

Video Management Platform User Manual

Manual Version: V2.01

Contents

1 System Introduction	1		
1.1 Function Overview	1		
1.2 System Login	1		
1.2.1 User Login	1		
1.2.2 Security Wizard	1		
2 Configuration Center	2		
2.1 Application Management	2		
2.2 Style Settings	4		
3 License Management	5		
3.1 Apply for Host File	5		
3.2 Import License File	5		
4 Live View	6		
4.1 Camera Live View	6		
4.1.1 Live View Service	6		
4.1.2 Audio Services	14		
4.2 Camera Group	16		
4.2.1 Configure Camera Group	16		
4.2.2 Activate Camera Group	17		
4.3 Camera Sequence	17		
4.3.1 Configure Camera Sequence Resource	17		
4.3.2 Start Camera Sequence	18		
4.3.3 Camera Sequence Toolbar	19		
4.4 Group Display	20		
4.4.1 Configure Group Display	20		
4.4.2 Start Group Display	21		
4.5 Group Sequence	21		
4.5.1 Configure Group Sequence Resource	21		
4.5.2 Start Group Sequence	23		
4.5.3 Group Sequence Toolbar	24		
4.6 Box-Dome Linkage (Panoramic Linkage)	25		
4.6.1 Add Box-Dome Linkage Resources	25		
4.6.2 Calibrate Dome Camera	26		
4.6.3 Start Box-Dome Linkage (Panoramic Linkage)	27		
4.7 Patrol	28		
4.7.1 Configure Presets	28		
4.7.2 Configure Patrol Route	29		
4.7.3 Configure Patrol Schedule	30		
4.7.4 Start Patrol	32		
4.8 Live Video Resource Management	32		
4.8.1 Camera Management	32		
4.8.2 Favorites	33		
4.8.3 Resource Statistics	34		
5 Playback	35		
5.1 Search and Playback	35		
5.2 Start Playback	36		
5.3 Playback Toolbar	36		
5.4 Playback by Segment	39		
5.5 Download Recording	40		
6 Video Wall	40		
6.1 DC Video Wall	40		
6.1.1 Add Video Wall	41		
6.1.2 Configure Camera Sequence Plan	42		
6.1.3 Configure Group Sequence on DC Video Wall	43		
6.1.4 Play Video Resources on Video Wall	44		
6.1.5 Window Operations	45		
6.2 A8 DX Video Wall	45		
6.2.1 Add Video Wall	45		
6.2.2 Configure Camera Sequence Plan	47		
6.2.3 Play Video Resources on Video Wall	47		
6.2.4 Window Operations	47		
6.3 DX Video Wall	48		
6.3.1 Video Wall	48		
6.3.2 Screen Control	58		
6.4 Multi-Decoder Video Wall	59		
6.4.1 Video Wall	59		
6.4.2 Screen Control	63		
7 Organization Management	65		
7.1 Add Organization	65		

7.2 Organization Management	66	9.4 Server Device	142
7.3 Organization Tree Operations	67	9.4.1 IP SAN	142
7.4 Resource Statistics	69	9.4.2 MS Server	144
7.5 Resource Allocation	70	9.4.3 MS Group	145
8 User Management	73	9.4.4 MD Server	145
8.1 Department Management	73	9.4.5 Intelligent IA Server	148
8.1.1 Add Department	73	9.4.6 TS Server	148
8.1.2 Edit Department	74	9.4.7 VOD Playback Server	149
8.1.3 Delete Department	74	9.4.8 BM Server	150
8.2 Role Management	74	9.4.9 DM Server	153
8.2.1 Add Role	74	9.4.10 DB Server	154
8.2.2 Edit Role Configuration	77	9.4.11 DAPA Server	155
8.3 User Management	78	9.4.12 Map Server	155
8.3.1 Add User	79	9.4.13 Log Auditing Server	156
8.3.2 Lock/Unlock User	81	9.4.14 NTP Server	157
8.3.3 Edit User Information	82	10 Storage Configuration	159
8.4 3-Role Mode	85	10.1 Direct Storage Resource	159
8.4.1 User Login Mode	85	10.1.1 Configure Direct Storage Resource	159
8.4.2 Add 3-Role User	86	10.1.2 Capacity Expansion/Reduction	162
8.4.3 Add User (by system administrator)	86	10.1.3 Start/Stop Storage	162
8.4.4 Assign Roles (by security administrator)	86	10.2 Forward-and-storage Resource	163
8.4.5 Audit User (by audit administrator)	87	10.2.1 Configure Forward-and-Storage for Cameras	163
9 Device Management	87	10.2.2 Configure Forward-and-Storage Schedule	164
9.1 Frontend Device	87	10.2.3 Start and Stop Forward-and-Storage Schedule	165
9.1.1 Add Frontend Device	88	10.3 Backup Resources	166
9.1.2 Edit Frontend Device and Channel	101	10.4 Image retention period configuration	166
9.1.3 Search Frontend Device	103	11 Alarm Service	168
9.1.4 Configure Frontend Device	104	11.1 (Optional) Alarm Customization	168
9.1.5 Delete Frontend Device	105	11.1.1 View Predefined Alarms	168
9.2 Edge Device	105	11.1.2 Global Customization	169
9.2.1 Network Video Recorder	106	11.2 Third-party Alarm Configuration	169
9.2.2 IoT Device	109	11.2.1 Configure Third-party Device Type	170
9.2.3 Landmark	110	11.2.2 Configure Third-party Device	171
9.3 Terminal Device	111	11.2.3 Configure Third-party Alarm Type	173
9.3.1 DX Device	111	11.3 Alarm Parameter Configuration	174
9.3.2 Video Integrated Management Platform	118	11.3.1 SMS Server	174
9.3.3 Decoder	126	11.3.2 Email Server	175
9.3.4 Network Keyboard	133	11.3.3 Alarm Pop-up Window	175
9.3.5 PTZ Control	141		

11.3.4 Resume Previous Video on Monitor after Playing Alarm-triggered Live Video	176	12.5.1 Alarm Subscription	215
11.4 Alarm Subscription	176	12.5.2 Subscribe to Directories	217
11.4.1 Configure Alarm Subscription Rules	177	12.5.3 Subscribe to Mobile Device Locations	218
11.4.2 Manage Alarm Subscription Rules	178		
12 Platform Casading	179	13 LAPI Management	219
12.1 SPN Server Configuration	179	13.1 LAPI Device Subscription	219
12.2 Platform Configuration	180	13.1.1 Add LAPI Device	219
12.2.1 Inter-Domain Communication Protocol Configuration	180	13.1.2 Subscribe from LAPI Device	220
12.2.2 GB Code Verification	181		
12.2.3 Local Domain Administrative Division Configuration	182	14 Advanced Settings	221
12.2.4 Camera Type Settings	182	14.1 Central Server Configuration	221
12.3 External Domain Management	183	14.1.1 Server Settings	222
12.3.1 Higher-level Platform	183	14.1.2 Operation log language configuration	224
12.3.2 Peer Platform	189	14.1.3 OSD Configuration	224
12.3.3 Lower-level Platform	195	14.2 Transcoding Rule	224
12.4 Resource Sharing	200	14.2.1 Add Transcoding Rule	224
12.4.1 Requirements	200	14.2.2 Edit Transcoding Rule	226
12.4.2 Configure the GB Sharing ID Data Dictionary	200	14.2.3 Delete Transcoding Rule	226
12.4.3 Query SPN	201	14.3 Trunk Management	226
12.4.4 Share Resources(for one platform)	202	14.3.1 Add Trunk	226
12.4.5 Platform Sharing (to Multiple Platforms)	207	14.3.2 Add Trunk Information	227
12.4.6 Manage Shared Resources	211	14.3.3 Manage Trunk	228
12.4.7 Manage Resources that Failed to be Shared	214		
12.4.8 Manage Resources Shared from Child/Peer Domains	214	15 System Watermark	229
12.5 Resource Subscription	215	15.1 System Watermark Policy	229
		15.2 System Watermark Configuration	230
		16 O&M Management	230
		16.1 Operation Logs	230
		16.2 Device Statistics	231
		16.3 Asset Statistics	231
		16.4 Storage Statistics	231

1 System Introduction

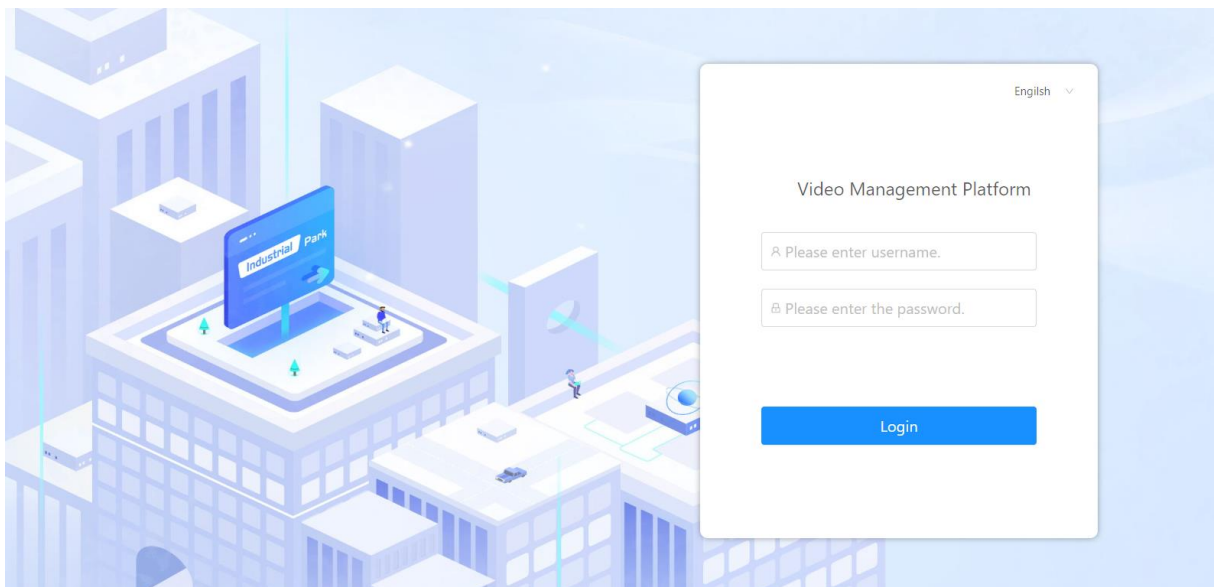
1.1 Function Overview

The video management platform provides solutions for large-scale security monitoring scenarios. It supports massive device connection, video management, resource storage, business management, is highly compatible, and can meet various requirements of video surveillance applications.

1.2 System Login

1.2.1 User Login

1. Use Chrome browser to visit **<http://VM server IP address>**
2. On the login page, input username and password, click **Login**.



NOTE!

- The default username/password of the Web interface is **admin/123456** or **admin/admin**. Please follow the security wizard to set a strong password.
- To use HTTPS for network access, you need to install the certificate. Please contact our technical support.

1.2.2 Security Wizard

When you log in for the first time, you need to follow system prompts to set a strong password for security.

System Root Password

* Old Password:

* New Password:

* Confirm Password:

Database Password

Database Name:

* New Password:

* Confirm Password:

Confirm and Reboot **Reset**

1. Follow system prompts to set strong passwords, including server root password, database password, FTP password, Web administrator and terminal passwords.



NOTE!

The old password of the Root is the root user's password for logging in to the operating system, default root password is 123456.

2. After you finish the settings, click **OK** and restart. The system will restart automatically.
3. Use the new password to log in again after restart.

2 Configuration Center

You can customize the system-presented applications and system style, and perform quick user management and third-party platform authentication management.

4. On the login page, press **Ctrl+Shift+F10** to go to the password verification page.

Figure 2-1 Login to Configuration Center

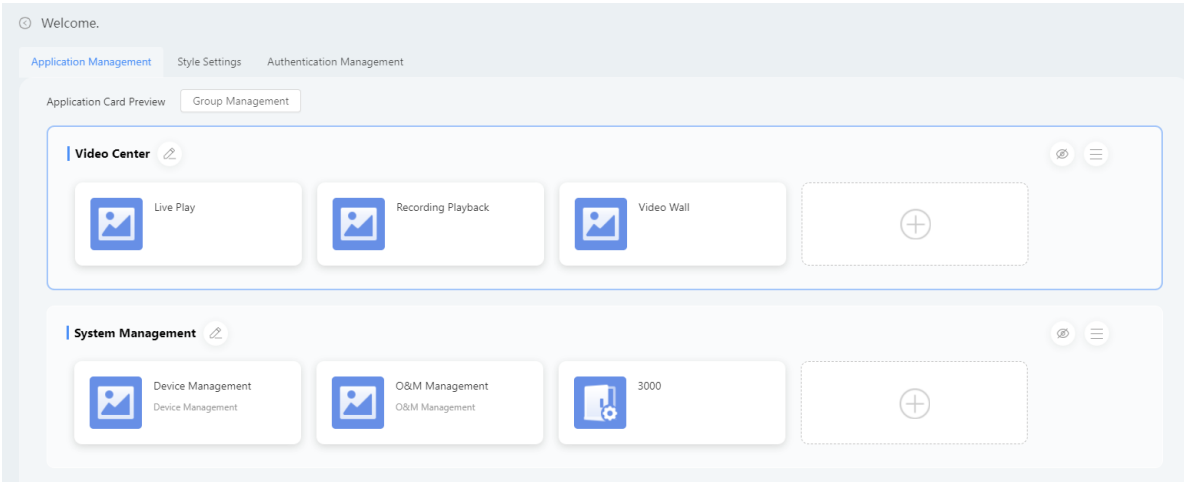
Admin Password **confirm** Cancel

5. Enter the admin password and click **OK** to go to the **Configuration Center** page.

2.1 Application Management

Customize display settings of application menus and add third-party applications.

Figure 2-2 Configuration Center

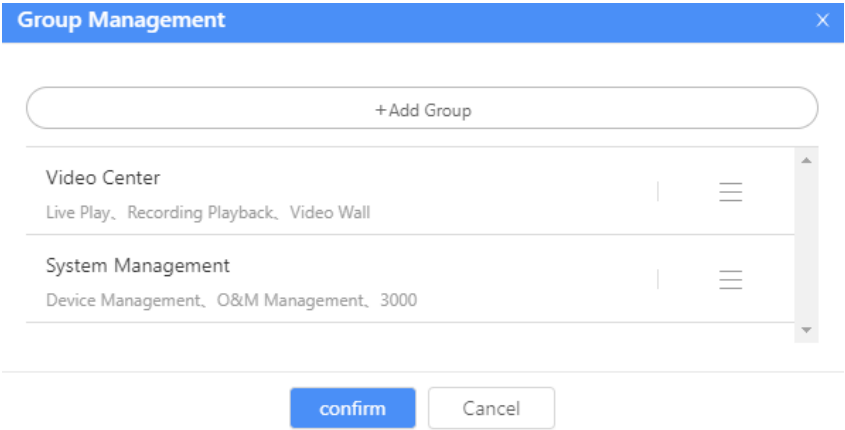


Group Management

Groups are primary menus.

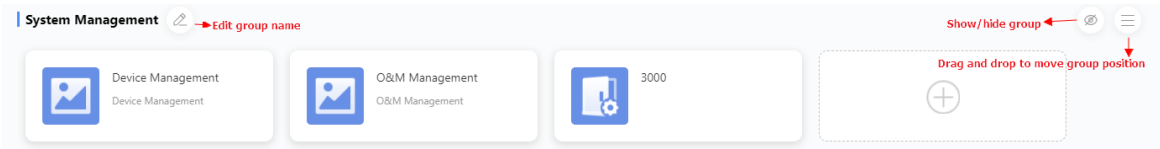
- **Add group:** Click **Group Management** to go to the **Group Management** page.
 - Click **Add Group** to add a group.
 - You can drag the group and adjust the order by pressing ≡.

Figure 2-3 Group Management



- **Edit groups**

Figure 2-4 Operations for Groups

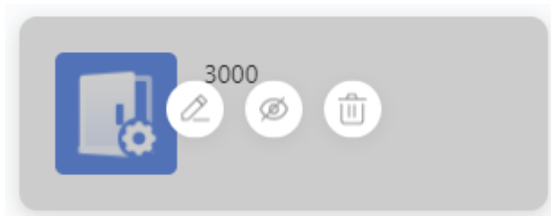


Application Card Management

Application cards are secondary menus.

- **Edit application card** (Note: only added applications can be deleted)

Figure 2-5 Operations for Cards



- **Adjust application card position:** Drag the application card to adjust its position within the current group or move it into other groups.
 - **Add application:** You can embed third-party webpages and display them as system applications.
6. Click the last card with symbol **+** to go to the **Add Application** page.

Figure 2-6 Add Application

Add Application [X]

Group:

*Application Title:

*Webpage URL: ?

Brief Description:

Homepage Icons: Mange Icons: Background Color:

7. Set the application title and webpage URL (such as <http://xxx>), and click **OK**.

2.2 Style Settings

You can customize the system name, logo in the upper left corner, background image of the login page, and homepage style.

Figure 2-7 Style Settings

Application Management **Style Settings** Authentication Management

Name: 30/50
Tip: Chinese characters, uppercase and lowercase English letters, numbers, underscores, strikethroughs, and periods are allowed. The maximum length is 50 characters.

LOGO:
Note: For a custom logo, please upload a 64*64px image; up to 4 custom logos can be uploaded.

Login Page:
Note: The recommended image size is 1920*1080px. The image must be in PNG or JPG format and cannot exceed 5MB.

Homepage Style:

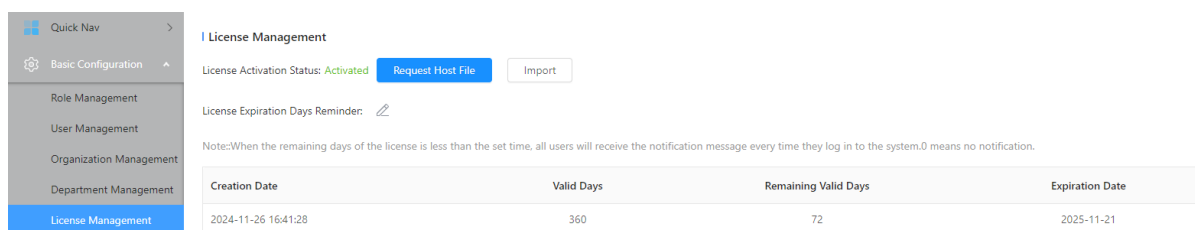
3 License Management

A license is an authorization certificate. The license file defines the authorization information of the devices and resources that can be managed by the system.

To manage more devices and resources in the system, you need to purchase a product license, apply for the activation of the license from Uniview according to the license code and detailed user information, and import the license file into the system.

3.1 Apply for Host File

1. Go to **Device Management > Basic Configuration > License Management**.



2. Click **Apply for Host File** to go to the **Apply for Host File** page.

User Info

- * Contract Number: Contract No.(up to 31 characters)
- * Customer Name: Customer Name (up to 20 characters)
- * Country: Please Enter Country
- * Province: Please Enter Province
- * County/City: Please Enter County/City
- * Company: Please enter the user's company na...
- * Telephone: Please Enter UserTelephone
- * Address: Please enter the user's address (up t...
- * Postal Code: Please Enter UserPostal Code
- * E-mail Address: Please Enter UserE-mail Address

Contact Info

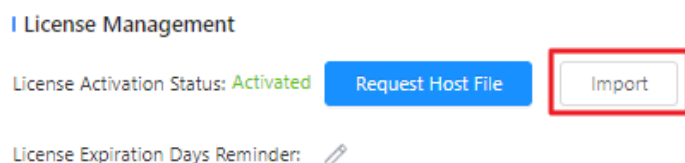
- * Name: Please Enter Contact PersonName:
- * Company Name: Please enter the contact's company ...
- * Telephone: Please enter the contact person's ph...
- * Address: Please enter the contact's address (u...
- * Postal Code: Please Enter Contact PersonPostal C...
- * E-mail Address: Please Enter Contact PersonE-mail A...

OK Cancel

3. Fill in the user information as required and click **OK**. A host file will be generated and saved to the local PC. You can use the host file to activate the license code at Uniview's official website.

3.2 Import License File

1. Go to **Device Management > Basic Configuration > License Management**.
2. Click **Import**, select the license file saved on the PC, and click **Open**.



3. After the license file is imported, you can view the license details in the license code list.

License Management

License Activation Status: Activated

[Request Host File](#)

[Import](#)

License Expiration Days Reminder: [✎](#)

Note: When the remaining days of the license is less than the set time, all users will receive the notification message every time they log in to the system. 0 means no notification.

Creation Date	Valid Days	Remaining Valid Days	Expiration Date
2023-12-07 11:31:03	360	307	2024-12-01

Authorization Code List	Service Type	Allowed Service Count	Used	Remaining
FWG737EQTIYUJZWVW36DRG6V4M		3	0	3
84YBUALPJRVL7CCL328JHUMU9S		1	0	1

- Set the days for license expiration reminder. When the remaining days of the license are less than the set days, a reminder appears every time a user logs in to the system (0 means no reminder).

License Expiration Days Reminder: [✕](#) [✓](#)

4 Live View

Play live videos captured by cameras and perform various operations during live view.

4.1 Camera Live View

View live images from cameras in real time.

4.1.1 Live View Service

1. Parameter Configuration

Before starting live view, configure stream format and network adaptation parameters according to network conditions.

(1) Configure Stream Format

Configure stream formats, that is, configure stream transport protocols supported by the monitoring system for different application scenarios.



NOTE!

Only the super administrator can configure stream formats.

- Go to **Device Management > Advanced Settings > Center Configuration > Server Settings**.

6. Choose the stream format supported by the system.

Table 4-1 Stream Format Reference

Parameter	Description
UDP+TS	Default value, which means TS streams transported by UDP. Caution: In a multi-domain networking environment, the inter-domain communication protocol for this stream format is the Private protocol, and the platform can connect IPC/encoder/decoder via the Private protocol, connect IPCs via ONVIF, and connect the child domain via the Private protocol. In a GB-connected two-level domain networking environment where IPCs are connected via the Private protocol and the central server in the child domain has enabled UDP+TS, if the parent domain requests live video streams from an IPC in the child domain, the live video streams must be processed through the MS in the child domain. If the decoding terminal is configured with TCP and the encoding terminal is configured with UDP, then the stream format can only be UDP+TS (currently MS does not support RTP-to-TCP conversion).
RTP+PS	Means PS streams transported by RTP. Caution: In a multi-domain environment, the corresponding inter-domain communication protocol is GB/T 28181 (hereinafter referred to as GB), and the platform can connect IPC/encoder/decoder via GB, IPCs via Onvif, encoder/IPC/decoder via the Private protocol, and child domains via DB33 2012, GB, and the Private protocol.
RTP/RTCP+TS	Means TS streams transported by RTP, and RTCP-based keepalive is required. Caution: In a multi-domain networking environment, the inter-domain communication protocol is DB33 2010, DB33 2012, Private, and Sichuan Electric Power, and the platform can connect IPC/encoder/decoder via the Private protocol, IPC via Onvif, encoder/IPC via GB, child domain via DB33 2012 or GB. Evaluation is required for other special networking environments.

7. Click **OK**. Enter the login password as prompted and then save the configurations.

(2) Configure Network Adaptability Parameters

Configure network adaptation parameters according to network status.

1. Click  at the right corner, select **Local Configuration**.

Local Configuration

09:26, 48:EA:63:73:98:BF, hzyo22

Live Video

Protocol type: TCP

Media streaming service selection protocol: Auto-Adaptation

Playback

Stream Transmission Protocol: TCP

Media streaming service selection protocol: Auto-Adaptation

Enable playback preview: ☒

Video

Video download format: .ts

Overlay IPC data on the screen: ☐

Disordered arrangement: ☐

Anti-packet loss: ☐

09:26, 48:EA:63:73:98:BF, hzyo22

Cancel OK

2. Configure network adaptability parameter by referring to the table below.

Table 4-2 Parameter Descriptions for Configuring Network Adaptability

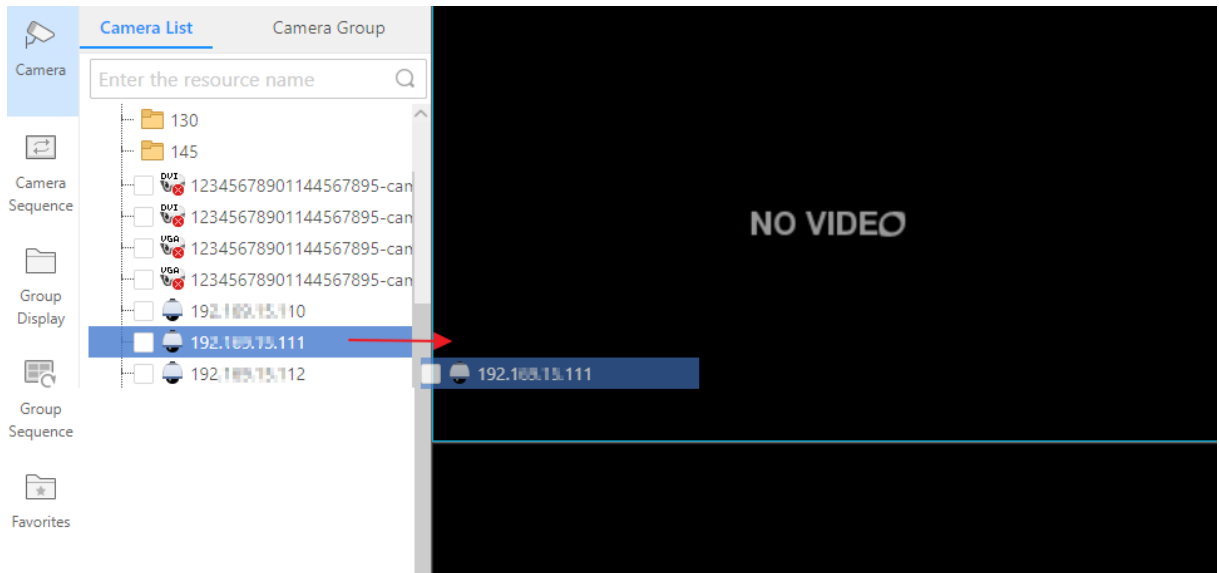
Parameter	Description
Live Vedio Protocol type	Choose TCP or Auto-Adaptation (the system automatically chooses a transport protocol according to network status).
Media Service Selection Policy	Choose Direct Connection First or Auto-Adaptation . ● Direct Connection First: For application scenarios where MS forwarding is not applicable, for example, when the MS is on the WAN and the B/S client or encoding terminal are on the LAN, and the sending bandwidth on the WAN is limited, the system can enable Direct Connection First to allow streams to be transmitted directly from the encoding terminal to the decoding terminal instead of forwarding streams via the MS in the local domain. This function only affects whether live video streams pass through the MS in the domain where the decoding terminal (B/S client) is located. ● Adaptive: The system chooses the appropriate policy according to network status.
Playback Transmission Protocol	Choose TCP or UDP . Note: This parameter is only applicable to playback.
Anti Packet Loss	Enabling this function can improve video&audio quality.

3. Click **OK**.

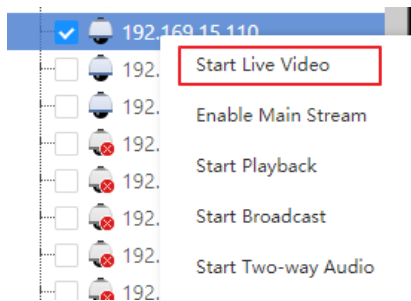
2. Start Live View

Use the following methods to start live video:

- Select a window, and then double-click the camera.
- Drag the camera to a window, and then choose **Live View**.



- Select a window, right-click the camera, choose **Start Live View**.



NOTE!

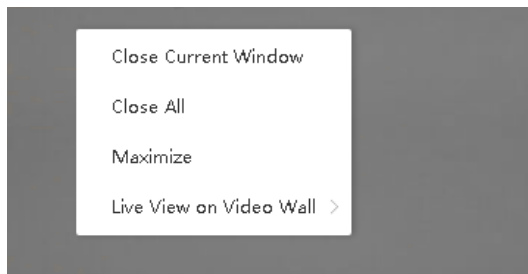
Start Main Stream: Play live video of the camera with the main stream.

3. Live Video Toolbar

Use the right-click menu, toolbar, PTZ control panel to set live video parameters, take snapshots, and more.

(1) Right-click Menu Operations

You can right-click a window and then use the menu to close the window, close all windows, maximize/restore the window, play live video to the video wall.



(2) Live Video Toolbar Operations

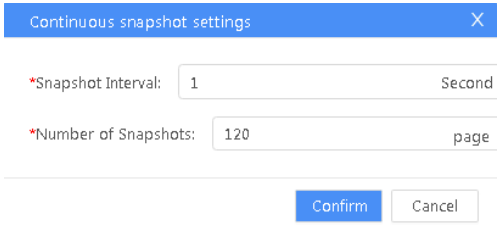
The toolbar appears when you point to the image.



The toolbar appears when you point to the image.



Table 4-3 Window Toolbar Functions

Icon	Function	Description
	Preset	Buttons for No.1 and other presets. Click to call a preset and quickly get the desired image. Note: This function is available to PTZ cameras only.
	Snapshot	Capture the current image(s) in the window and save to the computer.
	Continuous Snapshots	Note: You can set the snapshot interval and snapshot counts (0 means “not limited”) 
	Digital Zoom	Zoom in on an area of interest on the video image in the window. Note: - Digital zoom is applicable to PTZ cameras or cameras capable of adjusting zoom/focus. - Use the scroll wheel to zoom in or out.
	3D positioning	Perform 3D positioning, including click-to-position and drag-to-zoom. - Click to position: Click anywhere on the image, and the camera automatically centers on the point you clicked to display the image. - Drag to zoom: Drag on the image from top left to bottom right to zoom in, and drag in the opposite direction to zoom out.
	PTZ control	Click to expand the control panel to change settings such as focus, iris, rotation direction, rotation speed, preset, patrol route, etc. See PTZ control. Note: This function is only available to PTZ cameras.
	Start/stop recording.	local Record the live video playing in the window and save to the computer.

Icon	Function	Description
	Start/stop broadcast	Click to start one-way audio broadcast from the client to cameras.
	Start/stop two-way audio	Click to start audio intercom between the client and a camera.
	Instant playback	Start playing video backward from the current time to up to 24 hours earlier (if available).

You may also use the toolbar at the bottom of the live view page:

- : Switch the window layout. You can set the layout to 1/4/6/8/9/10/13/16/17/25 windows or to corridor mode (3-1-1 window layout for narrow scenes such as a corridor).
- : Save the current video display as a group display.
- : Close all the videos.
- : Broadcast list. **Click** to view and manage two-way audio and broadcast tasks.
- : Maximize the current window.

4. PTZ control

Use the PTZ control panel to control a PTZ camera.

(1) Using the PTZ Control Panel

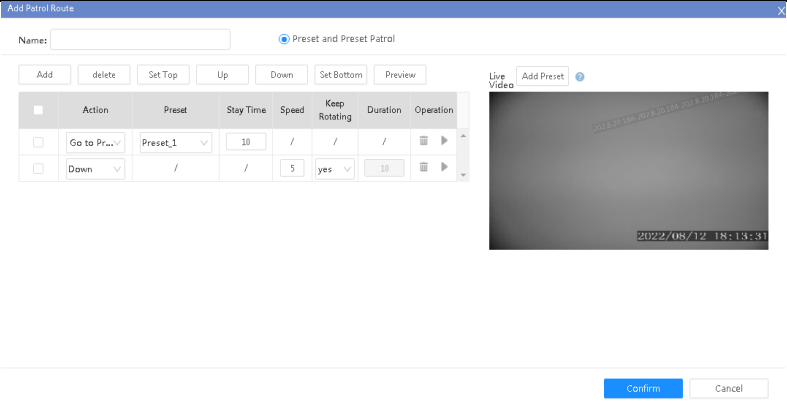
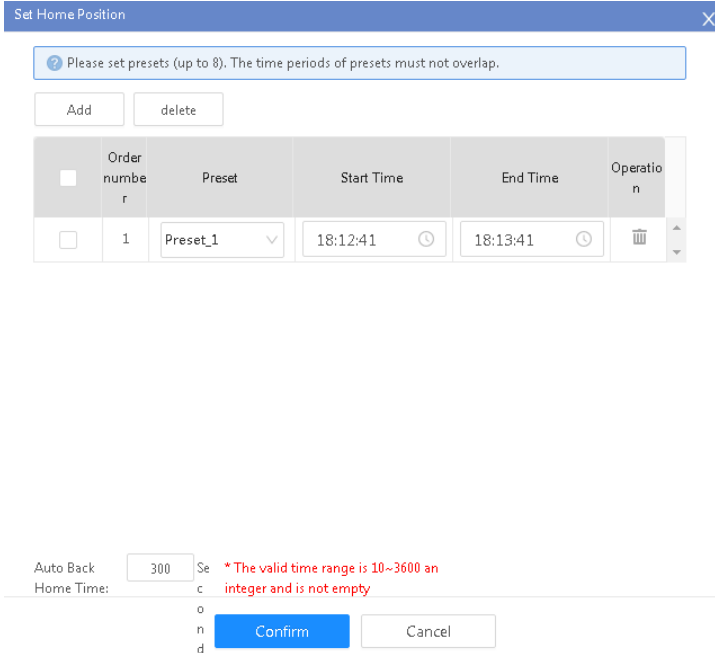
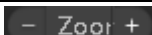
Click  in the live view toolbar to open the PTZ control panel.



Table 4-4 PTZ Control Panel Description

Icon	Description
 	Lock/unlock PTZ • When the PTZ is locked, only admin can preempt PTZ control. Other users can control the PTZ only after it is unlocked or the auto release time has expired. • When the PTZ is unlocked, a high-level user can preempt PTZ control from a low-level user. • For GB-connected parent and child domains, the parent domain can lock PTZ in the child domain. Note: Any user can control the PTZ when it is idle. Default PTZ control preemption policy: high-priority users can preempt control from a low-priority users; users in the parent domain can preempt control from users of the same priority level in the child domain; in other cases, the first user operating the PTZ gains the control. The priority level of a local-domain user is that of the user's role; the

Icon	Description
	priority level of an external-domain user is that of the user's role in the external domain. The PTZ control preemption policy and auto release time are configured on the central server.
	PTZ Release ● The PTZ is idle after being released and can be controlled by any user without preemption. ● After being released, the locked PTZ is automatically unlocked.
Preset	Preset position: You can set important shooting angles as presets. After being idle (no user action) for a certain length of time, the PTZ automatically goes to a specified preset to continue the monitoring.
	 Go to a preset: Pan/tilt the camera to a specified preset.
	 Add a preset. Add presets for cameras in the local or external domain, that is, add the current pan/tilt position as a preset to the list. Caution: Make sure the current preset ID is not in use; otherwise, the current preset will be overwritten by the new preset.
	 Sync with front-end presets Note: This function is available to GB and GB+ cameras, not on IMOS and ONVIF cameras. It is allowed between IMOS-connected and GB-connected domains.
	 Delete a preset.
	 Set the home position: The camera automatically returns to the home position after PTZ control is released. ● Set the home position and the idle time. By default, the newly added preset is the home position; you may also choose an existing preset as the home position. ● The camera will automatically return to the home position after PTZ control is released and the idle time expired. ● You can set one or multiple home positions. ● If you have set multiple home positions, you can set a schedule including up to eight time periods and assign a time period to each home position. ● If a home position already exists, it will be overwritten by the new home position.
Patrol	Patrol route: The camera pans and tilts according to a sequence of preset actions.
	 Start patrol.
	 Stop patrol.
	 Click to add a patrol route.

Icon	Description
	 ● To rotate to a preset, you need to set the preset number/description, and the length of time that the camera stays at the preset. ● To rotate up/down/left/right, you need to set the rotation speed, whether to rotate all the time, and rotation duration. Note: If the action is set to rotating up/down/left/right all the time, then actions after it will not be performed.
	Delete a patrol route
	Edit a patrol route.
	Configure a PTZ patrol schedule. See Configure Patrol Schedule.
Home position	Set whether to enable home position. To enable home position, click Set and then set the home position. 
	Control rotation directions (triangle buttons), stop patrol (the square button in the center).
	Focus far/near.
	Zoom in/out.
	Increase/decrease iris.

Icon	Description
	PTZ rotation speed Note: The rotation speed supports 9 levels from 1 to 9. 1 is the slowest and 9 is the fastest.
	Turn on/off the light.
	Turn on /off the wiper.
	Turn on/off the IR illumination.
	Turn on/off the heater.

(2) PTZ Parameters

Configure PTZ shortcut operations such as rotation speed, shortcut keys, etc. according to the actual needs.

- Click at the right corner, select **Local Configuration**.

PTZ

Rotate at a constant speed ☐
 Use the mouse to control the selected pane ☒

Use the keyboard to control the selected pane ☐

1 U 2 +

L 3 R -

4 D 5

Note: shortcut keys can be set for English letters (a~z) on the keyboard, keyboard 1~9, plus and minus symbols [+,-]

- Set PTZ parameters as needed.
- Click **OK**.

4.1.2 Audio Services

1. Two-way Audio

Two-way audio means audio intercom between the client and a camera.



NOTE!

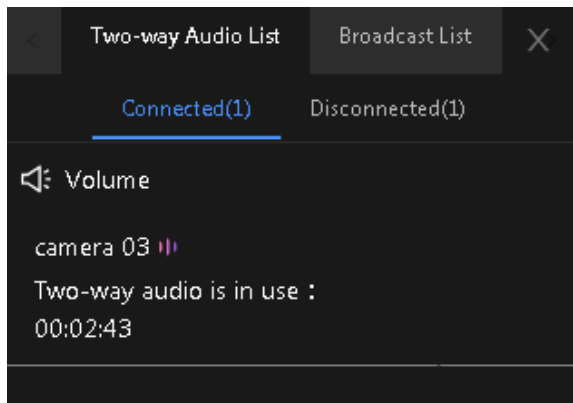
Check that the client is connected to audio input and output devices.

(1) Start/stop Two-way Audio

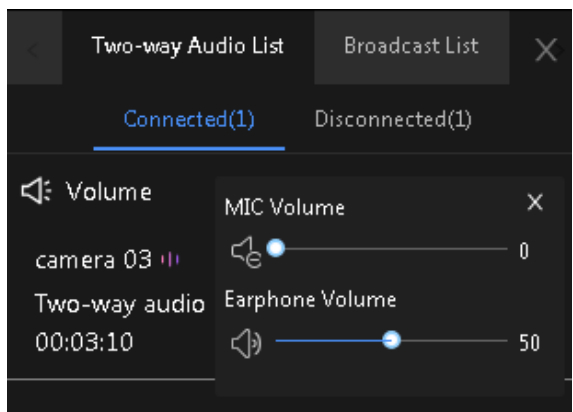
- Start two-way audio: Start live video and then click .
- Stop two-way audio: Click .

(2) View Two-way Audio Information

Start live video, click  to expand the two-way audio list showing two-way audio information.



- Adjust sound volume: Click  to adjust MIC or speaker volume.



- Restart two-way audio: Click .
- Delete two-way audio: Click .

2. Broadcast

Broadcast is one-way audio from the client to multiple cameras.



NOTE!

- Check that the client is connected to audio input and output devices.
- You can perform broadcast to up to 128 cameras at the same time.

(1) Start/stop Broadcast

- Start broadcast: Start live video and then click .
- Stop broadcast: Click .

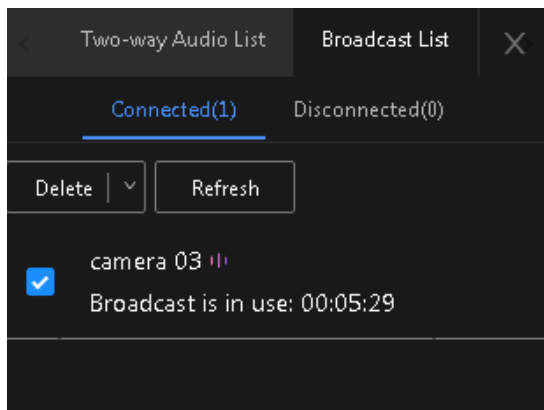


NOTE!

Two-way audio must be stopped before you can start broadcast.

(2) View Broadcast Information

Start live video, click  to expand the broadcast list and view broadcast information.



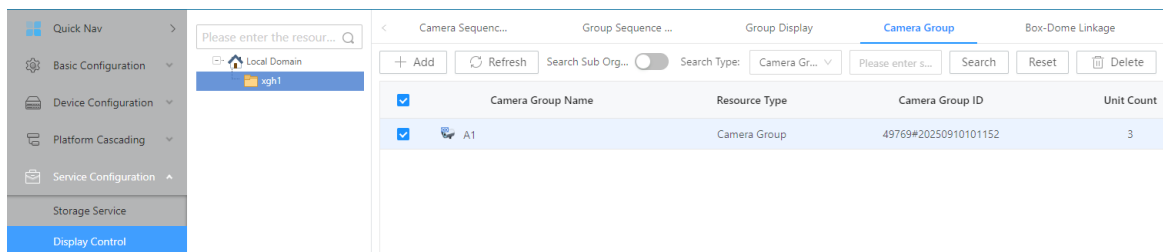
- Delete one: Point to a broadcast task, click .
- Delete the selected: Select broadcast tasks, click **Delete**, choose **Delete Selected**.
- Delete All: Click **Delete**, choose **Delete All**.

4.2 Camera Group

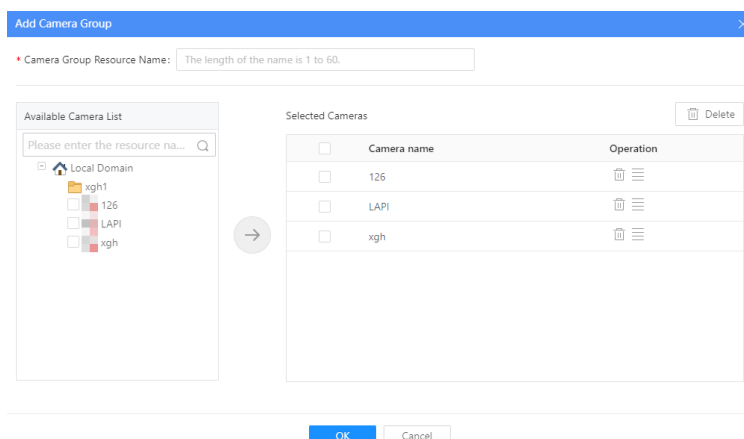
Supports adding multiple cameras into a group, enabling convenient one-click batch operations.

4.2.1 Configure Camera Group

1. Go to the **Device Management > Service Configuration > Display & Control Service** interface, and select the **Camera Group** tab.



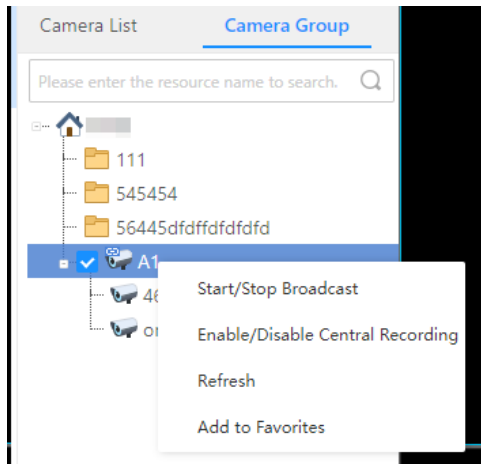
2. On the left side, select the organization to which resources will be added.
3. Click **Add** to enter the [Add Camera Group] interface.



4. Customize the camera group name, select multiple cameras from the camera list, and click  to move them to the selected camera list. .
5. Click **OK** to create the camera group.

4.2.2 Activate Camera Group

In the **Live View > Camera > Camera Group** interface, right-click a camera group and select **Start/Stop Broadcasting** or **Start/Stop Central Recording** to perform batch operations on all devices within the group.



4.3 Camera Sequence

Play live video of each camera in a sequence resource in sequence in a window.

4.3.1 Configure Camera Sequence Resource

1. Use either method to go to the **Add Camera Sequence Resource** page.
 - Go to **Live View > Camera Sequence**, click  at the top right of the sequence resource list. A window appears.
 - Go to **Device Management > Service Configuration > Display Control**, choose **Camera Sequence Resource**, click **Add**. A window appears.

Add Camera Sequence

*Camera Sequence Name:

Camera List

Enter the resource name

12345678901144567895-cam-04

192.168.1.15.110

192.168.1.15.111

192.168.1.15.112

192.168.1.15.113

192.168.1.15.114

192.168.1.15.118

192.168.1.15.122

192.168.1.15.123

3.124

IMOSztas

Stay Time: 10s

Stream Type: Auto-Adaptation

Selected Cameras

Delete

☐	Camera Name	Stay Time(s)	Stream Type	Operation
☐	192.168.1.15.110	10	Auto-Adaptation	
☐	192.168.1.15.111	10	Auto-Adaptation	

Organization: Please select organization

Confirm

Cancel

- Set the camera sequence name.
- Choose cameras from the left-side camera list, set display interval (length of time the camera's image is displayed during camera sequence) and stream type (auto, main stream, sub stream, and third stream).
- Click to add to the camera sequence group.



NOTE!

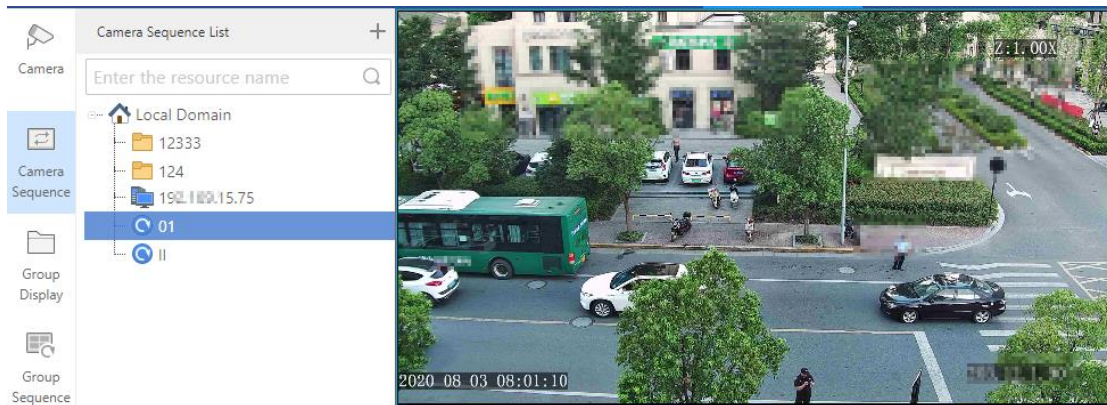
- Click to edit the display interval and stream type.
- Click the corresponding to delete a camera; or select multiple cameras and then click Delete.
- You can drag to rearrange the camera order.

- Choose an organization for the sequence.
- Click **OK**.

4.3.2 Start Camera Sequence

Use the following methods to start camera sequence:

- Select a window, and then double-click the sequence resource.
- Drag a sequence resource to a window.
- Select a window, right-click the sequence resource, choose **Start**.



4.3.3 Camera Sequence Toolbar

Use the right-click menu or camera sequence toolbar to set camera sequence parameters, take snapshots, and more.

1. Right-click Menu Operations

Right-click a camera sequence window and then use the menu to close the window, close all windows, maximize/restore the window, and play live video to the video wall.

2. Camera Sequence Toolbar Operations

The toolbar appears when you point to the image.



Table 4-5 Window Toolbar Functions

Icon	Function	Description
	Pause/resume sequence	● Pause sequence: Only to play the live video of the current camera. ● Resume sequence: Continue the camera sequence.
	Previous/next camera	Go to the previous/next camera in the sequence resource.
	Snapshot	Capture the current image(s) in the window and save to the computer.
	PTZ control	Click to expand the control panel to change settings such as focus, iris, rotation direction, rotation speed, preset, patrol route, etc. See PTZ control. Note: This function is only available to PTZ cameras.

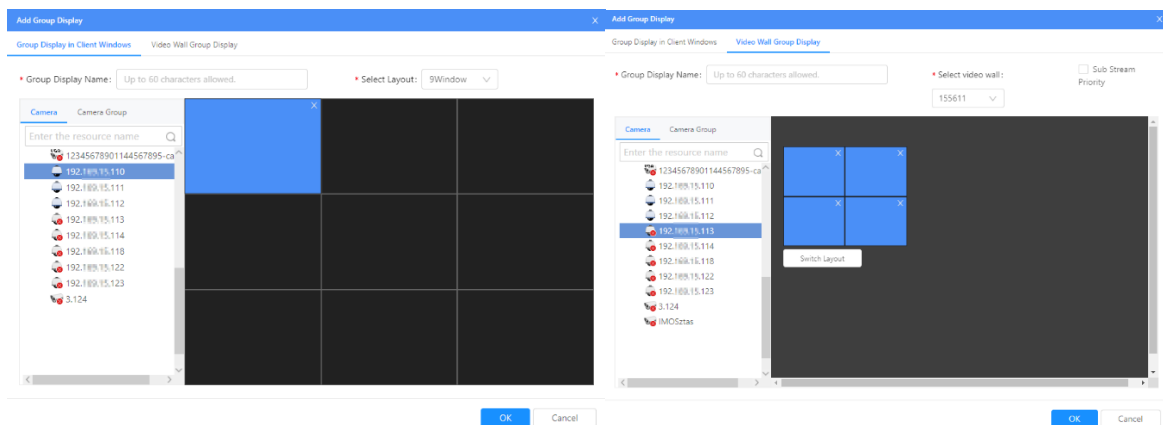
	Start/stop broadcast	Click to start one-way audio broadcast from the client to cameras.
	Start/stop two-way audio	Click to start audio intercom between the client and a camera.
	Instant playback	Start playing video backward from the current time to up to 24 hours earlier (if available).

4.4 Group Display

Simultaneously play the live video of all cameras in a camera group in multiple windows.

4.4.1 Configure Group Display

- Use the following methods to add a group display:
 - Go to **Live View > Group Display**, start live view, click  to save the current video display as a group display.
 - Go to **Device Management > Service Configuration > Display Control**, choose **Group Display**, click **Add**. A window appears.



- Choose a group display type: client window group display or video wall group display, and configure group display.

Table 4-6 Parameter Descriptions

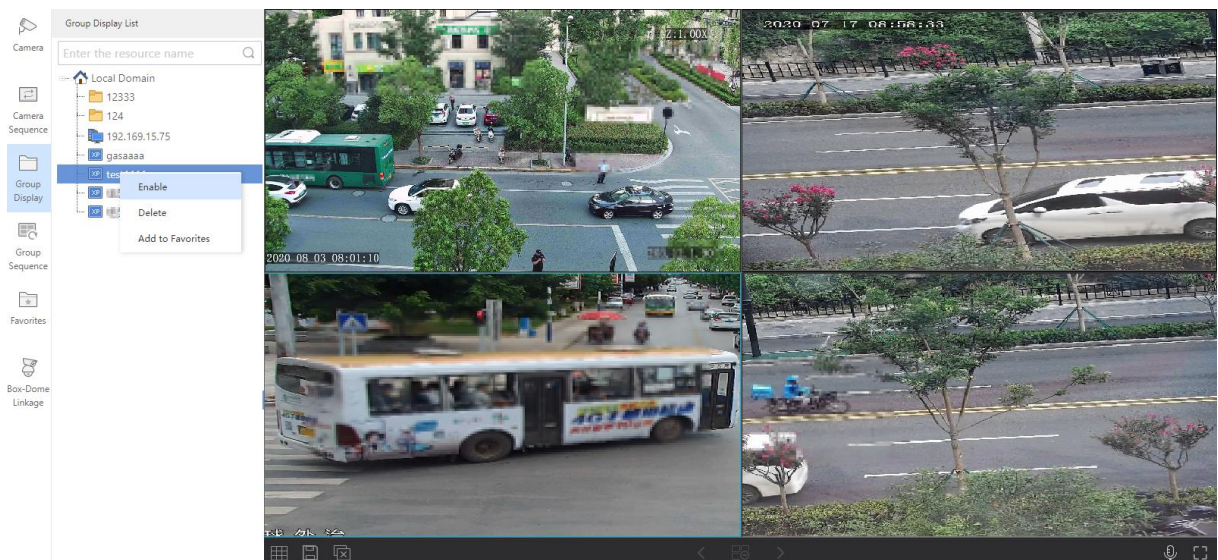
Type	Group display in Client Window	Group Display on Video Wall
Group display name	Enter the group display name. Up to 60 bytes.	
Choose layout/video wall	Choose a layout from the list. Up to 25 windows.	Choose a video wall from the list. Caution: You may want to choose sub stream priority to save bandwidth.
Choose camera/camera group	Drag resources from the resource list to client windows or monitor windows. Note: When you choose a camera group, the cameras in the group will bind to client windows or video wall screens one by one in sequence. To view all the cameras in the group, make sure the number of client windows or video wall screens is not less than that of the cameras. You can switch the window layout directly when playing group display on a video wall. See the Video Wall chapter for details.	

- Click **OK**.

4.4.2 Start Group Display

Use the following methods to start group display:

- Double-click the group display resource.
- Right-click a group display resource, choose **Start**.



4.5 Group Sequence

Play live video of multiple cameras in multiple windows (custom window layout) in sequence at a set time interval.

4.5.1 Configure Group Sequence Resource

Configure group sequence on client windows, DC video walls, and DX video walls.

1. Go to **Device Management > Service Configuration> Display Control**, choose **Group Sequence Resource**, click **Add**.
2. Choose client group sequence.



NOTE!

You can also add client group sequence in the **Live View** under **Live View > Group Sequence**.

Add Group Sequence

Client Group Sequence

DC Video Wall Group Sequence

Splicing Control Sequence

* Sequence Name:

Up to 60 characters al...

* Sequence Type:

☒ Auto Layout Sequence
 ☐ Group Display Sequence

* Stay Time:

10s

* Select Layout:

9Window

* Startup Mode:

☒ Non-preemption Mode
 ☐ Preemption Mode

Camera List

Enter the resource name

☐ 12345678901144567895-cam
 ☐ 192.168.1.110
 ☐ 192.168.1.111
 ☐ 192.168.1.112
 ☐ 192.168.1.113
 ☐ 192.168.1.114
 ☐ 192.168.1.118
 ☐ 192.168.1.122
 ☐ 192.168.1.123
 ☐ 3.124
 ☐ IMOSztas

Selected Cameras

☐ camera name
 Stream Type
 Operation

☐ 192.168.15.110
 Auto-Adaptation
 ☐ ☐ ☐

☐ 192.168.15.111
 Auto-Adaptation
 ☐ ☐ ☐

☐ 192.168.15.112
 Auto-Adaptation
 ☐ ☐ ☐

→

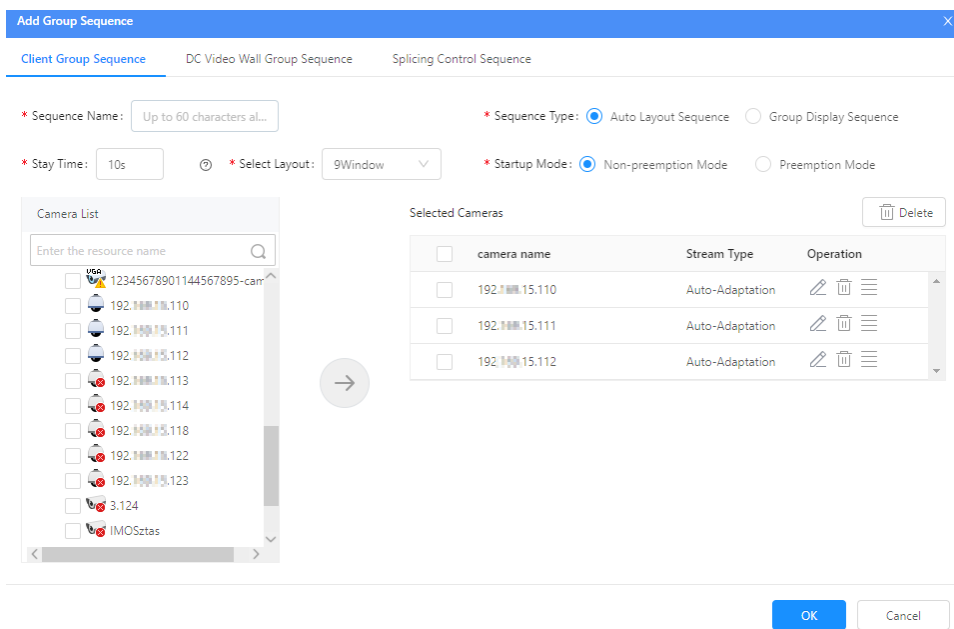
Delete

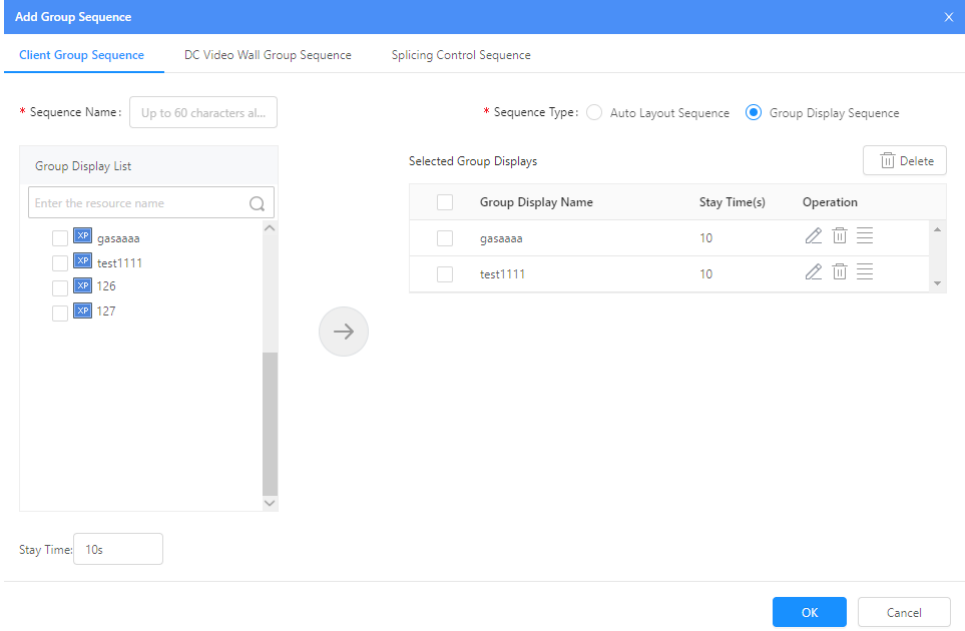
OK

Cancel

3. Set the parameters including the sequence name and add the sequence group.

Table 4-7 Sequence Configuration Description

Type	Description
Auto Layout Sequence	During sequence, cameras are automatically assigned to client or monitor windows and may not always be in the same windows. All cameras' images switch automatically after each display interval. If a camera or a monitor happens to fail, the sequence automatically skips the failed camera or monitor and needs no modification.  Configure the parameters, select cameras from the left-side list, and then click  to add the selected cameras to the sequence group. ● Display Interval: The duration of the live video of each camera in the sequence group. ● (Client group sequence): Layout: Number of windows used to play the group sequence. ● Organization: The organization to which the sequence resource belongs to. ● Startup Mode

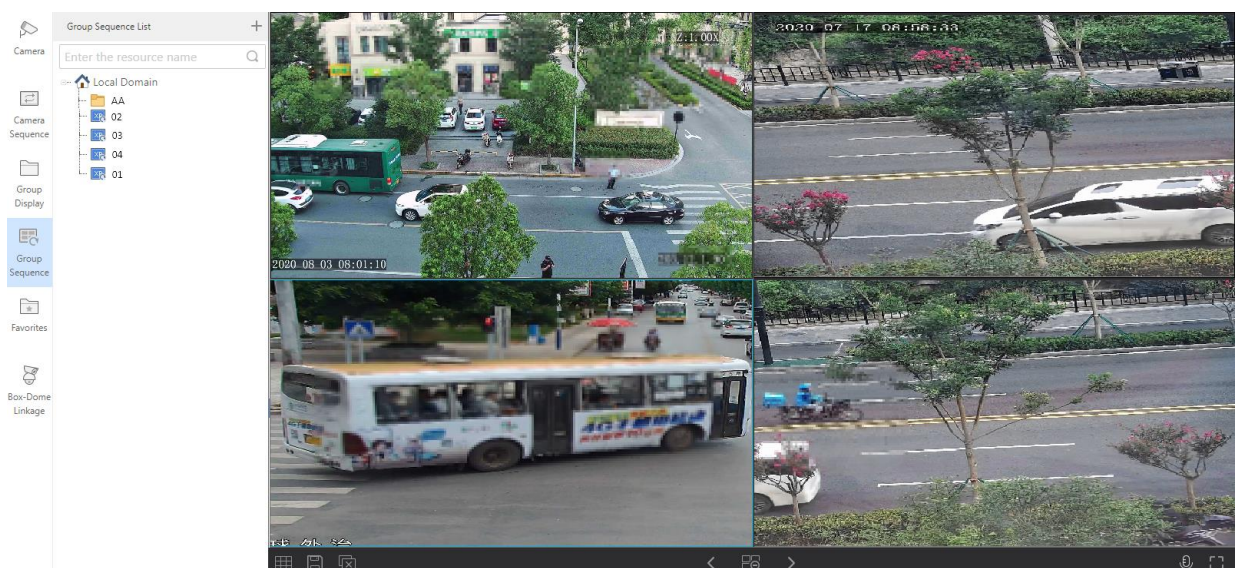
	➤ Preemption mode: The group sequence will replace the ongoing live video at startup. ➤ Non-preemption mode: The group sequence will not replace the ongoing live video at startup.
Group Display Sequence	Play live video of cameras in specified client windows or monitor windows, and the layout does not change during the sequence. If a camera or a monitor happens to fail, you need to modify the group display configuration. Make sure you have configured the group display resource. See Configure Group Display.  Choose group display resources from the left-side list, set a display interval for each group display, click  to add them to the sequence group.

