

Distributed UHD Codec (Seat Management System)

User's Manual



Foreword

This manual introduces the installation, configurations and operations of the Distributed UHD Codec (Seat Management System). Read carefully before using the platform, and keep the manual safe for future reference.

Model

DSMS0105UHI-4K; DSMS0105UHO-4K; DSMS0115EPI-4K

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
V1.0.0	First release.	February 2023

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 device, hazard prevention, and prevention of property damage. Read carefully before using the device, 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



WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- 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.
- To ensure heat dissipation, make sure the gap is wide enough between the device and the surrounding area.
- The rated current of the input box is 2 A and the rated power is 24 W.
The rated current of the output box is 5 A and the rated power is 50 W.

Operation Requirements



- Make sure that the power supply is correct before use.
- Do not unplug the power cord on the side of the device while 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 it.
- Do not disassemble the device.
- Operating temperature: –10 °C to +45 °C (14 °F to 113 °F).

Maintenance Requirements



Power off the device before maintenance.

Table of Contents

Foreword	I
Important Safeguards and Warnings.....	III
1 Overview	1
1.1 Introduction	1
1.2 Features.....	1
2 Installation	2
2.1 Unpacking the Box.....	2
2.2 Structure	2
2.2.1 Input Node	2
2.2.1.1 DSMS0105UHI-4K	2
2.2.1.2 DSMS0115EPI-4K	3
2.2.2 Output Node.....	5
2.3 Installation and Connection.....	6
2.3.1 Input Node	6
2.3.1.1 DSMS0105UHI-4K	6
2.3.1.2 DSMS0115EPI-4K	7
2.3.2 Output Node.....	8
2.4 Powering On/Off	9
2.4.1 Powering On.....	9
2.4.2 Powering Off	9
3 System Configuration	10
3.1 Login	10
3.2 Logout	10
3.3 Viewing Basic Information	10
3.4 Personalized Settings.....	10
3.4.1 Basic Configuration	10
3.4.2 Hot Key Configuration	11
3.5 Device Management	12
3.5.1 Adding Input Devices	12
3.5.2 Adding Output Devices	15
3.5.3 Signal Group.....	16
3.6 Seat Configuration.....	17
3.7 Matrix Configuration	19
3.8 User Management (Admin Account).....	21
3.8.1 User Group Management	21

3.8.2 Account Management	22
3.8.3 Configuring Password Update Cycle	23
3.9 Changing Password (Non-admin Account).....	24
3.10 Legal Information	24
4 Application	25
4.1 Multi-window Display	25
4.2 Audio Input and Output	26
4.3 Audio Output	26
4.4 Get	26
4.4.1 Getting Devices	26
4.4.2 Display Mode	27
4.4.3 Data Transmission through USB Flash Drive	27
4.5 Push	28
4.5.1 Pushing Devices	28
4.5.2 Push Device Category	29
Appendix 1 Cybersecurity Recommendations	30

1 Overview

1.1 Introduction

The Distributed Seat Management System transmits video signals and keyboard and mouse control messages through IP network to separate keyboard, mouse, and screen control from the computer host, switch between multiple computers, and push videos to other screens. It realizes human-machine separation and one person controlling multiple computers. Based on distributed architecture design, the system features high reliability and fault tolerance. Through H.264/H.265 high compression ratio encoding, videos consume small bandwidth, and the device enjoys flexible deployment. Ultra-low delay provides users with smooth experience. It is applicable to various kinds of command centers and monitoring centers.

1.2 Features

Structural Features

- Distributed deployment and unified management.
- Compact styling and easy to deploy. Digital transmission, free of cable interference.
- Flexible and stable system restructuring allows you to easily deploy input and output nodes.

Network Functions

- Supports TCP/IP and network protocols such as RTP/RTSP/RTCP/TCP/UDP/DHCP.
- Supports acquiring and configuring parameters in batches and remotely exporting and importing parameters.
- Supports acquiring system logs in batches.
- Supports restarting the device remotely, upgrading in batches, and restoring to factory default.
- Supports managing user group permissions.
- Supports PoE power supply.

Distinguished Features

- Displays with network.
- Enjoys flexible topology.
- Enjoys distributed system and independent maintenance.
- Supports getting and pushing signals and collaborating among multiple screens.

2 Installation

2.1 Unpacking the Box

When you receive the device, check whether there is any visible damage. The protective materials used for the package of the device can resist most accidental collisions during transportation. The label at the bottom of the box is very important, since there is serial number and other information. Usually we need you to present the serial number when we provide after-sales service. Do not tear or discard it.

2.2 Structure

2.2.1 Input Node

2.2.1.1 DSMS0105UHI-4K

Figure 2-1 Front panel introduction

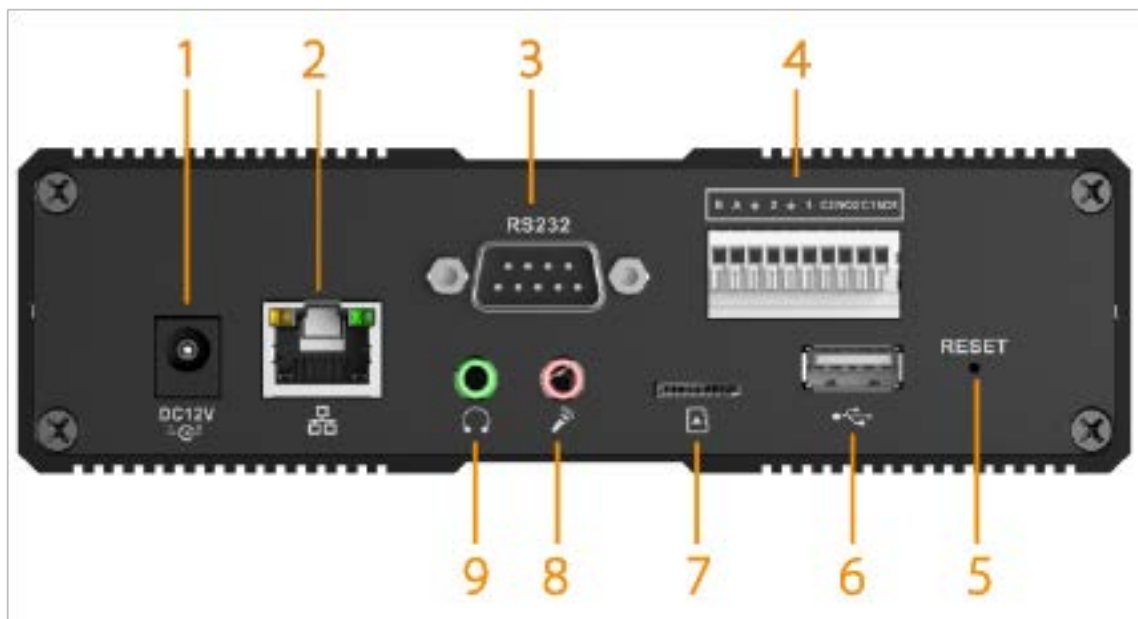


Table 2-1 Front panel description

No.	Description	No.	Description	No.	Description
1	Power input port	4	RS-485 port, alarm input and alarm output	7	SD card slot (reserved)
2	RJ-45 network port	5	Reset button Press and hold it for 3-5 seconds, and the system will restore to factory defaults.	8	Audio input port

No.	Description	No.	Description	No.	Description
3	RS-232 debugging serial port	6	USB port (reserved)	9	Audio output port (reserved)

Figure 2-2 Rear panel introduction

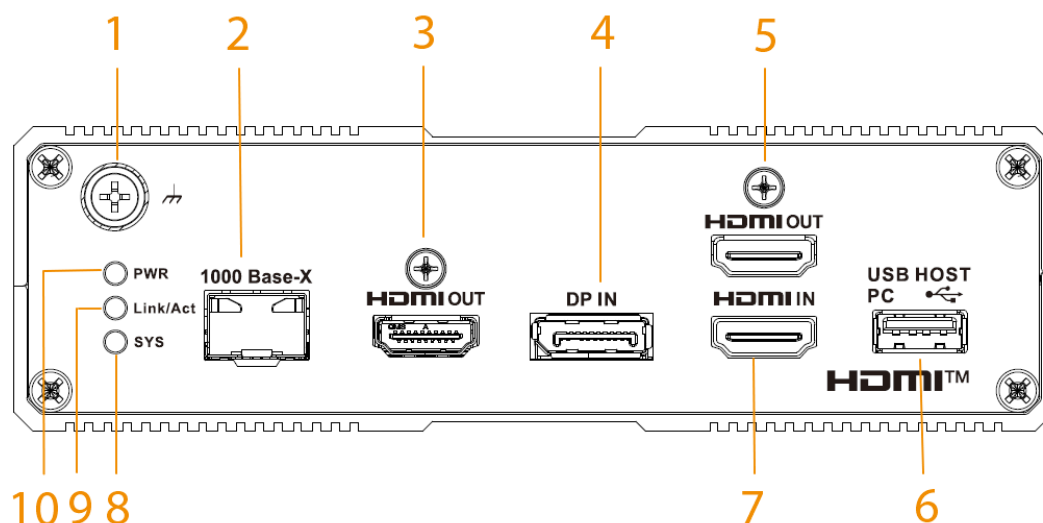


Table 2-2 Rear panel description

No.	Description	No.	Description	No.	Description
1	Ground screw	5	HDMI video loop output (HDMI IN signal)	9	Optical port indicator. Flashes quickly when data is transmitting.
2	Gigabit port. Used for inserting an optical module.	6	USB 3.0 port. Used for connecting a computer.	10	Power indicator. Red light is on when the power is on.
3	HDMI signal output (for debugging)	7	HDMI video input port	—	—
4	DP signal input	8	Activity indicator. It is on when the system is running.	—	—

