



DSS Professional

User Manual



Foreword

General

This user manual introduces the functions and operations of DSS Professional (hereinafter referred to as "the system" or "the platform").

You can get the user manual from <https://software.dahuasecurity.com/en/download>.

Safety Instructions

The following signal words might appear in the manual.

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

Frequently Used Functions

Icon/Parameter	Description
	View the details of an item.
	Clear all selected options.
	Search for items by keywords or specified content.
 or Delete	Delete items one by one or in batches.
 or Edit	Edit the parameters of an item.
 ,  , Enable , or Disable	Enable or disable items one by one or in batches.
 or Export	Exported the selected content to your local computer.
 or Refresh	Refresh the content.
*	A parameter that must be configured.

Privacy Protection Notice

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

About the Manual

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

Table of Contents

Foreword.....	I
1 Overview.....	1
1.1 Introduction.....	1
1.2 Highlights.....	1
2 Installation and Deployment.....	2
2.1 Standalone Deployment.....	5
2.1.1 Server Requirements.....	5
2.1.2 Installing Management Tool.....	5
2.1.3 Configuring Server IP Address.....	7
2.1.4 Management Tool.....	7
2.1.5 Installing and Logging in to DSS Client.....	10
2.1.6 Licensing.....	14
2.2 Multiple Sites Deployment.....	19
2.3 Distributed Deployment.....	20
2.3.1 Installing Main Server.....	20
2.3.2 Installing Sub Server.....	20
2.4 Hot Standby.....	21
2.5 Cascade.....	21
2.6 N+M.....	22
2.7 Configuring LAN or WAN.....	25
2.7.1 Configuring Router.....	25
2.7.2 Mapping IP or Domain Name.....	25
2.8 Virtualization Deployment.....	26
2.9 Installing Plugin.....	27
3 Basic Configurations.....	28
3.1 Managing Resources.....	28
3.1.1 Adding Organization.....	28
3.1.2 Managing Device.....	29
3.1.3 Binding Resources.....	42
3.1.4 Adding Recording Plans.....	44
3.1.5 Adding Video Retrieval Plans.....	48
3.1.6 Adding Time Template.....	53
3.1.7 Configuring Video Retention Period.....	54
3.1.8 Configuring Events.....	54
3.1.9 Configuring Information Display Content.....	55
3.1.10 Configuring Door.....	56
3.1.11 Configuring Parking Space Available Display.....	58

3.1.12 Synchronizing People Counting Rules.....	61
3.2 Adding Roles and Users.....	62
3.2.1 Adding a Role.....	62
3.2.2 Adding a User.....	64
3.2.3 Adding a User Group.....	65
3.2.4 Importing Domain Users.....	66
3.2.5 Syncing Domain Users.....	67
3.2.6 Configuring Auto Synchronization.....	67
3.2.7 Password Maintenance.....	68
3.3 Configuring Storage.....	70
3.3.1 Configuring Network Disk.....	70
3.3.2 Configuring Server Disk.....	73
3.3.3 Configuring Disk Group.....	74
3.3.4 Configuring Device Storage.....	75
4 Businesses Configuration.....	77
4.1 Configuring Events.....	77
4.1.1 Configuring Event Linkage.....	77
4.1.2 Configuring Combined Event.....	81
4.1.3 Configuring Alarm Parameter.....	82
4.1.4 Configuring Generic Event.....	85
4.2 Configuring Map.....	86
4.2.1 Preparations.....	86
4.2.2 Adding a Map.....	86
4.2.3 Marking Devices.....	91
4.2.4 Configuring Radar-PTZ Linkage.....	91
4.3 Personnel and Vehicle Management.....	93
4.3.1 Adding Person and Vehicle Groups.....	93
4.3.2 Configuring Person Information.....	94
4.3.3 Vehicle Management.....	112
4.4 Watch List Configuration.....	113
4.4.1 Face Arming List.....	114
4.4.2 Vehicle Watch List.....	117
4.5 Access Control.....	118
4.5.1 Preparations.....	118
4.5.2 Configuring Zone.....	119
4.5.3 Configuring Access Rule.....	126
4.5.4 Configuring Public Passwords.....	137
4.5.5 Configuring Access Card.....	137
4.5.6 Configuring Access Control Devices.....	138
4.6 Video Intercom.....	138

4.6.1 Preparations.....	138
4.6.2 Call Management.....	139
4.6.3 Configuring Building/Unit and Call Mode.....	141
4.6.4 Configuring Room.....	142
4.6.5 Synchronizing Contacts.....	143
4.6.6 Setting Private Password.....	143
4.6.7 QR Codes.....	144
4.6.8 App User.....	144
4.7 Visitor Management.....	145
4.7.1 Preparations.....	145
4.7.2 Configuring Visit Settings.....	145
4.8 Parking Lot.....	147
4.8.1 Preparations.....	147
4.8.2 Configuring Parking Lot.....	149
4.8.3 Managing Parking Space.....	162
4.8.4 Managing Vehicle Group.....	166
4.8.5 Configuring Scheduled Report.....	166
4.9 Intelligent Analysis.....	168
4.9.1 People Counting Group.....	168
4.9.2 Scheduled Report.....	169
4.10 Intelligent Inspection.....	170
4.10.1 Configuring Object Template.....	170
4.10.2 Configuring Inspection Object.....	172
4.10.3 Configuring Inspection Plan.....	174
4.10.4 Configuring Temperature Monitoring Event.....	175
4.11 Maintenance Center.....	176
4.11.1 Configuring Alert Rule.....	176
4.11.2 Configuring Video Integrity.....	176
4.12 AR.....	177
4.12.1 Configuring System Name.....	177
4.12.2 Configuring Tag Template.....	178
4.13 Configuring Visual Tracking.....	179
4.14 Video Analysis.....	182
4.14.1 Adding a Recording Task.....	183
4.14.2 Adding a Local Task.....	184
4.15 Synthesis.....	186
4.15.1 Event Transferral.....	186
4.15.2 Synchronizing Data.....	197
4.15.3 System Integration.....	199
5 Businesses Operation.....	202

5.1	Monitoring Center.....	202
5.1.1	Main Page.....	202
5.1.2	Video Monitoring.....	205
5.1.3	Playback.....	236
5.1.4	Map Applications.....	252
5.1.5	Video Wall.....	256
5.1.6	AR.....	265
5.2	Event Center.....	272
5.2.1	Real-Time Event.....	273
5.2.2	History Alarms.....	276
5.2.3	Event Statistics.....	276
5.2.4	Alarm Controller.....	278
5.2.5	Arming Control.....	280
5.3	DeepXplore.....	282
5.3.1	Searching for People.....	282
5.3.2	Searching for Vehicles.....	285
5.3.3	Searching for Records.....	286
5.3.4	Track Playback.....	288
5.3.5	Searching for POS Transaction.....	289
5.3.6	Adding a Case Bank.....	291
5.3.7	Viewing Track of MPT Devices.....	293
5.4	Access Management.....	294
5.4.1	Access Control.....	294
5.4.2	Video Intercom Application.....	302
5.4.3	Visitor Application.....	305
5.5	Parking Lot.....	317
5.5.1	Statistics Dashboard.....	317
5.5.2	Entrance and Exit Monitoring.....	318
5.5.3	Searching for Records.....	320
5.5.4	Parking Information.....	328
5.5.5	Visualized Parking Lot.....	330
5.5.6	Vehicle Location.....	330
5.6	Intelligent Analysis.....	332
5.6.1	People Counting.....	332
5.6.2	Heat Maps.....	334
5.6.3	In-Area People Counting.....	335
5.6.4	Metadata Analysis.....	335
5.7	Intelligent Inspection.....	336
5.7.1	Monitoring Point.....	336
5.7.2	Reviewing Inspection Result.....	337

5.7.3 Viewing Real-Time Inspection.....	337
5.7.4 Searching for Inspection History.....	338
5.7.5 Searching for Data Analysis.....	339
5.8 Maintenance Center.....	340
5.8.1 Viewing System Status.....	340
5.8.2 Monitoring Network Status.....	341
5.8.3 Maintenance Management.....	345
6 General Application.....	348
6.1 Target Detection.....	348
6.1.1 Typical Topology.....	348
6.1.2 Preparations.....	348
6.1.3 Live Target Detection.....	349
6.1.4 Searching for Metadata Snapshots.....	349
6.2 ANPR.....	350
6.2.1 Typical Topology.....	350
6.2.2 Preparations	350
6.2.3 Live ANPR.....	351
6.2.4 Searching for Vehicle Snapshot Records.....	352
6.3 Face Recognition.....	352
6.3.1 Typical Topology.....	352
6.3.2 Preparations.....	353
6.3.3 Arming Faces.....	353
6.3.4 Live Face Recognition.....	353
6.3.5 Searching for Face Snapshots.....	354
6.4 POS.....	355
6.4.1 Typical Topology.....	355
6.4.2 Preparations.....	355
6.4.3 Setting POS End Sign.....	356
6.4.4 POS Live View.....	356
6.4.5 Searching for POS Receipts.....	357
6.5 Lift Control.....	358
6.5.1 Typical Topology.....	359
6.5.2 Preparations.....	359
6.5.3 Lift Controller Maintenance.....	360
6.5.4 Configuring Event.....	362
6.5.5 Authorized Access.....	363
6.5.6 Calling Lift on VTO.....	365
6.5.7 Viewing Access Records.....	366
7 System Configurations.....	367
7.1 System Deployment.....	367

7.1.1	Distributed Deployment.....	367
7.1.2	Cascade Deployment.....	369
7.2	License Information.....	370
7.3	License.....	370
7.3.1	Activating License.....	371
7.3.2	Deactivating License.....	372
7.3.3	Maintenance Renewal.....	374
7.4	System Parameters.....	377
7.4.1	Configuring Security Parameters.....	377
7.4.2	Configuring Retention Period of System Data.....	378
7.4.3	Time Synchronization.....	379
7.4.4	Configuring Central Intelligent Server.....	380
7.4.5	Configuring Email Server.....	381
7.4.6	Configuring Active Directory.....	381
7.4.7	Configure POS Parameters.....	382
7.4.8	Configure Device Access Parameters	383
7.4.9	Remote Logs.....	384
7.4.10	Configuring Independent Database.....	384
7.4.11	Configuring Push Notification for App.....	385
7.4.12	Configuring Network Device Protocol.....	385
7.4.13	Configuring Privacy Policy.....	386
7.5	Backup and Restore.....	386
7.5.1	System Backup.....	386
7.5.2	System Restore.....	387
8	Management.....	389
8.1	Download Center.....	389
8.1.1	By Timeline or File.....	389
8.1.2	By Tagging Record.....	390
8.1.3	By Locking Record.....	391
8.2	Viewing Local Images.....	391
8.3	Playing Local Videos.....	391
8.4	Configuring Local Settings.....	393
8.4.1	Configuring General Settings.....	393
8.4.2	Configuring Video Settings.....	395
8.4.3	Configuring Video Wall Settings.....	398
8.4.4	Configuring Alarm Settings.....	399
8.4.5	Configure File Storage Settings.....	401
8.4.6	Viewing Shortcut Keys.....	401
8.4.7	Exporting and Importing Configurations.....	401
8.5	Managing Logs.....	402

8.5.1 Operation Log.....	402
8.5.2 Device Log.....	402
8.5.3 System Log.....	403
8.5.4 Service Log.....	403
8.6 Help.....	403
8.7 Quick Commands.....	403
Appendix 1 Service Module Introduction.....	406
Appendix 2 Security Commitment and Recommendation.....	408

1 Overview

1.1 Introduction

Dahua Security System (DSS) Professional is designed for centralized security management. Relying on powerful hardware performance, it provides centralized video monitoring, access control, video intercom, alarm management, and POS records search. Also, it can help you improve your security management efficiency with the help of artificial intelligence technologies such as face recognition, license plate recognition, and metadata.

Whether you are a small business with a few cameras, or a global business with over 20,000 cameras, DSS Professional is the right solution for you. Even if your needs change in the future, you can easily scale, upgrade or add functionalities to DSS Professional, so that your needs are met. Build your security management system on a solid foundation with DSS Professional.

1.2 Highlights

- Scalable design, easy to grow

With distributed deployment, you can easily expand the supported channels to 20,000 and central storage capacity to 4 PB. The multi-site function allows you to incorporate multiple DSS platforms into one, and you can perform operations such as viewing live video, playing back recorded videos, viewing real-time and historical events, and more of multiple platforms on one platform.

- AI-powered applications, proactive security

DSS Professional integrates various AI capabilities that devices have, such as face recognition, automatic number plate recognition, and video metadata. You will be notified immediately when the target you are interested in appears, allowing you or security personnel to take necessary security measures.

- Highly available technology, more stable

With hot standby and N+M redundancy, DSS Professional ensures that your business will not be interrupted by failed servers.

- Customized services, enhanced competitiveness

We offer services for you to build DSS Professional into your own platform, allowing it to fully suit your needs and give you a competitive edge in the market.

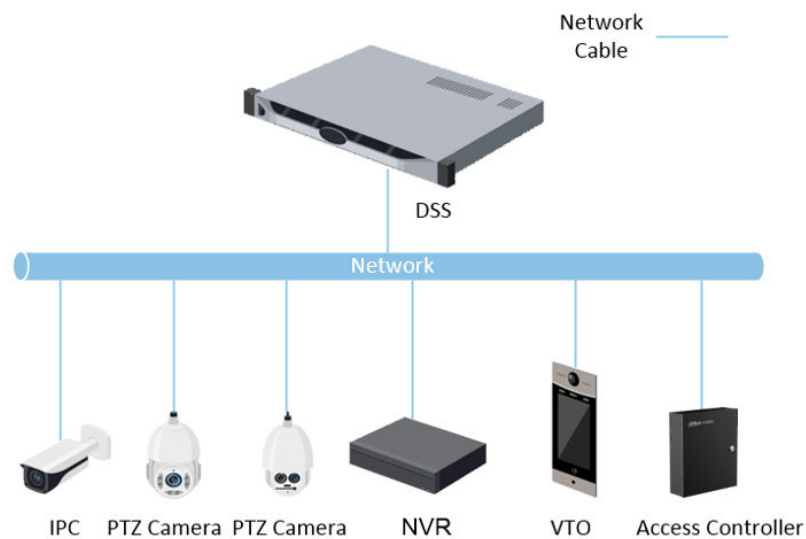
2 Installation and Deployment

DSS platform supports standalone deployment, multiple sites deployment, distributed deployment, hot standby, and N+M deployment, and LAN to WAN mapping.

Standalone Deployment

For projects with a small number of devices, only one DSS server is required.

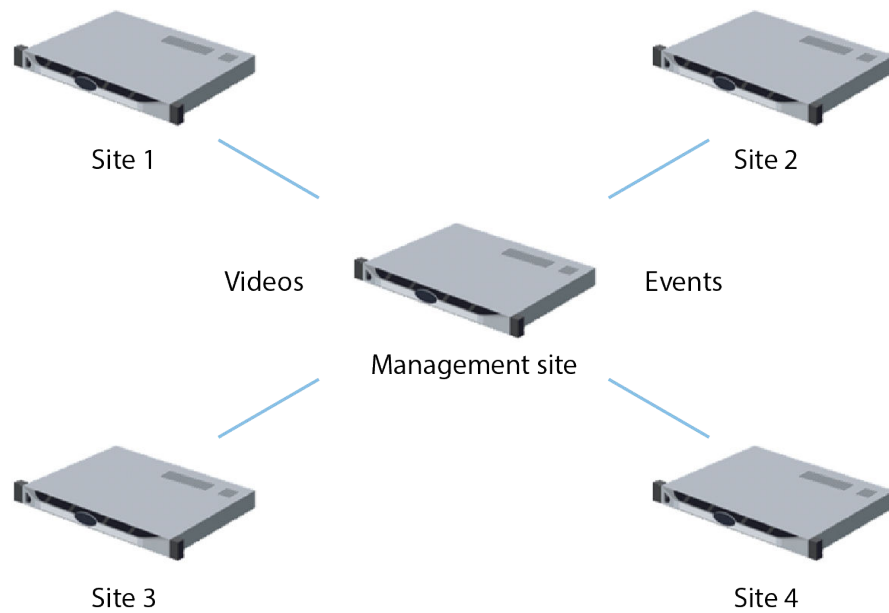
Figure 2-1 Standalone deployment



Multiple Sites Deployment

If you have multiple platforms, you can connect one or more platforms to your current one, so that you can view the resources from them directly on your main platform, including viewing real-time videos from video channels, searching for viewing real-time and historical events, and downloading recorded videos.

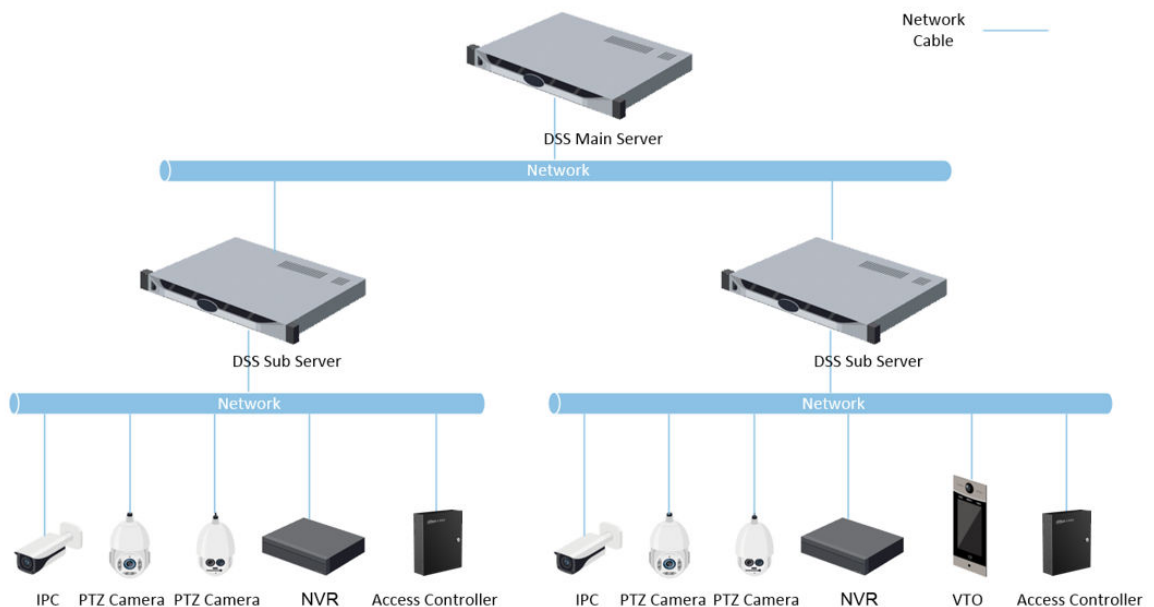
Figure 2-2 Multiple sites deployment



Distributed Deployment

Suitable for medium to large projects. Sub servers are used to share system load, so that more devices can be accessed. The sub servers register to the main server, and the main server centrally manages the sub servers.

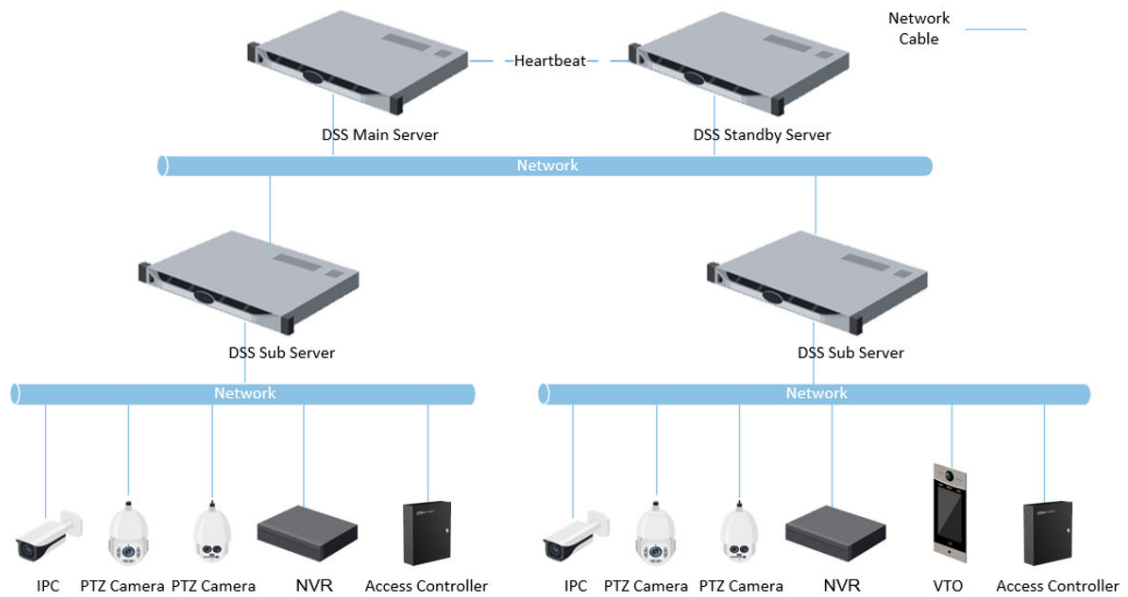
Figure 2-3 Distributed deployment



Hot Standby

Used with systems that require high stability. The standby server takes over the system when the active server malfunctions (such as with power-off and network disconnection). You can switch back to the original active server after it recovers.

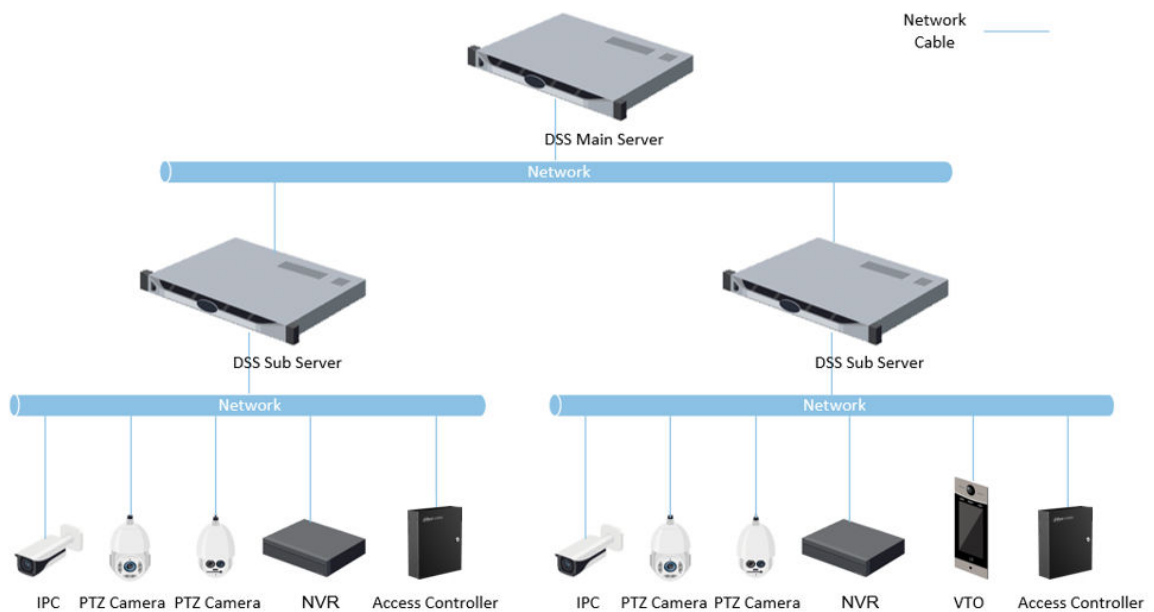
Figure 2-4 Hot standby



N+M

Each sub server has a standby server to maintain stability. When a sub server malfunctions, the system replaces it with an idle standby server. When the malfunctioning server normalizes, you can manually switch back to it. If you do not manually switch them, the system will automatically make the switch if the standby server malfunctions.

Figure 2-5 N+M



LAN to WAN Mapping

Perform port mapping when:

- The server of the platform and devices are on a local area network, and the DSS client is on the Internet. To make sure that the DSS client can access the platform server, you need to map the platform IP to the Internet.
- The platform is on a local area network, and the devices are on the Internet. If you want to add devices to the platform through automatic registration, you need to map the IP address and ports of the platform to the Internet. For devices on the Internet, the platform can add them by their IP addresses and ports.



The management tool does not differentiate service LAN ports and WAN ports. Make sure that the WAN ports and LAN ports are the same.

2.1 Standalone Deployment

2.1.1 Server Requirements

Table 2-1 DSS Professional hardware requirements

Parameter	Hardware Requirement	Operating System
Recommended requirements	• CPU: Intel Xeon Silver 4214 2.2 GHz • RAM: 32 GB • Network card: 4 × Ethernet port @ 1000 Mbps • Hard drive type: 7200 RPM Enterprise Class HDD 1 TB • DSS installation directory space: 500 GB	• Microsoft® Windows Server 2019 Standard (64-bit) • Microsoft® Windows Server 2022 Standard (64-bit) • Microsoft® Windows 10 20H2 Pro (64-bit) • Microsoft® Windows 11 21H2 Pro (64-bit)
Minimum requirements	• CPU: Intel Xeon E-2224 3.4 GHz/4 cores • RAM: 16 GB • Network card: 2 × Ethernet port @ 1000 Mbps • Hard drive type: 7200 RPM Enterprise Class HDD 1 TB • DSS installation directory space: 500 GB	



- Face recognition images, videos, and files cannot be stored on the system disk and DSS installation disk. We recommend you store these files on a separate local disk or a network disk.
- For best performance, we recommend adding additional hard drives to store pictures.

2.1.2 Installing Management Tool

Prerequisites

- You have downloaded the installation package from the official website or received it from our sales or technical support.

- You have prepared a server that meets the hardware requirements described in "2.1.1 Server Requirements".

Procedure

Step 1 Double-click the DSS installer .



The name of the installer includes version number and date, confirm before installation.

Step 2 Click **the software license agreement**, and then read the agreement.

Step 3 Select the check box to accept the agreement, and then click **Next**.

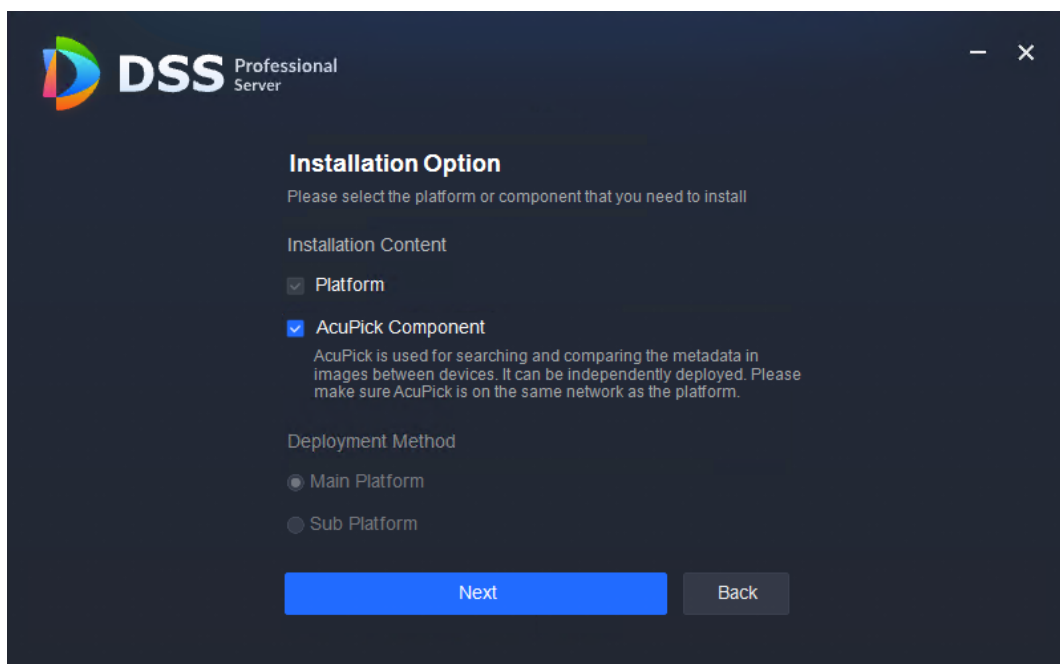
Step 4 Select the type of platform you want to install, and then click **Next**. **Main** is selected by default.

Step 5 Select **AcuPick** as needed, and then click **Next**.



AcuPick can be deployed on the same server as the platform, or on a separate one. For how to configure parameters for AcuPick, see "5.1.2.1.2 AcuPick".

Figure 2-6 Select a platform type



Step 6 Click **Browse**, and then select an installation path.

If the **Install** button is gray, check whether the installation path and space required meet the requirements. The total space required is displayed on the page.



We do not recommend installing the management tool on disk C, because features such as face recognition require higher disk performance.

Step 7 Click **Install**.



The installation process takes about 4 to 8 minutes. Do not cut off the power or close the program.

Step 8 Click **Run** after the installation completes.

Step 9 Configure the network parameters.

1. Configure the IP address of the network card.



- **Dual NIC** will be available if the server has 2 network cards. This is useful when you need to access devices on 2 different network segments.
- The platform supports using a maximum of 2 network cards at the same time. You can either use 1 network card for accessing devices on a local area network, and 1 network card for services on the Internet; or use both network cards for accessing devices on a local area network, and then map one of them to the Internet.

2. (Optional) Enable **WAN Mode**, enter a WAN IP address or a domain name, and then click **Next**.



If the platform is in a local network, use this function to connect it to the Internet so that you can access it from outside the local network.

3. Configure the TLS version, and then click **Finish**.

TLS1.2 is selected by default and cannot be changed. We do not recommend using TLS1.0 and TLS1.1 because they have serious security vulnerabilities.



If the available RAM of the server is less than 4 GB, you can only use basic functions related to video. If it is less than 2.5 GB, you cannot use any function.

For a distributed server, if the available RAM of the server is less than 4 GB, you cannot use any function.

Related Operations

- To uninstall the platform, log in to the server, go to "..\DSS\DSS Server\Uninstall", double-click uninst.exe, and then follow the on-screen instructions to uninstall the program.
- To update the system, directly install the new program. The system supports in-place update. Follow the steps above to install the program.

2.1.3 Configuring Server IP Address

Change the server IP address as you planned. Make sure that the server IP can access the devices in your system. For details, see the manual of the server.



After changing the IP address of the server, you need to update it in the management tool. See the following section.

2.1.4 Management Tool

The management tool allows you to view status of services, start or stop services, change service ports, and more.



On the server, double-click

Figure 2-7 Management tool

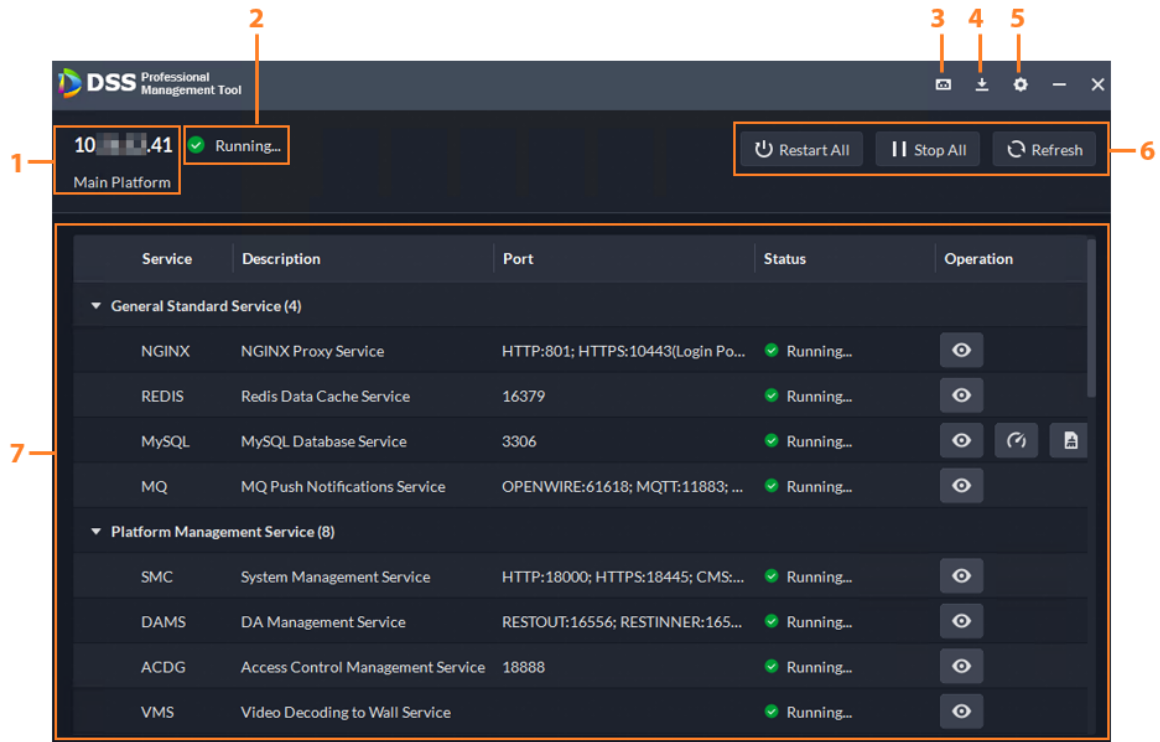


Table 2-2 Interface description

No.	Function	Description
1	Server information	Displays the IP address and type of the platform.
2	Status of services	There are 5 statuses of services, including starting, unavailable, stopping, running, and stopped. - The unavailable status only depends on the status of the SMC service. If the SMC service is not properly running, the overall status will be unavailable. - Running means that all services are running normally.
3	Information for port mapping	Displays the ports that you need to map for various functions. Select one or more functions, the ports you must map will be displayed on the right. Click  to export them to your computer so that you can check on them easily.
4	Download clients and logs	- Client: Displays how to download the PC client and App. - Logs: Download the operation logs of the management tool.

No.	Function	Description
5	Configurations and view information of the platform	• Network: Configure the network card mode, IP address, and the WAN mode. If the server has two network cards, you can select Dual NIC mode, configure two IP addresses, and then the platform will be able to connect to two networks and access the devices on each one. If the platform is in a local network and the devices are on the internet, or you need to access the platform that is in a local network from the Internet, you can enable WAN Mode and map the IP address of the platform to a WAN IP address or a domain name. • Security: Select a TLS protocol version when you access the webpage of the platform through a browser. TLS1.2 is selected by default and cannot be disabled. There are security vulnerabilities to TLS1.0 and 1.1. We strongly recommend you disable it to avoid security risks. After configuration, follow the on-screen instructions to configure the TLS protocol version in the IE browser so that you can access the webpage of the platform normally. • Language: Select the language of the management tool. Multiple languages are supported. • Port Self-adaption: If a port is occupied, the platform will change it automatically. After turning on or off this function, you must restart the server for it to be effective. • Reset system password: Reset the password of system user. 1. Click Export, set the encryption password, and then export the request file. 2. Contact the technical support to get the password reset file through the request file. 3. Click Reset to import the reset file, and then log in the DSS client to initialize the password. • User manual: View the user manual of the platform. • About: View the software version information, software license agreement, and more.
6	Service management	• Click Restart All to restart all services.  When starting the platform, if the available memory of the server does not reach 4 GB, only the basic video services can be enabled. If the server has less than 2.5 GB of available memory, no services are available. • Click Stop All to stop all services. • Click Refresh to refresh services.
7	Services	Displays all services, and their status and port numbers. Click  to change the port number of a service, and then the services will restart automatically after modification.

No.	Function	Description
	Database repair	If you cannot log in to the client because the database is abnormal, you can try to repair it manually. Click  of the MySQL service, and follow the instructions. Based on the items checked, the platform will determine whether repair or restoration is needed. If repair fails, you can try restoring the database. During restoration, the platform will back up the database. Please make sure that there is enough space. Otherwise, restoration will fail. Click  to view all backup files. You can delete them as needed.  • This operation cannot be performed in hot standby. • To restore the database, the platform needs to use port 3306. If a process is using the port, you need to terminate it first.

2.1.5 Installing and Logging in to DSS Client

Install the DSS client before licensing it.

2.1.5.1 Installing DSS Client

You can visit the system through the DSS Client for remote monitoring.

2.1.5.1.1 DSS Client Requirements



Press the Windows key, and type **dxdiag**, and then click . On the **System** page, the information of your computer is displayed.

To install DSS Client, prepare a computer in accordance with the following requirements.

Table 2-3 Hardware requirements

Parameters	Description
Recommended system requirements	• CPU: Intel® Core i7-11700 @ 2.50 GHz • Memory: 16 GB and above • Graphics: NVIDIA® GeForce® RTX 3060 • Network Card: 1000 Mbps • HDD: Make sure that at least 200 GB is reserved for the client.

2.1.5.1.2 Downloading and Installing DSS Client

Procedure

- Step 1 Go to <https://IP address of the platform> in the browser.
- Step 2 Click **PC**, and then **Download**.

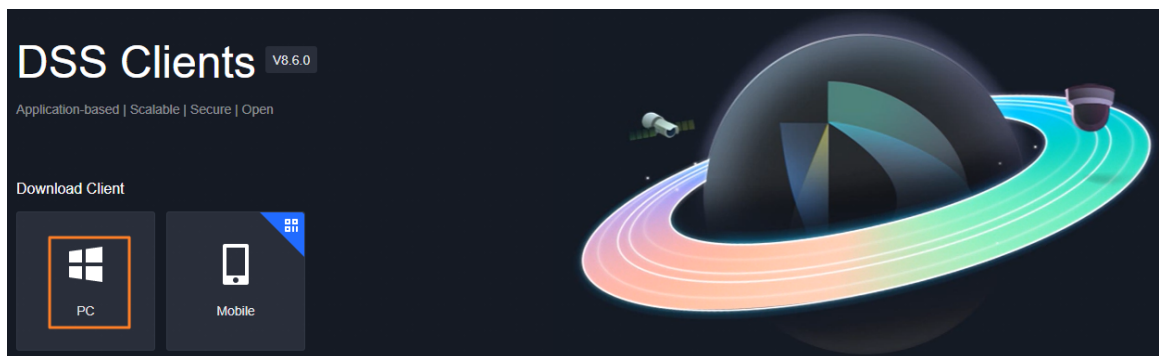


The platform also supports installation by MSI package. Visit <https://software.dahuasecurity.com/en/download/> and download the MSI package of the platform version you need. Please be advised that you cannot overwrite the PC client installed with an exe package, and vice versa. Also, the PC client installed with an MSI package does not support automatic update. You must download the package of the new version and install it manually.

If you save the program, go to Step 3.

If you run the program, go to Step 4.

Figure 2-8 Download DSS Client



Step 3 Double-click the DSS Client program.

Step 4 Select the checkbox of **I have read and agree to the DSS agreement** and then click **Next**.

Step 5 Select a path for installation, and then click **Install**.

The installation progress is displayed. It takes about 5 minutes to complete.

2.1.5.2 Logging in to DSS Client

Procedure

Step 1 Double-click  on the desktop.

Step 2 Select a language and user type.

Normal users are added on the platform manually. Domain users are imported from a domain.



If you want to log in using a domain user account, you must import the domain user first. For details, see "3.2.4 Importing Domain Users".

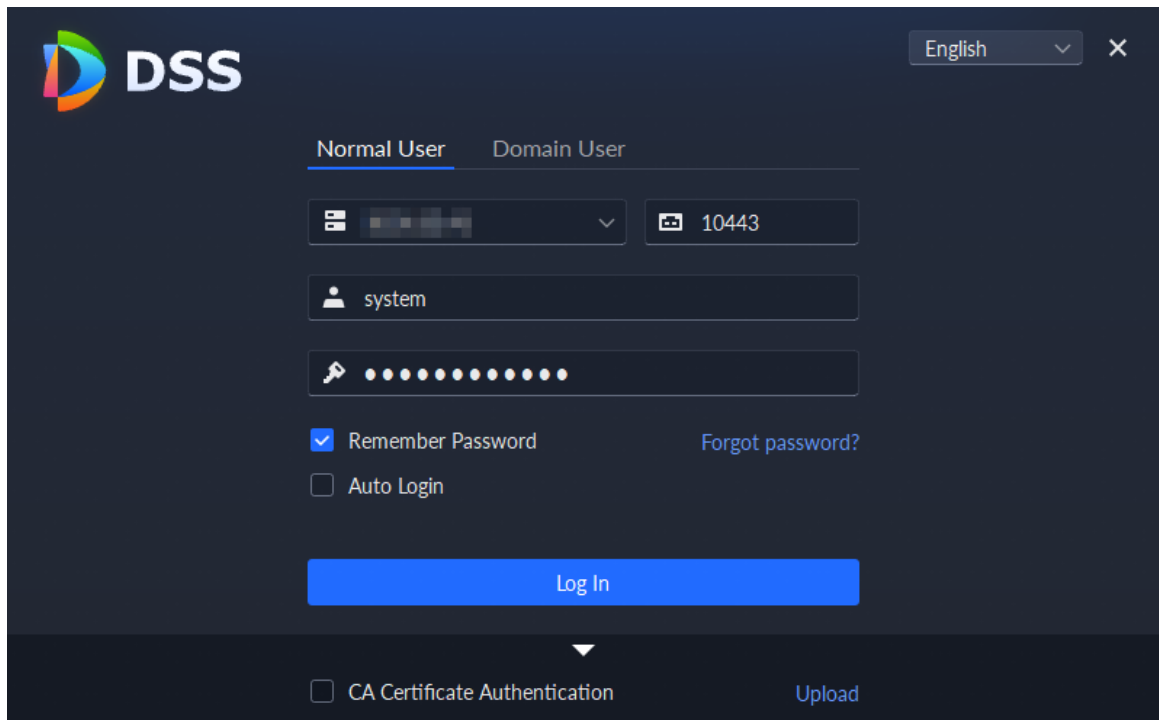
Step 3 Enter the IP address or domain name, and port number of the platform.

On the drop-down list, platforms that are in the same network as your computer will be shown.



- If you want to log in to the platform using a domain name, you must link its IP address to a domain name first. For details, see "2.7.2 Mapping IP or Domain Name".
- If you log in by localhost, the platform will automatically change it to 127.0.0.1.

Figure 2-9 Login



Step 4 Click anywhere else on the page to start initializing the platform.

For first-time login, you will be automatically directed to the initialization process.

If you are not logging in for the first time, enter the IP address or domain name, port number of the platform, username, and password, and then click **Login**.

1. The default user is system. Enter and confirm the password, and then click **Next**.

The password must consist of 8 to 32 non-blank characters and contain at least two types of characters: Uppercase, lowercase, number, and special character (excluding ' " ; : &).

2. Select your security questions and enter their answers, and then click **OK**.

The client will automatically log in to the platform by using the password you just set.



Please keep the security questions and answers properly. Otherwise, your password cannot be recovered if you forget it.

Related Operations

Select **CA Certificate Authentication** to enable client certification verification.

- Verification successful: You can log in to the client normally.
- Verification failed: Click **Upload** to upload the CA certificate. After the certificate is successfully imported, you can log in to the client normally.

2.1.5.3 Homepage of DSS Client

Figure 2-10 Homepage

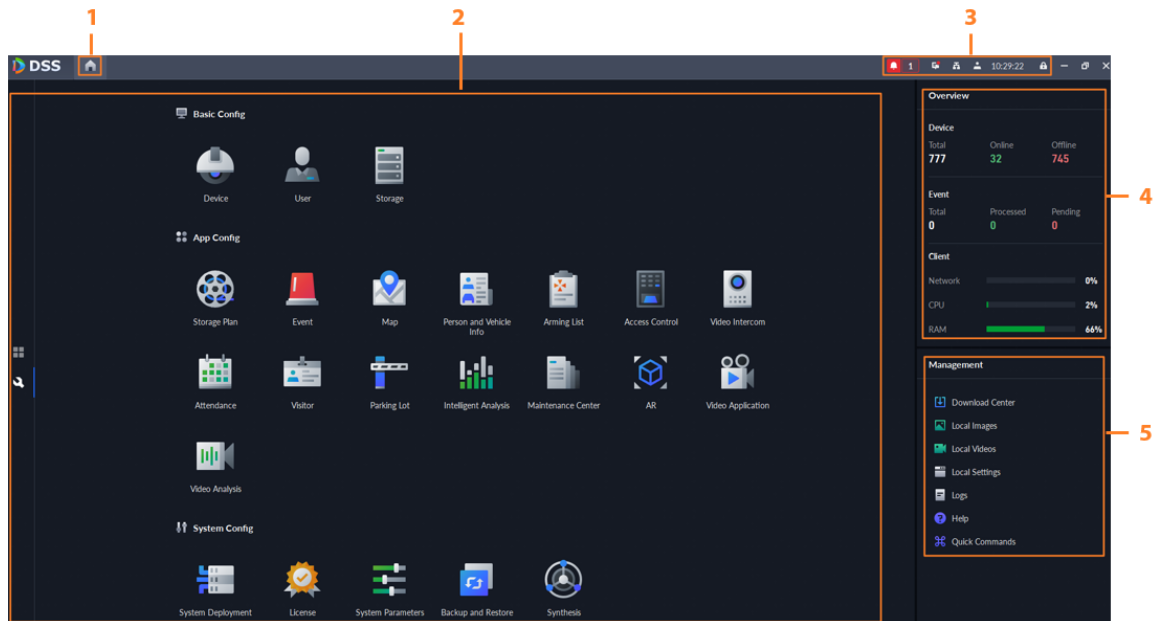


Table 2-4 Parameter description

No.	Name	Function
1	Tab	Displays the names of all tabs that are opened.
2	Applications	- Application options including monitoring center, access management, intelligent analysis and vehicle entrance control. - Configuration options.

No.	Name	Function
3	System settings	• : Enable or disable alarm audio. • : Displays number of alarms. Click the icon to go to Event Center. • Click  to view system messages, such as the information of a device was edited or deleted. The permissions of a user will determine what messages can be seen. For example, if user A does not have the permission of device A, then user A will not get the message when device A is deleted. • Click  to connect to other platforms as sites to your current platform. You can view certain resources from the sites. For details, see "2.2 Multiple Sites Deployment". • : User information: Click the icon, and then you can log in to the web page by clicking system IP address, change password, lock client and log out. ◇ Click platform IP address to go to the Web page. ◇ Click Change Password to change user password. ◇ Click Log Out to exit client. ◇ Click About to view version information. • Click  to lock client.
4	Overview	• The number of devices in total, offline and online. • The number of total, processed and pending events. • The client network, CPU and RAM usage.
5	Management	• Download videos. • Check local pictures and videos. • Settings for video, snapshot, video wall, alarm, security and shortcut keys. • View and manage logs. • View user manual. • Customize quick HTTP commands. For details, see "8.7 Quick Commands".

2.1.6 Licensing

Activate the platform with a trial or paid license the first time you log in to it. Otherwise you cannot use it. You can activate it by importing the license activation file offline or entering the activation code to activate it online, so that you can obtain the corresponding resources or business functions. You can upgrade your license for more features and increased capacity.

This section introduces license capacity, how to apply for a license, how to use the license to activate the platform, and how to renew your license.

2.1.6.1 Applying for a License

A license is used to confirm the features and number of channels you purchased. To get a formal license, contact our sales personnel. To apply for a trial license, visit our website and find DSS Professional, scroll to the bottom, click **Apply**, and then follow the instructions. You can only use a trial license on a server once.

2.1.6.2 Activating License



The following images of the page might slightly differ from the actual pages.

2.1.6.2.1 Online Activation

Prerequisites

- You have received your license. If not, see "2.1.6.1 Applying for a License".
A license is used to confirm the features and number of channels you purchased. To get a formal license, contact our sales personnel. To apply for a trial license, visit our website and find DSS Pro, and then follow the application instructions.
- The platform server can access the Internet.
- To activate hot standby, you need to deploy hot standby first. For details, see the *DSSReplicatorPlus3.0 Configuration Guide*. If you have any questions, contact technical support.

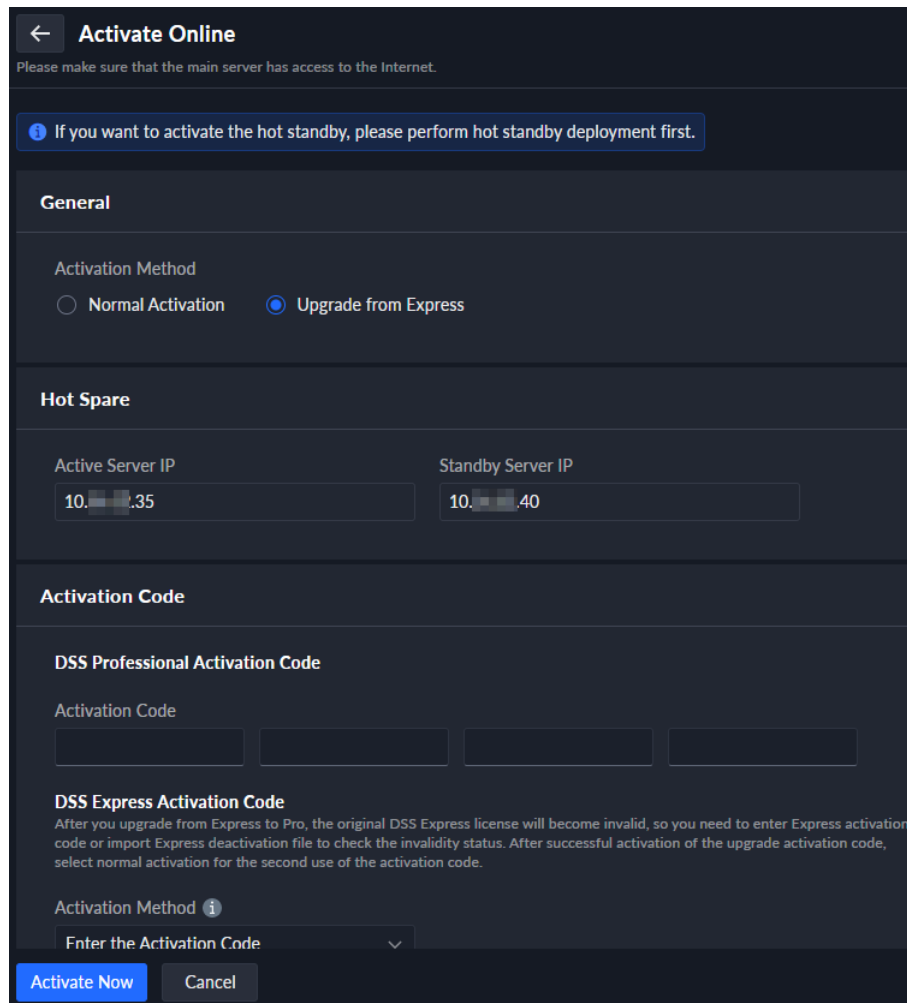
Background Information

- When hot standby is activated, the hardware information of the active and standby servers is obtained at the same time. You do not need to activate the servers separately, which simplifies the activation operation.
- When the active server is activated, the standby server obtains short-term license from the active server every 30 minutes, so that the standby server is always activated, as long as the servers are always connected; if the servers are disconnected, or the hot standby is uninstalled or stopped, the active server can be used normally, but the standby server will not be able to short-term license regularly. In this case, the standby server will expire within the specified time of the last license.
- If the hot standby is uninstalled, the active and standby servers can be activated and used separately.

Procedure

- Step 1 On the **Home** page, click , and then in **System Config**, select **License**.
- Step 2 Click **Activate License**, Select **Online Activate License**, then click **OK**.
- Step 3 Select an activation method. Select **Normal Active** to complete the process. If you upgraded the system from Express to DSS Pro, and DSS Express has a paid license, then select **Upgrade from Express** instead.

Figure 2-11 Select a method



Step 4 Enter your new **Activation Code**.

1. Enter the DSS Professional activation code that you received.
2. (Optional) If you select **Upgrade from Express**, enter the original Express activation code or import the deactivation file.
 - Enter the original activation code: Select **Enter Activation Code**, and then enter the original activation code.
 - Import the deactivation file: Select **Import DSS Express Deactivation Code**, click , and then select the deactivation file.

Step 5 Click **Activate Now**.

Step 6 On the **License** page, view your license details.

2.1.6.2.2 Offline Activation

Background Information

- When hot standby is activated, the hardware information of the active and standby servers is obtained at the same time. You do not need to activate the servers separately, which simplifies the activation operation.
- When the active server is activated, the standby server obtains short-term license from the active server every 30 minutes, so that the standby server is always activated, as long as the servers are always connected; if the servers are disconnected, or the hot standby is uninstalled

or stopped, the active server can be used normally, but the standby server will not be able to short-term license regularly. In this case, the standby server will expire within the specified time of the last license.

- If the hot standby is uninstalled, the active and standby servers can be activated and used separately.

Prerequisites

- You have received your license. If not, see "2.1.6.1 Applying for a License".

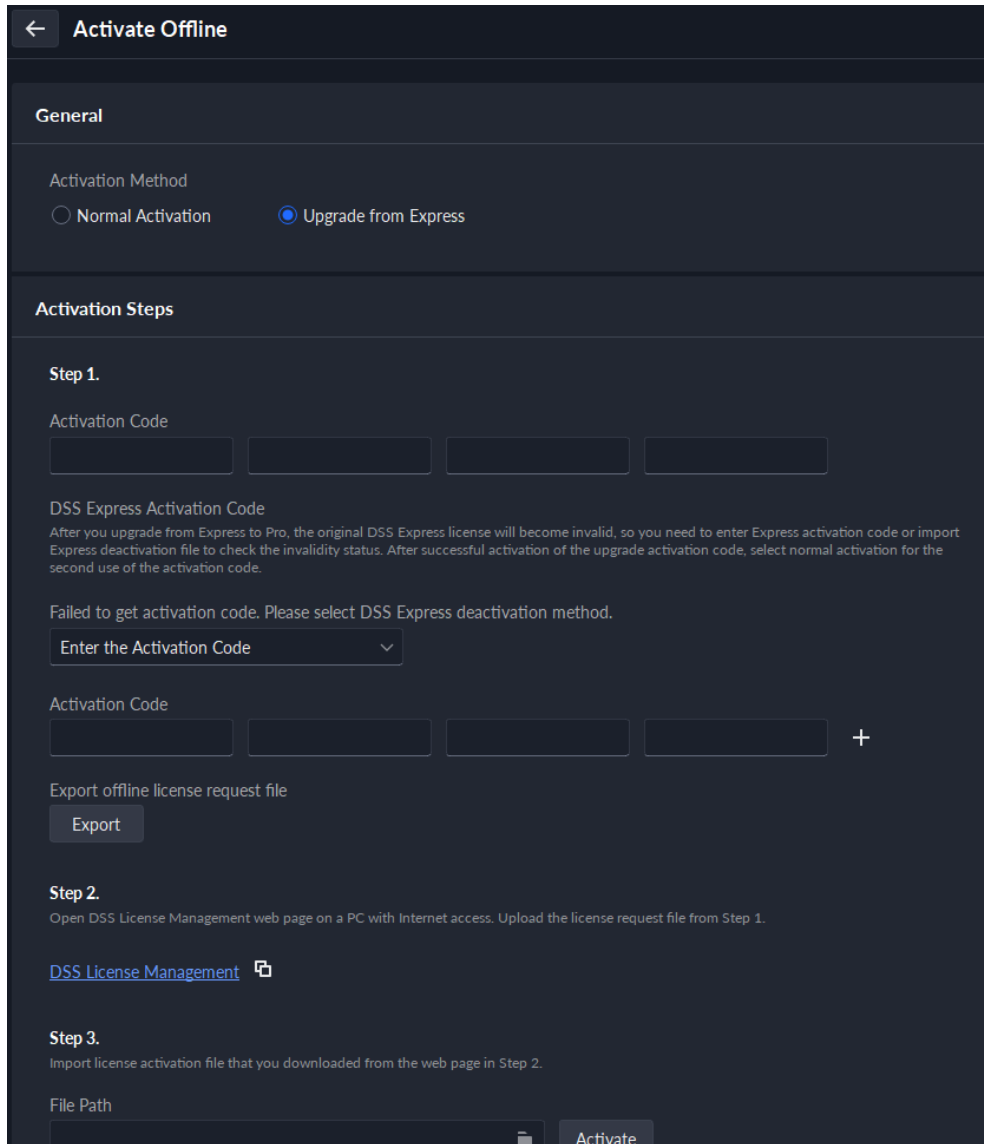
A license is used to confirm the features and number of channels you purchased. To get a formal license, contact our sales personnel. To apply for a trial license, visit our website and find DSS Pro, and then follow the application instructions.

- To activate hot standby, you need to deploy hot standby first. For details, see the *DSSReplicatorPlus3.0 Configuration Guide*. If you have any questions, contact technical support.

Procedure

- Step 1 On the **Home** page, click , and then in **System Config**, select **License**.
- Step 2 Click **Offline Activate License**, select **Offline Activate License**, then click **OK**.
- Step 3 Select an activation method. Select **Normal Active** to complete the process. If you upgraded the system from Express to DSS Pro, and Express has a paid license, then select **Upgrade from Express** instead.

Figure 2-12 Select a method



Step 4 Enter your new **Activation Code**.

1. Enter the DSS Professional activation code that you received.
2. (Optional) If you select **Upgrade from Express**, enter the original Express activation code or import the deactivation file.
 - Enter the original activation code: Select **Enter Activation Code**, and then enter the original activation code.
 - Import the deactivation file: Select **Import DSS Express Deactivation Code**, click , and then select the deactivation file.

Step 5 Click **Export** to export the license request file.

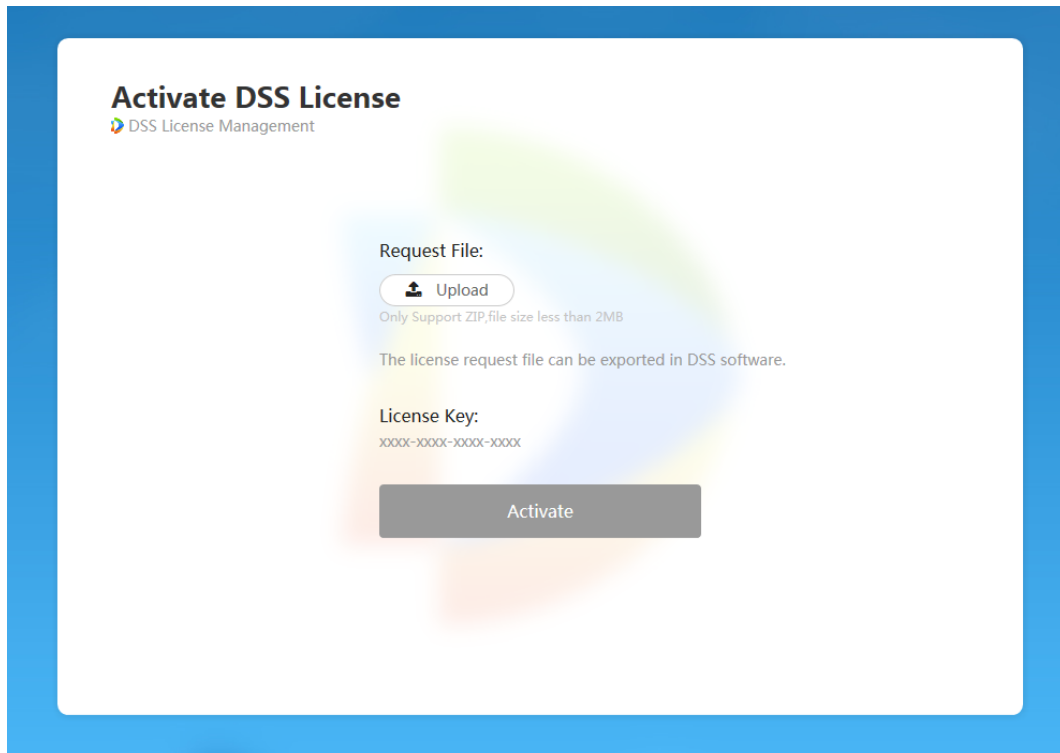
Step 6 Generate license file.

1. Move the request file to a computer with Internet access.
2. On that computer, open the system email that contains your license, and then click the attached web page address or **Click to go to DSS License Management** to go to the license management page.
3. Click **Activate License**.

4. Click **Upload**, select the license request file, and then when you are prompted **uploaded successfully**, click **Activate**.

The success page is displayed, where a download prompt is displayed asking you to save the license activation file.

Figure 2-13 Upload license request file



5. On the success page, click **Save** to save the file, and then move the file back to the computer where you exported the license request file.
6. On the **Offline Activate License** page, click **Import**, and then follow the on-screen instructions to import the license activation file.

Step 7 On the **License** page, view your license details.

2.2 Multiple Sites Deployment

If you have multiple platforms, you can connect one or more platforms to your current one, so that you can view the resources from them directly on your main platform, including viewing real-time videos from video channels, searching for real-time and historical events, and downloading recorded videos. The information of the platforms is linked to the user logged in to the main platform. When the user log in to the main platform again, the main platform will automatically connect to the other platforms. This function is only available to users assigned with the administrator role.

Prerequisites

The versions of different platforms must be the same.

Procedure

- Step 1 Log in to the DSS Client.
- Step 2 Click  on the upper-right corner, and then click **Add Site**.
- Step 3 Enter a name for the site, and the login information, and then click **OK**.

You can now view real-time videos of the devices, and real-time and historical events from the site.

Figure 2-14 Resources from the site shown in the monitoring center



Figure 2-15 Search for historical events from the site in Event Center

Sites

New Site

Time

06/20 00:00:00 – 06/20 23:59:59

Source Type

All

Export

Batch Process

No.	Alarm TL...	Site Name	Alarm Cate...	Alarm Type	Alarm Source	Priority	Remarks	Processed by	Alarm Status	Oper...
1	2024-06-20 ...	New Site	Device	Device Disc...	31.31.31.31	High	--	--	Not Processed	
2	2024-06-20 ...	New Site	Device	Device Disc...	31.31.31.31	High	--	--	Not Processed	
3	2024-06-20 ...	New Site	Access Cont...	Non-first Ca...	10.55.46.39-...	High	--	--	Not Processed	

2.3 Distributed Deployment

2.3.1 Installing Main Server

For details about how to install the main server, see the previous chapter or section.

After sub servers are deployed, log in to the main server, and then you can view the status of the sub servers.

2.3.2 Installing Sub Server

This section introduces how to install sub servers and register them to the main server.

Prerequisites

- You have received the DSS installer from our sales or technical support.
- You have prepared a server that meets the requirements mentioned in "2.1.1 Server Requirements", and the server IP address is set.

Procedure

Step 1 Double-click the DSS installer .



The name of the installer includes version number and date. Please confirm before installation.

Step 2 Click **agreement**, read through the agreement, and then accept it.

Step 3 Select the agreement check box, and then click **Next**.

Step 4 Select **Sub** for server type, and then click **Next**.

Step 5 Click **Browse**, and then select the installation path.

If the **Install** button is gray, check whether your installation path and space meet the requirements. The total space required is displayed on the page.



We recommend you do not install the platform into drive C because features such as face recognition require higher disk performance.

Step 6 Click **Install**.



The installation process takes about 5 to 10 minutes. Do not cut off the power or close the program.

Step 7 Click **Run** when the installation finishes.

Step 8 Select a network mode and the network card, and then click **Next Step**.



Dual NIC will be available if the server has two network cards. This is useful when you need to access devices on two different network segments.

Step 9 Configure the IP address and port of the main server.

Step 10 Click **Finish**.



After successfully installing a sub server, you need log in to the platform of main server to enable it so that it can work properly. For details, see "7.1.1 Distributed Deployment".

Related Operations

- To edit service ports, start or stop services, refresh services, view service status or more, see "2.1.4 Management Tool".
- To uninstall the platform, go to **Control Panel > Programs and Features**, and then locate DSS Server. Double-click it, and then uninstall it according to the on-screen instructions.

2.4 Hot Standby

For detailed steps, see *DSSReplicatorPlus3.0 Configuration Guide*. If you have any problems, contact technical support.

2.5 Cascade

Attach a DSS platform to another DSS platform, and then you can view videos of the child platform from the parent platform. You can create up to 3 cascade levels.

Prerequisites

Make sure that all the platforms on the system were already installed.

Background Information

- You only need to configure the child DSS information on the parent DSS information.
- DSS7016, DSS7116 and the paid version of DSS Express can be added as a child platform.

Procedure

Step 1 Log in to the parent DSS client. On the **Home** page, click  > **System Deployment**.

Step 2 Click .

Step 3 Click **Add**, and then configure parameters.

- **Organization**: Select an organization for the added platform, so that the resources of the platform will be attached to the organization of the current platform.

- IP Address, Port, Username and Password: Enter corresponding information of the added platform.

Step 4 Click **OK**.

2.6 N+M

On the main server, enable the sub server, and then create the sub-standby relationship.

Prerequisites

See "2.1 Standalone Deployment" and "2.3 Distributed Deployment" to deploy the servers you need.

Procedure

Step 1 Log in to the parent DSS client. On the **Home** page, click  > **System Deployment**.

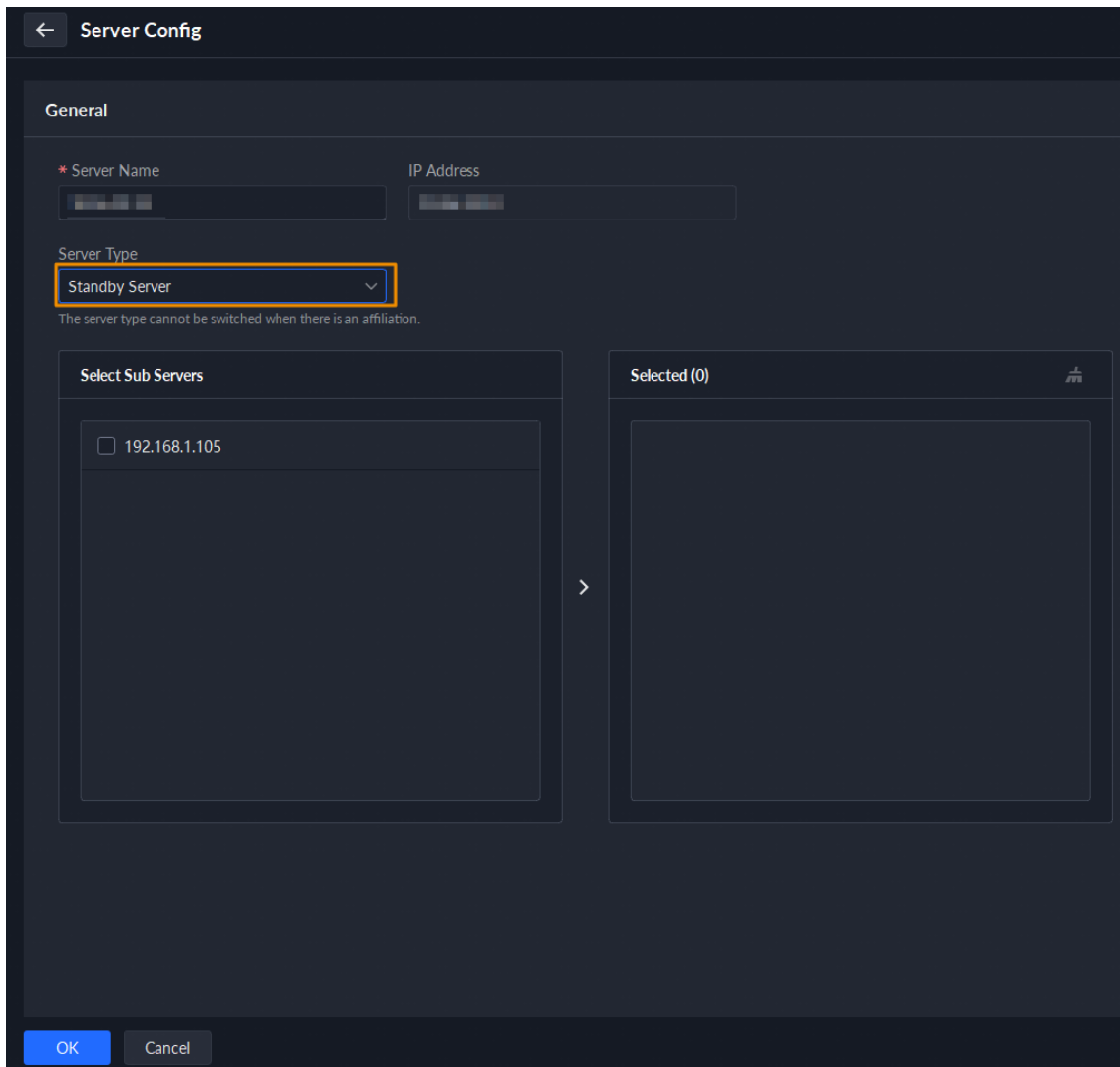
Step 2 Click .

Step 3 Click  to enable the sub servers.

Step 4 Configure a standby server.

1. Click  of a sub server.
2. Select **Standby Server** for **Server Type**, and then click **OK**.

Figure 2-16 Configure a standby server



← Server Config

General

* Server Name IP Address

Server Type
Standby Server

The server type cannot be switched when there is an affiliation.

Select Sub Servers

☐ 192.168.1.105

Selected (0)

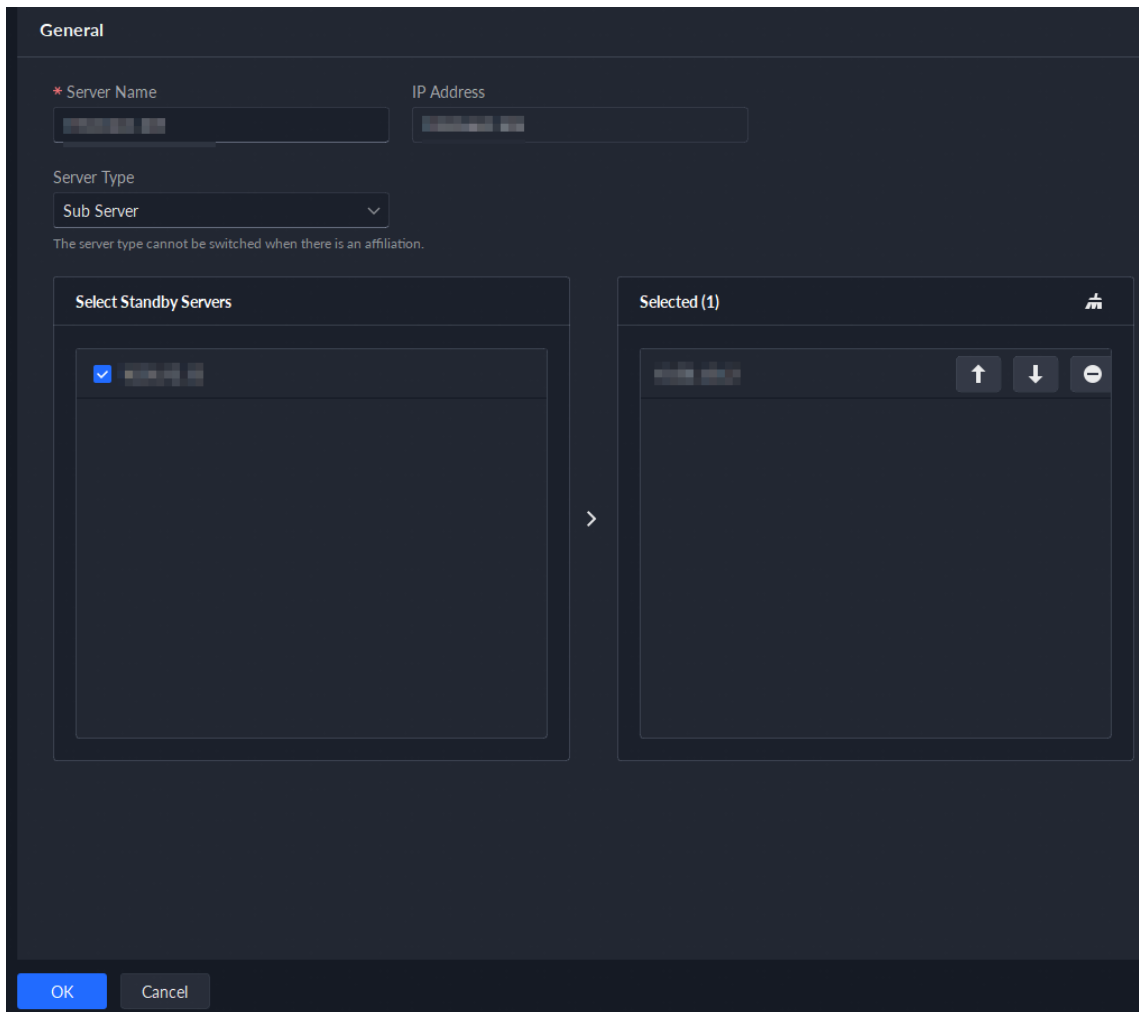
OK Cancel

Step 5 Configure the sub-standby relationship in either of the following ways.

- Go to the **Server Configuration** page of the sub server to select a standby server.

- Click  of a sub server.
- On the **Select Standby Server(s)** section, select one or more standby servers.

Figure 2-17 Select a standby server



General

* Server Name IP Address

Server Type
Sub Server

The server type cannot be switched when there is an affiliation.

Select Standby Servers

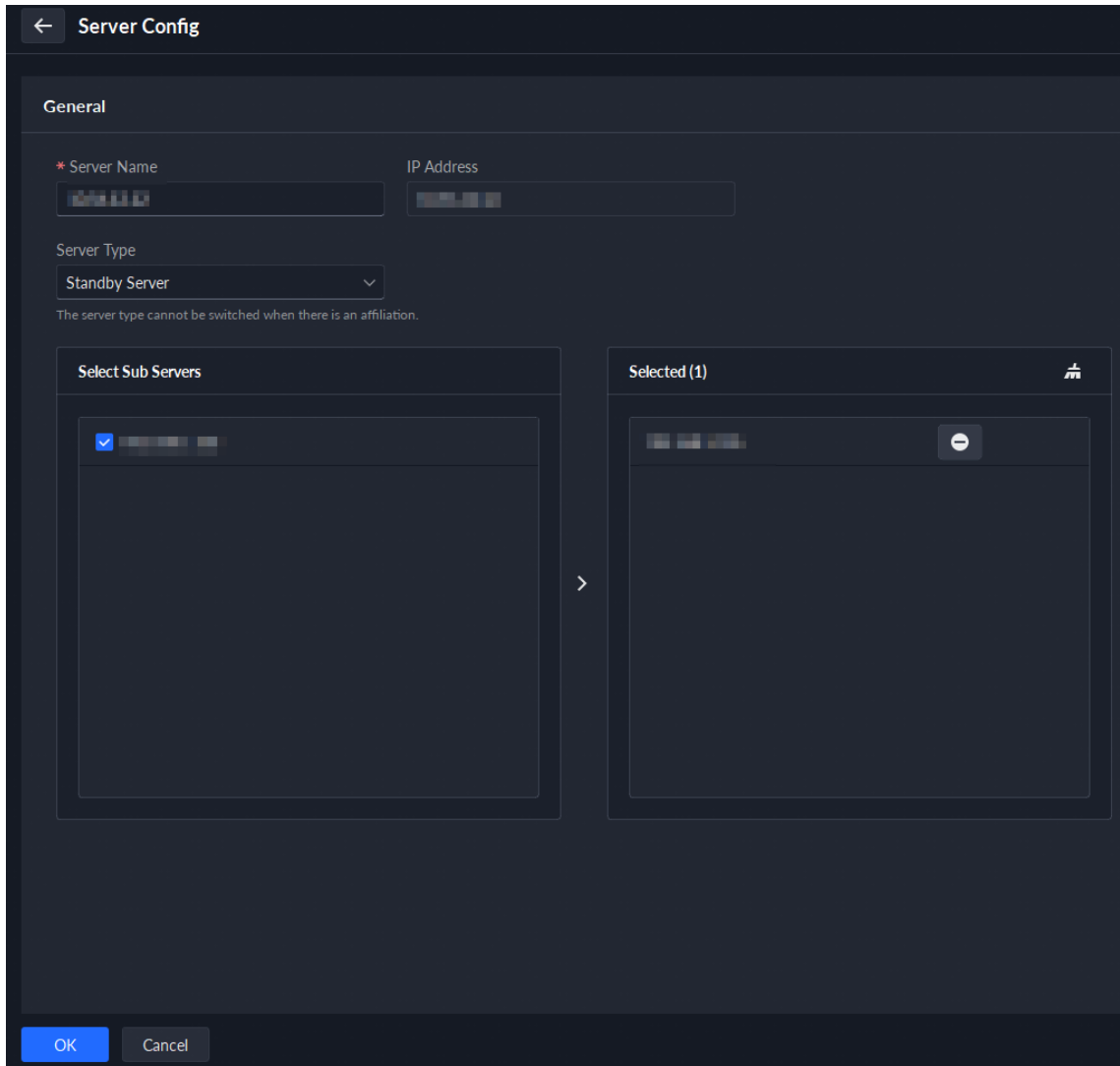
☒

Selected (1)

OK Cancel

3. Click **OK**.
- Go to the **Server Configuration** page of the standby server to select a sub server.
 1. Click  of a standby server.
 2. On the **Select Sub Server(s)** section, select one or more sub servers.

Figure 2-18 Select a sub server



3. Click **OK**.

2.7 Configuring LAN or WAN

2.7.1 Configuring Router

For the list of the ports that need to be mapped, see "Appendix 1 Service Module Introduction".



Make sure that the WAN ports are consistent with LAN ports.

2.7.2 Mapping IP or Domain Name

If the platform is deployed in a local network, you can map the IP address of the server to a fixed WAN IP or a domain name, and then log in to the server using the WAN IP or domain name.

The page might vary between the main server and the sub server. This section uses the main server page as an example.

Procedure

- Step 1 Log in to DSS server, and then double-click .
- Step 2 Click the  on the upper-right corner, and then select **Network**.
- Step 3 Enable WAN mode, enter a WAN IP address or a domain name, and then click **OK**.



If you want to use a domain name, you need to make corresponding configurations on the domain name server.

- Step 4 Click **OK**, and then the services will restart.

2.8 Virtualization Deployment

We usually apply virtualization deployment to better utilize hardware resources. In virtualization deployment, physical servers usually do not load virtual servers with all their allocated resources, and do not load virtual servers and the resources they need at the same time. However, the DSS platform frequently acquires the video streams from cameras for live view and storage, which puts high pressure on the CPU, memory, network, and storage. The benefits of virtualization deployment disappear when the DSS platform is running on a virtual server. Therefore, we do not recommend that you deploy the DSS platform on a virtual server. We recommend that you install an operating system on a physical server and directly deploy the DSS platform on the server to achieve optimal and reliable performance.

If you have to deploy the DSS server on a virtual server, pay attention to the following content during deployment.

Operating System for Virtual Server

- VMware® ESXi™ 7.x
- Microsoft® Hyper-V with Windows Server 2019

PC Client

When the PC client is running on a virtual server, the biggest issue is that the PC client cannot use the GPU to decode videos. Therefore, we do not recommend installing and running the PC client on a virtual server.

DSS Server

- If the resources, such as CPU and memory, allocated to the virtual server are more than a physical server required to run the DSS server, there should not be a problem for the DSS server to run on the virtual server.
- If the resources, such as CPU and memory, allocated to the virtual server are just the same as a physical server required to run the DSS server, you must consider that certain resources will be used to run the virtualized environment.
- When multiple virtual servers and other applications are running on the same physical server, there might be performance issues. For a virtual server, it cannot make sure that certain resources will always be used by a process. If this can be addressed, performance issues can be minimized or avoided.

- The DSS server will continuously store videos and other data to disks. We recommend that the DSS server should exclusively use the disks allocated to it by the virtual server, so that the DSS server can use all of the disks' read and write capability.
- The DSS server will continuously occupy certain bandwidth to acquire video and audio streams. We recommend that the DSS server should exclusively use the network cards allocated to it by the virtual server, so that the DSS server can use all of the network cards' performance.
- We do not recommend using virtual servers to configure hot standby and N+M deployment.
- In virtualization deployment, the license might become invalid due to change of hardware information.

2.9 Installing Plugin

You can add more functions to the platform by installing plugins.

Prerequisites

- Download the installation package from the official website.
- Purchase a license that allows you to use the functions of the plugin.

Background Information

For environments other than standalone deployment, you must make sure that the plugin versions installed on all servers are the same. Otherwise, the main server will not be able to balance the workload to other servers. For example, if the main server installs plugin version A, and the sub server the plugin version B, only the plugin on the main server will work properly, and all data can only be processed on the main server. The main server cannot use the resources of the sub server.

Procedure

- Step 1 Complete standalone deployment. For details, see "2.1 Standalone Deployment".
- Step 2 Double-click the installation package of the plugin.
- Step 3 Click **the software license agreement**, and then read the agreement.
- Step 4 Select the check box to accept the agreement, and then click **Next**.
- Step 5 Click **Install**.



The plugin is installed to the same directory as the management tool by default. It cannot be changed.

Related Operations

- To uninstall the plugin, log in to the server, go to "..\DSS\DSS Server\Uninstall", double-click `uninst_energy.exe`, and then follow the on-screen instructions to uninstall the plugin. For the main server, you can choose to keep related data. But for sub servers, related data will be kept by default. You cannot choose to delete it.
- To update the plugin, directly install the new program.

3 Basic Configurations

Configure basic settings of the system functions before using them, including system activation, organization and device management, user creation, storage and recording planning, and event rules configuration.

3.1 Managing Resources

Manage system resources such as devices, users, and storage space. You can add organizations and devices, configure recording plans and retrieval plans, bind resources, and more.

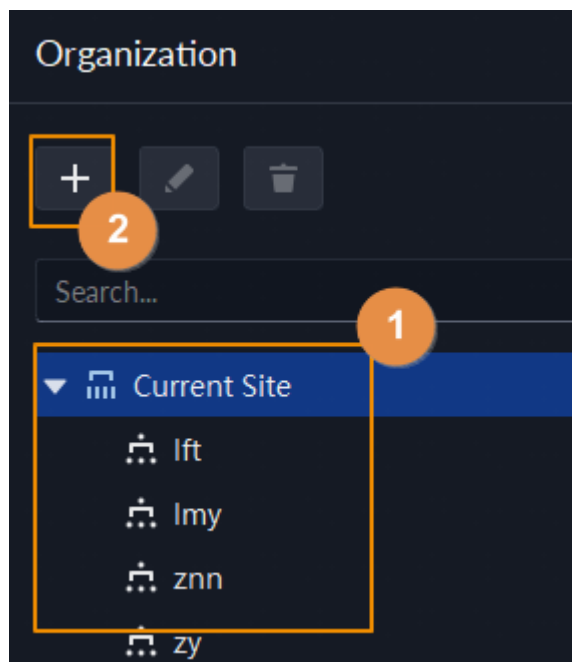
3.1.1 Adding Organization

Classify devices by logical organization for the ease of management. The default organization is **Root**. If the parent organization is not specified, newly added devices are attached to **Root**.

Procedure

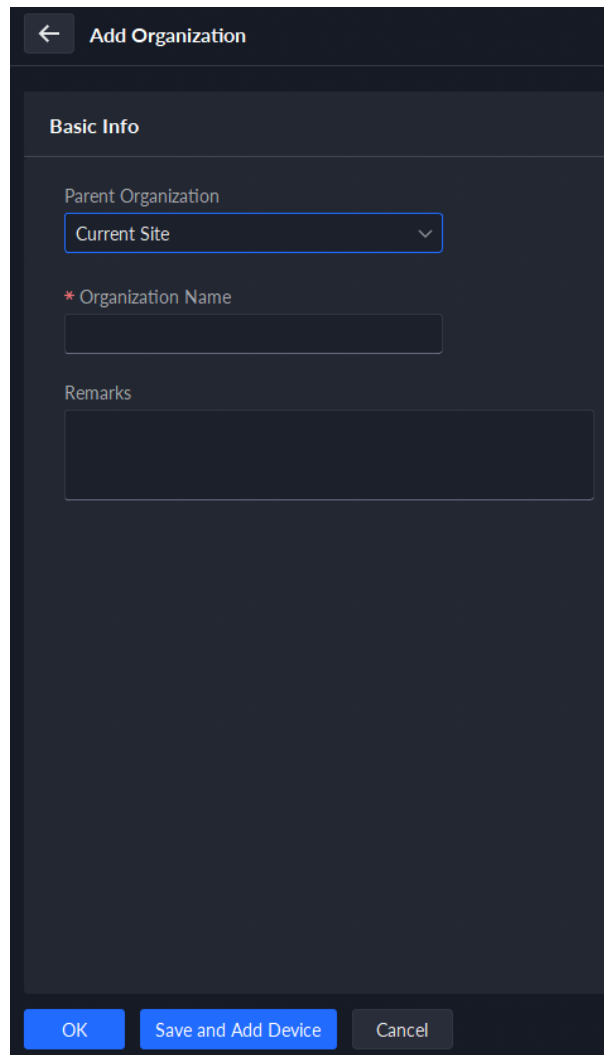
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Add an organization.
1. Select a parent organization.
 2. Click .

Figure 3-1 Add an organization



3. Enter the name of the organization, and then click **OK**.

Figure 3-2 Add an organization




You can also right-click the root organization, and then click **Add Organization** to add an organization.

Related Operations

- Change organization name
Right-click the organization, and then click **Rename**.
- Delete an organization
Organization with devices cannot be deleted.
Select the organization, click , or right-click an organization and select **Delete**.
- Change the organization of devices
Select one or more devices, and then click **Move To** to move them to another organization.

3.1.2 Managing Device

Add devices before you can use them for video monitoring. This section introduces how to add, initialize, and edit devices and how to change device IP address.

3.1.2.1 Searching for Online Devices

Search for devices on the same network with the platform before you can add them to the platform.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Click **Discover Device**.

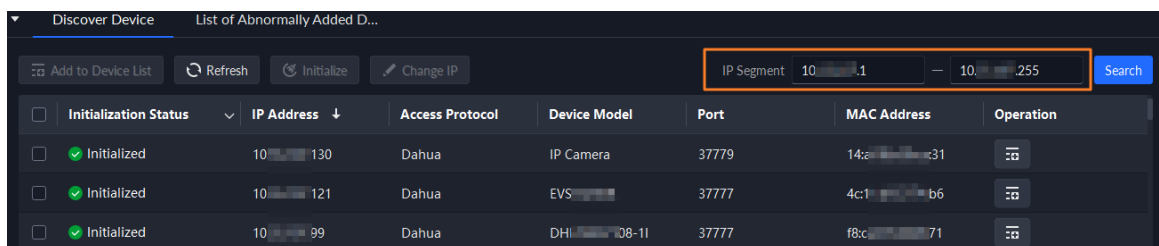


When using the platform for the first time, the platform displays the devices on the same network segment and across network segments discovered by multicast.

If not the first time, the platform displays the network segment that you configured last time and the search results by default. You can also set a new network segment for search.

Step 4 Specify **IP Segment**, and then click **Search**.

