2-Channel Splicing Unit

User's Manual

V1.0.0

Foreword

General

This manual introduces the installation, functions, and configuration of the 2-channel decoding splicing unit (hereinafter as the "device"). Read this manual before you use the product and keep this manual for future reference.

Models

NVD0200FX-A01

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Description
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.0	First release.	October 2023

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

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

Transportation Requirements

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

Store the device under allowed humidity and temperature conditions.

Installation Requirements

 **WARNING**

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Replace unwanted batteries with new batteries of the same type and model. 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.
- Do not expose the battery to extremely hot environments, such as direct sunlight and fire, to avoid the risk of fire and explosion.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 10 cm on the sides and 5 cm on top of the device.
- Install the device on a stable surface to prevent it from falling.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- Use the power cords that are recommended for the region and conform to the rated power specifications.

- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it.
- A safety circuit breaker is designed on the device panel to cut the power of the device. Make sure the breaker can be easily operated during installation.

Operation Requirements

This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not place an open flame on the device, such as a lit candle.
- Do not disassemble the device without professional instruction.

Table of Contents

1 Product Overview

1.1 Introduction

2-ch decoding splicing unit has powerful functions such as decoding, multi-device cascading, roaming, virtual LED and more. It can be applied in multiple scenarios such as the public security management center of the village, intelligent community control room, comprehensive management center, transparent kitchen, education and more.

1.2 Main Functions

Network Video Decoding

Decodes video data transmitted by front-end devices.

Display Function

- Content can be customized and overlaid.
- The background image can be configured.
- The background color can be configured.
- Schemes with video wall configurations can be saved and automatic scheme tour can be applied.

Screen Functions

- Splices one or more screens.
- Splices window on single or splicing screen.
- Controls screen on or off through RS-232 port.

2 Device Appearance and Installation

2.1 Unpacking and Checking

When you receive the device, check whether there is any visible damage. The protective packaging can withstand impacts during transportation.

The label at the bottom of the box contains the device serial number and other information. Protect the label and show it to the after-sales service personnel when you need assistance.

2.2 Device Appearance

2.2.1 Front Panel

Figure 2-1 Front panel

Table 2-1 Parameter description of front panel

No.	Description
1	Power indicator
2	Activity indicator
3	USB port. Used for connecting external devices such as mouse and keyboard
4	Power button

2.2.2 Rear Panel

Figure 2-2 Rear panel

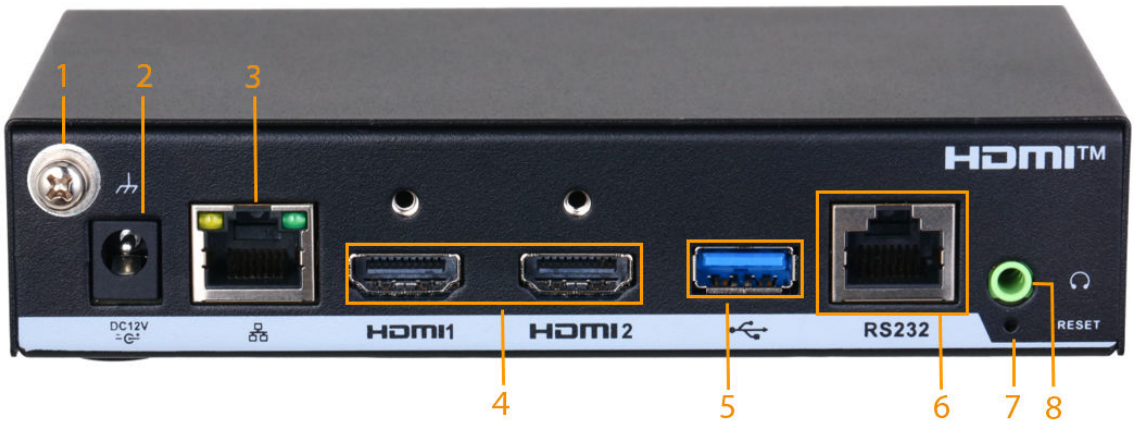


Table 2-2 Parameter description of rear panel

No.	Description
1	Ground
2	Power port
3	RJ–45 network port
4	HDMI output port
5	USB Port
6	RS–232 series port of screen control
7	Reset button. Press and hold it for more than 5 s, and then the device will restore factory default settings
8	3.5 mm audio output

2.2.3 Installation and Connection

- When installing the Unit, refer to engineering construction specifications and relevant national standards for specific requirements.
- HDMI cable quality and length affect the video quality. The video might be blurry, have noise or black edge. Sometimes the video quality might vary when the same video is output with different cables. Cables certified by relevant standards are recommended to ensure the reliability.

Installation and Connection of Front Panel

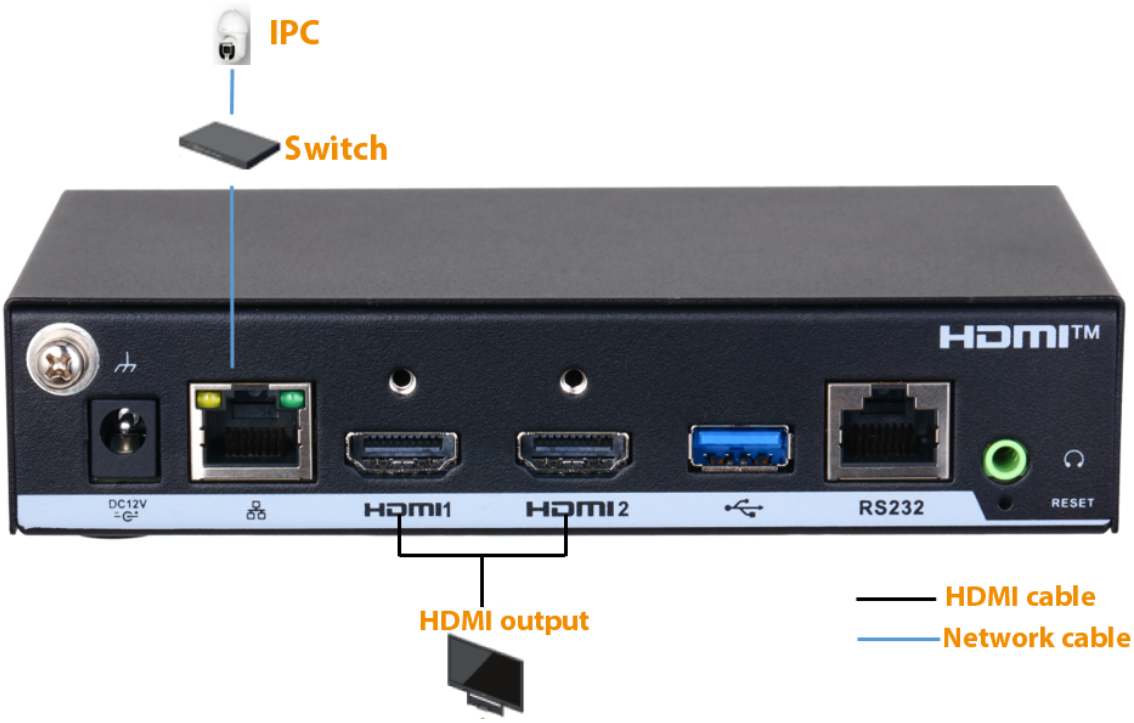
The 2 USB ports on the front panel are used for connecting mouse, keyboard and USB flash drive.

Figure 2-3 Connection of front panel

Installation and Connection of Rear Panel

The 2 HDMI video output ports are used for connecting with monitors.

Figure 2-4 Connection of front panel



3 Web Operations

3.1 Connecting to Network

Procedure

Step 1 Connect the network port of the device to the network port of your computer with the network cable.

Step 2 Set the computer and the device on the same IP segment.

Step 3 Ping ***.***.***.***(IP address of the device) on your computer to check whether the connection is working normally. Usually the returned TTL value should be less than or equal to 64.

Step 4 Enter the IP address of the device in the address bar of the browser, and then press the Enter key.

Step 5 After you log in to the webpage, change the IP address of the device according to the actual situation.

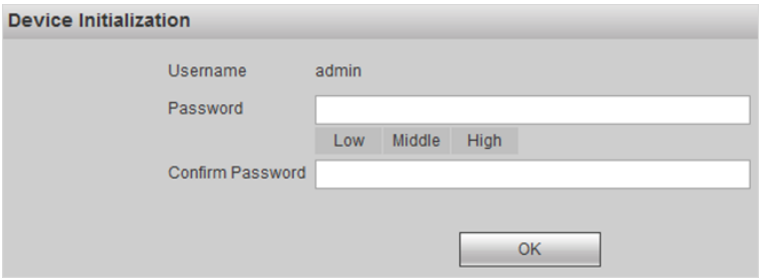
Web controls can be automatically recognized and downloaded. The system can download the latest web controls and remove the old one.

3.2 Logging in to the Webpage

Procedure

Step 1 Enter the IP address of the Unit in the browser address bar. (the IP address is 192.168.1.108 by default), and then press Enter.

Figure 3-1 Initialization



Step 2 Set the password for the admin user.

- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters among uppercase and lowercase letters, numbers, and special characters (excluding ' , ", ; : and &). The confirming password must be the same as the new password.
- Set a high security password according to the password strength prompt.

Step 3 Click **OK**.

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

Step 5 Check the notes and product highlights on the page.

- Follow the important notes on the page.
- Click to close the page.
- Select the **Do not show again** check box, and the prompt will not be displayed when you log in to the page next time.

Figure 3-2 Operation page

Step 6 Follow the system instructions to install or load controls.

3.3 Screen

Click **Screen** to enter the video wall page.

Figure 3-3 Screen

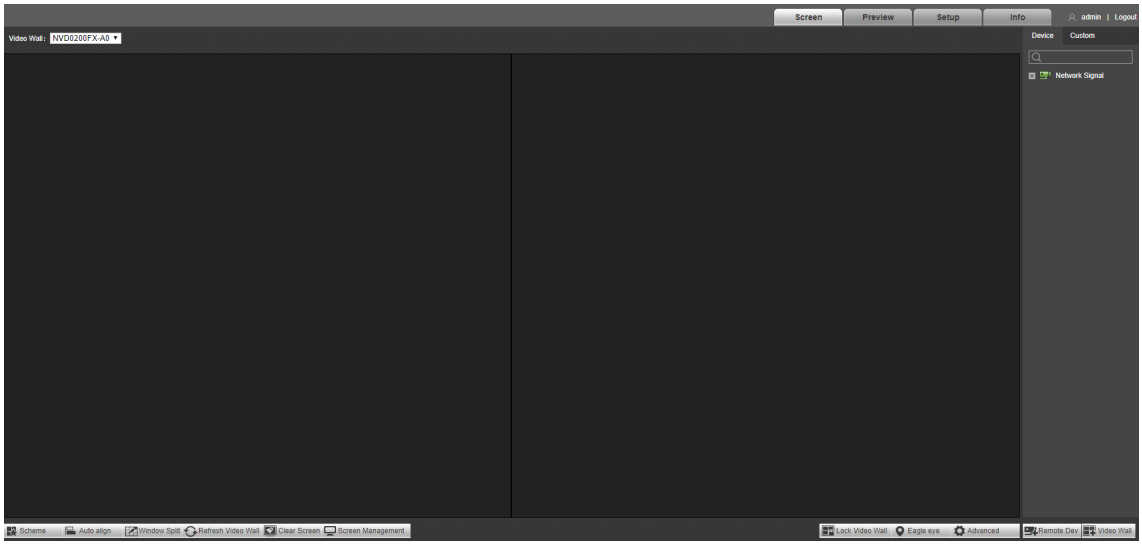
Table 3-1 Description of screen functions

No.	Parameter	Description
1	Video wall selection area	After adding a video wall, you can select the video wall from the drop-down list of **Video Wall**.
2	Window configuration	You can turn off signals and add, adjust and put windows down at the bottom.
3	Signal management	Select different tabs to operate. ● Click **Device**, and then you can view network signal, channel information, preview and display the signal on the video wall. ● Click **Custom**, and then you can view information on signal groups and configure signal tour on the video wall.
4	Video wall	Click **Video Wall** to enter **Video Wall Setup** page, and then you can add, modify and delete video walls.
5	Remote device	Click **Remote Dev** to go to the **Network Signal** page where you can add, modify, and delete devices.
6	Video wall management	You can manage schemes, align windows automatically, split windows, refresh the video wall, clear the screen and turn on/off screen, lock or unlock the video wall, and more.

Adding video walls

For first-time login, click **Screen** to go to the video wall page, you can see a default video wall. You can directly configure the default video wall or click to add new video walls.

Figure 3-4 Adding video walls

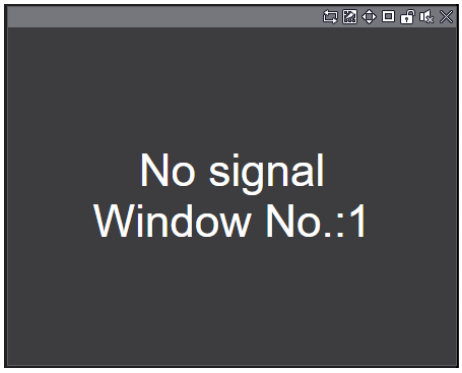


3.3.1 Window Configuration

3.3.1.1 Adding Windows

Press and hold the mouse to drag and form a window.

Figure 3-5 Add windows



- Select a window, press and move the left mouse button, and then the selected window will be moved to the required position.
- Select a window, drag the control point in any direction to change the dimensions of the selected window.
- Select a window, right-click and select **Bottom**. The selected window will appear at the bottom of other windows.
- Select a window that is displaying signal, right-click and then select **Signal Off**. The signal will be turned off.

Adjusting the Window

Click icons on the upper-right corner to adjust windows.

Table 3-2 Icon description

Icon	Name	Description
	Start/stop signal tour	Click the icon to start signal tour, and the icon becomes . Click to stop signal tour.
	Split	Split the window across 2 windows, including 2 splits (horizontal and vertical), 4 splits, 9 splits, 16 splits and 25 splits. When the window is maximized or pasted to the screen, the icon becomes . Click the icon to drag the window to any positions.
	Paste screen	The window is pasted to the screen and cannot change its size.
	Paste window	Maximize the window without overlapping other windows.

Icon	Name	Description
	Lock	When the window is locked, the position and size cannot be adjusted. Click to unlock the window.
/	Audio	Turn on/off audio (reserved function).
	Close	Close the window.

3.3.1.2 Configuring Window Information

Configure the coordinates and size of the window.

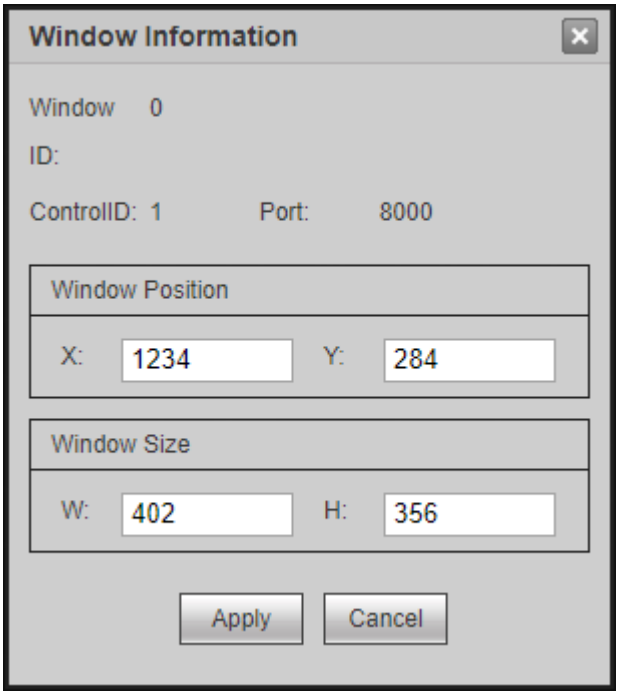
Procedure

Step 1 Log in to the webpage, and then click **Screen**.

Step 2 Double-click the window.

Step 3 Configure window position and size.

Figure 3-6 Window information



Step 4 Click **Apply**.

The window position and size are adjusted according to the configuration.

3.3.2 Signal Configuration

Select signals, or enter the name of the signal in the search bar to search for signals.

3.3.2.1 Device Tree

The device tree displays all the network signals. You can click **Add** to add signals.

3.3.2.2 Custom

The **Custom** tab displays groups that were added and the signal sources in groups. After you drag a signal group to a window, signals in the signal group are played in a loop.

3.3.2.3 Signal on Wall

You can view videos related to the signal on the video wall.

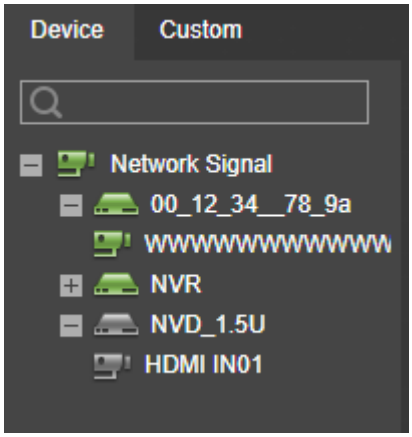
Procedure

Step 1 Log in to the webpage, and then click **Screen**.

Step 2 Select a window on the video wall, or press and hold the left mouse button to create a window on the video wall.

Step 3 Select a signal source from the **Device** or **Custom**.

Figure 3-7 Select signal source



Step 4 Display the signal on the video wall.

- Press and hold the left mouse button to drag the signal to the designated window, and the signal will be output to the window.
- Select a window, double-click channel preview or main/sub stream, and the signal will be output to the window.

Step 5 Log in to the webpage, and then click **Screen**.

Step 6 Select a window to tour signals.

Step 7 Select **Custom** > **Collection**.

Step 8 select a signal group, and press and hold left mouse button to drag the signal group to the designated window.

The window starts to tour signals automatically.

Step 9 Click  at the bottom of the page.

All signal information in the window is displayed.

Figure 3-8 Signal information

Step 10 Set **Stay Time** and **Stream Type**. The default stay time is 10 s.

- Click corresponding to a signal, and the signal will not appear in the tour queue, but still exists in the signal group.
- Click or to adjust the sequence of signal tour.
- The configuration takes effects immediately.
- Click on the upper-right corner of the window to stop signal tour.

3.3.3 Managing Video Wall

Manage schemes, align windows automatically, and more.

3.3.3.1 Scheme Management

You can manage video schemes, favorite schemes, and combined schemes, and set the time to switch schemes.

3.3.3.1.1 Video Scheme

Procedure

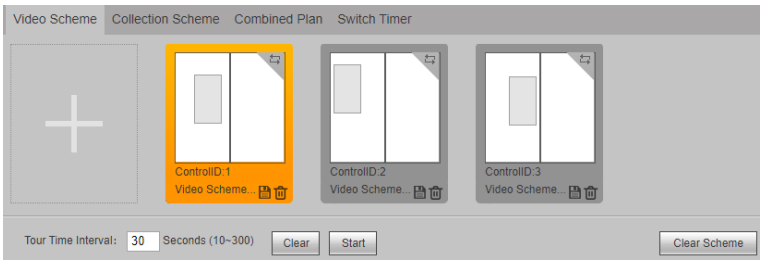
Step 1 Log in to the webpage, and then click **Screen**.

Step 2 Click **Scheme**.

Step 3 Click to add a scheme.

You can repeat Step 2 and Step 3 to add multiple schemes.

Figure 3-9 Video scheme



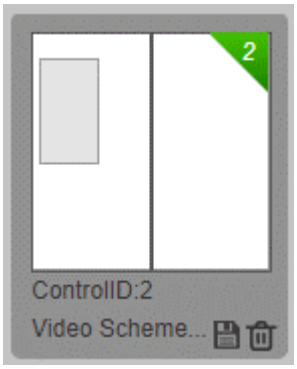
Step 4 Configure tour time interval.

Step 5 Click on the upper-right corner of each scheme to add the scheme to tour queue.

Step 6 changes to a number, indicating the sequence of the plan in the tour queue.

- To modify the control ID and scheme name, double-click **Control ID** and scheme name.
- Control ID distinguishes different schemes when central control device issues commands.
- No operation can be performed on the screen when the scheme is in tour.

Figure 3-10 Set tour sequence



Related Operations

- Click **Clear Scheme** to clear the whole scheme plan.
- Click **Stop** to stop scheme tour.

3.3.3.1.2 Collection Scheme

Save virtual LED and background configurations to an additional scheme. Multiple collection schemes can be displayed on the video wall in turn.