2.2.1.2 DSMS0115EPI-4K

Front Panel Introduction

Figure 2-3 Front panel

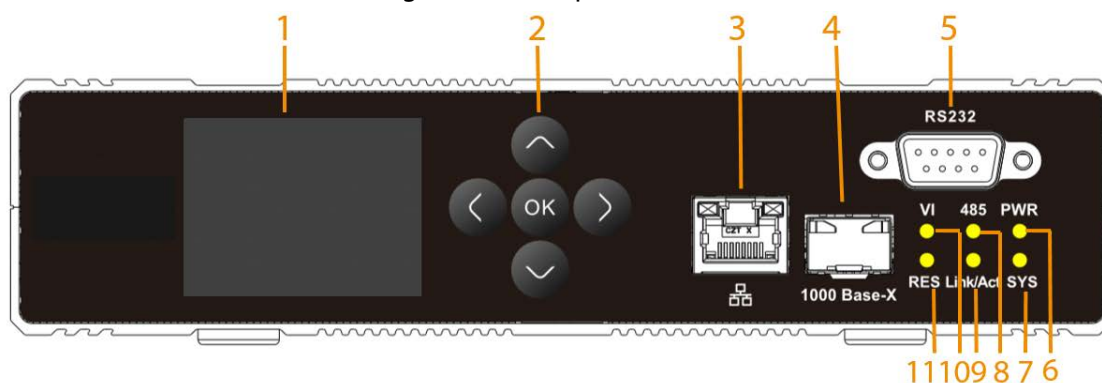


Table 2-3 Front panel description

No.	Description	No.	Description	No.	Description
1	LCD. Displays the device name and its IP.	5	RS-232 debugging serial port	9	Optical port indicator. Flashes quickly when data is transmitting.
2	LCD operation buttons (reserved)	6	Power indicator. It is solid red when the power is on.	10	VI indicator. By default, it is off after power-on. After signal is inserted and lock is identified, the indicator is solid green.
3	RJ-45 network port.	7	Activity indicator. It is on when the system is running.	11	Reserved
4	Gigabit port. Used for inserting an optical module.	8	485 communication indicator. It is off by default after power-on. When 485 signal is transmitting, it flashes green.	—	—

Rear Panel Introduction

Figure 2-4 Rear panel

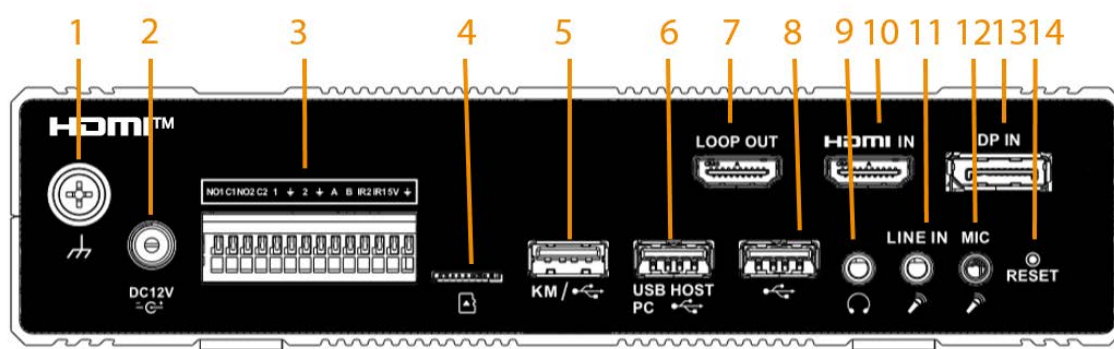


Table 2-4 Rear panel description

No.	Description	No.	Description	No.	Description
1	Ground screw	6	USB 3.0 port. Connects a computer to realize USB pass-through.	11	Audio in. Inputs audio from a computer or other devices.
2	Power input port	7	Loop output port	12	Mic audio in
3	RS-485 port for alarm input and alarm output.	8	USB 3.0 port. Connects a USB flash drive for debugging.	13	Inputs DP signals.
4	SD card slot (reserved)	9	Audio output	14	Reset button. Press and hold it for 3–5 seconds, and the system will restore to factory defaults.

No.	Description	No.	Description	No.	Description
5	USB port. Connects to a computer to transmit mouse and keyboard signaling.	10	HDMI video input port	—	—

2.2.2 Output Node

DSMS0105UHO-4K

Figure 2-5 Front panel

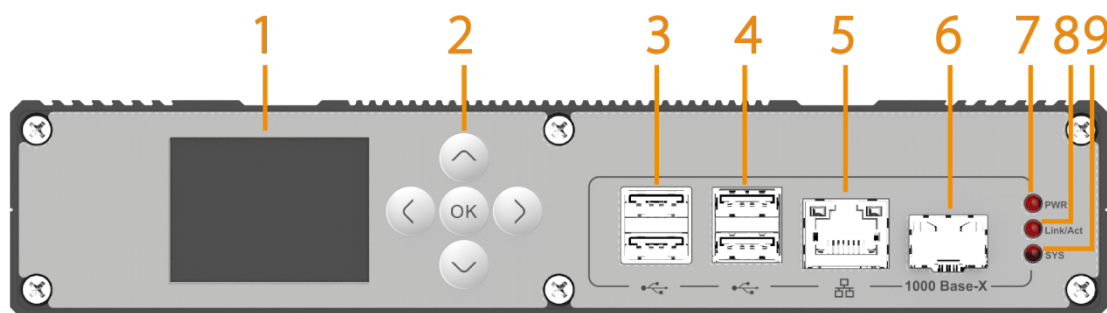


Table 2-5 Front panel description

No.	Description	No.	Description	No.	Description
1	LCD. Displays the device name and its IP.	4	2 USB3.0 ports. Connects a mouse, keyboard, or USB flash drive.	7	Power indicator. It is solid red when the power is on.
2	LCD operation buttons (reserved)	5	RJ-45 network port	8	Optical port indicator. Flashes quickly when data is transmitting.
3	2 USB3.0 ports. Used for connecting a mouse, keyboard, or USB flash drive.	6	Gigabit port. Used for inserting an optical module.	9	Activity indicator. It is on when the system is running.

Figure 2-6 Rear panel

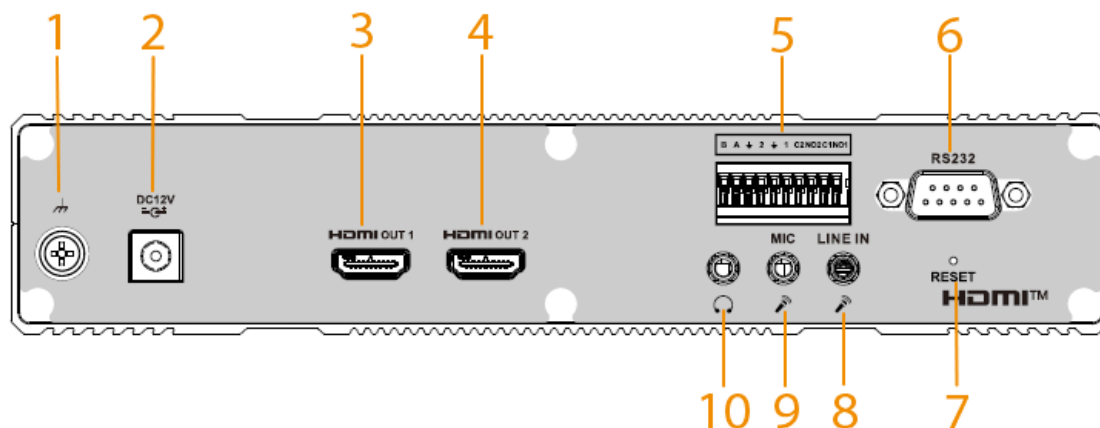


Table 2-6 Rear panel description

No.	Description	No.	Description	No.	Description
1	Ground screw	5	RS-485 port for alarm input and alarm output.	9	Mic audio in
2	Power input port	6	RS-232 debugging serial port	10	Audio output port
3	HDMI output port 1	7	Reset button. Press and hold it for 3–5 seconds, and the system will restore to factory defaults.	—	—
4	HDMI output port 2 (reserved)	8	Audio in. Inputs audio from a computer or other devices.	—	—