Figure 3-3 IP segment search



The devices have been added to the platform will not be displayed in the search results.

3.1.2.2 Initializing Devices

You need to initialize the uninitialized devices before you can add them to the platform.

Procedure

Step 1 Search for devices. For details, see "3.1.2.1 Searching for Online Devices".

Step 2 Select an uninitialized device, and then click **Initialize**.



- You can select multiple devices to initialize them in batches. Make sure that the selected devices have the same username, password and email information. The information of these devices will be the same after initialization, such as password and email address.
- Click **Initialization Status** to quickly display devices that are initialized or not.

Step 3 Enter the password, and then click **Password Security**.

Step 4 Enter the email address, and then click **Change IP**.



The email is used to receive security code for resetting password.

Step 5 Enter the IP address, and then click **OK**.

When setting IP addresses in batches, the IP addresses increase in an ascending order.

3.1.2.3 Changing Device IP Address

You can change IP addresses of the devices that have not been added to the platform.

Procedure

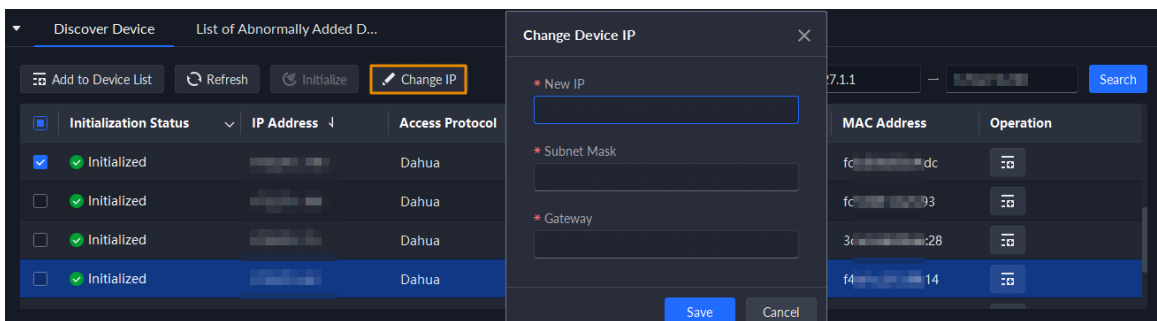
Step 1 Search for devices. For details, see "3.1.2.1 Searching for Online Devices".

Step 2 Select a device, and then click **Change IP**.



For devices that have the same username and password, you can select and modify their IP addresses in batches.

Figure 3-4 Change IP address



Step 3 Enter **New IP**, **Subnet Mask** and **Gateway**, and then click **Save**.

When setting IP addresses in batches, the IP addresses increase in sequence.

Step 4 Enter the username and password used to log in to the devices, and then click **OK**.

3.1.2.4 Adding Devices

You can add different types of devices, such as encoder, decoder, ANPR device, access control, displays, emergency assistance device, alarm box, radar device, and video intercom. This section takes adding an encoder as an example. The configuration pages shown here might be different from the ones you see for other types of devices.



When you add devices by using automatic registration, IP segment, or importing, some devices will fail to be added if they exceed the number of devices or channels allowed to be added to the platform. These devices will be displayed in **Devices without License**.

3.1.2.4.1 Adding Devices One by One

There are multiple ways you can add devices to the platform, including using domain names, serial numbers, IP addresses, IP segments, and automatic registration.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Click **Add**.

Step 4 Enter device login information, and then click **Next Step**.

Select a mode to add the device.

- **IP Address** : We recommend selecting this option when you know the IP address of the device.



Only **Encoder** devices support IPv6. If you want to add devices to the platform through IPv6 addresses, you must first configure an IPv6 address for the platform. Contact technical support for help.

- **IP segment** : Add multiple devices in the same segment. We recommend selecting this option when the login username and password of the multiple devices in the same segment are the same.
- **Domain Name** : We recommend selecting this option when the IP address of the device changes frequently and a domain name is configured for the device.
- **Auto Registration** : We recommend this method when the IP address of a device might change. The ID of auto register has to be in accordance with the registered ID configured on the device you want to add. The port number must be the same on the platform and on the device. The auto register port is 9500 on the platform by default. To change the auto register port number, open the configuration tool to change the port number of ARS service.



- ◇ After a device is added through auto registration, hover the mouse over its IP address on the device list, and then you can see its local IP address and the IP address it uses to connect to the platform.
- ◇ Sleep function is supported for IPCs that use 4G mobile network to communicate and are solar-powered only when they are added to the platform through automatic registration.

- **P2P** : Add devices under a P2P account to the platform. The platform must be able to access the P2P server. There is no need to apply for the dynamic domain name of the device, perform port mapping or deploy a transit server when using it.



- ◇ Before adding devices through P2P, you need to enable the P2P function from **System Parameters > Device Adding Config**.
- ◇ P2P mode cannot be used to configure central recording plans when adding devices. If you need to configure central recording plans, it is recommended to select a different method.

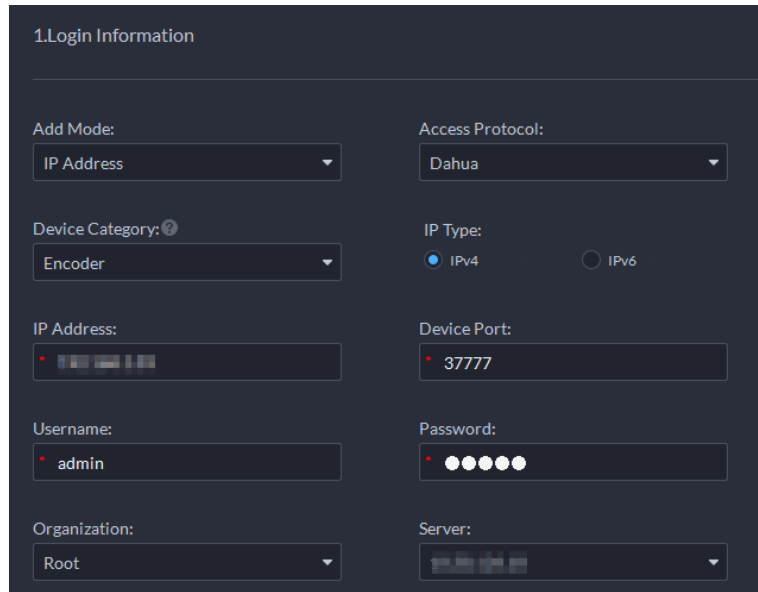
- **RTSP Address** : When a third-party device does not support standard protocol access, but supports RTSP, this mode can be considered.

- ◇ **Device Category** only supports **Encoder** and the **Access Protocol** only supports **RTSP**.
- ◇ Only live view and playback of central recordings are supported if devices are added through this way. For details of configuring central storage plan, see "3.1.4.1 Adding Recording Plan One by One".



- The parameters vary with the selected protocols.
- When you set **Device Category** to **Video Wall Control**, and you are using the **Dual NIC Mode**, **WAN Mode**, or both modes, you need to select the network in which the device works according to the actual situation.

Figure 3-5 Add an encoder



1.Login Information

Add Mode: IP Address

Access Protocol: Dahua

Device Category: Encoder

IP Type: IPv4 (selected) IPv6

IP Address: [Redacted]

Device Port: 3777

Username: admin

Password: [Redacted]

Organization: Root

Server: [Redacted]

Step 5 Enter the device information.

When setting **Device Category** to **Alarm Controller**, you need to set the number of subsystem and zone.

Step 6 Click **OK**.

- To add more devices, click **Continue to add**.
- To go to the web manager of a device, click .

Related Operations

☒ Include Sub Organization

: It is select by default. If selected, the system will display the devices of sub organization. If not selected, the system will only display the devices of the current organization.

3.1.2.4.2 Adding Devices through Searching

Devices on the same network with the platform server can be added using the automatic search function.

Procedure

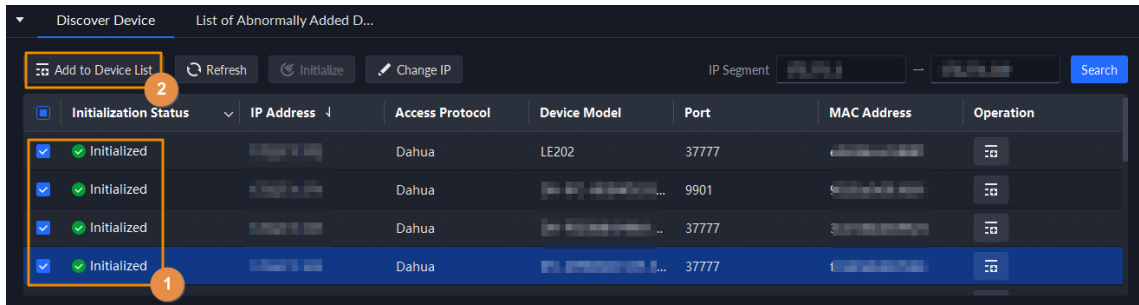
Step 1 Search for devices.

Step 2 Select a device, and then click **Add to Device List** or .



If devices have the same username and password, you can select and add them in batches.

Figure 3-6 Add in batches



Step 3 Select the server and organization, enter username and password, and then click **OK**.

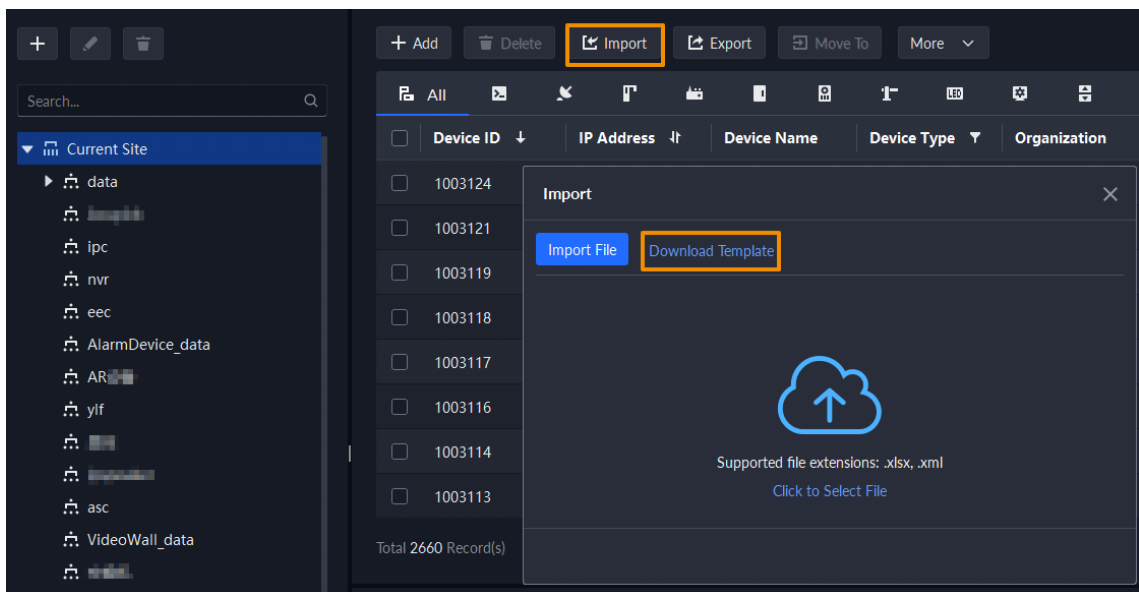
3.1.2.4.3 Importing Devices

Enter the device information in the template, and then you can add devices in batches.

Prerequisites

You have downloaded the template, and then enter device information in the template.

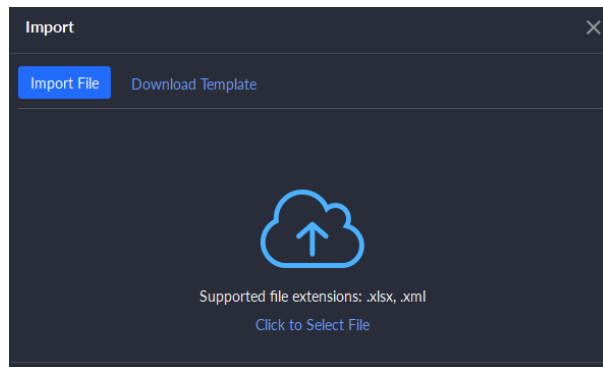
Figure 3-7 Download template



Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Click **Import**.

Figure 3-8 Import devices



Step 4 Click **Import File**, and then select the completed template.

Step 5 Click **OK**.

3.1.2.5 Editing Devices

Edit the information of devices.

3.1.2.5.1 Changing IP Address

For the devices that have been added to the platform, and their IP addresses have been changed, you can edit their IP addresses directly on the platform so that they can connect to the platform normally.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click **Device Config**.

Step 3 Click  of a device.

Step 4 Edit the IP address, and then click **OK**.

3.1.2.5.2 Modifying Device Information

Procedure

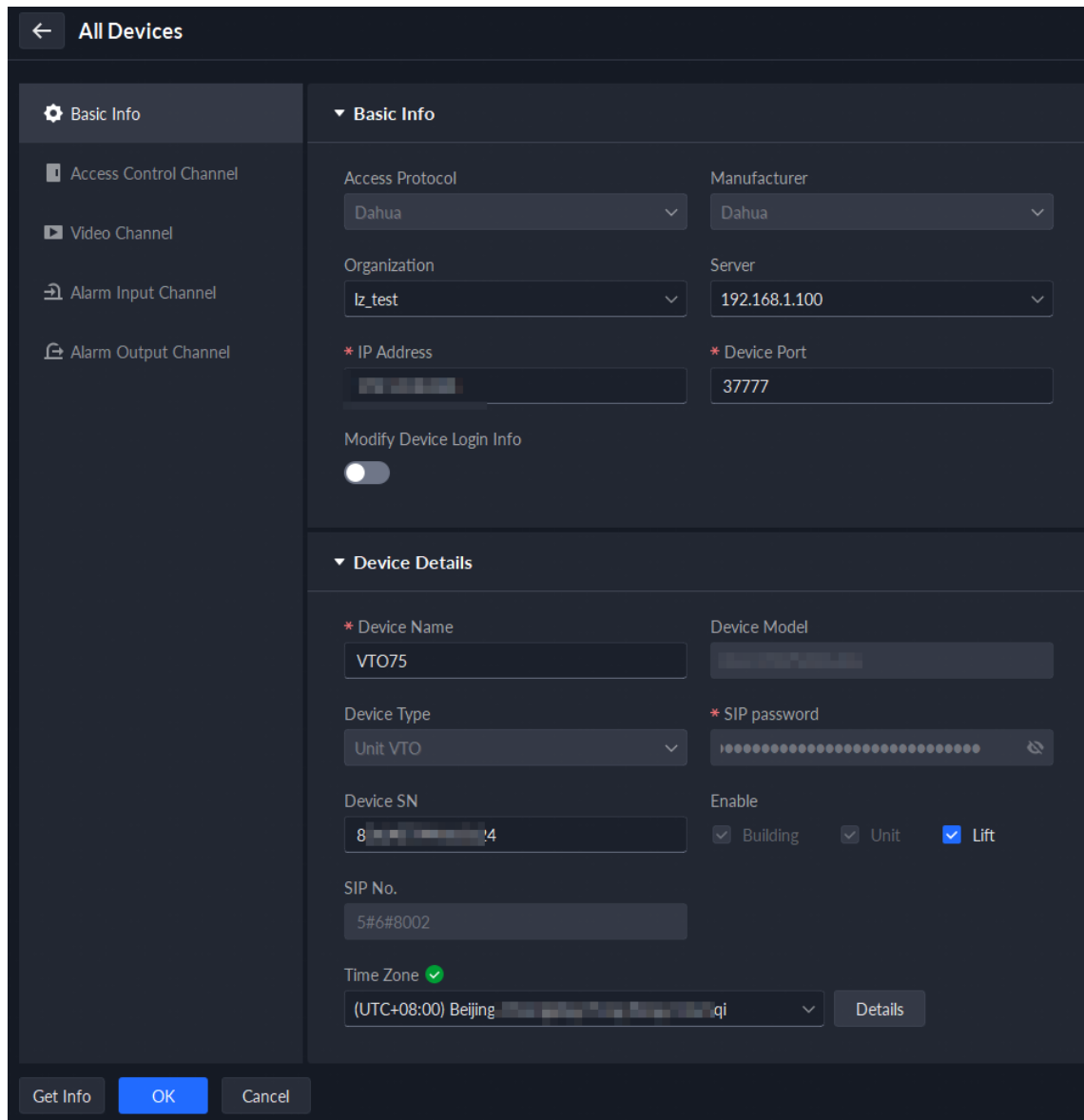
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Click  of a device, and then edit device information.

Click **Get Info** and the system will synchronize device information.

Figure 3-9 Basic information



The screenshot shows the 'All Devices' configuration page. On the left is a sidebar with navigation options: 'Basic Info' (selected), 'Access Control Channel', 'Video Channel', 'Alarm Input Channel', and 'Alarm Output Channel'. The main area is divided into two sections: 'Basic Info' and 'Device Details'.

Basic Info Section:

- Access Protocol:** Dropdown menu set to 'Dahua'.
- Manufacturer:** Dropdown menu set to 'Dahua'.
- Organization:** Dropdown menu set to 'lz_test'.
- Server:** Dropdown menu set to '192.168.1.100'.
- * IP Address:** Text input field with a blurred value.
- * Device Port:** Text input field set to '37777'.
- Modify Device Login Info:** Toggle switch, currently turned off.

Device Details Section:

- * Device Name:** Text input field set to 'VTO75'.
- Device Model:** Text input field with a blurred value.
- Device Type:** Dropdown menu set to 'Unit VTO'.
- * SIP password:** Password input field with a blurred value and a toggle for visibility.
- Device SN:** Text input field set to '8...4'.
- Enable:** Checkboxes for 'Building' (checked), 'Unit' (checked), and 'Lift' (checked).
- SIP No.:** Text input field set to '5#6#8002'.
- Time Zone:** Dropdown menu set to '(UTC+08:00) Beijing' with a green checkmark icon.
- Details:** Button to view more information.

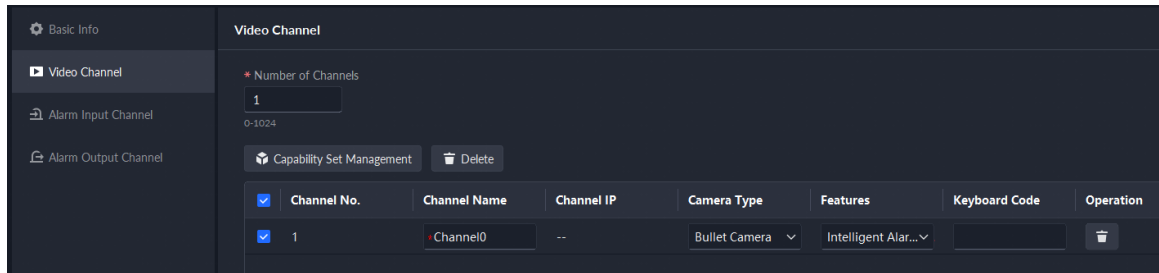
At the bottom of the page are three buttons: 'Get Info', 'OK', and 'Cancel'.

Step 4 Click **Video Channel**, and then configure the channel information, such as the channel name and channel features.



- The features that you can set for channels vary with the types of devices.
- If the device is added through the ONVIF protocol, you can configure the stream type of its video channels.
- Select multiple channels, and then click **Capability Set Management** to configure the video channel capability in batches.
- Select multiple channels, and then click **Delete** to delete channels in batches.

Figure 3-10 Modify the information of video channel



Step 5 Click the **Alarm Input Channel** tab, and then configure number, names, and alarm types of the alarm input channels.



Skip the step when the device does not support alarm input.

- Alarm type includes external alarm, Infrared detect, zone disarm, PIR, gas sensor, smoke sensor, glass sensor, emergency button, stolen alarm, perimeter and preventer move.
- Alarm type supports custom. Select **Customize Alarm Type** in the **Alarm Type** drop-down list. Click **Add** to add new alarm type. It supports up to 30 custom alarm types.

Step 6 Click the **Alarm Output Channel** tab and then edit the names and view the number of alarm output channels.

Step 7 Click the **POS Channel**, and then edit the number and names of the POS channels.



This tab will only appear if the device has POS channels.

Step 8 Click the **Audio and Light Channel** tab, and then edit the number and names of the audio and light channels.



This tab will only appear if the device has audio and light channels.

Step 9 Click **OK**.

3.1.2.5.3 Getting Device Information in Batches

This function allows you to get information from device in batches to reduce repeated operations. For example, if the platform fails to get information from certain devices after you add them in batches, you can use this function to get the information from them at the same time.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device** > **Add Device**.

Step 2 Select an organization, and then the devices in this organization and its sub organizations will be displayed on the right.

Step 3 Select multiple devices.

Step 4 Select **More** > **Get Info**, then click **OK**.

- **Get All Info** : Get all the information from devices to overwrite the existing device information.
- **Only Get Info on Newly Added Channels** : Get the information on the newly added channels from devices and keep the existing device information.

Wait for the platform to finish the process.

Related Operations

If the platform still cannot get information from certain devices, click  to see the reasons.

3.1.2.5.4 Configuring Channel Features in Batches

Configure the channel features in batches so that devices can work normally.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2 On the top of the page, select **More** > **Capability Set Management**.
- Step 3 In the **Capability Set Type** drop-down list, select a type, and then the platform will only display devices and channels that are configured with that type of capability set.
- Step 4 Select the channels you want to configure.
- Step 5 Click the area below the **Features** column, and then select one or more features.

Figure 3-11 Select capability sets

☐	Channel Name	Device Name	Organization	Features
☐	Channel0	n5Mpy	mpy	Intelligent Alarm,Electric Focus,IR Tem... ☒ Intelligent Alarm ☒ Electric Focus

- Step 6 Complete configuration.
 - If configuration is complete, click **Complete** to save the settings and exit the page.
 - If you want to configure more channels, click **Save** to save your current settings, and then continue your configuration. When it is complete, click **Complete** to save the settings and exit the page.

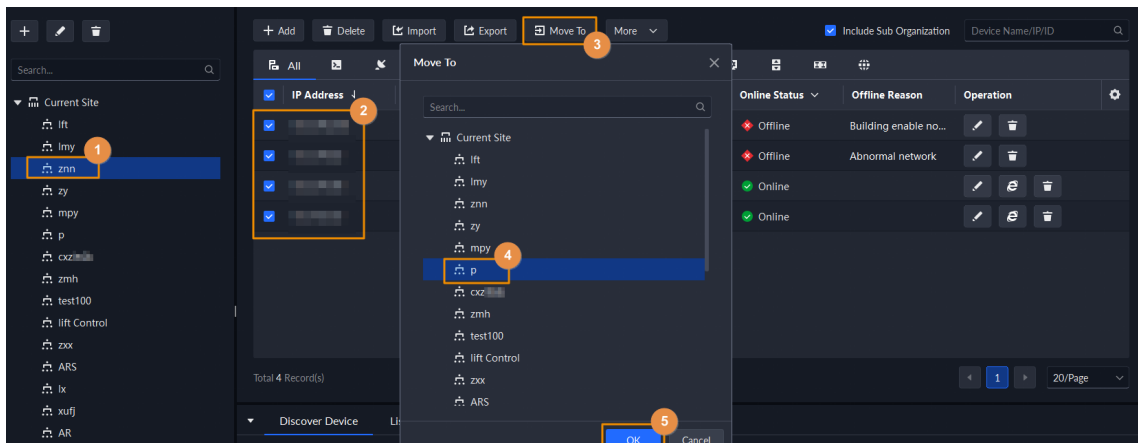
3.1.2.5.5 Modifying Device Organization

You can move a device from an organization node to another one.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2 Click .
- Step 3 Select a device to be moved, click **Move To**, select the target organization, and then click **OK**.

Figure 3-12 Move a device



3.1.2.5.6 Changing Device Password

You can change device usernames and passwords in batches.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

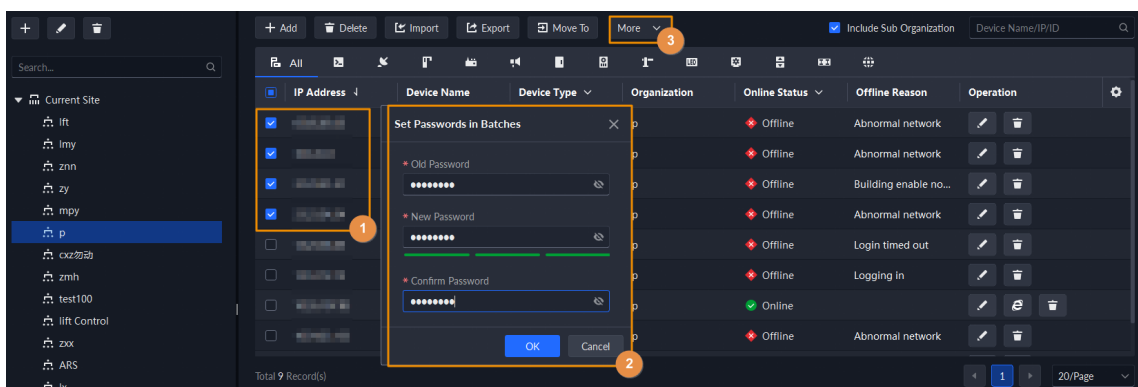
Step 2 Click .

Step 3 Select a device, click **More**, and then click **Change Password**.



You can select multiple devices and change their passwords at the same time.

Figure 3-13 Change device password



Step 4 Enter the old and new passwords, and then click **OK**.

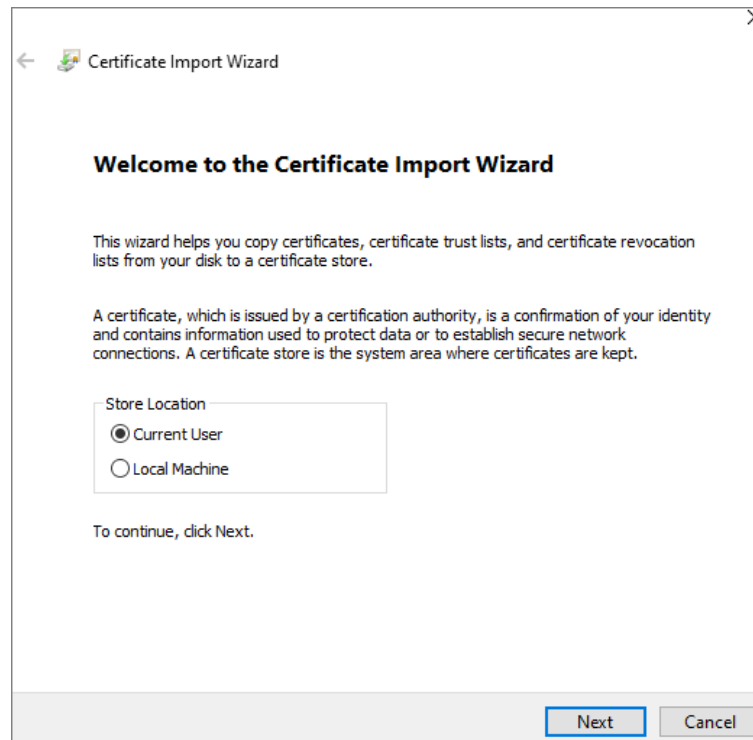
3.1.2.6 Logging in to Device Webpage

After a device is added to the platform, you can click  to go to the webpage of a device.

If you cannot go to the webpages of devices normally, you can follow the steps below to complete related settings. For procedures on the device webpage, see the user manual of the device.

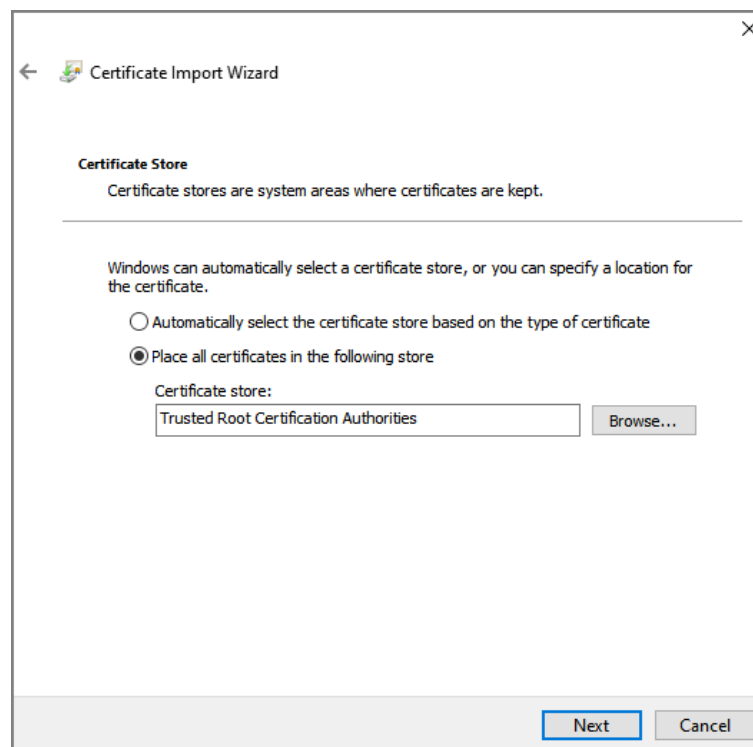
1. Log in to the webpage of the device, and then download the trusted CA root certificate.
2. Double-click the certificate, and then click **Install Certificate**.
3. Select **Current User**, and then click **Next**.

Figure 3-14 Certificate import wizard (1)



4. Store the certificate to **Trusted Root Certification Authorities** , and then click **Next**.

Figure 3-15 Certificate import wizard (2)



5. Click **Finish**.
6. On the webpage of the device, create a device certificate, and then apply it.



For the IP address in the certificate, you must enter the IP address of the computer that visits the webpage.

3.1.2.7 Exporting Devices

You can export the information of devices to your computer. This is useful when you need to switch or configure a new platform, you can quickly add them all by importing them. Only administrators are allowed to export the login passwords of devices.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** (Optional) Select only the devices that you need.
- Step 4** Click **Export**.
- Step 5** Enter the login password, encryption password, select whether to export the passwords of devices and the export range, and then click **OK**.



You can configure whether to verify the login password. For details, see "7.4.1 Configuring Security Parameters".

- The encryption password is used to protect the export file. It consists of 8–32 uppercase or lower case letters, numbers, or their combination. You need to enter it when using the export file.
- You can select **All** to export all the devices, or **Selected** to export the devices you selected.

- Step 6** Select a path on your PC, and then click **Save**.

3.1.2.8 Modifying Device Time Zone

Configure device time zone correctly. Otherwise you might fail to search for recorded video.

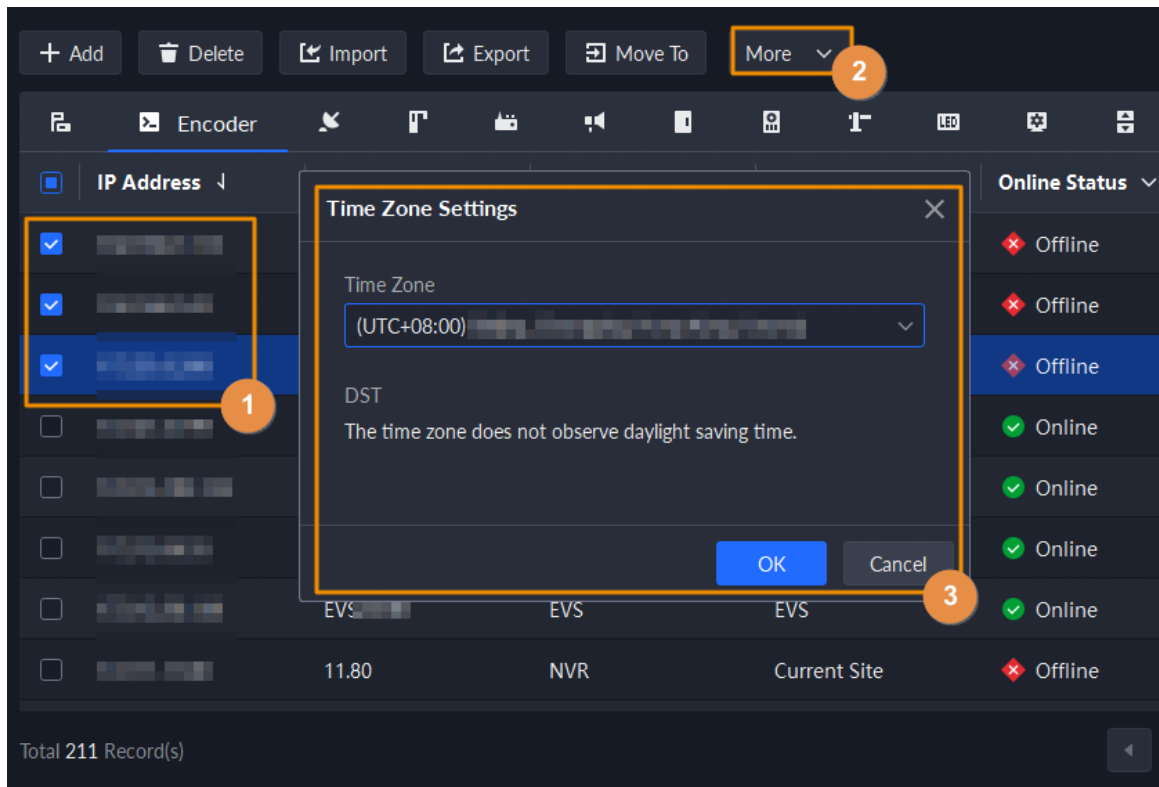


If a device is accessed through ONVIF and the ONVIF version is earlier than 18.12, the device DST cannot be edited on the platform. You can only edit it manually on the device.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Select a device, click **More**, and then click **Time Zone Settings**.

Figure 3-16 Modify device time zone



Step 4 Select a time zone.

Step 5 Click **OK**.

3.1.3 Binding Resources

You can bind different types of channels, such as an ANPR channel or door channel, to a video channel. You can view real-time videos of the bound channels in different functions, or linked them for certain actions in an event, such as recording a video.

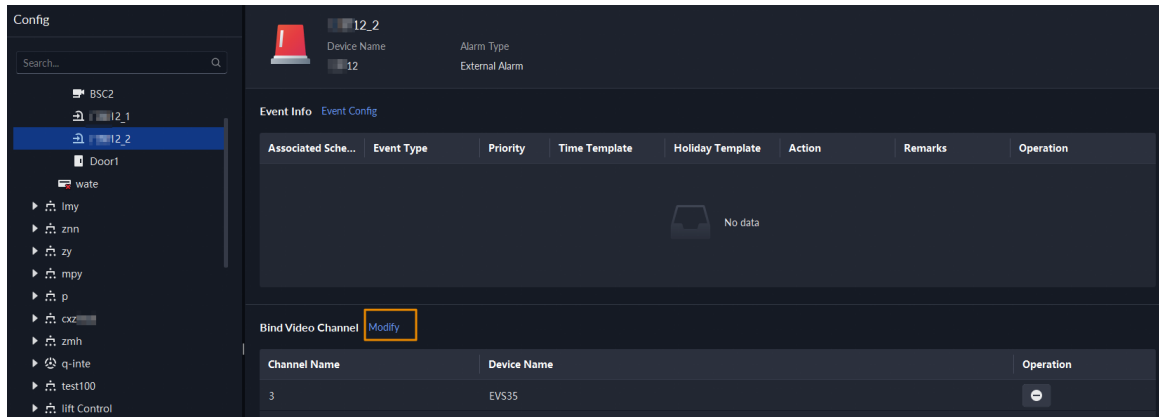
Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

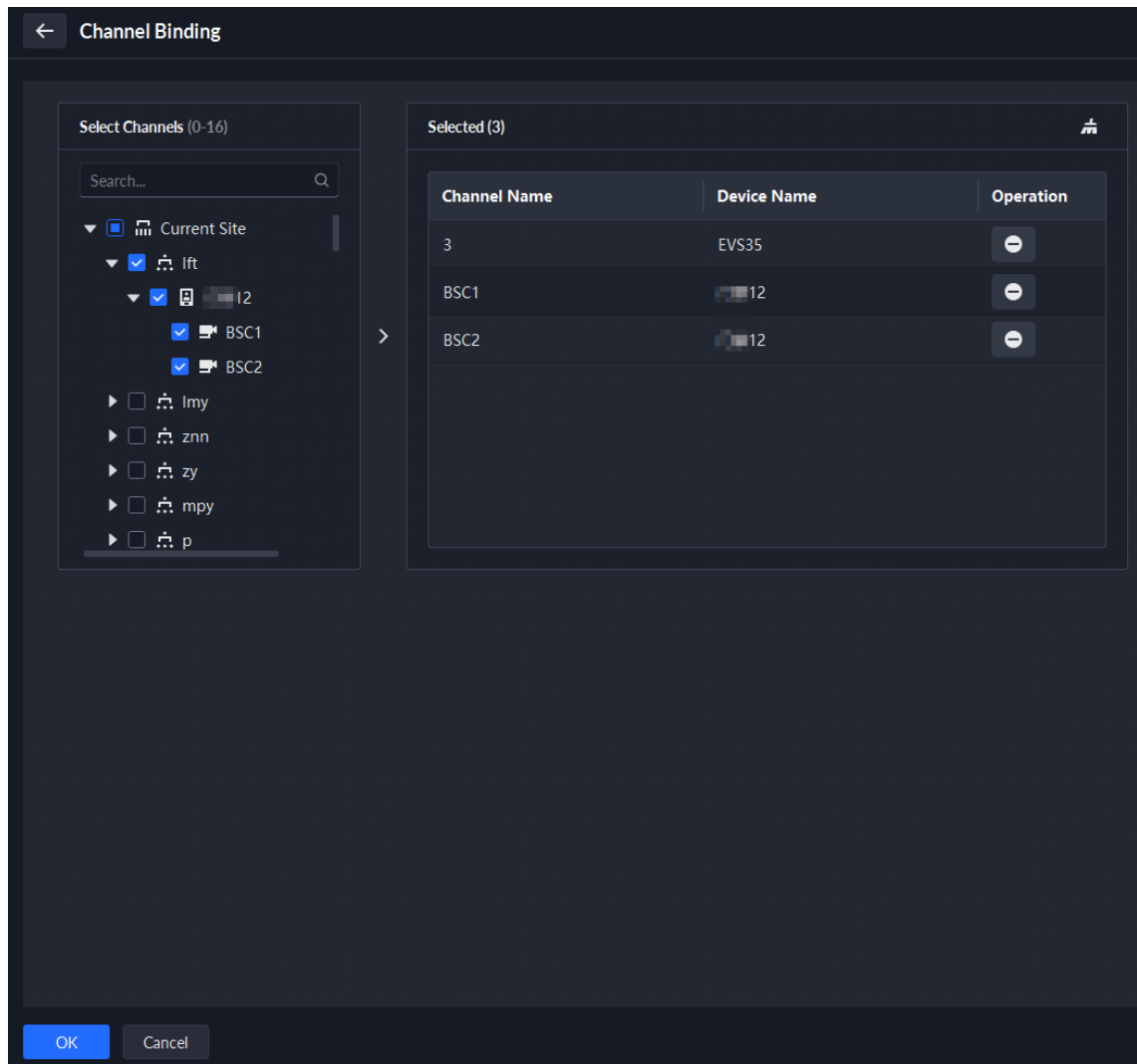
Step 3 Select a channel, and then click **Modify**.

Figure 3-17 Bind one or more channels



Step 4 Select one or more channels, and then click **OK**.

Figure 3-18 Select the channels you want to bind



Step 5 Click **OK**.

3.1.4 Adding Recording Plans

Configure recording plans for video channels so that they can record videos accordingly. You can configure 2 types of recording plans for a channel. One is general recording plan, and a device will continuously record videos during the defined period. The other is motion detection recording plan, and a device will only continuously record videos when motion is detected.

Prerequisites

Before adding a recording plan, you need to configure storage for the platform. For details, see "3.3 Configuring Storage".

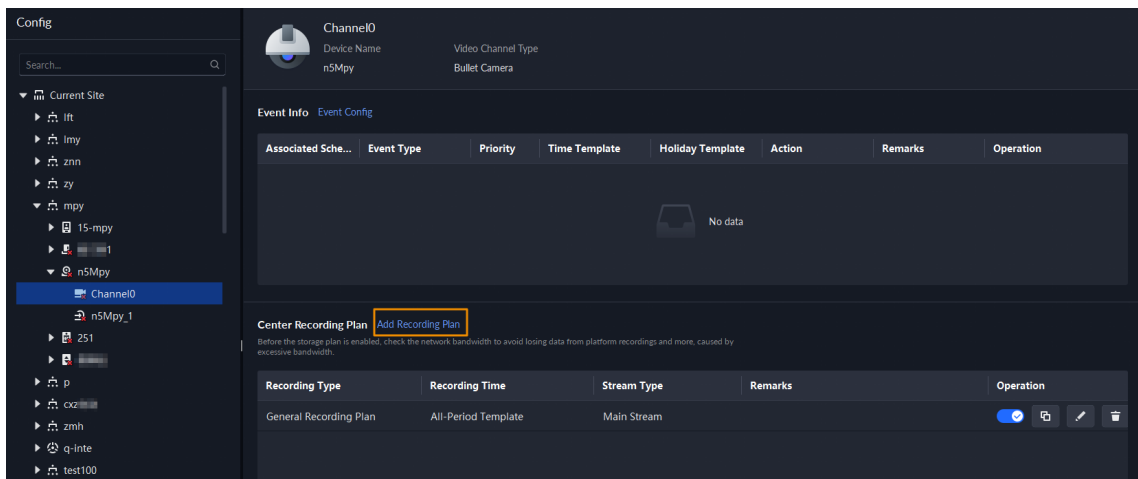
3.1.4.1 Adding Recording Plan One by One

Add a center recording plan or device recording plan for a channel, so that it can make general or motion detection videos within the defined period.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Select a channel, and then configure a recording plan.
 - Configure a center recording plan.
 1. Click **Add Recording Plan** next to **Center Recording Plan**.

Figure 3-19 Add a center recording plan (1)



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

Table 3-1 Parameter description

Parameter	Description
Enable	Turn on or off the recording plan.
Position	Videos will be stored on the server by default. It cannot be changed.

Parameter	Description
Recording Type	- General recording: The device will continuously record videos within the defined periods. - Motion detection recording: The device will continuously record videos within the defined periods on motion detections.
Stream Type	Select Main Stream , Sub Stream 1 or Sub Stream 2 . Videos recorded on the main stream will have the best quality, but they require more storage.
Remarks	Customizable description for the recording plan.
Recording Time	Select a default time template or click Create Time Template to add a new time template. See "3.1.6 Adding Time Template".

3. Click **OK**.

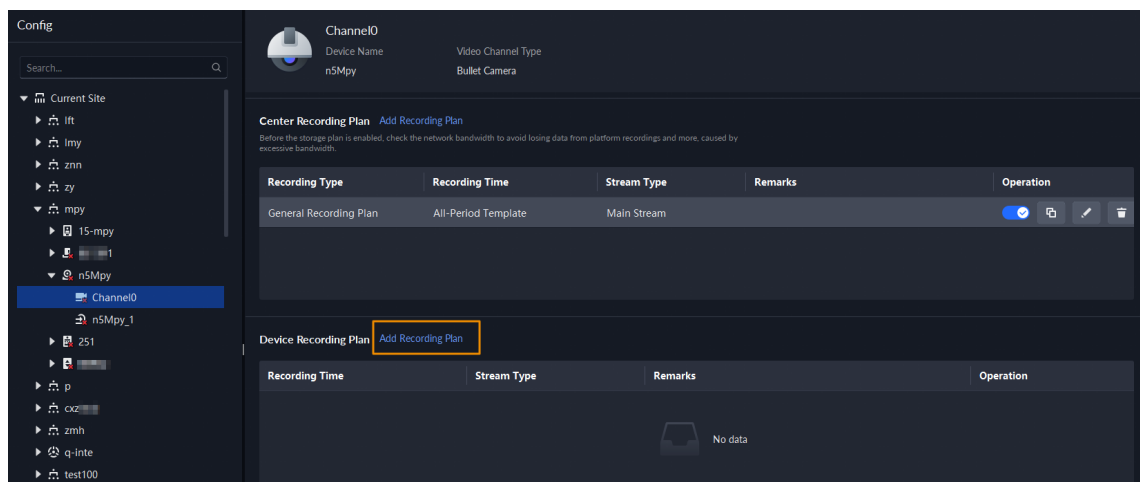
- Configure a device recording plan.



The platform can obtain and display the recording plan that has been configured on EVS of the latest versions. You can check if recording plan are obtained and displayed on the page to know if your EVS is of the latest version.

- Click **Add Recording Plan** next to **Device Recording Plan**.

Figure 3-20 Add a device recording plan (1)



- Configure the parameters, and then click **OK**.

Table 3-2 Parameter description

Parameter	Description
Enable	Turn on or off the recording plan.
Position	Videos will be stored on the device by default. It cannot be changed.
Stream Type	The device will make recordings using the main stream by default. It cannot be changed.
Remarks	Customizable description for the recording plan.
Recording Time	Select a default time template or click Create Time Template to add a new time template. See "3.1.6 Adding Time Template".

Related Operations

- Enable/disable a recording plan.

 means that the plan has been enabled. Click the icon and it becomes , and it means that the plan has been disabled.

- Click : Copy the recording plan to other channels.
- Edit a recording plan.

Click  of corresponding plan to edit the plan.

- Click  to delete recording plans one by one.

3.1.4.2 Adding Center Recording Plans in Batches

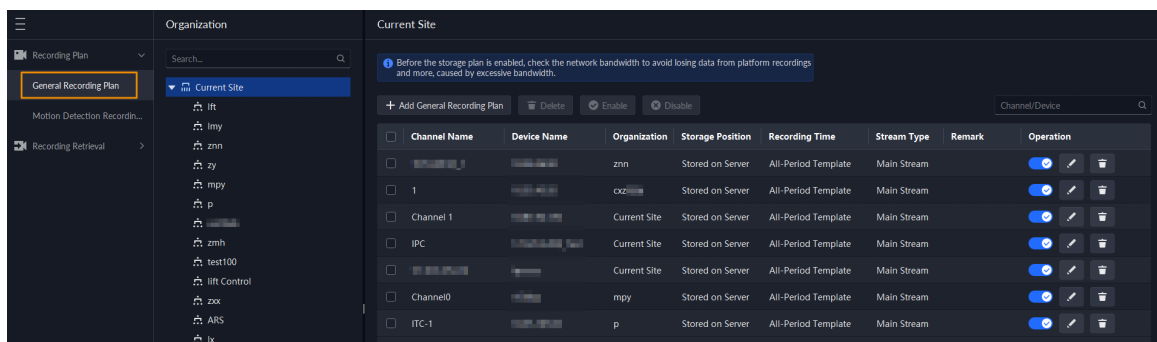
Add a center recording plan of general or motion detection videos for multiple channels at the same time.

3.1.4.2.1 General Recording Plan

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Storage Plan** > **Recording Plan**.

Figure 3-21 Center recording plan



- Step 2** Select **General Recording Plan** > **Add General Recording Plan**.

- Step 3** Configure the parameters, and then click **OK**.

Table 3-3 Parameter description

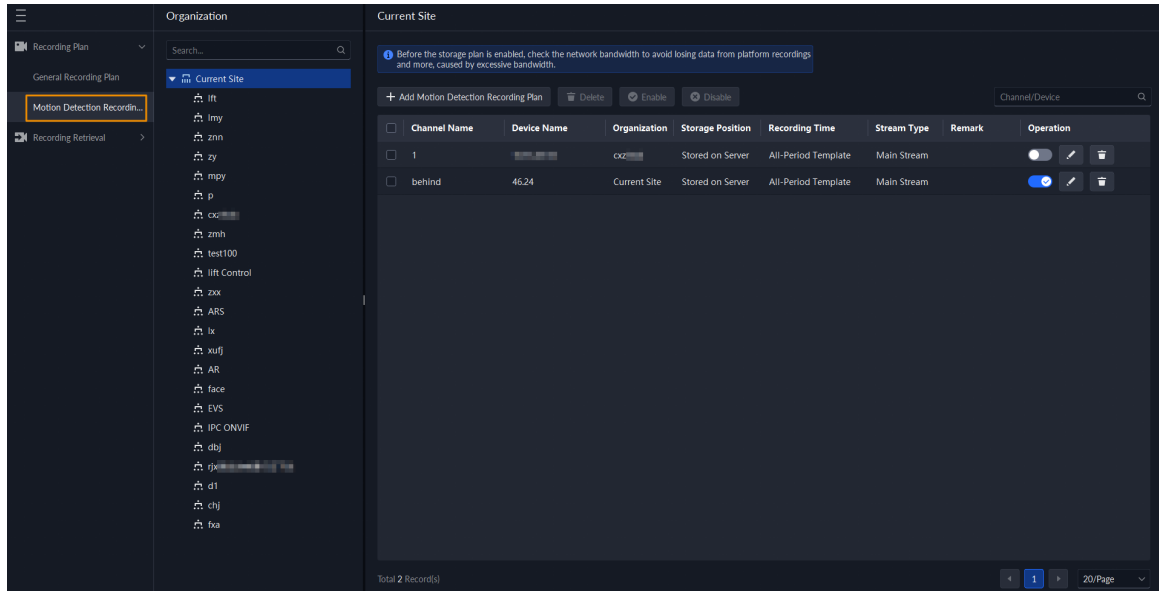
Parameter	Description
Enable	Turn on or off the recording plan.
Position	Videos will be stored on the server by default. It cannot be changed.
Stream Type	Select Main Stream , Sub Stream 1 or Sub Stream 2 . Videos recorded on the main stream will have the best quality, but they require more storage.
Remarks	Customizable description for the recording plan.
Recording Time	Select a default time template or click Create Time Template to add a new time template. See "3.1.6 Adding Time Template".
Recording Channel	Select the channels you want to add the recording plan for.

3.1.4.2.2 Motion Detection Recording Plan

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Storage Plan** > **Recording Plan**.

Figure 3-22 Motion detection recording plan



- Step 2** Select **Motion Detection Recording Plan** > **Add Motion Detection Recording Plan**.

- Step 3** Configure the parameters, and then click **OK**.

Table 3-4 Parameter description

Parameter	Description
Enable	Turn on or off the recording plan.
Position	Videos will be stored on the server by default. It cannot be changed.
Stream Type	Select Main Stream , Sub Stream 1 or Sub Stream 2 . Videos recorded on the main stream will have the best quality, but they require more storage.
Remarks	Customizable description for the recording plan.
Recording Time	Select a default time template or click Create Time Template to add a new time template. See "3.1.6 Adding Time Template".
Recording Channel	Select the channels you want to add the recording plan for.

Related Operations

- Enable/disable a recording plan.

 means that the plan has been enabled. Click the icon and it becomes , and it means that the plan has been disabled.

- Edit a recording plan.

Click  of corresponding plan to edit the plan.

- Edit a recording plan.

- Click of corresponding plan to edit the plan.
- **Delete**: Select multiple channels, and then delete them at the same time.
- **Enable** and **Disable**: Select multiple channels, and then enable or disable them at the same time.

3.1.5 Adding Video Retrieval Plans

Configure a video retrieval plan to upload the videos that devices record when they are disconnected from the platform. During the defined period, videos will be automatically uploaded to the platform. The platform supports uploading videos within the past 7 days, including the day when the retrieval plan is executed. You can add a retrieval plan for each channel one by one, or add one for multiple channels in batches.

Prerequisites

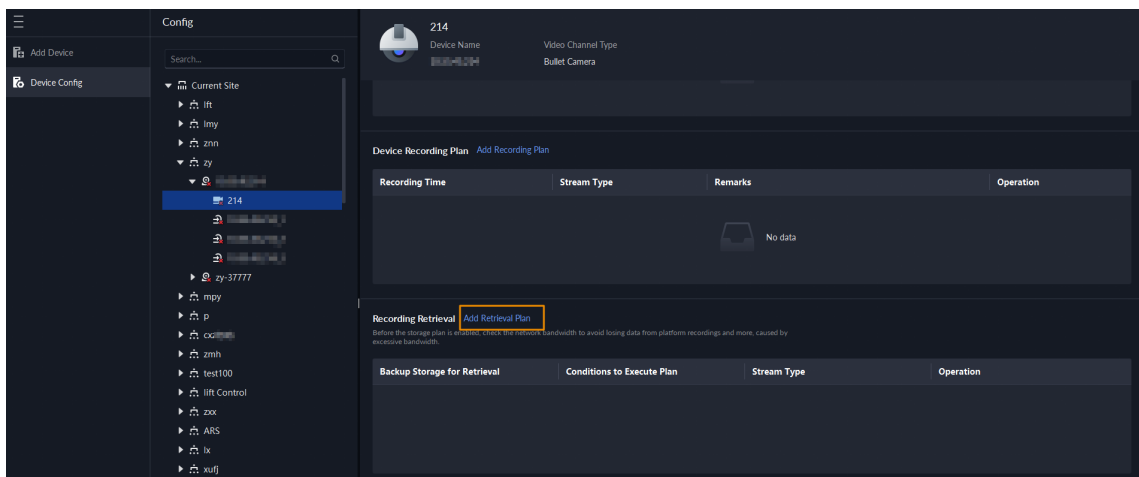
Before adding video retrieval plans, you need to configure storage for the platform. For details, see "3.3 Configuring Storage".

3.1.5.1 Adding Retrieval Plan One by One

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .

Figure 3-23 Add a retrieval plan for a channel



- Step 3** Select a device, and then click **Add Retrieval Plan**.

Figure 3-24 Add a retrieval plan

←

Recording Retrieval

Retrieve videos from devices and send them to the video storage disk of the platform in the stream format.

Channel Name

214

Enable

☒

Backup Storage for Retrieval

Yesterday

Stream Type

Main Stream

Videos stored on the current day will be retrieved.

Time to Execute Plan

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Execute the retrieval plan on the defined time. If the backup storage for retrieval is set as 2 days before, the data from the past 2 days will be retrieved.

OK

Cancel

Step 4 Configure the parameters.

Table 3-5 Parameter description

Parameter	Description
Enable	Turn on or off the retrieval plan.
Backup Storage for Retrieval	Select a period, and then the videos within the defined period will be uploaded. The platform supports uploading videos from devices within the past 7 days at most. Videos from the current day will also be included.
Stream Type	Select the stream type of the videos that you want to upload. If the videos are recorded on sub stream 1 and Main Stream is configured in this retrieval plan, uploading will fail.
Time to Execute Plan	Configure when to upload videos every day. Click  to configure specific periods. You can configure up to 6 periods.

Step 5 Click **OK**.

Related Operations

- Enable/disable retrieval plan

 means that the plan has been enabled. Click the icon and it becomes , and it means that the plan has been disabled.

- Edit retrieval plan

Click  of corresponding plan to edit the plan.

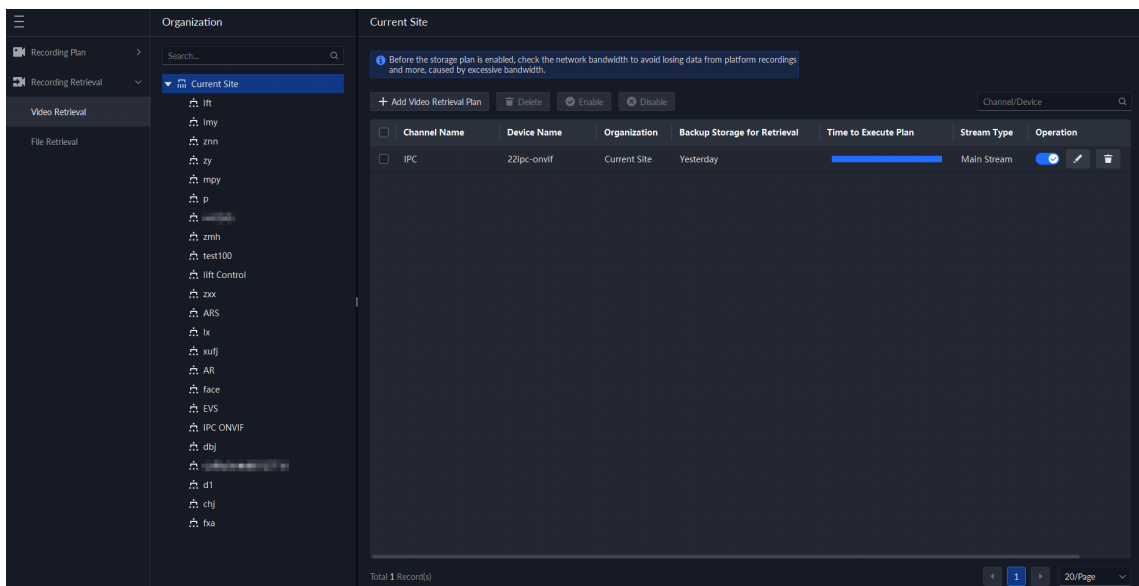
- Click  to delete recording plans one by one.

3.1.5.2 Adding Retrieval Plans in Batches

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Storage Plan** > **Recording Retrieval** > **Video Retrieval**.

Figure 3-25 Video retrieval



- Step 2** Click **Add Video Retrieval Plan**.

Figure 3-26 Configure a video retrieval plan

Step 3 Configure the parameters, and then select channels in the **Retrieval Channel** section.

Table 3-6 Parameter description

Parameter	Description
Enable	Turn on or off the retrieval plan.
Backup Storage for Retrieval	Select a period, and then the videos within the defined period will be uploaded. The platform supports uploading videos from devices within the past 7 days at most. Videos from the current day will also be included.
Stream Type	Select the stream type of the videos that you want to upload. If the videos are recorded on sub stream 1 and Main Stream is configured in this retrieval plan, uploading will fail.
Time to Execute Plan	Configure when to upload videos every day. Click to configure specific periods. You can configure up to 6 periods.

Step 4 Click **OK**.

3.1.5.3 Adding Retrieval Plan for MPT Devices

3.1.5.3.1 Adding One by One

The procedures are the same as other devices. For details, see "3.1.5.1 Adding Retrieval Plan One by One".

3.1.5.3.2 Adding in Batches

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Storage Plan** > **Recording Retrieval** > **File Retrieval**.
- Step 2** Click **Add File Retrieval Plan**, and then configure the parameters.

Figure 3-27 Configure a file retrieval plan

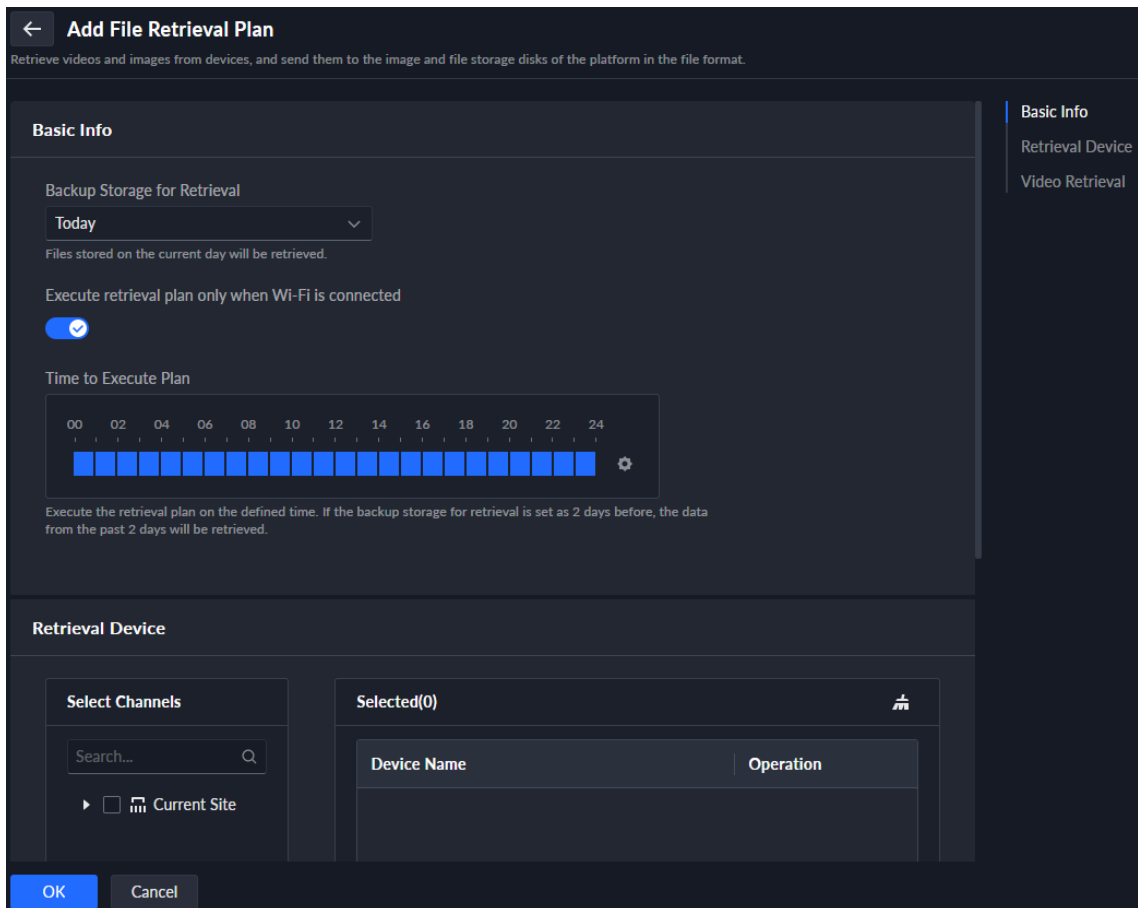


Table 3-7 Parameter description

Parameter	Description
Enable	Turn on or off the retrieval plan.
Backup Storage for Retrieval	Select a period, and then the videos within the defined period will be uploaded. The platform supports uploading videos from devices within the past 7 days at most.  Videos from the current day will also be uploaded.
Execute retrieval plan only when Wi-Fi is connected	When selected, videos on MPT devices will be uploaded only when they are connected to a Wi-Fi network.  If it is not selected and MPT devices are connected to the mobile network, uploading videos might result in additional charges.

Parameter	Description
Time to Execute Plan	Configure when to upload videos every day. Click  to configure specific periods. You can configure up to 6 periods.

Step 3 Select MPT devices in the **Retrieval Device** section.

Step 4 (Optional) Enable video retrieval as needed. After being enabled, the video stored on the device at the specified time will be automatically uploaded to the platform.

Step 5 Click **OK**.

3.1.6 Adding Time Template

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

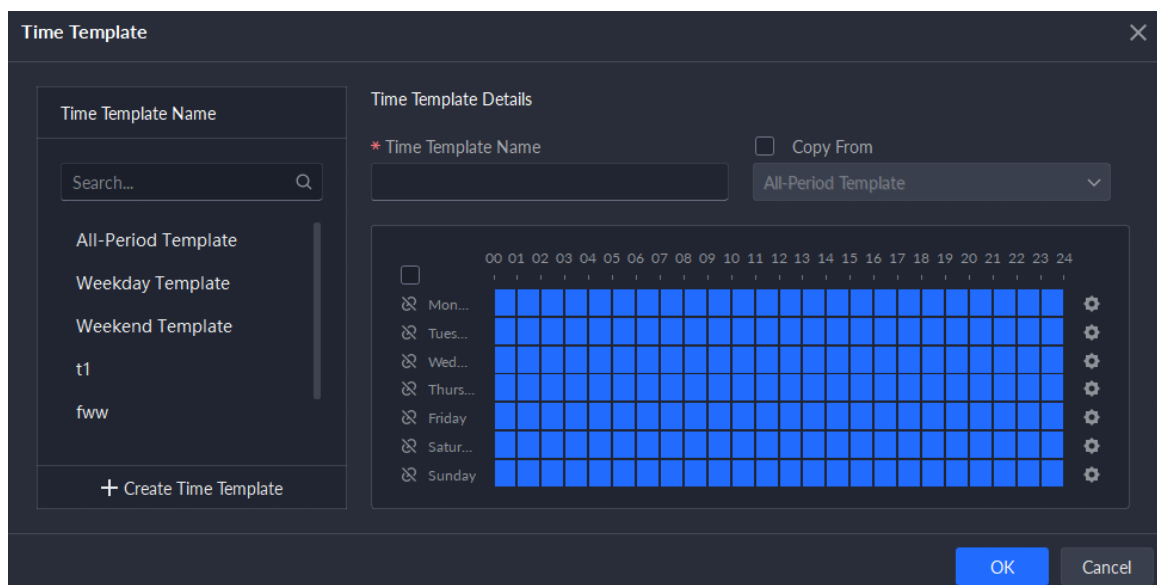
Step 2 Click .

Step 3 Select a channel, and then add a recording plan.

Step 4 In the **Recording Time** drop-down list, select **Create Time Template**.

Creating time template in other pages is the same. This chapter takes creating time template in **Record Plan** page as an example.

Figure 3-28 Create time template



Step 5 Configure name and periods. You can set up to 6 periods in one day.

Select the **Copy From** check box, and then you can select a template to copy from.

- On the time bar, click and drag to draw the periods. You can also click , and then draw the periods for multiple days.
- You can also click  to configure periods.

Step 6 Click **OK**.

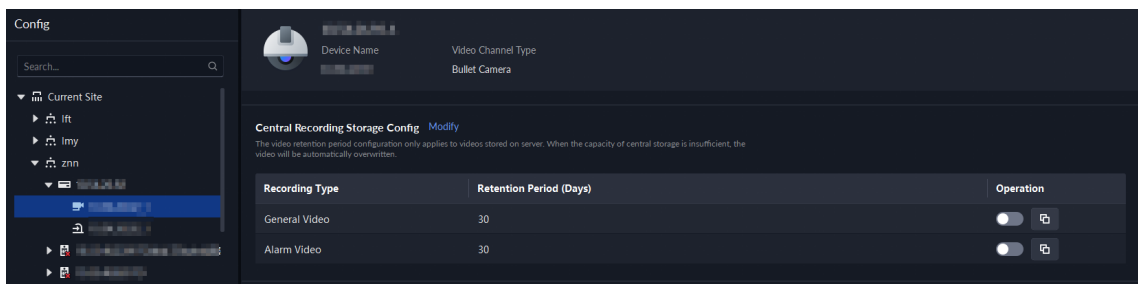
3.1.7 Configuring Video Retention Period

For videos stored on the platform, you can configure video retention period. When the storage space runs out, new recorded videos will cover the oldest videos automatically.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device** > **Device Config**.
- Step 2** Select a camera, and then click **Modify**.

Figure 3-29 Go to recording storage configuration page



- Step 3** Enable one or more video types, set the retention period for each one, and then click **OK**.
- Step 4** (Optional) Configure retention period for multiple channels.
 1. Click **OK and Copy**.
 2. Select which channels to apply the configuration.



Only administrators can select **All Channels**.

3. Click **OK**.

3.1.8 Configuring Events

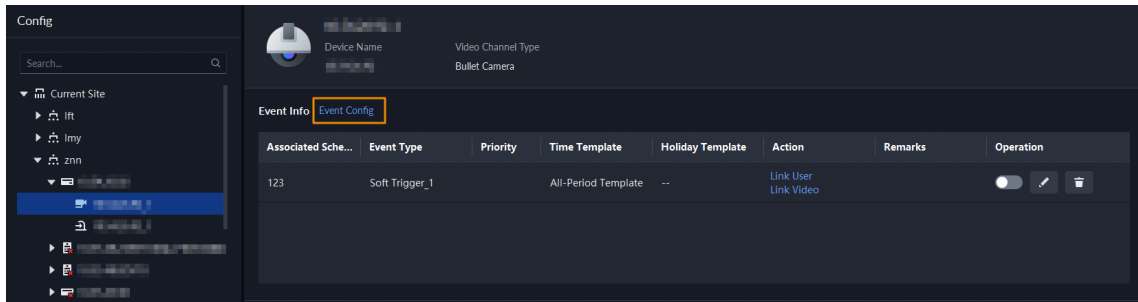
You need to set up the event configuration on a device or its channels to receive alarms on the platform.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device** > **Device Config**.
- Step 2** Select a channel or a device, and then click **Event Config**.

Events that can be configured are different for different types of devices. If you select **Device**, you can only configure general events. If you select **Channels**, various events supported by different types of channels will be displayed.

Figure 3-30 Go to the event configuration



Step 3 Configure events. For details, see "4.1 Configuring Events".

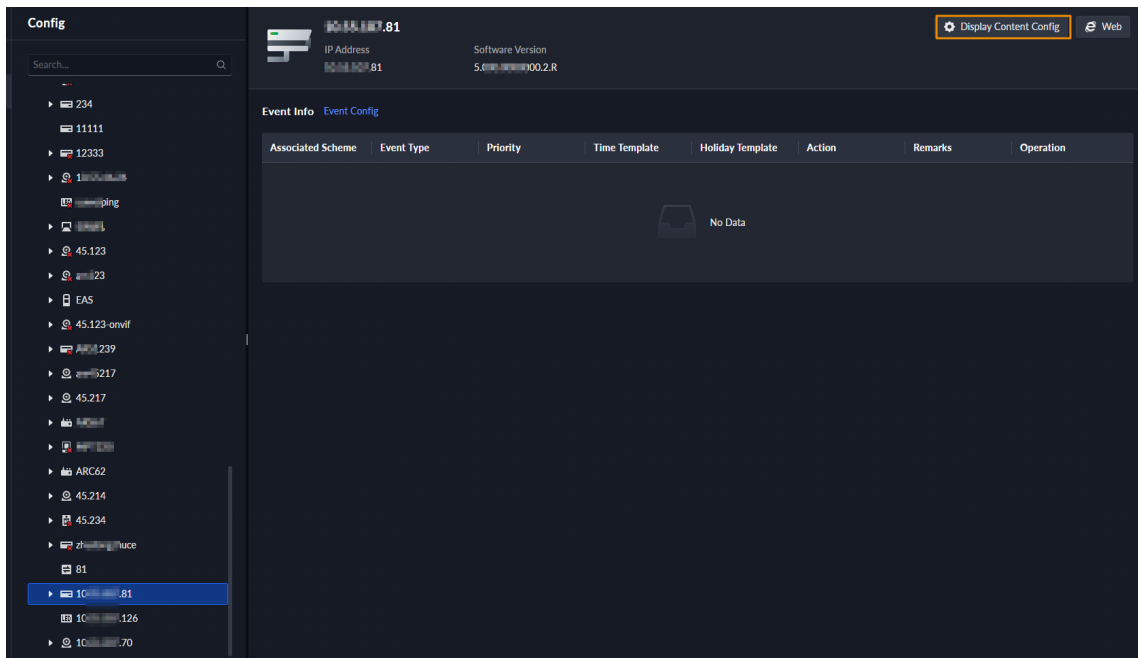
3.1.9 Configuring Information Display Content

ANPR cameras connect to the display screen via RS-485, supporting both platform mode and managed mode. Both modes can send information to the screen for display.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Select the ANPR camera, and then click **Display Content Config**.

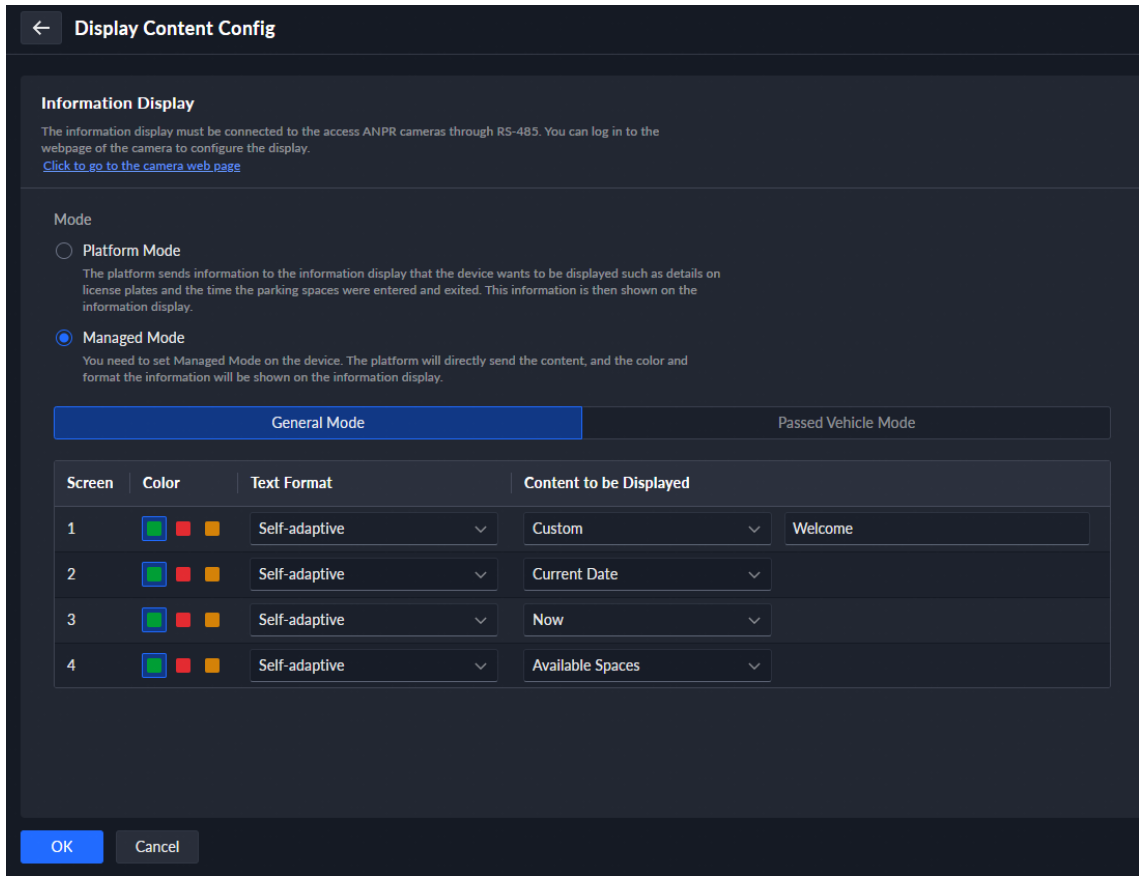
Figure 3-31 Display content configuration



Step 4 Select **Platform Mode** or **Managed Mode**.

- **Platform Mode** : The platform sends information to the information display that the device wants to be displayed.
- **Managed Mode** : You need to set managed mode on the device. The platform will directly send the content.

Figure 3-32 Managed mode



Display Content Config

Information Display
The information display must be connected to the access ANPR cameras through RS-485. You can log in to the webpage of the camera to configure the display.
[Click to go to the camera web page](#)

Mode

☐ Platform Mode
The platform sends information to the information display that the device wants to be displayed such as details on license plates and the time the parking spaces were entered and exited. This information is then shown on the information display.

☒ Managed Mode
You need to set Managed Mode on the device. The platform will directly send the content, and the color and format the information will be shown on the information display.

General Mode **Passed Vehicle Mode**

Screen	Color	Text Format	Content to be Displayed
1		Self-adaptive	Custom Welcome
2		Self-adaptive	Current Date
3		Self-adaptive	Now
4		Self-adaptive	Available Spaces

OK **Cancel**

- ◇ **General Mode** : The information to be displayed when no vehicles are detected passing by, including screen color, text style, content, and customized content.
- ◇ **Passed Vehicle Mode** : The information that needs to be displayed when a vehicle passes includes the screen color, text format, content, and customized content.

Related Operations

Click **Click to go to the camera web page** to open the web page of the camera.

3.1.10 Configuring Door

Configure the parameters of doors, including reader direction, mode, unlock duration, unlock method, and more.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Select a door channel, and then click **Door Config**.
- Step 4** Configure the parameters.

Figure 3-33 Door configuration

←

Door Config

Basic Info

Reader Direction

In

Reader 1

Out

Reader 2

Mode

Normal

Enable Door Sensor

Enable Alarm

☒ Duress

☐ Unsuccessful Attempts Exceeding Limit

☒ Forced Entry

☒ Timeout

Public Password

Unlock Duration

10

sec

Unlock Timeout

2

sec

Unlock Method

☐ Unlock by Period

OR

☒ Card

☒ Fingerprints

☒ Password

☒ Face

OK

Cancel

Copy to

Table 3-8 Parameter description

Parameter	Description
Reader Direction	Click  to switch the reader direction.
Mode	Select the mode of the door, including Normal , Always Closed and Always Open .
Enable Door Sensor	After enabling door sensor, it supports Forced Entry and Timeout alarms.
Enable Alarm	After enabling alarm, you can select uploading duress, unsuccessful attempts exceeding limit, forced entry and timeout to the platform.
Public Password	After configuring a public door password, anyone can open the door with this password.
Unlock Duration	The duration that the door opens.
Unlock Timeout	Close the door after the defined time.

Parameter	Description
Unlock Method	Supports selecting AND or OR , and selecting card, fingerprint, password and face for combined door unlock. You can also select Unlock by Period , and set the door unlock parameters according to time periods.

Step 5 (Optional) Click **Copy to** to copy the parameters to other door channels.

Step 6 Click **OK**.

3.1.11 Configuring Parking Space Available Display

Adjust the display format of the available parking display based on the available value.

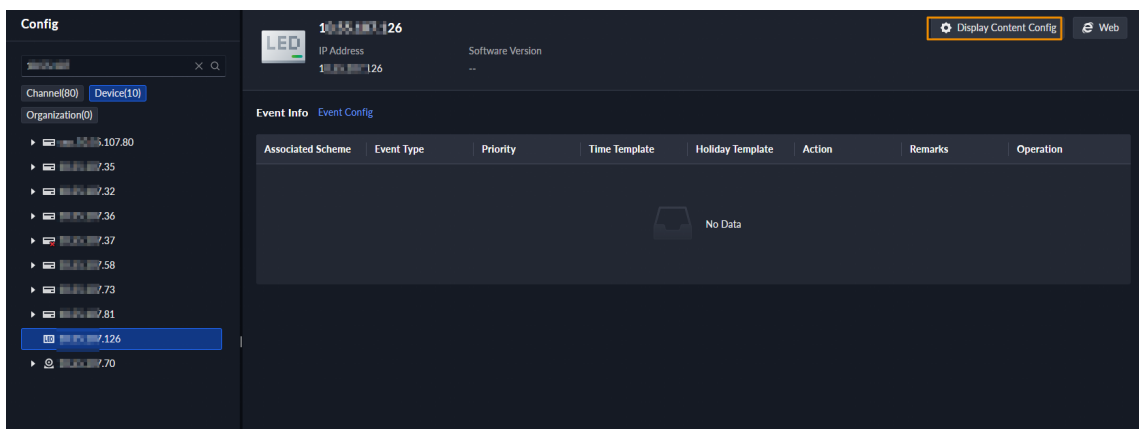
Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select parking space available display, and then click **Display Content Config**.

Figure 3-34 Display content config



Step 4 Configure the display format of parking space available display.

Figure 3-35 Parking space available display

←

Display Content Config

Basic Info

Copy from a Display

Screen Split

Number of Screens

2

Modify the number of screens and the display configuration will be restored to the default settings.

10. 26-2

Click the first or last square of the screen to adjust the screen width.

Screen No.	Screen Name	Screen Width
1		4
2		4

Display Content Config

Available Parking Spaces

Full Parking Lot Display

The available parking space can only be displayed in the position of the placeholder. If you need to display the available parking space, please make sure that the placeholders appear together.

10. 26-2

← 9 Z

↑ * * *

OK

Cancel

Figure 3-36 Display by available space rule

Display by Available Space Rule

Rule 1

* Select Screen

1

▼

* Range of Available Spaces

Available Parking Spaces<n

▼

* N

1

←9Z

+ Add

Table 3-9 Parameter description

Parameter	Parameter	Description
Basic Info	Copy from a Display	Select an existing display screen and reuse the current display format of that screen.
Screen Split	Number of Screens	Set the number of splits on the display screen and the name for each split.

Parameter	Parameter	Description
Display Content Config	-	● Available Parking Space : Configure the display format for available parking spaces, including screen colors and symbols. ● Full Parking Lot Display : Configure the display format for full parking spaces, including screen colors and symbols. ● Display by Available Space Rule : Click  to enable this function, and then select the screen, set the range of available space, and configure the screen colors and symbols for the available spaces display.  When only Available Parking Space is selected, the system supports configuring the rules for displaying available spaces.

Step 5 Click **OK**.

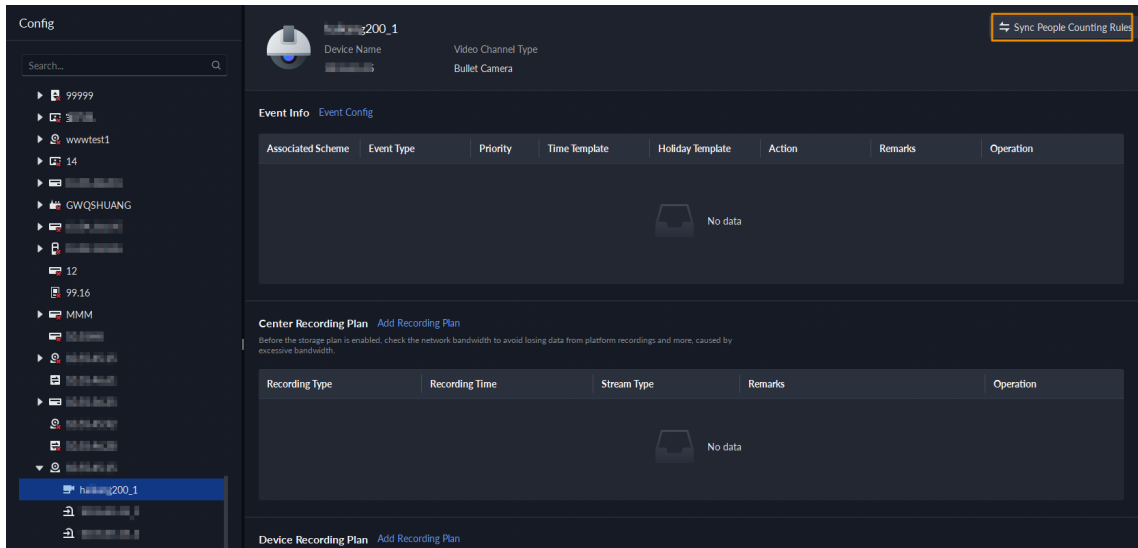
3.1.12 Synchronizing People Counting Rules

If you create, edit or delete people counting rules on a device, you have to manually synchronize them to the platform.

Procedure

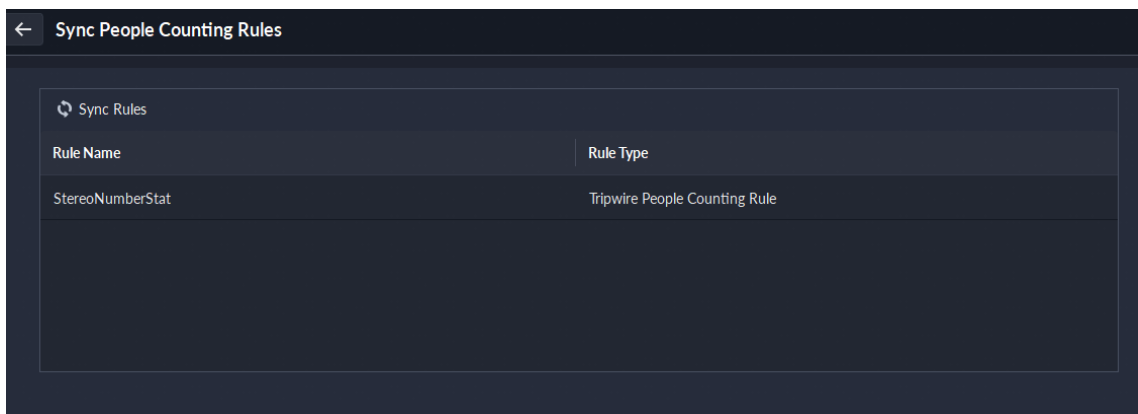
- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2 Click .
- Step 3 Select a channel, and then click **Sync People Counting Rules**.

Figure 3-37 Synchronize people counting rules from the device (1)



Step 4 Click **Sync Rules**.

Figure 3-38 Synchronize people counting rules from the device (2)



3.2 Adding Roles and Users

All users in the platform belong to a role, which defines the permissions of users. The permissions involve devices, menus, and operations. When creating a user, assign a role to it to give the corresponding permissions.

3.2.1 Adding a Role

A role is a set of permissions. Classify users of the platform into different roles so that they can have different permissions for operating the devices, functions and other system resources.

The following roles are available.

- **Super administrator:** A default role that has the highest priority and all the permissions. This role cannot be modified. A super administrator can create common administrator and common operator roles. The system supports 3 super administrators at most.
- **Administrator:** A default role that cannot be modified and has no permissions of cascade, storage, system deployment, license, backup and restoring. An administrator can create

common administrator and common operator roles. The number of administrators that can be created is not limited.

- Common administrator: This role has no permissions of cascade, multiple sites, user, storage, system deployment, license, and backup and restoring.

The device and control permissions of this role cannot be edited, but its menu permissions can be edited.