3.3.3.1.3 Combined Plan

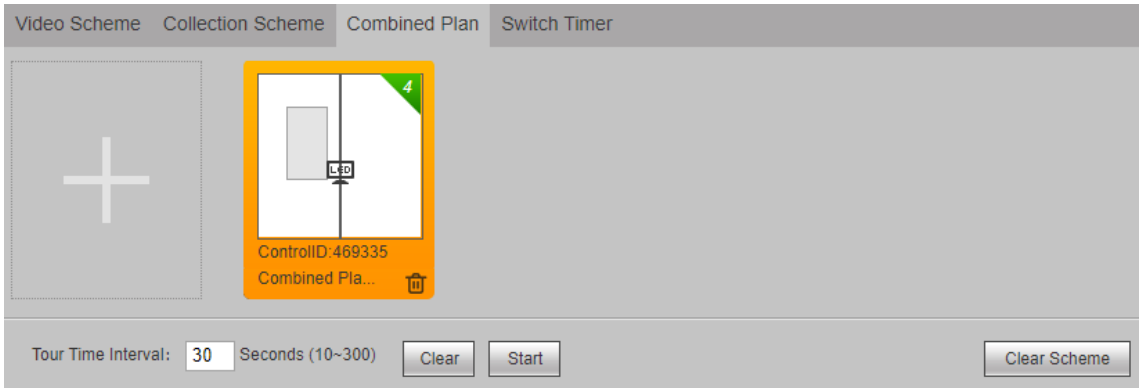
You can combine the video scheme and collection scheme into a combined scheme, and then display it on the video wall.

Procedure

Step 1 Log in to the webpage, and then click **Screen**.

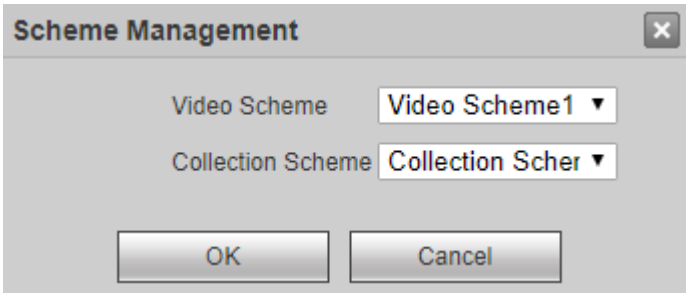
Step 2 Select **Scheme** > **Combined Plan**.

Figure 3-11 Combined plan



Step 3 Click to select a video scheme and collection scheme.

Figure 3-12 Scheme management



Step 4 Click **OK**.

3.3.3.1.4 Timed Switch

After setting switch time for a scheme, the system will switch to the scheme automatically at the switch time.

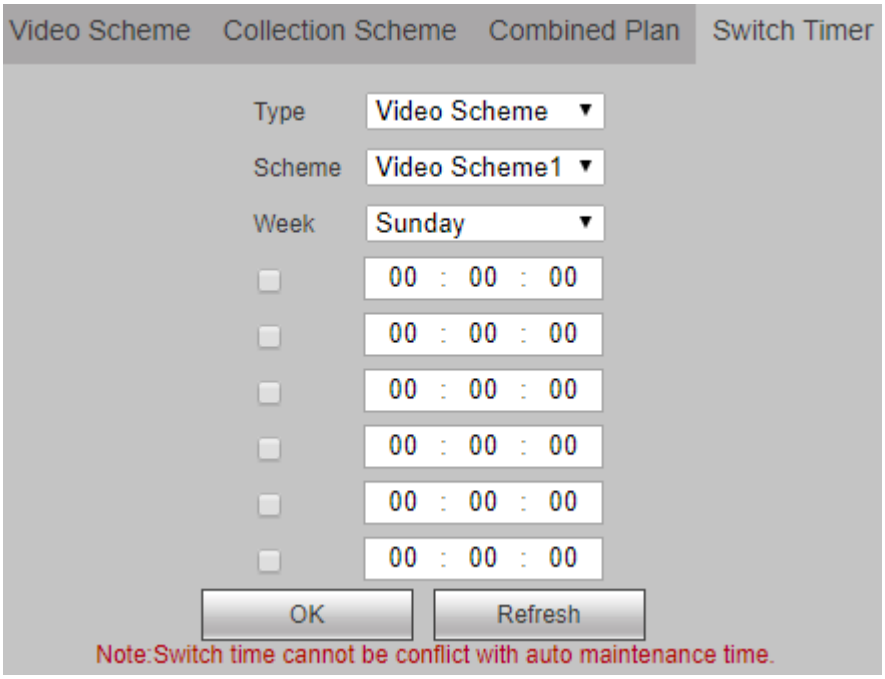
Procedure

Step 1 Log in to the webpage, and then select **Screen**.

Step 2 Select **Scheme** > **Switch Timer**.

Step 3 Select type, scheme and week, and then set the switch time.

Figure 3-13 Switch timer



- Select the check box corresponding to the time, and the time point takes effect.
- Scheme time periods cannot be the same.

Step 4 Click **OK**.

3.3.3.2 Automatic Alignment

Click **Auto-align**, and then all windows will be automatically aligned in the following ways:

- Windows with equal size must fill the entire video wall.
- Windows are arranged horizontally from top to bottom.

3.3.3.3 Window Splits

Select a block or window according to your needs. and then you can split the block or window or enter the number of splits manually.

3.3.3.3.1 Block Division

When you split a block, the system clears all windows in the block and splits windows based on the specified split number. After the block is split, the previous windows will be closed, and previous signals will not be kept.

Procedure

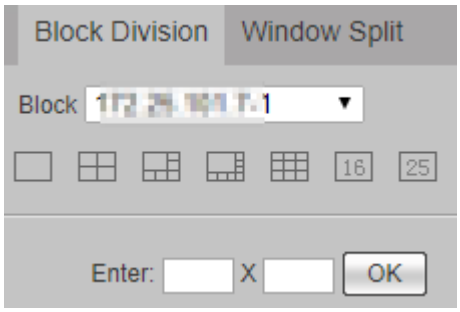
Step 1 Log in to the webpage, and then select **Screen**.

Step 2 Select **Window Split** > **Block Division**.

Step 3 Select the block that need to be split.

Step 4 Select the fixed split , or enter the split number manually (for example, 3 × 3 represents 9 splits).

Figure 3-14 Block division



Step 5 Click **OK**.

Step 6 Click **OK** in the pop-up window.

After the block is divided, the window is locked by default. If you need to adjust window position and size, click to unlock the window.

3.3.3.3.2 Window Split

The original signals are retained in the first window after customized splitting.

Procedure

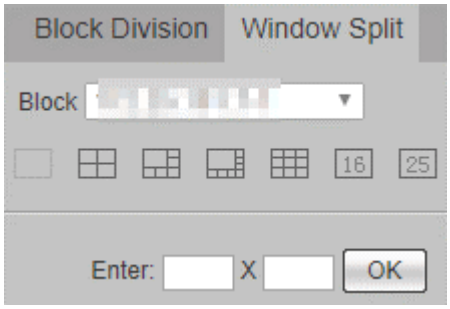
Step 1 Log in to the webpage, and then select **Screen**.

Step 2 Select a signal window.

We recommend not selecting tour window for window split.

Step 3 Select **Window Split** > **Window Split**.

Figure 3-15 Window split



Step 4 Select the fixed split or enter the split number manually (for example, 3×3 represents 9 splits).

Step 5 Click **OK**.

After window split, previous signal remains in the first window, while other windows display **No Signal**.

3.3.3.4 Refreshing Video Wall

Click **Refresh Video Wall** to refresh the channel preview and layout information of the current video wall.

3.3.3.5 Clearing Screen

Click **Clear Screen** to clear the configurations of the screen.

3.3.3.6 Screen Management

You can manage the screen, including controlling screen power, controlling power switch and adjusting screen parameters.

Prerequisites

Connect the device and the screen with serial cable properly to turn on/off the screen. After powering off the screen, the screen displays black.

Procedure

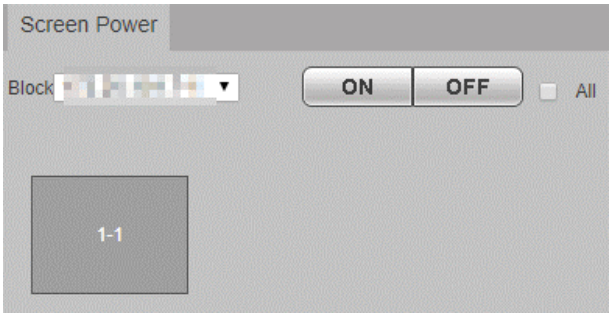
Step 1 Log in to the webpage, and then select **Screen**.

Step 2 Select **Screen Management** > **Screen Power**.

Step 3 Select a block.

- Select a block and then select a screen. After that click **ON** or **OFF** to turn on or off the selected the screen.
- Select **All** , and then select a screen block. After that click **ON** or **OFF** to turn on or turn off the screen.

Figure 3-16 Screen on/off



3.3.3.7 Locking Video Walls

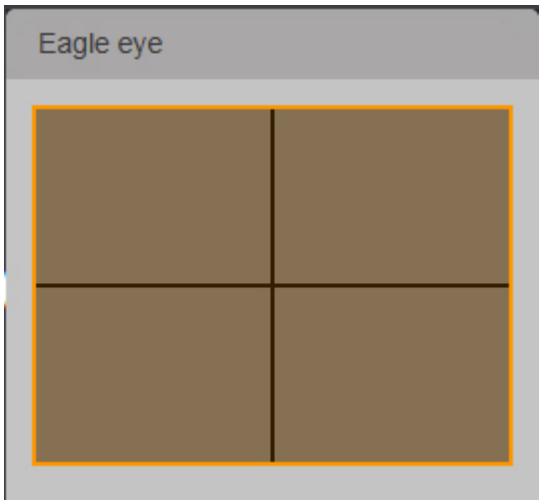
Click **Lock Video wall** to lock the video wall, and then users cannot adjust the relative position of the window. Click **Lock Video Wall** again to unlock the video wall.

3.3.3.8 Eagle Eye Map

Eagle eye map, also named thumbnail, is used for adjusting the display size and area of the screen.

Click **Eagle eye** , and then drag the black edge or rotate the scroll wheel to adjust the display area of the main window. Drag the area box in the eagle eye map to change the display area of the corresponding main window.

Figure 3-17 Eagle eye map



3.3.3.9 Advanced Functions

Configure advanced functions including PTZ control, virtual LED, background, decoding strategy and screen number.

3.3.3.9.1 PTZ Control

Select the window, and then click **PTZ control** to turn the PTZ device toward 8 directions, including up, down, left, right, upper left, upper right, lower left and lower right.

When using the local serial port to control PTZ device, you need to configure PTZ parameters and make sure that the connection is right.

Figure 3-18 PTZ control

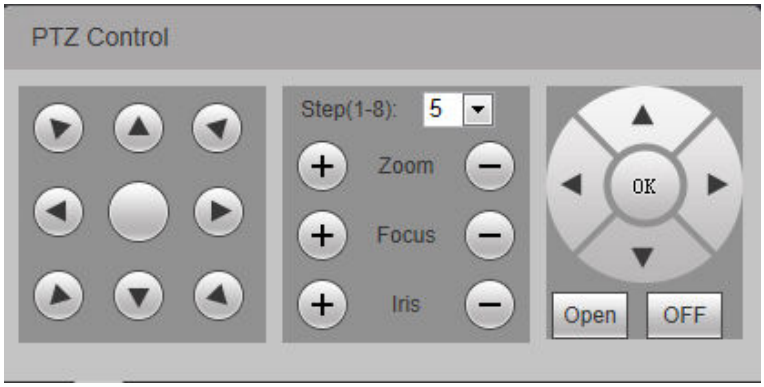


Table 3-3 Parameter description of PTZ control

Parameter	Description
Directions	Controls device towards 8 directions including up, down, left, right, upper left, upper right, lower left and lower right.
Step length	Control the speed of the PTZ rotation, which ranges from 1-8.
Zoom	Click ⊕ or ⊖ to adjust zoom.
Focus	Click ⊕ or ⊖ to adjust clarity.
Iris	Click ⊕ or ⊖ to adjust brightness.
PTZ Menu	Click **Open** to open the PTZ menu of the preview page, after that you can select different direction keys to operate the PTZ device. Click **OFF** to close the PTZ menu of the preview page.

3.3.3.9.2 Virtual LED

Create an area and enter any characters and then it will be displayed on LED screen.

Procedure

Step 1 Log in to the webpage, and then select **Screen**.

Step 2 Select **Advanced** > **Virtual LED**.

Step 3 Click 

to add virtual LED and configure the parameters.

Figure 3-19 Virtual LED

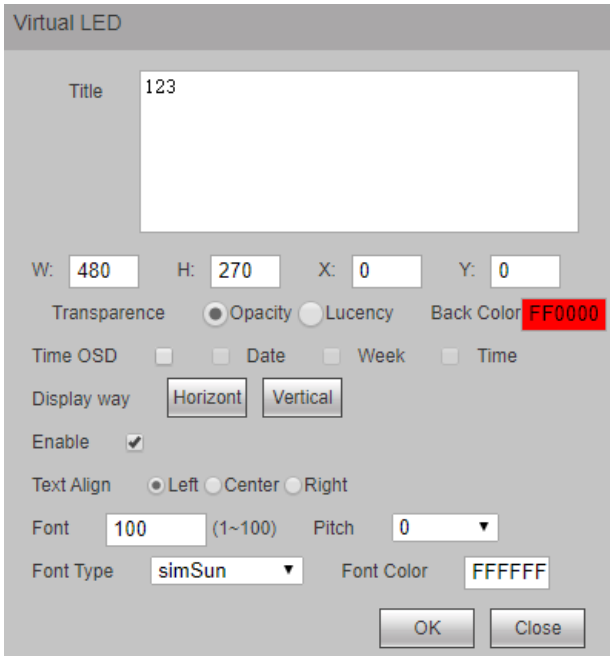


Table 3-4 Parameters description of virtual LED

Parameter	Description
Title	Enter the title of the virtual LED, which will be displayed on the video wall.
W/H	Enter the width and height of the virtual LED background.
X/Y	Coordinates of the virtual LED.
Transparency	Configure the **Transparence** of virtual LED. You can configure the transparence as **Opacity** or **Lucency**.
Background Color	Configure the background color of the virtual LED. You can enter 6 numbers of RGB or click the color area to select colors.
Time OSD	Select check box on the left to enable time display function. **Date** , **Week**, **Time** are displayed by default. You can select what you want to display. Select at least one item from **Date** , **Week** and **Time**.
Display way	Configure the OSD alignment of the title. You can select **Horizontal** or **Vertical**.
Enable	Select whether to display the virtual LED title on the video wall or not. • Select the check box, and then click **OK**. The video wall displays the title of virtual LED. • Cancel selecting the check box, and then click **OK**. The window of the webpage will display the title of the virtual LED but the video wall will not display.
Text Align	Configure the alignment of the virtual LED text on the background. You can choose **Left** , **Center** or **Right**.
Font	Configure the font size, which ranges from 0 to 100.

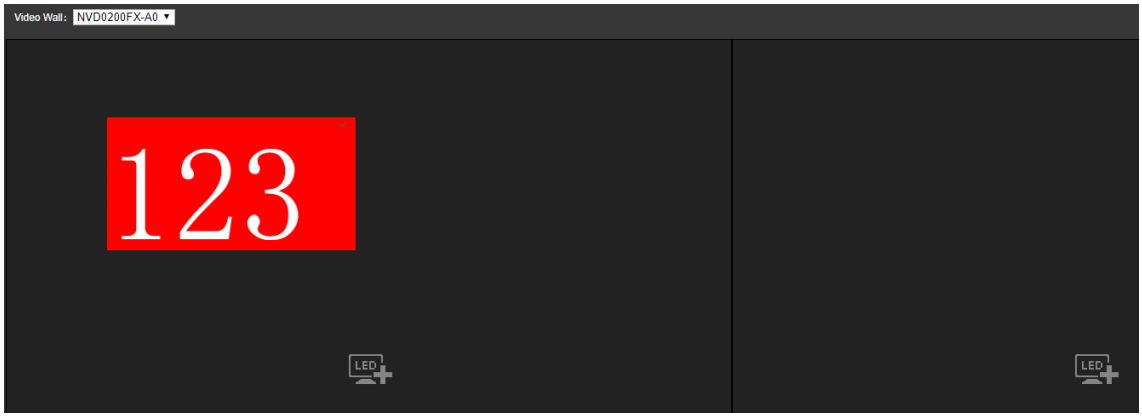
Parameter	Description
Pitch	Configure the title character distance from o to 5.
Font Type	Configure the font size of the title of the virtual LED. You can select **SimSun** or **FZHTJW**.
Font Color	Configure the font color of the title. You can enter 6 numbers RGB manually or click color area to select the font color.

Step 4 Click **OK**.

Virtual LED displays the title.

- Hover over the virtual LED, and then press and hold the mouse to move the virtual LED to any places you want.
- Click the virtual LED, and then drag any direction control point to change the size of the virtual LED.

Figure 3-20 Result



3.3.3.9.3 Background

You can set the uploaded image to the background, and then the image will be displayed as the background of the screen.

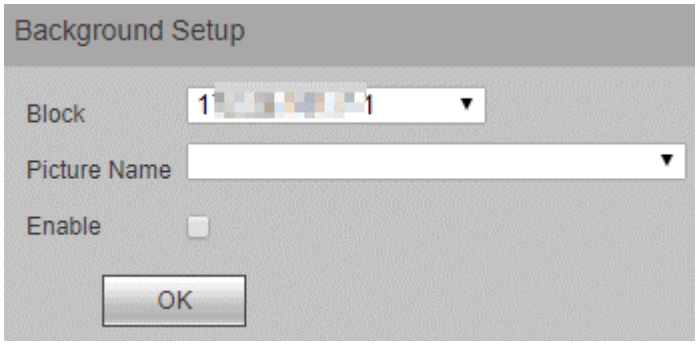
Procedure

Step 1 Log in to the webpage, and then select **Screen**.

Step 2 Select **Advanced** > **Background**.

Step 3 Select **Block** and **Picture Name**, and then select **Enable**.

Figure 3-21 Add background image



Step 4 Click **OK**.

3.3.3.9.4 Decoding Strategy

Background Information

Drag the slider to adjust window fluency, and thus balance real-time decoding and fluency.

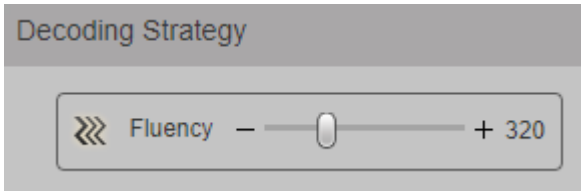
Procedure

Step 1 Log in to the webpage, and then select **Screen**.

Step 2 Select a network signal window.

Step 3 Select **Advanced** > **Decoding Strategy**.

Figure 3-22 Decoding strategy



Step 4 Drag the slider to adjust the fluency of the video.

The higher the fluency is, the more latency the video on wall has.

3.3.3.9.5 Showing Screen ID

Click **Show Screen ID**, and then the screen will display the number of the screen. Click it again to hide screen ID.

3.4 Preview

Install the web control to view live videos.

Click **Preview**, and then follow the instructions to install control to enter the preview page.

Figure 3-23 Preview

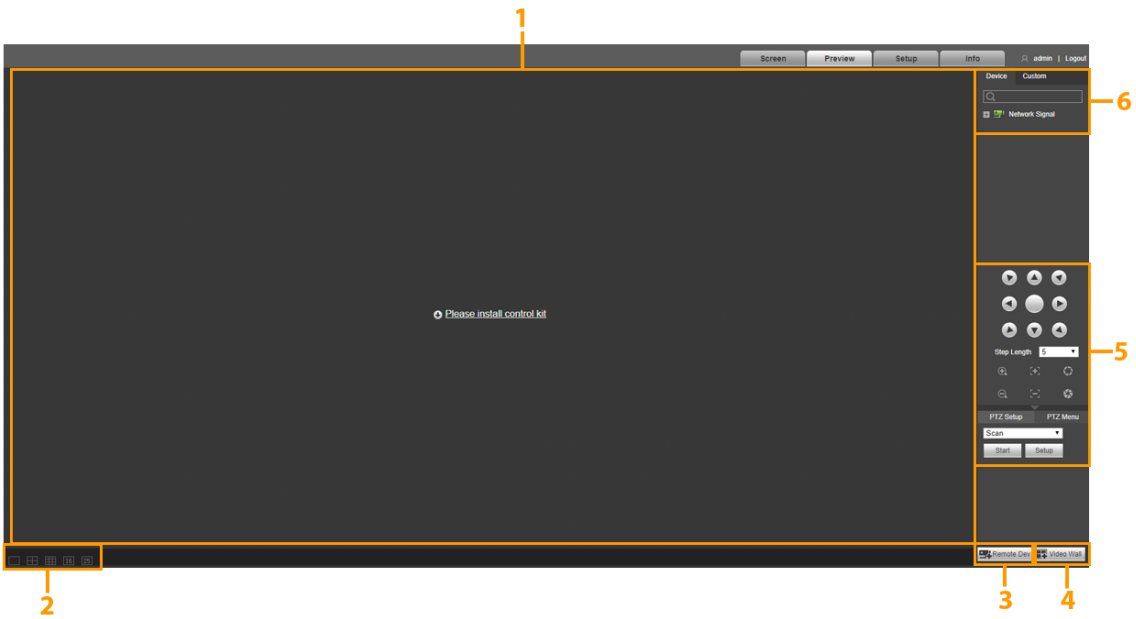


Table 3-5 Function description

No.	Name	Description
1	Window	You can view live videos in the window.
2	Window split	Includes single screen, 4 splits, 9 splits, 16 splits and 25 splits.
3	Remote device	Click **Remote Dev** to enter the network signal page. You can add, modify and delete devices.
4	Video wall	Click **Video Wall** to go to the **Video Wall Setup** page, and then you can add, modify and delete video walls.
5	PTZ control	You can perform simple operations on the PTZ camera.
6	Signal configuration area	You can configure signals.