4. Click **OK**.

4.5.2 Start Group Sequence

Use the following methods to start group sequence:

- Double-click the sequence resource.
- Right-click the sequence resource, choose **Start**.



4.5.3 Group Sequence Toolbar

Use the right-click menu or sequence toolbar to set sequence parameters, take snapshots, and more.

1. Right-click Menu Operations

Right-click a camera sequence window and then use the menu to close the window, close all windows, maximize/restore the window, and play live video to the video wall.

2. Group Sequence Toolbar Operations

Point to the image to show the toolbar.

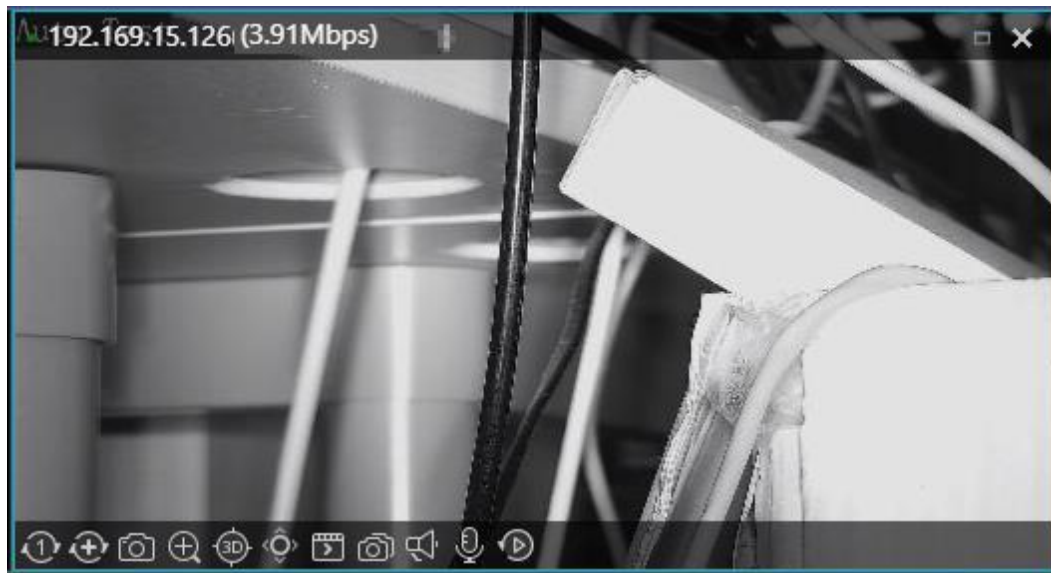


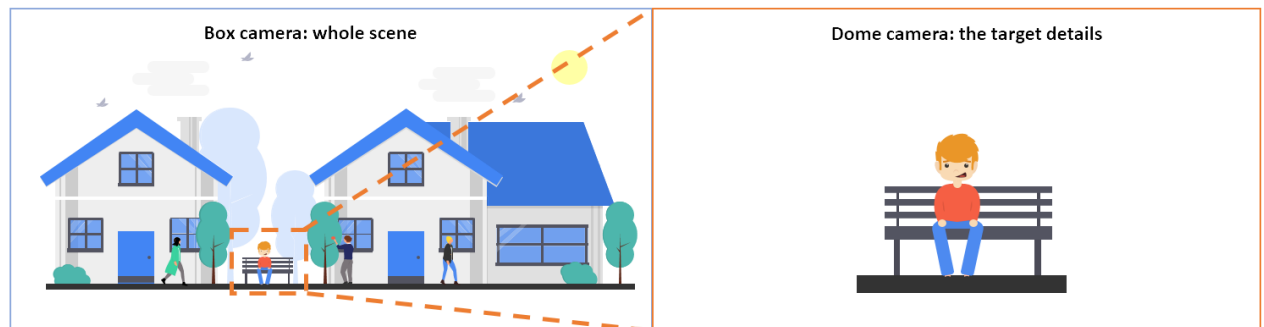
Table 4-8 Window Toolbar Functions

Icon	Function	Description
	Preset	Buttons for No.1 preset and other presets. You can click a preset to quickly switch to the desired image.
	Snapshot	Capture the current image(s) in the window and save to the computer.
	Continuous Snapshots	
	Digital Zoom	Zoom in on an area of interest on the video image in the window. Note: Use the scroll wheel to zoom in or out.
	3D positioning	Perform 3D positioning, including click-to-position and drag-to-zoom. ● Click to position: Click anywhere on the image, and the camera automatically centers on the point you clicked to display the image. ● Drag to zoom: Drag on the image from top left to bottom right to zoom in, and drag in the opposite direction to zoom out.
	PTZ control	Click to expand the control panel to change settings such as focus, iris, rotation direction, rotation speed, preset, patrol route, etc. See PTZ control. Note: This function is only available to PTZ cameras.
	Start/stop recording.	local Record the live video playing in the window and save to the computer.

Icon	Function	Description
	Start/stop broadcast	Click to start one-way audio broadcast from the client to cameras.
	Start/stop two-way audio	Click to start audio intercom between the client and a camera.
	Instant playback	Start playing video backward from the current time to up to 24 hours earlier (if available).

4.6 Box-Dome Linkage (Panoramic Linkage)

Box-dome linkage uses box and dome cameras to provide both a big picture of the whole scene and close-up images of the target for details.



The system supports two modes: 1 box camera + 1 dome camera, and 3 box cameras + 1 dome camera.

- 1 box camera + 1 dome camera: mainly used in small scenes, such as entrance&exit.
- 3 box camera + 1 dome camera: mainly used in large scenes, such as large parking lots.

4.6.1 Add Box-Dome Linkage Resources

Choose a way to add box-dome linkage resources:

- On the video management platform, go to **Device Management > Service Configuration > Display Control > Box-Dome Linkage**, choose online box camera(s) and a dome camera. You may choose 1 box camera & 1 dome camera, or 3 box cameras & 1 dome camera.



NOTE!

If the camera is a dual-channel network PTZ camera, go to **Device Management > Device Configuration** and add the camera via the Private protocol.

- Configure box-dome linkage on the camera's Web interface: Enable box-dome linkage, link box and dome cameras, and calibrate the linkage on the box camera's live view image. After you complete the box-dome linkage on the camera, add the camera to the platform via the Private or GB protocol, and then you can operate the cameras on the platform.

Prerequisite

The dome cameras and box cameras have been added on the video management platform and are online.

Steps

1. Go to **Device Management > Service Configuration > Display Control > Box-Dome Linkage**, double-click the target organization on the left-side list.
2. Click **Add**. A page as shown below appears.

3. Enter a name for the linkage, and then choose a linkage mode according to the scene.

4. Add cameras:

- Box camera: Select box camera(s) on the box camera list according to the linkage mode you chose.



CAUTION!

If the linkage includes three box cameras, make sure:

- The box cameras are added via the Private protocol.
- The encoding settings and resolutions of the three box cameras are the same.

- Dome camera: Choose the dome camera from the dome camera list.

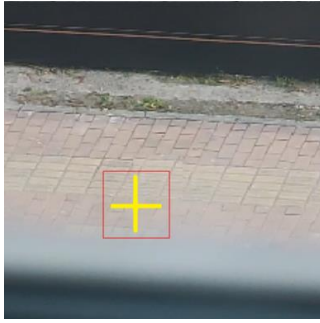
5. Click **OK**.

4.6.2 Calibrate Dome Camera

Calibrate the dome camera(s) on the platform. The figures below are for reference only. The actual UI display may be different.

Steps

1. Go to **Live View > Panoramic Linkage**, enable the box-dome linkage resource.
2. If the linkage includes 3 dome cameras, right-click on the box camera's image, choose **Start Splice**, and then splice images of the three dome cameras. After splicing is completed, the spliced image is displayed in the window at the center. Skip this step if the linkage involves only one dome camera.
3. Right-click on the box camera's image, choose **Calibrate Dome Camera**.
4. Set focus (range: 1-16, unit: mm), click **OK**.
5. Calibrate the linkage.
 - (1) Click on the box camera's image, the position marked with a yellow $\oplus$ means the demarcate point.



- (2) Rotate the dome camera till the center point (red +) on the dome camera's image coincides with the demarcate point (yellow +) on the box camera's image.

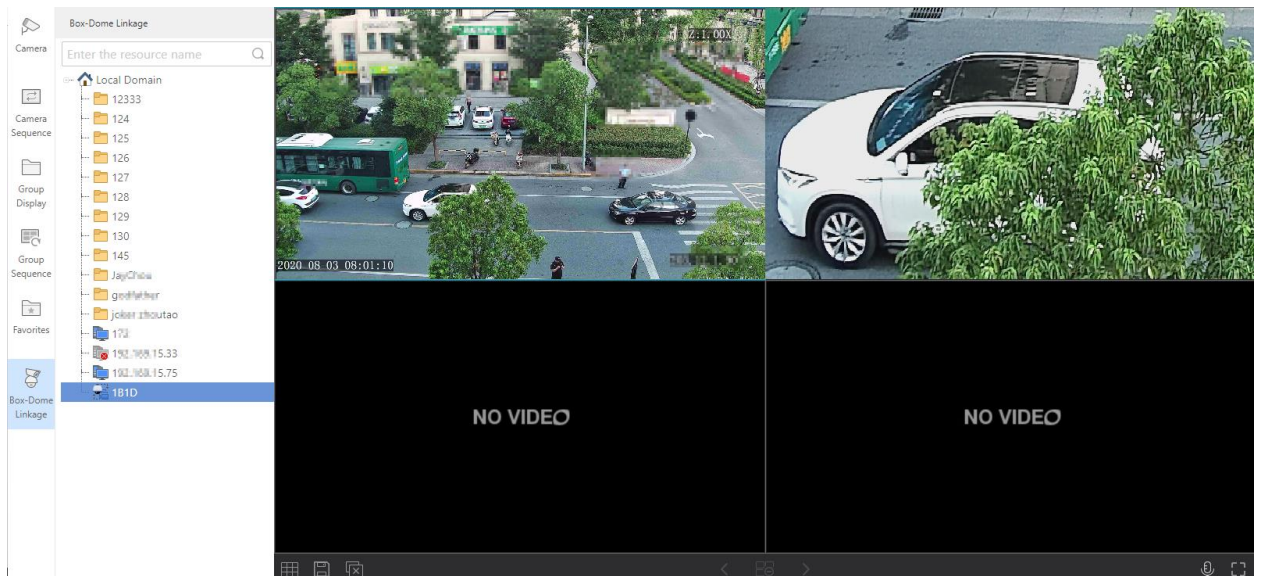


- (3) Right-click and then choose **Next Dome Demarcate Point**, and then repeat steps 1 to 2.
 (4) Repeat steps 1 to 3 for ten times. The calibration finishes when **Finish Calibration in Panoramic Linkage** appears on the box camera image.

4.6.3 Start Box-Dome Linkage (Panoramic Linkage)

Use the following methods to start box-dome linkage:

- Double-click the box camera.
- Right-click the dome camera, choose **Start**.



1. Drag to Zoom

After you drag the mouse to select an area on the dome camera's image (1 dome) or on the spliced image (3 domes), the dome camera automatically rotates and zooms in on the dragged area.

**Note:**

If the zoomed area is inconsistent with the dragged area, repeat the calibration steps (see Calibrate Dome Camera).

2. Click to Link

Right-click on the box camera's image and then choose **Click to Link**. After you click anywhere on the box camera's image (left), the dome camera (right) automatically adjusts direction and zoom to display the clicked point at the center of the image.

3. Track

Right-click on the box camera's image and then choose **Track**. After you choose a moving object (vehicle or human) on the box camera's image (left), the dome camera (right) automatically tracks the object till the object leaves the monitored area.

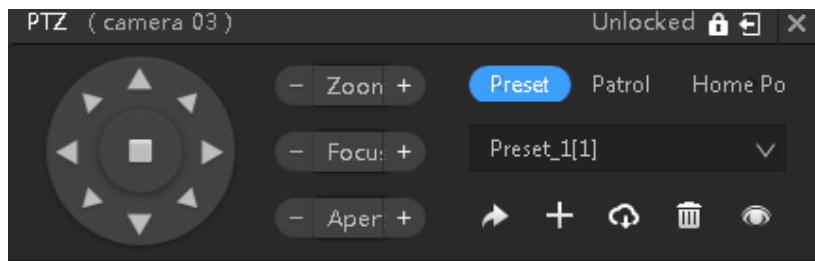
4.7 Patrol

The PTZ camera pans and tilts according to a sequence of preset actions. By configuring presets, patrol routes, and patrol schedules, you can enable the PTZ camera to patrol along the designated route or according to the schedule.

4.7.1 Configure Presets

Set specific shooting angles as presets. After being idle (no user action) for a certain length of time, the camera can automatically go to a specified preset to continue monitoring.

1. Go to **Live View**, point to the PTZ camera's live view window, click  to open the PTZ control panel.



2. Click  to add a preset.

Add Preset

X

PresetID :

Preset Name :

Confirm

Cancel

3. Enter the preset ID and name.
4. Click **OK**.

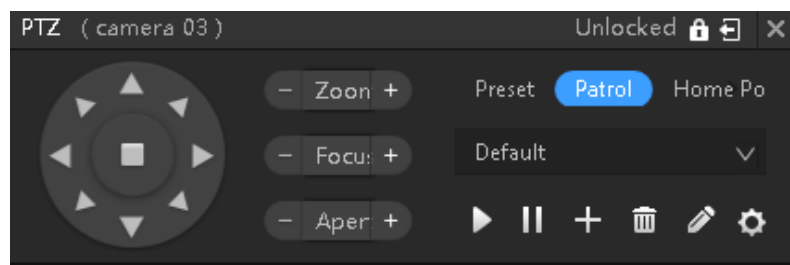
4.7.2 Configure Patrol Route

Three patrol types:

- Preset patrol: The PTZ camera patrols among multiple presets.
- Patrol: The PTZ camera rotates in the specified direction (e.g., up, left).
- Scan patrol: The PTZ camera rotates between two presets (one high, one low) at a certain tilt angle. This type is suitable for thermal imaging cameras to detect fires.

1. Add Patrol Route

1. Go to **Live View**, point to the PTZ camera's live view window, click  to open the PTZ control panel.
2. Click **Patrol**.



3. Click . A page as shown below appears.

Add Patrol Route

Name:

☒ Preset and Preset Patrol

Add

delete

Set Top

Up

Down

Set Bottom

Preview

	Action	Preset	Stay Time	Speed	Keep Rotating	Duration	Operation
No Data							

Live Video:

Add Preset

2022/08/16 11:24:29

Confirm

Cancel

4. Enter the patrol route name.
5. Click **Add**. The patrol route list appears.

☐	Action	Preset	Stay Time	Speed	Keep Rotating	Duration	Operation
☐	Down ▾	/	/	5	no ▾	10	
☐	Go to Pre... ▾	Preset_1 ▾	10	/	/	/	
☐	Up ▾	/	/	5	yes ▾	10	
☐	Go to Pre... ▾	Preset_1 ▾	10	/	/	/	

6. Configure patrol routes.

Table 4-9 Patrol Route Description

Patrol Type	Parameter	Description
Preset patrol	Action	Choose Go to Preset .
	Preset	Select presets to be used in the patrol route. Note: You can click Add Preset to add presets.
	Stay Time	Enter the length of time that the camera will stay at the preset. The default is 10s.
Recorded Patrol	Action	Choose Down/Up/Left/Right .
	Speed	Set a rotation speed level for the camera. The default is 5.
	Keep Rotating	Set whether the camera keeps rotating. - If you choose Yes, the camera will not perform the following actions, and will keep rotating until it stops patrol. - If you choose No, the camera will repeat the action until the specified length of time is over (default is 10s).
Scan patrol	Start preset	Preset where the patrol starts.
	End preset	Preset where the patrol ends.
	Patrol Gradient	Tilt angle. The camera ascends/descends the height according to the set gradient.
	Direction	Initial patrol direction, clockwise or counterclockwise.
	Speed	Set a rotation speed for the camera. The default is 5.

7. Click **OK**.

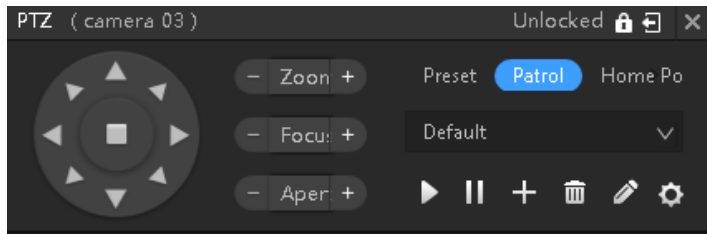
2. Manage Patrol Routes

You can edit or delete patrol routes as needed.

- To edit a patrol route, select the patrol route and then click .
- To delete a patrol route, select the patrol route and then click .

4.7.3 Configure Patrol Schedule

- Go to **Live View**, point to the PTZ camera's live view window, click to open the PTZ control panel.
- Click **Patrol**.



3. Click . A page as show below appears.

4. Configure the patrol schedule by referring to the table below.

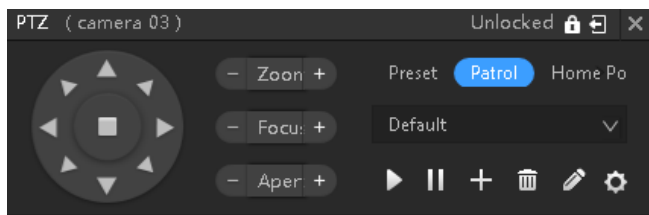
Table 4-10 Parameter Descriptions for Patrol Schedule

Parameter	Description
Patrol resuming time	Set the length of time that the camera stays at the current position after detecting a fire before continuing the patrol.
Patrol Schedule	Enable or disable the patrol schedule.
Program Name	Name of the patrol schedule.
Time Period	Start and end times of a patrol route (the time periods must not overlap). Set by day or by week and then assign the set periods to different patrol routes.
Enable Exception	If necessary, enable exception and set special time periods for certain patrol routes. During the special periods, only the specified patrol routes will be performed. On the special days, the system performs patrol only during the set periods; on other days, the system performs patrols according to the schedule. Note: Click  to add an exception. Up to 16 exceptions are allowed. Click  to delete an exception.

5. Click **OK**.

4.7.4 Start Patrol

1. Go to **Live View**, point to the PTZ camera's live view window, click  to open the PTZ control panel.
2. Click **Patrol**.



3. Choose a patrol route.
4. Click  to start patrol. To stop the patrol, click .

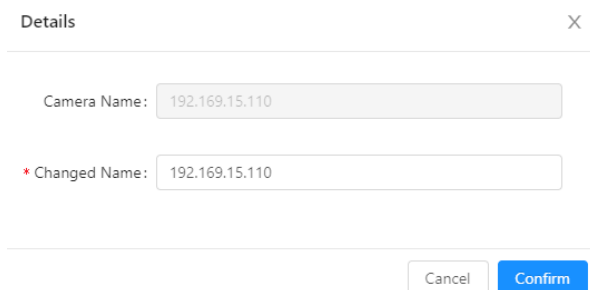
4.8 Live Video Resource Management

View camera resources and monitoring relationship, rename cameras, edit camera attributes, and view resource statistics.

4.8.1 Camera Management

1. Rename Camera

Right-click a camera on the resource list, choose **Change Name**, and then change the camera name in the window as shown below.



Details X

Camera Name: 192.169.15.110

* Changed Name: 192.169.15.110

Cancel Confirm

2. View Camera Information

Right-click a camera on the resource list, choose **View Detailed Information**. A window as show below appears. The window shows the camera name, type, device IP, organization, PTZ control protocol/address code information (of PTZ camera).

Details
X

Camera Name :

192.168.1.110

Camera Type :

PTZ Control Protocol :

PELCO-D

PTZ Address Code :

128

Home Device IP :

192.168.1.110

Organization :

Local Domain

3. View Camera's Monitoring Information

Right-click a camera on the resource list and then choose **View Monitoring Relation** to view the current services, service status, user name, and login IP of the camera.



Note:

The super administrator can choose a camera to stop monitoring.

Monitoring Relation
X

Camera Name: 192.168.1.110

Organization: Local Domain

Current Total Number of Monitoring: 1

Stop Live Video

Refresh

	Monitor	Window	Service Type	Username	Status	User IP
☐	window1...	1	Live Video	loadmin	Running	192.168.1.110

4. Configure Camera Details

Right-click a camera on the resource list and then choose **Details**. A page as shown below appears. You can view and edit the surveillance location, installation location, usage, and illumination information.

Details
X

Monitoring Site: Government Facilities

Installation Location: ☒ Outdoors ☐ Indoors

Camera Usage: ☒ Public Security ☐ Transportation ☐ Key Area

Illumination: ☒ No Illumination ☐ IR Illumination ☐ White Light Illumination

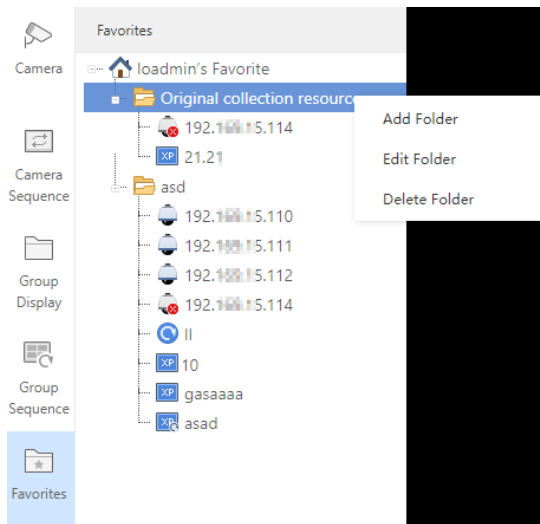
Monitoring Direction: East

Cancel

Confirm

4.8.2 Favorites

Add resources and scenes to favorites folders for quick operation (operations to resources, scenes, and plans in favorites folders are the same as operations to resources, scenes, and plans in their corresponding lists).



Manage Resources in Favorites

- To add a resource to favorites, right-click the resource and then choose **Add to Favorites**.
- To remove a resource from favorites, right-click the resource and then choose **Remove from Favorites**.

Favorites Folder Operations

Add, delete, or edit favorites folder. After the above actions, you need to right-click **Favorites** and then choose **Refresh** to update the favorites tree.

- To create a folder on the favorites tree, right-click the parent folder, choose **New Folder**, set the folder name, and then click **OK**.



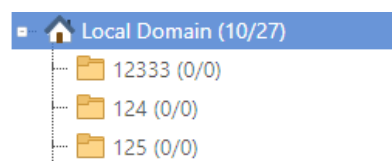
Note:

- Up to three levels of folders are allowed.
 - Each folder name must be unique.
-
- To delete a folder, right-click it and then choose **Delete Folder**. All the folders and resources under the folder will also be deleted.
 - To rename a folder, right-click the folder, choose **Change Folder**, enter the new name, and then click **OK**.

4.8.3 Resource Statistics

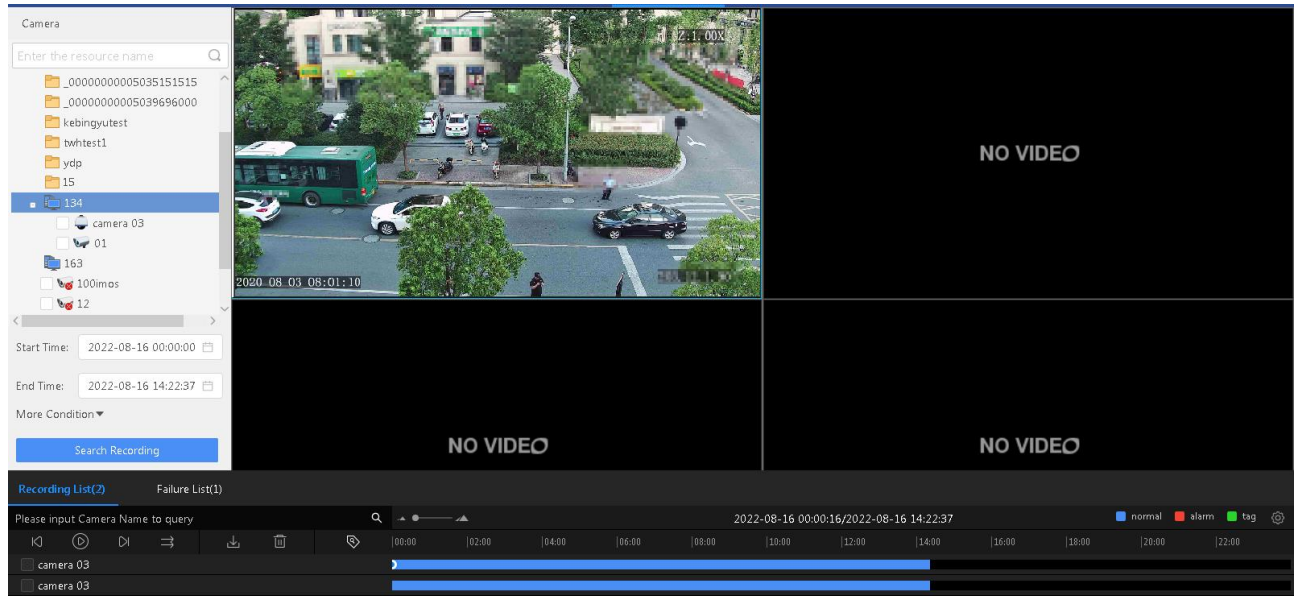
View camera resource statistics.

Right-click the target organization, and then choose **Resource Statistics** to view camera statistics of the organization, including the number of online cameras and the total number of cameras in the organization. After resources changed, you need to perform the above operation again to update the statistics.



5 Playback

Play recorded videos to review events.



Prerequisite:

- Add [DM/BM/IPSAN](#) devices.
- Configure [Storage Resource](#).

5.1 Search and Playback

Two methods are available to search recordings and start playback:

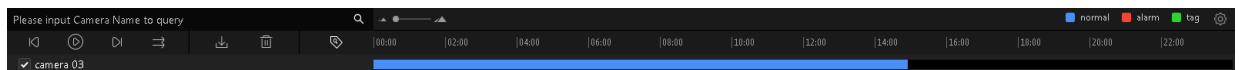
- Search multiple cameras at a time
 1. Select cameras on the left-side organization list.
 2. Set the start time, end time, target domain, storage location, and recording type. See the table below for detailed descriptions.

Table 5-1 Recording Parameter Descriptions

Parameter		Description
Start Time		Start time of recording playback.
End Time		End time of recording playback.
Domain	Registered Domain	Search recordings saved on the storage resources of the platform where the camera is registered.
	Current Domain	Search recordings saved on the storage resources in the local domain.
	Cloud Retrieval	● If CDS has been configured for a domain, cloud retrieval can only retrieve recordings saved on the CDS of this domain. ● If CDS has not been configured for a domain, cloud retrieval can retrieve recordings saved on all types of storages of this domain.
Storage Location	Edge Recording	Recordings saved on storage resources of IPC/NVR.

	Central Recording	Recordings saved on central storage resources of the platform, for example, IPSAN, CDS.
	Fuzzy Retrieval	Search all recordings, including edge recording and central recording.
Recording Type	Scheduled Recording	Recordings that are saved according to the set schedule.
	Alarm Recording	Alarm-triggered recordings.
	Manual Recording	Recordings that are saved manually.
	All Recordings	Includes scheduled recording, alarm recording, and manual recording.

3. Click **Search Recording**. Search results are displayed on the bottom toolbar.



- Search recordings of one camera:
4. Double-click the camera, and then set the start time and end time.
5. Click **OK**. Search results are displayed on the bottom toolbar (same as above).



NOTE!

If the search failed, you can view the failure cause at the bottom toolbar and delete playback tasks.

5.2 Start Playback

Use the following methods to start playback after finding the desired recordings.

- On the bottom toolbar, select a camera, click  (play all recordings one by one) or click  (play one).
- On the progress bar on the bottom toolbar, drag the desired recording segment, choose **Playback**.
- Double-click the progress bar at the bottom toolbar.

5.3 Playback Toolbar

During playback, you can use the playback toolbar, progress bar, and window toolbar, and window right-click menu to perform the desired operations.

1. Window Toolbar

The window toolbar appears when you point to the window.



Table 5-2 Window Toolbar Icon Description

Icon	Function	Description
	Snapshot	Capture the current image(s) in the window and save to the computer.
	Continuous Snapshots	Continuously capture current images in the window and save to the computer.
	Digital Zoom	Zoom in on an area of interest on the image in the window. Use the scroll wheel to zoom in or out, and click again to stop digital zoom.

2. Playback Toolbar

The playback toolbar is at the bottom of the playback page.

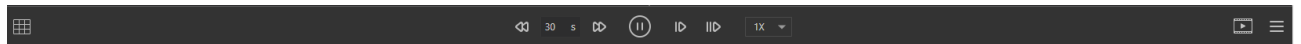


Table 5-3 Playback Toolbar Icon Description

Icon	Function	Description
	Switch the window layout.	1/4/6/9 window layouts are available.
	Play/Pause	Play/pause the video in the window.
	Forward/rewind	Play the previous/next recording at the set interval (1-999s, default is 30s).
	Forward by Frame	Fast forward by frame.
	Play by frame	Play one frame of image per second. Local recording playback does not support this function.
	Adjust speed	Change the playback speed.
	Hide/show toolbar	Show or hide the bottom toolbar and progress bar.
	More > Full Screen	Play video in full screen. Press Esc to exit.

3. Bottom Toolbar

The bottom toolbar shows the recording list and the failure list.

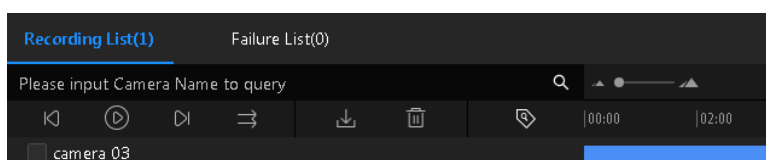
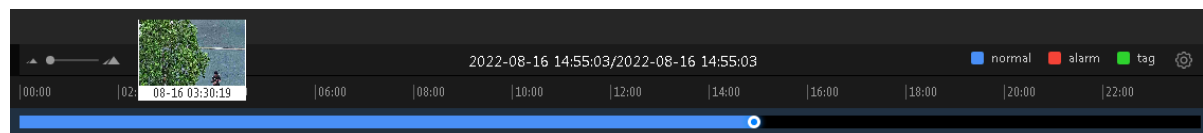


Table 5-4 Bottom Toolbar Description

Icon	Function	Description
	Previous/next	Play the previous/next segment.
	Play all	Play all video segments continuously from the current position on the progress bar.
	Play	Play a recording from the current position on the progress bar.
	Synchronous Playback	Play multiple recordings synchronously on the progress bar.
	Manual recording backup	Back up recordings manually.
	Download recording	Download recordings to your computer.
	Delete recording	Delete the search record.
	Search tag	Show yellow tags on the progress bar. By default it is selected. You can switch to the previous or next tag, search tags, and delete tags.

4. Playback Progress Bar

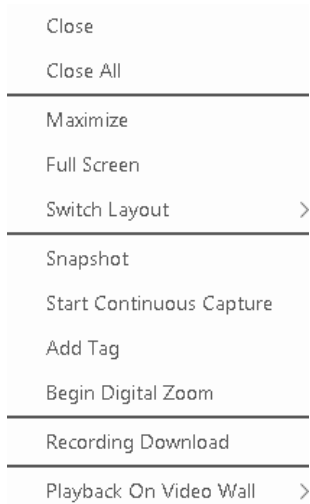
The playback progress bar shows the progress of the recording playing in the selected window.



- Drag to adjust the playing progress, or double-click on the progress bar to play the video of the corresponding moment.
- Use  to adjust the time scale on the progress bar.
- Select a tag to show the tag in green on the progress bar, point to the tag to view the tag name; double-click the tag to play the video of that moment.
- Select an alarm to show the alarm-triggered recording in red on the progress bar, double-click anywhere on the red segment to play the video of the corresponding moment.
- Drag to select a segment to perform the desired actions: play or download.
- Point to anywhere on the progress bar to preview the corresponding video clip (1s) and time information.

5. Right-click Menu

Right-click on a window and then perform the desired action: close the current window, close all windows, maximize/restore a window, switch to full screen, change the window layout, take a snapshot, take continuous snapshots, add a tag, enable digital zoom, download recording, and play recording on a video wall.



- To add a tag, right-click a window and then choose **Add Tag**.

Add Tag
✕

Tag Time : 2022-08-16 14:55:03

Tag Name :

Confirm
Cancel

5.4 Playback by Segment

Play recordings by segment.

1. Start playback.
2. Click . The bottom toolbar is displayed. Click the **Recording List** tab.
3. Drag on the progress bar to specify a segment and then choose **Segmented Playback**.

Playback
Download
Segmented Playback



Segmented Playback
✕

Time: 

Segment Number:

Confirm
Cancel

4. Check the time range of the recording. Change it if necessary.
5. Set the number of segments, click **OK**. The segments will play in different windows simultaneously.



NOTE!

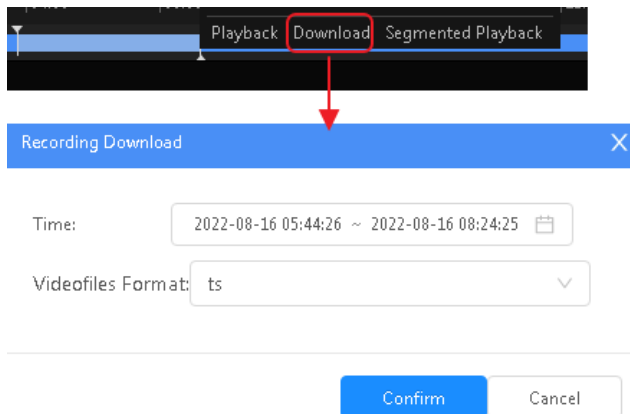
Up to 4 segments are allowed.

5.5 Download Recording

Download recordings from the storage device to your computer.

Steps

1. Start playback.
2. Click  in the lower right corner. The bottom toolbar is displayed. Click the **Recording List** tab.
3. Drag on the progress bar to specify a segment and then choose **Download**.



4. Check the time range of the recording. Change it if necessary.
5. Choose the file format, .ts or .mp4.
6. Click **OK**.



NOTE!

- You may also right-click a window and choose **Recording Download** to download recordings.
- Up to two channels of recordings can be downloaded at the same time.

6 Video Wall

The system supports DC video wall, DX video wall, and A8 video wall. Some DX video walls are created with one DX device, and some can be created with multiple DX devices.

6.1 DC Video Wall

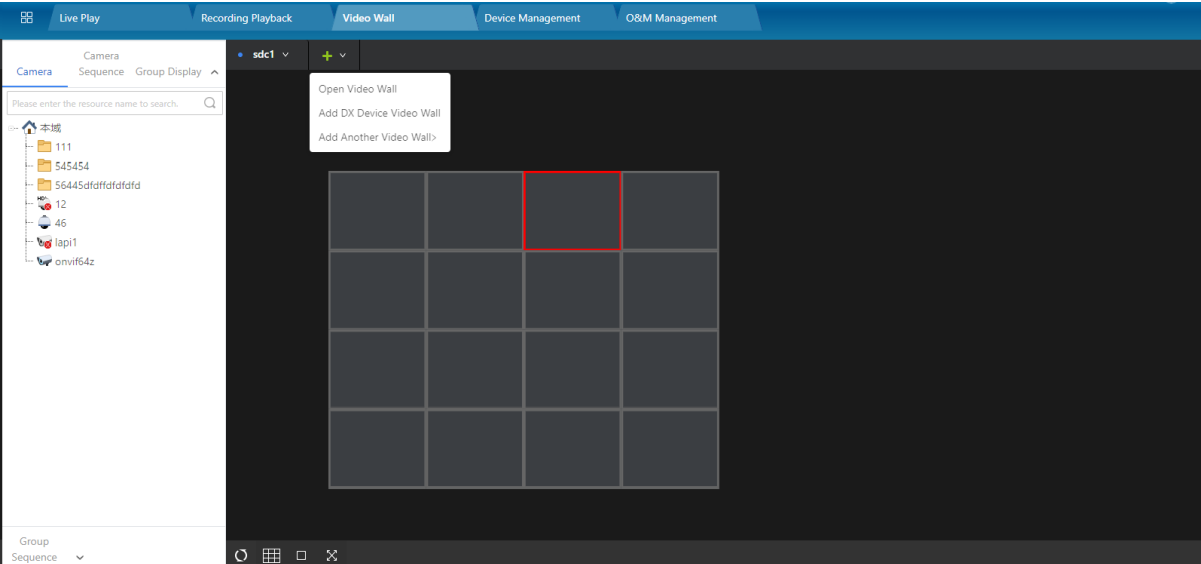
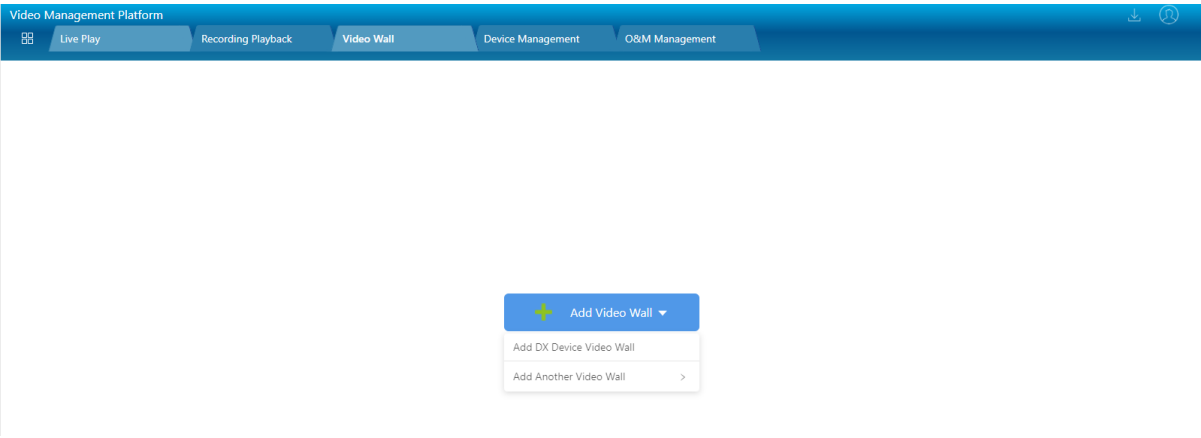
Add video walls created using DC/SDC devices.

Prerequisite:

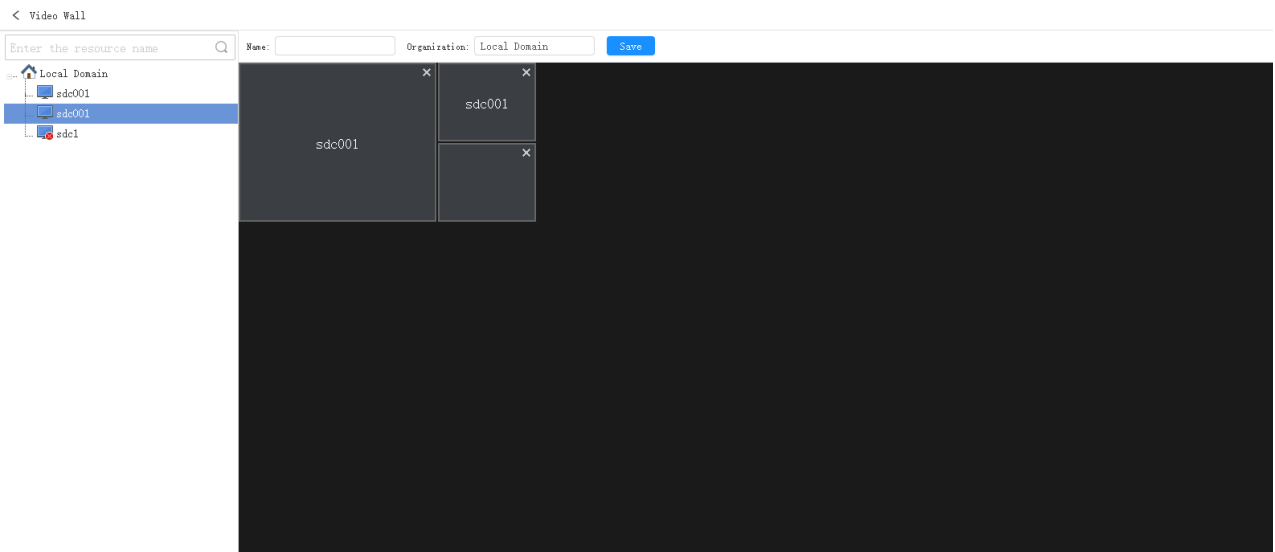
You have added a DC device. See Add Decoder.

6.1.1 Add Video Wall

1. If there's no video wall in the system, click  to add a video wall; otherwise, click  to add a video wall.



2. Choose **Add Other Video Wall > DC Video Wall**. A page as shown below appears.



3. Enter the video wall name, drag monitor icons to the configuration area, and adjust the layout to simulate the actual video wall.
4. After the layout is set, drag monitors from the left-side monitor list to the corresponding monitor icons in the configuration area.



5. Click **Save**.

6.1.2 Configure Camera Sequence Plan

After you have configured camera sequence resources (see Configure Camera Sequence Resource), you can configure a camera sequence plan.

1. Add a Camera Sequence Plan

1. Go to **Device Management > Service Configuration > Display Control > Camera Sequence Schedule**.
2. Select cameras from the left-side list and then click **Add**. A page as shown below appears.

Order...	Start Time	End Time	Camera Sequence R...	Operation
1	00:00:00	23:59:59	lunqietest	Save Cancel

3. Configure the parameters by referring to the table below.

Table 6-1 Camera Sequence Schedule Parameter Descriptions

Parameter	Description
Plan Name	Name of the camera sequence plan.
Output DC	Monitors to be used to play camera sequence resources according to the plan. Caution: The decoding format of the monitors must be consistent with the encoding format of the cameras in the camera sequence resource.
Window	Monitor to be used to play the camera sequence resource according to the plan. Note: The number of windows available may vary with decoder model.
Time Period	You can set by day or by week and then assign the periods to different sequence resources.
Enable Exception	If necessary, enable exception to set special time periods and perform certain sequence resources during these periods. On special days, the system plays camera sequence resources during the set periods only; on other days, the system plays camera sequence resources according to the plan. Note: Click Add Exception to add an exception. Up to 16 exceptions are allowed. Click  to delete an exception. After completing settings for a day, you can click  to copy and apply the same settings to other days.

4. Click **OK**.

2. Edit Camera Sequence Plan

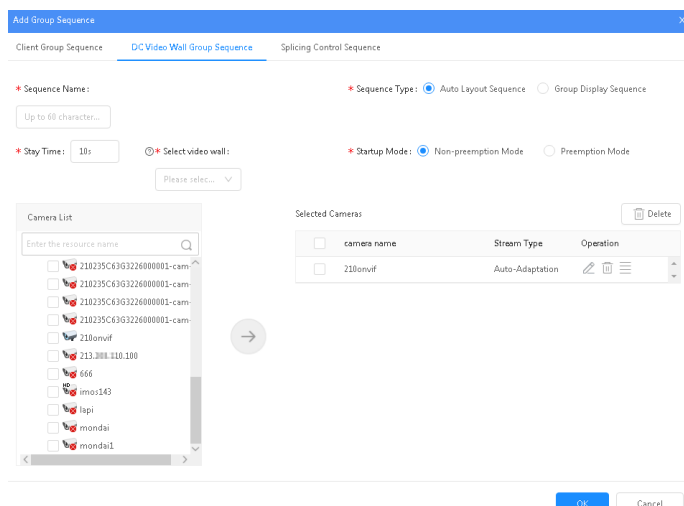
Click the corresponding  to edit the camera sequence plan.

3. Delete Camera Sequence Plan

Click the corresponding  to delete the camera sequence plan.

6.1.3 Configure Group Sequence on DC Video Wall

- Go to **Device Management > Service Configuration > Display Control > Camera Sequence Schedule > Group Sequence Resource**.
- Choose **DC video wall group sequence**.



- Set the parameters including the sequence name and add the sequence group.

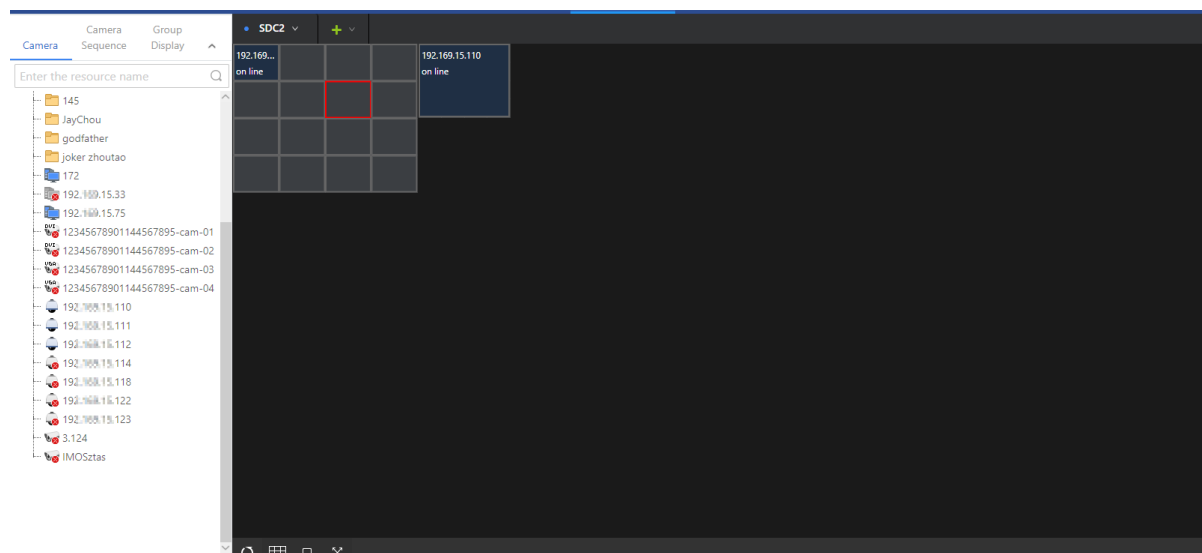
Table 6-2 Sequence Configuration Description

Type	Description
Sequence Name	The sequence name must not exceed 60 bytes.
Startup Mode	- Preemption mode: The group sequence will replace the ongoing live video at startup. - Non-preemption mode: The group sequence will not replace the ongoing live video at startup.
Stay Time	The duration of the live video of each camera in the sequence group.
Select Video Wall	Choose the video wall on which the group sequence will be played.
Select Camera	Select cameras from the left-side list and then click  to add them to the sequence group.

- Click **OK**.

6.1.4 Play Video Resources on Video Wall

- Go to the **DC Video Wall** page.



- Play video resource on the video wall. See the table below for details.

Table 6-3 Parameter Descriptions for Playing Video Resources on the Video Wall

Resource	Operation
Camera	- Play live video: Drag a camera to a window on the video wall; or click a window, right-click the camera, choose Live View on Video Wall, and then choose a stream type to start live video of the camera in the window. - Playback: To play recordings of a camera in a window on the video wall, click the window, right-click the camera and then choose Playback. In the pop-up window, set a time range of the recording and the target domain to search, and then click OK. - Live preview: Right-click a camera and choose Live Preview to view the live video of the camera.
Camera sequence	Drag a camera sequence resource to a window to start camera sequence.
Group Display	Drag a group display resource to a window to start the group display in the window.
Group sequence	Drag a group sequence resource to a window to start the group sequence in the window.

6.1.5 Window Operations

You may also use the toolbar at the bottom:

- : Refresh the page.
- : Choose a window layout.
- : Stop decoding video in a selected window.

6.2 A8 DX Video Wall

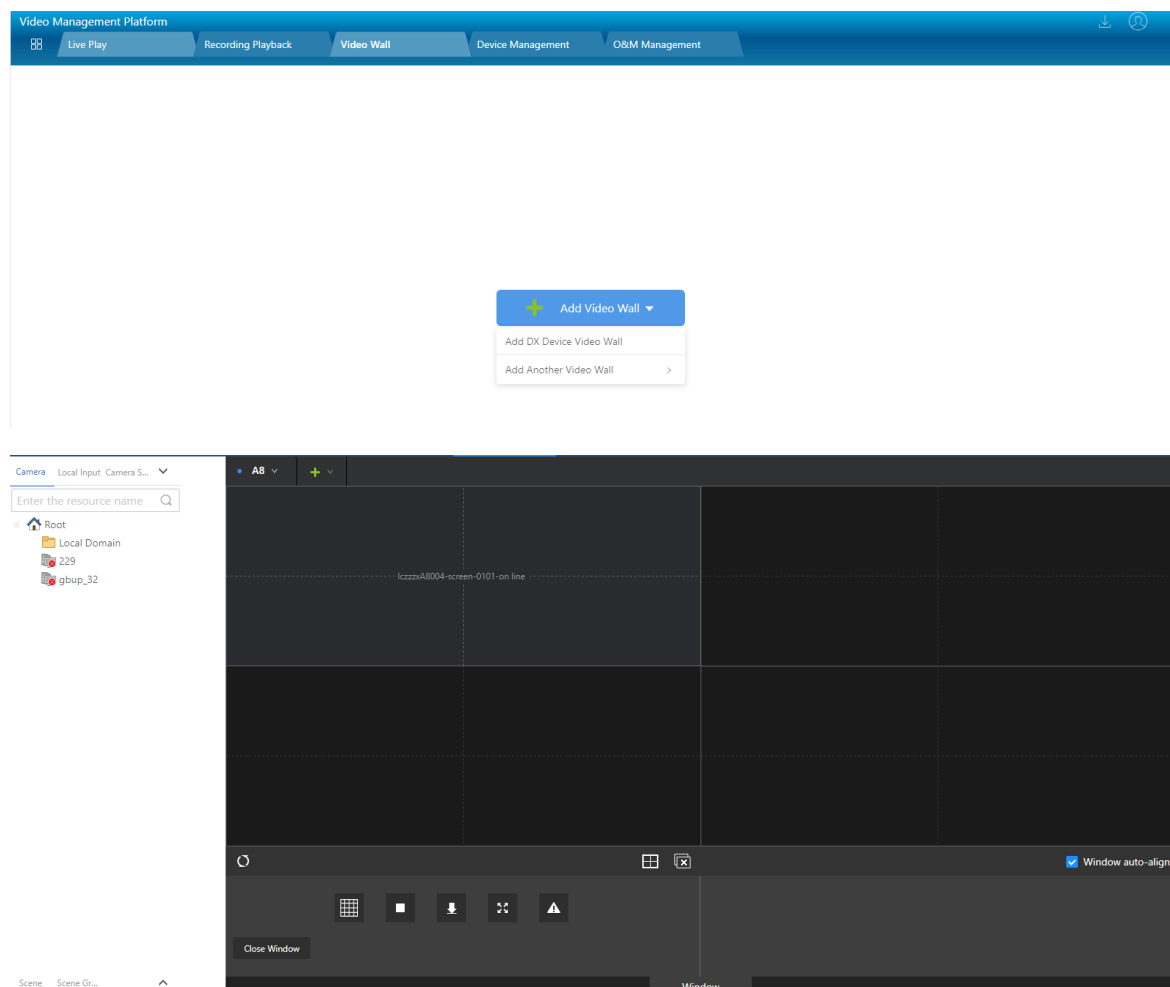
Add a A8 video wall to play live video, camera sequence, recorded video, and splice screens on the video wall.

Prerequisite:

You have added a video wall controller. See Video Integrated Management Platform.

6.2.1 Add Video Wall

1. If there's no video wall in the system, click  to add a video wall; otherwise, click  on the top.



2. Choose **Add Other Video Wall > A8 DX Video Wall**. A page as shown below appears.

The screenshot shows the 'Add Video Wall' configuration interface. It includes fields for Name, Input Format (1080@60), Video Wall specification (2x2), grid density (2*2), Organization (Local Domain), and Mode (Integrated Video Management Platform). The Input Channel section displays a list of available channels under 'Local Domain' and 'ADU85-32', including multiple 'IczzzxA8004-screen-0101' through '0108' entries. A visual representation of the video wall grid is shown, with one channel assigned to the top-left screen. The interface concludes with 'Confirm' and 'Cancel' buttons.

3. Configure the parameters by referring to the table below. After you complete the settings, the video wall is displayed.

Table 6-4 Parameter Descriptions

Parameter	Description
Name	Name of the video wall.
Video Wall Size	Set the columns and rows of the video wall (columns first, and then rows). ● Column: Number of columns of screens on the video wall. ● Row: Number of rows of screens on the video wall. Caution: Once set, the rows and columns cannot be changed.
Organization	Choose an organization for the video wall.
Grid Density	Set the number of grids for each screen, which will be used for alignment when configuring live view windows.
Output Format	Live video output resolution, that is, the maximum resolution supported by the video wall.

4. Drag the unused output channels from the left-side list to the right-side windows one by one.
5. Click **Confirm**. The video wall is added. You can view the added video wall on the video wall panel.



NOTE!

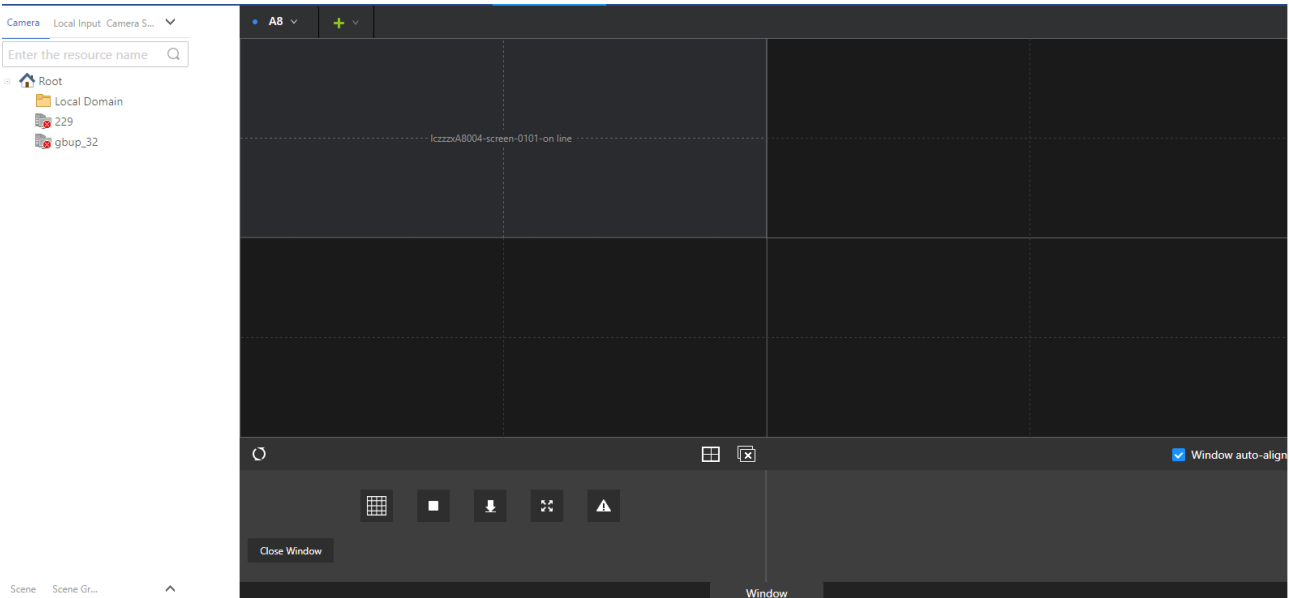
- You can click the arrow right to the video wall name to edit or delete the video wall.
- You cannot edit or delete the video wall when a window still exists in the scene.
- When editing a video wall, you cannot change the DC or DX device with which the video wall is created.

6.2.2 Configure Camera Sequence Plan

See Configure Camera Sequence Plan.

6.2.3 Play Video Resources on Video Wall

1. Go to the **A8 DX Wall** page.



2. Configure video resources to be played on the video wall. See the table below for details.

Table 6-5 Parameter Descriptions for Playing Video Resources on the Video Wall

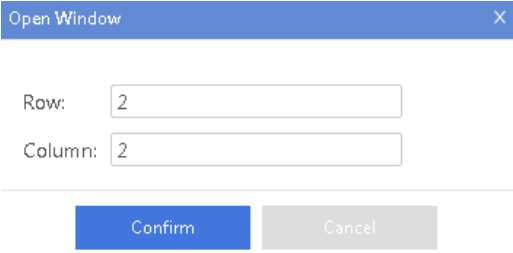
Resource	Operation
Camera	● Play live video: To play live video of a camera in a window on the video wall, drag the camera to the window on the video wall; or click the window, right-click the camera, choose Live View on Video Wall, and then choose a stream type. ● Playback: To play recordings of a camera in a window on the video wall, click the window, right-click the camera and then choose Playback. In the pop-up window, set a time range of the recording and the target domain to search, and then click OK. ● Live preview: Right-click a camera and choose Live Preview to view the live video of the camera.
Local Input	Input sub system of the video integrated management platform. Click a window, right-click the local input channel, choose Start to start the local input resource on the video wall.
Camera Sequence	Drag a camera sequence resource to a window to start camera sequence.
Scene	● Save scene: Right-click a scene, choose Save Scene to save the current video wall services as a scene. ● Start scene: Right-click a scene, choose Start Scene to start it on the video wall.

6.2.4 Window Operations

Use the toolbar at the bottom to open windows, close windows, set window layout, etc.

Table 6-6 Window Operations

Parameter	Description
	Refresh the page.

Parameter	Description
	Open Windows - Click the icon, confirm the message.  - Enter the number of rows and columns. - Click Confirm.
	Close Window
	Close all the windows.
 Window auto-align	When selected, the new window automatically aligns with a grid line.
	Choose a window layout.
	Stop decoding video in a selected window.
	Set the selected window to display it at the bottom when multiple windows overlap.
	If the window is not split, clicking the button magnifies the window to the full size of the video wall. If the window is split into multiple windows, clicking the button magnifies the split window to the full size of the whole window.
	Enable/disable alarm linkage for a selected window. Click to enable/disable alarm linkage for the selected window. When alarm linkage is enabled, the  icon appears in the window's lower-right corner, and the window starts to play live video when an alarm occurs. Note: You need to configure alarm-triggered live video on the DX video wall first.
	Close the selected window.

6.3 DX Video Wall

Add a DX video wall. A DX video wall can only bind to decoding channels of one decoding device.

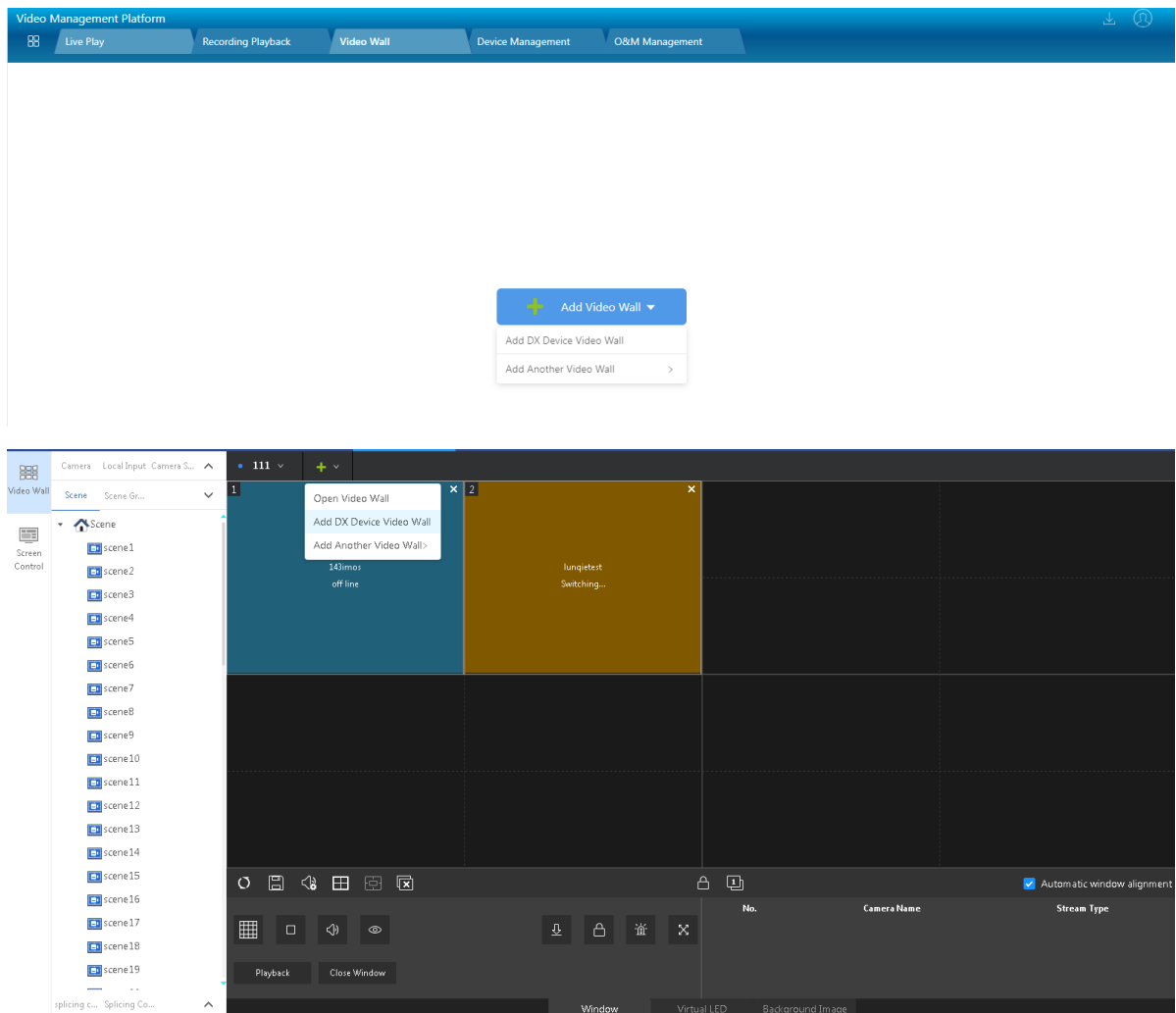
Prerequisite:

You have added a DX device. See DX Device.

