

Video Matrix Platform (N70)

User Manual



V1.0.0

Foreword

General

This document describes the appearance and functions of the video matrix platform (hereinafter referred to as the "Device") in details. Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

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

Signal Words	Meaning
 DANGER	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 WARNING	Indicates a potential risk which, if not avoided, may result in property damage, data loss, lower performance, or unpredictable result.
 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.	June 2025

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interfaces used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, comply with the guidelines when using it.

Transportation Requirements



- Transport the device under allowed humidity and temperature conditions.
- Do not transport the device with its front panel facing down.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Installation Requirements



-  **Electrical Hazard**
Preventive measures: Make sure the power is off when you put your hand into the device.
- **Stability Hazard**
Possible result: The rack might fall down and cause serious personal injury.
Preventive measures (including but not limited to):
 - ◇ Before extending the rack to the installation position, read the installation instructions.
 - ◇ When the Device is installed on the slide rail, do not place any load on it.
 - ◇ Do not retract the slide rail while the Device is installed on it.



-  **Rotating Fan Blades Hazard**
Avoid touching the fan blades, especially when they are moving.
-  Before installation, disconnect all the power cords.
- Use a cable tie to bundle the cables after they are connected to avoid risk of short circuits, overheating and electrocution caused by tangled cables.



- The device must be installed in a location that only professionals can access. Non-professionals are not allowed to enter the installation area.
- When installing the device, make sure that the power plug can be easily reached to cut off the power.

- A 5 A overcurrent protection device is required to be installed in the external power circuit of the product as a circuit breaker. Make sure the protection device is close to the product, offering safety of cutting power during maintenance.
- Install the device near a power socket for emergency disconnect.
- A safety circuit breaker is designed on the device bottom to cut the power of the device. Make sure the breaker can be easily operated during installation.
- Make sure the product is installed by trained professionals and it must be installed in locations that only professionals can access.
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 5 cm on the sides and 1 cm on top of the device.
- Do not block the ventilator of the device with objects, such as newspaper, table cloth or curtains.
- Do not put open flames, such as a lit candle, on the device.
- Prevent liquid from dripping or splashing on the device. Do not put any objects filled with liquid, such as a vase, on top of the device.
- Do not place or install the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, or soot.
- Make sure the device is installed stably and levelly, allowing normal status for internal tremor resistant modules.
- 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.
- An independent protective grounding terminal is designed at the lower-right corner of the product. Make sure the terminal is reliably grounded during installation.
- Connect the cables in sequence when linking the circuit, and connect the power cable last to avoid damaging the device.
- Make sure the negative binding post of the battery is disassembled while the device is being wired.
- 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.

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 subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.



WARNING

- Operating the device in a domestic environment may cause radio interference.
- Place the device in a location that children cannot easily access.
- When the redundant power supply is optional, use the power supply of the same manufacturer and model as the original one of the product.
-  High Current

Preventative measure: Ground the screw of the device to protective ground before you power it on.

-  Do not use multiple devices together to avoid generating high current.

Preventative measure: Ground the device to protective ground before you power it on.



- Use the device under the allowed humidity and temperature conditions.
- Use the device within the rated range of power input and output.
- Operating temperature: -10 °C to +50 °C (14 °F to 122 °F).
- Do not disassemble the device.
- Do not plug or unplug RS-232, RS-485 or the audio/video signal cable with the power on to avoid damaging the ports.

Maintenance Requirements



DANGER

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.



WARNING

- A blown fuse does not ensure disconnection of subsequent circuit. Please be cautious during maintenance.
- Power off the device before maintenance.

- The device can only be used with batteries possessing internal protection. To prevent explosion, dispose of the old batteries as instructed.
- Make sure to use the same model when replacing the battery to avoid fire or explosion.



- The device casing provides protection for internal components. Use a screwdriver to loosen the screws before detaching the casing. Make sure the casing is put back and fixed to the original spot before power on and use the device again.
- Damp dust on the circuit board might cause the device to short circuit, resulting in device damage. Make sure to regularly clear dust from the circuit board, connectors and the case with a brush.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	II
1 Overview.....	1
1.1 Introduction.....	1
1.2 Features.....	1
1.3 Main Box.....	2
1.4 Function Card.....	3
1.4.1 4 Channels UHD Encoding and Decoding Card VCC0402EH-N70.....	4
1.4.2 4 Channels UHD Decoding Card VDC0400EH-N70.....	4
2 Installation.....	5
2.1 Inspection Steps.....	5
2.2 Product Dimensions.....	5
2.3 Device Installation.....	6
2.3.1 Preparation of Installation Environment.....	6
2.3.2 Installation Steps.....	6
2.3.3 Booting and Shutdown.....	7
3 Local Interface Configuration.....	9
3.1 Power on and off.....	9
3.2 Initializing and Login.....	9
3.3 Network Settings.....	11
3.4 Other Settings.....	11
3.5 System Information.....	12
4 Web Operations.....	14
4.1 Network Connection.....	14
4.2 Initialization and Login.....	14
4.3 Device Configurations.....	15
4.3.1 Signal Management.....	15
4.3.2 Network Signal.....	18
4.4 Video Wall.....	21
4.4.1 Video Wall Configurations.....	21
4.4.2 Creating Compatible Video Wall.....	22
4.4.3 Video Wall Control.....	23
4.4.4 Video Wall Operations.....	31
4.4.5 Display Management.....	38
4.4.6 Network Configurations.....	43
4.4.7 System Management.....	46
4.4.8 Security.....	51

4.4.9 Maintenance Center.....59

4.4.10 Event Management.....63

4.4.11 Third-Party Device Connection.....63

Appendix 1 Serial Cable Assembly Guide.....65

Appendix 1.1 Screen Control through 485.....65

Appendix 1.2 Screen Control through 232.....66

Appendix 2 Matrix Serial Port Control Protocol.....69

Appendix 3 Security Recommendation.....71

1 Overview

1.1 Introduction

Based on Advanced Telecommunications Computing Architecture (ATCA), video matrix platform is designed as a modern telecommunication-level device which supersedes DVR, decoder, analog matrix, and video wall controller. It is compatible with past and current network monitoring environments.

1.2 Features

Structure

- Standard 19" 3U rack-mounted server with ATCA telecommunication-grade architecture.
- 8 slots for audio and video cards.
- Developed with a modular design, it is easy to insert cards and configure it to meet your needs.
- Offers redundant dual power supply, making it highly suitable for locations such as machine rooms.
- The intelligent fan can be automatically adjusted to moderate the temperature, ensuring the stability and reliability of the system.

Software

- The embedded LINUX operating system is secure, reliable, stable, efficient, and user-friendly for developers and maintenance personnel.
- Adopts the H.265 video compression standard, offering support for dual stream technology and variable bit rates. It can encode both composite and video streams while ensuring audio and video synchronization during composite stream encoding.
- Supports encoding of common video signals such as DP, HDMI, and DVI.
- Supports 4K signal capture and encoding.
- Supports up to 18 channels of 4K signal output through HDMI ports, allowing for seamless splicing across up to 36 screens.
- Supports input of up to 8 channels at 4K@60 fps for ultra HD encoding, or 8 channels at 4K@60 fps for HD encoding.
- H.264/H.265 decoding: Supports up to 432 channels of 1080p@25 fps HD video decoding.
- Simultaneously decodes audios and videos.
- Decodes videos in 32 MP, 24 MP, 12 MP, 8 MP, 5 MP, 3 MP, 1080p, 720p, and D1. Only H.265 can be used to decode videos in 32 MP, 24 MP and 12 MP.
- Supports the following standards: H.265, H.264, SVAC, MPEG4 and MJPEG.
- Features point-to-point output display in ultra-high resolution.
- Supports local signal/network signal input and matrix output.
- Supports processing multiple copies of signals, utilizing a maximum of 32 output channels for each signal.
- Supports 128 scene presets, allowing users to customize the video wall layout for each scenario.

Video Wall Splicing

- Features splicing, scaling, video integration, roaming, windowing, and OSD.
- Supports splitting to 1, 4, 6, 8, 9, 16, 25, and 36 windows. You can also customize the split windows.
- Supports point-to-point high-definition background image display.
- Supports subtitle overlay functionality, enabling virtual text display on single or spliced screens with customizable font, color, character spacing, and background color.

Other Features

- Supports control via web browsers, PC clients, mobile clients, and network keyboards.
- Supports 2 RJ-45 interfaces.
- Supports network mode configuration including fault tolerance, single NIC, link aggregation, and load balancing, with fault tolerance as the default setting.
- Supports RS-232 serial interface for matrix control, display power management, and related functions.
- Supports TCP/IP protocol stack including RTP, RTSP, RTCP, TCP, UDP, and DHCP network protocols.
- Displays local and network videos on the video wall through remote control.
- The system can be restarted, updated or restored to its default settings remotely.
- Supports the management of user permissions and allowlists.

1.3 Main Box

Video Matrix Platform with 19-inch 3U structure host case includes function card slot, power page and intelligent temperature-controlled fan.

- Air inlet of the case.
- Intelligent temperature-controlled fan allows hot swap.
- Dedicated slots for audio and video cards, a total of 8, numbered sequentially, used for installing the rear page card of the business cards.
- 1 dedicated slot of main control card, marked as **M**.
- Dual-power module supports redundant hot standby.



Two power cables should be unplugged simultaneously.

Figure 1-1 Front panel



Figure 1-2 Rear panel



Table 1-1 Port Description

No	Description
1	Power
2	Reset
3	Type-c Port
4	Indicator Light
5	USB3.0 Port
6	HDMI Output
7	Alarm Input, Alarm Output, Standard RS-485 Port
8	Network Port (10/100/1000 Mbps Ethernet Port)
9	RS-232 Port of Screen Control
10	Audio Out
11	Alarm Clear
12	Ground

1.4 Function Card

Function card with blade modular design is mainly used for audio and video signal acquisition and encoding, splicing and merging, and decoding output, and more.

1.4.1 4 Channels UHD Encoding and Decoding Card VCC0402EH-N70

Figure 1-3 VCC0402EH-N70



- 2 input ports: 1 HDMI 2.0 port and 1 HDMI 1.3 port.
- 4 output ports: 2 HDMI 2.0 port and 2 HDMI1.3 ports.
- 1 type-c port.

1.4.2 4 Channels UHD Decoding Card VDC0400EH-N70

Figure 1-4 VDC0400EH-N70



- 4 output ports: 2 HDMI 2.0 ports and 2 HDMI 1.3 ports.
- 1 type-c ports.

2 Installation

2.1 Inspection Steps

When you receive Video Matrix Platform, please inspect it according to the following steps.

Procedure

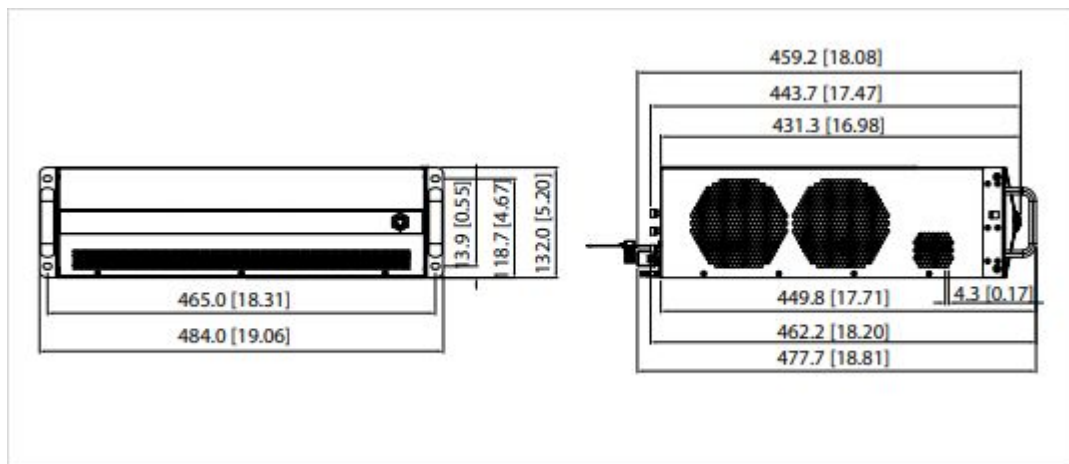
- Step 1 Inspect whether there are obvious damages on its appearance.
The material of product package should be able to protect the product from most impacts during transportation.
- Step 2 Open the external package, and check whether any part of accessories is missing. You may refer to accompanied accessory bag. After you have checked that all parts are included, you may remove protective film on the device.
- Step 3 Open device case to inspect data cable and power cable of front panel, and see if the connection between main control panel and page card is loose. Inspect whether main control panel, control panel and function card are inserted tightly.



One label at the side of the case owns serial number and other information of the device, which shall be provided when dialing after-sales calls. This label shall be protected well, and shall not be torn or discarded; otherwise, we may not be able to provide effective service.

2.2 Product Dimensions

Figure 2-1 Product dimensions (mm [inch])



2.3 Device Installation

2.3.1 Preparation of Installation Environment

As a system-level monitoring device, Video Matrix Platform is usually used in central machine room of monitoring system. Its installation site shall meet national and local machine room construction standards.

Video Matrix Platform is a standard rack-mounted device fixed in a cabinet. Please pay attention to the following points during installation and use:

- Ensure that the cabinet is sufficiently firm to support Video Matrix Platform and accessories. During installation, avoid dangers resulting from uneven mechanical load.
- Ensure that A/V cable owns sufficient installation space. Bending radius of cables shall not be less than 5 times as many as their outer diameter.
- Ensure well ventilation. It is suggested that its installation position shall be more than 50 cm above the ground.

Power Supply Requirement

- Rated current: 10 A / 5 A
- Rated power: ≤ 500 W
- Rated voltage: 100–240 VAC

Anti-interference Requirement

- On-site power supply system shall take effective anti-interference measures.
- Working ground shall not be shared with ground wire or lightning protection device of electrical device, and shall keep away from them as far as possible.
- Keep away from high-power radio transmitting stations, radars and high-frequency heavy-current devices.
- When necessary, adopt electromagnetic shielding methods to resist interference.

Environmental Requirement

- Ensure that temperature in the cabinet is from 0 °C to +55 °C.
- Ensure that humidity in the machine room is 10% RH–90% RH.
- Ensure air ventilation required by safe operation of the device.

2.3.2 Installation Steps

Procedure

- Step 1 The main control card has been installed.
- Step 2 Insert function cards or false cards according to actual needs.



In a fully loaded condition, the false panel does not need to be inserted; however, in a non-fully loaded condition, the false panel must be inserted, otherwise it may affect usage.

Step 3 Ground terminal of Video Matrix Platform shall realize reliable grounding.



To guarantee personal safety and device safety, Video Matrix Platform and those devices (such as video wall and PC) that are connected the platform with cables shall be grounded.

Step 4 Connect network cable, HDMI cable and other cables.

Step 5 Plug in the power cable to boot the device.

2.3.3 Booting and Shutdown

2.3.3.1 Booting

Plug in power cable, and press power switch on front panel. Power indicator light turns on and device boots up.

Please pay attention to the following points during booting:

- Make sure that the supplied voltage is within 100-240 VAC 47Hz-63Hz. Check power cable connection before you turn on the device.
- We recommend you use power supply with stable voltage and little interference (refer to international standard), which helps the device to work stably and prolong service life. This will also benefit external devices such as camera. UPS is the best choice if possible.

2.3.3.2 Shutdown

There are two shutdown methods:

- Method 1: Select **Maintenance Center** > **Maintenance Management** > **Maintenance**, and then click **Shutdown**.

Figure 2-2 Shutdown

The screenshot shows a web interface for system maintenance. It has two main sections: 'System Maintenance Operations' and 'System Maintenance Config'. The first section contains 'Restart' and 'Shutdown' buttons. The second section contains an 'Auto Restart' configuration area with a dropdown menu set to 'Tuesday' and a time field set to '02:00'. At the bottom, there are 'Apply' and 'Refresh' buttons.

- Method 2: Press and hold the power button on the panel for 5 seconds until the indicator light turns orange; the device will begin to shut down. Once the device is fully powered off, the indicator light will remain steadily orange. Press the power button again to turn the device on, and the indicator light will turn green.



- Method 1 is recommended, in order to protect the device from damages due to unexpected outage.
- Stop all operations of the device, before you unplug the device from power supply.

2.3.3.2.1 Outage Recovery

In case of outage or forced shutdown during working, after connecting power supply again, the device will automatically save and resume previous working status.

2.3.3.2.2 Replace Button Battery

We recommend that the same type of battery should be used. Inspect system time regularly. Generally speaking, battery shall be replaced once a year, to guarantee system time accuracy.



Before replacement, please export and save configurations, or all configurations will be lost!

3 Local Interface Configuration

Before performing local interface operations, connect the display and other control devices, such as mouse, to the equipment.

3.1 Power on and off

- Power on: Connect the power cable and press the power switch on the front panel. The power indicator will illuminate, indicating the device is powered on.
- Power off: Press and hold the power button on the front panel for 5 seconds to power off the device.



When the device is operational, if system power is interrupted or forcibly shut down, it will automatically reconnect to front-end devices upon power restoration and resume operation from the pre-interruption state.