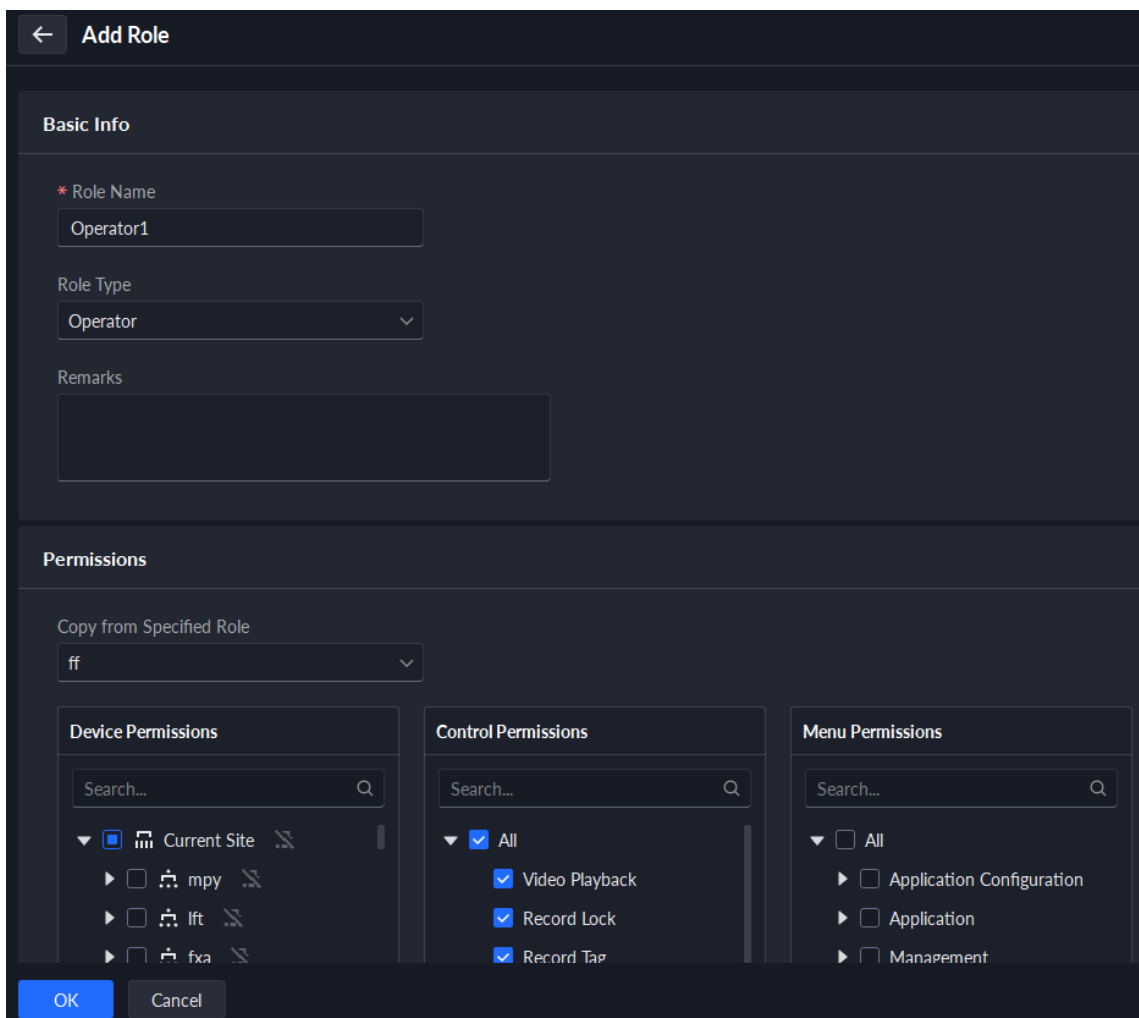
- Common operator: This role has no permissions of cascade, multiple sites, basic configuration, storage, license, system parameters, and backup and restoring.

The device, control and menu permissions of this role can be edited.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User**.
- Step 2** Click .
- Step 3** Click **Add**, set role information, and then select device and control permissions and assign the rule to users.

Figure 3-39 Add a role



- If a device is not selected under **Device Permissions** or a menu not selected under **Menu Permissions**, all users assigned with this role will not be able to see the device or menu.

- Click  of a selected organization. All permissions of subsequently added devices under this organization will also be assigned to users of this role.
- When the **Role Type** is set to **Operator**, you can copy the permissions from specified role.

Step 4 Click **OK**.

3.2.2 Adding a User

Create a user account for logging in to the platform.

Prerequisites

You need to add a role first; otherwise, only the default roles can be selected. This will limit your differentiation between users of their permissions and operations.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User**.

Step 2 Select **User Management**, click **Add**, and then configure the user parameters.

Table 3-10 Parameter description

Parameter	Description
Username	Used to log in to the client.
Multi-client Login	Allow the user to log in to multiple clients at the same time.
Password	Used to log in to the client.
Confirm Password	
MPT User	Enable and enter a name, and then this user will be set as an MPT user. This is used in the group talk function in the map. For details, see "5.1.4 Map Applications".  If you enable this function, you cannot enable Multi-client Login.
Enable Forced Password Change at First Login	The user is required to change the password at first-time login.
Enable Password Change Interval	Force the user to change the password regularly.
Enable Password Expiry Time	After the password expires, the user cannot log in to the client. If already logged in, the user will be forced to log out. The user must reset the password through email or contact the administrator.
PTZ Control Permissions	The PTZ control priority of the user. The larger the value, the higher the priority. For example, User A has a priority of 2 and User B has a priority of 3. When they operate on the same PTZ camera, which is locked, at the same time, the PTZ camera will only respond to the operations from User B.
Email Address	Used to receive emails in various situations, such as password reset, alarm messages, and visitor registration.

Parameter	Description
Bind MAC Address	Limit the user to log in from specific computers. One user can be bound to 5 MAC addresses at most.
Role	Select one or more roles to assign the user permissions, such as which devices are allowed to be operated.

Step 3 Click **OK**.

Related Operations

- Click  to lock user. The locked user cannot log in to the DSS Client and App.
- Click  to modify information of a user except the username. Users with a higher level of permissions can change the passwords of users with a lower level of permissions. Super administrators can change the passwords of administrators and common roles. Administrators can change the passwords of common roles.
- Click  to delete a user.

3.2.3 Adding a User Group

Add users to specified user groups to facilitate event linkage by user groups.

Prerequisites

You need to add users first.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User**.

Step 2 Select **User Management**, and then in the **User Group** section, click .

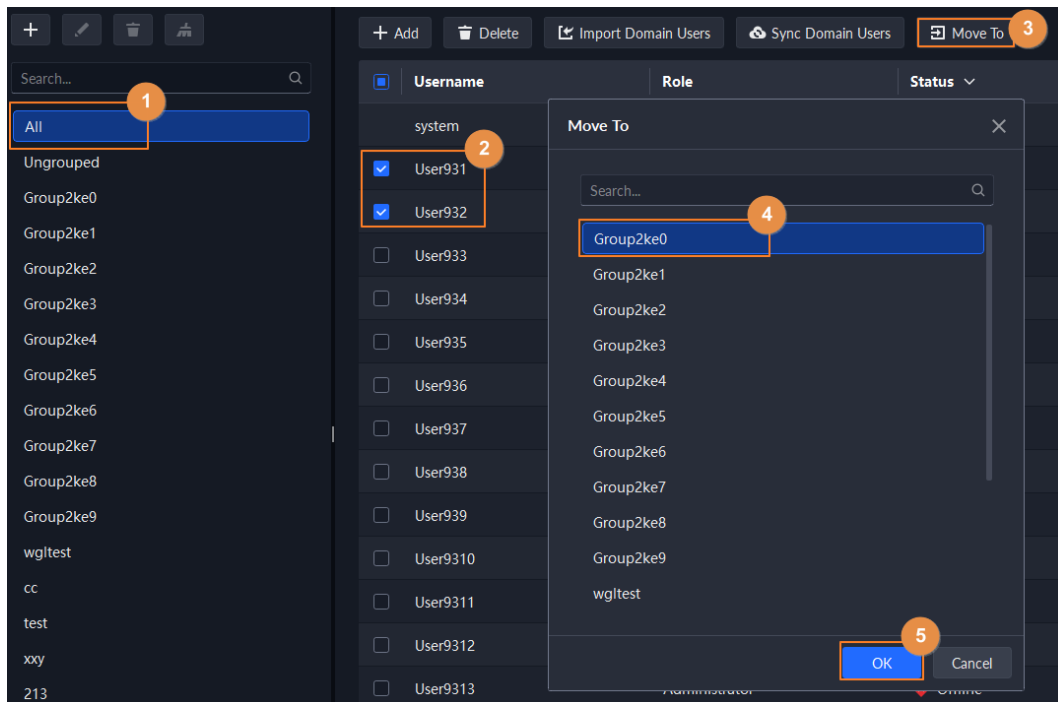
Step 3 Define the group name, set the remark, and then click **OK**.

Step 4 Select users, and then click **Move To** to move the users to the added user group.



One user can be only added to one user group.

Figure 3-40 Move users to a user group



Step 5 Click **OK**.

Click the user group, and you will see the users of the group.

Related Operations

In the **User Group** section, you can:

- Click to edit user group name and remarks.
- Click to delete the user group. After this operation, the users in the group will become ungrouped.
- Click to clear the user group. After this operation, the users in the group will become ungrouped.

3.2.4 Importing Domain Users

You can import domain users to the platform quickly through this function.

Prerequisites

You need to configure domain information first from > **System Parameters** > **Active Directory**. For details, see "7.4.6 Configuring Active Directory".

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User** > **User Management**.
- Step 2** Click **Import Domain Users**.
- Step 3** Select how you want to import users, and then click **Next Step**.

- **Import by Domain Group**: Import all users in the selected group.



If you import an entire domain group after the automatic synchronization function is enabled, the platform will remember that group and automatically synchronize its

new users at the defined time every day, and update the information of the users imported by manual selection at the defined time every day. For details, see the previous steps.

- **Import by Domain User** : Import selected users in a group.

Step 4 Click  to select a role for the users.

All the permissions in the role will be assigned to the users.

Step 5 Click **OK**.

3.2.5 Syncing Domain Users

You can synchronize the newly added domain users and delete all the invalid domain users.

Prerequisites

You need to configure domain information first in  > **System Parameters** > **Active Directory**. For details, see "7.4.6 Configuring Active Directory".

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User** > **User Management**.

Step 2 Click **Sync Domain Users**.

The platform prompts that this operation will synchronize the newly added domain users and delete all the invalid domain users.

Step 3 Click **OK**.

3.2.6 Configuring Auto Synchronization

The platform supports automatically synchronizing people that were added to the domain group, and updating the information for all imported people in the domain.

Prerequisites

You need to configure domain information first from  > **System Parameters** > **Active Directory**. For details, see "7.4.6 Configuring Active Directory".

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User** > **User Management**.

Step 2 Select **More** > **Auto Sync Config**.

Step 3 Enable the automatic synchronization function and set a time.

The platform will automatically synchronize the new users in the user groups that you previously imported, and update information on the users you manually selected for import at the defined time every day.

For example, if you imported user group A, the platform will synchronize the new users that are in user group A every day at the defined time. Click  to remove a group on the list, and then it will not be synchronized. For users imported by manual selection, the platform will check their information, and update if anything changes.

Step 4 Click **OK**.

3.2.7 Password Maintenance

Users can change passwords manually or reset it on the login page. Also, Users with a higher level of permissions can change the passwords of users with a lower level of permissions. Super administrators can change the passwords of administrators and common roles. Administrators can change the passwords of common roles.

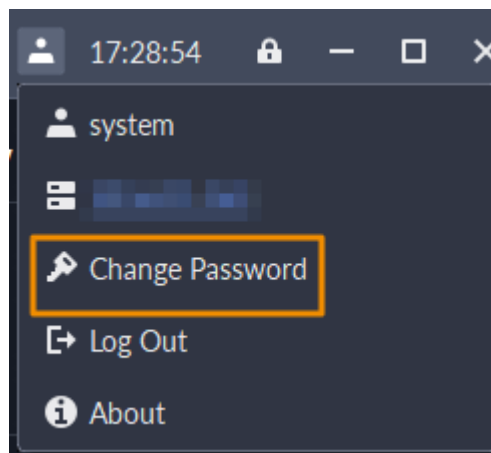
3.2.7.1 Changing Password for the Current User

We recommend changing your password regularly for account safety.

Procedure

- Step 1** Log in to the DSS Client, click  at the upper-right corner, and then select **Change Password**.

Figure 3-41 Change password



- Step 2** Enter the old password, new password, and then confirm the new password. Click **OK**.

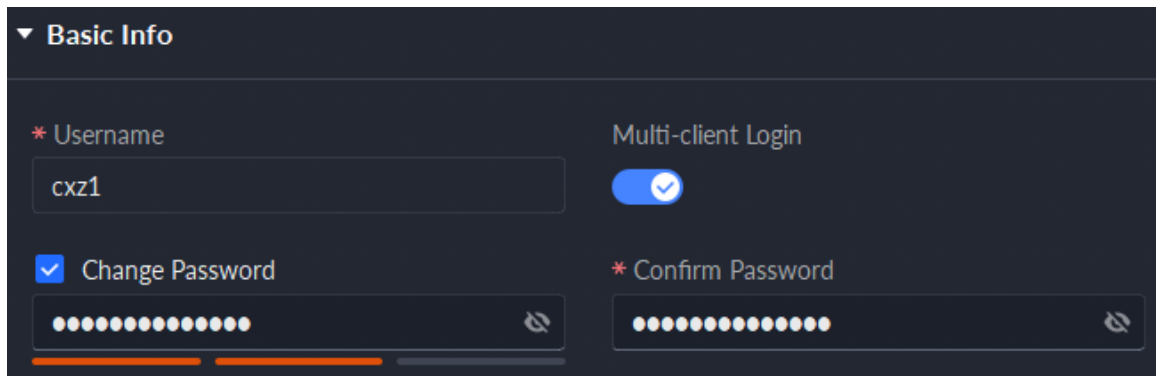
3.2.7.2 Changing Password for Other Users

Users with a higher level of permissions can change the passwords of users with a lower level of permissions without knowing their passwords. Super administrators can change the passwords of administrators and common roles. Administrators can change the passwords of common roles.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User**.
- Step 2** Click .
- Step 3** Select a user, and then click .
- Step 4** Enable **Change Password**, enter the new password and confirm password, and then click **OK**.

Figure 3-42 Change passwords for other users



3.2.7.3 Resetting User Password

Users can reset passwords through email addresses and security questions. Only the system user can reset the password through security questions.

Procedure

- Step 1** On the login page, click **Forgot password?**.
- Step 2** Enter the account that you want to reset the password for, and then click **Next Step**.
- Step 3** Select how you want to reset the password.
- By security questions. This is only applicable to the system user.
 1. Click **Reset Password through Security Questions**.
 2. Answer the questions, and then click **Next Step**.
 - By reset file. This is only applicable to the system user.
 1. Log in to the management tool.
 2. Click , and then select **Reset System Password**.
 3. Click **Export**, set the encryption password, and then export the request file.
 4. Contact the technical support to get the password reset file through the request file.
 5. Click **Reset** to import the reset file, and then log in the DSS client to initialize the password.
 - By email address. This is applicable to all accounts, but an email address must be configured first. For details, see "3.2.2 Adding a User".
 1. Click **Reset Password through Email Verification**.
 2. Click **Send Verification Code**.
 3. Enter the verification code that you received from the email address, and then click **Next Step**.
- Step 4** Set a new password and confirm it, and then click **Next Step**.
- The password has been reset.

3.2.7.4 Resetting Security Questions for the System User

The system user can reset the security questions that can be used to reset passwords.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User > User Management**.

Step 2 Click  to edit the information of the system user.

Step 3 Click **Reset** to reset the security questions after verifying the login password.

3.3 Configuring Storage

Manage the storage of the platform, including adding network disks, setting storage types to store different types of files, creating disk groups to store files from specified channels, and setting the storage location and retention period of the images and recorded videos from devices.

3.3.1 Configuring Network Disk

We recommend using Dahua's EVS devices.

Prerequisites

- The storage server is required to be deployed.
- One user volume of the current network disk can only be used by one server at the same time.
- User volume must be formatted when adding network disks. Check if you have backed up the data.

Background Information

The iSCSI target name usually uses the IQN (iSCSI Qualified Name) format. When connecting a third-party iSCSI storage to the DSS platform, we recommend that the iSCSI target name follow the naming rules as below.

iqn.YYYY-MM.reverse-domain.name:uniqueidentifier

- YYYY-MM: The year and month, such as 2024-12.
- reverse-domain.name: The reverse of the domain name (for example, com.Example). It is used by organizations that provide iSCSI services.
- uniqueidentifier: A unique identifier to ensure that the name is unique in the same namespace. It is usually a string generated by a serial number or other methods.

Example: iqn.2023-08.com.example:storage.disk1.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Storage**.

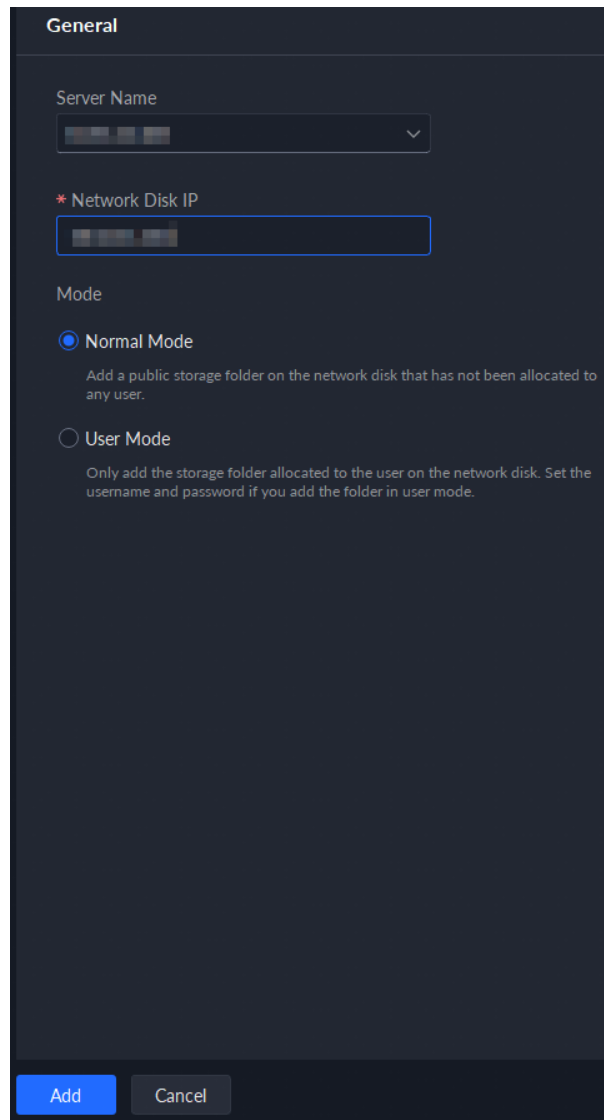
Step 2 Select .

Step 3 Click **Add**.

Step 4 Select server name and mode, enter the IP address of network disk, and click **OK**.

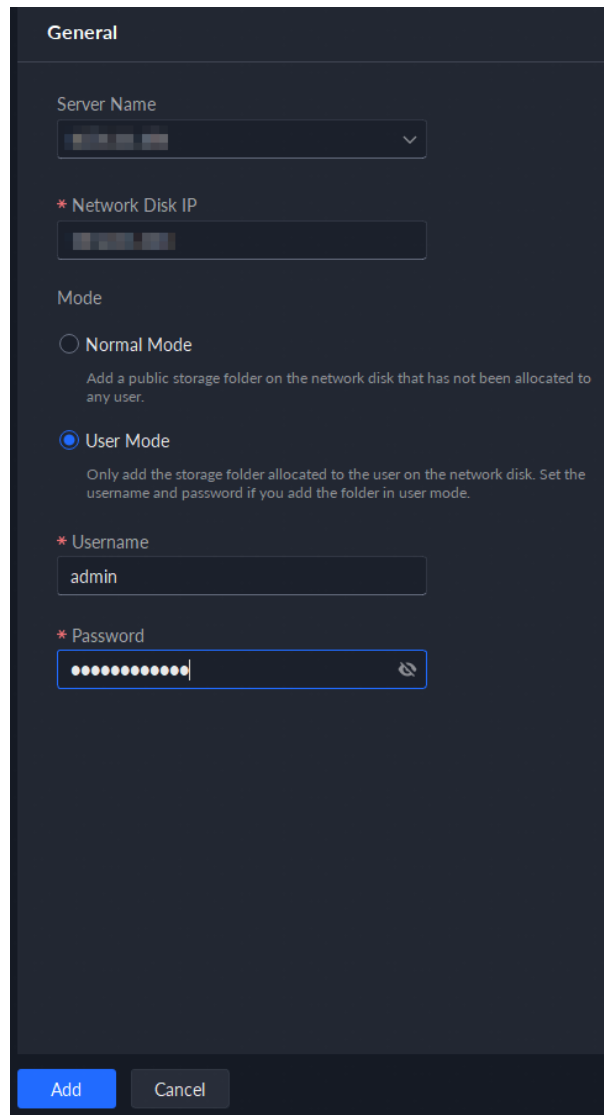
- Normal mode: All volumes of the network disk will be added. Those used by any user will be in red.
- User mode: Enter the username and password of a user. Only volumes of the network disk assigned to this user will be added.

Figure 3-43 Add a network disk (normal mode)

The image shows a dark-themed dialog box titled "General". It contains the following fields and options:

- Server Name:** A dropdown menu with a small "v" icon on the right.
- * Network Disk IP:** A text input field with a blue border.
- Mode:** Two radio button options:
 - Normal Mode:** Selected with a blue dot. Below it is the text: "Add a public storage folder on the network disk that has not been allocated to any user."
 - User Mode:** Unselected. Below it is the text: "Only add the storage folder allocated to the user on the network disk. Set the username and password if you add the folder in user mode."
- Buttons:** At the bottom, there are two buttons: "Add" (highlighted in blue) and "Cancel" (grey).

Figure 3-44 Add network disk (user mode)



General

Server Name

* Network Disk IP

Mode

☐ Normal Mode

Add a public storage folder on the network disk that has not been allocated to any user.

☒ User Mode

Only add the storage folder allocated to the user on the network disk. Set the username and password if you add the folder in user mode.

* Username

admin

* Password

●●●●●●●●

Add Cancel

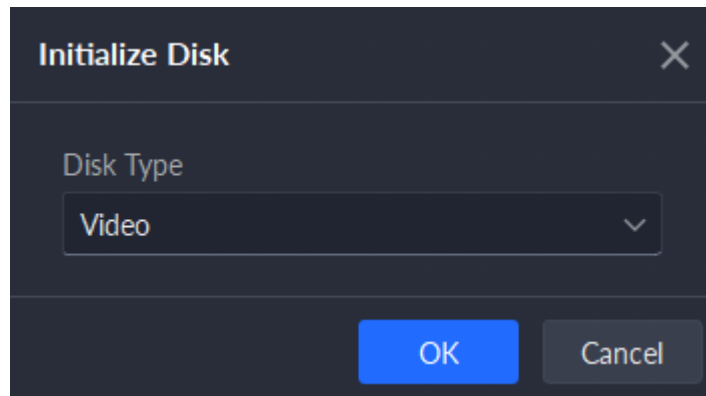
Step 5 Select a disk, and then click  to format the corresponding disk.

1. Select user volume, and then click .

2. Select format disk type, and then click **OK**.

- **Video** : Stores videos.
- **Image and File** : Stores all types of images and files.

Figure 3-45 Format disk



Related Operations

- To configure disk type, click .
- To format a disk, click .



Formatting will clear all data on the disk. Please be advised.

3.3.2 Configuring Server Disk

Configure local disk to store different types of files, including videos, ANPR snapshots, incident files, and face or alarm snapshots. In addition to the local disks, you can also connect an external disk to the platform server, but you have to format the external disk before using it.



Do not use a USB drive as a server disk. It usually does not have the performance and stability required by the platform, which might result in data lost.



- To set up local storage, you need a physical disk with only one volume or any volume of one physical disk. Back up the data of the disk or volume before setting its disk type, which will format and erase all data from it.
- One physical disk with only one volume or any volume of one physical disk can only store one type of files. If you need to store more than one type of files, you need more than one physical disks or volumes, but it cannot be the one where you installed the operating system of the server or the management tool.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Storage**.
- Step 2** Select .
- Step 3** Format a disk to set a storage type.



This operation will clear all data on the disk. Please be advised.

1. Select user volume, and then click .
2. Select storage type, and then click **OK**.

- **Video** : Stores videos.
- **Images and Files** : Stores all types of images and files.
- **Incident File** : Stores videos and images in the case bank. This disk cannot be overwritten.



If you do not set up one or more disk types, you will not be able to properly use corresponding functions. For example, if you do not set up an **Image and File** disk, you will not see images in all alarms.

Step 4 Manage local disks.

- Initialize disk

Click .

- To configure disk type: Click .
- To format a disk: Select a disk or user volume, click .

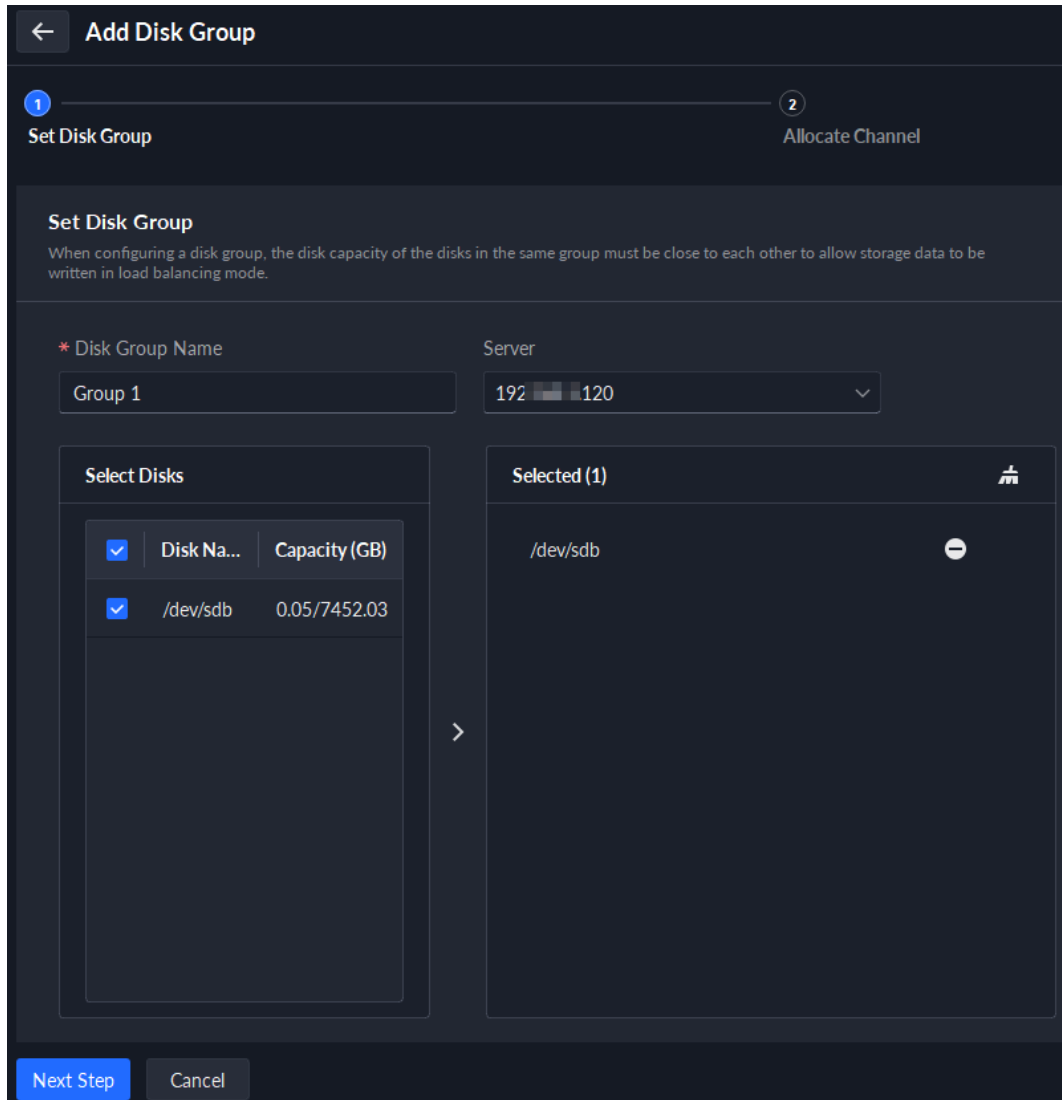
3.3.3 Configuring Disk Group

Allocate disk groups for video storage.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Storage**.
- Step 2 Click .
- Step 3 Click **Add**, enter disk group name, and then select a server and disks.

Figure 3-46 Configure disk group



Step 4 Click **Next Step**.

Step 5 Select devices or channels on the left.

Step 6 Click **OK**.

3.3.4 Configuring Device Storage

When there are a large number of devices on the platform, it will put too much pressure on the network disks or local disks because they might produce a lot of face, video metadata, and event images, and videos that need to be stored. The platform supports setting the storage location and retention period of the images and videos for storage devices, such as an IVSS, to reduce the pressure on the server.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Storage** > **Device Storage Config**.

Only organizations with storage devices are displayed, such as IPC, NVR and IVSS.

Step 2 Select an organization, click  of a device on the right.

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

Table 3-11 Parameter description

Parameter	Description
Event Image Storage Location	● Save to Central Storage : All images produced by the channels connected to this device will be stored on the network disks or local disks of the platform. ● Link to Images on Device : All images produced by the channels connected to this device will be stored on the device itself. The platform will obtain images from the device.
Event Video Storage Location	● Save to Central Storage : All alarm videos produced by the channels connected to this device will be stored on the network disks or local disks of the platform. ● Link to Videos on Device : All alarm videos produced by the channels connected to this device will be stored on the device itself. The platform will obtain videos from the device.  To make sure that alarms videos are complete, we recommend you set a 24-hour recording plan for the device. Otherwise, the platform might not be able to obtain videos. For example, a recording plan of 00:00–14:00 has been configured on the device so that the channels connected to it will record videos during that period. If an alarm is triggered on 14:01, the platform will not be able to obtain videos for this alarm.
Retention Time of Images and Videos on Device	This function is applicable to the images and videos stored on the device. After enabled, the platform will obtain the value from the device, and you can change it to 1–255. The images and videos that have been stored longer than this value will be automatically deleted.  Deleted files cannot be recovered. Please be advised.

Related Operations

Click **Batch Config** to configure device storage in batches.

4 Businesses Configuration

This chapter introduces the basic businesses, such as storage plan, video monitoring, access control, video intercom, target detection, face recognition, parking lot, and intelligent analysis.

4.1 Configuring Events

Configure event schemes of devices or channels in the platform, and then you can receive device events, event linkage among devices, event pop-ups, and more.

4.1.1 Configuring Event Linkage

Configure the event source, and the linked actions. When the event is triggered, the platform will perform the actions you defined, such as taking a snapshot recording a video.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Event** > **Event Config**.
- Step 2** Click **Add**.
- Step 3** Select the event source type, events, and event sources.

Table 4-1 Parameter description

Parameter	Description
Device, video channel, alarm input channel, subsystem, zones, EAS alarm channel, access control channel, radar, parking lot, people counting group, lift control channel, and POS alarms	Select an event source type.  - Before configuring the event, check whether the channel features match the event type; otherwise the event type cannot be selected as the alarm source. To configure channel features, see "3.1.2.5.2 Modifying Device Information". - If Alarm Input Channel is selected, check whether the Triggered Event that you select matches the channel feature of the alarm input channel you select. Otherwise, the event will not be triggered.
Soft Trigger	This is a type of event that is manually triggered. Click  to customize its name and icon. When viewing the live video image of the configured channel in the Monitoring Center, you can click the icon to trigger an alarm manually.
Combined Event	When a combined event is triggered, the platform performs the defined linked actions. For how to configure combined events, see "4.1.2 Configuring Combined Event".

Parameter	Description
Custom Alarm	- DHOP event: Access events developed through Dahua Hardware Open Platform (DHOP). - Extended standard event: This is used for events that devices support, but the platform currently does not. Click Add Extended Event, and then configure the parameters. Event Protocol : Select the protocol of the event. Alarm Source : Select an event source type based of the event protocol. Event Image : When configuring an event for a video channel, you can choose whether to subscribe to images from the event. When subscribing to pictures, the platform will receive alarm images generated by the alarm source. However, if the alarm source does not generate alarm images, subscribing to the event images will cause the platform to not receive the alarm. Name , Alarm Code, CID Code and DCS Code: Enter the name and code of the event.
Generic Event	Receives simple strings sent to the system by third-party hardware or software through the network, and then generates alarms or triggers corresponding linkage actions in the system. When configuring event source, select Generic Event from Event Source Type and Event, and select added generic events from Event Source. For details of add a generic event, see "4.1.4 Configuring Generic Event".
Third-party event	- Import events from a third-party system to the platform through bridge. - Devices, and person and vehicle information can be synchronized from a third-party platform to the DSS platform to be used in various functions.  When configuring event source, select a defined third-party event from Event Source Type , and Third-party Event will automatically show in Event.

Step 4 Configure the priority, when the event can be triggered, and other information.

Table 4-2 Parameter description

Parameter	Description
Scheme Name	Enter a name for the scheme.
Priority	The priority level is used to quickly know the urgency of the event when it is triggered.
Time Template	Select a time template for when the event can be triggered. If you want to create a new template, see "3.1.6 Adding Time Template".

Parameter	Description
Holiday Template	If the time template and holiday template overlap, only the holiday template will be effective. During the defined periods, events will be received by the platform normally. Outside of the defined periods, events will not be received by the platform. To create a new template, follow the steps below. 1. In the drop-down box, click Create Custom Holiday Template. 2. Enter a name for the template. 3. Click Add, and then add a period and adjust the time. You can add up to 6 periods. 4. (Optional) If there are other holiday templates, you can select Copy From, and then select a template to copy its periods. 5. Click OK.
Alarm Storm Config	After enabled, if certain alarms are frequently triggered, you can configure an interval during which they can only be triggered once. For example, a tripwire alarm can only be triggered once in 10 seconds. This function is only available to event sources selected in the previous step. The configurations here enjoy higher priority if alarm storm for the same event is configured from Event > Alarm Config > Alarm Storm Config.
Remarks	Enter remarks on events.

Step 5 Click  next to **Linked Action** to enable the alarm linkage function.

Step 6 Configure alarm linkage actions.

- To link video, enable **Link Video**, and then configure the parameters.

Table 4-3 Parameter description

Parameter	Description
Camera	◇ Event source: The camera of the alarm itself is linked when the alarm occurs. ◇ Bound camera: If the channel is bound to one or more video channels, you can view the real-time videos of the bound channel when an alarm is triggered. To bind a channel, see "3.1.3 Binding Resources". ◇ Select camera: Select a camera so that you can view the camera video when the associated alarm is triggered.
When an alarm is triggered, display camera live view on client	Enable this parameter, and then the platform will open the real-time video of the channel where an alarm is triggered, and play it in the defined stream type.  After the event is configured, select Local Settings > Alarm, enable Open Alarm Linkage Video and set how the video will be opened, As Pop-up or Open in Live View. For details, see "8.4.4 Configuring Alarm Settings".
Event Recording	The platform will record videos when an alarm is triggered. It will be saved to the video disk of the platform.

Parameter	Description
Stream Type	Define the stream type of the recorded video. If you select main stream, the recorded video will be in higher quality than sub stream, but it requires more storage.
Recording Time	The duration of the recorded video.
Prerecording Time	When there is recorded video that is stored on the device or platform before the alarm is triggered, the platform will take the defined duration of that video, and then add it to the alarm video. For example, when the prerecording time is set to 10 s, then the platform will add 10 s of video before the alarm is triggered to the alarm video.  For how to configure the pre-recording mode for devices in batches, see "4.1.3.3 Configuring Alarm Video Pre-Recording".  ◇ If the alarm video is stored on the device, we recommend you configure a 24-hour recording plan to make sure that there is prerecorded content to add to the alarm video. ◇ If the alarm video is stored on the platform, the platform will record videos and use certain input bandwidth continuously. ◇ This parameter is not applicable to alarms in parking lots and combined alarms.

- To trigger a snapshot, enable **Trigger Snapshot**. The platform takes 1 snapshot, and save them to the Image and File disk.

Select a video channel, and then it will take a snapshot when an alarm is triggered.

- To link a PTZ action, click **Link PTZ**, and then select the PTZ channels and presets to be linked.
- Click **Alarm Output**, select an alarm output channel, and then set the duration. The channel will send out alarm signal when an alarm is triggered.
- To link audio and light, click **Link Audio and Light**, select the audio and light channels, and then select the action duration.
- Click **Link Access Control Device**, select door channels, and then select a linked action. When an alarm is triggered, the door channels you selected will be locked, unlocked, normally open or normally closed.
- Display the live video of specified channels on a video wall when alarms are triggered.

Click **Link Video Wall**, and then select the channels and video wall.



You must add a video wall and configure its alarm on video wall mode first. For details, see "5.1.5.1 Configuring Video Wall" and "4.1.3.2 Configuring Alarm on Video Wall".

If you set **Camera** to **Select Camera**, you can configure which channels to be displayed on the specified video wall. When the video wall you select is configured with the override mode, you can also select **Customize Alarm Window**, and then you can select which channels to be displayed on the specified windows of the video wall.

- Link one or more IP speakers to play the defined audio files when an alarm is triggered.

Enable **Link IP Speaker**, and then select one or more IP speakers and the audio files to be played.

- To execute an HTTP URL command, enable **Link HTTP URL Command**. Click **Add**, and then click **New** to add a new command, or **Copy from Quick Command**. When

adding a new command, you need to set the name of the command, the request method, HTTP URL, and remarks. You can click  to test if the command is valid.



When selecting **POST** or **PUT**, you can click  to customize the body of HTTP URL.

- To link emails, enable **Email**, and click  to add the email address, and then an email will be sent to the selected email address when an alarm is triggered. You can also manually enter an email address, but you must press Enter to make it valid.

To configure the email template, select **Add Email Template** from the **Email Template** drop-down list.

- To link client sound, enable **Client Sound**, and then enter the audio content (up to 50 characters). When an alarm is triggered, the client will play the defined audio content.

Make sure that **Play Audio Defined in Scheme** is selected from **Local Settings > Alarm > Alarm Sound**.



Click , and then you can test playing the defined audio content.

- Enable **Event Transferral**, and then select the project. The platform will send device statuses, events, and more to the third-party system.



You need to configure the project first from  > **Synthesis > Event Transferral**. For details, see "4.15.1 Event Transferral".

Step 7 Apply an alarm protocol to help users process alarms when they are triggered.

Click **Alarm Protocol**, and then select a protocol from the **Protocol Template** drop-down list, or you can click **Add protocol template** to create a new protocol.



You can enter the website address in the body of the template, so that the corresponding website can be opened quickly when an alarm is triggered. Separate the website address with space and line break.

Step 8 Select users or user groups who will receive the notification when an alarm is triggered.

The users will only receive notifications when they are logged in. If you need to add more users, see "3.2 Adding Roles and Users"; to add more user groups, see "3.2.3 Adding a User Group".



If the page becomes too long because you need to configure many parameters, you can use the pane on the right to quickly go to different positions.

Step 9 Click **OK**.

4.1.2 Configuring Combined Event

Configure the relation between the time of trigger of 2 events, and then you can configure what actions to performed when the event is triggered.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Event > Combined Event Rule Config**.

- Step 2** Click **Add Combined Event Rule** to add a rule for combined events.
- Step 3** Enter a name for the rule, and then configure the details.
For example, select **Event B** occurs and configure the **X** and **Y** to be 10 and 50 seconds respectively. If event B occurs during the 10 seconds to 50 seconds after event A occurs, a combined event is triggered, and then the platform will perform defined linked actions.
- Step 4** Click **OK**.
The previous page displays.
- Step 5** Click **Add**, and then configure the parameters of the combined event.

Table 4-4 Parameter description

Parameter	Description
Basic Info	Define the name for the combined event, and then set the remarks.
Combined Event Rule	Select a rule.
Source of Combined Event	Select the event and event source for event A and B.

- Step 6** Click **OK**.

Related Operations

Configure the linked actions for the combined event. For details, see the previous section.

4.1.3 Configuring Alarm Parameter

4.1.3.1 Filtering Repetitive Alarm

If certain alarms are frequently triggered, you can configure an interval during which they can only be triggered once. For example, a tripwire alarm can only be triggered once in 10 seconds.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Event** > **Alarm Config** > **Alarm Storm Config**.
- Step 2** Click **Add**.
- Step 3** Select event sources and events, and then configure the interval.
- Step 4** Click **OK**.

4.1.3.2 Configuring Alarm on Video Wall

When an alarm is triggered, the live video of a channel can be linked to a window on a video wall. The platform supports override and loop modes.

Prerequisites

You must add a video wall first. For details, see "5.1.5.1 Configuring Video Wall".

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Event** > **Alarm Config** > **Alarm on Video Wall**.
- Step 2** Click .
- Step 3** Select a mode, and configure related parameters.

Table 4-5 Parameter description

Parameter	Description
Alarm on Video Wall Mode	● Override mode: When an alarm occurs, a live video is opened on the specified window of a video wall. For example, if the live video of channel 1 is opened on window 1, another alarm is triggered. The platform will display the live video of channel 2 on window 1. ● Loop mode: Linked live videos will be displayed on windows of a video wall according to the order of windows. If there are no available windows, the first window will be used. The number at the end of the name of a window indicates its order. For example, window (2) indicates it is the second window.
Stay Duration	In either mode, if no other alarms are triggered, the current video will be closed after the stay duration. If a new alarm is triggered: ● In override mode, the stay duration of the new video start from the time when the alarm is triggered. It will be displayed on the window after the stay duration of the current one ends. For example, the stay duration is set to 30 s. An alarm is triggered when video 1 is being played for 15s. At 30 s, video 1 will be closed, and video 2 will be played. After 15 s, video 2 will be closed. ● In loop mode, a new video will be displayed immediately even if the stay duration of the current video does not end.
The latest alarm video will immediately override the one that is currently playing on the video wall.	This parameter is only available for override mode. After enabled, the stay duration will not work, and new videos will be displayed immediately.

Step 4 Configure the size, location, and other parameters of a window.

Table 4-6 Parameter description

Parameter	Description
Set the number of windows	There is only 1 window by default. Click it, and then you can set the number of windows to 4, 9, 16, 32, or 64.

Parameter	Description
Resize a window	- Click a window, and then drag its frame near the lower-right corner to resize it.  - Right-click a window and then select Properties. Configure the left margin, top margin, width, and height to resize the window.
Adjust the locations of windows	Drag the windows to adjust their locations. This operation will not change the order of the windows. The order is used to determine which window will be used to display videos first in loop mode. The number at the end of the name of a window indicates its order. For example, a window named Window (2) means that it is the second window.
Change the names of windows	- Right-click a window, and then select Rename to rename a window. - Right-click a window, select Properties, and then rename it in Window Name.

Step 5 Click **OK**.

4.1.3.3 Configuring Alarm Video Pre-Recording

You can configure the pre-recording mode for a device. When an alarm is configured to link pre-recording from a device, the device will apply the mode you have specified.

Background Information

Pre-recording modes include **Platform Cache** and **Get from Device**.

- Platform cache: Alarm videos will be stored on the platform, the platform will record videos and occupy certain input bandwidth continuously.
- Get from device: Alarm videos will be stored on the device. We recommend you configure a 24-hour recording plan to make sure that there is prerecorded content for the time of alarms.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Event** > **Alarm Config** > **Alarm Video Pre-recording**.
- Step 2 Click an organization, and then all devices and channels in that organization will be displayed on the right.
- Step 3 Configure the pre-recording mode.
- Click  of a channel, select a mode, and then click **OK**.
 - Select multiple channels, click **Edit**, select a mode, and then click **OK**.

4.1.4 Configuring Generic Event

Defines a generic event where a third-party hardware or software can send simple strings to the system through an IP network, so that alarms or corresponding linkage actions can be triggered in the system.

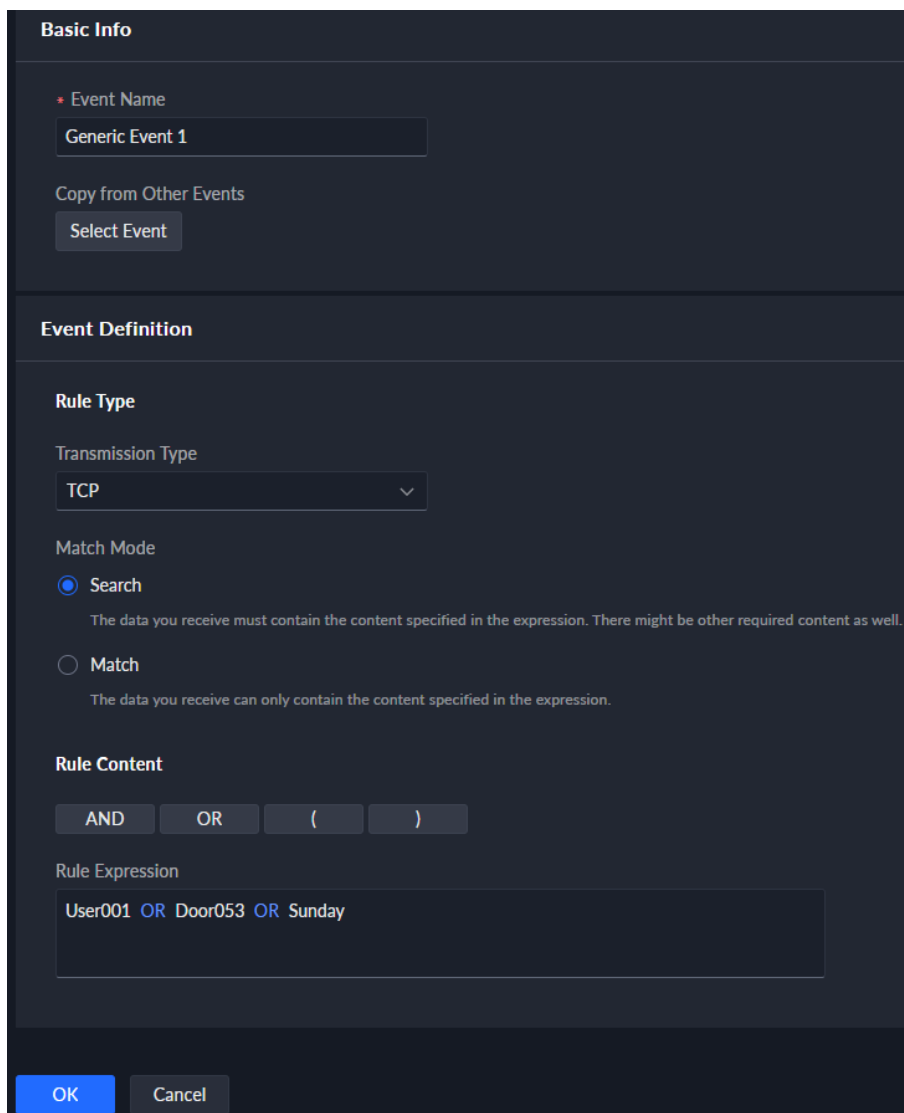
Prerequisites

To ensure system security, go to  > **System Parameters** > **Security Config**, add the IP address to the allowlist in the **Generic Event Allowlist** section.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Event** > **Generic Event Config**.
- Step 2** Click **Add**, and then you can start adding the generic event.

Figure 4-1 Add generic event



Basic Info

• Event Name
Generic Event 1

Copy from Other Events
Select Event

Event Definition

Rule Type

Transmission Type
TCP

Match Mode

☒ Search
The data you receive must contain the content specified in the expression. There might be other required content as well.

☐ Match
The data you receive can only contain the content specified in the expression.

Rule Content

AND OR ()

Rule Expression
User001 OR Door053 OR Sunday

OK Cancel

Table 4-7 Parameter description of generic event

Parameter	Description
Event Name	The name that identifies the event.
Select Event	Click Select Event , select from the existing generic event, and then the system automatically fills in parameters of the selected event (event name excluded).
Transmission Type	TCP, UDP, HTTP, and HTTPS are available.
Match Mode	Select Search or Match according to onscreen instructions.
Rule Content	Select AND , OR , (,) rules, and then set the rule expression. The system operates the expression from left to right.
Rule Expression	Select AND, OR, and () operations and set the expression. The system operates on expressions from left to right.  AND and OR must be preceded and followed by characters; (and) must appear in pairs. - Rule expression supports HTTP URL, for example, <code>http://192.168.1.1:9090/test/Keywords/Newwords/Header/Body xxxxxxxxxxxxxxxxx</code>.

Step 3 Click **OK**.

4.2 Configuring Map

4.2.1 Preparations

- Devices are deployed. For details, see device user manuals.
- Basic configurations of the platform have been finished. For details, see "3 Basic Configurations".
- If you need to use a raster map, prepare an image of the map.
- To show device alarms on the map, make sure that **Map flashes when alarm occurs** is enabled in **Home > Management > Local Settings > Alarm**.

4.2.2 Adding a Map

The platform supports adding raster and vector maps.

4.2.2.1 Adding a Vector Map

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Map**.

Step 2 In the map list, select the vector map, and then click .

Figure 4-2 Map

←

Modify Vector Map

Basic Info

Map Mode

Online

Offline

Import Offline Google Maps

Import

Supports .zip. The file must not exceed 1G.

Map Initial Status

* Central Latitude of Map

.1892863586331

* Central Longitude of Map

.178299258354

* Min Map Display Level

1

* Max Map Display Level

21

* Map Initial Zoom Level

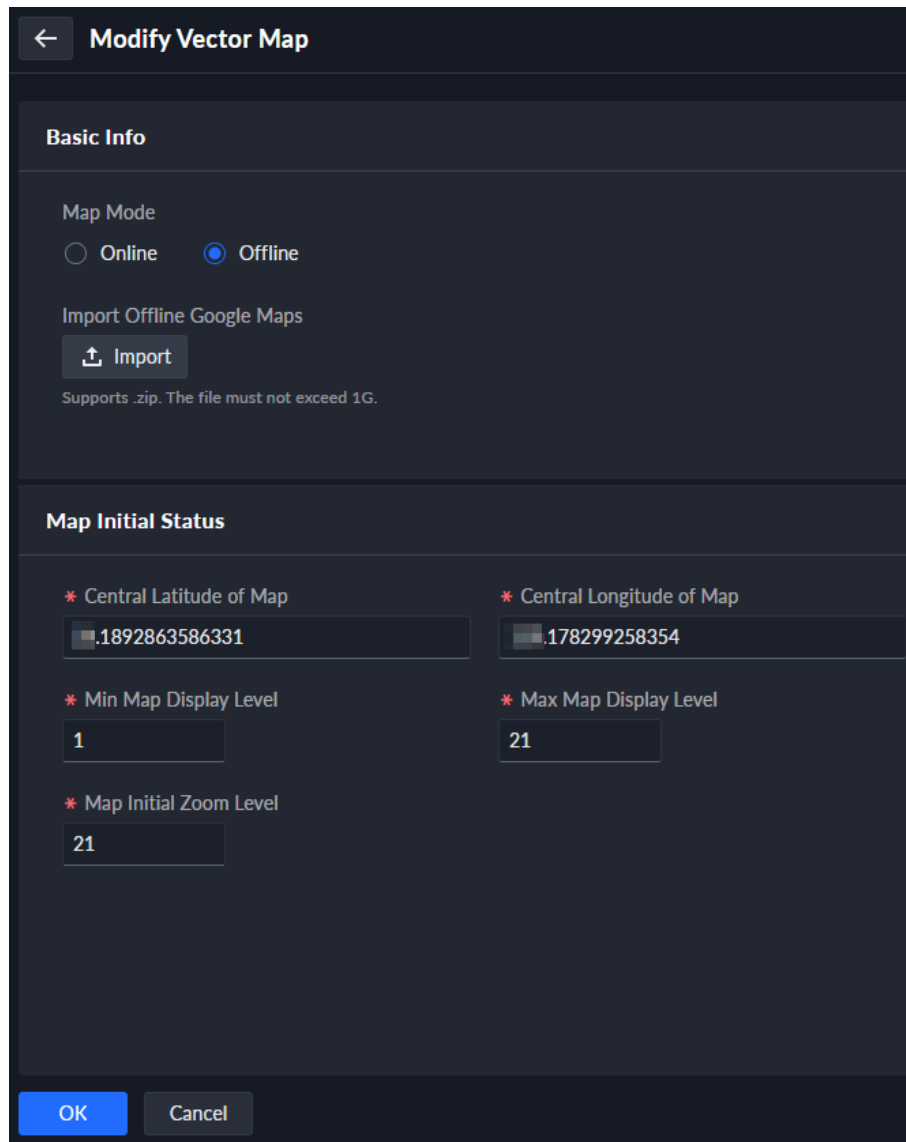
21

OK

Cancel

Step 3 Configure the parameters.

Figure 4-3 Map information



- Online map
 1. Select **Online**.
 2. Configure the information of the map, and then click **OK**.
- Offline map
 1. Select **Offline**.
 2. Click **Import** and import offline map.
 3. Configure map information, and then click **OK**.

Table 4-8 Parameter description

Parameter	Description
Map Link	Enter the URL of the map. Only Google Maps is supported.
Central Latitude of Map	Define the center of the map by entering its latitude and longitude. When opening the map, this will be the center of the map by default.
Central Longitude of Map	

Parameter	Description
Min Map Display Level	The minimum level you can zoom out on the map. The lower the level is, the map will contain more areas, but less details. The higher the level is, the map will contain less areas, but more details.
Max Map Display Level	The maximum level you can zoom in on the map. The lower the level is, the map will contain more areas, but less details. The higher the level is, the map will contain less areas, but more details.
Map Initial Zoom Level	The default zoom level when opening the map. The lower the level is, the map will contain more areas, but less details. The higher the level is, the map will contain less areas, but more details.

Step 4 Add a sub map.

If there is a specific area on the map that you want to view its detailed information, you can add an image of it on the map as a sub map. For example, you can add a plane image of a parking lot on the map.

1. On the map resource tree on the left, click the name of the map that you have just added, or open the GIS map and click **Add Sub Map**.
2. Name the sub map, upload a map image, and then click **OK**.
3. Drag the map to adjust its position, and then click **OK**.

The sub map is added.

Related Operations

Click the image of the added map, and then you can:

- View device details

Click a device on the map, and then click  to view device name and organization; click the icon again to hide the name and organization.

- Show device

Select which type of resources that you want to display on the map.

- Move

To move a device, click **Move** and then drag the device on the map.

- Configure static visible range

For devices that do not support sending visible range to the platform, you can customize the visible range on the map. After that, when you monitor or track back a target, you can quickly find the monitoring devices according to the visible range.

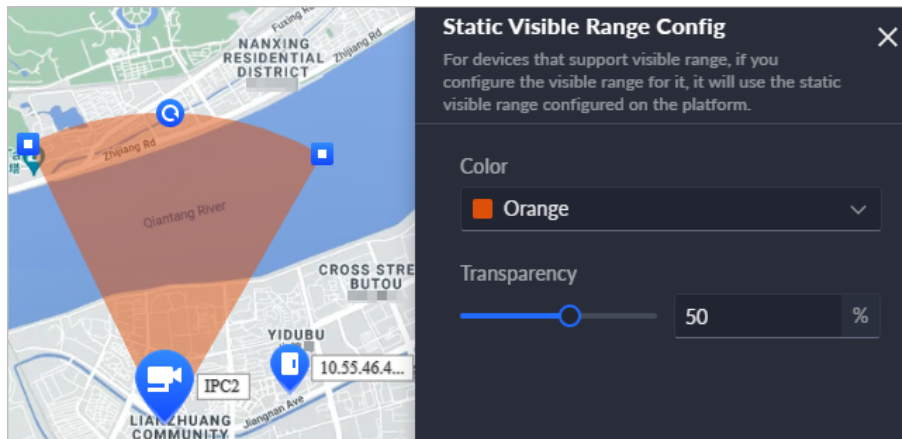


For devices that support dynamic visible range (for example, PTZ camera), if static visible range is configured at the same time, refer to the static visible range.

Click the device on the map, click  to configure the color and transparency of the static visible range, and then click **OK**.

You can drag  to adjust coverage, and drag  to enlarge or reduce the distance.

Figure 4-4 Configure static visible range



- Delete devices
 - ◇ Select **Selected** > **Checked**, click a device on the map, and then click .
 - ◇ Select **Selected** > **Rectangle**, draw a rectangle on the map. A device list covered by the rectangle is displayed. Select the devices, and then click .
- Hide device names

Select **Display Settings** > **Hide Device Name**, and then only the icons of devices will be displayed.
- View the satellite map

Select **Display Settings** > **Satellite Map**, and then the satellite map will be displayed.
- Point clustering

Select **Display Settings** > **Point Clustering**, the system clusters adjacent channels into one point according to the map scale, and identifies the number of channels with numbers.
- Clear

To clear all markings on the map, click **Clear**.
- Add a sub map

To add a sub map on the current map, click **Add Sub-map**, click on the map to locate it, enter a name, upload a map picture, and then click **OK**.

 - ◇ Click  to edit the sub map.
 - ◇ Double-click  to go to the sub map page, where you can drag channels to the sub map.
- Length

Select **Box** > **Length**, connect 2 points with a line on the map (double-click to finish drawing), and then the distance between the points is shown.
- Area

Select **Box** > **Area**, select a region on the map (double-click to finish drawing), and then the area is measured.
- Add Mark

Select **Box** > **Add Mark**, and then mark information on the map.
- Reset

Select **Box** > **Reset** to restore the map to its initial position and zoom level.

4.2.2.2 Adding a Raster Map

A raster map is suitable for places where you want to view their detailed information, such as a parking lot. You can add multiple ones.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Map**.
- Step 2** Select **Main Map**, and then click **Add Map**.
- Step 3** Enter the map name, select the image and then click **OK**.
- Step 4** Add a sub map.
 1. Click the added raster map, and then click **Add Sub Map**.
 2. Enter the map name, upload the image, and then click **Next Step**.
 3. Drag the image to the desired position and click **OK**.

Related Operations

For details, see "4.2.2.1 Adding a Vector Map".

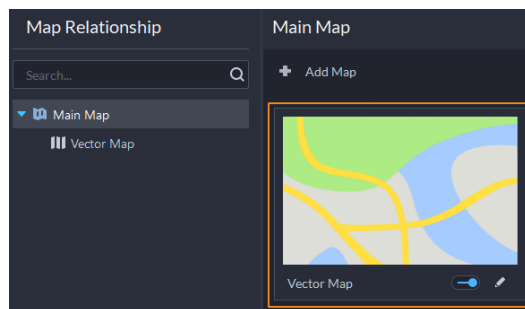
4.2.3 Marking Devices

Link a device to the map by dragging it to the corresponding location on the map according to its geographical location.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Map**.
- Step 2** Click the map.

Figure 4-5 Map



- Step 3** Drag the device channel from the left device tree to the corresponding location of the map.



If you mark a radar on the map, you can configure the radar-PTZ linkage function. For details, see "4.2.4 Configuring Radar-PTZ Linkage".

4.2.4 Configuring Radar-PTZ Linkage

A radar can meet most security needs because it can penetrate fog, smoke, and dust. After a target is detected by the radar, you can view real-time videos of PTZ cameras to understand the situation better and faster.

Before configuring the function, you must complete the following configurations first:

- The radar and PTZ cameras are directly added to the platform through their IP addresses. Also, they must be on the same network, or different networks that can connect to each other. One radar can link up to 8 PTZ cameras.
- Configure a vector or raster map. If you use a raster map, you must configure the map scale so that the alarm area and detection area of the radar can be displayed normally.
- If you also need to monitor the area around the radar, you can bind it with video channels. For details, see "3.1.3 Binding Resources".

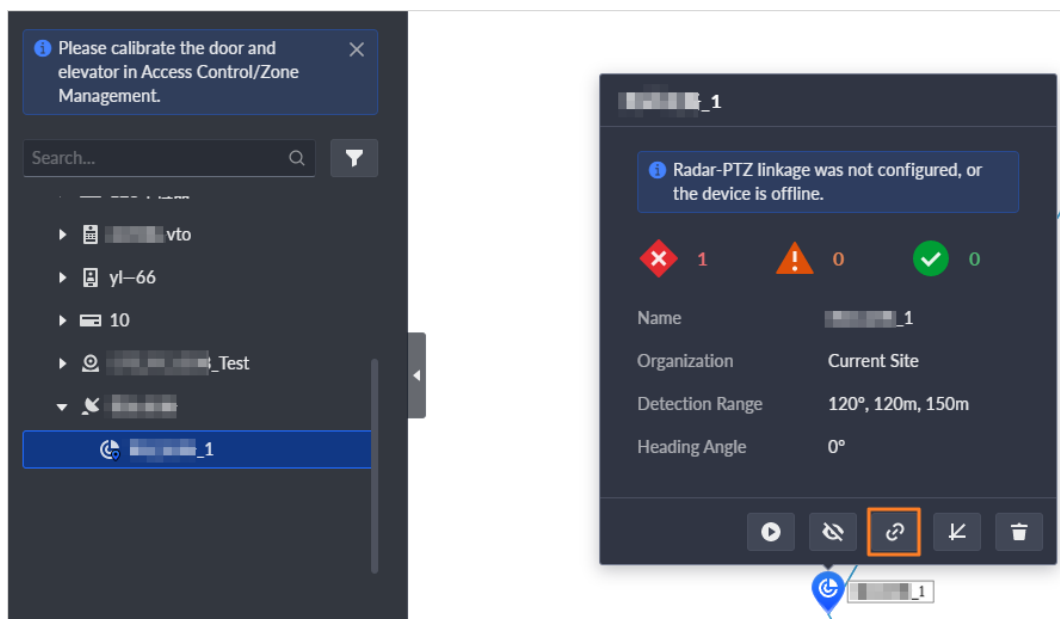
4.2.4.1 Configuring Linkage

Configure the linkage between the radar and PTZ cameras. When an alarm is triggered, PTZ cameras will track the target. Operations on a vector map or raster maps are similar, and this section uses vector map as an example.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Map**.
- Step 2** Click the vector map to open it.
- Step 3** In the device tree on the left, drag the radar channel to the map.

Figure 4-6 Select radar from device tree



- Step 4** Click , and then configure the parameter.
1. In the device tree, select one or more PTZ cameras to be linked to the radar.


If you already configured related parameters on the webpage of the radar, the platform will automatically obtain the information of the PTZ cameras. Click **Bind** to save the linkage relationship and skip the following steps.
 2. Click **Bind and Configure** to save the linkage relationship, and then go to the webpage of the radar.
 3. On the webpage of the radar, configure the parameters related to radar-PTZ linkage, such as upload an image of the map, set the position and heading angle of the radar, and, calibrate the PTZ cameras. For details, see the user manual of the radar.

4.2.4.2 Configure a Radar Event

Configure an event so that an alarm will be triggered after a target enters the warning area and alarm area of the radar, and then the platform will perform the defined linkage actions, such as taking a snapshot.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Event** > **Event Config**.
- Step 2** Click **Add**, and then configure the parameters. For details, see "4.1.1 Configuring Event Linkage".

4.3 Personnel and Vehicle Management

Configure personnel and vehicle information for the applications of access control, vehicle control, and video intercom.

- Personnel information contains card number, password, face image, and more. People bound with vehicle information will be displayed in the vehicle list.
- Vehicle information helps to confirm the entry of the vehicle into a certain area. Vehicle bound with personnel information will be displayed in the personnel list.

4.3.1 Adding Person and Vehicle Groups

Add person and vehicle groups to easily manage people and vehicles. People and vehicles use the same groups. Only administrators can add, edit, and delete person and vehicle groups.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Person and Vehicle Info**.
- Step 2** Click **Person List** or **Vehicle List**.
- Step 3** Click , and then configure the parameters.

Table 4-9 Parameter description

Parameter	Description
Parent Group	This is for permission control. For example, if a user has permissions for group A, then the user will also have permissions for all groups under group A; if not, the user can also edit the permissions of the groups under it to have permissions for selected roles.
Group Name	Enter a name for the group.
Roles Allowed Access	Only the roles and their users can view this group.  • Administrators have the permissions of all person groups by default. For customized roles, administrators can configure permissions for them of the corresponding groups. • Click  to view the users assigned with the roles.

- Step 4** Complete configuration.

- Click **Add** to add the group and exit the page.
- Click **Save and Add Person** to add people to the group. For details, see "4.3.2 Configuring Person Information".

Related Operations

- Edit person and vehicle group: Click  to edit the group name and the roles allowed to access. Group permissions are updated after editing.
Administrators have permissions for all groups by default. Roles without permissions can see the group in the tree on the left, but the group icon is grayed out, and the roles cannot view the people under the group.
- Delete person and vehicle group: Click , and then enter the login password. The group and its sub groups, and also people in all these groups are deleted from the platform.
- Clear person and vehicle group: Select **Include Sub Groups**, click , and then enter the login password to delete people in the current group and its subgroups; if **Include Sub Groups** is not selected, only the people in the current group will be deleted. The people in the sub groups will not be affected.

4.3.2 Configuring Person Information

Add people to the platform and grant them access to different access control devices, entrance and exits permissions, and more.



To collect fingerprints or card number, connect a fingerprint collector or card reader to the computer where the PC client is installed.

4.3.2.1 Extending Person Information

You can customize more information you want to configure for persons. If existing information is not enough, you can add more information for a person. This function is available to administrators. Others users can only configure information for attributes that have been added. You can add up to 10 attributes.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Person and Vehicle Info**.
- Step 2 Select **Person List** > **More** > **Enable More Info**.
- Step 3 Click **Add**, enter a name for the attribute, and then click **OK**.

This attribute will be displayed in the **Basic Info** section of a person's information.

Figure 4-7 More information

Person Info

Basic Info

* ID

28162378

Linked ID ⓘ

--

* Name

111222333

Gender

Unspecified

Person Group

All Persons and Vehicles

Phone No.

ID Type

Others

Company

Position

Email

Address

ID No.

Department

customer1

customer2

Add



If you change the name of the attribute or click  to disable it, the information you have configured will still be on the platform. But if you click  to delete the attribute, the information you have configured will also be deleted and cannot be recovered.

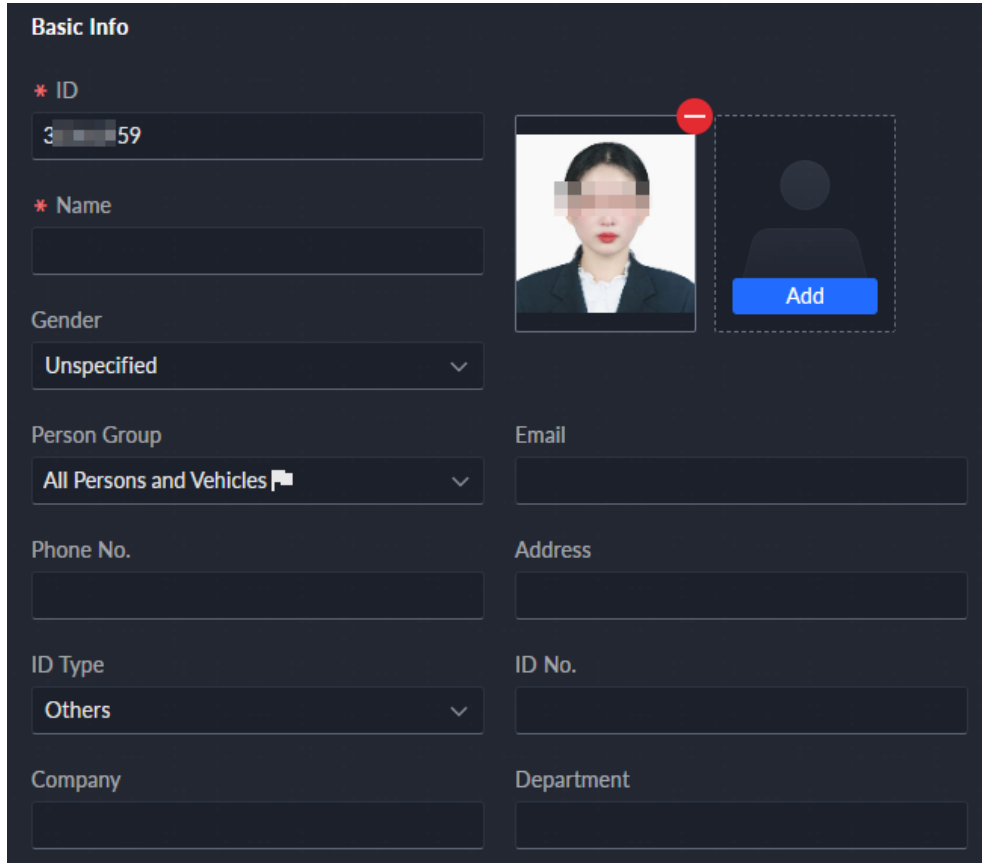
4.3.2.2 Adding a Person

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Person and Vehicle Info**.
- Step 2 Select **Person List** > **Persons** > **Add**.
- Step 3 Click **Person Info**, and then configure the information of the person.
 - Configure the basic information.

1. Hover over the profile, select **Add** > **Select from Local Folder**, and then follow the on-screen instructions to upload an image from your computer. Or if your computer is connected to a camera, you can select **Add** > **Snapshot** to take an image.

Figure 4-8 Basic information



Basic Info

* ID
3 59

* Name
[Text Field]

Gender
Unspecified

Person Group
All Persons and Vehicles

Email
[Text Field]

Address
[Text Field]

Phone No.
[Text Field]

ID Type
Others

ID No.
[Text Field]

Company
[Text Field]

Department
[Text Field]

Profile Picture: [Image] [Add]

- When taking a picture with a camera, click , and then you can select a camera, pixel format, resolution, and image quality. These parameters are only effective on the current PC client.
- You can upload or take 2 images for better recognition results. Only certain devices support this function. The 2 icons under the images indicate the first and second images. If the icon is in blue, it means the corresponding image is selected.



You can import images for multiple people at the same time. For details, see "4.3.2.6 Importing Images of People".

2. Enter the information of the person as necessary.
 - The ID is required and must be unique. It can be up to 30 characters, and letter-number combination is also supported.
 - The name of the person can be up to 127 characters.
 - The person can be added to up to 20 person groups. Click  to set one as the main person group, which will be used in attendance shift.
3. (Optional) Click **Show More**, and then enter the information of the person.



The nickname will be used in the contact information for VTOs.

- Configure the verification information for unlocking doors or using lifts.

Table 4-10 Parameter description

Parameter	Description
Card	1. Click Setting, select a device to issue cards, and then click OK. 2. Click , swipe a card on the device you select, the card number will be recognized and displayed. Or manually enter the card number.  One person can have up to 5 cards. A card number comes with 8–16 numbers. Only second-generation access control devices support 16-digit card numbers. When a card number is less than 8 numbers, the system will automatically add zeros prior to the number to make it 8 digits. For example, if the provided number is 8004, it will become 00008004. If there are 9-16 numbers, the system will not add zero to it. 3. Click . 4. (Optional) Click  to add more cards. You can add up to 5 cards for each person. After adding a card, you can: ◇ : Set a card as duress card. When opening door with a duress card, there will be a duress alarm. Click this icon, it turns into , and  is displayed at upper right, which indicates that the card is set as a duress card. To cancel the duress setting, click . ◇ : Update the card number. ◇ : Remove the card, and then it has no access permissions.
Fingerprints	1. Click Setting, select a fingerprint scanner, and then click OK. You can select from fingerprint scanner and device (VTO, access control device) for the fingerprint collector. 2. Click Add, and then follow the on-screen instructions to collect your fingerprint on the scanner. 3. Click Add Fingerprint. 4. (Optional) Click Add to add more fingerprints. You can add up to 3 fingerprints for each person. After adding a fingerprint, you can: ◇ : Set the fingerprint as the duress fingerprint. When opening doors with the duress fingerprint, there will be a duress alarm. Click this icon, it turns into , which indicates that the fingerprint has been set as the duress fingerprint. Click it again to reset the duress fingerprint as a normal one. ◇ : Change the name of the fingerprint. ◇ : Delete the fingerprint, and then it has no access permissions.

Parameter	Description
Password	The password must be used with a card, person ID, or fingerprint to unlock the door. For details, see the user manual of the access control device you are using. Click , enter a password, and then click . After adding a password, you can: ◇ : Change the password. ◇ : Delete the password, and then it has no access permissions.

- If the person has one or more vehicles, click **Vehicle** to add their information to the platform.
 - ◇ If the vehicles have been added to the platform, click **Select from Vehicle List**, and then select the vehicles for this person.
 - ◇ If the vehicles have not been added to the platform, click , enter the plate number, and then select a color and brand.

Step 4 If the person is a resident, click **Video Intercom**, and then configure the room information.

Table 4-11 Parameter description

Parameter	Description
Room No.	The number of the room this person lives in. It is displayed in the access records and video intercom operation records.
Homeowner	When several people live in the same room, you can set one of them as the homeowner. Only the homeowner can register an account on DSS Agile VDP.
App User	This function is only available for the homeowner. After you select the option, you must enter an email address for the person. It will be used as the username for the person to log in to DSS Agile VDP. After the person is added, the platform will send the username and password to the email address. If the person does not receive the email, you can click Send Email to send a new email.  The person can log in to DSS Agile VDP, and then go to Me > My QR Code to view the QR code. The QR code is valid for 10 minutes. After the QR code expires, the person can tap the QR code to refresh it, or exit the current menu and reopen it to automatically refresh it.  If you cancel selecting this option after an App account is created for the person, the App account will be deleted. This person can no longer log in to the App. If this person is a homeowner, all App accounts in the corresponding room will be deleted, and all people in this room can no longer log in to the App.

Step 5 Click **Access Control**, and then configure the access permissions for this person.

1. Select an access type.

- **General:** When the person uses an access point, a general event is reported. The person is restricted by door mode, combination unlock (card, fingerprint, face, and password), unlock by period, and all types of access rules.



- ◇ Door mode, combination unlock (card, fingerprint, face, and password) and unlock by period can be configured by selecting  > **Device** > **Device Config**, clicking **Channel** to filter the access control channel, and then selecting  > **Door Config**.

- ◇ Access rules can be configured from  > **Access Control** > **Access Rule** > **All Rules**.

- **VIP:** When using an access point, the person is restricted by all rules except combination unlock (card, fingerprint, face, and password), multi-person unlock, and unlock by period rules.



- ◇ Combination unlock (card, fingerprint, face, and password) and unlock by period can be configured by selecting  > **Device** > **Device Config**, clicking **Channel** to filter the access control channel, and then selecting  > **Door Config**.

- ◇ Multi-person unlock and other rules can be configured from  > **Access Control** > **Access Rule** > **All Rules**.

- **Patrol:** When the person uses an access point, a patrol event is reported, and the door will not open.
- **Blocklist:** The person cannot use an access point. Also, a blocklist event is reported. People in blocklist are subject to the global anti-passback rules.
- **Extend time:** When the person uses an access point, if the access point is a door, the door will stay unlocked for additional 5 seconds.

2. Configure validity period. The person is only effective within this period. You can modify the value to extend the validity period.

3. Select **Quote** > **Add**, and then configure the access rules.

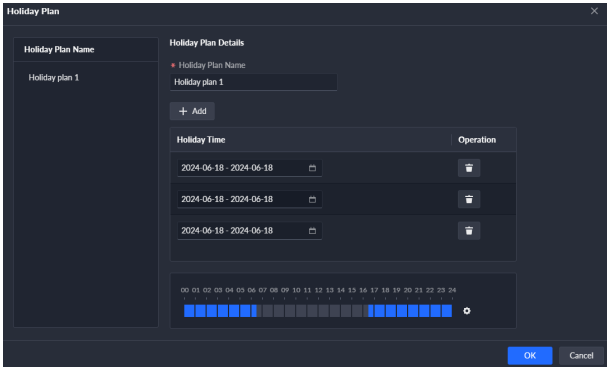


If you already added access rules of general verification, this page will display them for you to select.

Figure 4-9 Available access rules

General			
 Add		Rule Name 	
☐	Rule Name	Access Point Type	Time Plan
☐	46.39	Door	 All-Period Template
☐	ASI6214S-PW	Door	 All-Period Template
☐	rule_name1786455	Door	 All-Period Template

Table 4-12 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Select Door or Lift .
Time Template	Select a time template to define when the rule will be effective. For how to create a new template, see "3.1.6 Adding Time Template".
Holiday Plan	Select a holiday plan when the rule will not be effective. You can add up to 4 holiday plans. Follow the steps below to create a holiday plan:  Lift does not support holiday plans. - Select Add Holiday Plan in the drop-down list. - Enter a name for the holiday plan. - Click Add to add a holiday. You can add up to 16 holidays. - Configure the effective periods for each day in the holiday. You can drag on the timeline below, or click  to configure the time more accurately. You can add up to 4 periods. - Click OK. 
Select by Zone	Select one or more zones. This person will have access permissions to all the access points in these zones.  For how to configure a zone, see "4.5.2 Configuring Zone".
Select by Access Point	Select one or more access points. This person will have access permissions to all these access points.

4. Click **OK** to finish adding the rule.

5. Select one or more rules for this person, and then click **OK**.

Step 6 If you want to recognize this person by face images, add the person to a face arming group.

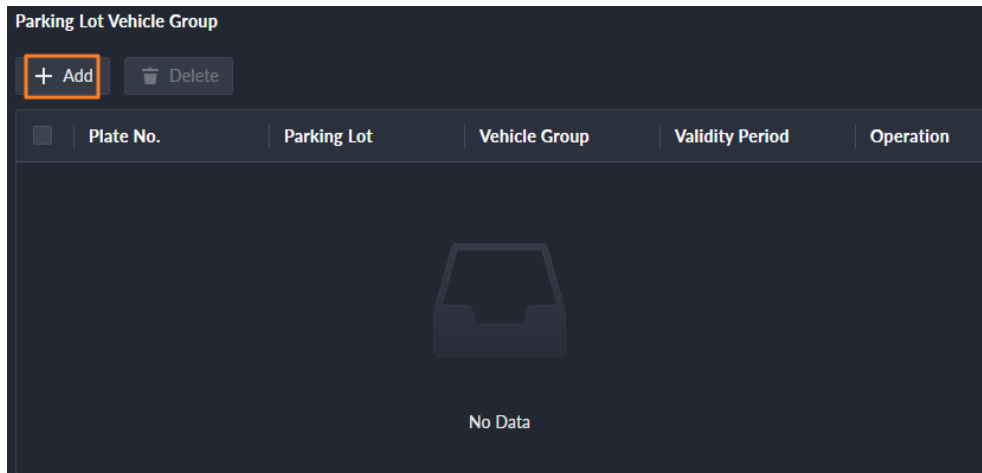


You need to create a face arming group first. To add one, select **Add Face Arming Group** in the drop-down list. For details, see "4.4.1.1 Creating Face Arming Group".

Step 7 If this person has one or more vehicles, you can grant parking lot access permissions to them.

1. In the **Parking Lot Vehicle Group** section, click **Add** to select the license plate number, and then select which one or more vehicle group it belongs to.

Figure 4-10 Parking lot vehicle group



Step 8 Click **OK**.

Related Operations

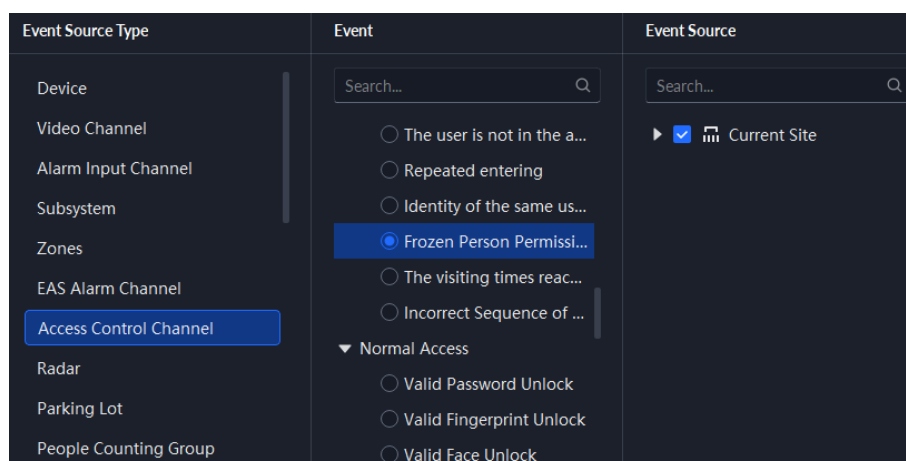
- Click  to edit the basic information of a person.
- Cancel the access permissions of a person

Click  to cancel the access permissions of a person; click  to restore the permissions.



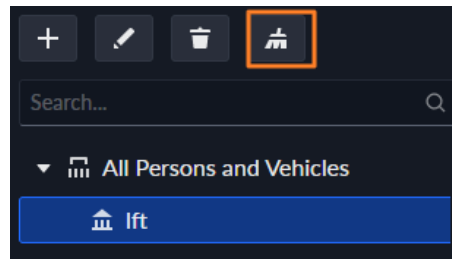
After canceling, if the access control device is configured with **Frozen Person Permissions** from  > **Event** > **Event Config**, an alarm will be triggered if the person is detected trying to access.

Figure 4-11 Configure frozen person permissions event



- To delete a person:
 - ◇ Click  to delete a person and associated permissions.
 - ◇ Select multiple people, and then click **Delete Selected Items** to delete them and associated permissions. If you delete more than 10 persons, you must verify your login password.
 - ◇ Select a person and vehicle group, and then click  to delete all the persons and their permissions in the group. To perform this operation, you must verify your login password.

Figure 4-12 Delete all persons in a group



- : View authorization exception of a person.
- To search for a person, enter keywords in the

If you select **Include Sub Groups**, all the persons in the selected group and the sub groups in this group will be displayed.

4.3.2.3 Importing Multiple People

Prepare the information of the people first, and then you can import them to the platform quickly.

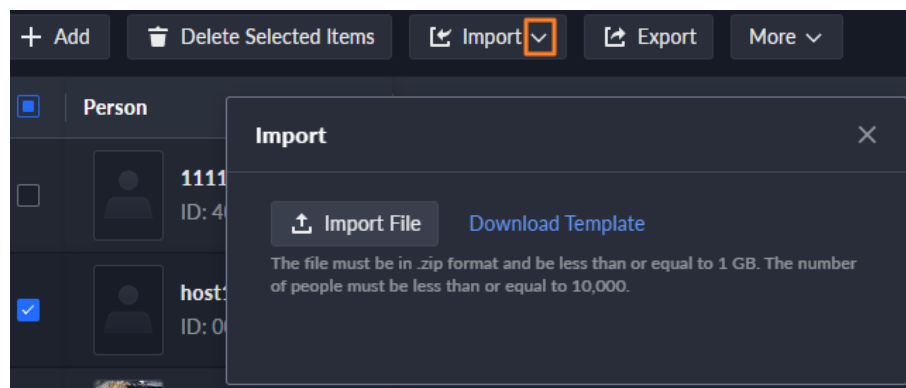
Prerequisites

- Prepare an .xlsx file that includes the information of the people you want to import, their face images (optional), and then compress them into a .zip file. The .xlsx file can include information of up to 10,000 people. The .zip file cannot be greater than 1 GB.
- If a person belongs in a first-person unlock rule, set the access type of the person to **General**.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Person and Vehicle Info** > **Person List**.
- Step 2 Select **Import** > **Import from File**.

Figure 4-13 Import personnel information



- Step 3 Import the person information file.



If there is no personnel information file, click **Download Template** and follow the instructions on the page to create personnel information.

- Step 4 Click **OK**.

The following cases might occur during an import:

- If the person already exists on the platform, you can choose to replace the selected, replace all, or not replace data of the existing person. If you choose not replace, the historical data on the platform will be kept, and the new data will not be imported.
- If there are failures, you can download the failures list to view details.
- Read carefully the instructions in the template to make sure all the information is correct.
- Cannot read the contents with a parsing error reported directly.

Related Operations

- Export person information.

Select an organization, click **Export**, and then follow the instructions on the page to save the exported information to a local disk.

- Import people from device: Select **Import** > **Import from Device**. For details, see "4.3.2.4 Extracting Person Information".
- Import person image: Select **Import** > **Import Person Image**, click **Download Template** to download the template, prepare the images according to requirements in the template, and then click **Import File**.

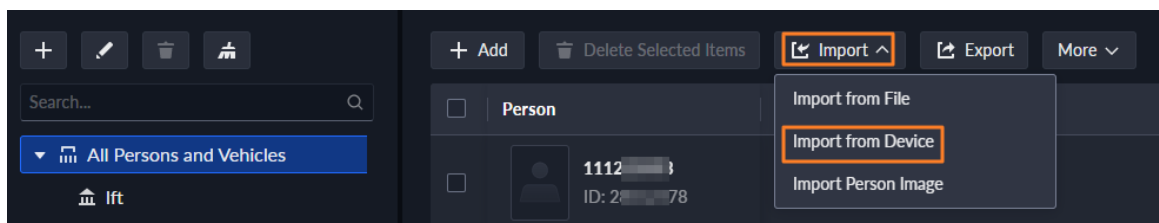
4.3.2.4 Extracting Person Information

When person information has been configured on access control devices or door stations, you can directly synchronize the information to the platform.

Procedure

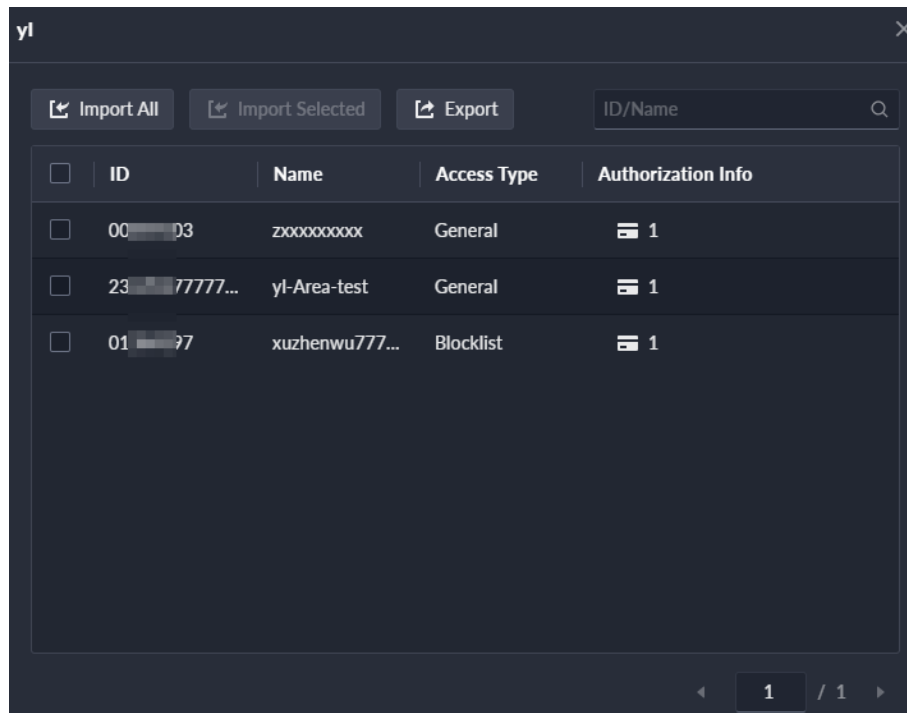
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Personal and Vehicle Info**.
- Step 2** Click **Person List**.
- Step 3** Click **Import**, and then select **Import from Device**.

Figure 4-14 Import from device



- Step 4** Click , select a channel from an access control device or door station, and then click **OK**.
- Step 5** Double-click a result to view the details.
- Step 6** Synchronize person information to the platform, or export information.

Figure 4-15 Personnel extraction results



☐	ID	Name	Access Type	Authorization Info
☐	00...	zxxxxxxxx	General	1
☐	23...	yl-Area-test	General	1
☐	01...	xuzhenwu777...	Blocklist	1

- If the person already exists on the platform, you can choose to replace the selected, replace all, or not replace data of the existing person. If you choose not replace, the historical data on the platform will be kept, and the new data will not be imported.
- To add all the person information to the platform, click **Import All**.
- To add part of the information, select the people of interest, and then click **Import Selected**.
- To export information, select the people that you want, and then click **Export**.

4.3.2.5 Synchronizing People in Domain

Create persons based on the information imported from the domain. Also, the information of the persons can be kept up-to-date with that in the domain.