6.3.1 Video Wall

1. Add Video Wall

- If there's no video wall in the system, click  to add a video wall; otherwise, click  on the top.



2. Choose **Add Other Video Wall > DX Video Wall**. A page as shown below appears.

Add Video Wall

Name : Specifications: X Organization:

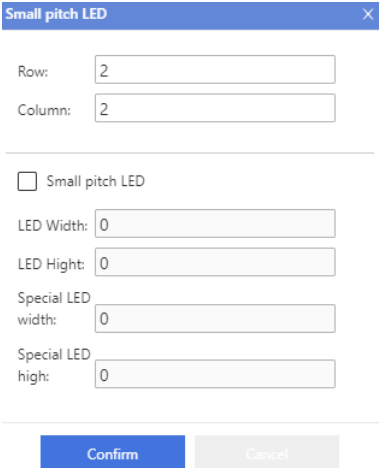
Output Mode : Grid : Mode:

Output Channel

- Local Domain
 - video wall
 - 210235C446320B0000...
 - 210235C446320B0000...
 - 210235C446320B0000...
 - 210235C446320B0000...
 - 210235C446320B0000...
 - 210235C446320B0000...
 - 210235C446320B0000...
 - 210235C446320B0000...
 - 210235C446320B0000...
 - 210235C446320B0000...

3. Configure the parameters by referring to the table below.

Table 6-7 Parameter Descriptions

Parameter	Description
Name	Name of the video integrated management platform.
Video Wall specification	Set the columns and rows of the video wall (columns first, and then rows). ● Column: Number of columns of screens on the video wall. ● Row: Number of rows of screens on the video wall. Caution: Once set, the rows and columns cannot be changed. (Optional) Small pixel pitch LED screens provide seamless splicing, ultra-high brightness and contrast, and ultra-wide viewing angle. If small pixel pitch LEDs are used, you must set small pixel pitch LED (unit: pixel). 4. Click Small Pixel Pitch LED. A page as shown below appears.  5. Select the Small pitch LED checkbox, and then configure the parameters. ● Special LED width: Width of the last column of the video wall. ● Special LED height: Height of the last row of the video wall. Click OK.
Organization	Choose an organization for the video wall.
Grid Density	Set the number of grids for each screen, which will be used for alignment when configuring live view windows.
Output Format	Live video output resolution, that is, the maximum resolution supported by the video wall.

4. Drag the unused output channels from the left-side list to the right-side windows one by one.

Bind all channels with one-click: Select the device on the left-side list, click  in the lower left corner of the video wall. The idle channels of the device are bound automatically to the video wall windows. To cancel all the bindings, click .



NOTE!

If any windows on the video wall are already bound, the current bindings will be cancelled first.

5. Click **Confirm**. The video wall is added. You can view the added video wall on the video wall panel.



NOTE!

- You can click the arrow right to the video wall name to edit or delete the video wall.
- You cannot edit or delete the video wall when a window still exists in the scene.
- When editing a video wall, you cannot change the DC or DX device with which the video wall is created.

2. Configure Camera Sequence Plan

See Configure Camera Sequence Plan.

3. Configure DX Video Wall Group Sequence Resource

1. Choose Splicing Control Sequence.

The screenshot shows the 'Add Group Sequence' dialog box with the 'Splicing Control Sequence' tab selected. The dialog includes fields for 'Sequence Name' (with a character limit of 60), 'Startup Mode' (radio buttons for 'Non-preemption Mode' and 'Preemption Mode'), 'Stay Time' (set to 10s), and 'Select video wall' (a dropdown menu showing '111/scene1'). Below these fields are two lists: 'Camera List' on the left and 'Selected Cameras' on the right. The 'Camera List' contains various camera names with checkboxes. The 'Selected Cameras' list shows the selected cameras with their 'Stream Type' and 'Operation' (edit, delete, and menu icons). A blue arrow button is positioned between the two lists. At the bottom right are 'OK' and 'Cancel' buttons.

2. Set the parameters including the sequence name and add the sequence group.

- Select cameras from the left-side list and then click  to add them to the sequence group.
- Stay Time: The duration of the live video of each camera in the sequence group.
- Select the video wall on which the group sequence will be played.
- Startup Mode:
 - Non-preemption mode: The group sequence will not replace the ongoing live video at startup.
 - Preemption mode: The group sequence will replace the ongoing live video at startup.

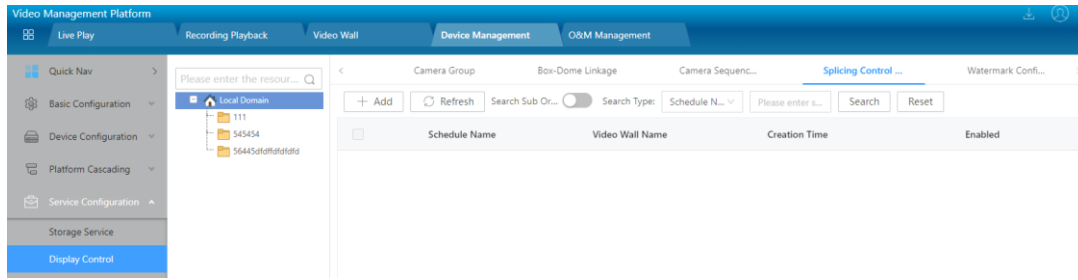
3. Click **OK**.

4. Configure DX Video Wall Group Sequence Plan

Configure sequence plans for group sequence resources.

(1) Add Group Sequence Plan on DX Video Wall

1. Go to **Device Management > Service Configuration > Display Control > Splicing Control Schedule**.



2. On the left-side organization tree, click the target organization, click **Add**. A page as shown below appears.

3. Configure the parameters by referring to the table below.

Table 6-8 Parameter Descriptions for Configuring DX Video Wall Group Sequence Plan

Parameter	Description
Plan Name	Name of the group sequence plan.
Video Wall	DX video wall to be used to play the group sequence resource according to the plan. Caution: The decoding format of the video wall must be consistent with the encoding format of the cameras in the DX group sequence resource.
Time Period	You can set by day or by week and then assign the periods to different sequence resources.
Enable Exception	If necessary, enable exception to set special time periods and perform certain sequence resources during these periods. On special days, the system plays DX group sequence resource during the set periods only; on other days, the system plays DX group sequence resources according to the plan. Note: Click Add Exception to add an exception. Up to 16 exceptions are allowed. To delete an exception, click . After you complete settings for a day, you can click to apply the settings to other days.

4. Click **OK**.

(2) Edit Group Sequence Plan on DX Video Wall

1. Go to **Device Management > Service Configuration > Display Control > Splicing Control Schedule**.
2. On the left-side organization tree, double-click the target organization, click .
3. Edit the settings, click **OK**. The changed plan becomes effective immediately.

(3) Delete Group Sequence Plan on DX Video Wall

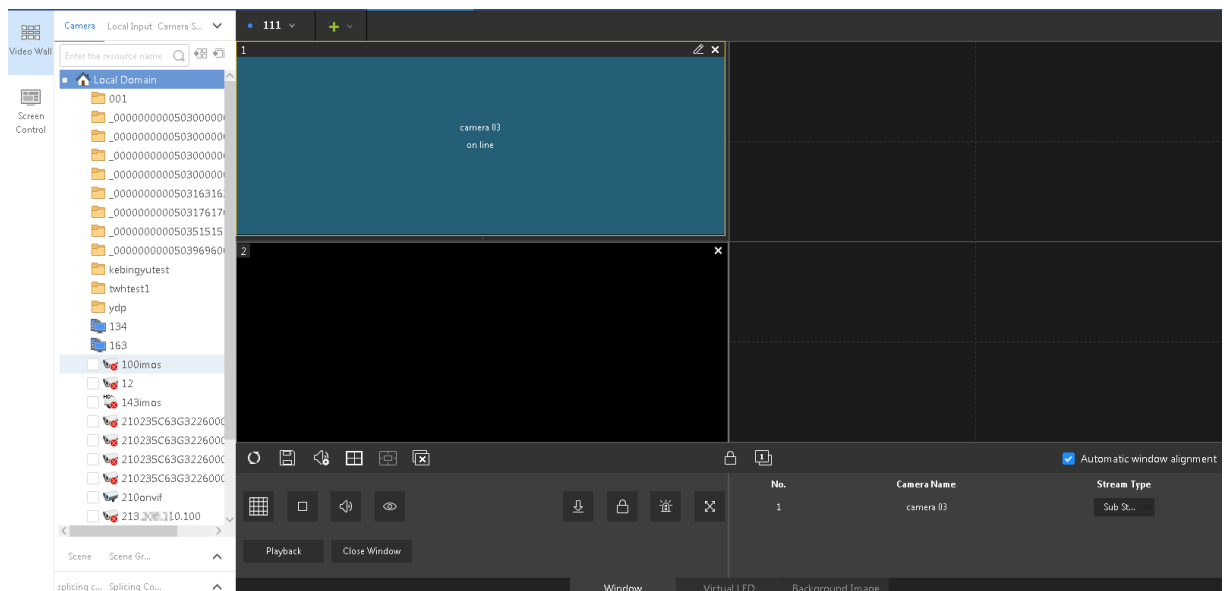
- Delete one: Point to a schedule, click .
- To delete multiple schedules at a time, select the schedules and then click **Delete**.

(4) Enable/Disable Group Sequence Plan on DX Video Wall

- Click  to enable a schedule.
- Click  to disable a schedule.

5. Play Video Resources on Video Wall

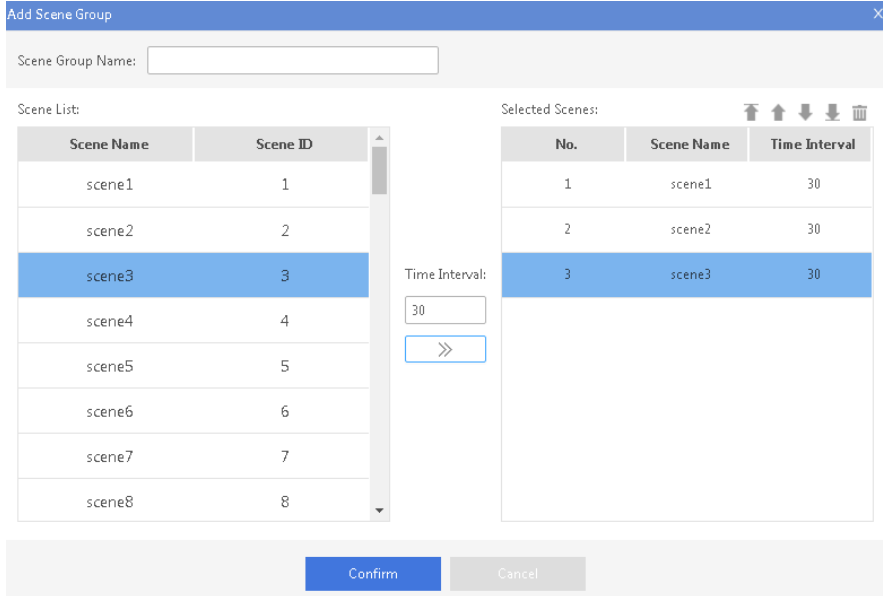
1. Go to **DX Video Wall > Video Wall**.



2. Configure video resources to be played on the video wall. See the table below for details.

Table 6-9 Playing Different Video Resources on Video Wall

Resource	Operation
Camera	● Live video: Drag a camera to a window to start its live video in the window; or click the window, right-click the camera and then choose Live View on Video Wall > Play Main Stream on Video Wall or Play Sub Stream on Video Wall or Auto. ● Playback: To play recordings of a camera in a window on the video wall, click the window, right-click the camera and then choose Playback. In the pop-up window, set a time range of the recording and the target domain to search, and then click OK. ● Live preview: Right-click a camera and choose Live Preview to view the live video of the camera.
Local Input	Input sub system of the DX device. Click a window, right-click the local input channel, choose Start to start the local input resource on the video wall.

Resource	Operation
Camera Sequence	Drag a camera sequence resource to a window to start camera sequence.
Scene	- Save scene: Right-click a scene, choose Save Scene to save the current video wall services as a scene. - Start scene: Right-click a scene, choose Start Scene to start it on the video wall.
Scene Sequence	Add scene group: Click  on the Scene Sequence tab. A page as shown below appears. Select a scene from the left-side scene list, configure a time interval, and then click  to add the scene to the scene group. Click Confirm. The scene group appears in the scene sequence resource list.  Note: You can use the right-click menu to edit or delete a scene group. Start scene sequence: Right-click a scene group, choose Start to start it on the video wall. A pop-up window appears to indicate the current scene. To stop the scene sequence on the video wall, click Stop.
Group Sequence on DX Video Wall	Right-click a group sequence resource, choose Start to start it on the video wall. After video is started on the video wall, you can use the right-click menu to switch to the previous or next display or to stop or pause the sequence.
Group Sequence Plan on DX Video Wall	Right-click a group sequence plan, choose Start to start it on the video wall. After group sequence is started, you can stop it using the right-click menu.

6. Window Operations

Use the toolbar at the bottom to open windows, close windows, set window layout, etc.

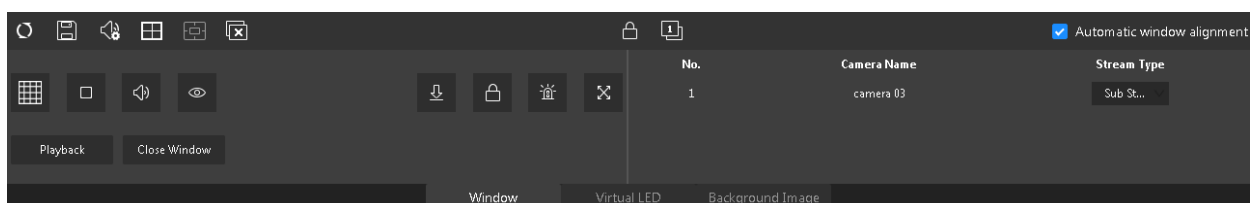


Table 6-10 Window Operations

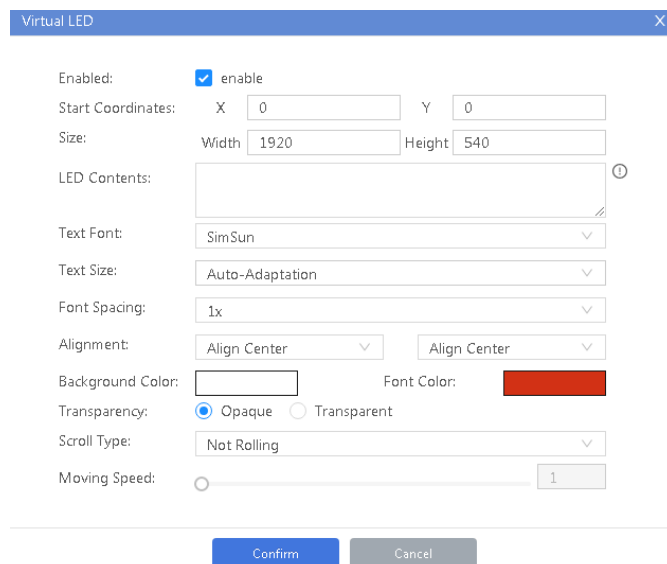
Parameter	Description
	Refresh the page.

Parameter	Description
	Save the current video wall layout and video services (live view, sequence) as a scene.
	Audio control. Choose output audio to play in the channel.
	Open windows with one-click. Set the rows and columns of windows, offset position of the start point to create windows. 
	Set coordinates, width, and height to open windows. Note: This function is available when auto-alignment is disabled.
	Close Window
	Close all the windows.
	Lock/unlock all windows. The position and shape of the locked windows cannot be changed.
	Number all the windows according to their positions (from top to bottom, left to right). The re-numbered window IDs are displayed in the window's upper-left corner.
 Window auto-align	When selected, the new window automatically aligns with a grid line.
	Choose a window layout.
	Stop decoding video in a selected window.
	Adjust sound volume in a selected window.
	Start/stop live video in a selected window.
	Set the selected window to display it at the bottom when multiple windows overlap.
	Lock/unlock a window. The position and shape of a locked window cannot be changed.
	Enable/disable alarm linkage for a selected window. Click to enable/disable alarm linkage for the selected window. When alarm linkage is enabled, the  icon appears in the window's lower-right corner, and the window starts to play live video when an alarm occurs. Note: You need to configure alarm-triggered live video on the DX video wall first.
	If the window is not split, clicking the button magnifies the window to the full size of the video wall. If the window is split into multiple windows, clicking the button magnifies the split window to the full size of the whole window.
Playback	Switch live video to playback for a selected window, set a search time range to play the found recordings in a pop-up window.
Close Window	Close the selected window.

7. Virtual LED

You can configure virtual LEDs on the video wall and customize text displayed on the screen.

1. Switch to the **Virtual LED** page by clicking **Virtual LED** on the toolbar displayed at the bottom of the page.
2. Drag on the video wall using the right button to draw a virtual LED; or click  behind Virtual LED on the toolbar.
3. In the Virtual LED window, set the position, size, contents, style and scroll mode, and then click **Confirm**.



NOTE!

- A video wall allows one scrolling virtual LED and 16 static virtual LEDs.
- If multiple virtual LEDs are configured, their positions must not overlap.

4. The virtual LED appears on the video wall.

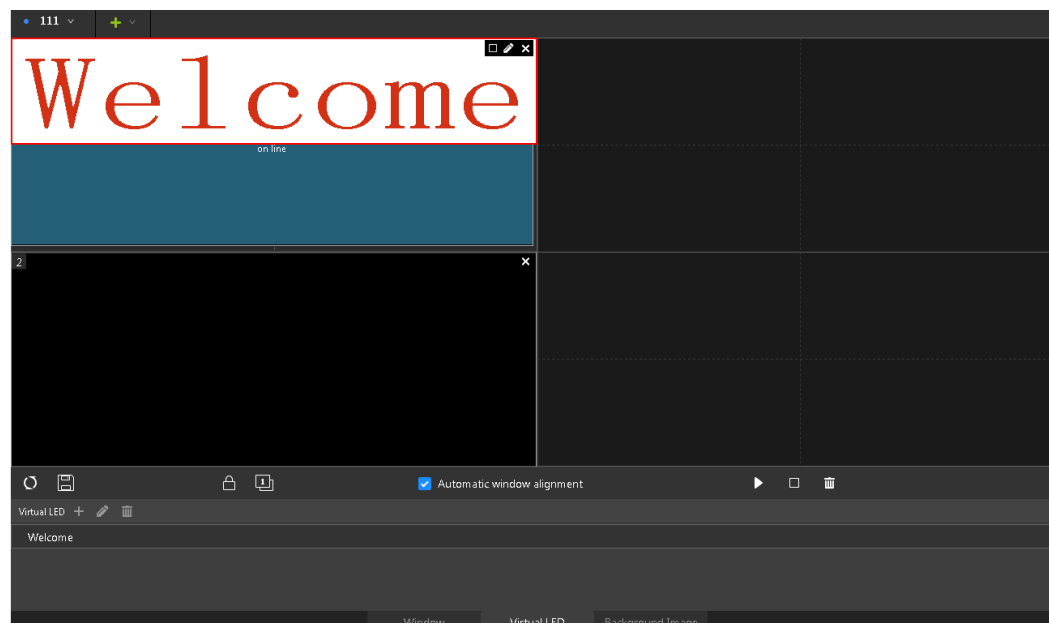


Table 6-11 Virtual LED Operations

Function	Description
Adjust the position/size of a virtual LED	Drag the virtual LED to move it, or drag its border to resize it.
Enable/disable a virtual LED	- Click /  in its upper right corner to enable/disable it. /  appears when you point to the text below Virtual LED in the toolbar, and click the button to enable/disable the virtual LED. - Click /  in the toolbar to enable/disable all virtual LEDs.
Edit Virtual LED	Click  in the upper right corner; or select the virtual LED, and then click  behind the virtual LED in the toolbar.
Delete a virtual LED	- Click  in the upper right corner; or select the virtual LED, and then click  behind the virtual LED in the toolbar. - Click  in the toolbar to delete all virtual LEDs.

8. Configure Background Image

Configure a background image of the video wall. When video is playing, the video plays on the background image. When no video is playing, the background image is displayed.

1. Switch to the Background Image by clicking on the toolbar displayed at the bottom of the page.
2. Click  behind **Background Image** on the toolbar.
3. Click **Browse** in the pop-up window to select the background image.

Add Background Image

Background Image Name :

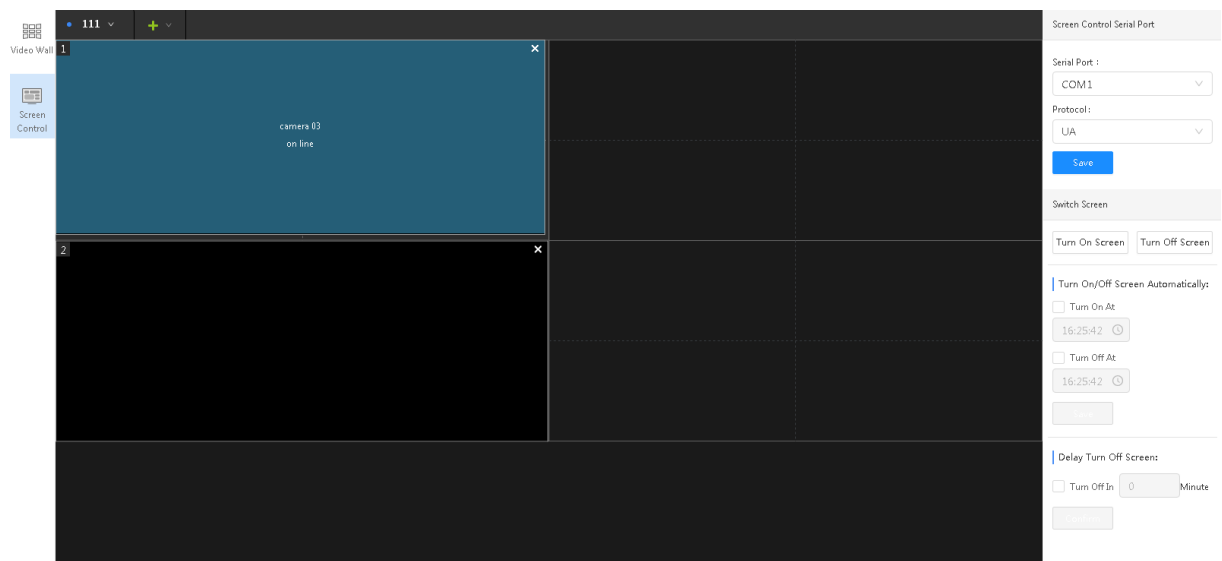
4. Click **Confirm**.

Background Image Operations

- Enable/disable background image: Click /  behind the background image.
- Delete background image: Select the background image and then click  on the toolbar.

6.3.2 Screen Control

Screen control is used to manage serial ports on the screens and turn on/off video wall screens.



1. Go to **DX Video Wall > Screen Control**.
2. Configure the parameters by referring to the table below.

Table 6-12 Parameter Descriptions for Screen Control

Category	Parameter	Description
Serial Port	Serial Port	Port type. Choose COM1 or COM2 .
	Protocol	Serial port protocol. Choose LIA , LIA-A or MODBU .
Turn On/Off Screen	Turn On Screen	Turn on all the screens on the video wall.
	Turn Off Screen	Turn off all the screens on the video wall. Note: If Delay Turn Off Screens are enabled, the screens will turn off automatically after the set time is over.
	Turn On At	When enabled, the screens will turn on automatically at the set time. Note: If the set time is earlier than the current time, the system will perform the task the next day.
	Turn Off At	When enabled, the screens will turn off automatically at the set time. Note: If the set time is earlier than the current time, the system will perform the task the next day.
	Delay Turn Off Screens	Select the checkbox and set the time (unit: minute). Click Turn Off Screen . The screens will turn off at the end of the set time. Note: After Delay Turn Off Screen is configured, clicking Turn On Screen will automatically cancel the configured Delay Turn Off Screen .

6.4 Multi-Decoder Video Wall

Add a DX video wall using output channels of multiple decoding devices.

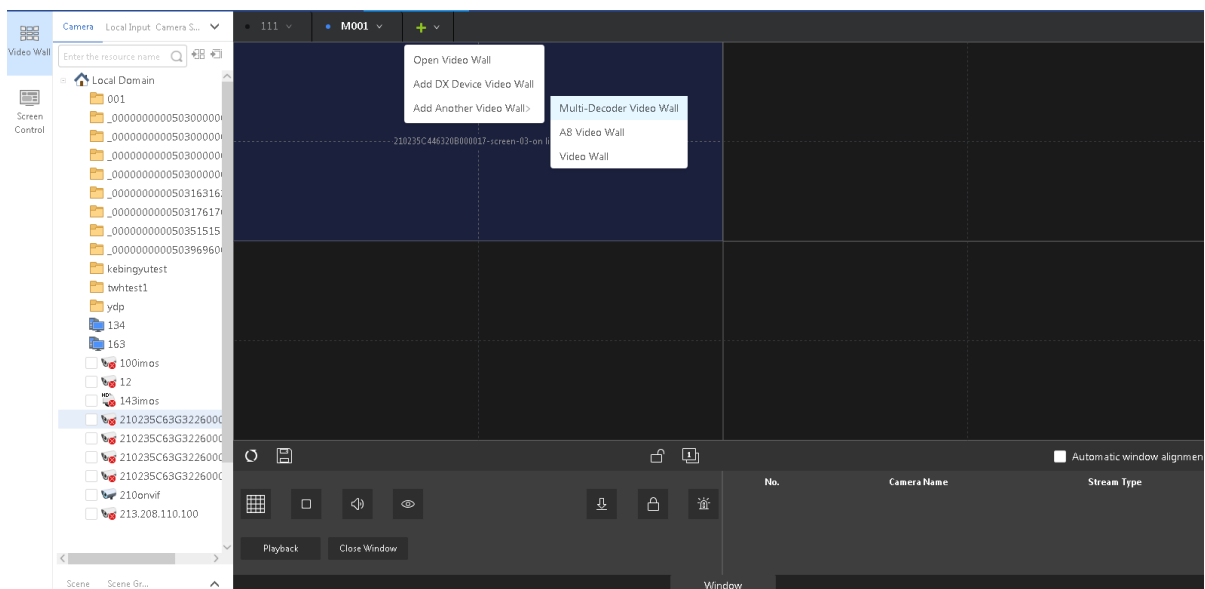
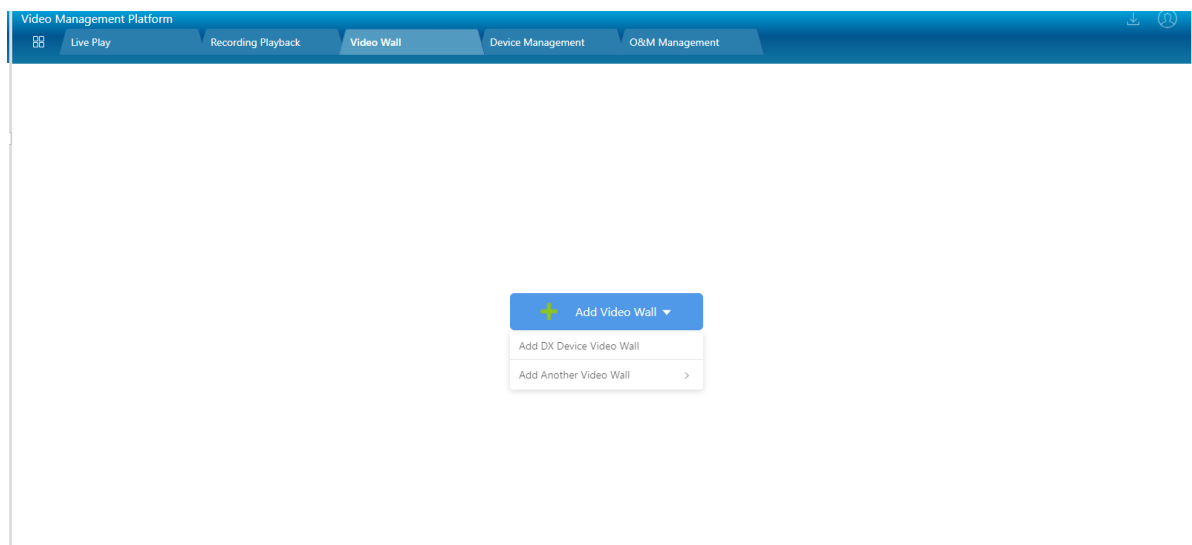
Prerequisite:

You have added a DX device. See DX Device.

6.4.1 Video Wall

1. Add Video Wall

1. If there's no video wall in the system, click  to add a video wall; otherwise, click  on the top.



2. Choose **Add Other Video Wall > Multi-Decoder Video Wall**. A page as shown below appears.

3. Configure the parameters by referring to the table below.

Table 6-13 Parameter Descriptions

Parameter	Description
Name	Name of the video wall.
Video Wall Size	Set the columns and rows of the video wall (columns first, and then rows). ● Column: Number of columns of screens on the video wall. ● Row: Number of rows of screens on the video wall. Note: Once set, the rows and columns cannot be changed.
Organization	Choose an organization for the video wall.
Grid Density	Set the number of grids for each screen, which will be used for alignment when configuring live view windows.
Output Format	Live video output resolution, that is, the maximum resolution supported by the video wall.

4. Drag the unused output channels from the left-side list to the right-side windows one by one.

Bind all channels with one-click: Select a device on the left-side list, click  in the lower left corner of the video wall. The idle channels of the device are bound automatically to video wall windows. To cancel all the bindings, click .



NOTE!

If any windows on the video wall are already bound, the current bindings will be cancelled first.

5. Click **Confirm**. The video wall is added. You can view the added video wall on the video wall panel.



NOTE!

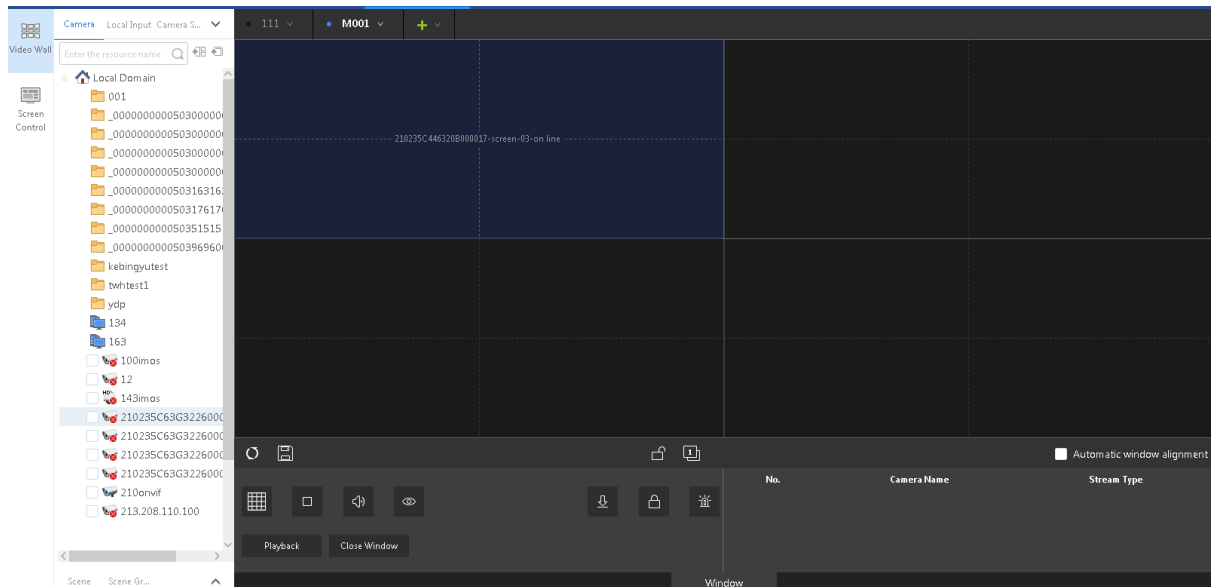
- You can click the arrow right to the video wall name to edit or delete the video wall.
- You cannot edit or delete the video wall when a window still exists in the scene.
- When editing a video wall, you cannot change the DC or DX device with which the video wall is created.

2. Configure Camera Sequence Resource

See Configure Camera Sequence Plan.

3. Play Video Resources on Video Wall

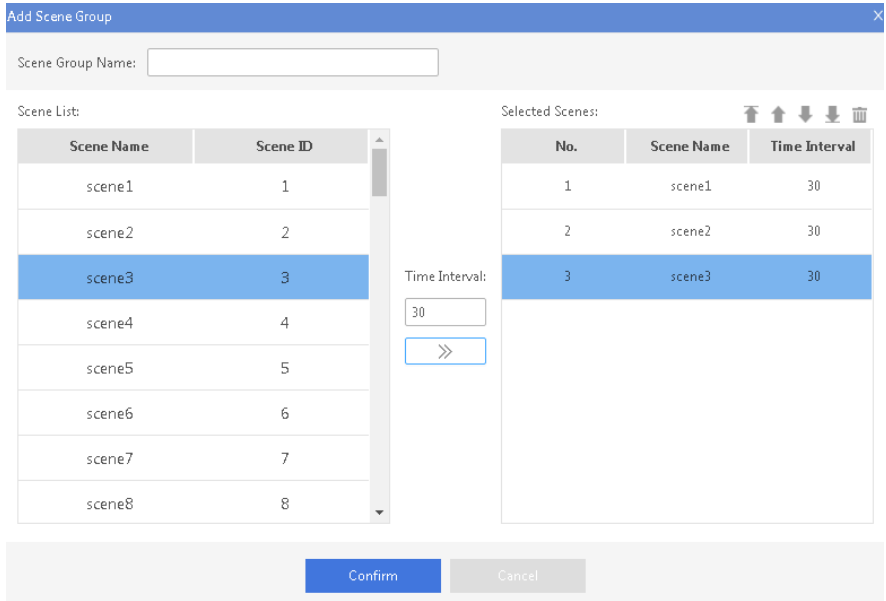
1. Go to **Multi-Decoder Video Wall > Video Wall**.



2. Configure video resources to be played on the video wall. See the table below for details.

Table 6-14 Playing Different Video Resources on Video Wall

Resource	Operation
Camera	• Live video: Drag a camera to a window to start its live video in the window; or click the window, right-click the camera and then choose Live View on Video Wall > Play Main Stream on Video Wall or Play Sub Stream on Video Wall or Auto. • Playback: To play recordings of a camera in a window on the video wall, click the window, right-click the camera and then choose Playback. In the pop-up window, set a time range of the recording and the target domain to search, and then click OK. • Live preview: Right-click a camera and choose Live Preview to view the live video of the camera.
Local Input	Input subsystem of multi-decoder DX device. Click a window, right-click the local input channel, choose Start to start the local input resource on the video wall.
Camera Sequence	Drag a camera sequence resource to a window to start camera sequence.
Scene	• Save scene: Right-click a scene, choose Save Scene to save the current video wall services as a scene. • Start scene: Right-click a scene, choose Start Scene to start it on the video wall.

Resource	Operation
Scene Sequence	● Add scene group: Click  on the Scene Sequence tab. A window as shown below appears. Select a scene from the left-side scene list, configure a time interval, and then click  to add the scene to the scene group. Click Confirm. The scene group appears in the scene sequence resource list.  Note: You can use the right-click menu to edit or delete a scene group. ● Start scene sequence: Right-click a scene group, choose Start to start it on the video wall. A pop-up window appears to indicate the current scene. ● To stop the scene sequence on the video wall, click Stop.

4. Window Operations

Use the bottom toolbar to set the screen layout, manage audio, etc.

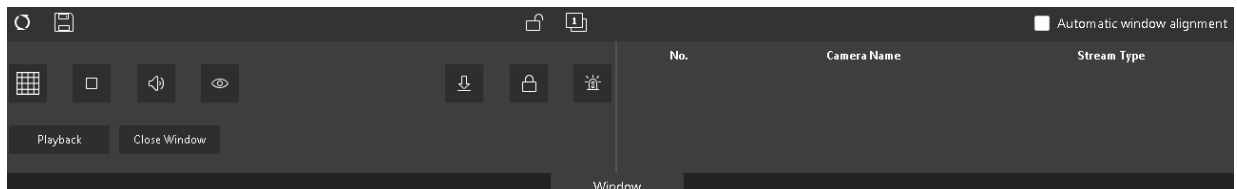


Table 6-15 Window Operation Description

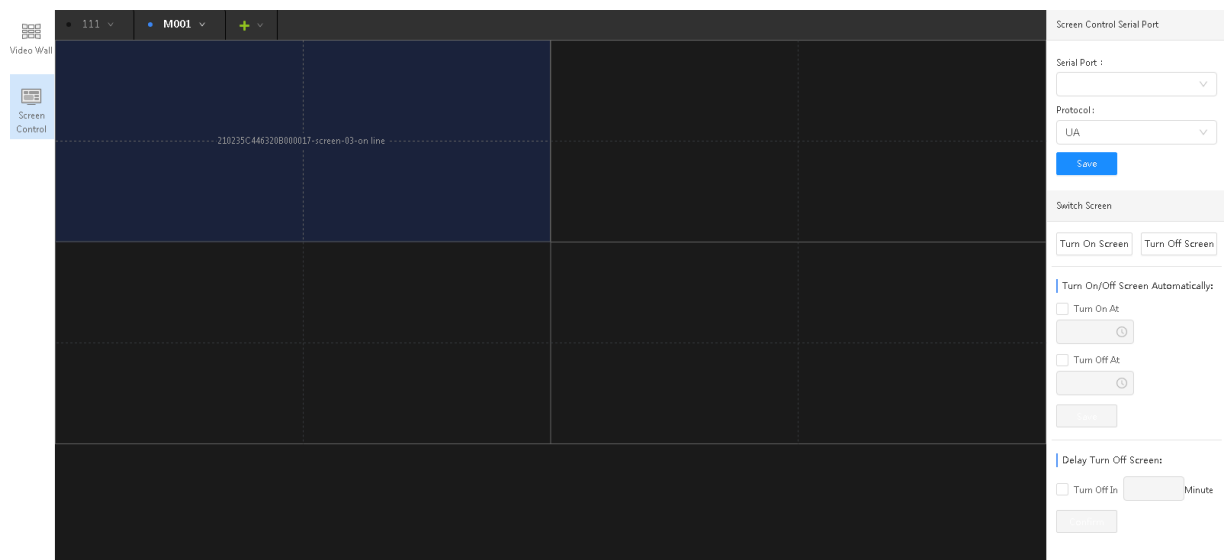
Parameter	Description
	Refresh the page.
	Save the current video wall layout and video services (live view, sequence) as a scene.
	Choose a window layout.
	Stop decoding video in a selected window.
	Adjust sound volume in a selected window.
	Start/stop live video in a selected window.
	Lock/unlock a window. The position and shape of a locked window cannot be changed.

Parameter	Description
	Enable/disable alarm linkage for a selected window. Click to enable/disable alarm linkage for the selected window. When alarm linkage is enabled, the  icon appears in the window's lower-right corner, and the window starts to play live video when an alarm occurs. Note: You need to configure alarm-triggered live video on the DX video wall first.
Playback	Switch live video to playback for a selected window, set a search time range to play the found recordings in a pop-up window.
Close Window	Close the selected window.

6.4.2 Screen Control

Screen control is used to manage serial ports on the screens and turn on/off video wall screens.

1. Go to **Multi-Decoder Video Wall > Screen Control**.



2. Configure the parameters by referring to the table below.

Table 6-16 Screen Control Parameter Description

Category	Parameter	Description
Serial Port	Serial Port	Port type. Choose COM1 or COM2 .
	Protocol	Serial port protocol. Choose LIA , LIA-A or MODBU .
Turn On/Off Screen	Turn On Screen	Turn on all the screens on the video wall.
	Turn Off Screen	Turn off all the screens on the video wall. Note: If Delay Turn Off Screens are enabled, the screens will turn off automatically after the set time is over.
	Turn On At	When enabled, the screens will turn on automatically at the set time. Note: If the set time is earlier than the current time, the system will perform the task the next day.
	Turn Off At	When enabled, the screens will turn off automatically at the set time. Note: If the set time is earlier than the current time, the system will perform the task the next day.
	Delay Turn Off Screens	Select the checkbox and set the time (unit: minute). Click Turn Off Screen . The screens will turn off at the end of the set time. Note: After Delay Turn Off Screen is configured, clicking Turn On Screen will automatically cancel the configured Delay Turn Off Screen .

7 Organization Management

Organization is the collection of resources. Through organization management, we can easily manage various devices and other resources. The structure of organizations should be planned appropriately to facilitate resource management.

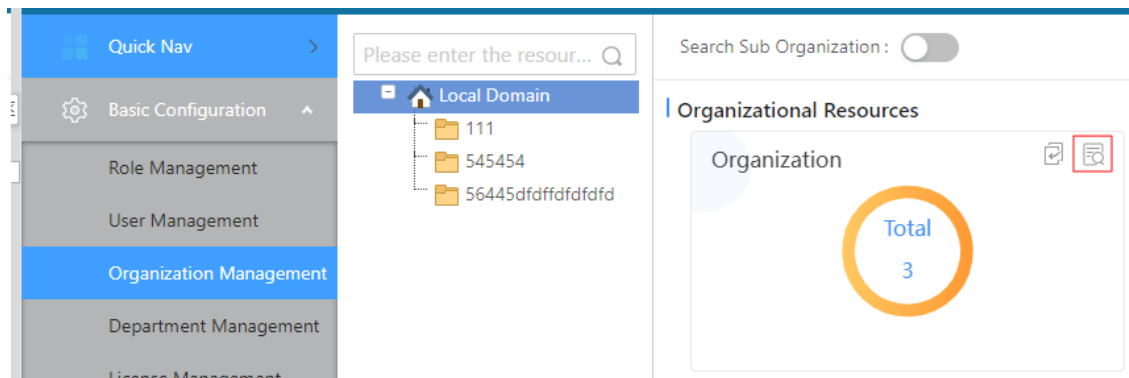


NOTE!

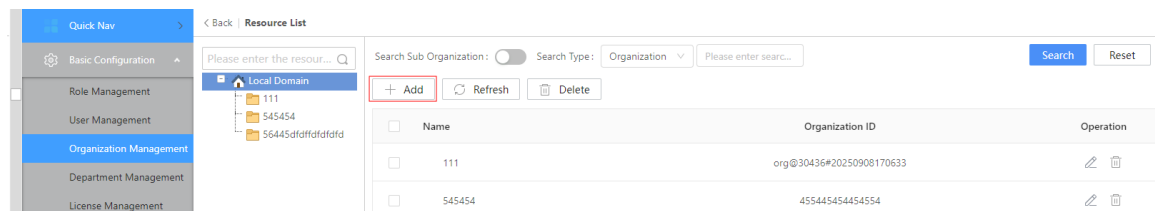
Organization configuration must be completed before you can allocate resources, manage roles and users.

7.1 Add Organization

1. Go to **Device Management > Basic Configuration > Organization Management**, Click



2. In the organization list, select the parent organization of the new organization (local domain or other organizations).



3. Click **Add** to go to the **Add Organization** page.

Figure 7-1 Add Organization - Automatically Generate GB Code

Figure 7-2 Add Organization - Generating GB Code by Administrative Area

AgregarOrganización

* Organización:

Ingrese nombre de la organización

* ID de organizac...

org@54826#20240220035752

▼ Código GB:

6511110002150000039

Método de generación:

☐ Generar automáticamente

☒ Generar por GB

Área ubica...

Descripción:

Ingrese la descripción de la organización

Confirmar

Cancelar

4. Enter the organization name, organization code, GB code (optional), and organization description (optional).



Note!

- The organization code and GB code cannot be duplicate in the local domain.
- GB Code: If you need to [share the organization](#) between GB domains, it is recommended to enter the GB code.
 - Generate Automatically: A list of GB codes will be automatically generated and filled into the input box if this option is selected. The generation rule is: Bits 1-10 indicate the parent organization ID or the first 10 bits of the inter-domain interconnection domain of the local domain (supplement with 0 if there are less than 10 bits), bits 11-13 must be 215 if the parent organization is the local domain and otherwise 216, and bits 14-20 indicate the serial number which starts from 1 and increases by 1 each time.
 - Generate by Administrative Area: You need to [Configure the Local Domain Administrative Division](#) on the platform configuration page. The administrative area code will be automatically filled in the GB code area when you select the area located for adding an organization.
 - Enter Manually: The code must consist of 2, 4, 6, 8, or 20 digits and be unique. In the case of a 20-digit code, bits 11-13 must be 215 or 216.

5. Click **OK** to complete the addition.

7.2 Organization Management

Go to **Device Management > Basic Configuration > Organization Management**, Click to view all organization.

Search Sub Organization : ☐ Search Type : Organization ▼ Please enter searc...

Search Reset

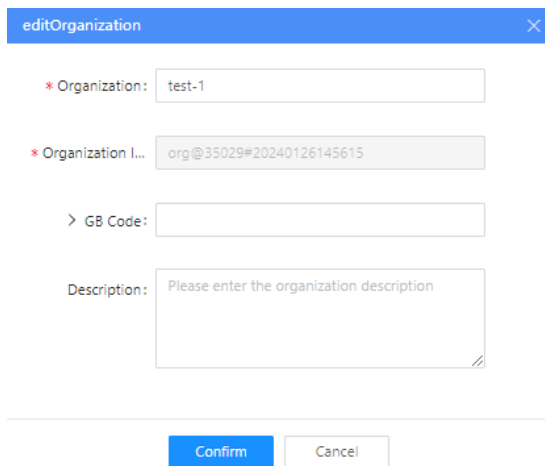
+ Add

Refresh

Delete

☐	Name	Organization ID	Operation
☐	test-1	org@35029#20240126145615	
☐	test-2	org@88655#20240126123032	

- Search organization: Select the query type as Organization Name or Code, enter the keyword information, and click **Search**. If you want to search sub-organization, enable **Search Sub-Organization**.
- Edit organization: Click  to edit the organization name, organization description, and GB code.

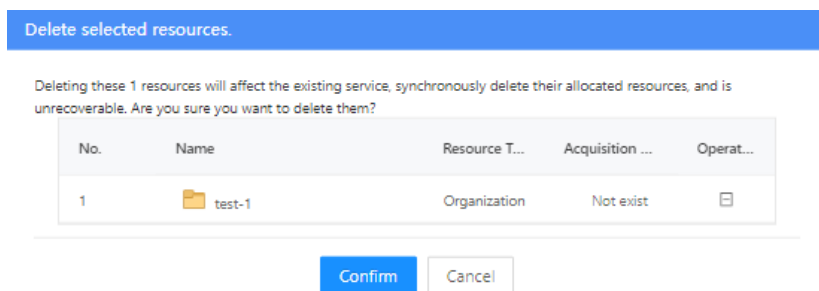


- Delete organization: Select an organization, click **Delete**, and confirm to delete the organization.



Note!

If devices or user resources exist in an organization, the organization cannot be deleted.

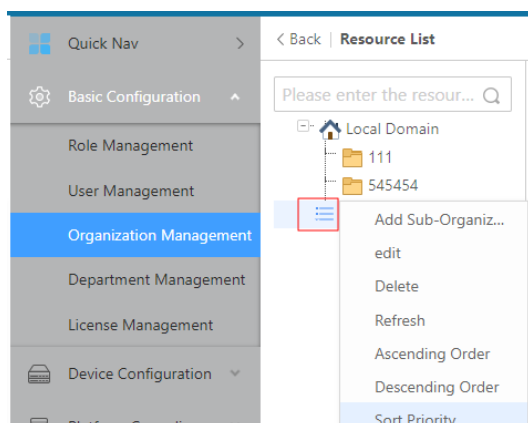


No.	Name	Resource T...	Acquisition ...	Operat...
1	 test-1	Organization	Not exist	

7.3 Organization Tree Operations

Go to Device Management > Basic Configuration > Organization Management. Click  on the left side of the organization to add sub-organizations, edit organizations, delete organizations, or sort sub-organizations.

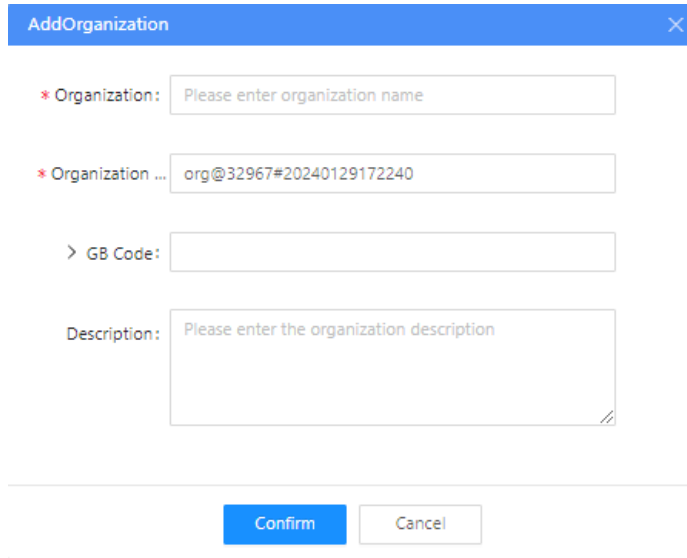
Figure 7-3 Organization Tree Operations



1. Add Sub-Organization

1. Select the parent organization and click  on the left side of the organization.
2. Click **Add Sub-Organization** to go to the **Add Organization** page.
3. Enter the organization name, organization code, GB code (optional), and organization description (optional), and click **OK** to complete the addition.

Figure 7-4 Add Sub-Organization

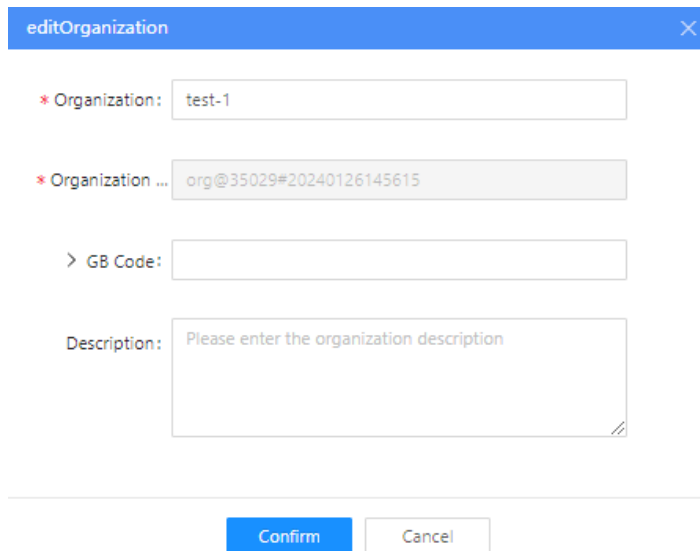


The dialog box titled "AddOrganization" has a blue header bar with a close button (X). It contains four input fields: "Organization:" with a placeholder "Please enter organization name", "Organization ..." with the value "org@32967#20240129172240", "> GB Code:" which is empty, and "Description:" with a placeholder "Please enter the organization description". At the bottom, there are two buttons: "Confirm" (blue) and "Cancel" (white).

2. Edit Organization

1. Click  on the left side of the organization to be modified.
2. Click **Edit** to go to the **Edit Organization** page.
3. Edit the organization name, GB code, or organization description, and click **OK**.

Figure 7-5 Edit Organization

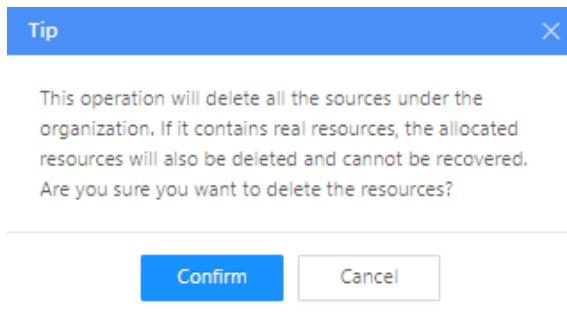


The dialog box titled "editOrganization" has a blue header bar with a close button (X). It contains four input fields: "Organization:" with the value "test-1", "Organization ..." with the value "org@35029#20240126145615", "> GB Code:" which is empty, and "Description:" with a placeholder "Please enter the organization description". At the bottom, there are two buttons: "Confirm" (blue) and "Cancel" (white).

3. Delete Organization

1. Click  on the left side of the organization to be deleted.
2. Click **Delete** and click **OK** to delete the organization.

Figure 7-6 Delete Organization

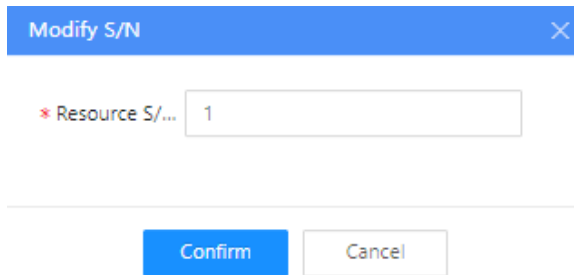


4. Sort Organization

- Ascending: Click **Ascending** to sort level-1 sub-organizations under the selected organization in ascending order by organization name.
- Descending: Click **Descending** to sort level-1 sub-organizations under the selected organization in descending order by organization name.
- Sort priority: Specify a sequence number to an organization. The organization tree will be sorted by the specified sequence number preferentially.

Click **Sort Priority** to go to the **Edit Sequence Number** page. After editing the resource sequence number, click **OK**.

Figure 7-7 Edit Sequence Number



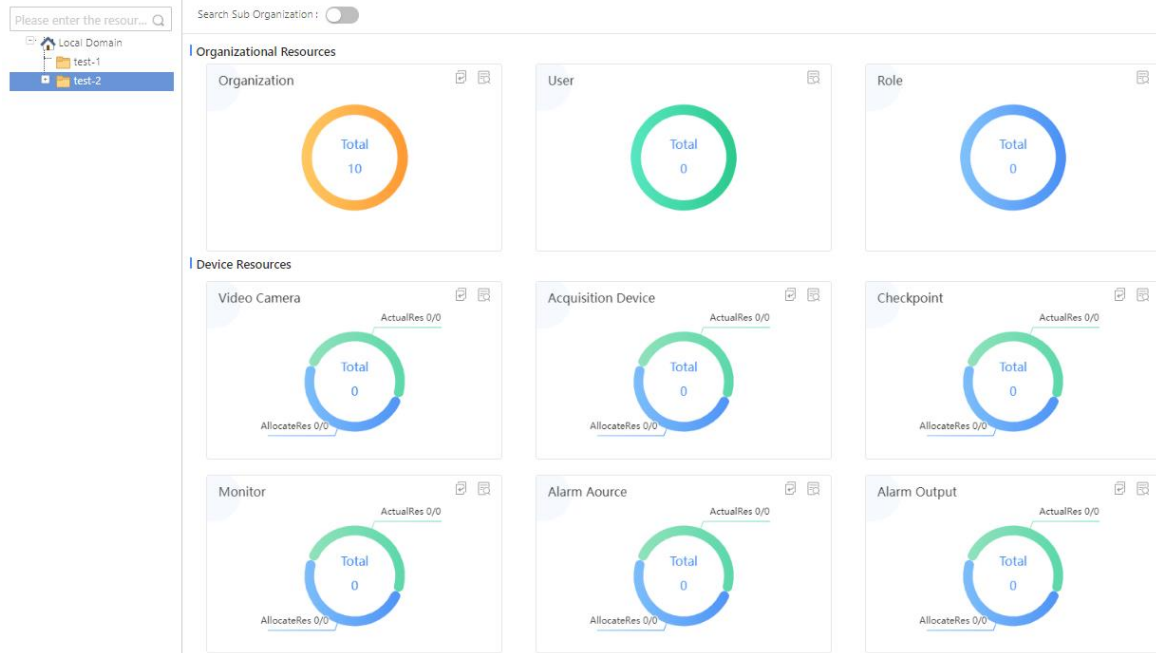
7.4 Resource Statistics

Go to **Device Management > Basic Configuration > Organization Management**. Select an organization in the organization tree. The number of resources under the organization will be counted and displayed in a chart on the right side. The statistics items include organization, user, role, camera, acquisition device, checkpoint, monitor, alarm source, and alarm output. If you want to count sub-organizations, enable **Search Sub-Organization**.



Note!

- Click  to go to the management page of the selected resource, where you can add, edit, and delete resources.
- Click  to go to the resource allocation page, where you can allocate resources to other organizations. For details, see [Resource Allocation](#).



7.5 Resource Allocation

Allocate the existing resources (such as cameras, monitors, alarm outputs, alarm sources) in organization A to organization B for sharing, so authorized users in organization B can operate these resources.

For example, after camera 1 in organization A is allocated to organization B, users with live view permissions in organization B can view live video from camera 1.

On the **Resource Allocation** page, you can allocate resources, cancel allocation, and view resource sharing information.



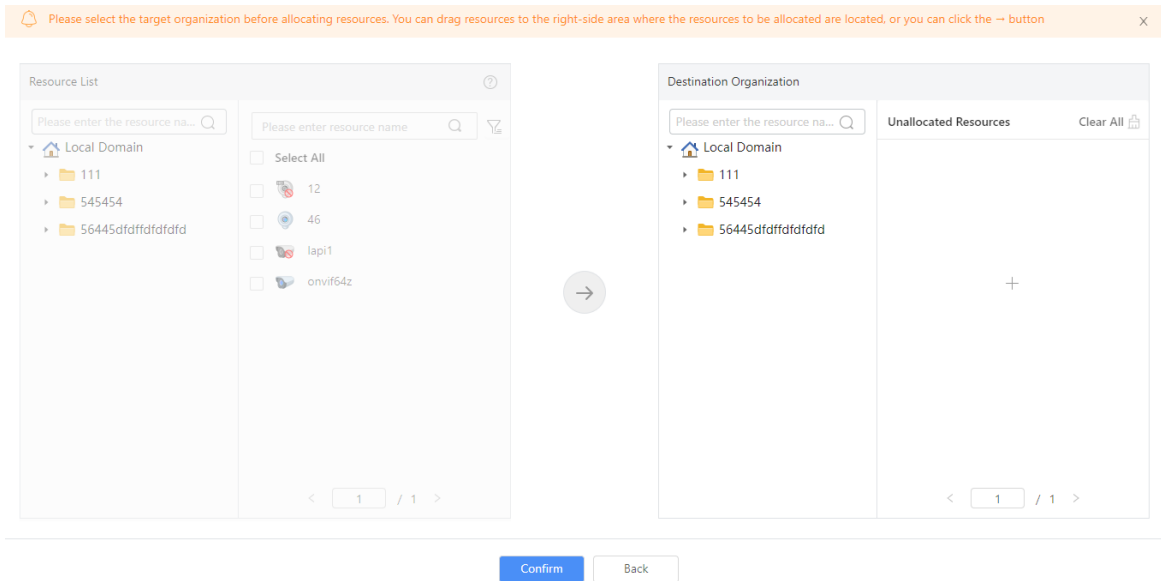
NOTE!

- One resource can be allocated to multiple organizations.
- Multi-channel IPCs cannot be allocated; their channels can be allocated.

1. Allocate Resource

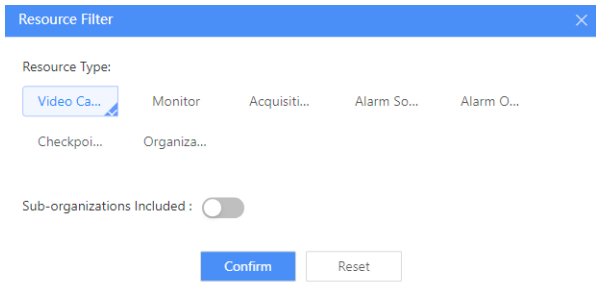
1. Go to **Device Management > Basic Configuration > Organization Management**.
2. Click  in the upper-right corner of the organization/device statistics card to go to the **Resource Allocation** page.