3.2 Initializing and Login

Procedure

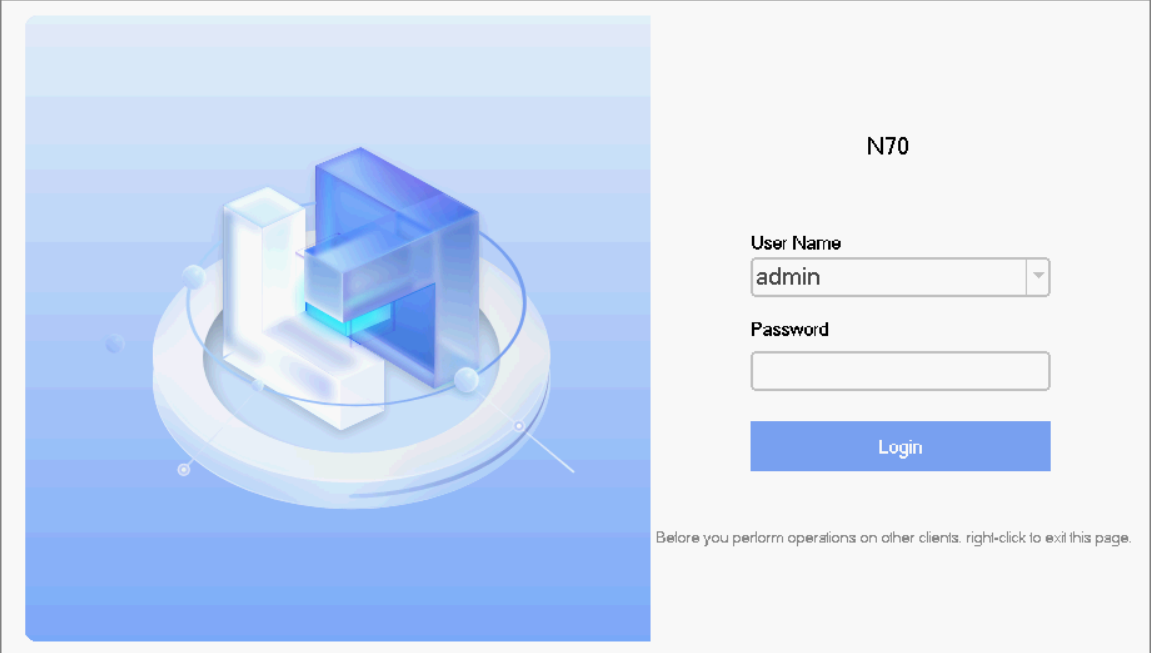
- Step 1 Connect the power cable and wait for the device to start up.
After the device starts up, it enters the initialization page.
- Step 2 Configure your own password, confirm the password, and then tap **OK**.
After the initialization is complete, the device enters the login page.



- The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &). The new password and confirmation password must match. Set a password with high strength according to the on-screen instructions.
- Account locks after 5 consecutive failed password attempts within 30 minutes.

- Step 3 On the login page, enter user name and password, and then tap **OK**.

Figure 3-1 Login screen



Step 4 The system displays the home screen.

Figure 3-2 Home screen

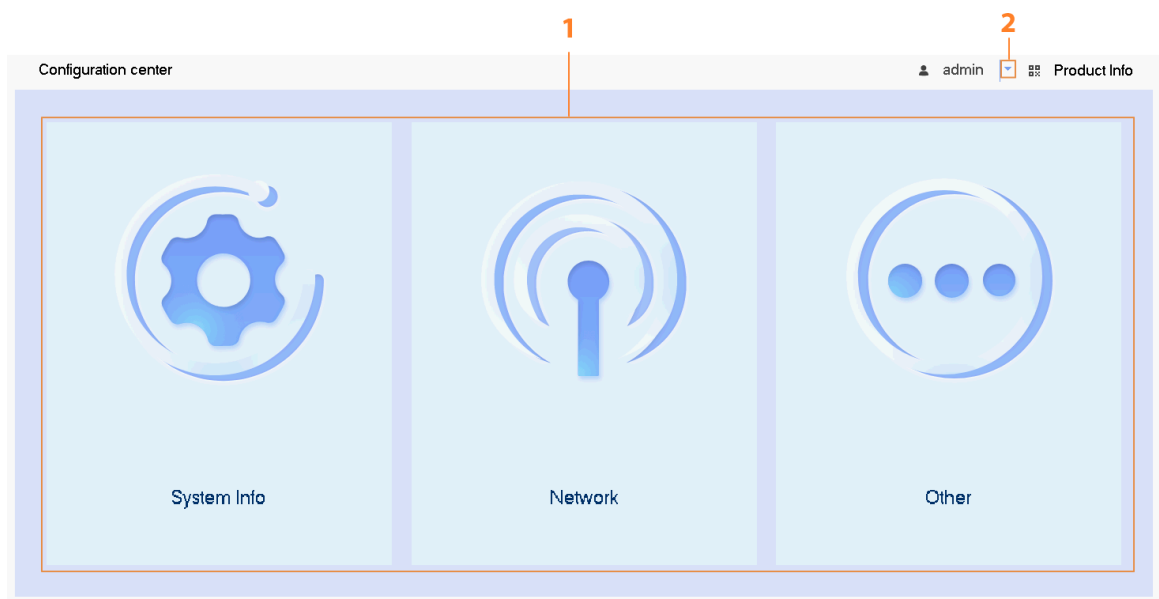


Table 3-1 Introduction of home screen

No.	Description
1	Function menu, including system information, network settings, and other configurations.
2	Account information, viewing account name, logging in/out, or restarting the system.

3.3 Network Settings

Configure the network of the device to ensure the communication between the devices.

Procedure

- Step 1** Click **Network** on the home screen.
- Step 2** Configure the network parameters of the device, and then click **Save**.

Figure 3-3 Network settings

The screenshot displays the 'Network' configuration page. At the top, there's a header with a home icon, the title 'Network', and user information 'admin' and 'Product Info'. The main area contains several settings: 'NetCard' is set to 'Bond1' with a dropdown arrow; 'Net Mode' is 'Fault-tolerance'; 'IP Version' is 'IPv4'; 'DHCP' is an unchecked checkbox; 'IP Address' is '172.168.1.108'; 'Subnet Mask' is '255.255.0.0'; 'Gateway' is '172.168.1.1'; 'Max Connection' is '128'; and 'Default Card' is 'Bond1'. A 'MAC ADDRESS' field shows 'b2:98:35:e6'. At the bottom left are 'Save' and 'Default' buttons.

Table 3-2 Description of network settings

Parameter	Description
IP Version	Select IPv4 by default.
DHCP	If you select the function, the system automatically assigns IP addresses.
IP Address	Set the IP address of the device. The initial address is 192.168.1.108.
Subnet Mask	Set the subnet mask of the device.
Gateway	The gateway address of the device.
Max Connection	The number of connected users. The maximum number is 128.
Default Card	Select the default card for the device.

3.4 Other Settings

General Settings

1. On the home screen, click **Other**.
2. Click **General** . Configure the parameters, and then click **OK**.

Figure 3-4 General settings

The screenshot shows the 'Other' settings page in a web interface. The left sidebar has 'General' and 'Auto Maintenance' options. The main content area contains the following settings:

- System Time: 2025 - 06 - 24 13 : 54 : 49
- Date Format: YYYY MM DD
- Date Separator: -
- Time Format: 24-HOUR
- Synchronous remote device: ☐
- NTP: ☐
- Server address: cn.ntp.org.cn (with a 'Manual Update' button)
- Time Zone: GMT+08:00
- NTP port: 123
- NTP update period: 10

At the bottom, there are 'OK' and 'Default' buttons.

Auto maintenance

1. On the home screen, click **Other**.
2. Click **Auto Maintenance**. Configure the parameters, and then click **OK**.

Figure 3-5 Auto Maintenance

The screenshot shows the 'Auto Maintenance' settings page. The left sidebar has 'General' and 'Auto Maintenance' options. The main content area contains the following settings:

- Emergency Maintenance: ☒ For easy access to our after-sales service, enable this function.
- SSH: ☒ There may be a security risk when this service is enabled.
- Auto maintenance: Every Tuesday (dropdown) 02:00 (dropdown)
- Default:
- All configurations except network Settings are restored to default

At the bottom, there are 'OK' and 'Default' buttons.

3.5 System Information

On the home screen, click **System Info** to view the device information.

Version Information

Click **Version** to view device SN, device type, system version, baseline version and more.

Figure 3-6 Version information

System Info	
Version	
Legal information	
SN	
Device Class	N70
Web	V5.509.839436
System	V4.0.0.R, Build Time: 2025-06-23 16:15:17
Security Baseline Version	V2.4
ONVIF Version	V2.4.1

Legal Information

Click **Legal Information** to view the information.

Figure 3-7 Legal information

System Info	admin	Product Info
Version	OpenSource Statement	
Legal information	OPEN SOURCE SOFTWARE NOTICE This document contains open source software notice for the product which includes this file does not necessarily use all of the third party software components referred to below. And this document is confidential information of copyright holder. Recipient shall not disseminate it without permission. Warranty Disclaimer THE OPEN SOURCE SOFTWARE IN THIS PRODUCT IS DISTRIBUTED IN THE HOPE THAT IT WILL BE USEFUL, BUT WITHOUT ANY WARRANTY, WITHOUT EVEN THE IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SEE THE APPLICABLE LICENSES FOR MORE DETAILS. Copyright Notice and License Texts Software(s) using GNU General Public License, Version 2 *linux_kernel Copyright (C) 2012 ARM Ltd. *u-boot Copyright (C) 2000-2006 Wolfgang Denk, DENX Software Engineering, wd@denx.de. GNU General Public License, Version 2 GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA. Everyone is permitted to copy and distribute verbatim copies of this license...	

4 Web Operations

4.1 Network Connection

Procedure

Step 1 Connect the device to a computer through network.

Step 2 Configure the IP address, subnet mask and gateway of the Device and the computer respectively. For network setup of video matrix platform.



- If there is no router on the network, distribute IP address on the same network segment.
- If there is a router on the network, configure the corresponding gateway and subnet mask.

Step 3 Ping `***.***.***.***`(IP address of the Device) to check whether connection is available.

Step 4 Open Google Chrome, enter the IP address, and then press the Enter key.



Supports Chrome 65 and above, Firefox 65 and above, and Edge 79 and above. Internet Explorer is not supported.

4.2 Initialization and Login

Procedure

Step 1 Enter IP address of the device in the address bar of the browser, and then press Enter.

Step 2 Enter and confirm the new admin password.

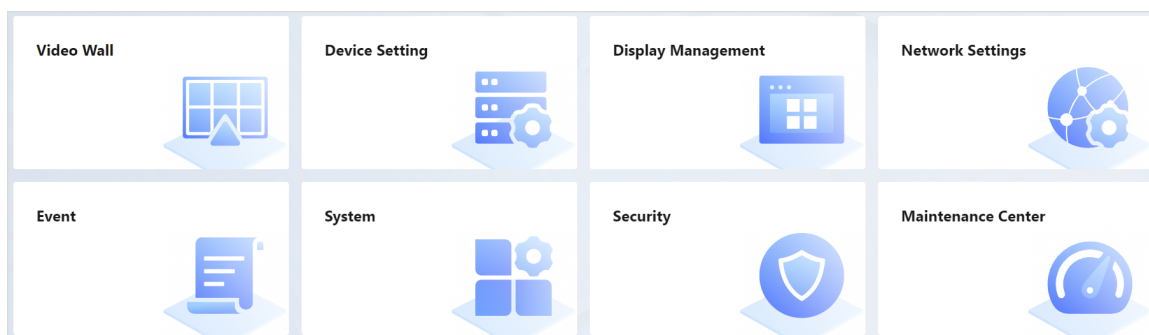


- You need to configure your own password for the first-time login.
- The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &). The new password and confirmation password must match.
- Set a high security password according to the prompt of password strength.

Step 3 Click **OK**.

Step 4 Enter username and password, and then click **Login**.

Figure 4-1 Login



4.3 Device Configurations

Support adding device one by one, searching for the device, and importing devices in batches.

4.3.1 Signal Management

Configure the channel name, control number, and encoding settings for the local signal.

Select **Device Setting** > **Local Signal** > **Signal Management**.

Figure 4-2 Signal management

Local Signal

Signal Management

Network Signal

No Signal Connected

No Signal

No.	Camera Name	Slot	Control No.	Signal Source Type	Interface Status	Operation
1	 Slot04-01	Slot4	13	HDMI	1920 * 1080@60	
2	 Slot04-02	Slot4	14	HDMI	1920 * 1080@60	

Total 2 records

1

2

- Click the specific channel name to edit the channel name.
- Click the specific control number to edit the control number.
- Click to edit encoding settings.

Figure 4-3 Encoding mode

The 'Encode' dialog box is shown with the 'Compression' tab selected. It contains two main sections: 'Main Stream' and 'Sub Stream'.

Main Stream Settings:

- Encoding Mo...: H.265
- Image Encodi...: YUV420
- Resolution: 0 * 0
- Frame Rate (F...: 60
- Bit Rate Type: CBR
- Reference Bit ...: 5120 - 5120Kbps
- Custom Strea...: ☐
- Bit Rate: 8192

Sub Stream Settings:

- Sub Stream toggle: ☒
- Encoding Mo...: H.265
- Image Encodi...: YUV420
- Resolution: D1
- Frame Rate (F...: 60
- Bit Rate Type: CBR
- Reference Bit ...: 1024 - 5120Kbps
- Custom Strea...: ☐
- Bit Rate: 4096

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

Table 4-1 Parameter description

Parameter	Description
Encode Mode	H.265 encode mode in default.
Image Encoding Format	The default format for compressing and storing image data is YUV420.
Resolution	It includes a variety of resolution types. Every type corresponds to different recommended stream value.
Frame	Configure video frame per second. The higher frame rate is, the more natural and smooth the video will be, but more bandwidth will be required.

Parameter	Description
Bit Rate Type	● CBR : The bit stream changes slightly around the defined bit stream value. We recommend selecting the CBR when the monitoring scene changes a little. ● VBR : The bit stream will change with the environmental conditions. We recommend selecting VBR when the monitoring scene changes greatly. ● Fixed Quality : The smaller the image quality parameter value, the better the image quality.  Image quality can be set in VBR mode only.
Reference Bit Rate	Reference bit rate provides the range of bit rate.
Custom Stream	You can click  corresponding to Custom Stream , and then you can enter stream value manually, or select the bit rate from the Bit Rate list.  The reference bit rate is not displayed when no information is collected on the channel.
Bit Rate	

Figure 4-4 Audio encoding

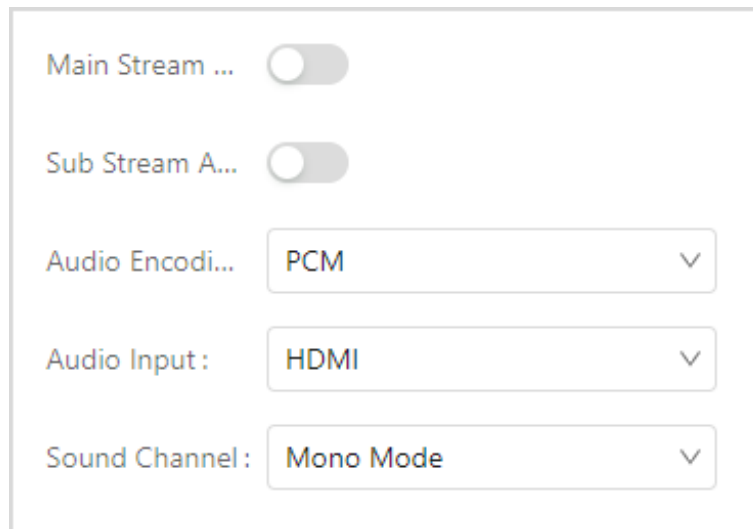


Table 4-2 Audio encoding description

Parameter	Description
Main Stream Audio	Click  to enable main stream audio capture.
Sub Stream Audio	Click  to enable sub stream audio capture.
Audio Encoding	Select audio encode format. the default format is PCM.
Audio Input	Select HDMI audio input.
Sound Channel	You can select Mono Mode or Stereo Mode .

4.3.2 Network Signal

You can add devices in the network and display network signals on the video wall.

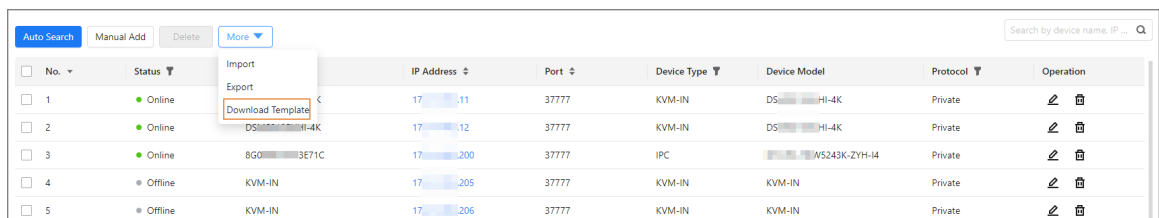
4.3.2.1 Adding Signals in Batches

Enter the device information in the template and import the template to add devices. This method is recommended when devices are added in batches.

Procedure

- Step 1** On the main page, Select **Device Setting** > **Network Signal** > **Device**.
- Step 2** Click **More**, and then click **Download Template** to download the template to your local PC.

Figure 4-5 Download templates



No.	Status	IP Address	Port	Device Type	Device Model	Protocol	Operation
1	Online	172.16.1.11	37777	KVM-IN	DS-HI-4K	Private	
2	Online	172.16.1.12	37777	KVM-IN	DS-HI-4K	Private	
3	Online	172.16.1.200	37777	IPC	W5243K-ZYH-I4	Private	
4	Offline	172.16.1.205	37777	KVM-IN	KVM-IN	Private	
5	Offline	172.16.1.206	37777	KVM-IN	KVM-IN	Private	

- Step 3** Enter the device information, and then save the template.
- Step 4** Click **More**, and then select **Import** to import the template.

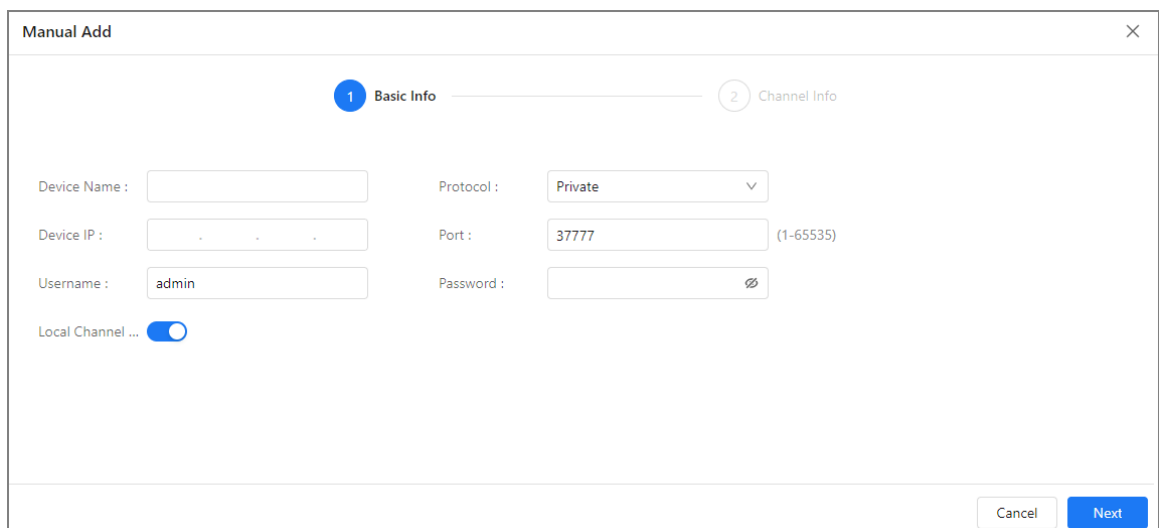
4.3.2.2 Adding Devices One by One

Configure the IP address, username, and password of the device manually. This mode is recommended when a small number of devices are added and the IP addresses, usernames, and passwords of the devices are known.