3.4.1 Window Functions

Click the icon on the upper-right corner to adjust the window.

Figure 3-24 Window function

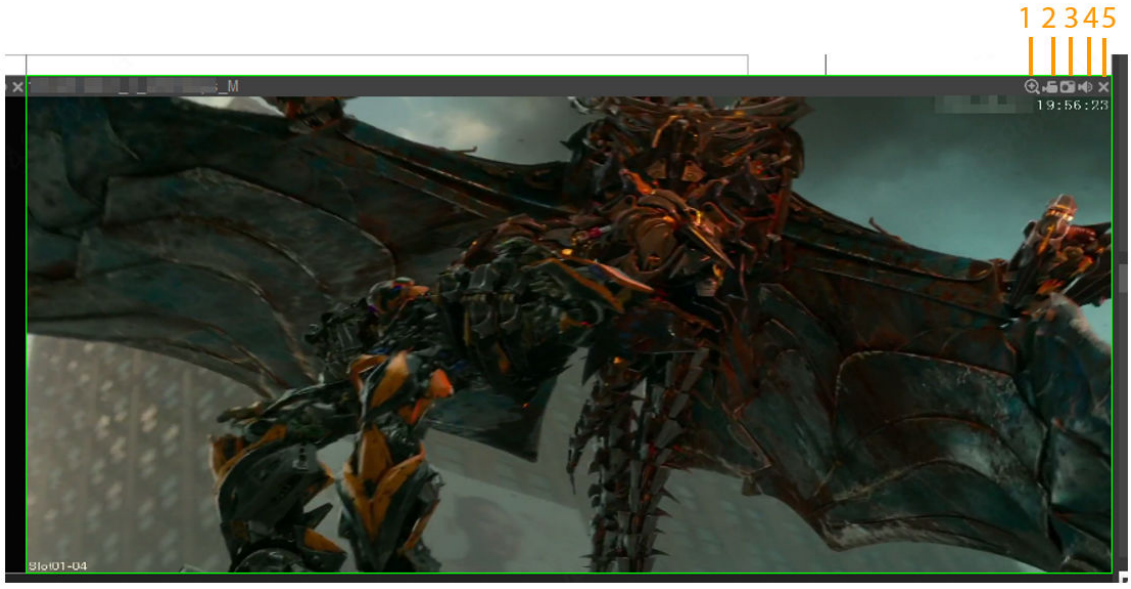


Table 3-6 Function description

No.	Name	Description
1	Digital zoom	• When the video is in the original status, click the icon, press and hold the left mouse button to select any area. The selected area will be zoomed in. When the video is zoomed in, press and hold the left mouse button to drag the video image. Right-click to restore original status. • Click it to zoom in and zoom out the video image with the wheel button.
2	Local videos recording	Record videos to your computer.

No.	Name	Description
3	Snapshot	Take a snapshot of the video.
4	Turn on the sound	Turn on the sound of video.
5	Close	Close the window.

3.4.2 Signal Configuration

After adding signals, you can view the information or the added signal group information, and configure signal preview.

3.4.2.1 Device Tree

Device tree displays the added network signals.

Displays signal source of the device on the **Remote Device** page.

3.4.2.2 Custom

You can customize signal group. The **Custom** tab displays added group and signal source. You can drag signal group to the window for loop play of signals in the group.

3.4.2.3 Video Preview

Add signal to preview window from **Device Tree** or signal group. Click the signal, and then view the video in the window.

3.4.3 PTZ Control

PTZ control is used to adjust the directions of PTZ device (up, down, left, right, upper left, upper right, lower left and lower right) and carry out scan, presets, patrol and pattern and other settings.

When using local serial port to control PTZ devices, you need to configure the parameters in advance and ensure the connection is right.

Figure 3-25 PTZ control

Table 3-7 Functions description

Function	Description
Scan	• Click **Setup** , and then turn the camera with direction buttons. Click **Set Left Border** and **Set Right Border** to configure the scan limit. • Click **Start** , and the PTZ starts to scan. Click **Stop** to stop scanning.
Preset	• Fixed point. Click **Add** to add a preset. • Enter the value of the preset, and then click **View**, the camera towards to the preset.
Point Tour	• Enter the preset number, and then click **Add** to the preset to the tour route. • Enter the tour route in the input box, and then click **Start** to start tour. Click **Stop** to stop tour.
Pattern	• Click **Add** to add a new pattern route through **Start Record** and **Stop Record**. • Enter the pattern value, and then click **Start** to start pattern. Click **Stop** to stop pattern.
Pan	Click **Start** , and then the PTZ starts to rotate horizontally. Click **Stop** to stop panning.

3.5 Setup

3.5.1 System Configuration

System configuration includes general settings, user management, backup, system maintenance, system upgrade, image management, font template, serial port management and security management.

3.5.1.1 General Configuration

Configure the device information includes device information and system date.

3.5.1.1.1 Configuring General Information

Create an area and enter any characters and then it will be displayed on LED screen.

Procedure

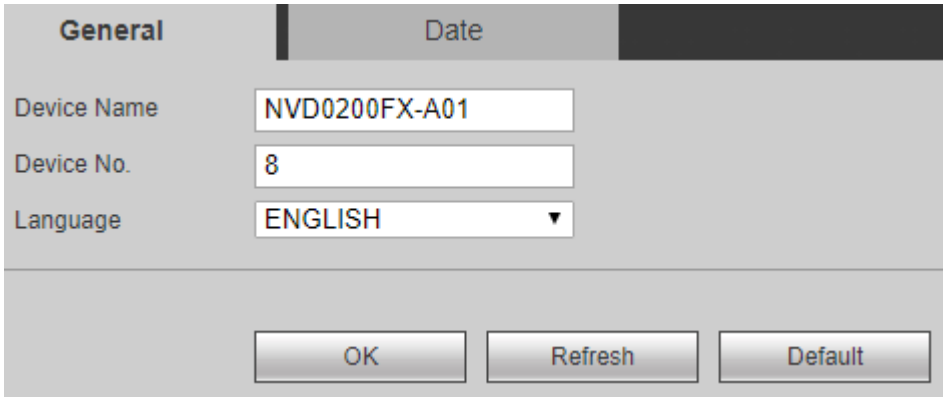
Step 1 Log in to the webpage.

Step 2 Select **Setup** > **System Config** > **General** > **General**.

Step 3 Configure the parameters.

- **Device Name and Device No.** : Name the device and set the number of the device to differentiate it from others.
- **Language** : The system language is determined by the language of program package.

Figure 3-26 General configuration



Step 4 Click **OK**.

3.5.1.1.2 Configuring the Date

Configure the date and time of the system or you can enable NTP (Network Time Protocol) according to your needs. After enabling NTP, video matrix platform (VMP) can synchronize the system time with the NTP server.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Setup** > **System Config** > **General** > **Date**.

Step 3 Configure the parameters.

Figure 3-27 Setting time

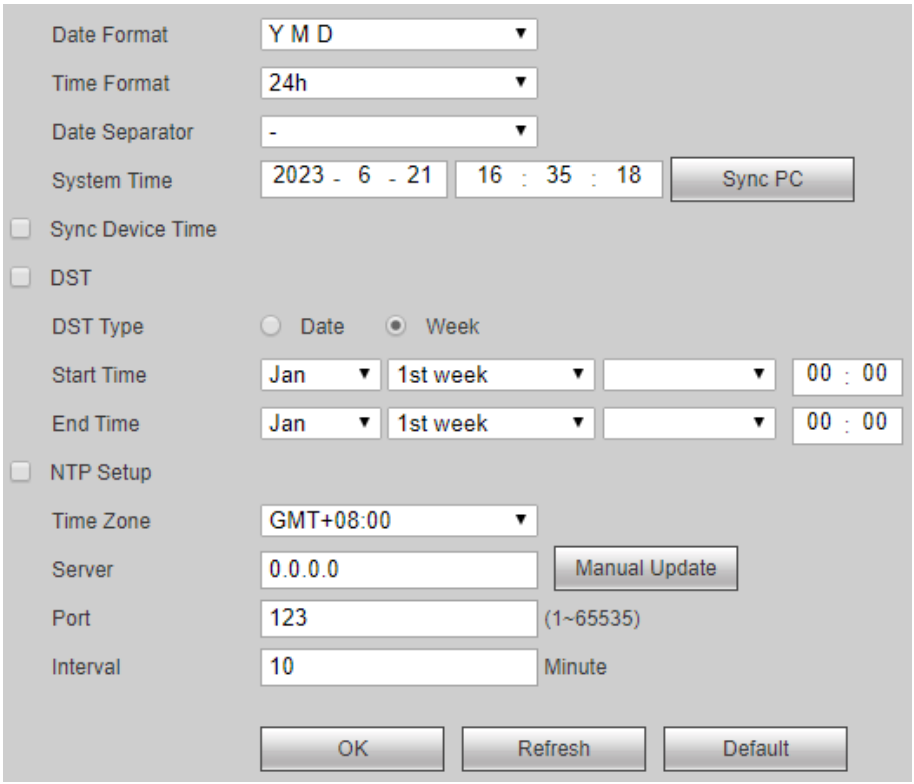


Table 3-8 Parameter description

Parameter	Description
Date Format	Select the format of the date and time, including **Y M D** , **M D Y** and **D M Y**.
Time Format	Select time format that you want to display, including 24 hour and 12 hour.
Date Separator	Select the date separator you want to display, including **.** , **-** and **/**.
System Time	Set the system time. Click **Sync PC** to synchronize the system time with current computer time.
Sync Device Time	Select the check box to enable **Sync Device Time**.
DST	Select the check box to enable DST.
DST Type	Select DST Type. You can select **Date** or **Week**.
Start Time/End Time	• When the **Date** is selected, enter the **Year**, **Month**, **Day**, **Start Time** and **End Time**. • When the Week is selected, select **Month** , **Week**, **Start Time** and **End Time** from the drop-down list.
NTP Setup	Select the check box to enable NTP, and the device time will be automatically synchronized with the server.
Time Zone	Select time zone from the drop-down list.
Server	Enter the server IP address or domain name.
Port	Enter the NTP server port number.

Parameter	Description
Interval	Configure the updating interval. The device updates with the NTP server regularly.

Step 4 Click **OK**.

3.5.1.2 User Management

User management and user group management are the two methods for managing the information of users.

- User name and group name support a maximum of 6 characters and must consist 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 characters (excluding ' " ; : &). Users can change their own password and password of other users.
- Up to 64 users and 20 user groups are supported.
- User management adopts a two-level method of group and user. Neither group names nor user names can be duplicated, and a user can only belong to one group.
- The user logged in cannot modify their own permissions.
- During initialization, the default user is admin and it enjoys high permissions when leaving factory.

3.5.1.2.1 Group

Different users might have different permissions to access the device. You can divide the users with the same permissions into one group. It is easy for you to maintain and manage the user information.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **System Config** > **User Management** > **User Management** > **Group**.

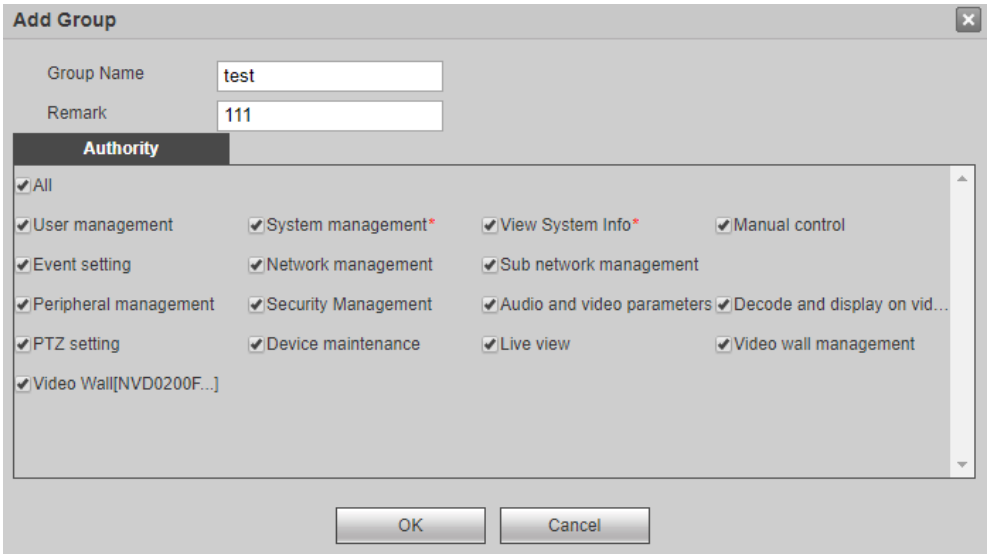
Step 3 Click **Add Group**.

Step 4 Enter the group name and the remark.

Step 5 Select operation authorities for the user from the authority list.

- Select the check box to enable the permission.
- Select **All** to select all permissions.

Figure 3-28 Add group



Step 6 Click **OK**.

3.5.1.2.2 Adding Users

Add one user to the group, and configure user permissions.

Procedure

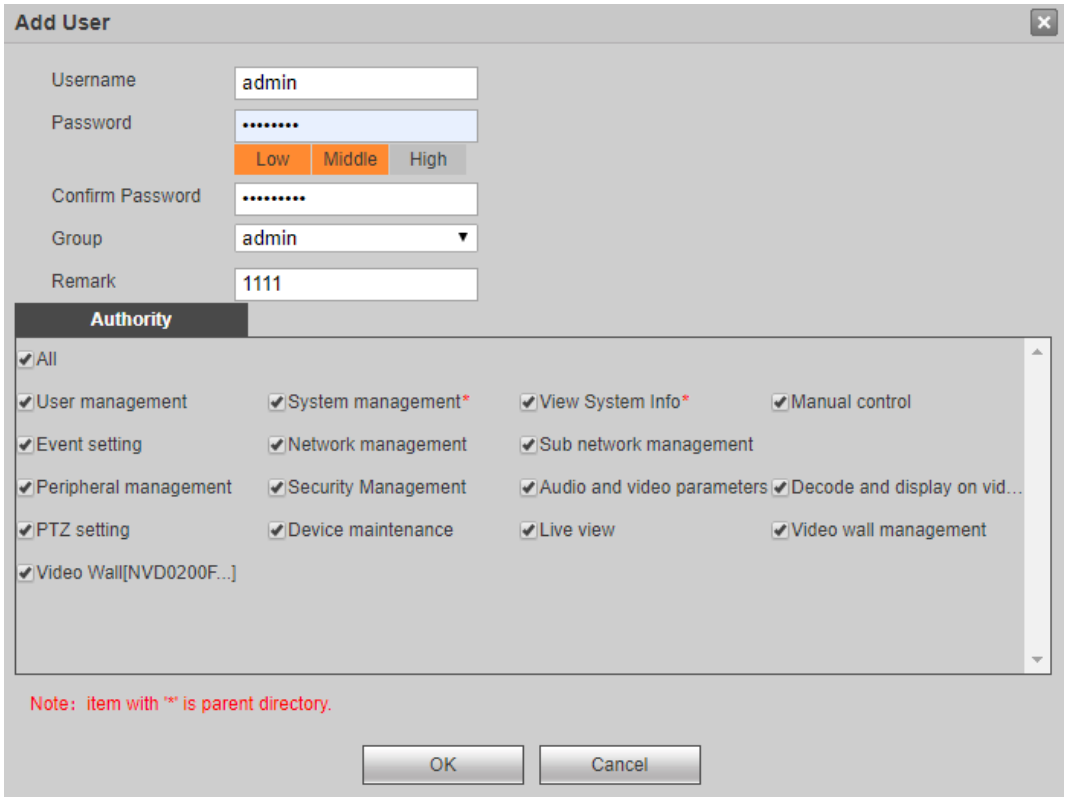
Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **System Config** > **User Management** > **User Management** > **User**, and then click **Add User**.

Step 3 Enter the username, password and confirm password. Select group and enter the remark.

- Once you select the group, the permission of the user cannot exceed permission attributes of the group.
- We recommend giving fewer permissions to normal users than premium users.

Figure 3-29 Add user



Step 4 Select operation permissions for the user from the authority list.

- Select the check box to enable the permission.
- Select **All** to select all permissions.

Step 5 Click **OK**.

3.5.1.3 Configuring Backup

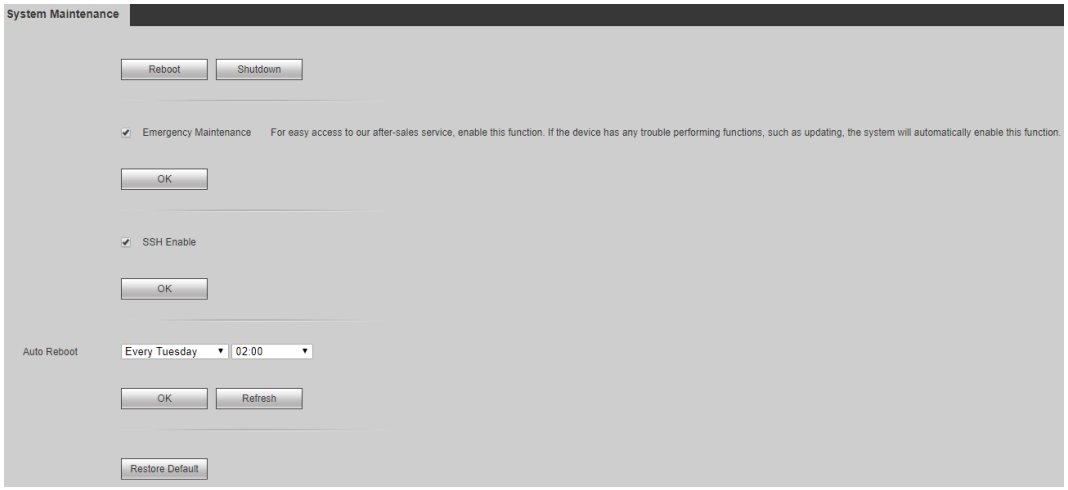
Select **Setup** > **System Config** > **Config Backup** > **Config Backup**, and then export the configuration file to the local computer for backup. When the device is abnormal, you can import configuration file to restore configuration quickly.

- Click **Import Config**, and then select configuration file (.backup) to import the configuration file.
- Click **Export Config**, and then select storage path to export configuration file for backup.

3.5.1.4 Auto Maintenance

Select **Setup** > **System Config** > **Auto Maintenance** > **System Maintenance**, and then you can restart, shutdown, enable SSH, configure automatic reboot and restore to default.

Figure 3-30 System maintenance



- To manually reboot the system, click **Reboot**, and the system restarts immediately.
- Select **Emergency Maintenance** , and then select **OK**. The function can be used with fault diagnostic tool.
- Select **SSH Enable** , and then click **OK** to enable remote debugging for technical stuff.
- When you select **Auto Reboot** , configure the week and time, and then click **OK**.

Click **Restore Default**, and then the configurations will be restored to defaults except network configurations.

3.5.1.5 System Upgrade

Store upgrade file in local computer that is associated with the device. You can import upgrade file to upgrade the system version.

Prerequisites

Import the upgrade file to the local computer.

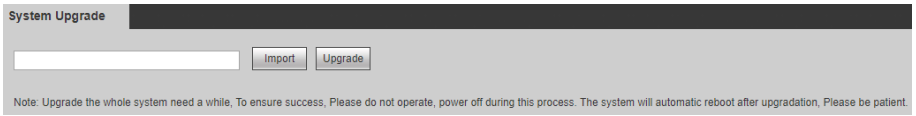
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **System Config** > **System Upgrade**.

Step 3 Click **Import**, and then select the update file.

Figure 3-31 System upgrade



Step 4 Click **Upgrade** to upgrade the system. There is a progress bar during upgrade.

Step 5 After the upgrading file uploaded, the device will reboot automatically.

Please keep the power supply on, and wait patiently until the system reboots successfully.

3.5.1.6 Picture Management

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **System Config** > **Picture Management**.

Step 3 Click **Browse** to select a local picture.

Step 4 Click **Upload** to upload local picture to the device.

Related Operations

- Select a picture, and then click **Delete** to delete it.
- After the background is uploaded successfully, select the background in video wall configuration.

3.5.1.7 Comm Setup

After the serial port parameters are configured, the device can connect other devices through serial port, for the purpose of debugging and operation.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **System Config** > **Comm Setup**.