Figure 7-8 Resource Allocation



3. Select the destination organization from the organization tree on the right.
4. Select the source organization for resource allocation from the source organization list on the left side. The resources in the organization will be displayed. You can click  to search resources by resource type and resource name.

Figure 7-9 Resource Type Filter



5. Select the resources from the resource list on the left side, and click  or drag them to **Resources to Be Allocated**.
6. Click **OK** to complete resource allocation.

2. **Cancel Allocation**

1. Go to **Device Management > Basic Configuration > Organization Management**. Click  on the upper right corner of the device resource card to go to the corresponding resource list page.

2. Double-click the organization on the left-side origin organization list. Camera resources in the organization are displayed. You can search resources by resource type and resource name.
3. Select resources, click **Cancel Allocation**, and then confirm.



NOTE!

If the cancellation failed, click **View Failure Report** to view the detailed information. You can export the failure report if you want.

3. Manage Sharing Relationship

Only the super administrator can view which external domains the local domain is sharing device resources with, cancel sharing, and edit permissions.

(1) Query sharing relationship

Click the corresponding  for the resource. A page as shown below appears.

(2) Stop Sharing in Batches

Select resources, click **End Sharing Relationship**, and then confirm.

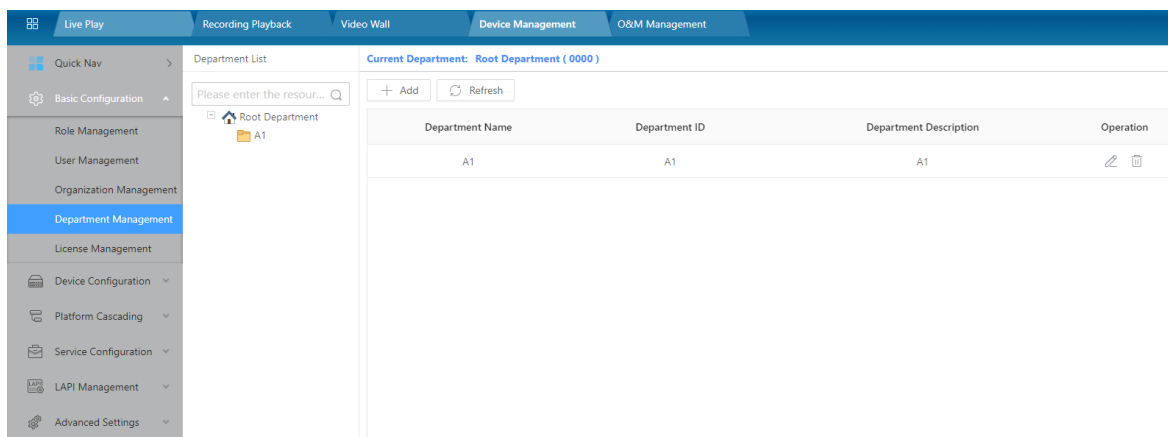
8 User Management

8.1 Department Management

Add departments so you can assign users to different departments.

8.1.1 Add Department

1. Go to **Device Management > Basic Configuration > Department Management**.



2. Choose the target department, click **Add**. A page as shown below appears.

3. Enter the department name, ID, and description.
4. Click **OK**.

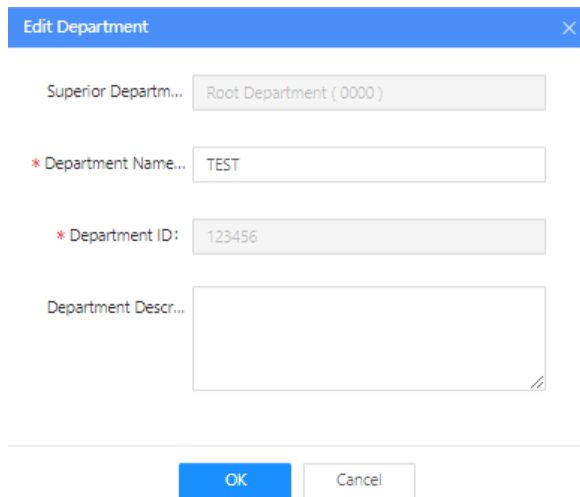


NOTE!

Make sure the department ID you entered is unique in the local domain. You may also leave it blank and let the system generate one.

8.1.2 Edit Department

1. Choose the target department, click **Edit**. A page as shown below appears.



2. Edit the department name, description.
3. Click **OK**.

8.1.3 Delete Department

Click the corresponding  for the department you want to delete. A confirmation message appears. Click **Delete** to delete the department.



NOTE!

The root department cannot be deleted.

8.2 Role Management

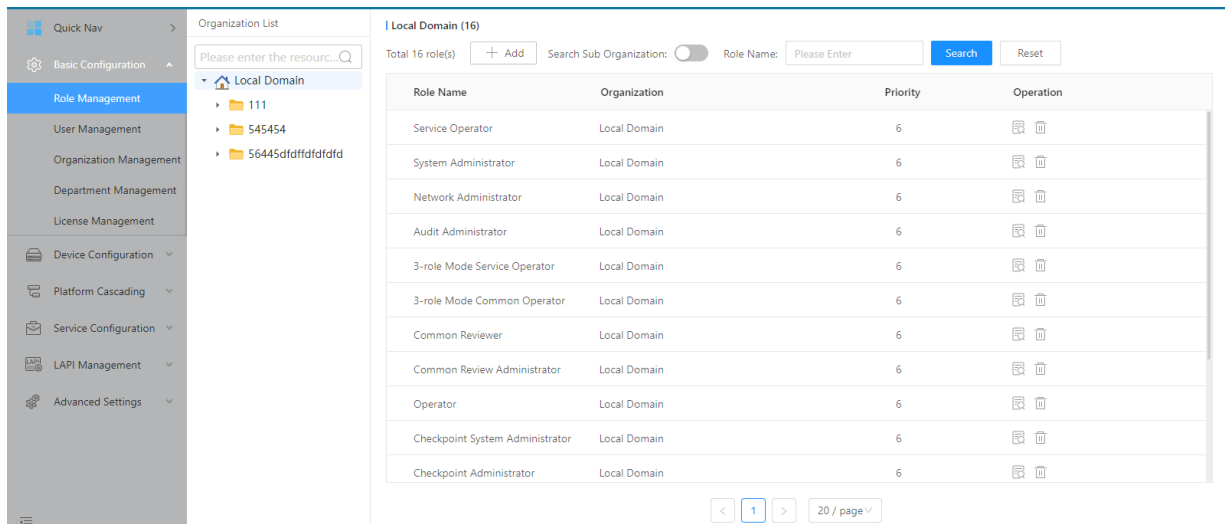
A role is a collection of operation permissions. After a role is assigned to a user, the user has all the permissions defined in the role. Role management facilitates the management and assignment of user permissions.

On the role management page, you can add roles, configure role permissions, edit roles, delete roles, and view operations of users who have been assigned a role.

8.2.1 Add Role

1. Configure Basic Role Info

1. Go to **Device Management > Basic Configuration > Role Management**.



2. Select an organization on the left-side organization list, click . A page as shown below appears.

1 Basic Info 2 Permission Configuration

Role Information

* Role Name: * Priority:

Organization: Linan District

Role Description:

3. Configure the basic information.

Table 8-1 Parameter Descriptions

Parameter	Description
Role Name	Name of the role template. Caution: The role name must be unique in the system. Duplicate role names are not allowed.
Priority	Priority level of the role (1-63). The smaller the value, the higher the priority. In resource preemption operations, roles with a higher priority level have higher privilege.
Role Description	A description of the role.

4. Click **Next**. A page as shown below appears. Assign permissions to the role.



Permission Configuration

Permissions Template: ▼

Menu Permission

Global Permission

Resource Permission

☒ Select All☒ Video Center☒ Live View☒ Playback☒ Video Wall☒ System Management☒ Device Management☒ O&M Management

2. Configure Role Permissions

Role permissions are divided into menu permission, global permissions and resource permissions.

- **Menu permission:** The user's permission to view and operate the system application management menu. Menu permissions are preferentially configured, and if there are no corresponding menu permissions, you cannot perform operations even if resource permissions and global permissions are configured.
- **Global permission:** Permissions to view and operate service modules in the system. Global permissions are effective to the entire system and are independent of specific organizations and resources.
- **Resources permission:** Permission to operate resources in the system. Resource permissions are configured for organizations or cameras. When a role is assigned resource permissions in an organization, the role has the assigned permissions to all the resources in the organization to which permissions are not assigned individually. When a role is assigned device permissions (for example, camera, monitor), the role has the specified permissions to the device.

Follow the principles stated in the table below when you configure resource permissions for a role.

Table 8-2 Principles of Configuring Resource Permissions for a Role

Principle	Description
Depth First	● If permissions are configured for an organization and its parent organization at the same time, then permissions configured for the organization take precedence when the organization is authenticated. ● If permissions are configured for an organization and the cameras/monitors in the organization at the same time, then permissions configured individually for these cameras/monitors take precedence when the cameras/monitors are authenticated.
Inherit	● If permissions are configured for an organization but not for its child organization, then the child organization inherits the permissions configured for its parent organization. ● After permissions are configured for an organization, the cameras/monitors without individually configured permissions in the organization automatically inherit permissions of the organization.
Combination	● If permissions are configured at the same time for a device (for example, camera, monitor) allocated to multiple organizations, then the permissions configured for the device are the total permissions configured for the device. ● If a user has multiple roles, the permissions of the user are the total permissions of the roles, and the priority level of the permissions is determined by the highest priority of all the roles.

Configuration References

The following recommendations are for your reference when you configure resource permissions in different situations.

- To assign same permissions of all the resources in an organization, you only need to assign organization permission to the role, then all the resources (such as cameras) in the organization will inherit the assigned organization permission.
- To assign same permissions of most resources in an organization and assign different permissions of a few resources (e.g., cameras, monitors), you only need to assign permissions of the most resources to the role, and then select the few devices (e.g., camera, monitor) and assign permissions separately.
- To assign permissions of a few cameras or monitors, you only need to select these devices when assigning permissions to the role; you don't need to assign organization permission. The role has no permissions to the unassigned cameras or monitors.

Configuration operations

1. After you complete the basic role information, a page as shown below appears.

2. Select the permission template predefined by the system, or select global permissions and resource permissions as needed.
3. Click **Complete**. The role is created.

8.2.2 Edit Role Configuration

Edit the basic information, permissions, and linked users of a role.

1. Role Information

1. Go to **Device Management > Basic Configuration > Role Management**. Select the target role on the role list.
2. Click **Edit** behind **Role Information**.

3. Edit the role name, priority level, and description.
4. Click **Save**.

2. Link a user

1. Go to **Basic Info**.

Relevant user Revoke Authentication		
☐ Username	Organization	Operation
☐ test	Local Domain	🔗

2. View all the users linked to the role, revoke the role as needed.

- Revoke a role from selected users: Select users and then click **Revoke Authentication**.
- Revoke a role from one user: Click the corresponding 🔗. The role is revoked from the user.

3. Permission Setup

1. Go to **Permissions Setup**.
2. Click **Edit** behind **Permission Setup**.

Permission Setup

Permissions Template:

Menu Permission Global Permission Resource Permission

☐ Select All

☒ Other

☒ Template Management
 ☒ System Maintenance
 ☒ Alarm Subscription
 ☒ Alarm Customization
 ☒ Third-Party Alarm Confi...
 ☒ Asset Management
 ☒ Bulletin

☒ Social Camera Manage...
 ☒ Image Retention Period...
 ☒ Dual Bus

☒ VIID Management

☒ VIID device management
 ☒ VIID networking manag...
 ☒ resource synchronization
 ☒ Subscription message
 ☒ Subscription task mana...

☒ Organization Management

☒ Department Manageme...
 ☒ External Domain Mana...

3. (Optional) Reselect the permission template.
4. Add or delete role permissions.
 - Add permissions: Select permissions.
 - Delete permissions: Deselect permissions.
5. Click **Save**.

8.3 User Management

Users are entities that manage and operate the system. After being assigned role(s), a user can log in to the system and perform the allowed operations.

The system allows simultaneous login to the same account from multiple clients. This simplifies user configuration and management, and allows normal operations with a small number of user accounts.

On the User Management page, the following operations are allowed in the local domain and its sub-organizations: add users, view/configure roles of users, manage logins, lock/unlock users, edit user info, export user info, delete users, assign users to departments, etc.



NOTE!

The system has two default users: admin and loadmin.

- Both have the role of the super administrator and the highest privilege in the system.
- The admin can grant/revoke the super administrator privilege to/from other users.
- Neither admin nor loadmin can be deleted.
- By default, admin cannot log in simultaneously from different clients.

8.3.1 Add User

Add users as needed and assign roles.

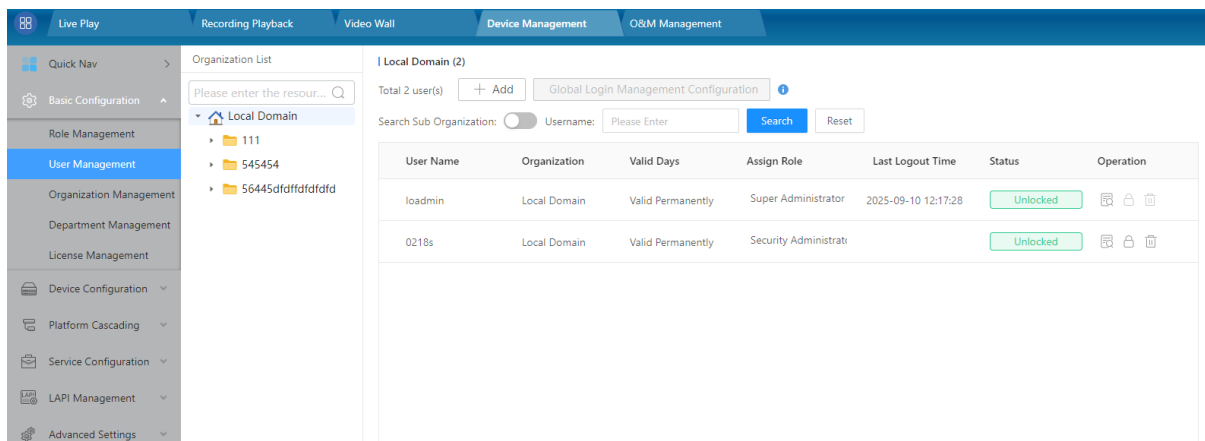


NOTE!

The system allows 10000 users (including admin and loadmin).

1. Configure Basic User Info

1. Go to **Device Management > Basic Configuration > User Management**.



2. Select an organization on the left-side organization list, click **NEW**. A page as shown below appears.

1 Basic Info — 2 Permission Setup — 3 Login Setup

Basic Info

* Username:

* Password:

Telephone:

Fax:

ID No.:

Max. Window ...: 25-Window

* User ID:

* Confirm Pass...:

Mobile Phone...:

Department:

Email:

Description:

Next Cancel

3. Enter the basic user information (fields with * are required), including username, user ID, password and confirmation password.



NOTE!

- Username and user ID must not be duplicate.
- The password must be at least 9 characters long and include all three types: letters, digits, and symbols (can only be & * _)
- The departments from which you can choose are existing departments created on the Department Management page.
- Max. Window Count means the maximum number of windows that can be displayed for the user. Options are 1/4/25 windows.

4. Click **Next**.

2. User Permission Setup

Assign role(s) to the new user to grant permissions defined in the assigned role(s). (Admin can set an ordinary user in the local domain as a super administrator.)

1. After you complete the basic user information, a page as shown below appears.

2. Click  right to **Assign Role** to expand the role list.

3. Select role(s), click **OK**.



NOTE!

- A user can be assigned one of the three roles: system administrator, security administrator, and audit administrator.
- A user can have up to 64 roles.

4. Click **Next**.

3. User Login Setup

Customize user login settings.

1. After you complete the user permission information, a page as shown below appears.

2. Configure login conditions by referring to the table below.

Table 8-3 Login Parameter Descriptions

Parameter	Description
Valid Days	Number of days that the user can operate the system. You can choose Valid Permanently (default setting) or set the number of days.
Usable Time	Day(s) in a week that the user can log in to the system.
Daily Login Period	Periods that the user can log in to the system in the allowed days. Up to two time periods are allowed.
Binding Policy	You can choose Use Global Configuration or Use Local Configuration . ● Global configuration: By default, simultaneous logins from multiple clients are allowed, and IP address is not bound, and admin can modify global configuration. ● Custom configuration: Allows user to configure whether simultaneous logins from multiple clients are allowed, whether to bind IPs (up to 50 IP address ranges can be bound. If the end IP and the start IP of an IP range are the same, or if the end IP is empty, it means only one IP is bound in this range).

3. Click **Complete**. The user is created.

8.3.2 Lock/Unlock User

A locked user cannot log in to the system until being unlocked.



NOTE!

- Only admin and loadadmin can lock/unlock other super administrators.
- When an online user is locked, the user is forced out of the system directly. The user can log in again only after it is unlocked.

Follow the steps to lock or unlock a user:

1. Go to **Device Management > Basic Configuration > User Management**.
2. Double-click an organization on the left-side organization list, choose the user you want to lock or unlock, click the corresponding  (lock) or  (unlock).
3. Confirm to complete the operation.

8.3.3 Edit User Information

Edit basic user information, permissions, login time, and manage login. Go to **Device Management > Basic Configuration > User Management**, click  behind user to view details and edit user information.

1. Basic Info

1. Click **Edit** behind **Basic Info**.
2. Edit basic user information (user ID cannot be changed).

| Basic Info

☐ Change Password

* Username:	loadmin	* User ID:	loadmin
Telephone:		Mobile Phone...	
Fax:		Department:	
ID No.:		Email:	
Max. Window ...	25-Window		
Description:			

3. (Optional) Select **Change Password** to set a new password. Only the super administrator has the permission.
4. Click **Save**.

2. Permission Setup

1. Click **Edit** behind **Permission Setup**.

Permission Setup

Assign Role:

Menu Permission Global Permission Resource Permission

Video Center		
Live View	Playback	Video Wall

System Management	
Device Management	O&M Management

2. You can add or delete roles.

- Add role: Click , select roles in the list, and then click **OK** to add the role(s).
 - Delete roles: Click the corresponding to delete a role.
3. Click **Save**.

3. Set Login Time

1. Click **Edit** behind **Set Login Time**.

Set Login Time

Valid Days: ☒ Valid Permanently ☐ Customization

Usable Time: ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

Daily Login Period1: ~

Daily Login Period2: ~

Login Management

Binding Policy: ☒ Use Global Config... ☐ Use Local Config...

Login Type: ☒ Multi-client logi... ☐ Allow Login Pree...

☐ Bound IP Address

2. Select/deselect the usable time.
3. Edit the daily login periods.
4. Click **Save**.

4. Login Management

1. Click **Edit** behind **Login Management**.
2. Edit the login policy. See User Login Setup.
3. Click **Save**.

5. Global Login Management (admin only)

Only admin can edit the global login management policy.

1. Go to **Device Management > Basic Configuration > User Management**.
2. Click **Global Login Management**.

3. Set global login method by referring to the table below.

Table 8-4 Parameter Descriptions for Configuring Global Login Method

Parameter	Description
Multi-client login allowed	Allows the same user to log in from different clients at the same time. Note: This feature is not applicable to admin.
Allow Login Preemption	When enabled, a user can log in only from one client at a time. Login from different clients at the same time is not allowed.
Bound IP Address	To bind IP addresses, select the Bound IP Address checkbox, enter the start and end IP addresses, and then click Save . Note: Up to 50 IP ranges are allowed. If the end IP and the start IP of an IP range are the same, or if the end IP is empty, it means only one IP is bound in this range.

4. Edit Daily Login Period

5. Click **Save**.



NOTE!

After the global login management policy is changed, the login policy of users who use the global configuration will change accordingly.

6. Super Administrator

The admin user can set other users as a super administrator. You can assign the super administrator role to a user during permission setup. For details, see [Permission Setup](#).

Figure 8-1 Super Administrator Setup

8.4 3-Role Mode

Three roles means system administrator, security administrator, and audit administrator. In 3-role mode, creating a user requires the system administrator to add the user, the security administrator to assign role(s) to the user, and the audit administrator to audit the user.

In 3-role mode, the legal status of a user who wants to log in will be verified. Only users who have passed the audit and users added in normal mode (including the super administrator and 3-role users) can access the system and operate according to the assigned roles/permissions. This prevents login by illegal users and protect system security.



NOTE!

To switch between normal mode and 3-role mode, see User Login Mode.

3-Role Permissions

User Role	User Management Permission	Task Description
System administrator	User management	Add, delete, edit, search user
Security administrator	Role management	Add, delete, edit, search role
	User management	Assign roles to users
Audit administrator	User management	Audit user

Configuration Procedure

No.	Login Mode	Login User	Task Description
1	Normal mode	Super Administrator	Add users of three roles: system administrator, security administrator, and audit administrator.
2	Separation of powers	System administrator	Add user (user status is "added, not authorized")
3	Separation of powers	Security administrator	Assign roles to new users (user status is "authorized, not audited")
4	Separation of powers	Audit administrator	Audit new user (user status is "audit passed")
5	Separation of powers	Audited user	Perform operations allowed by its roles and permissions

8.4.1 User Login Mode

1. Go to **Device Management > Advanced Settings > Center Configuration > User Login Mode**.

User login mode

User login mode:

☒ Normal mode ☐ Separation of powers

2. Choose **Normal Mode** or **Separation of powers**. Re-login is required after the login mode is changed.



NOTE!

In normal mode, any user can log in to the system.

8.4.2 Add 3-Role User

Users of three roles added by the super administrator in normal mode: system administrator, security administrator, audit administrator.

1. Log in to the system as super administrator.
2. Set Login Mode to Normal Mode. See User Login Mode.
3. Go to **Device Management > Basic Configuration > User Management** to add users of the three roles: system administrator, security administrator, administrator. See Add User.



NOTE!

A user can be assigned one of the three roles: system administrator, security administrator, and audit administrator.

8.4.3 Add User (by system administrator)

In 3-role mode, users are added by the system administrator.

1. Set Login Mode to Separation of powers. See User Login Mode.
2. Log in to the system as system administrator, go to **Device Management > Basic Configuration > User Management**.
3. Create the user, configure the basic user information, and then click **Next**.
4. Go to the **Permission Setup** page, click **Next** directly (system administrator has no permission to assign roles).
5. Go to the **Login Setup** page and configure login (see User Login Setup).
6. Click **Complete**. The user is created, and the user status is “added, not authorized”.



NOTE!

In Separation of powers mode, the super administrator also can add users but cannot assign roles.

8.4.4 Assign Roles (by security administrator)

In Separation of powers mode, roles are assigned by the security administrator.

1. Set **Login Mode** to **Separation of powers**. See User Login Setup.
2. Log in to the system as security administrator, go to **Device Management > Basic Configuration > User Management**.
3. (Optional) Go to the **Role List** page, add roles and assign permissions to the roles. In Separation of powers mode, the system has different roles: service operator and normal operator. You can change permissions of the default roles and customize roles as needed.



NOTE!

- In Separation of powers mode, roles of normal mode are not displayed.
 - In Separation of powers mode, roles do not have the User Management permission.
-

4. Go to the **User List** page, double-click an organization on the left-side organization list. Users in the organization appears.
5. Click a “**Added, Not Authorized**” user. User information is displayed.
6. Click **Edit** behind **Permission Setup**.

7. Click  to expand the role list, select roles, and then click **OK**.
8. Click **Save**. The roles are assigned (user status is “authorized, not audited”).

8.4.5 Audit User (by audit administrator)

In Separation of powers mode, users must be audited by the audit administrator.

1. Set **Login Mode** to **Separation of powers**. See User Login Mode.
2. Log in to the system as audit administrator, go to **Device Management > System Configuration > User Management > User List**.
3. Double-click an organization node on the left-side organization list. Users in the organization are displayed.
4. Click an “Authorized, Not Audited” user. User information is displayed.
5. Click **Account Audit** behind the account status.
6. Click **Audit Passed**. The user is created (user status is “audit passed”).



NOTE!

- A user who has passed audit cannot be audited again, and its audit status cannot be changed.
- If you want to change the roles of a user who has passed the audit, the user must go through the audit process again.

9 Device Management

Go to **Device Management > Local Domain** to add, edit, or delete devices.

9.1 Frontend Device

On the **Frontend Device** page, you can add various types of video devices and data devices.

- Video devices include GB cameras (single-channel and multi-channel), ONVIF cameras, IMOS cameras, and LAPI cameras.
- Data devices include acquisition devices, video checkpoints, and checkpoints.

9.1.1 Add Frontend Device

Go to **Device Management > Frontend Device**. Select the organization to which the device belongs in the organization tree on the left side. Click **New** to go to the **Add Frontend Device** page.

1. GB Single-Channel Camera

Single-channel cameras that are added via the GB protocol.

1. On the **Add Frontend Device** page, select **Video Device** as the tag.
2. Set **Protocol Type** to **GB Protocol** and **Camera Channel Type** to **Single-Channel Camera**.

Figure 9-1 GB Single-Channel Camera - Required Information

The screenshot shows the 'Add Frontend Device' page with the 'Required Information' tab selected. The 'Basic Info' section contains fields for 'Device Name', 'Device ID', and 'Organization'. The 'Tag Info' section shows 'Video Device' selected. The 'Video Device' section includes fields for 'Protocol type' (GB/T 28181 Protocol), 'Camera Channel Type' (Single-Channel), 'Camera Type' (Fixed Camera), 'Camera subtype' (Common Camera), 'Camera GB Code', 'Camera Capability' (normal), 'Code rate(Kbps)' (2048), 'User Name', 'Max IPC Streams' (4), 'Stream Transmission Prot...' (TCP), 'TCP Type' (GB2016), 'TCP Direction' (IPC as Client), 'Playback/Download Servi...' (Auto-Adaptation), 'Support Direct Storage' (no), and 'Authentication' (yes).

3. See the following table to configure the required information for the camera.

Table 9-1 Required Parameters of GB Single-Channel Cameras

Parameter	Description
Camera Name	Camera name.
Camera ID	Camera ID in the local domain, which must be unique in the local domain. Note! The camera-side device code must match this parameter. Otherwise, the device cannot go online.
Organization	Select the parent organization to which the camera is to be added.
Camera Type	12 types available (Fixed Camera, PTZ Camera, Fixed HD Camera, HD PTZ Camera, In-Vehicle Camera, Uncontrollable SD Dome Camera, Uncontrollable HD Dome Camera, Isolate Video Access, Motorized Lens Camera, Ultra Clear Face Capture Camera, Multi-eye Splicing Camera, Access Control Device).

Parameter	Description	
Camera Subtype	Choose common camera, smart cameras (to recognize pedestrians, non-motor vehicles, and motor vehicles, and analyze structured attributes), LAPI camera (camera connected via LAPI to capture image data, and the corresponding image asset information is required).	
Camera Capability	Choose the camera capability: Common/Support Area People Counting/Support Tripwire People Counting/Support Area and Tripwire People Counting.	
Bit Rate	Encoding rate. Calculate storage space based on the bitrate.	
Username	Camera's username (required when authentication is enabled).	
Password	Camera password (required when authentication is enabled).	
Max IPC Streams	This parameter limits the maximum number of unicast, direct-connection live video streams of the IPC in the local domain (1-51).	
Stream Transmission Protocol	The default is TCP. TCP is recommended if the network environment is poor. If you choose TCP , you need to choose the TCP type (GB2014/GB2016) and TCP direction (IPC as Client or as Server).	
Playback/Download Media Service Policy	● Auto-Adaptation: Default setting. All MS share the load (except when the client player or decoder in the local domain adopts the Direct Connection First policy). When the forwarding capacity of the MS is insufficient, follow the policy of Direct Connection First. ● You can choose whether to bypass the specified MS (group) as needed. If you need to forward multiple media streams, specify the MS (group). ● This configuration takes effect only for playback and download.	
Support Storage	Direct	● Yes: Streams are stored directly by iSCSI without using the DM. It is only applicable to Uniview cameras, and you need to check the camera capability first. ● No: Streams are received and directly stored via the DM.
Authentication	Default: Yes ● Authentication enabled: When connecting to the server, the IPC verifies the username and password stored on the server, and gets online after authentication succeeds. ● Authentication disabled: When connecting to the server, the IPC can get online without requiring the server to enter the username and password.	
Image Information	Asset	When the camera subtype is LAPI camera, you need to configure image asset information. Image asset information * IP Address: Please enter the IP address. * Port: 80 * User Name: Please enter the user name. * Password: Please enter the password. * Transfer Protocol: HTTP MD地址: Push Mode: Image Subscription Type: Cros... X Intru... X +42
	Device ID	Device ID of the camera.
	IP Address/Port Number	IP address and port number (80) of the camera.
	Transmission Protocol	● HTTP: The camera reports LAPI data. ● WebSocket: The camera reports radar and video data.
	Username/Password	Username/password for logging in to the camera.
	MD Address	IP address of the MD server that accesses the LAPI device data. (Required when HTTP is selected.)
	Push Mode	Select the image push mode: Image, Local URL, or Cloud Storage URL. (Required when HTTP is selected.)
	Subscription Type	Select the data type of the LAPI device to be subscribed. (Required when HTTP is selected. The subscription is activated after you

Parameter	Description
	configure this parameter. You can view or edit it on the LAPI Device Subscription page.)

- Click **OK** to complete the addition.
- (Optional) Click **Next** and fill in the optional information.

Figure 9-2 GB Single-Channel Camera - Optional Information

The screenshot shows the 'Optional Information' configuration page for a GB Single-Channel Camera. At the top, there are two steps: '1 Required Information' (completed) and '2 Optional information (it can be skipped)' (current step). The page is titled 'Other Info' and 'Video device_GB'. The configuration fields include:

- Longitude: [text input]
- Latitude: [text input]
- Height: [text input]
- NAT Config: [dropdown menu showing 'Without NAT']
- Live Video Media Service ...: [dropdown menu showing 'Auto-Adaptation']
- Apply for Scrambling Cert...: [radio buttons for 'yes' and 'no', with 'no' selected]
- Support Multicast: [radio buttons for 'yes' and 'no', with 'no' selected]
- Asset Info: [checkbox]

Table 9-2 GB Single-Channel Camera - Optional Information

Parameter	Description
GB/T 28181 Code Rules Camera GB Code	To achieve sharing between GB domains, you need to configure the GB code for the camera. ● Generate Automatically: Choose a rule for the ID specified in the GB/T 28181 ID data dictionary. The system generates the camera ID automatically. ● Enter Manually: Follow the GB code rules. There must be 20 bits, of which bits 11-13 must be 119-129, 131, or 132.
Longitude	Longitude of the camera's location.
Latitude	Latitude of the camera's location.
Height	Height of the camera's location.
NAT config	● If the IPC is behind the NAT and the local domain is in front of the NAT, choose IPC Behind the NAT. ● If the local domain is behind the NAT and the IPC is in front of the NAT, choose IPC in front of the NAT. ● If IPC and the external domain are behind different NATs, choose IPC and Local Domain Behind Separate NATs. ● If data streams of the IPC do not need to traverse the NAT, choose No NAT.
Live Video Media Service Policy	● Auto-Adaptation: Default setting. All MS share the load (except when the client player or decoder in the local domain adopts the Direct Connection First policy). When the forwarding capacity of the MS is insufficient, follow the policy of Direct Connection First. ● You can choose whether to bypass the specified MS (group) as needed. If you need to forward multiple media streams, specify the MS (group). ● This configuration takes effect only for live videos.
Apply for Scrambling Certificate	Choose whether to enable video scrambling. When enabled, videos will be scrambled at the front end for security, and a key is required in order to watch the video at the back end. Note: Only certain cameras support the scramble function. Please consult our sales for the specific camera models. For child domain IPCs, it is required to add a TS server in the child domain and configure transcoding rules .

Parameter	Description
Asset Information	(Optional) If checked, configure the asset information of the device as required. Asset Info ✖ ✖ Asset ID: Please enter the asset ID. ✖ Asset Name: Please enter the asset name. ✖ Asset Model: Please enter the asset model. ✖ Asset Status: Running ✖ Warranty Period: 2024-01-30 ✖ Vendor: Please enter the vendor name. ✖ Purchase Time: 2024-01-30 ✖ Contractor: Please enter the contractor name. ✖ Installation Time: 2024-01-30 16:41:47 ✖ Installation Site: Please enter the installation location Maintainer: Please enter the maintainer. Service Telephone: Please enter service phone number MAC Address: Please enter the MAC address.

6. Click **OK** to complete the addition.

2. GB Multi-Channel Camera

Multi-channel cameras accessed with the national standard protocol, multi-channel cameras, i.e. cameras with multiple video channels (multiple lenses) present.

1. On the **Add Frontend Device** page, select **Video Device** as the tag.
2. Set **Protocol Type** to **GB Protocol** and **Camera Channel Type** to **Multiple-Channel Camera**.

Figure 9-3 GB Multi-Channel Camera - Required Information

[< Back](#) | Add Frontend Device

1 Required Information

2 Optional information (it can be skipped)

Basic Info

✖ Device Name: Please Enter

✖ Device ID: Please Enter

✖ Organization: Local Domain

Tag Info

Tag: ☒ Video Device

Video Device

Protocol type: GB/T 28181 Protocol

Camera Type: Fixed Camera

Camera GB Code: 01234567891310000018

✖ code rate(Kbps): 2048

✖ Password: Please enter the password.

Stream Transmission Prot...: TCP

TCP Direction: IPC as Client

Camera Channel Type: ☒ Single-Chann... ☐ Multi-channel ...

Camera subtype: Common Camera

Camera Capability: normal

✖ User Name: Please enter the user name.

✖ Max IPC Streams: 4

TCP Type: GB2016

Playback/Download Servi...: Auto-Adaptation

Confirm

Next

3. See the following table to configure the required information for the camera.

Table 9-3 Required Parameters of GB Multi-Channel Cameras

Parameter	Description
Camera Name	Camera name.
Camera ID	Camera ID in the local domain, which must be unique in the local domain.

91

Parameter	Description
	Note! The camera-side device code must match this parameter. Otherwise, the device cannot go online.
Organization	Select the parent organization to which the camera is to be added.
Camera Subtype	Choose common camera, smart cameras (to recognize pedestrians, non-motor vehicles, and motor vehicles, and analyze structured attributes), LAPI camera (camera connected via LAPI to capture image data, and the corresponding image asset information is required).
Camera Quantity	The number of channels for the multi-channel camera, up to 16 channels.
Username	Camera's username (required when authentication is enabled).
Password	Camera password (required when authentication is enabled).
Support Storage Direct	Select whether the camera supports direct storage as required.
Authentication	Default: Yes - Authentication enabled: When connecting to the server, the IPC verifies the username and password stored on the server, and gets online after authentication succeeds. - Authentication disabled: When connecting to the server, the IPC can get online without requiring the server to enter the username and password.

4. Click **OK** to complete the addition.

5. (Optional) Click **Next** and fill in the optional information.

Figure 9-4 GB Multi-Channel Camera-Optional information

< Back | Add Frontend Device

✓

Required Information

2

Optional information (it can be skipped)

Other Info

Video device_GB

Longitude:

Latitude:

Height:

NAT Config:

Without NAT

Live Video Media Service ...

Auto-Adaptation

Apply for Scrambling Cert...

yes

no

☐ Asset Info

Table 9-4 GB Multi-Channel Camera-Optional information

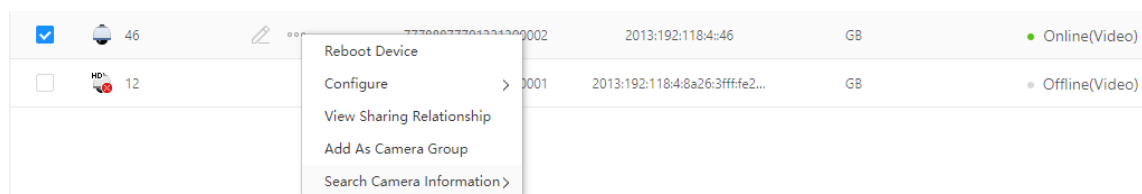
Parameter	Description
NAT config	- If the IPC is behind the NAT and the local domain is in front of the NAT, choose IPC Behind the NAT. - If the local domain is behind the NAT and the IPC is in front of the NAT, choose IPC in front of the NAT. - If IPC and the external domain are behind different NATs, choose IPC and Local Domain Behind Separate NATs. - If data streams of the IPC do not need to traverse the NAT, choose No NAT.
Asset Information	(Optional) If checked, configure the asset information of the device as required.

Parameter	Description
	Asset Info * Asset ID: Please enter the asset ID. * Asset Name: Please enter the asset name. * Asset Model: Please enter the asset model. * Asset Status: Running * Warranty Period: 2025-09-10 * Vendor: Please enter the vendor name. * Purchase Time: 2025-09-10 * Contractor: Please enter the contractor name. * Installation Time: 2025-09-10 13:53:25 * Installation Site: Please enter the installation location Maintainer: Please enter the maintainer. Service Telephone: Please enter service phone number MAC Address: Please enter the MAC address. Confirm Cancel

6. Click **OK** to complete the addition.

7. After the GB multi-channel camera is added and released, click **Get Resource** to get the channels for it.

Figure 9-5 GB Multi-Channel Camera - Get Resource



8. Select the GB multi-channel camera in the frontend device list. The channel list will be displayed.

Figure 9-6 GB Multi-Channel Camera - Channel List

☒	192.168.1.55	Click here	192163155	192.163.1.55	IPC	HC121@UC-00560	On...
☐	192.168.1.58		192163158	192.163.1.58	NVR		Off...

total 14 1 20 / page

Camera List

☐	Camera name	Camera ID	Camera Type	Device Status
☐	192.168.1.55_1	538095600013427144-Q-1	PTZ Camera	Online
☐	192.168.1.55_2	538095600013427144-Q-2	Fixed Camera	Online



Note!

- GB single-channel cameras have only one channel, and the channel configuration and the device configuration are integrated.
- GB multi-channel cameras have multiple channels, and the channel configuration and the device configuration are separate.

3. ONVIF Camera

Cameras that are connected via Onvif.

1. On the **Add Frontend Device** page, select **Video Device** as the tag.
2. Set **Protocol Type** to **ONVIF**.

Figure 9-7 ONVIF Camera - Required Information

The screenshot displays a configuration form for an ONVIF camera. At the top, there are two tabs: '1 Required Information' (active) and '2 Optional information (it can be skipped)'. The 'Basic Info' section includes fields for 'Device Name' (placeholder: 'Please Enter'), 'Device ID' (placeholder: 'Please Enter'), and 'Organization' (placeholder: 'Local Domain'). The 'Tag Info' section shows 'Tag:' with a checked 'Video Device' option. Below this, the 'Video Device' section contains various configuration fields: 'Protocol type:' (dropdown: 'ONVIF'), 'Camera Type:' (dropdown: 'Fixed Camera'), 'Camera GB Code:', 'Camera Capability:' (dropdown: 'normal'), '* code rate(Kbps):' (input: '2048'), '* IP Address:', '* Port:' (input: '80'), '* User Name:' (placeholder: 'Please enter the user name.'), '* Password:' (placeholder: 'Please enter the password.'), '* Max IPC Streams:' (input: '4'), 'Stream Transmission Prot...' (dropdown: 'TCP'), 'Playback/Download Servi...' (dropdown: 'Auto-Adaptation'), and 'Authentication:' (radio buttons: 'yes' selected, 'no'). At the bottom, there are 'Confirm' and 'Next' buttons.

3. See the following table to configure the required information for the camera.

Table 9-5 Required Parameters of ONVIF Cameras

Parameter	Description
Device Name	Device name.
Camera ID	Camera ID in the local domain, which must be unique in the local domain. Note! The camera-side device code must match this parameter. Otherwise, the device cannot go online.
Organization	Select the parent organization to which the camera is to be added.
Camera Type	12 types available (Fixed Camera, PTZ Camera, Fixed HD Camera, HD PTZ Camera, In-Vehicle Camera, Uncontrollable SD Dome Camera, Uncontrollable HD Dome Camera, Isolate Video Access, Motorized Lens Camera, Ultra Clear Face Capture Camera, Multi-eye Splicing Camera, Access Control Device).
Camera Capability	Choose the camera capability: Common/Support Area People Counting/Support Tripwire People Counting/Support Area and Tripwire People Counting.
Bit Rate	Encoding rate. Calculate storage space based on the bitrate.
IP Address	IP address of the camera.
Port Number	Port number on which the camera receives messages.
Username	Camera's username (required when authentication is enabled).
Password	Camera password (required when authentication is enabled).

Parameter	Description
Max IPC Streams	This parameter limits the maximum number of unicast, direct-connection live video streams of the IPC in the local domain (1-51).
Stream Transmission Protocol	The default is TCP. TCP is recommended if the network environment is poor. If you choose TCP , you need to choose the TCP type (GB2014/GB2016) and TCP direction (IPC as Client or as Server).
Playback/Download Media Service Policy	- Auto-Adaptation: Default setting. All MS share the load (except when the client player or decoder in the local domain adopts the Direct Connection First policy). When the forwarding capacity of the MS is insufficient, follow the policy of Direct Connection First. - You can choose whether to bypass the specified MS (group) as needed. If you need to forward multiple media streams, specify the MS (group). - This configuration takes effect only for playback and download.
Authentication	Default: Yes - Authentication enabled: When connecting to the server, the IPC verifies the username and password stored on the server, and gets online after authentication succeeds. - Authentication disabled: When connecting to the server, the IPC can get online without requiring the server to enter the username and password.

- Click **OK** to complete the addition.
- (Optional) Click **Next** and fill in the optional information.

Figure 9-8 ONVIF Camera - Optional Information

The screenshot shows the 'Optional Information' step of the ONVIF Camera configuration. At the top, there are two progress indicators: a blue circle with a checkmark for 'Required Information' and a blue circle with the number '2' for 'Optional Information (it can be skipped)'. Below this, the 'Other Info' section is expanded, showing 'Video device_ONVIF'. The form contains several fields: 'Longitude' and 'Latitude' (text input), 'Height' (text input), 'Live Video Media Service ...' (dropdown menu set to 'Auto-Adaptation'), 'Protocol type:' (dropdown menu set to 'ONVIF2.X'), 'Enable Alarm:' (radio buttons for 'yes' and 'no', with 'no' selected), and 'Enable Time Sync:' (radio buttons for 'yes' and 'no', with 'no' selected). At the bottom left, there is a checkbox for 'Asset Info' and a gear icon.

Table 9-6 ONVIF Camera - Optional Information

Parameter	Description
GB/T 28181 Code Rules Camera GB Code	To achieve sharing between GB domains, you need to configure the GB code for the camera. - Generate Automatically: Choose a rule for the ID specified in the GB/T 28181 ID data dictionary. The system generates the camera ID automatically. - Enter Manually: Follow the GB code rules. There must be 20 bits, of which bits 11-13 must be 119-129, 131, or 132.
Longitude	Longitude of the camera's location.
Latitude	Latitude of the camera's location.
Height	Height of the camera's location.
Live Video Media Service Policy	- Auto-Adaptation: Default setting. All MS share the load (except when the client player or decoder in the local domain adopts the Direct Connection First policy). When the forwarding capacity of the MS is insufficient, follow the policy of Direct Connection First. - You can choose whether to bypass the specified MS (group) as needed. If you need to forward multiple media streams, specify the MS (group). - This configuration takes effect only for live videos.
Protocol Type	Choose a protocol type for the camera (ONVIF1.0/ONVIF2.X).

Parameter	Description
Enable Alarm	When enabled, Onvif cameras will report alarms to the system when an alarm occurs. This function is disabled by default. Two types of alarms can be reported: motion detection alarm and alarm input. Note: IPC online/offline alarms are not restricted by this function.
Enable Time Sync	When enabled, the system will sync the server time to the camera. To ensure time is accurate, the system calibrate the camera time at one o'clock in the morning every day.
Asset Information	(Optional) If checked, configure the asset information of the device as required. Asset Info × *Asset ID: Please enter the asset ID. *Asset Name: Please enter the asset name. *Asset Model: Please enter the asset model. *Asset Status: Running ▼ *Warranty Period: 2024-01-30 📅 *Vendor: Please enter the vendor name. *Purchase Time: 2024-01-30 📅 *Contractor: Please enter the contractor name. *Installation Time: 2024-01-30 16:48:44 📅 *Installation Site: Please enter the installation location Maintainer: Please enter the maintainer. Service Telephone: Please enter service phone number MAC Address: Please enter the MAC address.

6. Click **OK** to complete the addition.

4. LAPI Device

Add cameras and NVRs (to achieve access to the video channels) as well as radar devices (to achieve access to radar human body data, such as fall detection and rise detection) via Uniview's private protocol (LAPI).

1. On the **Add Frontend Device** page, select **Video Device** as the tag.
2. Set **Protocol Type** to **LAPI**.

Figure 9-9 LAPI Device - Required Information

1 Required Information
 2 Optional Information (it can be skipped)

Basic Info

Device Name:

Organization:

Device ID:

Tag Info

Tag: ☒ Video Device

LAPI Device

Protocol type:

Transfer Protocol:

User Name:

IP Address:

LAPI Image Function: ☐ yes ☒ no

LAPI Device Type:

Stream Transmission Prot...:

Password:

Port:

3. See the following table to configure the required information for the camera.

Table 9-7 Required parameters of LAPI devices

Parameter	Description
Device Name	Device name.
Device ID	Camera ID in the local domain, which must be unique in the local domain. Note! The camera-side device code must match this parameter. Otherwise, the device cannot go online.
Organization	Select the parent organization to which the camera is to be added.
LAPI Device Type	IPC, NVR, and radar.
Transmission Protocol	- HTTP: The device type is IPC/NVR and the camera reports LAPI data. - WebSocket: The device type is radar and the camera reports radar data.
Stream Transmission Protocol	The default is TCP. TCP is recommended if the network environment is poor. If you choose TCP , you need to choose the TCP type (GB2014/GB2016) and TCP direction (IPC as Client or as Server).
Username/Password	Username and password of camera login (required).
IP Address	IP address of the camera.
LAPI Image	If enabled, you can subscribe to images from LAPI devices (on the Subscribing to LAPI Devices page). Otherwise, you cannot subscribe to images.

4. Click **OK** to complete the addition.

5. (Optional) Click **Next** and fill in the optional information.

Figure 9-10 LAPI Device - Optional Information

The screenshot shows a configuration window for a LAPI device. At the top, there are two tabs: 'Required Information' (active) and 'Optional Information (it can be skipped)'. Below the tabs, the 'Other Info' section is visible. It contains the following fields:

- Media Service Policy:** A dropdown menu set to 'Auto-Adaptation'.
- Enable Alarm:** Radio buttons for 'yes' (selected) and 'no'.
- Enable Time Sync:** Radio buttons for 'yes' and 'no' (selected).
- Asset Info:** A checkbox that is currently unchecked.

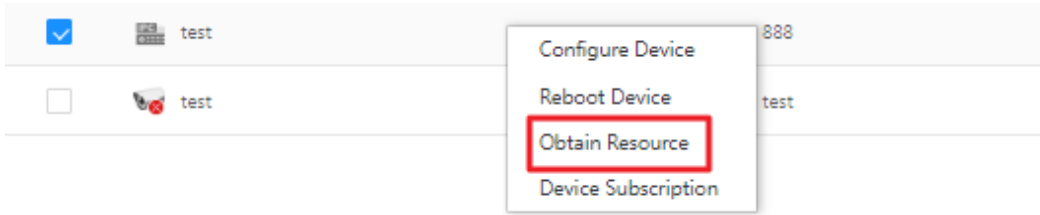
Table 9-8 LAPI Device - Optional Information

Parameter	Description
Port Number	The registered port number of the LAPI device (default: 80).
Media Service Policy	● Auto-Adaptation: Default setting. All MS share the load (except when the client player or decoder in the local domain adopts the Direct Connection First policy). When the forwarding capacity of the MS is insufficient, follow the policy of Direct Connection First. ● You can choose whether to bypass the specified MS (group) as needed. If you need to forward multiple media streams, specify the MS (group).
Enable Alarm	If the alarm function is enabled, the IPC will report the alarm to the system when it detects an alarm. By default, the alarm function is disabled. Alarm types include the motion detection alarm and digital input alarm. Note! The alarms of IPC going online/offline are not restricted by this function.
Enable Time Synchronization	When time synchronization is enabled, the system synchronizes the server time to the camera. To ensure the time is accurate, the system will calibrate the camera time at 1:00 a.m. every day.
Asset Information	(Optional) If checked, configure the asset information of the device as required. Asset Info X * Asset ID: Please enter the asset ID. * Asset Name: Please enter the asset name. * Asset Model: Please enter the asset model. * Asset Status: Running * Warranty Period: 2024-01-30 * Vendor: Please enter the vendor name. * Purchase Time: 2024-01-30 * Contractor: Please enter the contractor name. * Installation Time: 2024-01-30 16:52:17 * Installation Site: Please enter the installation location - Maintainer: Please enter the maintainer. - Service Telephone: Please enter service phone number - MAC Address: Please enter the MAC address.

6. Click **OK** to complete the addition.

7. After the LAPI device is added and released, click **Get Resource** to get the channels for it.

Figure 9-11 LAPI Device - Get Resource



8. Select the LAPI device in the frontend device list. The camera list will be displayed.

Figure 9-12 LAPI Device - Camera List

☒	LAPI	Click here	LAPI	172.20.81.234	LAPI Device	Online(Video)
☐	test		999		GB	Offline(Video)

total 2 < 1 > 20 / page

Camera List Batch Delete

☐	Camera name	Camera ID	Camera Type	Device Status
☐	LAPL_17	24013020081324411957	Fixed Camera	Online
☐	LAPL_19	24013020081324441034	Fixed Camera	Online
☐	LAPL_20	24013020081324488301	PTZ Camera	Online

5. Mobile Frontend

Mobile frontend refers to mobile terminals connected to the platform via the GB protocol, including in-vehicle cameras (onboard cameras), body worn cameras, etc.



Note!

Please add [TS Server](#) firstly.

1. On the **Add Frontend Device** page, select **Video Device** as the tag.
2. Set **Protocol Type** to **Mobile Frontend**.

Figure 9-13 Mobile Frontend - Required Information

< Back | Add Frontend Device

* Device Name: * Device ID:

* Organization:

Tag Info

Tag: ☒ Video Device

Video Device

Protocol type: Camera Type:

Camera GB Code: * Code rate(Kbps):

Port: * Max IPC Streams:

Confirm Next

3. See the following table to configure the required information for the camera.

Table 9-9 Required parameters of LAPI devices

6. Parameter	7. Description
8. Camera Name	9. Camera name.
10. Camera ID	Camera ID in the local domain, which must be unique in the local domain. Note! The camera-side device code must match this parameter. Otherwise, the device cannot go online.
11. Organization	12. Select the parent organization to which the camera is to be added.
13. Camera Type	14. 12 types available (Fixed Camera, PTZ Camera, Fixed HD Camera, HD PTZ Camera, In-Vehicle Camera, Uncontrollable SD Dome Camera, Uncontrollable HD Dome Camera, Isolate Video Access, Motorized Lens Camera, Ultra Clear Face Capture Camera, Multi-eye Splicing Camera, Access Control Device).
15. Max IPC Streams	16. This parameter limits the maximum number of unicast, direct-connection live video streams of the IPC in the local domain (1-51).
17. Bit Rate	18. Encoding rate.

4. Click **OK** to complete the addition.

5. (Optional) Click **Next** and fill in the optional information.

Figure 9-14 Mobile Frontend-Optional information

< Back | Add Frontend Device

Required Information — 2 Optional information (it can be skipped)

Other Info

Video device_Mobile Frontend

Longitude: Latitude:

Height: Live Video Media Service ... Auto-Adaptation

☐ Asset Info

Table 9-10 Mobile Frontend-Optional information

19. Parameter	20. Description
21. GB/T 28181 Code Rules	22. To achieve sharing between GB domains, you need to configure the GB code for the camera.
23. Camera GB Code	- Generate Automatically: Choose a rule for the ID specified in the GB/T 28181 ID data dictionary. The system generates the camera ID automatically. - Enter Manually: Follow the GB code rules. There must be 20 bits, of which bits 11-13 must be 119-129, 131, or 132.
24. Longitude	25. Longitude of the camera's location.
26. Latitude	27. Latitude of the camera's location.
28. Height	29. Height of the camera's location.
30. Live Video Media Service Policy	- Auto-Adaptation: Default setting. All MS share the load (except when the client player or decoder in the local domain adopts the Direct Connection First policy). When the forwarding capacity of the MS is insufficient, follow the policy of Direct Connection First. - You can choose whether to bypass the specified MS (group) as needed. If you need to forward multiple media streams, specify the MS (group). - This configuration takes effect only for live videos.

19. Parameter	20. Description
31. Asset Information	32. (Optional) If checked, configure the asset information of the device as required. Asset Info X * Asset ID: Please enter the asset ID. * Asset Name: Please enter the asset name. * Asset Model: Please enter the asset model. * Asset Status: Running ▼ * Warranty Period: 2025-09-10 📅 * Vendor: Please enter the vendor name. * Purchase Time: 2025-09-10 📅 * Contractor: Please enter the contractor name. * Installation Time: 2025-09-10 14:01:58 📅 * Installation Site: Please enter the installation location Maintainer: Please enter the maintainer. Service Telephone: Please enter service phone number MAC Address: Please enter the MAC address. Confirm Cancel

6. Click **OK** to complete the addition.

9.1.2 Edit Frontend Device and Channel

The GB multi-channel cameras, LAPI devices of the video devices are presented in the form of parent device + channel.

- You only need to add the parent device. The channels of IMOS cameras and LAPI devices will be obtained automatically, while the channels of GB multi-channel cameras need to be obtained by clicking **Get Resource**.
- The modification involves the parent device and the channel.

1. Edit Frontend Device

You can edit the parameters of the video devices and data devices of all protocols by editing the frontend device.

1. Click the corresponding  for the device to go to the **Edit Frontend Device** page.

Figure 9-15 Edit Frontend Device

< Back | Modify Frontend Device

1

Required Information

2

Optional information (it can be skipped)

Basic Info

* Device Name:

46

* Device ID:

77788877701321300002

* Organization:

本城

Tag Info

Tag:

☒ Video Device

Video Device

Protocol type:

GB/T 28181 Protocol

Camera Channel Type:

☒ Single-Chann...☐ Multi-channel ...

Camera Type:

PTZ Camera

Camera subtype:

Common Camera

Camera GB Code:

Camera Capability:

normal

* code rate(Kbps):

2048

* Max IPC Streams:

4

Stream Transmission Prot...:

TCP

TCP Type:

GB2016

TCP Direction:

IPC as Client

Playback/Download Servi...:

Auto-Adaptation

Support Direct Storage:

no

Authentication:

☐ yes☒ no

Confirm

Next

2. Edit the required information of the device, and click **OK** to save the modification.
3. (Optional) Click **Next** to edit the optional information of the device, and click **OK** to save the modification.

2. Edit Device Parameters

There is a special page for editing parameters of GB multi-channel cameras.

GB Multi-Channel Camera

1. Click the corresponding  for the GB multi-channel camera, and select **Configure Device** to configure parameters.

Figure 9-16 GB Multi-Channel Camera - Parameter Configuration

Parameter Configuration

Basic Settings

Camera name:

46

Camera ID:

77788877701321300002

Audio&Video...

Camera GB Code:

Support Direct Storag...

no

Main and Su...

Camera Capability:

normal

IP Address:

2013:192:118:4:46

OSD Parame...

Port:

5062

Camera Type:

PTZ Camera

GB/T 28181 ...

Camera subtype:

Common Camera

Protocol type:

GB

Alarm Source

Max IPC Streams:

4

NAT Config:

Without NAT

Access Resources

Stream Transmission P...

TCP

TCP Type:

GB2016

TCP Direction:

IPC as Client

code rate(Kbps):

2048

Longitude:

Latitude:

Height:

Live Video Media Serv...

Auto-Adaptation

OK

Cancel

3. Edit Channel Parameters

The channel configuration page is available to video devices of all protocols.

1. Click the corresponding  for the device or channel of each protocol, and select **Configuration > Channel Configuration** to configure parameters.

Figure 9-17 GB Single-Channel Camera

Parameter Configuration

Basic Settings

Camera name: 46 Camera ID: 77788877701321300002

Camera GB Code: Support Direct Storag... no

Camera Capability: normal IP Address: 2013:192:118:4::46

Port: 5062 Camera Type: PTZ Camera

Camera subtype: Common Camera Protocol type: GB

Max IPC Streams: 4 NAT Config: Without NAT

Stream Transmission P... TCP TCP Type: GB2016

TCP Direction: IPC as Client code rate(Kbps): 2048

Longitude: Latitude:

Height: Live Video Media Serv... Auto-Adaptation

OK Cancel

Figure 9-18 ONVIF Protocol

Parameter Configuration

Basic Settings

Camera name: onvif64z Camera ID: onvif64

Camera GB Code: Camera Capability: normal

User Name: admin Password: *****

IP Address: 2013:192:118:4::46 Port: 80

Camera Type: Fixed Camera Protocol type: ONVIF2.X

Max IPC Streams: 4 Stream Transmission P... TCP

code rate(Kbps): 2048 Longitude:

Latitude: Height:

Live Video Media Serv... Auto-Adaptation

Playback/Download S... Auto-Adaptation

OK Cancel

9.1.3 Search Frontend Device

You can search frontend devices by device type, device name, device code, and IP address.

1. Select the type of device you want to search from the **Device Type** drop-down box.

Figure 9-19 Search by Device type

Device Type: all x |

all ✓

GB

ONVIF

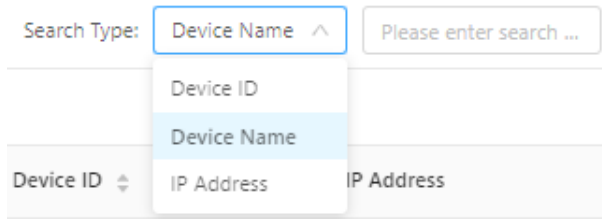
Mobile Frontend

GB Multi-channel

LAPI

2. Select the query type and enter the name/code/IP address of the device to be searched.

Figure 9-20 Query Device



3. The devices under the suborganization will be searched if **Search Sub-Organization** is enabled.
4. Click **Search** to search the devices of the selected type.

9.1.4 Configure Frontend Device

1. Storage Configuration

Click the corresponding  for the device. Under the **Configuration** menu, select **Direct Storage Configuration/Forward Storage Configuration/Backup Configuration**.

For details, see [Storage Configuration](#).

2. Video Scrambling Configuration

The video scrambling function can scramble the code stream at the front end. If there is no descrambling secret key at the back end, the video cannot be watched normally. In this way, the video security is ensured.



Note!

- Only cameras with the video scrambling capability and accessed via GB support the video scrambling function.
- For a lower-domain IPC, you need to [add a TS server](#) in the lower domain and configure [transcoding rules](#).
- The video scrambling certificate must be enabled when you need to add or edit a camera (select **Yes** for **Apply for Video Scrambling Certificate**).

1. Go to **System Management > Device Management**, and select the **Frontend Device** tab. Select the organization in the local domain. The device list on the right side shows the devices under this organization.
2. Click the corresponding  for the device, and select **Configuration > Video Scrambling Configuration** to go to the **Video Scrambling Configuration** page.

Figure 9-21 Video Scrambling Configuration

Scrambling Configuration

Enable Video Scrambling ☐ Disable ☒ Enable

Video Scrambling Mode Certificate Mode

Key Update Period 30

确认 取消

3. Configure video scrambling by referring to the table below.

Table 9-11 Parameter Description for Video Scrambling

Parameter	Description
Enable Video Scrambling	Select whether to enable the video scrambling function. If enabled, the video scrambling function can scramble the code stream at the front end. If there is no descrambling secret key at the back end, the video cannot be watched normally. In this way, the video security is ensured.
Video Scrambling Mode	Select the mode as Simple Mode/Certificate Mode. Note! The certificate mode requires the KDM9000 server.
Key Update Period	Set the period of automatic key update.

9.1.5 Delete Frontend Device

1. In the frontend device list, select the frontend device to be deleted.
2. Click **Delete**.
3. Confirm the prompt information to delete the frontend device.

Figure 9-22 Prompt

Delete selected resources.

Deleting these 2 resources will affect the existing service, synchronously delete their allocated resources, and is unrecoverable. Are you sure you want to delete them?

No.	Name	Resource Type	Acquisition device	Operation
1	HD 12	Video Camera	Not exist	
2	lapi1	Video Camera	Not exist	

Confirm Cancel

9.2 Edge Device

On the **Edge Device** page, you can add Network Video Recorders, IoT devices, and landmarks.

9.2.1 Network Video Recorder

You can add Network Video Recorders (NVRs) via the GB protocol and view the camera resources under the NVR on the management platform.