Prerequisites

Configure the information of the domain. For details, see "7.4.6 Configuring Active Directory".

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Person and Vehicle Info**.
- Step 2 Select **More** > **Sync Person in Domain**.
- Step 3 Import persons in the domain to the specified person group.

Table 4-13 Parameter description

Parameter		Description
Manual Sync	Sync Add	Import all or certain people in the selected domain group to the selected person group on the platform. After importing the entire domain group, the group will be added to the automatic synchronization list. When you import the same entire domain group again, the platform will import the new people and update the existing people.
	Sync Delete	When this option is selected, the platform automatically detects and displays the people that have been deleted from the domain. You can select whether to remove them from the platform.
	Sync Now	- For people imported from an entire domain group, the platform immediately imports the new people or updates the existing people's information. - For people imported by manual selection, the platform immediately updates their information.
Auto Sync		The list holds the domain groups that have been imported entirely. After setting the time, the platform will synchronize the new people and update the information of the existing people every day. For people imported by manual selection, the platform will update their information. Click  to remove the group, the platform will not synchronize the new people, but will still update the information of the existing people.

Step 4 Click **OK**.

4.3.2.6 Importing Images of People

If people are added to the platform but their images have not been configured, you can import images for multiple people at the same time.

Prerequisites

You can upload up to 10,000 images in a zip file that can be up to 1 GB. Also, each image should meet the following requirements:

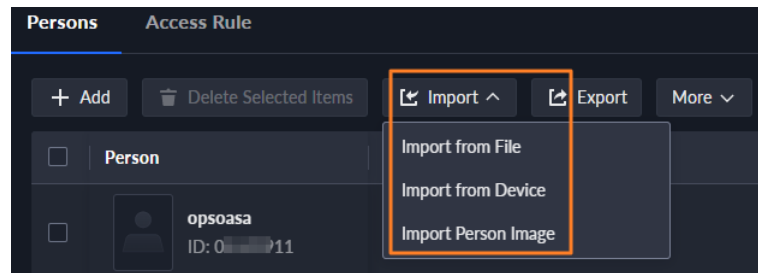
- A person can have up to 2 images, but only certain devices support recognizing people with 2 images.
- The image must be in .jpg format, and has a resolution ranging from 150 × 300 to 540 × 1080. It is preferred that it be 500 × 500. The image must not exceed 100 KB.
- Make sure that there is only 1 face in the image, with proportions between 1/3 and 2/3 of the whole image. The aspect ratio of the image must not exceed 1:2.
- Both eyes should be open with a natural expression. Expose the forehead and the face, and keep the hair away from blocking the forehead and the face. The face shape should be similar to that of the original image.
- Normal light colors should be used (without whitening, yellowing, and backlight). Items should not block the face (such as hat, face mask, and glasses). The image must be processed by Photoshop.

- Use an image with a white background.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Person and Vehicle Info** > **Person List** > **Persons**.
- Step 2** Select **Import** > **Import Person Image**.

Figure 4-16 Import person image



- Step 3** Click **Download Template** to save the zip file to your computer. It contains the instructions on how to prepare images, and 2 images for reference.
- Step 4** Prepare images according to the requirements, and then rename them in the format of **Person ID-Person Name-1**.
1 means the first image of the person. Change it to **2** to make the second image of the person.
- Step 5** Compress the images into a .zip file.
- Step 6** Click **Import File**, and then open the .zip file.
The page will display the number of successes and failures. Click **Download Failure List** to see the reasons for the failures.

4.3.2.7 Moving People in Batches

Move people in batches to another person group. This operation will delete the access rules of the current group, and apply those of the target group on the people.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Person and Vehicle Info** > **Personal List**.
- Step 2** Select a person group, and then the people in this group are displayed on the right.

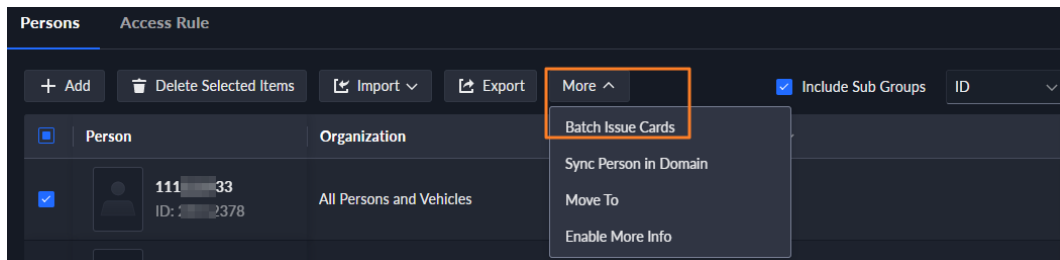
Select **Include Sub Groups** to display all the people in this group and all its sub groups.
- Step 3** Select multiple people, and then select **More** > **Move To**.
- Step 4** Select a target group, and then click **OK**.
- Step 5** Click **OK** again.

4.3.2.8 Issuing Cards in Batches

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Person and Vehicle Info** > **Person List** > **Persons**.
- Step 2** Select the people to issue card to, and then select **More** > **Batch Issue Cards**.

Figure 4-17 Issue card in batches



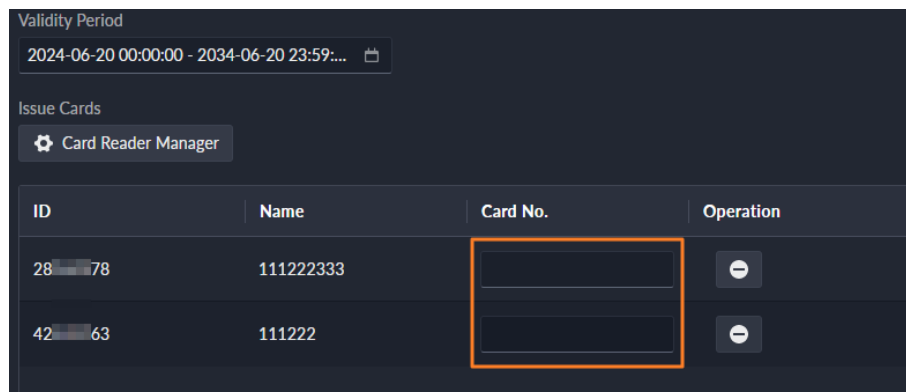
Step 3 Set validity period.

Step 4 Issue cards to personnel.

Support issuing cards by entering card number or by using a card reader.

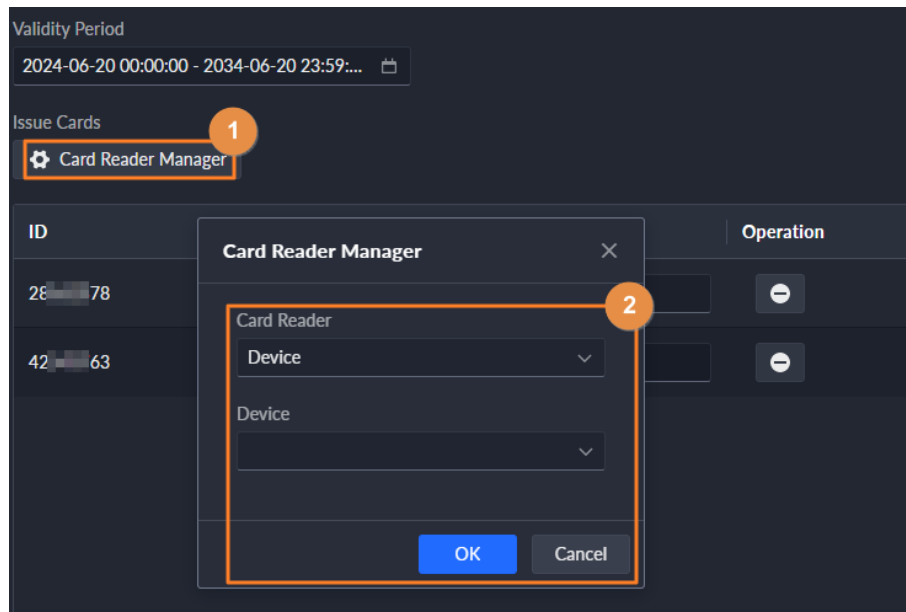
- By entering card number
 1. Double-click the **Card No.** input boxes to enter card numbers one by one.
 2. Click **OK**.

Figure 4-18 Enter card number



- By using a card reader
 1. Click .
 2. Select a card reader or device, and then click **OK**.
 3. Select people one by one and swipe cards respectively until everyone has a card number.
 4. Click **OK**.

Figure 4-19 Reader manager



4.3.2.9 Deleting People

Notes

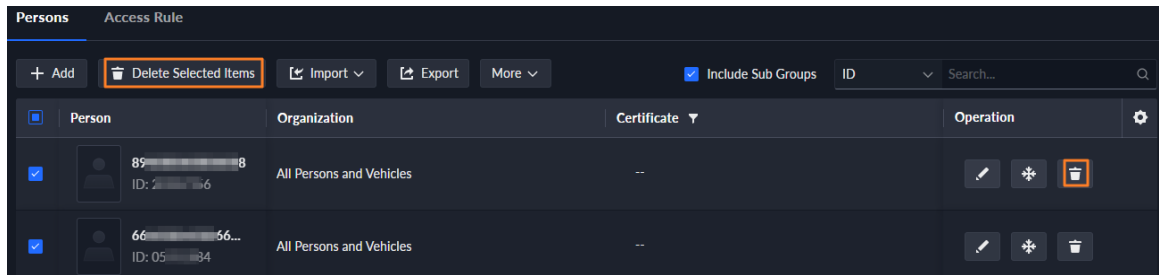
- After deleting people, their permissions (including vehicle access, person access, vehicle arming, person arming and parking lot permissions of vehicles) will also be deleted.
- After deleting people, the vehicles associated with the person will also be automatically deleted. After deleting a vehicle, the relationship between the person and the vehicle information will be unbound.
- If the deleted person belongs to the main person group, the person in the sub-person group will also be deleted; if the deleted person belongs to the sub-person group, the person will not be deleted in the main person group.

Operations

- Delete a person: On the **Person List** page, click  of a person, and then you can delete the person and the permissions according to prompts.
- Delete people in batches: On the **Person List** page, select multiple people, click **Delete Selected Items** to delete the selected people and their permissions according to prompts.

A maximum of 100 people can be deleted in batches at a time. When deleting more than 10 people, you need to enter the login password.

Figure 4-20 Delete people



4.3.2.10 Editing Person Information

You can modify person information including basic information, authentication details, and authorization. Person ID cannot be modified.

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Personal and Vehicle Info** > **Person List** > **Persons**.

Step 2 Click  to edit information. For details, see "4.3.2.2 Adding a Person".

After editing person information, their permissions are automatically updated. For example, after the validity period of the access rule is updated from December 1, 2024–June 1, 2025 to December 1, 2024–December 31, 2025, the corresponding lift control, credentials and video intercom permissions of the person will also be extended to December 31, 2025.

4.3.2.11 Searching for and Filtering People

View certain people and their information by searching for keywords or filtering the type of information to be displayed, such as ID, name, card number, ID number, plate number, company, department, and more.

Searching for People

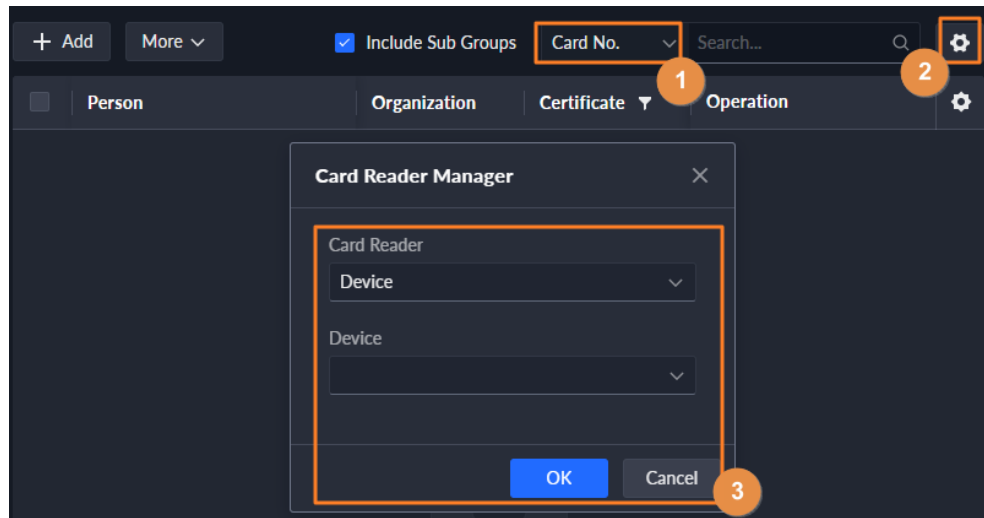
Select a person and vehicle group, enter keywords in the search area on the upper-right corner, and then click  or press Enter to search for people who have that information. If **Include Sub Groups** is selected, the platform will also search for people in the sub groups of the one that you select.

Filtering People

Click  on the upper-right corner to select which information to be displayed, such as person, linked ID, organization, phone number, email, certificate, card number, ID number, vehicle, company, department, room, and more.

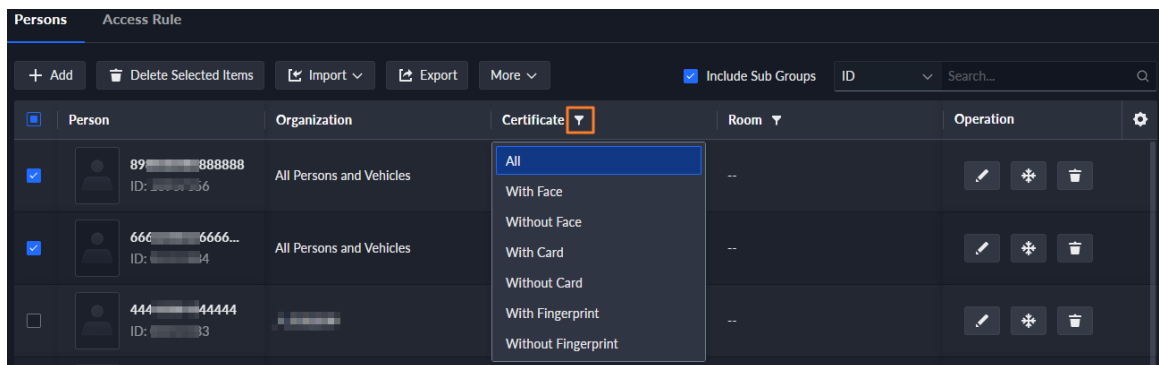
For example, when **Card No.** is selected, click , and then select swiping the card with a card reader or a device. When you swipe the card, the platform can directly read the card number and search, with no need of manually entering the card number.

Figure 4-21 Search by card number



Certificate, vehicle, linked ID, and room can be used to further filter person information. For example, you can choose to display or hide people with no linked ID.

Figure 4-22 Filter by certificate



4.3.2.12 Configuring Access Rule

An access rule defines the permission and effective time of that permission to lift or door channels. Configure an access rule for a person and vehicle group, and then it will be applied to all the people inside the group. Only administrators can configure access rules.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Person and Vehicle Info** > **Person List**.
- Step 2** Click a group, and then click **Access Rule**.
- Step 3** Click **Quote**. This page displays rules that have been added. You can select and use any one of them directly.
- Step 4** Click **Add**, and then configure the parameters of the new access rule.



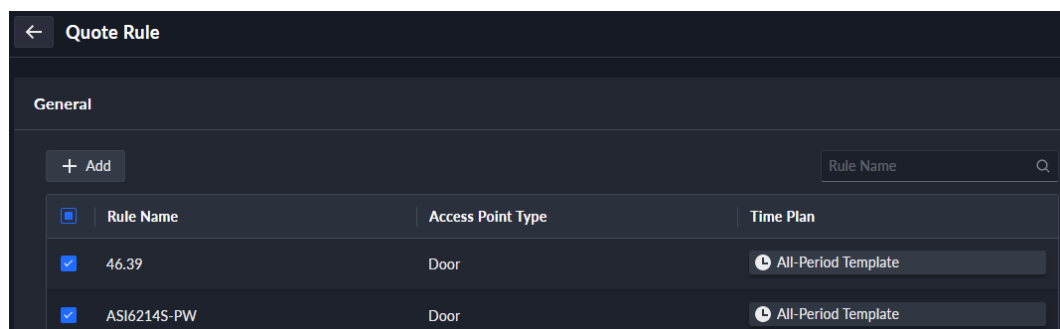
When configuring an access rule for a person and vehicle group, you can only configure general verification rules. If you want to configure other types of rules, see "4.5.3 Configuring Access Rule".

Table 4-14 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Select Door or Lift .
Rule Type	Only General Verification is available. For this type of rules, doors can be unlocked by face, card, fingerprint, and password.
Time Template	Select when this rule is effective. If you want to create a new time template, see "3.1.6 Adding Time Template".
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. Follow the steps below to create a new holiday plan: 1. Select Add Holiday Plan in the drop-down list. 2. Enter a name for the holiday plan. 3. Click Add to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click  to configure the periods more precisely. You can configure up to 4 periods. 5. Click OK.
Select by Zone	People can access all the access points in the selected zones.
Select by Access Point	People can access the selected access points.

Step 5 Select the access rules, and then click **OK**.

Figure 4-23 Select access rules



4.3.3 Vehicle Management

Manage vehicle information including vehicle type, owner, entry and exit permissions and arming groups.

Prerequisites

You need to add parking lot first. For details, see "4.8.2 Configuring Parking Lot".

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Person and Vehicle Info** > **Vehicle List**.

Step 2 Add vehicles.

- Add vehicles one by one

1. Click **Add**.

2. In the **Owner Info** section, click **Select from Person List** to select the owner of the vehicle.



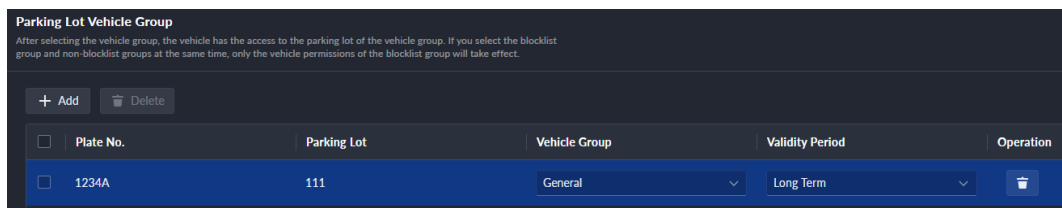
When personnel and vehicles are not in the same vehicle group, the vehicle owner should be selected based on the vehicle group of the personnel.

3. Configure the information of the vehicle in the **Vehicle Info** section, such as the vehicle group, plate number (required and unique), vehicle color, brand and more.

If you have selected an owner, you can add multiple vehicles.

4. In the **Parking Lot Vehicle Group** section, click **Add**, and then you can select the plate number (the one added in the previous step) and parking lot, set the vehicle group that the vehicle belongs to, and the validity period of the vehicle's access permissions.

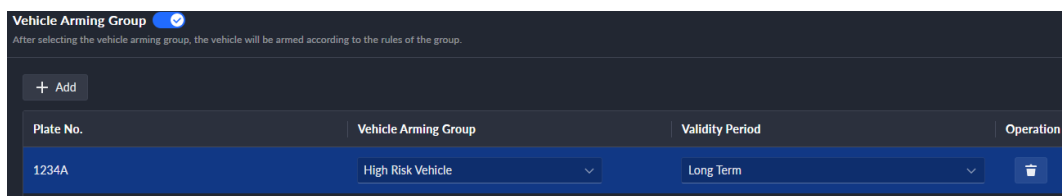
Figure 4-24 Parking lot vehicle group




If the owner has more vehicles than the defined parking spaces, once no parking spaces available, the owner cannot access the parking lot.

5. Click  to enable **Vehicle Arming Group**, and then click **Add** to arm the vehicles that you have just added.

Figure 4-25 Vehicle arming group





For arming group details, see "4.4.2.1 Adding Vehicle Arming Group".

6. Click **OK**.

- Add vehicles in batches

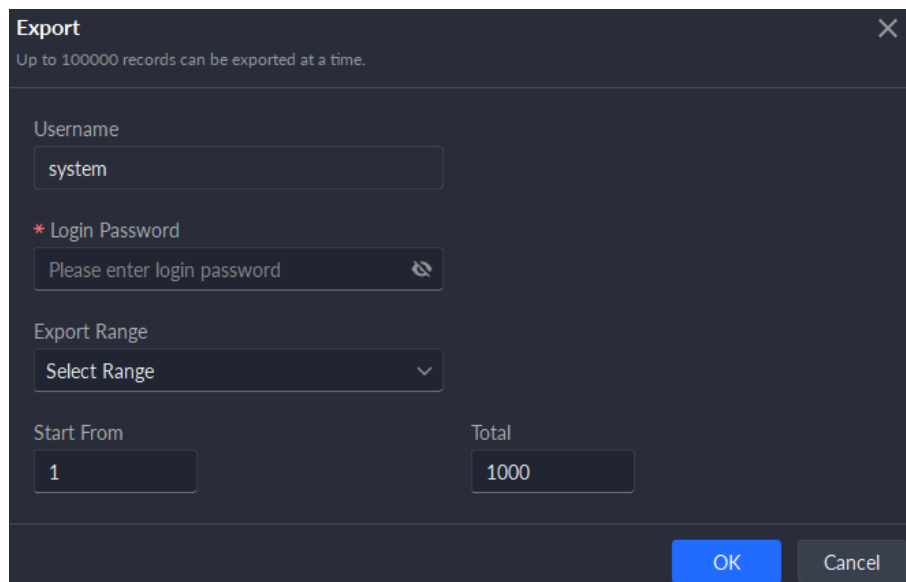
1. Click **Import**, and then click **Download Template**.
2. Fill in the template, and then select **Import File**. Select the file and import the information to the platform.



- You can click **Import File** or **Click to Select File** to import the vehicle information if you have already prepared them.
- The platform supports downloading files that failed to import for you to check and fix.

Step 3 (Optional) Export vehicle information to local storage as needed.

Figure 4-26 Export vehicle information



- Set **Export Range** to **All**, and then enter required information, such as passwords for login and encryption, to export all the items.
- Set **Export Range** to **Select Range**, and then the start record and total records that you want to export.

Related Operations

- You can search vehicles by entering keywords in search box at the upper-right corner.
- Click  or double-click the column to edit the vehicle information.
- Click  to delete vehicles one by one. You can also select multiple vehicles and then click **Delete** at the top to delete in batches.

4.4 Watch List Configuration

Configure face and vehicle watch list for future investigation.

- For face watch list, you can create and arm face comparison groups to recognize faces.

- For vehicle watch list, you can create vehicle comparison groups, add vehicles and then link devices for plate recognition.

4.4.1 Face Arming List

Configure a face arming list and send the it to devices for face recognition and alarms.

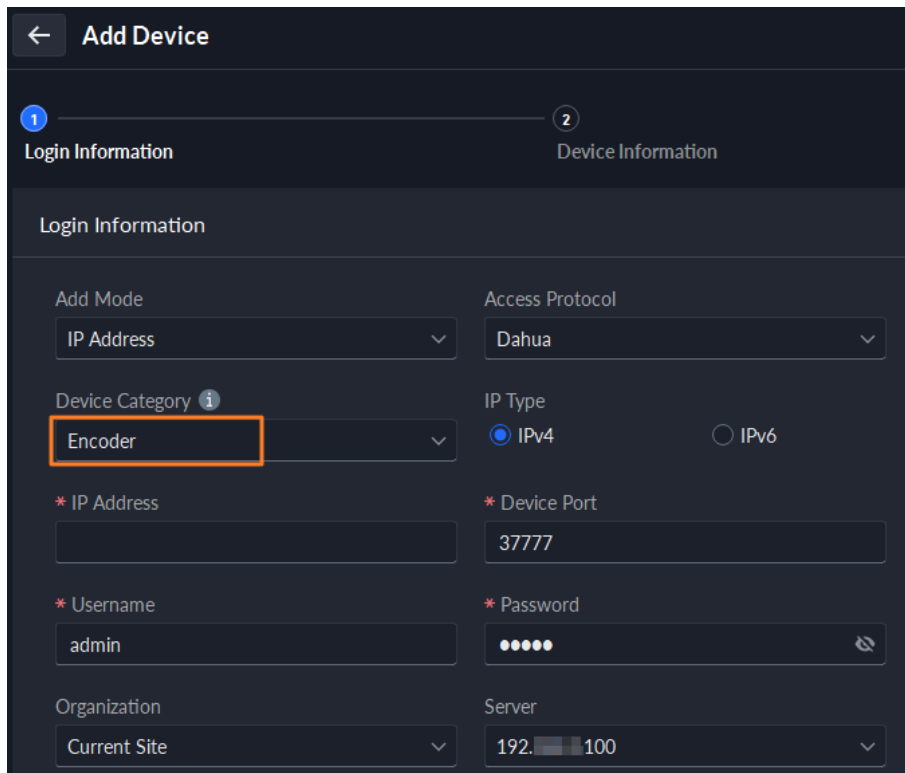
4.4.1.1 Creating Face Arming Group

Only administrators can add, edit, and delete person and face arming groups.

Prerequisites

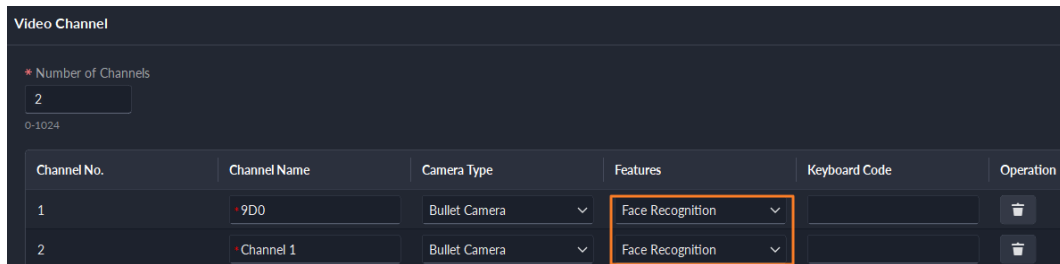
- Make sure that the devices for face recognition have been successfully configured onto the Platform.
- Make sure that the basic configuration of the Platform has completed. For details, see "3 Basic Configurations". During the configuration, you need to pay attention to following parts.
 - ◇ When adding devices on the **Device** page, set the **Device Category** to **Encoder**.

Figure 4-27 Device category



- ◇ When adding devices like NVR or IVSS which support face recognition, set the device feature to **Face Recognition**. For details, see "3.1.2.5 Editing Devices".

Figure 4-28 Feature configuration



- ◇ Make sure that you have configured at least one disk with the type of **Images and Files** to store face images. Otherwise, the snapshots cannot be displayed.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Arming List** > **Face Arming List**.
- Step 2** Click **Add**, and then configure the parameters.

Table 4-15 Parameter description

Parameter	Description
Face Arming Group Name	Enter a name for the group.
Color	You can use colors to quickly differentiate each group. For example, red indicates key targets.
Roles Allowed Access	Only the roles and their users can view this group.  Click  to see the users assigned with the roles.

- Step 3** Click **Add**.

4.4.1.2 Adding Faces

Add people to face arming groups. Their faces will be used for face comparison.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Arming List** > **Face Arming List**.

- Step 2** Click  of a group you want to add people to it.



The same person can be added to different face arming groups.

- Add people by person groups. This is the most efficient way, provided that you have created person groups based on the access permissions. For details, see "4.3.2 Configuring Person Information".

Click **Add by Person Group**, select one or more groups, and then click **OK**. You can also select **Include Sub Groups** to include the people in the sub groups of the groups you select.

- Select the people you want to add. This is applicable to people in different person groups have the same access permissions.

Click **Add by Person** , select the people you want to add, and then click **OK**.

4.4.1.3 Arming Faces

The faces of the people in face arming groups will be sent to devices for real-time face recognition. If the similarity reaches the defined threshold, alarms will be triggered.

Procedure

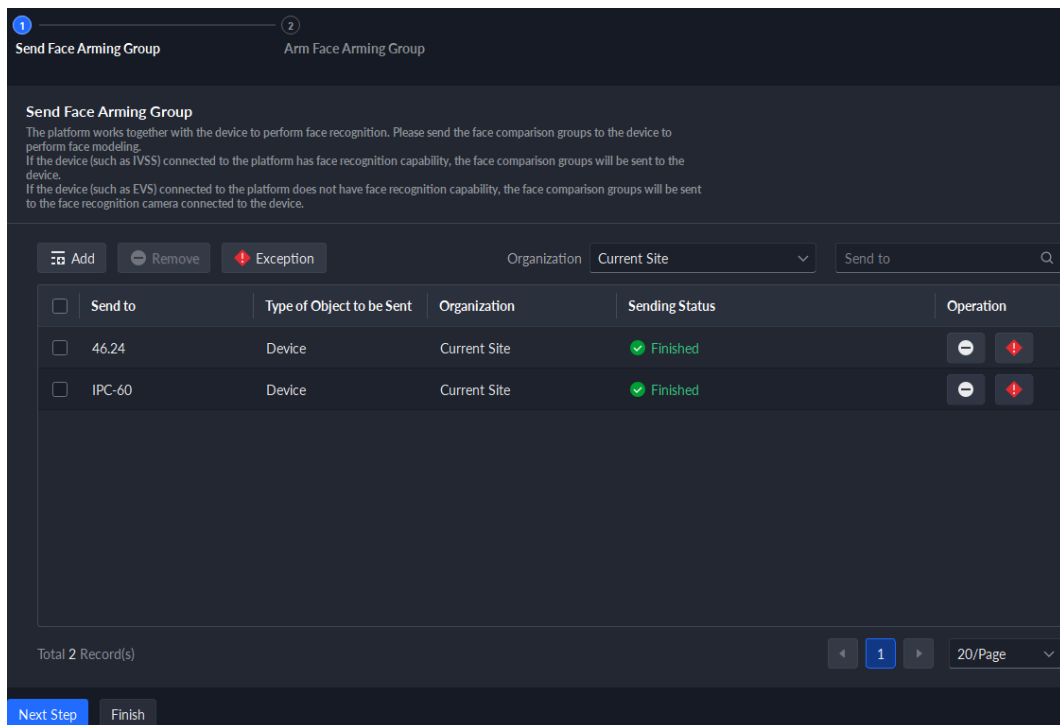
Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Arming List** > **Face Arming List**.

Step 2 Click of the face arming group you want to arm.

Step 3 Click **Add** , select one or more devices or channels, and then click **OK**.

The platform will send the information of the face arming group to the devices and channels you selected, and display the progress. If exceptions occur, you can click to view the reason.

Figure 4-29 Send face arming group



Step 4 After the face arming group is successfully sent, click **Next Step**.

Step 5 Click **Add**, select the channels you want to arm, and then configure the similarity for each channel.



When the similarity between the face captured by the channel and a face in the face arming group reaches or is greater than the defined value, it is considered a match.

Step 6 Click **OK**.

Step 7 (Optional) View exceptions and arm the face arming group again.

1. Click to view why arming failed and address the issue.
2. Click **Arm Again** to arm the face arming group again.

4.4.2 Vehicle Watch List

Create a vehicle comparison group and add vehicles to it. Alarms will be triggered if the vehicles in the group are captured and recognized.

4.4.2.1 Adding Vehicle Arming Group

A vehicle arming group contains the information of multiple vehicles. When arming the group, you can arm all the vehicles inside the group at the same time. Only administrators can add, edit, and delete person and face comparison groups. You can add up to 32 vehicle arming groups.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then click **Watch List > Vehicle Watch List**.
- Step 2** Click **Add**, and then configure the parameters.

Table 4-16 Parameter description

Parameter	Description
Vehicle Arming Group Name	Enter the name that identifies the group.
Color	You can use colors to quickly differentiate each group. For example, red indicates key targets.
Roles Allowed Access	Only the roles and their users can view this group.  Click  to see the users assigned with the roles.

- Step 3** Click **Add**.

4.4.2.2 Adding Vehicles

Add vehicles to vehicle arming groups. After armed, devices will recognize their plate numbers and trigger alarms.

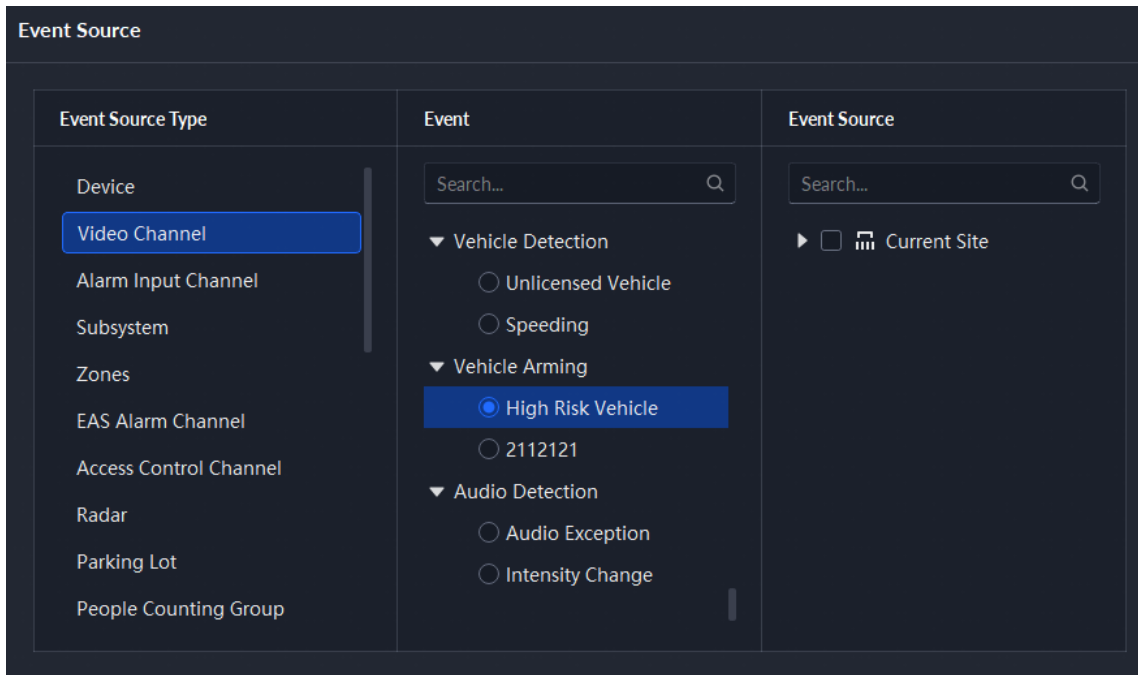
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then click **Watch List > Vehicle Watch List**.
- Step 2** Click  of a group, or double-click a group, and then click **Select from Vehicle List**.
- Add vehicles by vehicle groups. This is the most efficient way, provided that you have created vehicle groups. For details, see "4.3.2 Configuring Person Information".
Click **Add by Vehicle Group**, select one or more groups, and then click **OK**. You can also select **Include Sub Groups** to include the vehicles in the sub groups of the groups you select.
 - Select the vehicles you want to add. This is applicable to vehicles that you want to add are in different vehicle groups.
Click **Add by Vehicle**, select the vehicles you want to add, and then click **OK**.

4.4.2.3 Arming Vehicles

The plate numbers of the vehicles in comparison groups will be sent to devices for real-time recognition and trigger alarms.

Log in to the DSS Client. On the **Home** page, click , and then arm the vehicle on the **Event** page. Click **Add** to add an event to arm a vehicle watch list. For how to configure events, see "4.1 Configuring Events".

Figure 4-30 Arm vehicle event



4.5 Access Control

- Access control

Issue cards, collect fingerprints and face data, and apply permissions, so that the authorized people can open door by using card, face or fingerprint.

- Advanced functions

Configure advanced access control rules such as First-card Unlock, Multi-card Unlock, Anti-pass Back and Interlock to enhance security.

4.5.1 Preparations

Make sure that the following preparations have been made:

- Access control devices are correctly deployed. For details, see the user manual of the device you are adding to the platform.
- Basic configurations of the platform have been finished. See "3 Basic Configurations" for details.
 - ◇ When adding access control devices, select **Access Control** from **Device Category**.
 - ◇ (Optional) You can bind video channels to access control channels, so that you can monitor the area near access control devices. For details, see "3.1.3 Binding Resources".

- ◇ Add persons to the platform. For details, see "4.3 Personnel and Vehicle Management".

4.5.2 Configuring Zone

A zone is a collection of access permissions to doors and lifts. Create zones to quickly define security control areas with different permissions. Only the administrator can add, edit and delete zones.

- After adding the access control device on the **Device** page, the access point is automatically generated, and it is added to the **Unassigned** zone by default.
- The access points in the **Unassigned** zone can be moved to other zones, and you can view the details of the access points, but you cannot move access points to this zone, set them to boundaries or filter them by boundary.
- The **Unassigned** zone does not support the **Map Info** and **Access Rule** tabs, cannot be edited and deleted, and does not support adding, editing, and deleting sub zones.

4.5.2.1 Adding a Zone

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Zone Management**.
- Step 2** Click .
- Step 3** Configure the information, and then click **OK**.

Table 4-17 Parameter description

Parameter	Description
Parent Zone	Select a parent zone for permission management. For example, if a user has permissions for zone A, the user also has permissions for all sub zones under zone A by default. Additional permissions can be set for the sub zones.
Zone Name	Enter a name for the zone.
Icon	Select an icon for the zone. Icons are used for users to quickly identify different zones.
Select Access Point	Select access points from an existing zone. After selection, the rules and map zones linked to the original zone will be deleted from the access point. Rules in the target zone will be applied to the access points.
Roles Allowed Access	Only the selected roles and their users can access this zone.  Click  to see the users assigned with the roles.

4.5.2.2 Adding Zones in Batches

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Zone Management**.

Step 2 Click a zone, and then click .

All zones will be added as sub zones of the one you select.

Step 3 Click **Add** to add more levels.

There is only 1 level by default. There can be up to 8 levels of zones. For example, if the zone you select is a level 3 zone, you can only add 5 levels of zones under it.

Step 4 Configure the parameters for each level, and then click **OK**.

You can check the results for your current configurations.

Figure 4-31 Add zones in batches

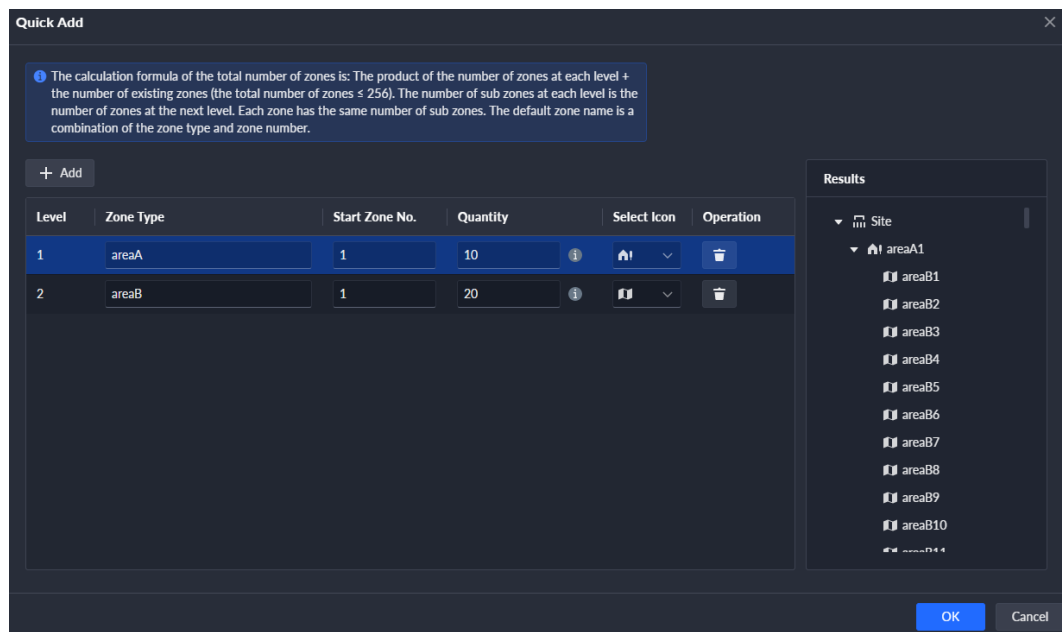


Table 4-18 Parameter description

Parameter	Description
Level	The number indicates the level of the zone. The region with a larger number is a sub zone of the region with the smaller number. For example, the level 2 zone is a sub zone of the level 1 zone.
Zone Type	Enter a name for the zone.
Start Zone No.	Enter a start number and then all the zones of this level will be automatically numbered. For example, if the start number is 1 and the quantity of zones is 3, then zones will be numbered as zone 1, zone 2, and zone 3.
Quantity	Enter a number for each zone. The number of each level of zones = upper levels $\times$ the current level. For example, the numbers of level 1, 2 and 3 are 1, 2, and 3. Then, the number of level 3 zones = $1 \times 2 \times 3 = 6$.
Select Icon	Select an icon for the zone. Icons are used for users to quickly identify different zones.

Step 5 Click **OK**.

The roles that are allowed to access the parent zone will be automatically applied to the sub zones.

4.5.2.3 Editing and Deleting Zone

Only administrators can edit and delete zones.

Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Zone Management**.

- Click a zone and then click  to edit the information of the zone, including the name, icon, and roles allowed access.
- Click a zone and then click  to delete it. After deleting the zone, all information related to the zone will also be deleted, including sub zones, access rules, and maps. Access points in this zone and its sub zones will be moved to the root zone.

4.5.2.4 Moving Access Points

Access points include door and lift control channels. The access points in a zone can be moved to other zones. After you add access control devices, video intercom devices with access control functions, and lift control devices to the platform, access points of door and lift control channels will be generated and added to the **Unassigned** zone by default. You need to allocate them to other zones.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Zone Management**.

Step 2 Click a zone, and then click **Access Point**.

All access points and sub zones will be displayed.

Step 3 Move the access points.

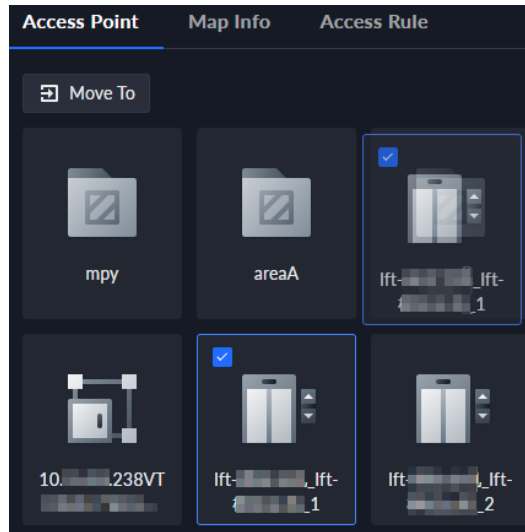
After moving the access points, access rules of the current zones will not be applied to them, and their information on the map will also be deleted. The access rules of the target zone will apply to them.



Access points that have been configured with access rules cannot be moved.

- Move an access point.
 - ◇ Drag an access point to a sub zone.
 - ◇ Right-click an access point, select **Move To**, and then select a zone.

Figure 4-32 Move an access point



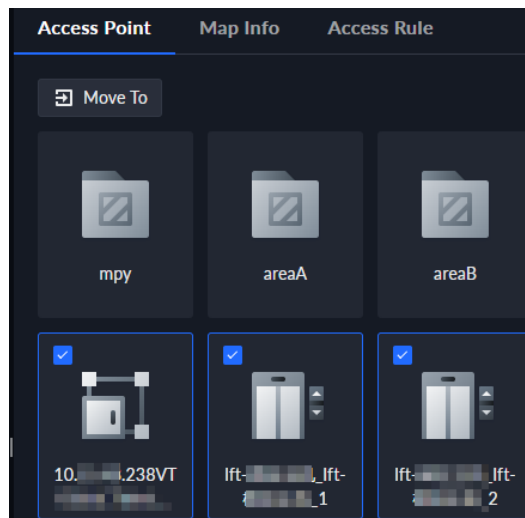
- Move multiple access points.



You cannot move the access points in batches if the current or target access points have been configured with access rules.

1. Drag to select multiple access points. Or hover the mouse over an access point, click the checkbox to select it, and then repeat the operations to select multiple access points.
2. Drag the access points to a sub zone. Or click **Move To** and then select a zone. Or right-click any selected access point, click **Move To** and then select a zone.

Figure 4-33 Move multiple access points



4.5.2.5 Configuring Access Point

4.5.2.5.1 Viewing Access Point Details

View the information of an access point, including the name, type, zone it belongs to, linked resources, and access rules.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click  and then in the **App Config** section, select **Access Control** > **Zone Management**.
- Step 2 Click a zone, and then click **Access Point**.
- Step 3 Double-click an access point to view its details.
- **Access Point Name** : The name of the access point.
 - **Access Point Type** : Displays the type of the access point, door or lift.
 - **Zone Name** : Displays the name of the zone the access point belongs to.
 - **Linked Resources** : Displays the channel name and type of the access point, the name and type of the intercom device it belongs to, and video channels that are bound to it. If you want to bind resources to this access point, you can click **Channel Binding** to quickly go to the page. For details on channel binding, see "3.1.3 Binding Resources".
 - **Access Rule** : Displays the access rules applied to this access point itself, and from the zone it belongs to. Double-click a rule to view its details. You can click **Quote** or **Remove** to add or delete the rules, but the rules from the zone cannot be deleted.

4.5.2.5.2 Setting Boundary

Setting access points as boundaries to count people that entered, exited, or entered but did not exit.

- Step 1 Log in to the DSS Client. On the **Home** page, click  and then in the **App Config** section, select **Access Control** > **Zone Management**.
- Step 2 Click a zone, and then click **Access Point**.
- Step 3 Right-click an access point (door, not lift) and select **Set as Boundary**.

The icon of the access point changes to .

4.5.2.6 Configuring Access Rule for a Zone

An access rule defines the permission and effective time of that permission to lift or door channels. Configure an access rule for a zone, and then it will be applied to all the access points inside. Only administrators can configure access rules.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click  and then in the **App Config** section, select **Access Control** > **Zone Management**.
- Step 2 Click a zone, and then click **Access Rule**.
- Step 3 Click **Quote**. The system displays rules that have been added.

You can:

- Select and use any one of the existing rules directly.
- Click **Add**, and then configure the parameters to add a new access rule.



When configuring an access rule for a zone, you can only configure general verification rules for doors. If you want to configure other types of rules, see "4.5.3 Configuring Access Rule".

Table 4-19 Parameter description

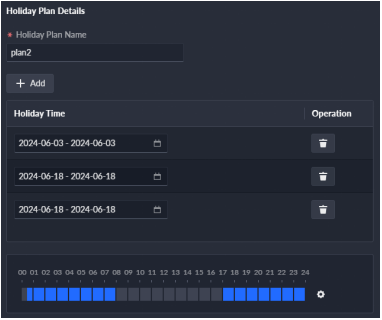
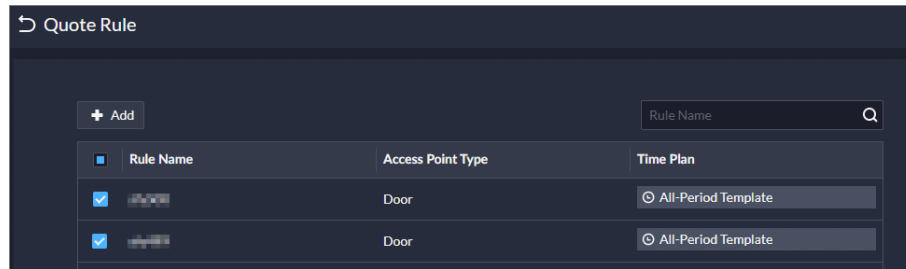
Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only Door is available.
Rule Type	Only General Verification is available. For this type of rules, doors can be unlocked by cards, fingerprints, and passwords.
Time Template	Select when this rule is effective. If you want to create a new time template, see "3.1.6 Adding Time Template".
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. Follow the steps below to create a new holiday plan: 1. Select Add Holiday Plan in the drop-down list. 2. Enter a name for the holiday plan. 3. Click Add to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click  to configure the periods more precisely. You can configure up to 4 periods. 5. Click OK. 
Select by Person Group	Select one or more person groups, and then all the persons in the groups will have permissions to access all the door channels in the zone.  Select Link Sub Node, and then you can select a zone and all its sub zones at the same time.
Select by Person	Select one or more persons, and then they will have permissions to access all the door channels in the zone.  Select Include Sub Groups to display all the persons in the selected group and its sub groups.

Figure 4-34 Select access rules



Step 4 Click **OK**.

4.5.2.7 Configuring Map

On the map of a zone, you can mark access points and sub zones so that you can better manage them and quickly locate events. You can configure a map for each zone. Besides administrators, any user can configure maps for zones if they have permissions to access the zones. But if a user does not have access to the map function, the user will not be able to configure the map for any zone.

4.5.2.7.1 Adding a Map

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Zone Management**.
- Step 2** Click a zone, and then click **Map Info**.
- Step 3** Click **Configure Map** to add a map for the zone.
- Select a map that has been added to the platform.
 - Upload an image as the map. After added, the map will be added to the platform as a main map. To know more about maps, see "4.2.2 Adding a Map".
- Step 4** Click **OK**.

4.5.2.7.2 Marking Access Point and Sub Zone

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Zone Management**.
- Step 2** Click a zone, and then click **Map Info**.
- Step 3** Drag a sub zone or access point to the map.

When marking a sub zone, you need to configure a map for it.

- If a map was added as the sub map of the current map, you can select it directly as the map for the sub zone.
- If no map was added for the sub zone, you can add a new map for it. The new map will be added as the sub map of the current one.
- If you added a map for the sub zone, but it is not a sub map of the current one, you cannot mark the sub zone on the map.



If you want to configure maps first, see "4.2 Configuring Map".

Related Operations

- Hide access point name
Only displays the icon of access points.
- Show access point
Select which types of access points to be displayed on the map.
- Move
Click **Move**, and then you can adjust the locations of the sub zones and access points on the map.
- Reset
Restore the map to its initial position and zoom level.
- Remove map
Remove the map from this zone. This operation will not delete the map from the platform.

4.5.3 Configuring Access Rule

An access rule defines the permission and effective time of that permission to lift or door channels. Only administrators can configure access rules.

4.5.3.1 Viewing Access Rule Details

This page displays all access rules on the platform, including those configured for a person, person group, zone, and access point.

Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.

- Double-click a rule to view its details.
- Click  of a rule to view its authorization progress. If exceptions occur, click  to view their details. Follow the reason and prompt to handle the exception, and then click **Send Again** to send the rule again, but it only applies to **General Verification** rules. For other types of rules, you can only send them again manually.

4.5.3.2 Configuring General Verification

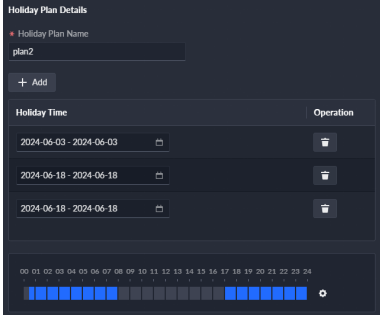
Grant permissions to persons so that they can verify their identifications and access doors or lifts within the effective periods.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.
- Step 2** Click **Add**.
- Step 3** Configure the parameters, and then click **OK**.

Table 4-20 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.

Parameter	Description
Access Point Type	Select Door or Lift , and then the platform will only display corresponding channels.
Rule Type	Select General Verification .
Time Template	Select when this rule is effective. If you want to create a new time template, see "3.1.6 Adding Time Template".
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. Follow the steps below to create a new holiday plan: 1. Select Add Holiday Plan in the drop-down list. 2. Enter a name for the holiday plan. 3. Click Add to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click  to configure the periods more precisely. You can configure up to 4 periods. 5. Click OK. 
Select by Zone	Select one or more zones, and then this rule will be applied to all access points in the zones.  Select Link Sub Node, and then you can select a zone and all its sub zones at the same time.
Select by Access Point	Select one or more access points.  Select Include Sub Zone to display all the access points in the selected zone and its sub zones.
Select by Person Group	Select one or more person groups, and then all the persons in the groups will have permissions to access the selected access points.  Select Link Sub Node, and then you can select a zone and all its sub zones at the same time.

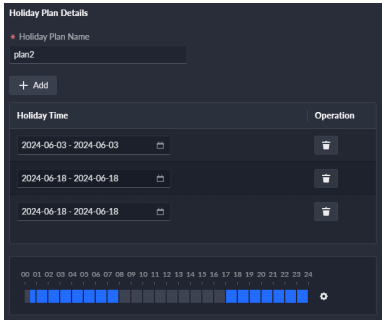
Parameter	Description
Select by Person	Select one or more persons, and then they will have permissions to access the selected access points.  Select Include Sub Groups to display all the persons in the selected group and its sub groups.

4.5.3.3 Configuring Normally Open

Within the effective periods, all people can pass access points without verifying their identifications.
Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.
- Step 2** Click **Add**.
- Step 3** Configure the parameters, and then click **OK**.

Table 4-21 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only Door is available.
Rule Type	Select Remains Open during Period .
Time Template	Select when this rule is effective. If you want to create a new time template, see "3.1.6 Adding Time Template".
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. Follow the steps below to create a new holiday plan: 1. Select Add Holiday Plan in the drop-down list. 2. Enter a name for the holiday plan. 3. Click Add to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click  to configure the periods more precisely. You can configure up to 4 periods. 5. Click OK. 

Parameter	Description
Holiday Plan Authentication	After defining the period in holiday plan authentication, authentication is required for access within the defined period on the holiday. The operations are similar to those of adding holiday plan.  You can add up to 4 plans.
Access Point	Select one or more doors.  Select Include Sub Zone to display all the access points in the selected zone and its sub zones.

4.5.3.4 Configuring Normally Closed

All people are not allowed to pass access points.

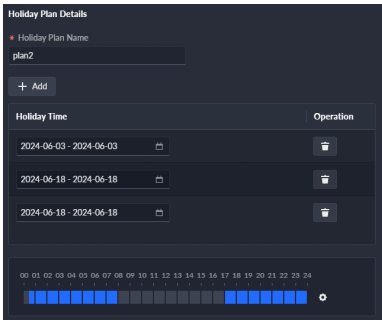
Step 1 Log in to the DSS Client. On the **Home** page, click  and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.

Step 2 Click **Add**.

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

Table 4-22 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only Door is available.
Rule Type	Select Remains Closed during Period .
Time Template	Select when this rule is effective. If you want to create a new time template, see "3.1.6 Adding Time Template".

Parameter	Description
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. Follow the steps below to create a new holiday plan: 1. Select Add Holiday Plan in the drop-down list. 2. Enter a name for the holiday plan. 3. Click Add to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click  to configure the periods more precisely. You can configure up to 4 periods. 5. Click OK. 
Holiday Plan Authentication	After defining the period in holiday plan authentication, authentication is required for access within the defined period on the holiday. The operations are similar to those of adding holiday plan.  You can add up to 4 plans.
Access Point	Select one or more doors.  Select Include Sub Zone to display all the access points in the selected zone and its sub zones.

4.5.3.5 Configuring First-Person Unlock

Any person can access doors only after the persons you specify pass through. When you specify multiple persons, other persons can access doors after any one of specified persons pass through.

Prerequisites

Persons can only be set as first persons when they have permissions to access doors. For how to use general verification rules to grant permissions to persons, see "4.5.3.2 Configuring General Verification".

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.
- Step 2** Click **Add**.
- Step 3** Configure the parameters, and then click **OK**.

Table 4-23 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only Door is available.
Rule Type	Select First-person Unlock .
Rule Type after Unlocked by First Person	● Normal : Other persons must verify their identifications to pass. ● Always Open : All people can pass without verifying their identifications.
Time Template	Select when this rule is effective. If you want to create a new time template, see "3.1.6 Adding Time Template".
Access Point	Select one or more doors.  Select Include Sub Zone to display all the access points in the selected zone and its sub zones.
Person	Select one or more persons, and then they will have permissions to access the doors.  Select Include Sub Groups to display all the persons in the selected group and its sub groups. Access types that will affect the rule are listed below. For how to configure access types, see "4.3.2.2 Adding a Person". ● First-person unlock rules only support General access type. ● People whose access types are Patrol will not be restricted by the rule. When no one in the first-person unlock rule unlocks the door, a patrol event for people whose access types are Patrol, and the door will not open.

4.5.3.6 Configuring Multi-Person Unlock

Multiple unlock groups must swipe their cards on doors in the specified order to unlock them.

Prerequisites

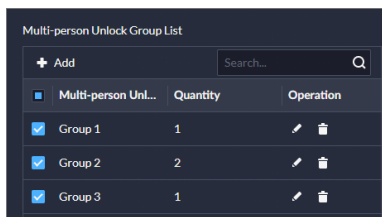
Persons can only be added to unlock groups when they have permissions to access doors. For how to use general verification rules to grant permissions to persons, see "4.5.3.2 Configuring General Verification".

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.
- Step 2** Click **Add**, and then configure the parameters.

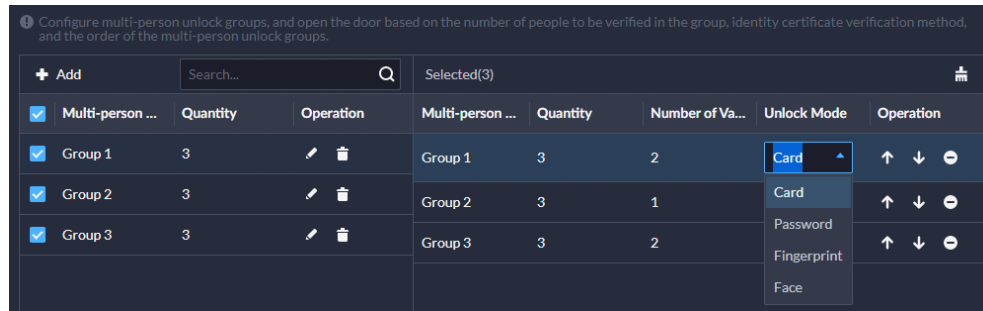
Table 4-24 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.

Parameter	Description
Access Point Type	Only Door is available.
Rule Type	Select Multi-person Unlock .
Time Template	The all-period time template is used by default and cannot be changed.
Access Point	Select one or more access points.  Select Include Sub Zone to display all the access points in the selected zone and its sub zones.
Person	Configure up to 4 unlock groups. Persons must verify their identifications in the group order to unlock doors. - Click Add. - Enter a name for the group. - Add one or more persons to the group. You can add up to 50 persons to the group. Select Include Sub Groups to display all the persons in the selected group and its sub groups.  - A person can only be added to one group. - If a person has been selected in a first-person rule, we do not recommend add the person to a multi-person unlock group because when the person access a door, the platform will execute the first-person unlock rule. - Persons with access types as Patrol and VIP cannot be added to the group. Also, multi-person unlock rules do not apply to them. For how to configure access types for persons, see "4.3.2.2 Adding a Person". - Click OK. (Optional) Repeat the steps below to add more groups. - Select the groups that you added, and then click OK.  - Click the up or down arrows to adjust the group order, and then click OK.

Step 3 Configure the unlock method for each group, including card, password, fingerprint, and face.

Figure 4-35 Configure unlock methods



Step 4 Click **OK**.

4.5.3.7 Configuring Anti-Passback

People can only pass in the defined order. For example, if people want to go to building D, they must go through building A, B, and C in this order. They cannot enter building D directly.

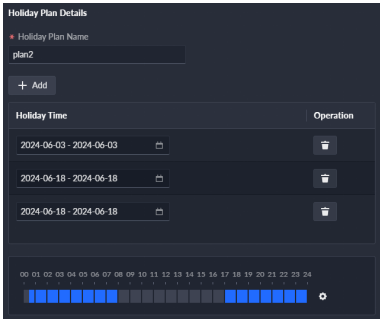
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.

Step 2 Click **Add**.

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

Table 4-25 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only Door is available.
Rule Type	Select Anti-passback .
Anti-passback Type	For Local Anti-passback, you can select only the door channels of an access control device; for Global Anti-passback, you can select door channels from any zone (make sure that the channels support global anti-passback). If you select Global Anti-passback, you can configure the offline operation strategy at the same time: Execute: Offline access points will execute the anti-passback configurations. Do Not Execute: People can pass normally through offline access points.
Reset Time	If people do not pass in the defined order, they will not be allowed to pass any door within the reset time. After the reset time, they must follow the order from the beginning. The reset time can be between 1 minute and 24 hours.
Time Template	Select when this rule is effective. If you want to create a new time template, see "3.1.6 Adding Time Template".

Parameter	Description
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. Local Anti-passback does not support holiday plan. Follow the steps below to create a new holiday plan: 1. Select Add Holiday Plan in the drop-down list. 2. Enter a name for the holiday plan. 3. Click Add to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click  to configure the periods more precisely. You can configure up to 4 periods. 5. Click OK. 
Access Point	Add doors to different groups, and then people must pass in the group order to access the doors in the last group.  When setting Anti-passback Type to Global Anti-passback: • You can add up to 64 card readers • The platform will only display devices that support this function. • You can select Include Sub Zone to display all the access points in the selected zone and its sub zones.
Person	Select the persons that will not be subject to the global anti-passback rules. You can only add up to 1,000 persons to a single rule.  Make sure that the General Verification rule has been configured for the person. For details, see "4.5.3.2 Configuring General Verification".

4.5.3.8 Configuring Multi-Door Interlock

When a door is unlocked, people cannot pass through any other door. This rule has 3 types:

- Local interlock: Only door access points of 1 device are supported. The platform will generate interlock groups based on the number of door access points of the device you select. Each group can contain 2 to 4 door access points. After a door is opened, other doors in the same group cannot be opened, but those in other groups can still be opened.
- Global interlock within groups: Only 1 interlock group is supported. The group can contain 2 to 4 door access points. After a door is opened, other doors cannot be opened.

- Global interlock between groups: Only 2 interlock groups are supported. Each group can contain 1 to 4 door access points. After a door is opened, other doors in the same group can still be opened, but those in other groups cannot be opened.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.
- Step 2** Click **Add**.
- Step 3** Configure the parameters, and then click **OK**.

Table 4-26 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only Door is available.
Rule Type	Select Multi-door Interlock .
Interlock Type	Select an interlock type. If you select a global interlock rule, you can configure the offline execution strategy at the same time: • Execute : Offline access points will execute the interlock configurations. • Do Not Execute : People can pass normally through offline access points.
Time Template	The all-period time template is used by default and cannot be changed.
Access Point	Select an access control device, and then add its doors to different groups. When a door in any group is unlocked, people cannot pass through any other door.  If remote verification is also configured at the same time, the platform will verify remote verification first. When it passes, multi-door interlock will then be verified. For example, if person A wants to open door B in group C, the remote verification will be sent to the platform. After the platform confirms that the remote verification, it will then check whether any door in other groups are opened. If any door is opened, person A cannot open door B.  When configuring a global interlock rule, select Include Sub Zone to display all the access points in the selected zone and its sub zones.

4.5.3.9 Configuring Remote Verification

When people want to pass a door configured with remote verification, they can only pass after the platform confirms.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.

- Step 2** Click **Add**.
- Step 3** Configure the parameters, and then click **OK**.

Table 4-27 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only Door is available.
Rule Type	Select Remote Verification .
Time Template	Select when this rule is effective. If you want to create a new time template, see "3.1.6 Adding Time Template".
Access Point	Select one or more doors.  Select Include Sub Zone to display all the access points in the selected zone and its sub zones.

Results

When a person wants to unlock a door, a pop-up will be displayed on the platform. You can open the door or ignore the request.

4.5.3.10 Viewing Rule Exception

After adding rules, exceptions might happen when they are being applied to access points. The platform displays all exceptions on this page and provides reasons and prompts for each one. You can handle the exceptions accordingly and then quickly send the rules again in one click, but it only applies to **General Verification** rules. For other types of rules, you can only send them again manually.

Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **Rule Maintenance** > **All Abnormalities**.

Click the name of a person or access point to quickly go to the corresponding page for configurations. Handle the exceptions according to the reasons and prompts, and then click **Send Again** to send the rules again.

4.5.3.11 Verifying Consistency of Person Information

Rules will not be applied successfully if the people on the devices and the platform are not the same. You can use this function to check the people on a device against those on the platform, and quickly address issues if any occurs.

Prerequisites

Before using this function, you must configure an **Image and File** disk for the server where the device is added to. For details, see "3.3 Configuring Storage".

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **Rule Maintenance** > **Consistency Verification**.
- Step 2** Select an access control device, and then click **Verify**.

A verification record will be generated on the right. If **Completed** is displayed, it means that the people on the device match those on the platform, and the device pass the verification.

Step 3 If any issue occurs, click **View Details** to view its details.

Step 4 Click **One-click Process** to automatically address all issues.

The following issues might occur and how the platform will address each of them:

- A person is not on the device: Send the person information from the platform to the device again.
- A person is not on the platform: On the **Person List** page, select **Import** > **Import from Device** to import the person information from the device to the platform.
- The person information is inconsistent: Send the person information from the platform to the device again.

4.5.4 Configuring Public Passwords

For a door, any person with the public password can unlock it. You can configure up to 1,500 passwords in the platform, and up to 500 passwords for a single device.

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Basic Config** > **Public Password**.

Step 2 Click .

Step 3 Enter a name for the password, configure the password, and then select the door channels from access control and video intercom devices that the password will be applied to.

Step 4 Click **Save**.

Step 5 (Optional) If exceptions occur, click  to view details. Handle the exceptions according to the reasons provided by the platform, and then click **Send Again**.

4.5.5 Configuring Access Card

You can enable **Device DESFire Card** or **Block NFC Cards** as needed. After enabling DESFire card, the platform can issue cards to people by DESFire card reader, and then people can access by using DESFire cards; by enabling **Block NFC Cards**, the device will not recognize copied NFC cards, and people cannot use NFC cards to open doors.

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Basic Config** > **Access Card Config**.

Step 2 Enable **DESFire card** and **Block NFC Cards** as needed.

Table 4-28 Access card configuration description

Parameter	Description
Device DESFire Card	After enabled, the DESFire card can be used normally.  Make sure that the device supports reading DESFire card; otherwise, the card cannot be recognized.
DESFire Card Encryption	After enabled, the DESFire card reader only shows the encrypted information.

Parameter	Description
Write to DESFire	After enabling Device DESFire Card and DESFire Card Encryption , you can click this icon, select a device that supports reading and writing DESFire cards from  , enter the card number, and then the device can write the card number to the card.
Block NFC Cards	Enable Block NFC Cards , and then click Apply to Device , the devices will not recognize copied NFC cards, and people cannot use NFC cards to open doors.
Apply to Device	

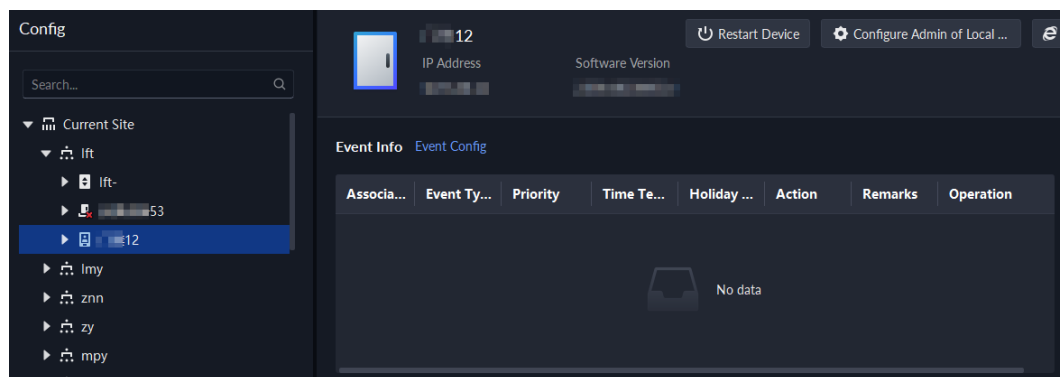
4.5.6 Configuring Access Control Devices

If an access control device is online, you can restart it, and synchronize its time with the platform. Also, you can set a person as the administrator, and then the person can log in to the configuration page of the access control device to configure parameters.

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device** > **Device Config**.

Step 2 Select an access control device from the device tree.

Figure 4-36 Select an access control device



Step 3 Configure the access control device.

- Click **Restart Device** to restart the device.
- Click **Configure Admin of Local Device** and add people from person groups. Then, the people can use their usernames and passwords to log in to the configuration page of the device.
- Click  at the upper-right corner to go to the webpage of the device.

4.6 Video Intercom

4.6.1 Preparations

Make sure that the following preparations have been made:

- Access control devices are correctly deployed, and the SIP server IP of the devices are filled in with IP of central servers of the platform. For details, see the corresponding user manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".

- ◇ When adding video intercom devices on the **Device** page, select **Video Intercom** as the device category.
- ◇ When adding access control devices that support intercom, select **Device Category** to **Access Control** in **Login Information**, and then select **Access Control Recognition Terminal**.



- The platform automatically creates a room after you add a VTH. For details, see "4.6.4 Configuring Room".
- Any configuration modification on the device will not be reported to the platform. You need to go to the device modification page of Web Manager to manually synchronize the modification.

4.6.2 Call Management

Create call group, management group and relation group respectively and define restricted call relations. This function is only available for administrators.



Click  on the page of call group, management group or relation group, the system will restore management group and relation group to their original status.

4.6.2.1 Configuring Call Group

Only devices in the same call group can call each other.

- A call group will be automatically generated after you add to the platform a VTO or access control device that supports intercom. All VTHs in the same unit will also be automatically added to the group. 2 VTHs or a VTH and VTO in the group can call each other.
- A call group will be automatically generated after you add a second confirmation station to the platform. Add the VTHs in the same house to the group, then the second confirmation station and the VTHs can call each other.
- A call group will be automatically generated after you add a fence station to the platform. All the VTHs on the platform will be automatically added to the group by default, then the fence station and the VTHs can call each other. You can also click  to edit the VTHs in the group, so that the fence station can only call certain VTHs.
- After added to the platform, VTHs will be automatically added to corresponding groups if they are associated with VTOs, second confirmation stations, or fence stations, so that they can call each other.

4.6.2.2 Adding a Manager Group

Divide administrators into different groups and link them to call groups in different combinations. This is useful when certain administrators can only answer calls from certain devices. Administrators include VTS and users with permissions to use the video intercom function and operate the devices. VTS will be automatically added to the default manager group after added.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Video Intercom** in the **App Config** section.
- Step 2** Select **Call Management** > **Manager Group Config**.
- Step 3** Click .

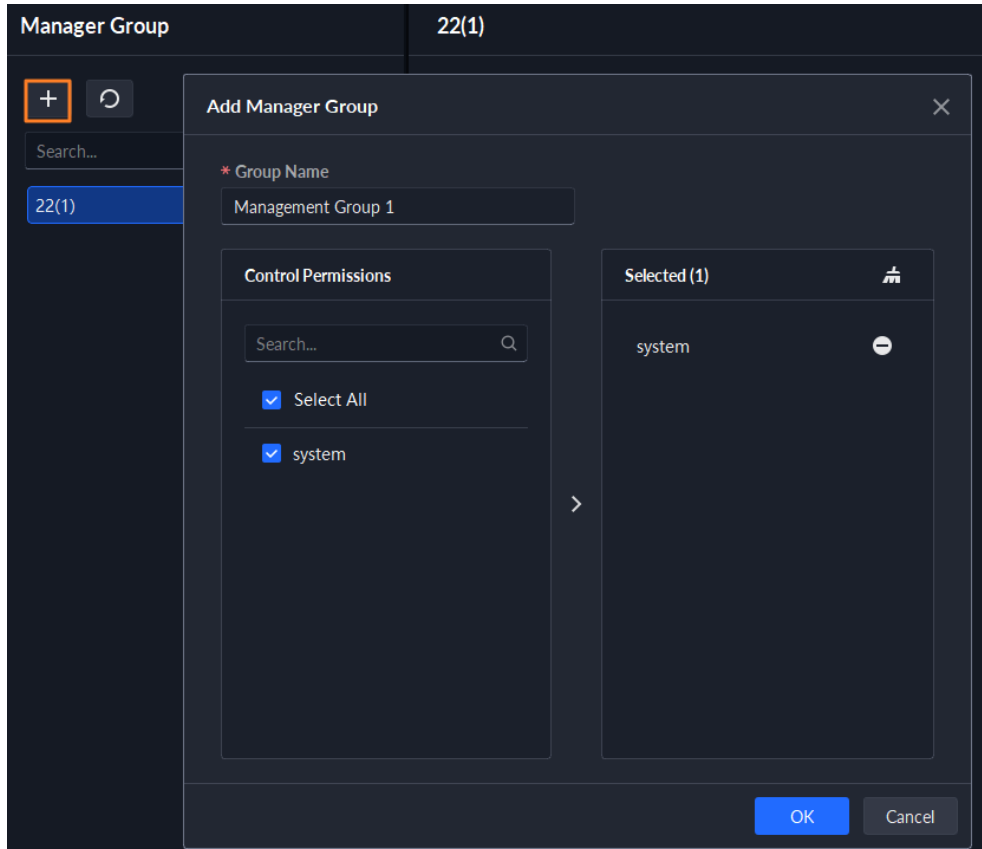
Step 4 Enter the group name, select an administrator account or VTS, and then click **OK**.

The added management group is displayed in the list.



- To transfer members, click  and move the member to other groups.
- To manage group members, click  to add or delete group members.

Figure 4-37 Add a manager group



4.6.2.3 Configuring Relation Group

Link call groups and manager groups, and VTOs or VTHs in a call group can only call administrators or VTSs of a linked manager group. There are 2 types of relations:

- A call group links to 1 manager group.

All online administrators in the manager group will receive the call when any device is calling. If an administrator answers, it will stop ringing for other administrators. The call will only be rejected if all administrators reject it.

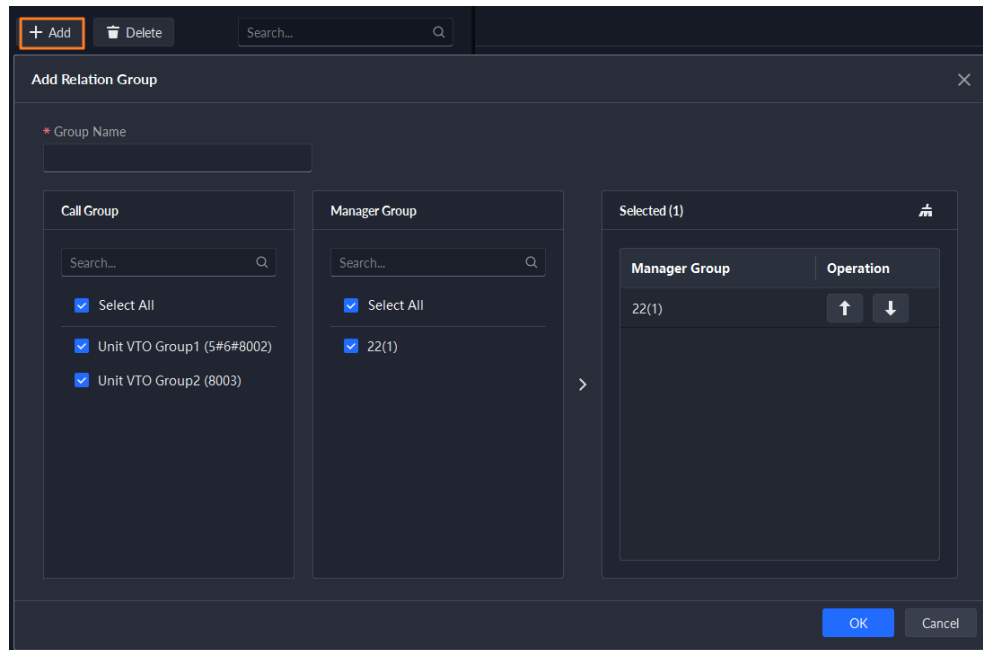
- A call group links to multiple manager groups.

Priorities vary for different manager groups. When any device is calling, all online administrators in the manager group with the highest priority will receive the call first. If no one answers for 30 seconds, then the call will be forwarded to the manager group with the second highest priority. If still no one answers, the device will prompt that there is no response for the call.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Video Intercom** in the **App Config** section.
- Step 2** Select **Call Management** > **Relation Group Config**.
- Step 3** Click .
- Step 4** Enter the group name, and then select one or more call groups and manager groups.

Figure 4-38 Add a relation group



Because only up to 2 manager groups can receive a call, we recommend you select no more than 2 manager groups.

- Step 5** Click  or  to adjust priorities of the manager groups, and then click **OK**.
The upper manager group has the higher priority.

4.6.3 Configuring Building/Unit and Call Mode

Make sure the status of building and unit of the DSS client is the same as the VTO. If building and unit are enabled on the platform, they must also be enabled on the device, and vice versa; otherwise, the VTO will be offline after it is added. That also affects the dialing rule. Take room 1001 unit 2 building 1 as an example, the dialing rule is as follows:

- If building is enabled while unit is not, the room number is "1#1001".
- If building is enabled, and unit is enabled as well, the room number is "1#2#1001".
- If building is not enabled, and unit is not enabled either, the room number is "1001".

Select a call mode to specify the order of calling VTH and App.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Video Intercom** in the **App Config** section.
- Step 2** Click **Residence Config**.

Step 3 Enable or disable building and unit as required, and then click **OK**.



This configuration must be the same as the device configurations. Otherwise, information of the devices might be incorrect. For example, if only **Building** is enabled on a VTO, you must only enable **Building** on the platform.

Step 4 Configure the call mode.

- **Simultaneous Call** : When a room is being called, all the VTHs and App users in it will receive the call. If there are only App users in the room, then all App users will receive the call.
- **Group Call** : When calling a room, only the VTHs in it will receive the call. If call forwarding is enabled on the VTHs, then all App users will receive the call.

Step 5 Click **Save**.

4.6.4 Configuring Room

Add a room to include the VTHs and app users in it.

Background Information

When you add a VTH to the platform, the platform will automatically create a room. You can also create a room and add the VTH later. The VTH will automatically join the corresponding room. The rooms that are automatically created cannot be deleted. You can only delete those that are manually created.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Video Intercom** > **Room Config**.

Step 2 Click .

Step 3 Select an organization, enter a name for the room and the room number, and then click **Add**.

If the VTH with the same room number has been added to the platform, or the homeowner with the same room number has registered, the VTH or the app user will join the room automatically.

Related Operations

Operations on the app users:

- : Set an app user to be the homeowner after it is linked with a person.
- : Reset the password of an app user. The app user will need to log in to the app with the new password.
- : Link an app user to a person.
- : Delete an app user. The user can no longer log in to the app. If the user is also a homeowner, all app accounts in the corresponding room will be deleted, and all people in this room can no longer log in to the app.

4.6.5 Synchronizing Contacts

Send room information to a VTO and then you can view it on the VTO or its webpage.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Video Intercom** in the **App Config** section.
- Step 2 Click **Contacts Sync**.
- Step 3 Send room information.

- Select a VTO, and then click  of a room.
- Select a VTO, and then click **Send Contacts** to send all or selected rooms.

Now you can view the room information on the VTO or its webpage. If any room cannot be sent, the reason will be provided.

Related Operations

After sending room information successfully, you can delete it from the VTO, then it will not be displayed on the VTO or its webpage anymore.

- Click  to delete one room at a time.
- Click **Delete Contacts** to delete all or selected rooms.

4.6.6 Setting Private Password

Set room door passwords so that the room door can be opened by entering password on the VTO (outdoor station).



Make sure that contacts are sent to the VTO; otherwise you cannot set private password.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Video Intercom** in the **App Config** section.
- Step 2 Click **Private Password**.
- Step 3 Select a VTO, and then you can see all the VTHs linked to this VTO.
- Step 4 Select a VTH and click , or select several VTHs and click **Change Password**.
- Step 5 Enter password, and then click **OK**.

You can use the new password to unlock on the VTO.

Results

Use room number + private password to unlock the door. The room number consists of 6 digits. For example, a person who lives in 1001 with the private password of the VTO in the building being 123456, can enter **#001001123456#** to unlock the door.

4.6.7 QR Codes

Configure the information of the QR codes that are used by homeowners to download the App and register an account.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Video Intercom** > **QR Codes**.

Step 2 Enter a name and some notes for your community, and then click **Save**.

Homeowners can scan the **QR Code for App Download** to download and install the App on the phone, and then scan the **QR Code for App Registration** to register. For how to register, see the user manual of the App.

4.6.8 App User

You can view information of App users, freeze user, modify login password and delete user.

Prerequisites

App users have registered by scanning the QR code on the platform or the VTH. For details, see the user manual of the App.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Video Intercom** in the **App Config** section.

Step 2 Click **App Users**.

Table 4-29 Parameter description

Operation	Description
Freeze APP user	The App user cannot log in for 300 seconds after being frozen. The account will be frozen when invalid password attempts exceeds 5 by an App user.
Change APP user login password	Click  , enter a new password on the Reset Password page, and then click OK .  - The password must be 8 to 16 characters and include numbers and letters. - Click  to display password, or  to mask password.
Refresh the list of App users	Click Refresh to display the App users that recently registered.
Delete APP user	Click  to delete App users one by one, or select multiple App users, click Delete , and then follow the instructions to delete them. The users can no longer log in to the App. If a user is a homeowner, all App accounts in the corresponding room will be deleted, and all people in this room can no longer log in to the App.

4.7 Visitor Management

After appointment is made on the platform, and visitor information is registered, the visitor has the access permission. Access permission is disabled after the visitor leaves.

4.7.1 Preparations

- Access control devices and lift control devices have been added to the platform.
- Basic configurations of the platform have been finished. For details, see "3 Basic Configurations".
- Configure email server first if you want to send emails to the visitor. For details, see "7.4.5 Configuring Email Server".

4.7.2 Configuring Visit Settings

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Visitor**.



You can also go to the **Visitor Config** page by selecting **Access Management** > **Visitor**, and then clicking  at the lower-left side.

Step 2 Configure the parameters.

Table 4-30 Parameters of configuring visitor

Parameter	Description
Create Appointment	The platform administrator can configure visitor appointment information and send the link to visitors' emails or provide QR codes. Visitors can enter the link or scan the QR code to fill out their visitor information. After approval, visitors will receive an access pass via email.
Host Invitation	The system supports creating appointment by visitors (see "5.4.3.4.2 Creating Appointment by Visitors") and host invitation (see "5.4.3.4.3 Appointment Invited by Host").  Make sure that LAN and WAN mapping is configured. For details, see "2.7 Configuring LAN or WAN".

Parameter	Description
Appointment Expiration Config	Enable Configure Appointment Expiration Time, and then set the timeout period. If the visitor does not visit within the defined period after the appointment, the appointment will automatically expire. For example, if the visitor's appointment arrival and leaving time are set to 9:00 am and 9:00 pm respectively, and the expiration time is set to 1 hour, the appointment will be invalid if the visitor does not arrive at 10:00 am; if the expiration time is set to 13 hours, then the appointment will be invalid at 9:00 pm.  • The appointment will expire after the appointment leaving time expires. • The appointment will expire if the appointment is not approved after the appointment leaving time. • The visitor status will be automatically updated at the defined time of each day. It is 2:00 am each day by default.
Visitor Registration	• Arrival and registration: Enable the function, and then select the channels as needed. Visitors with appointment can verify their identities on the selected channels without registering. • Leave registration: ◇ Enable the function, and then select the channels as needed. Visitors who are visiting can verify their identities on the selected channels to end their visits automatically. ◇ Set the visitor on-site notification time (10 am every day by default). When a visitor has not left after the visit time, the platform sends notifications to users with permissions of the visitor management menu to remind them of the number of visitors that overstayed.
Visitor Access Permission	Set the access permission group for visitors. Set the access permission group for visitors, including access control, video intercom, lift control and parking lot. Access permission control has the following 3 security levels. • Low security level: After enabling the automatic visit access point from Visitor > Visitor Registration > Arrival and Registration, and selecting the channel, if the corresponding channels are also selected when adding the visitor access permission group, the visitor can be automatically authorized to enter when the visitor visits. • Medium security level: Automatic visit and permission group are not enabled, and only automatic leave is enabled. When the visitor visits, manual registration and authorization are required, but authorization and registration are not required when leaving. • High security level: Automatic visit and leave are disabled, and default permission group is not configured. Registration and authorization are required for both visit and leave.
Visitor Pass	Customize the content of remarks on a visitor pass.

Parameter	Description
Email Template	Click Visitor Appointment (Visitor) , Visitor Appointment (Host), Visitor Arrival or Visitor Leave to set an email template, and then the system will automatically send emails when visitors or hosts make an appointment, visitors arrive for their appointment or end their visit. You can customize the email subject and content with the visitor information by entering information or selecting the fields such as Visitor Name and Visitor Company.

Step 3 Click **Save**.

4.8 Parking Lot

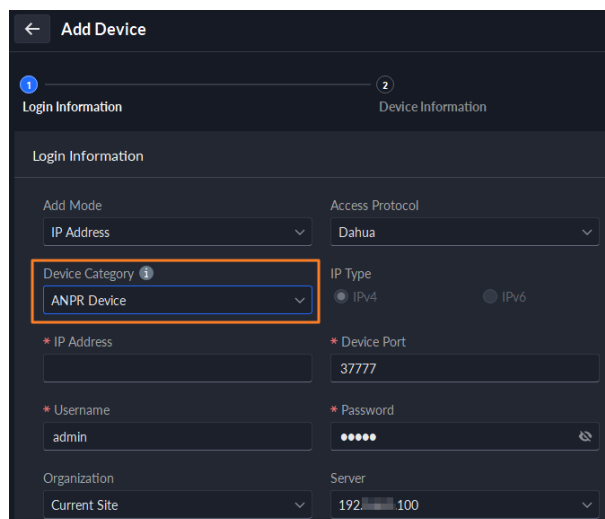
Configure entrance and exit point of the parking lot, barrier opening rules, number of parking space, event parameters, vehicle group, and more to realize barrier opening management, parking space management, event management, and more.

4.8.1 Preparations

Make sure that the following preparations have been made:

- Devices, such as ANPR cameras, parking space detectors, VTOs, and displays for available parking spaces are added to the platform.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
 - ◇ When adding an ANPR camera, set **Device Category** to **Access ANPR Device**.

Figure 4-39 Set device category



The screenshot shows the 'Add Device' configuration interface. It has two main sections: 'Login Information' and 'Device Information'. In the 'Login Information' section, the 'Device Category' dropdown menu is highlighted with an orange box, and 'ANPR Device' is selected. Other fields in this section include 'Add Mode' (set to 'IP Address'), 'Access Protocol' (set to 'Dahua'), 'IP Type' (radio buttons for 'IPv4' and 'IPv6'), 'IP Address', 'Device Port' (set to '3777'), 'Username' (set to 'admin'), and 'Password'. The 'Device Information' section includes 'Organization' (set to 'Current Site') and 'Server' (set to '192.168.1.100').