2.3 Installation and Connection

2.3.1 Input Node

2.3.1.1 DSMS0105UHI-4K

Figure 2-7 Connection of the front panel

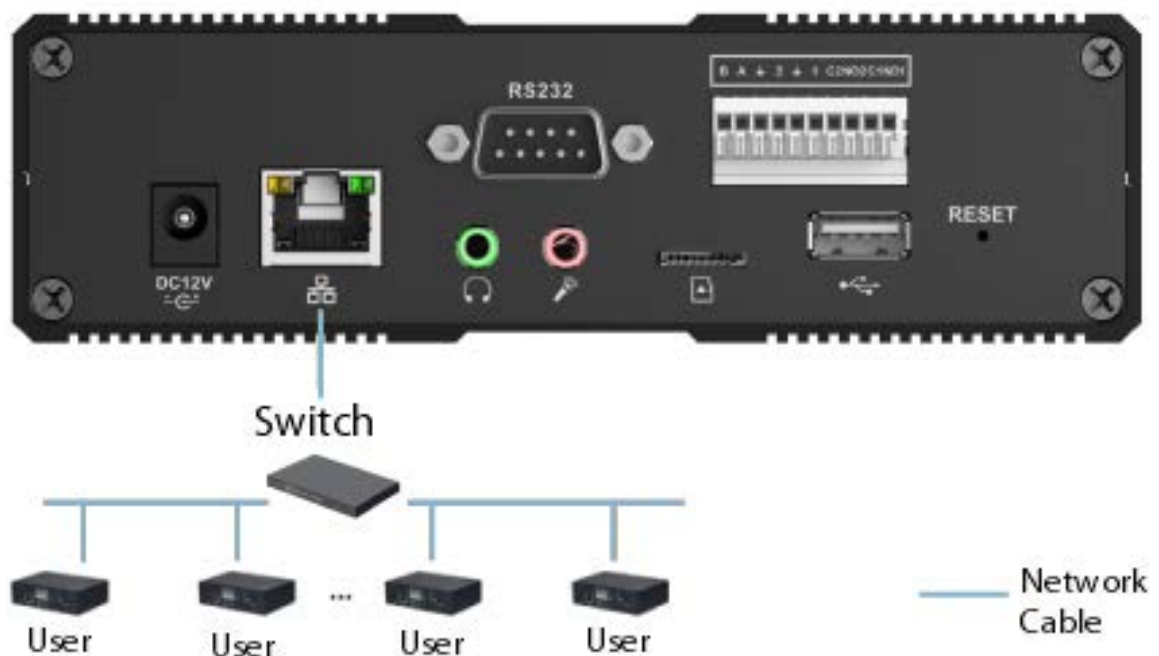
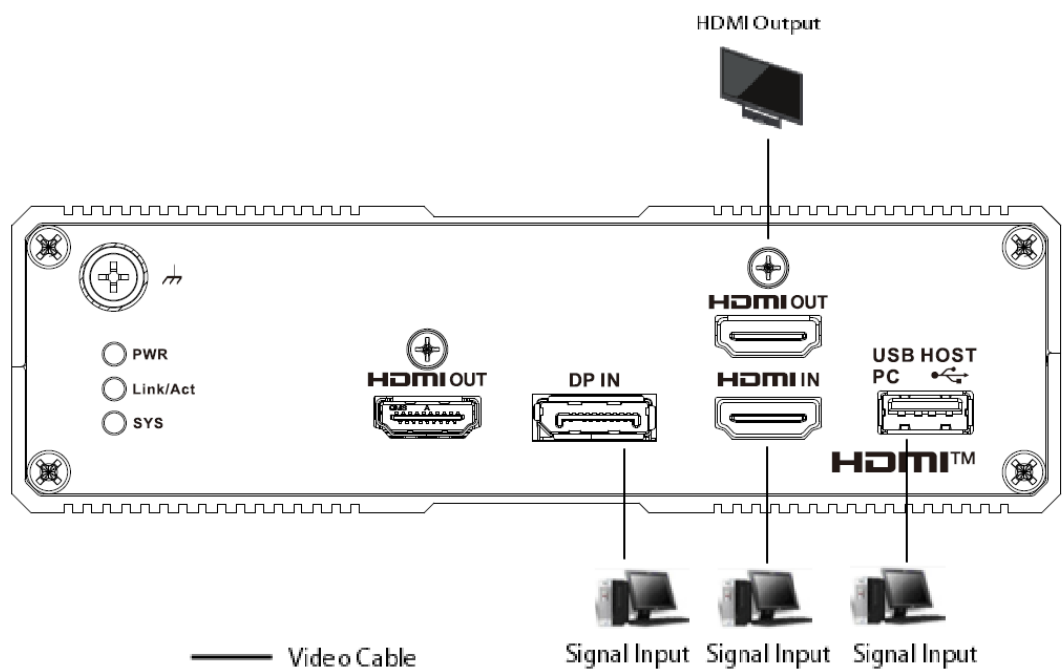


Figure 2-8 Connection of the rear panel



2.3.1.2 DSMS0115EPI-4K

Figure 2-9 Connection of the front panel

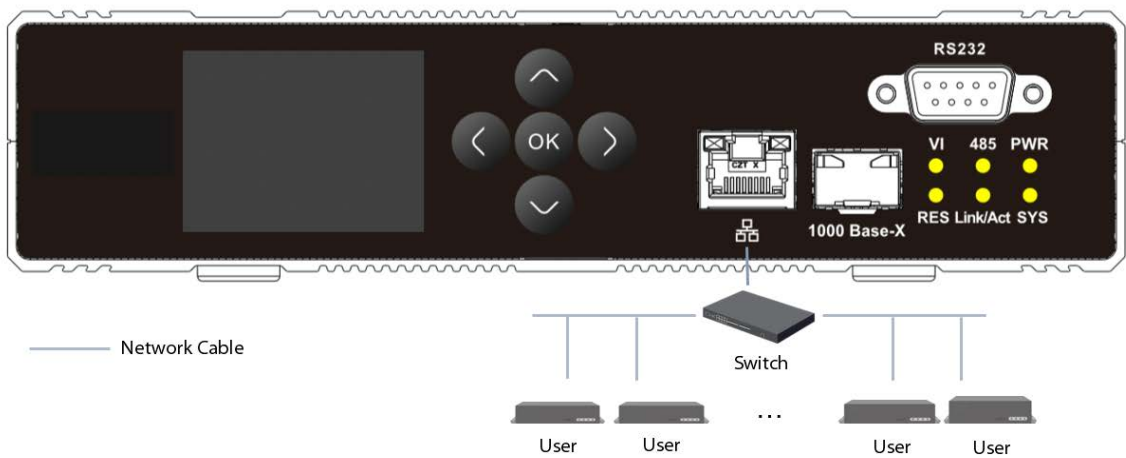
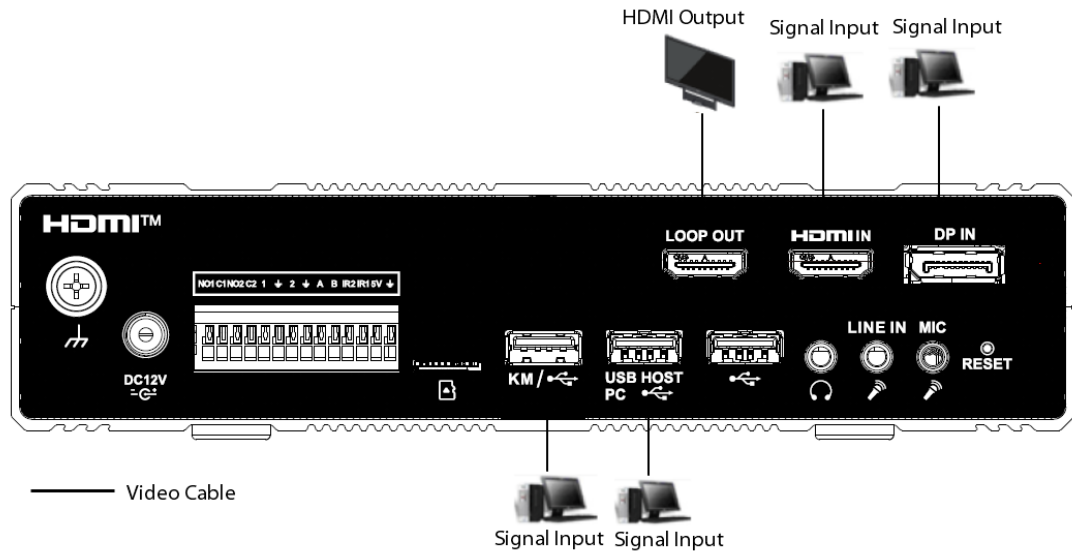