Procedure

- Step 1** On the main page, Select **Device Setting** > **Network Signal** > **Device**.
- Step 2** Click **Manual Add**, and then configure the parameters.

Figure 4-6 Add the device manually



Manual Add

1 Basic Info 2 Channel Info

Device Name :

Protocol :

Device IP :

Port : (1-65535)

Username :

Password :

Local Channel ... ☒

Cancel Next

Step 3 Click **Next**, and then configure the number of the channels.

Figure 4-7 Configure the channels

Manual Add

Basic Info — 2 Channel Info

Video Channel

Number of Ch... 4 (1-981) Get Info

☒	Channel No.	Camera Name
☒	1	Channel 1
☒	2	Channel 2
☒	3	Channel 3
☒	4	Channel 4

Cancel Back Done

Step 4 Click **Done**.

4.3.2.3 Adding by Search

Search for devices on the same network. This method is recommended when the IP address of the device to be added is uncertain.

Procedure

Step 1 On the main page, select **Device Setting** > **Network Signal** > **Device** > **Auto Search**.

Step 2 Configure the IP segment, and then click **Start Search**.

Step 3 Select the devices you want to add, and then click **Add**.

Figure 4-8 Add the devices by search

Auto Search						
Search Netwo... 172 . . . 1 - 172 . . . 255 Stop Search						
☒	No.	IP Address	Device Type	Protocol	MAC Address	Port
☒	1	172 . . . 4	Matrix	Private	f4 . . . a8	37777
☒	2	172 . . . 8	IEG	Private	f8 . . . a	37777
☒	3	172 . . . 13	KVM-IN	Private	4c . . . be	37777
☐	4	172 . . . 14	KVM-IN	Private	8c . . . :84	37777
☐	5	172 . . . 16	KVM-IN	Private	6c . . . :31	37777
☐	6	172 . . . 17	KVM-OUT	Private	fc . . . da	37777
☐	7	172 . . . 19	KVM-OUT	Private	fc . . . fe	37777
☐	8	172 . . . 20	KVM-OUT	Private	fc . . . ea	37777
☐	9	172 . . . 22	KVM-OUT	Private	b4 . . . :94	37777
☐	10	172 . . . 37	Matrix	Private	0c . . . :5f	37777
☐	11	172 . . . 38	Matrix	Private	f4 . . . e0	37777
☐	12	172 . . . 61	LCS	Private	b4 . . . :a6	37777
☐	13	172 . . . 62	LCS	Private	3c . . . :ee	37777
☐	14	172 . . . 121	Matrix	Private	e0 . . . :2c	37777
☐	15	172 . . . 123	Matrix	Private	f8 . . . :ec	37777
☐	16	172 . . . 127	Matrix	Private	e0 . . . :24	37777
☐	17	172 . . . 130		Onvif		80
						Cancel Add

Related Operations

- Click  to edit the device information.
- Click  to delete the device.
- Select the devices, and then click **Delete** to delete the devices in batches.

4.3.2.4 Viewing Channel Information

On the main page, select **Device Settings** > **Network Signal** > **Channel** to view the channel status, channel name, channel type, and more.

You can search for channel by device name, IP address, and channel name.

Figure 4-9 Channel information

Channel ...							
Channel ...	Status	Camera Name	Channel Type	Control No.	Device Name	IP Address	Port
33	Online	Slot00-01	Remote Channel	10001	DSA . . . HI-4K	172 . . . 11	37777
34	Online	00-01	Remote Channel	10002	DSA . . . HI-4K	172 . . . 12	37777
35	Online	kil-200_1	Remote Channel	10003	8GD . . . 3271C	172 . . . 200	37777
36	Online	IPC	Remote Channel	10004	9EO . . . 297995	172 . . . 212	37777

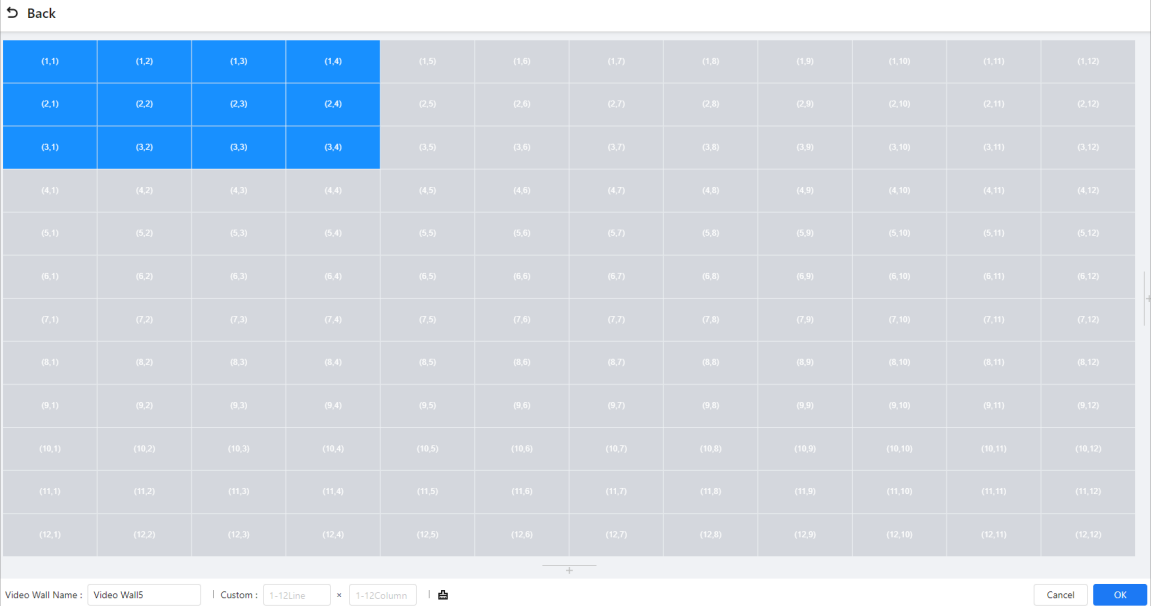
4.4 Video Wall

4.4.1 Video Wall Configurations

Procedure

- Step 1** On the main page, click **Video Wall** > **Video Wall Config**.
- Step 2** Click **Add**, and then configure the layout and the video wall name.

Figure 4-10 Add video wall



- Step 3** Click **OK**.



Press and hold the left mouse button to drag the screen.

- Step 4** Bind the output channel and the screen.

1. Select the output slot and screen.
2. Click  or  to automatically bind the slot with single screen horizontally or vertically.

- Step 5** Adjust the layout of the video wall.

Table 4-3 Adjust the layout

Icon	Description
	Zoom in and zoom out of the screen.  You can adjust the screen with the mouse wheel.
	Screen self-adaptive.
	Clear screen. Clear all screens on the video wall.
	Every splicing screen will show a name or ID.

Icon	Description
	Displays the screen control ID that you can use the network keyboard to control the video wall.

Step 6 Click **Save Video Wall**.



The new added video wall is enabled by default, you can click  to close it.

Related Operations

- Click  to edit the name of video wall.
- Click  to delete the video wall. Move the mouse to the screen, and then click  to delete the screen.

4.4.2 Creating Compatible Video Wall



Compatible with ISEE 2.0/NKB network keyboard.

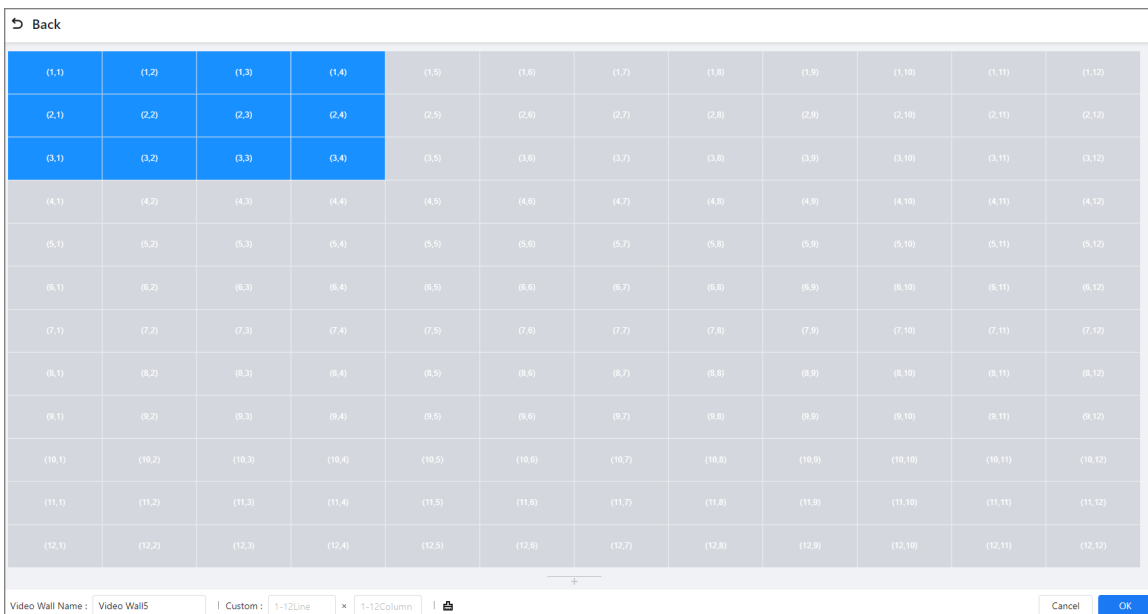
Procedure

Step 1 On the main page, select **Video Wall** > **Create Compatible Video Wall**.

Step 2 Click **Add**.

Step 3 Configure the video wall name, set the number of rows and columns for the video wall, and then click **OK**.

Figure 4-11 Configure the video wall




Press and hold the left mouse button to drag the screen.

Step 4 Bind the output channel and the screen.

- Select the output slot and screen.
- Click  or  to automatically bind the slot with single screen horizontally or vertically.

Step 5 Adjust the layout of the video wall.

Table 4-4 Adjust the layout

Icon	Description
	Zoom in and zoom out of the screen.  You can adjust the screen with the mouse wheel.
	Screen self-adaptive.
	Clear screen. Clear all screens on the video wall.
	Every splicing screen will show a name or ID.
	Displays the screen control ID that you can use the network keyboard to control the video wall.

Step 6 Click **Save Video Wall**.



The new added video wall is enabled by default, you can click  to close it.

4.4.3 Video Wall Control

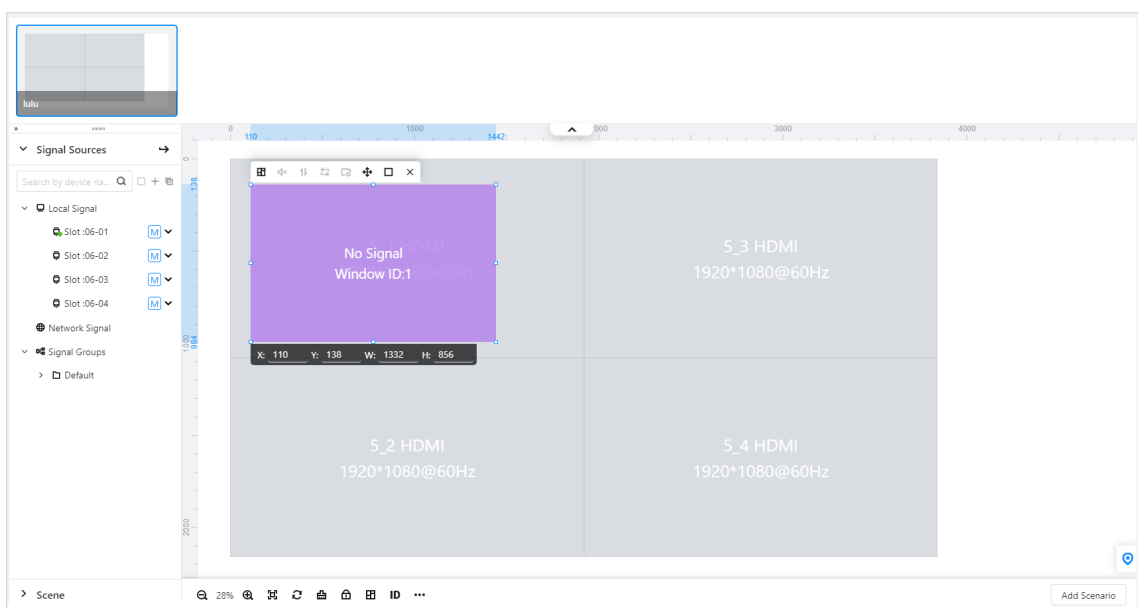
4.4.3.1 Window Configuration

Procedure

Step 1 On the main page, click **Video Wall**, and then select **Video Wall Control**.

Step 2 Select a video wall, and then press and hold the mouse to drag a window.

Figure 4-12 Add windows



- Select a window, press and hold the left mouse button, and you can move it to the desired position.

- Select a window, and hover over the window border. When the mouse pointer becomes a double-headed arrow, drag the mouse pointer to re-size the window.

Figure 4-13 Window icons

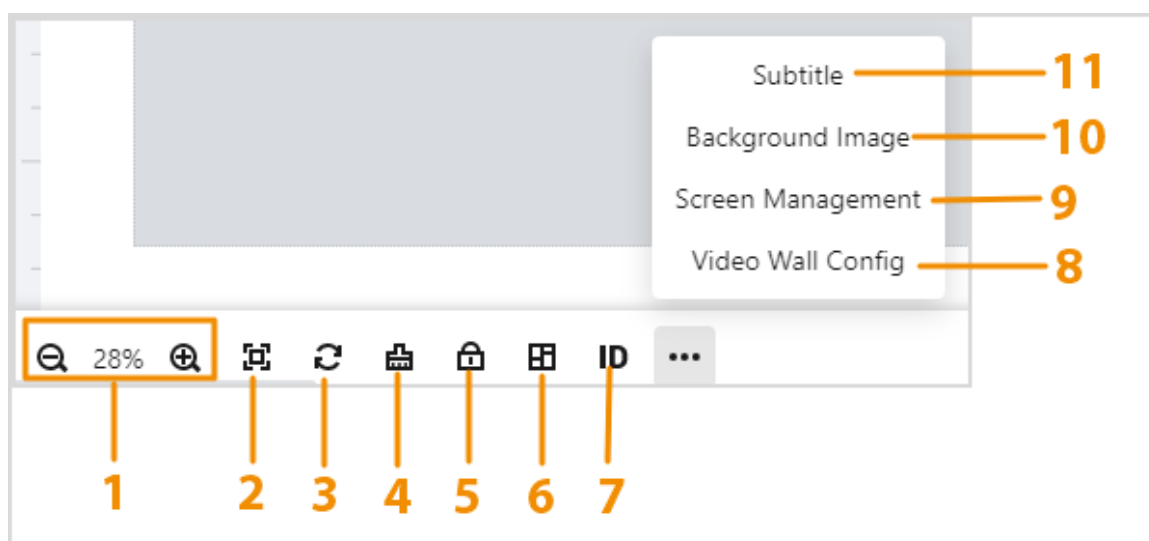


Table 4-5 Icon description

No.	Description
1	Click or to adjust.
2	Self-adaptive. Click the icon, the screen will automatically adjust itself to adapt to the layout.
3	Refresh. Click to refresh the page.
4	Clear. Click to clear the layout.
5	Click to lock the video wall. Click to unlock the video wall.
6	Quick layout. Click to select defined video wall layout.
7	Click to show the screen ID.
8	Video wall configuration. Configure the operations of the video wall including stream and display strategy and performance strategy.
9	Screen management. Configure the screen on/off and scheduled tasks.
10	Background image. Configure the background image of the display.
11	Subtitle. Configure the subtitles that the screen displays.

Step 3 Adjust the window.