Step 3 Configure the parameters.

Figure 3-32 Setting serial port

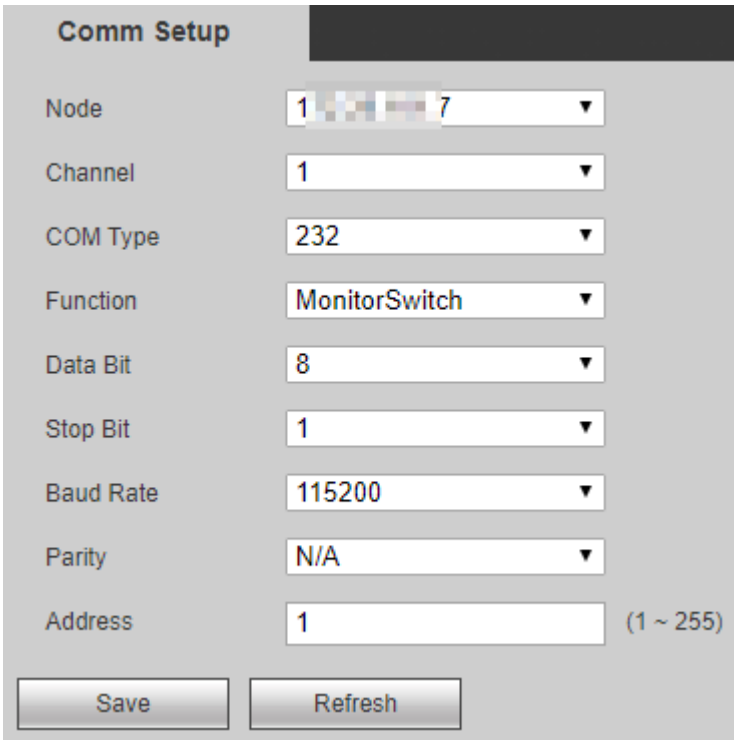


Table 3-9 Description serial port parameters

Parameter	Description
Node	Select the node to be configured.

Parameter	Description
channel	Select the channel you want to configure.
Com Type	The default serial port is RS-232.
Function	Configure comm function.
Data Bit	Select a data bit. The options includes 5, 6, 7 and 8.
Stop Bit	Select stop bit of comm, including 1 and 2.
Baud Rate	Configure Baud rate of comm. It shall be consistent with the device that will be connected. When select common serial ports, the baud rate is 115200 by default and cannot be changed.
Parity	Select a parity mode from **N/A** , **Odd**, **Even**, **Flag Parity** and **Empty Parity**.
Address	Configure COMM address from 0 to 255.

Step 4 Click **Save**.

3.5.1.8 Security Management

Configure firewall, system service, HTTPS, security exception linkage, static ARP bind, enable or disable HTTPS as needed to improve system security management.

3.5.1.8.1 Firewall

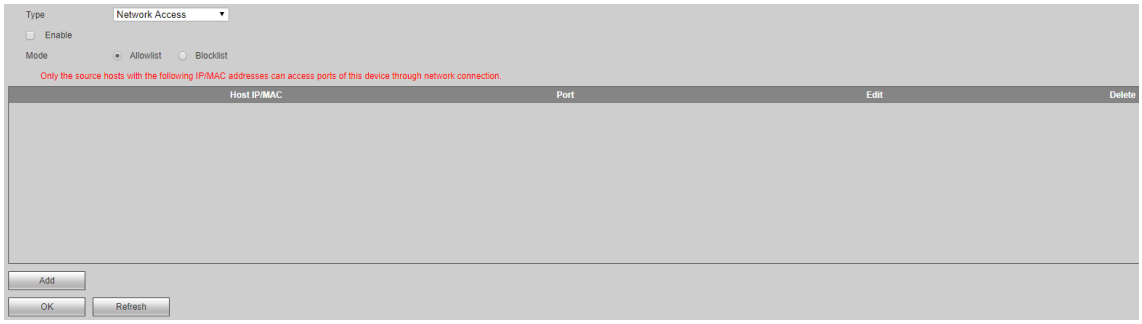
Select **Enable** to enable the firewall.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **System Config** > **Security Management** > **Firewall**.

Figure 3-33 Firewall



Step 3 Select **Type** , supports **Network Access**, **Prohibited Ping** and **Semi join**.

- Network Access: Add the IP address to allowlist or blocklist to allow or restrict it from accessing the corresponding ports of the device.
- Forbid Ping: IP address of the device is prohibited from ping. This helps to prevent unauthorized attempts at accessing your network system.
- Semi join: After it is enabled, the probability of network connection is 50%.

Step 4 Select **Enable**.

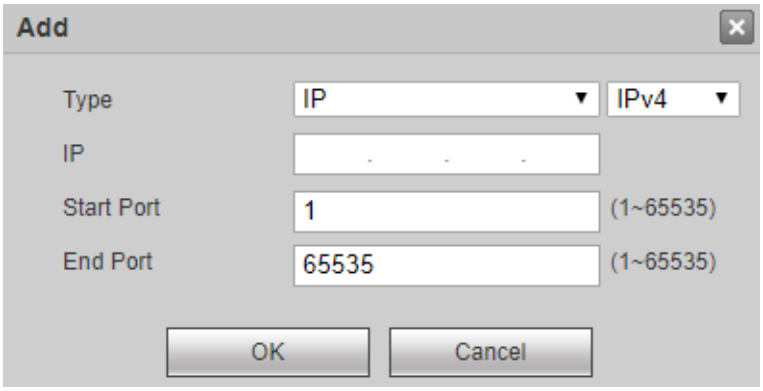
Step 5 (optional) Select **Mode**, and then configure Blocklist and Allowlist.

- Allowlist: Only the listed IP or MAC addresses are allowed to visit corresponding ports.
- Blocklist: The listed IP or MAC addresses are prohibited from visiting the corresponding ports.

- Only **Network Access** supports configuring allowlist and blocklist.
- The configuration of blocklist and allowlist is identical, here uses allowlist configuration as an example.

1. Select **Allowlist**.
2. Click **Add**.

Figure 3-34 Add



3. Select the type, and then configure the IP address, enter IP address, start port, end port and more.

Support IP Address, IP Network Segment and MAC address. The Differentiated by the parameters, you need to configure the parameters according to actual situation.

4. Click **OK**.

Step 6 Click **OK**.

Related Operations

You can upload image to the system, and set the uploaded image to the screen background.

3.5.1.8.2 System Service

Select the system service you want to enable.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **System Config** > **Security Management** > **System Service**.

Step 3 Enable system service according to actual situation.

Figure 3-35 System service

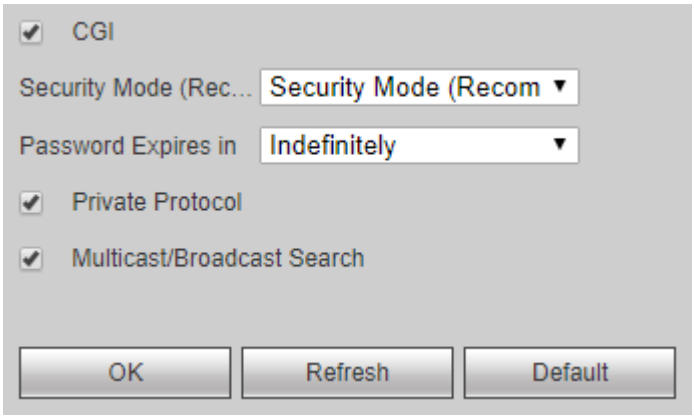


Table 3-10 System service parameter description

Parameter	Description
CGI	Common Gateway Interface (CGI) is the port between external application programs and web server. Enable this function, and then devices access the webpage through CGI.
Security Mode	Security mode is recommended. After **Compatibility Mode** is enabled, there might be security risks.
Password Expires in	Configure the password update period. You can select indefinitely, 30 days, 60 days, 90 days and 180 days.
Private Protocol	Enable private protocol.
Multicast/Broadcast Search	Select to enable multicast/broadcast search function.

Step 4 Click **Save**.

Related Operations

- Click **Refresh** to clear the unsaved configurations.
- Click **Default** to restore the device to default settings.

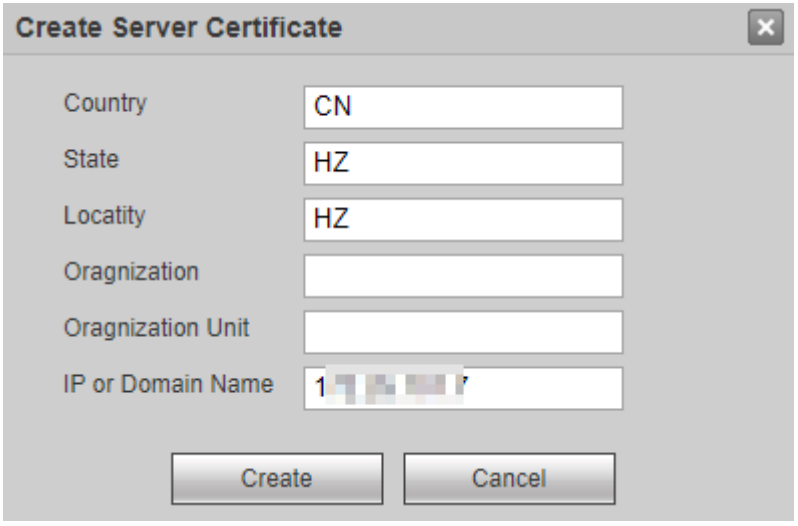
3.5.1.8.3 HTTPS

Background Information

On the HTTPS page, users can create certificate or download authenticated certificate to enable HTTPS protocol, and log in to the computer through HTTPS. It can ensure the confidentiality of data and secure communication, and guarantee the safety for user information and device through reliable and stable technical approach.

- For the first time to use this function or after changing the device IP address, click **Create Server Certificate** to create server certificate again.

Figure 3-36 Create server certificate



- For the first time to use HTTPS after changing the computer, you need to click **Download Root Certificate**.
- If a local signature certificate already exists in local computer, click **Install Signature Certificate** to select the certificate.
- Reboot to enable HTTPS.

Procedure

Step 1 Log in to the webpage of the device.

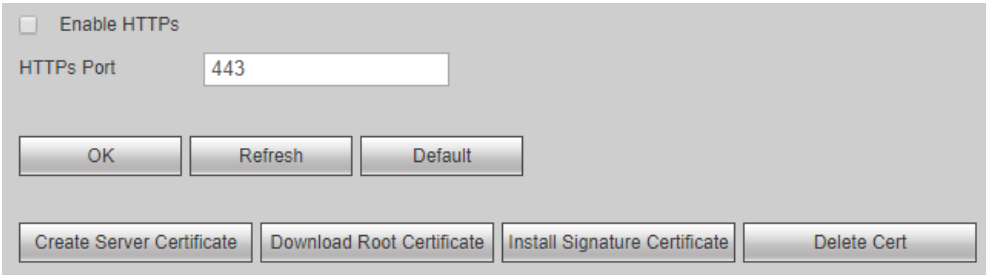
Step 2 Select **Setup** > **System Config** > **Safe Management** > **HTTPS**.

Step 3 Select **Enable HTTPS**.

Step 4 Configure HTTPS port.

Step 5 Click **OK**.

Figure 3-37 HTTPS



When HTTPS is enabled, you cannot access the device through HTTPS. The system will switch to HTTPS if you access the device through HTTPS.

The created and installed certificates that are deleted cannot be restored. Please be advised.

3.5.1.8.4 Security Exception Linkage

Background Information

Set alarm actions. Execute alarm linkage actions when an abnormal event occurs.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **System Config** > **Security Management** > **Security Exception Linkage**.

Step 3 Select **Enable** to enable abnormal alarm linkage.

Step 4 Select alarm linkage including **B uzz** and **Log.**

You can select two alarm linkage method at the same time.

Step 5 Click **OK**.

3.5.1.8.5 Static ARP Binding

Bind devices on a LAN to a fixed IP address through Address Resolution Protocol (ARP), and then other devices cannot use the IP address. In this way, you can manage the devices on the LAN better.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **System Config** > **Security Management** > **Static ARP Binding**.

Step 3 Select **Static ARP Binding** checkbox, enter the **IP** and **MAC Address**.

Step 4 Click **OK**.

3.5.2 Network

3.5.2.1 TCP/IP

Set the IP address and DNS server of the device according to the network planning.

Prerequisites

- Before configuring network parameters, make sure that the device is connected to the network properly.
- If there is no router in the network, assign an IP address on the same network segment.
- If there is a router in the network, set the corresponding gateway and subnet mask.

Procedure

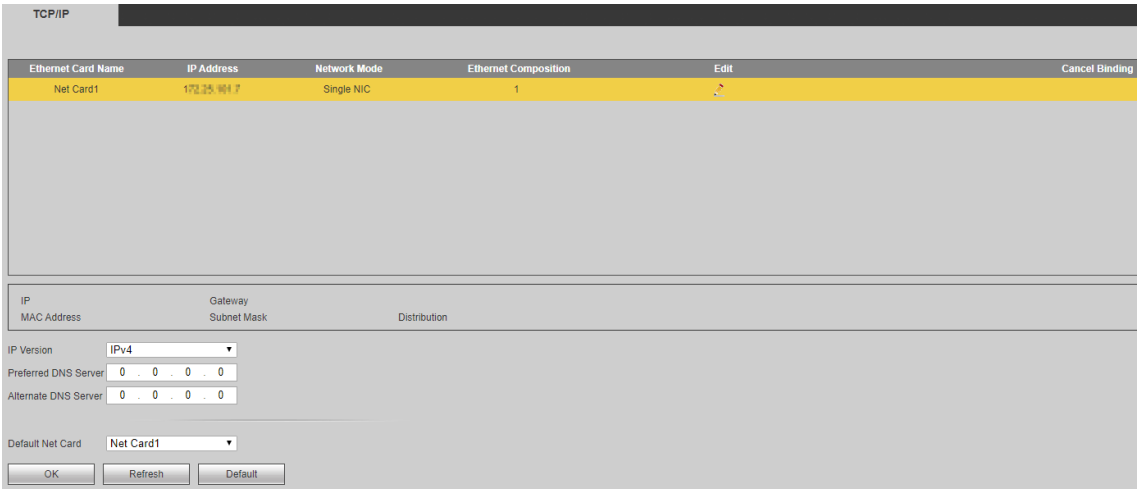
Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Network** > **TCP/IP**.

Step 3 Configure TCP/IP parameters.

- IP Version: It is IPv4 by default.
- Preferred DNS Server: Fill in the configured IP address of DNS server.
- Alternate DNS Server: Fill in the configured IP address of alternate DNS server.
- Default Net Card: Select default network card.

Figure 3-38 TCP/IP



Step 4 Click to edit Ethernet card information.

Figure 3-39 Modify Ethernet card

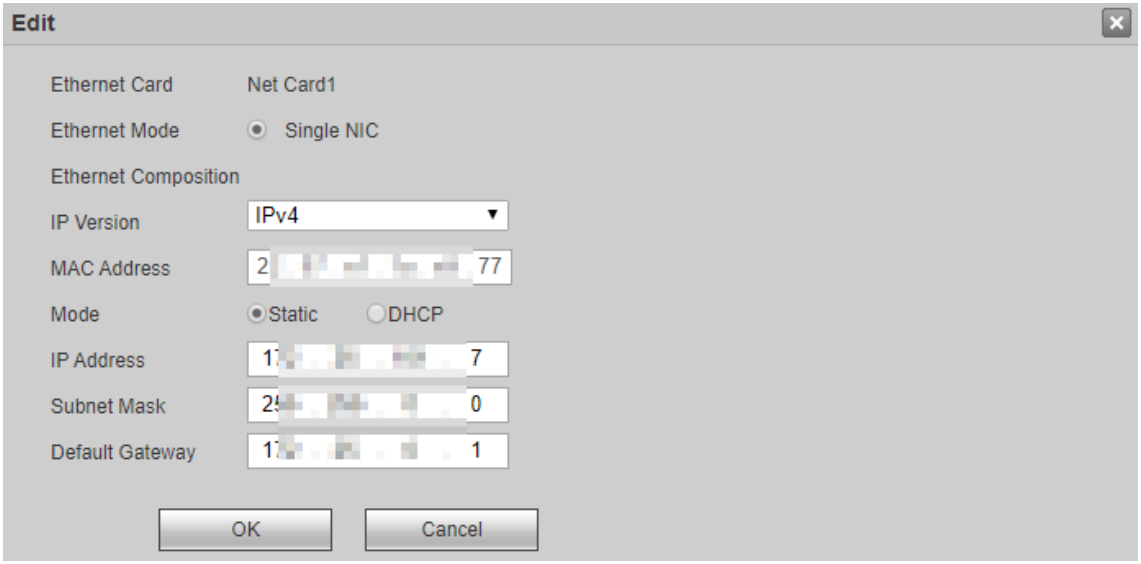


Table 3-11 Parameters description

Parameter	Description
Ethernet Mode	Single NIC: Multiple Ethernet cards can be used independently. You can use any NIC to request the HTTP and RTSP services. Set up a default NIC (NIC 1 by default) to apply for DHCP, Email, FTP, and other network services initiated from the device. During network status detection, if one network card is disconnected, network is believed to be disconnected.
IP version	It is IPv4 by default.
MAC address	Display the MAC address of the device.

Parameter	Description
Mode	• Static: You need to manually enter the IP address, subnet mask, and gateway. • DHCP: Automatically obtains IP. When enabling DHCP, the IP address, mask and default gateway cannot be configured manually. ◇ If DHCP is effective, the obtained information will be displayed in **IP Address** box, **Subnet Mask** and **Default Gateway**. If DHCP is not effective, they all display 0. ◇ To view manually defined IP when DHCP is not effective, disable DHCP first, and then the device will display IP information that is not obtained through DHCP. If DHCP is effective, when 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 **Default Gateway**. The IP address and the default gateway must be on the same network segment.
Subnet Mask	
Default Gateway	

Step 5 Click **OK** to complete modification of net card information.

Step 6 Click **OK**.

3.5.2.2 Port

Set max connection number and port number to visit the device through client (including webpage and desktop client).

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Network** > **Port** > **Connection Setup**.

Step 3 Configure max connection and port number and their respective values.

Figure 3-40 Setting connection

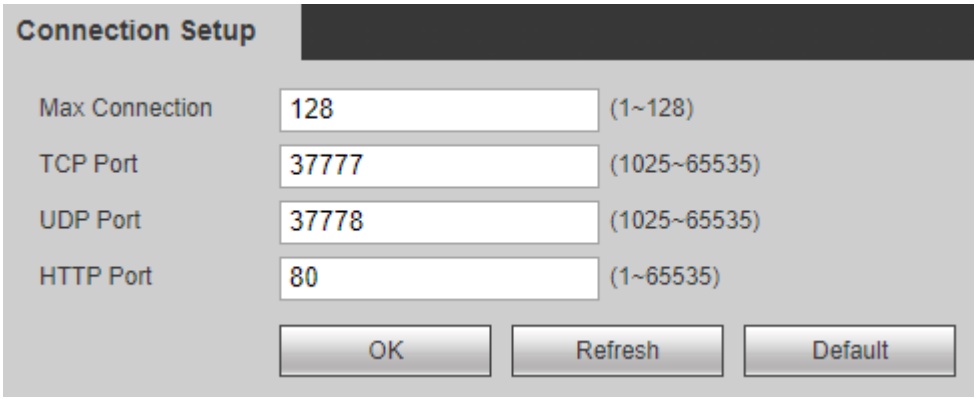


Table 3-12 Description of port parameters

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. You can enter the value as needed. The default value is 37777.
UDP Port	User datagram protocol port. You can enter the value as needed. The default value is 37778.
HTTP Port	HTTP transmission port. You can enter the value as needed. The default value is 80. If you enter other values, enter the modified port number after the IP address when logging in to the device through the browser.

Step 4 Click **OK**.

Except for **Max Connection**, modifications of other parameters will take effect after reboot.

3.5.2.3 Synchronizing IP

Sync IP address of a device with the timing function, to synchronize system time, and ensure the system time is correct.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Network** > **Sync IP**.

Step 3 Enter the IP address, and then click **Add**.

Step 4 Click **OK**.

3.5.3 Event Management

Set alarm mode of abnormal events for the device. When an abnormal event occurs during local device operation, alarm linkage is triggered.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Event Management** > **Abnormal**.

Step 3 Select abnormality mode, including **Network Offline** , **IP Conflict**, and **MAC Conflict**.

Step 4 Select the **Enable** check box, and then configure the parameters.

The parameters of the 3 abnormal event should be the same.