Figure 9-23 Network Video Recorder page

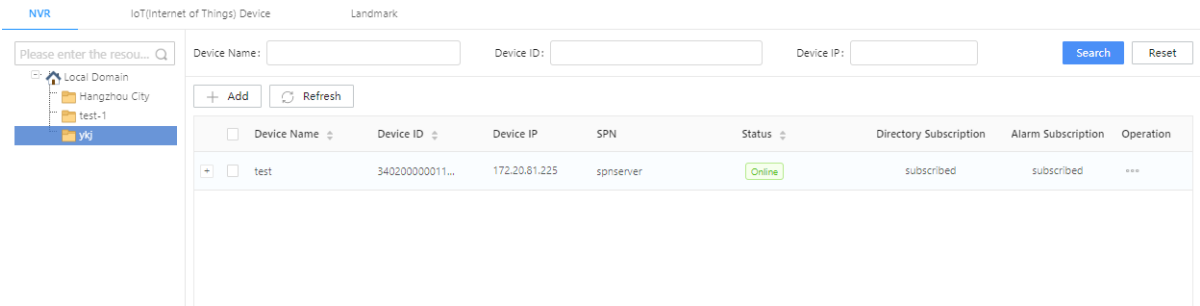
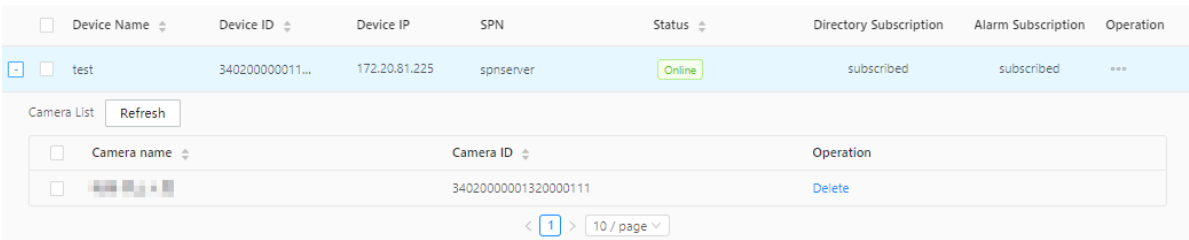


Figure 9-24 View NVR and Cameras Under It



1. Add Network Video Recorder

1. Go to **Device Management > Edge Device > Network Video Recorder**.
2. Click **Add** to go to the **Add** page, where you can configure the device parameters.

Figure 9-25 Add Page

The screenshot shows the 'Add Page' for a Network Video Recorder. It has two main sections: 'Basic Settings' and 'Advanced Settings'.
Basic Settings:
 - Device Name: [Text input field]
 - Device ID: [Text input field]
 - Stream Transmission Protocol: [Dropdown menu, currently set to 'Auto-Adaptation']
 - SPN: [Text input field]
Advanced Settings:
 - Authentication: [Radio buttons, 'no' is selected]
 - Domain Name: [Text input field]
 - NAT Config: [Dropdown menu, currently set to 'Without NAT']
 - Playback/Download Service Policy: [Dropdown menu, currently set to 'Bypass IMS']
 - Media Service Policy: [Dropdown menu, currently set to 'Auto-Adaptation']
 At the bottom, there are 'Save' and 'Cancel' buttons.

Parameter	Description
Device Name	Customize the device name of the Network Video Recorder for easy differentiation.
Device ID	Consistent with the device code of the Network Video Recorder.

Device Type	NVR
Media Stream Transmission Protocol	● Auto-Adaption: This platform can receive TCP or UDP video streams sent by the Network Video Recorders, which is determined by system negotiation. Auto-adaptation is adopted by default. ● TCP: This platform can only receive TCP video streams sent by the Network Video Recorder.
Sharing Server	Select the SPN server for the Network Video Recorder to push resources.
Enable Authentication	If authentication is enabled, the username/password of the Network Video Recorder will be authenticated.
Domain	Optional. For GB protocol authentication. If configured, it should be the same as the domain name configured on the Network Video Recorder.
NAT Configuration	Select the corresponding scenario depending on whether the Network Video Recorder and the cameras under it are in the same network with this platform.
Playback/Download Service Policy	Configure the service policy for playing back or downloading resources of the Network Video Recorder on this platform: ● Auto-Adaption: Default settings. If there is no MS available, the policy of Not Bypass MS will be followed. If there is MS available, the policy of Bypass MS First will be followed. ● Not Bypass MS: The playback/download will not bypass the MS. Note! Whether the media streams bypass the MS is determined based on multiple configurations and MS deployment. See the playback/download service selection policy in Local Configuration > Video Parameters > Advanced Configuration.
Media Service Policy	● Auto-Adaption: Default settings. Whether the video streams bypass the MS is determined by the system according to the media service selection policy of the Network Video Recorder and the MS deployment. ● Specified MS: The video streams must bypass the specified MS. ● Specified MS Group: The video streams must bypass the MS in the specified MS group. ● Not Bypass MS: The video streams do not bypass the MS. Note! When there is an MS but the MS forwarding capacity is insufficient, the policy of Not Bypass MS will be followed.

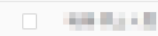
3. Click **Save**.

After the Network Video Recorder has been added, you can view the Network Video Recorder in the device list. When the device is online, the system will automatically obtain the camera resources under the Network Video Recorder.

2. View/Delete Device Resource

Click  on the left side of the Network Video Recorder to expand the list of cameras under it.

Figure 9-26 Camera List

☐	Device Name	Device ID	Device IP	SPN	Status	Directory Subscription	Alarm Subscription	Operation
	☐ test	340200000011...	172.20.81.225	spnserv	Online	subscribed	subscribed	...
Camera List Refresh								
☐	Camera name	Camera ID	Operation					
☐		34020000001320000111	Delete					
< 1 > 10 / page								

Click **Delete** corresponding to a camera to delete the camera from the list, and synchronize the deletion of the camera from the Network Video Recorder.

3. Search Device Resource

You can manually obtain camera resources under the Network Video Recorder.

1. Go to **Device Management > Edge Device > Network Video Recorder**.
2. Click **⋮** in the **Action** column of the corresponding Network Video Recorder and select **Search Device Resource** to obtain the latest device resources.

Figure 9-27 Operation Menu

☐	Device Name	Device ID	Device IP	SPN	Status	Directory Subscription	Alarm Subscription	Operation
☐	test	340200000011...	172.20.81.225	spnservr	Online	subscribed	subscribed	Configure Delete Search Device Resource Directory subscription cancelled. Alarm subscription cancelled.

4. Subscribe to Directories

Subscribe to Directories to synchronize the status and names of the camera resources under the Network Video Recorder.

Subscription Description

1. Go to **Device Management > Edge Device > Network Video Recorder**.
2. Click **⋮** in the **Action** column of the corresponding Network Video Recorder and select **Subscribe to Directories**.

Figure 9-28 Operation Menu

☐	Device Name	Device ID	Device IP	SPN	Status	Directory Subscription	Alarm Subscription	Operation
☐	test	340200000011...	172.20.81.225	spnservr	Online	subscribed	subscribed	Configure Delete Search Device Resource Directory subscription cancelled. Alarm subscription cancelled.

Cancel Subscription

To cancel the subscription to directories, select **Cancel Subscription to Directories** in the **Action** menu.

5. Subscribe to Alarms

You can subscribe to the alarms generated by the Network Video Recorder and the cameras under it.

Subscription Description

1. Go to **Device Management > Edge Device > Network Video Recorder**.
2. Click **⋮** in the **Action** column of the corresponding Network Video Recorder and select **Subscribe to Alarms**.

Cancel Subscription

To cancel the subscription to alarms, select **Cancel Subscription to Alarms** in the **Action** menu.

6. Edit Network Video Recorder

You can edit the parameters of the Network Video Recorder.

1. Go to **Device Management > Edge Device > Network Video Recorder**.

2. Click  in the **Action** column of the corresponding Network Video Recorder and select **Configuration**, or double-click the device name to go to the configuration page.
3. Edit the basic configuration parameters. See the parameter description in [Add Video Recorder](#).
4. Click **Save**.

7. Delete Network Video Recorder

1. Go to **Device Management > Edge Device > Network Video Recorder**.
2. Click  in the **Action** column of the corresponding Network Video Recorder and select **Delete**, or select the Network Video Recorder and click **Delete** at the top of the list.
3. The Network Video Recorder will be deleted after you confirm the deletion.

9.2.2 IoT Device

1. Add IoT Device

1. Go to **Device Management > Edge Device** and select the **IoT Device** tab.
2. Click **Add** to go to the **Add IoT Device** page.

AddIoT(Internet of Things) Device
×

* Device ID:

* Device Name:

* Device Type:

* Device Attribute:
☒ Fixed IOT
☐ Mobile IOT

Confirm

Cancel

3. Configure device parameters. The device ID must be consistent with the device code configured on the Web page of the device, or with the product serial number if the device code is not configured.
4. Click **OK**.

2. View Device Configuration

You can view the access resources, place configuration, and security vendor configuration of IoT devices.

- Access resources: Frontend sensors, which collect environmental information such as temperature and humidity, MAC, and RFID data. You can view the code, name, status, and other information of the access resources. Access resources can be added and configured on the Web page of the device.
- Place configuration: Location of the device, including the place code, place name, latitude, and longitude. It is automatically reported by the device and can also be configured on the Web page of the device.
- Security vendor configuration: View the organization code, vendor name, address, contact person, phone number, e-mail, and other information of the vendor. You can configure it on the Web page of the device.

Click the corresponding  for the IoT device, and select **View Configuration Information**.

Figure 9-29 View Configuration Information

☒	Device Name	Resource Type	IoT Device ID
☐	Q1	DAE2000	Q1
☒	Q2	DAE2000	Q2

View Resource Information

View Configuration Information

Delete

9.2.3 Landmark

A landmark is a positioning device that can obtain the exact location of RFID cards.

1. Add Landmark

1. Go to **Device Management > Edge Device** and select the **Landmark** tab.
2. Click **Add** to go to the **Add Landmark** page.

Figure 9-30 Add Landmark

AddLandmark ×

* Device ID:

Please Enter Device ID

* Device Name:

Please Enter Device Name

Longitude:

Please Enter Longitude

Latitude:

Please Enter Latitude

Confirm

Cancel

3. Configure device parameters and click **OK**.

2. Edit Landmark

1. Click  corresponding to the landmark to go to the **Edit Landmark** page.
2. Click **Add**.

Figure 9-31 Edit Landmark

editLandmark ×

* Device ID:

D1

* Device Name:

D1

Longitude:

68

Latitude:

35

Confirm

Cancel

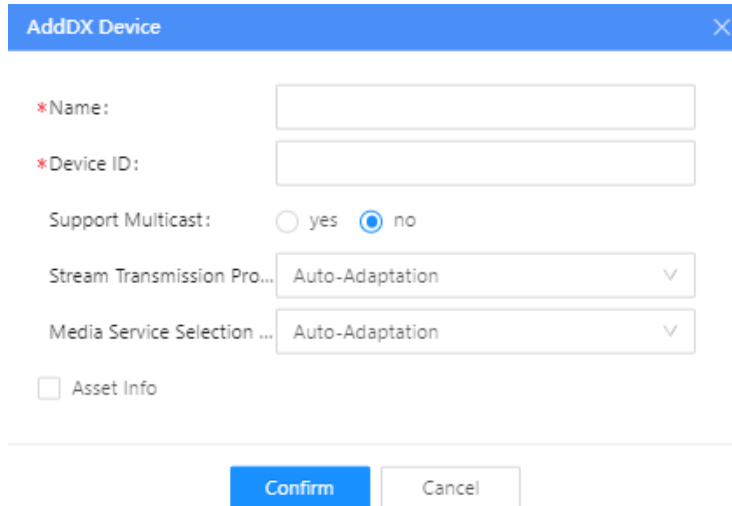
3. Edit the device name, longitude, or latitude, and click **OK** to save the modification.

9.3 Terminal Device

9.3.1 DX Device

1. Add DX Device

1. Go to **Device Management > Terminal Device > DX Device**.
2. Click to select an organization for the DX device in the local domain.
3. Click **Add**. A page as shown below appears.



4. Configure the DX device by referring to the table below.

Table 9-12 Parameter Descriptions for Adding a DX Device

Parameter	Description
Name	Name of the DX device.
Device ID	ID of the DX device.
Enable Multicast	Choose whether the device supports multicast.
Stream Transmission Protocol	● Auto-Adaptation: The client can receive live video streams transmitted by UDP or TCP, and the protocol is determined by the system through automatic negotiation. The default is Auto-Adaptation. ● TCP: The client only receives live video streams transmitted by TCP.
Media Service Selection Policy	● Auto-Adaptation: (default) Whether live video streams are transmitted via MS are determined by the system according to the media service selection policy configured on the encoding device or the external domain and whether MS is deployed. ● Direct Connection First ➢ For local-domain cameras, live video streams are not forwarded via MS unless the following conditions are met in the local domain: 1. Direct connections has exceeded the maximum number. 2. MS is deployed. 3. Encoders or IPCs allow forwarding via MS. ➢ For external-domain cameras, if the maximum number of direct connections is not reached in the local domain or the child/peer domain, live video streams will be transmitted directly; otherwise, live video streams will be forwarded via MS (if deployed in the local domain). Note: Direct Connection First is adopted when these conditions are met: 1. MS is deployed but its forwarding capacity is insufficient. 2. The encoding device or the external domain adopts Auto-Adaptation as the media service selection policy.

2. Channel Configuration

The DX device has three types of channels:

- Input sub system: Channel of video input board.
- Output sub system: Channel of video output board.
- Serial port configuration: Configured for device maintenance or for transparent data transmission with third-party device.

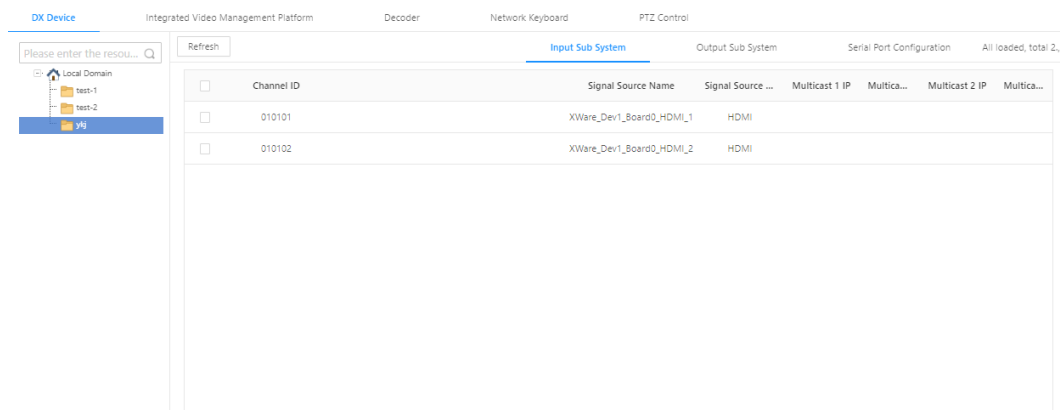


NOTE!

- The displayed parameters may vary with device type.
- The parameters that are grayed out cannot be configured.

(1) Input Sub System

1. Click the corresponding  for the DX device, choose **Channel Configuration**. A page as shown below appears.



2. Click the **Input Sub System** tab, choose the channel you want to configure. Click the corresponding . A page as shown below appears.

Channel Configuration

* Signal Source Name:

XWare_Dev1_Board0_HDMI_1

* Signal Source ID:

xwareeee-cam-01

Multicast Configuration

Multicast 1 IP:

Multicast 1 Port:

Multicast 2 IP:

Multicast 2 Port:

Audio Configuration

Sound Track:

Stereo

Audio Encoding:

G.711U

Sampling Rate:

8000

Audio Bitrate:

64Kb

Confirm

Cancel

3. Configure the channel by referring to the table below.

Table 9-13 Parameter Description for Channel Configuration

Type	Parameter	Description
Basic Settings	Signal Source Name	Name of the input signal source connected to the channel.
	Signal Source ID	ID of the input signal source connected to the channel.
Multicast Configuration	Multicast IP	IP address of the multicast group for audio & video streams. Note: Multicast IP address is valid only when the IPC supports multicast. The combination of the multicast IP address and port number must be unique in the network. To avoid conflict, it is recommended to set the multicast address within this range: 224.0.1.0 to 239.255.255.255. The IP addresses and port numbers of multicast 1 and multicast 2 cannot be identical; otherwise, conflict will occur.
	Multicast Port	Port number of the multicast group for audio & video streams.
Audio Configuration	Sound Track	Sound track information of the signal source.
	Audio Encoding	Audio compression format of the signal source. Note: AAC-LC is recommended for good sound quality if the environment is noisy.
	Sampling Rate	Audio sampling rate of the signal source.
	Audio Bitrate	Audio bit rate of the signal source.
	Mute	Whether to mute sound. Sound is not muted by default.

Type	Parameter	Description
		Note: When Mute is enabled, encoding will not include audio data, and which will improve device performance to a certain extent.
	Input Gain	Audio input gain of the signal source. The greater the value, the greater the sound volume.
Video Configuration	Brightness	Image brightness.
	Contrast	Image contrast.
	Saturation	Image saturation.
	Hue	Image hue.
	Tampering Detection Alarm	Whether to enable tampering detection alarm for the channel.
	Motion Detection Alarm	Whether to enable motion detection alarm for the channel.
Streaming Media Configuration	Media Service Selection Policy	Auto-Adaptation: Default setting. All MS share the load (except when the client player or decoder in the local domain adopts the Direct Connection First policy). Note: If MS is deployed but has insufficient forwarding capability, then Direct Connection First will be adopted. Specified MS: Specify an MS to provide service. Bypass MS: Live video streams from the IPC will not be forwarded via the MS in the local domain.
EDID Configuration	EDID	Click Browse to select the EDID configuration file and upload.
Main Stream	Enable	Whether to enable the stream.
	Encoding Format	Keep the encoding format consistent with that configured for the main or sub stream in the stream profile.
	Stream Encoding Mode	● CBR: The device transmits data at a constant bit rate. ● VBR: The device adjusts bit rate dynamically according to image quality. Note: When set to CBR, if the IPC has enabled auto-adaptation, the bit rate will still be adjusted dynamically according to image quality.
	Frame Rate	Image frame rate. Unit: FPS (frame/second).
	Priority	Default: Smoothness Priority Note: Smoothness Priority: Give priority to video fluency, and may compromise image details in complex scenes. Clarity Priority: Give priority to image clarity, and may compromise image frame rate (smoothness) in complex scenes.
	Resolution	Image resolution.
	Bit Rate	Encoding rate. Note: When the encoding format is H.264, H.265, MPEG2, or MPEG4, the bit rate unit is kbps. When the encoding format is MJPEG, the bit rate unit is MBytes/frame.
	Image Quality	1 to 9 (high to low).
	I Frame Interval	Set I frame interval. 25 is recommended.

Type	Parameter	Description	
		Note: The greater the I frame interval, the longer the interval between cameras during camera sequence.	
	GOP Mode	Configure GOP structure parameters. Note: The values vary with device model. Please set appropriately.	
	Smoothing	Whether to enable video smoothing. Note: In poor network environment, enabling video smoothing can improve video fluency with certain delay.	
Sub Stream	Enable	Whether to enable the stream.	
	Encoding Format	Keep the encoding format consistent with that configured for the main or sub stream in the stream profile.	
	Stream Encoding Mode	● CBR: The device transmits data at a constant bit rate. ● VBR: The device adjusts bit rate dynamically according to image quality. Note: When set to CBR, if the IPC has enabled auto-adaptation, the bit rate will still be adjusted dynamically according to image quality.	
	Frame Rate	Image frame rate. Unit: FPS (frame/second).	
	Priority	Default: Smoothness Priority Note: Smoothness Priority: Give priority to video fluency, and may compromise image details in complex scenes. Clarity Priority: Give priority to image clarity, and may compromise image frame rate (smoothness) in complex scenes.	
	Resolution	Image resolution.	
	Bit Rate	Encoding rate Note: When the encoding format is H.264, H.265, MPEG2, or MPEG4, the bit rate unit is kbps. When the encoding format is MJPEG, the bit rate unit is MBytes/frame.	
	Image Quality	1 to 9 (high to low).	
	I Frame Interval	Set I frame interval. 25 is recommended. Note: The greater the I frame interval, the longer the interval between cameras during camera sequence.	
	GOP Mode	Configure GOP structure parameters. Note: The values vary with device model. Please set appropriately.	
	Smoothing	Whether to enable video smoothing. Note: In poor network environment, enabling video smoothing can improve video fluency with certain delay.	
OSD Configuration	Time OSD	Show time OSD	Whether to display time information on the screen.
		Date Format	Date display format.
	Site Name OSD	Show Site Name OSD1	Whether to display site name information on the screen.

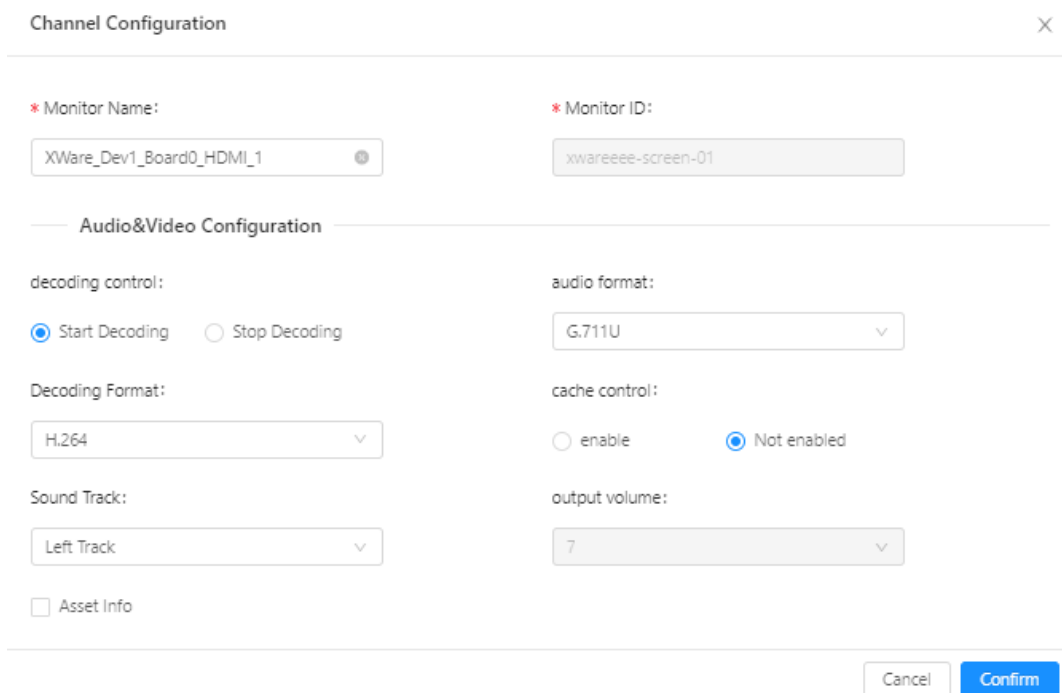
Type	Parameter	Description	
		Site Name	Site name OSD information.

4. Click **OK**.

(2) Output Sub System

1. Click the corresponding  for the DX device, choose **Channel Configuration**. A page as shown below appears.

2. Click the **Output Sub System** tab, choose the channel you want to configure. Click the corresponding . A page as shown below appears.



Channel Configuration X

* Monitor Name: XWare_Dev1_Board0_HDMI_1

* Monitor ID: xwareeee-screen-01

Audio&Video Configuration

decoding control:
☒ Start Decoding ☐ Stop Decoding

Decoding Format:
H.264

Sound Track:
Left Track

audio format:
G.711U

cache control:
☐ enable ☒ Not enabled

output volume:
7

☐ Asset Info

Cancel Confirm

3. Configure the channel by referring to the table below.

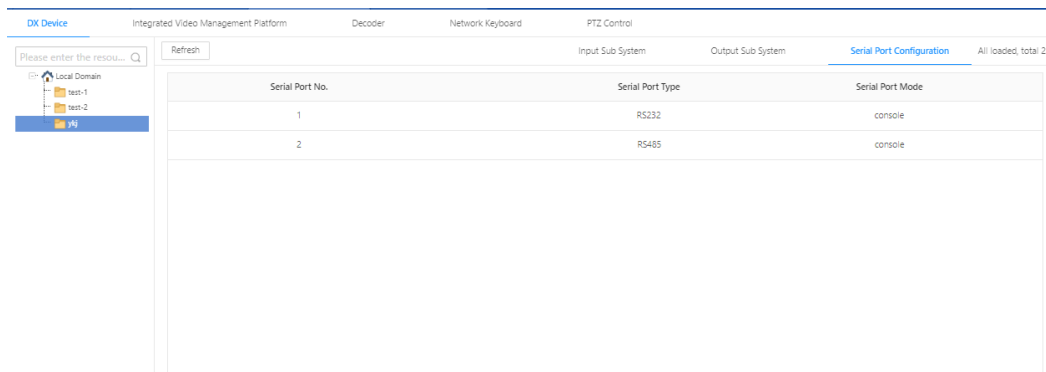
Table 9-14 Parameter Description for Output Sub System Channel Configuration

Category	Parameter	Description
Basic Settings	Monitor Name	Name of the monitor connected to the channel.
	Monitor ID	ID of the monitor connected to the channel.

Category	Parameter	Description
Audio&Video Configuration	Enable Decoding	Whether to enable decoding. By default it is enabled. Note: The channel stops live video when decoding is stopped.
	Audio Format	Select the audio output format.
	Decoding Format	Select the video decoding format.
	Cache Control	Whether to enable cache.
	Sound Track	Sound track information of the IPC.
	Output Volume	Select the output volume.

(3) Serial Port Configuration

1. Click the corresponding  for the DX device, choose **Channel Configuration**. A page as shown below appears.



2. Click the **Serial Port Configuration** tab, choose the channel you want to configure. Click the corresponding  for the channel. A page as shown below appears.

Serial Port Configuration

Serial Port Type:

RS232

Serial Port Mode:

console

Baud Rate:

9600

data bit:

8

stop bit:

1

Check digit:

None

flow control:

None

Confirm

Cancel

3. Configure the serial port by referring to the table below.

Table 9-15 Parameter Description for Serial Port Configuration

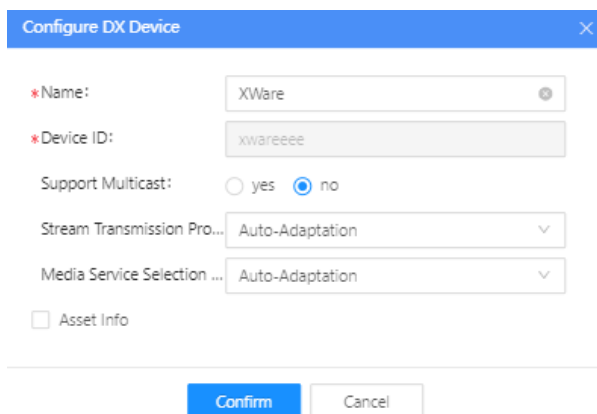
Parameter	Description
Serial Port Type	● RS232: Mainly used for device maintenance, such as connecting to a PC. ● RS422 or RS485: Mainly used for connecting external devices, such as a PTZ camera.

Parameter	Description
	Note: The type value is determined by the device model.
Serial Port Mode	● PTZ Control: Used to control a PTZ camera through the RS485 or RS485/422 serial port. ● Transparent Channel: Used for transparent transmission of data with a third-party device through the RS485 or RS485/422 serial port. ● Console: Used for device maintenance through the RS232 serial port.
Baud Rate	Baud rate of the serial port. The default is 9600. Note: Make sure the baud rate is consistent with that of the connected external device.
Data Bit	Data bit of communication through the serial port. The default is 8.
Stop Bit	Means how many bits are used to indicate the end of the data. The default is 1.
Check Digit	Method for verifying data transmitted through the serial port. The default is None.
Flow Control	Method for controlling the flow of data through the serial port. The default is None.

3. Manage DX Device

(1) Edit DX Device

1. Click the corresponding . A page as shown below appears.



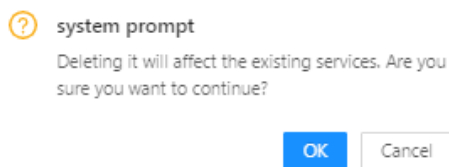
The dialog box titled "Configure DX Device" contains the following fields and controls:

- Name:** Text input field with "XWare" entered.
- Device ID:** Text input field with "xwareeee" entered.
- Support Multicast:** Radio buttons for "yes" and "no", with "no" selected.
- Stream Transmission Pro...:** Dropdown menu with "Auto-Adaptation" selected.
- Media Service Selection ...:** Dropdown menu with "Auto-Adaptation" selected.
- Asset Info:** A checkbox that is currently unchecked.
- Buttons:** "Confirm" (blue) and "Cancel" (grey) buttons at the bottom.

2. Edit the DX device information, click **OK** to save the changes.

(2) Delete DX Device

Click the corresponding  for the device, choose **Delete**, and then confirm the deletion.



The "system prompt" dialog box contains the following text and controls:

- Text:** "Deleting it will affect the existing services. Are you sure you want to continue?"
- Buttons:** "OK" (blue) and "Cancel" (grey) buttons at the bottom.

9.3.2 Video Integrated Management Platform

1. Add Video Integrated Management Platform

1. Go to **Device Management > Terminal Device > Video Integrated Management Platform**.

- Click to select an organization for the video integrated management platform in the local domain.
- Click **Add**. A page as shown below appears.

- Configure the video integrated management platform by referring to the table below.

Table 9-16 Parameter Descriptions for Video Integrated Management Platform

Parameter	Description
Name	Name of the video integrated management platform.
Device ID	ID of video integrated management platform.
Support Multicast	Choose whether the device supports multicast.
Stream Transmission Protocol	● Auto-Adaptation: The client can receive live video streams transmitted by UDP or TCP, and the protocol is determined by the system through automatic negotiation. The default is Auto-Adaptation. ● TCP: The client only receives live video streams transmitted by TCP.
Media Service Selection Policy	● Auto-Adaptation: (default) Whether live video streams are transmitted via MS are determined by the system according to the media service selection policy configured on the encoding device or the external domain and whether MS is deployed. ● Direct Connection First ➢ For local-domain cameras, live video streams are not forwarded via MS unless the following conditions are met in the local domain: 1. Direct connections has exceeded the maximum number. 2. MS is deployed. 3. Encoders or IPCs allow forwarding via MS. ➢ For external-domain cameras, if the maximum number of direct connections is not reached in the local domain or the child/peer domain, live video streams will be transmitted directly; otherwise, live video streams will be forwarded via MS (if deployed in the local domain). Note: Direct Connection First is adopted when these conditions are met: 1. MS is deployed but its forwarding capacity is insufficient. 2. The encoding device or the external domain adopts Auto-Adaptation as the media service selection policy.

- Click **OK**.

2. Manage Video Integrated Management Platform

(1) Edit Video Integrated Management Platform

- Click the corresponding  for the device. A page as shown below appears.

Configure Integrated Video Management Platform
X

* Name:

A8

* Device ID:

12123

Support Multicast:

☒ Yes
☐ No

Stream Transmission Protocol:

Auto-Adaptation

Media Service Selection Policy:

Auto-Adaptation

☐ Asset Info

OK

Cancel

2. Edit the platform information and then click **OK**.

(2) Delete Video Integrated Management Platform

Click the corresponding  for the device, choose **Delete**, and then confirm the deletion.


system prompt

Deleting it will affect the existing services. Are you sure you want to continue?

Cancel

OK

3. Channel Configuration

There are three types of channels of video integrated management platform:

- Input sub system: Channel of video input board.
- Output sub system: Channel of video output board.
- Serial port configuration: Configured for device maintenance or for transparent data transmission with third-party device.

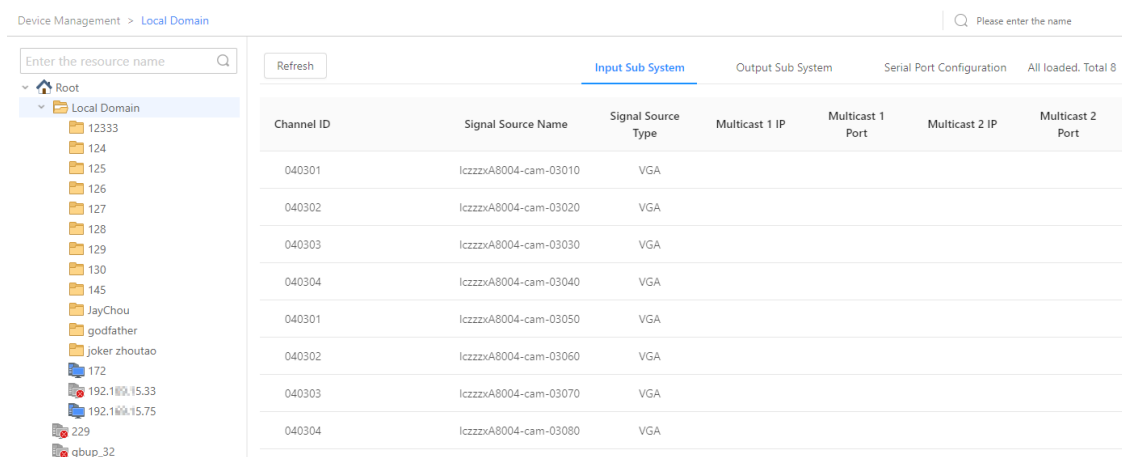


NOTE!

- The displayed parameters may vary with device type.
- The parameters that are grayed out cannot be configured.

(3) Input Sub System

1. Click the corresponding  for the video integrated management platform, choose **Channel Configuration**. A page as shown below appears.



- Click the **Input Sub System** tab, choose the channel you want to configure. Click the corresponding . A page as shown below appears.

Channel Configuration

* Signal Source Name: lczzzxA8004-cam-03030 * Signal Source ID: lczzzxA8004-cam-03030

Multicast Configuration

Multicast 1 IP: Multicast 1 Port:

Multicast 2 IP: Multicast 2 Port:

Audio Configuration

Sound Track: Stereo Audio Encoding: G.711A

Sampling Rate(kHz): 8000 Audio Bitrate: 64Kb

Mute: ☐ mute ☒ not mute Input Gain: 255

Video Configuration

Brightness: 128 Contrast: 128

Confirm Cancel

- Configure the channel by referring to the table below.

Table 9-17 Parameter Description for Channel Configuration

Type	Parameter	Description
Basic Settings	Signal Source Name	Name of the input signal source connected to the channel.
	Signal Source ID	ID of the input signal source connected to the channel.
Multicast Configuration	Multicast IP	IP address of the multicast group for audio & video streams. Note: Multicast IP address is valid only when the IPC supports multicast. The combination of the multicast IP address and port number must be unique in the network. To avoid conflict, it is recommended to set the multicast address within this range: 224.0.1.0 to 239.255.255.255. The IP addresses and port numbers of multicast 1 and multicast 2 cannot be identical; otherwise, conflict will occur.
	Multicast Port	Port number of the multicast group for audio & video streams.

Type	Parameter	Description
Audio Configuration	Sound Track	Sound track information of the signal source.
	Audio Encoding	Audio compression format of the signal source. Note: AAC-LC is recommended for good sound quality if the environment is noisy.
	Sampling Rate	Audio sampling rate of the signal source.
	Audio Bitrate	Audio bit rate of the signal source.
	Mute	Whether to mute sound. Sound is not muted by default. Note: When Mute is enabled, encoding will not include audio data, and which will improve device performance to a certain extent.
	Input Gain	Audio input gain of the signal source. The greater the value, the greater the sound volume.
Video Configuration	Brightness	Image brightness.
	Contrast	Image contrast.
	Saturation	Image saturation.
	Hue	Image hue.
	Tampering Detection Alarm	Whether to enable tampering detection alarm for the channel.
	Motion Detection Alarm	Whether to enable motion detection alarm for the channel.
Streaming Media Configuration	Media Service Selection Policy	Auto-Adaptation: Default setting. All MS share the load (except when the client player or decoder in the local domain adopts the Direct Connection First policy). Note: If MS is deployed but has insufficient forwarding capability, then Direct Connection First will be adopted. Specified MS: Specify an MS to provide service. Bypass MS: Live video streams will not be forwarded via the MS in the domain where the IPC is located.
EDID Configuration	EDID	Click Browse to select the EDID configuration file and upload.
Main Stream	Enable	Whether to enable the stream.
	Encoding format	Keep the encoding format consistent with that configured for the main or sub stream in the stream profile.
	Stream Encoding Mode	● CBR: The device transmits data at a constant bit rate. ● VBR: The device adjusts bit rate dynamically according to image quality. Note: When set to CBR, if the IPC has enabled auto-adaptation, the bit rate will still be adjusted dynamically according to image quality.
	Frame Rate	Image frame rate. Unit: FPS (frame/second).
	Priority	Default: Smoothness Priority Note: Smoothness Priority: Give priority to video fluency, and may compromise image details in complex scenes. Clarity Priority: Give priority to image clarity, and may compromise image frame rate (smoothness) in complex scenes.

Type	Parameter	Description
	Resolution	Image resolution.
	Bit Rate	Encoding rate Note: When the encoding format is H.264, H.265, MPEG2, or MPEG4, the bit rate unit is kbps. When the encoding format is MJPEG, the bit rate unit is MBytes/frame.
	Image Quality	1 to 9 (high to low).
	I Frame Interval	Set I frame interval. 25 is recommended. Note: The greater the I frame interval, the longer the interval between cameras during camera sequence.
	GOP Mode	Configure GOP structure parameters. Note: The values vary with device model. Please set appropriately.
	Smoothing	Whether to enable video smoothing. Note: In poor network environment, enabling video smoothing can improve video fluency with certain delay.
Sub Stream	Enable	Whether to enable the stream.
	Encoding Format	Keep the encoding format consistent with that configured for the main or sub stream in the stream profile.
	Stream Encoding Mode	● CBR: The device transmits data at a constant bit rate. ● VBR: The device adjusts bit rate dynamically according to image quality. Note: When set to CBR, if the IPC has enabled auto-adaptation, the bit rate will still be adjusted dynamically according to image quality.
	Frame Rate	Image frame rate. Unit: FPS (frame/second).
	Priority	Default: Smoothness Priority Note: Smoothness Priority: Give priority to video fluency, and may compromise image details in complex scenes. Clarity Priority: Give priority to image clarity, and may compromise image frame rate (smoothness) in complex scenes.
	Resolution	Image resolution.
	Bit Rate	Encoding rate. Note: When the encoding format is H.264, H.265, MPEG2, or MPEG4, the bit rate unit is kbps. When the encoding format is MJPEG, the bit rate unit is MBytes/frame.
	Image Quality	1 to 9 (high to low).
	I Frame Interval	Set I frame interval. 25 is recommended. Note: The greater the I frame interval, the longer the interval between cameras during camera sequence.
	GOP Mode	Configure GOP structure parameters. Note: The values vary with device model. Please set appropriately.

Type	Parameter	Description	
	Smoothing	Whether to enable video smoothing. Note: In poor network environment, enabling video smoothing can improve video fluency with certain delay.	
OSD Configuration	Time OSD	Show Time OSD	Whether to display time information on the screen.
		Date Format	Date display format.
	Site Name OSD	Show Site Name OSD1	Whether to display site name information on the screen.
		Site Name	Site name OSD information.

4. Click **OK**.

(4) Output Sub System

1. Click the corresponding  for the video integrated management platform, choose **Channel Configuration**. A page as shown below appears.

Device Management > Local Domain

Enter the resource name

Refresh

Input Sub System **Output Sub System** Serial Port Configuration All loaded, Total 8

Channel ID	Monitor Name
050101	lczzzx8004-screen-0101
050102	lczzzx8004-screen-0102
050101	lczzzx8004-screen-0103
050102	lczzzx8004-screen-0104
050101	lczzzx8004-screen-0105
050102	lczzzx8004-screen-0106
050101	lczzzx8004-screen-0107
050102	lczzzx8004-screen-0108

2. Click the **Output Sub System** tab, choose the channel you want to configure. Click the corresponding . A page as shown below appears.

Channel Configuration

* Monitor Name: lczzzx8004-screen-0101 * Monitor ID: lczzzx8004-screen-0101

Audio&Video Configuration

audio format: G.711A Decoding Format: H.264

cache control: ☐ Enable ☒ Not enabled Sound Track: Left Track

output volume: 7

☐ Asset Info

Confirm Cancel

3. Configure the channel by referring to the table below.

Table 9-18 Parameter Description for Output Sub System Channel Configuration

Category	Parameter	Description
Basic Settings	Monitor Name	Name of the monitor connected to the channel.
	Monitor ID	ID of the monitor connected to the channel.
Audio/Video Configuration	Enable Decoding	Whether to enable decoding. By default it is enabled. Note: The channel stops live video when decoding is stopped.
	Audio Format	Select the audio output format.
	Decoding Format	Select the video decoding format.
	Cache Control	Whether to enable cache.
	Sound Track	Sound track information of the IPC.
	Output Volume	Select the output volume.

(5) Serial port configuration

1. Click the corresponding  for the video integrated management platform, choose **Channel Configuration**. A page as shown below appears.

Device Management > Local Domain

Enter the resource name

Root

Local Domain

12333

124

125

126

127

128

129

130

145

JayChou

godfather

joker zhoutao

172

192.168.16.33

192.168.15.75

229

gbup_32

Refresh

Input Sub System

Output Sub System

Serial Port Configuration

All loaded. Total 8

Serial Port No.	Serial Port Type	Serial Port Mode
1	RS232	console
2	RS232	console
3	RS232	console
4	RS232	console
5	RS232	console
6	RS232	console
7	RS232	console
8	RS232	console

2. Click the **Serial Port Configuration** tab, choose the channel you want to configure. Click the corresponding . A page as shown below appears.

Serial Port Configuration
✕

Serial Port Type: RS232 ▼

Serial Port Mode: console ▼

Baud Rate: 9600 ▼

data bit: 8 ▼

stop bit: 1 ▼

check digit: None ▼

flow control: None ▼

OK
Cancel

3. Configure the serial port by referring to the table below.

Table 9-19 Parameter Description for Serial Port Configuration

Parameter	Description
Port Type	● RS232: Mainly used for device maintenance, such as connecting to a PC. ● RS422 or RS485: Mainly used for connecting external devices, such as a PTZ camera. Note: The type value is determined by the device model.
Serial Port Mode	● PTZ Control: Used to control a PTZ camera through the RS485 or RS485/422 serial port. ● Transparent Channel: Used for transparent transmission of data with a third-party device through the RS485 or RS485/422 serial port. ● Console: Used for device maintenance through the RS232 serial port.
Baud Rate	Baud rate of the serial port. The default is 9600. Note: Make sure the baud rate is consistent with that of the connected external device.
Data Bit	Data bit of communication through the serial port. The default is 8.
Stop Bit	Means how many bits are used to indicate the end of the data. The default is 1.
Check Bit	Method for verifying data transmitted through the serial port. The default is None.
Flow Control	Method for controlling the flow of data through the serial port. The default is None.

9.3.3 Decoder

The decoder is a device that decodes digital audio and video data streams received from the network and outputs analog audio and video signals.

1. Add Decoder

1. Go to **Device Management > Terminal Device > Decoder**.
2. Click to select an organization for the encoder in the local domain.
3. Click **Add**. A page as shown below appears.

Add Decoder

Device Type: DC1001-FF

* Name:

* Device ID:

Stream Transmission Protocol: Auto-Adaptation

Media Service Selection Policy: Auto-Adaptation

Device Password:

Correct Password:

format: PAL

Profile Type: H.264

Support Multicast: ☒ support ☐ not support

Enable Alarm: ☒ Yes ☐ No

☐ Asset Info

Confirm and Configure Channel Confirm Cancel

4. Configure the parameters by referring to the table below.

Table 9-20 Decoder Parameter Descriptions

Parameter	Description
Device Type	Select the decoder model.
Name	Enter the decoder name.
Device ID	Enter the decoder ID. Note: The ID must be consistent with the ID configured in the decoder's Web interface.
Stream Transmission Protocol	- Auto-Adaptation: The decoder can receive live video streams transmitted by UDP or TCP, and the protocol is determined by the system through automatic negotiation. This is the default setting. - TCP: The decoder only receives live video streams transmitted by TCP.
Media Service Selection Policy	- Auto-Adaptation: (default) Whether live video streams are transmitted via MS are determined by the system according to the media service selection policy configured on the encoder, IPC, or external domain, and whether MS is deployed. Note: Direct Connection First is adopted when these conditions are met: 1. MS is deployed but its forwarding capacity is insufficient. 2. The encoding device or the external domain adopts Auto-Adaptation as the media service selection policy. - Direct Connection First - For local-domain cameras, live video streams are not forwarded via MS unless the following conditions are met in the local domain: 1. Direct connections has exceeded the maximum number. 2. MS is deployed. 3. Encoders or IPCs allow forwarding via MS. - For external-domain cameras, if the maximum number of direct connections is not reached in the local domain or the child/peer domain, live video streams will be transmitted directly; otherwise, live video streams will be forwarded via MS (if deployed in the local domain).
Device Password	Reset the password of the decoder's Web interface.
Confirm Password	Confirm the password you just entered.
Mode	Choose image encoding format, PAL or NTSC . Caution: The device will restarts after you change the image encoding format.

Parameter	Description
Profile Type	Video stream decoding format.
Enable Multicast	Whether the decoder supports multicast.
Enable Alarm	Whether the decoder can receive alarms.

- Click **Confirm** and **Configure Channel** to add the decoder and go to the **Configure Decoding Channel** page. Click **OK** to finish the steps.

2. Channel Configuration

The decoder has three channel types:

- Audio & video channel: Used for audio and video decoding.
- Serial port channel: Used for device maintenance or transparent data transmission with third-party device.
- Alarm input/output channel: Used with alarm input or output devices.



NOTE!

- The displayed parameters may vary with device type.
- The parameters that are grayed out cannot be configured.

(1) Audio/Video Channel Configuration

- Click the corresponding  for the decoder, choose **Channel Configuration**. A page as shown below appears.

- Click the **A/V Channel** tab, select the channel you want to configure. Click the corresponding . A page as shown below appears.

3. Configure audio and video parameters by referring to the table below.

Table 9-21 Audio/Video Channel Parameter Configuration

Category	Parameter	Description
Basic settings	Monitor Name	Name of the monitor connected to the channel.
	Monitor ID	ID of the monitor. Note: Make sure the monitor ID is unique in the local domain.
Audio&Video Configuration	Choose template	Use the parameters in the matching DC template. Note: Make sure the DC template has been configured. To add a DC parameter template, click  . The existing channel information will be overwritten by the selected template.
	Audio Format	Audio decoding format
	Output Volume	Options: 1 to 7. The greater the value, the higher the output volume.
	Decoding Format	Keep the decoding format consistent with that configured in the stream profile. Note: For information about stream profile operations, see Add Decoder.
	Cache Control	Whether to enable cache. Default: Disabled. Note: In poor network environment, enabling cache can improve video fluency with certain delay.
	Sound Track	Information about the sound track of the decoder.
	Mute	Whether to mute sound. Sound is not muted by default. Note: If there's no audio input, mute is recommended because it will improve device performance to some extent.
	Max. Window Count	Maximum number of windows of the channel. Note: The number of windows supported by the channel may vary with decoder model. If the original multi-window setting of the channel is changed to 1-window, then service on the monitor bound to the channel will be cleared.
	Decoding Control	Whether to enable decoding. By default, it is enabled. Caution: Stop decoding will stop both audio decoding and video decoding, and the decoder will stop outputting video and audio streams.
OSD Configuration	Show Time OSD	Whether to display time information on the screen. By default, this setting is disabled. Note: SDC does not support time OSD configuration.
	Date Format	Date display format.
	Show Site Name OSD	Whether to display site name information on the screen. Note: SDC allows one site name OSD only.

Category	Parameter	Description
	Site Name 1	The first site name OSD.
	Site Name 2	The second site name OSD.
	Switching Time (s)	Time interval for switching site name OSD 1 and site name OSD 2. Note: SDC does not support this setting. If the switching time is set to 0, the site name OSDs will not switch, and only site name OSD 1 will be displayed.

4. Click **Confirm**.

(2) Serial port channel configuration

1. Click the corresponding  for the decoder, choose **Channel Configuration**. A page as shown below appears.

Device Management > Local Domain > Configure Decoding Channel Q Please enter the name

Local Domain

12333
124
125
126
127
128
129

Refresh

A/V Channel
Serial Port Channel
Alarm Input/Output Channel
All loaded. Total 2

Serial Port No.	Serial Port Type	Serial Port Mode
1	RS232	console
2	RS485	Transparent Channel

2. Click the **Serial Port Channel** tab, choose the channel you want to configure. Click the corresponding . A page as shown below appears.

Serial Port Configuration ✕

Serial Port Type: RS232

Serial Port Mode: console

Baud Rate: 9600

data bit: 8

stop bit: 1

Check digit: None

flow control: None

Confirm

Cancel

3. Configure the serial port by referring to the table below.

Table 9-22 Parameter Description for Serial Port Configuration

Parameter	Description
Serial Port Type	● RS232: Mainly used for device maintenance, such as connecting to a PC. ● RS485 or RS485/422: Mainly used for connecting an external device, for example, a third-party device, for transparent data transmission. Note: The type value is determined by the device model. For a device with multiple RS485 serial ports, the type values correspond to the RS485 prints on the device panel one by one.
Serial Port Mode	Transparent Channel: Used for transparent transmission of data with a third-party device through the RS485 or RS485/422 serial port. Console: Used for device maintenance through the RS232 serial port.
Baud Rate	Baud rate of the serial port. Note: Make sure the baud rate is consistent with that of the connected external device.
Data Bit	Data bit of communication through the serial port. The default is 8.
Stop Bit	Means how many bits are used to indicate the end of the data. The default is 1.
Check Bit	Method for verifying data transmitted through the serial port. The default is None.
Flow Control	Method for controlling the flow of data through the serial port. The default is None.

4. Click **OK**.

(3) Alarm Input/Output Channel Configuration

1. Click the corresponding  for the decoder, choose **Channel Configuration**. A page as shown below appears.

Refresh

A/V Channel

Serial Port Channel

Alarm Input/Output Channel

All loaded. Total 2

Alarm Input/Output Index	Input/Output Type	Status	Status
1	Input	Normally open	☐ Disable
1	Output	Normally open	☐ Disable

2. Click the **Alarm Input/Output Channel** tab, select the channel you want to configure. Click the corresponding . A page as shown below appears.

Alarm Input/Output Configuration

✕

* Alarm Name:

Status:

Normally open

▼

Whether to enable

☐ Yes

☒ No

Confirm

Cancel

3. Configure the parameters by referring to the table below.

Table 9-23 Parameter Description for Alarm Input/Output Configuration

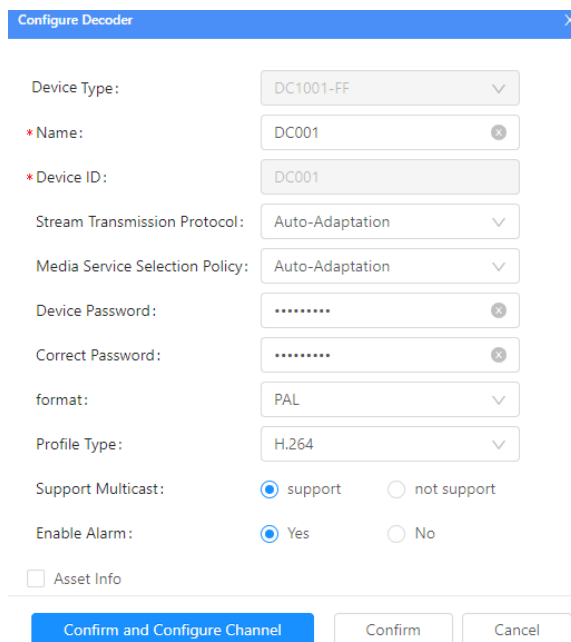
Parameter	Description
Alarm Name	Alarm input name.
Status	Set the status according to the connected third-party alarm input device. For example, if the third-party alarm input device is normally open, then the status here must be set to normally open (N.O.), so the decoder can properly receive alarm information.
Whether to enable	Whether to enable the alarm input.

4. Click **Confirm**.

3. Manage Decoder

(4) Edit Decoder Configuration

1. Click the corresponding  for the decoder. A page as shown below appears.



2. Edit the settings (**Device Type** and **Device ID** cannot be changed).

3. Click **Confirm** and **Configure Channel** or click **Confirm**.

(5) Reboot Device.

Click the corresponding  for the decoder, choose **Reboot Device**, and then confirm to restart the device immediately.

(6) Delete Device

Click the corresponding  for the decoder, choose **Delete Device**, and confirm to delete the device immediately.

 system prompt

Are you sure you want to delete the device?

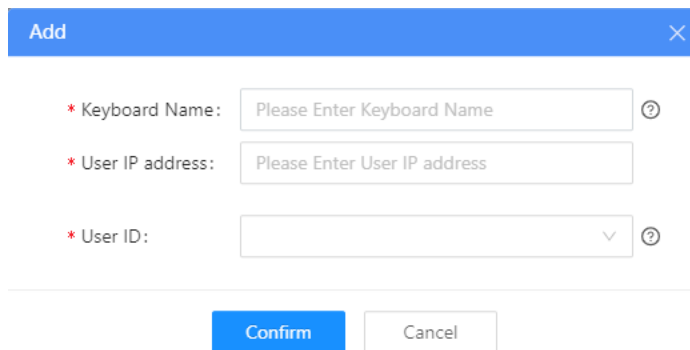
Cancel OK

9.3.4 Network Keyboard

The network keyboard is used to control the PTZ camera. It provides basic functions such as direction change, zoom, and focus. It also supports live video on video wall.

1. Add Network Keyboard

1. Go to **Device Management > Terminal Device > Network Keyboard**.
2. Click **Add** to go to the **Add Network Keyboard** page.



3. Configure the network keyboard by referring to the table below.

Table 9-24 Parameter Description for Network Keyboard

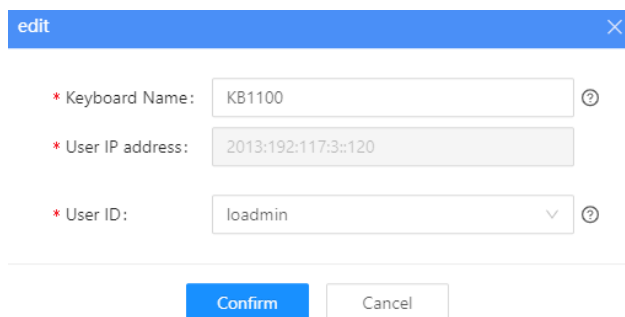
Parameter	Description
Keyboard Name	Name of the keyboard.
IP Address of Keyboard User	IP address of the keyboard. Note! The IP address is the same as the IP address configured for the keyboard.
User ID	User to whom the keyboard is bound. After successful binding, the keyboard has the user's privileges. Note! If you do not add a keyboard to the VM, but use the keyboard for direct control, the keyboard will obtain the loadadmin user's privileges by default.

4. Click **OK** to complete the addition.

2. Edit Network Keyboard

1. Click  corresponding to the network keyboard to go to the **Edit Network Keyboard** page.

Figure 9-32 Edit Network Keyboard



2. Edit the network keyboard information, and click **OK** to save the modification.

3. Export Network Keyboard

1. Go to the **Network Keyboard** page.

2. Select the network keyboard and click **Export**. Select **Export Selected** to export the information of the selected network keyboard to an Excel file.
3. Click **Export** and select **Export All** to export the information of all network keyboards to an Excel file.

Figure 9-33 Export Network Keyboard

DX Device	Integrated Video Management Platform	Decoder	Network Keyboard	PTZ Controller
Network Keyboard	+ Add Delete Export Refresh			
Keyboard Control Configuration	Keyboard Name User IP address User ID Operation			
	KB1100 2013:192:117:3::120 loadadmin			

4. Delete Network Keyboard

Click  corresponding to the device and confirm to delete the device.

5. Keyboard Control Configuration

Go to **Device Management > Terminal Device > Network Keyboard**, and select the **Keyboard Control Configuration** tab.

Figure 9-34 Keyboard Control Configuration

DX Device	Integrated Video Management Platform	Decoder	Network Keyboard	PTZ Controller
Network Keyboard	Camera control relationship Monitor control relationship Decode the camera sequence resource control relationship			
Keyboard Control Configuration	+ Add Delete Batch Configuration Export Refresh			
	Keyboard control number Camera ID Operation			

(1) Camera Control Relationship

When you want to control a camera with the keyboard, you need to set the relationship between the keyboard control number and the camera code: one keyboard number corresponds to one camera.

Add Camera Control Relationship

1. Go to the Camera Control Relationship tab.
2. Click **Add** to go to the **Add Camera Control Relationship** page.

Figure 9-35 Add Camera Control Relationship

Add

Keyboard control number	Camera name	Camera ID	Operation
888	46	77788877701321300002	
999	onvif54z	onvif54	

Add

Confirm

Cancel

3. Enter the keyboard control ID. After you enter the camera name, the corresponding camera code will be automatically filled in. You can click **Add** to add more relationships.
4. Click **OK** to complete adding the camera control relationship.



Note!

- The keyboard control ID can only contain numbers. The camera code is the code of the camera to be controlled by the user.
- One keypad control ID can only correspond to one camera code.

Edit Camera Control Relationship

1. Click  for the added camera control relationship to go to the **Edit** page.

Figure 9-36 Edit Camera Control Relationship

2. Edit the camera code, and click **OK** to complete the modification.

Batch Configure Camera Control Relationships

1. Click **Batch Configure** to go to the **Batch Configure Camera Control Relationships** page.

Figure 9-37 Batch Configure Camera Control Relationships

2. Click **Download Camera Control Relationship Import Template**, enter the keyboard control IDs and camera codes in batches in the downloaded Excel file, and save the configuration.
3. Click **Upload File**, select the completed Excel file, and click **Start Import** to complete the batch addition of camera control relationships.

Export All/Export Selected Camera Control Relationships

1. Select multiple camera control relationships and click **Export Selected** to export the selected camera control relationships.

Figure 9-38 Export Selected

Keyboard control number	camera ID	Operation
888	77788877701321300002	
999	onvif64	

2. Click **Export All** to export all camera relationships.

Delete Camera Control Relationship

1. Select multiple camera control relationships and click **Delete** to delete the selected camera control relationships.
2. You can click  after a camera control relationship to delete the camera control relationship.

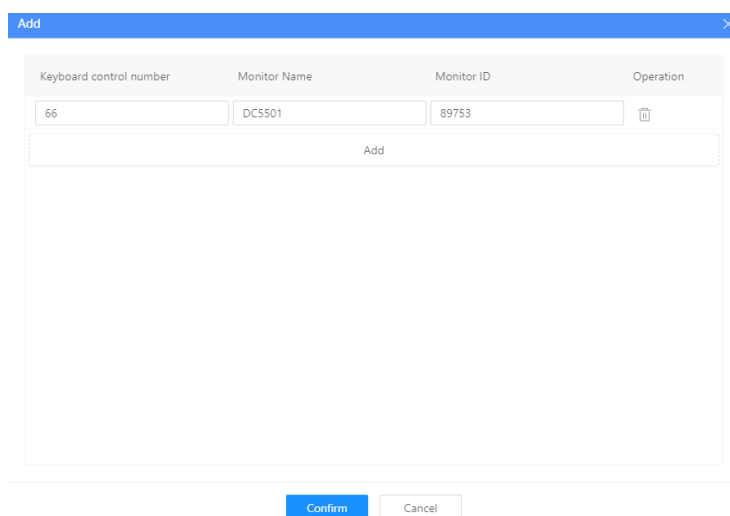
(2) Monitor Control Relationship

To control a monitor with the keyboard, you need to set the correspondence between the keyboard control ID and the monitor code. One keyboard ID corresponds to one monitor.

Add Monitor Control Relationship

1. Go to the **Monitor Control Relationship** tab.
2. Click **Add** to go to the **Add Monitor Control Relationship** page.

Figure 9-39 Add Monitor Control Relationship



Keyboard control number	Monitor Name	Monitor ID	Operation
66	DC5501	89753	

Add

Confirm Cancel

3. Enter the keyboard control ID, monitor name, and monitor code, and click **Add** to add more relationships.
4. Click **OK** to complete the addition of monitor control relationships.



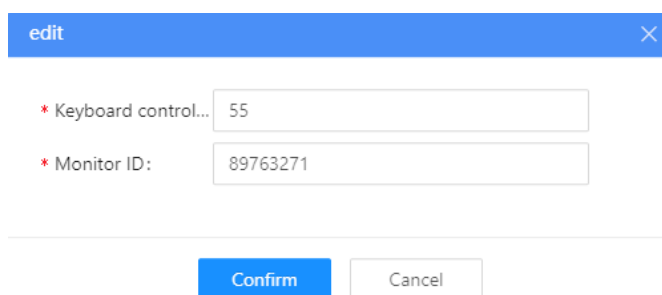
Note!

- The keyboard control ID can only contain numbers. The monitor code is the code of the monitor to be controlled by the user.
- One keypad control ID can only correspond to one monitor code.

Edit Monitor Control Relationship

1. Click  for the added monitor control relationship to go to the **Edit** page.

Figure 9-40 Edit Monitor Control Relationship



* Keyboard control... 55

* Monitor ID: 89763271

Confirm Cancel

2. Edit the monitor code, and click **OK** to complete the modification.

Batch Configure Monitor Control Relationships

1. Click **Batch Configure** to go to the **Batch Configure Monitor Control Relationships** page.

Figure 9-41 Batch Configure Monitor Control Relationships

Import Data ✕

1. Please prepare the data to import according to the template format.

[DownloadMonitor control relationshipimport template](#)

2. Please select the file to import.

Upload File

Must be .xls or .xlsx file, and the maximum file size is 10MB.