After you have added ANPR cameras, you can bind video channels to their channels. This is available when you have installed other cameras at the entrance to view and record videos of the entire scene, not just the vehicle. You can view the video from the bound camera when checking the alarm details. For how to bind channels, see "3.1.3 Binding Resources".

- ◇ When adding an NVR, set **Device Category** to **Encoder**.



NVR devices are used for transparent transmission of ANPR camera events, as well as for storing images and videos.

- ◇ Select **Entrance ANPR** from **Features** for the corresponding NVR channels.



Applicable only in scenario without barrier of entrance and exit mode.

- ◇ When adding VTO, set **Device Category** to **Video Intercom**.

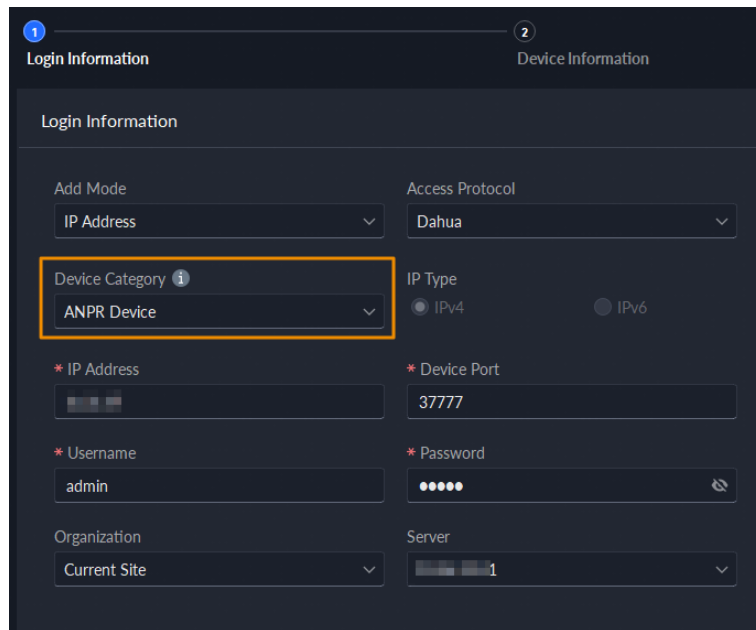
Also, you need to add the information of people and assign them permissions so that they can use the VTO normally. For details, see "4.3 Personnel and Vehicle Management".



Make sure that the configurations of building and unit on the DSS client are the same as the device. If building and unit are enabled on the platform, they must also be enabled on the device, and vice versa. Otherwise, the VTO will be offline after being added. For details, see "4.6.3 Configuring Building/Unit and Call Mode".

- ◇ Add a vehicle parking space detector
- Set **Device Category** to **ANPR Device**.

Figure 4-40 Add a parking space detector



Set the **Device Type** to **Indoor Parking Space Detector** or **Outdoor Parking Space Detector**.

- **Indoor Parking Space Detector** : Supports license plate recognition.
 - **Outdoor Parking Space Detector** : Supports license plate recognition and available space count mode.
- ◇ Add a screen.

Add a display for available parking space. Set **Device Category** to **Display Device**. Dahua screen and Jiuzhou screen are supported as the display for available parking space.

- ◇ Snapshots taken by ANPR cameras are stored in the **Images and Files** disks. You must configure at least one **Images and Files** disk so that snapshots of vehicles can be normally displayed. For details, see "3.3 Configuring Storage".

- If it is necessary to enable access recognition for personnel through the VTO, then personnel need to be added and authorized, and open barrier by two-factor verification should be enabled. For details, see "4.3 Personnel and Vehicle Management" and "4.8.2.1 Adding Parking Lots".

4.8.2 Configuring Parking Lot

A parking lot includes parking spaces, entrances and exits, barrier control rules and other information. Link an ANPR camera for recognizing license plates, and a VTO for abnormal situation call.

4.8.2.1 Adding Parking Lots

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Parking Lot** > **Parking Lot Configuration** > **Parking Lot Basic Config**.
- Step 2** Add parking lot organizations.
1. Click , and then configure the organization name, parent organization and roles allowed to access.
 2. Click **OK**.
- Step 3** Select a parking lot organization, and then click  to add a parking lots.
- 
- Up to 16 main parking lots can be added. Every main parking lot can add up to 16 sub parking lots.
- Step 4** Configure the basic information of the parking lot, and then click **Next Step**.

Table 4-31 Parameter description

Parameter	Description
Parking Lot Name	To differentiate from other parking lots.
Parking Lot Organization	Select the organization to which the parking lot belongs.
Parking Lot Mode	• Entrance and Exit Mode : The parking lot has access management. • No Entrance and Exit Mode : This is generally used for managing open parking areas, primarily through vehicle detector to manage parking spaces. For example, street parking.
Enable Parking Space Counting	• Count parking spaces by entering and exiting vehicles : Set up the total and available parking spaces in the parking lot, and then the parking spaces will be automatically counted based on each vehicle that enters or exits the parking lot. • Count parking spaces using parking space detectors : After parking space detectors are added to the platform and configured, parking spaces will be automatically counted.

Parameter	Description
Entry and Exit Rule	In the no entrance and exit mode, you can configure entry and exit rule. ● Default : When a vehicle is parked in a space, it means it is inside the parking lot. When it leaves the parking space, it is considered as having exited the parking lot. ● Custom : Configure the interval. If a vehicle parks in a space that is different to its previous one during the interval, the vehicle is still in the parking lot. This rule only applies to parking spaces that have monitoring cameras which support ANPR.
Reset Available Parking Space	In the entrance and exit mode, enable Enable Parking Space Counting and Count parking spaces by entering and exiting vehicles before configuring Reset Available Parking Space. ● For reset type, you can select Reset to Total Parking Space, Auto Calculate Available Parking Spaces Based on Vehicles in Parking Lot and Reset to Specified Available Parking Spaces. ◇ Reset to Total Parking Space : You can enable or disable the function of clearing vehicles in parking lot automatically. After the function is enabled, the platform automatically clears the vehicles in the parking lot at the specified time and reset the available parking spaces to the total parking spaces. After the function is disabled, the platform automatically reset the available parking spaces to the total parking spaces. ◇ Auto Calculate Available Parking Spaces Based on Vehicles in Parking Lot : The available parking spaces will be automatically calculated based on the currently present vehicles. ◇ Reset to Specified Available Parking Spaces : you can configure the available spaces and the vehicles in the parking lot will not be cleared. ● Reset time: The default reset time is at midnight each day. You can customize the reset time.

Parameter	Description
Fuzzy Match of Entrance & Exit Plate No. Snapshot	● First Character Rule ◇ 1 character added to the front of the plate number: It will still be considered as a match when an additional character is added to the plate number. For example, AB12345 is recognized as AAB12345. ◇ Missing the first character of the plate number: It will still be considered as a match when the first character is missing from the plate number. For example, AB12345 is recognized as B12345. ● Last Character Rule ◇ 1 character added to the end of the plate number: It will still be considered as a match when an additional character is added to the end of the plate number. For example, AB12345 is recognized as AB123455. ◇ Missing the last character of the plate number: It will still be considered as a match when the last character is missing from the plate number. For example, AB12345 is recognized as AB1234. ● Misread Character Rule: It will still be considered as a match if a character is recognized incorrectly, but the number of characters is correct. For example, AB12345 is recognized as AB12B45.  When you enable multiple rules, the platform will check if each rule is satisfied. Only when one or more rules are satisfied will platform consider it to be a match. For example, 1 character added to the front of the plate number, and missing the first character of the plate number are both enabled. When the plate number AB12345 is recognized as AAB12345, it satisfied 1 character added to the front of the plate number, but not missing the first character of the plate number. This will be considered as a match. If the plate number AB12345 is recognized as AB112345, it does not satisfy both rules. This will not be considered as a match.
Auto overwrite when captured vehicle has not exited	If a vehicle entered the parking lot but has not exited, a new entry record will be generated when the vehicle is recognized to have entered again. The original entry recorded will be changed to a forced exit record.  After enabled, when there are 0 available parking spaces in the parking lot for authorized vehicles on site, 0 remaining parking spaces for personnel, and 0 remaining parking spaces for vehicle groups, access is still permitted.
Filter Invalid Access Records	Click  to enable the function, and then set the time range. Vehicles with multiple access records within the set period, only after their first access record will be retained. All the others will be filtered out.

Step 5 Configure the entrance and exit points, and then click **Next Step**.



The platform supports up to 128 entrances and exits from all parking lots.

1. Click **Add Entrance and Exit Point**.
2. Enter a name (for example, south gate), and then click **OK**.
3. Select a mode for the entrance point.

- **With Barrier** : It is generally used for managing closed parking lots, and the platform can configure entry and exit rules to determine whether vehicles need to automatically open the barrier based on these rules.
- **Without Barrier** : It is generally used for managing open parking lots, such as gas stations, service areas, and similar scenarios, where it only records vehicle passage.



When EVS or IVSS transparently transmits the images or videos of the events, we recommend selecting the **Without Barrier** mode.

4. If there is an entrance point, click  in the **Entrance** section.
5. Enter a name for the point, select a capture mode, and then add a camera, video intercom device (optional).

If limited by the surroundings, you can install two cameras for this point to extend the capture range, and then set **Capture Mode** to **Dual Camera** to improve the successful rate of recognition number plates.

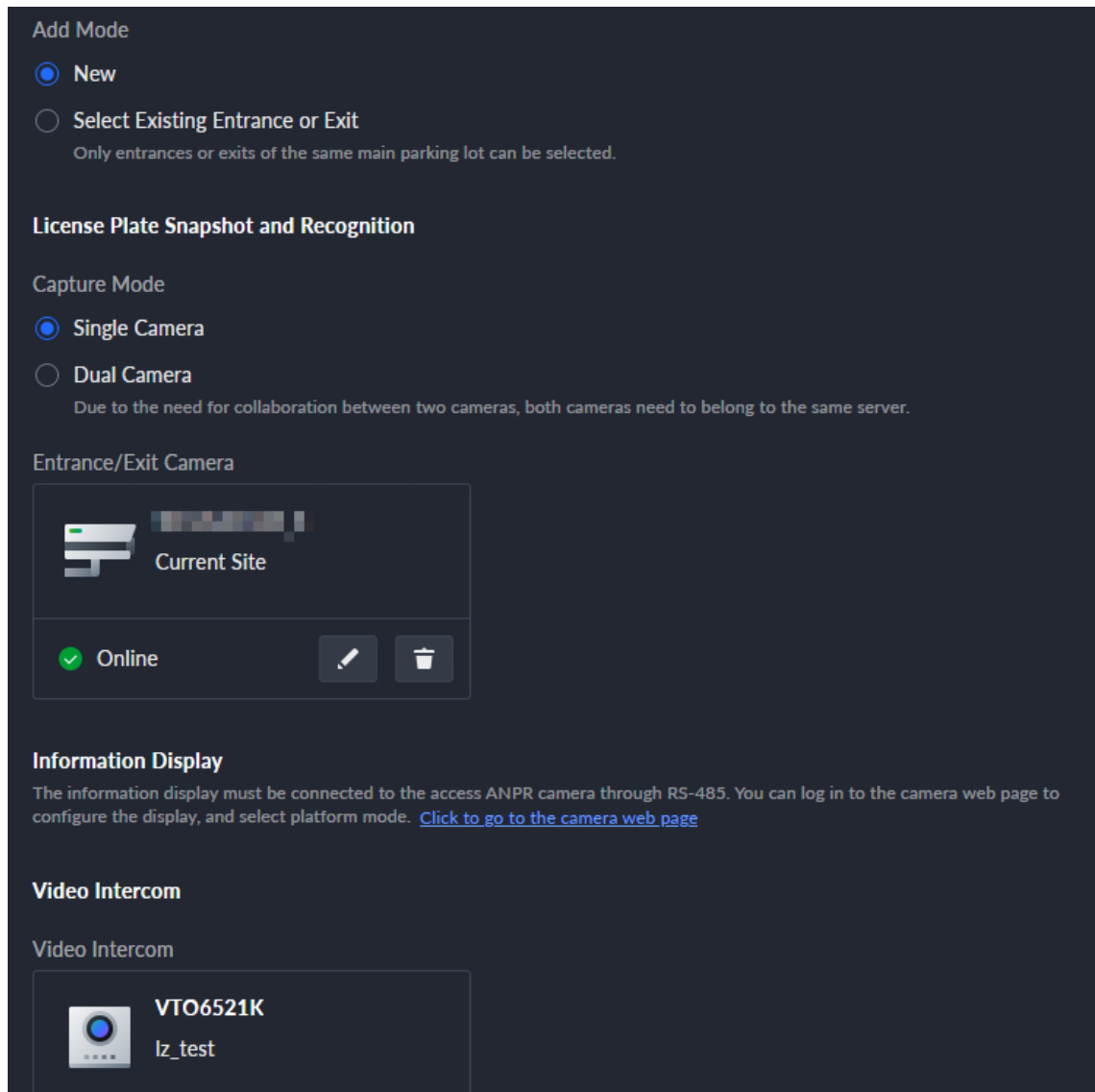
In **Dual Camera** mode, the vehicles captured by the two cameras within the defined **Dual Camera Coordinative Time** will be considered as the same one. You must configure the time properly according to the installation positions of the cameras and the distance between them.



The 2 cameras must be added to the same server.

When adding entrance or exit points for sub parking lots, you can select the existing entrance or exit points of the main parking lot.

Figure 4-41 Entrance point configuration




Click **Click to go to the camera web page** to open the device web page.

6. If there is an exit point, click  in the **Exit** section, and then configure the parameters.

The parameters are similar to the ones in **Entrance**. For details, see the steps above.

Step 6 Configure the passing rules, and then click **Next Step**.



If all the entrances and exits in the parking lot select **Without Barrier** mode or reusing the existing entrances and exits in the parking lots, you do not need to configure the passing rules.

1. Select a vehicle entrance rule, and then configure the parameters.

Table 4-32 Parameter description

Parameter	Description
Registered Vehicles	Allow Passage When Available Space is 0 : After being enabled, vehicles are allowed to enter the parking lot even if there are no available parking spaces. Click  to enable this function for an entrance point.  This function is available only when parking space counting is enabled and the parking space counting mode is Count parking spaces by entering and exiting vehicles for the parking lot.
All Vehicles	All vehicles can enter the parking lot. ● Allow Passage When Available Space is 0 : After being enabled, vehicles are allowed to enter the parking lot even if there are no available parking spaces. ● Allow Unlicensed Vehicles to Enter : Vehicles with no license plates can also enter the parking lot. ● Allow Vehicles on the Blocklist to Enter : Vehicles on the blocklist are also allowed to enter the parking lot.

Parameter	Description
Custom	You can customize the passing rule for the entrance. A more flexible direction rule configuration allows users to set passing rules based on their specific needs for certain special scenarios. Registered Vehicles Access Rule Click Add , and then select By Parking Lot or By Point. By parking lot: The vehicle groups will be added to all entrance and exit points of the parking lot, and the vehicles in these group can enter and exit through any entrance or exit. By point: You can add different vehicle groups to different entrance or exit points. For example, vehicle group is added to the east entrance but not the south entrance, then the vehicles in the group can only enter the parking lot through the east entrance. - Click  to enable Allow Passage When Available Space is 0, and then the vehicle groups will be synchronized. When the available space is 0, the vehicles in these added groups can enter and exit the parking lot. All Vehicles : Select a default time template or create a new one, and then any vehicle can enter the parking lot within the specified duration. For how to create a new time template, see "3.1.6 Adding Time Template". Open Barrier by Verification : Configure rules, the access permission of a vehicle must be verified, and then an administrator can manually open the barrier for it. None : No additional verification is required; barrier opens directly according to the configured passing rules. Open Barrier by Manual Verification : The barrier opens automatically after the vehicle has been successfully verified through card or face. Open Barrier Directly by Verification : The barrier opens automatically after the vehicle has been successfully verified through card or face. Open Barrier by Two-Factor Verification : Configure vehicle owner or vehicle color verification. Verification by Vehicle Owner : The barrier opens automatically after a vehicle has been successfully verified through the license plate and a verification method such as card or face. Verification by Vehicle Color : The barrier opens automatically after a vehicle has been successfully verified through its license plate and the color of the vehicle.  You can enable Automatically opens the barrier even if the vehicle color fails to be verified, and then the barrier opens when the vehicle color fails to be verified. Available Parking Space Counting  You must enable parking space counting and select Count parking spaces by entering and exiting vehicles. Count each vehicle as an occupied parking space : The number of parking spaces decreases after a vehicle enters. Count each unregistered vehicle as an occupied parking space : The number of parking spaces decreases only after vehicles that are not added to the vehicles groups of the current parking lot enter. Custom : Configure the vehicle groups that do not need to calculate available parking spaces, while all other vehicles need to calculate available parking spaces.



For how to configure vehicle groups, see "4.8.4 Managing Vehicle Group".

2. Select a vehicle exit rule, and then configure the parameters.

The parameters are similar to the ones in the entrance. See the previous step.

3. Enable **Send Plate No. to Devices**, and then add vehicle groups to the allowlist and blocklist.

Devices can use this information to determine which vehicles to let in when the platform is offline.

Step 7 (Optional) Configure parking space detection, and then click **Next Step**.



If you do not need to calculate parking spaces by using parking space detectors, you can skip this step and click **Next Step**.

1. Click **Add** or **Add Parking Space**.



You need to add parking space detectors to the platform first. For how to add parking space detectors, see "3.1.2 Managing Device".

2. Select the parking space detectors that belong to this parking lot, and then click **OK**.

Step 8 (Optional) Add indoor and outdoor parking space available display screens to the parking lot and configure the content to be displayed, and then click **Save and Exit**.

For different device protocols and models, the content that can be displayed varies. The content includes arrows, placeholders (for displaying parking spaces), numbers, letters, icons, and the color of the display when there are parking spaces available or the parking lot is full. The sources for the placeholders can be one of the following options:

- **Count parking spaces by entering and exiting vehicles** : Displays the number of parking spaces based on the total number and available parking spaces of the parking lot.
- **Selected Parking Spaces** : Only displays the number of parking spaces from the parking space detectors you select.
- **Count parking spaces by parking space detectors** : Displays the number of parking spaces from all parking space detectors in this parking lot.

Related Operations

- : Edit the passing rules of the parking lot.
- : Edit the available parking space of the parking lot.

4.8.2.2 Parking Lot Layer

Add a plan view image to the parking lot, and then mark the entrance and exit points, parking spaces, parking space available displays, and monitoring devices on it, so that you can manage the parking lot in an intuitive way. If a parking lot needs to be managed in multiple areas, multiple layers can be added for a single parking lot.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Parking Lot** > **Parking Lot Configuration** > **Parking Lot Layer Config**.
- Step 2 Select a parking lot, and then click **Add**.
- Step 3 Enter a name for the layer, upload an image, and then click **Save and Configure Layer**.

- Step 4 Drag an entrance or exit point to the image.
- Step 5 Click the **Parking Space** tab, drag a parking space to the image, adjust its size and direction.
- Step 6 Click the **Parking Space** tab, and then drag a parking space detector to the image.
- Step 7 Click the **Parking Space Available Display** tab, and then drag a parking space available display to the image.
- Step 8 Click **Vehicle Search Point** tab, and then drag a vehicle search point to the image.
- Step 9 Click the **Monitoring Location** tab, and then drag a channel of a monitoring device to the image.
- Step 10 Click **Save and Exit**.

Related Operations

- : Edit the name and image of the layer.
- : Delete the layer.

4.8.2.3 Parking Lot Event

4.8.2.3.1 Event Parameter

For certain parking lot events, such as parking over time, it is necessary to initialize and configure the corresponding event parameters in order to perform anomaly detection.

Procedure

- Step 1 Configure an event, and you need to select **Parking Lot** as the type of event source. For how to configure an event, see "4.1 Configuring Events".
- Step 2 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Parking Lot** > **Parking Lot Configuration** > **Event Parameter Config**.
- Step 3 Select a parking lot, events that were configured will be displayed on the right.
- The following events will not be displayed because there are no additional parameters to be configured.
- Blocklist alarm: An alarm will be triggered when a vehicle on the blocklist enters the parking lot.
 - Reserved parking space alarm: An alarm will be triggered when a vehicle parks in a parking space, but its plate number is not linked to the parking space.
 - Parking over line: An alarm will be triggered when a vehicle crosses a line after it is parked.
- Step 4 Click  to configure an event.

Table 4-33 Parameter description

Parameter	Description
Overtime Parking in Parking Lot	● Overtime Parking Rule : Select the overtime parking rule from the drop-down list, and then overtime parking detection will be performed according to the rule. For the detailed information of overtime parking rule, see "4.8.2.3.2 Overtime Parking Rule". ● Detection Interval : How long the platform will check which vehicles have parked overtime. For example, select 5 minutes, then the platform will check whether there are vehicles that have parked overtime in the parking lot. If yes, then an alarm will be triggered. ● Vehicles to Trigger Alarms : ◇ All Vehicles : All vehicles will trigger alarms if they park overtime, but VIP vehicles are not included. If you enable Include VIP Vehicles, VIP vehicles will also trigger alarms when they park overtime. ◇ Non-registered Vehicle and Vehicle in the Blocklist : The vehicles whose information is not registered to the platform will trigger alarms when they park overtime. ◇ Custom : Enable Non-registered Vehicle, and then the vehicles whose information is not registered to the platform will trigger alarms when they park overtime; enable Registered Vehicle and add vehicle groups, and then the vehicles in these groups will trigger alarms when they park overtime.  You can enable Non-registered Vehicle and Registered Vehicle at the same time.
Overtime Parking in Parking Space	● Overtime Parking in Parking Space : The unit is minute. Alarm will be triggered if a vehicle has parked for longer than the defined value. ● Parking Space : ◇ If All Parking Space is selected, select the overtime parking rule from the drop-down list, and then the overtime parking in parking space detection will be performed according to the rule. ◇ If Select Parking Space is selected, click Add to add parking spaces that need to be configured. ◇ If Parking Space Category is selected, click Add to add parking space category that need to be configured. ● Parking Space Detection Camera that Supports License Plate recognition : After enabling, a parking space monitoring camera that supports ANPR must be connected, and then the vehicles to trigger alarms should be configured. After being disabled, you can configure all vehicles to trigger alarms.
No Entry and Exit Record	● No Entrance/Exit Record Duration : The unit is day. When there are entrance/exit records and no new entrance/exit records exist within the duration after the last record, it is determined that there are no entrance/exit records. ● Statistical Time Point : The platform will start calculating the duration of a vehicle that has not entered or exited the parking lot on the defined time. ● Entrance and Exit Vehicle Group of Interest : Only calculate the duration for the vehicles in the vehicle groups that are added.

4.8.2.3.2 Overtime Parking Rule

The overtime rules can be configured to have different overtime durations for various time periods each day, while no overtime detection is performed during other times. You can configure up to 6 overtime parking rules for each day.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Parking Lot** > **Parking Lot Configuration** > **Event Parameter Config** > **Overtime Parking Rule Config**.
- Step 2 Click , and then configure the parameters.

Figure 4-42 Add rules

Rule Info

* Rule Name

Rule1

☒ Copy From

Rule Details

Sunday

Monday

Tuesday

Wednesd...

Thursday

Friday

Saturday

+ Add

Copy To

Period	Overtime Parking Threshold	Operation
10:00 - 23:59	10 Minutes	
12:00 - 00:00	10 Minutes	
13:00 - 00:00	10 Minutes	
14:00 - 00:00	10 Minutes	

Overtime parking detection will not be performed during periods that were not configured.

OK

Cancel

Table 4-34 Parameter description

Parameter	Description
Rule Name	Configure the rule name to differentiate it from others.
Copy From	Select the check box, and then select a rule from the drop-down list to reuse the existing rules.

Parameter	Description
Rule Details	View the rule details or add new period. Click Add to add overtime parking period and set over time parking threshold.  Click Copy To to copy the configured rules to another times.

Step 3 Click **OK**.

4.8.2.4 Vehicle Finder

Enable vehicle search for parking lots, so that vehicle owners can find where their vehicles are parked through the vehicle search system. For parking lots configured with vehicle detectors, specific parking spaces can be identified. However, for parking lots that only have entrance and exit points, it is only possible to locate the parking lot where the vehicle is parked.

Prerequisites

Parking space detectors have been configured for the parking lot. They are used to provide exact locations of vehicles.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Parking Lot > Vehicle Search Config**.

Step 2 Click **Add**, and then configure the parameters.

Table 4-35 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Unlicensed Vehicle Search	If enabled, the unlicensed vehicle will be searched.
Display Vehicle Snapshots	If enabled, the snapshots of vehicles will be displayed.
Fuzzy Search	If enabled, fuzzy search will be supported on the vehicle search page.
Parking Lots Allowed to be Searched for	Select the parking lots you want to enable vehicle search for.
Upload Vehicle Search Interface Logo	You can customize the logo on the page of the vehicle search system. The logo must not exceed 256 KB.

Step 3 Click **Add**.

The rules will be effective immediately after added.

Related Operations

- Add Point URL

Click  to add point URL. When searching for a vehicle, you can query the vehicle by scanning the location points, and the location of the point can be retrieved.

1. On the **Configure the point URL** page, click **Add**.
2. Configure the point name, and then select the parking lot and enter the IP address.
3. Click **OK**.

4. Select **Parking Lot Layer Config**, and then click **Vehicle Search Point** to add the point URL to the parking lot layer.
 - Click  to copy the link, and then you can use it to visit the vehicle search system in a browser.
 - Click  to view the QR codes. Vehicle owners can scan them via their phones to visit the vehicle search system. You can download the QR codes to your computer, or send them to a defined email address.

4.8.3 Managing Parking Space

4.8.3.1 Parking Space Category

Classify the parking spaces in the parking lot. After classification, parking spaces can be managed by category.

Parking Space Category

1. Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Parking Lot > Parking Space Management > Parking Space Category**.
2. Click **Add**, and then configure parameters.

Figure 4-43 Add parking space category

Add Parking Space Category

Basic Info

* Name: 456

* Parking Lot: A-changed1

* Color: Brown

Remarks:

Add Parking Spaces to the Category

Select Parking Space (0-1000)

Search...

☒	Parking Space ID	Device Name	IP	Organization
☒	P1_3_1	--	--	--

Selected(1)

P1_3_1

OK Cancel

- Click **OK**.

Parking Space List

- Log in to the DSS Client. On the **Home** page, click and then in the **App Config** section, select **Parking Lot** > **Parking Space Management** > **Parking Space Category** > **Parking Space List**.

Figure 4-44 Parking space list

☒	Parking Space ID	Parking Lot	Organization	Parking Space Category	Operation
☒	P1_3_1	A-changed1	112		
☐	P1_3_2	A-changed1	112		
☒	P1_3_3	A-changed1	112		

- Click to change the category.

Select multiple parking space, and then click **Change Category** to change category in batches.



A single parking space supports up to 5 categories, with each category able to accommodate up to 1000 parking spaces. The number of unclassified parking spaces is unlimited.

4.8.3.2 Reserved Parking Space

Link one or more parking spaces to one or more plate numbers. Alarms will be triggered if vehicles with other plate numbers park in this parking space.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Parking Lot > Parking Lot Configuration > Reserved Parking Space Config**.
- Step 2 Select a parking lot, and then click **Add**.

Figure 4-45 Link a parking space to plate numbers

←

Added the reserved parking space group

Basic Info

* Reserved Parking Space Group Name

11122233

Parking Lot

A-changed1

Reserved Parking Space

Add Type

☒ Add by Parking Space Category
The category must have parking spaces under it with vehicle detectors that support license plate recognition.

☐ Custom

Parking Space Category

testA

Vehicles that Can be Parked

Add Mode

☒ Add By Vehicle Group
If a new vehicle is added to the vehicle group, it will be automatically added to the reserved parking space group.

☐ Add By Vehicle

Select Vehicle Groups

Search...

☒ All

Selected(6)

General

VIP

2222444-----

OK

Cancel

- **Add Type**
 - ◇ **Add by Parking Space Category** : You can only select one parking space category, and any newly added parking spaces will be automatically added to the designated parking spaces for that category.
 - ◇ **Custom** : Add multiple parking spaces.
- **Add Mode**

165

- ◇ **Add By Vehicle Group** : When adding a vehicle group, any new vehicles that are added to the group will be automatically added to the reserved parking spaces associated with that vehicle group.
- ◇ **Add By Vehicle** : Add multiple vehicles.

Step 3 Enter the parking space group name, select a parking space you want to link plate numbers to, a vehicle group, and one or more plate numbers, and then click **OK**.

4.8.4 Managing Vehicle Group

Add vehicles to different groups, so that you can quickly apply different parking lot functions to multiple vehicles at the same time. General, VIP, and blocklist are the default groups. If you need to use them, you can directly add vehicles to them.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Parking Lot > Vehicle Management > Vehicle Group**.

Step 2 Click .

Step 3 Enter a name, select a color for the group, and then select the parking lot that the vehicle group belongs to.

Step 4 Click  of a group, and click **Select from Vehicle List**, select the vehicles that you want to add to the group, and then click **OK**.



Select **Vehicle List**, configure the search conditions and then the results will be displayed on the right. Click **Select from Vehicle List** to add vehicles.

Related Operations

Available Parking Spaces

1. Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Parking Lot > Vehicle Management**.
2. Select a parking lot, and then available parking space to display available parking space information.
 - **Available Parking Spaces for Person** : Display available parking space information for person.
 - **Available Parking Spaces for Vehicle Group** : Display available parking space information for vehicle.
3. Click **Add**, and then configure the parameters of the available parking space.
4. Click **OK**.

4.8.5 Configuring Scheduled Report

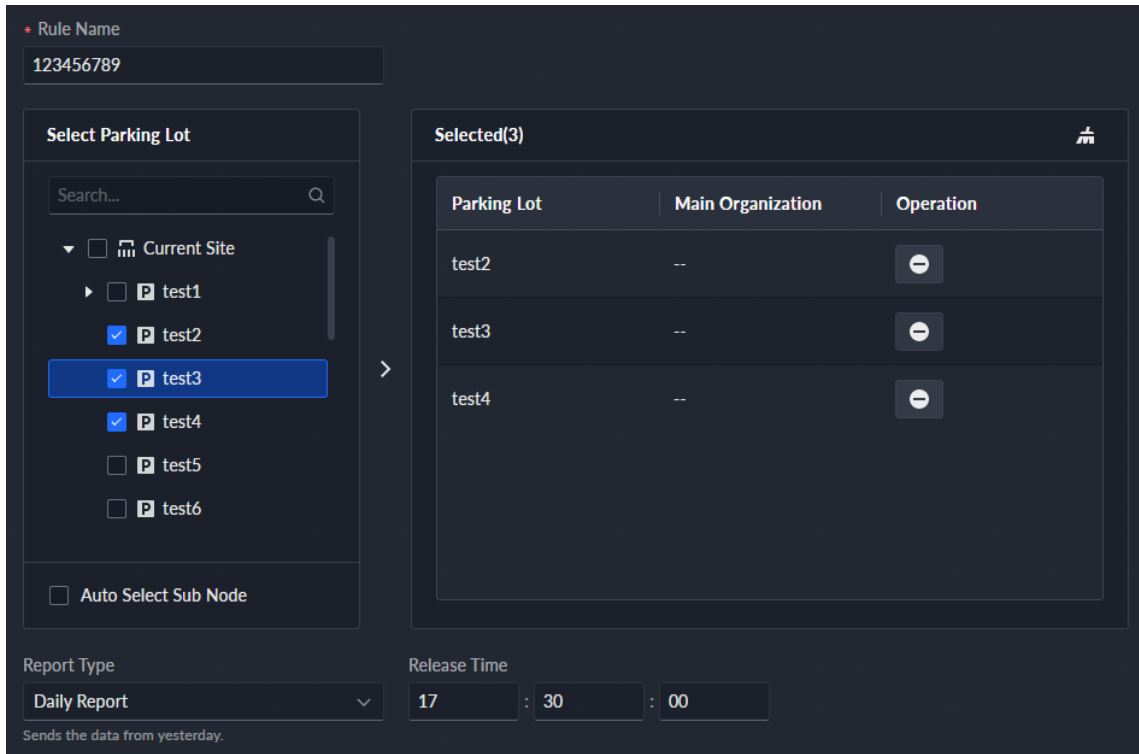
Procedure

Step 1 Log in to the client. On the **Home** page, click , and then in the **APP Config** section, select **Parking Lot > Scheduled Report Config**.

Step 2 Click .

Step 3 Configure the parameters of the basic information and email information.

Figure 4-46 Configure the information



Rule Name
123456789

Select Parking Lot

Search...

- ☐ Current Site
- ☐ test1
- ☒ test2
- ☒ test3
- ☒ test4
- ☐ test5
- ☐ test6

☐ Auto Select Sub Node

Selected(3)

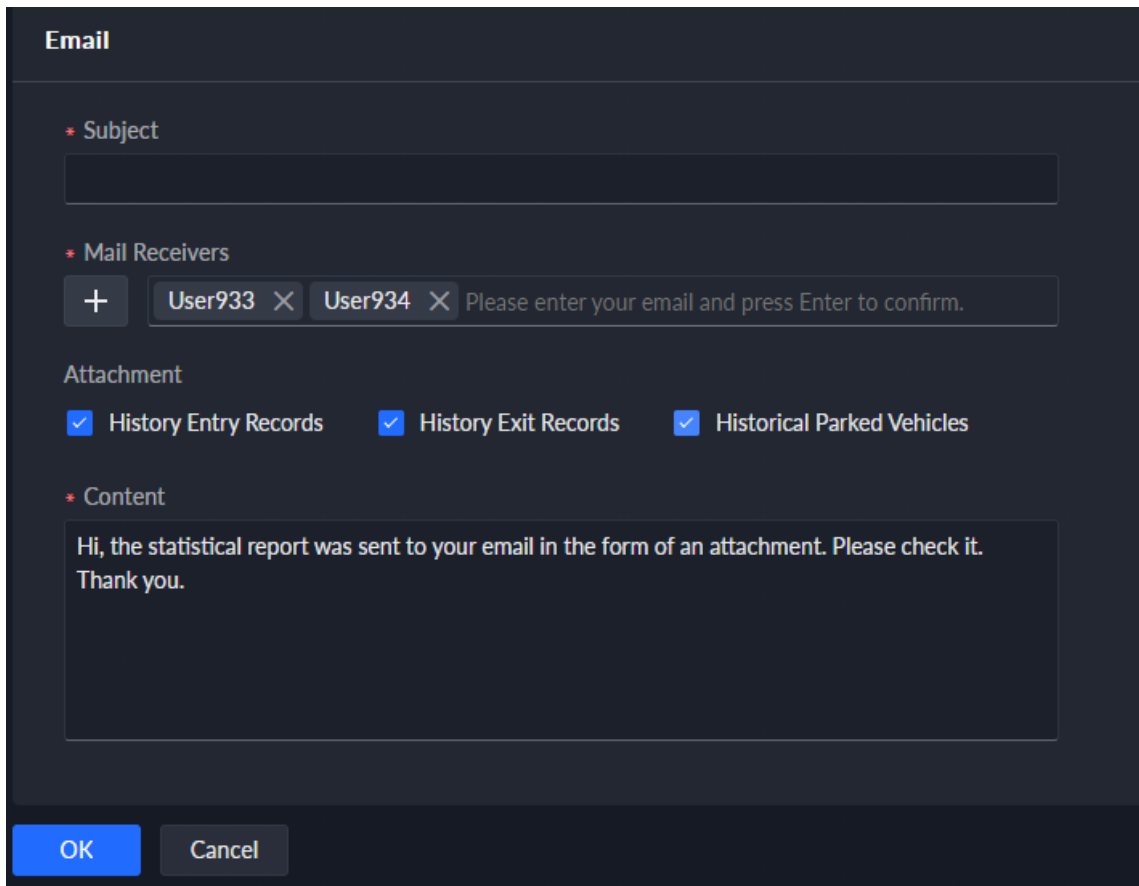
Parking Lot	Main Organization	Operation
test2	--	⊖
test3	--	⊖
test4	--	⊖

Report Type
Daily Report

Release Time
17 : 30 : 00

Sends the data from yesterday.

Figure 4-47 Configure email



Email

*** Subject**

*** Mail Receivers**

+ User933 × User934 × Please enter your email and press Enter to confirm.

Attachment

☒ History Entry Records ☒ History Exit Records ☒ Historical Parked Vehicles

*** Content**

Hi, the statistical report was sent to your email in the form of an attachment. Please check it.
Thank you.

OK Cancel

Step 4 Click **OK**.

The added emails will be displayed in the list. Select the email to view the detailed information.

Related Operations

The added emails are enabled by default, you can click  to disable it.

4.9 Intelligent Analysis

Before using the people counting and scheduled report functions, you must configure them first.

- **People counting:** Create a people counting group and add multiple people counting rules from one or more devices to it. Then, you can view the real-time and historical number of people of the group.
- **Scheduled report:** Configure the when to send a report with historical people counting data, the email address to send the report to, and the content of the email.

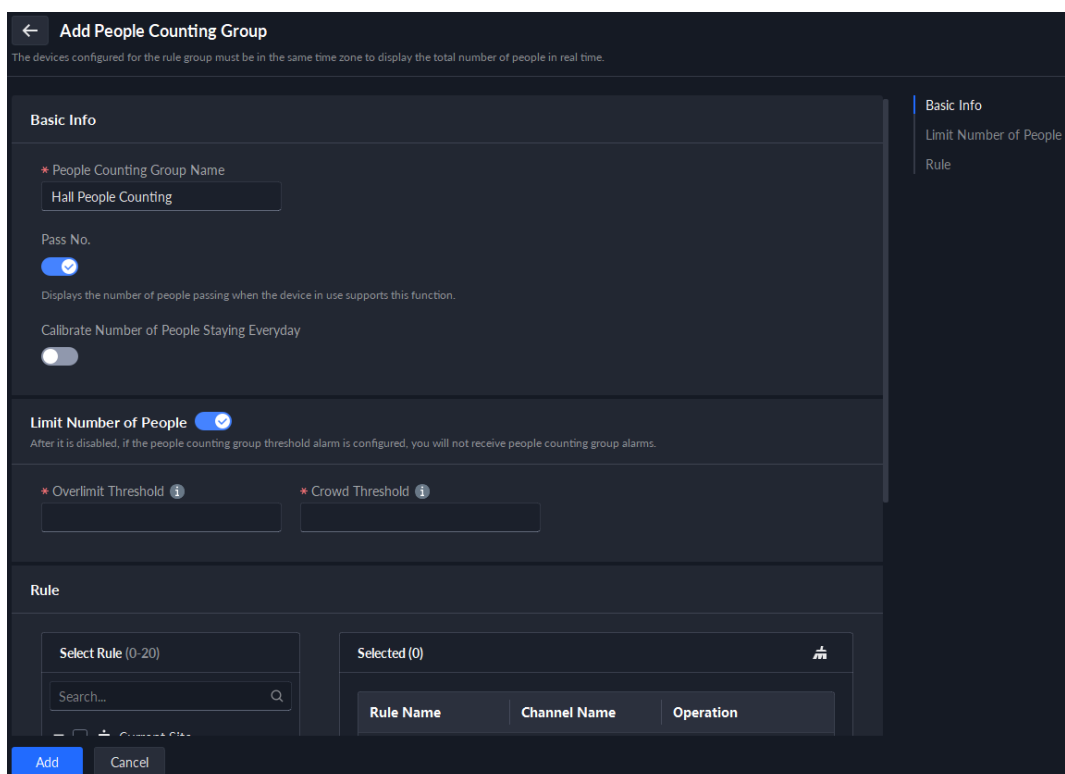
4.9.1 People Counting Group

Create a people counting group, and then add multiple people counting rules from one or more devices. In Intelligent Analysis, you can view the real-time and historical number of people of the group.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Intelligent Analysis > People Counting Group Config**.
- Step 2** Click  at the upper-left corner.
- Step 3** Configure the parameters, and then click **Add**.

Figure 4-48 Add a people counting group



← Add People Counting Group

The devices configured for the rule group must be in the same time zone to display the total number of people in real time.

Basic Info

* People Counting Group Name
Hall People Counting

Pass No.
☒

Displays the number of people passing when the device in use supports this function.

Calibrate Number of People Staying Everyday
☐

Limit Number of People ☒
After it is disabled, if the people counting group threshold alarm is configured, you will not receive people counting group alarms.

* Overlimit Threshold ⓘ

* Crowd Threshold ⓘ

Rule

Select Rule (0-20)
Search...

Selected (0)

Rule Name	Channel Name	Operation
-----------	--------------	-----------

Add Cancel

Table 4-36 Parameter description

Parameter	Description
People Counting Group Name	Name of the people counting group.
Pass No.	The calibration time can only be configured on the hour. It is the start of a counting cycle. - After Pass No. is enabled, the number of people pass by will be displayed. The value will be set to 0 every day on the calibration time by default. - The number of people entered but did not exit will be set to the defined value every day on the calibration time.
Calibrate Number of People Staying Everyday	
Calibration Time	
Calibrated Number of People	
Limit Number of People	When enabled, you can configure the crowd and overlimit thresholds of the people in the group. If an alarm is configured at the same time, alarms will be triggered when the number of people reach the thresholds. For details, see "4.1 Configuring Events". - When the number of people in the group reaches the defined overlimit threshold, the light will turn red. - When the number of people in the group reaches the defined crowd threshold but smaller than the overlimit threshold, the light will turn yellow.
Overlimit Threshold	
Crowd Threshold	
Rule	Select the devices whose people counting rules you want to include in the group, and then their data will be combined together.

4.9.2 Scheduled Report

Historical data will be sent on a regular basis to one or more email address that you set on the scheduled time.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Intelligent Analysis** > **Scheduled Report Config**.
- Step 2** Configure one or more types of report.
- Daily report: Data from yesterday will be sent to your email at a defined time. If set to 03:00:00, the data from the day before (00:00:00–23:59:59) will be sent to your email at 03:00:00 every day.
 - Weekly report: Data from last week will be sent to your email at a defined time. If set to 03:00:00 on Wednesday, the data from Wednesday to Tuesday of each week will be sent to your email at 03:00:00 every Wednesday.
 - Monthly report: Data from last month will be sent to your email at a defined time. If set to 03:00:00 on 3rd, the data from 3rd of last month to 2nd of the current month will be sent to your email at 03:00:00 on 3rd of each month.
- Step 3** Configure one or more email addresses to send the report to, and the content of the email.
- Click  to select the users that have been configured email addresses, or enter an email address, and then press Enter.

Figure 4-49 Invalid email address, you must press Enter

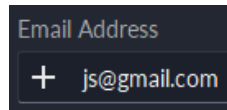
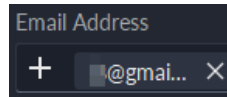


Figure 4-50 Valid email address



2. Configure the content of the email.

Step 4 Send the report.

- Click **Send Now** to immediately send the report that you configured.
- Click **Save**, and then the report will be sent at the defined time.

4.10 Intelligent Inspection

Configure inspection objects and plans so that the platform can regularly inspect devices, such as power equipment, or an area, and collect images and data during the process.

Before using this function, you must:

1. Purchase a license with the intelligent inspection function and activate the license. For details, see "2.1.6 Licensing".
2. Obtain and install the plugin of intelligent inspection. For details, see "2.9 Installing Plugin".
3. Configure image and file and video disks, to store snapshots and recorded videos during inspections. For details, see "3.3 Configuring Storage".
4. Add devices used for inspection to the platform, and configure their video retention periods. For details, see "3.1 Managing Resources".

4.10.1 Configuring Object Template

Configure frequently used object types and inspection points. When you are configuring an actual inspection point, you can select them to automatically fill in most of the information.

4.10.1.1 Adding an Object Type

Customize the name of an object type, such as "circuit breaker".

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Intelligent Inspection** > **Object Template**.
- Step 2** Click .
- Step 3** Enter a name for the object type, and then click **OK**.

Related Operations

- Change the name of an object type
 - Select an object type, and then click  to change its name.
- Delete an object type

Select an object type, and then click  to delete it.

4.10.1.2 Adding Inspection Point

Configure the information of the inspection point of an object type. For example, the area on the circuit breaker to be inspected, items to be inspected, and technologies to be used.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Intelligent Inspection** > **Object Template**.
- Step 2** Click an object type, and then click **Add**.
- Step 3** Configure the parameters, and then click **OK**.
- Or click **Save and Continue** to add more inspection points.

Table 4-37 Parameter description

Parameter	Description
Inspection Area	Click the input box to enter a name manually. If there are inspection points that have been added, you can select an inspection area from the drop-down list.
Point Type	Enter a name for the point type.
Inspection Item	Enter the items to be inspected.
Inspection Item	● Visible Snapshot : The platform will only take snapshots. ● Thermal Temperature Monitoring : Use thermal technology to monitor temperature. You can configure temperature warning threshold and temperature different warning threshold, but they are optional parameters. ◇ Temperature Warning Threshold : Configure the thresholds for low, medium, and high. When the temperature is greater than either one, an alarm will be triggered. ◇ Temperature Difference Warning Threshold : Configure the thresholds for low, medium, and high. When the temperature difference is greater than either one, an alarm will be triggered. The difference is calculated by 2 inspection points. When you are configuring an actual inspection point, you must select another point so that the platform can calculate the difference.

4.10.1.3 Importing Object Types and Inspection Points

If you need to add a lot of object types and inspection points, you can import them to the platform.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Intelligent Inspection** > **Object Template**.
- Step 2** Click .
- Step 3** Click **Download Template**, and then save the template to your computer.
- Step 4** Fill in the information, and then save the changes.



Click  to download a template with common object types and inspection points related to substations for reference.

Step 5 Click **Import File**, and then open the template.

The information is imported to the platform.



If there are inspections points that are already on the platform, their information will be updated.

4.10.2 Configuring Inspection Object

Add inspection objects to so that the platform can inspect one or more points. Inspection objects are managed by inspection organizations. Only specified roles and users can access the certain organizations.

4.10.2.1 Adding Inspection Organization

Inspection organizations are used to manage inspection objects and points. Only administrators can configure them, and specify which roles and their users can access certain organizations.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Intelligent Inspection** > **Inspection Object**.
- Step 2** Click .
- Step 3** Configure the parameters.

Table 4-38 Parameter description

Parameter	Description
Organization Name	Enter a name for the organization.
Parent Organization	This is for permission control. For example, if a user cannot access A, then the user cannot access all the organizations under A.
Roles Allowed Access	Only selected roles and their users can access this organization.  Click  to see the users assigned with the roles.

Step 4 Click **OK**, or click **OK and Add Object** to add objects to this organization.

4.10.2.2 Adding Inspection Object

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Intelligent Inspection** > **Inspection Object**.
- Step 2** Select an organization, and then click **Add**.
- Step 3** Configure the basic information, and then click **Next Step**.

Table 4-39 Parameter description

Parameter	Description
Inspection Object Name	Enter a name for the inspection object.
Organization	Displays the name of the organization you selected from the previous step. You can select another one.
Type of Object to be Sent	Select an object type that has been added. This is optional.

Step 4 Click **Add Point**.

If you select an object type from the previous step, all inspection points in that object type will be automatically added.

Step 5 Configure the information of the point, and then click **OK**.

Table 4-40 Parameter description

Parameter	Description
Point Name	Enter a name for the point.
Inspection Area	Click the input box to enter a name manually. If there are inspection points that have been added, you can select an inspection area from the drop-down list.
Point Type	Enter a name for the point type.
Inspection Item	Enter the items to be inspected.
Inspection Technology	● Visible Snapshot : The platform will only take snapshots. ● Thermal Temperature Monitoring : Use thermal technology to monitor temperature. You can configure temperature warning threshold and temperature difference warning threshold, but they are optional parameters. ◇ Temperature Warning Threshold : Configure the thresholds for low, medium, and high. When the temperature is greater than either one, an alarm will be triggered. ◇ Temperature Difference Warning Threshold : Configure the thresholds for low, medium, and high. When the temperature difference is greater than either one, an alarm will be triggered. The difference is calculated by 2 inspection points. When you are configuring an actual inspection point, you must select another point so that the platform can calculate the difference.

Step 6 Click **Bound Camera**.

Step 7 Configure the parameters, and then click **OK** to bind the point to a channel.

Table 4-41 Parameter description

Parameter	Description
Select Channel	Double-click a channel to be bound. Its live video and information will be displayed on the right.

Parameter	Description
PTZ	If you are binding a PTZ channel, you can operate it by using the PTZ control panel. Also, you must bind to a preset of the PTZ channel. Click  , and then click  of a preset to bind it to the point. For how to configure presets, see "5.1.2.4.1 Configuring Preset".
Temperature monitoring parameters	- After you bind a thermal channel, you must add a temperature monitoring rule on the live video. The rules include point, line, rectangle, and polygon. The device will take highest temperature in the area included by the rule you set. For example, if you add a rectangle on the live video, then the device will take the highest temperature in that rectangle. Temperature Warning Threshold : Configure the thresholds for low, medium, and high. When the temperature is greater than either one, an alarm will be triggered. Temperature Difference Warning Threshold : Configure the thresholds for low, medium, and high. When the temperature difference is greater than either one, an alarm will be triggered. The difference is calculated by 2 inspection points. When you are configuring an actual inspection point, you must select another point so that the platform can calculate the difference.

Step 8 Click **Save and Exit**.

4.10.3 Configuring Inspection Plan

During the set periods, the platform will inspect the objects and points you selected, and save related data to the platform.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Intelligent Inspection** > **Inspection Plans**.
- Step 2** Select an inspection organization, and then click **Add**.
- Step 3** Configure the basic information, and then click **Next Step**.

Table 4-42 Parameter description

Parameter	Description
Plan Name	Enter a name for the plan.
Plan ID	This is automatically generated. You can edit it as needed.
Inspection Organizations	Displays the name of the organization you selected from the previous step. You can select another one.
Inspection Type	Select a type for the plan. It is used for searching for certain inspection plans.
Processing Time	The processing time works in the following 2 ways: - For the reviewers' reference when they review inspection results. - When there are 5 minutes remaining and the inspection plan is still unprocessed, all users that are allowed to access the organization that this plan belongs to are notified.
Enable	After enabled, this plan is effective after added.

Step 4 Configure the inspection objects and points.

1. Click **Add**.

Only the organization you selected, its sub organizations, and their objects and points are displayed.

2. Select one or more objects, and then click **OK**.

3. Click the up and down arrows to adjust the order of objects and points.

4. Click **Next Step**.

Step 5 Configure the time of execution, and then click **OK**.

Table 4-43 Parameter description

Parameter	Description
Execution Mode	● By Period : The plan is automatically executed within the specified periods. ◇ Execute at a Specified Time : The plan will be executed at a specified time. ○ Daily Cycle at a Specified Time : The plan will be executed at defined time every day. ○ Weekly Cycle at a Specified Time : The plan will be executed at defined time every week. ◇ Looping : Configure the looping interval, and then the plan will be executed within the effective periods at every interval you configure. For how to create a time template, see "3.1.6 Adding Time Template". ● Only Once : The plan will only be executed once after added or at defined time.
Execution Strategy	
Inspection Interval	Inspection interval between inspection points. The default value is 10 seconds, ranging from 5 seconds to 300 seconds.
Light Mode	Select whether to turn on the light on devices during inspection. Because it might take time for devices to turn on their light, you can configure a warm-up period to make sure that light can be normally turned on before inspection starts.

4.10.4 Configuring Temperature Monitoring Event

If you have configured warning thresholds in inspections, you can configure events to perform linkage actions when thresholds are reached. For example, an inspection point monitored a temperature that is greater than the threshold, a camera will record a video of the area it is monitoring. For details, see "4.1 Configuring Events".

4.11 Maintenance Center

Configure alert rules to monitor servers and devices so that you can handle them timely to ensure that the system is working properly. You can also configure video storage detection. You will be prompted if the duration or integrity of recording is abnormal.

4.11.1 Configuring Alert Rule

Configure alert rules to monitor servers and devices so that you can handle them timely.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Maintenance Center > Alert Rule Config**.
- Step 2** Click .
- Step 3** Configure the parameters, and then click **OK**.

Table 4-44 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule. It can be up to 50 characters.
Alert Level	Select a level for the alert. This is used to quickly know the urgency of the alert when it is triggered.
Rule Execution Time	The alert will only be triggered within the defined period.
Monitoring Targets	Targets include servers and devices. You can select different alert sources for each of them.
Rule Conditions	Set the threshold for each condition. When the value is greater than or equal to the threshold, the alert will be triggered.
Push Notifications	After enabled, you can select the users who will receive notifications when the alert is triggered.
Email Notification	After enabled, you can customize the content to be sent to specified email addresses. You can configure the email addresses in the following ways: - Click  to select the email addresses of users. - Manually enter an email address, and then press Enter.

4.11.2 Configuring Video Integrity

The platform will continue to check the duration and integrity of the videos. You will be prompted if the one of them is abnormal. For example, 30 days of duration and video integrity have been configured for channel A. If there are only 24 days of video, or the video does not last for 24 hours on any day, the platform will give corresponding prompts.

Prerequisites

Recording plans have been configured for channels and videos have been recorded.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Maintenance Center** > **Video Integrity Config**.
- Step 2** Click .
- Step 3** Configure consecutive storage days, and then select the channels for detection.
- Step 4** Click **OK**.

Results

Select  > **Maintenance Center** > **Resource Monitoring** > **Device Status**, and then click  of the device configured with storage detection.

If the duration of video is not enough, the number of days will be displayed in red. If the duration of video for a day is less than 24 hours, the integrity status will be abnormal and displayed in red.

4.12 AR

Through the AR panoramic image, and adding tags to the targets in the real-time video, you can quickly get the information of the targets when watching the video.

Before using this function, note that:

1. Purchase a license with the AR function and activate the license. For details, see "2.1.6 Licensing".
2. The AR function is only available for panoramic + PTZ cameras.
 - When adding a panoramic + PTZ camera on the **Device** page, set **Device Category** to **Encoder**, and **Device Type** to **IPC**.
 - Change the channel feature of the panoramic + PTZ camera to **AR**. For details, see "3.1.2.5.2 Modifying Device Information".

4.12.1 Configuring System Name

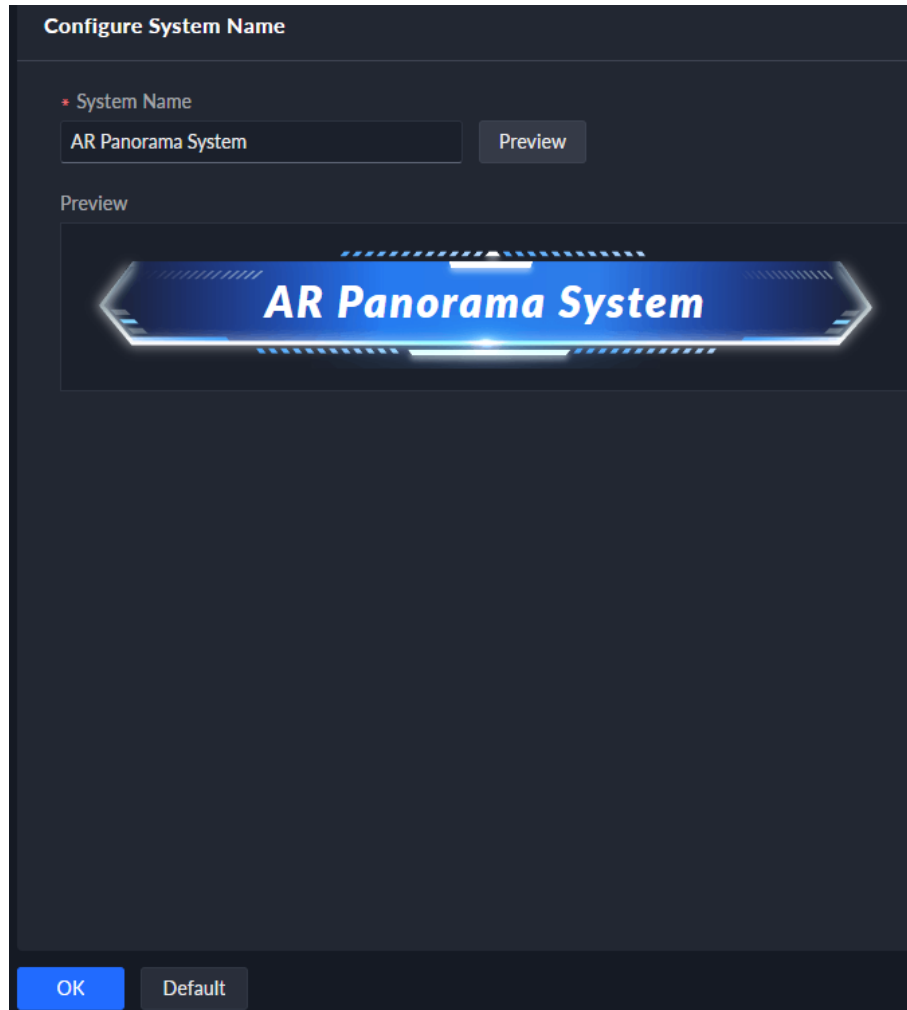
Define the name of the AR system. The name will show on the AR homepage in the monitoring center.

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **AR** > **System Name Config**.
- Step 2** Enter the system name, and then click **Preview** to preview the name.
- Step 3** Click **OK**.



Click **Default** to restore the name to its default value.

Figure 4-51 Configure system name



Configure System Name

* System Name

AR Panorama System

Preview

Preview

AR Panorama System

OK Default

4.12.2 Configuring Tag Template

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **AR > Template Config**.
- Step 2 Click **Add**, and then you can start adding the template.
1. Select template type (**Video**, **Building**, **Parking Lot**, **Airport Plate**, **Post Office**, **Hospital**, **Bank**, and **Station**), and customize the template name.
 2. Select layout (here uses **Horizontal Layout** as an example).
 3. Select the tags, and then click **Save**.

Figure 4-52 Add tag template

Basic Info

Template Type

Video

Template Name

Template Config

Select Layout

☒ Horizontal Layout

☐ Vertical Layout

Select

☒ Tag Name

☒ Priority

☒ Live View

☒ Video Playback

☒ Image

☒ Linked Channel

☒ Remark

Selected

Tag Name

Priority

☒ General

☐ Important

Linked Channel

Remark

Save

Return

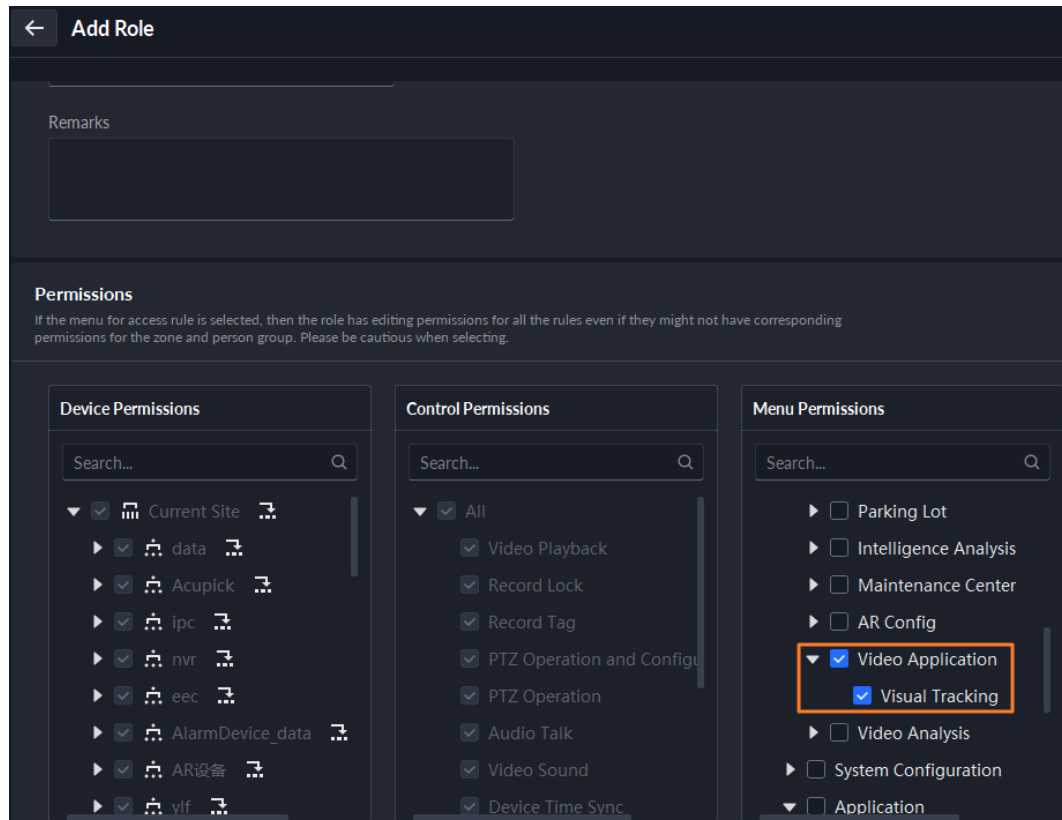
4.13 Configuring Visual Tracking

By configuring visual tracking, you can overlay icons that correspond to adjacent cameras over the video. Clicking the icons, you can quickly jump to the associated cameras, to follow a target across different areas or locations, without losing sight of the target, as long as the places that the target passes through are covered by the associated cameras.

Prerequisites

You need to have the **Visual Tracking** menu permission from  > **User** > **Role Management**.

Figure 4-53 Select visual tracking permission



Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Video Application**.



Select **Configured**, and then you can filter the channels configured with visual tracking.

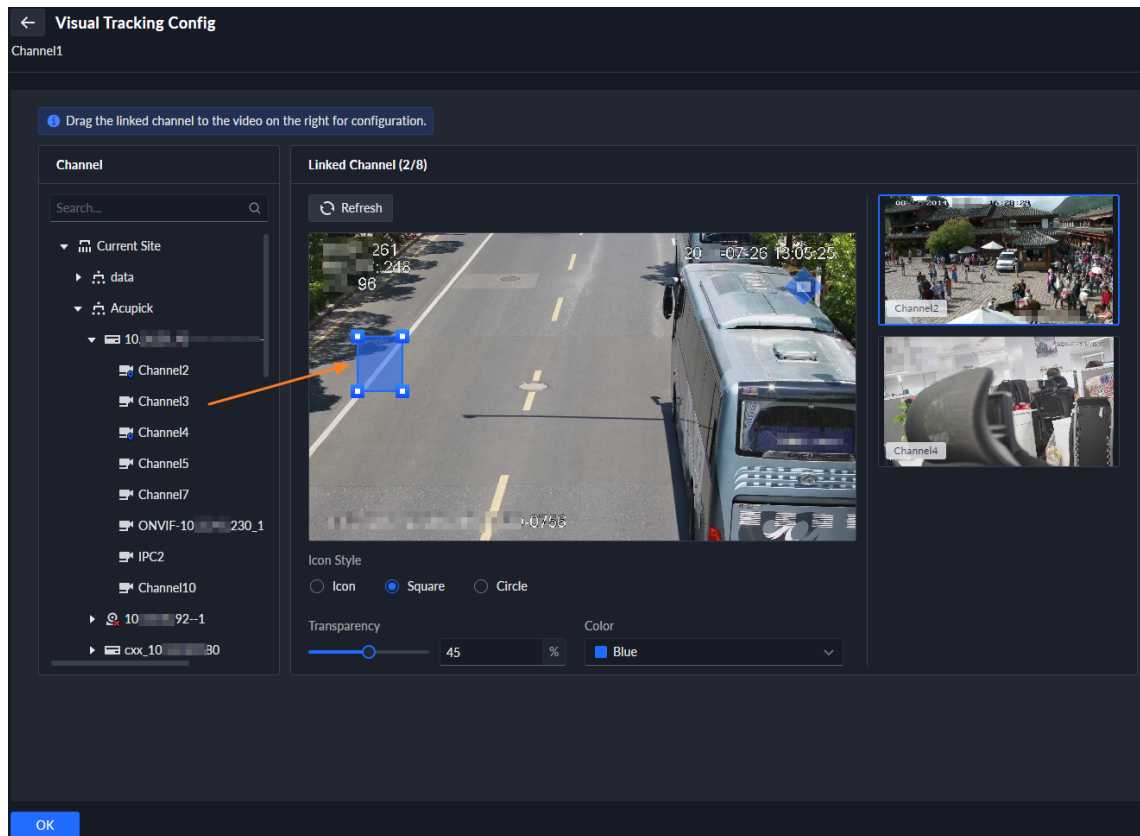
- Step 2** Select a channel from the resource tree on the left, and then click  to start configuring visual tracking.



Click , and then you can refresh the channel cover.

- Select an adjacent camera from the resource tree, and drag it to the video image of the displayed relayed camera.
 - 1 camera can be associated with 8 adjacent cameras.
- Select the icon style overlaid on the video image, and set the transparency and color (only square and circular icon styles support setting colors).
 - Drag the icon over the video image to adjust the icon position.
 - Square and circular icons can be resized.
- Hover over the adjacent camera, and then you can perform the following operations.
 - Click  to view the channel video.
 - Click  to refresh the channel cover.
 - Click  to associate adjacent channels with the current channel.
 - Click  to remove the channel from the associated channel.

Figure 4-54 Configure visual tracking



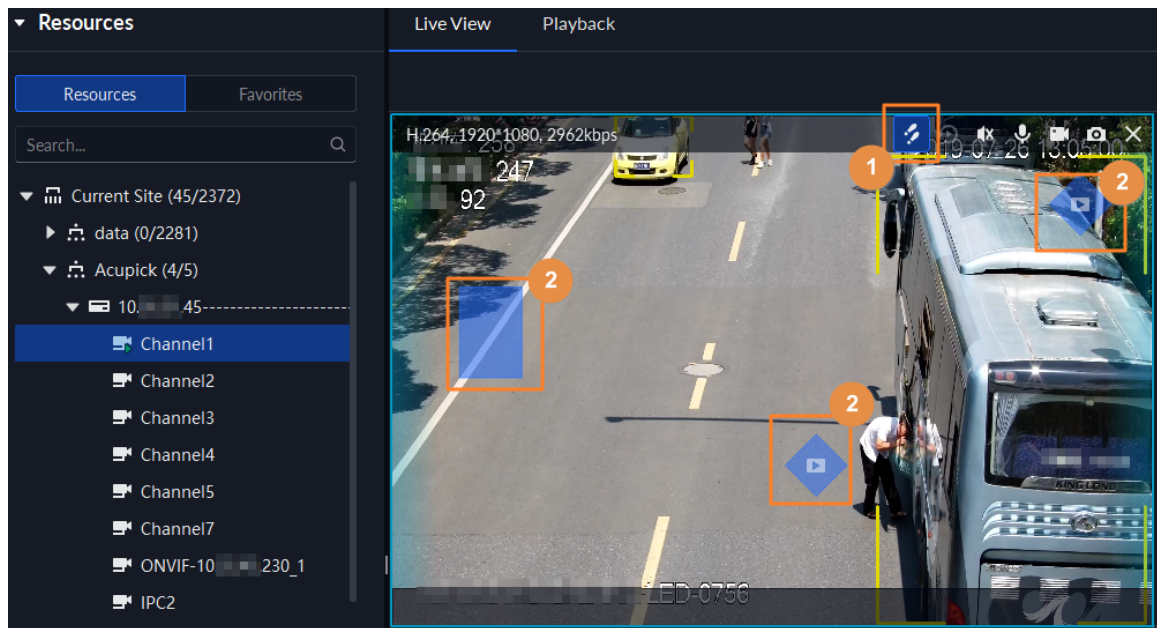
Step 3 Click **OK**.

Results

Go to  > **Monitoring Center** > **Monitoring**, select **Live View** or **Playback**, and then click  to turn on visual tracking.

After that, you can click the shape over the video image to view the video of associated channels, so that you can track the area or location where the target passes through.

Figure 4-55 Visual tracking in live view or playback



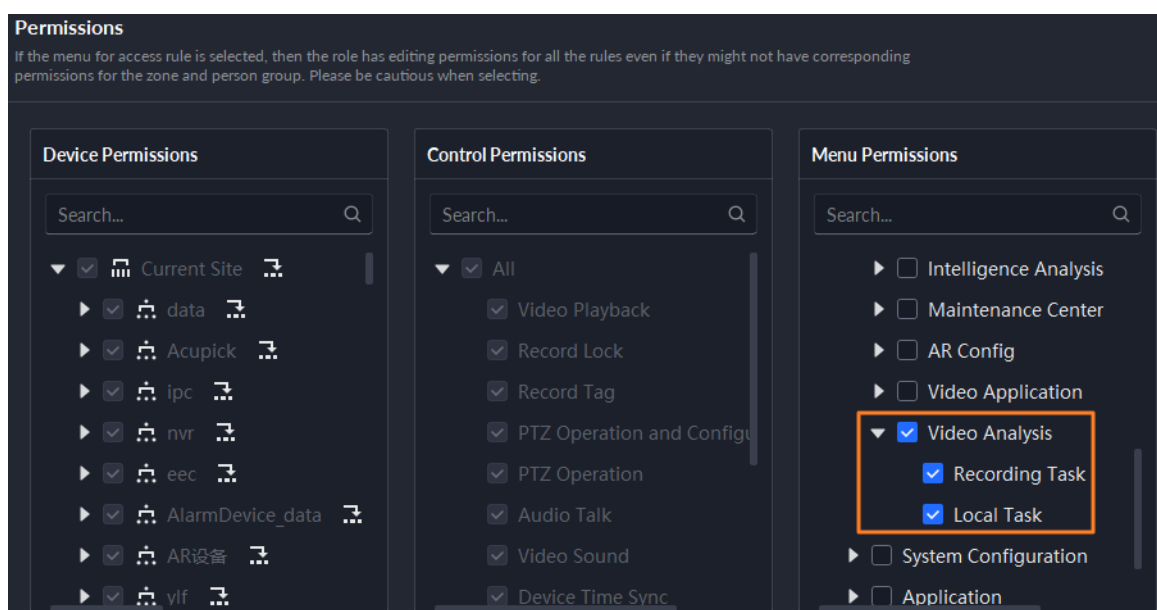
4.14 Video Analysis

Supports performing video analysis on local videos and recorded videos (including central recordings and device recordings). You can view the analysis results on the **DeepXplore** page.

Prerequisites

You need to have the **Video Analysis** menu permission from  > **User** > **Role Management**.

Figure 4-56 Select video analysis menu permission



4.14.1 Adding a Recording Task

Add a video analysis task to be performed on the central recordings or device recordings, to analyze face, human body, motor vehicle and non-motor vehicle. You can search for the analysis results on the **DeepXplore** page.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click and then in the **App Config** section, select **Video Analysis** > **Recording Task**.
- Step 2** Click **Add**, and then configure the recording task.

Table 4-45 Parameter description

Parameter	Description
Task Name	The name that identifies the task.
Target to be Analyzed	Select the target object to be analyzed. Face cannot be selected at the same time as human body, motor vehicle, and non-motor vehicle.
Select Channels	Click to select a channel from the channel list, or click to select a channel from the map.
Analysis Time	Select how long the analysis will be performed. You can select 1 hour at most.
Storage Location	Select the storage location for the video recording. It is Central Storage by default.
Intelligent Analysis Device	Select the IVSS device that performs video analysis. When there are multiple intelligent analysis devices, the one with the largest number of available intelligent capabilities will be displayed by default. The intelligent analysis device can be configured in System Parameters > Central Intelligent Server .

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

The analysis task is enabled by default.



Click of a failed task to view the failure reason.

Figure 4-57 Recording task

Recording Task						
Add Delete Enable Disable Task or Channel Name						
☒	Task Name	Channel Name	Task Progress	Analysis Results	Analysis Status	Operation
☒	123	ip-...1-100...	100%	0	Failed	
☐		Channel4-45	100%	419	Completed	
☐	12	Channel2-45	100%	992 0 0	Completed	
☐	ren	Channel1-45	100%	1436	Completed	

Results

After the analysis is completed, click  to go to the **DeepXplore** page to view the analysis results.

Related Operations

- Click  next to **Analysis Status**, and then you can filter the tasks by the status, which includes all, executing, stop, failed, and completed.
- Click  to enable a task; select tasks, and then click **Enable** to enable them in batches.
- Select tasks, and then click **Disable** to disable them in batches.
- Click  to edit the task name.
- Click  to delete the analysis task; select tasks, and then click **Delete** to delete the selected tasks.

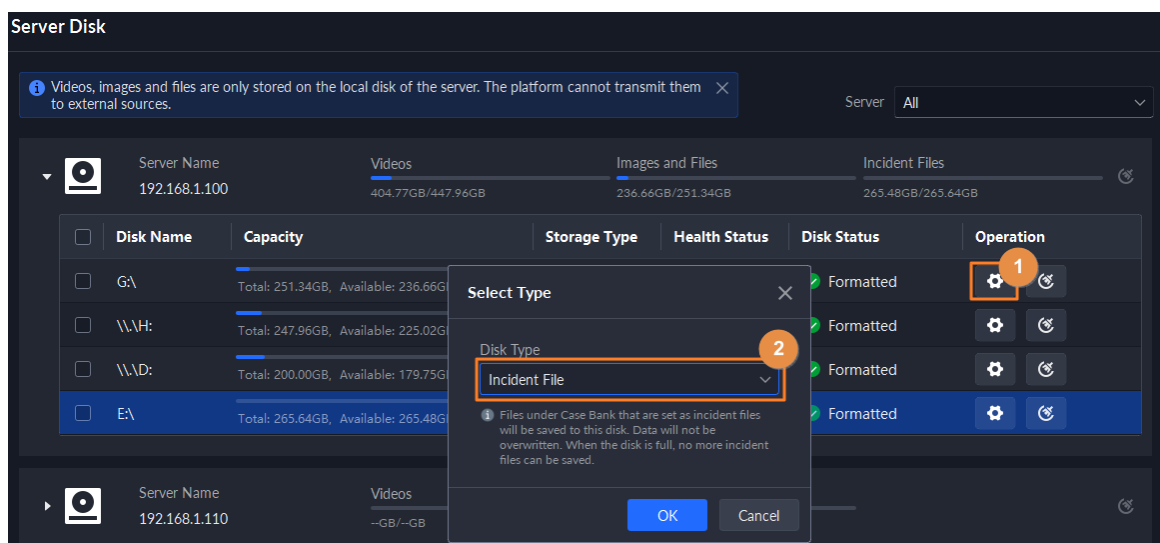
4.14.2 Adding a Local Task

Add an analysis task for the local video to perform video analysis on faces, human bodies, motor vehicles, and non-motor vehicles. You can search for the analysis results on the **DeepXplore** page.

Prerequisites

Go to **Storage > Server Disk**, and then set the disk type of at least one disk to **Incident Files**.

Figure 4-58 Disk type



Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Video Analysis > Local Task**.
- Step 2** Click **Add**, and then configure the local task.

Table 4-46 Parameter description

Parameter	Description
Task Name	The name that identifies the task.

Parameter	Description
Target to be Analyzed	Select the target object to be analyzed. Face cannot be selected at the same time as human body, motor vehicle, and non-motor vehicle.
Video Type	Supports videos in .mp4 and .dav formats.
Upload Video	Click Import , and then upload a video of the selected type.
Time	Select how long the analysis will be performed. You can select 1 hour at most.
Intelligent Analysis Device	Select the IVSS device that performs video analysis. When there are multiple intelligent analysis devices, the one with the largest number of available intelligent capabilities will be displayed by default.  The intelligent analysis device can be configured in System Parameters > Central Intelligent Server .

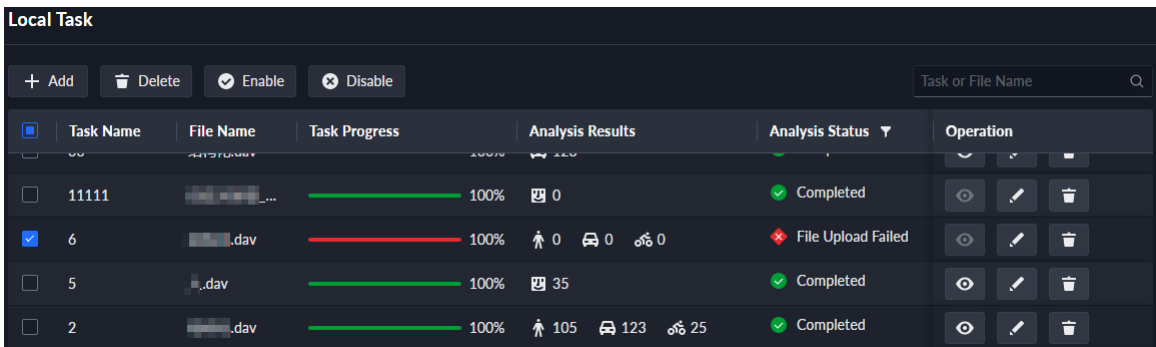
Step 3 Click **OK**.

The analysis task is enabled by default.



Click  of a failed task to view the failure reason.

Figure 4-59 Local task



Task Name	File Name	Task Progress	Analysis Results	Analysis Status	Operation
11111	...	100%	0	Completed	  
6	...dav	100%	0	File Upload Failed	  
5	...dav	100%	35	Completed	  
2	...dav	100%	105	Completed	  

Results

After the analysis is completed, click  to go to the **DeepXplore** page to view the analysis results.

Related Operations

- Click  next to **Analysis Status**, and then you can filter the tasks by the status, which includes all, executing, stop, failed, and completed.
- Click  to enable a task; select tasks, and then click **Enable** to enable them in batches.
- Select tasks, and then click **Disable** to disable them in batches.
- Click  to edit the task name.
- Click  to delete the analysis task; select tasks, and then click **Delete** to delete the selected tasks.

4.15 Synthesis

Through integration between the platform and third-party systems, these systems can send events to the platform through bridge, and realize event linkage after configuring event schemes on the platform. The platform can also send device status and events to third-party systems through standard protocols.

Through the data synchronization function, third-party systems can directly obtain access control and attendance data from the platform, and write them into their own databases. Also, through the system integration function, the access control system can be highly integrated with the platform.

4.15.1 Event Transferral

The platform supports multiple protocol bridges for integrating the platform with third-party platforms or systems.

The bridges include:

- General bridge: Used for synchronizing events from third-party systems to DSS platform.
- SNMP bridge: Allows the DSS platform to send its device status and events to other systems through SNMP protocol.
- Modbus bridge: Allows the DSS platform to send its device status to other systems through Modbus protocol. The third-party systems will receive Modbus commands to control access control devices (door open and close).
- BACnet bridge: The BACnet integration provides the ability for the DSS platform to act as BACnet device or host when integrating with third-party systems. It allows the DSS platform to send its device statuses and events to other systems (such as smart building management system) through BACnet protocol.
- SIA Bridge: Allows the DSS platform to send its device (such as alarm controller) status and events to other systems through SIA protocol.



A total of 5 bridges can be added, and only 1 can be added for each kind of bridge.

4.15.1.1 General Bridge

A bridge serves as a connector between the platform and third-party systems, and is responsible for importing events from a third-party system to the platform. It must comply with the connection protocol between the third-party system and the platform. For different systems, the protocol might vary and you might need to develop a new bridge. Before using this function, make sure that the bridge has been deployed and is running.

Procedure

Step 1 Add the third-party system to the allowlist of DSS.

1. Log in to the DSS client, select  > **System Parameters** > **Security Config**.
2. In the **Synthesis Allowlist** area, click .
3. Enter the IP address of the third-party system, and then click **OK**.

Step 2 Configure the bridge project.

1. Select  > **Synthesis** > **Event Transferral**, and then click .
2. Define the project name, and then select **Trigger In** and **Bridge**.
3. Configure the bridge connection information, and then click **OK**.

Figure 4-60 Configure the bridge

←

Add Project

Bridge serves as a connector integrating this platform with third party systems.

Basic Info on Event Transferral

For your security, please go to System Parameters > Security Config > Synthesis Allowlist to add IP addresses to the allowlist that are to gain access.

* Event Transferral Type

Trigger In

* Bridge Type

Bridge

Bridge Connection Info

Bridge Info

* Identity Certificate

x7E...Do

* Secret Key

.....

* IP Address/Domain

* Port

1

Protocol Type

HTTPS

Third-Party Info

IP Address/Domain

Port

Identity Certificate

Secret Key

OK

Cancel

Table 4-47 Parameter description

Parameter	Description
Identity Certificate	Automatically generated. Copy them to the configuration of the bridge.
Secret Key	- Click  to verify your password, and then generate a new secret key. - Click  to verify your password, and then you can click  to copy the secret key.
IP Address/Domain	Enter the IP address or domain name, and port number of the bridge, and select the protocol.
Port	

Parameter	Description
Protocol	
Third-Party Info	Configure the IP address/domain, port, identity certificate, and secret key of the third-party system.

4. Select the created project, and then click **Edit**.

a. In the **Incoming Triggered Event Type** section, add the event type.

You can click  to add an event type, or click **Import** to download the template, fill in the information, and then upload the file to the platform.

b. In the **Status of Incoming Event Source** section, add the event source status.

You can click  to add a status, or click **Import** to download the template, fill in the information, and then upload the file to the platform.



Click  to enable **Composite Mode**. After enabling, if an event source has multiple statuses, the platform will combine and display the statuses based on the defined statuses.

c. In the **Type of Incoming Event Source** section, add the event source type.

You can click  to add a type, or click **Import** to download the template, fill in the information, and then upload the file to the platform.



Click **Extended Info**, and then you can click  to enable displaying extended information in the event; or click **Add** to customize and enable displaying the extended information.

d. In the **Incoming Event Source** section, add the event source.

You can click  to add an event source, or click **Import** to download the template, fill in the information, and then upload the file to the platform.



Click **Extended Info**, and then you can click  to enable displaying extended information in the event; or click **Add** to customize and enable displaying the extended information.

e. (Optional) Enable **Receive and Store Events**, and then the platform will receive and store the events reported through this bridge. If not enabled, you can also define the event linkage actions in **Event > Event Config**.

5. Click **OK**.

Step 3 Configure the event linkage.

1. Go back to the **Home** page, click . In the **App Config** area, select **Event**.

2. Click .

3. In the **Event Source Type** section, select the one that you import from the third-party system.

For details of configuring other event parameters, see "4.1.1 Configuring Event Linkage".

Figure 4-61 Add a third-party event

Event Source Type	Event	Event Source
POS Alarms	Search...	Search...
Combined Event	▼ Third Party Event	☐ Select All
Custom Alarm	☒ 1111	☐ 503
Generic Event	☐ c323	☐ 503
111	☐ e814	☐ 503
test	☐ e80b	☐ 503
	☐ e809	☐ 503
	☐ c305	☐ 503

4. Click **OK**.

4.15.1.2 SNMP Bridge

The SNMP bridge allows the DSS platform to send its device statuses and events to other systems through SNMP protocol. Users of a third-party system do not need to perform additional development. They only need to configure the bridge on the client and their own platform.

Prerequisites

Purchase and activate the **Event Transferral SNMP** license. For details of activating the license, see "2.1.6 Licensing".

Procedure

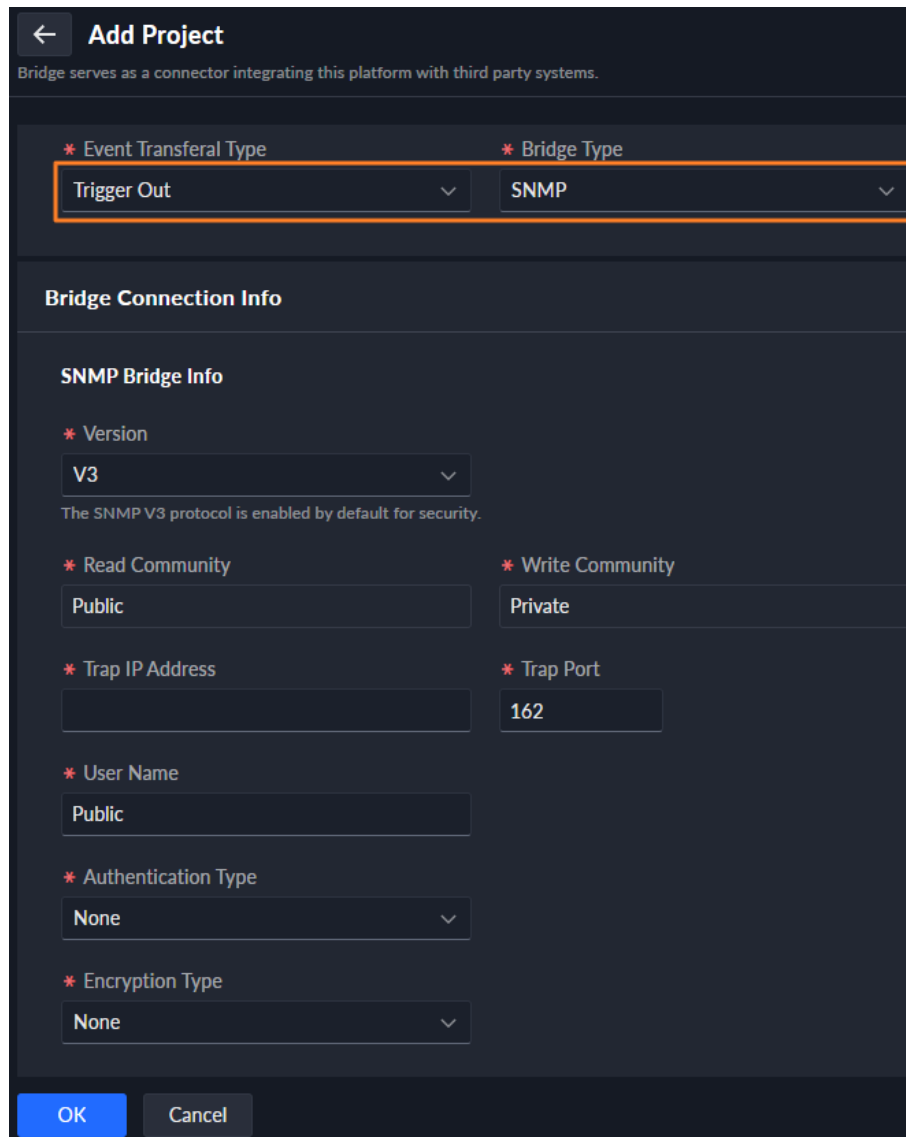
Step 1 Add the third-party system to the allowlist of DSS.

1. Log in to the DSS client, select  > **System Parameters** > **Security Config**.
2. In the **Synthesis Allowlist** area, click .
3. Enter the IP address of the third-party system, and then click **OK**.

Step 2 Configure SNMP project.

1. Select  > **Synthesis** > **Event Transferral**, and then click .
2. Define the project name, select **Trigger Out** and **SNMP**, and then configure the bridge connection information.
 - **Trap IP Address** and **Trap Port**: The IP address and port of the third-party system.
 - **User Name** : The username that the third-party needs to fill in on the DSS platform when establishing a communication connection.
Require when **V3** version is selected.
 - **Authentication Type** : You can select from **None**, **MD5**, and **SHA**. When selecting **MD5** or **SHA**, you need to set the authentication password.
Require when **V3** version is selected.
 - **Encryption Type** : You can select from **None**, **CBC-DES**, or **CFB-AES**.
CBC-DES and **CFB-AES** are available when **Authentication Type** is set to **MD5** or **SHA**. When **CBC-DES** or **CFB-AES** is selected, you need to set the encryption password.