Figure 3-41 Abnormal event handling

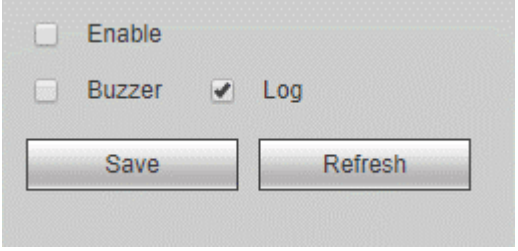


Table 3-13 Parameters description of abnormal handling

Parameter	Description
Buzzer	The system activates a buzzer alarm when an alarm event occurs.
Logs	The log records alarm information when an alarm event occurs.

Step 5 Click **Save**.

Cascade Configuration

Set the operating device as the main node, and add other devices as the sub nodes. In cascade system, you can use any output ports of the devices to create video wall.

Procedure

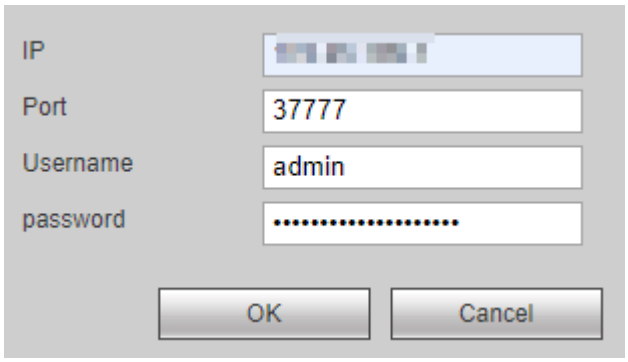
Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Cascade Config** > **Cascade Config**.

Step 3 Click **Add**.

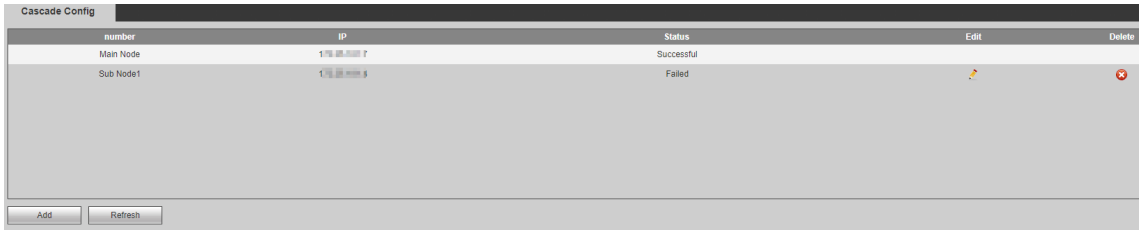
Step 4 Enter the IP address, port number, username, and password of the sub node device.

Figure 3-42 Add child node



Step 5 Click **OK**.

Figure 3-43 Sub node



- Main node can delete any sub nodes from cascade system.
- Sub node can be removed from the cascade system, and then you can perform operations on the webpage.

Related Operations

- Click to edit sub node information.
- Click to delete the sub node.

3.5.4 Signal Management

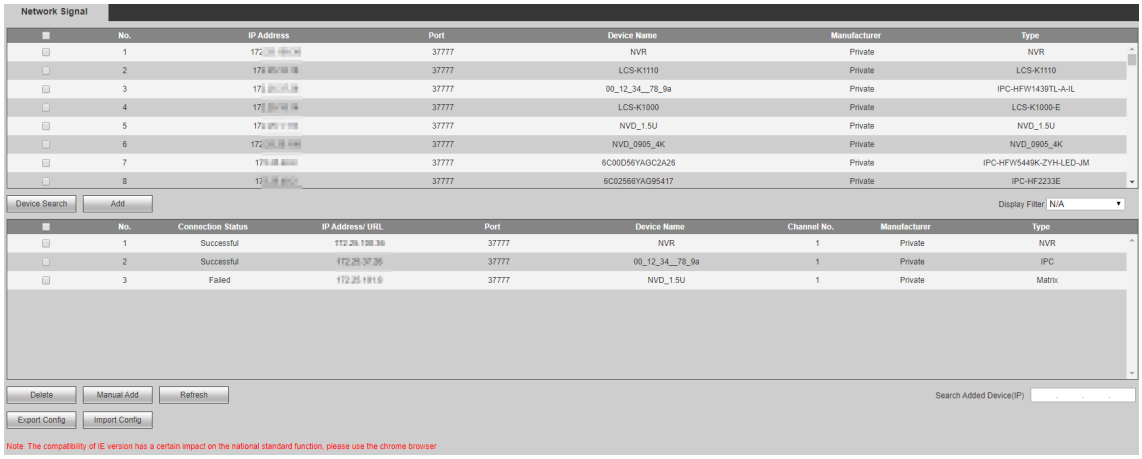
You can manage network signal, local signal, and add signal groups.

3.5.4.1 Network Signal

Select **Setup** > **Signal Management** > **Network Signal**, and then you can add devices in the network to preview and display network signal on wall, and also control the remote device.

The device shall have a decoding card, so network signal can be decoded and displayed on the video wall.

Figure 3-44 Network signal



3.5.4.1.1 Adding Signals in Batches

Procedure

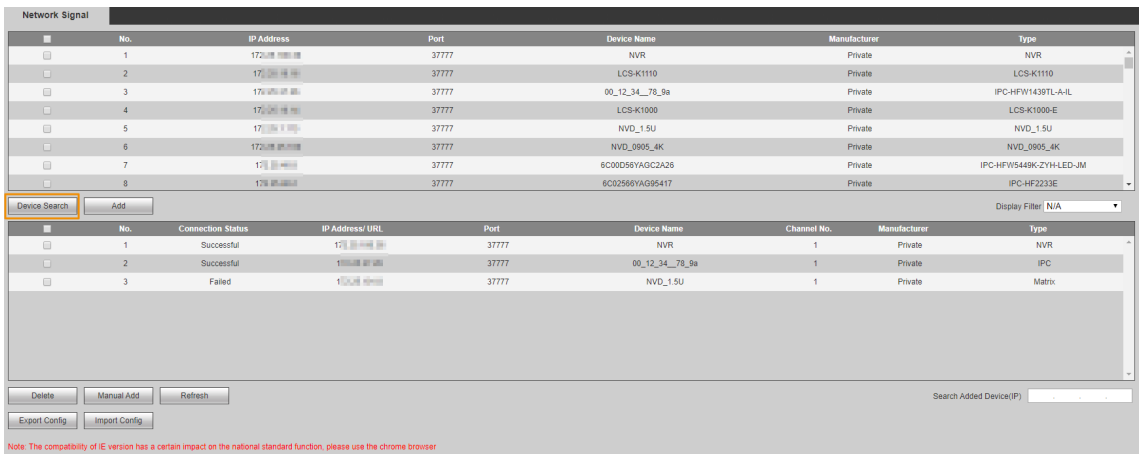
Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Signal Management** > **Network Signal**.

Step 3 Select the check box corresponding to the network signal, and then click **Add**.

- If the device is in normal use, **Connection Status** will change from **Failed** to **Successful** after several seconds. The system will display **Saved Successfully** again.
- If **Connection Status** remains **Failed**, the device might not be started, or a block list has been configured, or it is not included in a allowlist.

Figure 3-45 Add signals



Related Operations

- Search for devices
  - Filter device type in **Display Filter**. For example, select IPC, and then all IPC devices will be displayed here.
  - Enter IP address in **Search Added Device (IP)** search box, and then the device information will be highlighted in yellow on the list.
- Delete devices

  Select devices from the device list, and then click **Delete**.
- Sort

  Click each attribute field, and will appear on the right of the field, which means that the network signal is arranged in descending order. Click it again, and the icon turns into , meaning the network signal is arranged in ascending order.

3.5.4.1.2 Adding Signals Manually

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Signal Management** > **Network Signal**, and then click **Manual Add**.

Step 3 Enter the device parameters.

- The system supports **Private** , **Hikvision**, **Onvif**, and **General**. Select the protocol according to the devices.
- The parameters might be different depending on actual situation. We use **P rivate** protocol as an example.

Figure 3-46 Manual add

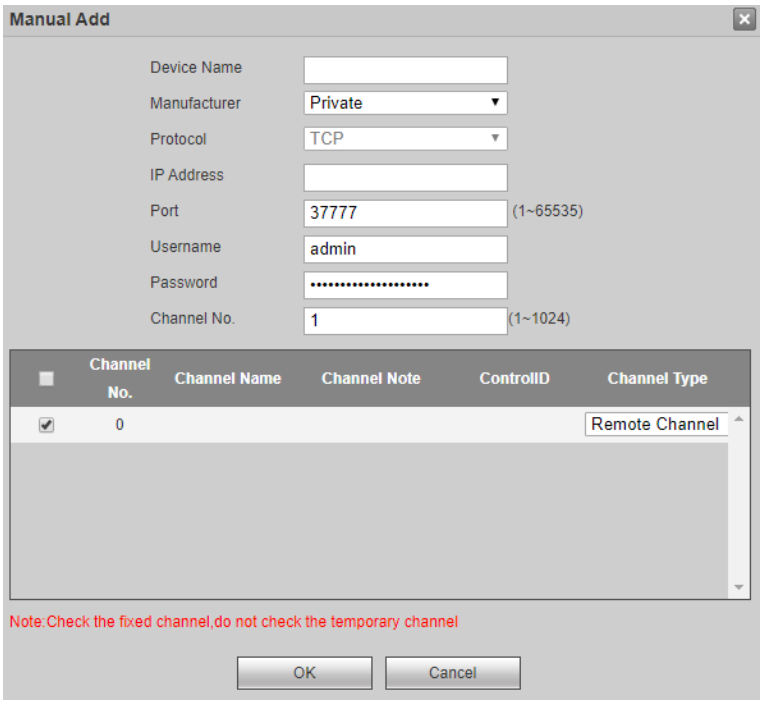


Table 3-14 Description of manual add parameters

Parameter	Description
Device Name	Enter the custom device name to differentiate it from others.
Manufacturer	Private.
Protocol	Transmission Control Protocol (TCP) is the default protocol and cannot be changed.
IP Address	Enter the IP address of the device to be added.
Port	TCP service port. You can enter the value as needed. The value is 37777 by default.
Username	Username and password used to log in to the device.
Password	
Channel No.	The total number of channels.

Step 4 (Optional) Configure the note, control ID and channel type.

- **Control ID** can correspond to the binding source (such as keyboard), so the binding source can be displayed on video wall.
- The channel type is remote channel by default.

Step 5 Click **OK**.

3.5.4.1.3 Importing and Exporting Configuration

Import and export configurations, to add network signals in batches.

Prerequisites

Enable HTTPS before using import and export configuration.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Signal Management** > **Network Signal**.

Step 3 Import or export configurations.

- Click **Import Config** to import the preset device information into the system.
- Click **Export Config** to export configuration files and save them to your local computer.

Step 4 (Optional) Click **Import Config** or **Export Config** in HTTPS environment. You need to login again, and then click **Import Config** or **Export Config**.

3.5.4.2 Signal Grouping

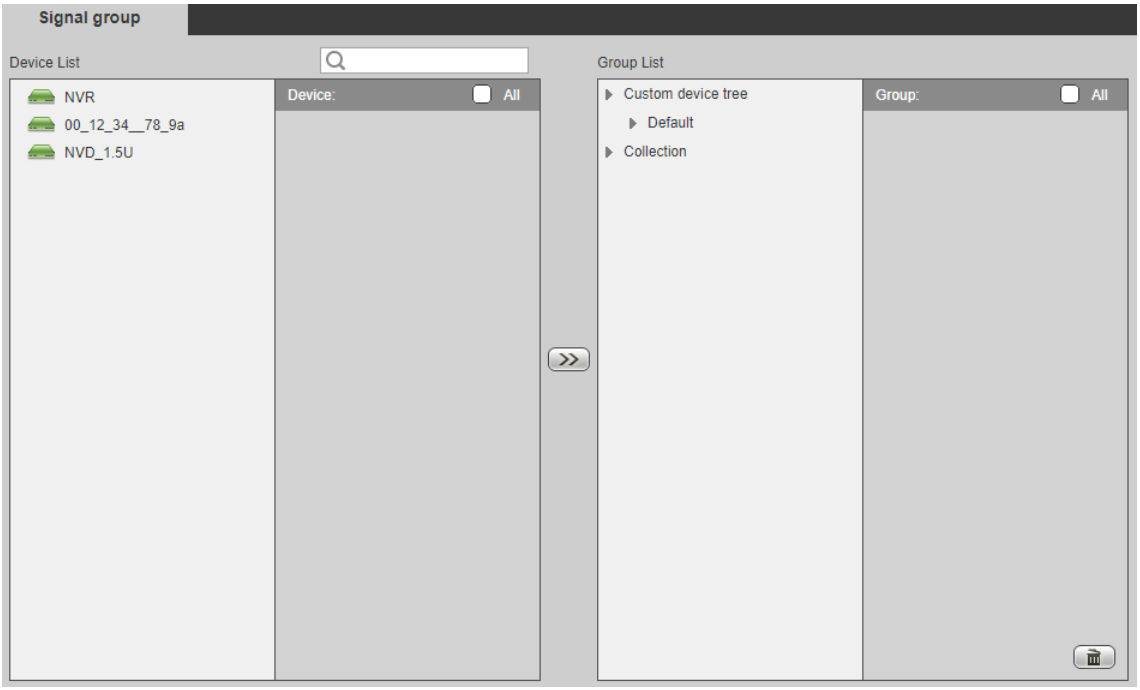
You can customize signal group and drag signals on the wall or for loop play of signals in the group.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Signal Management** > **Signal Group**.

Figure 3-47 Signal group



Step 3 Add Groups.

1. Move your mouse to **Custom device tree** or **Collection** in **Group List**, and then click +.
2. Enter the group name, and then click **OK**.
3. Move your mouse to the name of newly created group to edit the group.

Click + to create a sub group under this group. Sub group cannot be created for groups in **Collection**.

Step 4 Select a signal.

1. Select a device from **Device List**.
2. Select one signal or multiple signals.

Step 5 Select one group, and then click >>.

3.5.5 Display Management

You can configure video wall, manage screen, configure output screen, output name, and structured information.

3.5.5.1 Adding Video Walls

You can configure video walls according to actual quantity of screens, so signals can be displayed on video walls.

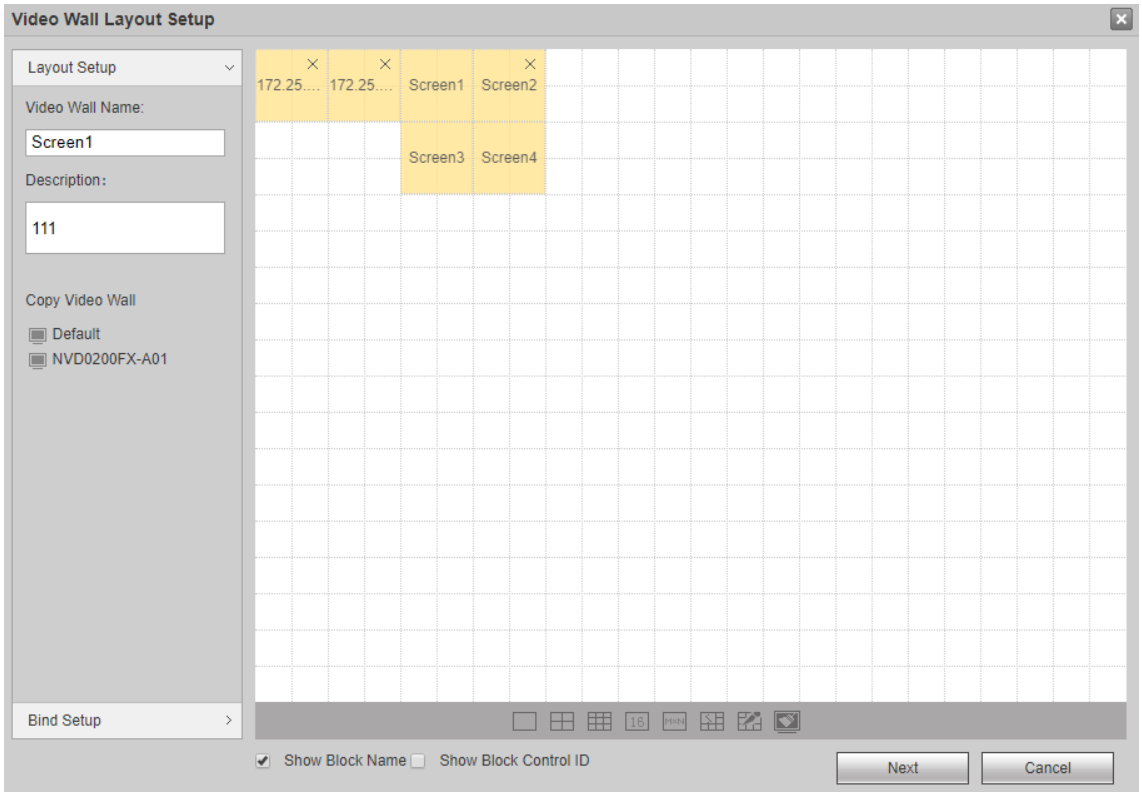
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Display Management** > **Video Wall Setup**.

Step 3 Click **Add Video Wall** to configure video wall layout.

Figure 3-48 Video wall layout configuration



1. Customize **Video Wall Name** and **Description**.
2. Click icons at the bottom of the page to add single screen and split screen quickly.

Press and hold the mouse to drag the screen to any positions you want.

Table 3-15 Parameters description

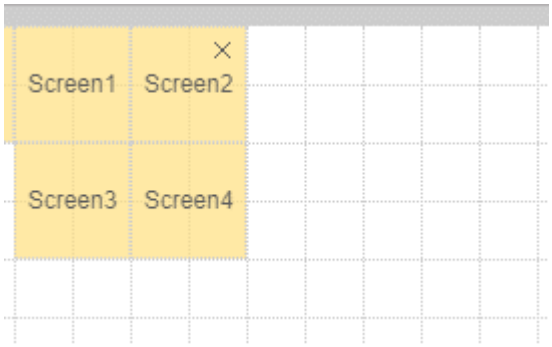
Icon	Name	Description
	Single screen and splicing screen	Click the icon to add single screen, 4-split, 9-split or 16-split screen.
	Customized splicing	Click this icon, enter row and column number in the pop-up **User Custom** page, and then add a custom screen.
	Splicing	Select single screens, and click the icon to splice them. ● Splicing screen cannot be selected. ● Single screens must be connected horizontally or vertically.
	Cancel splicing	Select splicing screens, and click this icon to cancel splicing.
	Screen clearing	Clear all screens on the video wall.

3. (Optional) You can select existing video wall from the **Copy Video Wall** zone on the left, and then display the video wall layout on the right. You can modify the layout directly.

Step 4 (Optional) Select **Show Block Name** or **Show Block ID**, and then every splicing screen will display a block name or ID.

- You cannot select **Show Block Name** and **Show Block Control ID** at the same time.
- Double-click to modify block name.

Figure 3-49 Display block name

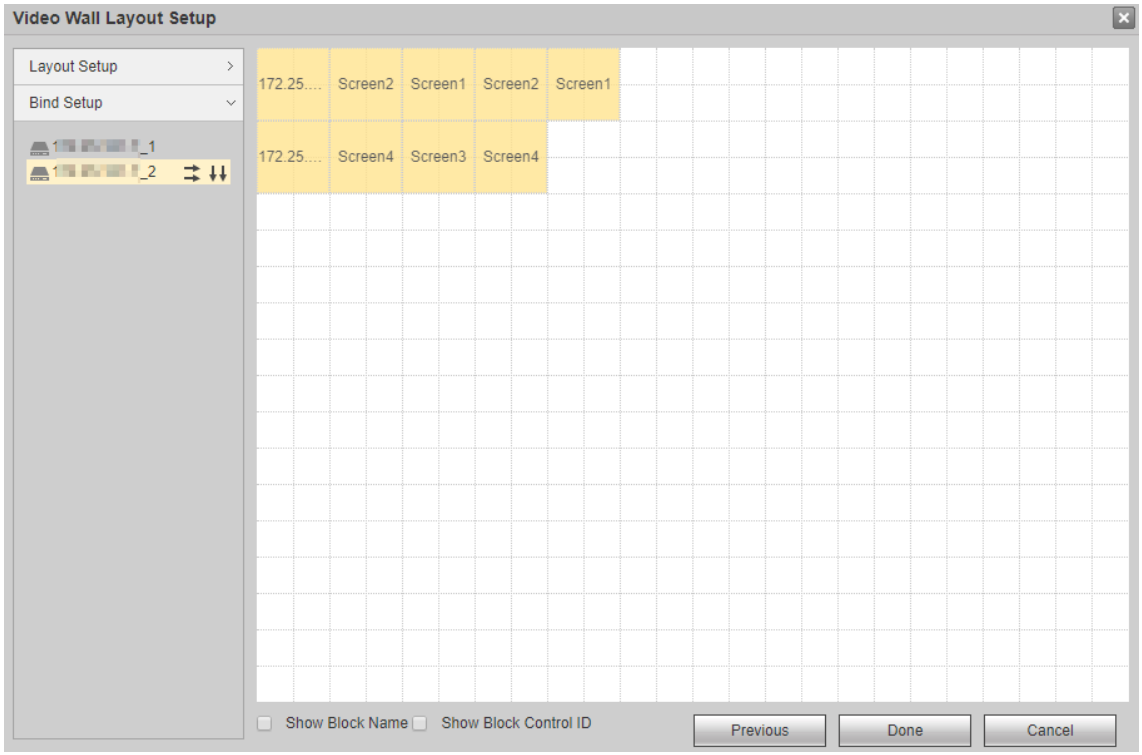


Step 5 Click **Bind Setup**.