Figure 2-10 Connection of the rear panel



2.3.2 Output Node

DSMS0105UHO-4K

Figure 2-11 Connection of the front panel

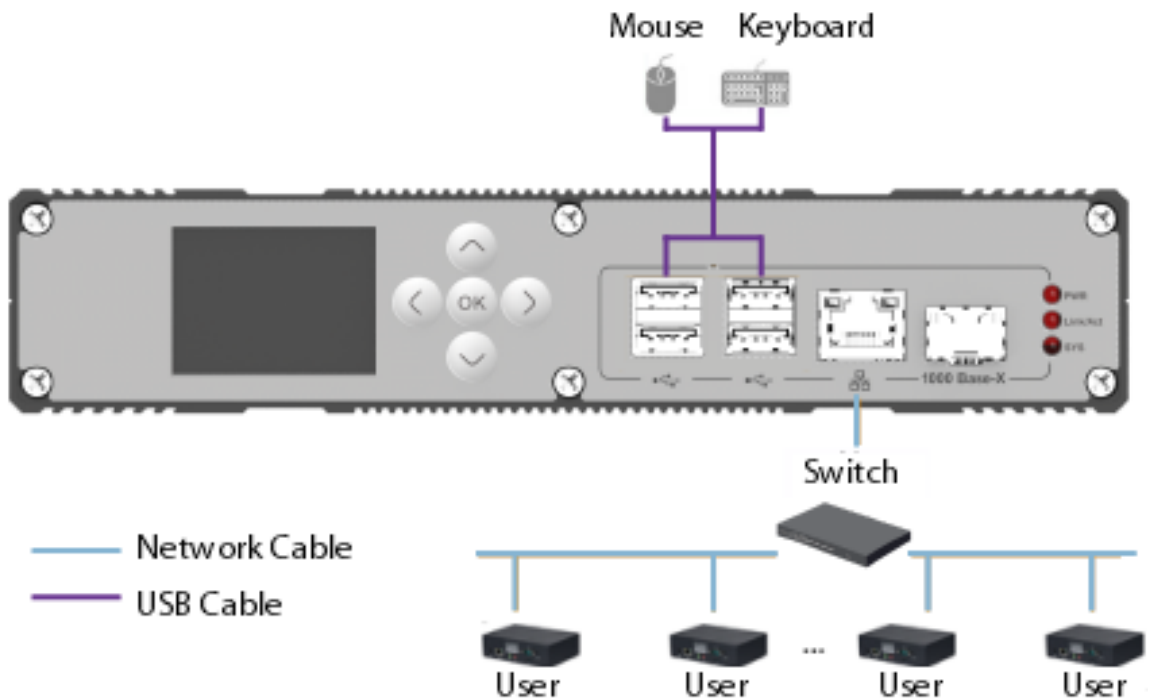
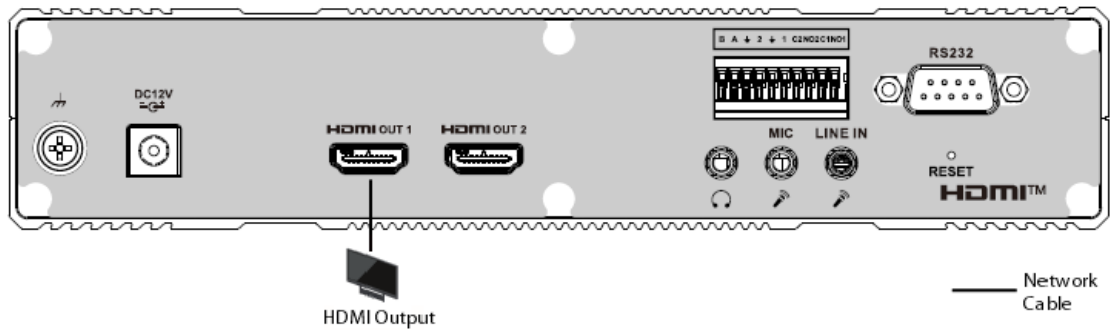


Figure 2-12 Connection of the rear panel



2.4 Powering On/Off

2.4.1 Powering On

Plug in the power cable, and the power indicator is on, which indicates that the device is successfully started.



Make sure that the input voltage of power supply complies with the device power requirements.

2.4.2 Powering Off

Cut off the power cable to shut down the device.

3 System Configuration



Only output nodes support local operation of the system. For input nodes, you need to log in to its webpage.

3.1 Login

Procedure

- Step 1 Log in to the Distributed Seat Management Manage System.
Step 2 Enter the username and password.



- Tick **Remember password**, and your password will be automatically filled in for future login.
- The account will be locked for 30 minutes if wrong password is entered for 5 times within 30 minutes.

- Step 3 Click **Log in**.

3.2 Logout

Procedure

- Step 1 Click the account name at the upper-left corner of the page.
Step 2 Click **Log out**.

3.3 Viewing Basic Information

Procedure

- Step 1 Log in to the Distributed Seat Management Manage System.
Step 2 Click  at the upper-right corner, and then click **Basic Info**. You can view network configuration, network status, and get devices.
Step 3 (Optional) Click  to leave the page.

3.4 Personalized Settings

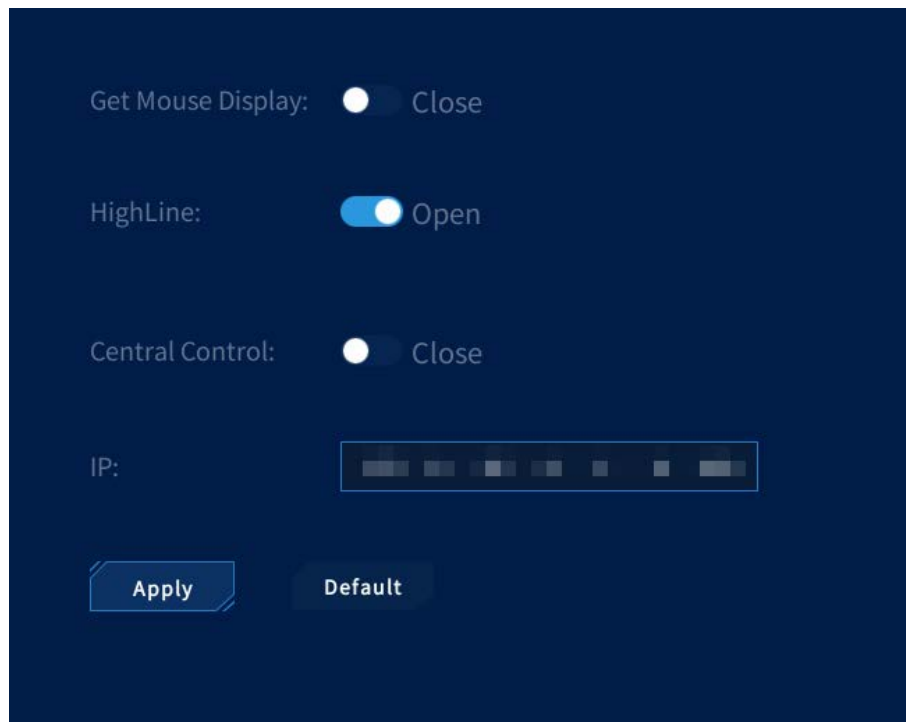
3.4.1 Basic Configuration

Procedure

- Step 1 Log in to the Distributed Seat Management Manage System.

Step 2 Click  and then select **Personal Settings > Basic Config.**

Figure 3-1 Basic configuration



Step 3 Configure mouse display.

- If it is enabled, the cursor of the computer where the system is deployed will be displayed. If the device that you get is also a computer, there will be 2 cursors.
- If it is disabled, the cursor of the computer where the system is deployed will not be displayed. If the device you get is a camera or other network devices, no cursor will be displayed.

Step 4 Configure whether to highlight the current window.

- Enable it, and the rim of the window where the mouse is on will be highlighted in red.
- If it is disabled, the rim of the window where the mouse is on will not be highlighted. The rim of the current screen is still highlighted in red.

Step 5 Configure central control.

- Enable it, and then enter the IP address of the central control system, and you can shut down computers from the **Get** page. For details, see "4.4.1 Getting Devices".
- If it is disabled, you cannot shut down or start computers through the distributed seat management system.



The center control function is disabled by default.

Step 6 Click **Apply**, and the configuration will take effect.

Click **Default** to restore the parameters to default.

3.4.2 Hot Key Configuration

Configure hot keys to quickly get devices.

Procedure

Step 1 Log in to the Distributed Seat Management Manage System.

- Step 2 Click  and then select **Personal Settings > Hotkey Config**.
- Step 3 Configure hot keys and the devices to take over, and then click **OK**.