Figure 4-62 Configure SNMP project

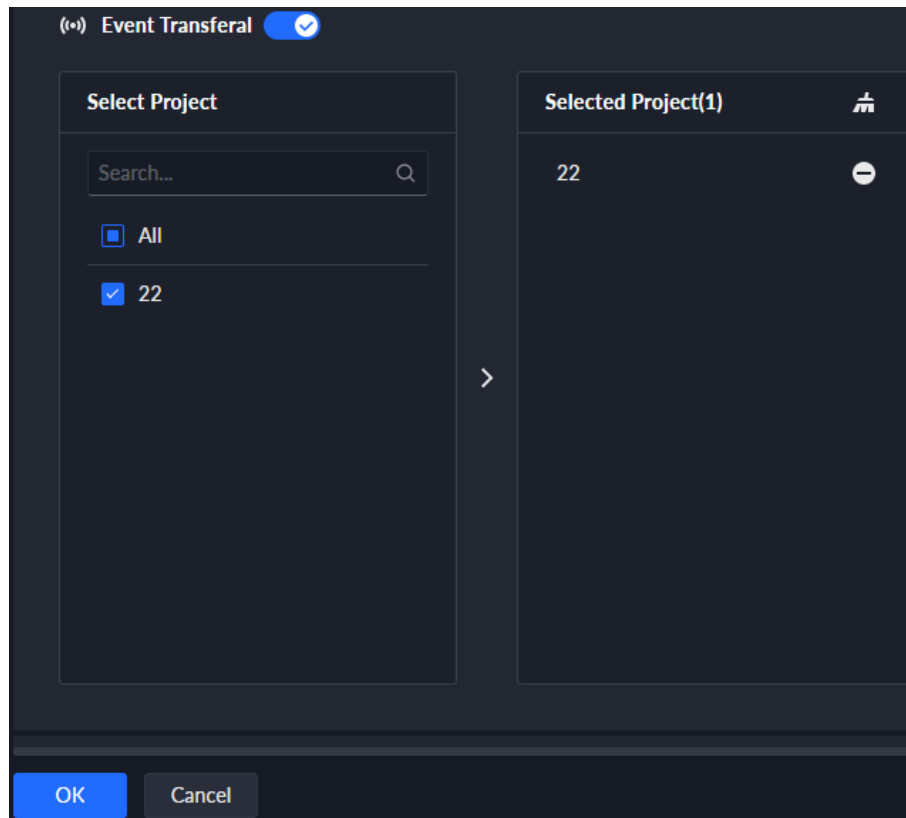


3. Click **OK**.
4. Select the created SNMP project, and then click **Edit**.
5. In the **Event Type and Event Source to be Exported** area, click , and then select the event pushed from the DSS platform to the third-party system (including event source type, event, and event source).
6. Click **OK**.

Step 3 Configure the event linkage.

1. Go back to the **Home** page, click . In the **App Config** area, select **Event**.
2. Click .
3. In the **Event Source** area, select the event source type, event, and event source that are consistent with those defined in [5](#).
4. Enable **Linked Action**, and then enable **Event Transferral**.
5. Select the created SNMP project.

Figure 4-63 Select the created SNMP project



6. Click **OK**.

For details of configuring other event parameters, see "4.1.1 Configuring Event Linkage".

4.15.1.3 Modbus Bridge

The Modbus bridge allows the DSS platform to send its device statuses to other systems through Modbus protocol. The third-party systems will receive Modbus commands to control access control devices (door open and close). Users of a third-party system do not need to perform additional development. They only need to configure the bridge on the client and their own platform.

Prerequisites

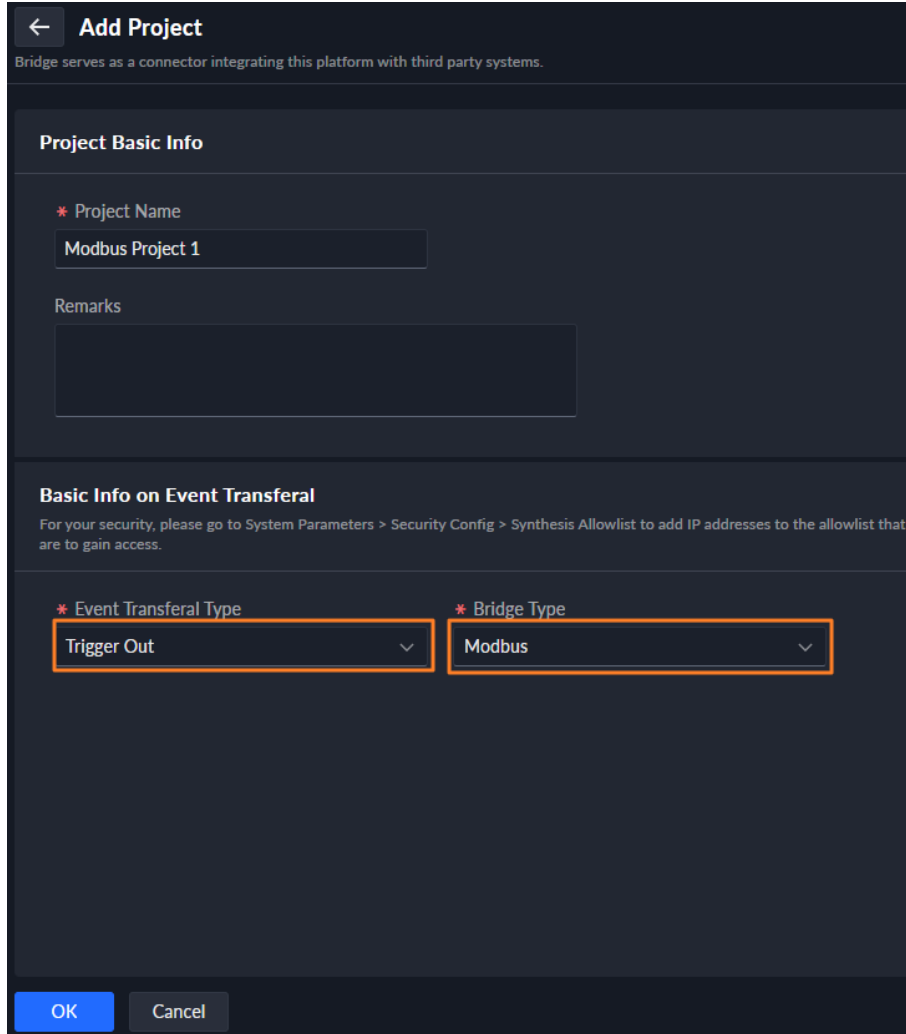
- Purchase and activate the **Event Transferral Modbus** license. For details of activating the license, see "2.1.6 Licensing".
- The default communication port of Modbus integration is 502. If the DSS platform and the third-party system are not on the same network segment, you need to go to the DSS management tool, click  of **Third-party Plug-in Management System**, and then configure the Modbus port.

Procedure

- Step 1** Add the third-party system to the allowlist of DSS.
1. Log in to the DSS client, select  > **System Parameters** > **Security Config**.
 2. In the **Synthesis Allowlist** area, click .
 3. Enter the IP address of the third-party system, and then click **OK**.
- Step 2** Configure Modbus project.

1. Select  > **Synthesis** > **Event Transferal**, and then click .
2. Define the project name, select **Trigger Out** and **Modbus**, and then click **OK**.

Figure 4-64 Configure the Modbus project



3. Select the created Modbus project, and then click **Edit**.
4. In the **Modbus Sub Server Config** area, click , and then configure the Modbus sub server parameters.

- **Sub Server Name** : The name that identifies the sub server.
- **Sub Server No.** : The unique identifier in Modbus communication. The value ranges from 1 through 247.
- **Type** and **Resource Type**: Select the type and resource type to send to the third-party system. For example, when selecting **Status** and **Device** respectively, it means that the device status will be sent to the third-party platform.

When selecting **Access Control** from **Type**, only **Channel** is available from **Resource Type**.

- Click , select event sources from the pop-up resource tree, and then click **OK**.



Click **Export** to export all configured resources and the corresponding holding register address list.

5. Click **OK**.

You can know whether the device or channel is online or offline by searching the value in the holding register address. For access control channels, you can open and close the door by sending a control command to the holding register address of the channel.

4.15.1.4 BACnet Bridge

The BACnet integration provides the ability for the DSS platform to act as BACnet device or host when integrating with third-party systems. It allows the DSS platform to send its device statuses and events to other systems (such as smart building management system) through BACnet protocol. Users of a third-party system do not need to perform additional development. They only need to configure the bridge on the client and their own platform.

Prerequisites

- Purchase and activate the **Event Transferal BACnet** license. For details of activating the license, see "2.1.6 Licensing".
- The default communication port of BACnet integration is 47808. If the DSS platform and the third-party system are not on the same network segment, you need to go to the DSS management tool, click  of **Third-party Plug-in Management System**, and then configure the BACnet port.

Procedure

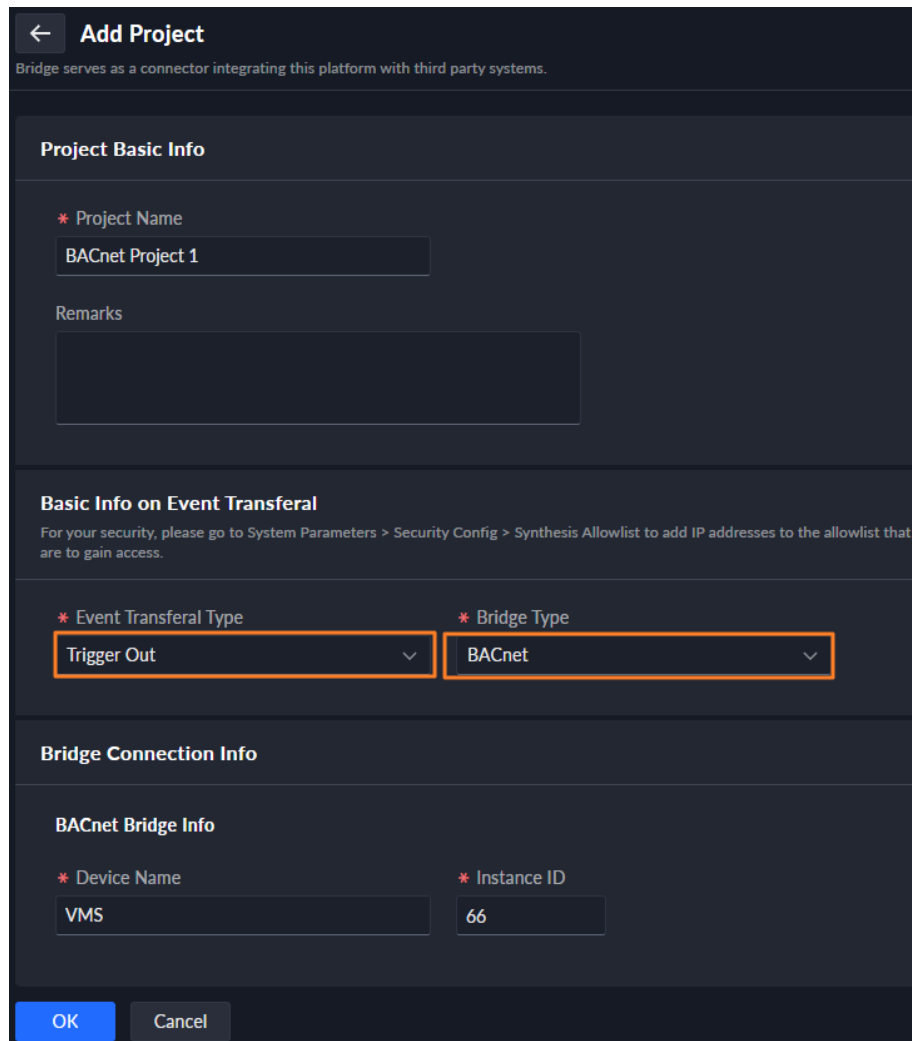
Step 1 Add the third-party system to the allowlist of DSS.

1. Log in to the DSS client, select  > **System Parameters** > **Security Config**.
2. In the **Synthesis Allowlist** area, click .
3. Enter the IP address of the third-party system, and then click **OK**.

Step 2 Configure the BACnet project.

1. Select  > **Synthesis** > **Event Transferal**, and then click .
2. Define the BACnet project name, and then select **Trigger Out** and **BACnet**.
3. Configure the bridge connection information, and then click **OK**.
 - **Device Name** : Used to identify the DSS platform in the third-party system. It is VMS by default.
 - **Instance ID** : Serves as the unique identity of the BACnet device, which in this case, is the DSS platform.

Figure 4-65 Configure BACnet project



← Add Project

Bridge serves as a connector integrating this platform with third party systems.

Project Basic Info

* Project Name
BACnet Project 1

Remarks

Basic Info on Event Transferal

For your security, please go to System Parameters > Security Config > Synthesis Allowlist to add IP addresses to the allowlist that are to gain access.

* Event Transferal Type: Trigger Out
* Bridge Type: BACnet

Bridge Connection Info

BACnet Bridge Info

* Device Name: VMS
* Instance ID: 66

OK Cancel

4. Select the created BACnet project, and then click **Edit**.
5. In the **Object Config** area, click , and then configure the object information.
 - **Object Name** : The name that identifies the object.
 - **Object Template** and **Resource Type**: Select the object and resource type to be sent to the third-party system. For example, when you select **Status** and **Device** respectively, it means that the device status will be sent to the third-party platform.
 - Click , select event sources from the pop-up resource tree, and then click **OK**.

Based on selected event sources, the DSS platform will automatically generate a unique target instance ID for different devices and channels. This ID is a unique identifier used by third-party systems to distinguish objects in BACnet devices. Each event source (device or channel) is represented by an object ID.



Click **Export** to export all configured resources and the corresponding objects and target instance ID.

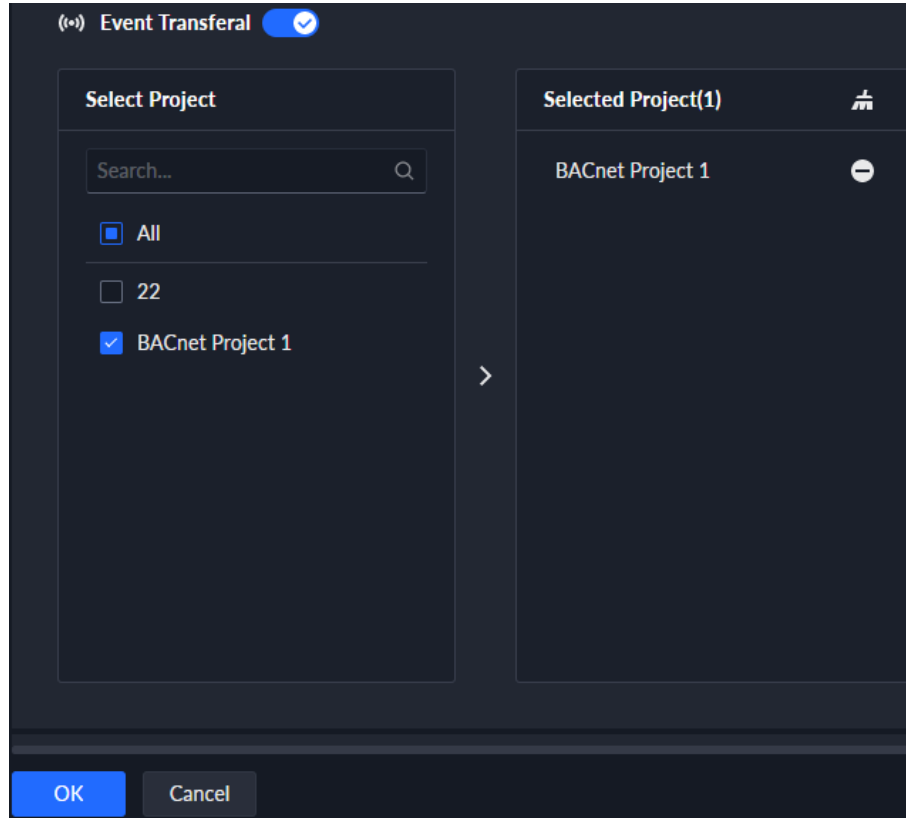
6. Click **OK**.

Step 3 Configure the event linkage.

1. Go back to the **Home** page, click . In the **App Config** area, select **Event**.

2. Click .
3. In the **Event Source** area, select the event source type, event, and event source that are consistent with those defined in 5.
4. Enable **Linked Action**, and then enable **Event Transferal**.
5. Select the created BACnet project.

Figure 4-66 Select the created BACnet project



6. Click **OK**.

For details of configuring other event parameters, see "4.1.1 Configuring Event Linkage".

4.15.1.5 SIA Bridge

The SIA bridge allows the DSS platform to send its device statuses and events to other systems through SIA protocol. Users of a third-party system do not need to perform additional development. They only need to configure the bridge on the client and their own platform.

Prerequisites

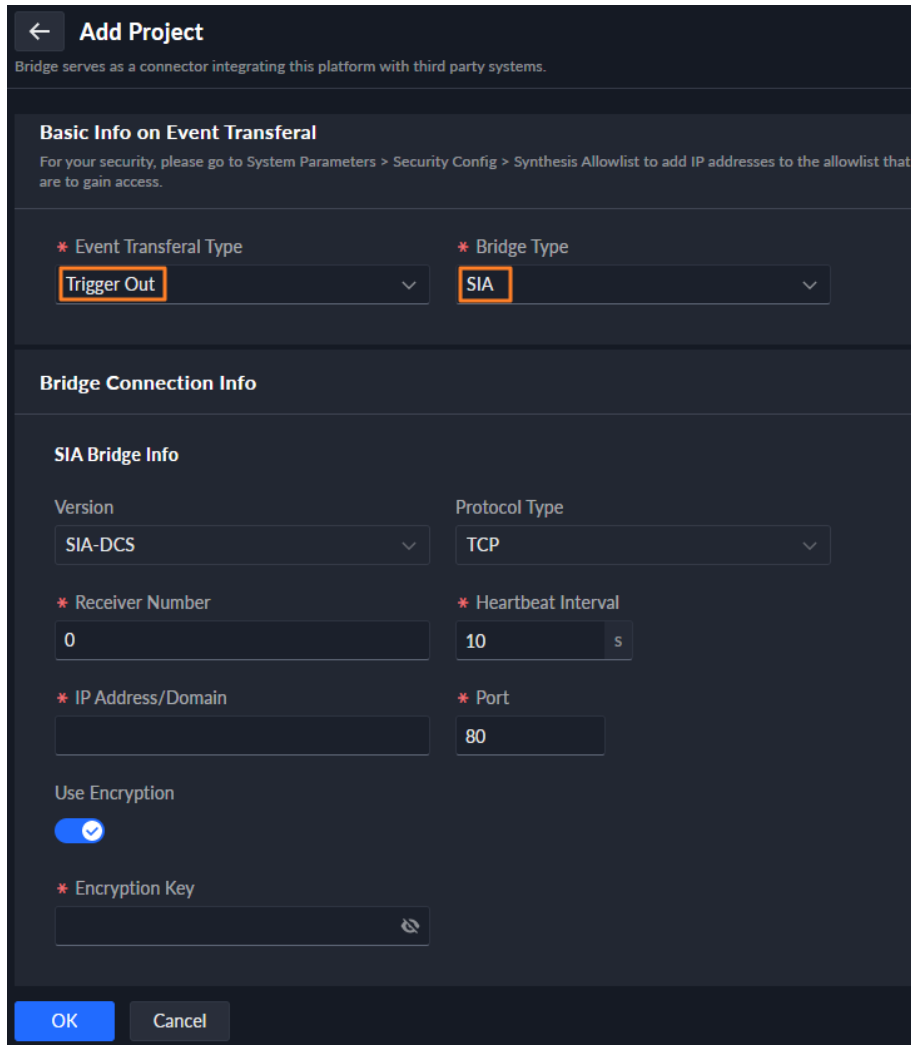
Purchase and activate the **Event Transferal SIA** license. For details of activating the license, see "2.1.6 Licensing".

Procedure

- Step 1 Add the third-party system to the allowlist of DSS.
 1. Log in to the DSS client, select  > **System Parameters** > **Security Config**.
 2. In the **Synthesis Allowlist** area, click .
 3. Enter the IP address of the third-party system, and then click **OK**.
- Step 2 Configure SIA project.

1. Select  > **Synthesis** > **Event Transferal**, and then click .
2. Define the project name, select **Trigger Out** and **SIA**, and then configure the bridge connection information.
 - **Receiver Number** : Only numbers and letters are supported.
 - **Heartbeat Interval** : Communication heartbeat interval. Only numbers are supported.
 - **IP Address/Domain , Port**: IP address/domain and port of the third-party system.
 - **Use Encryption** : After turning it on, you can set the **Encryption Key** to encrypt the communication.

Figure 4-67 Configure SIA project



← Add Project

Bridge serves as a connector integrating this platform with third party systems.

Basic Info on Event Transferal

For your security, please go to System Parameters > Security Config > Synthesis Allowlist to add IP addresses to the allowlist that are to gain access.

* Event Transferal Type: Trigger Out

* Bridge Type: SIA

Bridge Connection Info

SIA Bridge Info

Version: SIA-DCS

Protocol Type: TCP

* Receiver Number: 0

* Heartbeat Interval: 10 s

* IP Address/Domain:

* Port: 80

Use Encryption: ☒

* Encryption Key:

OK Cancel

3. Click **OK**.
4. Select the created SIA project, and then click **Edit**.
5. In the **Event Template** area, click **Add**, configure the event template name, select the event source type, configure the SIA Code for the event, and then click **OK**.
6. In the **Zone** area, click **Add**, set the account ID and group ID.
7. Select the event source type and event template, click **Add** , select the event source, and then click **OK**.

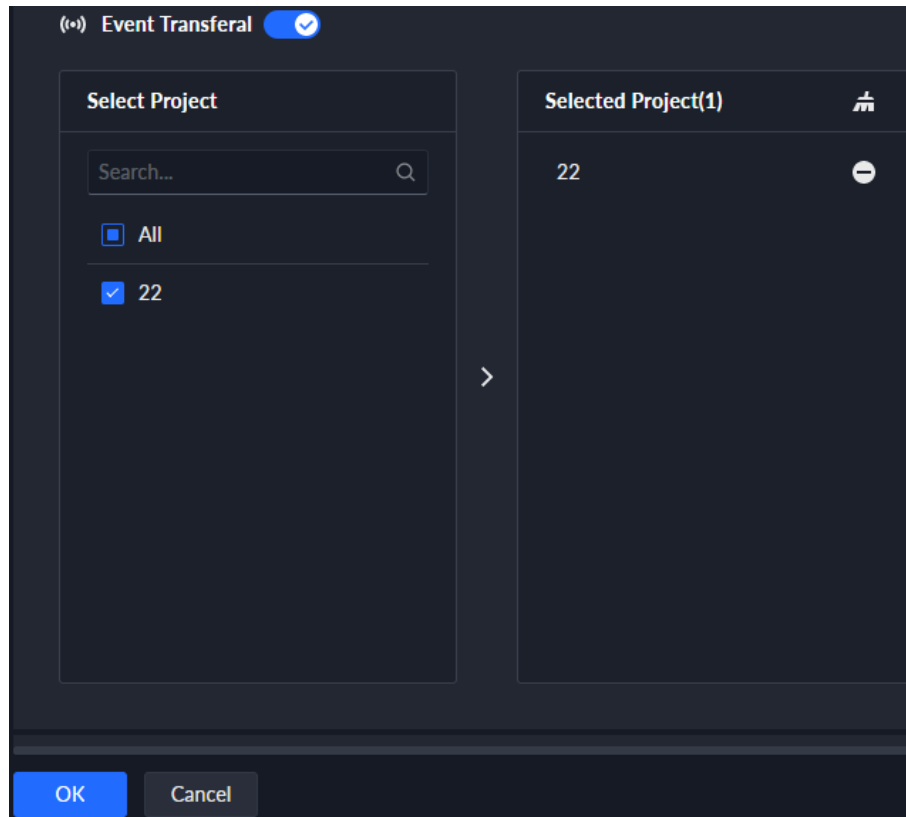
The platform automatically assigns a unique zone ID to each zone.

8. Click **OK**.

Step 3 Configure the event linkage.

1. Go back to the **Home** page, click . In the **App Config** area, select **Event**.
2. Click .
3. In the **Event Source** area, select the event source type, event, and event source that are consistent with those defined in [Z](#).
4. Enable **Linked Action**, and then enable **Event Transferal**.
5. Select the created SIA project.

Figure 4-68 Select the created SIA project



6. Click **OK**.

For details of configuring other event parameters, see "4.1.1 Configuring Event Linkage".

4.15.2 Synchronizing Data

You can manually or regularly synchronize data in the platform to third-party databases.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **Synthesis** > **Data Sync**.

Step 2 Click .



You can only add one database.

Step 3 Configure the basic parameters of the database, and then click **Connection Test**.

If the connection can be established, the system will prompt that it connects to the database successfully.

Step 4 Configure the data to be synchronized.

1. Click  in the **Synchronization Data** section.

Figure 4-69 Configure parameters

2. Set **Business Module** to **Access Control** or **Attendance**, and then enter the name of the data table in the third-party system.



You can only add the access control module once.

3. Configure when the platform will automatically synchronize the data every day. You can select **Every Day**, **Every Hour** or **Never Synchronize**.



- You can only configure 4:00–23:00.
- When setting **Business Module** to **Attendance**, you can only select from **Every Day** and **Never Synchronize**.

4. Click  to enable the type of data to be synchronized. You must disable the data that you do not want to synchronize.
5. Enter the corresponding names in the table in the third-party table for the data to be synchronized.
6. Click **OK**.

Related Operations

- **Edit** : Edit the information of the database or the data that is being synchronized. You can view each synchronization result in the log. See "8.5.3 System Log".
- **Manually Sync Now** : Synchronize the access control or attendance data immediately. All the data will be synchronized on the first attempt, including after you delete and then add the database again. Only new data will be updated on subsequent synchronizations.

4.15.3 System Integration

Devices and person and vehicle information can be synchronized from a third-party platform to the DSS platform to be used in various functions.

Background Information

- Device management: View the parameters of devices.
- Person and vehicle information: View the information of organizations, persons, and vehicles.
- Event: Configure event schemes, and receive and process alarms.
- Monitoring center: View linked real-time videos, recorded videos, map information, and more.
- Zone management: Access points will be created for each access control channel.
- Access control: View linked real-time videos, and open and close doors.
- Access control records: Display real-time and historical records, extract access records from devices, and view entering and exiting statistics of people.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **Synthesis > System Integration**.

Step 2 Click **Add Now**.



You can add up to 5 bridges for system integration.

Step 3 Configure the parameters.

Table 4-48 Parameter description

Parameter		Description
Basic Info	Project Name	Enter a name for this project. This name will be used in different resources, such as organization name and event source type.
	Integrated Platform Type	Select the type of the third-party platform. Currently, only access control platform is supported.
	Identity Certificate	Automatically generated. Copy them to the configuration of the bridge. The bridge will use this information to verify its identity to the DSS platform.
	Secret Key	• Click  to verify your password, and then generate a new secret key. • Click  to verify your password, and then you can click  to copy the secret key.
	Remarks	Customize the content. When an event is triggered and sent to the platform, this information will be displayed in the event details.
Bridge Connection Info	IP Address/Domain	Enter the IP address or domain name and port number of the bridge, and select the protocol.
	Port	
	Protocol Type	

Parameter		Description
	Identity Certificate	Enter the identity certificate and secret key of the bridge. The DSS platform will use this information to verify its identity to the bridge.
	Secret Key	
Auto Collect Data	Collection Frequency	Configure the frequency and time for the DSS platform to automatically acquire data from the third-party platform.
	Collection Time	

Step 4 Click **Show More**, and then configure third-party information, including IP address/ domain, port, identity certificate and secret key.

Step 5 Click **OK**.

Step 6 Import events from the third-party platform to the DSS platform.

- One by one

1. Click **Add**.

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

- **Event Type Code** : Enter the code of the event in the third-party platform.
- **Event Type Name** : Enter the name of the event in the third-party platform.
- **Event Source Type** : Select the type of source that will trigger the event.
- **Event Type** : When the type of event source is channel, you need to configure the event type. They correspond to the types of access control events of the DSS platform, including normal, abnormal, and alarm.

- In batches

1. Click **Import**.

2. Click **Download Template**, save the template to your PC, and then enter the information in it.

3. Click **Upload File** , select the file, and then click **Open**.

Related Operations

- Configure an event scheme.

1. Go to the **Home** page, click , and then in the **Applications Configuration** section, select **Event**.

2. Click .

3. In the **Event Source Type** section, select the one you import from the third-party system.

Figure 4-70 Add a third-party event

Event Source Type	Event	Event Source
POS Alarms	Search...	Search...
Combined Event	▼ Third Party Event	☐ Select All
Custom Alarm	• test	
Generic Event		
111		
test-		
lmy2-		
chj-t		
chj-test		

4. For other parameters, see "4.1 Configuring Events".

- **Manually Collect** : Synchronize data immediately.
- **View List of Failures** : View the person or device that the platform failed to synchronize.

5 Businesses Operation

5.1 Monitoring Center

The monitoring center provides integrated real-time monitoring applications for scenarios such as CCTV center. The platform supports live video, face and license plate recognition, target detection, access control, emap, snapshots, events, video playback, video wall, and more.

5.1.1 Main Page

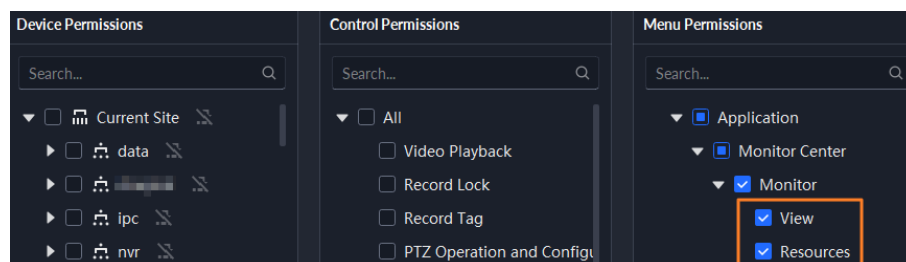
Provides frequently used functions such as video, event and alarm.

Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center**.

Prerequisites

The **Resources** and **View** menu permissions are required; otherwise, you cannot view resources, add them to favorites, and save the resources to view. Permissions can be configured from  > **User > Role Management**.

Figure 5-1 Configure view and resources permissions



Page Description

Figure 5-2 Monitoring center

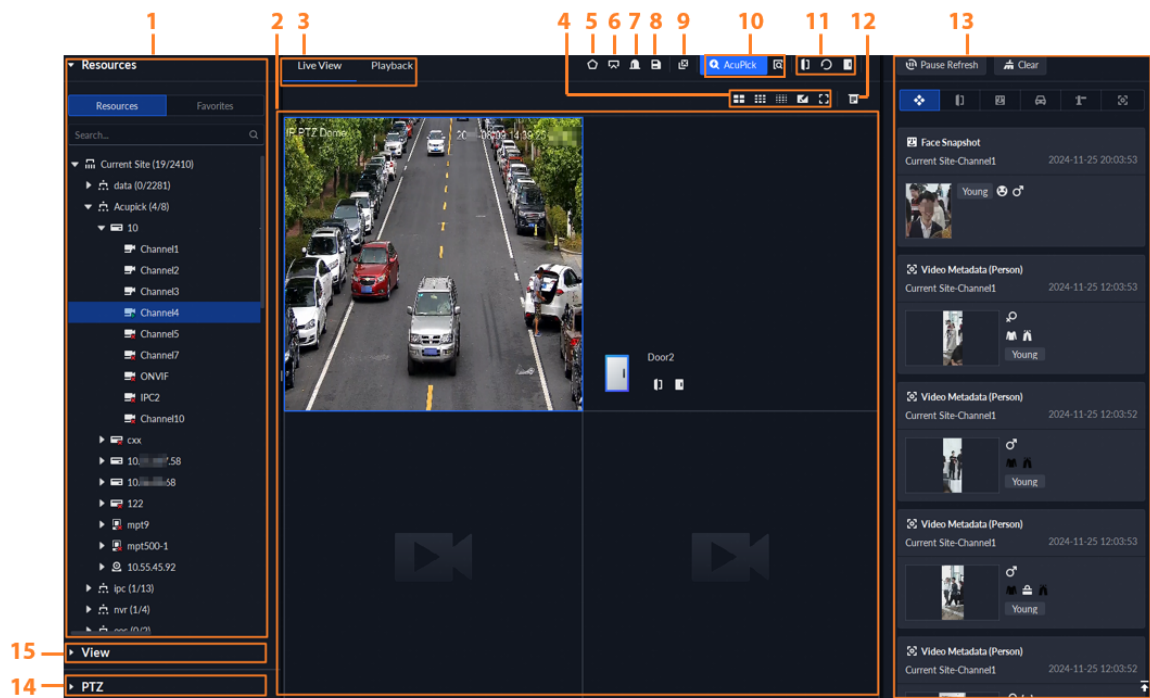


Table 5-1 Description

No.	Parameter	Description
1	Favorites and device tree	- List of resources including devices, browser, and maps. - You can search for a device or channel in the search field. Fuzzy search is supported so that you can simply enter part of the name and then select the exact one from the provided name list. - Add, delete or rename the favorites. You can also tour the channels in favorites.
2	Real-time videos	Drag a channel to the windows and view its real-time video.
3	Live view and playback	- Live view: View real-time videos. - Playback: View recorded videos. For details, see "5.1.3 Playback".  Drag  between the resource tree and the video window to the left, to hide the resource tree, and then the View and Resource selection bar will show at the top, where you can select or search the views and resources that you need, and then drag them to the window to play the video. Click  to show the resource tree.

No.	Parameter	Description
4	Window split mode and full screen	- Set a window split mode. Supports 1, 4, 6, 8, 9, 13, 16, 20, 25, 36 or 64 splits, or click to set a customized split mode. If the live-view channel number is more than the number of current windows, then you can turn page(s) by clicking the buttons on the top of the page. - Switch the video window to Full Screen mode. To exit Full Screen, you can press the Esc key or right-click on the video and select Exit Full Screen.
5	AI rule overlay	The function is available when AI Rule Overlay is turned on from Local Settings > Video > General. Default : Shows AI rules on the video by default. Open All : Shows the AI rules of the channels on the video, and the right-click menus of AI Overlay and SMD Overlay are also displayed. Close All : Hides the AI rules of the channels on the video, and the right-click menus of AI Overlay and SMD Overlay are also hidden.
6	Push videos to a video wall	Real-time videos that are currently opened can be quickly displayed on a video wall. You must configure a video wall before using this function. For details, see "5.1.5 Video Wall".
7	Set alarm windows in batches	Set all windows as alarm windows. After selecting "Open alarm linkage video in live view" in Local Settings > Alarm, then the alarm videos will be displayed on the alarm windows. If the number of alarm windows is less than that of linkage videos, the video linked to the earliest-triggered alarm will be opened.
8	Save view	Save all the channels or websites that are opened in to a view so that you can quickly open all of them later. For details, see View.
9	Close all windows	Close all windows in live view.
10	Search for targets in the video	The platform supports manually selecting targets and automatically recognizing targets in the video, and then quickly searching for them in DeepXplore. For details, see Selecting and Searching for Target Manually and AcuPick.
11	Control doors	For a door channel, you can configure its mode through these icons  , including normally open and closed modes, and restoring it to the normal status. After restoring it to the normal status, people must verify their identifications to pass within defined periods.
12	Event panel button	Displays or hides the event panel.
13	Events	Displays events from channels that you are viewing live videos from. - Click different tabs to display only that type of events. - Click  clear all the events. - Click  to go to the top of the list to view the latest events.

No.	Parameter	Description
14	PTZ	If the channel you are viewing live video from is of a PTZ camera, you can control it through the control panel. For details, see PTZ.
15	View	- Save the current view of window split and video channels in the live view section, and name the view. You can directly select the view from the View tab to display it quickly next time. - Channels under a view or view group can be displayed by tour (in turn). You can set the tour interval to be 10 s, 30 s, 1 min, 2 min, 5 min or 10 min. - A maximum of 100 views can be created.

5.1.2 Video Monitoring

View live videos. For ANPR and face cameras, you can view information of ANPR, face detection and face recognition. For video metadata cameras, you can view metadata information.

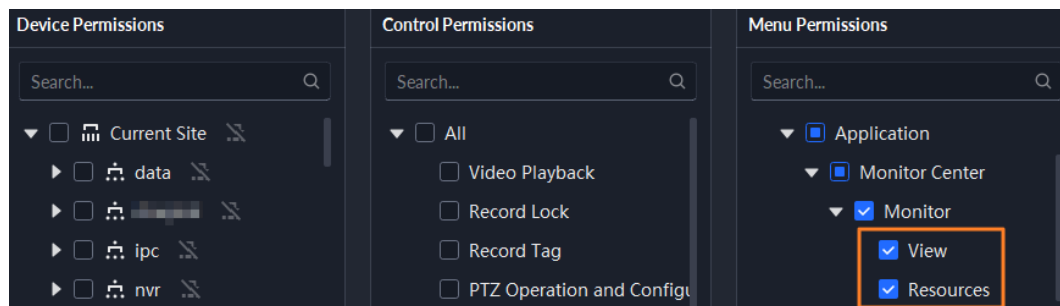
5.1.2.1 Viewing Live Video

View the live video of connected devices.

Prerequisites

The **Resources** and **View** menu permissions are required; otherwise, you cannot view resources, add them to favorites, and save the resources to view. Permissions can be configured from > **User** > **Role Management**.

Figure 5-3 Configure view and resources permissions



Background Information



This section only introduces viewing live video. For POS live view, see "6.4 POS". For map live view, see "4.2 Configuring Map".

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click and then click **Monitoring Center** > **Monitoring**.
- Step 2** Click **Live View** tab.
- Step 3** View real-time video.

You can view live video in the following ways:

- Double-click a channel or drag the channel from the device list on the left to one window on the right.

- Double-click a device to view all channels under the device.
- Right-click a node, select **Tour**, and then set tour interval. The channels under this node will play in turn according to the defined interval.

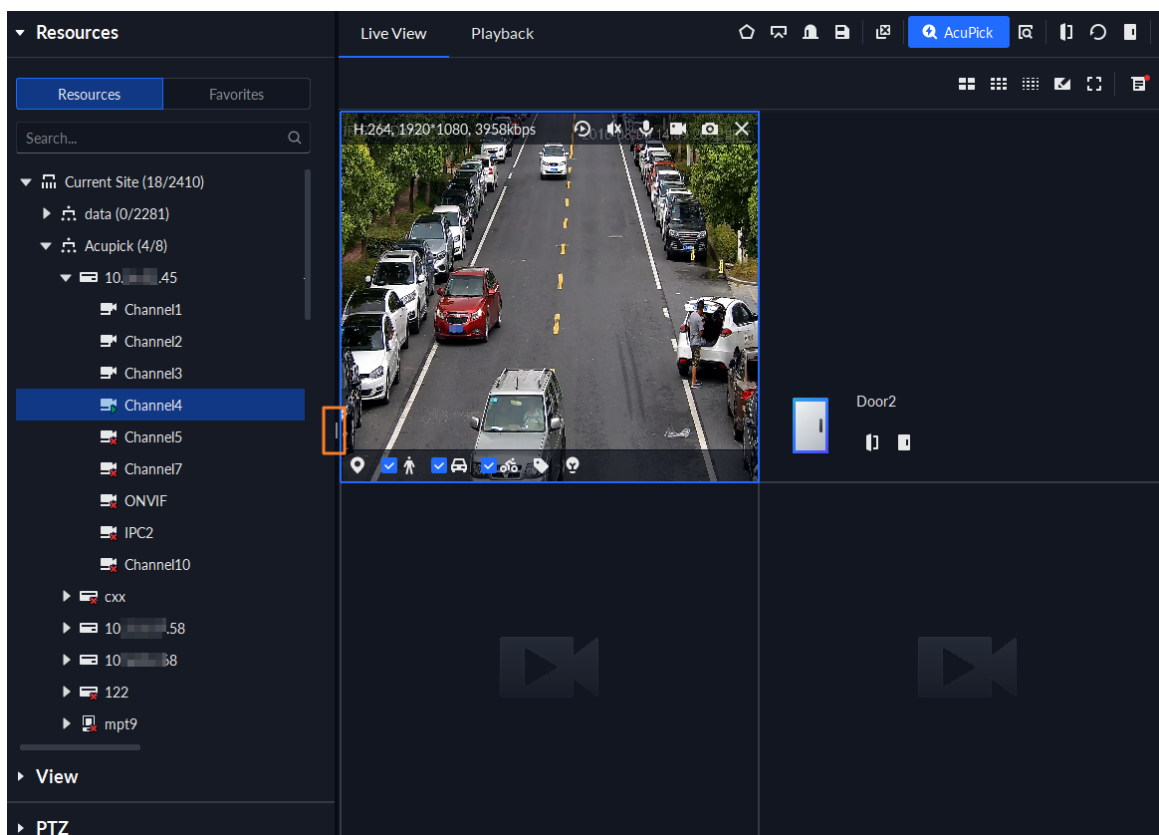


- ◇ Drag  between the resource tree and the video window to the left, to hide the resource tree, and then the **View and Resource** selection bar will show at the top, where you can select or search the views and resources that you need, and then drag them to the window to play the video.

Click  to show the resource tree.

- ◇ If the number of window splits is more than the number of online channels, video of all channels will be displayed in the window. Otherwise, double-click the root node, and then click  1/32  on the top of the page to turn pages.
- ◇ Close the on-going tour before starting live view.

Figure 5-4 Live view



Step 4 You can perform the following operations during live view.

- View channel status.

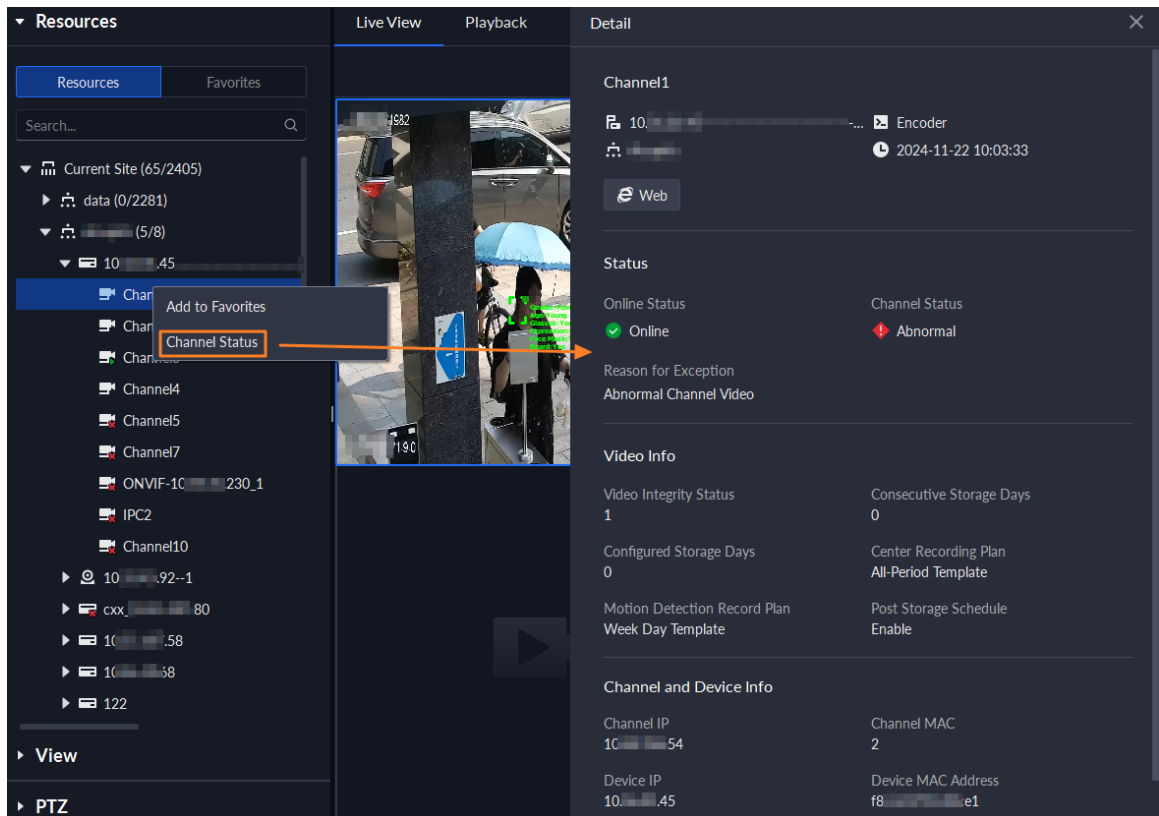
Right-click a node, select **Channel Status**, and then you can view the channel details, including status, video information, channel and device information.

Click , and then it goes to the login page of the device webpage.



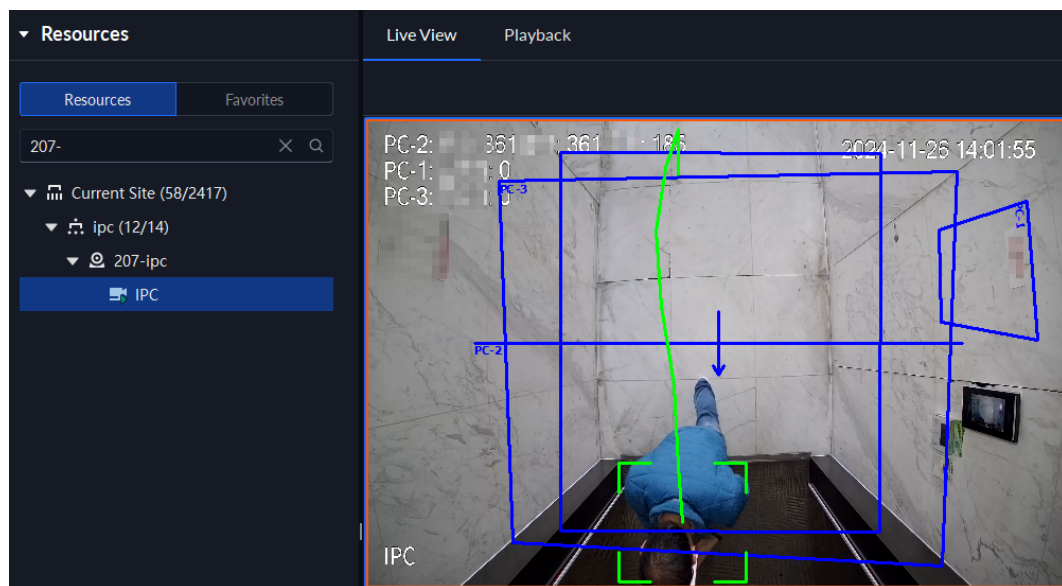
If you do not have the device permissions, you can only open the webpage, but not log in. To configure device permissions, go to  > **User** > **Role**.

Figure 5-5 View channel status



- When viewing live video of people counting cameras (make sure that the people counting function is enabled on the camera), right-click the monitoring image, and then select **AI Overlay > Bounding Box Overlay**, you can view the person tracks on the monitoring image.

Figure 5-6 View person track



- Display intelligent snapshots.

When viewing live video of face detection cameras, face recognition cameras, ANPR cameras, or target detection cameras, right-click the monitoring image, and then select **Start Picture Overlay**. The snapshot will be displayed on the upper-right corner

of the live window. If no more images are captured, a snapshot will be displayed up to 5 seconds by default, and it will disappear after 5 seconds.

Point to the live window, and then select type of images to be displayed.

- Point to the video window, and then you can see the shortcut menu at the upper right.

Figure 5-7 Live window

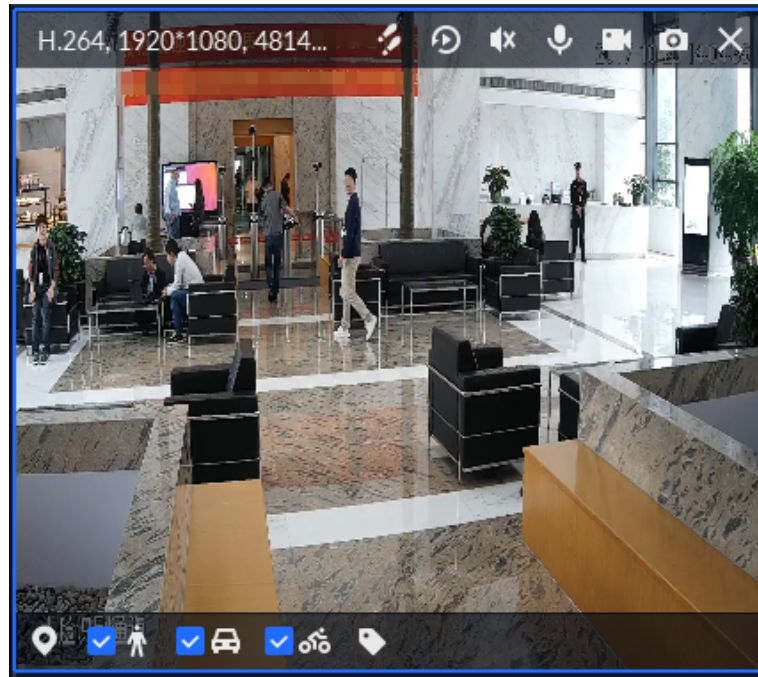


Table 5-2 Parameter description

Icon	Name	Description
	Visual tracking	Click  to turn on the visual tracking, and then you can click the shape over the video image to view the video of associated channels, so that you can track the area or location where the target passes through. For details, see "5.1.2.1.3 Visual Tracking".
	Instant playback	Turn on/off instant playback. The playback time can be defined from Local Settings > Video > Video Playback .  Instant playback requires that there are central or device recordings. Central recordings will be played first if there are both central and device recordings.
	Audio	Turn on/off the audio of the channel.  The audio is not enabled by default. To enable the audio function, the Video Sound permission is required from  > User > Role Management .

Icon	Name	Description
	Audio communication	Start two-way audio with the device the channel belongs to. If the channel is bound to a IP speaker, then you will talk to the device the channel belongs to through the IP speaker.  The audio communication is not enabled by default. To enable this function, you need to add the audio talk permission on the role management page.
	Local record	Click it, and then the system begins to record local file and you can view the record time on the upper left. Click again, and then system stops recording and saves the file to your PC. The recorded video is saved to..\\DSS\\DSS Client\\Record by default. To change the storage path, see "8.4.5 Configure File Storage Settings".
	Snapshot	Take a snapshot. The snapshots are saved to..\\DSS\\DSS Client\\Picture by default. To change the snapshot storage path, see "8.4.5 Configure File Storage Settings".
	Close	Close the video.
	Map location	If the channel has been tagged on the map, click the icon, and then you can open the map in a new window to view the device position on the map.
	Tag	Tag the videos of interest for easy search in the future. You can search for the tagging records from Download Center > Tagging Record.  Device Permissions and the Record Tag control permission are required from  > User > Role Management; otherwise, you cannot tag the video.

- Sleep function is supported for IPCs that use 4G mobile network to communicate and are solar-powered.
 - ◇ When the device is asleep, you can click  to wake it up.
 - ◇ The device will regularly request to sleep to save battery. When you are viewing its live video, the device will request to sleep every 2 minutes. When you are not viewing its live video, the device will request to sleep every 1 minute. You can accept or reject so that you can continue to watch live video. When rejecting the request, you can choose whether to delay the next request from the device.
- Right-click the live video, and then the shortcut menu is displayed.



The menu varies depending on the functions supported by the device you are operating on.

Table 5-3 Description

Parameters	Description
Select Audio Input	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Start Remote Recording	Record the audio and video in the current window.  ◇ If a channel already has a center recording plan, you cannot start remote recording. ◇ If a video storage disk is configured on the platform, the videos will be saved to the platform server.
Continuous Snapshot	Take snapshots of the current image (three snapshots each time by default). The snapshots are saved to <code>..\DSS\DSS Client\Picture</code> by default. To change the snapshot storage path, see "8.4.5 Configure File Storage Settings".
Detailed Tag	Tag the videos of interest for easy search in the future. You can set tag details such as tag name, tagging time, time before and after tag, the user who adds the tag, tag object, and more. The tagging records can be searched from Download Center > Tagging Record.  ◇ Device Permissions and the Record Tag control permission are required from  > User > Role Management; otherwise, you cannot tag the video. ◇ The channel that you want to tag is configured with recording plan; otherwise, no video can be searched after you adding the tag.
Stream Type	Select stream type as required. Generally, main stream requires the most bandwidth, and sub stream 2 the least. The smaller the bandwidth is required by the stream, the smoother the video image.
Play Mode	When playing videos, both fluency and real-time performance matter. To deal with network fluctuations, the platform has a set of buffer control strategies to ensure fluency and real-time performance. You can select one of the following play modes as needed. ◇ Real-time Play Priority : The system might lower the image quality to avoid video lag. It is suitable for special scenarios with high requirements on real-time performance. ◇ Fluency Priority : The system might lower the image quality and allow for lag to ensure video fluency. The higher the image quality, the lower the video fluency will be. ◇ Balance Priority (recommended): The system balances real-time priority and fluency priority according to the actual server and network performance. ◇ Custom : The system adjusts video buffering and lowers the impact on video quality caused by unstable network. The bigger the value, the more stable the video quality will be.

Parameters	Description
Video Adjustment	Adjust the brightness, contrast, saturation, and chroma of the video for video enhancement.
Digital Zoom	Click it, and then click and hold the video image to zoom in on the image. Right-click the image, and then select Digital Zoom again to exit zooming in.
Window Mode	Divide one window into 2 (1+1 mode), 4 (1+3 mode), and 6 (1+5 mode). One window will play the real-time video, and the others play different defined areas of the real-time video. If a device supports target tracking, you can enable this function in any window mode, the windows that play defined areas of the real-time video will follow the target when detected, until it disappears.
Stop Image Overlay	Click it, and then the snapshot information of people and vehicle metadata will be overlaid over the upper right of the video image, click it again to stop image overlay.  Make sure that the device supports people and vehicle metadata snapshot.
AI Overlay	Displays rule lines, bounding box on targets, and detection area for intelligent rules, except for motion detection. After enabled, the configuration will be saved, and only works on the current channel in the live view and playback.  AI overlay information is not displayed by default.
SMD Overlay	Displays the bounding box on targets. After enabled, the configuration will be saved, and only works on the current channel in the live view and playback.
Disable Privacy Masking	For a camera that supports privacy masking of human face, you can disable the masking here to view the face image.
Alarm Output Control	Turn on or turn off alarm output channels.
Audio and Light Control	You can turn on or off the audio and light channels one by one or at the same time.  This function is available on select device only.
Device Intercom	For channels added through NVR, XVR/DVR, IVSS or EVS, you can select this option to talk to the NVR, XVR/DVR, IVSS or EVS.
Add to Favorites	You can add the active channel or all channels to favorites.
Time Sync	Synchronize device time with server time.  This function requires Device Permissions and the Device Time Sync control permission from  > User > Role Management .

Parameters	Description
Set as Alarm Window	When selecting open alarm linkage video In Preview (in live window) from Local Settings > Alarm , then the video will be displayed on the window which is set to alarm window. If multiple alarms are triggered, the video linked to the latest alarm will be opened. If the number of alarm windows is fewer than the number of linkage videos, the video linked to the earliest-triggered alarm will be opened. After enabling Set as Alarm Window , the window frame is displayed in red.
Fisheye View	According to different installation methods, the fisheye view can be varied. ◇ In-ceiling mount: 1P+1, 2P, 1+2, 1+3, 1+4, 1P+6, 1+8. ◇ Wall mount: 1P, 1P+3, 1P+4, 1P+8. ◇ Ground mount: 1P+1, 2P, 1+3, 1+4, 1P+6, 1+8.  This function is available on fisheye cameras only. When changing the video stream, the fisheye view mode will maintain the current configuration.

- To view real-time temperature of a point on the thermal camera view, hover over that point.
- If a channel supports electronic focus, you can enable electronic focus for it on the platform to adjust video definition and size.



The page might vary according to the lens types of cameras. Lens types include embedded zoom lens and external CS electronic lens. The following figure is for reference only.

Figure 5-8 Live view

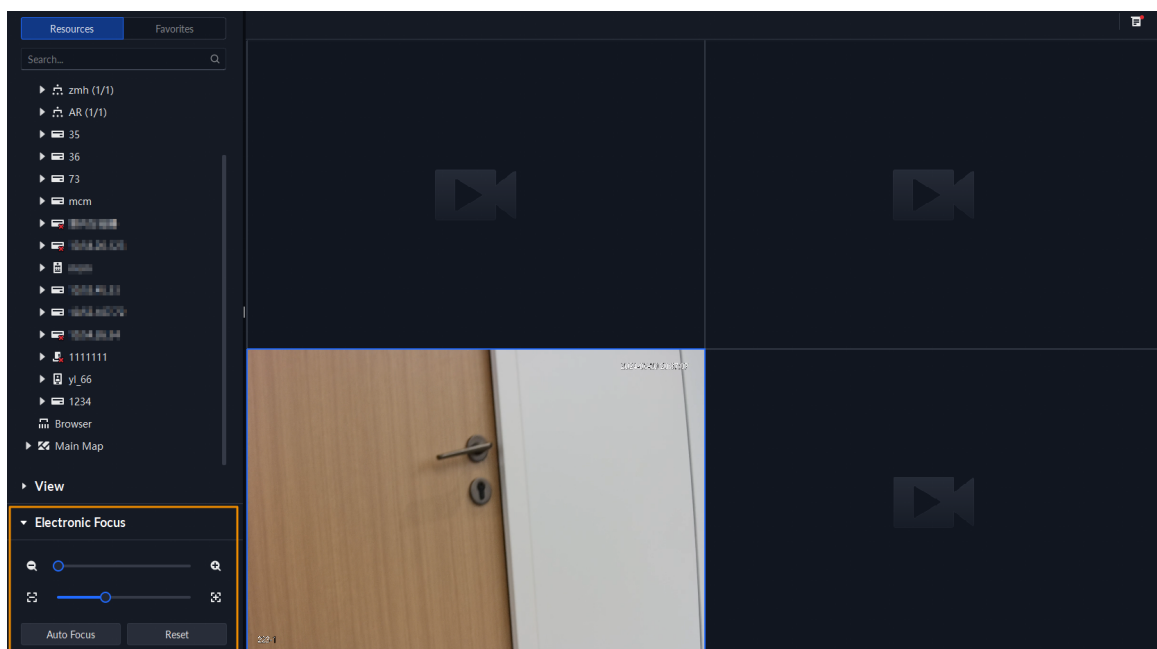


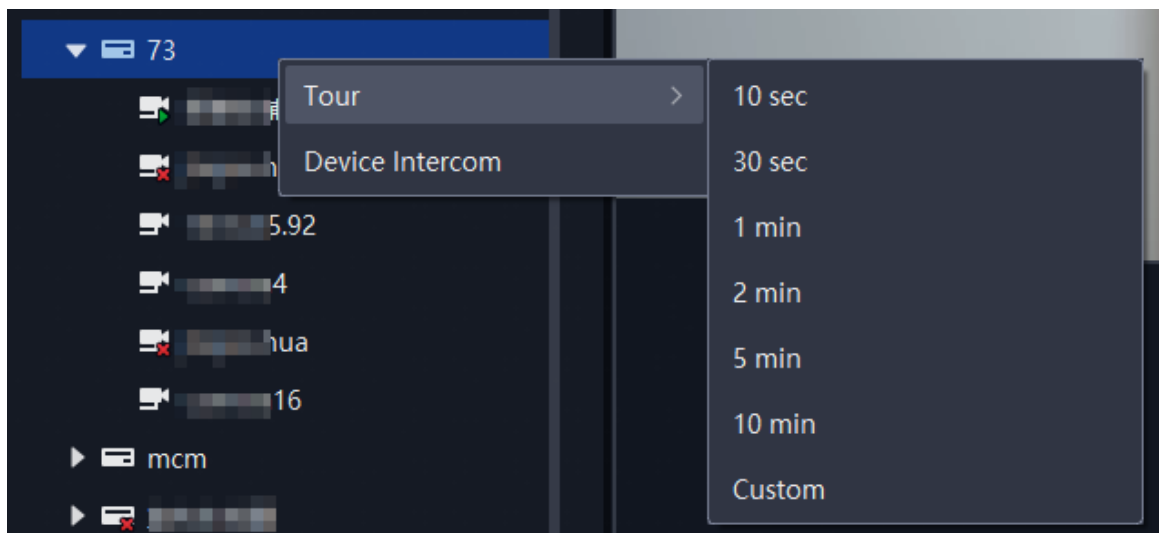
Table 5-4 Description

Parameters	Description
Zoom +/- (for embedded zoom lens)	Zoom in/out. Click, or click and hold  or  , or drag the slider  to the left or right to zoom in/out.
Focus +/-	Adjust camera focus to achieve the best video definition. Click or click and hold  or  , or drag the slider  to the left or right to adjust focus.
Auto Focusing (for embedded zoom lens)	Adjust image definition automatically.
ABF (auto back focusing, for external CS electronic lens)	 Other focusing operations are unavailable during auto focusing.
Reset	When image definition is imperfect, or after many times of zooming or focusing operations, you can click Reset to reset the lens, so as to eliminate lens deviation.

- Tour

On the live view page, right-click a device or node, select **Tour**, and then select an interval. The channels under this device or node will be played in turn at the pre-defined interval. You can also customize the interval.

Figure 5-9 Start tour



- ◇ To view remaining time of a channel during tour, check .
- ◇ To pause, click .
- ◇ To exit tour play, click .
- Region of interest (RoI)

A window can be divided into 4 or 6 regions during live view. One area is used to play live video and other regions are used to zoom in regional image.

On the live view page, right-click the window, select **Window Mode**, and then select a mode. For example, select a 1+3 mode.



To exit the **Window Mode**, right-click the window and then select .

Figure 5-10 Split mode

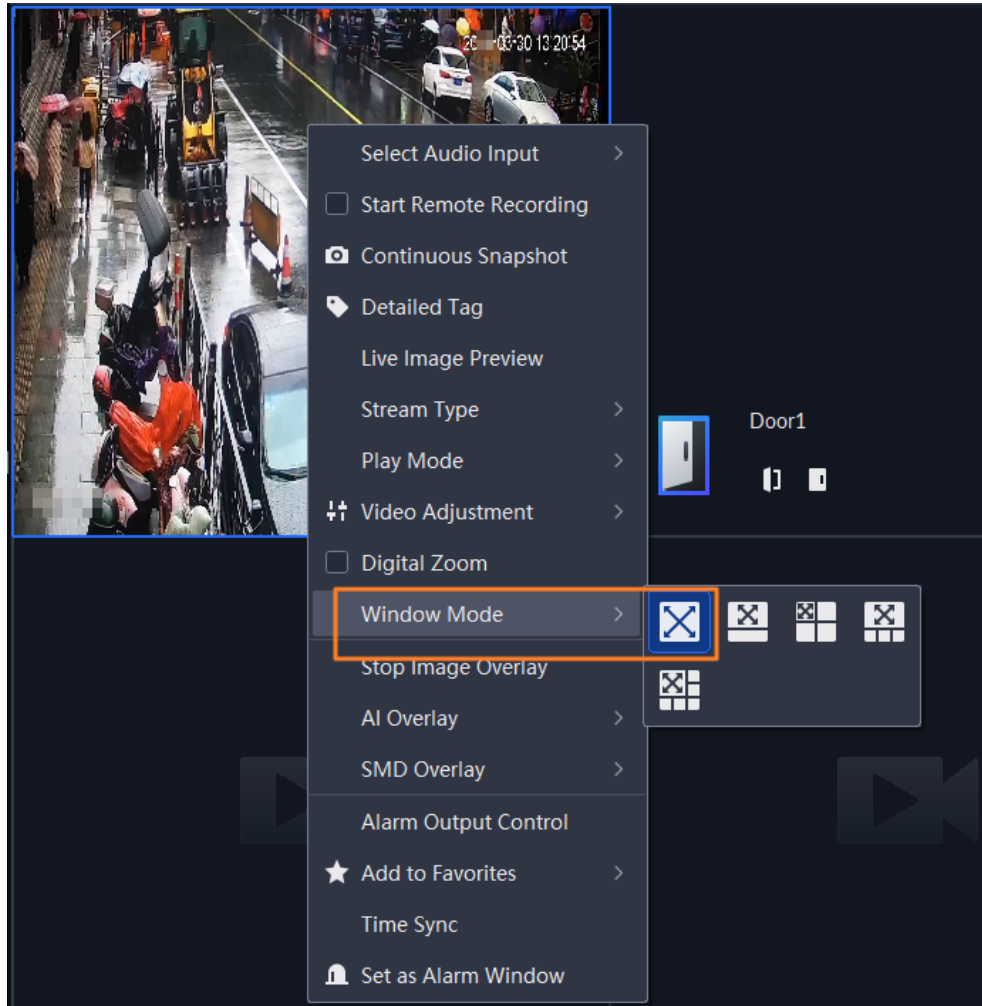
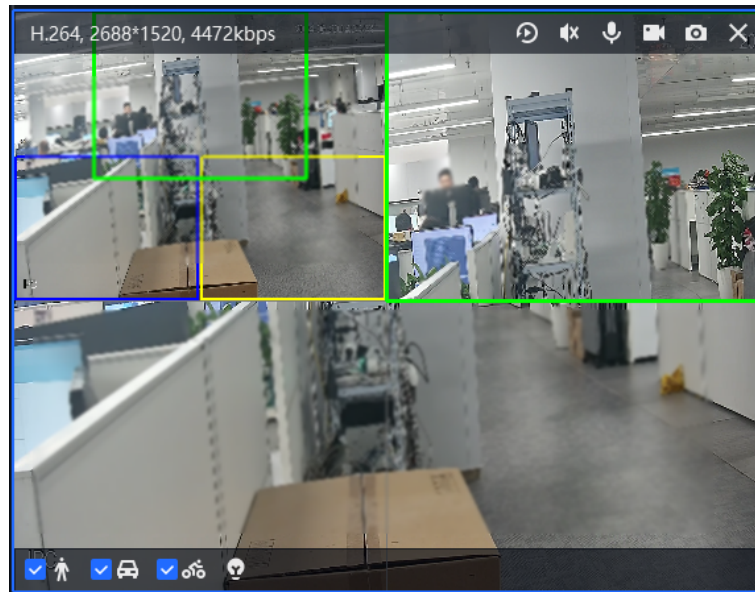


Figure 5-11 1+3 mode



- View real-time events.

Click  to open the event panel, which displays the real-time alarm events of opened channels.

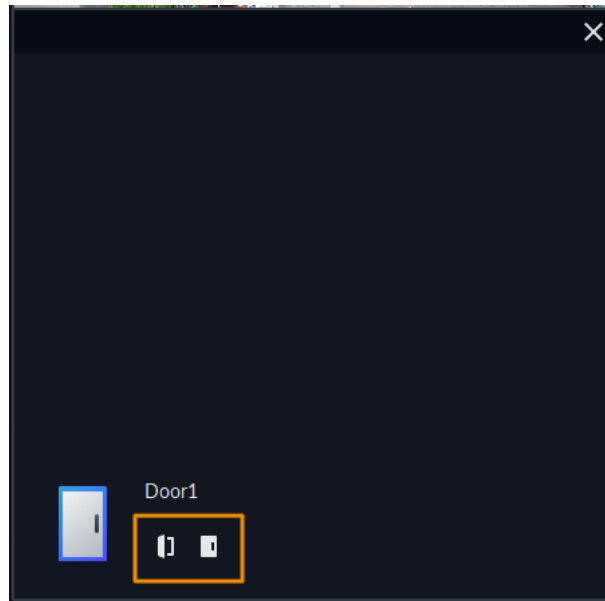
- ◇ Click the event type on the top of the event panel to view the corresponding event.
- ◇ Click event record to view the snapshot. Video playback is also supported. Operations related to different events might be different.
- ◇ : Refreshes events in real time. : Stops refreshing.
- ◇ Click  to clear the events in the event panel.
- ◇ Click  to quickly view the latest events.
- ◇ : View the recorded video of the event.
- ◇ : Go to DeepXplore to search for the target.
- ◇ : This function is only available when a license plate is recognized. Click this icon to add the vehicle to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the vehicle is recognized.
- ◇ : Add the vehicle to the platform.
- ◇ : Add the person to the platform.
- ◇ : Add the face to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the face is recognized.

- Remotely unlock the door.

When viewing the access control channel, you can remotely control the status of the door on the upper-right corner: Normally open () , normally closed () , or normal status () . You need to enter the login password of the current user before operation. Restore the door to normal status first, and then the door can be opened and closed according to defined period or through face recognition.

In the video window of the access control channel, you can remotely lock or unlock the door.

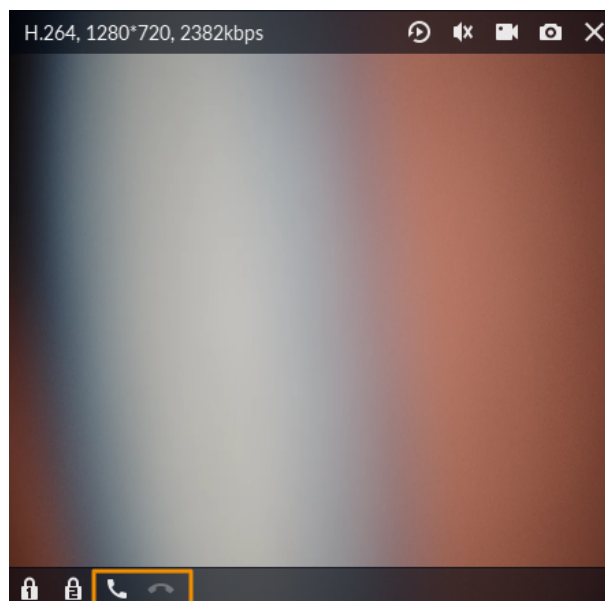
Figure 5-12 Lock/unlock the door



- Video intercom.

When viewing the video intercom channel, you can answer or hang up the call.

Figure 5-13 Video intercom



5.1.2.1.1 Selecting and Searching for Target Manually

Manually select a target in the video and quickly search for it in DeepXplore.

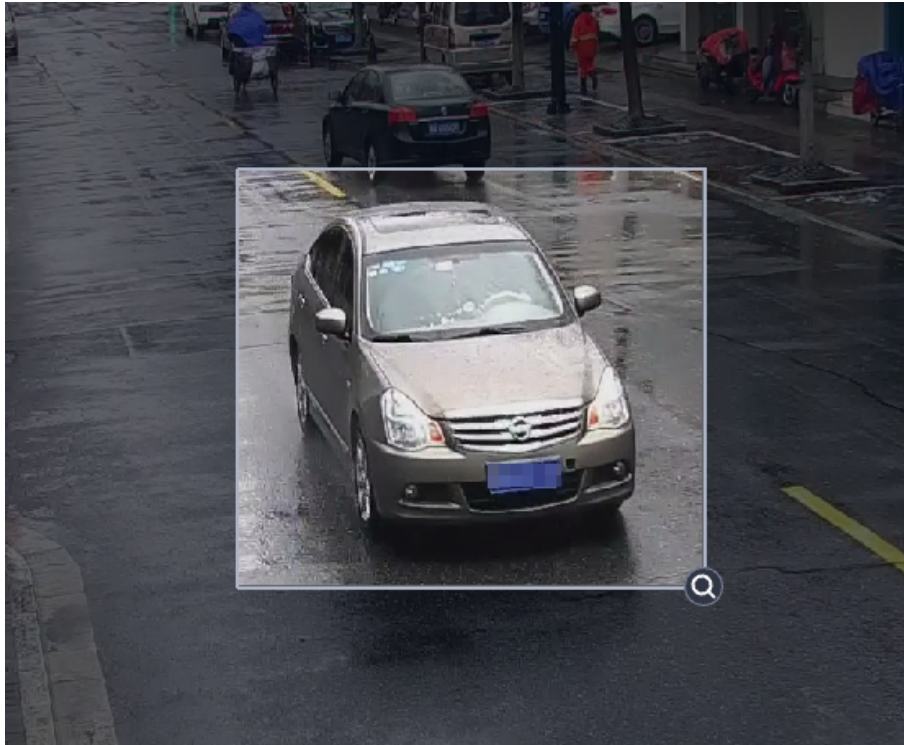
Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center** > **Monitoring**.
- Step 2 Double-click or drag a channel to a window on the right.
- Step 3 Click  on the upper-right corner.
- Step 4 Drag on the video to select a target.



Right-click to exit this function.

Figure 5-14 Select a target



Step 5 (Optional) Adjust the area of selection.

- Move the selection box: Place the mouse cursor over the selected area, click the left button, and then drag the mouse.
- Resize the selection box: Place the mouse cursor over the top-left, bottom-left, or top-right corner of the selected area. Click the left mouse button and drag it to adjust the size accordingly.

Step 6 Click  and select a type for the target, and then you are directed to DeepXplore to search for it. For details, see "5.3 DeepXplore".

5.1.2.1.2 AcuPick

The platform can automatically recognize different types of targets in the video. You can select a target and then quickly search for it in DeepXplore.

Prerequisites

1. Purchase a license with the AcuPick function, and then activate the license. For details, see "2.1.6 Licensing".
2. Configure the parameters of AcuPick. For details, see "7.4.4 Configuring Central Intelligent Server".
3. Configure the identity certificate and secret key in the AcuPick service in the management tool. For details, see "2.1.4 Management Tool".

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center** > **Monitoring**.

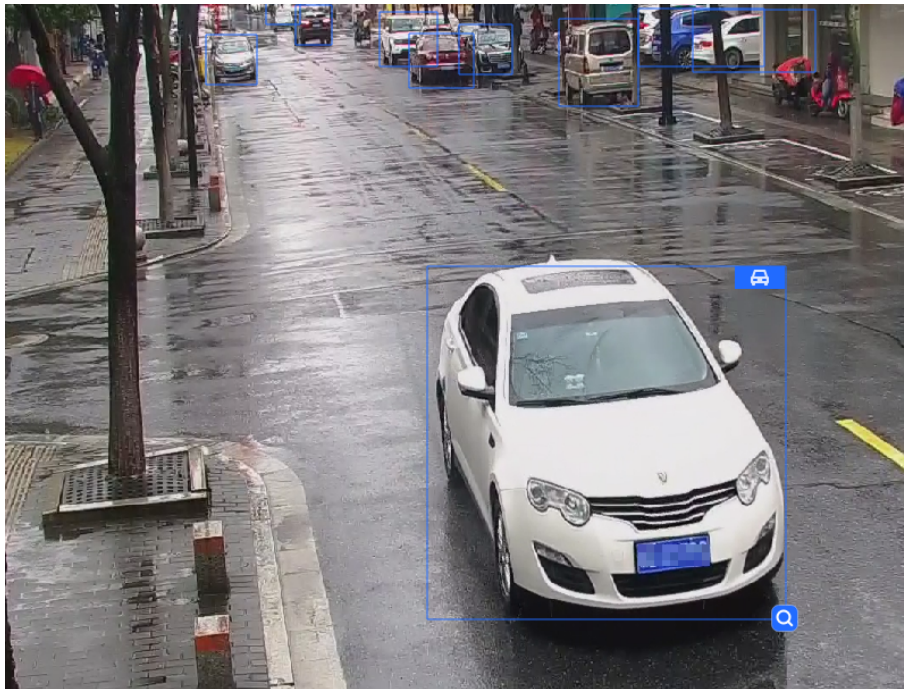
Step 2 Double-click or drag a channel to a window on the right.

Step 3 Click  on the bottom of the page to automatically recognize targets in the video, including faces, human bodies, and vehicles.



Click  to exit this function.

Figure 5-15 Automatically recognize targets



Step 4 Hover over the recognized target, and then click  of a target to search for it in DeepXplore. For details, see "5.3 DeepXplore".



If certain targets are not recognized, you can click  to manually select one. For details, see "5.1.2.1.1 Selecting and Searching for Target Manually".

5.1.2.1.3 Visual Tracking

On the **Live View** and **Playback** pages, through visual tracking, you can quickly jump to the associated cameras, to follow a target across different areas or locations, without losing sight of the target, as long as the places that the target passes through are covered by these cameras. Here uses operations on the **Live View** page as an example.

Prerequisites

Click , and then in the **App Config** area, select **Video Application** to configure visual tracking first. For details, see "4.13 Configuring Visual Tracking".

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center** > **Monitoring**.

Step 2 Double-click or drag the channel that has configured visual tracking to the window on the right.

Step 3 Point to the top of the video image, and then click  to start visual tracking.

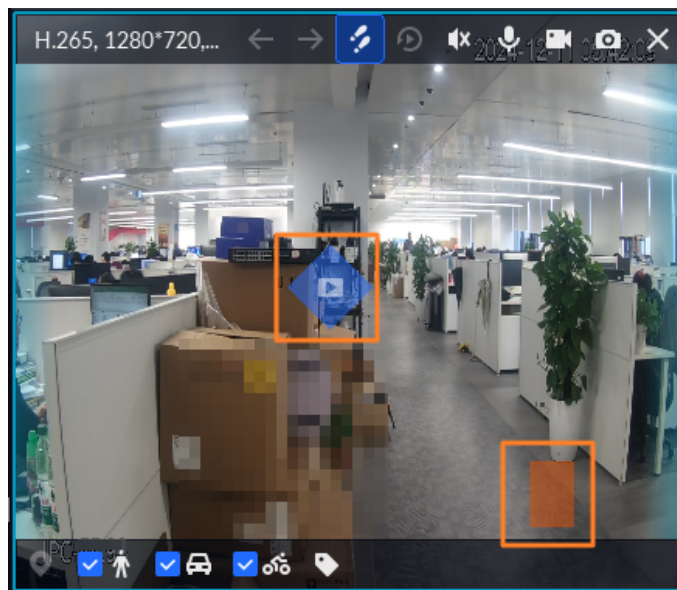
- Click a shape over the video image (for example ) to view the associated video.
- Click  or  to view the previous or next adjacent video.



You can switch single window and multiple windows from **Local Settings > Video > General**.

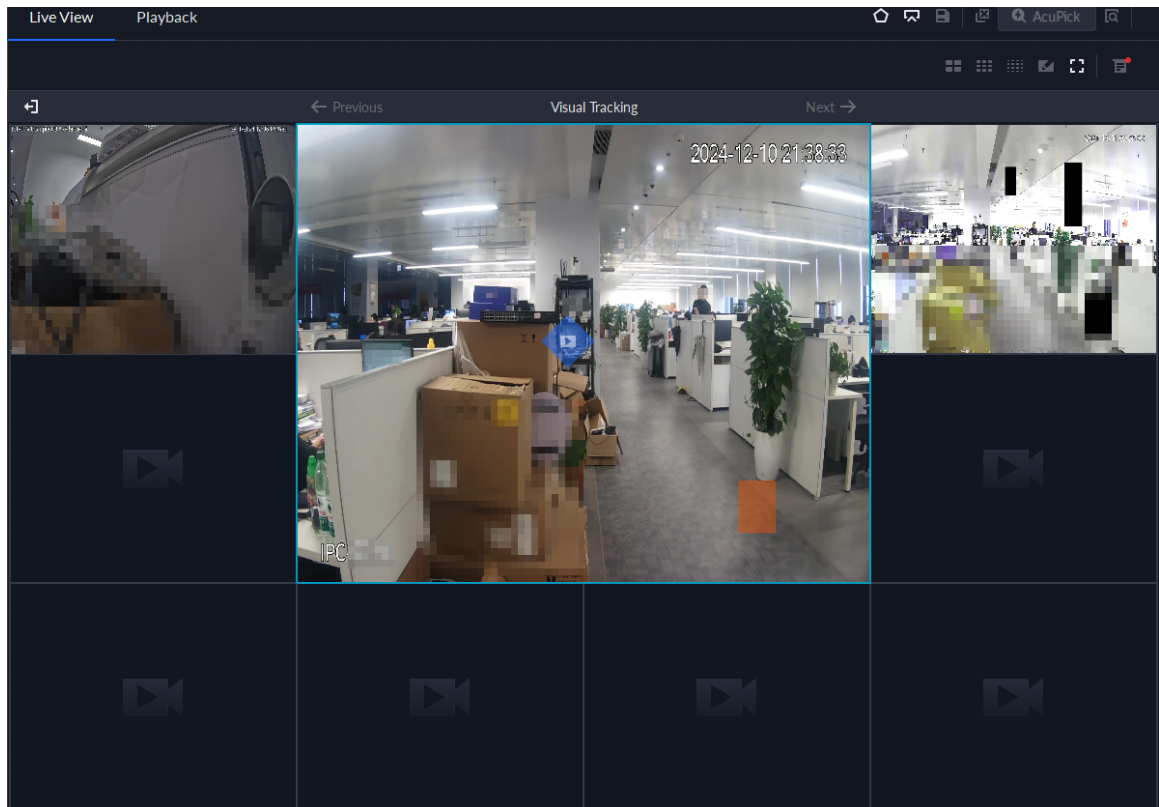
In single window mode, there is light green shadow on the edge of the video to distinguish it from other video windows. Click  to exit visual tracking.

Figure 5-16 Single window tracking



In multiple windows mode, the associated videos are displayed in a certain order. You can click  to exit visual tracking.

Figure 5-17 Multiple windows tracking



5.1.2.2 View

The current layout and resources can be saved as a view to be quickly played next time.

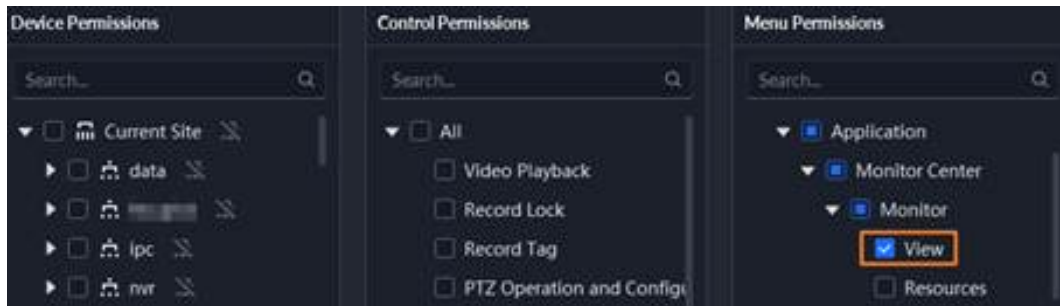
Views can be categorized as public views and private views. Only administrators are allowed to configure public views, and the users specified by them can access certain public views. Private views are configured and owned by users themselves. They can share private views with other users.

Views are categorized into different groups, which include three levels: First-level root node, second-level grouping and third-level view. Tour is supported for first-level root node and second-level grouping. The tour time can be 10 seconds, 30 seconds, 1 minutes, 2 minutes, 5 minutes, 10 minutes, or customized (5 seconds–120 minutes). You can create up to 1000 views.

Prerequisites

The **View** menu permission is required; otherwise, you cannot save the resources to view. The permission can be configured from  > **User** > **Role Management**.

Figure 5-18 Configure view permission



5.1.2.2.1 Creating a Public View Group

Public view groups are used to organize public views. There is the default root group of the Public View. You can only create one level of sub groups. Only administrators are allowed to create public view groups.

Background Information

By default, all users are allowed to access **Public View** and its views. If you want to control access, create groups that can be accessed by specified roles and their users, and save views to the groups.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then click **Monitoring Center > Monitoring**.
- Step 2** Click **View**.
- Step 3** Right-click **Public View**, and then select **Create View Group**.
- Step 4** Enter a name for the group, and then select the roles that are allowed to access this group.
Click  to view the users of a selected role.
- Step 5** Click **OK**.

5.1.2.2.2 Creating a Private View Group

Private view groups are used to organize private views. There is the default group of the Private View. You can only create one level of sub groups. Private views are configured and owned by users themselves. They can share private views with other users.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then click **Monitoring Center > Monitoring**.
- Step 2** Click **View**.
- Step 3** Right-click **Private View**, and then select **Create View Group**.
- Step 4** Enter a name for the group, and then click **OK**.

5.1.2.2.3 Creating a View

Views are categorized into public or private view groups. They are used to quickly apply different resources and settings. For example, a view can contain the configurations of multiple live video,

split mode, alarm windows, and more. When you open the view, these configurations will be applied at the same time, and you do not need to configure them again.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then click **Monitoring Center > Monitoring**.
- Step 2** Configure the split mode, and then drag channels, maps, and the browser to the windows.
- Step 3** Click  on the upper-right corner to save the current layout.
- Step 4** Configure the parameters, and then click **OK**.

Table 5-5 Parameter description

Parameter	Description
View Type	Select a type for the view. Only administrators can create a public view.  If the view is saved to Public View , all users can access it.
View Name	Enter a name for the view. It can be the same as other groups or views.
View Group	Select a group for the view based on its type.

5.1.2.2.4 Updating a View

When you need to change the resources or settings in a view, you can update them directly without creating a view.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then click **Monitoring Center > Monitoring**.
- Step 2** Click **View**.
- Step 3** Double-click or drag a view to a window to open it.
- Step 4** Change the resources or settings, such as the split mode, number of channels and alarm windows, and the locations of the channels.
- Step 5** Click  on the upper-right corner to update the view.

5.1.2.2.5 Viewing a View

- Live view
Double-click or drag a view to a window to view its resources.
- Tour
Right-click a view group, select **Tour** and set the tour period.
 - ◇ To view remaining time for a view, check .
 - ◇ To pause, click .
 - ◇ To exit tour, click .

5.1.2.2.6 Sharing a Private View

Privates views can be shared with other users.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then click **Monitoring Center > Monitoring**.
- Step 2** Click **View**.
- Step 3** Right-click a private view, and then select **Share View**.
- Step 4** Select a user and enter a message in remarks, and then click **OK**.

The view will be saved to **Private View** of the user.



It will fail to share if the user's view groups or views reach the limit. You can share again after the user deletes a group or view.