Start import

Cancel

2. Click **Download Monitor Control Relationship Import Template**, enter the keyboard control IDs and camera codes in batches in the downloaded Excel file, and save the configuration.
3. Click **Upload File**, select the completed Excel file, and click **Start Import** to complete the batch addition of monitor control relationships.

Export All/Export Selected Monitor Control Relationships

1. Select multiple monitor control relationships and click **Export Selected** to export the selected monitor control relationships.

Figure 9-42 Export Selected

< Camera control relationship

Monitor control relationship

Decode the camera sequence resource control relationship

+ Add

Delete

Batch Configuration

Export ▼

Refresh

☒	Keyboard control number	Monitor ID	Operation
☒	55	89763271	
☒	66	89753	

2. Click **Export All** to export all monitor control relationships.

Delete Monitor Control Relationship

1. Select multiple monitor control relationships and click **Delete** to delete the selected monitor control relationships.
2. You can click after a monitor control relationship to delete the monitor control relationship.

(3) Decoding Camera Sequence Resource Control Relationship

To use the keyboard to control the playback of the camera sequence resources on the DC video wall, you need to configure the monitor control relationship and set the correspondence between the monitor ID and the camera sequence resource name. One keyboard ID corresponds to one monitor, and one monitor corresponds to one camera sequence resource.

Add Decoding Camera Sequence Resource Control Relationship

1. Go to the **Decoding Camera Sequence Resource Control Relationship** tab.
2. Click **Add** to go to the **Add Decoding Camera Sequence Resource Control Relationship** page.

Figure 9-43 Add Decoding Camera Sequence Resource Control Relationship

The 'Add' dialog box contains a table with the following columns: Monitor ID, Monitor Pane, Camera Sequence Resource Name, and Operation. The first row has the values '1', '1', 'Seq1', and a trash icon. Below the table is an 'Add' button. At the bottom of the dialog are 'Confirm' and 'Cancel' buttons.

Monitor ID	Monitor Pane	Camera Sequence Resource Name	Operation
1	1	Seq1	

Add

Confirm Cancel

3. Enter the monitor ID, monitor pane, and camera sequence resource name, and click **Add** to add more relationships.
4. Click **OK** to complete the addition of the decoding camera sequence resource control relationship.

Edit Decoding Camera Sequence Resource Control Relationship

1. Click for the added decoding camera sequence resource control relationship to go to the **Edit** page.

Figure 9-44 Edit Decoding Camera Sequence Resource Control Relationship

The 'edit' dialog box contains three input fields: Monitor ID (value: 1), Monitor Pane (value: 1), and Camera Sequenc... (value: 7873626758191251457). At the bottom are 'Confirm' and 'Cancel' buttons.

* Monitor ID: 1

* Monitor Pane: 1

* Camera Sequenc... 7873626758191251457

Confirm Cancel

2. Edit the monitor ID, monitor pane, and camera sequence resource ID, and click **OK** to complete the modification.

Batch Configure Decoding Camera Sequence Resource Control Relationships

1. Click **Batch Configure** to go to the **Batch Configure Decoding Camera Sequence Resource Control Relationships** page.

Figure 9-45 Batch Configure Decoding Camera Sequence Resource Control Relationships

The 'Import Data' dialog box contains two instructions: 'Please prepare the data to import according to the template format.' and 'Please select the file to import.' Below the first instruction is a link to download a template. Below the second instruction is an 'Upload File' button. At the bottom are 'Start import' and 'Cancel' buttons.

1. Please prepare the data to import according to the template format.

[DownloadDecode the camera sequence resource control relationshipimport template](#)

2. Please select the file to import.

Upload File Must be .xls or .xlsx file, and the maximum file size is 10MB.

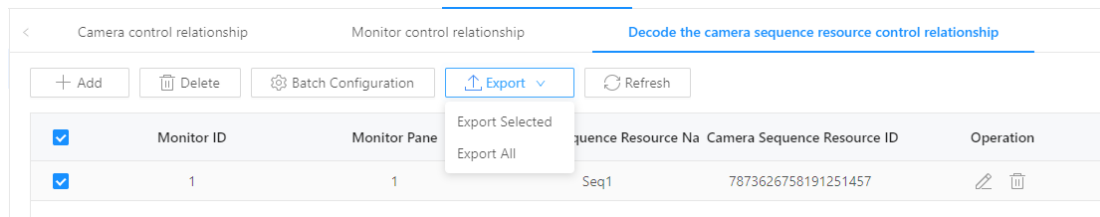
Start import Cancel

2. Click **Download Decoding Camera Sequence Resource Control Relationship Import Template**, enter the monitor ID, monitor pane, and camera sequence resource name in batches in the downloaded Excel file, and save the configuration.
3. Click **Upload File**, select the completed Excel file, and click **Start Import** to complete batch addition of decoding camera sequence resource control relationships.

Export All/Export Selected Decoding Camera Sequence Resource Control Relationships

1. Select multiple decoding camera sequence resource control relationships and click **Export Selected** to export the selected decoding camera sequence resource control relationships.

Figure 9-46 Export Selected



2. Click **Export All** to export all decoding camera sequence resource control relationships.

Delete Decoding Camera Sequence Resource Control Relationship

1. Select multiple decoding camera sequence resource control relationships and click **Delete** to delete the selected decoding camera sequence resource control relationships.
2. You can click after a decoding camera sequence resource control relationship to delete the decoding camera sequence resource control relationship.

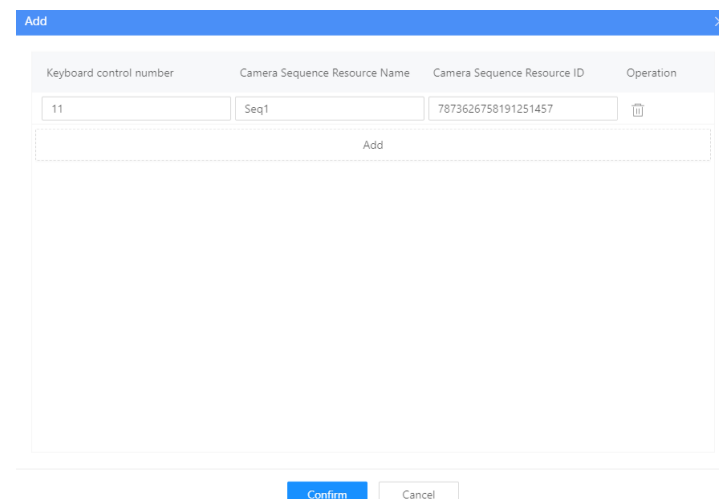
(4) Splicing Control Camera Sequence Resource Control Relationship

To use the keyboard to control the playback of the camera sequence resources on the decoded splicing control video wall, you need to set the correspondence between the keyboard control ID and the camera sequence resource. One keyboard ID corresponds to one camera sequence resource.

Add Splicing Control Camera Sequence Resource Control Relationship

1. Go to the **Splicing Control Camera Sequence Resource Control Relationship** tab.
2. Click **Add** to go to the **Add Splicing Control Camera Sequence Resource Control Relationship** page.

Figure 9-47 Add Splicing Control Camera Sequence Resource Control Relationship

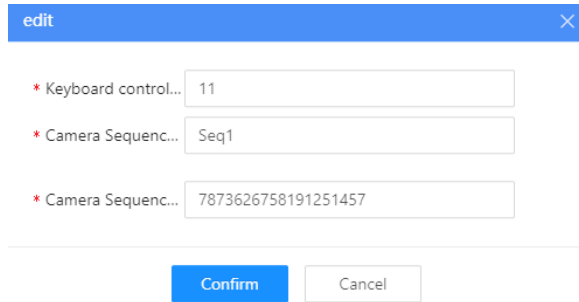


3. Enter the keyboard control ID, camera sequence resource name, and camera sequence resource code, and click **Add** to add more relationships.
4. Click **OK** to complete the addition of the splicing control camera sequence resource control relationship.

Edit Splicing Control Camera Sequence Resource Control Relationship

1. Click  for the added splicing control camera sequence resource control relationship to go to the **Edit** page.

Figure 9-48 Edit Splicing Control Camera Sequence Resource Control Relationship

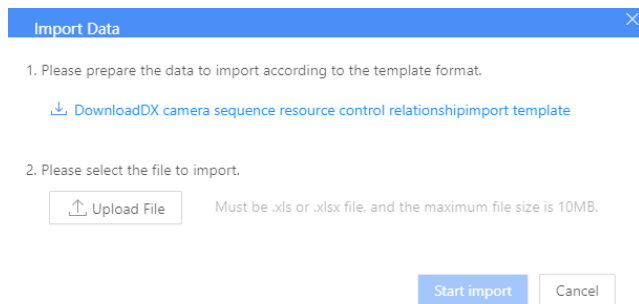


2. Edit the keyboard control ID, camera sequence resource name, and camera sequence resource code, and click **OK** to complete the modification.

Batch Configure Splicing Control Camera Sequence Resource Control Relationships

1. Click **Batch Configure** to go to the **Batch Configure Splicing Control Camera Sequence Resource Control Relationships** page.

Figure 9-49 Batch Configure Splicing Control Camera Sequence Resource Control Relationships

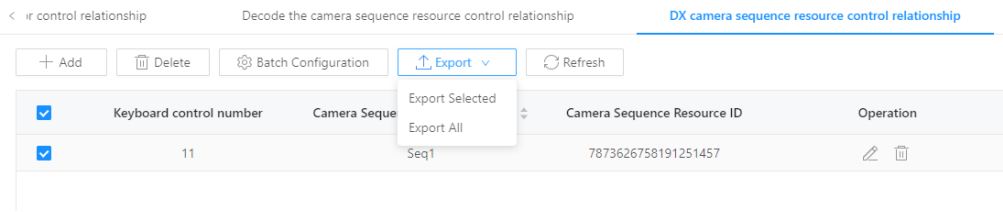


2. Click **Download Splicing Control Camera Sequence Resource Control Relationship Import Template**, enter the keyboard control IDs, camera sequence resource names, and camera sequence resource codes in batches in the downloaded Excel file, and save the configuration.
3. Click **Upload File**, select the completed Excel file, and click **Start Import** to complete batch addition of splicing control camera sequence resource control relationships.

Export All/Export Selected Splicing Control Camera Sequence Resource Control Relationships

1. Select multiple splicing control camera sequence resource control relationships and click **Export Selected** to export the selected splicing control camera sequence resource control relationships.

Figure 9-50 Export Selected



2. Click **Export All** to export all splicing control camera sequence resource control relationships.

Delete Splicing Control Camera Sequence Resource Control Relationship

1. Select multiple splicing control camera sequence resource control relationships and click **Delete** to delete the selected splicing control camera sequence resource control relationships.
2. You can click after a splicing control camera sequence resource control relationship to delete the splicing control camera sequence resource control relationship.

9.3.5 PTZ Control

A PTZ control is used to perform PTZ control for some non-PTZ cameras.

1. Add PTZ Control

1. Go to **Device Management > Terminal Device > PTZ Control**.
2. Select the organization to add the PTZ control in the local domain.
3. Click **Add** to go to the **Add PTZ Control** page.

Figure 9-51 Add PTZ Control

Add
×

* Device Type:

PTZ Controller

* Device ID:

Please Enter Device ID

* Device Name:

Please Enter Device Name

IP Address:

Please Enter IP Address

Port:

Please Enter Port

Service Management...

Please Enter Service Management URL

Device Extended Info...

Please Enter Device Extended Info

Confirm

Cancel

4. Configure PTZ control by referring to the table below.

Table 9-25 Parameter Description for Decoded Splicing Control Devices

Parameter	Description
Device Type	PTZ Control
Device ID	Enter the code of the PTZ control.
Device Name	Name of the PTZ control.
IP Address	IP address of the PTZ control.
Port Number	Port number of the PTZ control.

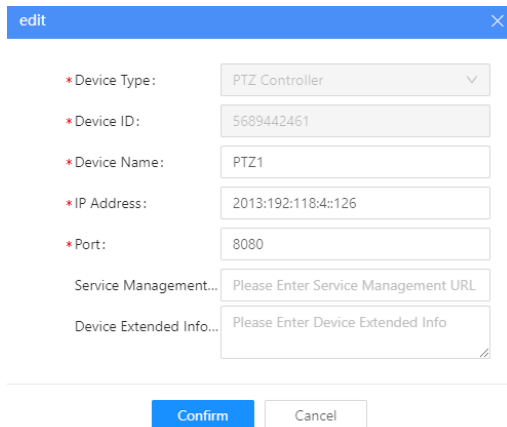
Parameter	Description
Service Management URL	Service management URL of the PTZ Control. After configuring this field, you can log in to the system to perform service management.
Device Extra Information	Device Extra Information of the PTZ Control

5. Click **OK** to complete the addition.

2. Edit PTZ Control

1. Click  corresponding to the PTZ control to go to the **Edit PTZ Control** page.

Figure 9-52 Edit PTZ Control



2. Edit the PTZ control information, and click **OK** to save the modification.

3. Delete PTZ Control

Click  corresponding to the device and confirm to delete the device.

9.4 Server Device

Add, configure, or delete servers.

9.4.1 IP SAN

By IP SAN management, you can store and view audio and video data from cameras.

1. Add an IP SAN

1. Go to **Device Management > Server Device**.
2. Click **Add** and select **IP SAN**.

AddIPSAN
✕

*Storage Device Type: IX/EX Series

*Device Name: Please Enter Name

*Device ID: Please Enter Device ID

*IP Address: Please Enter IP Address

*User Name: Please Enter User Name

*Password: Please Enter Password

*Confirm Password: Please Enter Confirm Password

*DM List: Please Select

☐ Asset Info

OK
Cancel

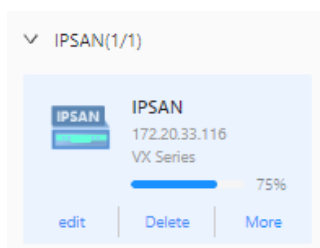
3. Refer to the table below to configure the IP SAN.

Storage Device Type	Parameter	Description
IX/EX	Name	IP SAN device name.
	Device ID	IP SAN device ID.
	IP Address	IP SAN device IP.
	Username	IP SAN device login username.
	Password	IP SAN device login password.
	Confirm	Confirm the login password of the IP SAN device.
	DM List	Select a DM list for the IP SAN device.
VX	Storage Device Subtype	Select VX1500-E, VX1500 or VX1600.
	Name	IP SAN device name.
	Device ID	IP SAN device ID.
	IP Address	IP SAN device IP.
	DM List	Select a DM list for the IP SAN device.

4. Click **OK**.

2. Scan Capacity

- Go to **Device Management > Server Device**.
- Select an IP SAN device, click **More**, and select **Scan Capacity** to scan the capacity usage of the IP SAN device.



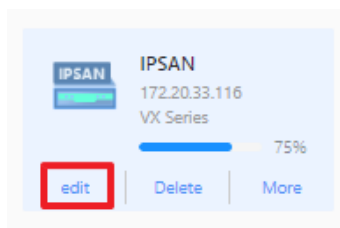
3. Query Cameras

1. Go to **Device Management > Server Device**.
2. Select an IP SAN device, click **More**, and select **Query Camera** to view the cameras mounted under the IP SAN device.

< Back		Refresh	
Camera name	Storage Type	Recording Schedule Configured	Schedule Status
test	Direct Storage	yes	Enable

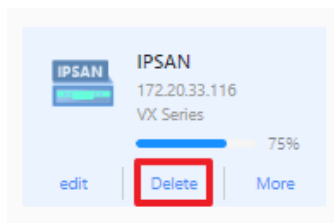
4. Edit an IP SAN

1. Go to **Device Management > Server Device**.
2. Select the IP SAN you want to edit and click **Edit**.
3. You can edit the device name.
4. Click **OK**.



5. Delete an IP SAN

1. Go to **Device Management > Server Device**.
2. Select the IP SAN you want to delete and click **Delete**.



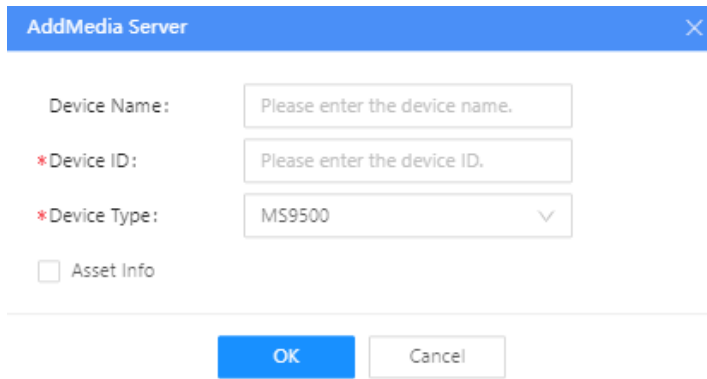
9.4.2 MS Server

Media server (MS) mainly forwards, replicates, and distributes audio and video streams in real time, including:

- Receive real-time audio and video streams from encoding devices and forward them to decoding devices for decoding and playback.
- Replicate and distribute a received media stream to multiple decoding devices for decoding and playback, so that multiple users can view the same video at the same time even if the uplink access bandwidth of the encoding device is insufficient.
- Receive multicast media streams or unicast media streams and send unicast media streams to adapt to different network conditions.

1. Add an MS

1. Go to **Device Management > Server Device**.
2. Click **Add** and select **MS**.



AddMedia Server [X]

Device Name:

*Device ID:

*Device Type: ▼

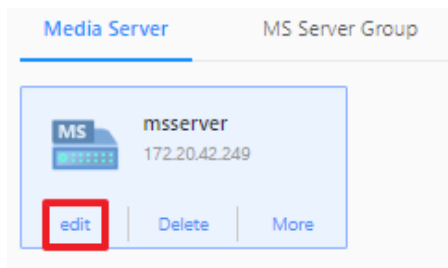
☐ Asset Info

OK Cancel

3. Enter the device name and device ID, and select the device model.
4. Click **OK**.

2. Edit an MS

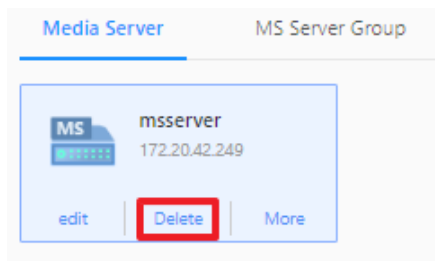
1. Go to **Device Management > Server Device**.
2. Select the MS you want to edit and click **Edit**.



3. You can edit the device name.
4. Click **OK**.

3. Delete an MS

1. Go to **Device Management > Server Device**.
2. Select the MS you want to delete and click **Delete**.



9.4.3 MS Group

9.4.4 MD Server

Multidimensional data server (MD) supports the access of multidimensional data such as passing vehicle/MAC/RFID, as well as cascading and interconnection between VIID platforms.

1. Add an MD

1. Go to **Device Management > Server Device**.
2. Click **Add** and select **MD**.

AddMD✕

Device Name:

*Device ID:

*Device Type:

MD9500(primary server)
▼

☐ Asset Info

OK

Cancel

3. Enter the device name and device ID, and select the device model.
4. Click **OK**.

2. Configure Storage Resources

1. Go to **Device Management > Server Device**.
2. Select an MD server, click **More**, and select **Configure Storage Resources** to configure storage resources for the MD.

< Back + Add 🗑 Delete 🔄 Refresh					
☐	Device Name	Resource Type	Resource Usage	Resource Status	Total Capacity(GB)
☐	MDStorage	IP SAN Storage	Passing Vehicle Image	Formatting	1024.000
					1024.000

3. Click **Add**.

Add Storage Resource✕

*Resource Name

*Resource Type:

IP SAN Storage
▼

*Resource Usage

Passing Vehicle Image
▼

*Storage Device:

Select
▼

Available Capac

*Allocated Capa

OK

Cancel

4. Refer to the table below to complete the storage resource settings.

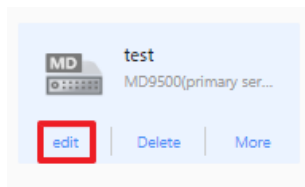
Parameter	Description
Resource Name	Set a name for the storage resource.
Resource Type	Select the storage resource type. ● IP SAN: Storage to the specified IPSAN storage device. Multiple MD servers can share one IP SAN storage device, which is convenient for unified management and backup of stored images. Before selecting it, you need to add an IP SAN storage device and configure it. ● Third-party IP SAN: Storage to third-party IP SAN storage devices. ● Cloud Storage: Storage to the cloud storage system. Before selecting it, you need to configure the cloud storage system.

Parameter		Description
IP SAN	Resource Usage	Used to store passing vehicle images, passing vehicle alarm images, face images, face alarm images or structured images. Note: To store multiple types of images, you need to add storage resources separately.
	Storage Device	The IP SAN device where the storage resource is located.
	Available Capacity	The free capacity of the storage device.
	Allocated Capacity	The storage capacity allocated to the MD on the storage device.
Third-party IP SAN	Resource Usage	Used to store passing vehicle images, passing vehicle alarm images, face images, face alarm images or structured images. Note: To store multiple types of images, you need to add storage resources separately.
	Device ID	Device ID.
	Initiator	Initiator name.
	Target	Target name.
	LUN ID	Logical unit ID number.
	Resource Path	The path where the resource is mounted to the third-party IP SAN.
Cloud Storage	Resource Usage	Used to store passing vehicle, alarm, and general resources. Note: To store multiple types of resources, you need to add storage resources separately. Multiple resources of the same type can be configured.
	Storage Device	The cloud storage device where the storage resource is located.
	Available Capacity	The free capacity of the storage device. The default is all the capacity of the device.
	Allocated Capacity	The capacity allocated to the storage resources of the multidimensional data server on the storage device. The default is all the capacity of the device.

5. Click **OK**.

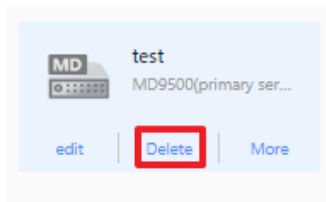
3. Edit an MD

1. Go to **Device Management > Server Device**.
2. Select the MD you want to edit and click **Edit**.
3. You can edit the device name.
4. Click **OK**.



4. Delete an MD

1. Go to **Device Management > Server Device**.
2. Select the MD you want to delete and click **Delete**.



9.4.5 Intelligent IA Server

IA server mainly analyzes video content and triggers alarms according to the preset rules.

1. Add an IA Server

1. Go to **Device Management > Server Device**.
2. Click **Add** and select **IA Server**.

3. Enter the device name and device ID, and select the device model.
4. Click **OK**.

2. Edit an IA Server

1. Go to **Device Management > Server Device**.
2. Select the IA server you want to edit and click **Edit**.
3. You can edit the device name.
4. Click **OK**.

3. Delete an IA Server

1. Go to **Device Management > Server Device**.
2. Select the IA server you want to delete and click **Delete**.

9.4.6 TS Server

Transcoding server (TS) can convert streams from third-party devices to standard streams, enabling seamless integration between different surveillance systems.

1. Add a TS

1. Go to **Device Management > Server Device**.
2. Click **Add** and select **TS**.

Add TS

* Device Name :

Please Enter Device Name

* Device ID :

Please Enter Device ID

* Device Model :

TS8500

▼

☐ Asset Info

Confirm

Cancel

- Enter the device name and device ID, and select the device model.
- Click **OK**.

2. Edit a TS

- Go to **Device Management > Server Device**.
- Select the TS you want to edit and click **Edit**.
- You can edit the device name.
- Click **OK**.

3. Delete a TS

- Go to **Device Management > Server Device**.
- Select the TS you want to delete and click **Delete**.

9.4.7 VOD Playback Server

In the CDS cloud storage system, VOD playback server is based on cloud architecture, supports cluster deployment, focuses on stored video on-demand playback service, maximizes playback performance, and has special features such as video editing.

1. Add a VOD

- Go to **Device Management > Server Device**.
- Click **Add** and select **VOD**.

Add VOD Server

* Device Name :

Please Enter Device Name

* Device ID :

Please Enter Device ID

☐ Asset Info

Confirm

Cancel

- Enter the device name and device ID.
- Click **OK**.

2. Edit a VOD

- Go to **Device Management > Server Device**.

2. Select the VOD you want to edit and click **Edit**.
3. You can edit the device name.
4. Click **OK**.

3. Delete a VOD

1. Go to **Device Management > Server Device**.
2. Select the VOD you want to delete and click **Delete**.

9.4.8 BM Server

Backup management server (BM) supports forwarding storage, backup, video playback, etc.

1. Add a BM

1. Go to **Device Management > Server Device**.
2. Click **Add** and select **BM**.

3. Refer to the table below to complete the BM server settings.

Parameter	Description
Name	BM name.
Device ID	BM ID. Note: The ID must be consistent with the device ID set during BM installation.
Device Type	Select the BM type. Note: The device types listed here may not match actual device types one by one.

Parameter	Description
Media Service Selection Policy	● Auto-Adaptation: (default) Whether live video streams used for forward-and-storage are transmitted via MS is determined by the system based on the media service selection policy of the encoder, IPC, hybrid NVR, and the external domain, and on whether MS is deployed. Note: Direct Connection First is adopted when these conditions are met: 1. MS is deployed but its forwarding capacity is insufficient. 2. The encoding device or the external domain adopts Auto-Adaptation as the media service selection policy. ● Direct Connection Priority: ➢ For local-domain cameras, live video streams for forward-and-storage are not forwarded via MS unless the following conditions are met in the local domain: 1. Direct connections has exceeded the maximum number. 2. MS is deployed. 3. The encoding devices such as encoder, IPC, or hybrid NVRs allow forwarding via MS. ➢ For external-domain cameras, if the maximum number of direct connections is not reached in the local domain or the child/peer domain, live video streams will be transmitted directly; otherwise, live video streams will be forwarded via MS (if deployed in the local domain).
When Storage Full	Select whether to overwrite the backup data or stop backup when the backup storage space allocated to the camera is full. ● Overwrite: The oldest backup data will be overwritten when the backup storage space allocated to the camera is used up. ● Stop: The system will stop backup when the backup storage space allocated to the camera is used up.
Case Resource Storage	Set whether the BM server supports case resource storage. Not support by default. Note: Each VM supports only one BM for case resource storage.
Cloud/Archive Storage	Set whether the BM server supports cloud storage or archive storage. Note: The cloud storage configuration in BM's WEB interface must be consistent with the cloud storage configuration here. Archive storage means storage to a tape library.

4. Click **OK**.

2. Configure Storage Resources

1. Go to **Device Management > Server Device**.
2. Select a BM server, click **More**, and select **Configure Storage Resources** to configure storage resources for it.

< Back + Add Delete Refresh

☐	Resource Name	Resource Type	Device Name	Total Capacity(GB)	Free Space(GB)	Resources used for cases	Resource Status
☐	test	Data Management Server	bmserver	3,000	2,875	no	Normal

3. Click **Add**.

AddStorage resource of BM server ✕

* Resource Name:

* Resource Type:

Data Management Server ▼

* Select Storage:

Please Select Select Storage ... ▼

Available Capacity:

Please Enter Available Capacity

* Allocated Capacity:

Please Enter Allocated Capacity

Resource Path:

Please Enter Resource Path

OK

Cancel

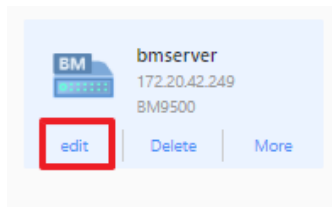
4. Refer to the table below to complete the storage resource settings.

Resource Type	Parameter	Description
Data Management Server	Storage Device	Select the storage device in the system.
	Available Capacity	The free capacity of the storage device.
	Allocated Capacity	The storage capacity allocated to the BM on the storage device.
	Resource Path	The path where the resource is mounted to the IPSAN.
Third-party Resource IPSAN	Storage Device Address	The IP address of the third-party IPSAN device.
	Initiator	Initiator name.
	Target	Target name.
	LUN ID	Logical unit ID number.
	Resource Path	The path where the resource is mounted to the third-party IPSAN.
File System Resource	Resource Capacity	The capacity of the storage device.
	Resource Path	The path where the resource is mounted.
Local Block Resource	Resource Path	The path where the resource is mounted.
Cloud Storage	Select Storage Device	The cloud storage device where the storage resource is located.
	Available Capacity	The free capacity of the storage device. The default is all the capacity of the device.
	Allocated Capacity	The capacity allocated to the storage resources of the multidimensional data server on the storage device. The default is all the capacity of the device.

5. Click **OK**.

3. Edit a BM

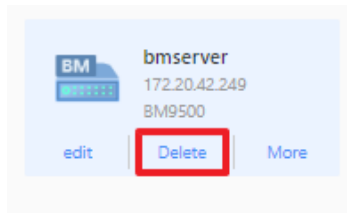
1. Go to **Device Management > Server Device**.
2. Select the BM you want to edit and click **Edit**.



3. Modify the BM server parameters as needed.
4. Click **OK**.

4. Delete a BM

1. Go to **Device Management > Server Device**.
2. Select the BM you want to delete and click **Delete**.



9.4.9 DM Server

Data management server (DM) supports storage resource management, direct storage, video retrieval and playback, etc.

1. Add a DM

1. Go to **Device Management > Server Device**.
2. Click **Add** and select **DM**.

AddData Management Server
×

Device Name:

*Device ID:

*Device Type:

DM9500
▼

☐ Asset Info

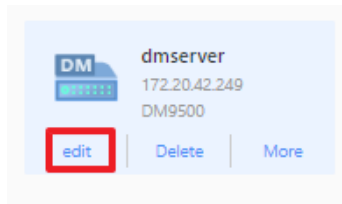
OK

Cancel

3. Enter the device name and device ID, and select the device model.
4. Click **OK**.

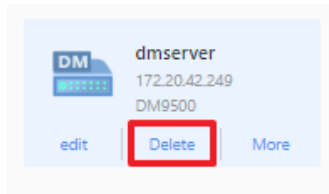
2. Edit a DM

1. Go to **Device Management > Server Device**.
2. Select the DM you want to edit and click **Edit**.
3. You can edit the device name.
4. Click **OK**.



3. Delete a DM

1. Go to **Device Management > Server Device**.
2. Select the DM you want to delete and click **Delete**.



9.4.10 DB Server

Database management server (DBE/DBF) is used to store structured and semi-structured data, provides high-speed database read and write services, and can meet the needs of large-capacity data services.

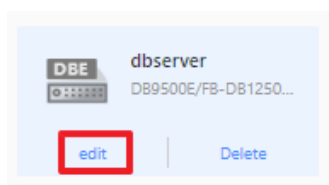
1. Add a DB

1. Go to **Device Management > Server Device**.
2. Click **Add** and select **DB**.

3. Enter the device name and device ID, and select the device model.
4. Click **OK**.

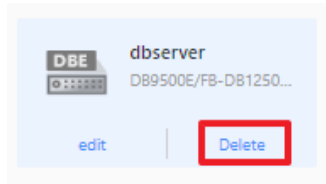
2. Edit a DB

1. Go to **Device Management > Server Device**.
2. Select the DB you want to edit and click **Edit**.
3. You can edit the device name.
4. Click **OK**.



3. Delete a DB

1. Go to **Device Management > Server Device**.
2. Select the DB you want to delete and click **Delete**.



9.4.11 DAPA Server

DAPA server is mainly used to forward face or vehicle images.

1. Add a DAPA

1. Go to **Device Management > Server Device**.
2. Click **Add** and select **DAPA**.

3. Enter the device name and device ID.
4. Click **OK**.

2. Edit a DAPA

1. Go to **Device Management > Server Device**.
2. Select the DAPA you want to edit and click **Edit**.
3. You can edit the device name.
4. Click **OK**.

3. Delete a DAPA

1. Go to **Device Management > Server Device**.
2. Select the DAPA you want to delete and click **Delete**.

9.4.12 Map Server

Map server (MAP) can connect to mainstream map manufacturers to provide map display service.

1. Add a MAP

1. Go to **Device Management > Server Device**.
2. Click **Add** and select **MAP**.

Add Map Server

* Device Name:

Please Enter Device Name

* Device ID:

Please Enter Device ID

* Device Model:

MAP9500

☐ Asset Info

Confirm

Cancel

3. Enter the device name and device ID, and select the device model.
4. Click **OK**.

2. Edit a MAP

1. Go to **Device Management > Server Device**.
2. Select the MAP you want to edit and click **Edit**.
3. You can edit the device name.
4. Click **OK**.

3. Delete a MAP

1. Go to **Device Management > Server Device**.
2. Select the MAP you want to delete and click **Delete**.

9.4.13 Log Auditing Server

The log auditing server (LOG) supports log collection, backup, analysis and retrieval.

1. Add a Log Auditing Server

3. Go to **Device Management > Server Device**.
4. Click **Add** and select **LOG**.

Add Log Auditing Server

* Device Name:

Please Enter Device Name

* Device ID:

Please Enter Device ID

* Device Model:

LOG9500

☐ Asset Info

Confirm

Cancel

5. Enter the device name and device ID, and select the device model.
6. Click **OK**.

2. Edit a Log Auditing Server

7. Go to **Device Management > Server Device**.
8. Select the LOG you want to edit and click **Edit**.
9. You can edit the device name.
10. Click **OK**.

3. Delete a Log Auditing Server

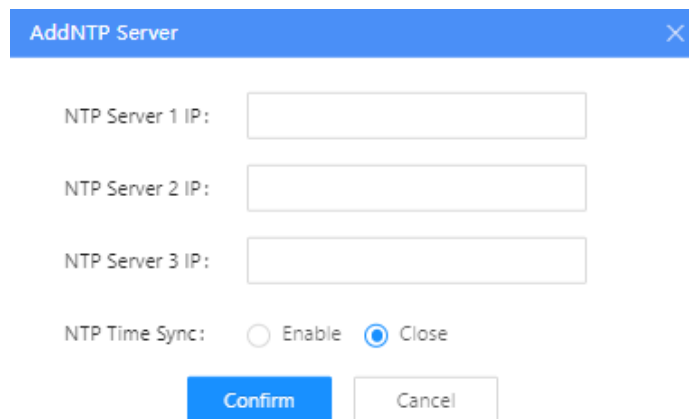
11. Go to **Device Management > Server Device**.
12. Select the LOG you want to delete and click **Delete**.

9.4.14 NTP Server

You can configure the IP address of the NTP server for time synchronization and enable/disable time synchronization.

1. Add NTP Server

1. Go to **Device Management > Server Device**.
2. Click **Add** and select **NTP Server** to go to the **Add NTP Server** page.



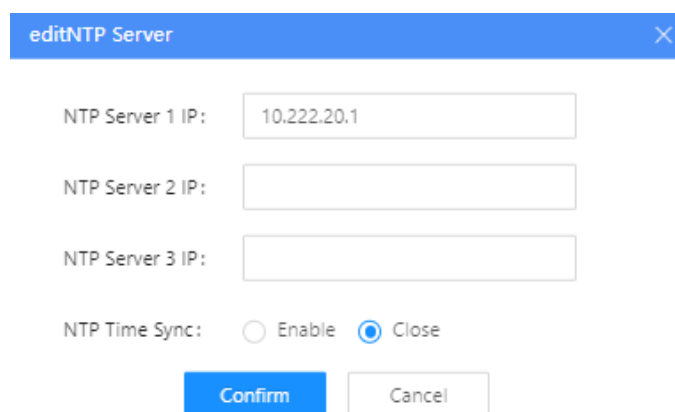
The image shows a dialog box titled "AddNTP Server" with a close button (X) in the top right corner. It contains three input fields for "NTP Server 1 IP:", "NTP Server 2 IP:", and "NTP Server 3 IP:". Below these fields is a radio button group for "NTP Time Sync:" with "Enable" and "Close" options. The "Close" option is selected. At the bottom are "Confirm" and "Cancel" buttons.

3. Enter the IP address of the NTP server. Configure at least one IP address. The first IP address is active and the other two IP addresses are standby.
4. Click **OK** to complete the addition. Note that you can add only one NTP server.

2. Configure NTP Server

1. Click **Configure** corresponding to the NTP server to go to the **Configure NTP Server** page.

Figure 9-53 Edit NTP Server



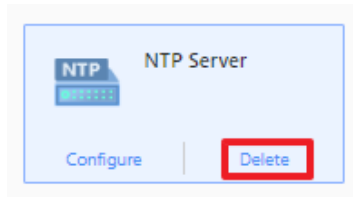
The image shows a dialog box titled "editNTP Server" with a close button (X) in the top right corner. It contains three input fields for "NTP Server 1 IP:", "NTP Server 2 IP:", and "NTP Server 3 IP:". The first field contains the IP address "10.222.20.1". Below these fields is a radio button group for "NTP Time Sync:" with "Enable" and "Close" options. The "Close" option is selected. At the bottom are "Confirm" and "Cancel" buttons.

2. You can edit the IP address of the NTP server and enable/disable NTP time synchronization.
3. Click **OK** to save the modification.

3. Delete NTP Server

Click **Delete** corresponding to the NTP server and confirm to delete the NTP server.

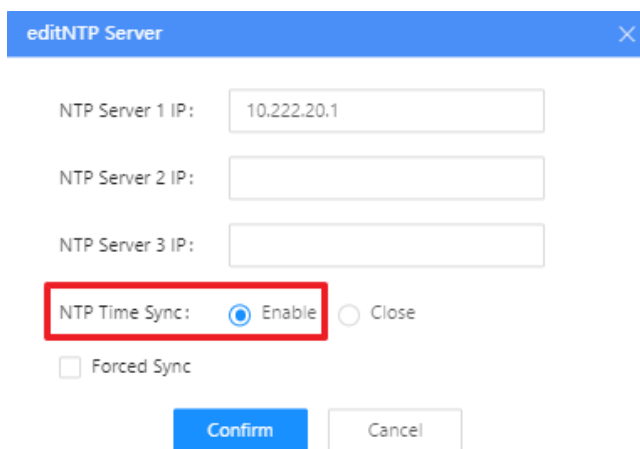
Figure 9-54 Delete NTP Server



4. Enable NTP Time Sync

Add or configure the NTP time server. After you enable NTP time synchronization, the server time will be synchronized with the NTP time immediately. Click the **On** switch for NTP time synchronization and click **OK**.

Figure 9-55 Enable NTP Time Synchronization

A screenshot of a dialog box titled "editNTP Server" with a close button (X) in the top right corner. The dialog contains three input fields for "NTP Server 1 IP:", "NTP Server 2 IP:", and "NTP Server 3 IP:". The first field contains the IP address "10.222.20.1". Below these fields is a section for "NTP Time Sync:" with two radio buttons: "Enable" (which is selected and highlighted with a red box) and "Close". Below this is a checkbox for "Forced Sync" which is currently unchecked. At the bottom of the dialog are two buttons: "Confirm" and "Cancel".

Note!

When the time difference between the server and the NTP server is more than 30s, the time synchronization fails and an NTP clock source exception will be reported.

5. Forced Sync

When NTP time sync is enable, you can perform forced sync. Select **Forced Sync**, select the IP address of the NTP server, and click **OK**. Then, the server time will be synchronized with the selected NTP server immediately, and the time difference between the server and the NTP server will not be checked.

Figure 9-56 Forced Sync

editNTP Server

NTP Server 1 IP: 10.222.20.1

NTP Server 2 IP:

NTP Server 3 IP:

NTP Time Sync:
☒ Enable
☐ Close

☒ Forced Sync

Please select the IP address to be forcibly synchronized:

☒ Select All
☒ NTP Server1...
☐ NTP Server1...
☐ NTP Server1...

Confirm
Cancel

10 Storage Configuration

10.1 Direct Storage Resource

Assign storage space and configure video recording modes so cameras can record video in specified modes.

10.1.1 Configure Direct Storage Resource

Assign storage devices and storage space to cameras. The following storage modes are available: manual storage, alarm-triggered storage, and scheduled storage.

- Manual storage: User starts/stops central recording manually.
- Alarm-triggered storage: Storage is triggered by alarms. You need to configure post-alarm recording time (see Post-Alarm Recording Time).
- Scheduled storage: Configure a storage schedule for the camera.

4. Go to **Device Management >Service Configuration > Storage Service> Storage Resource**.

Video Management Platform

Live Play
Recording Playback
Video Wall
Device Management
O&M Management

Quick Nav
Basic Configuration
Device Configuration
Platform Cascading
Service Configuration
Storage Service
Display Control
Alarm Service
Asset Management
LAPI Management
Advanced Settings

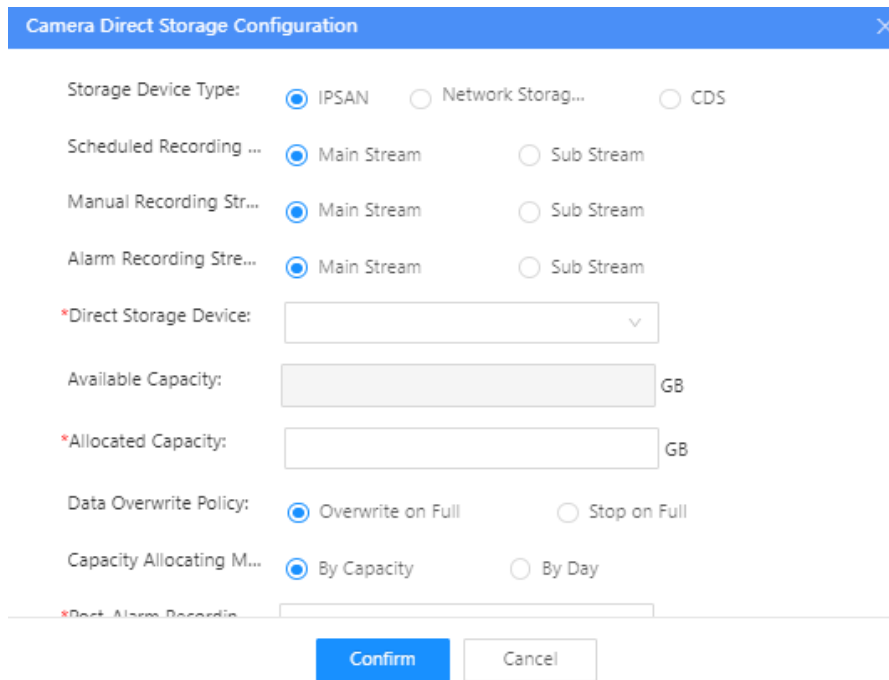
Storage Configuration
Forward-and-Storage Configuration
Backup Configuration
Image Retention Period Configuration

Please enter the resour...

Batch Add
Batch Edit
Enable Schedule...
Disable Schedule...
Start Central Rec...
Stop Central Rec...
Batch Migrate
Delete
Refresh
Advanced Search Criteria

	Camera name	code rate(Kbps)	Configure Capacity(G)	Home Device	Space Storage Mode	Storage Device	Data M
☐	12	2048	Storage is not configured	IPC	Unknown		
☐	46	2048	Storage is not configured	IPC	Unknown		
☐	lapi1	2048	Storage is not configured	IPC	Unknown		
☐	onvif64z	2048	Storage is not configured	IPC	Unknown		

5. On the left-side organization tree, choose an organization, choose the target camera, click the corresponding , or select multiple cameras of the same type (IPC or EC) and then click **Batch Add**. A page as shown below appears. The parameters displayed may vary with camera. The figure below is an example.



6. Configure the parameters by referring to the table below.

Table 10-1 Parameter Descriptions for Direct Storage Configurations

Parameter	Description
Storage Device Type	Storage device types: IP SAN , Network Storage Device VX500 , CDS .
Scheduled Recording Stream	Choose main stream or sub stream. The selected stream type will be used for scheduled storage.
Manual Recording Stream	Choose main stream or sub stream. The selected stream type will be used for manual storage.
Alarm Recording Stream	Choose the stream type for alarm-triggered recording. Note: Choose main stream or sub stream according to the encoding parameters of the IPC or the encoder connected to the camera.
Direct Storage Device	Actual storage device, on which you will allocate storage resources. Note: Only storage devices that have been added to the system will appear in the list.
Available Capacity	Available capacity on the storage device. The system reads the capacity automatically after you select a direct storage device.
Allocated Capacity	Storage space assigned to the camera.
When HDD Full	● Overwrite: When the storage space assigned to the camera is used up, new data will overwrite the old data from the beginning repeatedly. ● Stop: The system stops saving new data when the space assigned to the camera is full, and an alert will be sent to the central server. Note: The “stop” policy is not applicable to cloud storage.

Parameter	Description
Device Selection Policy	Whether to allow the system to automatically choose other storage devices if the user-specified storage space is insufficient. Note: This parameter needs to be configured only when you configure IPSAN for cameras in batches.
Capacity Allocating Mode	● By Capacity: Allocate storage resource to the camera according to the allocated space. ● By Day: Calculate the space to be allocated based on stream type, storage days, and scheduled storage settings, and then allocate storage resource to the camera. Note: This parameter is displayed only when you are configuring a single camera.
Storage Days	This parameter is required if you are configuring for a single camera and the capacity allocating mode is "By Day". Set the storage days and then click Calculate. The system automatically calculates the needed forward-and-storage space and displays it in "allocate capacity" or "expansion capacity". Note: The video storage space needed by a camera is calculated using this formula: $\text{Needed space} = N (\text{hours}) * 3600 (\text{seconds}) * \text{encoder stream} / \text{IPC (bps)} * (1.08) / 8$, where 1.08 is the needed space plus 8% margin. For example, assume each video channel is 2M, so the space needed every hour is $2048 * 3600 * 1.08 / (8 * 1024 * 1024) = 0.95\text{GB}$, so 22.8GB is needed for 24-hour recording. If each camera records 30 days, then one VX1600 with 16 1TB HDDs can satisfy space requirements of $16000 / (22.8 * 30) \approx 24$ cameras at most.
DM Server	DM server that manages storage devices. Note: This parameter is only applicable to GB/ONVIF IPCs whose storage device type is IPSAN. When you configure storage for GB/Onvif cameras, make sure the storage managed by the DM does not exceed the value in the configuration file, otherwise configuration will fail and an error message will be displayed.
Post-Alarm Recording Time	Storage duration after an alarm is triggered.

7. Enable/disable scheduled recording (when enabled, the camera records video according to the schedule).

Camera Direct Storage Configuration

☒ Scheduled Direct Storage Configuration

Time Period:

By Day

No.	Start Time	End Time	Operation
1	00:00:00	23:59:59	

+

☒ Enable E...

Exception1

2024-01-31

Confirm

Cancel

- (Optional) If scheduled direct storage is enabled, configure scheduled direct storage by referring to the table below.

Table 10-2 Parameter Descriptions for Scheduled Direct Storage

Parameter	Description
Time Period	You can set the storage schedule by day or by week. Note: After completing the storage schedule for a day, you can click Copy to copy and apply the schedule to other days.
Enable Exception	If necessary, enable exception to set special time periods and perform special storage during these periods. On special days, the system performs storage during the set periods only; on other days, the system performs storage according to the schedule. Note: Click Add Exception to add an exception. Up to 16 exceptions are allowed. Click  to delete an exception. After completing the storage schedule for a day, you can click  to copy and apply the schedule to other days.

- Click **OK**.

10.1.2 Capacity Expansion/Reduction

- Go to **Device Management >Service Configuration > Storage Service > Storage Resource**.

Choose the target camera, click the corresponding . The camera direct storage configuration page is displayed.

- In expansion capacity, enter the capacity you want to expand or reduce. A positive number means expansion. A negative number means reduction.
- Click **OK**.



NOTE!

- For capacity expansion, make sure the expansion is less than or equal to the capacity available.
- To reduce IPSAN capacity, make sure the modified capacity is greater than or equal to 3GB.

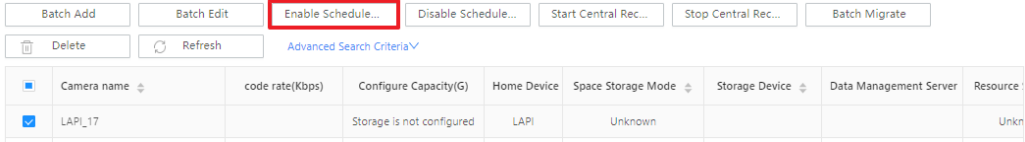
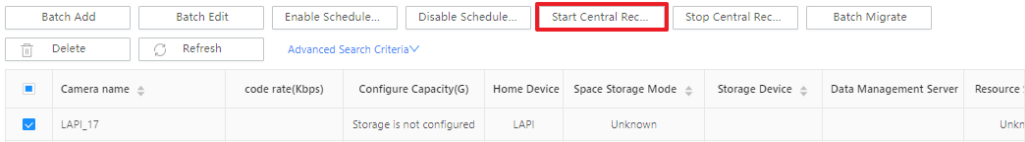
Batch Management

- Add in batches: Select multiple cameras and then click **Batch Add**. The camera direct storage configuration page appears. Batch add direct storage as needed.
- Edit in batches: Select multiple cameras and then click **Batch Edit**. The camera direct storage configuration page appears. Batch edit direct storage as needed.

10.1.3 Start/Stop Storage

You can start or stop storage after completing storage resource configuration for a camera.

Table 10-3 Descriptions for Starting/Stopping Recording

Storage Type	Operation
Scheduled Storage	- Go to Device Management >Service Configuration > Storage Service > Storage Resource. - Click the organization on the left-side organization list, and then select the target camera in the organization. - Click Start Scheduled Storage. To stop scheduled storage, click Stop Scheduled Storage.  Note: The system automatically starts the recording schedule when scheduled recording is configured.
Manual storage	You can perform manual storage after configuring storage resources for the camera. Go to Device Management >Service Configuration > Storage Service > Storage Resource, enable central recording for the camera. 

10.2 Forward-and-storage Resource

Configure forward-and-storage, including the following operations:

- Configure forward-and-storage for cameras.
- Configure a schedule to forward and store live videos of cameras according to the schedule.
- Start/stop forward-and-storage schedule.

10.2.1 Configure Forward-and-Storage for Cameras

- Go to **Device Management > Service Configuration > Storage Service > Forward-and-Storage Resource**.
- Click the target organization on the left-side organization list.
- Select multiple cameras (at least 2) in the organization, click **Batch Add**; or click the corresponding  for the camera. A page as shown below appears.

Forward-and-Storage Configuration

Camera name: test

*Select Stream:

☒ Main Stream
☐ Sub Stream

*Select Forward-and-St...

Available Capacity:

0

GB

*Allocated Capacity:

GB ⓘ

*Data Overwrite Policy:

☒ Overwrite on Full
☐ Stop on Full

☒ Scheduled Forward-and-Storage Configuration

*Capacity Allocating M...

☒ By Capacity
☐ By Day

Plan Template:

Apply

Time Period:

By Day

OK

Cancel

4. Configure the parameters by referring to the table below.

Table 10-4 Forward-and-Storage Configuration Description

Parameter	Description
Select Stream	Choose the stream type to be used for forward-and-storage. You can choose main stream or sub stream. The main stream provides higher resolutions than the sub stream.
Select Forward-and-Storage Device	Choose a backup device that is not being used by the camera. The system will allocate backup resources for forward-and-storage on the backup device. Note: You need to add BM first (see Add a BM). Only the added BM will appear in the drop-down list.
Available Capacity	Available capacity on the forward-and-storage device. After you select a device, the system automatically reads its capacity.
Allocated Capacity	Allocate forward-and-storage capacity for the camera.
When HDD Full	● Overwrite: When the forward-and-storage space assigned to the camera is used up, new data will overwrite the old data from the beginning repeatedly. ● Stop: When the space assigned to the camera is used up, the system will stop saving new data and meanwhile send an alert to the central server.

5. Click **OK**.

10.2.2 Configure Forward-and-Storage Schedule

1. Enable/disable scheduled forward-and-storage (when enabled, videos of the camera will be forwarded and stored according to the schedule).

Camera Direct Storage Configuration

☒ Scheduled Direct Storage Configuration

Time Period: By Day

No.	Start Time	End Time	Operation
1	00:00:00	23:59:59	

☐ Enable E...

Confirm **Cancel**

- (Optional) Enable scheduled forward-and-storage, and then configure a schedule by referring to the table below.

Table 10-5 Parameter Descriptions for Configuring Scheduled Forward-and-Storage

Parameter	Description
Capacity Allocating Mode	● By Capacity: Allocate storage resource to the camera according to the allocated space. ● By Day: Calculate the space to be allocated based on stream type, storage days, and scheduled storage settings, and then allocate storage resource to the camera. Note: This parameter is displayed only when you are configuring a single camera.
Storage Days	This parameter is required if you are configuring for a single camera and the capacity allocating mode is "By Day". Set the storage days and then click Calculate. The system automatically calculates the needed forward-and-storage space and displays it in "allocate capacity" or "expansion capacity". Note: The video storage space needed by a camera is calculated using this formula: $\text{Needed space} = N (\text{hours}) * 3600 (\text{seconds}) * \text{encoder stream} / \text{IPC (bps)} * (1.08) / 8$ where 1.08 is the needed space plus 8% margin. For example, assume each video channel is 2M, so the space needed every hour is $2048 * 3600 * 1.08 / (8 * 1024 * 1024) = 0.95\text{GB}$, so 22.8GB is needed for 24-hour recording. If each camera records 30 days, then one VX1600 with 16 1TB HDDs can satisfy space requirements of $16000 / (22.8 * 30) \approx 24$ cameras at most.
Time Period	You can set the storage schedule by day or by week. Note: After you complete settings for a day, you can click Copy to apply the setting to other days.

- Click **OK**.

10.2.3 Start and Stop Forward-and-Storage Schedule

Start or stop forward-and-storage schedules for cameras in the management system.

- To start or stop the forward-and-storage schedule for a camera, click the corresponding Stop / Enable for the camera.
- To start or stop forward-and-storage schedules for multiple cameras at a time, select the cameras and then click **Start** or **Stop**.

10.3 Backup Resources

10.4 Image retention period configuration

The system automatically clears the images of passing vehicles and alarms according to the upper and lower limits of space and the image retention period to free up the storage space.

Go to **Device Management>Service Configuration > Storage Service> Image retention period configuration**.

	Rule Name	Server Type	Resource Type	Service Type	Image Type	Retention Per...	Capacity Alarm	Camera Group Name	Whether is an	Operation
☐	Alarmas_reglas gene...	TMS/MD	Alarm	All	All	1460	-		no	
☐	Cruzando el coche_r...	TMS/MD	Passing Vehicle	All	All	730	-		no	
☐	General_reglas gene...	TMS/MD	General	All	All	730	-		no	

By default, there is one rule for the retention period of alarms, passing vehicles, and general resources, respectively. The rules are effective for all image types and all cameras. You can click corresponding to the rule to edit the rule name, overwrite mode, and rule configuration, but you cannot edit the application object.

Figure 10-1 Edit Rule

* Rule Name:

Server Type:

Resource Type:

Service Type:

Image Type:

Capacity Alarm: More than Alar...

Overwrite Mode: ☒ Cleanup Based on Retention Period ☐ Clean Up based on Capacity

* Retention Peri... Day(s)

You can add rules and set the application object. The operation steps are as follows:

1. Click **Add Rule** to go to the **Add Rule** page.
2. After configuring the rule, click **OK**.

Figure 10-2 Add Rule

Add Rule
✕

* Rule Name:

Resource Type:

Image Type:

Overwrite Mode: ☒ Cleanup Based on Retention Period ☐ Clean Up based on Capacity ?

* Retention Peri... Day(s)

☐ Select Camera

Server Type:

Service Type:

Capacity Alarm: More than Alar...

确定

取消

Parameter	Description
Rule Name	To be customized.
Server Type	Server type for accessing images: IA, TMS/MD.
Resource Type	Options: All, General, Passing Vehicle, Alarm.
Service Type	- If the resource type is Passing Vehicle, you can select the service type of images, which includes All, Structured, and Passing Vehicle. - For other resource types, the services type is not distinguished.
Image Type	Options: All, Big Image, Small Image, Radar Data. Note! You can set the image type only when images are cleared by retention period, that is, you can clear only images of the configured type.
Capacity Alert	When the storage resource utilization exceeds d%, the system reports an alert.
Overwrite Mode	- Clear by Retention Period: You need to set the number of days for the retention period. Data will be cleared when the retention period is over and the disk utilization exceeds 80%. If the disk is full but the retention period is not over, new data will be discarded. - Clear by Capacity: Set a percentage (%d) for starting and a percentage (d%) for stopping clearing images. Note! If images are cleared by capacity, you cannot set the image type or select a specific camera.
Select Camera	By default, images from all cameras are cleared. You can select a specific camera only when the image type is All and images are cleared by retention period, that is, only clear all images from the specified camera.



Note!

If multiple rules apply to the same resource type, the priority is: Camera rule > Image type rule > Default rule.

11 Alarm Service

The video management platform supports unified management of alarms from devices in the surveillance system. When a device encounters an exception or detects an events, it will send an alarm to the management platform to alert the user for attention or actions.

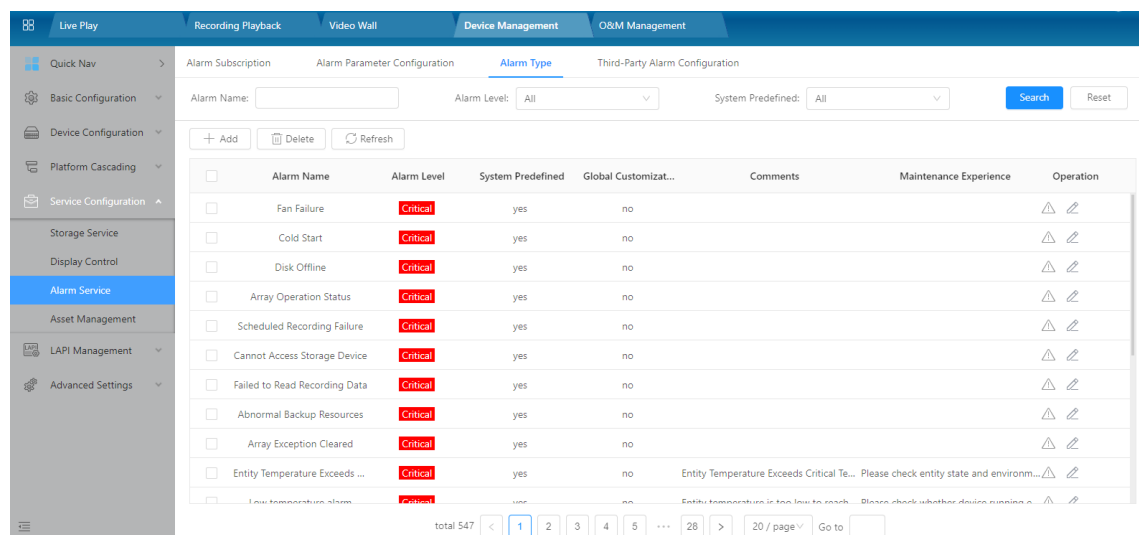
11.1 (Optional) Alarm Customization

The predefined alarm types in the system are effective to all users. You can change their names and levels as needed.

11.1.1 View Predefined Alarms

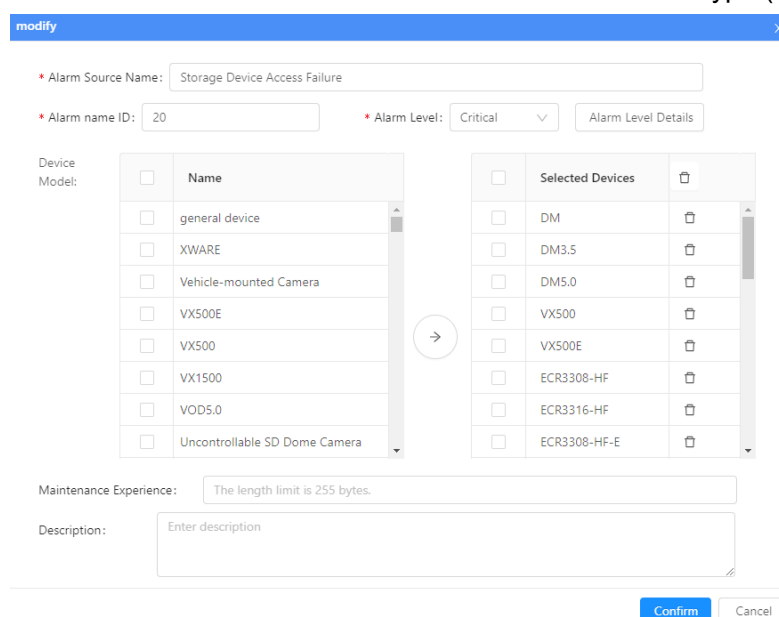
View the name, ID, and level of alarms predefined in the system and the linked alarm devices.

1. Go to **Device Management > Service Configuration > Alarm Service > Alarm Type**.



☐	Alarm Name	Alarm Level	System Predefined	Global Customizat...	Comments	Maintenance Experience	Operation
☐	Fan Failure	Critical	yes	no			
☐	Cold Start	Critical	yes	no			
☐	Disk Offline	Critical	yes	no			
☐	Array Operation Status	Critical	yes	no			
☐	Scheduled Recording Failure	Critical	yes	no			
☐	Cannot Access Storage Device	Critical	yes	no			
☐	Failed to Read Recording Data	Critical	yes	no			
☐	Abnormal Backup Resources	Critical	yes	no			
☐	Array Exception Cleared	Critical	yes	no			
☐	Entity Temperature Exceeds ...	Critical	yes	no	Entity Temperature Exceeds Critical Te... Please check entity state and environm...		