Figure 4-14 Adjust the window

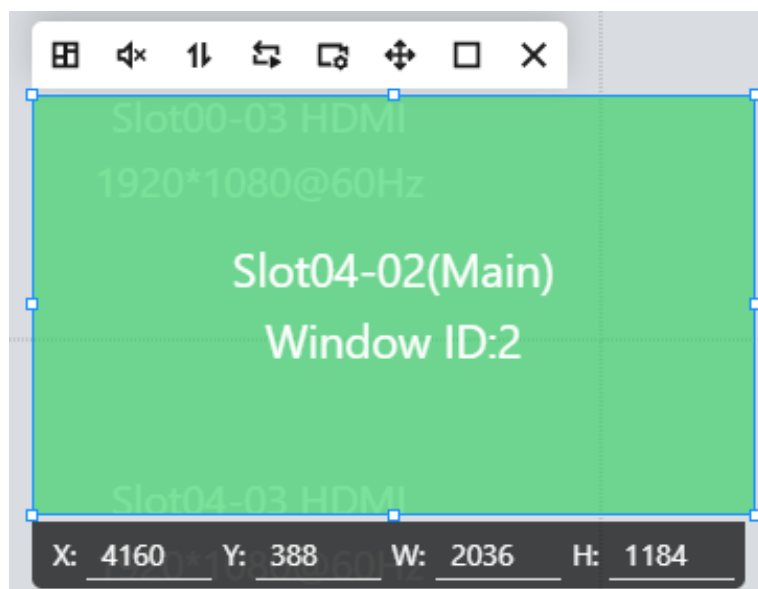
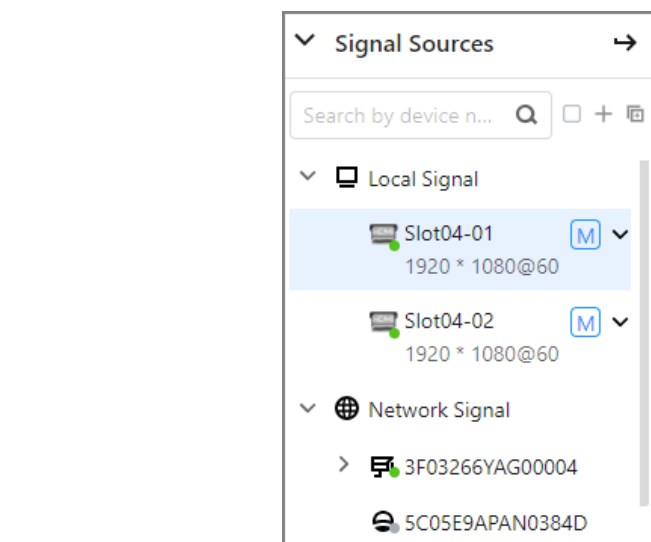


Table 4-6 Icon description

Icon	Description
	You can select fixed splits or enter the rows and columns to customize the fixing.
	Click the icon to turn on/off the audio.
	Click the icon, and then you can pin the window to the top or bottom, elevate this window by one level or move the window down one level.
	- Click the icon to start a signal tour, and the icon becomes . - Click to stop a signal tour.
	Click this icon to enter the signal management page. - Select the signal, and then click Add to Signal Group. - Select the default signal group or click Custom Signal Group to add a signal group. - Enter the signal group name, and then click OK.
	Click the icon to lock the position, and then the icon becomes . The window position and size cannot be adjusted. Click to unlock the positions of the window.
	Click the icon to maximize the window, and then the icon becomes . Click to reset.
	Click the icon to close this window.

Step 4 Select one window, drag or double-click the slot to the window, and bind the slot channel with the window.

Figure 4-15 Bind the slot channel with the window



You can click  to select main or sub stream.

Related Operations

- Click  to select the signal sources in batches.
- Click  to add the signal to the group.
- Click  to add signals in batches.
- Hover over the signal, and then click  to crop the image.

4.4.3.2 Scene Management

You can save the video wall layout and windows as a scene, and then configure multiple video scenes to be displayed on the screen in turn.

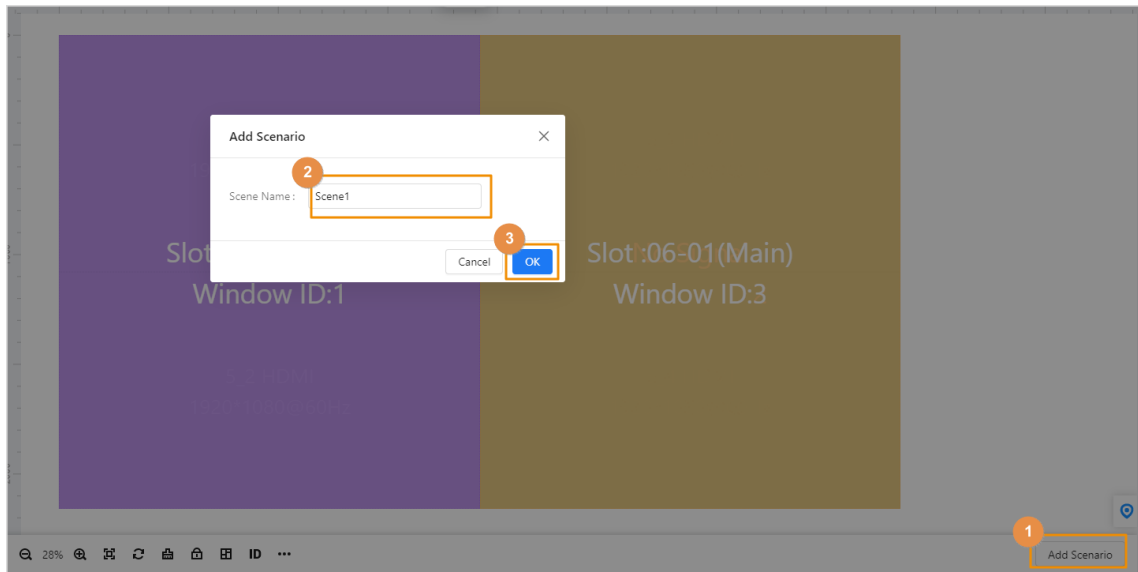
Prerequisites

The video wall layout and windows have been configured.

Procedure

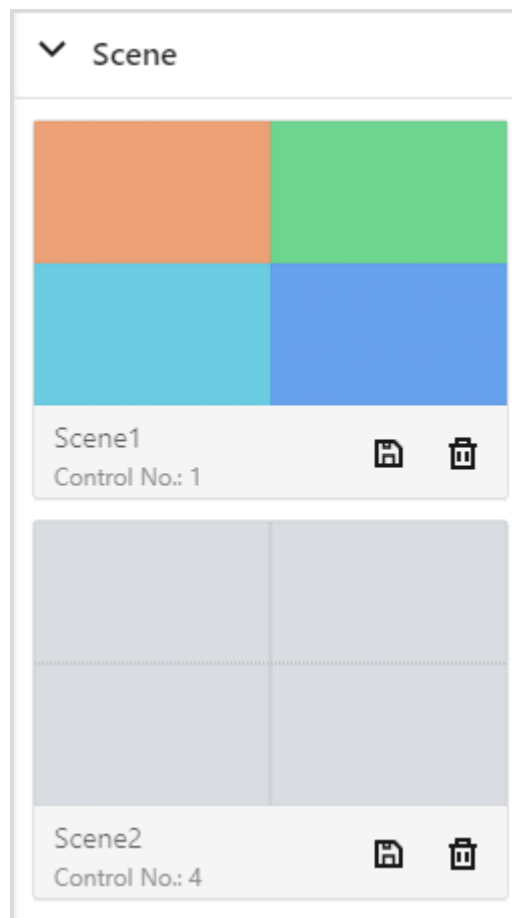
- Step 1 On the main page, select **Video Wall**.
- Step 2 Select **Video Wall Control**, and then click **Add Scenario**.

Figure 4-16 Add scenario



Step 3 Enter the scene name, and then click **OK**.

Figure 4-17 Scene



Related Operations

- Click  to edit scene name or control number.
- Click  to save the video wall display information to this scene.

- Click  to delete the scene.
- Click  to clear all scenes.

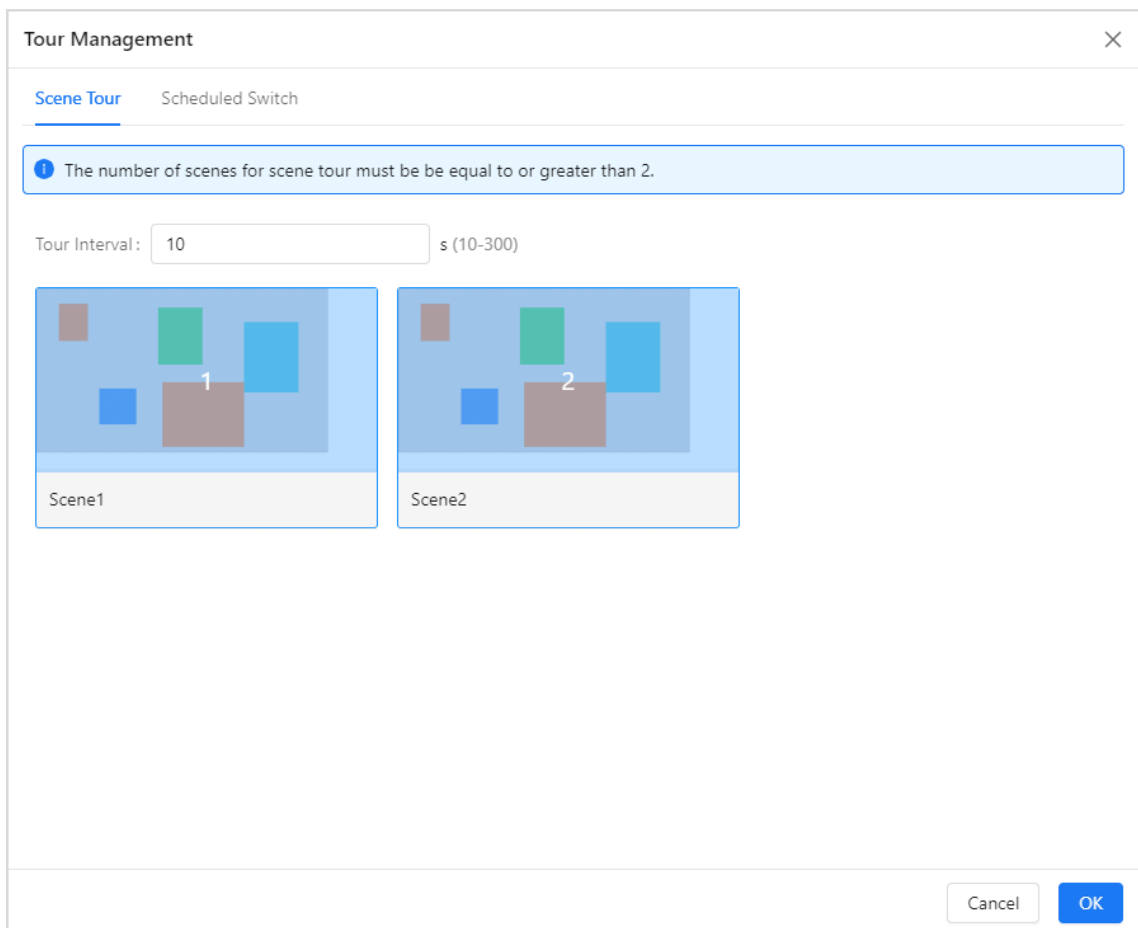
4.4.3.3 Tour Management

Configure the switch time, and then display the scene on the screen in turn.

Scene Tour

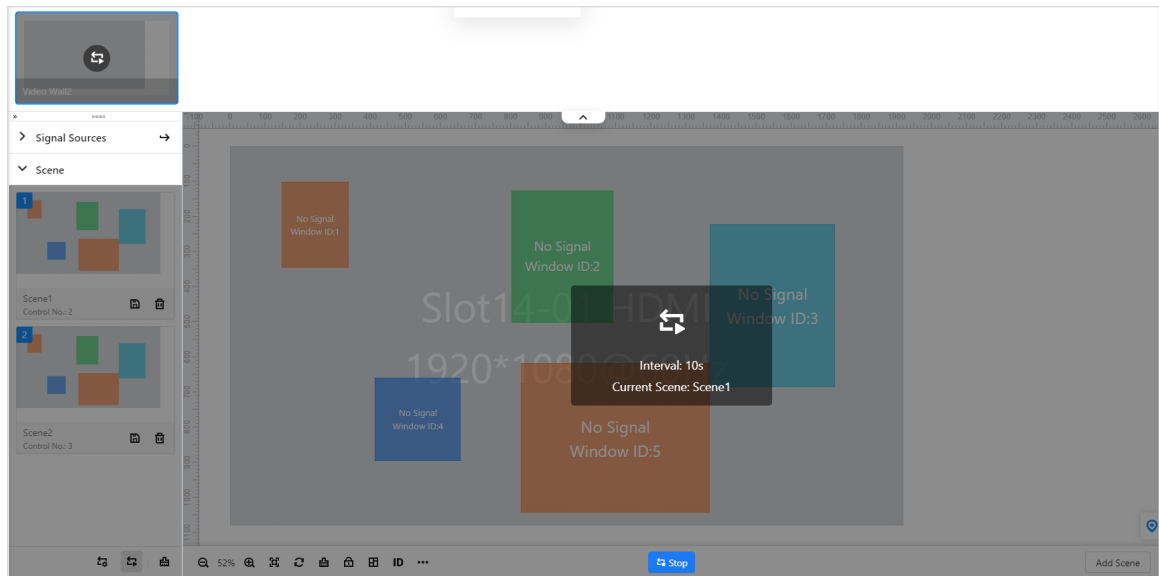
1. On the main page, select **Video Wall** > **Video Wall Control**.
2. Click **Scene**.
3. Click , and then select **Scene Tour**.
4. Configure the **Tour Interval**, select 2 or more scenes, and then click **OK**.

Figure 4-18 Configure scene tour



5. Click  to start scene tour.

Figure 4-19 Scene tour



6. Click **Stop** to exit scene tour.

Scheduled Switch

If a switch time is set for a scene, the system will switch to this scene automatically at the switch time.

1. On the main page, select **Video Wall > Video Wall Control > Tour Management > Scheduled Switch**.

Figure 4-20 Scheduled switch

The screenshot shows the 'Tour Management' window with the 'Scheduled Switch' tab selected. On the left, a list of scenes includes 'Scene111' (highlighted) and 'Scene222'. The main area displays a schedule for 'Scene111' with rows for each day of the week. Sunday and Monday are configured with a green status indicator, a blue toggle switch, and a time of 08:00:00 and 09:00:00 respectively. Tuesday through Saturday are currently off (grey toggle) and have an 'Add Schedule' button. Each row has a 'Copy' link. At the top right are 'Delete' and 'Clear' buttons, and at the bottom right are 'Cancel' and 'OK' buttons.

2. Select a scene, and then click **Add Schedule**.
3. Configure the time, and then click ☑.

Figure 4-21 Configure switch time (1)

This close-up shows the 'Add Schedule' dialog box. It contains a text input field with '08:00' (highlighted with an orange box and labeled '2'), a clock icon, and a checkmark icon (labeled '3'). Below the input field is an 'Add Schedule' button (labeled '1').

Figure 4-22 Configure switch time (2)

You can click to add multiple point-in-time. The new added time schedule is enabled by default, and you can click to disable it.

4. Click **OK**.



After creating a schedule, click **Copy**, select the target time slots, and then click **OK** to quickly duplicate the schedule.

4.4.4 Video Wall Operations

4.4.4.1 Video Wall Settings

Procedure

- Step 1 On the homepage, select **Video Wall** > **Video Wall Control**.
- Step 2 Click *******, and then click **Video Wall Config**. For details, see "4.4.5 Display Management".

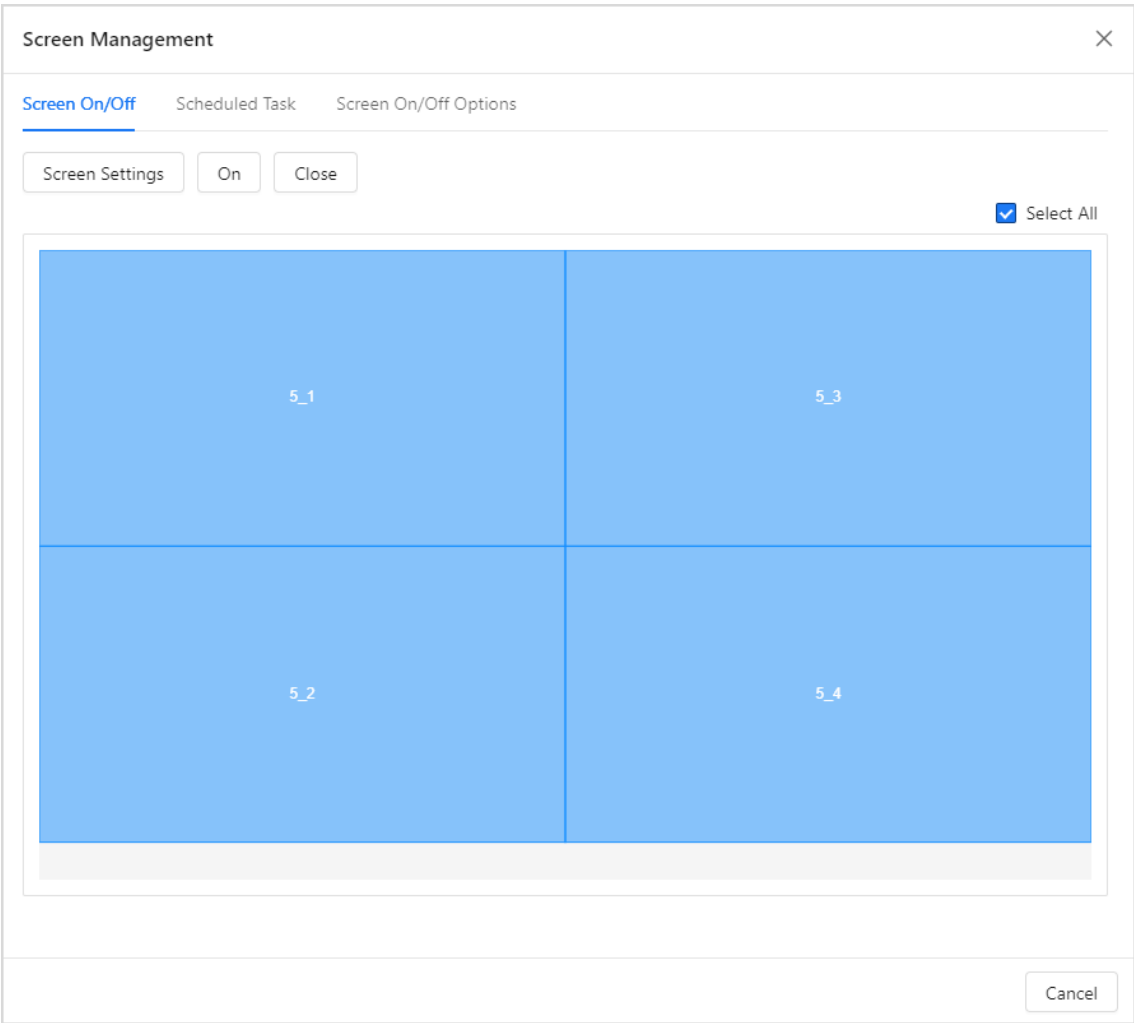
4.4.4.2 Screen Management

Screen On/Off

You can configure screen parameters to turn on and turn off the screen.