Step 6 Press and hold the mouse to drag the slot to the screen, and bind the slot channel with screen.

- All screens on the video wall should be bound with slot channel.
- Slot cannot be bound repeatedly. In case of error, drag a correct slot channel to the screen to cover it directly.
- Click to bind the channel horizontally.
- Click to bind the channel vertically.

Figure 3-50 Slot binding



Step 7 Double-click a new video wall block to configure block parameters.

Figure 3-51 Block configuration

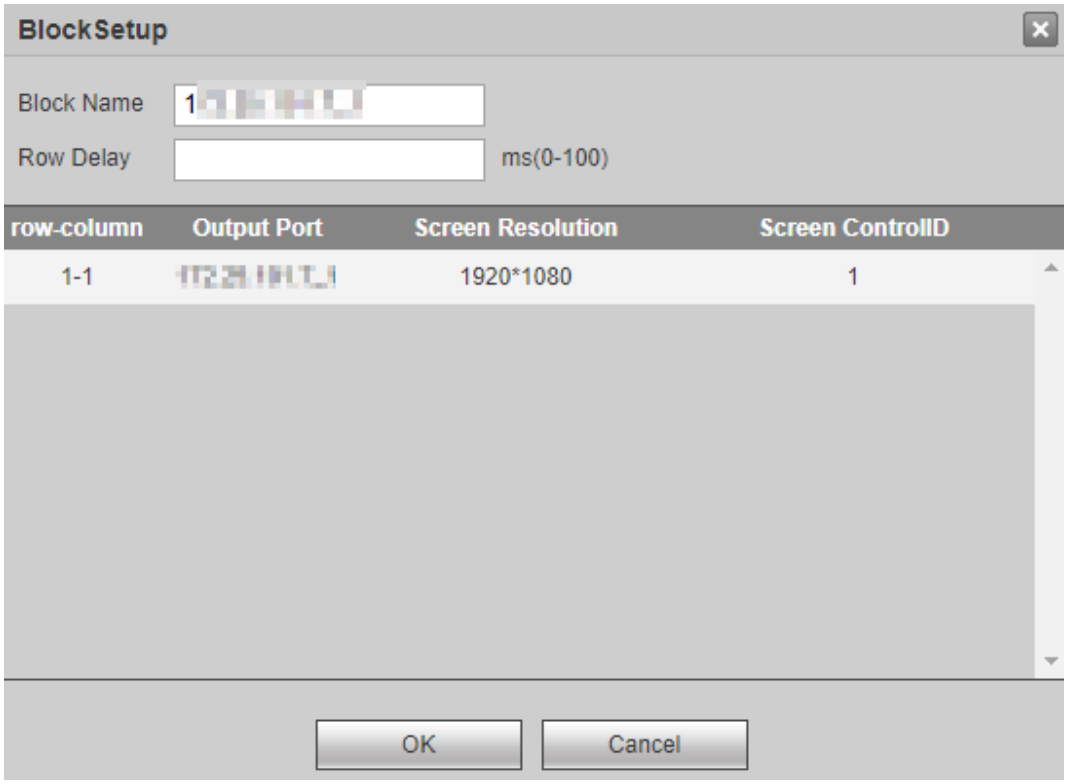


Table 3-16 Description of block configuration parameters

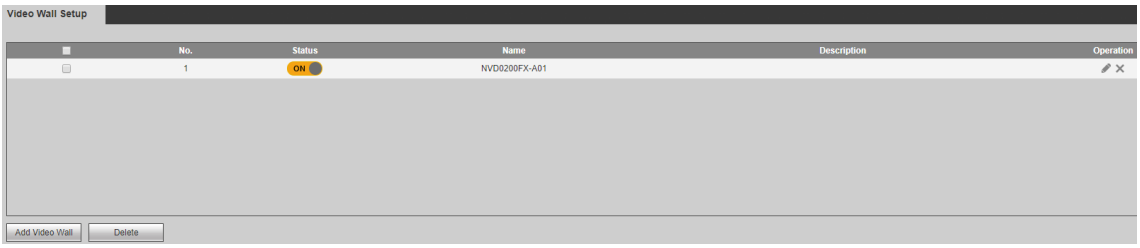
Parameter	Description
Name	Configure block name.
Row Delay	Configure row delay time ranging from 0 ms to 100 ms to display video synchronously.
Resolution	Select **Custom** to configure the resolution of output screen corresponding to each slot.

Step 8 Click **OK**.

Step 9 Click **Done**.

The system exits the **Video Wall Layout Setup** page. The new video wall is displayed in video wall list.

Figure 3-52 Add video wall



The new video wall is on by default. Click ON to turn off it.

3.5.5.2 Screen Management

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

3.5.5.2.1 Output Screen Setup

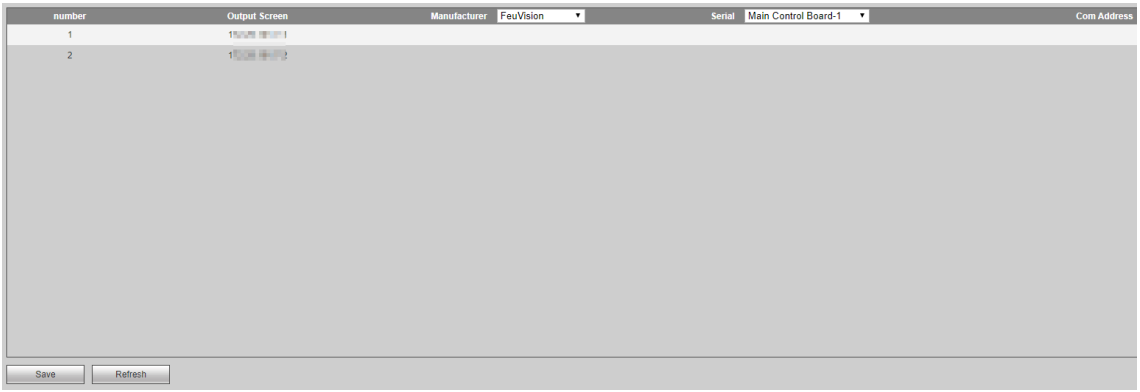
Configure manufacturer, port and port address of every output screen. To realize communications between screen and device, port address must be the same with DIP address of video wall.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Display Management** > **Screen Management** > **Screen Setup**.

Figure 3-53 Screen setup



Step 3 Click drop-down list or text box to configure manufacturer, port and port address.

- They should be the same with actual manufacturer, port and port address (DIP address) of video wall.
- Click the drop-down list on the **Title** can configure manufacturer and serial port.

Step 4 Click **Save**.

3.5.5.2.2 Screen On/Off

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

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Display Management** > **Screen Management** > **Screen ON/OFF**.

Step 3 Enable **Regional Switch** to enable the function, and then configure the parameters.

- **Switch Times** : The times of sending on/off command.
- **Switch Interval** : Interval of sending on/off command.
- **Screen Interval** : The interval for every screen to receive on/off command.

Step 4 Click **OK**.

3.5.5.2.3 Screen Timer

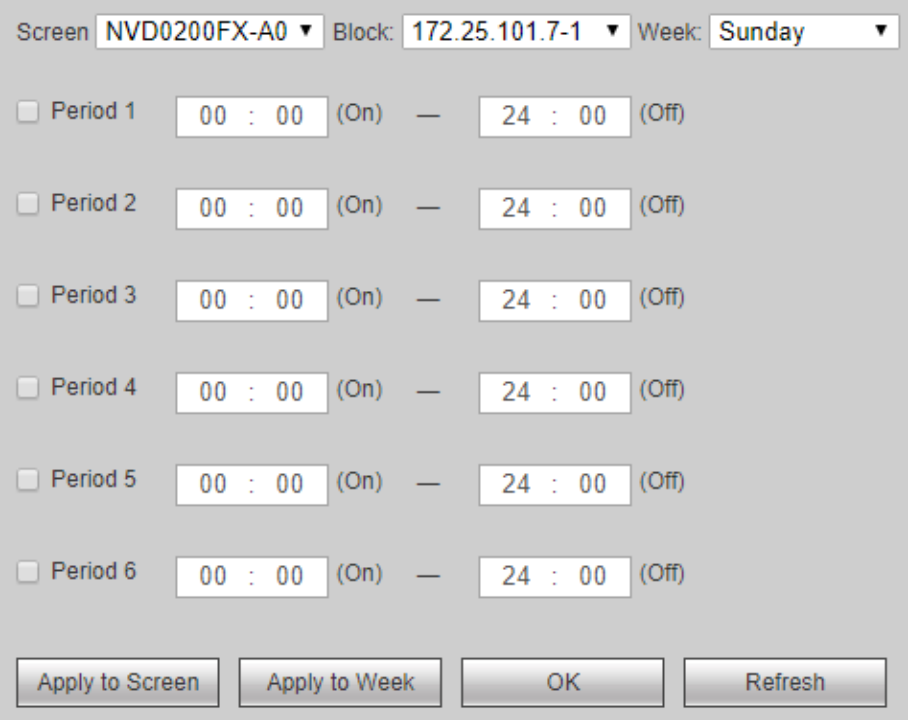
Configure fixed on/off time for every screen, and then every screen will be turned on/off at the fixed time.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Display Management** > **Screen Management** > **Screen Timer**.

Figure 3-54 Screen timer



Step 3 Select **Screen** , **Block** and **Week**.

Step 4 Select corresponding period, and then configure on/off time.

Step 5 Click **OK**.

Related Operations

- Click **Apply to Screen**, and then select another slot in the pop-up page to apply this configuration slot.
- Click **Apply to Week**, and then select another week in the pop-up page to apply this configuration week.

3.5.5.2.4 Screen Custom Control

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Display Management** > **Screen Management** > **Screen Custom Control**.

Step 3 Select **Enable**.

Step 4 Configure **Screen on command** and **Screen off command**.

You need to set hexadecimal number.

Step 5 Click **Save**.

3.5.5.3 Display Setup

You can configure display parameters, enable main/sub stream automatic switch, window prompt information, and more.

3.5.5.3.1 Configuring Display Setup

You can configure the resolution, video mode, output port, hue, brightness contrast, saturation and other parameters of the display to adjust the display.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Display Management** > **Display Setup** > **Display Setup**.

Step 3 Configure the parameters of output screen.

Figure 3-55 Configure output screen

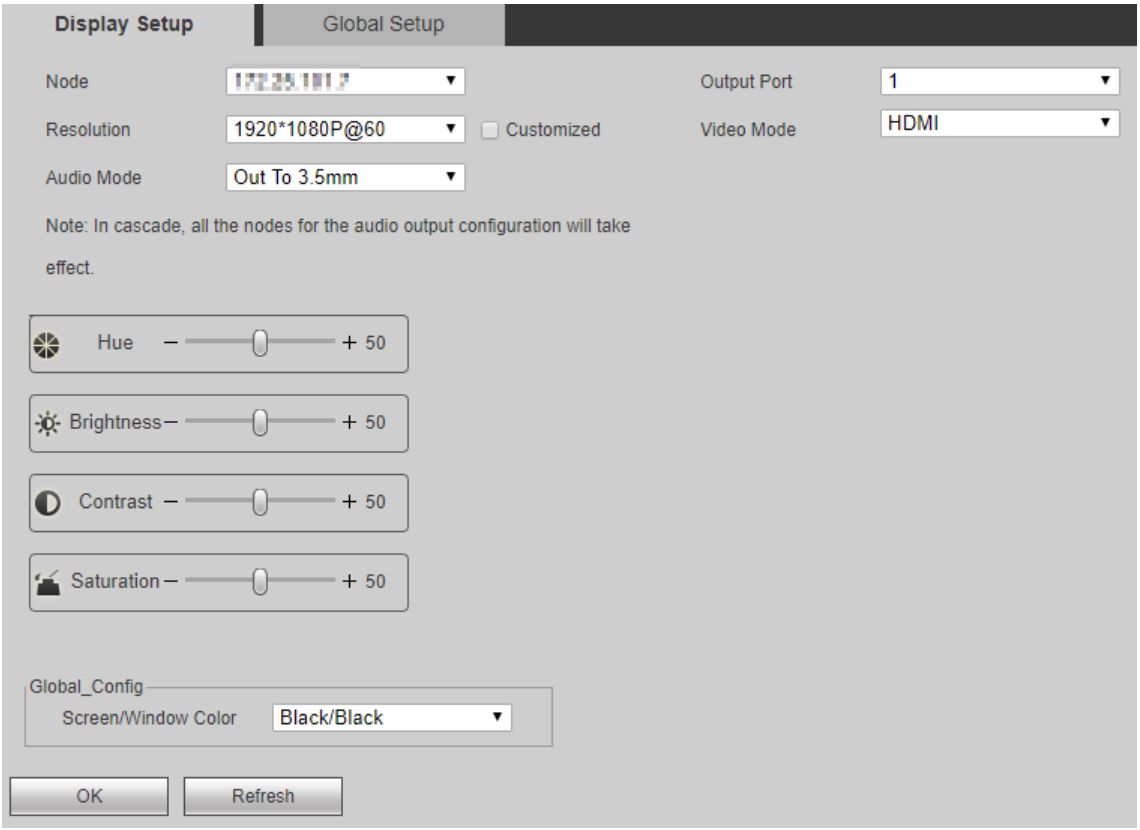


Table 3-17 Parameters description

Parameter	Description
Node	Select the designated device from the baseline system.
Output Port	Every device has two HDMI output ports, and the HDMI output port can be determined according to the node.
Resolution	Select **Customized**, and then you can configure the resolution.
Audio Mode	Configure the audio output mode. HDMI output and 3.5 mm output are available. • HDMI output: The sound is output from the audio output port of the connected display. • 3.5 mm output: The sound is output from the audio output port of the main device.

Parameter	Description
Video Mode	Configure the video output mode. DVI and HDMI are available.
Hue	Drag the slider to adjust the image hue. For example, change red to blue. The default value is made by the light sensor and normally it does not have to be adjusted. The range is from 0 to 128 (64 by default).
Brightness	Adjust the image brightness through linear adjustment. The bigger the value is, the brighter the image will be, and the smaller the value is, the darker the image will be. The image is likely to become dim if the value is too big.
Contrast	Adjust the image contrast. The light and dark contrast is larger as the value increases. If the value is too big, the dark area is likely to become darker and the light area will be overexposed. If the value is too small, the image is likely to become dim.
Saturation	Adjusts image saturation Larger value means more intense color. This value does not affect the overall brightness of image.
Screen/Window Color	Set the color of the screen and window, including black/black and blue/black.

Step 4 Click **OK**.

Configuration takes effect after restarting the device.

3.5.5.3.2 Global Setup

You can configure to enable main/sub stream automatically switch, window prompt information, and do not decode when being covered.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Setup** > **Display Management** > **Display Setup** > **Global Setup**.

Step 3 Select the check box according to actual need.

Figure 3-56 Global configuration

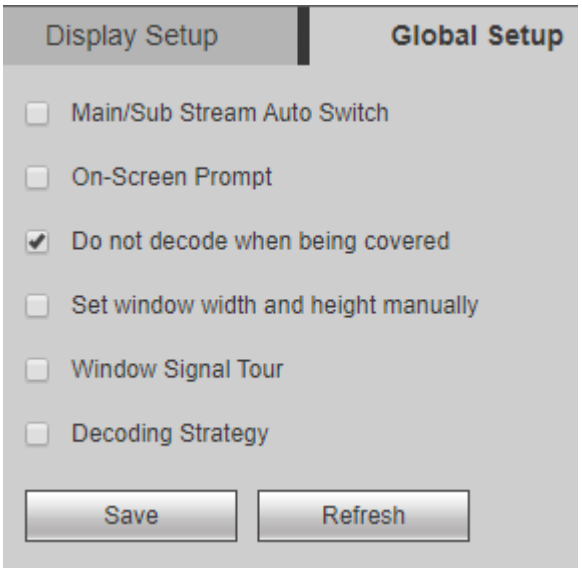


Table 3-18 Parameters description

Parameter	Description
Main/Sub Stream Auto Switch	If main stream is displayed on the window, when you reduce the window to below D1 resolution, main stream will automatically switch to sub stream.
On-Screen prompt	Window displays prompt information.
Do not decode when being covered.	When the window is covered by other window, the window will stop decoding.
Set window width and height manually.	Double-click the window on the video wall to adjust the coordinates and size.
Window Signal Tour	You can configure multiple signals on wall in one window, and then set the signal tour automatically.
Decoding Strategy	After enabling **Decoding Strategy**, the page displays fluency adjustment. You can drag the slider to adjust window fluency, and balance real-time decoding and fluency. Only network signal support fluency adjustment.

Step 4 Click **Save**.

3.5.5.4 Output Name

You can configure output name and controlID of each channel on the board card. Bind **ControlID** to the binding source (such as keyboard), so the binding source can be displayed on the video wall.

Procedure

Step 1 Log in to the webpage of the device.

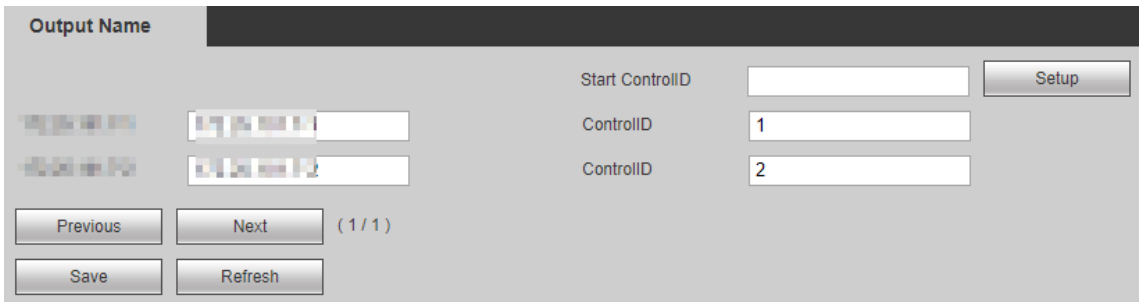
Step 2 Select **Setup** > **Display Management** > **Output Name**.

Step 3 Configure output name and controlID for each channel.

- Output name is only used to distinguish channels.
- When the keyboard or other devices are configured with video wall display, you can select the corresponding output screen based on the controlID.

Enter **Start ControlID** and click **Setup**. Then, controlID of each channel will be numbered starting from **Start ControlID**.

Figure 3-57 Output name



Step 4 Click **Save**.

3.6 Information

You can view device information, including card information, decode information, system log and online users, and more.

3.6.1 Decoding Information

Log in to the webpage, and then select **Info** > **Device Info** > **Decode Info** to view information about decoding channels, including output port, decoding status, resolution, FPS, data flow and decode flow.

Figure 3-58 Decode information

You can configure **Record Time Interval** at the upper-right corner of the page, and then click . The system records this channel according to the time interval.

3.6.2 Device Information

3.6.2.1 Acquiring Device information

You can acquire the device information and node log.

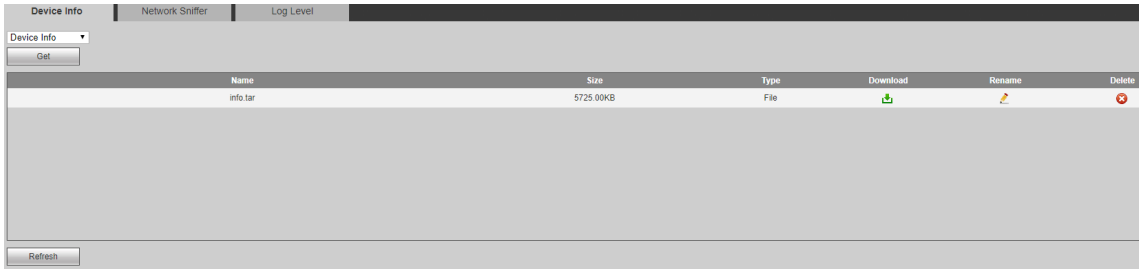
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Info** > **Device Info** > **Device Info** > **Device Info**.

Step 3 Select **Device Info** , and then click **Get**.

Figure 3-59 Device information



3.6.2.2 Network Sniffer

Network sniffer is to intercept, resend, edit and transfer the data received through network, so as to inspect network security. When a network error occurs to the device, you can carry out sniffer operation on this page, and then download the sniffer file to local device and provide the file to technical support to analyze network status.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Info** > **Device Info** > **Device Info** > **Network Sniffer**.

Step 3 Configure the parameters.