2. Click to view detailed information about an alarm type (edit is not allowed).



modify

* Alarm Source Name: Storage Device Access Failure

* Alarm name ID: 20 * Alarm Level: Critical Alarm Level Details

Device Model:

☐	Name
☐	general device
☐	XWARE
☐	Vehicle-mounted Camera
☐	VX500E
☐	VX500
☐	VX1500
☐	VOD5.0
☐	Uncontrollable SD Dome Camera

☐	Selected Devices	
☐	DM	
☐	DM3.5	
☐	DM5.0	
☐	VX500	
☐	VX500E	
☐	ECR3308-HF	
☐	ECR3316-HF	
☐	ECR3308-HF-E	

Maintenance Experience: The length limit is 255 bytes.

Description: Enter description

Confirm

Cancel

11.1.2 Global Customization

Global customization means after you change an alarm type, the change is effective to **all the applicable alarm sources**.

1. Go to **Device Management > Service Configuration > Alarm Service > Alarm Type** to view the predefined alarm type you want to edit.

Alarm Subscription		Alarm Parameter Configuration		Alarm Type		Third-Party Alarm Configuration	
Alarm Name:		Alarm Level: All		System Predefined: All		Search Reset	
+ Add		Delete		Refresh			
☐	Alarm Name	Alarm Level	System Predefined	Global Customizat...	Comments	Maintenance Experience	Operation
☐	Fan Failure	Critical	yes	no			⚠ ✎
☐	Cold Start	Critical	yes	no			⚠ ✎
☐	Disk Offline	Critical	yes	no			⚠ ✎
☐	Array Operation Status	Critical	yes	no			⚠ ✎
☐	Scheduled Recording Failure	Critical	yes	no			⚠ ✎
☐	Cannot Access Storage Device	Critical	yes	no			⚠ ✎
☐	Failed to Read Recording Data	Critical	yes	no			⚠ ✎
☐	Abnormal Backup Resources	Critical	yes	no			⚠ ✎
☐	Array Exception Cleared	Critical	yes	no			⚠ ✎
☐	Entity Temperature Exceeds ...	Critical	yes	no	Entity Temperature Exceeds Critical Te... Please check entity state and environm...		⚠ ✎
☐	Low temperature alarm	Critical	yes	no	Entity temperature is too low to each... Please check whether device supplies a...		⚠ ✎
total 547 < 1 2 3 4 5 ... 28 > 20 / page Go to							

2. Click ⚠. A page as shown below appears.

Alarm ✕

System Predefined:

Alarm Type: Fan Fault

Alarm Level: Critical

Global Customization:

Alarm Source Name:

Alarm Level: Critical Alarm Level Details

Confirm Restore Global Customization Stop

3. Edit the alarm name, alarm level.
4. Click **OK**.



NOTE!

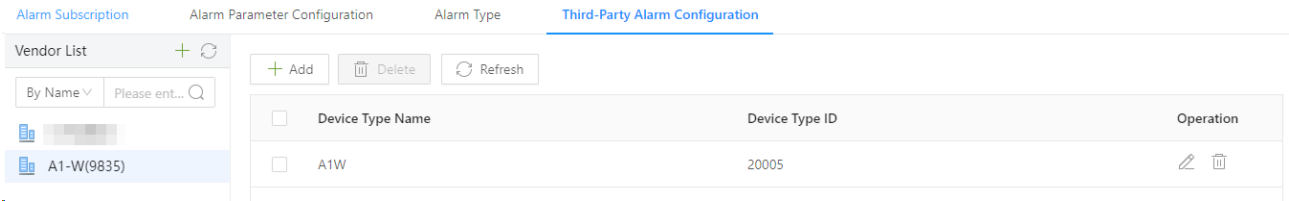
To restore the predefined alarm name and level, click **Restore Global Customization**.

11.2 Third-party Alarm Configuration

Add third-party devices and alarm types so the management platform can receive alarms from third-party devices.

11.2.1 Configure Third-party Device Type

Go to **Device Management > Service Configuration > Alarm Service > Third-party Alarm Configuration** to add third-party device types.



1. Configure Vendor Information

- Add vendor information:

1. Click  behind **Vendor List**.
2. Enter the vendor name, vendor ID, and a description, click **OK**.

Add Vendor ✕

* Vendor Name:

* Vendor ID:

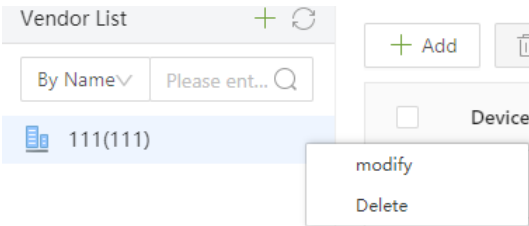
Description:

OK

Cancel

- Edit/delete vendor information:

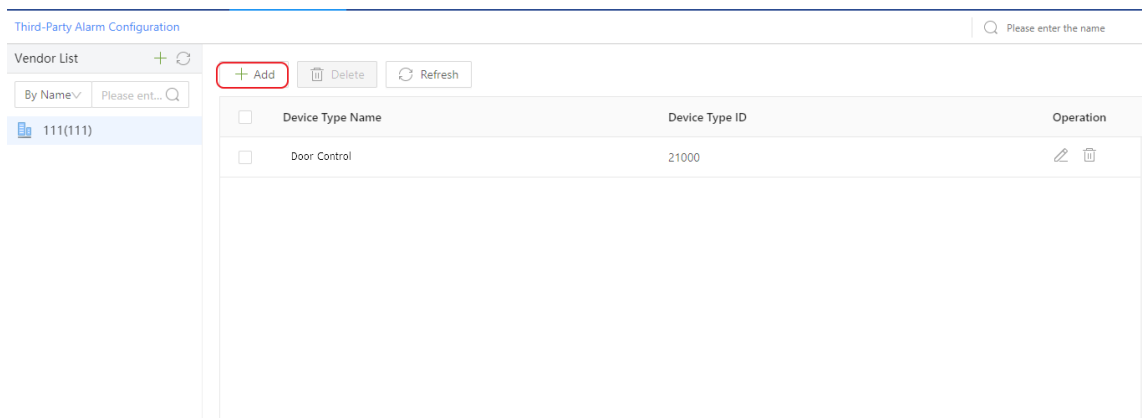
Right-click the vendor name, click **Modify** or **Delete**.



2. Configure Device Types

- Add device type

1. Choose an added vendor on the vendor list, click **Add**.



A page as shown below appears.

Add Device Type
✕

* Device Type Name:

* Device Type ID:

OK
Cancel

2. Enter the device type name, device ID (a number in the range 20000~40000), click **OK**.

- Edit device type

Click for the device type, change the name (ID cannot be changed).

- Delete device type

Click for the device type and then confirm the deletion.



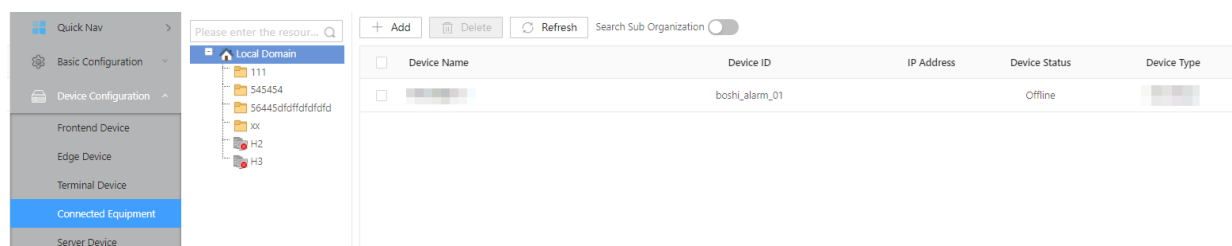
NOTE!

Before deleting a third-party device type, check that all the third-party devices of this type are deleted; otherwise, the device type cannot be deleted. See [Configure Third-party Device](#).

11.2.2 Configure Third-party Device

Add third-party devices to the system so the system can receive alarms from them.

Go to **Device Management > Connected Equipment** to configure third-party devices.



1. Add Third-Party Device

1. Click **Add**. A page as shown below appears.

Add
✕

* Device Type:

Please Select Device Type

▼

* Device ID:

Please Enter Device ID

* Device Name:

Please Enter Device Name

IP Address:

Please Enter IP Address

Port:

Please Enter Port

Service Management ...

Please Enter Service Management URL

Device Extended Info:

Please Enter Device Extended Info

Confirm

Cancel

2. Configure the parameters by referring to the table below. Click **OK** when you complete.

Parameter	Description
Device Type	Select a third-party device type from the drop-down list. Note: ● In addition to the existing device types, you can add more. (see Configure Device Types). ● After adding a PTZ controller, you need to connect it to the system via AG. Contact our technical support to install AG.
Device ID	ID of the third-party device.
Device Name	Name of the third-party device.
IP Address	IP address of the third-party device.
Port Number	Port number of the third-party device.
Service Management URL	Used to access the third-party device to perform service management operations.
Device Extended Info	Extended information about the third-party device.

2. Edit Third-party Device

In the third-party device list, click  for the device, and then edit the device information (device type and device ID cannot be changed).

☐	Device Name		Device ID	IP Address	Device Status	Alarm Type
☐	4564	 	12345679801191234567	192.168.1.88	Online	MeLucky Access Control Device

3. Delete Third-party Device

In the third-party device list, click  for the device, and then confirm the deletion.



CAUTION!

Deleting a third-party device will also delete the related alarm linkage (if configured)

11.2.3 Configure Third-party Alarm Type

In addition to the alarm types predefined in the system, you can add more alarm types as needed.

Typical scenarios for adding alarm types:

- **Scenario 1: Add alarm types for third-party device types**
Add alarm types for third-party device types so the system can receive alarms from these devices and perform alarm linkage.
- **Scenario 2: Add alarm types for DA-connected devices**
Add alarm types (if not defined) for devices connected to the system via DA, so the system can receive alarms from these devices and perform alarm linkage.

1. Add Alarm Type

1. Go to **Device Management > Service Configuration > Alarm Service > Alarm Type**.
2. Click **Add**. A page as shown below appears.

Add

* Alarm Source Name: Please enter the alarm name.

* Alarm name ID: * Alarm Level: Critical

Device Model:

☒	Name
☐	Uncontrollable SD Dome Camera
☐	Uncontrollable HD Dome Camera
☒	Ultra-clear face capture bayonet
☐	Toll Station
☐	Third-party Alarm
☐	TS5.0
☐	TS
☐	TMS7.1

☐	Selected Devices
☐	Ultra-clear face capture bayonet

Maintenance Experience: The length limit is 255 bytes.

Description:

3. Enter the alarm type name, alarm level ID, and choose an alarm level.



NOTE!

- Make sure the alarm type ID is unique in the local domain.
- You can click **Alarm Level Details** to add more alarm levels if necessary.

4. Add devices that support the alarm type (multiple selections allowed).
5. Enter maintenance experience and alarm description to facilitate alarm handling by other users.
6. Click **Confirm**.

2. Modify Alarm Type

You can edit the alarm type name, alarm level, and linked device types of custom alarm types that you added.

1. On the **Alarm Type** page, search the custom alarm type you want to edit.

Alarm Type Q Please enter the name

Alarm Source Name: Alarm Level: All System Predefined: No

☐	Alarm Source Name	Alarm Level	Comments	Maintenance Experience	Operation
☐	alarm001	Critical			Warning Edit Delete

- Click  for the alarm type you want to edit (alarm ID cannot be changed).

3. Delete Alarm Type

You can delete the custom alarm types that you have added.



NOTE!

Alarm types that are being used in alarm subscription cannot be deleted.

- On the **Alarm Type** page, search the custom alarm type you want to delete.
- Click  and then confirm the deletion.

11.3 Alarm Parameter Configuration

Go to **Device Management > Service Configuration > Alarm Service > Alarm Parameter Configuration** to configure SMS server, e-mail server, pop-up alarm window, resume previous video after playing alarm-triggered video.

11.3.1 SMS Server

Configure SMS server so the system can send important alarm information to user in the form of SMS message when an alarm occurs. For information about configuring alarm-triggered SMS, see [错误!未找到引用源。](#).



NOTE!

The SMS function requires an SMS modem. You can use the VM server as the SMS server: connect the SMS modem and the VM server with a USB cable, and install SMS modem service on the VM server.

SMS Server

* SMS Server Address:

* SMS Server Port:

Recipient Mobile Phone:

- Enter the actual SMS server's address and port number (keep the default setting if the VM server is used as the SMS server), click **OK**.
- Enter a mobile phone number and then click **SMS Test** to check whether the SMS message can be received properly.

11.3.2 Email Server

Configure E-mail service so the system can send important alarm information to user in the form of E-mail when an alarm occurs. For information about configuring alarm-triggered E-mail, see [错误!未找到引用源。](#) .



NOTE!

Please first configure an email server and make sure it operates properly.

Email Server

* Email Server Address: ?

* Email Server Port: ?

* Max Recipients of Bulk Messaging: ?

☒ Email server requires ID verification.

Verify Username: ?

Verify Password: ?

Sender: ?

* Sender E-mail Address: ?

3. Configure email server parameters, click **OK**.

Parameter	Description
Email Server Address/Port	Address and port number (default 24) of the SMTP server.
Max Recipients of Bulk Messaging	Maximum number of recipients that the email server supports each time. The value shall be set according to the email server's actual capability. A value exceeding the limit will cause alarm-triggered email to fail.
Verify Username/Password	If Email server requires ID verification is enabled, you need to set the username/password of the recipient's email to ensure the security of information transmitted by both parties and to verify the authenticity and reliability of the website.
Sender	(Optional) Used for the recipient to identify the sender.
Sender Email Address	The email will be sent from the set email address.

4. Click **Test E-mail**. The system will send a test email from the set email address to the same email address.

11.3.3 Alarm Pop-up Window

When enabled, an alarm window pops up in the lower-right corner of the screen to alert the user when an alarm occurs.

Alarm Pop-up Window Configuration

Enable Alarm Pop-up Window:

☐

After the display time is set, the pop-up alarm window disappears automatically when the time expired.

Display Time in Pop-Up Window:



OK

11.3.4 Resume Previous Video on Monitor after Playing Alarm-triggered Live Video

If this function is enabled and the monitor was playing live video before playing an alarm-triggered live video, then after the recover time is over, the monitor will continue the previous live video; otherwise, the monitor will be in idle status.

Restore Stream Settings for Alarm Triggered Playing on Monitor

* Restore Stream Output: ☒ Yes ☐ No

Please enter an integer in the range of [1-360000].

* Recover Time (s):



OK

Parameter	Description
Restore Stream Output	Whether to enable resuming the previous video streaming. This setting is disabled by default.
Recover Time	Set the time to resume the previous video streaming. The previous video will be resumed after the set time is over. Note: ● If the current alarm-triggered live video is replaced by another alarm-triggered live video before the current recover time is over, then the recover time will be timed again. ● If a device event (for example, encoder/decoder or MS is disconnected) occurs before stream settings are restored, the original stream settings will be restored immediately on the monitor when the event is detected by the system, regardless of whether the recover time is over.

11.4 Alarm Subscription

Configure alarm subscription rules so the specified users can receive alarms. When an alarm occurs, the system pushes the alarm to all the online users according to the alarm subscription rules.



NOTE!

The system has a predefined rule.

- The predefined rule subscribes to alarms of all sources and all levels. You may choose alarm levels according to the actual needs.
- The predefined rule includes admin (so admin can view all alarms). You may add other users to the predefined rule as needed.

11.4.1 Configure Alarm Subscription Rules

1. Go to **Device Management > Service Configuration > Alarm Service > Alarm Subscription**.

The screenshot shows the 'Alarm Subscription' page under 'Device Management > Service Configuration > Alarm Service'. The left sidebar contains a 'Quick Nav' menu with options: Basic Configuration, Device Configuration, Platform Cascading, Service Configuration (selected), Storage Service, Display Control, Alarm Service (highlighted), and Asset Management. The main area has tabs for 'Alarm Subscription', 'Alarm Parameter Configuration', 'Alarm Type', and 'Third-Party Alarm Configuration'. The 'Alarm Subscription' tab is active, showing a 'Rule Name' input field, 'Search', and 'Reset' buttons. Below are '+ Add', 'Delete', and 'Refresh' buttons. A table lists subscription rules with columns: Rule Name, System Predefined, Alarm Level, and Operation. One rule is shown: 'System Pre-defined Rule 1' with 'yes' for System Predefined, 'Critical, Major, Minor, Warning, Note' for Alarm Level, and edit/delete icons for Operation.

2. Click **Add** to add subscription rules.
3. Select alarm devices. You can select devices directly or by alarm type.



NOTE!

The alarm source list lists all the devices in the user's organization and its sub-organizations (including external domain and external-domain organization), not including devices to which the user has no permission.

- Select by device: On the **Local Domain** tab, select devices, and then click ➔.

The 'Add' dialog box shows a three-step process: 1. Select Alarm Device, 2. Select Alarm Subscriber, and 3. Fill Alarm Info. The 'Local Domain' tab is selected under 'Alarm Type'. A search bar 'Enter the resource name' is at the top. A list of devices follows, including IP addresses (192.168.1.114, 192.168.1.118, 192.168.1.122, 192.168.1.123) and camera names (12345678901144567895-cam-03, etc.). The device 192.168.1.118 is selected with a blue checkmark. A blue arrow button points from the list to the 'Selected Alarm Sources' table. This table has columns 'Selected Alarm Source' and 'Operation'. It contains one entry: 192.168.1.118 with a delete icon. A 'Delete' button is at the top right of the table. At the bottom of the dialog are 'Next' and 'Cancel' buttons.

- Select by alarm type: On the **Alarm Type** tab, select alarm sources of a certain type, and then click ➔.

Add
×

1 Select Alarm Device
2 Select Alarm Subscriber
3 Fill Alarm Info

Local Domain Alarm Type

▼

●

Alarm Aource

☒ Video Alarm Source
☐ Alarm Input Source
☐ Third-Party Device Alarm Source
☐ Device O&M Alarm Source
☐ Checkpoint Alarm Source

Selected Alarm Sources Delete

☐	Selected Alarm Source	Operation
☐	Video Alarm Source	🗑️

➔

Next
Cancel

4. Click **Next** to select alarm subscribers.



NOTE!

The left-side list lists all the viewable users in the current organization according to your permission, and the right-side list lists all the users corresponding to the rule (not including users that you have no permission to view).

5. Select users from the list and then click ➔.

Add
×

✓ Select Alarm Device
2 Select Alarm Subscriber
3 Fill Alarm Info

Enter the resource name 🔍

🏠

Local Domain

☐ 001
☐ 002
☐ JayClou
☐ joker
☐ loadmin

12333

124

125

126

127

128

129

130

145

Selected Users Delete

☐	Selected User	Operation
☐	001	🗑️

➔

Back
Next
Cancel

6. Click **Next**, enter the alarm subscription name and alarm level.

7. Click **OK**.

The rule appears on the **Alarm Subscription** page. Users specified in the rule can receive the subscribed alarms.

11.4.2 Manage Alarm Subscription Rules

- View alarm source: Click to view alarm sources included in the rule.

View Alarm Source ✕

Alarm Source Name: Search Reset

Alarm Source Name	Device Model
192.168.15.114	Camera

- Edit subscription rule: Click  to edit the subscription rule.



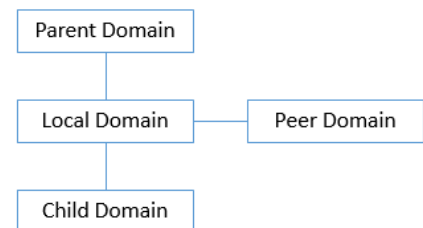
NOTE!

A user in a sub-organization cannot view alarm sources in the parent organization when viewing an alarm subscription rule. If the users changes the alarm subscription rule, it doesn't change alarm sources in the related parent organization.

- Delete subscription rule: Click . The system predefined subscription rule cannot be deleted. (The system predefined rules cannot be deleted)

12 Platform Casading

In a large surveillance application system, the video surveillance system needs to be divided into multiple independent surveillance systems known as domains in accordance with application requirements. These domains connect to the platform via cascading or interconnection to share resources with each other, and this requires multi-level and multi-domain configuration for unified management and deployment.



Inter-domain management can achieve external domain interconnection, resource sharing, and can interconnect independent and divided surveillance domains to provide unified management and alarming, inter-domain monitoring, and it plays an important role in networked monitoring.

The local domain has three types of external domains: parent domain, child domain, and peer domain. A child domain can share resources with its parent domain, and peer domains can share resources with each other.



Note!

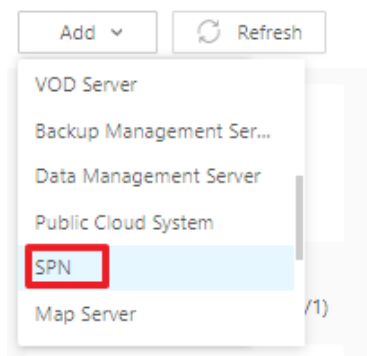
Before adding Higher-level Platform, Peer Platform and Lower-level Platform, complete the [SPN server configuration](#) and [Inter-Domain Communication Protocol Configuration](#).

12.1 SPN Server Configuration

A Share Process Node (SPN) server is used to push shared resources among domains to realize inter-domain monitoring and operations.

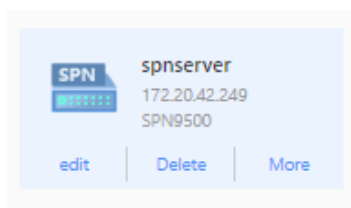
Add SPN

1. Go to **Device Management > Server Device**.
2. Click **Add**, select **SPN**.



- On the page as shown below, enter the device name (user-defined), device ID (same as the device ID configured on the server), device model (SPN8500/SPN9500/SPN12500), enter asset information as needed.

- Click **Confirm**. The device is added (blue means “online”, gray means “offline”).



SPN management operations:

Operation	Description
Edit device	Click Edit to edit device name and asset information.
Delete device	Click Delete and then confirm. Caution: Cannot delete an SPN that is bound to an external domain.
View the bound external domains	Click More to view external domains the device is bound to.

12.2 Platform Configuration

12.2.1 Inter-Domain Communication Protocol Configuration

Log in to the management platform of the **local domain** and the **external domain**, respectively, to configure the inter-domain communication protocol.

- Go to **Device Management > Platform Cascading > Platform Configuration > Inter-Domain Communication Protocol Configuration**.

2. Configure the parameters by referring to the table below.

Platform interconnection communication protocol configuration

GB	* Platform Level:	4
Private Protocol		
DB33 2012	* Interconnection ID:	20240131002000000001
DB33 2010		
DB33	* Interconnection User ID:	20240131002000000001_user
		<button>Confirm</button>

Table 12-1 Parameter Descriptions

Parameter	Description
Inter-Domain Communication Protocol	Choose a protocol, and then configure the protocol. Note: The local domain supports multiple inter-domain communication protocols to meet different networking requirements.
Domain Level	We can know the relationship between the local domain its external domain by comparing their levels (from low to high is 1 to 7): Parent domain level > Local domain level Peer domain level = Local domain level Child domain level < Local domain level
Inter-Domain Domain ID	The domain ID must conform to the inter-domain communication protocol you chose. For GB, inter-domain domain IDs are 20 digits long, and digits 11-13 are 200. For other protocols, there are no specific requirements. Note: For the same inter-domain communication protocol, duplicate domain IDs are not allowed. If you change the inter-domain domain ID after the external domain is added, the system will prompt you to restart service. Follow on-screen instructions and perform with caution.
Inter-Domain User ID	The inter-domain user ID must conform to the inter-domain communication protocol you chose. Note: For the same inter-domain communication protocol, duplicate user IDs are not allowed, and inter-domain user IDs must be different from inter-domain domain IDs. If you change the inter-domain user ID after the external domain is added, the system will prompt you to restart service. Follow on-screen instructions and perform with caution.

3. Click **OK**. The system will restart service.

12.2.2 GB Code Verification

1. Go to **Device Management > Platform Cascading > Platform Configuration > GB Code Verification**.
2. Click ☐ to enable GB code verification.

Figure 12-1 GB Code Verification

GB/T 28181 Code Check

Enable GB/T 28181 Code Check ☐

Note: If this feature is enabled, the system will perform GB code verification in case of sharing cameras.

If this field is enabled, the local domain will use the camera GB code as the sharing ID when sharing camera resources to the parent domain by default. If this field is not enabled, the device ID will be used as the sharing ID. It is recommended to enable it for GB inter-domain use.

12.2.3 Local Domain Administrative Division Configuration

1. Go to **Device Management > Platform Cascading > Platform Configuration > Local Domain Administrative Division Configuration**.
2. Click the drop-down box to select the administrative area to which the local domain belongs.

Figure 12-2 Administrative Area of Local Domain

Local Domain Administrative Division Configuration

Administrative Area:

Confirm

3. After selecting the administrative area, click **GB Sharing ID Data Dictionary** on the **Parent Domain**, **Peer Domain**, and **Child Domain** tabs to view the administrative areas on the **GB Sharing ID Data Dictionary** page. Only the administrative areas to which the domains belong are displayed. All administrative areas in the country are displayed when the administrative area of the local domain is not configured.

Figure 12-3 GB Shareing ID Data Dictionary

GB/T 28181 Sharing ID Data Dictionary

Administrative Area

Industry Code

Category Code

Network Type

Add

Name	code	Level	Operation
------	------	-------	-----------

12.2.4 Camera Type Settings

1. Go to **Device Management > Platform Cascading > Platform Configuration > Camera Type Settings**.
2. Click the drop-down box to select the camera type (131 or 132). The default value is 131.

Figure 12-4 Camera Type Settings

Camera Type Setting

Camera Type:

Note: It is used when the GB code of the camera is generated automatically. The default type is 131.

Confirm

- When you add a frontend device on the **Device Management > Frontend Device** page, fill in the required information and click **Next**. The camera GB code will be automatically generated based on the value set for the camera type. If the camera type is 131, bits 11-13 of the camera GB code shall be 131. If the camera type is 132, bits 11-13 of the camera GB code shall be 132.

Figure 12-5 Camera GB Code

The screenshot shows a configuration form for a video device. The fields are as follows:

Video Device	
Protocol type:	GB/T 28181 Protocol
Camera Type:	PTZ Camera
Camera GB Code:	01234567891310000016
Camera Channel Type:	☒ Single-Chann... ☐ Multi-channel ...
Camera subtype:	Common Camera
Camera Capability:	normal

12.3 External Domain Management

On the **Device Management > Platform Cascading > Higher-level Platform** page, you can add and manage the Higher-level Platform.

On the **Device Management > Platform Cascading > Peer Platform** page, you can add and manage the Peer Platform.

On the **Device Management > Platform Cascading > Lower-level Platform** page, you can add and manage the Lower-level Platform.

Add external domains, so the platform can establish connections with external-domain servers and build a multi-domain network environment.



Note!

You need to complete the configuration of SPN and inter-domain communication protocol first. See [SPN Server Configuration](#) and [Inter-domain Interconnection Configuration](#).

Log in to the management platforms of the **local domain and the external domain separately**, and add each other's platform as an external domain.

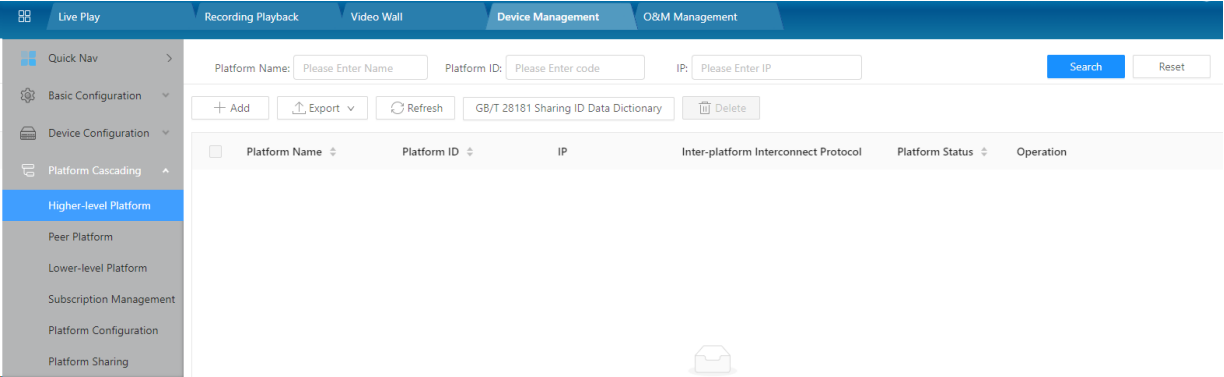
- Add Higher-level Platform: On the **Higher-level Platform** page of the local domain, add the Higher-level Platform. On the **Lower-level Platform** page of the Higher-level Platform, add the local domain.
- Add Peer Platform: On the **Peer Platform** page of the local domain, add the Peer Platform. On the **Peer Platform** page of the Peer Platform, add the local domain.
- Add Lower-level Platform: On the **Lower-level Platform** page of the local domain, add the Lower-level Platform. On the **Higher-level Platform** page of the Lower-level Platform, add the local domain.

12.3.1 Higher-level Platform

1. Add Higher-level Platform

- Go to the **Device Management > Platform Cascading** page and select **Higher-level Platform**.

Figure 12-6 Higher-level Platform



2. Click **Add** to go to the **Add Higher-level Platform** page.
3. Configure the required information. Different parameter items will be displayed for different parameter values configured. The actual page shall prevail.
4. Click **OK** to save the configuration.
You can also click **Next** to configure the optional information. Then, click **OK** to complete the addition of the Higher-level Platform.
5. After adding the local domain as the Lower-level Platform on the Higher-level Platform, click **Refresh** on the **Higher-level Platform** page. The corresponding Higher-level Platform will be online.

Figure 12-7 Add Higher-level Platform - Required Information

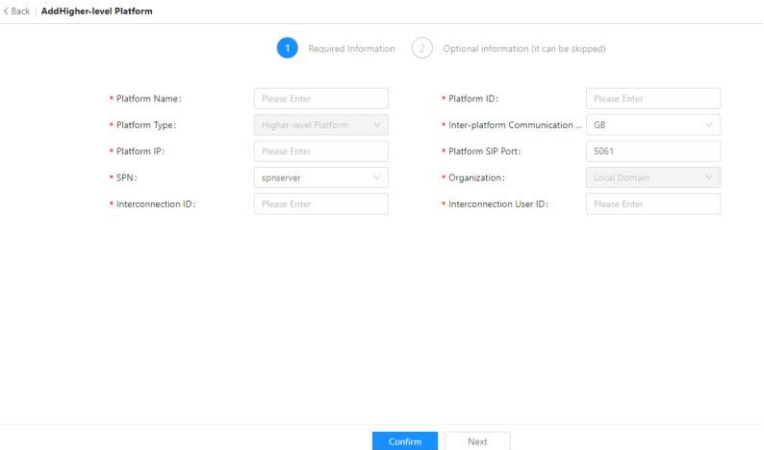


Figure 12-8 Add Higher-level Platform - Optional Information

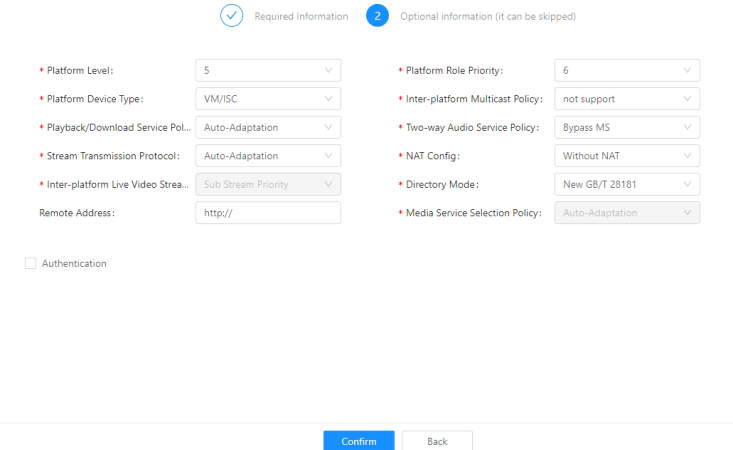


Table 12-2 Parameter Descriptions for Higher-level Platform

Parameter	Description
Platform ID	ID of the Higher-level Platform used in the local domain. The ID must be unique in the local domain.
Platform Name	Name of the Higher-level Platform used in the local domain.
Platform Type	Default is Higher-level Platform, not allow edit.
Inter-Platform Communication Protocol	Choose the appropriate protocol according to the network environment. Support GB protocol, private protocol, DB33, DB33 2012
Platform IP	IP address of the Higher-level Platform server. Currently only IPv4 IP addresses are allowed.
Platform SIP Port	Used for signaling interaction with other domains. Make sure the setting is consistent with the SIP port configured on the server in the Higher-level Platform.
SPN	Select the SPN Server to be used to share and push inter-domain resources.
Organization	The Higher-level Platform can only be added under the root node and displayed in parallel with the local domain, and it is displayed only for admin in the resource tree.
Inter-Domain Domain ID	After you select an inter-domain communication protocol, set an inter-domain domain ID that conforms to the protocol specifications. Note: Make sure the setting is unique and consistent with the corresponding inter-domain interconnection parameters configured for this Higher-level Platform.
Inter-Domain User ID	After you select an inter-domain communication protocol, set an inter-domain user ID that conforms to the protocol specifications. Note: Make sure the setting is unique and consistent with the corresponding inter-domain interconnection parameters configured for this Higher-level Platform.
Platform Level	Level of the Higher-level Platform (low to high is 1-7). See Inter-Domain Communication Protocol Configuration .
PlatformRole Priority	Priority level of the Higher-level Platform when using resources in the local domain (low to high is 1 to 63).
Platform Type	Platform type of the Higher-level Platform server. Note: When adding a third-party platform, choose "other".
Inter-Platform Multicast Policy	Whether inter-domain networking supports multicast. Note: Inter-domain multicast is not available when the inter-domain communication protocol is Sichuan Electrics Power Corporation.
Playback/Download Service Policy	Configure inter-domain playback/download service selection policy. ● Auto-Adaptation: If MS is not available, streams will not pass through MS. If MS is available, streams will pass through MS as the first option. ● Bypass MS: Inter-domain playback/download streams will not pass through MS in the local domain. Note: Whether inter-domain playback streams pass through MS is determined by multiple configurations and whether MS is deployed. See Local Configuration > Video Parameters > Advanced Configuration > Playback Service Selection Policy . The service selection policy for inter-domain download is similar to that for inter-domain playback.
Two-way Audio Service Policy	● Auto-Adaptation: Whether inter-domain two-way audio passes through MS is determined by the system based on the deployment of MS. If MS is not available, two-way audio will not pass through MS; if MS is available, two-way audio will pass through MS as the first option.

Parameter	Description
	● Bypass MS: Inter-domain two-way audio will not pass through MS in the local domain.
Stream Transmission Protocol	● Auto-Adaptation: Decoding terminals in the Higher-level Platform can receive UDP or TCP live video streams from the local domain. This is determined by the system through auto-negotiation. This is the default setting. ● UDP: The decoding terminal in the Higher-level Platform receives only UDP live video streams from the local domain. Note: This parameter can be set to UDP only when the inter-domain communication protocol is GB.
NAT Configuration	● If the external domain is behind the NAT and the local domain is in front of the NAT, choose External Domain Behind the NAT. ● If the local domain is behind the NAT and the external domain is in front of the NAT, choose External Domain in Front of the NAT. ● If the local domain and the external domain are behind separate NATs, choose Device and Local Domain Behind Separate NATs. ● If inter-domain streams do not need to traverse the NAT, choose No NAT. Note: If GAP is configured in the network, choose No NAT.
Inter-Domain Live Video Stream Policy	When the live video stream policy is Auto-Adaptation, choose the inter-domain live video stream that the system prefers during negotiation. The default is Sub Stream Priority. ● Main Stream Priority: During negotiation, the system chooses stream types in main/sub/third order and prefers the main stream. ● Sub Stream Priority: During negotiation, the system chooses stream types in sub/third/main order and prefers the sub stream. ● Third Stream Priority: During negotiation, the system chooses stream types in third/sub/main order and prefers the third stream. Note: This parameter is configurable only when the external domain is a parent domain or a peer domain, and the inter-domain communication protocol is DB33, DB33 2010, DB33 2012, or Private. Configure local-domain live video stream policy by referring to Central Server > Server Settings.
Target Stream Format	The default is the original stream. This setting affects the format of streams received by the parent domain or the peer domain. ● Onvif to UDP+TS: Streams from Onvif cameras in the local domain are transcoded by MS and then sent to the parent domain as UPD+TS streams. ● Onvif to RTP+TS: Streams from Onvif cameras in the local domain are transcoded by MS and then sent to the parent domain as RTP+TS streams. Note: This parameter is configurable only when the external domain is a parent domain or a peer domain, and the inter-domain communication protocol is DB33 2012 or Private.
Directory Mode	Methods of pushing and mounting resources between GB domains. ● New GB: New GB/T 28181 (GB2016 and later). ● Old GB: Old GB/T 28181 (GB2014 and earlier). ● Administrative Area: New GB protocol based on administrative division. ● Parent organization: Both the pushed organizations and cameras carry the sharing ID of the parent organization of the resources, and the parent organization is mounted when you mount the resources. Note: This parameter is configurable only when the inter-domain communication protocol is set to GB.
Remote Address	Higher-level Platform no need to config.
Media Service Selection Policy	● Auto-Adaptation: (default) Whether live video streams sent to the Higher-level Platform pass through MS is determined by the system based on the media service selection policy of the encoding device or the external domain and on whether MS is deployed.

Parameter	Description
	- Specified MS: Live video streams sent to the Higher-level Platform must pass through the specified MS. - Specified MS group: Live video streams sent to the Higher-level Platform must pass through an MS in the specified MS group. - Bypass MS: Live video streams sent to the Higher-level Platform will not pass through MS. Note: If MS is deployed but has insufficient forwarding capability, then Direct Connection First will be adopted.
Authentication	When Authentication is selected, you need to config Username, Password, Domain Name used for authentication of the external domain, and the Username, Password, Domain Name must be the same in both domains. Note: When the inter-domain communication protocol is not DB33, this parameter can be set

2. Edit Higher-level Platform

Click **More** in the **Action** column of the parent domain list, and select **Edit Platform** to go to the **Edit Higher-level Platform** page. After editing the parameters, click **OK** to save the modification.



Note!

Parameters grayed out on the page, such as platform code, platform type, and inter-platform interconnection protocol, cannot be modified.

Figure 12-9 Edit Higher-level Platform - Required Information

< Back | Modify Higher-level Platform(H1)

1 Required Information

2 Optional information (it can be skipped)

* Platform Name:	H1	* Platform ID:	65101000002001000013
* Platform Type:	Higher-level Platform	* Inter-platform Communication ...	GB
* Platform IP:	2013:192:118:4::121	* Platform SIP Port:	5061
* SPN:	spnserver	* Interconnection ID:	65101000002001000015
* Interconnection User ID:	65101000002001000015_user		

Confirm

Next

Figure 12-10 Edit Higher-level Platform - Optional Information

✓ Required Information

2 Optional information (it can be skipped)

* Platform Level:

5

* Platform Device Type:

VM/ISC

* Playback/Download Service Pol...

Auto-Adaptation

* Stream Transmission Protocol:

Auto-Adaptation

* Inter-platform Live Video Strea...

Sub Stream Priority

Remote Address:

http://

* Platform Role Priority:

6

* Inter-platform Multicast Policy:

not support

* Two-way Audio Service Policy:

Bypass MS

* NAT Config:

Without NAT

* Directory Mode:

New GB/T 28181

* Media Service Selection Policy:

Auto-Adaptation

☐ Authentication

Confirm

Back

3. Delete Higher-level Platform

Before deleting the Higher-level Platform, you need to confirm that:

The Higher-level Platform has canceled the [subscription to alarms](#) and [subscription to directories](#) from the local domain. The local domain has [canceled the sharing](#) of resources with the Higher-level Platform.

To delete the Lower-level Platform, do as follows:

- Delete one by one: Click **More** in the **Action** column of the Higher-level Platform list, and select **Delete Platform**.
- Batch Delete: Select multiple Higher-level Platforms in the Higher-level Platform list, and click **Delete** at the top of the list.

4. Search Higher-level Platform

You can search Higher-level Platforms by name, interconnection code, and IP address.

Figure 12-11 Search Criteria for Higher-level Platform

名称:

互联编码:

IP:

查询

重置

5. Export Higher-level Platform

You can export the Higher-level Platform information to an Excel file.

- Export Selected: Select multiple Higher-level Platforms in the Higher-level Platform list, and click **Export** > **Export Selected** at the top of the list to export the selected Higher-level Platforms.
- Export All: Click **Export** > **Export All** to export all Higher-level Platforms.

Figure 12-12 Export Higher-level Platform

+ Add

Export

☒ Platform

☒ H1

Export Selected

Export All

12.3.2 Peer Platform

1. Add Peer Platform

1. Go to **Device Management > Platform Cascading** and select **Peer Platform**.

Figure 12-13 Peer Platform page

The screenshot shows the 'Peer Platform' page under 'Platform Cascading'. On the left is a sidebar with navigation options: Quick Nav, Basic Configuration, Device Configuration, Platform Cascading (selected), Higher-level Platform, Peer Platform (highlighted), Lower-level Platform, Subscription Management, Platform Configuration, and Platform Sharing. The main area has a header with search filters: Platform Name (Please Enter N...), Platform ID (Please Enter code), IP (Please Enter IP), and Organization (本城). There are buttons for '+ Add', 'Export', 'Refresh', and 'Delete', along with a 'Search External Domain Resources' button. Below is a table with columns: Platform Name, Platform ID, IP, Inter-platform Interconnect Protocol, Platform Status, and Operation. One entry is visible: H2, 6510100002001000017, 2013:192:1184:126, GB, Offline. The Operation column has links for 'Shared Resource', 'Search shared resource', 'Resources shared from others', and 'More'.

2. Click **Add** to go to the **Add Peer Platform** page.
3. Configure the required information for the Peer Platform. Different parameter items will be displayed for different parameter values configured. The actual page shall prevail.
4. Click **OK** to save the configuration.
You can also click **Next** to configure the optional information. Then, click **OK** to complete the addition of the Peer Platform.
5. After adding the local domain as the Peer Platform on the Peer Platform, click **Refresh** on the **Peer Platform** page. The corresponding Peer Platform will be online.

Figure 12-14 Add Peer Platform - Required Information

The screenshot shows the 'Add Peer Platform' page. At the top, there's a breadcrumb: '< Back | AddPeer Platform'. Below it are two tabs: '1 Required Information' (active) and '2 Optional information (it can be skipped)'. The 'Required Information' section contains several fields: Platform Name (Please Enter), Platform ID (Please Enter), Platform Type (Peer Platform), Platform IP (Please Enter), SPN (spnserver), Interconnection ID (Please Enter), Inter-platform Communication ... (GB), Platform SIP Port (5061), Organization (Local Domain), and Interconnection User ID (Please Enter). At the bottom, there are 'Confirm' and 'Next' buttons.

Figure 12-15 Add Peer Platform - Optional Information

[< Back](#) | **AddPeer Platform**

✓ Required Information
2 Optional information (it can be skipped)

* Platform Level:

* Platform Device Type:

* Playback/Download Service Pol...:

* Two-way Audio Service Policy:

* NAT Config:

* Directory Mode:

* Media Service Selection Policy:

* Platform Role Priority:

* Inter-platform Multicast Policy:

* Max. Directly-Connected Strea...:

* Stream Transmission Protocol:

* Inter-platform Live Video Strea...:

Remote Address:

☒ Authentication

* User Name:

Domain Name:

* Password:

Confirm
Back

Table 12-3 Parameter Descriptions for Adding a Peer Platform

Parameter	Description
Platform ID	ID of the Peer Platform used in the local domain. The ID must be unique in the local domain.
Platform Name	Name of the Peer Platform used in the local domain.
Platform Type	Default is Peer Platform, not allowed edit.
Inter-Platform Communication Protocol	Choose the appropriate protocol according to the network environment. Support GB protocol, private protocol, DB33, DB33 2012
PlatformIP	IP address of the Peer Platform server. Currently only IPv4 IP addresses are allowed.
PlatformSIP Port	Used for signaling interaction with other domains. Make sure the setting is consistent with the SIP port configured on the server in the Peer Platform.
SPN	Select the SPN Server to be used to share and push inter-domain resources.
Organization	Peer Platform can only be added to the local domain or below an organization of the local domain.
Inter-Domain Domain ID	After you select an inter-domain communication protocol, set an inter-domain domain ID that conforms to the protocol specifications. Note: Make sure the setting is unique and consistent with the corresponding inter-domain interconnection parameters configured for this Peer Platform.
Inter-Domain User ID	After you select an inter-domain communication protocol, set an inter-domain user ID that conforms to the protocol specifications. Note: Make sure the setting is unique and consistent with the corresponding inter-domain interconnection parameters configured for this Peer Platform.
Platform Level	Level of the Peer Platform (low to high is 1-7). See Inter-Domain Communication Protocol Configuration .
Platform Role Priority	Priority level of the Peer Platform when using resources in the local domain (low to high is 1 to 63).

Parameter	Description
Platform Type	Platform type of the Peer Platform server. Note: When adding a third-party platform, choose “other”.
Inter-Platform Multicast Policy	Whether inter-domain networking supports multicast. Note: Inter-domain multicast is not available when the inter-domain communication protocol is Sichuan Electric Power Corporation.
Playback/Download Service Policy	Configure inter-domain playback/download service selection policy. ● Auto-Adaptation: If MS is not available, streams will not pass through MS. If MS is available, streams will pass through MS as the first option. ● Bypass MS: Inter-domain playback/download streams will not pass through MS in the local domain. Note: Whether inter-domain playback streams pass through MS is determined by multiple configurations and whether MS is deployed. See Local Configuration > Video Parameters > Advanced Configuration > Playback Service Selection Policy . The service selection policy for inter-domain download is similar to that for inter-domain playback.
Max. Directly-Connected Stream Count	This parameter limits the maximum number of unicast, direct-connection based live video streams of IPCs in the Peer Platform in the local domain. It is effective only when Direct Connection First is enabled on the decoding terminal. That means, when a direct-connection-first enabled decoding terminal in the local domain establishes live video with an encoding terminal in the peer domain, the system checks whether the Max. Directly-Connected Stream Count is exceeded. If not exceeded, live video streams will be transmitted directly from the encoding terminal to the decoding terminal; otherwise, if MS is deployed in the local domain, live video streams will be forwarded via MS as the first option; if MS is not deployed, live video streams will still be transmitted directly from the encoding terminal to the decoding terminal. Note: The modified Max. Directly-Connected Stream Count takes effect the next time live video is established.
Two-way Audio Service Policy	● Auto-Adaptation: Whether inter-domain two-way audio passes through MS is determined by the system based on the deployment of MS. If MS is not available, two-way audio will not pass through MS; if MS is available, two-way audio will pass through MS as the first option. ● Bypass MS: Inter-domain two-way audio will not pass through MS in the local domain.
Stream Transmission Protocol	● Auto-Adaptation: Decoding terminals in the local domain can receive UDP or TCP live video streams from the Peer Platform. This is determined by the system through auto-negotiation. This is the default setting. ● TCP: The decoding terminal in the local domain receives only TCP live video streams from the Peer Platform. Note: This parameter can be set to TCP only when the inter-domain communication protocol is Private or GB.
NAT Configuration	● If the Peer Platform is behind the NAT and the local domain is in front of the NAT, choose External Domain Behind the NAT. ● If the local domain is behind the NAT and the Peer Platform is in front of the NAT, choose External Domain in Front of the NAT. ● If the local domain and the Peer Platform are behind separate NATs, choose Device and Local Domain Behind Separate NATs. ● If inter-domain streams do not need to traverse the NAT, choose No NAT. Note: If GAP is configured in the network, choose No NAT .
Inter-Platform Live Video Stream Policy	When the live video stream policy is Auto-Adaptation , choose the inter-domain live video stream that the system prefers during negotiation. The default is Sub Stream Priority .

Parameter	Description
	● Main Stream Priority: During negotiation, the system chooses stream types in main/sub/third order and prefers the main stream. ● Sub Stream Priority: During negotiation, the system chooses stream types in sub/third/main order and prefers the sub stream. ● Third Stream Priority: During negotiation, the system chooses stream types in third/sub/main order and prefers the third stream. Note: This parameter is configurable only when the inter-domain communication protocol is DB33, DB33 2010, DB33 2012, or Private. Configure local-domain live video stream policy by referring to Central Server > Server Settings.
Target Stream Format	The default is the original stream. ● Onvif to UDP+TS: Streams from Onvif cameras in the local domain are transcoded by MS and then sent to the parent domain as UPD+TS streams. ● Onvif to RTP+TS: Streams from Onvif cameras in the local domain are transcoded by MS and then sent to the parent domain as RTP+TS streams. Note: This parameter is configurable only when the inter-domain communication protocol is DB33 2012 or Private.
Directory Mode	Methods of pushing and mounting resources between GB domains. ● New GB: New GB/T 28181 (GB2016 and later). ● Old GB: Old GB/T 28181 (GB2014 and earlier). ● Administrative Area: New GB protocol based on administrative division. ● Parent organization: Both the pushed organizations and cameras carry the sharing ID of the parent organization of the resources, and the parent organization is mounted when you mount the resources. Note: This parameter is configurable only when the inter-domain communication protocol is set to GB.
Remote Address	URL address of the external domain server, used to manage the external domain server remotely.
Media Service Selection Policy	● Auto-Adaptation: (default) Whether live video streams from the Peer Platform pass through MS is determined by the system based on the media service selection policy of the encoding device or the external domain and on whether MS is deployed. ● Specified MS: Live video streams of the Peer Platform must pass through the specified MS. ● Specified MS group: Live video streams of the Peer Platform must pass through an MS in the specified MS group. ● Bypass MS: Live video streams in the Peer Platform will not pass through MS. Note: If MS is deployed but has insufficient forwarding capability, then Direct Connection First will be adopted.
Authentication	When Authentication is selected, you need to config Username, Password, Domain Name used for authentication of the external domain, and the Username, Password, Domain Name must be the same in both domains. Note: When the inter-domain communication protocol is not DB33, this parameter can be set
Max External Domain Backup Channels	Maximum number of backup channels for the Peer Platform. The default value is 0, which means no limit. Note: This parameter is configurable only when the central server has enabled backup channel limit for external domains.

2. Edit Peer Platform

Click **More** in the **Action** column of the Peer Platform list, and select **Edit Platform** to go to the **Edit Peer Platform** page. After editing the parameters, click **OK** to save the modification.



Note!

Parameters grayed out on the page, such as platform code, platform type, and inter-platform interconnection protocol, cannot be modified.

Figure 12-16 Edit Peer Platform - Required Information

< Back | ModifyPeer Platform(H2)

1 Required Information 2 Optional information (it can be skipped)

* Platform Name:	H2	* Platform ID:	65101000002001000017
* Platform Type:	Peer Platform	* Inter-platform Communication ...	GB
* Platform IP:	2013:192:118:4::126	* Platform SIP Port:	5061
* SPN:	spnserver	* Interconnection ID:	65101000002001000018
* Interconnection User ID:	65101000002001000018_user		

Figure 12-17 Edit Peer Platform - Optional Information

1 Required Information 2 Optional information (it can be skipped)

* Platform Level:	4	* Platform Role Priority:	6
* Platform Device Type:	VM/ISC	* Inter-platform Multicast Policy:	not support
* Playback/Download Service Pol...	Auto-Adaptation	* Max. Directly-Connected Strea...	1024
* Two-way Audio Service Policy:	Bypass MS	* Stream Transmission Protocol:	Auto-Adaptation
* NAT Config:	Without NAT	* Inter-platform Live Video Strea...	Sub Stream Priority
* Directory Mode:	New GB/T 28181	Remote Address:	http://
* Media Service Selection Policy:	Auto-Adaptation		

☒ Authentication

* User Name:		* Password:	
Domain Name:			

Confirm Back

3. Delete Peer Platform

Before deleting the Peer Platform, you need to confirm that:

- The Peer Platform has canceled the [subscription to alarms](#) and [subscription to directories](#) from the local domain. The local domain has [canceled the sharing](#) of resources with the Peer Platform.
- The local domain has canceled the [subscription to alarms](#) and [subscription to directories](#) from the peer domain. The peer domain has [canceled the sharing](#) of resources with the local domain.

To delete the Peer Platform, do as follows:

- Delete one by one: Click **More** in the **Action** column of the Peer Platform list, and select **Delete Platform**.
- Batch Delete: Select multiple Peer Platforms in the Higher-level Platform list, and click **Delete** at the top of the list.

4. Search Peer Platform

You can search external domains by name, interconnection code, IP address, and organization. If you uncheck **Search All**, the search result will only include all Peer Platforms under the currently selected organization node.

Figure 12-18 Search Criteria or Peer Platform

Platform Name: Platform ID: IP: Organization: ☒ Search All

5. Export Peer Platform

You can export the Peer Platform information to an Excel file.

- Export Selected: Select multiple Peer Platforms in the Peer Platform list, and click **Export** > **Export Selected** at the top of the list to export the selected Peer Platforms.
- Export All: Click **Export** > **Export All** to export all Peer Platforms.

Figure 12-19 Export Peer Platform

☒	Platform
☒	H2
☒	H3

6. Remote Management

Through remote management, you can directly log in to a server in a Peer Platform.



Note!

Before using this function, check that the server in the Peer Platform is a third-party server that supports remote management.

Search resources shared from child or peer domains
Query the shared server
Search device information
Search device status
Restart External Domain
Remote Management
Modify External Domain
Delete External Domain

12.3.3 Lower-level Platform

1. Add Lower-level Platform

1. Go to the **Device Management** > **Platform Cascading** page and select **Lower-level Platform**.

Figure 12-20 Lower-level Platform page

The screenshot shows the 'Lower-level Platform' management interface. At the top, there are search filters for Platform Name, Platform ID, IP, and Organization, along with 'Search All', 'Search', and 'Reset' buttons. Below the filters are action buttons: '+ Add', 'Export', 'Refresh', 'Delete', and 'Search External Domain Resources'. The main area contains a table with columns: Platform Name, Platform ID, IP, Inter-platform Interconnect Protocol, Platform Status, and Operation. One entry is visible with Platform Name 'test', Platform ID '967654', and Status 'Offline'. A link 'Resources shared from others More' is present in the Operation column.

2. Click **Add** to go to the **Add Lower-level Platform** page.
3. Configure the required information for the Lower-level Platform. Different parameter items will be displayed for different parameter values configured. The actual page shall prevail.
4. Click **OK** to save the configuration.
You can also click **Next** to configure the optional information. Then, click **OK** to complete the addition of the Lower-level Platform.
5. After adding the local domain as the Higher-level Platform on the Lower-level Platform, click **Refresh** on the **Lower-level Platform** page. The corresponding Lower-level Platform will be online.

Figure 12-21 Add Lower-level Platform - Required Information

The screenshot shows the 'Add Lower-level Platform' configuration form. It has two tabs: '1 Required Information' (active) and '2 Optional Information (it can be skipped)'. Under the 'Required Information' tab, there are six fields: Platform Name, Platform ID, Platform Type (dropdown), SPN (dropdown), Interconnection ID, Inter-platform Communication (dropdown), Organization (dropdown), and Interconnection User ID. Each field has a 'Please Enter' placeholder. At the bottom, there are 'Confirm' and 'Next' buttons.

Figure 12-22 Add Lower-level Platform - Optional Information

< Back | AddLower-level Platform

1 Required Information 2 Optional information (it can be skipped)

* Platform Level: 3

* Platform Device Type: VM/ISC

* Playback/Download Service Pol... Auto-Adaptation

* Stream Transmission Protocol: Auto-Adaptation

* NAT Config: Without NAT

Remote Address: http://

* Platform Role Priority: 6

* Inter-platform Multicast Policy: not support

* Max. Directly-Connected Strea... 1024

Playback TCP Direction: Platform as Server

* Directory Mode: New GB/T 28181

* Media Service Selection Policy: Auto-Adaptation

☐ LAPI Attribute ☒ Authentication

* User Name:

Domain Name:

* Password:

Confirm Back

Table 12-4 Parameter Descriptions for Adding a Lower-level Platform

Parameter	Description
Platform ID	ID of the Lower-level Platform used in the local domain. The ID must be unique in the local domain.
Platform Name	Name of the Lower-level Platform used in the local domain. Name of the Lower-level Platform used in the local domain.
Platform Type	Default is Lower-level Platform, not allowed edit.
Inter-Platform Communication Protocol	Choose the appropriate protocol according to the network environment. Support GB protocol, private protocol, DB33, DB33 2012
Platform IP	IP address of the Lower-level Platform server. Currently only IPv4 IP addresses are allowed.
Platform SIP Port	Used for signaling interaction with other domains. Make sure the setting is consistent with the SIP port configured on the server in the Lower-level Platform.
SPN	Select the SPN Server to be used to share and push inter-domain resources.
Organization	Lower-level Platform can only be added to the local domain or below an organization of the local domain.
Inter-Domain Domain ID	After you select an inter-domain communication protocol, set an inter-domain domain ID that conforms to the protocol specifications. Note: Make sure the setting is unique and consistent with the corresponding inter-domain interconnection parameters configured for this Lower-level Platform.
Inter-Domain User ID	After you select an inter-domain communication protocol, set an inter-domain user ID that conforms to the protocol specifications. Note: Make sure the setting is unique and consistent with the corresponding inter-domain interconnection parameters configured for this Lower-level Platform.
Platform Level	Level of the Lower-level Platform (low to high is 1-7). See Inter-Domain Communication Protocol Configuration .

Parameter	Description
PlatformRole Priority	Priority level of the Lower-level Platform when using resources in the local domain (low to high is 1 to 63).
Platform Type	Platform type of the Lower-level Platform server. Note: When adding a third-party platform, choose “other”.
Inter-Platform Multicast Policy	Whether inter-domain networking supports multicast. Note: Inter-domain multicast is not available when the inter-domain communication protocol is Sichuan Electrics Power Corporation.
Playback/Download Service Policy	Configure inter-domain playback/download service selection policy. ● Auto-Adaptation: If MS is not available, streams will not pass through MS. If MS is available, streams will pass through MS as the first option. ● Bypass MS: Inter-domain playback/download streams will not pass through MS in the local domain. Note: Whether inter-domain playback streams pass through MS is determined by multiple configurations and whether MS is deployed. See Local Configuration > Video Parameters > Advanced Configuration > Playback Service Selection Policy . The service selection policy for inter-domain download is similar to that for inter-domain playback.
Max. Directly-Connected Stream Count	This parameter limits the maximum number of unicast, direct-connection based live video streams of IPCs in the Lower-level Platform in the local domain. It is effective only when Direct Connection First is enabled on the decoding terminal. That means, when a direct-connection-first enabled decoding terminal in the local domain establishes live video with an encoding terminal in the Lower-level Platform, the system checks whether the Max. Directly-Connected Stream Count is exceeded. If not exceeded, live video streams will be transmitted directly from the encoding terminal to the decoding terminal; otherwise, if MS is deployed in the local domain, live video streams will be forwarded via MS as the first option; if MS is not deployed, live video streams will still be transmitted directly from the encoding terminal to the decoding terminal. Note: The modified Max. Directly-Connected Stream Count takes effect the next time live video is established.
Stream Transmission Protocol	● Auto-Adaptation:Decoding terminals in the local domain can receive UDP or TCP live video streams from the Lower-level Platform. This is determined by the system through auto-negotiation. This is the default setting. ● TCP: The decoding terminal in the local domain receives only TCP live video streams from the Lower-level Platform. Note: This parameter can be set to TCP only when the inter-domain communication protocol is Private or GB.
TCP Type	Currently only GB2014 and GB2016 are available. Note: This parameter is configurable when TCP is chosen as the stream transmission protocol for media streams between GB-connected domains.
TCP Direction	● Lower-level Platform as SERVER: The XP in the local domain initiates TCP connections. ● Lower-level Platform as CLIENT: The external domain initiates TCP connections. Note: This parameter is configurable when TCP is chosen as the stream transmission protocol for media streams between GB-connected domains.
NAT Configuration	● If the Lower-level Platform is behind the NAT and the local domain is in front of the NAT, choose External Domain Behind the NAT. ● If the local domain is behind the NAT and the Lower-level Platform is in front of the NAT, choose External Domain in Front of the NAT.