On the home page, select **Video Wall** > **Video Wall Control**. Click **⋮**, and then select **Screen Management** > **Screen On/Off**.

Figure 4-23 Screen on/off



- On: Select a screen, and then click **On** to enable the selected screen.
- Off: Select a screen, and then click **Close** to disable the selected screen.

Scheduled Tasks

Configure fixed on/off time for every screen. Within the configured period, every screen will be turned on/off at the fixed time.

1. Click **⋮**, and then select **Screen Management** > **Scheduled Task**.
2. Click **Add Schedule** to add on/off time.

Figure 4-24 Scheduled time

Screen Management

Screen On/Off **Scheduled Task** Screen On/Off Options

Delete Clear

Sunday	☒ On 08:00:00	☐ Close 18:00:00	Copy
Mon	☒ On 07:00:00	☐ Close 18:00:00	Copy
Tue	☒ On 23:00:00	☐ Close 23:07:00	Copy
Wed	☒ On 08:00:00	☐ Close 18:00:00	Copy
Thu	☐	Add Schedule	Copy
Fri	☐	Add Schedule	Copy
Sat	☐	Add Schedule	Copy

Cancel OK

3. Click **OK**.

Screen On/Off Options

According to preset interval and time, the Device sends on/off commands to all screens continuously, and ensures that each screen receives commands and turns on/off.

1. Click , select **Screen Management** > **Screen On/Off Options**.
2. Click ☐ to enable screen on/off options function.

Figure 4-25 Screen on/off options

Screen Management

Screen On/Off Scheduled Task Screen On/Off Options

Control Specif... ☒

On/Off Times : (1-9)

On/Off Interval : ms (1-999)

Interval of Sen... ms (1-999)

Cancel OK

3. Click **OK**.

4.4.4.3 Configuring Background Image

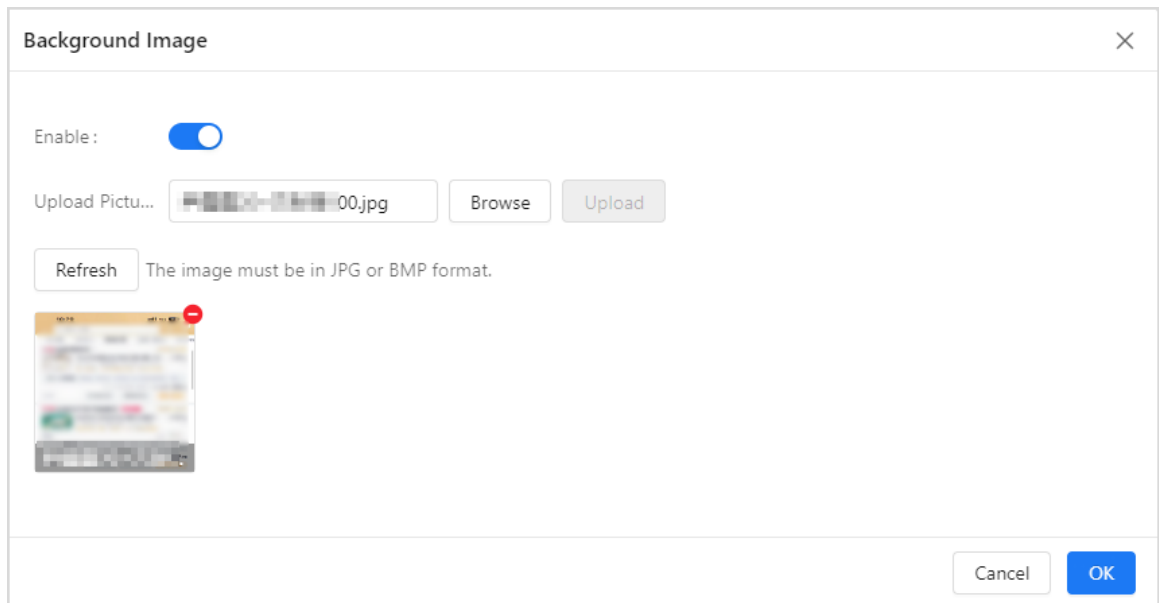
You can upload a picture to the system, and set the uploaded picture to be screen background.

Procedure

Step 1 On the home page, select **Video Wall** > **Video Wall Control**.

Step 2 Click **...**, and then click **Background Image**.

Figure 4-26 Background image



Step 3 Click  to enable background image function.

Step 4 Click **Browse** to select the image, and then click **Upload**.



- The image size cannot exceed 32 MB.
- The supported image formats include JPG and BMP.

Step 5 Click **OK**.

Related Operations

Click **Refresh** to refresh the interface.

4.4.4.4 Configuring Subtitles

Divide a customized area on the video wall, enter any characters, and display them on the screen.

Configuring subtitles

1. On the home page, select **Video Wall** > **Video Wall Control**.
2. Click , and then select **Subtitles**.

Figure 4-27 Subtitles

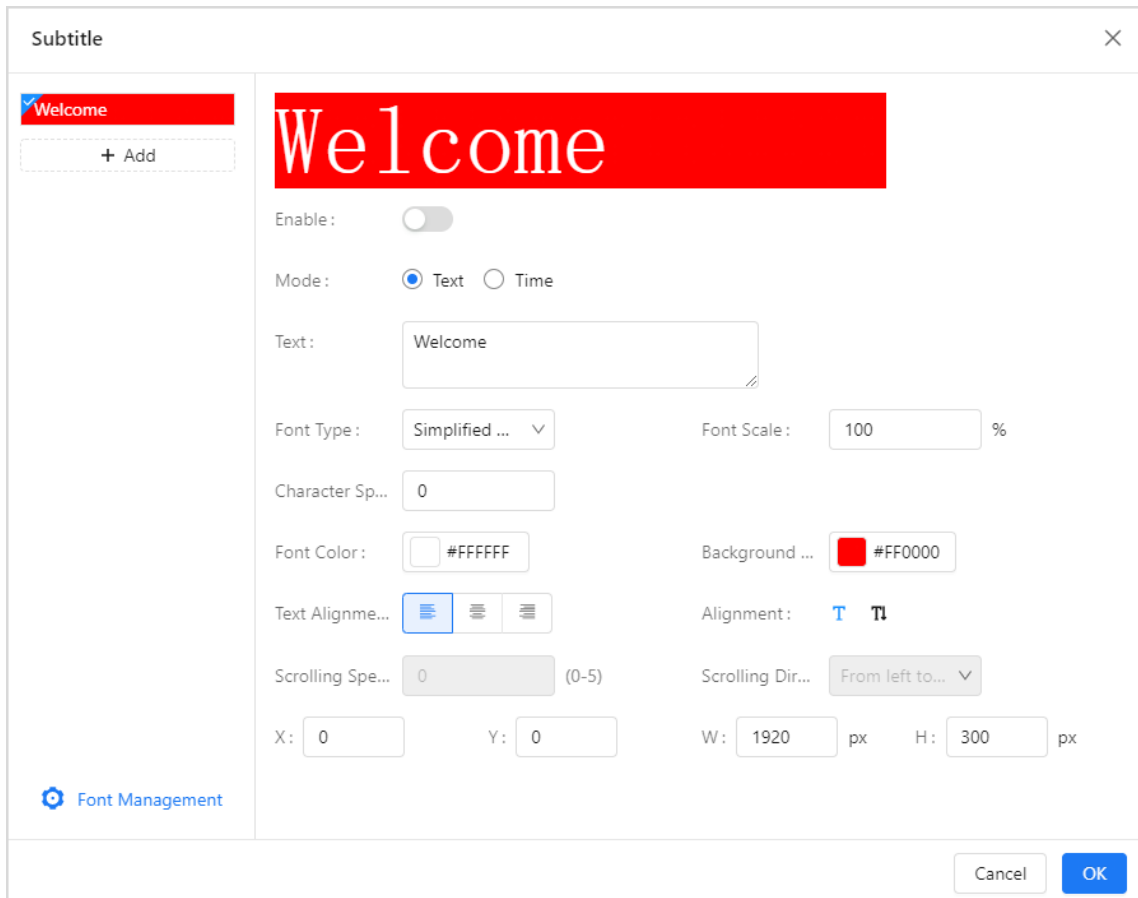


Table 4-7 Parameter description

Parameter	Description
Enable	Click  to enable subtitle function.
Mode	Set the mode of the subtitles. You can choose Text or Time .
Text	Configure the content of the subtitle that will be displayed on the video wall.  When select Time, the text cannot be configured. But you can configure the time format.
W/H	Set the width and height of the subtitle background.
X/Y	Configure the starting coordinates of the subtitles.
Background Color	Enter a 6-digit RGB value, or click the color area to select the color.
Font Type	Select the font type, including Simplified Chinese Song Typeface and Simplified Chinese Boldface .
Font Scale	Set the font scale within a range of 1 to 100.
Character Spacing	Set the character spacing, ranging from 0 to 5.
Font Color	Enter a 6-digit RGB value, or click the color area to select the color.
Text Alignment	Configure the alignment of the text.

Parameter	Description
Alignment	Configure the alignment of the subtitle.

- Click **Add**, and then configure the subtitle parameters.



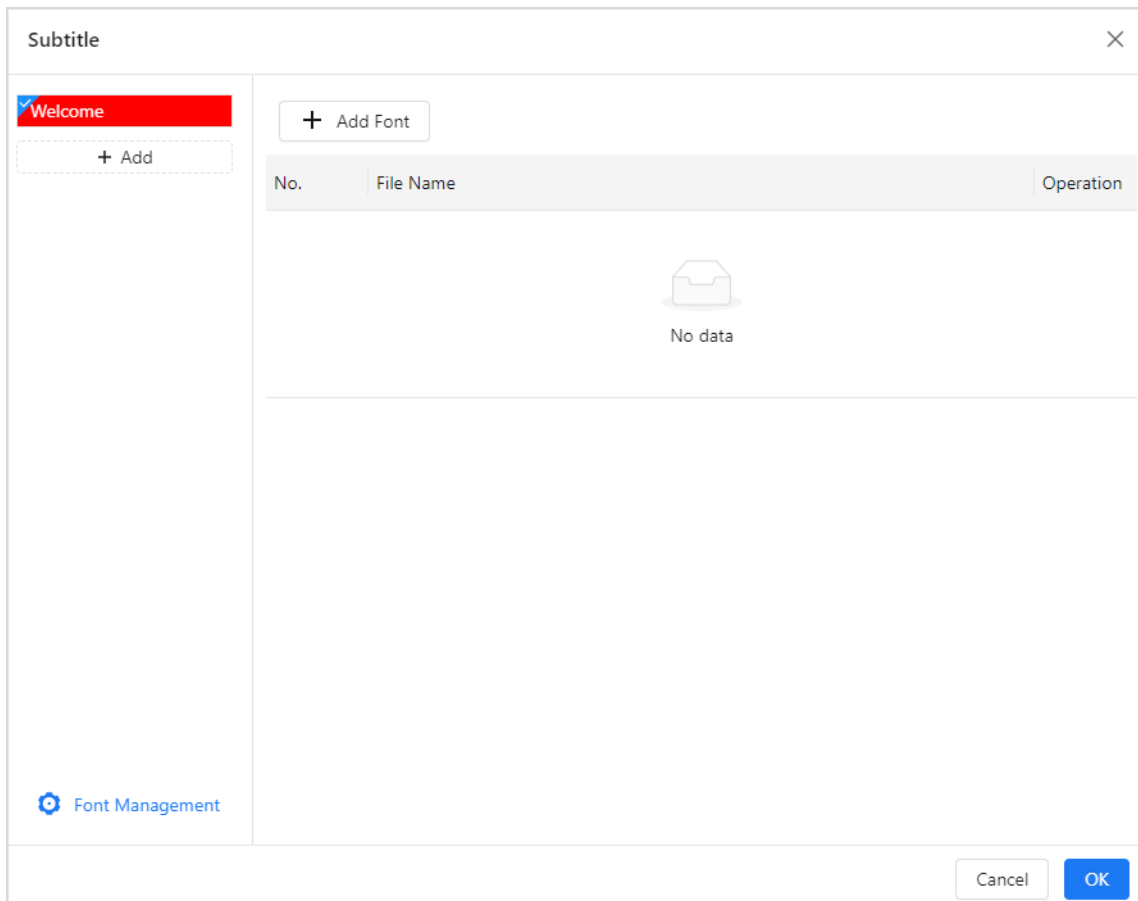
- You need to enable **Scrolling Subtitles** first on the performance strategy tab, and then you can configure scrolling speed and scrolling direction.
- When selecting the subtitle mode as **Time**, scrolling playback cannot be configured.

- Click **OK**.

Font Management

- On the management page, select **Video Wall** > **Video Wall Control**.
- Click **...**, and then select **Subtitles**.
- Click **Font Management**.

Figure 4-28 Font management



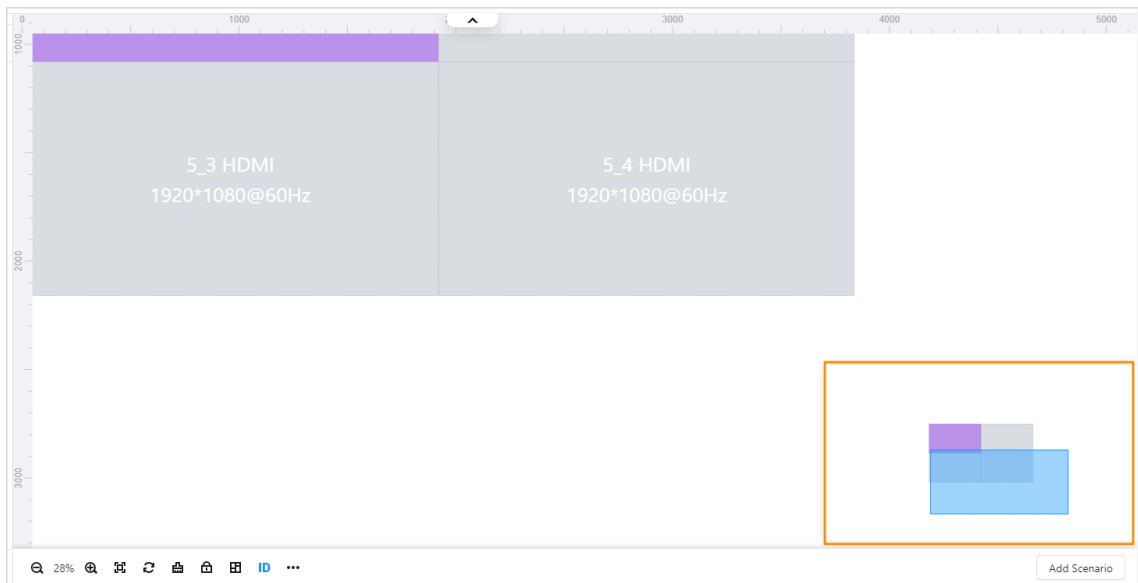
- Click **Add Font** to select font package, and then click **Upload**.

4.4.4.5 Eagle Eye

Eagle eye map, also known as thumbnail, is used to adjust the display size and display area of the main window of the web screen.

On the **Video Wall Control** page, move the mouse to , and then the eagle eye map appears. You can change the main window display area size with mouse or wheel button. Drag the blue box in the eagle eye map to change main window display area.

Figure 4-29 Eagle eye



4.4.5 Display Management

4.4.5.1 Screen Settings

You can configure manufacturer, serial port and serial port address for every output screen, in order to realize communications between screen and Device. The serial port address must be the same as the DIP address of the connected screen.

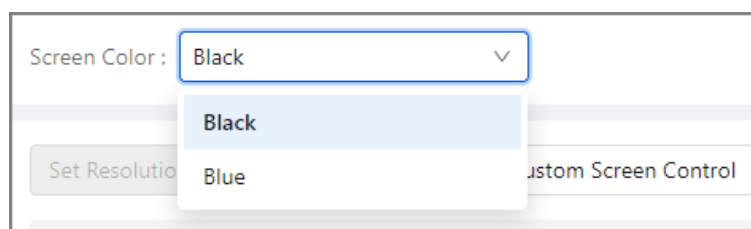
Procedure

Step 1 On the main page, select **Display Management** > **Output Conifg** > **Output Config**.

Step 2 Configure the screen color and window color.

Select color from the drop-down list.

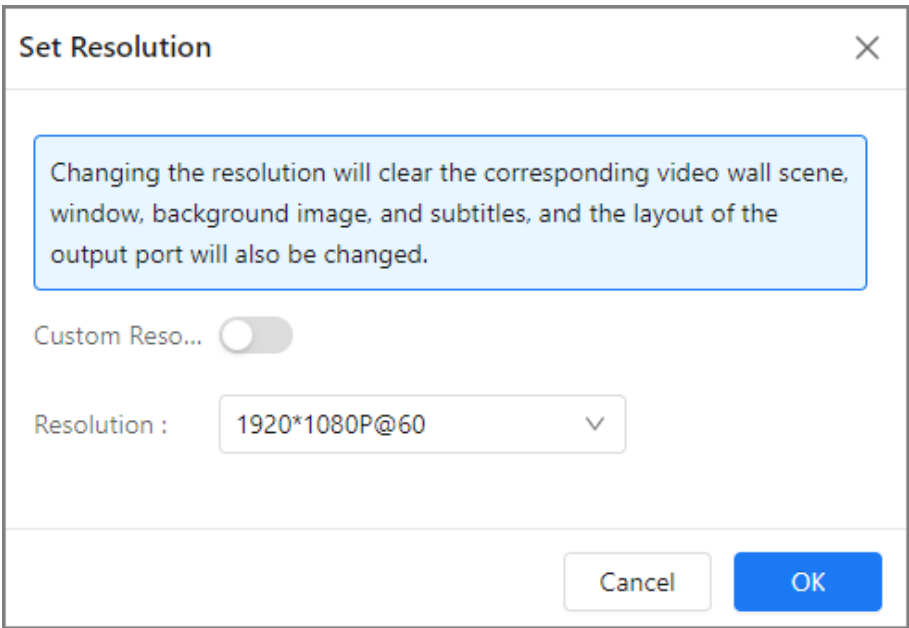
Figure 4-30 Configure the screen color/window color



Step 3 Configure the control number, color space mode, manufacturer, and serial port according to your actual needs.

