, select Screen off . Press the button again to turn on the box screen.
Reboot	Press  . In the pop-up dialog box, select Reboot .
Adjust volume	• Volume up: Press , and then press the right arrow button. • Volume down: Press , and then press the left arrow button.

Operation Item	Buttons Needed
Log in	1. When you find the screen is locked, you can use your remote control to type the password. Press  on your remote control. The Login page is displayed. 2. Operate arrow keys, move pointer to password box, and then type the password. 3. Move pointer to Done on virtual keyboard. 4. Move pointer to OK, and then press  on your remote control to log in to the box.
Return to the previous page	Press  .
Return to the main menu	Press  .
Bring up the frequently used tool bar	Press  , and operate the left/right arrow keys to select a function you want.

Appendix 2 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 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:

Account Management

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.

2. Change passwords periodically

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

3. Allocate accounts and permissions appropriately

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

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.

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.

Service Configuration

1. Enable HTTPS

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

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.

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.

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.

Network Configuration

1. Enable Allowlist

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

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. 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.

Security Auditing

1. Check online users

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

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.

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.

Software Security

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.

2. **Update client software in time**

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

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