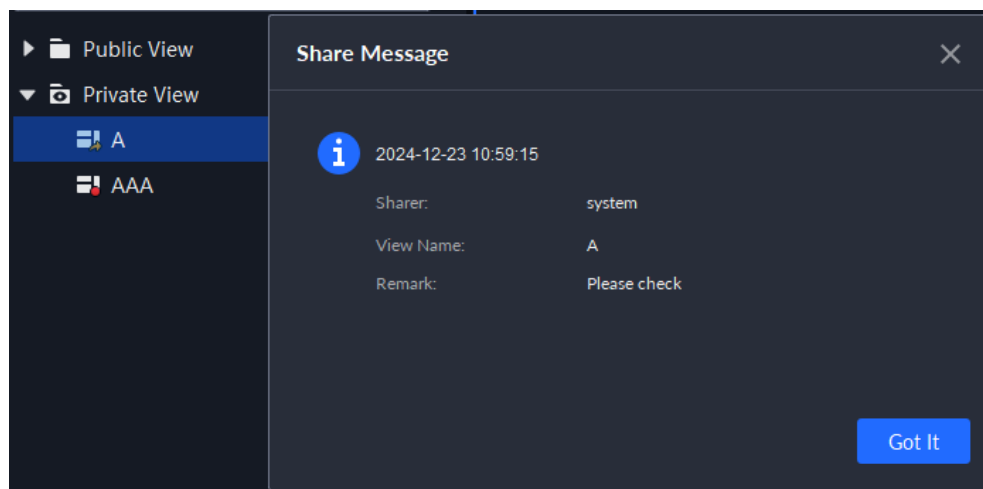
Results

The user who receives the shared view can right-click a view, and then click **View Details** to check the details of the shared view.



 indicates read, and  indicates unread.

Figure 5-19 Check the shared view



5.1.2.2.7 Related Operations

- Change the group a view belongs to

Drag a view to other groups. You can only do so for private views. You cannot drag a private view to a public view group, or a public view to a private view group.

- View the details of a public view group or a view

Right-click a public view group, and then select **View Details** to check the roles and users that are allowed to access it.

Right-click a public view group, and then select **Resources Details** to check the information of the channels, including the name, type, and organization.

- Edit the information of a public view group

Right-click a public view group, and then select **Edit** to change its name and the roles and users that are allowed to access it.

- Rename a view

Right-click a view, and then select **Rename** to change its name.

- Delete a group or view

Right-click a group or view, and then select **Delete** to delete it. If there are multiple views in the group, they will also be deleted.

5.1.2.3 Favorites

Add frequently used channels to favorites so that you can quickly locate and use them. You can also share your favorites with other users.

Prerequisites

The **Resources** menu permission is required; otherwise, you cannot view resources, add them to favorites, and save the resources to view. Permissions can be configured from  > **User** > **Role Management**.

5.1.2.3.1 Creating Favorites Folder

Each user can create up to 999 favorites folders. The number of channels in all favorites folders can be up to 2,000.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring**.

Step 2 Click **Favorites**.

Step 3 Click a folder and click , or right-click a folder and select **Add a Favorites**.

Step 4 Select a parent node, enter a name for the folder, select the channels to be added to the folder, and then click **OK**.

The favorites folder is added as a sub folder under the parent node you selected. The maximum level of a favorites folder can be up to 10.

5.1.2.3.2 Editing or Deleting Favorites Folder

Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring** > **Favorites**.

- Edit a folder: Click a folder and click , or right-click a folder and select **Edit**, and then you can edit the name and channels of the folder.
- Delete a folder: Click a folder and click , or right-click a folder and select **Delete**, and then you can delete the folder, its sub folders and all channels.

You can also right-click a channel and select **Delete** to remove it from a folder.

5.1.2.3.3 Sharing Favorites Folder

You can share a folder and its channels with other users. For permission control, if users have permission to access certain channels, or do not have any permission to access the channels, they will receive a folder with only the channels they have permission to, or an empty folder.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring**.
- Step 2** Click **Favorites**.
- Step 3** Right-click a folder, and then select **Share the Favorites**.
- Step 4** Select one or more users, and then click **OK**.

The folder, its sub folders, and all the channels will be shared with the users you selected. But if any of the follow situation occurs with the users you are sharing with, this operation will fail:

- They have more than 999 folders.
- They have 2,000 channels in all folders.
- The levels of their folders have reached 10.

5.1.2.3.4 Viewing Favorites Folder

- Live view

On the **Monitoring** page, and then click **Favorites** to open list of favorites folders. Double-click or drag a folder or channel to the window on the right to view live videos.

- Tour

On the **Monitoring** page, and then click **Favorites** to open list of favorites folders. Right-click a folder and select **Tour**, and then select a duration. The platform plays live videos of all the channels in the folder and its sub folders in a loop.

- ◇ To view remaining time of a channel during tour, click .
- ◇ To pause, click .
- ◇ To exit tour play, click .

5.1.2.4 PTZ

Operate PTZ cameras during live view on the DSS Client.

Background Information



If you want to configure PTZ control, you need to add **PTZ Operation and Configuration** permission on role management page. If you want to call the PTZ functions, you need to add **PTZ Operation** permission on the role management page.

5.1.2.4.1 Configuring Preset

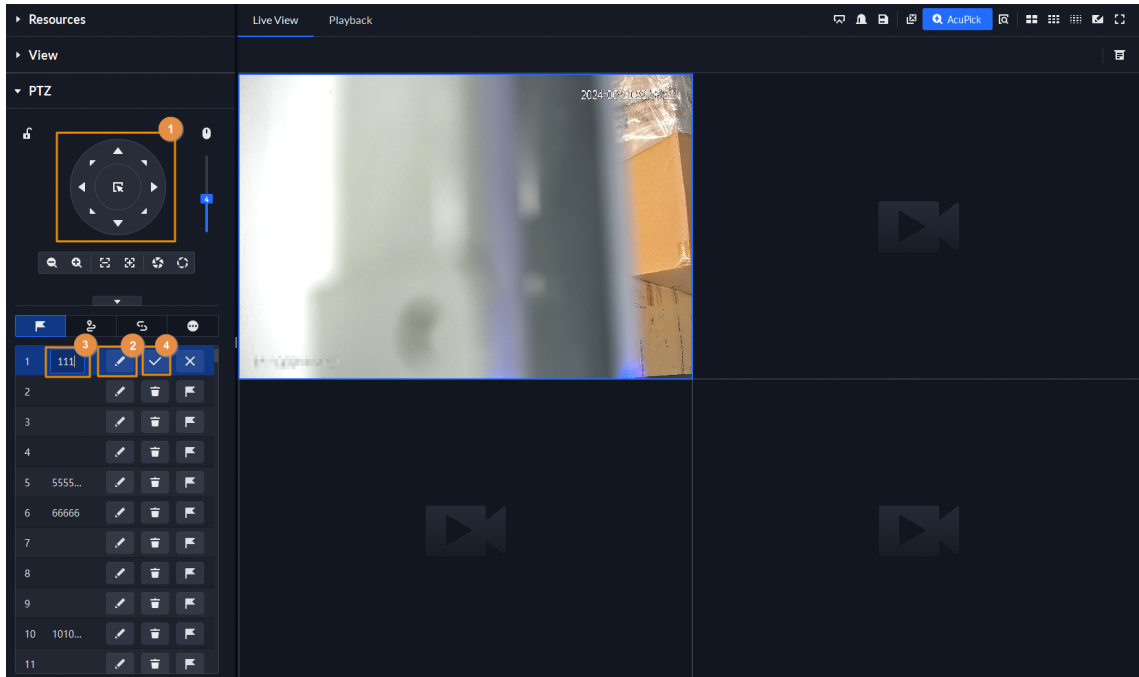
A preset is a set of parameters involving PTZ direction and focus. By calling a preset, you can quickly rotate the camera to the pre-defined position.

Procedure

- Step 1** On the **Monitoring Center** page, open the video of a PTZ camera.
- Step 2** Click .

- Step 3** Click .
- Step 4** Add a preset.
1. Rotate the PTZ camera to a specific point.
 2. Click , enter the preset name, and then click .

Figure 5-20 Add a preset



Related Operations

Call a preset: Click  of a specific preset, and then camera will rotate to the related position.

5.1.2.4.2 Configuring Tour

Set the tour parameters so that a camera can go back and forth among different presets. Set tour to enable camera to automatically go back and forth between different presets.

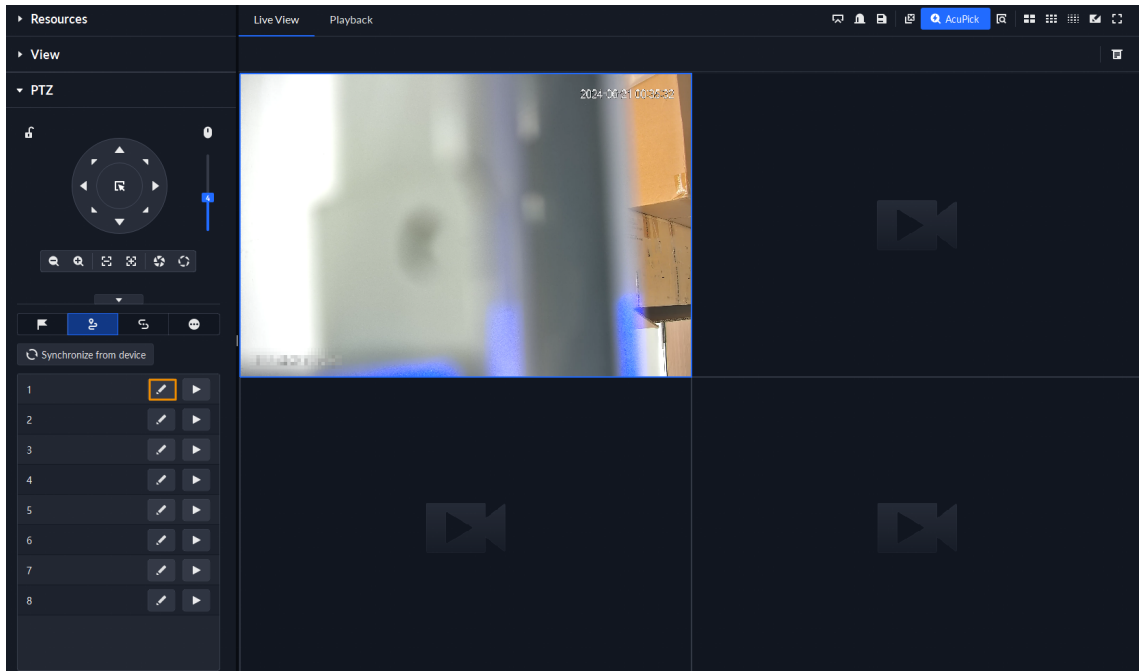
Prerequisites

You have added at least 2 presets.

Procedure

- Step 1** On the **Monitoring Center** page, open the video of a PTZ camera.
- Step 2** Click .
- Step 3** Click .
- Step 4** Click .

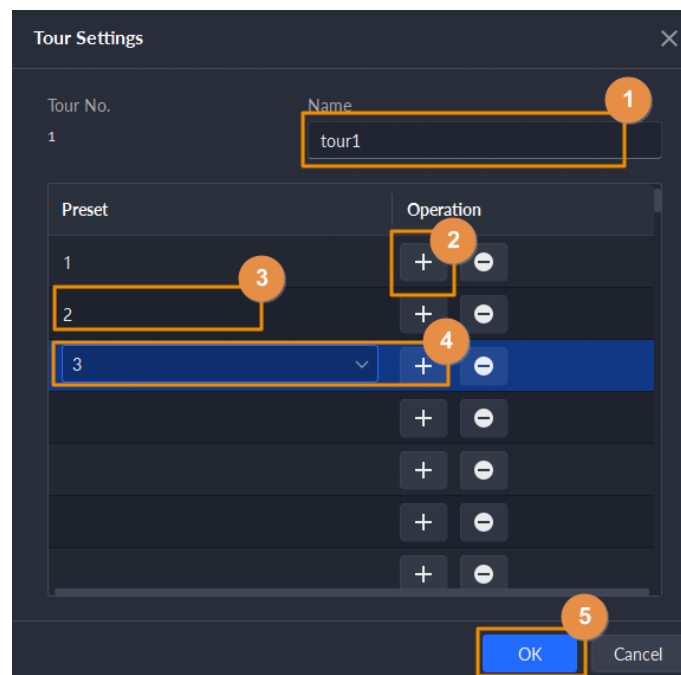
Figure 5-21 Add tours



Step 5 Add tours.

1. Enter tour name, and click **+**.
2. Select a preset from the drop-down list on the left.
3. Repeat the previous 2 steps to add more presets.
4. Click **OK**.

Figure 5-22 Add tours (2)



Related Operations

To start tour, click **▶**, then camera goes back and forth among the presets.

5.1.2.4.3 Configuring Pattern

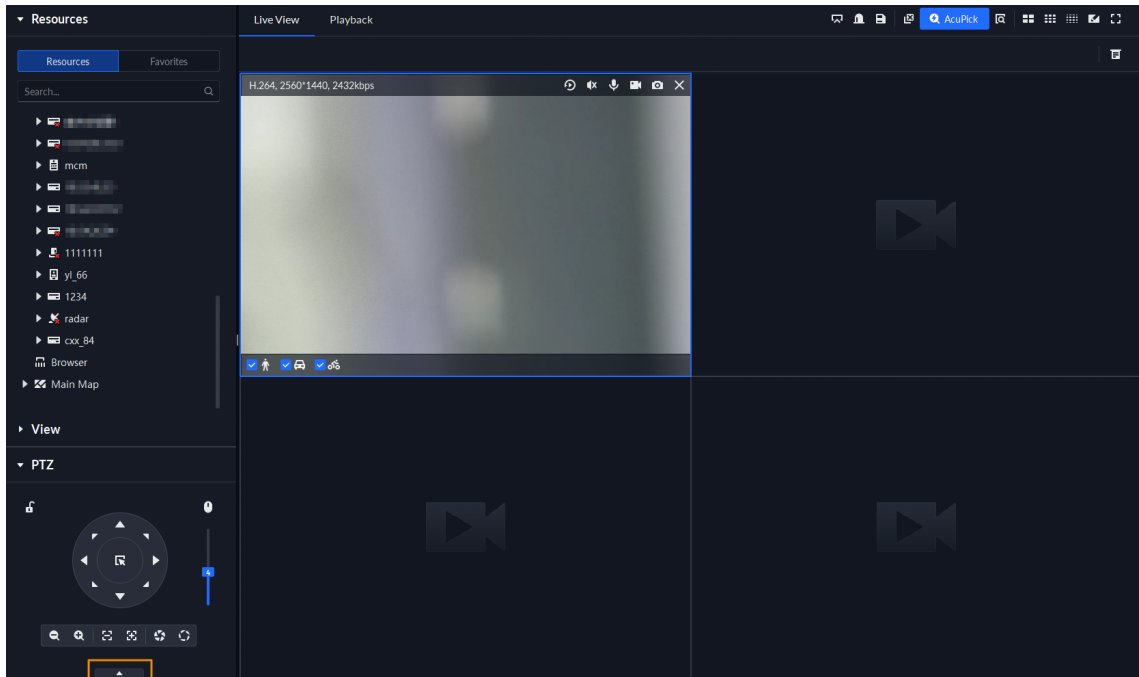
A pattern is a record of a consecutive series of PTZ operations. You can select a pattern to repeat the corresponding operations quickly. See pattern configuration instructions as follows.

Procedure

Step 1 On the **Monitoring Center** page, open the video of a PTZ camera.

Step 2 Click .

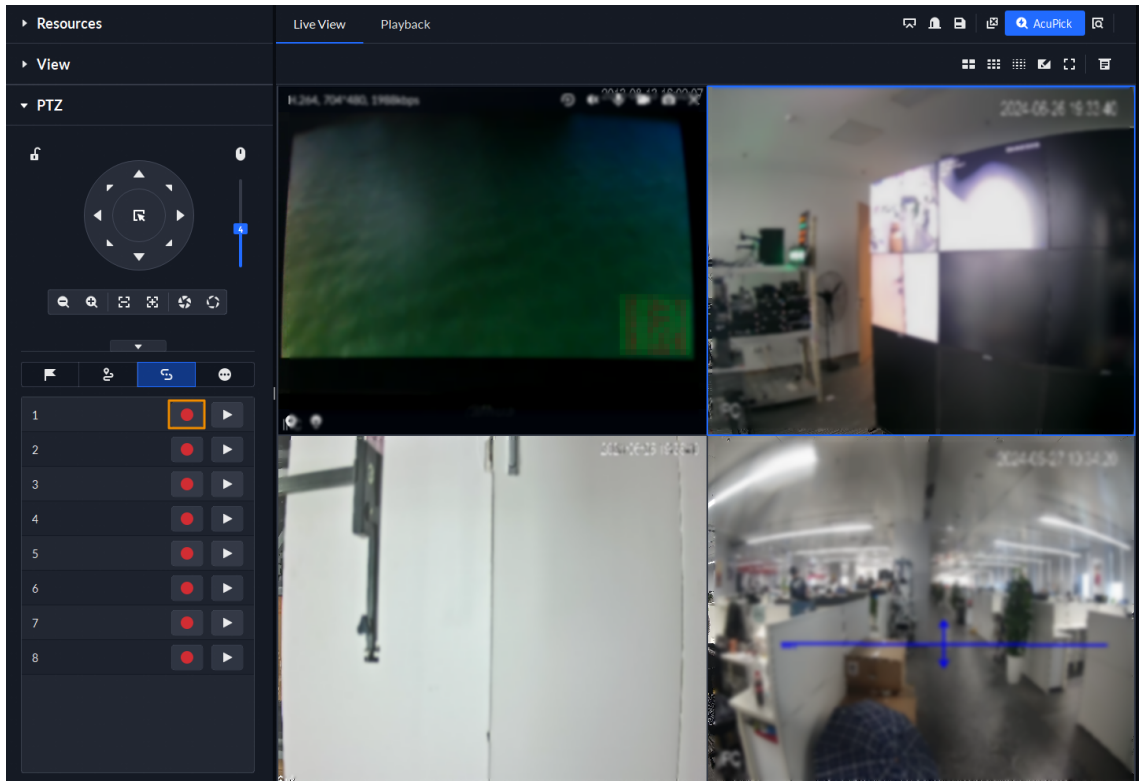
Figure 5-23 Go to PTZ control panel



Step 3 Click .

Step 4 Click , and then operate the 8 PTZ buttons to set pattern.

Figure 5-24 Set pattern



Step 5 Click .

Related Operations

Call pattern: Click , and then the camera will automatically repeat the pattern that you have configured.

5.1.2.4.4 Configuring Scan

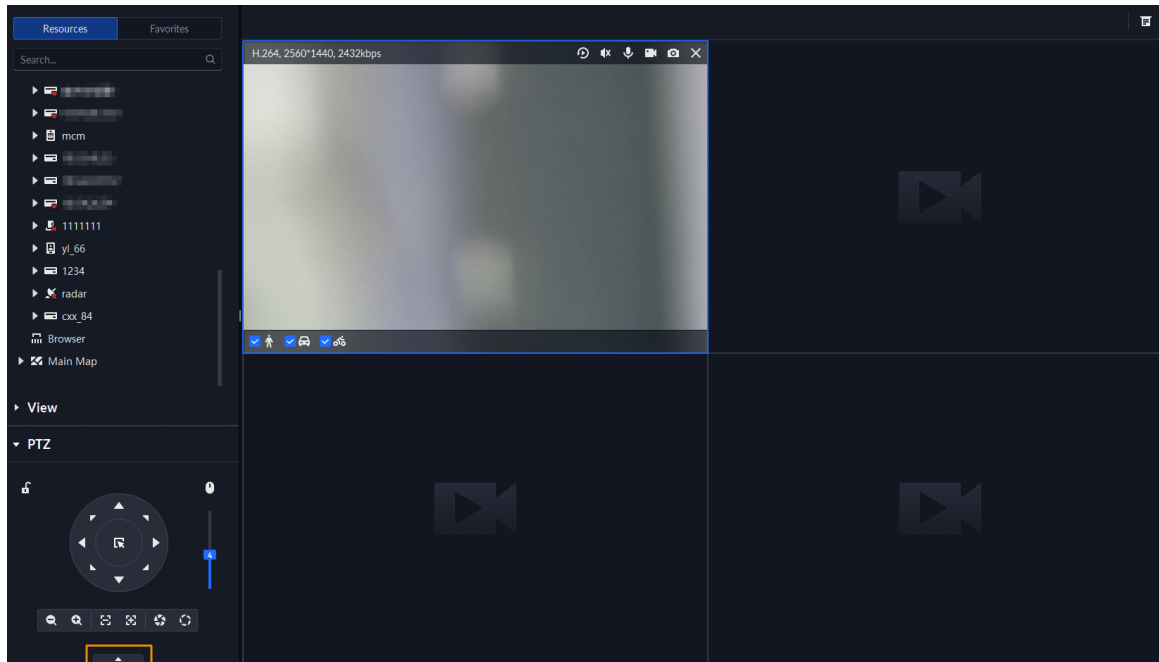
The camera automatically scans horizontally at a certain speed.

Procedure

Step 1 On the **Monitoring Center** page, open the video of a PTZ camera.

Step 2 Click .

Figure 5-25 Go to PTZ control panel



Step 3 Click .

Step 4 Click PTZ button, and rotate PTZ to the left to a position, and then click  to set the left boundary.

Step 5 Continue to rotate PTZ to the right to a position, and then click  to set the right boundary.

Step 6 Click  to start scanning, then PTZ will rotate back and forth automatically within the two boundaries.

5.1.2.4.5 Enabling/Disabling Pan

On the **Monitoring Center** page, open the video of a PTZ camera. Click , and then click . PTZ rotates 360° at a specified speed. Click  to stop camera rotation.

5.1.2.4.6 Enabling/Disabling Wiper

Enable/disable the PTZ camera wiper. Make sure that the camera supports wiper function.

On the **Monitoring Center** page, open the video of a PTZ camera. Click , and then click  to turn on wiper. Click  to turn off wiper.

5.1.2.4.7 Enabling/Disabling Light

Turn on/off camera light. Make sure that the camera supports light.

On the **Monitoring Center** page, open the video of a PTZ camera. Click , and then click  to turn on light. After enabling light, click  to turn off light.

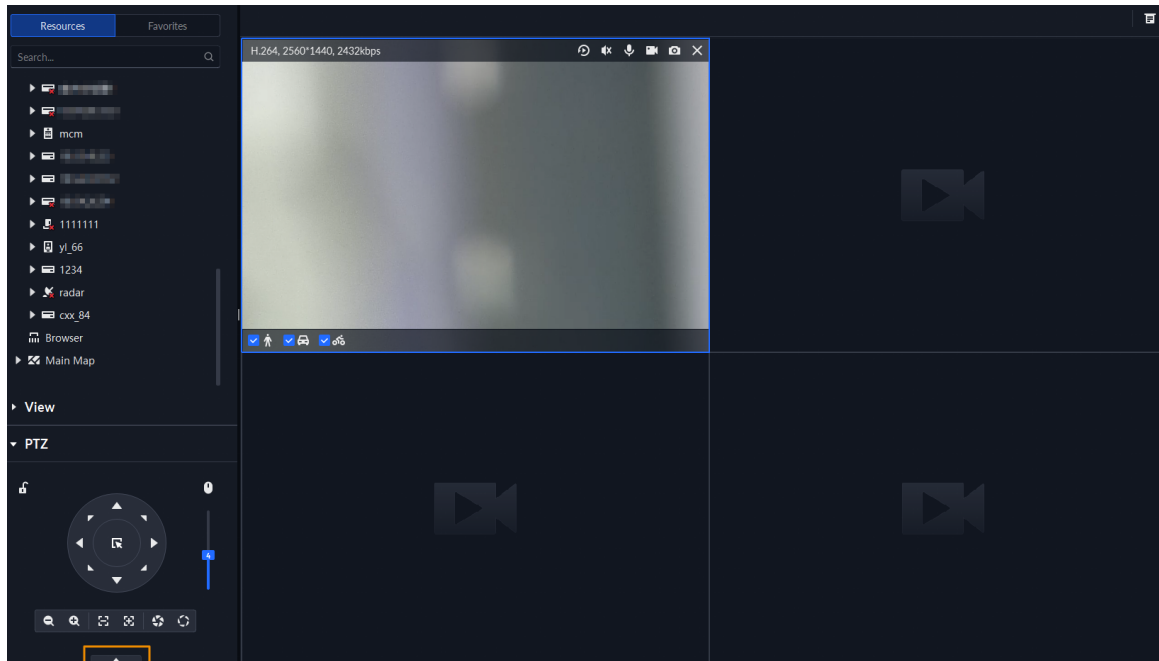
5.1.2.4.8 Configuring Custom Command

Procedure

Step 1 On the **Monitoring Center** page, open the video of a PTZ camera.

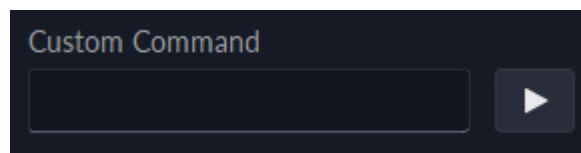
Step 2 Click .

Figure 5-26 Go to PTZ control



Step 3 Enter your command in the **Command** box.

Figure 5-27 Custom command



Step 4 Click  to show the command functions.

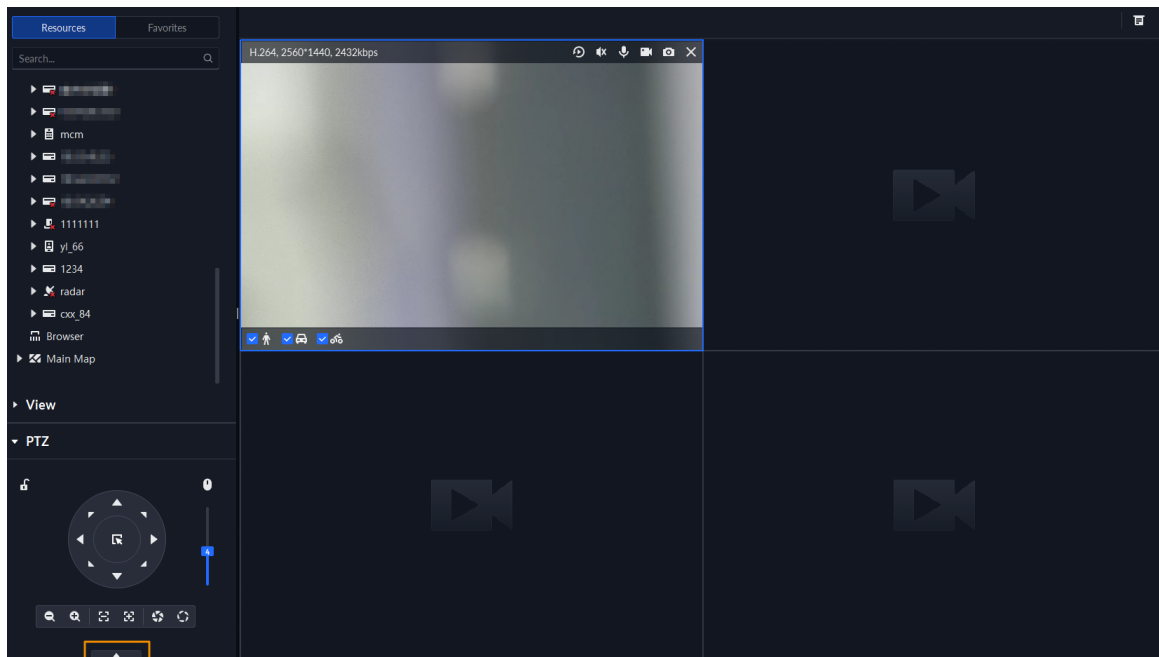
5.1.2.4.9 PTZ Menu

Procedure

Step 1 On the **Monitoring Center** page, open the video of a PTZ camera.

Step 2 Click .

Figure 5-28 Go to PTZ control panel



Step 3 Click .

Step 4 Click .

Step 5 Use the panel to go to the menu configuration page.

Figure 5-29 Go to PTZ menu configuration page

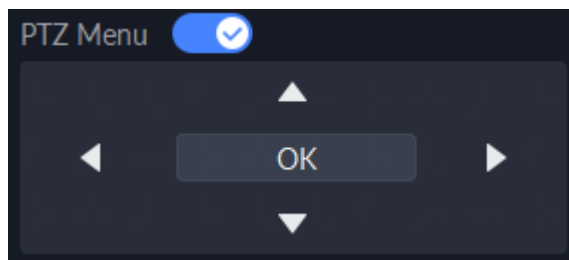


Table 5-6 PTZ menu description

Parameters	Description
	Up/down.
	Left/right. Point to set parameters.
	Click  to enable PTZ menu function. System displays main menu on the monitor window.
	Click  to close PTZ menu function.
OK	It is the confirm button. It has the following functions. • If the main menu has the sub-menu, click OK to enter the sub-menu. • Point to Back and then click OK to go to go back to the previous menu. • Point to Exit and then click OK to exit the menu.

Parameters	Description
Camera	Point to Camera and then click OK to enter camera settings sub-menu page. Set camera parameters. It includes picture, exposure, backlight, day/night mode, focus and zoom, defog, and default.
PTZ	Point to PTZ and then click OK to go to PTZ sub-menu page. Set PTZ functions. It includes preset, tour, scan, pattern, rotation, PTZ restart, and more.
System	Point to System and then click OK to go to system sub-menu page. Set PTZ simulator, restore camera default settings, video camera software version and PTZ version.
Return	Point to the Return and then click OK to go back to the previous menu.
Exit	Point to the Exit and then click OK to exit PTZ menu.

5.1.2.5 Fisheye-PTZ Smart Track

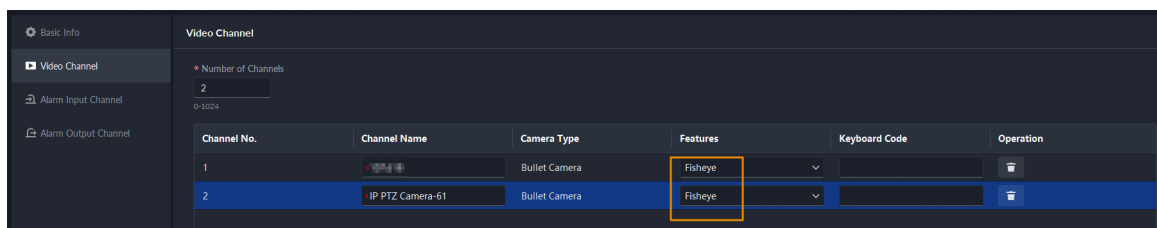
Link a PTZ camera to a fisheye camera so that when the fisheye camera detects a target, the PTZ camera automatically rotates to it and track.

5.1.2.5.1 Preparations

Make sure the following preparations have been completed:

- Fisheye camera and PTZ camera are well deployed. For details, see corresponding user manuals.
- Basic configurations of the platform have been finished. For details, see "3 Basic Configurations".
 - ◇ When adding cameras, select **Encoder** from **Device Category**.
 - ◇ The **Features** of a fisheye camera is set to **Fisheye**. For details, see "3.1.2.5.2 Modifying Device Information".

Figure 5-30 Set the feature to Fisheye

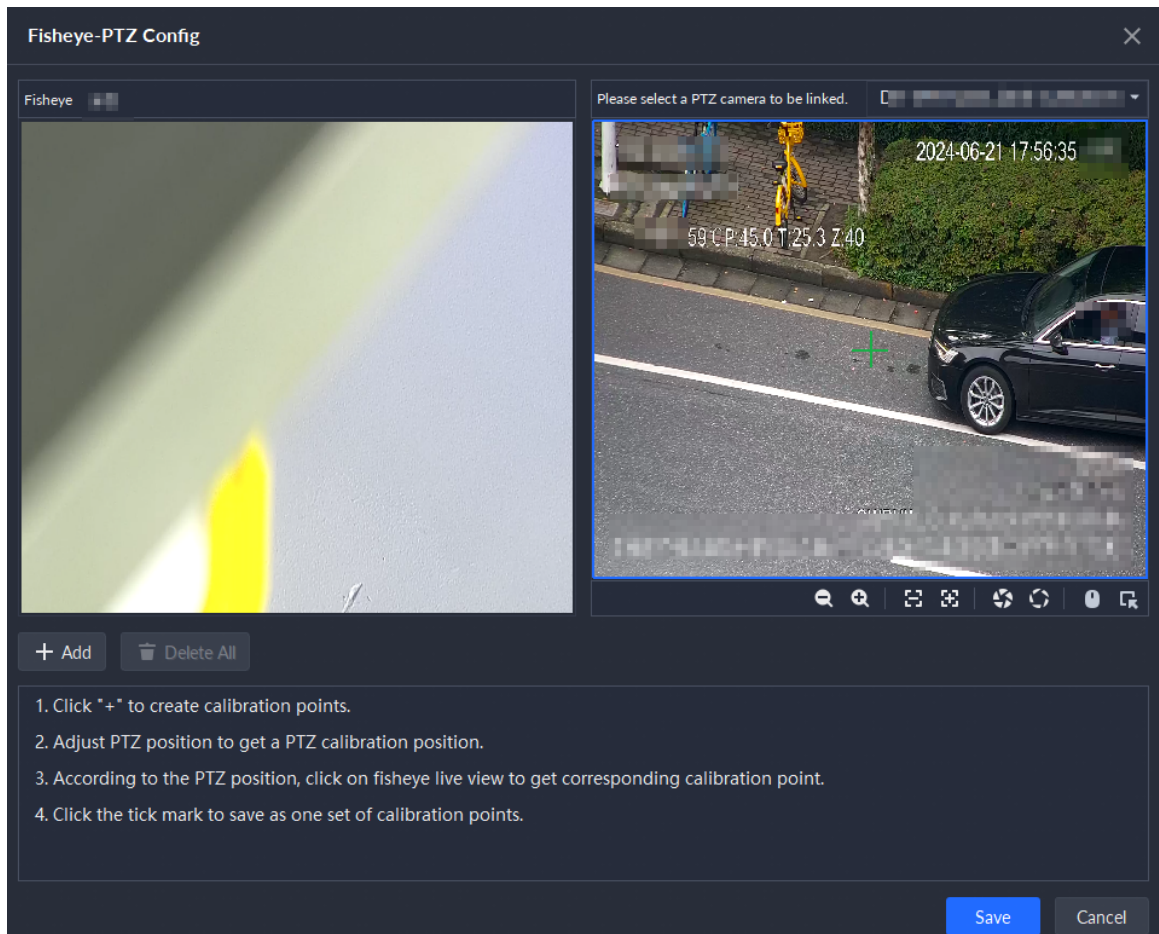


5.1.2.5.2 Configuring Fisheye-PTZ Smart Track

Procedure

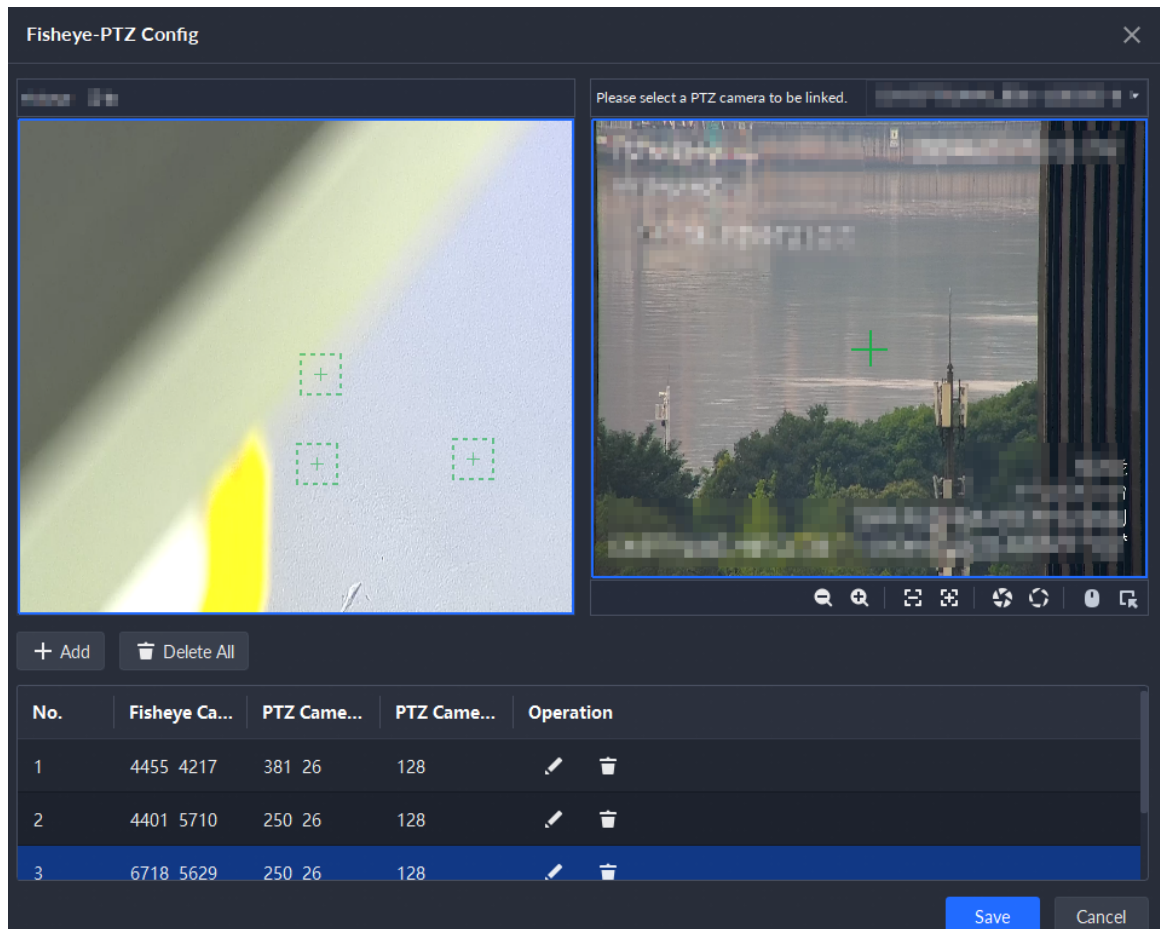
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then click **Monitoring Center**.
- Step 2** Click .
- Step 3** In the device tree on the left, right-click a fisheye camera, and then select **Modify Smart Track**.
- Step 4** Click  next to **Please select a PTZ camera to link**, and then select a PTZ camera.

Figure 5-31 Set smart track rules (1)



Step 5 Click **+** and then move the **+** of the fisheye on the left to select a position. Click **📍** of the PTZ camera to find the position. Adjust the PTZ camera to find the position and move the PTZ to the center position (The green cross on the image).

Figure 5-32 Set smart track rules (2)



- Select 3-8 mark points on fisheye camera.
- When you find mark point on the right side of the PTZ camera, click to zoom out PTZ.
- Click to 3D position, and when you click a certain point on the left side of PTZ camera, it will automatically move to the center.

Step 6 Click to save the calibration point.

See above steps to add at least three calibration points. These three points shall not be on the same straight line.

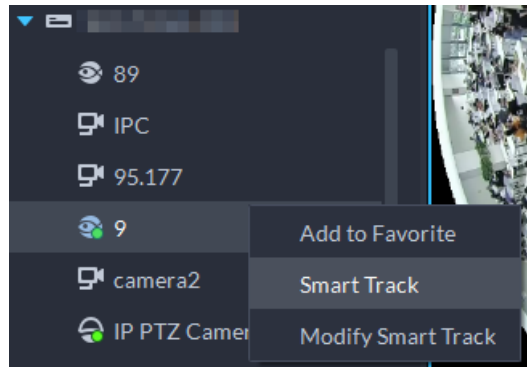
Step 7 Click **Save**.

5.1.2.5.3 Applying Fisheye-PTZ Smart Track

Procedure

Step 1 Log in to the DSS Client. On the **Monitoring Center** page, select the fisheye camera on the device tree and then right-click to select **Smart Track**.

Figure 5-33 Select a smart track channel



Step 2 Click any point on the left of fisheye, PTZ camera on the right will automatically rotate to corresponding position.

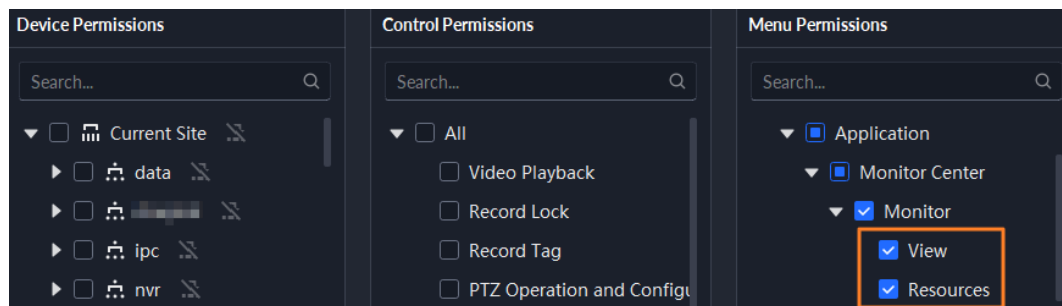
5.1.3 Playback

Play back recorded videos.

Prerequisites

The **Resources** and **View** menu permissions are required; otherwise, you cannot view resources, add them to favorites, and save the resources to view. Permissions can be configured from  > **User** > **Role Management**.

Figure 5-34 Configure view and resources permissions



5.1.3.1 Page Description

Log in to the DSS Client. On the **Home** page, click , and then click **Monitoring**. Click the **Playback** tab.



Drag  between the resource tree and the video window to the left, to hide the resource tree, and then the **View and Resource** selection bar will show at the top, where you can select or search the views and resources that you need, and then drag them to the window to play the video.

Click  to show the resource tree.

Figure 5-35 Playback page

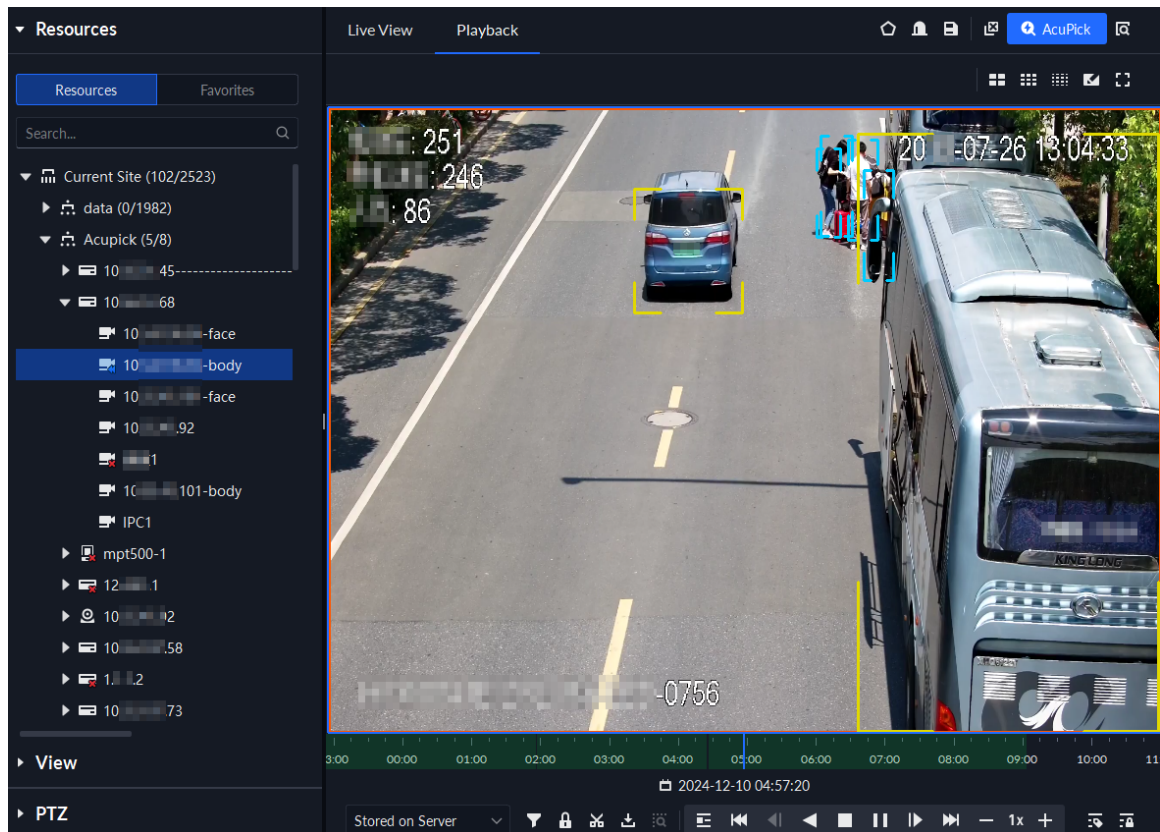
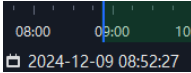
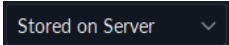
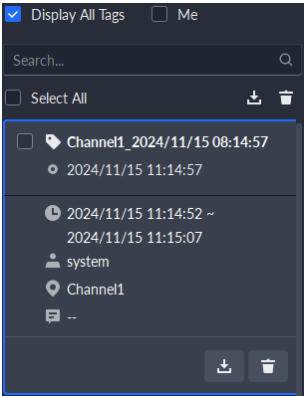


Table 5-7 Function description

Icon	Description
	Filter video according to record type.
	Lock the video stored to the server within some period of designated channel. Locked video will not be overwritten when disk is full.
	Select and download a duration of video on the progress bar.
	Download the video.
	Make dynamic detection analysis over some area of the record image, and it only plays back the video with dynamic image in the detection area.
	Play multiple recorded videos from the same time. For example, you are playing recorded videos from 3 channels at the same time. Select channels, configure when you want to play the recorded video from, and then click this icon. All 3 channels will play recorded videos from the same time.

Icon	Description
	Play the previous or next video clip of the most recent time. For example, when searching for videos, if you do not remember the exact event time, and there is no video clip at the time that you search, you can try to play the previous or next video of the most recent time, to track the event.  This function is not available when  is enabled.
	Play back or forward by frame.
	Play the video backwards.
	Stop or pause the video.
	Fast forward or slow down the video to up to 64 times. When playing a video backwards or forwards alternately, the play speed will not be changed.
	Click  to select the date to view the video. The time period of the video is displayed on the timeline. During playback, you can drag time progress bar to play back video at the specific time. Stay your mouse on the time progress bar, and then the system displays the video thumbnail of that time, which makes it easy to determine whether it is the video that you want to view.
	Select the storage location of the video to be searched. Supports searching for the video on the platform server or storage device.

Icon	Description
	Open the tag to view the tag records. You can also: • Select Display All Tags or Me to view all tags or tags added by you. • Double-click a tag record to play the video related to the tag. • Click  to view tag details, such as the time before and after tagging, the user who added the tag, the channel name, remarks, and more. • Download the records one by one or in batches. When downloading, you need to set an encryption password to encrypt the tag records. • Delete the tags one by one or in batches. 
	Lock records.

5.1.3.2 Playing Back Video

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center > Monitoring**.
- Step 2** Click the **Playback** tab.
- Step 3** Double-click or drag a channel to a window on the right.



- Drag  between the resource tree and the video window to the left, to hide the resource tree, and then the **View and Resource** selection bar will show at the top, where you can select or search the views and resources that you need, and then drag them to the window to play the video.

Click  to show the resource tree.

- View channel status.

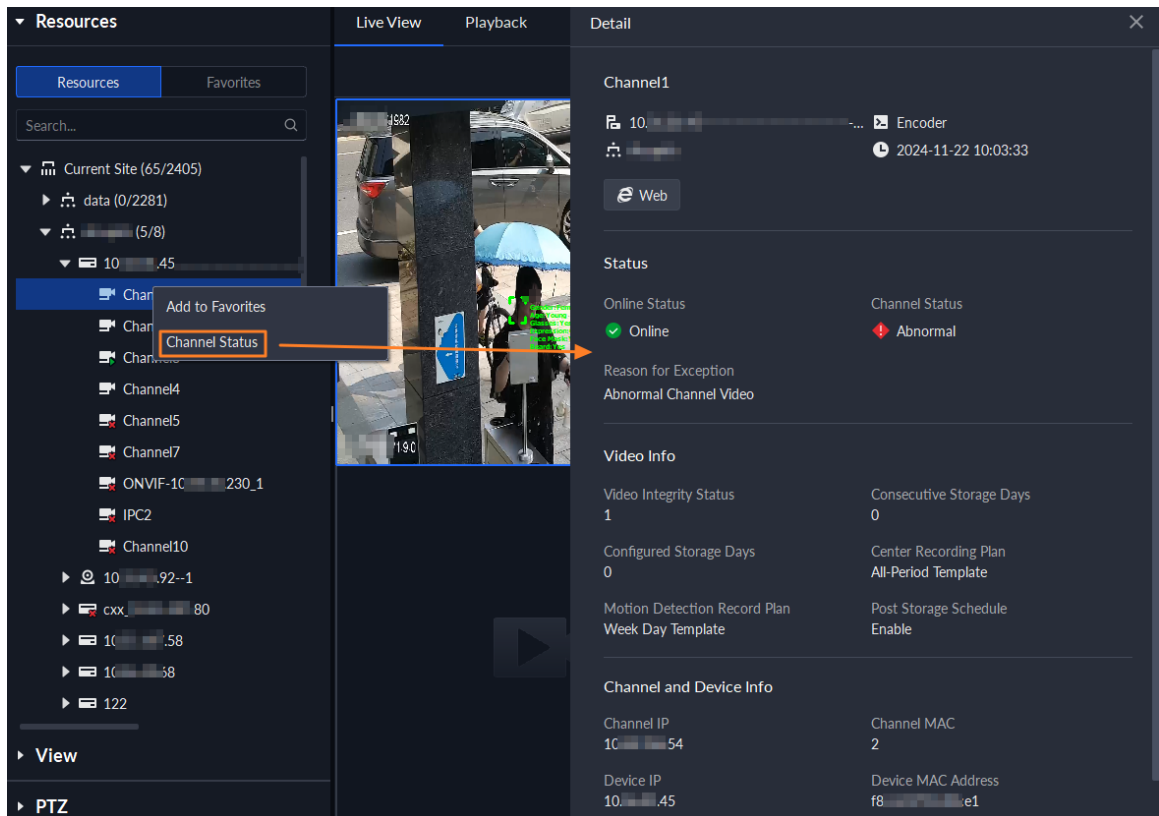
Right-click a node, select **Channel Status**, and then you can view the channel details, including status, video information, channel and device information.

Click , and then it goes to the login page of the device webpage.



If you do not have the device permissions, you can only open the webpage, but not log in. To configure device permissions, go to  > **User > Role**.

Figure 5-36 View channel status



Step 4 Select the storage path of recorded video from **Stored on Server**, and then click  to select the date.



- Dates with blue dots means there are videos.
- After selecting a date, the platform will search for videos on that date from other channels. If you switch to the **Live View** page, or close the page or the PC client, the date will be reset.

Step 5 Click  to play the video.

Step 6 Hover over the video, and then the icons appear. You can perform the following actions.

Figure 5-37 Video playback

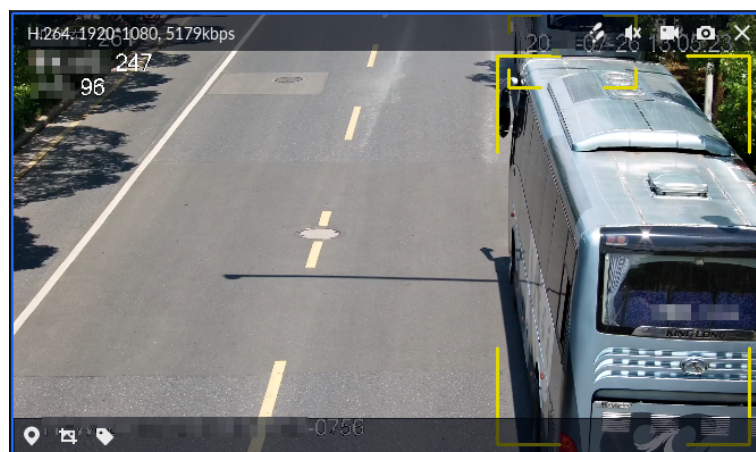


Table 5-8 Function description

Icon	Name	Description
	Visual tracking	Click  to turn on visual tracking, and then you can click the shape over the video image to view the video of associated channels, so that you can track the area or location where the target passes through. For details, see "5.1.2.1.3 Visual Tracking".
	Audio	Turn on/off the audio of the channel.  The audio is not enabled by default. To enable the audio function, the Video Sound permission is required from  > User > Role Management .
	Take a recording on the device	Click it to start recording. The recorded video is stored locally. The saving path is C:\DSS\DSS Client\Record\ by default.
	Take a snapshot on the device	Take a snapshot of the current image and save it locally. The saving path is C:\DSS\DSS Client\Picture\ by default.
	Close	Close the window.
	Map location	If the device has been marked on the map, click the icon to open the map in a new window to display map location of the device.
	Search by snapshot	Capture the target in the playback window. Click  to select the search method, and then the system goes to the page with search results. More operations: - Place the mouse on the selected area, and then drag to move the selection area. - Place the mouse to the upper-left, upper-right, and lower-left corner of the selected area, drag to adjust the size of the selection area. - Right-click to exit search by snapshot.
	Tag	Tag the videos of interest for easy search in the future. You can search for the tagging records from Download Center > Tagging Record .  Device Permissions and the Record Tag control permission are required from  > User > Role Management ; otherwise, you cannot tag the video.

Right-click the video, and then you can perform the following actions. The menu might vary, depending on the devices that you use.

Figure 5-38 Shortcut menu

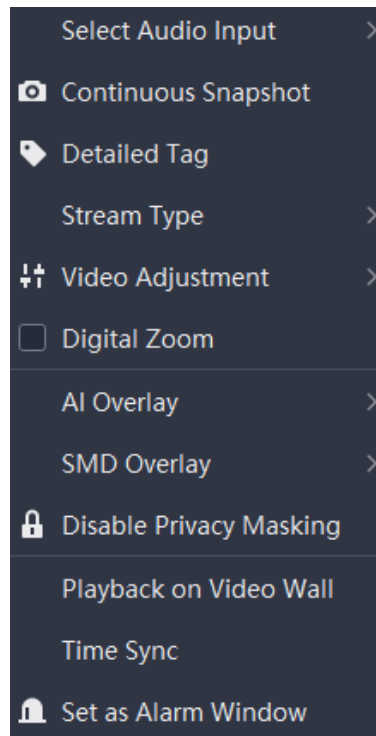


Table 5-9 Description

Parameters	Description
Select Audio Input	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Continuous Snapshot	Take snapshots of the current image (three snapshots each time by default). The snapshots are saved to <code>..\DSS\DSS Client\Picture</code> by default. To change the snapshot saving path, see "8.4.5 Configure File Storage Settings".
Detailed Tag	Tag the videos of interest for easy search in the future. You can set tag details for that tag such as its name, time, the moment before and after it, the user who created it, and its object. You can also search for the tag records in Download Center > Tagging Record.  - You must gain control permission in Device Permissions and the Record Tag. Go to  > User > Role Management to set them, otherwise, you will not be able to tag the video. - The channel that you want to tag must be configured with recording plan, otherwise you will not be able to search for videos after you add tags.

Parameters	Description
Stream Type	Select Main Stream, Sub Stream 1 or Sub Stream 2. Videos recorded on the main stream will have the best quality, but they require more storage.  This function is available for recordings stored on device only.
Video Adjustment	Adjust the brightness, contrast, saturation, and chroma of the video for video enhancement.
Digital Zoom	Click it, and then double-click the video image to zoom in the image. Double-click the image again to exit zooming in.
AI Overlay	The client does not show rule lines over live video by default. When needed, you can click AI Overlay , enable Rule Overlay and Bounding Box Overlay , and then the live video shows rule lines if the AI detection rules are enabled on the device. This configuration is effective with the current selected channel both in live video and playback.
SMD Overlay	Enable SMD Overlay to show target bounding box over live video. When SMD is enabled on the device, you can enable SMD Overlay for the device channel, and then the live video will display dynamic target bounding boxes. This configuration is effective with the current selected channel both in live video and playback.
Disable Privacy Masking	For cameras that support privacy masking for human faces, you can disable the masking here to view the face image.
Playback on Video Wall	Play the video of the current channel on video wall. Make sure that video wall is configured (see "5.1.5 Video Wall").
Time Sync	Synchronize the device time with server time.  This function requires that you gain control permission in Device Permissions and the Device Time Sync. Go to  > User > Role Management.
Set as Alarm Window	When selecting open alarm linkage video In Preview (in live window) from Local Settings > Alarm , then the video will be displayed on the window which is set to alarm window. If multiple alarms are triggered, the video linked to the latest alarm will be opened. If the number of alarm windows is fewer than the number of linkage videos, the video linked to the earliest-triggered alarm will be opened. After enabling Set as Alarm Window , the window frame is displayed in red.

5.1.3.3 Locking Videos

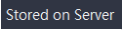
Lock the video stored on the server within a period of a specific channel. The locked video will not be overwritten when disk is full.

Background Information



Only the videos stored on server can be locked.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center**.
- Step 2** Click the **Playback** tab.
- Step 3** Select a channel from the device tree, and then double-click it, or drag it to the window.
- Step 4** Select the storage path of recorded video from , and then click  to select the date.
The search results are displayed.



Dates with blue dot means there are video recordings.

- Step 5** Select a window that has recorded video, and then click  on the bottom of the page, and then click on the timeline to mark the start point and end point of the video clip you need.
- Step 6** Confirm the start and end time, and then click **OK**.

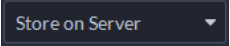
Related Operations

Click  on the lower-right corner, and then all the recordings locked by the user currently logged in to the client are displayed. Double-click one to quickly play the recording.

5.1.3.4 Tagging Videos

You can tag records of interest for quick search.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center**.
- Step 2** Click the **Playback** tab.
- Step 3** Double-click or drag a channel to a window.
- Step 4** Select the storage path from  where the recorded videos are stored, and then click  to select the date.
The search results are displayed.



Dates with blue dot means there are video recordings.

Figure 5-39 Playback page



Step 5 Point to the window, and then click .

Step 6 Enter a name for the tag, and then click **OK**.

Related Operations

Click  on the lower-right corner to view all the tags in the current recorded video. Double-click a tag to play the recorded video from the time of the tag. You can search for tags by their names.

5.1.3.5 Filtering Recording Type

Filter video according to record type, record type includes scheduled recording, alarm video, motion detection video, and videos recorded in main or sub stream.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center**.

Step 2 Click the **Playback** tab.

Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

Step 4 Click , select one or more types, and then click **OK**.

The platform only displays videos of the selected types in different colors on the timeline.



Filtering videos by video stream is only supported when you are viewing a video stored on a device, and the search type of device video stream is set to main and sub streams. For details, see "8.4.2 Configuring Video Settings".

5.1.3.6 Searching for Targets

When playing back a video, you can manually select a target, or select one automatically recognized by AcuPick, and then search for it in DeepXplore.

5.1.3.6.1 Selecting Target Manually

Manually select a target in the video and quickly search for it in DeepXplore.

Procedure

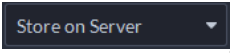
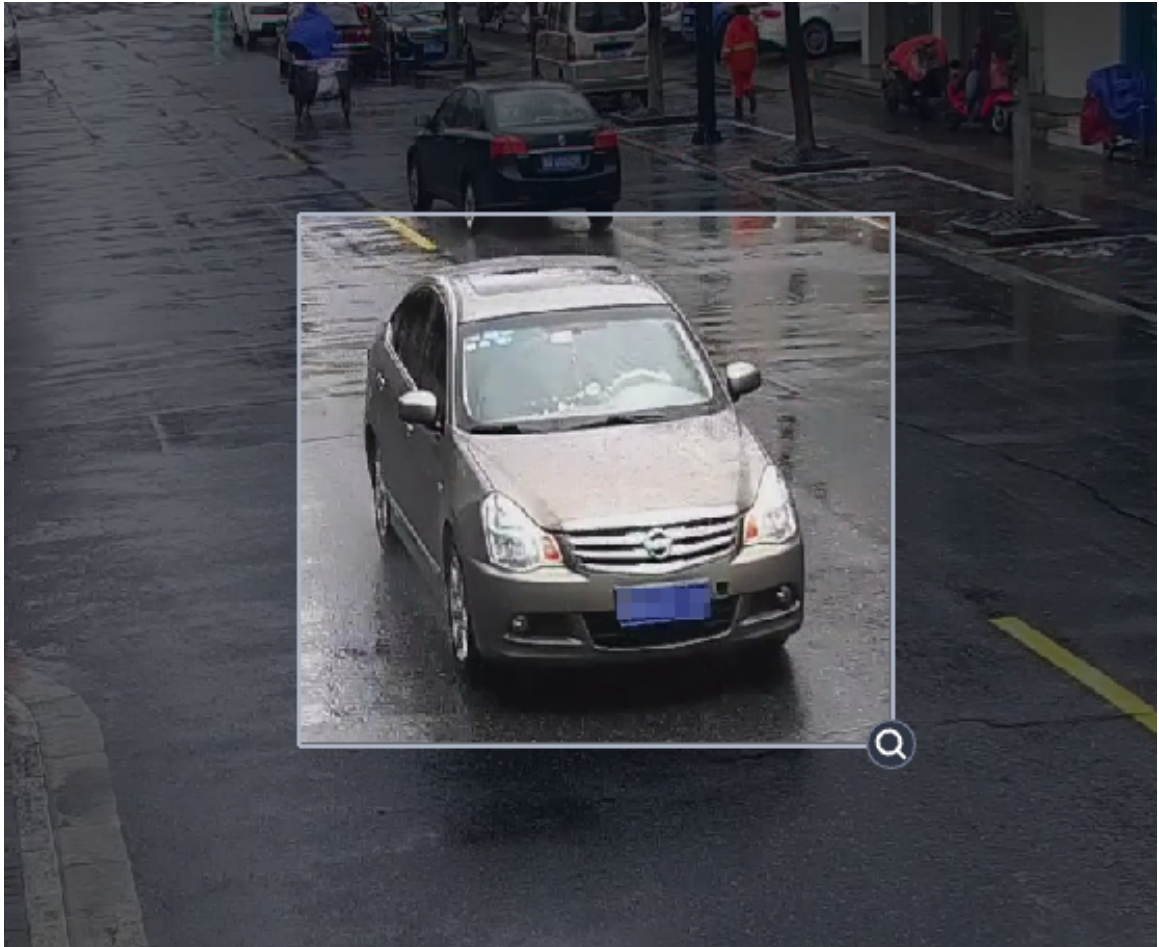
- Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center** > **Monitoring**.
- Step 2 Double-click or drag a channel to a window on the right.
- Step 3 Select the storage path of recorded video from , and then click  to select the date.
- 
- Dates with blue dot means there are recordings.
- Step 4 Click  on the bottom of the page.
- Step 5 Drag on the video to select a target.
- 
- Right-click to exit this function.

Figure 5-40 Select a target



Step 6 (Optional) Adjust the area of selection.

- Move the selection box: Place the mouse cursor over the selected area, click the left button, and the drag the mouse.
- Resize the selection box: Place the mouse cursor over the upper-left, lower-left, or upper-right corner of the selected area. Click the left mouse button and drag it to adjust the size accordingly.

Step 7 Click  and select a type for the target, and then you are directed to DeepXplore to search for it. For details, see "5.3 DeepXplore".

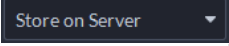
5.1.3.6.2 AcuPick

The platform can automatically recognize different types of targets in the video. You can select a target and then quickly search for it in DeepXplore.

Prerequisites

1. Purchase a license with the AcuPick function, and then activate the license. For details, see "2.1.6 Licensing".
2. Configure the parameters of AcuPick. For details, see "7.4.4 Configuring Central Intelligent Server".
3. Configure the identity certificate and secret key in the DSS Server. For details, see "2.1.4 Management Tool".

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center** > **Monitoring**.
- Step 2** Double-click or drag a channel to a window on the right.
- Step 3** Select the storage path of recorded video from , and then click  to select the date.



Dates with blue dot means there are recordings.

- Step 4** Click  **AcuPick** on the bottom of the page to automatically recognize targets in the video, including faces, human bodies, and vehicles.



Click  to exit this function.

Figure 5-41 Automatically recognize targets



- Step 5** Hover over the target, and then click  of a target to search for it in DeepXplore. For details, see "5.3 DeepXplore".

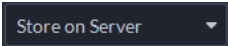


If certain targets are not recognized, you can click  to manually select one. For details, see "5.1.2.1.1 Selecting and Searching for Target Manually".

5.1.3.7 Clipping Videos

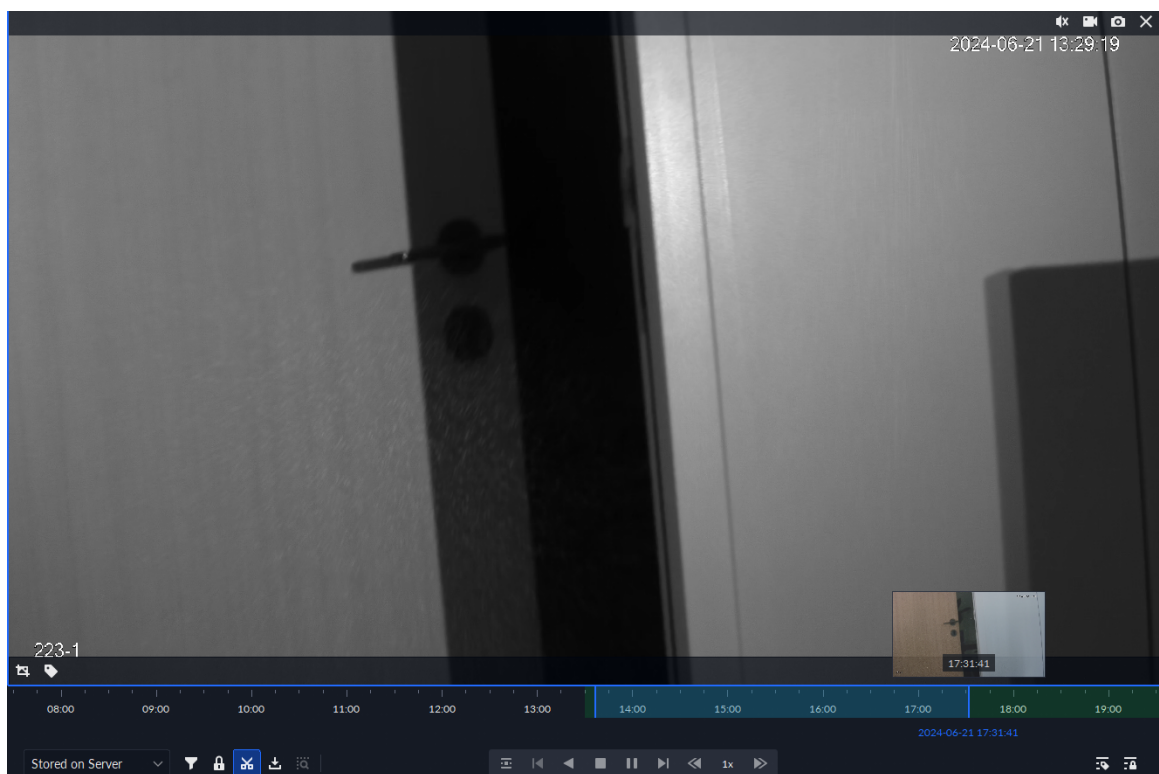
Download a video by selecting a period on the timeline.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center**.
- Step 2 Click the **Playback** tab.
- Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.
- Step 4 Select the storage path of videos from , and then click  to select the date.
The search results are displayed.

Dates with blue dot means there are videos.
- Step 5 Select a date with video recordings, and then click .
- Step 6 On the timeline, click the point with green shade to start clipping, drag your mouse, and then click again to stop.

Figure 5-42 Select a period



- Step 7 Enter the password and encryption password, and then click **OK**.



You need to verify your password by default before downloading. You can configure whether to verify the password. For details, see "7.4.1 Configuring Security Parameters".

- Step 8 Configure the parameters of the video, and then click **OK** to start downloading.



The video will be downloaded to the default path configured in the local settings. For details, see "8.4.5 Configure File Storage Settings".

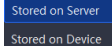
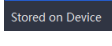
Table 5-10 Parameter description

Parameter	Description
Start Time	The start and end time represents the length of video you selected. You can adjust it more specifically here.
End Time	
Transcode	The format is .dav by default. Other formats include .avi, .mp4, and .asf.
File Format	
Storage Path	Configure the storage path for the recordings. Click  to edit the name of the recording file and select the local storage path.
Privacy Masking	If disabled, faces in the video will not be blurred.  Make sure that the device supports the privacy masking function, and the function on the device is enabled.

5.1.3.8 Smart Search

With the smart search function, you can select a zone of interest on the video image to view motion records within this section. The relevant camera is required to support Smart Search; otherwise the search result will be empty.

Procedure

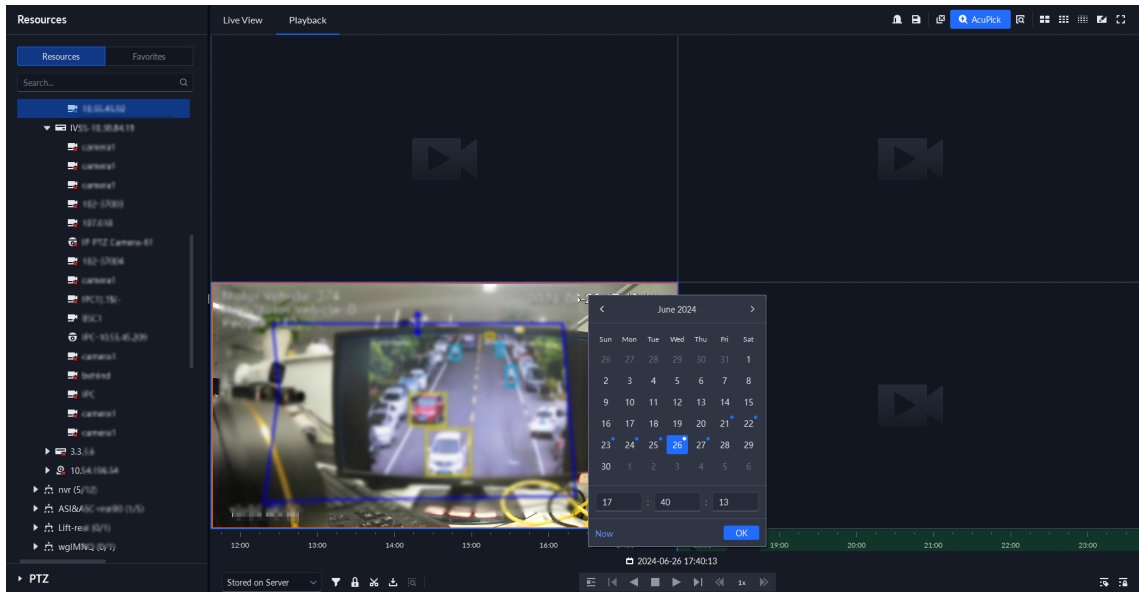
- Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center**.
- Step 2 Click the **Playback** tab.
- Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.
- Step 4 Select the storage path of recorded video from  or , and then click  to select the date.

The search results are displayed.



Dates with blue dot means there are video recordings.

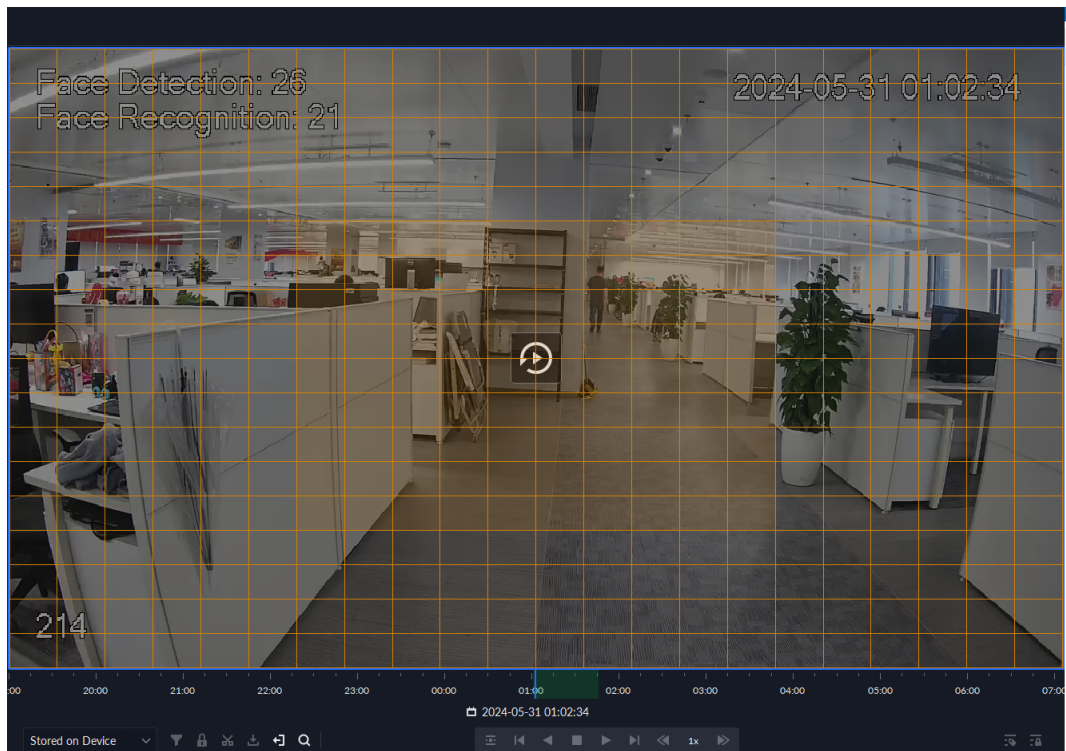
Figure 5-43 Playback page



Step 5 Select a window that has videos, click , and then select a type.

The smart search page is displayed, with 22 × 18 squares in the window.

Figure 5-44 Smart search



Step 6 Click the squares and select detection areas.



- Select a detection area: Point to image, click and drag to select a square.
- For the selected area, click again or select square to cancel it.

Step 7 Click  to start smart search analysis.

- If there are search results, the time progress bar will become purple and display dynamic frame.
- It will prompt that the device does not support smart search if the device you selected does not support the function.



Click  to select the detection area again.

Step 8 Click  button on the image.

- : The system only plays back the retrieved results, which are indicated by purple frames on the timeline bar.
- : Plays back the whole video.

Step 9 Click  to exit smart search.

5.1.4 Map Applications

On the map, you can view real-time videos of devices, locations of channels that trigger alarms, cancel alarms, and more.

Prerequisites

Make sure that you have configured a map. For details, see "4.2 Configuring Map".

Procedure

Step 1 Log in to the DSS Client, and on the **Home** page, select  > **Monitoring Center** > **Map**.

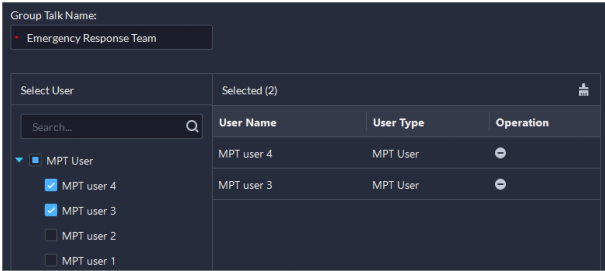
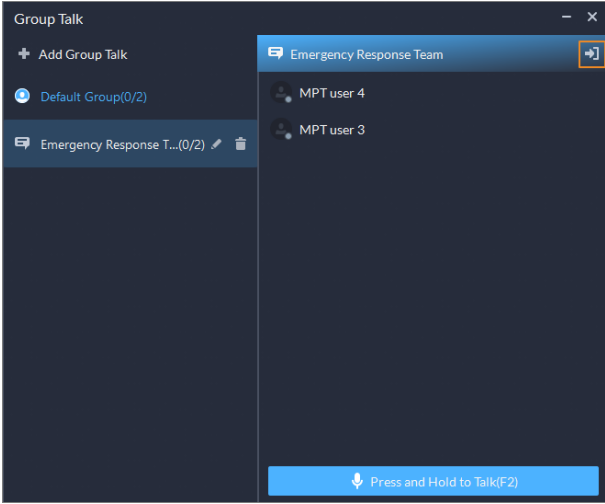
Step 2 In the list of maps, click a map.

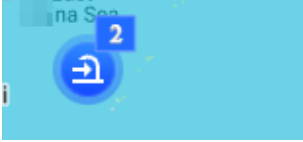
Step 3 View video, cancel alarms, and more.



The functions vary with the types of maps and devices. Slight differences might be found in the actual page.

Table 5-11 Function description

Function	Description
Group talk	You can engage in a group talk with MPT users. Only administrators are allowed to use the group talk function. - Click next to the list of maps. The default group includes all MPT users. - Click Add Group Talk. - Enter a name for the group, select MPT users, and then click OK. Only MPT users are displayed. For how to configure an MPT user, see "3.2.2 Adding a User".  - Click the new group, and then click on the upper-right corner to join the group. indicates the group that you are in.  (Optional) Click and you can edit the users in the group. The users removed from the group will return to Default Group. - Press the F2 key to talk to the users in the group, and then release the key to stop talking. You can only talk to and hear the MPT users in the current group. If you want to talk to and hear other users, you must click on the upper-right corner to join that group.

Function	Description
Zoom in and out on the map	Rotate the wheel or click  and  to zoom in and out on the map. Select Display Settings > Point Clustering, and then when you zoom out on the map, the same type of devices or channels will be merged together if they are near each other. 
Satellite map	Select Display Settings > Satellite Map, and then if you are using an online map, you can view its satellite map.  This function is only available on GIS maps.
Hide device name	Select Display Settings > Hide Device Name, and then only displays the icons of devices or channels.
View device details	Click a device on the map, and then click  to view device name and organization; Click the icon again to hide the name and organization.
View live video	- View live videos in batches: Click Rectangle, select devices on the map, and then click . - View the live video of a device: Click a device on the map, and then click .  PTZ control and presets are supported when viewing the live video. Make sure that the device supports the PTZ function.
Playback	- View videos in batches: Click Rectangle, select devices on the map, select the time and storage type (either device or central recordings can be selected), and then click . - View the video of a device: Click a device on the map, select the time and storage type (either device or central recordings can be selected), and then click .  Drag the timeline to quickly locate the recorded video at the corresponding time and play it.
View alarms	Click  to view all alarms that are triggered. Click an alarm and the map will zoom in to the location of the device that triggered the alarm. Alarms will be automatically canceled after 30 seconds.

Function	Description
Cancel alarms	Click a device on the map, and then select . The alarm will also be automatically canceled after 30 seconds.
Monitor a radar	• The alarm area and detection area are displayed on the map by default. If a target is detected, its real-time location will be displayed in these areas. • Click a radar channel, you can view its information and use the following functions: ◇ : View the raster map on the radar. You can use this function to check if the maps on the radar and the platform are consistent. ◇ : View the real-time videos of the linked PTZ cameras. ◇ : Search for and view recordings of the linked PTZ cameras. ◇ : View the real-time videos of the channels bound to the radar. You can use this function to monitor the area around the radar. ◇ : If the alarm area and detection area of the radar are keeping you from operating other channels, you can click this icon to hide these areas.
Show devices	Click Show Device, and then select the types of devices and channels that you want to display on the map.  You can click an alarm output channel to control whether it will output alarm signals.
Visual range	• For devices that do not support sending the visual range to the platform, after you configure static visual range from  > Map, you can view the monitoring area of the device on the map. • If a device supports visual range, click Dynamic Visual Range, and then double-click a device on the map to show its monitoring area.  ◇ For devices that support dynamic visible range (for example, PTZ camera), if static visible range is configured at the same time, refer to the static visible range. ◇ This function is only available on GIS maps.
Initial angle	If a device supports initial angle, click Initial Angle and double-click a device on the map to show the initial angle.  This function is only available on GIS maps.
Measure distance	Select Box > Length, connect 2 points with a line on the map (double-click to finish drawing), and then the distance between the points is shown.  This function is only available on GIS maps.

Function	Description
Measure area	Select Box > Area, select a region on the map (double-click to finish drawing), and then the area is measured.  This function is only available on GIS maps.
Clear	To clear all markings on the map, click Clear .
Add marks	Select Box > Add Mark , and then mark information on the map.
Reset	Select Box > Reset to restore the map to its initial position and zoom level.
Sub maps	Click  to view the information of the sub map.
	Double-click  , and then the platform will go to the sub map, where you can view the resources on it.

5.1.5 Video Wall

A video wall, which consists of multiple video screens, is used for displaying videos on the wall, instead of small PC displays.

Complete video wall settings before you can view videos on the wall.

5.1.5.1 Configuring Video Wall

5.1.5.1.1 Page Description

Before using the video wall function, you should get familiar with what you can do on the video wall page.

Figure 5-45 Video wall

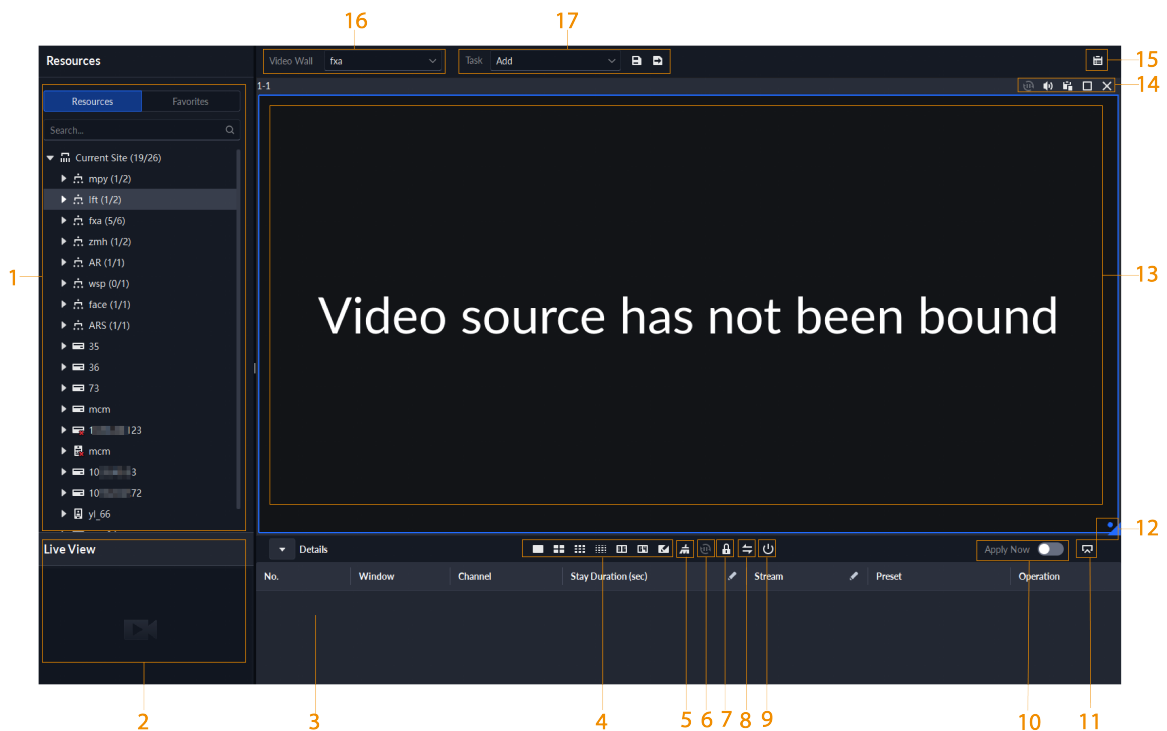


Table 5-12 Page description

No.	Function	Description
1	Device tree	If you have selected Device and Channel in Local Settings > General, the device tree will display all devices and their channels. Otherwise, it will only display all channels. Click  to view channels that you have saved to favorites. You can enter keywords in  to search for the channels you want.
2	Live view	View live videos from channels.

No.	Function	Description
3	Detailed information	View the channel information in a screen of the video wall. - Click  and view the live video of the channel in Live View on the lower-left corner. This can be helpful when you need to make sure whether it is the channel you want. - Click  to adjust the order of channels. - Click  to delete the channel from the screen. - Click Stay Duration (sec) or  to define for how long the live video of the channel will be displayed during each tour. - Click Stream or  to change the video stream of the channel.
4	Window split	Select how you want the window to split.
5	Clear screen	Clear all the screens.
6	Stopping or starting all tours	Stop or start all tours.
7	Lock window	If multiple screens in a video wall are configured to be a combined screen, then you can perform video roaming on the window that has been locked.
8	Display mode	Displays the real-time video, or a snapshot of the real-time video every 10 minutes of the bound channel in the screen. If nothing happens after operation, you can just click another screen, then click the screen you want, and then it should work properly.
9	Turning on or off screens	Turn on or off the screens configured for the currently selected video wall.
10	Decoding to wall immediately after configuration	When a task has been configured, the platform will immediately decode channels to the video wall.
11	Decoding to wall	Manually decode channels to the video wall.
12	Video wall layout	Click to view the layout of the current video wall.
13	Video wall display area	The display area for video walls.
14	Screen operations	Includes stopping tour for the screen, muting, pasting, maximizing or restoring the screen, and closing the screen.
15	Video wall plan	Configure a timed or tour plan for the video wall.
16	Video wall selection	Select the video wall you want to configure.
17	Display task management	Add, save, and delete tasks.

5.1.5.1.2 Preparations

To display video on the wall, make sure that:

- Cameras, decoders and video wall are well deployed. For details, see the corresponding user manuals.
- Basic configurations of the platform have been finished. For details, see "3 Basic Configurations". During configuration, make sure that:
 - ◇ When adding a camera, select **Encoder** from **Device Category**.
 - ◇ When adding a decoder, select **Video Wall Control** from **Device Category**.

5.1.5.1.3 Adding Video Wall

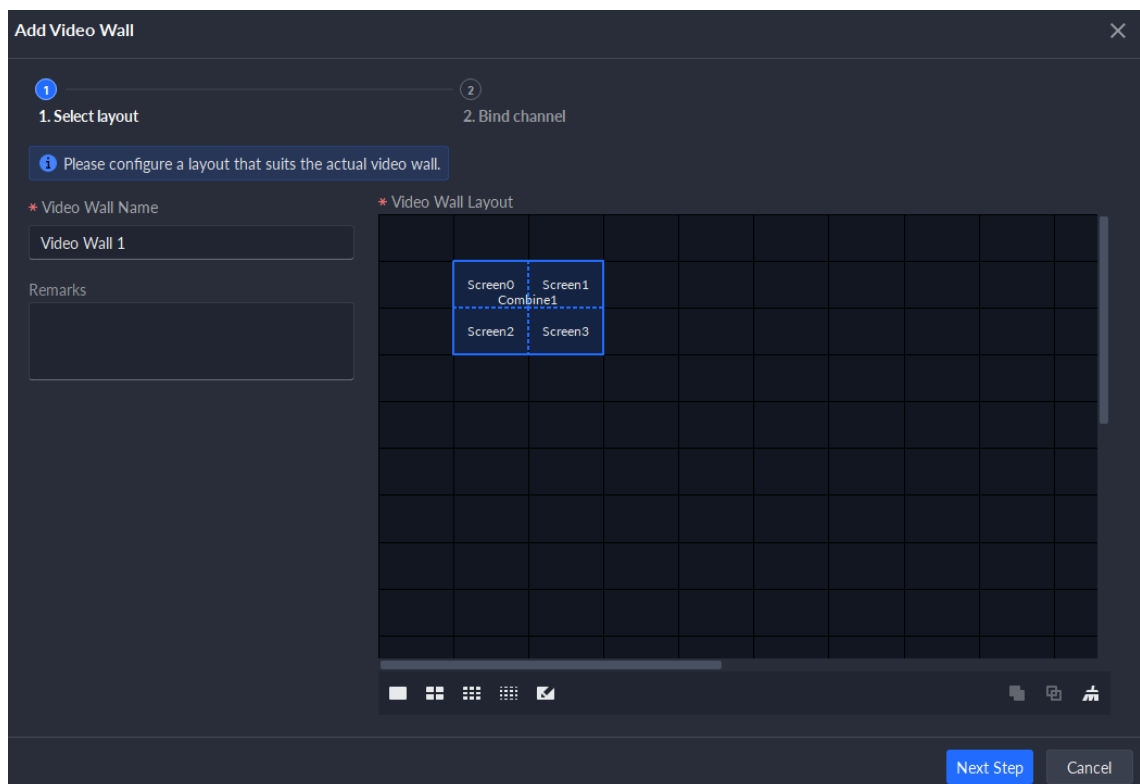
Add a video wall layout on the platform.