Step 4 Click  to configure the resolution.

Figure 4-31 Resolution



- You can select the fixed resolution from the drop-down list. The default resolution is 1920 × 1080.
- Click  to enable custom resolution, and then you can configure the resolution according to your needs.

Step 5 Click  to configure screen color.

Figure 4-32 Configure screen color



Table 4-8 Parameter description

Parameter	Description
Hue	Drag the slider to adjust the image hue.

Parameter	Description
Brightness	Drag the slider to adjust the image brightness through linear adjustment. The bigger the value is, the brighter the image will become. And vice versa. However, the image is likely to become dim if the value is too big.
Contrast	Configure the contrast of the image.
Saturation	Drag the slider to adjust the color shades. The bigger the value is, the darker the color will become. And vice versa. This value does not affect the overall brightness of image.

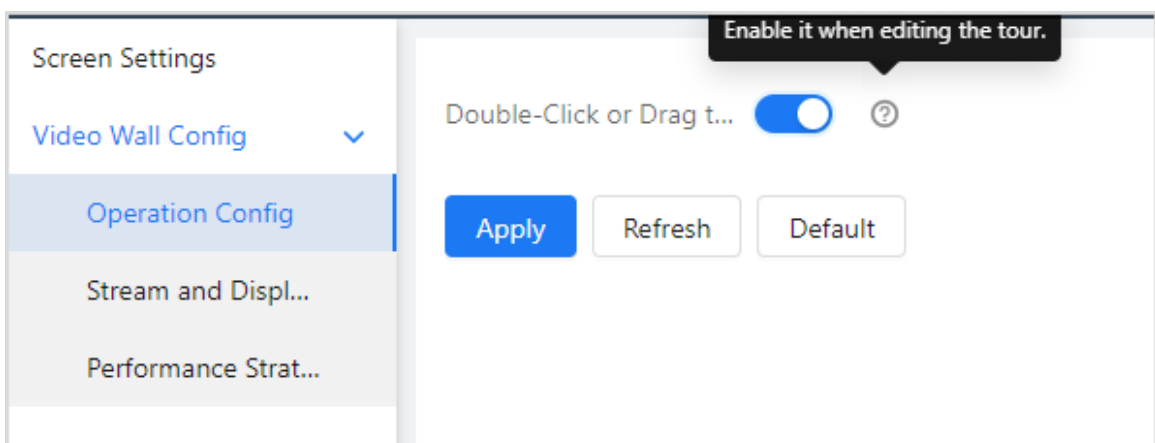
Step 6 Click **Apply**.

4.4.5.2 Video Wall Configuration

Operation Configuration

1. On the main page, select **Display Management > Video Wall Config > Operation Config**.

Figure 4-33 Operation configuration



2. Click ☐ to enable **Double-Click or Drag to Add Signal Source**.



- After enabling this function, you can add another signal source to the window that there already has a signal.
- Enable this function when editing the tour.

3. Click **Apply**.

Stream and Display Strategies

1. On the main page, select **Display Management > Video Wall Config > Stream and Display Strategies**.

Figure 4-34 Stream and display strategies

Stream Strategies

Sub Card Acquires Stre... ☒

Sub Card Acquires Stre... ☐

Network Signal Smoot... 240 (40-1000) ?

Auto Switch Between ... ☐

Semi-Transcoding of S... ☐ ?

No RTP Streaming : ☐ ?

Display Strategies

On-Screen Prompt : ☐

Keep Last Frame When... ☒

Neat Scene Switching : ☐ ?

Table 4-9 Parameter description

Parameter	Description
Sub Card Acquires Streams from Platform	Click ☐ to enable this function, and then the sub board will acquire stream from the platform.
Sub Card Acquires Streams from Front-End Devices	Click ☐ to enable this function, and then the sub board will acquire stream from the front-end devices.
Network Signal Smoothness	Drag the slider to adjust the smoothness of the network signal.
Auto Switch Between Main and Sub Stream	If main stream is displayed on the window, when the resolution is lower than D1, main stream will automatically switch to sub stream.
Semi-Transcoding of Streaming Media Database	The stream media library does not encapsulate streams but pass streams to devices for decoding.  Enable it when the stream SDP information of the streaming scene is not standard.
No RTP Streaming	After you enable this function, streams without RTP head can be decoded and displayed on the wall.  ● Enable it when the stream does not have an RTP header. ● This function cannot be used together with audio/video encryption.

Parameter	Description
On-Screen Prompt	Prompt information will be displayed on the window.
Keep Last Frame When Switch Scene	Keep the last frame when switching schemes to avoid black screen.  Only suitable for fixed split or full-screen scene switching.
Neat Scene Switching	Scene stream will be switched synchronously and neatly, to enhance the visual effect.  The function is only supported by splicing screen. For a better experience, please enable Keep Last Frame function.

- Click  to enable the corresponding functions according to actual needs.
- Click **Apply**.

Performance Strategies

- On the main page, select **Display Management > Video Wall Config > Performance Strategies**.

Figure 4-35 Performance strategies

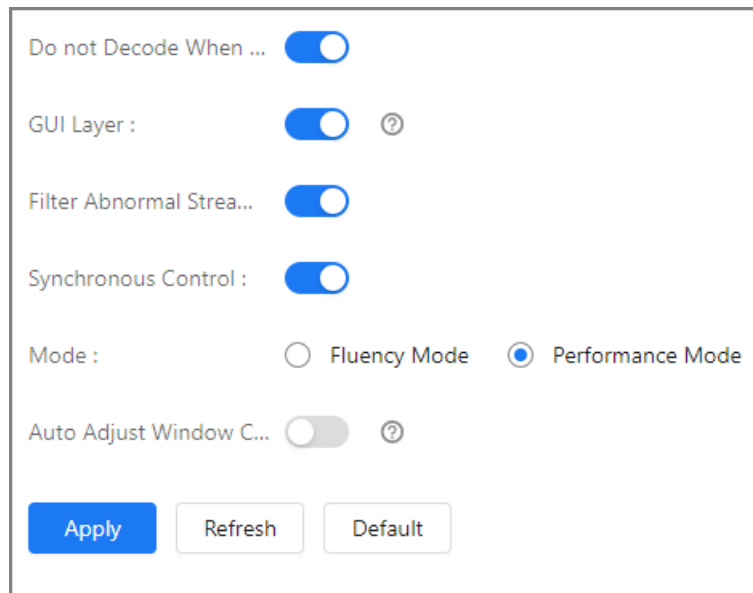


Table 4-10 Parameter description

Parameter	Description
Do not Decode When Video is Overwritten	The covered window will pause decoding.

Parameter	Description
GUI Layer	When this function is not enabled, only video images can be displayed on the output screen. The screen number and virtual LED functions cannot be used. If you need to decode 8K videos and have 4K display output simultaneously, please disable the GUI function.  Disable this function when using 4K display output. After disabling this function, certain functions such as screen ID and subtitles cannot be used.
Filter Abnormal Streams	The system checks and filters abnormal stream, in order to prevent green screen.
Synchronous Control	Enable this function, and then you can configure the Fluency Mode and Performance Mode. ● Fluency mode: There might be an issue with the image not being synchronized when dragging it across the screen. However, selecting fluency mode will increase the frame rate to ensure that the image is synchronized. ● Performance mode: When streaming across screens, there may be issues with picture synchronization. After selecting performance mode, the frame rate will be lowered to ensure the images are synchronized.
Auto Adjust Window Coordinates	Automatically adjust the edge coordinates of the window.

2. Click  to enable the corresponding functions according to actual needs.

3. Click **Apply**.

4.4.6 Network Configurations

4.4.6.1 TCP/IP

You can bind the IP and MAC address of the Device to reduce the risk of ARP (Address Resolution Protocol) deception.

Procedure

Step 1 On the main page, select **Network Settings** > **TCP/IP**.

Step 2 Select a NIC card, and then click  to configure the network parameter, and then click **OK**.

Figure 4-36 Network parameter

Edit
✕

NIC Name : Link Aggregation (NIC 1+2)

Binding Mode : ☒ Link Aggregation

IP Version : IPv4 ▼

Mode : ☐ DHCP ☒ Static

IP Address : Test

Subnet Mask :

Default Gatew...

NIC Name	MAC Address	Speed
☒ NIC 1	aa:aa:aa:aa:aa:aa	2500M
☒ NIC 2	aa:aa:aa:aa:aa:aa	2500M

Cancel OK

Table 4-11 Parameter description

Parameter	Description
Binding Mode	Link Aggregation: When the NIC is bound for communication with the outside world, the bound NICs participate in the workload and share the network load. Based on the user-configured port load balancing policy, packets are sent from a member port to the peer switch. If a link on one member port becomes faulty, the system stops sending packets through that port and recalculates the port for sending packets based on the load balancing policy using the remaining links. Once the faulty port recovers, the system recalculates the port for sending packets again.
IP Version	It is IPv4 by default.

Parameter	Description
Mode	Select the DHCP check box, the system automatically obtains an IP address. • Static: You need to configure the IP address, subnet mask, and gateway manually. • DHCP: The IP address, gateway, and subnet mask cannot be set manually. ◇ If DHCP is effective, the obtained information will be displayed in the IP Address box, Subnet Mask box and Gateway box. If DHCP is not effective, they all display 0. ◇ To view manually set IP when DHCP is not effective, you shall disable DHCP first, and then the device will display IP information that is not obtained through DHCP. If DHCP is effective, if DHCP is not enabled, static IP information will restore default settings. You need to configure IP again.
IP Address	Enter numbers to change the IP address, and then configure its Subnet Mask and Gateway.  Click Test to test if the IP address can be used in order to avoid IP conflict.
Subnet Mask	
Default Gateway	

Step 3 Click **Apply**.

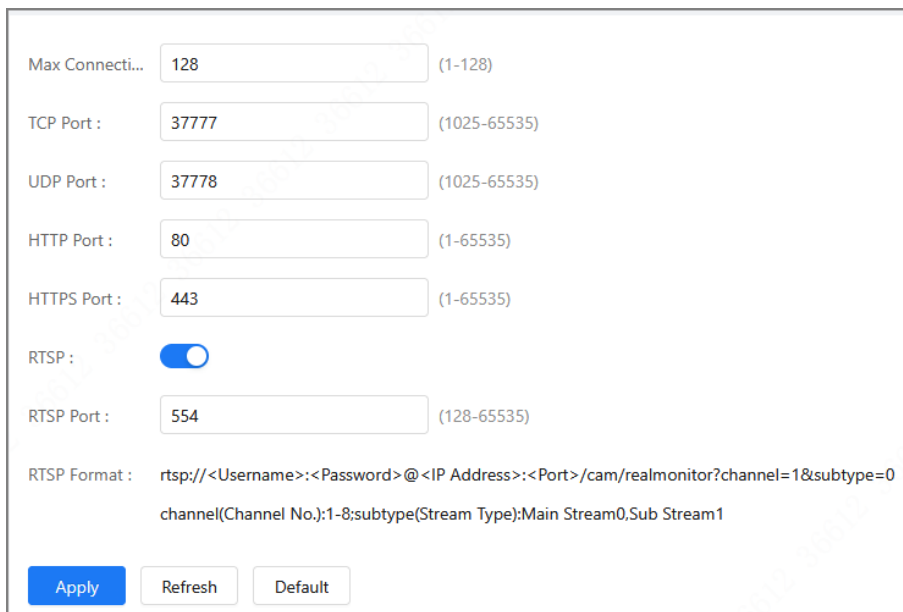
4.4.6.2 Port

You can configure the maximum connections and port to access the Device through the clients (including web client and computer client).

Procedure

Step 1 On the main page, select **Network Settings > Port**.

Figure 4-37 Port



Max Connecti... 128 (1-128)

TCP Port : 37777 (1025-65535)

UDP Port : 37778 (1025-65535)

HTTP Port : 80 (1-65535)

HTTPS Port : 443 (1-65535)

RTSP : ☒

RTSP Port : 554 (128-65535)

RTSP Format : rtsp://<Username>:<Password>@<IP Address>:<Port>/cam/realmonitor?channel=1&subtype=0
channel(Channel No.):1-8;subtype(Stream Type):Main Stream0,Sub Stream1

Apply Refresh Default

Table 4-12 Parameter description

Parameter	Description
Max Connection	The allowable maximum number of clients accessing the Device at the same time, such as web, platform, and mobile phone. The default value is 128.
TCP Port	TCP service port. The default setting is 37777. You can configure this parameter.
UDP Port	User Datagram Protocol port. The default value setting is 37778. You can enter the value.
HTTP Port	Hyper Text Transfer Protocol port. The default setting is 80. You can enter the value according to actual situation, and in this case, add the modified port number after the address when you log in to the Device on the browser.
RTSP Port	Select Enable RTSP.  RTSP port can be enabled only when the Device is equipped with encoding cards including HD and UHD encoding cards. • Real Time Streaming Protocol port. Keep the default value 554 if it is displayed. If you play live view through Apple's QuickTime or VLC, the following format is available. • Username: username, for example admin. • Password: password, for example admin. • IP: The Device IP • Port: It is 554 by default. Keep it as default. • Channel: channel number, starting from one. In case of channel 2, channel=2. • Subtype: stream type. The main stream is zero (subtype=0), the sub stream is one (subtype=1). • For example, if you acquire the sub stream of channel two from a certain device, then the URL should be: rtsp://admin:admin@192.168.1.1/cam/realmonitor? channel=2&subtype=1 If certification is not required, you do not need to specify the username and password. Use the following format: rtsp://ip:port/cam/realmonitor?channel=1&subtype=0

Step 2 Configure the port parameters, and then click **Apply**.

4.4.7 System Management

4.4.7.1 Basic Settings

On the main page, select **System** > **General Config** > **Basic Settings**. Configure the parameters, and then click **Apply**.

Figure 4-38 Basic settings

Device Name : N70

Language : ENGLISH

Apply Refresh Default

- Device Name: Customize the device name to differentiate it from others.
- Language: The system language is determined by program package, and cannot be configured here.

4.4.7.2 Date and Time

Procedure

- Step 1 On the main page, select **System** > **General Config** > **Data & Time**.
- Step 2 Configure the parameters according to actual needs.

Figure 4-39 Configure the parameters

Time and Time Zone

Date : 2000-01-01 Saturday

Time : 01:59:56

Time : ☒ Manual Settings ☐ NTP

System Time : 2000-01-01 01:59:56 Sync PC

Time Format : YYYY-MM-DD 24-Hour

Time Zone : (UTC+08:00) Beijing, Chon...

Correct Remote D... ☐

Table 4-13 Parameter description

Parameter	Description
Time	• Manual Settings : Set the system time manually. • NTP : Enable NTP time server to ensure that system time, network devices, and computer time are kept accurate and synchronized.
System Time	Configure the system time. Click Sync PC to synchronize with current computer time.
Time Format	Select time display format.
Time Zone	Select time zone.

Parameter	Description
Correct Remote Device Time	Click ☐ to correct the time of remote devices.

Step 3 Click **Apply**.

4.4.7.3 Account

User management adopts two-level management mode: User and user group. You can manage basic information. Only those with user management authority can operate user management.

Background Information

- User name and group name support maximum 6 characters and can only be consisted of letter, number, and underline (_).
- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &). The user with authority can modify not only his/her own password, but also modify the password of other users.
- According to factory defaults, maximum user quantity is 64, and maximum user group quantity is 20.
- Group name and user name shall be unique. One user can only belong to one group.
- Current user cannot modify his/her own authority.
- During initialization, there is 1 default user—admin. Admin is defined as high-authority user when leaving factory.

Procedure

Step 1 Add user groups.

1. On the main page, select **System > Account**.
2. Click **+** to add a user group.

Figure 4-40 User group

3. Enter the user group name, and then click **OK**.

Step 2 Add users.

1. Select a user group, and then click **Add**.

Figure 4-41 Add users

The 'Add' dialog box has a title bar with a close button. Inside, there are four main input areas: 'Username' with the value '111', 'Password' with the value 'minmin123' and a strength indicator (two orange bars), 'Group' with a dropdown menu showing '111', and 'Remarks' with an empty text box. A 'Confirm Pass...' field with masked characters and a toggle icon is also present. At the bottom right, there are 'Cancel' and 'OK' buttons.

2. Configure the username, password and confirm the password, and then click **OK**.

Related Operations

- Select password expiration time includes **Never**, **30**, **60**, **90**, **180**, or **Custom**. If **Custom** is select, configure the expiration time.

Figure 4-42 Expiration time

The 'Password Expi...' section features a dropdown menu currently set to 'Custom'. Next to it is a text input field containing the number '180'. To the right of this field, the text 'Days (0-180)' indicates the valid range for the value.

- Click  to change password.

4.4.7.4 Fan Control

You can configure fan temperature control and fan speed.

1. Select **System** > **Fan Control**.

Figure 4-43 Fan control

The 'Fan Control' window displays a status message at the top. Below it, the 'Fan Mode' is set to 'General Mode' via a radio button. The 'Fan Group1' section shows three temperature thresholds: 'Low Speed' at 50 °C, 'Medium' at 70 °C, and 'High Speed'. At the bottom, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

2. Select **Case Fan Mode**, and configure the fan speed and temperature for every fan group.
 - **General Mode** : There are three levels: low speed, medium speed, and high speed. Different temperature ranges correspond to different speeds. The system will trigger different fan speed levels according to the different temperature ranges. The higher the temperature, the faster the fan speed.
 - **Meeting Mode** : In meeting mode, the fan operates at low speed.
3. Click **Apply**.

4.4.7.5 Buzzer Configuration

Select **System** > **Buzzer Config**, configure the buzzing duration, and then click **Apply**.

Figure 4-44 Buzzer configuration

If the time is set to 0, the buzzer will be turned off. If it is set to 600, the buzzer will continuously beep.

Buzzing Durat... s (0-600)



Click **Turn off Buzzer** to turn off the current beep.

4.4.7.6 Serial Port

After serial port parameters are set, the video matrix platform can connect to other devices through com ports, for the purpose of debugging and operation.