3.5 Device Management

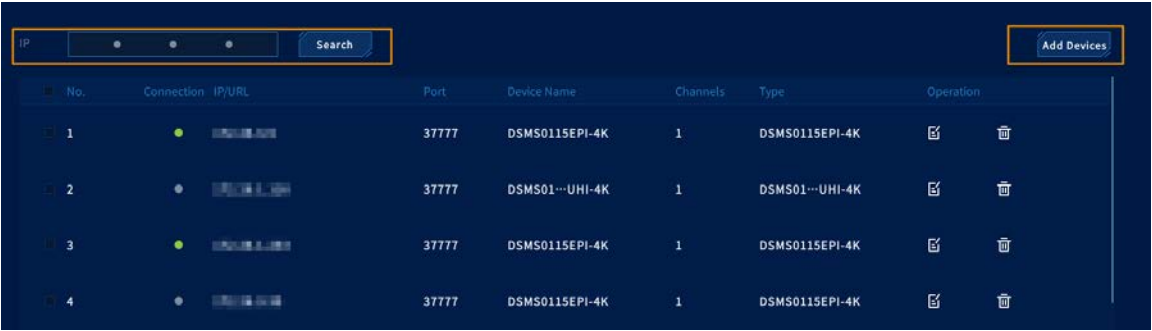
You can add input and output devices. Devices on the same network segment with the device that the system connects to will be automatically added.

3.5.1 Adding Input Devices

Procedure

- Step 1 Log in to the Distributed Seat Management Manage System.
- Step 2 Click  and then select **Device Management > Input Devices**.
- Step 3 (Optional) Enter the device IP address in the bar at the upper-left corner, and then click **Search**.
- Step 4 Click **Add Devices**.

Figure 3-2 Add input devices



No.	Connection	IP/URL	Port	Device Name	Channels	Type	Operation
1		192.168.1.100	37777	DSMS0115EPI-4K	1	DSMS0115EPI-4K	
2		192.168.1.101	37777	DSMS01---UHI-4K	1	DSMS01---UHI-4K	
3		192.168.1.102	37777	DSMS0115EPI-4K	1	DSMS0115EPI-4K	
4		192.168.1.103	37777	DSMS0115EPI-4K	1	DSMS0115EPI-4K	

- Step 5 Enter device parameters.
Supported protocols include **Private**, **Onvif**, and **General**. Select the protocol that the device uses. Parameters vary depending on the protocol.

Figure 3-3 Device parameters (Private protocol)

The screenshot shows a dark-themed 'Add Devices' dialog box with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Devices name:** A text input field.
- Protocol:** A dropdown menu currently showing 'Private'.
- IP:** A text input field with three dots (.) indicating an IP address format.
- Protocol Type:** A text input field showing 'TCP'.
- Port:** A text input field showing '37777'.
- User name:** A text input field.
- Password:** A text input field.
- Channel No.:** A text input field showing '1'.

At the bottom right, there are two buttons: 'Cancel' and 'OK'.

Table 3-1 Device parameter description (Private protocol)

Parameter	Description
Device Name	Enter a device name to differentiate it from others.
Protocol	Select Private .
IP	Enter the IP address of the device to be added.
Protocol type	TCP (Transmission Control Protocol) by default and cannot be changed.
Port	Transmission control protocol port. It is 37777 by default and can be changed.
User name	Username and password used to log in to the device.
Password	
Channel No.	Total number of channels of the device.

Figure 3-4 Device parameters (Onvif protocol)

The screenshot shows a dialog box titled "Add Devices" with a close button (X) in the top right corner. The dialog contains the following fields and values:

- Devices name: [Empty text box]
- Protocol: [Dropdown menu showing "Onvif"]
- IP: [Empty text box with three dots indicating a dotted IP address]
- RTSP Port: [554]
- HTTP Port: [80]
- User name: [Empty text box]
- Password: [Empty text box]
- Channel No.: [1]

At the bottom right of the dialog are two buttons: "Cancel" and "OK".

Table 3-2 Device parameter description (Onvif protocol)

Parameter	Description
Device Name	Enter a device name to differentiate it from others.
Protocol	Select Onvif .
IP	Enter the IP address of the device to be added.
RTSP Port	The RTSP command tells the server which port the client is using to receive media data. It is 554 by default, and can be changed.
HTTP Port	Enter the actual port the device is using. It is 80 by default.
Username	Username and password used to log in to the device.
Password	
Channel No.	Total number of channels of the device.

Figure 3-5 Device parameters (General protocol)

Table 3-3 Device parameter description (General protocol)

Parameter	Description
Device Name	Enter a device name to differentiate it from others.
Protocol	Select General .
URL	Enter a URL for acquiring the device stream.
Username	Username and password used to log in to the device.
Password	

Step 6 Click **OK**.

The imported device is displayed on the device list.

- Click  to edit device information.
- Click  to delete the device.

3.5.2 Adding Output Devices

Procedure

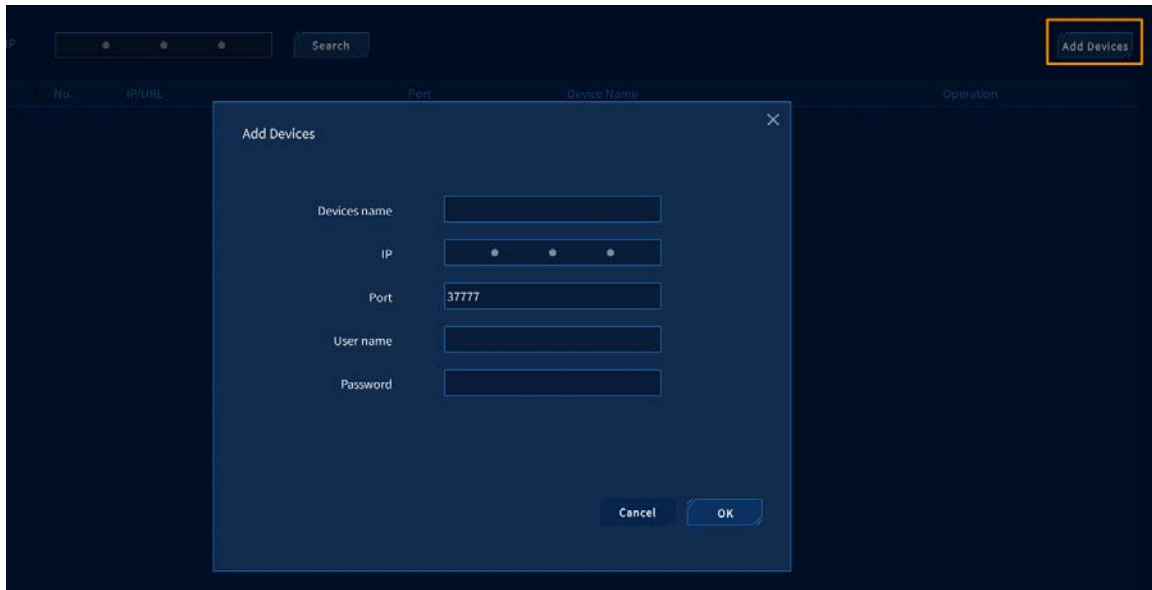
Step 1 Log in to the Distributed Seat Management Manage System.

Step 2 Click  and then select **Device Management > Output Devices**.

Step 3 (Optional) Enter the device IP address in the bar at the upper-left corner, and then click **Search**.

Step 4 Click **Add Devices**.

Figure 3-6 Add output devices



Step 5 Enter device parameters.

Table 3-4 Device parameter description

Parameter	Description
Device Name	Enter a device name to differentiate it from others.
IP	Enter the IP address of the device to be added.
Port	Configure the port number of device to be added. It is 37777 by default.
Username	Username and password used to log in to the device.
Password	

Step 6 Click **OK**.

The added device is displayed in the device list.

- Click  to edit device information.
- Click  to delete the device.

3.5.3 Signal Group

Prerequisites

Group signal sources so that you can quickly find the signal source that you need on the **Get** page.

Procedure

Step 1 Log in to the Distributed Seat Management Manage System.

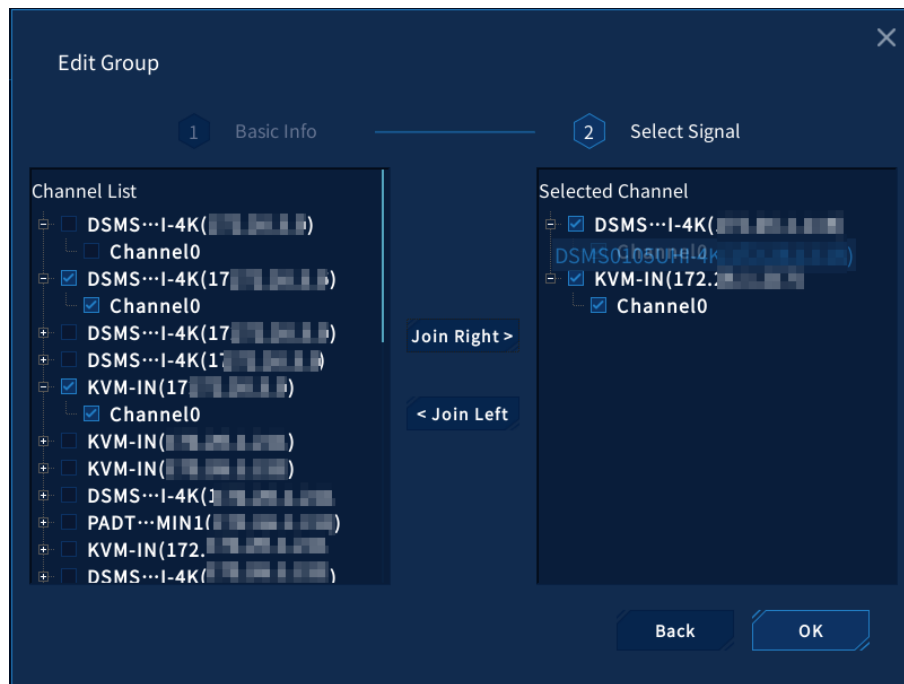
Step 2 Click  and then select **Signal Group**.