Figure 3-60 Network sniffer

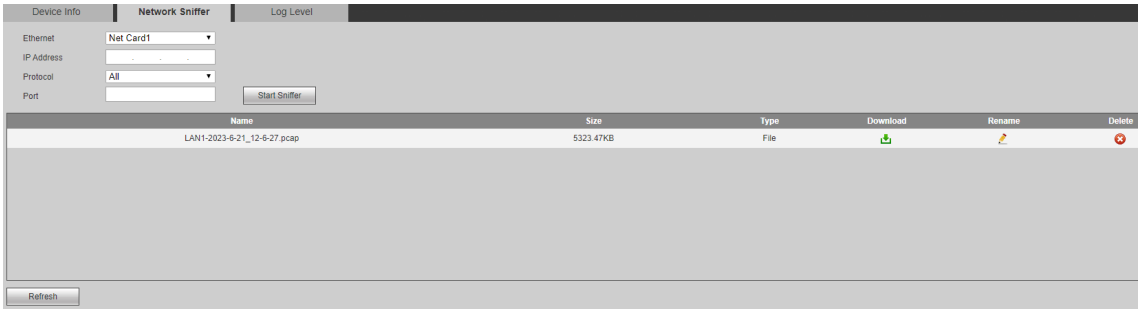


Table 3-19 Parameters description

Parameter	Description
Ethernet	Select the network card that has been bound.
IP Address	Set the network IP address.
Protocols	Select network protocols, including **All** , **TCP** and **UDP**.
Port No.	Set network port.

Step 4 Click **Start Sniffer**.

Step 5 After a while, click **Stop Sniffer**.

3.6.2.3 Log Level

Configure the log level of debugging.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Info** > **Device Info** > **Device Info** > **Log Level**.

Step 3 Configure the log level according to your needs.

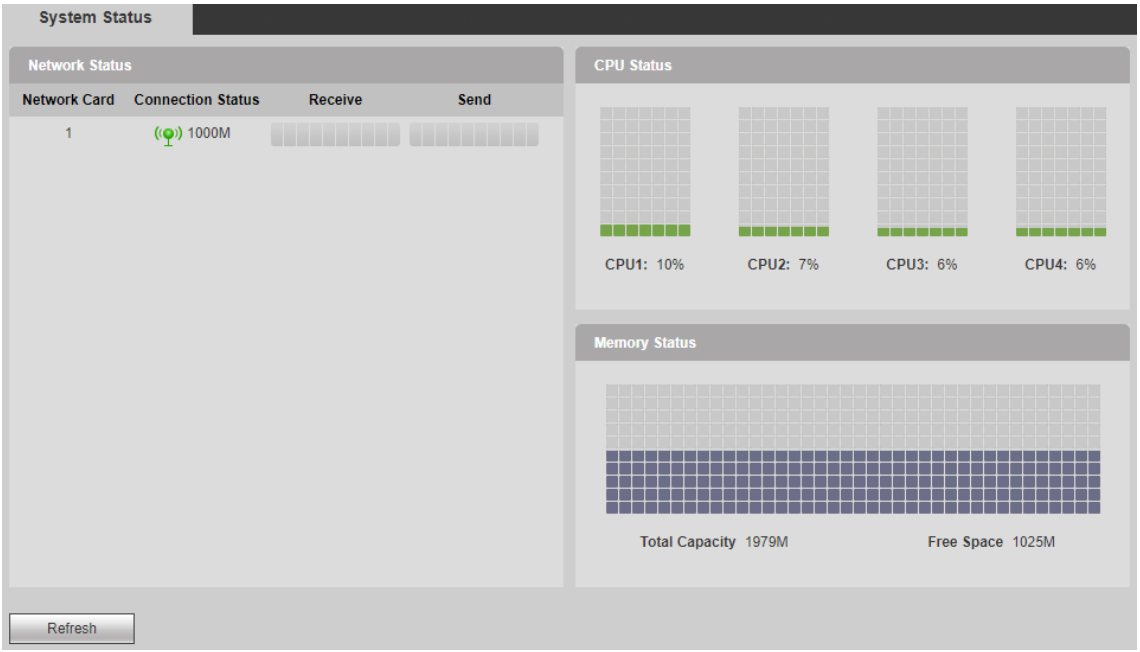
Step 4 Click **OK**.

3.6.3 System Status

Log in to the webpage, select **Info** > **Device Info** > **System Status** to view the network status and CPU usage and memory usage.

- **Network Status** : Displays connection status of data receiving and sending of network card.
- **CPU Status** : Displays CPU status of the device.
- **Memory Status** : Displays memory status.

Figure 3-61 System status



3.6.4 System Log

You can search and view system log information about the device according to log type, and backup the log to local computer.

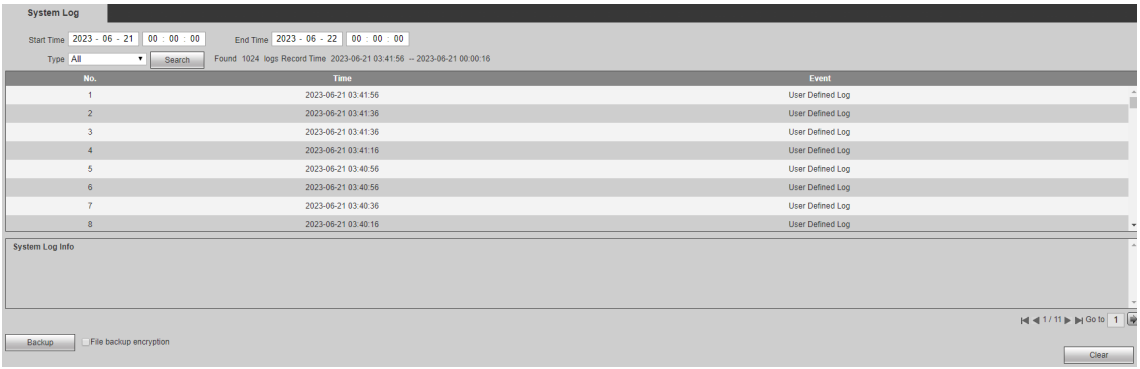
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Info** > **Device Info** > **System Log**.

Step 3 Configure **Start Time** , **End Time** and **Type**, and then click **Search**.

Figure 3-62 System log



Related Operations

- Click a log to display the detailed information of the log.
- Click **Clear** to clear all log information on the device.
- Click **Backup** to back up the searched system log information to the computer in use.
- Select **File Backup Encryption** to encrypt and backup the searched system log information to the computer in use.

3.6.5 Online User

Log in to the webpage, and then select **Info** > **Device Info** > **Online User** to view the information of online users, including **Username** , **Group**, **IP Address**, and **User Login Time**.

3.6.6 About

Log in to the webpage, and then select **Info** > **Device Info** > **About** to view the version information, including SN, device type, WEB version, system version, microcontroller version, safety baseline version and ONVIF version.

3.6.7 Legal Information

Log in to the webpage, select **Info** > **Device Info** > **Law information** to view **Open Source Software Agreement**.

4 Configuring GUI

You need to connect the display and mouse to the device.

4.1 Start and Shutdown

4.1.1 Start

Connect the device to the power supply, and then press the power button on the front panel. Power indicator on indicate the device starts.

4.1.2 Shutdown

Press and hold the power button on the front panel for 3 s to shut down the device.

- Unplug power supply to shut down the device.
- If the device is forcibly shut down or suddenly disconnected from its power supply while it is working, it will resume working on the operations it was doing before it was turned off.

4.2 Software Operations

Initialize the system, and then log in.

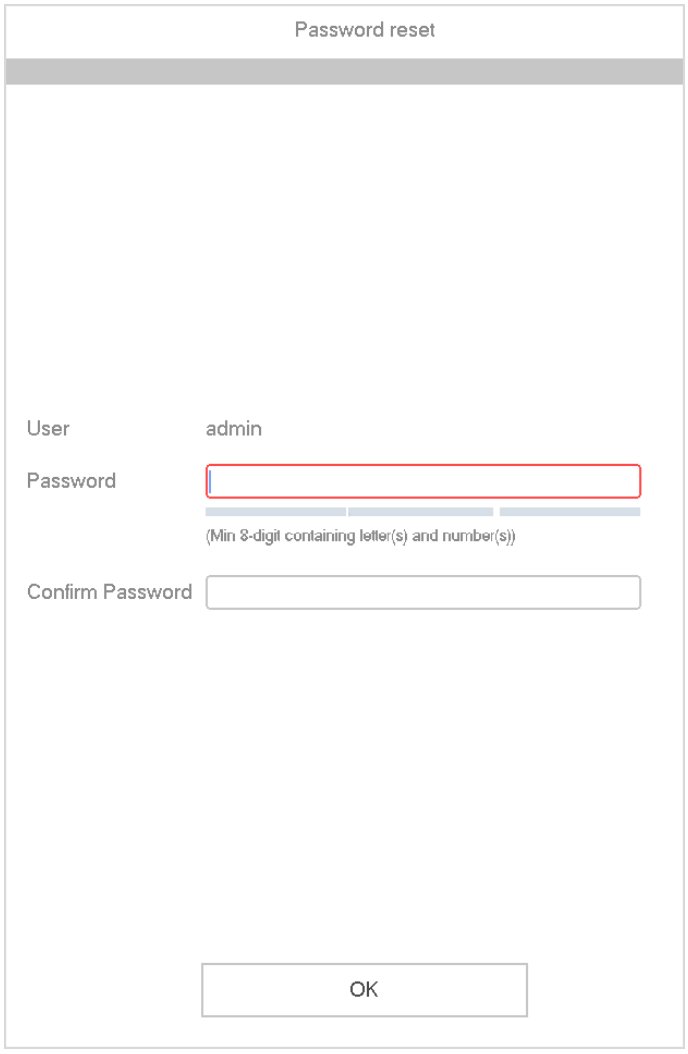
Procedure

Step 1 Power on the Device to enter the initialization page.

Step 2 Set the admin password, and then click **OK**.

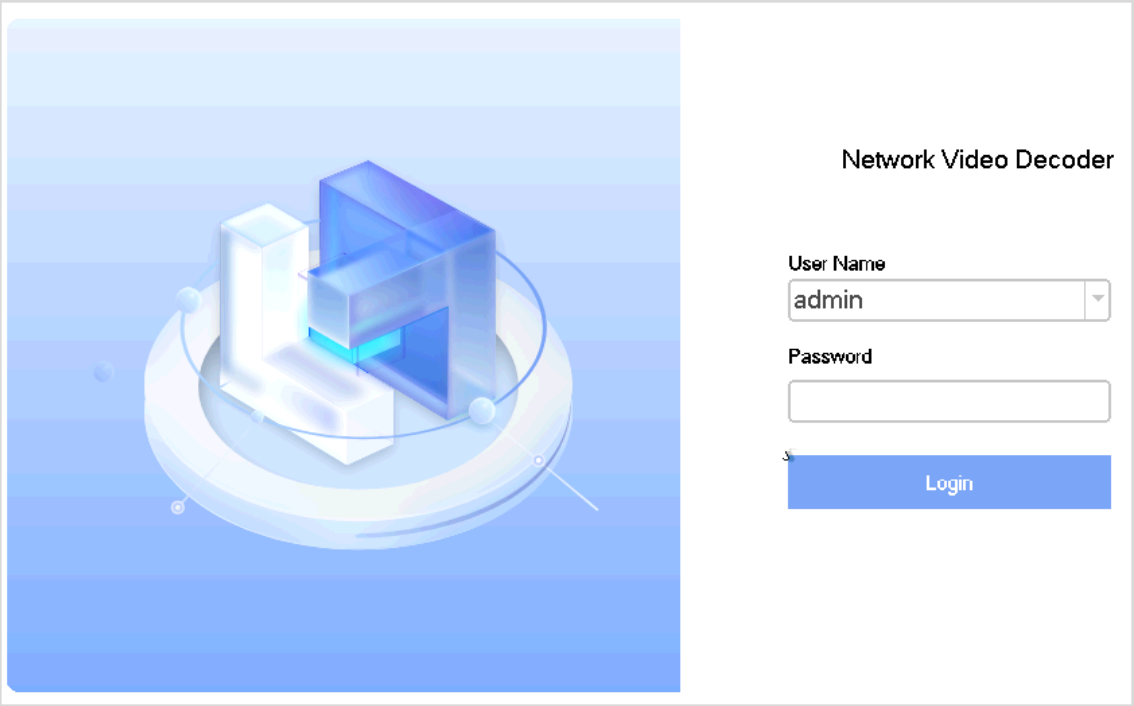
- The password must consist of 8 to 32 non-blank characters, and can consist of upper case, lower case, numbers, and special characters (excluding **'** , **"**, **;**, **: &**). The confirming password must be the same as the new password. Set a strong password based on the password strength prompt.
- For password security, the account will be locked if the wrong password is entered for 5 times within 30 minutes.

Figure 4-1 Initialization



Step 3 Enter the password, then click **Login** to log in.

Figure 4-2 Login

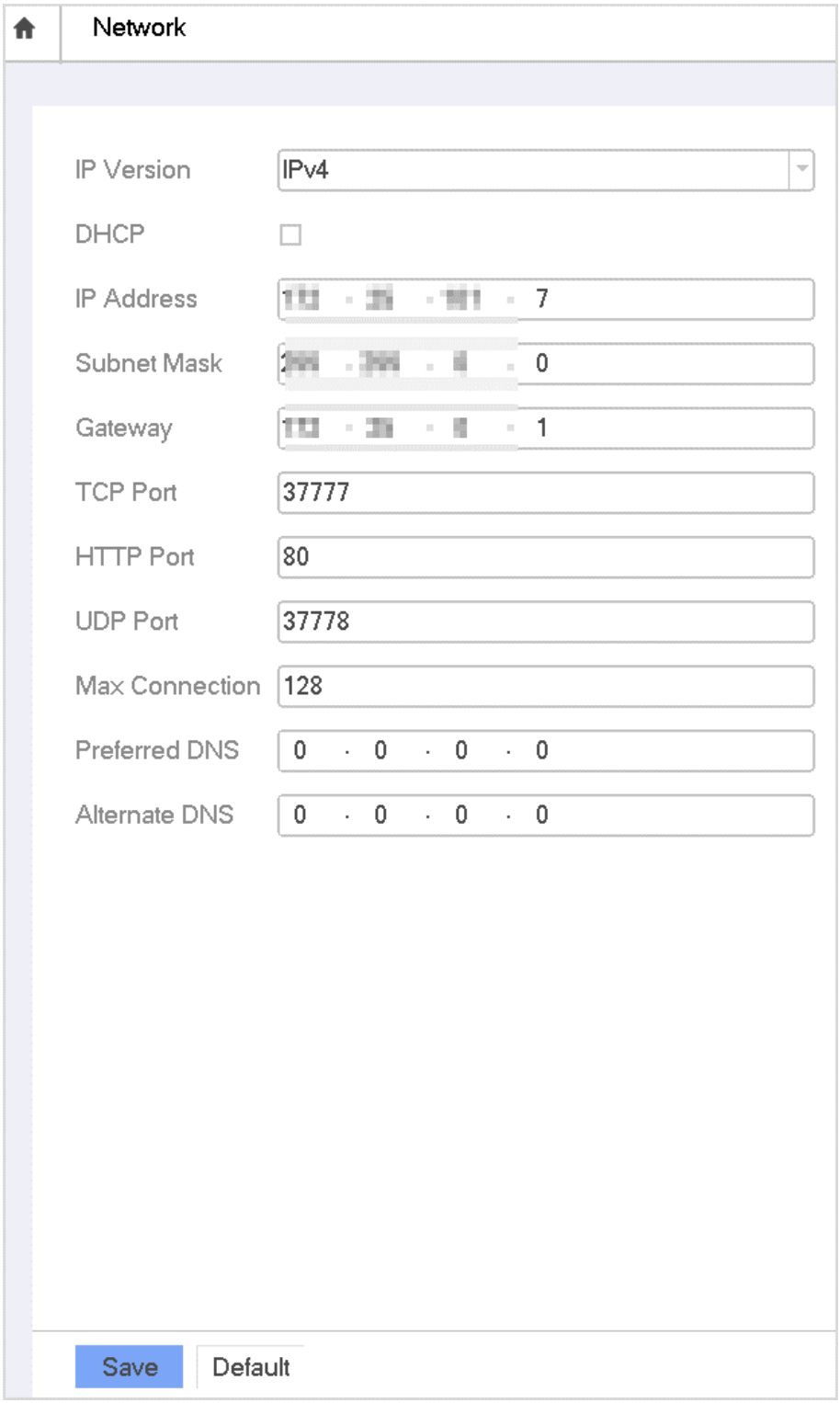


4.3 Configuring the Network

Configure the network of the device to ensure that it is connected.

On the home page, Click **Network Settings** to configure the **IP Address**, **Subnet Mask** and **Gateway**. After that, click **OK**.

Figure 4-3 Network settings



4.4 Signal Management

4.4.1 Adding Signals Automatically

Search and add signals automatically.

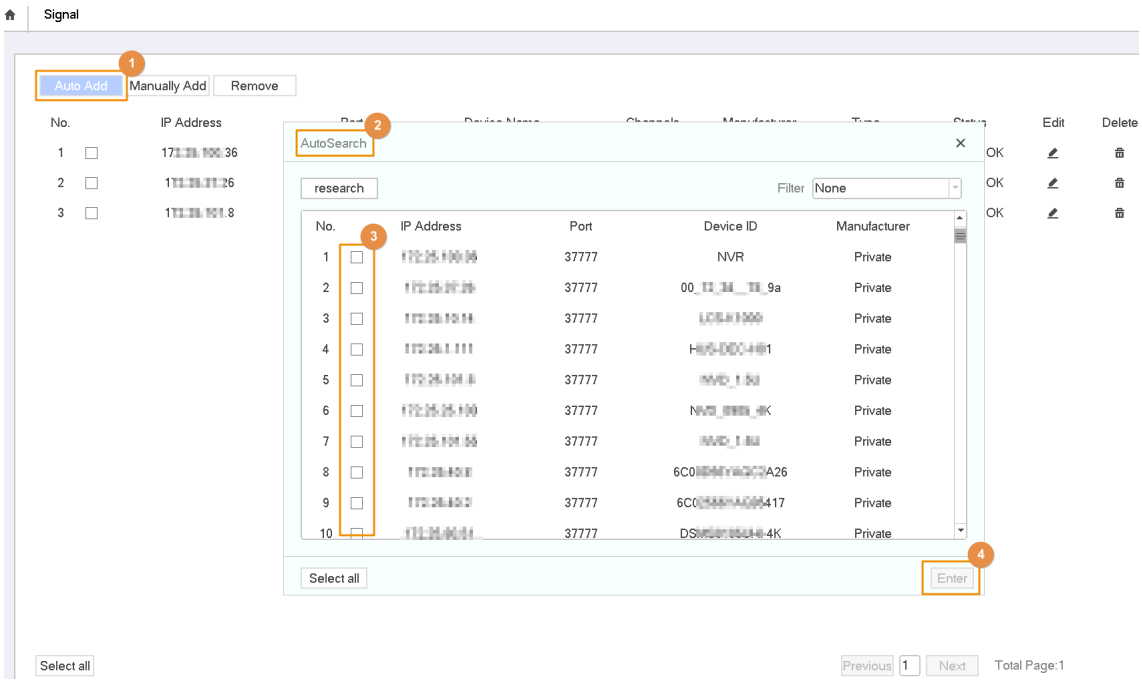
Procedure

Step 1 On the GUI page, click **Signal**.

Step 2 Select **Auto Add** > **Auto Search**.

Step 3 Select a signal or multiple signals, and then click **Enter**.

Figure 4-4 Add the signal automatically



Related Operations

- Select a signal or multiple signals, and then click **Delete** to delete the added signals.
- Click the corresponding to the signal to delete the signal.
- Click to edit the signal.
- Click **Select a ll** to select all signals.
- Click **Research** to search for signals again.
- Click **Filter** to filter by device models.

4.4.2 Adding Manually

Add the network signal manually.