Parameter	Description
	● If the local domain and the Lower-level Platform are behind separate NATs, choose Device and Local Domain Behind Separate NATs. ● If inter-domain streams do not need to traverse the NAT, choose No NAT. Note: If GAP is configured in the network, choose No NAT.
Directory Mode	Methods of pushing and mounting resources between GB domains. ● New GB: New GB/T 28181 (GB2016 and later). ● Old GB: Old GB/T 28181 (GB2014 and earlier). ● Administrative Area: New GB protocol based on administrative division. ● Parent organization: Both the pushed organizations and cameras carry the sharing ID of the parent organization of the resources, and the parent organization is mounted when you mount the resources. Note: This parameter is configurable only when the inter-domain communication protocol is set to GB.
Remote Address	URL address of the external domain server, used to manage the external domain server remotely.
Media Service Selection Policy	● Auto-Adaptation: (default) Whether live video streams from the Lower-level Platform pass through MS is determined by the system based on the media service selection policy of the encoding device or the external domain and on whether MS is deployed. ● Specified MS: Live video streams of the Lower-level Platform must pass through the specified MS. ● Specified MS group: Live video streams of the Lower-level Platform must pass through an MS in the specified MS group. ● Bypass MS: Live video streams in the Lower-level Platform will not pass through MS. Note: If MS is deployed but has insufficient forwarding capability, then Direct Connection First will be adopted.
Authentication	When Authentication is selected, you need to config Username, Password, Domain Name used for authentication of the Lower-level Platform, and the Username, Password, Domain Name must be the same in both domains. Note: When the inter-domain communication protocol is not DB33, this parameter can be set
Max External Domain Backup Channels	Maximum number of backup channels for the Lower-level Platform. The default value is 0, which means no limit. Note: This parameter is configurable only when the central server has enabled backup channel limit for external domains.
LAPI Attribute	When LAPI Attribute is selected, you can add a Lower-level Platform (such as NVR/AIBOX) via LAPI protocol.
Protocol Type	● HTTP: The camera reports LAPI data. ● WebSocket: The camera reports radar and video data.
LAPI Account/Password	Account/password of the LAPI external domain device.
LAPI External Domain IP/Port Number	The IP/port number of the LAPI external domain device.
MD Address	IP address of the MD server that accesses the LAPI device data. (Required when HTTP is selected.)
Push Mode	Select the image push mode: Image, Local URL, or Cloud Storage URL. (Required when HTTP is selected.)

Parameter	Description
Subscription Type	Select the data type of the LAPI device to be subscribed. (Required when HTTP is selected. The subscription is activated after you configure this parameter. You can view or edit it on the LAPI Device Subscription page.)

2. Edit Lower-level Platform

Click **More** in the **Action** column of the Lower-level Platform list, and select **Edit Platform** to go to the **Edit Lower-level Platform** page. After editing the parameters, click **OK** to save the modification.



Note!

Parameters grayed out on the page, such as platform code, platform type, and inter-platform interconnection protocol, cannot be modified.

Figure 12-23 Edit Lower-level Platform - Required Information

< Back | Modify Lower-level Platform(xjy15)

1 Required Information 2 Optional information (it can be skipped)

* Platform Name:	xjy15	* Platform ID:	xjy15
* Platform Type:	Lower-level Platform	* Inter-platform Communication ...	GB
* SPN:	spnserver	* Interconnection ID:	65010100002000013515
* Interconnection User ID:	65010100002000013515_user		

Figure 12-24 Edit Lower-level Platform - Optional Information

< Back | Modify Lower-level Platform(xjy15)

1 Required Information 2 Optional information (it can be skipped)

* Platform Level:	3	* Platform Role Priority:	6
* Platform Device Type:	VM/ISC	* Inter-platform Multicast Policy:	not support
* Playback/Download Service Pol...	Auto-Adaptation	* Max. Directly-Connected Strea...	1024
* Stream Transmission Protocol:	Auto-Adaptation	Playback TCP Direction:	Platform as Server
* NAT Config:	Without NAT	* Directory Mode:	New GB/T 28181
Remote Address:	http://	* Media Service Selection Policy:	Auto-Adaptation

☐ LAPI Attribute ☒ Authentication

* User Name:		* Password:	
Domain Name:			

3. Delete Lower-level Platform

Before deleting the Lower-level Platform, you need to confirm that:

- The local domain has canceled the [subscription to alarms](#) and [subscription to directories](#) from the child domain. The child domain has [canceled the sharing](#) of resources with the local domain.

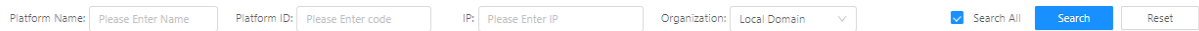
To delete the Peer Platform, do as follows:

- Delete one by one: Click **More** in the **Action** column of the Lower-level Platform list, and select **Delete Platform**.
- Batch Delete: Select multiple Lower-level Platforms in the Lower-level Platform list, and click **Delete** at the top of the list.

4. Search Lower-level Platform

You can search external domains by name, interconnection code, IP address, and organization. If you uncheck **Search All**, the search result will only include all Lower-level Platforms under the currently selected organization node.

Figure 12-25 Search Criteria for Lower-level Platform

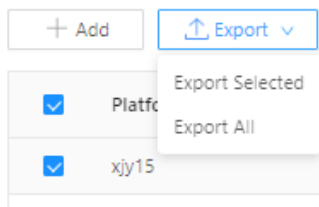
A search form with four input fields: 'Platform Name' (placeholder: Please Enter Name), 'Platform ID' (placeholder: Please Enter code), 'IP' (placeholder: Please Enter IP), and 'Organization' (dropdown menu showing 'Local Domain'). To the right of these fields are three buttons: a checkbox labeled 'Search All' (checked), a blue 'Search' button, and a 'Reset' button.

5. Export Lower-level Platform

You can export the Lower-level Platform information to an Excel file.

- **Export Selected:** Select multiple Lower-level Platforms in the Lower-level Platform list, and click **Export > Export Selected** at the top of the list to export the selected Lower-level Platforms.
- **Export All:** Click **Export > Export All** to export all Lower-level Platforms.

Figure 12-26 Export Lower-level Platform



12.4 Resource Sharing

In a multi-domain network environment, you can share resources in the local domain and its organizations with the parent or peer domain for inter-domain operations. The shareable resources include cameras, alarm sources, checkpoints, organizations, alarm output, etc.

12.4.1 Requirements

Different inter-domain communication protocols have different requirements on the types of shared resources and sharing IDs. In particular, there are strict specifications on sharing IDs for GB-based inter-domain sharing.

Protocol Resource Type	GB Protocol	Private Protocol
Organization	Sharing IDs must be 2/4/6/8/10/20 digits long. For 20-digit sharing IDs, digits 11-13 must be 200, 215, or 216.	Sharing IDs must consist of 1- 32 digits or letters.
Camera	Sharing IDs must be 20 digits long, and digits 11-13 must be 119-129, 131, or 132.	
Alarm Source	Sharing IDs must be 20 digits long, and digits 11-13 must be 134.	
Alarm Output	Not applicable.	

12.4.2 Configure the GB Sharing ID Data Dictionary

When the inter-domain communication protocol is GB, sharing IDs must comply with GB specifications.

Sharing ID is a string of 20 decimal digits, including administrative region code (8 digits), industry code (2 digits), category code (3 digits), network type code (1 digit), and serial number (6 digits). The sharing ID data dictionary is a collection of sharing IDs. You can configure the dictionary in advance so you can use it when adding external domains and shared resources.

Add GB/T 28181 IDs

1. Go to **Device Management > Platform Cascading > Higher-level Platform**.
2. Click **GB/T 28181 Sharing ID Data Dictionary**.
3. Choose the administrative region, industry code, category code, network type, click **Add**, enter the name and code.



NOTE!

The administrative region is divided into four levels: province/city/county/district/basic (2 digits each level), industry code (2-digit), category code (3-digit), and network type (1-digit).

12.4.3 Query SPN

A Share Process Node (SPN) is used to push shared resources between domains. Before you start to share resources, check that the SPN bound to the target external domain is online.

1. Go to **Device Management > Platform Cascading > Higher-level Platform, Peer Platform, Lower-level Platform**.
2. Click **More** in the **Operation** column in the external domain list, choose **Query the shared server**.

Details✕



Query the shared server

Device Name: spnsrver

Device IP: 192.168.1.32

Device ID: spnsrver

Device Model: SPN9500

Device Status: on line

12.4.4 Share Resources(for one platform)

Share resources (such as cameras, alarm sources, checkpoints) of the local domain and organizations in it with its parent or peer domain.

Go to **Device Management > Platform Cascading > Higher-level Platform, Peer Platform**,. Choose the target parent/peer domain, click **More** in the Operation column, choose **Shared resource**. The **Shared Resource** page appears.

☐ 229 229 Parent ... 192.169... 5061 not sup... Bypass MS

Share Resource

☐ gbup_32 gbup_32 Parent ... 192.169... 5061 not sup... Bypass MS

Search shared resources
 Query the shared server

Inter-domain Management > External Domain Management > Shared Resource

Please first share the organization and all its parent organizations and then share its resources such as cameras in it.

Enter the resource name

Local Domain

- 12333
- 124
- 125
- 126
- 127
- 128
- 129
- 130
- 145
- JayChou
- godfather
- joker zhoutao
- 172
- 192.168.1.33
- 192.168.1.75

Sharing ID: 14785296

Include Sub-resource: ☐ yes ☒ no

Automatic Sharing: ☐

Share Organization

Stop Sharing

Camera
Alarm Source
Checkpoint

CameraName:

Sharing Status:

With or Without Latitude and Longitude:

One-click sharing: ☐

☐	Camera Na	Camera ID	Device Sta	Sharing St	Latitude ar	Sharing ID	Permissions
☐	12345...	12345...	off li...	Not S...	Witho...	123456789011445i	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Cont
☐	12345...	12345...	off li...	Not S...	Witho...	123456789011445i	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Cont
☐	12345...	12345...	off li...	Not S...	Witho...	123456789011445i	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Cont
☐	12345...	12345...	off li...	Not S...	Witho...	123456789011445i	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Cont
☐	192.16...	43810...	on li...	Not S...	Witho...	438107160413299'	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Cont
☐	192.16...	59717...	on li...	Not S...	Witho...	597172418713283!	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Cont

total 17



NOTE!

You need to share an organization and all its parent organizations before you can share resources (such as cameras) in it.

1. Share Organization

- On the **Shared Resource** page, select the organization you want to share on the left-side resource tree.



NOTE!

- Before you can share an organization, you must share its parent organization first.
- A shared organization is displayed as . An organization not being shared is displayed as .

2. Set sharing IDs.

- The sharing ID of an organization must conform to requirements of the inter-domain communication protocol and must be unique among all the shared resources (such as camera).
- If the inter-domain communication protocol is the Private protocol, the sharing ID only needs to be a string of 1-32 digits or letters; there are no other requirements.
- If the inter-domain communication protocol is GB, **the sharing ID must consist of 2/4/6/8/10/20 digits. For a 20-digit ID, digits 11-13 must be 200, 215, or 216.**

If you have configured the sharing ID data dictionary (see Configure the GB Sharing ID Data Dictionary), click , choose the names you have configured in the data dictionary, and then click **Confirm**. The system will generate a sharing ID automatically.

3. Set whether to share its sub organizations, including their resources, when sharing the current organization.
4. Click **Share Organization**.
5. (Optional) Enable **Automatic Sharing**, so new cameras and organizations added to the organization in the future and cameras allocated to the organization in the future will be automatically shared with the parent or peer domain. The icon is displayed as when **Automatic Sharing** is enabled.

2. Share Resource

If an organization is shared, resources under the organization can also be shared, such as cameras, alarm sources, checkpoints, and alarm inputs (only when the inter-domain communication protocol is Private).

(1) Share Camera



NOTE!

For GB-connected domains, before you can share a camera, you must perform directory subscription to the local domain in the parent domain (see [Subscribe to Directories](#)). Only shared cameras are displayed in the parent domain.

On the **Shared Resource** page, select a shared organization, click the **Camera** tab. Cameras in the organization are displayed.

Camera Alarm Source Checkpoint

CameraName: Sharing Status: With or Without Latitude and Longitude:

One-click sharing: ☐

☐	Camera Na	Camera ID	Device Sta	Sharing St	Latitude ar	Sharing ID	Permissions
☐	192.16...	43810...	on li...	Not S...	Witho...	438107160413299	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Cont
☐	192.16...	59717...	on li...	Not S...	Witho...	597172418713283	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Cont
☐	192.16...	05828...	on li...	Shared	Witho...	058282492313217	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Cont
☐	192.16...	63492...	off li...	Not S...	With L...	634926993913262	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Cont
☐	192.16...	85253...	off li...	Not S...	Witho...	852537495813289	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Cont

total 5 < 1 > 20 / page

Follow the steps to share cameras:

1. Configure camera sharing IDs.

- (1) Select the cameras you want to share.
- (2) Set sharing IDs for the cameras. The IDs must conform to requirements of the inter-domain communication protocol and must be unique among all the shared resources.



Note!

For the GB protocol: Camera sharing IDs must consist of 20 digits, and digits 11-13 are 119-129, 131, or 132.

- Batch config: Click , and configure ID rules for cameras. You can configure based on the GB rules (firstly [Configure the GB Sharing ID Data Dictionary](#)) or define the rules. After confirmation, the system will automatically generate the GB sharing ID based on the configured rules.

Batch Set Codes

Config Mode: Configure by GB Rules Custom Configuration

* Area Located: (110101)

* Industry Code: ,00

* Category Code: (111)

* Network Flag:

Device/User ID: 00000

code:11010100001110000000

Confirm Cancel

Batch Set Codes

Config Mode: Configure by GB Rules Custom Configuration

Code Length: 20

☐ Fixed Part Custom Serial Number ☐ Fixed Part

Please Enter Please Enter Please Enter

code:

Confirm Cancel

- **Config one by one(only for GB camera):** If you have configured the sharing ID data dictionary (see [Configure the GB Sharing ID Data Dictionary](#)), click the corresponding  for the camera. On the **Set GB/T 28181 Sharing ID** page, select the names that you have configured in the data dictionary, and then click **Confirm**. The system will generate a sharing ID automatically.

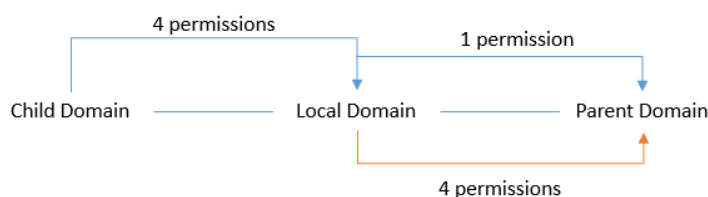
2. Set camera operation permissions for the external domain

☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Cont



NOTE!

- If the shared cameras belong to the local domain, 4 permissions are allowed.
- If the shared cameras belong to the local domain's child domain, only one permission is allowed: PTZ Control.



3. Share cameras with existing sharing IDs.

Select cameras, click **Share** to share the camera.



NOTE!

Sharing will fail if the sharing ID is invalid.

(2) Share Alarm Source

On the **Shared Resource** page, select a shared organization, click the **Alarm Source** tab. Alarm sources in the organization are displayed.

Camera
Alarm Source
Checkpoint

Alarm SourceName:
Sharing Status:

One-click sharing: ☐

☐	Alarm Source Name	Alarm Source ID	Sharing Status	Sharing ID
☐	4564	12345679801191234567&thir	Not Shared	12345679801191234567&thir

total 1
20 / page

Follow the steps to share alarm sources:

- Configure sharing IDs for alarm sources.
 - Sharing IDs must comply with the inter-domain communication protocol and must be unique among all the shared resources (including other resource types such as camera).
 - For GB: **Sharing IDs consist of 20 digits, and digits 11-13 are 134.**
 If you have configured the sharing ID data dictionary (see Configure the GB Sharing ID Data Dictionary), click for the alarm source. On the **Set GB/T 28181 Sharing ID** page, select the names that you have configured in the data dictionary, and then click **Confirm**. The system will generate a sharing ID automatically.

- Share alarm sources with existing sharing IDs.

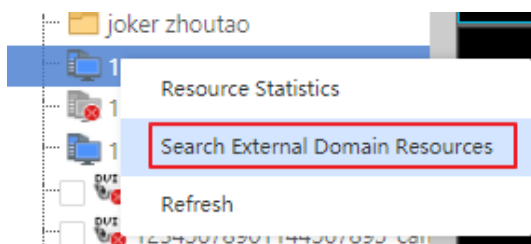
Share one by one: Select an alarm source, click **Share** to share the alarm source.



NOTE!

Sharing will fail if the sharing ID is invalid.

- If the inter-domain communication protocol is GB, do the following on the **Live View** page in the parent domain to view alarm sources shared from the child domain: right-click the child domain in the resource tree, click **Search External Resources**.



(3) Share Alarm Output



NOTE!

Alarm outputs can be shared only when the inter-domain communication protocol is **Private**.

On the **Shared Resource** page, select a shared organization, and then click the **Alarm Output** tab. Alarm outputs in the organization are displayed.

Camera Alarm Source Checkpoint **Alarm Output**

Alarm Output Name: Sharing Status: Search Reset

One-click sharing: ☐

☐	Alarm Output Name	Alarm Output ID	Sharing Status	Sharing ID
☐	4564	12345679801191234567&third	Not Shared	12345679801191234567&thir

total 1 < 1 > 20 / page ▼

Shared Stop Sharing Back

Follow the steps to share alarm outputs:

1. Configure sharing IDs for alarm outputs.
Sharing IDs must comply with the inter-domain communication protocol and must be unique among all the shared resources (including other resource types such as camera).
2. Share alarm outputs with existing sharing IDs.
 - Share one by one: Select alarm output and then click **Share** to share the alarm output.
 - Share in batches: Enable **One-click sharing** and then click **One-click sharing** to share all the alarm inputs that are not shared.

12.4.5 Platform Sharing (to Multiple Platforms)

On the **Platform Sharing** page, you can share resources of the local domain to multiple Higher-level Platforms or Peer Platforms at the same time. The requirements for sharing various types of resources on this page are the same as those described on the individual platform page.

Entry:

Go to **Device Management** > **Platform Cascading**. The resource tree on the left side shows the organizations of the local domain and the child domain. The list in the middle shows the organizations, cameras, alarm sources, checkpoints, and alarm outputs under the selected organization. On the right side, all parent domains and peer domains that you want to share are listed.

Figure 12-27 Platform Sharing Page



Note!

- This page only supports sharing. It does not support canceling sharing or showing the sharing status of each resource. You need to check the sharing relationship on the [corresponding platform](#) page.
- Please share the organization and all its parent organizations, and then share the resources in the organization such as cameras.

1. Share Organization

1. Go to **Device Management** > **Platform Cascading**, and select the **Platform Sharing** tab to go to the **Platform Sharing** page.
2. Select the local domain in the resource tree on the left, and select the **Organization** tab on the right.
3. Select the organization to be shared in the organization list, and fill in the [sharing ID](#).
4. Select multiple external domains to be shared on the right side and click **Share**.

Figure 12-28 Share Organization to Multiple External Domains

2. Share Resource

For an organization that has been shared, you can share cameras, alarm sources, checkpoint resources, and alarm outputs (only between private protocol domains) under the organization.

(1) Share Camera



Note!

For GB inter-domain scenarios, before sharing a camera, [subscribe to directories](#) of the local domain in the parent domain. After sharing the camera, you can view the camera in the parent domain.

1. Go to **Device Management** > **Platform Cascading**, and select the **Platform Sharing** tab to go to the **Platform Sharing** page.
2. Select the shared organization in the resource tree on the left, and select the **Camera** tab on the right.
3. Select the camera to be shared in the camera list, and fill in the [sharing ID](#).
4. Select multiple external domains to be shared on the right side and click **Share**.

Figure 12-29 Share Cameras to Multiple External Domains

Organization: Video Camera Alarm Source Checkpoint Alarm Output

Camera name: Camera ID: Latitude and Longitude: All

Camera Status: All Search Reset

☐ Search All Sub-organizations Batch Configure Permissions Batch Configure Sharing IDs

☐	Camera name	Camera ID	Device Status	Latitude and Longitude	Organization
☐	12	34020000001320000001	Offline	Without Latitude and Longi...	
☒	46	77788877701321300002	Online	Without Latitude and Longi...	
☐	lapi1	lapi1	Offline	Without Latitude and Longi...	
☐	onvif64z	onvif64	Online	Without Latitude and Longi...	

total 4 < 1 > 20 / page

Please select the external

Please enter the extern...

☐ Select All

☒ H1 (GB)

☐ H2 (GB)

☐ H3 (GB)

total 3

Shared

(2) Share Alarm Source

1. Go to **Device Management** > **Platform Cascading**, and select the **Platform Sharing** tab to go to the **Platform Sharing** page.
2. Select the shared organization in the resource tree on the left, and select the **Alarm Source** tab on the right.
3. Select the alarm source to be shared in the alarm source list, and fill in the [sharing ID](#).
4. Select multiple external domains to be shared on the right side and click **Share**.

Figure 12-30 Share Alarm Source to Multiple External Domains

(3) Share Alarm Output



Note!

You can share alarm outputs **only between private protocol domains**.

1. Go to **Device Management > Platform Cascading**, and select the **Platform Sharing** tab to go to the **Platform Sharing** page.
2. Select the shared organization in the resource tree on the left, and select **Alarm Output** tab on the right.
3. Select the alarm output to be shared in the alarm output list, and fill in the [sharing ID](#).
4. Select multiple external domains to be shared on the right side and click **Share**.

Figure 12-31 Share Alarm Output to Multiple External Domains

3. One-click Sharing

You can share a large number of resources to the Higher-level Platform or Peer Platform through an Excel file in batches.

1. Go to **Device Management > Platform Cascade > Platform Sharing**.
2. Click **One-click Sharing** in the upper right corner.

Figure 12-32 One-click Sharing Page

One-click sharing
✕

1. Please prepare the data to import according to the template format.

📄 [Download the template, modify the sharing IDs, and then import the file.](#)

2. Please select the file to import.

📁 Upload File

Must be .xls or .xlsx file, and the maximum file size is 10MB.

3. Please select the external domain to share.

Please select the external domain to share.

One-click sharing

Cancel

- Click **Download the template, modify the sharing IDs, and then import the file.**, and export an Excel file. The sharing ID will be automatically generated in the Excel file. You can filter the resources to be shared.

Figure 12-33 Batch Sharing ID Import Data

No.	Sharing ID	Resource ID	Resource Name	Parent Organization ID	Parent Organization Name	Resource Type	Resource Status
0		77788877701321300002	46	iccsid			1001 Online
1		onvif64	onvif64z	iccsid			1001 Offline
2		34020000001320000001	12	iccsid			1001 Online
3		lap11	lap11	iccsid			1001 Offline
4		test11	test11	org@71952#20250910162151	xx11		1001 Offline
5		test12	test12	org@41786#20250910162138	xx12		1001 Offline
6		77788877701321300002	46	org@29731#20250910162121	xx1		1001 Online
7		77788877701321300002	46	org@79163#20250910162127	xx2		1001 Online

- Click **Upload File** to upload the Excel file.
- Select the external domains to be shared and click **One-click Sharing** to complete batch sharing.

12.4.6 Manage Shared Resources

Search resources shared by the local domain with a parent or peer domain, stop sharing, or modify sharing permissions.

Go to **Device Management > Platform Cascading > Higher-level Platform, Peer Platform**. Choose the parent/peer domain on the external domain list, click **Search shared resources**. The **Shared Resource** page appears, showing shared resources such as cameras, alarm sources, checkpoints, and organizations.

Inter-domain Management > External Domain Management > Search shared resources
🔍 Please enter the name

Camera

Alarm Source

Checkpoint

Organization

CameraName:

Cameracode:

Search

Reset

📄 Import Sharing ID

📄 Export

🔄 Refresh

Batch Configure Permissions

🛑 Stop Sharing

☐	Camera Name	Camera ID	Device Status	Sharing ID	Permissions	Operation
☐	192.168.1.112	05828249231321733518	on line	05828249231321733518	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Co	⚙️ 🗑️ ***
☐	192.168.1.122	48715686411324372312	off line	48715686411324372312	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Co	⚙️ 🗑️ ***

total 2 < 1 > 20 / page

1. View Sharing Relationship

Click  in the **Operation** column to view the external domains with which a resource is being shared.

Sharing Relationship ✕

Number of Shared External Domains: 1 Stop Sharing

☐	External Dom	External Dom	External Dom	Inter-domain	external dom	Operation
☐	229	Parent D...	VM/ISC	GB	Online	

2. Edit Sharing Permissions

Select multiple resources, click **Batch Configure Permissions** on the top to edit the external domain's permission to operate the resource.



NOTE!

- If the shared cameras belong to the local domain, then 4 operation permissions are allowed.
- If the shared cameras belong to the local domain's child domain, then only one operation permission is allowed: PTZ Control

Batch Configure Permissions ✕

Batch Configuration

☒ All

☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Control ☒ Two-way Audio & Broadcast

Camera Name	Camera ID	Permissions
192.168.1.112	05828249231321...	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Control
192.168.1.122	48715686411324...	☒ PTZ Control ☒ Real-time Monitoring ☒ Playback Control

< 1 >

Confirm Cancel

3. Export Shared Resources

Export the selected or all resources.

Import Sharing ID Export ▼

☐ Camera Name

☒ 192.168.1.112

☐ 192.168.1.122

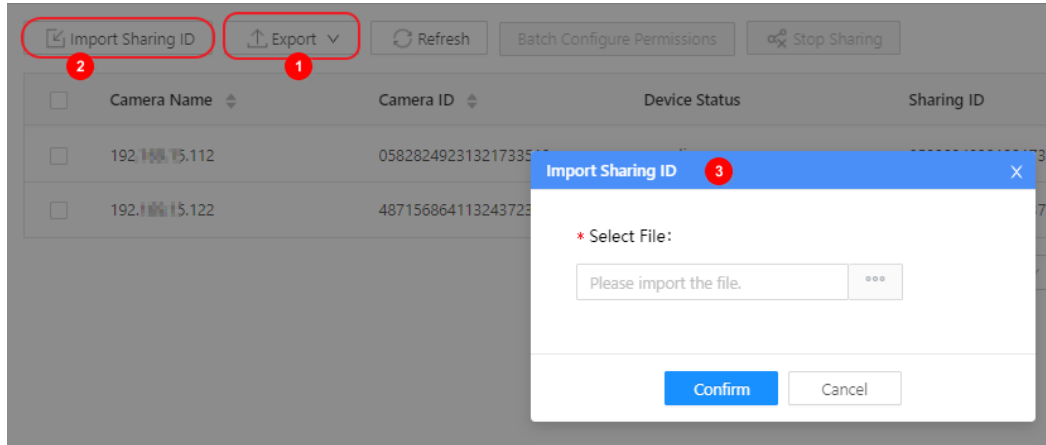
Export Selected

Export All

4. Batch Edit Sharing IDs

Edit sharing IDs of cameras shared from the local domain with the parent domain. (Perform the batch editing operation if you want to number camera sharing IDs in sequence).

1. Click **Export** to export information about the shared cameras to a .xlsx file, and then edit the sharing IDs in the file.
2. Click **Import Sharing ID**, selected the .xlsx file.



NOTE!

The sharing IDs of cameras can be changed in the child domain. Camera names can only be changed in the parent domain. See Batch Edit Sharing IDs.

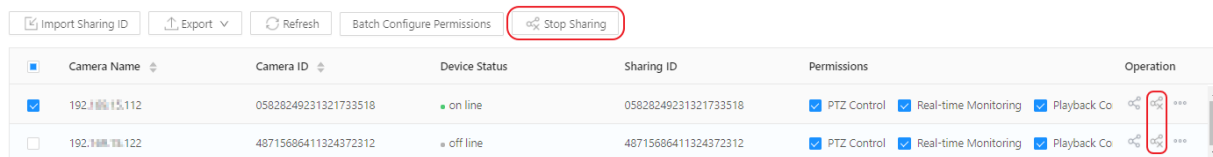
5. Stop Sharing

- Stop sharing one by one: Click  in the **Operation** column to stop sharing the resource with all the external domains.
- Stop sharing in batches: Select multiple resources, click **Stop Sharing** on the top.



NOTE!

Before you can stop sharing an organization, make sure you have stopped sharing all resources in the organization; otherwise, sharing cannot be stopped.

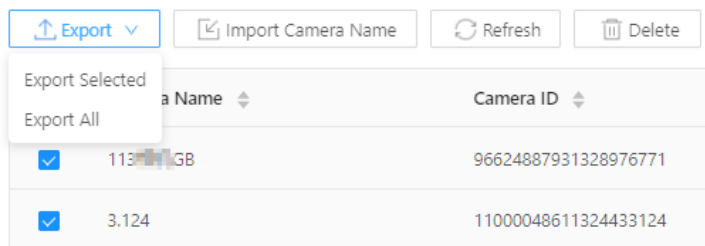


To view resources such as cameras, checkpoints, and organizations that failed to stop sharing:

Go to **System Management > Platform Cascading > Higher-level Platform, Peer Platform..** On the external domain list, choose a parent/peer domain, click **More** in the **Operation** column, choose **Search resources that failed to stop sharing**.

IP	Port	Parent Do...	IP	Port	not support	Bypass MS	spnserv...	...
☐	229	229	Parent Do...	192.169.12....	5061	not support	Bypass MS	spnserv...
☐	gbup_32	gbup_32	Parent Do...	192.169.15....	5061	not support	Bypass MS	spnserv...

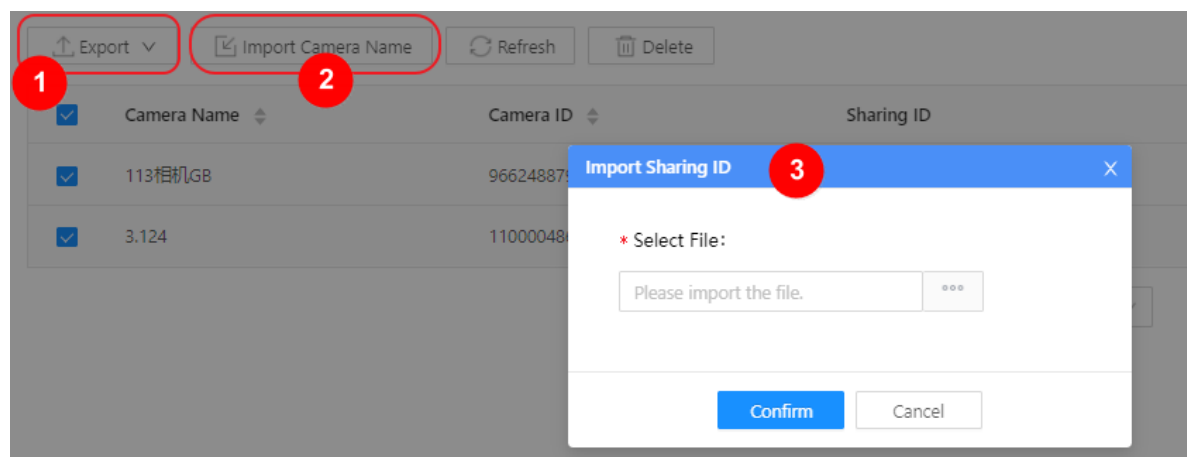
- Shared Resource
- Search shared resources
- Query the shared server
- Search resources that failed to be shared
- Search resources that failed to stop sharing
- Modify External Domain
- Delete External Domain



2. Rename Cameras in Batches Shared from Child/Peer Domains

Rename cameras shared from the child domain in batches in the local domain.

1. Click **Export** to export information of the shared cameras to a .csv file. Change the camera names in the file and then save.
2. Click **Import Shared Cameras Name**, select the modified .csv file and import.



NOTE!

Camera names can be changed in the parent domain. Sharing IDs can only be changed in the child domain. See Batch Edit Sharing IDs.

3. Delete Resource Shared from External Domain

Delete resource shared with the local domain from an external domain.



NOTE!

If storage or backup resource has been configured for a camera shared from an external domain, you must delete the configured storage resource or backup resource before you can delete the camera.

Select the resource in the resource list, click **Delete**, and then confirm to delete it from the local domain.

12.5 Resource Subscription

After a child or peer domain shares resources with the local domain, the local domain can subscribe to alarms, directories, and locations of GB mobile devices from the shared resources and manage information about the shared resources.

12.5.1 Alarm Subscription

Subscribe to alarms from shared resources to view and acknowledge alarms from these resources.



NOTE!

In order for the parent domain to receive alarms from the shared resources:

1. In the child domain, go to **Device Management > Service Configuration > Alarm Service > Alarm Subscription** to configure alarm subscription.
2. In the parent domain, go to **Device Management > Platform Cascading > Subscription Management > Alarm Subscription**, subscribe to alarms from resources shared from the external domain.

Subscribe to alarms from resources shared from external domain

1. Go to **Device Management > Platform Cascading > Subscription Management > Alarm Subscription**.

Resource Name	Resource Type	Subscription Type	Operation
---------------	---------------	-------------------	-----------

2. Click **Add**. A page as shown below appears.

Please select an organization or resource before selecting an alert subscription type

* Please select organization:

Enter the resource name

- 128
- 129
- 130
- 145
- JayChou
- godfather
- joker zhoutao
- 172
- 192.168.15.33
- 192.168.15.75
- 3.124

* Subscribed Alarm Types:

Please enter the subscribed alarm types.

- All Alarms
 - Telephone Alarm
 - Device Alarm
 - SMS Alarm
 - GPS Alarm
 - Video Alarm
 - Device Fault Alarm
 - Other

Confirm Cancel

3. First select organizations or resources from the external domain, and then select alarm types.
4. Click **Confirm**.

Cancel Alarm Subscription

Cancel alarm subscriptions one by one or in batches:

Resource Name	Resource Type	Subscription Type	Operation
192.168.15.75	Organization	All Alarms	Cancel the subscription

12.5.2 Subscribe to Directories

Subscribe to directories from a GB-connected external domain to keep resource status and names synced between the parent and child domains.



NOTE!

Directory subscription is applicable only when **the external domain is a physical domain** (that actually exists). You cannot subscribe directories from an external organization.

Subscription

1. Go to **Device Management > Platform Cascading > Subscription Management > Directory Subscription**.

2. Click **Add**. A page as shown below appears.

3. Select an online GB-connected external domain, click **Confirm**.

Cancel Subscription

Cancel subscriptions one by one or in batches:

12.5.3 Subscribe to Mobile Device Locations

Subscribe to locations of GB mobile devices, so the GB mobile devices will report locations to VM periodically. The locations will be pushed by VM to the map server and displayed on maps.

Subscription

1. Go to **Device Management > Platform Cascading > Subscription Management > Alarm Subscription > Subscribe to Mobile Device Location**.

Resource Name	Resource Type	Reporting period	Operation
46	Video Camera	5	

2. Subscribe one by one or in batches.

- **Single subscription**

- (1) Click **Add**. A page as shown below appears.

* Please select organization:

- 3.124
- 192.168.15.110
- 192.168.15.111
- 192.168.15.112
- 192.168.15.114
- 192.168.15.118
- 192.168.15.122
- 192.168.15.123

Reporting cycle: 5 Second

Confirm Cancel

- (2) Select a GB mobile device in the local domain or in an GB-connected external domain, or select a GB-connected external domain to select all the GB mobile devices in it.



NOTE!

- When you subscribe from an external domain, first go to the external domain and subscribe to mobile devices in it, and then go to the parent domain and subscribe to the external domain or specified mobile devices in the external domain.
- You can only subscribe from an external domain when it is online.

- (3) Set the report period. The value range is [1-3600] (unit: second).

- (4) Click **OK**.

- **Subscribe in batches**

- (1) Click **Batch Export**. All the GB devices in the local domain, all the GB-connected external domains and all the devices in the GB-connected external domains are exported.
- (2) Delete the non-GB mobile devices and then save the file as a CSV file.
- (3) Click **Batch Subscribe**, select the CSV file you just saved and import.

Batch Subscribe

✕

* Select File:

Please import the file.

...

Confirm

Cancel

Cancel Subscription

Cancel subscriptions one by one or in batches:

+ Add
Batch Export
Batch Subscribe
Cancel the subscription

	Resource Name	Resource Type	Reporting cycle	Operation
☒	172	Organization	5	
☒	192.168.1.110	Camera	5	

13 LAPI Management

13.1 LAPI Device Subscription

13.1.1 Add LAPI Device

LAPI devices refer to cameras that access video image data via the LAPI protocol. (LAPI is set as the Communication Type for the Intelligent Server in the camera).

1. Go to **Device Management > Device Configuration > Frontend Device**.
2. Click **Add**, a page as shown below appears.

< Back | Add Frontend Device

1 Required Information
2 Optional information (it can be skipped)

Basic Info

Device Name: Please Enter
Device ID: Please Enter

Organization: Local Domain

Tag Info

Tag: ☒ Video Device

Video Device

Protocol type: GB/T 28181 Protocol
Camera Channel Type: ☒ Single-Chann... ☐ Multi-channel ...

Camera Type: Fixed Camera
Camera subtype: LAPI Camera

Camera GB Code: 20240131001310000001
Camera Capability: normal

code rate(Kbps): 2048
User Name: Please enter the user name.

Password: Please enter the password.
Max IPC Streams: 4

Stream Transmission Prot...: TCP
TCP Type: GB2016

TCP Direction: IPC as Client
Playback/Download Servi...: Auto-Adaptation

Support Direct Storage: no
Authentication: ☒ yes ☐ no

Image asset information

IP Address: Please enter the IP address.
Port: 80

User Name: Please enter the user name.
Password: Please enter the password.

Transfer Protocol: HTTP
MD地址:

Confirm Next

3. Configure LAPI camera parameters.

- For camera subtype, choose **LAPI Camera**.
- Image asset information is required.
- For descriptions of other parameters, see the [LAPI Device](#).

13.1.2 Subscribe from LAPI Device

Subscribe to alarms, structured data from LAPI cameras.

Go to **Device Management > LAPI Management > LAPI Device Subscription** to subscribe to data or cancel subscriptions.

Platform as Client
Platform as Server

Device Name: Please Enter
Device ID: Please Enter
Device IP: Please Enter

Subscription Stat...: all
Subscription Type: all

Search Reset

Cancel the subscription
Batch Subscribe
Refresh

☐	Device Name	Device ID	IP Address	Device Status	Subscription Status	Organization	Subscription Type	Device Type	Operation
☐	test1	777	172.20.81.219	Offline	not subscribed	Local Domain		IPC	Subscription
☐	test	999	172.20.81.210	Offline	not subscribed	ykj		IPC	Subscription

- As a client platform: Data is reported via HTTP protocol and supports subscribing to various data from LAPI devices.
- As a server platform: Data is reported via WebSocket protocol and only supports subscribing to vehicle traffic data from LeiShi devices.

1. Subscription

1. Click **Subscribe**. A page as shown below appears.
2. Configure the parameters by referring to the table below. Click **Confirm** to save the settings.

220

Subscription
✕

* IP Address:

* Port Number...:

* Subscription ...:

* Subscription Type:

☐ Select All

☐ Cross Line Detect...

☐ Intrusion Detecti...

☐ Enter Area

☐ Leave Area

☐ Loitering Detecti...

☐ Object Removed

☐ Object Left Behin...

☐ Quick Moving Al...

☐ Fire Alarm

☐ Smoke and Fire ...

☐ No Helmet Alarm

☐ No Chef Hat Alar...

☐ Calling Alarm

☐ Smoking Alarm

☐ Face Recognition...

☐ No Work Clothes...

☐ No Mask

☐ Abnormal Tempe...

☐ High-rise Litterin...

☐ Fall Detection Al...

☐ Climbing Detecti...

☐ Absence Detecti...

☐ Sleep on Duty D...

☐ Fight Detection ...

☐ ...

* Push Mode:

Confirm
Cancel

Parameter	Description
IP Address	IP address used to receive data. Set it to the IP of the MD server.
Port Number	To subscribe to people counting data, fill in 55013. To subscribe to structured data, alarm images, fill in 55010.
Subscription Cycle	Data subscription interval. Input an integer within 30-3600.
Subscription Type	Type of data to subscribe to. Currently three types are supported: Structured Data, Alarm Image Data, People Counting Statistics.
Push Type	Image push options: Image, local URL, cloud storage URL.

2. Cancel Subscription



CAUTION!

Cancelling subscription will affect the existing services.

1. Select the devices you want to unsubscribe from, click **Cancel Subscription**.
2. Confirm to cancel the subscription.

14 Advanced Settings

14.1 Central Server Configuration

The central server refers to the video management server in the local domain on which the VM software has been installed.

14.1.1 Server Settings

1. Configure Stream Format

Configure stream formats, that is, configure stream transport protocols supported by the monitoring system for different application scenarios.



NOTE!

Only the super administrator can configure stream format.

1. Go to **Device Management > Advanced Settings > Center Configuration > Server Settings**.

2. Choose the stream format supported by the system.

Table 14-1 Stream Format Reference

Parameter	Description
UDP+TS	This is the default setting, which means media streams are encapsulated into TS streams and carried by UDP. Note: In a multi-domain networking environment, the inter-domain communication protocol for this stream format is the Private protocol, and the platform can connect IPC/encoder/decoder via the Private protocol, connect IPCs via ONVIF, and connect the child domain via the Private protocol. In a GB-connected two-level domain networking environment where IPCs are connected via the Private protocol and the central server in the child domain has enabled UDP+TS, if the parent domain requests live video streams from an IPC in the child domain, the live video streams must be processed through the MS in the child domain. If the decoding terminal is configured with TCP and the encoding terminal is configured with UDP, then the stream format can only be UDP+TS (currently MS does not support RTP-to-TCP conversion).
RTP/RTCP+TS	Means TS streams transported by RTP, and RTCP-based keepalive is required.
RTP+PS	Means PS streams transported by RTP. Caution: In a multi-domain networking environment, the corresponding inter-domain communication protocol for this stream format is GB, and the platform can connect IPC/encoder/decoder via GB, connect IPCs via ONVIF, connect the child domain via the GB and Private protocols.

3. Click **OK**.

2. Max. Directly-Connected Stream Count

Max. Directly-Connected Stream Count is effective when Direct Connection First is enabled on the decoding terminal.

- For local-domain cameras, live video streams are not forwarded via MS unless the following conditions are met in the local domain: 1. Direct connections has exceeded the maximum number. 2. MS is deployed. 3. Encoders or IPCs allow forwarding via MS.
- For external-domain cameras, if the maximum number of direct connections is not reached in the local domain or the child/peer domain, live video streams will be transmitted directly; otherwise, live video streams will be forwarded via MS (if deployed in the local domain).



NOTE!

Only the super administrator can configure Max. Directly-Connected Stream Count.

1. Go to **Device Management > Advanced Settings > Center Configuration > Server Settings**.

The screenshot shows the 'Server Settings' page in a web interface. On the left, there is a 'Quick Nav' sidebar with options like Basic Configuration, Device Configuration, Platform Cascading, Service Configuration, LAPI Management, Advanced Settings, Center Configuration, Transcoding Rules, Trunk Management, and Dual Bus. The 'Center Configuration' section is expanded, showing 'Server Settings'. The 'Server Settings' page has a list of configuration items on the left: Cloud Recording Retrieval Configuration, PTZ Release Configuration, Preemption Policy Configuration, Asset Record Policy, Camera Main/Sub Stream Policy, Password Rules for Standard-Protocol IPC, User login mode, LAPI subscription type predefined, Operation log language configuration, and OSD Configuration. The main area shows the 'Server Settings' configuration. The 'Stream Format' is set to 'UDP+TS'. The 'Max. Directly-Connected Stream Count' is set to '2'. The 'Local Domain Live Video Stream Policy' is set to 'Main Stream Priority'. The 'Stream Policy for Multicast Address' is set to 'Main Stream'. The 'Stream Policy for Multicast Address' is set to 'Close'. The 'Adaptive Stream Type According to' is set to '0'. A 'Confirm' button is at the bottom.

2. Set **Max Directly-Connected Stream Count**.
3. Click **OK**.

3. Local Domain Live Video Stream Policy



NOTE!

Only the super administrator can configure **Max. Directly-Connected Stream Count**.

1. Go to **Device Management > Advanced Settings > Center Configuration > Server Settings**.

The screenshot shows the 'Server Settings' page in a web interface. On the left, there is a 'Quick Nav' sidebar with options like Basic Configuration, Device Configuration, Platform Cascading, Service Configuration, LAPI Management, Advanced Settings, Center Configuration, Transcoding Rules, Trunk Management, and Dual Bus. The 'Center Configuration' section is expanded, showing 'Server Settings'. The 'Server Settings' page has a list of configuration items on the left: Cloud Recording Retrieval Configuration, PTZ Release Configuration, Preemption Policy Configuration, Asset Record Policy, Camera Main/Sub Stream Policy, Password Rules for Standard-Protocol IPC, User login mode, LAPI subscription type predefined, Operation log language configuration, and OSD Configuration. The main area shows the 'Server Settings' configuration. The 'Stream Format' is set to 'UDP+TS'. The 'Max. Directly-Connected Stream Count' is set to '2'. The 'Local Domain Live Video Stream Policy' is set to 'Main Stream Priority'. The 'Stream Policy for Multicast Address' is set to 'Main Stream'. The 'Stream Policy for Multicast Address' is set to 'Close'. The 'Adaptive Stream Type According to' is set to '0'. A 'Confirm' button is at the bottom.

2. Choose local domain live video stream policy (sub stream priority or main stream priority).

3. Click **OK**.

14.1.2 Operation log language configuration

Select the language in which to save the operation logs.

Operation log language configuration

Language Selection: ^

Chinese

English

Spanish

Confirm

14.1.3 OSD Configuration

When enabled, the user's name will be superimposed on the PTZ live view when the user operates the PTZ camera.

OSD Configuration

Whether to turn on username OSD ?

☒ Normally open ☐ Normally Closed

14.2 Transcoding Rule

After configuring the transcoding rule, you can convert the output streams of cameras, NVRs and other devices to a certain stream type (such as TS stream and GB stream), and then transmit the streams to panes, monitors or parent domains via a transmission protocol (such as UDP, RTP and TCP).

Before configuring the transcoding rules, [add a transcoding server](#) on the **Server Devices** page.

14.2.1 Add Transcoding Rule

1. Go to **Advanced Settings > Center Configuration > Transcoding Rules**
2. Click **Add** to go to the **Add TS Transcoding Rule** page.

Figure 14-1 Transcoding Rule

Quick Nav

Basic Configuration

Device Configuration

Platform Cascading

Service Configuration

LAPI Management

Advanced Settings

Center Configuration

Transcoding Rules

Trunk Management

Dual Bus

+ Add

🗑 Delete

🔄 Refresh

☐	Name	Stream Policy	Enabled	Operation
☐	e1	UDP + TS	yes	✎ 🗑

3. Fill in the rule name and select the stream policy. After selecting the devices in the **Source** area, click  to add the devices to the listed of selected sources.

Figure 14-2 Add Transcoding Rule - Select Source

Add Transcoding Rules

* Rule Name:

* Stream Policy:

UDP + TS

Enable Rules: ☒ Enable Rules

Unselected Sources:

Video Camera

☒

Device Name

Device Type

☒

126

Video Camera

☒

LAPI

Video Camera

☒

xgh

Video Camera

→

☐

Device Name

Device Type

Operation

☐

126

Video Camera

🗑

☐

LAPI

Video Camera

🗑

☐

xgh

Video Camera

🗑

< 1 > 10 / page

Cancel

Next

4. Click **Next**. After selecting the devices in the **Destination** area, click  to add the devices to the listed of selected destinations.

Figure 14-3 Add Transcoding Rule - Select Destination

Add Transcoding Rules

Unselected Destination:

Player Window

☒

Device Name

Device Type

☒

XP

Player Window

→

☐

Device Name

Device Type

Operation

☐

XP

Player Window

🗑

< 1 > 10 / page

Back

Confirm

Cancel

225

5. Click **OK** to complete the addition.

Table 14-2 Parameter Description for Adding Transcoding Rules

Parameter	Description
Rule Name	Name of the transcoding rule.
Stream Policy	Destination stream type for the transcoding rule. Five types are supported: UDP+TS, RTP+TS, TCP+TS, GB UDP, and GB TCP. For example, if UDP+TS is selected, the camera live streams selected for this rule will be converted to UDP TS streams.
Enable/Disable Rule	Enabled by default. A transcoding rule will take effect only after it is enabled.
Source	Configure the source device for transcoding. Options include Camera, ECR, NVR, Child Domain, and Peer Domain. Note! Camera/ECR/NVR: Show the camera/ECR/NVR of the local domain. The transcoding rule takes effect only for the selected camera/ECR/NVR. Child Domain/Level Domain: The transcoding rule takes effect for all cameras in the selected child domain/peer domain.
Destination	Configure the destination of the streams after transcoding. Options include Player Pane, Monitor, Parent Domain, Peer Domain, and Video Wall. Note! Player Pane: Live videos started from the live streaming page. Monitor: Live videos started from the DC video wall. Video Wall: Live videos started from the decoded splicing control wall. Parent Domain/Peer Domain: Live videos started from the player pane, monitor, and video wall in the parent domain/peer domain.

14.2.2 Edit Transcoding Rule

1. Click the  button on the right of the added transcoding rule to go to the **Edit Transcoding Rule** page.
2. Edit the rule name, select the stream policy and source, and click **Next**.
3. Edit the destination and click **OK** to complete the modification.

14.2.3 Delete Transcoding Rule

1. Click the  button on the right of the added transcoding rule and confirm to delete the transcoding rule.
2. After selecting multiple transcoding rules, click the **Delete** button and confirm to delete the rules in batches.

14.3 Trunk Management

Trunk management allows you to set the maximum number of live/playback media stream channels that can be received/shared by platform.

14.3.1 Add Trunk

1. Go to **Advanced Settings > Center Configuration > Trunk Management**.

2. Click **Add** to go to the **Add Trunk** page.

Figure 14-4 Add Trunk

Trunk Name:

Trunk Type:

Max Trunk Count: ⓘ

Live View Trunk Value: ⓘ

Playback Trunk Value: ⓘ

Live view trunk value + Playback trunk value = Total trunk value

3. Fill in the trunk name, trunk quantity, live view trunk value, playback trunk value, and trunk type.
4. Click **OK** to complete the addition.

Table 14-3 Parameter Description for Adding a Trunk

Parameter	Description
Trunk Name	Name of the local trunk.
Trunk Type	Three types of trunks are supported: Device Trunk, Parent Domain Trunk, and Child Domain Trunk. ● Device Trunk: You can only select the local domain device or organization for the trunk information, and the device only supports IMOS cameras. The number of streams will be limited by this trunk when the selected local domain device starts live videos or playback. ● Parent Domain Trunk: You can only select the parent domain for the trunk information. The number of streams will be limited by this trunk when the selected parent domain starts camera live videos or playback shared by the local domain. ● Child Domain Trunk: You can only select the child domain for the trunk information. The number of streams will be limited by this trunk when the local domain starts camera live or playback shared by the child domain.
Trunk Value	Maximum number of live and playback streams allowed. Live View Trunk Value + Playback Trunk Value ≤ Trunk Value.
Live View Trunk Value	Maximum number of live streams allowed.
Playback Trunk Value	Maximum number of playback streams allowed.

14.3.2 Add Trunk Information

Trunk information is used to specify the device, parent domain or child domain that is subject to the trunk.

1. Go to **Advanced Settings > Center Configuration > Trunk Management**.
2. Click  corresponding to a trunk in the trunk list, and select **Add Trunk Information** to go to the **Add Trunk Information** page.

Figure 14-5 Add Trunk Information

Available Resource List

Please enter the resource ...

- All
- All External Domains
- Local Domain

Selected Resources

Resource Name	Resource ID	With Sub Organization
No Data		

Confirm Cancel

3. Select the device, parent domain or child domain, click to add it to the list of selected resources, and click **OK** to complete the addition.

14.3.3 Manage Trunk

1. View Trunk Information

1. Click corresponding to a trunk in the trunk list, and select **View Trunk Information** to go to the **View Trunk Information** page.

Figure 14-6 View Trunk Information

Batch Delete

☐	Resource Name	Resource ID	With Sub Organization
No Data			

Confirm Cancel

2. After selecting the resources, click **Batch Delete** to delete the resources in the trunk information.

2. Edit Resource Name

1. Click corresponding to a trunk in the trunk list, and select **Edit Resource Name** to edit the trunk name.
2. After editing the trunk name, click to complete the modification.

Figure 14-7 Edit Resource Name

☐	干线名称
☐	下级域干线 ✓ ✕

3. Start/Stop Trunk

- Click ☐ on the right of the trunk to start the trunk. Trunk management takes effect once the trunk is started.
- Click ☒ on the right of the trunk to stop the trunk. Trunk management does not take effect once the trunk is stopped.

4. Delete Trunk

- Click  corresponding to the trunk and confirm to delete the trunk.
- Select multiple trunks, click **Delete**, and confirm to delete the trunks in batches.



Note!

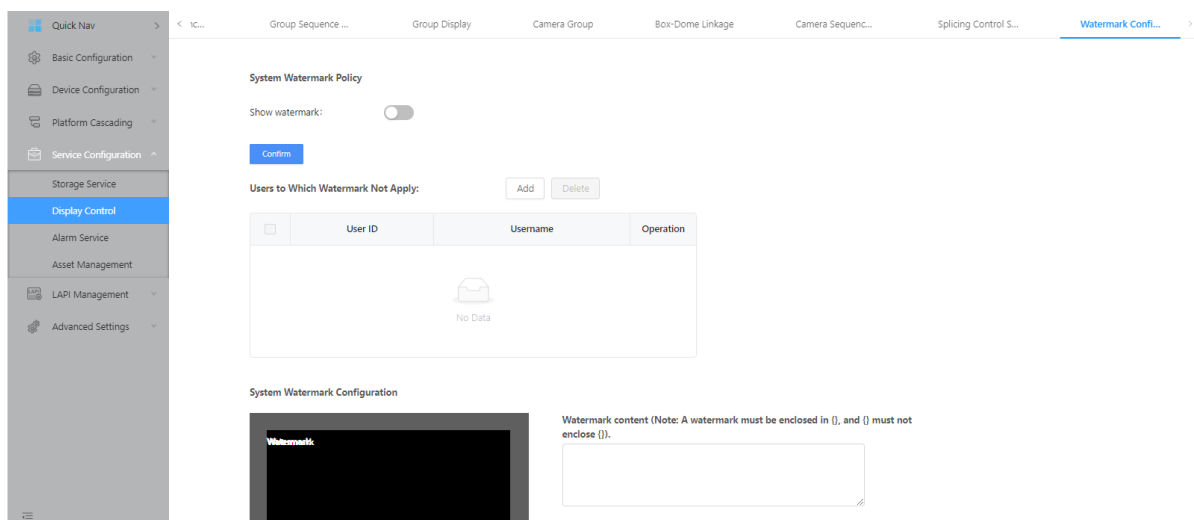
Before deleting a trunk, you need to delete the trunk information on the **View Trunk Information** page and stop the trunk.

15 System Watermark

After watermark is enabled and you log in as a user with watermark permission, watermark is visible on videos and people/vehicle images (except on the locally imported videos/images without watermarks), and is also visible on the downloaded recordings and exported images.

15.1 System Watermark Policy

1. Go to **Device Management > Service Configuration > Display Control > Watermark Configuration**.



The screenshot shows the 'Watermark Conf...' page in a web interface. The left sidebar contains a navigation menu with 'Display Control' selected. The main content area is titled 'System Watermark Policy'. It features a 'Show watermark:' toggle switch, a 'Confirm' button, and a section 'Users to Which Watermark Not Apply:' with 'Add' and 'Delete' buttons. Below this is a table with columns 'User ID', 'Username', and 'Operation', which is currently empty with a 'No Data' message. At the bottom, there is a 'System Watermark Configuration' section with a preview of a watermark on a video frame and a text input field for 'Watermark content'. A note specifies that the watermark must be enclosed in brackets and not enclosed in a single pair.

2. Enable **Show Watermark** and **Duplicate Watermarks** as needed. Select applicable video types (live video, playback control, download template).
3. Click **OK**.



NOTE!

You can choose users to whom the configured watermark is not effective. Watermark will not be displayed for the user after the user logs in to the system.

15.2 System Watermark Configuration

4. Go to **Device Management > Service Configuration> Display Control > System Watermark Policy**.

5. Enter watermark contents (each watermark is enclosed with {}, nested brackets {} are forbidden).
6. Set the watermark style.
7. Click **OK**.

16 O&M Management

16.1 Operation Logs

In the **System Management > O&M Management > Operation Logs** interface. The system automatically records user operations and generates system logs, allowing users to quickly locate and review them.

- Query Logs: In the left-side search criteria panel, configure conditions such as time, business type, operation object, operation result, and user name to display the log results on the right.
- Export Logs: Click to export the logs to your local device.
- Refresh Logs: Click to view the latest logs.

Operation Logs

Device Statistics

Asset Statistics

Storage Statistics

Username :

Please enter

IP address :

Please enter

Operation Type :

All

Log Type :

All

Operation Time :

2025-09-10 00:00:00 - 2025-09-10 23:59:59

Today

Last 7 Days

Last 30 Days

Search

Reset

Expand

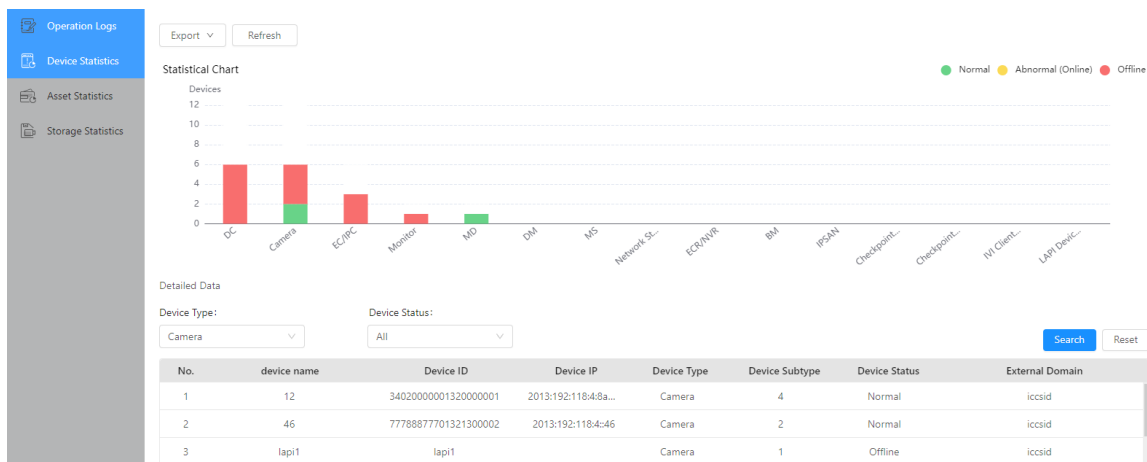
Export

Refresh

No.	Username	Operation Time	IP address	Operation Object	Operation Type	Lo
1	loadmin	2025-09-10 16:59:00	192.117.1.101	e103rulecode#1757495489850317	Add Configuration	Device
2	loadmin	2025-09-10 16:56:21	192.117.1.101	48598020250910165621+XP	Modify Configuration	Device
3	loadmin	2025-09-10 16:56:21	192.117.1.101	loadmin(loadmin)	User Login	
4	loadmin	2025-09-10 15:41:10	192.117.1.200	loadmin(loadmin)	User Logout	
5	loadmin	2025-09-10 15:40:29	192.117.1.200	12119020250910154029+XP	Modify Configuration	Device

16.2 Device Statistics

In the **System Management > O&M Management > Device Statistics** interface, the system supports statistics on the number and online status of various device types on the management platform, displays detailed information, and enables data filtering by device type and device status.



16.3 Asset Statistics

In the **System Management > O&M Management > Asset Statistics** interface, the system supports statistics on all assets within the current domain and its subordinate domains, and displays the information in report format. Users can query asset details based on criteria such as organization, asset type, manufacturer, purchase date, contractor, installation date, location name, and warranty expiration date.

Operation Logs

Device Statistics

Asset Statistics

Storage Statistics

Select Organization

Local domain

Asset Type

All

Search

Reset

No.	Organization Name	Running	Damaged	Under Repair	Scrapped	All	Stocked	To be Installed	Installed	Tested	Total
1	Local domain	0	0	0	0	0	0	0	0	0	0
2	111	0	0	0	0	0	0	0	0	0	0
3	545454	0	0	0	0	0	0	0	0	0	0
4	56445dfdfdfdfdfdf	0	0	0	0	0	0	0	0	0	0
5	H2	0	0	0	0	0	0	0	0	0	0
6	H3	0	0	0	0	0	0	0	0	0	0
7	xx	0	0	0	0	0	0	0	0	0	0

16.4 Storage Statistics

In the **System Management > O&M Management > Storage Statistics** interface.

- Set the camera name/status, whether a recording schedule is configured, storage device name, storage status, and whether the storage plan is enabled. Click **Statistics** to query camera storage information. Select the desired records from the results, and click **Export** to export the data to the local device.

Operation Logs

Device Statistics

Asset Statistics

Storage Statistics

Camera Name

Please enter

Camera Status

All

Recording Schedule Set

All

Storage Device Name

Please enter

Storage Status

All

Recording Schedule Enabled

All

Statistics

Reset

Camera Info Statist...

Export

☐	No.	Camera Name	Camera ID	EC Chan...	Camera St...	Parent Device ID	Device IP	Storage Device	Operation
☐	1	12	34020000001320000001	2	Normal	ECPAGGUOBIAO			
☐	2	46	77788877701321300002	1	Normal	ECPAGGUOBIAO			
☐	3	lapi1	lapi1	3	Offline	ECPAGGUOBIAO			
☐	4	onvif64z	onvif64	1	Offline	ECPAGIMOSCODE			
☐	5	test11	test11	4	Offline	ECPAGGUOBIAO			
☐	6	test12	test12	5	Offline	ECPAGGUOBIAO			

- Click **Camera Info Statistics** to view the count of cameras by type.

Camera Info Statistics		
No.	Camera Type	Qty
1	All Cameras	6
2	External Domain Camera	0
3	Local Domain Camera	6
4	Offline Camera in Local Domain	4
5	Online Camera in Local Domain	2
6	Video Lost Camera in Local Domain	0

Cancel

OK