Step 3 Click **Add Groups** at the upper-right corner.

Step 4 Enter a group name, and then click **Next**.

Step 5 Select signal sources from the channel list on the left, click **Join Right**, and then click **OK**. You can then select the added groups from the drop-down box at the upper-right corner on the get page.

Figure 3-7 Select signal sources



3.6 Seat Configuration

The flexible seat mechanism assigns different operation permissions to different users. Within the permissions, you can log in to operate the host computer for signal call, command and dispatch.

Procedure

- Step 1 Log in to the Distributed Seat Management Manage System.
- Step 2 Click  and then select **Seat Management**.
- Step 3 Click **Add Seats** at the upper-right corner.
- Step 4 Enter a seat name, set the number of rows and columns, and then click **Next**.

Figure 3-8 Seat matrix splitting

Add Seats

1 Seat Splitting — 2 Bind Seats — 3 Set Main Screen

Seat Name

Row

Column

Cancel Next

Step 5 Drag a device from the left list to a matrix block on the right to bind it. Click **Next**.



- Each seat matrix can only bind one output device. If you bind a new input source, it will overwrite the previous one.
- Click  to delete the bound input source.

Figure 3-9 Bind seats

Add Seats

✓ Seat Splitting — 2 Bind Seats — 3 Set Main Screen

Drag the left device to the corresponding matrix block on the right to bind.

DSMS...O-4K
DSMS...O-4K
DSMS...O-4K
DSMS...O-4K
DSMS...O-4K
DSMS...O-4K
DSMS...O-4K
DSMS...O-4K
DSMS...O-4K

test

DSM...4K(172...108) DSM...4K(172...108)

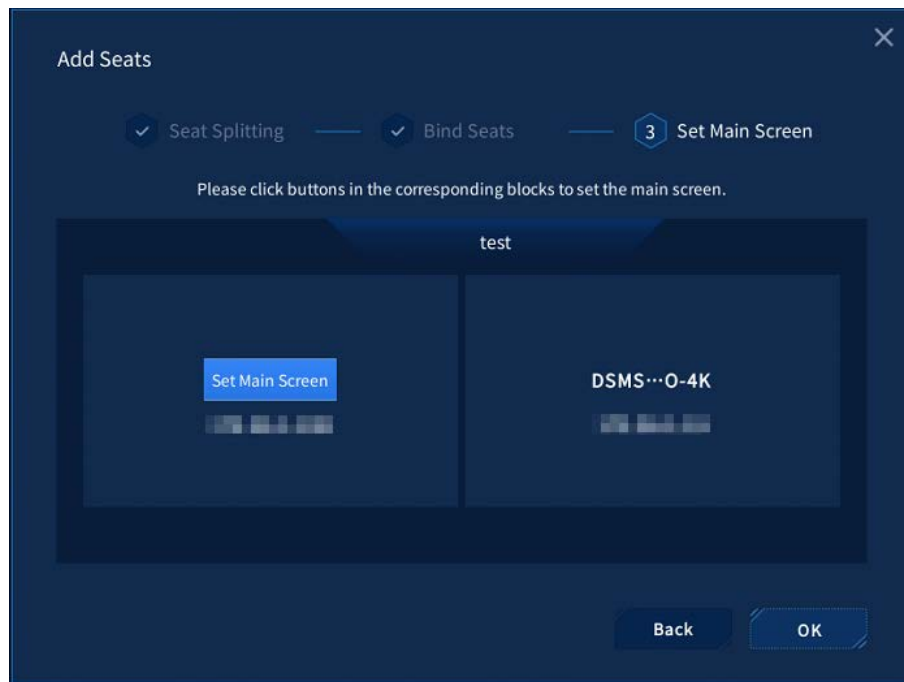
Back Next

Step 6 Move your mouse to the device name, and then click **Set Main Source**.



Your mouse and keyboard must be connected to the node of the main screen.

Figure 3-10 Set the main screen



- Step 7 Click **OK**.
The new seat will be displayed in the list.
- Step 8 (Optional) Click  to exit the page.

3.7 Matrix Configuration

When the source signal screen is too large to be collected by one box, you can group multiple input devices to collect the same signal source.

Procedure

- Step 1 Log in to the Distributed Seat Management Manage System.
- Step 2 Click , and then select **Matrix Config**.
- Step 3 Click **Add Matrix**.
- Step 4 Enter a matrix name, set the number of rows and columns, and then click **Next**.
- Step 5 Bind the input source. Drag an input source from left to the box on the right to bind it. Configure whether to get by one click and the getting mode. Click **Next**.



- Each matrix can only bind one input source. If you bind a new input source, it will overwrite the previous one.
- Click  to delete the bound input source.

Figure 3-11 Bind input source

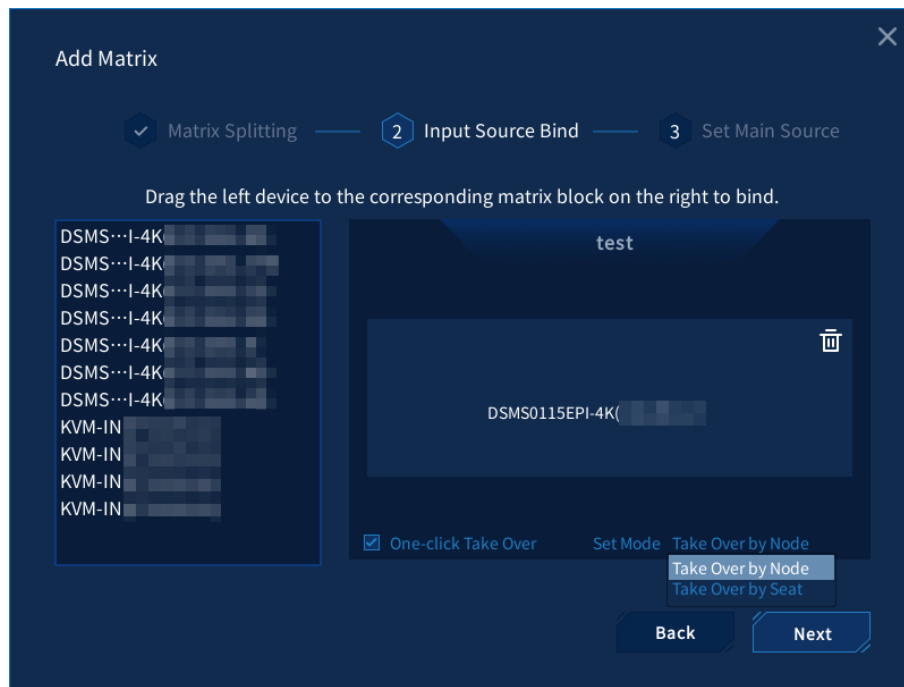


Table 3-5 Description of input source binding parameters

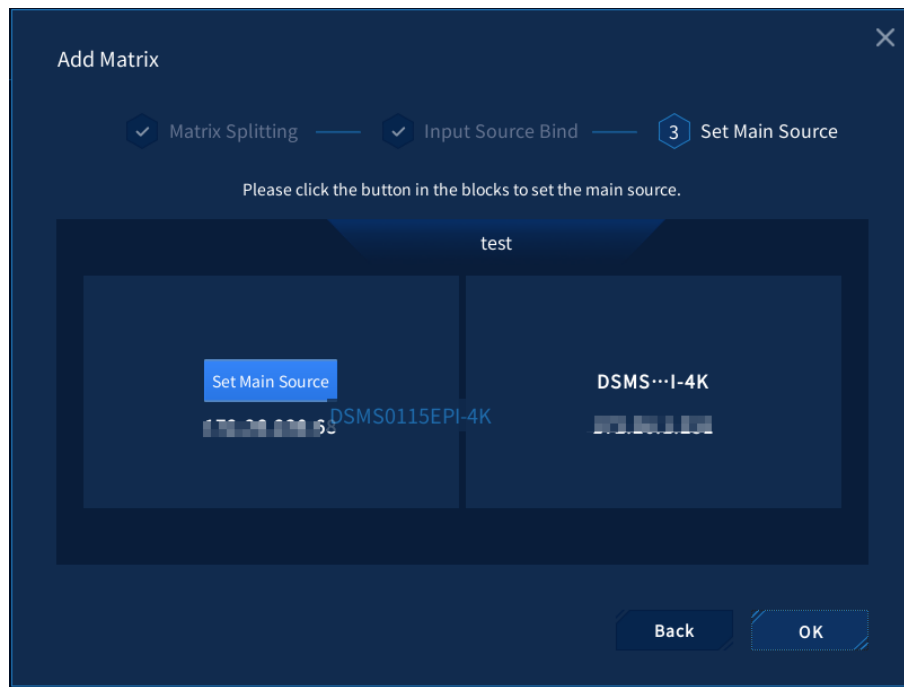
Parameter	Description
SetOneKeyGet	Displays the entire screen of the input matrix and keep its split mode.
Set Mode	By default, the system gets sources by node. - Get by node: Automatically opens windows and gets sources on the current output node based on the layout of the input matrix. - Get by seat: The sources are equally distributed to each output node of the current seat based on the input matrix layout, with the extra sources placed on the first row/column.