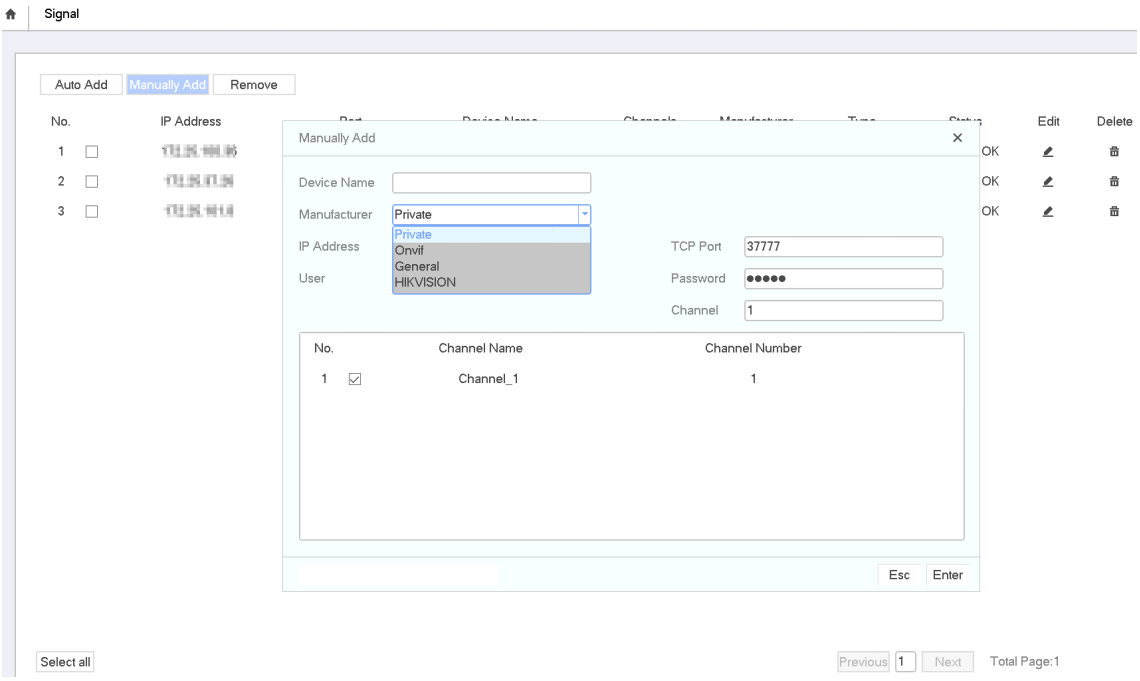
Procedure

Step 1 On the home page, click **Signal**.

Step 2 Select the **Manually Add**.

Step 3 Configure the parameters, and then click **Save**.

Figure 4-5 Manually add



4.5 Video Wall Operations in GUI

You can open windows, configure signals on the wall, download schemes, and more.

Log in to the GUI, and then click **TV wall**. Open a window on the video wall, and then drag the signal to the window.

Figure 4-6 Video wall

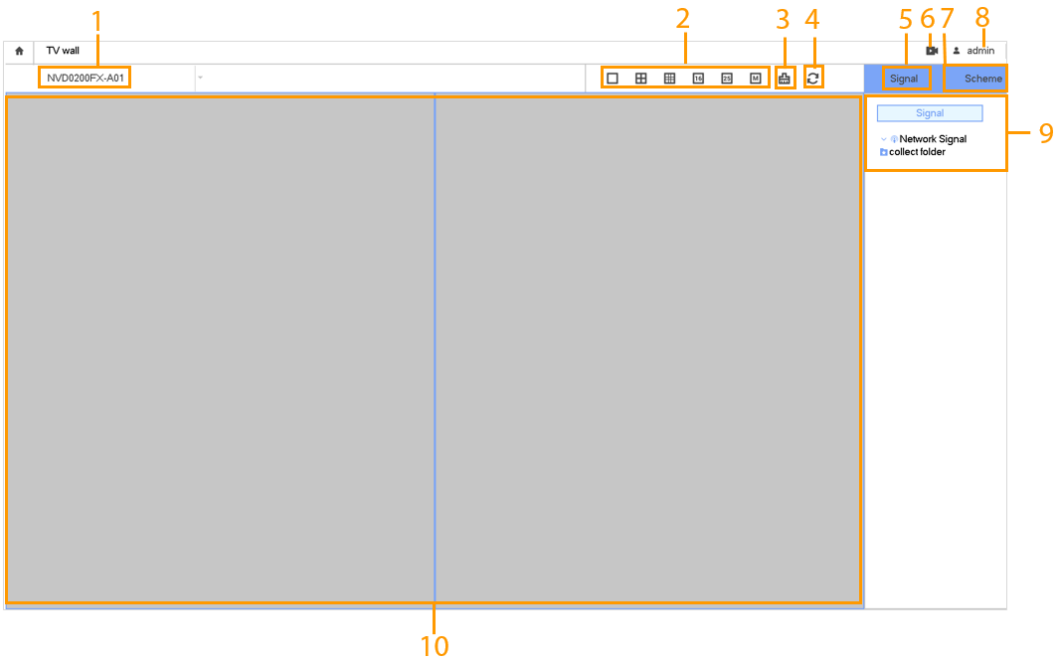


Table 4-1 Description of the TV wall

No.	Description
1	Video wall list.
2	Block division. You can select single screen, 4, 9, 16 and 25 windows.
3	Screen clearing.
4	Refresh.
5	Click to display the signal list.
6	Preview. Click to view the video of the current signal.
7	Scheme. Click to select scheme.
8	Account. You can log out, shutdown and restart.
9	Signal list.
10	Video wall layout.

4.5.1 Window Configuration

Add windows in video wall blocks.

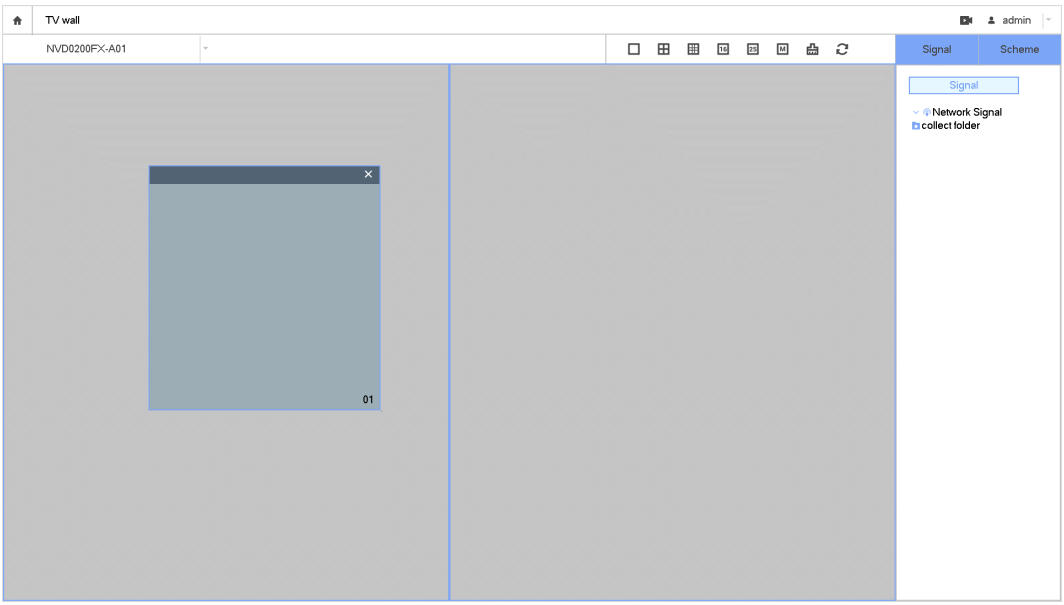
Procedure

Step 1 In GUI, click **TV wall**.

Step 2 Configure block division for the video wall.

Step 3 Press and hold the mouse to form one or more windows on video wall.

Figure 4-7 Add windows



Step 4 Drag the signal from the signal list to the window to enable signal on wall.

Related Operations

Click to close the window.

4.5.2 Scheme Management

Configure scheme tour, and load the scheme in GUI.

Prerequisites

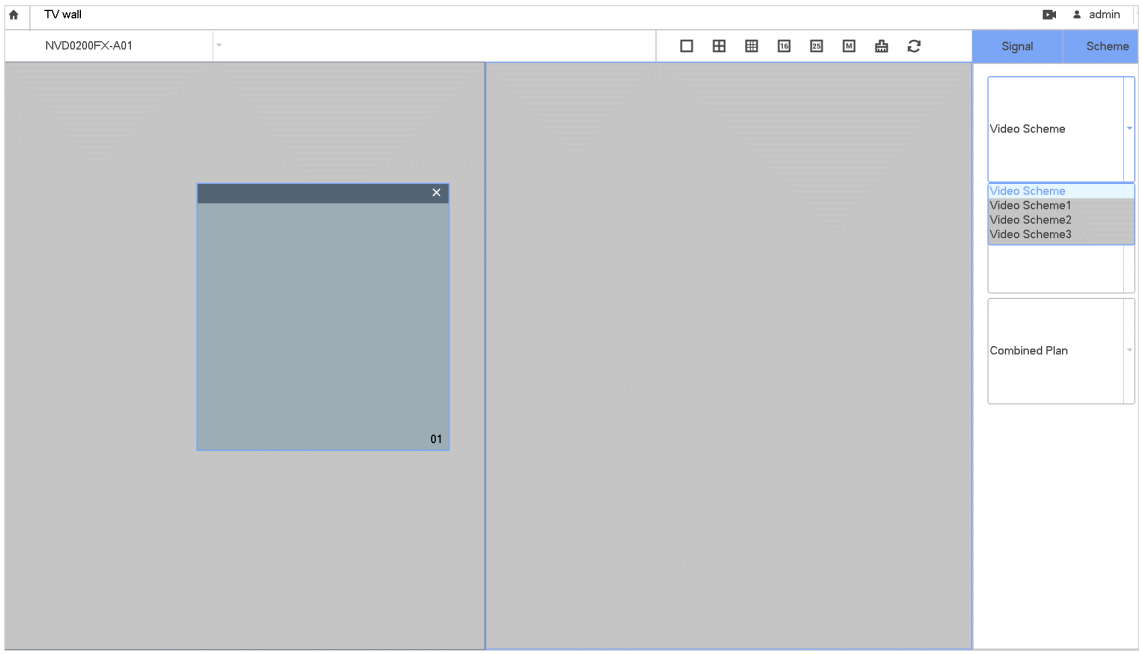
You have configured schemes and scheme tour on the webpage.

Procedure

Step 1 Log in to the GUI, and then click **TV wall**.

Step 2 Click **Scheme** on the right side to load the scheme.

Figure 4-8 Load the scheme



4.6 System Information

On the GUI page, click **System Info** to view version information and legal information.

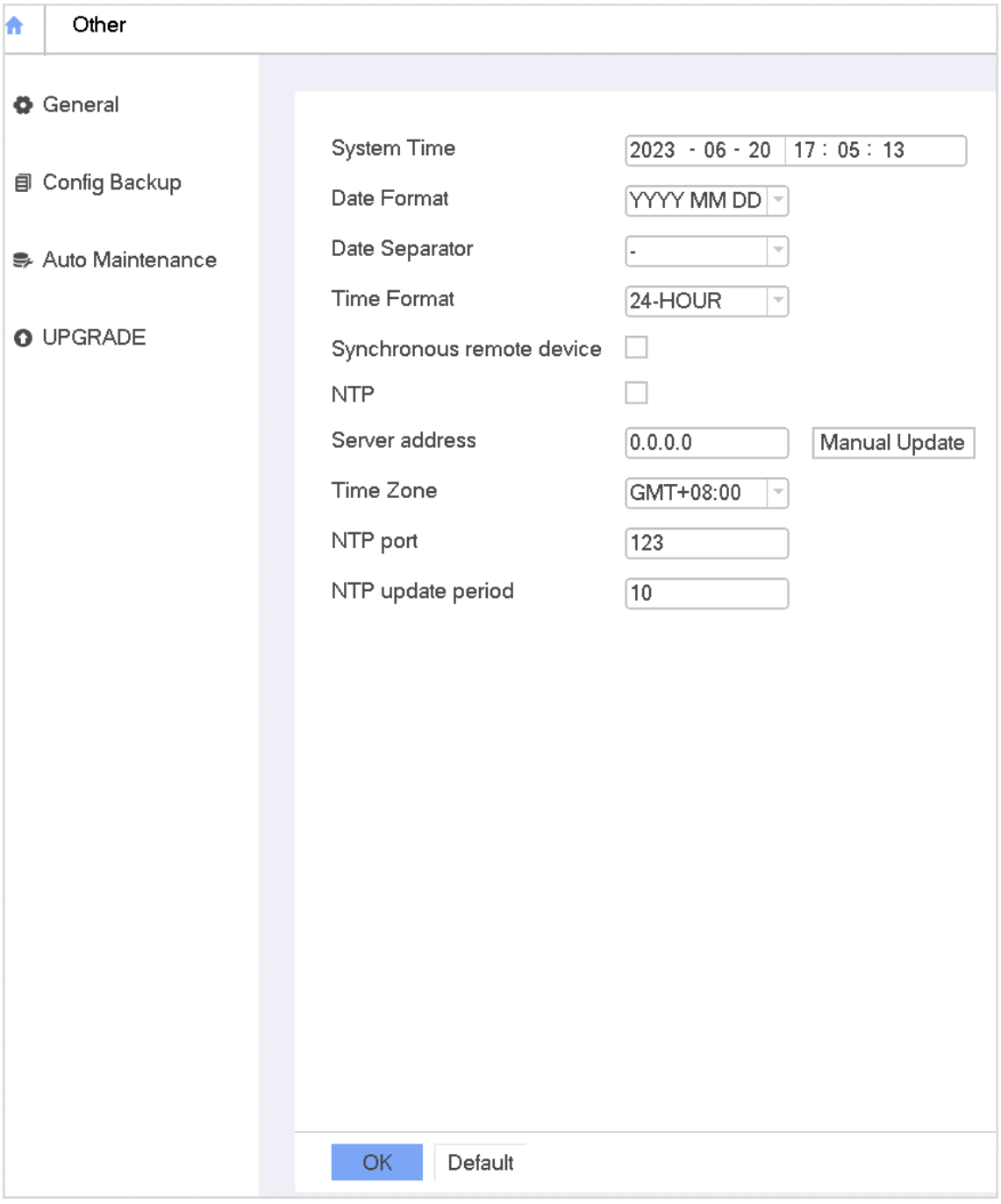
4.7 Other Configurations

Configure the time, date, update interval, emergency maintenance and system maintenance.

4.7.1 General Configurations

On the GUI page, click **Other** , and then select **General**. After you finish configuring the settings, click **OK**.

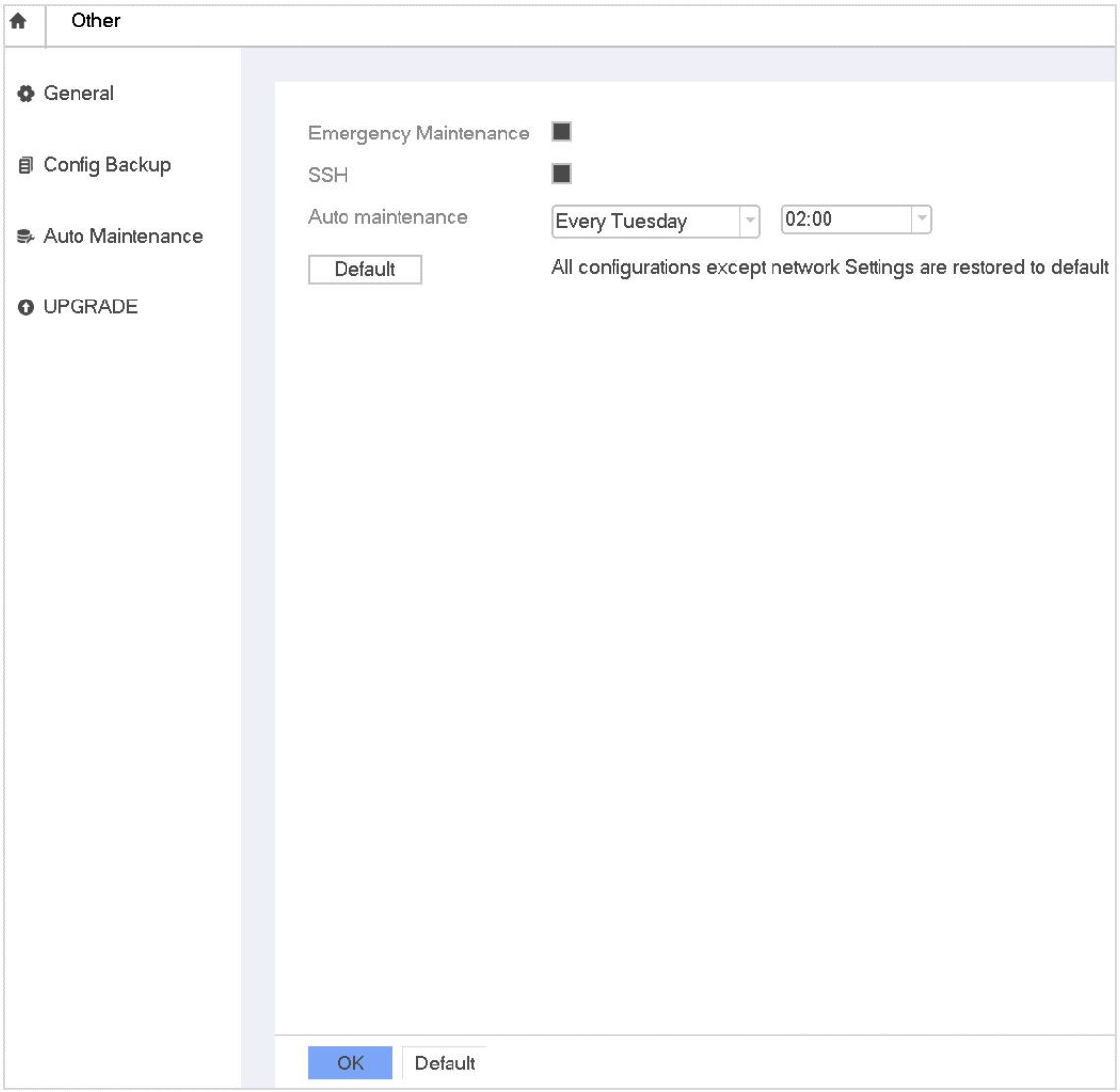
Figure 4-9 General configurations



4.7.2 System Maintenance

On the GUI page, click **Other** , select **Auto Maintenance**, and then configure the parameters. After you finish configuring the settings, click **OK**.

Figure 4-10 System maintenance



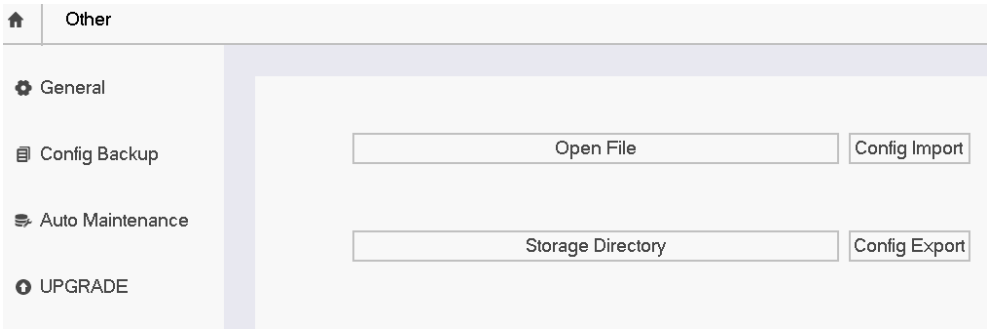
- **Emergency Maintenance** : This function can be used with the fault diagnostic tool. If any anomaly occurs and the device cannot reboot, you can upgrade the device. and then reboot it using the **Emergency Maintenance** function.
- **SSH** : Enable remote debugging for technical stuff.
- **Auto Maintenance** : Configure the automatic maintenance time, and the device will reboot at that time.
- **Default** : click **Default** for the page to be restored to its default settings.

4.7.3 Backup Configuration

On the GUI page, click **Other** , and then select the **Config Backup**.

- **Config Import** : Insert a USB drive, and then click **Open File** to select the storage directory. Select configuration file, and then click **Config Import** to import the configurations from the USB drive.
- **Config Export** : Insert a USB drive, and then click **Storage Directory** to select the storage directory. Click **Config Export** to export the configuration file to the USB drive.

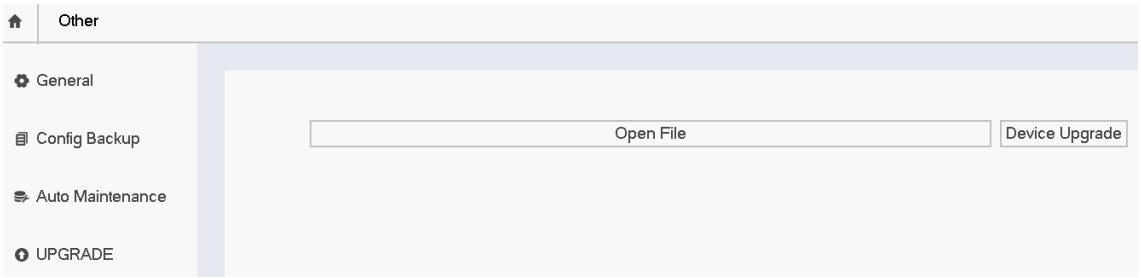
Figure 4-11 Backup Configuration



4.7.4 Upgrade

On the GUI page, click **Other** , and then select the **UPGRADE**. Insert a USB drive, click **Open File** to select upgrade file, and then click **Device Upgrade**.

Figure 4-12 Upgrade



Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.