1. Select **System** > **Serial Port**.

Figure 4-45 Serial port

Slot :	Main Control Card	▼
Channel :	1	▼
Serial Port Typ...	232	▼
Function :	MonitorSwitch	▼
Data Bit :	8	▼
Stop Bit :	1	▼
Baud Rate :	115200	▼
Parity :	None	▼
Address :	1	(1-255)
Apply Refresh Default		

Table 4-14 Parameter description

Parameter	Description
Slot	Select the slot and channel you want to configure.
Channel	
COM Type	It is 232 by default.
Function	Configure the serial port function.
Data Bit	Select a data bit. The options include 5, 6, 7 and 8.
Stop Bit	Select the stop bit of the serial port including 1 and 2.
Baud Rate	Configure the baud rate of the serial port. It must be consistent with the device that will be connected.
Parity	Select a parity mode from None , Odd , Even , Mark and Space .
Address	Configure the serial port address, which ranges from 1 to 255.

2. Configure the parameters, and then click **Apply**.

4.4.8 Security

4.4.8.1 System Service

4.4.8.1.1 Basic Services

Enable the services according to actual needs.

1. Select **Security** > **System Service** > **Basic Services**.

Figure 4-46 Basic services

The screenshot shows the 'Basic Services' configuration interface. At the top, there are tabs for 'Basic Services' and 'HTTPS'. Below the tabs, the following settings are visible:

- SSH :** A toggle switch that is currently turned off (disabled).
- Private Protocol :** A toggle switch that is currently turned on (enabled).
- Private Protocol Authentication...**: A dropdown menu showing 'Security Mode (Recommen...' with a downward arrow.
- Multicast/Broadcast Search :** A toggle switch that is currently turned on (enabled).
- CGI :** A toggle switch that is currently turned on (enabled).

At the bottom of the configuration area, there are three buttons: a blue 'Apply' button, a 'Refresh' button, and a 'Default' button.

2. Enable the services according to actual needs.

Table 4-15 Service description

Parameter	Description
SSH	The remote debugging function can be enabled for technical personnel.
Private Protocol	Enable the private protocol.
Private Protocol Authentication Mode	Select the authentication mode.
Multicast/Broadcast Search	Enable the function.
CGI	Encrypt before requesting video service from video server.

3. Click **Apply**.

4.4.8.1.2 HTTPS

Through creating server certificate or downloading root certificate on the HTTPS page, you can log in to the PC by HTTPS, to ensure the security of communication data, and guard the users' information and device security with stable technology measure.

Using HTTPS, you need to download root certificate.

1. Select **Security > System Service > HTTPS**.
2. Click ☐ to enable HTTPS.

Figure 4-47 HTTPS

Basic Services **HTTPS**

Enable: ☒

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service and RTSP access service.

Auto Redirect to H...: ☒

*Select a device certificate

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1		343633 66353832393 436363	2000-12-31 00:21:16	00000000000000000000	General Device Matrix CA	HTTPS, RTSP over TLS

Apply Refresh Download Root Certificate Default

3. Click ☐ to enable redirect to HTTPS automatically.
4. Click **Apply**.

4.4.8.2 Attack Defense

Configure the firewall and anti-DoS attack to enhance security management.

Firewall

1. On the main page, select **Security > Attack Defense > Firewall**.

Figure 4-48 Firewall

2. Click to enable firewall.
3. Select **Blocklist** or **Allowlist** to configure the blocklist or allowlist.

The configuration of blocklist is similar to allowlist. We use allowlist configuration as an example.

4. Select the mode as **Allowlist**.
5. Click **Add**, and then configure the parameters.

Figure 4-49 Add allowlist

- Add mode: Supports IP, IP segment, MAC address and all IP.
 - IP Version: It is IPv4 by default.
 - All Device Port: After enabling the function, there is no need to enter the start port and end port. After disabling it, you will need to enter the start port and end port.
6. Click **OK**.
 7. Select the allowlist, and then click **Apply**.

Anti-Dos Attack

1. On the main page, select **Security** > **Attack Defense** > **Anti-DoS Attack**.

Figure 4-50 Anti-DoS Attack

SYN Flood Attack Defense : ☒

An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.

ICMP Flood Attack Defense : ☒

An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

[Apply](#) [Refresh](#) [Default](#)

2. Click ☒ to enable **SYN Flood Attack Defense** or **ICMP Flood Attack Defense**.

- **SYN Flood Attack Defense** : An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.
- **ICMP Flood Attack Defense** : An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

3. Click **Apply**.

4.4.8.3 CA Certificate

4.4.8.3.1 Installing Device Certificate

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with your PC.

Creating Certificate

Create certificate in the device.

Procedure

Step 1 Select **Security** > **CA Certificate**.

Step 2 Click **Install Device Certificate**.

Figure 4-51 Install device certificate

System Service

Attack Defense

CA Certificate

A/V Encryption

Security Warning

Security Authentication

Device Certificate Trusted CA Certificates

A device certificate is a proof of device legal status. For example, when the browser is visiting device via HTTPS, the device certificate shall be verified.

[Install Device Certificate](#) [Enter Edit Mode](#)

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by	Certificate Status	Default	Download	Delete
1										

Step 1: Select installation mode.

☐ Create Certificate

Fill in certificate information, and the device will create and issue the certificate.

☒ Apply for CA Certificate an...

After you fill in certificate information, the device will generate a certificate request file. Please submit the file to a CA institute to apply for a signature and certificate, and then import them into the device.

☐ Install Existing Certificate

If you already have a certificate and private key file, please import the certificate and private key file in this way.

[Next](#) [Cancel](#)

Step 3 Select **Create Certificate**, and then click **Next**.

Step 4 Enter the certificate information.

Step 5 Click **Create and install certificate**.

After the certificate is created successfully, you can view the created certificate on the **Device Certificate** page.

Related Operations

- Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

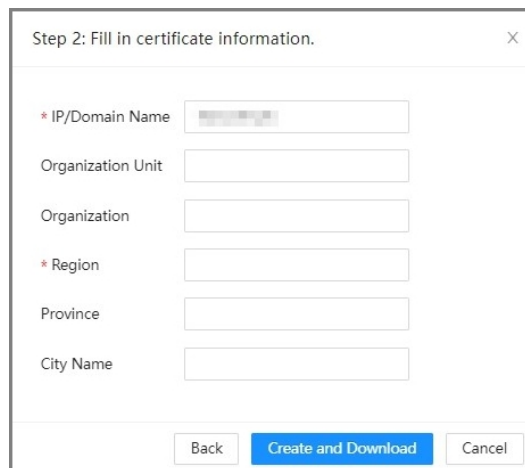
Applying for and Importing CA Certificate

Import the third-party CA certificate to the device.

Procedure

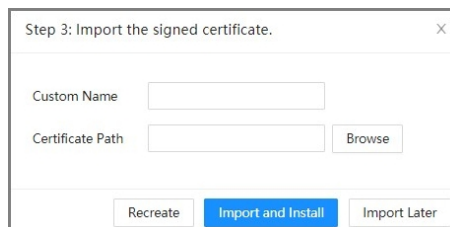
- Step 1 Select **Security > CA Certificate > Device Certificate**.
- Step 2 Click **Install Device Certificate**.
- Step 3 Select **Apply for CA Certificate and Import (Recommended)**, and then click **Next**.
- Step 4 Enter the certificate information.

Figure 4-52 Certificate information (2)



- Step 5 Click **Create and Download** and save the request file to your computer.
- Step 6 Use the request file to apply for a CA certificate with a third-party certificate authority.
- Step 7 Click **Browse**, and then open the CA certificate.

Figure 4-53 Import a CA certificate



- Step 8 Click **Import and Install**.

Related Operations

- Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

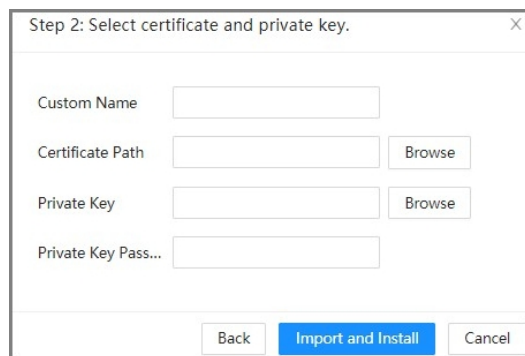
Installing Existing Certificate

Import the existing third-party certificate to the camera. When applying for the third-party certificate, you also need to apply for the private key file and private key password.

Procedure

- Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.
- Step 2 Select **Install Device Certificate**.
- Step 3 Select **Install Existing Certificate**, and then click **Next**.
- Step 4 Click **Browse** to open the CA certificate and private key, and enter the private key password.

Figure 4-54 Certificate and private key



- Step 5 Click **Import and Install**.

After the certificate is created successfully, you can view the created certificate on the **Device Certificate** page.

Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

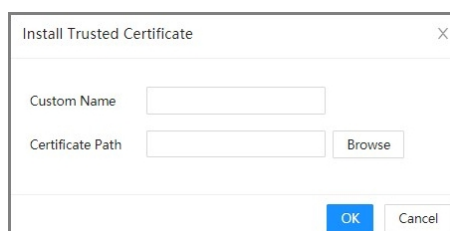
4.4.8.3.2 Installing Trusted CA Certificate

A CA certificate is a digital certificate for the legal identity of the device.

Procedure

- Step 1 Select **Security** > **CA Certificate** > **Trusted CA Certificates**.
- Step 2 Select **Install Trusted Certificate**.
- Step 3 Click **Browse** to open the certificate.

Figure 4-55 Installing trusted certificate



- Step 4 Click **OK**.

After the certificate is created successfully, you can view the created certificate on the **Trusted CA Certificate** page.

Related Operations

- Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

4.4.8.4 A/V Encryption

The device supports encrypting data during audio and video transmission.



We recommend enabling the A/V Encryption function. Otherwise, there might be safety risks.

Procedure

- Step 1** Select **Security** > **A/V Encryption**.
- Step 2** Configure the parameters.

Figure 4-56 A/V encryption

The screenshot shows the 'A/V Encryption' configuration page. On the left is a sidebar with navigation links: System Service, Attack Defense, CA Certificate, **A/V Encryption**, Security Warning, and Security Authentication. The main content area is titled 'Encrypted Transmission'. It has two sections: 'Private Protocol' and 'RTSP over TLS'. Both sections have an 'Enable' toggle switch turned on. Below the 'Private Protocol' toggle, there is a blue box stating 'Stream transmission is encrypted by using private protocol.' and an orange box with a warning: '*Please make sure that the corresponding device or software supports video decryption.' Below this, there are dropdowns for 'Encryption Type' (set to AES256-OFB) and 'Update Period of S...' (set to 12 hr (0-720)). The 'RTSP over TLS' section also has a blue box stating 'RTSP stream is encrypted by using TLS tunnel before transmission.' and an orange warning box. Below this is a section titled '*Select a device certificate' with a 'Certificate Management' link. It contains a table with columns: No., Custom Name, Certificate Serial Number, Validity Period, User, Issued by, and Used by. One certificate is selected (No. 1). At the bottom are 'Apply', 'Refresh', and 'Default' buttons.

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1		36635383239	2000-12-31 00:21:16	00000000000000000000	General Device Matrix CA	HTTPS, RTSP over TLS

Table 4-16 Parameter description

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol.  There might be safety risk if this service is not enabled.
	Encryption Type	Use the default setting.

Area	Parameter	Description
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS.  There might be safety risk if this service is not enabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For details about certificate management, see "4.4.8.3 CA Certificate".

Step 3 Click **Apply**.

4.4.8.5 Security Warning

The device monitors exceptions and triggers a warning when one occurs.

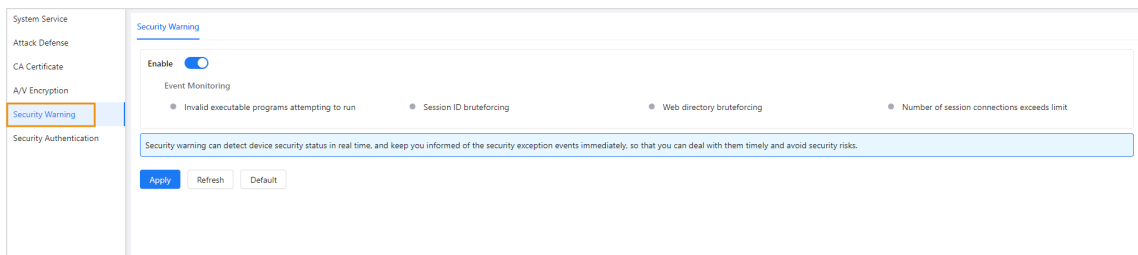
Procedure

Step 1 Select **Security** > **Security Warning**.

Step 2 Click  to enable the function.

Step 3 Configure the parameters.

Figure 4-57 Security warning



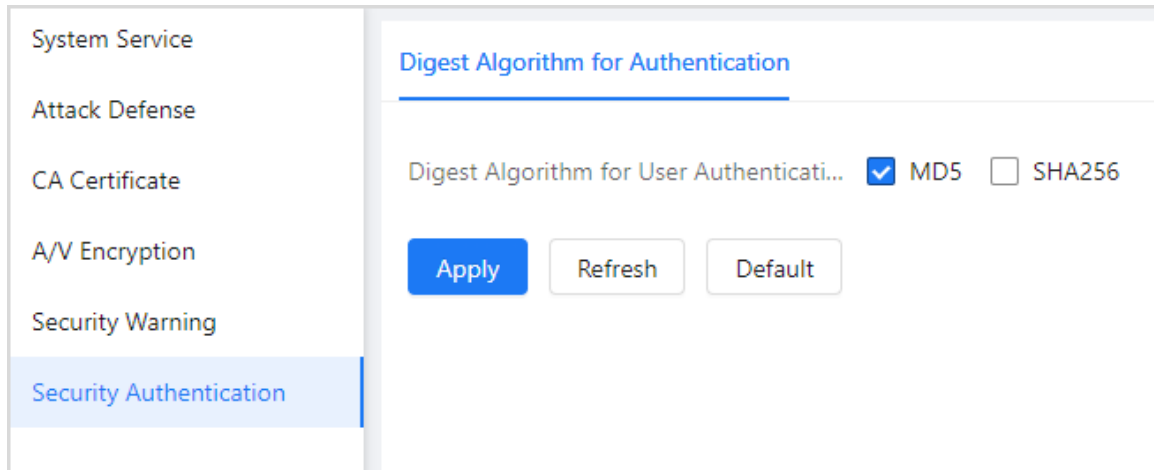
Step 4 Click **Apply**.

4.4.8.6 Security Authentication

Authenticating user identity and ensuring secure algorithms for authentication information

Select **Security** > **Digest Algorithm for User Authentication**, and then select a digest algorithm.
Click **Apply**.

Figure 4-58 Authentication



4.4.9 Maintenance Center

4.4.9.1 Overview

Click **Overview** to view the storage status, CPU status, power supply status, fan status, and network status.

4.4.9.2 System Information

Device Information

Select **System Info** > **Device Info** to view the device information such as device type.

Figure 4-59 Device information

Device Model :	N70
SN :	123[REDACTED]890
Video Input Chann...	0
Video Output Cha...	4
Alarm Input Chann...	2
Alarm Output Cha...	1
Web Version :	V5.50[REDACTED]10834951
System Version :	V4.00[REDACTED].0.R, Build Time: 2025-06-19 20:09:44
Security Baseline V...	V2.4
ONVIF Client Versi...	V2.4.1

Board Information

Select **System Info** > **Board Info** to view the board status, temperature, port type, and more.

Figure 4-60 Board information

Slot	Type	Port Type	Status	Temperature	MCU Version	FPGA Version	Program Version
Control Card	Main Control Card	HDMI	● Normal	31.5℃	V1.0.0, 2024-09-03		V1.000, Build Time: 2024-12-11 16:55:50
Switching Card	Switching Card		● Normal	40℃	V1.0.0, 2024-09-03	V1.001, 2024-11-21	V1.000, Build Time: 2024-12-11 04:16:55
Touchscreen Board	Touchscreen Board		● Normal	33.8℃			V1.000, Build Time: 2024-12-04 10:03:37
Slot2	Decoding Output Card	HDMI	● Normal	41℃	V1.0.0, 2024-09-03 VV1.0.0, 2024-04-22		V1.000, Build Time: 2024-12-11 04:43:28
Slot9	Encoding Card	HDMI	● Normal	55℃	V1.0.0, 2024-09-03 V1.0.0, 2024-11-28	V1.000, 2024-12-11	V1.000, Build Time: 2024-11-30 22:28:47
Refresh							

Online User

Select **System Info** > **Online User** to view the online users.

Figure 4-61 Online user

No.	Username	Group	IP Address	User Login Time
1	admin	admin	192.168.1.7	1970-01-01 00:02:15
2	admin	admin	192.168.1.7	1970-01-01 00:02:15
3	admin	admin	192.168.1.234	1970-01-01 00:02:21
4	admin	admin	192.168.1.234	1970-01-01 00:02:21
5	admin	admin	192.168.1.234	1970-01-01 00:02:25
6	admin	admin	192.168.1.234	1970-01-01 00:02:25
7	admin	admin	192.168.85	2000-01-01 00:12:44
Refresh				

Update

Log

Click **Log** , and then configure the search conditions. Click **Search** to search logs.

Maintenance

Select **Maintenance Management** > **Maintenance** to restart or shutdown the device. You can configure the reboot time, and then click **Apply**.

Configuring Backup

Select **Maintenance Management** > **Config Backup**, and then export the configuration file of the device to the local PC. When the exception occurs, import the configuration file to restore the device.

Default

Select **Maintenance Management** > **Default**, and then other configurations will be reset to their default settings, with the exception of network configuration, user management, and other specific settings.

Click **Factory Default**, and then all configurations will be restored to factory settings.

Advanced Maintenance

Click **One-click Diagnosis** , select **Decoding Diagnosis**, video wall and window, and then click **Diagnose**. After that you can view the diagnosis file.

Click **System Diagnosis** , select board type from the drop-down list, and then click **Diagnose**. After that you can view the diagnosis file.

Click **Packet Capture**, and then configure the IP address and serial port. After that click  to download the packet capture file.