Step 6 Hover over your mouse to the device name, and then click **Set Main Source**.



A USB flash drive is needed to connect the main source and the computer.

Figure 3-12 Set the main source



- Step 7** Click **OK**.
The new input matrix will be displayed in the matrix list.
- Step 8** (Optional) Click  to leave the page.

3.8 User Management (Admin Account)

3.8.1 User Group Management

You can manage user groups, set user permissions, and view get-push details.

Procedure

- Step 1** Log in to the Distributed Seat Management Manage System.
- Step 2** Click  and then select **User Management > Uses Group**.
- Step 3** Click **Add Group**.

Figure 3-13 User groups

No.	Group Name	Operation
1	admin	
2	test	  
3	test2	  

- Step 4** Set a user group name, and then click **Next**.
- Step 5** Set the getting permissions and devices to push to.
- 1) Click the **Get Permission** tab.
 - 2) Select the devices to get.



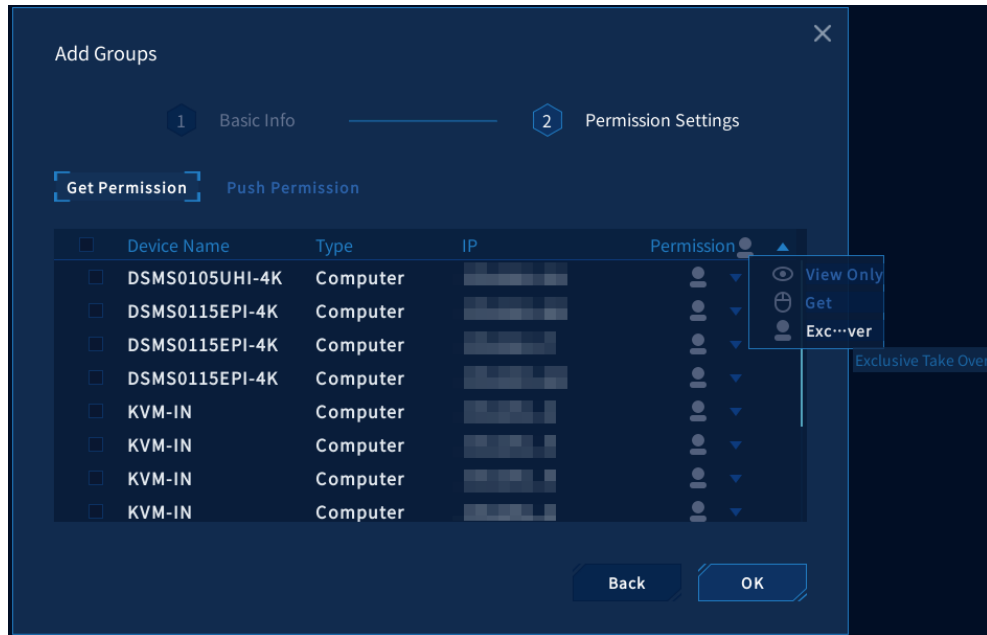
Permissions set for unselected devices will not take effect.

3) Set push permissions.

On the **Permission** column, click the triangle after .

- : Group members can only view but not operate the device.
- : Group members can control the device by mouse and keyboard.
- : Group members have exclusive permissions to control the device.

Figure 3-14 Set take over permissions



4) Click **Push**, and then select the devices that you push signals to.



Unselected devices cannot be pushed to.

Step 6 Click **OK**, and the new user group will be displayed in the list.

Step 7 (Optional) Click  to exit the page.

3.8.2 Account Management

Procedure

Step 1 Log in to the Distributed Seat Management Manage System.

Step 2 Click  and then select **User Management > Account**.

Step 3 Click **Add Account** at the upper-right corner.

Step 4 Configure the account name, password, and the group it belongs to.



The password must contain 8 to 32 characters and at least two types from number, letter and special character (excluding "", "", "", ":", ":", and "&"). The password must contain two or more of the previous types of characters. Enter a strong password according to the security level indication.

Step 5 Click **Next** to set the devices to get and account permissions.

User permissions must not be greater than its group permissions.

- 1) On the **Get** tab, select devices.



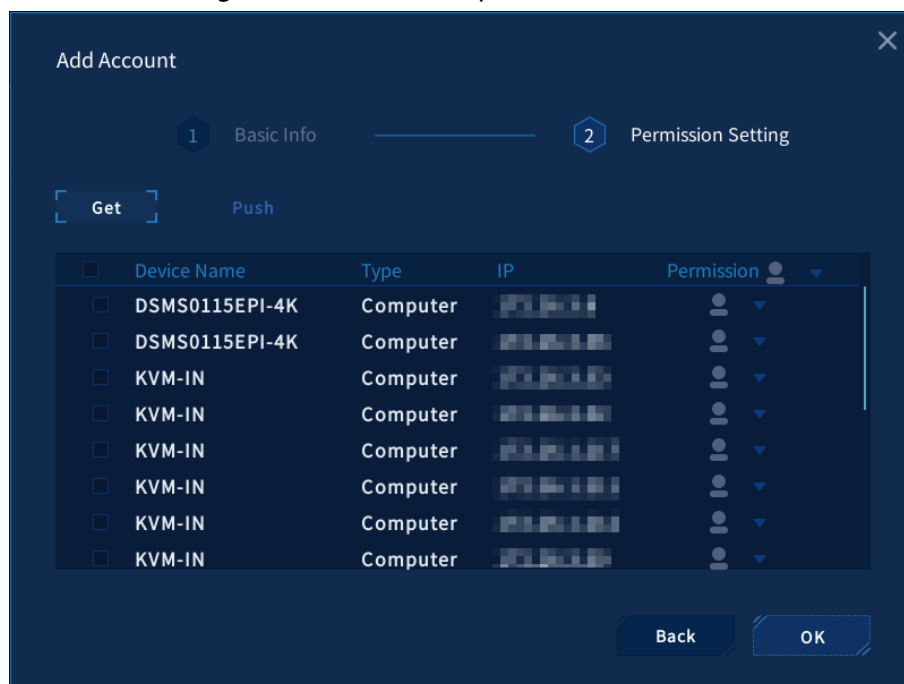
Permissions set for unselected devices will not take effect.

- 2) Set getting permissions.

On the **Permission** column, click the triangle.

- **View Only:** You can only view but not operate the device.
- **Get:** You can use your mouse and keyboard to control the device that you get. Users with the get permission can control devices at the same time.
- **Exclusive:** You have exclusive mouse and keyboard control over other users. If you are to take over the control of an exclusive user, the user will receive a request. Otherwise, you take over the control with a takeover notice.

Figure 3-15 Set account permissions



- 3) Click **Push**, and then select the devices that you push signals to.



Unselected devices cannot be pushed to.

Step 6 Click **OK**, and the new account will be displayed in the list.

Step 7 (Optional) Click  to exit the page.

3.8.3 Configuring Password Update Cycle

Set a password update cycle so that when the cycle ends you will receive a prompt noticing that you need to update your password.

Procedure

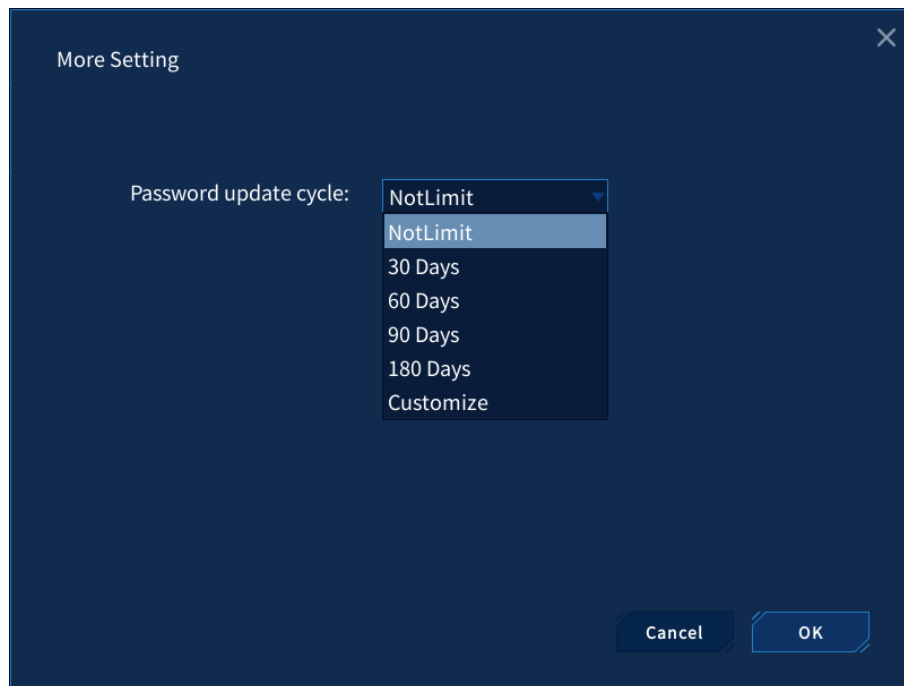
Step 1 Log in to the Distributed Seat Management Manage System.

Step 2 Click , and then select **User Management > Account**.

Step 3 Click **More Setting** at the upper-right corner.

Step 4 Click the drop-down box, select a period, and then click **OK**.

Figure 3-16 Set password update cycle



3.9 Changing Password (Non-admin Account)

The password of the admin account cannot be changed. You can change the password of a non-admin account by the following two methods.

By Logging in to the Admin Account

1. Log in to the admin account, and then select **User Management > Account**.
2. Click  of a non-admin account, and then set a new password.

By Logging in to the Non-admin Account

1. Log in to the non-admin account.
2. At the upper-left corner of the screen, click the triangle on the right of the account name.
3. Set a new password.

3.10 Legal Information

Procedure

- Step 1 Log in to the Distributed Seat Management Manage System.
- Step 2 Click  at the upper-right corner, and then select **System Info**. You can view the software license agreement, privacy policy, and open source software notice.

4 Application

The distributed seat management system supports menu mode and split screen mode. Click **Menu Mode** or **Split Screen Mode** to switch.

You can switch the pages through shortcut keys, which can be configured by the configuration tool. If you need to change them, contact our technical support.

- Press the Alt key on the right side of the keyboard twice to enter the split screen mode.
- Press the Ctrl key on the right side of the keyboard twice to enter the get page.
- Press the Shift key on the right side of the keyboard twice to enter the **Push** page.

4.1 Multi-window Display

Multiple host screens can be shown on one display. You can operate on each split screen with one mouse, including zooming in by double-clicking the screen. Fast signal scheduling and response help improve your work efficiency greatly.

Procedure

Step 1 Log in to the Distributed Seat Management Manage System.

Step 2 In the menu mode, click **Split Screen Mode** or press the Alt key on the right side of the keyboard twice in a row to quickly enter the split screen mode.

Four modes are available.

- : Single screen.
- : 2 screens.
- : 4 screens.
- : Customized. Click and drag your mouse to split the screen into sub ones.



If the number of screens reach the limit, a message will be displayed.

Figure 4-1 Window split



4.2 Audio Input and Output

Audio input and output are available between input nodes and output nodes.

Procedure

- Step 1 Log in to the Distributed Seat Management Manage System.
- Step 2 On menu mode, click **Split Screen Mode** or press the Alt key on the right side of the keyboard twice in a row to quickly enter the split screen mode.
- Step 3 Click the mic icon at the upper-right corner to control audio input and output.



- The icon is not displayed if there is no screen display.
- The icon is not displayed for non-input devices.
- The mic and the speaker cannot be enabled at the same time.

4.3 Audio Output

After it is enabled, audio output of the signal source is available.

Procedure

- Step 1 Log in to the Distributed Seat Management Manage System.
- Step 2 On menu mode, click **Split Screen Mode** or press the Alt key on the right side of the keyboard twice in a row to quickly enter the split screen mode.
- Step 3 Click the speaker icon at the upper-right corner to control audio output.



- The icon is not displayed if there is no screen display.
- The icon is not displayed for non-input devices.
- The mic and the speaker cannot be enabled at the same time.

4.4 Get

After getting, the system displays the screen of the device that you get. You can operate the input devices based on your permissions.

4.4.1 Getting Devices

Procedure

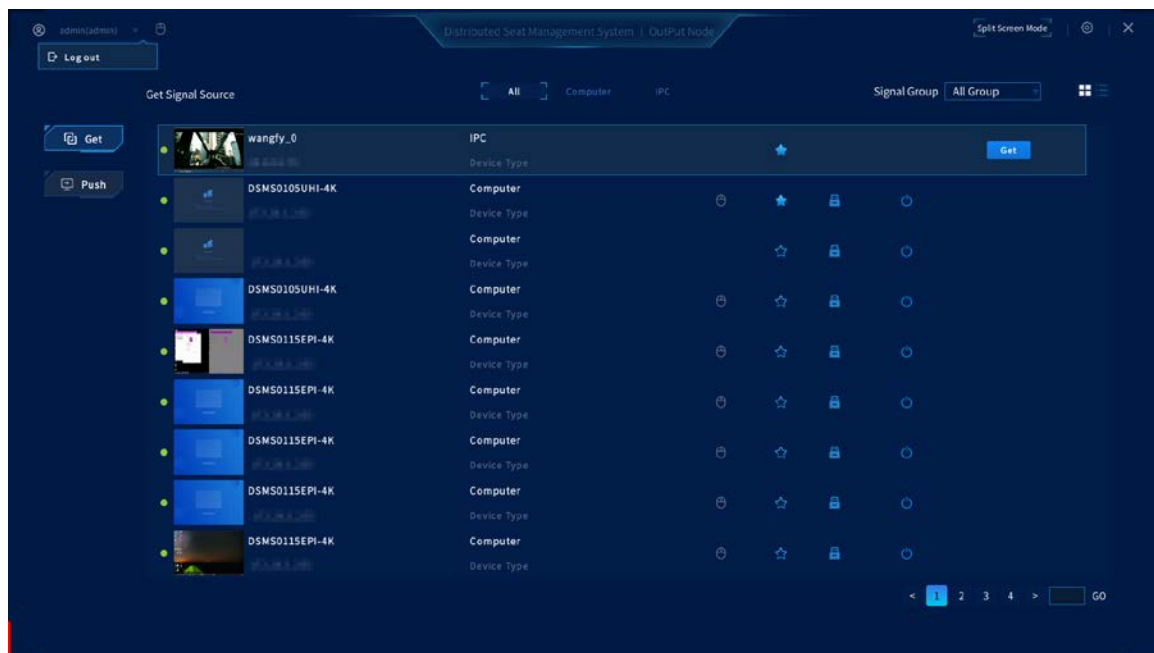
- Step 1 Log in to the Distributed Seat Management Manage System.
- Step 2 Press the right Ctrl key twice in a row or click **Get** on the menu mode.
- Step 3 Click **Get** of a device.
The system displays the screen of the device you get. Use a mouse and a keyboard to operate.



After getting, you cannot directly exit the device screen but you can use the shortcut keys

to switch between the interface.

Figure 4-2 Get a device



- : Click the icon (and it becomes ) to favorite the device, which will be pinned to top.
- : This icon indicates that you can operate the device after you get it. If the icon is not displayed, you can only view but not operate the device.
- : Click the icon to remotely shut down or start the computer that you get.



- ◇ You need to enable the center control function on **Basic Config** before the icon can be displayed.
- ◇ Only computers support remote shutdown.

4.4.2 Display Mode

There are two display modes.

- View Mode
On the **Get** page, click , and the thumbnails of the devices are displayed.
- List Mode
On the **Get** page, click , and the devices are displayed as a list.

4.4.3 Data Transmission through USB Flash Drive

Insert a USB flash drive into the output node, and it can be recognized and operated on the computer.

Figure 4-3 Data transmission through USB flash drive



Connecting a USB Flash Drive

On the **Get** page, select a signal source, click the triangle icon, and select a USB flash drive. Click , and the icon becomes . The computer can then recognize the USB flash drive, and you can copy, cut, and paste files from the computer to the USB flash drive.  means it is unavailable.



When multiple USB flash drives are inserted, only one can be passed through at a time.

Disconnecting a USB Flash Drive

Click  again to disconnect. The computer does not display the USB flash drive accordingly.

4.5 Push

Push the current screen to a specified seat or video wall.

4.5.1 Pushing Devices

Procedure

Step 1 Log in to the Distributed Seat Management Manage System.

Step 2 Press the right Shift key twice in a row or click **Push** on the menu mode.

Step 3 Push a device. You can push a device manually or by one click.

- Push Manually
 1. Click **Push**.
 2. Select a window to push to, and then click **Push**.

- By One Click

Click  to push the entire screen of the current seat. The split mode and the screen display of the target seat are the same with the current device.



- ◇ Only seat devices support the one click function.
- ◇ If the current seat is consisted of multiple devices, the one-click function will push the screen that the menu is on.
- ◇ If the group you select contains input matrix, the system will push the input matrix to the seat, including its split mode and the entire screen display.

4.5.2 Push Device Category

There are three types: All, TV Wall, and Seat.

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.