Click **Ping** , and then configure the IP address. Click **Test**, and then view the result.

Click **Running Logs**, and then configure the search conditions to search for the system running logs.

Click **Signaling Interaction**, and then click  to enable signaling interaction. Configure search time or key words to search for signaling records sent by the device.

Click **Decoding Info** to view the decoding information of each channel. Configure the recording interval, and then click **Record** to record the channels.

4.4.9.3 Update

Click **Update** to select the update package to update the program.

4.4.9.4 Log

Click **Log**, and then configure the search conditions. Click **Search** to search logs.

4.4.9.5 Maintenance Management

Maintenance

Select **Maintenance Management** > **Maintenance** to restart or shutdown the device. You can configure the reboot time, and then click **Apply**.

Configuring Backup

Select **Maintenance Management** > **Config Backup**, and then export the configuration file of the device to the local PC. When the exception occurs, import the configuration file to restore the device.

Default

Select **Maintenance Management** > **Default**, and then other configurations will be reset to their default settings, with the exception of network configuration, user management, and other specific settings.

Click **Factory Default**, and then all configurations will be restored to factory settings.

4.4.9.6 Advanced Maintenance

One-click Diagnosis

Select **Advanced Maintenance** > **One-click Diagnosis** > **Decoding Diagnosis**, select video wall and window, and then click **Diagnose**. After that you can view the diagnosis file.

Click **System Diagnosis**, select board type from the drop-down list, and then click **Diagnose**. After that you can view the diagnosis file.

Packet Capture

Select **Advanced Maintenance** > **Packet Capture**, and then configure the IP address and serial port. After that click  to download the packet capture file.

Ping

Select **Advanced Maintenance** > **Ping**, and then configure the IP address. Click **Test**, and then view the result.

Running Logs

Select **Advanced Maintenance** > **Running Logs**, and then configure the search conditions to search for the system running logs.

Signaling Interaction

Select **Advanced Maintenance** > **Signaling Interaction**, and then click  to enable signaling interaction. Configure search time or key words to search for signaling records sent by the device.

Decoding Information

Select **Advanced Maintenance** > **Decoding Info** to view the decoding information of each channel. Configure the recording interval, and then click **Record** to record the channels.

4.4.10 Event Management

4.4.11 Third-Party Device Connection

4.4.11.1 Configuring Serial Port

Procedure

- Step 1 Select **System** > **Serial Port**.
- Step 2 Select slot and channel, set the serial port type to **232** or **485** (keep it the same as the controlled device), set the function to **MatrixCom**, and set other parameters the same as the controlled device.

4.4.11.2 Signal on Wall

Display signal on the wall by sending control commands on the controlled device.

Procedure

- Step 1 View the screen control number.

Select **Video Wall > Video Wall Config**, select **ID** at the lower section, and then you can view the part, and the screen control number of the corresponding channel on the video wall.

- Step 2** Select **Device Setting > Local Signal > Local Signal**, and then you can view the control number of the local signal source.

Figure 4-62 View local signal source control number

No.	Camera Name	Slot ▼	Control No. ↗	Color Space Mode ↗	Signal Source Type	Interface Status	Operation
1	 Slot06-01	Slot6	21	Limited	HDMI	1920 * 1080@60	
2	 Slot06-02	Slot6	22	Limited	HDMI	0 * 0	
3	 Slot06-03	Slot6	23	Limited	HDMI	0 * 0	
4	 Slot06-04	Slot6	24	Limited	HDMI	0 * 0	
Total 4 records							< 1 >
Apply Refresh							

- Step 3** Select **Device Setting > Network Signal > Channel**, and then you can view the control number of the network signal source.

- Step 4** Enter the commands on the controlled device, such as 7Ma99#a, which means that switch the input source with the control number of 99 to the screen with the control number of 7.

4.4.11.3 Switching Scene

Scene switching is achieved by issuing control commands from the central control device.

Procedure

- Step 1** View the scene control number, and the select **Video Wall > Scene**.
- Step 2** Enter the command line in the central control device, such as **1Pa**, which means calling the scene whose control number is 1.

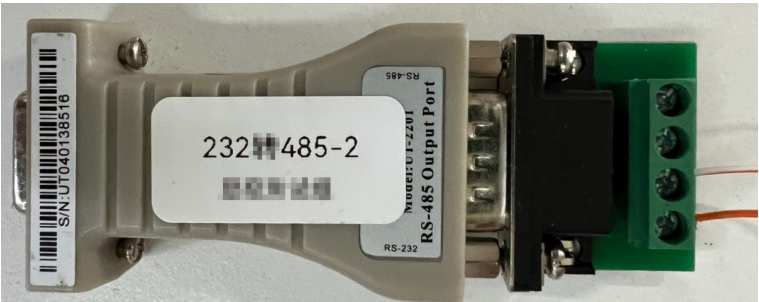
Appendix 1 Serial Cable Assembly Guide

Appendix 1.1 Screen Control through 485

You need to prepare the network cable, 232 to 485 tool, and the green female terminal, which is in the accessory box. The 232 to 485 tool is shown as the following figure.

Connect the 485 interface of the main control to the tool, to convert it to 232. The 485 end is the green terminal adapter, and the 232 end is the DB9 female.

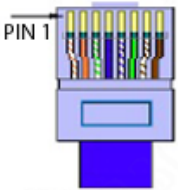
Appendix Figure 1-1 232 to 485 tool



- Connection of the 232 end: The meaning of DB9 female is shown in the following figure. PIN2 is TX, PIN3 is RX, and PIN5 is GND.

Face the crystal head metal to yourself, and it is 1 to 8 from left to right (white orange, orange, white green, blue, white blue, green, white brown, and brown). Connect PIN2 of the network cable to PIN2 (TX) of DB9, PIN6 of the network cable to PIN3 (RX) of DB9, and PIN5 of the network cable to PIN5 (GND) of DB9.

Appendix Figure 1-2 Network cable pin



Appendix Table 1-1Pin of RS-232C

DB9 Female (Pin)	RS-232C Interface Signal
2	Send data SOUT (TXD)
3	Receive data SIN (RXD)
5	Signal ground (GND)

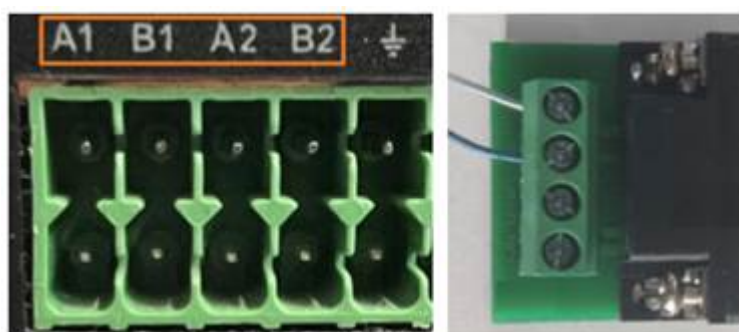
- Connection of the 485 end: 485 of the tool is defined as shown in the following table. 2 wires are required for connection, and the wires do not need to distinguish between positive and negative.

Appendix Table 1-2 RS-485 output signal and terminal pin

DB9 Male (Pin)	Output Signal	RS-485 Half-Duplex Wiring
1	T/R+	RS-485 (A+)
2	T/R-	RS-485 (B-)
5	GND	Ground
6	VCC	+5 V standby power input

- Connect the green terminal of the main control to A and B. The green terminal connection of the tool is shown as the following figure. The power supply does not need to be connected.

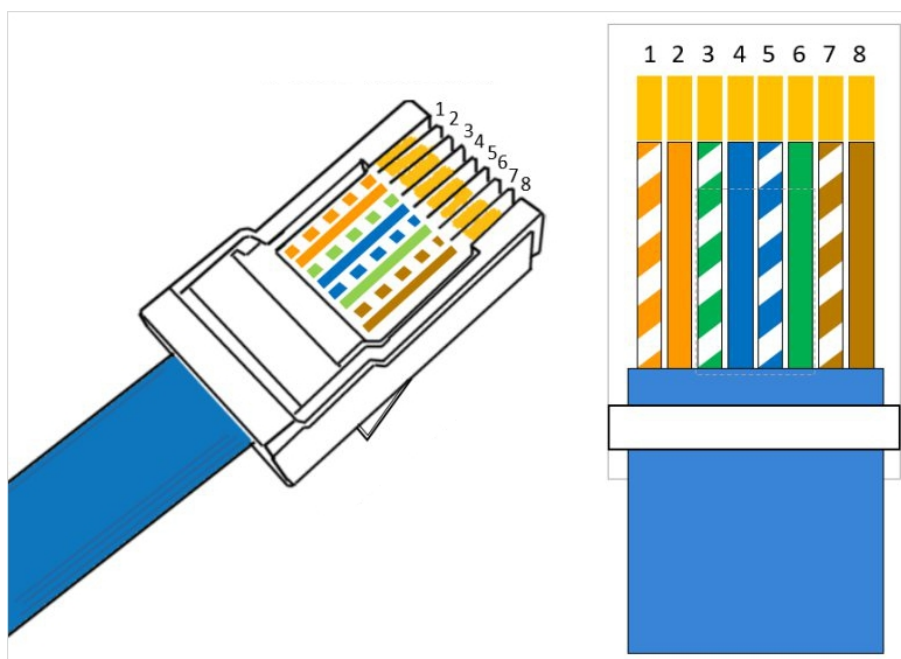
Appendix Figure 1-3 Connection of the 485 end



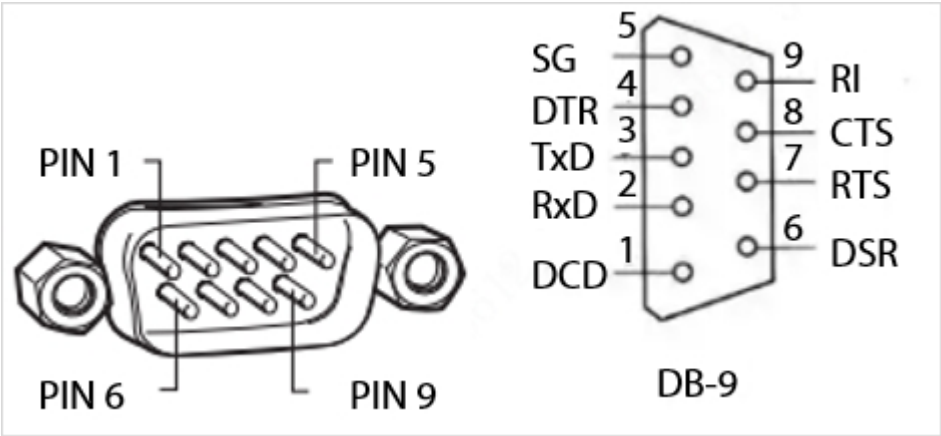
Appendix 1.2 Screen Control through 232

If the serial port of the peer device is a DB9-pin standard serial port of RS-232, select a RJ45 network cable of T568B line sequence and a RS-232 serial port cable.

Appendix Figure 1-4 T568B-wired RJ45 Ethernet cable



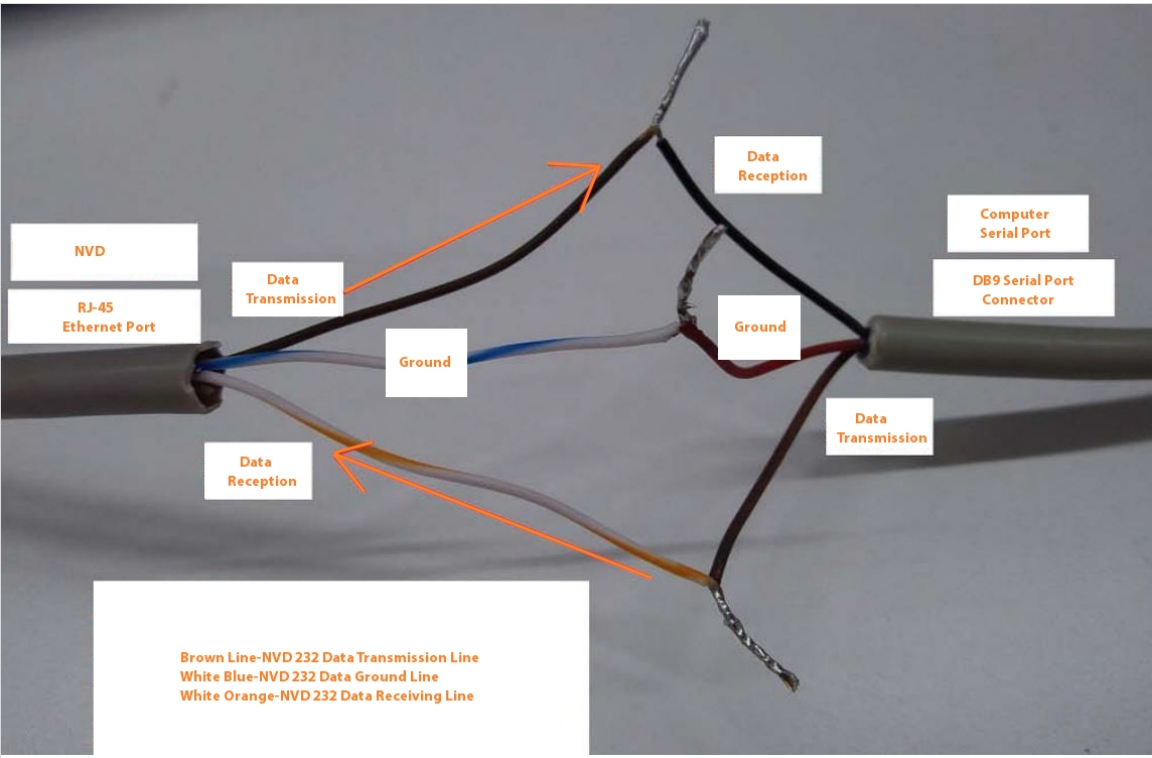
Appendix Figure 1-5 Definition of RS-232 connecting line pin



Appendix Table 1-3RS-485 output signal and terminal pin

Video Integrated Platform	RJ45 Ethernet Cable	RS-232 Serial Cable	Peer Device
RXD	1 White-Orange	3	TXD
GND	5 White-Blue	5	GND
TXD	8 Brown	2	RXD

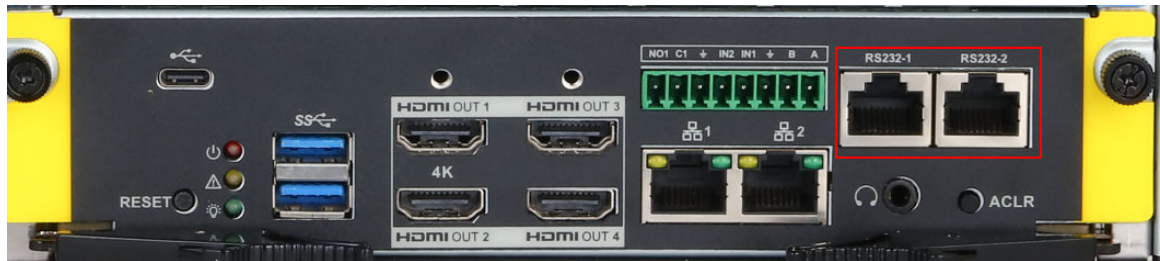
Appendix Figure 1-6 Wiring diagram



- If no signal transmission is detected after wiring as above, swap the TXD and RXD connections and retest.

- If the serial port of the peer device is not a DB9-pin standard serial port, ensure that the data sending line is connected to the peer receiving line, the data receiving line is connected to the peer sending line, and the ground line is connected to the peer ground line according to the actual situation.

Appendix Figure 1-7 Equipment RS-232 interface



Appendix 2 Matrix Serial Port Control Protocol

Appendix Table 2-1 Description of matrix serial port control protocol

Serial Port Control	Code	Description
Select screen number	1Ma	1 refers to the switched screen number. The value ranges from 1 to 999.
Specify window number	1Xa	1 refers to the window number on a screen.
Select the camera number	1#a	1 refers to the switched camera or local channel number. The value ranges from 1 to the 99,999,999.
Camera preset	1^a: Set 1\ a: Use	1 refers to the defined or used preset value. The value ranges from 1 to 999.
Control the PTZ camera up	0-6Ua	0-6 refers to the speed level. 6 refers to the maximum speed. Send codes continuously.
Control the PTZ camera down	0-6Da	0-6 refers to the speed level. 6 refers to the maximum speed. Send codes continuously.
Control the PTZ camera left	0-6La	0-6 refers to the speed level. 6 refers to the maximum speed. Send codes continuously.
Control the PTZ camera right	0-6Ra	0-6 refers to the speed level. 6 refers to the maximum speed. Send codes continuously.
Control PTZ camera iris +	Wa	Send codes continuously.
Control PTZ camera iris -	Ta	Send codes continuously.
Control PTZ camera focus +	Na	Send codes continuously.
Control PTZ camera focus -	Fa	Send codes continuously.
Turn off PTZ camera	Ca	Send codes continuously.
Turn on PTZ camera	Oa	Send codes continuously.
User scheme	1Pa	1 refers to the scheme number. The value ranges from 1 to 999.
Turn on screen	Ka	Send codes continuously.
Turn off screen	Ga	Send codes continuously.
Turn on specified screen	1Ka	1 refers to the switched screen number. The value ranges from 1 to 999.
Turn off specified screen	1Ga	1 refers to the switched screen number. The value ranges from 1 to 999.
Stream type	Ea	5 refers to bare data (only for local signals), 0 refers to the main stream (default), and 1 refers to the sub stream.

Appendix Table 2-2Serial port control protocol examples

Example	Code
Display camera 99 in screen 7	7Ma99#a
Use scheme 10	10Pa
Control PTZ camera 47 to display in screen 8, and control the PTZ camera right	8Ma47#a5Ra
Control PTZ camera 47 to display in screen 8, and control the PTZ camera focus +	8Ma47#aWa
Control the selected PTZ camera in screen 8 to turn right	8Ma5Ra
Turn all screens on	Ka
Turn off screen 5	5Ga
Display camera 2 in window 1 of screen 1	1Ma1Xa2#a

Appendix 3 Security Recommendation

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

The 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, it is recommended 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**

It is recommended 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).