Step 1 Log in to the DSS Client, and on the **Home** page, select **Monitoring Center** > **Video Wall**.

Step 2 From the **Video Wall** drop-down list, select **Add Video Wall**.

Step 3 Enter video wall name, and then select a window splicing mode.

Figure 5-46 Add a video wall



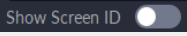
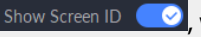
- The video wall name cannot consist of special characters including < > % & = " ' and /.
- Select a splicing mode from among 1 × 1, 2 × 2, 3 × 3, 4 × 4 or set a custom mode by clicking .
- A multi-screen splicing mode is a combined screen by default. You can perform video roaming on it. For example, with a 2×2 combined screen, if you close 3 of them, the other one will be spread out on the combined screen. To cancel combination, click the combined screen, and then click .

- To create a combined screen, press and hold Ctrl, select multiple screens, and then click .
- To clear the created screen, click .

Step 4 Click **Next Step**.

Step 5 Select the encoders which need to be bound in the device tree, and drag it to the corresponding screen.



- You can set whether to show ID in the screen,  means that the screen ID is disabled; click the icon and it becomes , which means that screen ID is enabled.
- Each screen in a combined screen must be bound with a decoding channel.

Step 6 Click **Finish**.

5.1.5.1.4 Configuring Video Wall Display Tasks

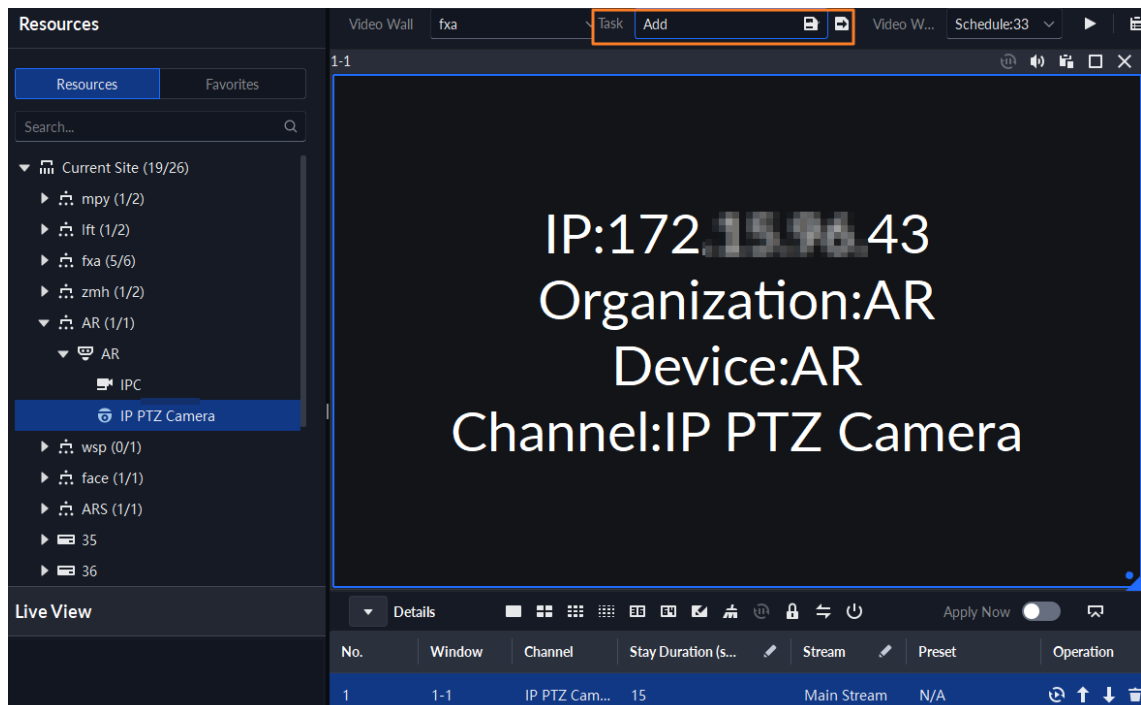
Displays videos on the wall manually or in accordance with the pre-defined configuration.

Procedure

Step 1 Log in to the DSS Client, and on the **Home** page, select **Monitoring Center** > **Video Wall**.

Step 2 In the **Task** drop-down list, select **Add**.

Figure 5-47 Add a video wall task



Step 3 From the device tree, select a camera, and then drag it to a screen, or select a window, drag the camera to the **Details** section.

If you do not close video wall display in advance, this action will delete the bound camera and play the selected camera on the wall.

Step 4 Click .



If you have selected an existing task in the **Task** drop-down list, after dragging the video channel to the window, click  to save it as a new task, which will be played on the wall immediately.

Step 5 Name the task, and then click **OK**.

- During video wall display of a task, if you have rebound the video channel, click  to start video wall display manual.
- During video wall display, click  or  to stop or start tour display.

Step 6 Click  to start video wall display.

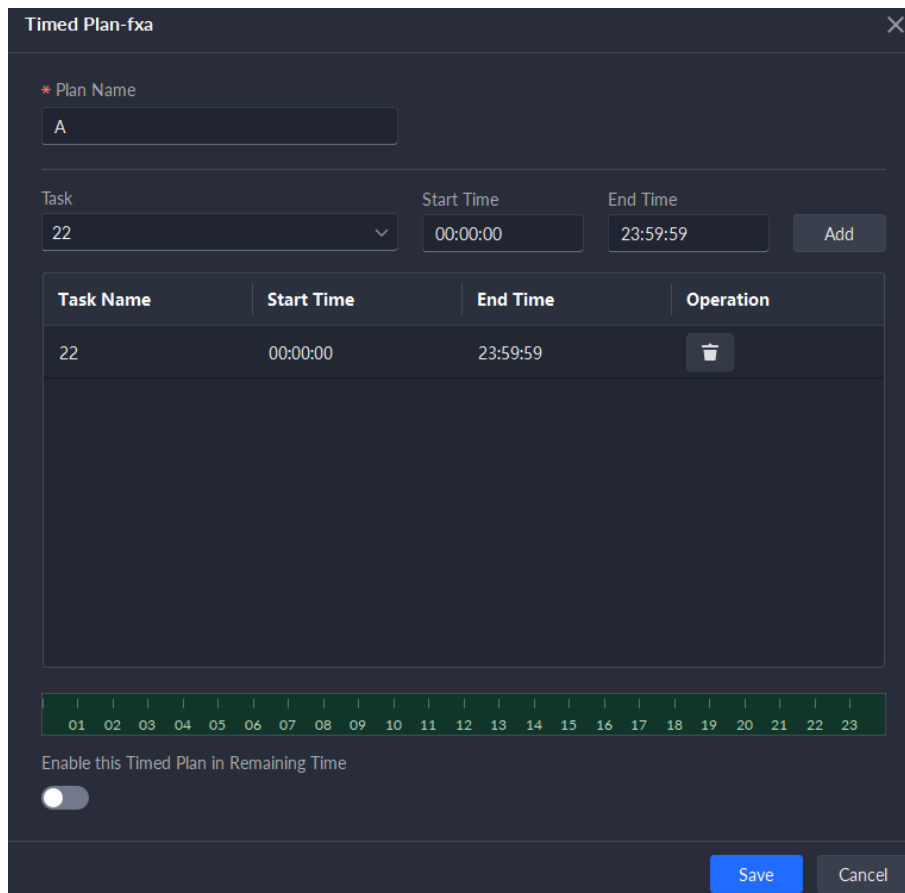
5.1.5.1.5 Configuring Timed Plans

Step 1 Log in to the DSS Client, and on the **Home** page, select **Monitoring Center** > **Video Wall**.

Step 2 Click  on the upper-right corner.

Step 3 Hover over , and then select **Timed**.

Figure 5-48 Set timed plan



Timed Plan-fxa

* Plan Name
A

Task: 22 Start Time: 00:00:00 End Time: 23:59:59 Add

Task Name	Start Time	End Time	Operation
22	00:00:00	23:59:59	

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23

Enable this Timed Plan in Remaining Time ☐

Save Cancel

Step 4 Enter the plan name.

Step 5 Select a video task, set start time and end time, and then click **Add**.

Repeat this step to add more tasks. The start time and the end time of tasks cannot be repeated.



Select the **Enable This Timed Plan in Remaining Time** check box, and then set the task. The video wall displays the selected task during the remaining period.

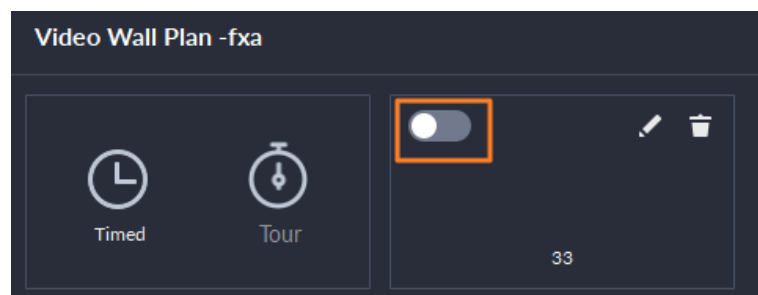
Step 6 Click **Save**.

Step 7 Click  to start the plan.



You cannot display multiple plans on the wall at the same time. When a plan is enabled, the previous plan on the wall is automatically terminated.

Figure 5-49 Enable timed plan



5.1.5.1.6 Configuring Tour Plans

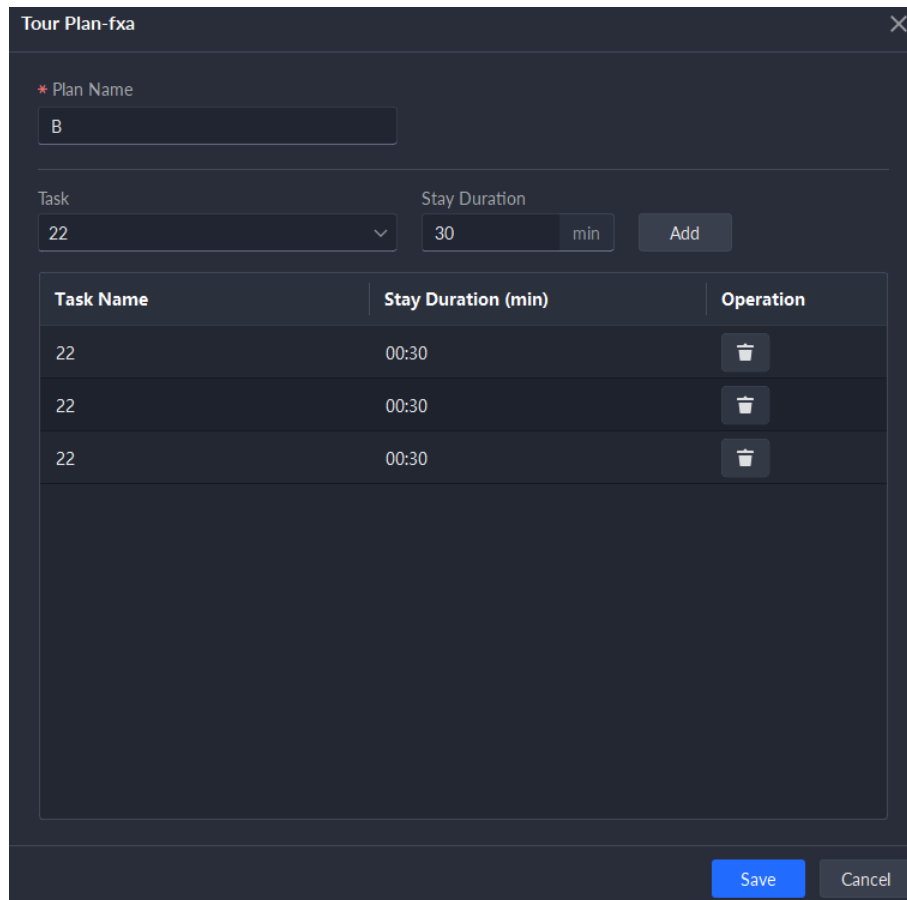
After setting video wall tasks, you can configure the sequence and interval of tasks so that they can automatically play in turn on the wall.

Step 1 Log in to the DSS Client, and on the **Home** page, select **Monitoring Center** > **Video Wall**.

Step 2 Click  on the upper-right corner.

Step 3 Hover over , and then select **Tour**.

Figure 5-50 Tour plan



Tour Plan-fxa

* Plan Name
B

Task: 22 Stay Duration: 30 min Add

Task Name	Stay Duration (min)	Operation
22	00:30	
22	00:30	
22	00:30	

Save Cancel

Step 4 Enter task name, select a video task and then set stay time. Click **Add**.

Repeat this step to add more tasks.

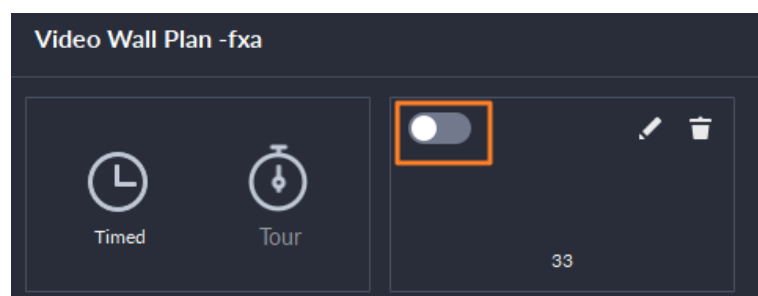
Step 5 Click **Save**.

Step 6 Click  to start the tour plan.



You cannot display multiple plans on the wall at the same time. When a plan is enabled, the previous plan on the wall is automatically terminated.

Figure 5-51 Enable tour plan



Video Wall Plan -fxa

Timed Tour

33

5.1.5.2 Video Wall Applications

Before using the video wall function, make sure that display devices are properly connected to video wall screens.

5.1.5.2.1 Instant Display

Drag a camera to the video wall screen for instant display on the wall.

The video wall display task is configured. For details, see "5.1.5.1.4 Configuring Video Wall Display Tasks".

Procedure

Step 1 Log in to the DSS Client, and on the **Home** page, select **Monitoring Center** > **Video Wall**.

Step 2 In the **Video Wall** drop-down list, select a video wall.

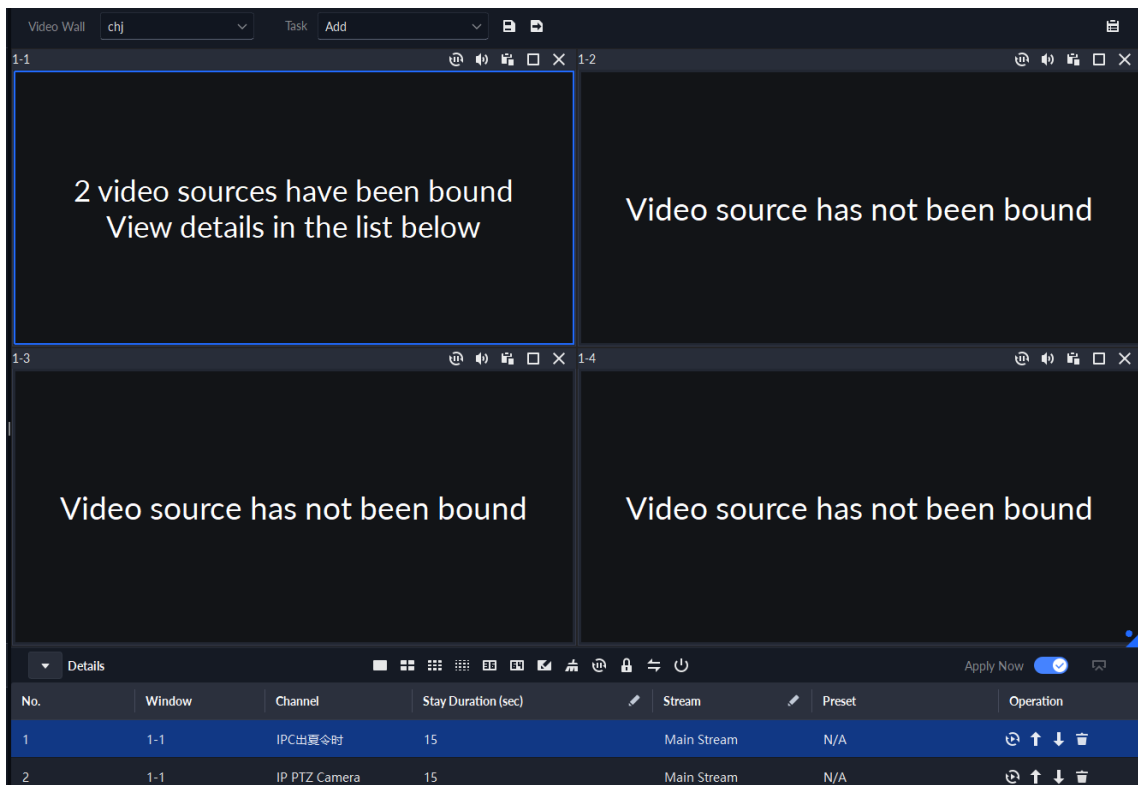
Step 3 Click  to start video wall display.

Step 4 Drag a camera from the device tree to a screen, or select a window and drag the camera to the **Details** section.



- A window can be bound to multiple video channels.
- The binding mode, which includes **Tour**, **Tile**, and **Ask Every Time**, can be set in **Local Settings** > **Video Wall**. For details, see "8.4.3 Configuring Video Wall Settings".
- For a fisheye camera, right-click it to select the installation mode for fisheye dewarping.

Figure 5-52 Bind video channel



Step 5 Select a screen, and then click **Details** to view detailed information about the screen and channel, including stream type, preset and display sequence.

- Click  to view live video of the current channel on the lower left.
- Click  to adjust sequence.
- Click  to delete the video channel on the current window.

5.1.5.2.2 Video Wall Task Display

Displays a pre-defined task on video wall.

Step 1 Log in to the DSS Client, and on the **Home** page, select **Tools** > **Video Wall**.

Step 2 In the **Task** drop-down list, select a task.

Step 3 Operations available.

- After changing the video channel that is being displayed, click  at the lower-right corner before you can see the effect on video wall.
- Click   to pause or stop.
- Select a screen, and then click **Details** to view detailed information about the screen and channel, including stream type, preset and display sequence.

5.1.5.2.3 Video Wall Plan Display

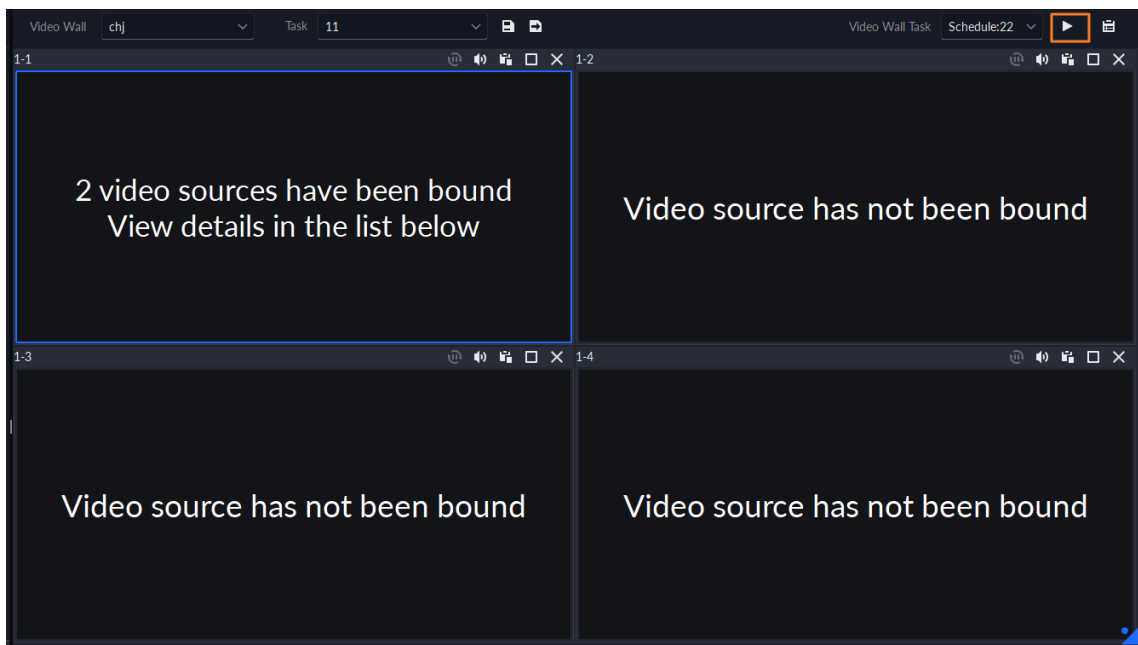
Display a pre-defined plan on video wall.



Make sure that there are pre-defined plans.

The video wall automatically works as the plans have been configured. To stop the current plan, click  on the upper-right corner of the **Video Wall** page, and then it changes to . Click  to start displaying video on wall again.

Figure 5-53 Display video wall plan



5.1.6 AR

5.1.6.1 AR Homepage

Step 1 Log in to the DSS Client, and then on the **Home** page, select  > **Monitoring Center** > **AR**.

Step 2 Click  at the upper-right corner to show the device tree, and then you can double-click the channel to view the live video.



The device tree only displays channels configured with AR feature. For details, see "3.1.2.5.2 Modifying Device Information".

Figure 5-54 AR homepage



Table 5-13 Description of AR homepage

No.	Function	Description
1	Device tree	Click  to show the device tree; click it again to hide the tree. You can double-click the channels in the device tree to open the live video of the channels.
2	AR system name	You can configure the name from  > AR > System Name Config .
3	Tag	The added tags are displayed on the video image. - Click the tag to view the tag details. - Point to the tag, and then you can add the tag to favorite, edit and delete the tag, and make the tag stop flashing when an alarm is triggered.
4	-	Minimize, maximize and close the AR client.

No.	Function	Description
5	Show/hide function menu	Click  to show the function menu; click it again to hide it. ● Add Tag : Supports adding calibration point tag, area tag, vector tag, and direction tag. ● Tags : Supports filtering and searching tags, and adding tags to favorite. ● Filter Layer : Supports filtering tags by all, favorite and important tags, and by tag type. ● Setting : Configure target tracking, AI overlay, smart rectangular selection, and real-time alarm. For details, see "5.1.6.4 Setting".
6	Device video image	Click  to view the PTZ control window of speed dome. You can adjust directions of, zoom, and focus the speed dome.

5.1.6.2 Tag Management

5.1.6.2.1 Adding Tags

You can add tags based on the created tag template to mark the targets on the monitoring screen. The tags can help you classify monitoring targets such as hospital and road junctions to quickly find and manage the monitoring targets. The tags are related to the devices installed at high points. The tags are marked to the device and can be seen by any user with permissions to the selected device.

Prerequisites

Configure the tag template. For details, see "4.12.2 Configuring Tag Template".

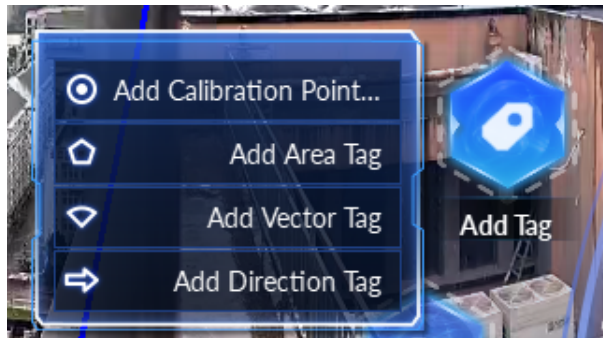
Procedure

Step 1 On the AR homepage, click **Add Tag**.

You can add calibration point tag, area tag, vector tag, and direction tag. Here uses **Add Calibration Point Tag** as an example.

- Calibration point tag: Mark the target as a point. For example, a fire hydrant.
- Area tag: Mark the target as an area by using the polygon. For example, such as a building.
- Vector tag: Mark the target by sector.
- Direction tag: The tag is in an arrow shape which shows the direction. For example, the direction of people flow.

Figure 5-55 Add tags



Step 2 Click **Add Calibration Point Tag**, and a dot appears. Select the location to add tags and then click on this place.



Press Esc or right-click to exit the operation.

Figure 5-56 Set tag parameters

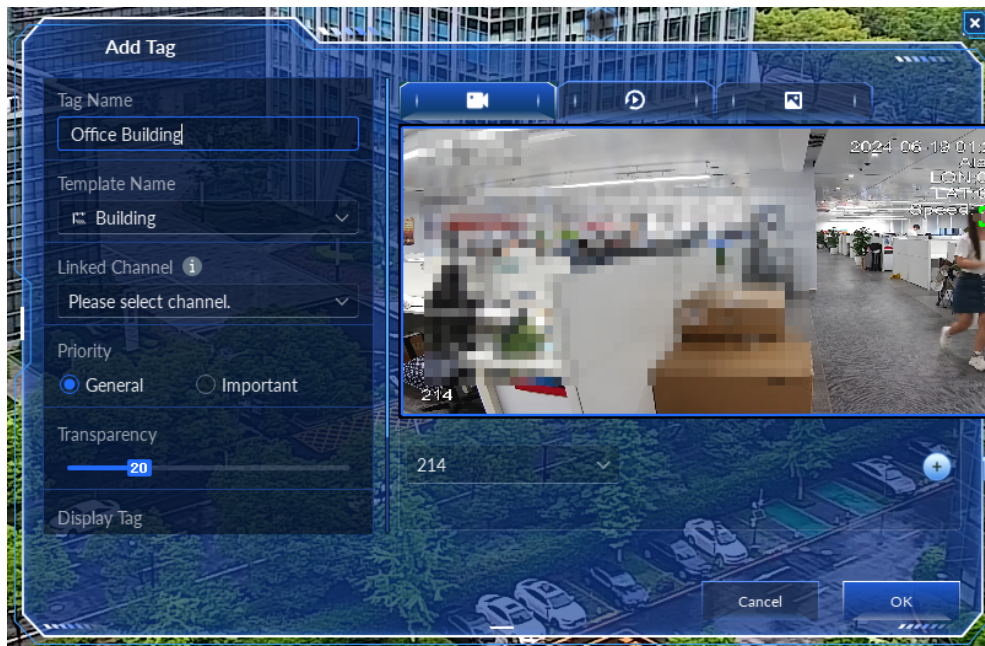


Table 5-14 Description of tag parameter

Parameter	Description
Tag Name	The name that identifies the tag.

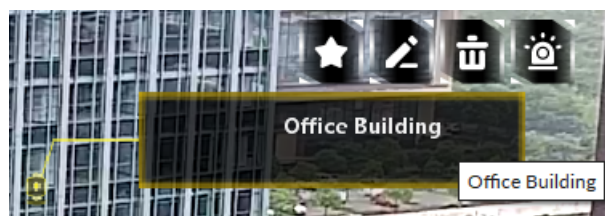
Parameter	Description
Template Name	After selecting a tag template, the icons of elements defined in the template appear will on the right side. • Live video: . • Recorded video: . • Image: . Click an icon, and then click , you can select channels (5 at most) to view live video or video recordings (double-click the video image to zoom in the video; double-click again to restore), or upload images (5 at most).
Linked Channel	Select the channels that the tag needs to be associated with. Up to 16 channels can be selected.  You need to select Linked Channel when configuring the tag template from  > AR > Template Config.
Priority	When you set Priority to Important , the tag will be displayed in the Important Tags list in Tags .
Transparency	Drag the slider to adjust the transparency of the tag.
Display Tag	Select whether to display the name and connection line of the tag on the video image.
Remark	Add remarks on the tag.  You need to select Remark when configuring the tag template from  > AR > Template Config.

Step 3 Click **OK**.

Related Operations

- Click a tag to view its details.
- Point to the tag, and then you can:

Figure 5-57 Tag



- ◇ Click  to add the tag to favorite, and then the tag will be displayed in **Tags** > **Favorite Tags**.

Also, select **Filter Layer** > **Favorite Tags**, the tag added to the favorite will show.

- ◇ Click  to edit the tag.
- ◇ Click  to delete the tag.

- ◇ Click , and then the tag stops flashing when an alarm is triggered.

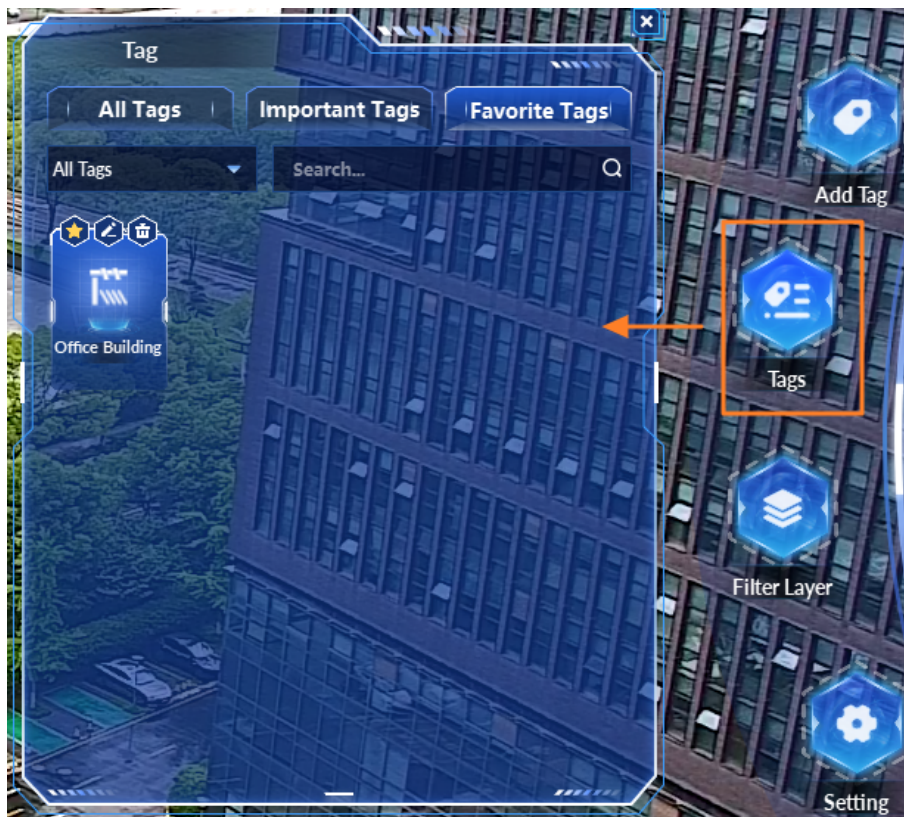


If you want the tag to flash when an alarm is triggered, you need to go to the AR homepage, select **Setting**, and then select **Linked Tag** in the **Real-time Alarm** section.

5.1.6.2 Viewing Tags

- Step 1 On the AR homepage, click **Tags**.
- Step 2 Click **All Tags**, **Important Tags** or **Favorite Tags** to view all and important tags, and tags added to favorite respectively.

Figure 5-58 View tags



- Step 3 (Optional) Click the tag, and then click  in turns to add/cancel adding the tag to favorite, edit, and delete the tag.

5.1.6.3 Filtering Layer

Supports filtering tags by all and important tags and tags added to the favorite. You can also filter the tags by type, which includes video, building, parking lot, airport plate, post office, hospital, bank and station.

On the AR homepage, click **Filter Layer**.

Figure 5-59 Filter layer



- **Display Name** is enabled by default. Click  to disable it.
- Click **All Tags**, **Favorite Tags**, or **Important Tags**, tags of the corresponding type and the number of tags (for example ) are displayed.



The light color (for example, ) means displaying the tag, and the dark color (for example,



) means not displaying the tag.



Supports filtering tags by combining all, favorite and important tags.

5.1.6.4 Setting

You can enable or disable auto target tracking, AI overlay, smart rectangular selection, and real-time alarm.

Step 1 On the AR homepage, click **Setting**.

Step 2 Configure the parameters.

- **Auto Tracking** : The panoramic + PTZ camera will track the target according to the rules configured on the webpage of the camera.
- **AI Rule** : The smart rules defined on the webpage of the panoramic + PTZ camera will show on the AR page.
- **Bounding Box** : The smart bounding box will show on the AR page.
- **Vehicle Statistics** : After enabling it, draw a rectangle on the AR page to select an area, the platform shows the real-time statistics of vehicles in the selected area.
- **Linked Tag** : The tag flashes 15 seconds when the channel associated with the tag triggers an alarm.

You can make the tag to stop flashing in advance by pointing to the tag, and then

clicking .

Figure 5-60 Setting



Step 3 Click **OK**.

5.2 Event Center

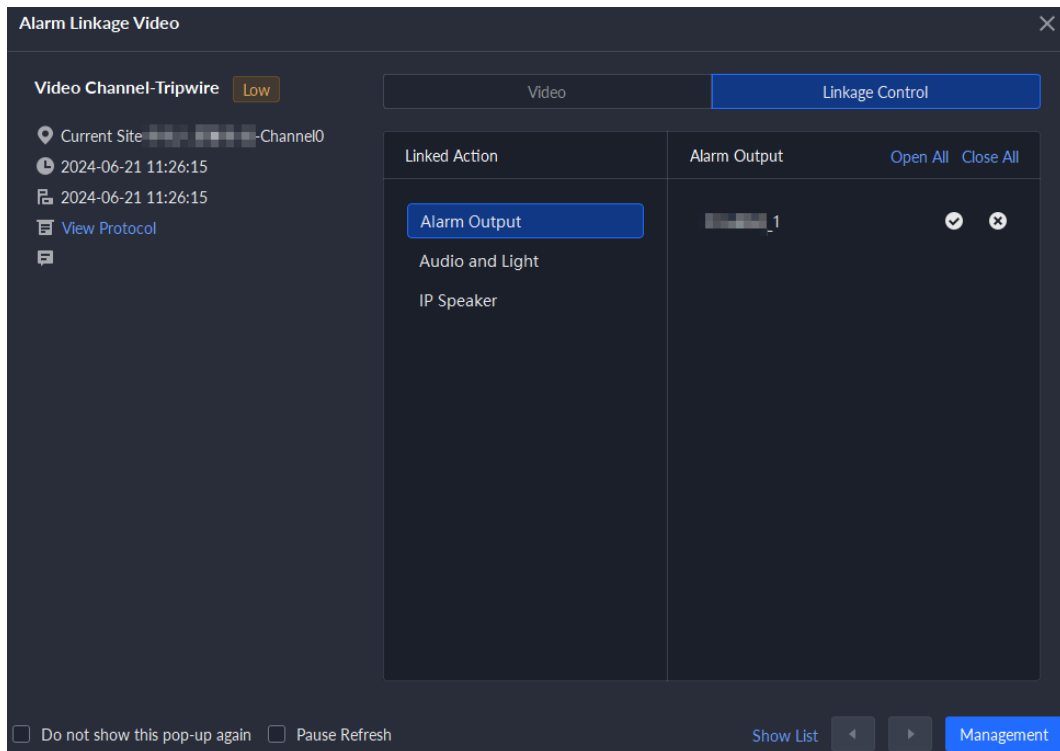
When alarms are triggered, you will receive notifications on real-time alarms.

You can view their details, such as snapshots and recordings, and process them.

If you miss alarms occurred during a certain period, or want to check certain alarms, such as high priority alarms occurred in the past day or all alarms that have not been processed in the past week, you can set the search conditions accordingly and search for these alarms.

Based on all the alarms that were triggered, the platform will generate statistics ready for your review. This can be helpful for how you can optimize your security measures.

Figure 5-62 Alarm pop-up



Step 3 Click  to claim an alarm.

After an alarm has been claimed, the username of your account will be displayed under the **Processed by** column.

Step 4 Process alarms.



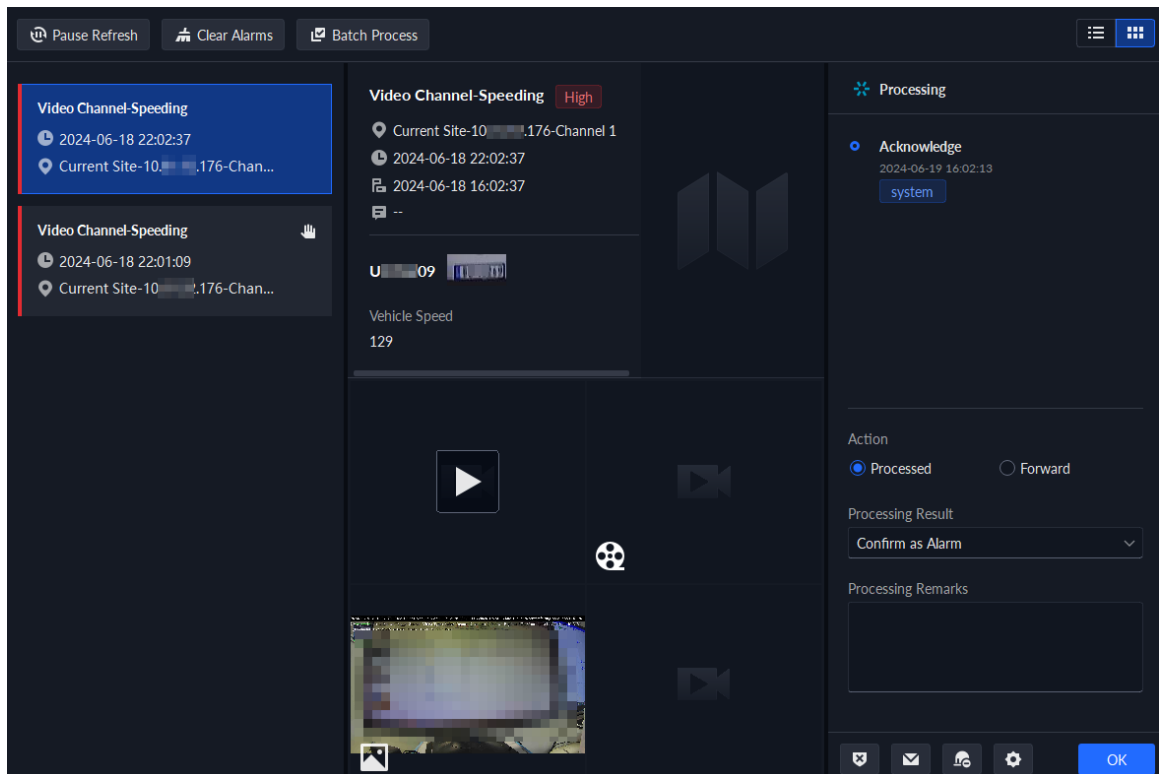
You can use the up and down arrow keys on the keyboard to quickly select other alarms.

1. Click  or double-click the alarm to view the claimed alarm.



Alarms related to vehicles also display vehicle information such as plate number, speed, and more.

Figure 5-63 Alarm details



2. The middle area displays the time when the alarm was triggered, name and location of the alarm source, alarm type, and the live video images of linked channels, alarm videos, and alarm snapshots.

Double-click a window to view them in larger size. Click  to go back.

3. On the right side, select how to process the alarm, enter some comments, and then click **OK**.

Forward allows you to forward the alarm to another user who will process it.

4. (Optional) Click  to disarm the alarm. You can disarm for a period, or disarm until the defined time.

After disarming, all users will not receive this alarm within the defined time; and after the defined time, if the alarm is not eliminated, it will continue to alarm.

5. (Optional) Click  to send the alarm information to other users as an email. Events that are processed or forwarded can also be sent as emails.
6. Click  and configure the parameters related to the processing comments, and then click **OK**.

- **Require Processing Remarks to be Entered** : After enabled, users must enter some content in the processing comments to successfully process alarms.
- **Pre-processing Remarks** : Configure the predefined comments for each processing status. The content will be automatically filled in when users select different status for alarms.

Related Operations

- The platform also supports processing alarms in batches. Click **Batch Process**, select multiple alarms, and then you can process them in batches.
- When viewing the recorded videos, you can select a target manually or select one automatically recognized by AcuPick, and then search for it in DeepXplore.

5.2.2 History Alarms

Search for and process history alarms.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Event Center**.

Step 2 Click **Event History**.

Step 3 Set search conditions, and then click **Search**.



In the **Processing Remarks** section, you can search for events by entering remarks that are defined when processing or forwarding the event.

Figure 5-64 History alarms

Resources

Sites

Current Site

Time

06/21 00:00:00 ~ 06/21 23:59:59

Source Type

All

Priority

All

Processed by

All

Alarm Status

All

Processing Remarks

Search

Reset

Event History

Export

Batch Process

No.	Alarm TL...	Site Name	Alarm Cate...	Alarm Type	Alarm Source	Priority	Remarks	Processed by	Alarm Status	Oper...	
1	2024-06-21 ...	Current Site	Soft Trigger	Soft Trigger_1	AR-IP PTZ C...	High	--	--	Not Processed		
2	2024-06-21 ...	Current Site	Video Chan...	Tripwire		Low	...	system	Processing		
3	2024-06-21 ...	Current Site	Soft Trigger	Soft Trigger_1	AR-IP PTZ C...	High	--	system	Processing		
4	2024-06-21 ...	Current Site	Video Chan...	Tripwire		Low	...	--	Not Processed		
5	2024-06-21 ...	Current Site	Soft Trigger	Soft Trigger_1		High	--	--	Not Processed		
6	2024-06-21 ...	Current Site	Video Chan...	Tripwire		Low	...	--	Not Processed		
7	2024-06-21 ...	Current Site	Soft Trigger	Soft Trigger_1		High	--	--	Not Processed		
8	2024-06-21 ...	Current Site	Soft Trigger	Soft Trigger_1		High	--	--	Not Processed		
9	2024-06-21 ...	Current Site	Soft Trigger	Soft Trigger_1		High	--	--	Not Processed		
10	2024-06-21 ...	Current Site	Soft Trigger	Soft Trigger_1		High	--	--	Not Processed		
11	2024-06-21 ...	Current Site	Soft Trigger	Soft Trigger_1		High	--	--	Not Processed		
12	2024-06-21 ...	Current Site	Soft Trigger	Soft Trigger_1		High	--	--	Not Processed		

Step 4 Claim and process alarms. For details, see "5.2.1 Real-Time Event".



You can use the up and down arrow keys on the keyboard to quickly select other alarms.

Related Operations

When viewing the recorded videos and snapshots, you can select a target manually or select one automatically recognized by AcuPick, and then search for it in DeepXplore.

5.2.3 Event Statistics

With alarms being triggered and processed, statistics are generated to give you a clear picture of what is happening in your area, such as the number of alarms that were processed, and the type of alarms that are triggered most frequently.

Log in to the DSS Client. On the **Home** page, click , and then select **Event Center** > **Event Statistics**.

Figure 5-65 Alarm overview



Table 5-15 Alarm overview description

No.	Parameter	Description
1	Search conditions and export records	- To view real-time alarm overview, click Real Time, select a site (if any), an organization, and refresh frequency. - To view daily alarm overview, click Daily, configure the time, select a site, an organization, and then click Search. - To view weekly alarm overview, click Weekly, configure the time, select a site, an organization, and then click Search. - To view monthly alarm overview, click Monthly, configure the time, select a site, an organization, and then click Search. If the time zone of the server is not the same as the DSS client, statistics will be generated based on the time zone of the server. For example, daily statistics will be generated from 00:00 to 24:00 based on the time zone of the server. - Export: Export the page of the current search results to local.
2	Alarm Overview	Statistics is generated based on the alarms that the current user has access to. The number and proportion of alarm events that are pending, processed, or not processed are displayed. The data will only refresh in real-time when you are viewing daily statistics.
3	Alarm Trend	Displays trend of alarms of all priorities.

No.	Parameter	Description
4	Top 10 Alarm Sources and Alarm Types	Top 10 alarm sources and alarm types that the current user has access to are sorted by the number of alarms. The data will only refresh in real-time when you are viewing daily statistics.  You can click high, medium, or low to not include the number of certain alarms. For example, if you click High, the number of the alarms in this priority will not be counted.

5.2.4 Alarm Controller

You can monitor and manage alarm controllers.

Prerequisites

Alarm controllers are added to the platform. For details, see "3.1.2 Managing Device".

Background Information

- Arm and disarm
 - ◇ Home arm: An arming mode when a user is within the zone of the alarm system. In this mode, zones around the system, such as outdoor perimeter detectors, balcony curtain detectors, are armed, while zones inside the system, typically indoor infrared detectors, are bypassed by the system. People can move in this area without triggering alarms. If there are internal zones within a subsystem, they will be disarmed.
 - ◇ Away arm: An arming mode when all users have left the zones of the alarm system. In this mode, all zones are armed.
 - ◇ Disarm: Cancel arming.
- Bypass

When detectors connected to the alarm controller malfunction or there is movement within specific zones, the normal arming operations within the system will be affected. In this case, the system allows users to bypass these zones.

 - ◇ Unbypass: Restores bypassed zones to the enabled status.
 - ◇ Bypass: The zone is temporarily disabled during the arm, and it automatically returns to the enabled status when the system is disarmed.
 - ◇ Isolate: The zone is permanently disabled. When the system is disarmed and then armed again, the isolated zone remains disabled.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Event Center**.

Step 2 Click **Alarm Controller**.

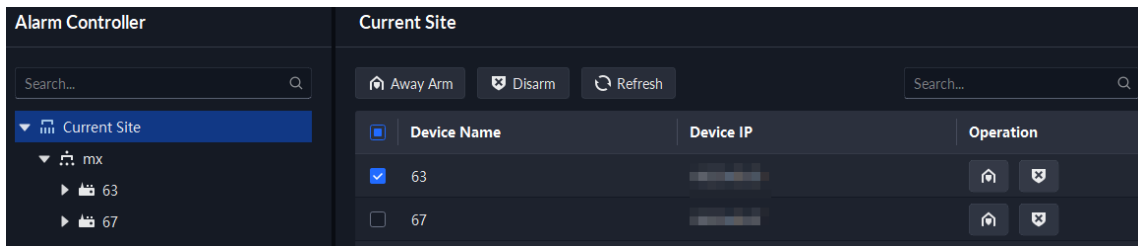
Step 3 In the device tree, click an organization.

All alarm controllers under this organization will be displayed on the right. You can select one or more alarm controllers, and then click  (**Away Arm**) or  (**Disarm**) to arm or disarm the alarm controllers you selected.



If arming failed, you can click **Force Arm** on the prompt window to arm again.

Figure 5-66 Alarm controller organization



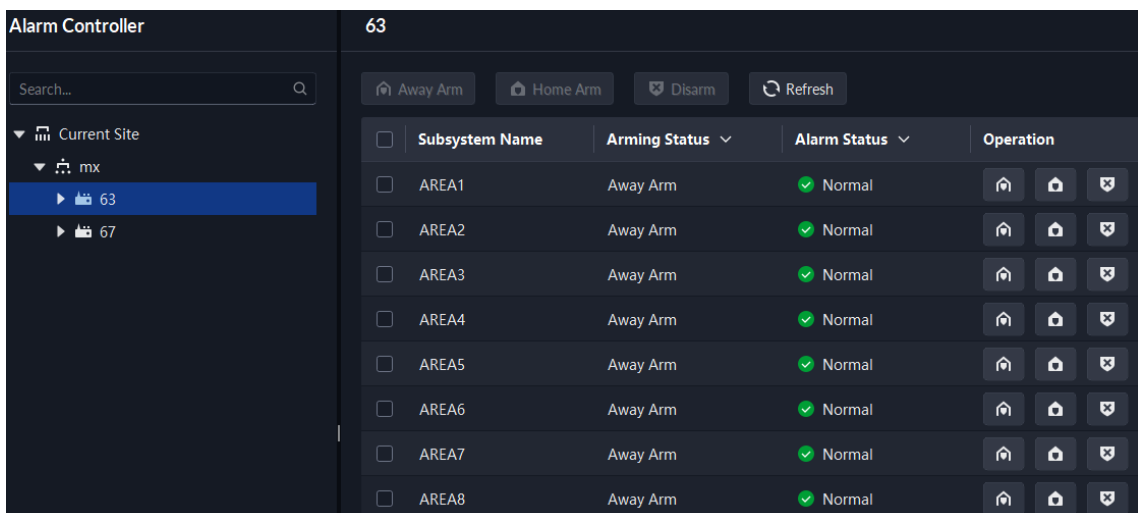
Step 4 In the device tree, click an alarm controller.

All subsystems under this alarm controller will be displayed on the right.



You can right-click an alarm controller, and then click **Update Alarm Controller** to update its information.

Figure 5-67 Subsystems



Step 5 Arm or disarm subsystems.

-   : Operate on multiple subsystems.
-   : Operate on one system.

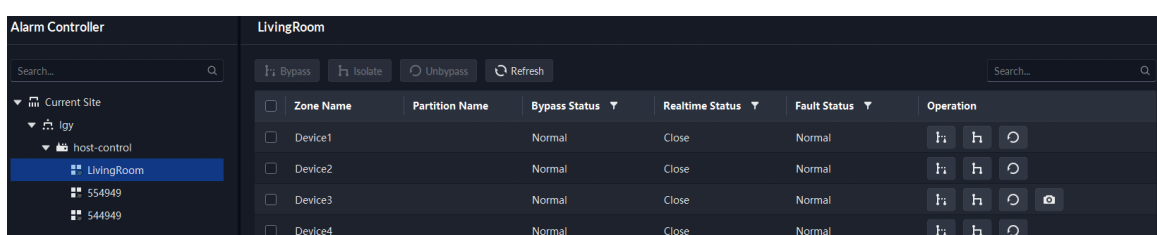


- See the user manual of the alarm controller for detailed description on each function.
- If arming failed, you can click **Force Arm** on the prompt window to arm again.

Step 6 In the device tree, click a subsystem of the alarm controller.

All zones under this subsystem will be displayed on the right.

Figure 5-68 Zone



Step 7 Bypass, isolate, or unbypass zones.

-   : Operate on multiple zones.
-   : Operate on one zone.
-    : Operate on one zone.



- ◇ The snap function () is available only when the alarm controller is online, and PIR camera is connected to the corresponding zone.
- ◇ The snapshot can be downloaded to local in .jpg format.



- See the user manual of the alarm controller for detailed description on each function.
- If arming failed, you can click **Force Arm** on the prompt window to arm again.

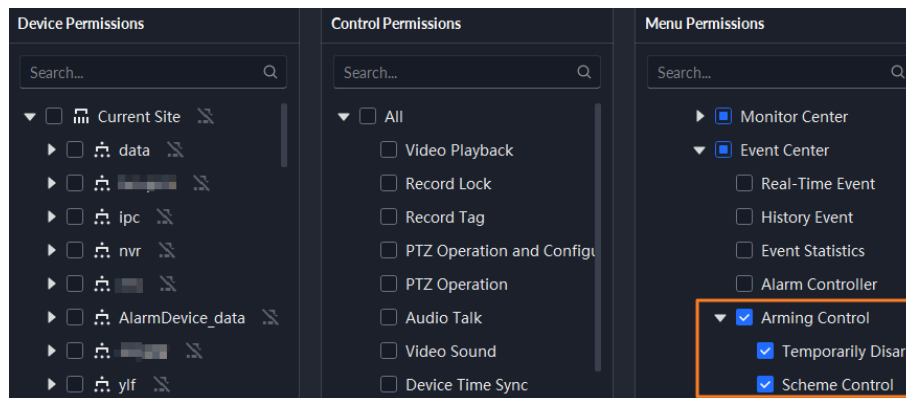
5.2.5 Arming Control

You can edit or cancel temporary disarming on the platform to avoid unnecessary alarms, and enable or disable event schemes to with one click.

Prerequisites

The **Arming Control** menu permission is required. The permission can be configured from  > **User** > **Role Management**.

Figure 5-69 Configure arming control permission



5.2.5.1 Temporary Disarming

You can edit or cancel temporary disarming to avoid unnecessary alarms. For example, if an industrial park holds a celebration activity, it can temporarily disarm the park or some zones as needed.

Prerequisites

You need to configure temporary disarming on the **Real-Time Event** or **Event History** page.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Event Center**.

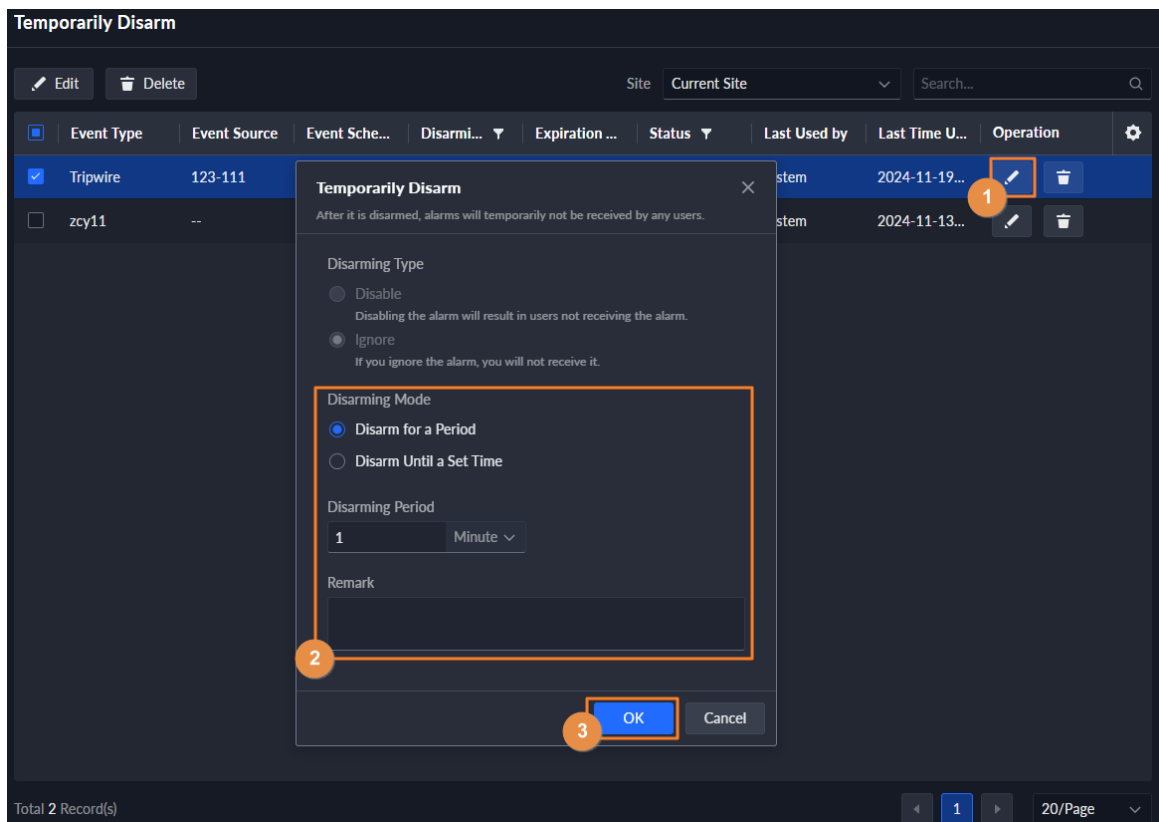
Step 2 Select **Arming Control** > **Temporarily Disarm**, and then click  corresponding to a disarming record to edit the disarming period.



Select several disarming records, and then click **Edit** to edit the disarming periods in batches.

You can set disarming for a period, or disarming until the defined time. After disarming, all users will not receive this alarm within the defined time; and after the defined time, if the alarm is not eliminated, it will continue to alarm.

Figure 5-70 Edit temporary disarming



Step 3 Click **OK**.

Related Operations

Click  corresponding to a disarming record to cancel disarming and delete the record.



Select several disarming records, and then click **Delete** to cancel disarming and delete the records in batches.

5.2.5.2 Scheme Control

The platform provides ease of enabling or disabling event schemes with one click. For example, when a device generates events frequently, you can disable it, so that no such events will be received.

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Event Center**.

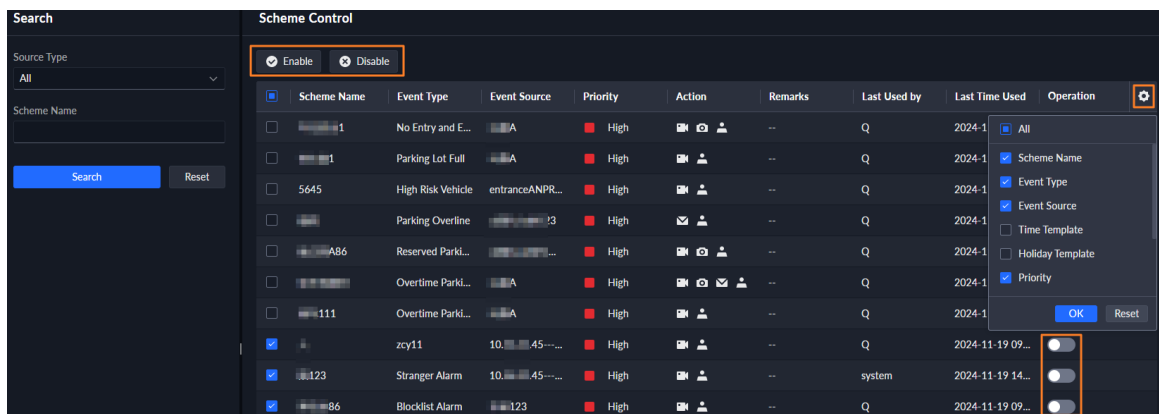
Step 2 Select **Arming Control** > **Scheme Control**, and then enable or disable event schemes.

- Enable or disable schemes one by one: Click  corresponding to a scheme to enable it, and then the icon changes to ; click  to disable the scheme.
- Enable or disable schemes in batches: Select the schemes that you want to enable or disable, and then click **Enable** or **Disable**.



- You can filter schemes by **Source Type**, or search for schemes by the name.
- Click , and then you can select the fields to be displayed on the page.

Figure 5-71 Scheme control



5.3 DeepXplore

You can set multiple search conditions to view records of people, vehicle snapshots, access, POS, MPT and MPT track.

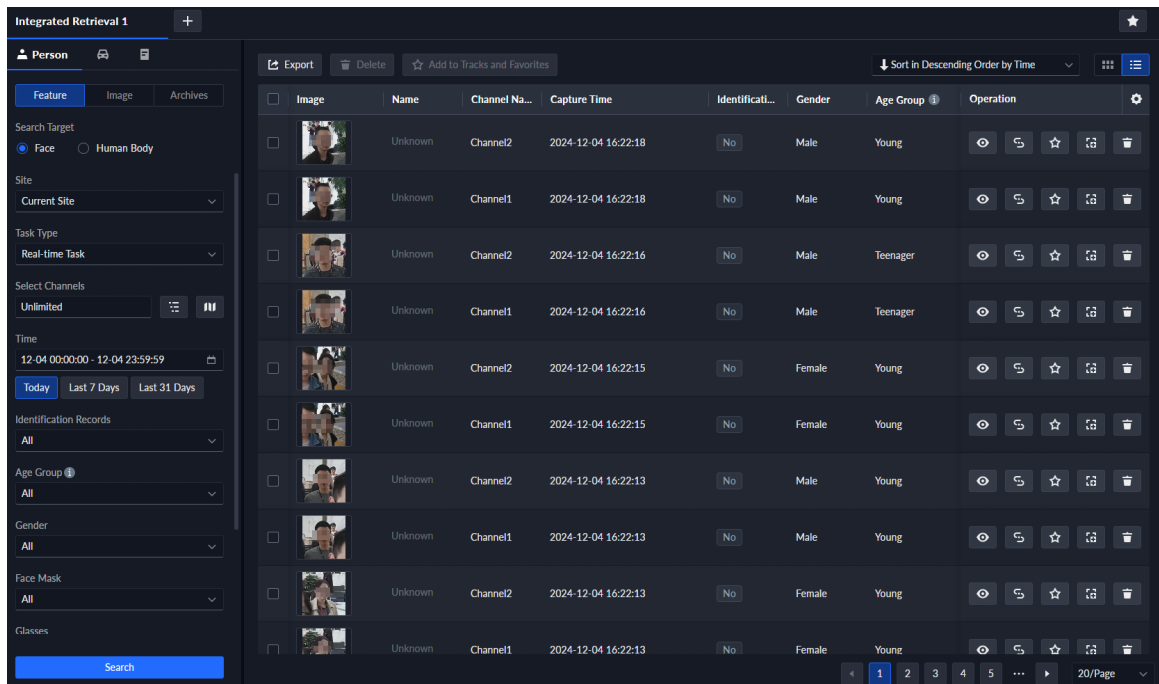
5.3.1 Searching for People

Based on the defined search conditions, you can view capture records of faces, bodies and other information.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **DeepXplore**.
- Step 2** Click **Integrated Retrieval**, and then click .

Figure 5-72 Person search



- Search type

- ◇ **Feature** : Search for records by the defined features, including age, gender, face mask, glasses, beard, expression, and more.



When selecting whether to search for identification records, the difference is that, besides the age and gender, identification records will also show the similarity between the captured face and those in the arming lists.

- ◇ **Image** : The platform compares the image you upload to capture records on the selected devices. If the similarity between a captured image on the platform and the one you upload equals to or higher than the defined value, the platform will display the result.



Only new versions of IVSS devices support displaying similarity.

- ◇ **Archives** : Search for records in the person information database.

- Search target

- ◇ **Face** : Search for records in the face capture database.
- ◇ **Human Body** : Search for records in the body capture database.
- ◇ Search channel: Select device channels of the records by clicking **Selected Channel**.
- ◇ Search time: Select time period of the records from **Today** , **Last 7 Days** and **Last 31 Days**.

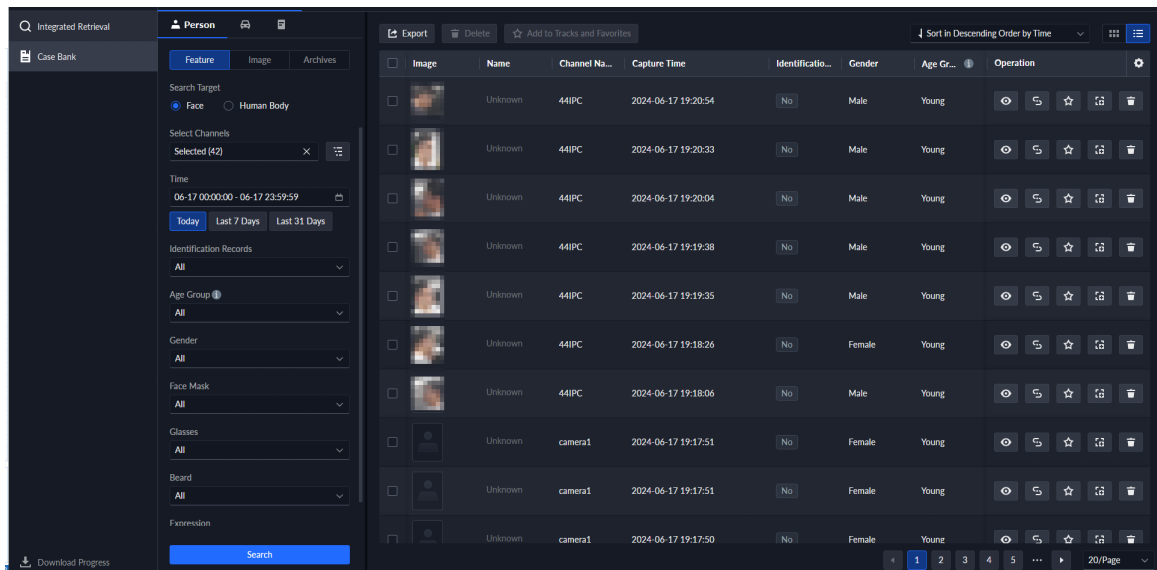


Only available for face and body capture records.

- Search conditions: Set search conditions such as age, gender, top color, ID, name and more to search for specific records.

Step 3 Set the search object, type and conditions, and then click **Search**.

Figure 5-73 Search results



Step 4 Manage the results.

For the search result, you can perform the following operations.

- View details on records

Select a record, and then click . Its details are displayed on the right, including snapshots, recorded videos (can be downloaded to your computer), and targets that can be further searched for (manually select a target or use AcuPick to automatically recognize targets).

- When viewing recorded videos and snapshots, you can select a target manually or select one automatically recognized by AcuPick, and then search for it in DeepXplore.
- If the channel is bound to other video channels, the recorded video from the bound video channels will play automatically.
- You can select a record, and then click  to view the track playback. Perform searching by image using the current captured snapshot, with the search criteria defaulting to the current retrieval conditions. You can click  on the track playback page, and then configure the conditions to search again.
- Add a record to a case

Click  to add a record to the tracks and favorites, and then click  at the upper-right corner to view all records in the tracks and favorites. You can add them to a case.

- Generate tracks

Click  to add a record to the temporary records, and then click  at the upper-right corner to view all records in the temporary records. Select multiple records, and then click **Generate Track** to generate a track.

- Click  to add the person to a face arming group. After you send the group to devices and configure an event, devices can trigger alarms when the face is recognized.

- Click  to delete it one by one.



You cannot delete the records of searching by image on devices.

- For the archives searching, double click the searching results or click to view the details. You can see the face capture, vehicle capture, access records and other information of the corresponding person.

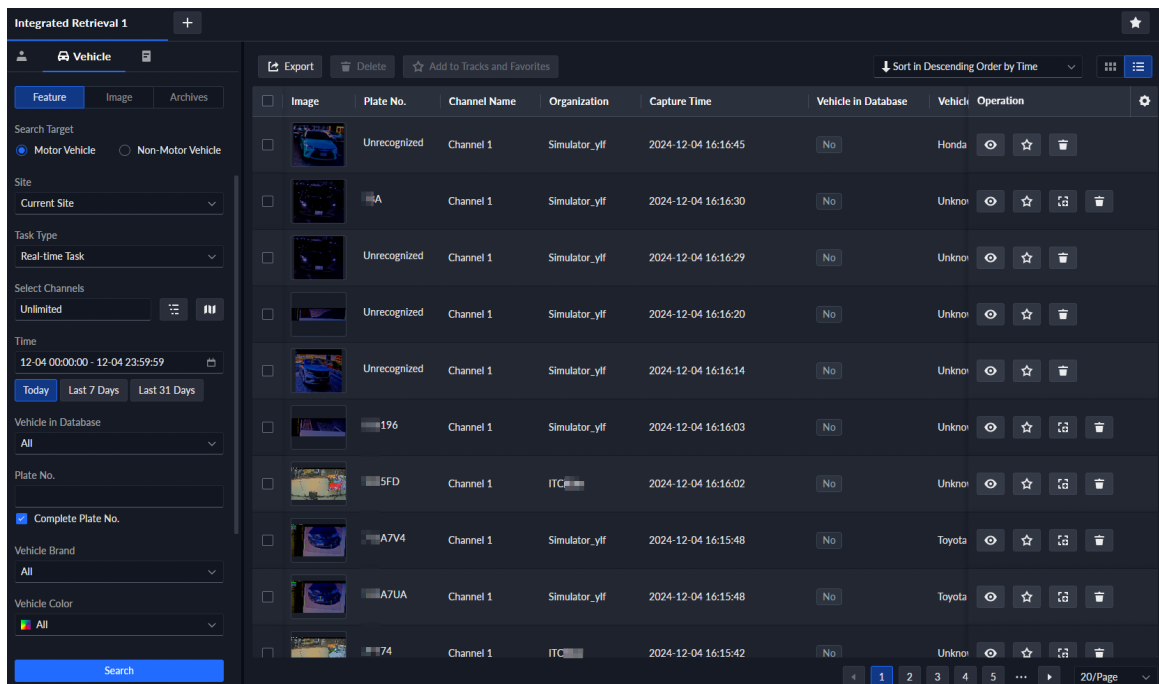
5.3.2 Searching for Vehicles

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click and then select **DeepXplore**.

Step 2 Click **Integrated Retrieval**, and then click .

Figure 5-74 Vehicle search



- Search type
 - ◇ **Feature** : Search for records by the defined attributes, including vehicle in database, plate number, vehicle brand, vehicle color, vehicle category, place of issue, and more.
 - ◇ **Image** : The platform compares the image you upload to all capture images. If the similarity between a captured image on the platform and the one you upload equals to or higher than the defined value, the platform will display the result.
 - ◇ **Archives** : Search for records in vehicle information database.
- Search target
 - ◇ **Vehicle** : Search for records in vehicle capture database.
 - ◇ **Non-Motor Vehicle** : Search for records in non-motor vehicle capture database.
 - ◇ Search channel: Select device channels of the records by clicking **Selected Channel**.
 - ◇ Search time: Select time period of the records from **Today** , **Last 7 Days** and **Last 31 Days**.



Only available for vehicle capture records.

- **Vehicle in Database (Yes/No)** : Select whether to search for capture records of vehicles in vehicle list.
- Search conditions: Set search conditions such as plate number (full plate number optional), vehicle brands and more to search for specific records.

Step 3 Set the search conditions, and then click **Search**.

For the search results, you can perform following operations.

- View details on records

Select a record, and then click  to view its details on the right, including snapshots, recorded videos (can be downloaded to your computer), and targets that can be further searched for (manually select a target or use AcuPick to automatically recognize targets).

- If the license plate is incorrectly or cannot be recognized, you can correct it manually. Then, it can be added to an arming group.
- If the channel is bound to other video channels, the recorded video from the bound video channels will play automatically.
- You can select a record, and then click  to view the track playback. Perform searching by image using the current captured snapshot, with the search criteria defaulting to the current retrieval conditions. You can click  on the track playback page, and then configure the conditions to search again.
- Add a record to a case

Click  to add a record to the tracks and favorites, and then click  at the upper-right corner to view all records in the tracks and favorites. You can add them to a case.

- Generate tracks

Click  to add a record to the temporary records, and then click  at the upper-right corner to view all records in the temporary records. Select multiple records, and then click **Generate Track** to generate a track.

- If a license plate is recognized, click  to add the vehicle to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the vehicle is recognized.
- Click  to delete it one by one.



The records of searching by image on devices, access records and POS records cannot be deleted.

- For vehicle archives, double-click a record to view recognition records of a license plate.

5.3.3 Searching for Records

In this section, you can view integrated records of people, vehicle, access control, POS transactions, MPT records and MPT track.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **DeepXplore**.

Step 2 Click **Integrated Retrieval**.

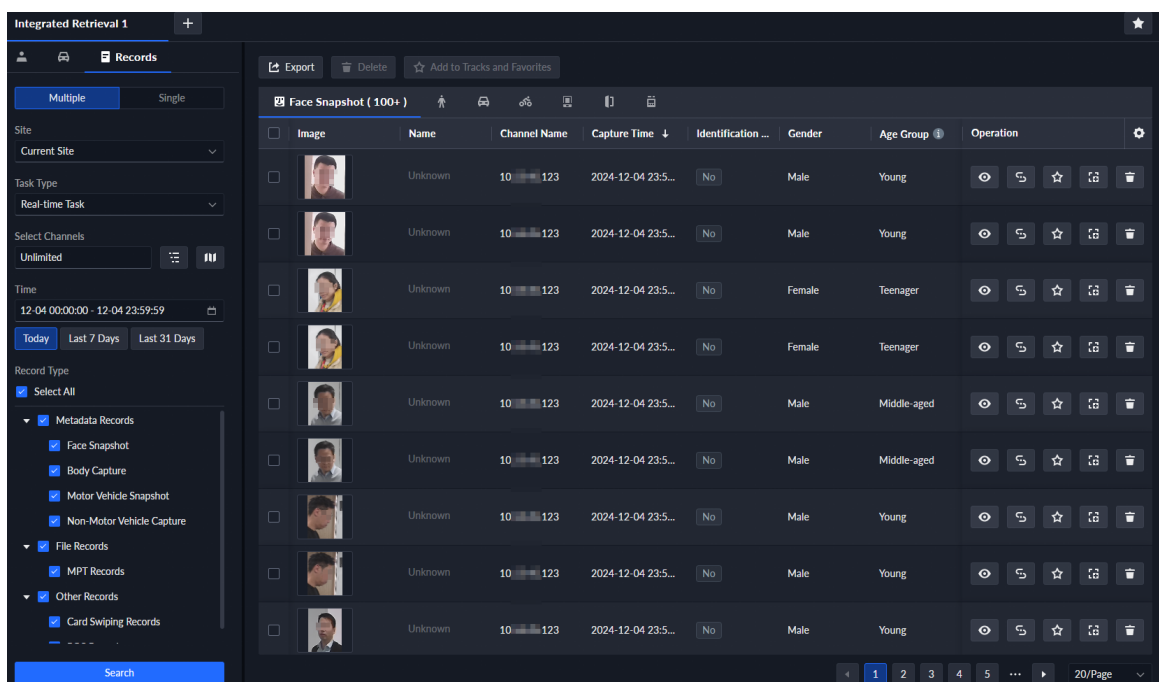
Step 3 Click .

- **Multiple** : you can search for the records of multiple types. Select site, task type, channel and time, and then click **Search**.



- ◇ The task type is **Real-time Task** by default. For recording task and local task, you need to add tasks according to "4.14 Video Analysis" before they are available.
- ◇ When selecting channels, you can click  to select channels from the channel list, or click  to select channels from the map.
- ◇ MPT records can only be searched for after MPT devices have uploaded records, or the platform has obtained records from MPT or EEC devices by retrieval plans. For how to configure a retrieval plan, see "3.1.5.3 Adding Retrieval Plan for MPT Devices".

Figure 5-75 Records search



- **Single** : You can search for the records of a single type, including MPT records, MPT track, POS records and card swiping records. Set information such as site, channel, and time, and then click **Search**.

Step 4 Manage the results.

For the search result, you can perform the following operations.

- View details on records

Select a record, and then click  to view its details on the right, including snapshots, recorded videos (can be downloaded to your computer), and targets that can be further searched for (manually select a target or use AcuPick to automatically recognize targets).

- When viewing recorded videos and snapshots, you can select a target manually or select one automatically recognized by AcuPick, and then search for it in DeepXplore.
- If the channel is bound to other video channels, the recorded video from the bound video channels will play automatically.
- Add a record to a case

Click  to add a record to the tracks and favorites, and then click  at the upper-right corner to view all records in the tracks and favorites. You can add them to a case.

- Generate tracks

Click  to add a record to the temporary records, and then click  at the upper-right corner to view all records in the temporary records. Select multiple records, and then click **Generate Track** to generate a track.

- You can also click  to add it to a face arming group. After you send the group to devices and configure an event, devices can trigger alarms when the face is recognized.
- For the face snapshot and body capture, you can select a record, and then click  to view the track playback. Perform searching by image using the current captured snapshot, with the search criteria defaulting to the current retrieval conditions. You can click  on the track playback page, and then configure the conditions to search again.
- If a license plate is recognized, click  to add the vehicle to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the vehicle is recognized.
- Click  to delete it one by one.



The access records, MPT records which are stored in EEC, and POS records cannot be deleted.

5.3.4 Track Playback

The search results of face or body captured images support track playback, allowing for the playback and display of target trajectories on a map.

Prerequisites

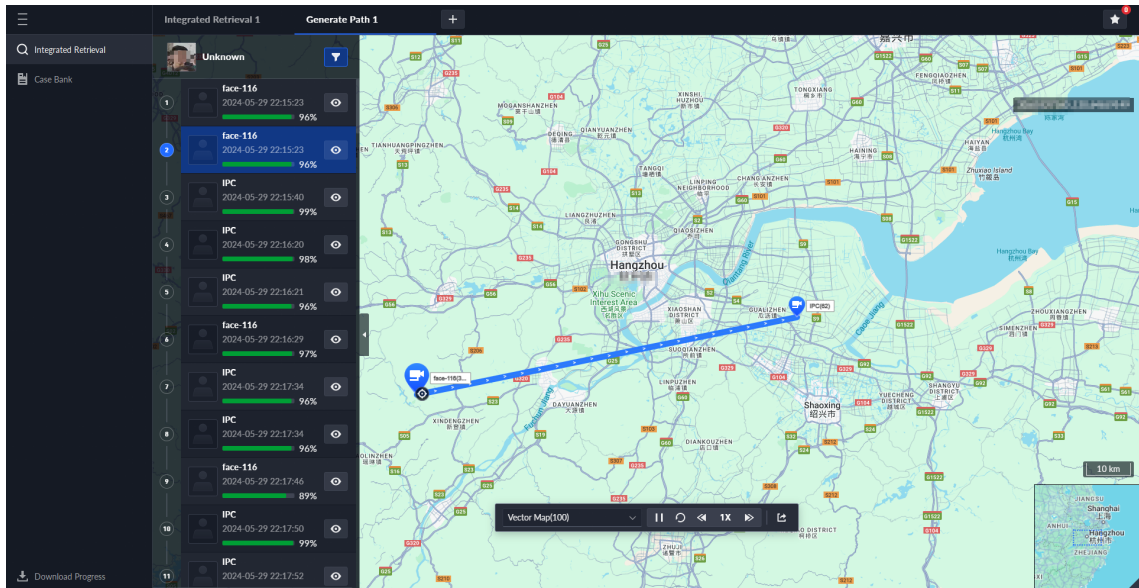
- The devices support structured feature reporting.
- You have configured the map.

Procedure

Step 1 On the person searching result page, or on the face snapshot or body capture searching result page of archives searching, select a result, and then click  to view the track playback. Perform searching by image using the current captured snapshot, with the search criteria defaulting to the current retrieval conditions.

Step 2 (Optional) You can click  on the track playback page, and then configure the conditions to search again.

Figure 5-76 Track playback



Step 3 Displays and play the track in time order. Click  on the snapshot card in the list to view the details.

Step 4 On the track playback page, supports the following operations.

Table 5-16 The operation instruction of track playback

Icon	Description
	Switch the map.  If the first location is within a subgraph, the system will automatically switch to the subgraph and start playing the trajectory. However, it does not support switching the map.
	Stop playing.
	Replay.
	Control the speed of track playback.
	Export the trajectory.

5.3.5 Searching for POS Transaction

You can search for POS transactions by keywords or specific conditions.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select  > **DeepXplore** > **Integrated Retrieval** > 

Step 2 Click **Single**, and then set the **Record Type** as **Post Records**.

Step 3 Configure the search conditions.

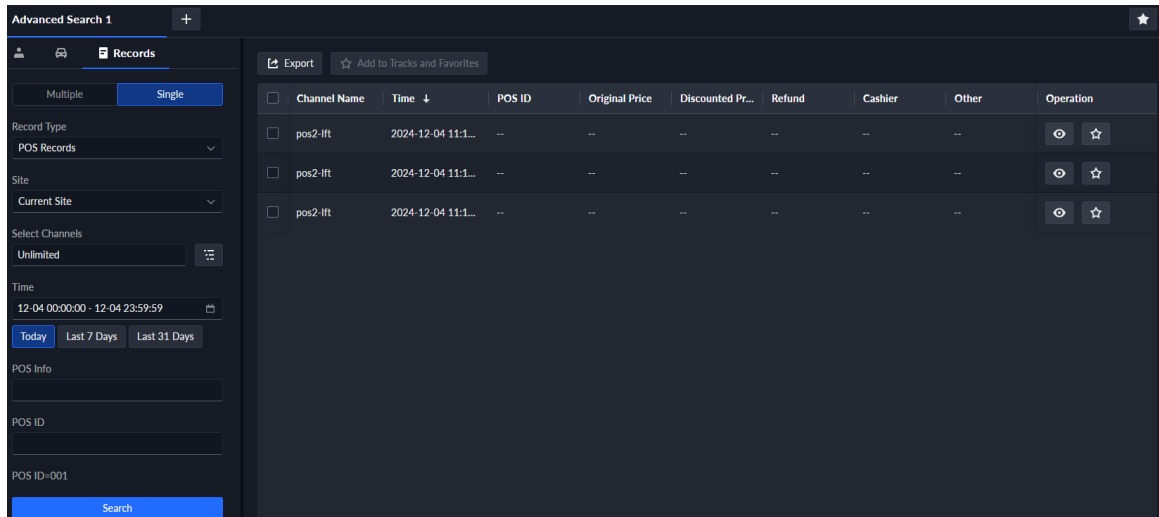
1. Select POS channels, site and then configure the period.

2. Configure the information you want to search for.

POS Info : Keywords in the transaction information. This can be used with one or more POS fields at the same time.

3. Click **Search**.

Figure 5-77 Search results



Channel Name	Time	POS ID	Original Price	Discounted Pr...	Refund	Cashier	Other	Operation
pos2-lft	2024-12-04 11:1...	--	--	--	--	--	--	
pos2-lft	2024-12-04 11:1...	--	--	--	--	--	--	
pos2-lft	2024-12-04 11:1...	--	--	--	--	--	--	

Step 4 Manage the search results.

- View details.

Select a transaction, and then click  to view the detailed information and video at that time on the right. The video can be directly downloaded to your computer. Also, you can also search for targets in the video by selecting one manually or automatically recognized by AcuPick.



If you need video at the time of transaction, you must bind POS channels with video channels, and configure recording plans for the video channels. For details, see "3.1.3 Binding Resources" and "3.1.4 Adding Recording Plans".

- Add to a case.

1. Click  of a transaction to add it to the track and favorites.
2. Click  on the upper-right corner.
3. Select one or more transactions, and then click **Add to Case**.
4. Select a case, and then click **OK**.



In the track and favorites, select one or more transactions, and then click  to remove them. This operation will only remove them from the track and favorites, but not delete them.

- View track.

1. Click  of a transaction to add it to the track and favorites.
2. Click  on the upper-right corner.
3. Select transactions, and then click **Generate Track**. The platform will open a page and display the track based on the transactions you select.

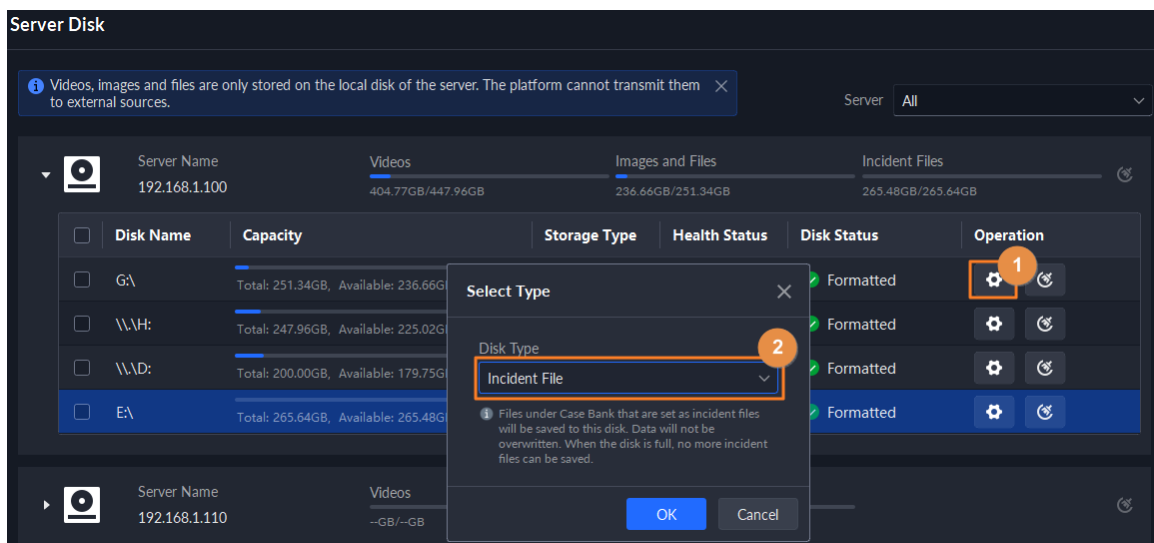
5.3.6 Adding a Case Bank

Inside the case bank, you can integrate the records of face, plate, access and more into one complete case, and configure its details for future investigation. The platform supports storing up to 10,000 cases.

Prerequisites

The case files can only be stored in **Incident File** disk. Make sure that you have configured such disk type in advance from **Storage > Server Disk**.

Figure 5-78 Disk type



Users with access to **Case Bank** :

- Super administrator: View, edit and delete incident files.
- Administrator:
 - ◇ View incident files created by themselves and common users. No access to incident files of other administrators.
 - ◇ Edit and delete files opened.
 - ◇ Cannot edit or delete files closed.
- Common user:
 - ◇ Can only view files created by themselves.
 - ◇ Edit and delete files opened.
 - ◇ Cannot edit or delete files closed.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **DeepXplore**.

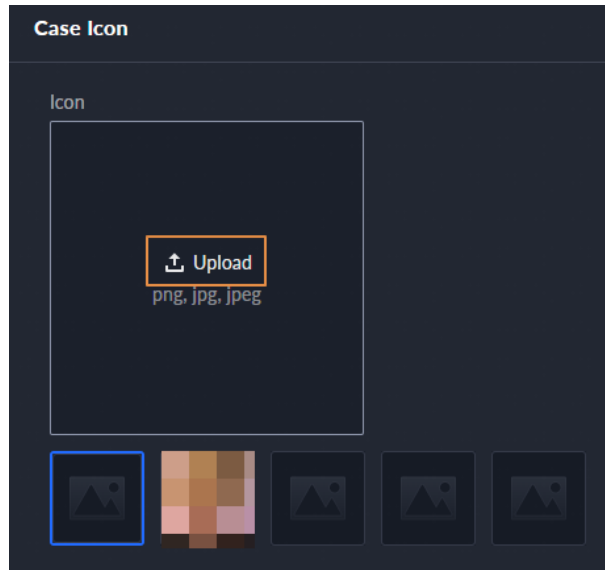
Step 2 click .

Step 3 Click **Add** to add a new case.

Step 4 In the **Case Icon** section, click one of the 5 small squares, or click  on the uploading area, and then upload the image file.

The image you select will be displayed on the upper-left corner of the case you export.

Figure 5-79 Select an image for the case



Step 5 Select an image from the **Case Icon** section.



Only one icon can be added onto the case file.

Step 6 Enter the basic information of the case.

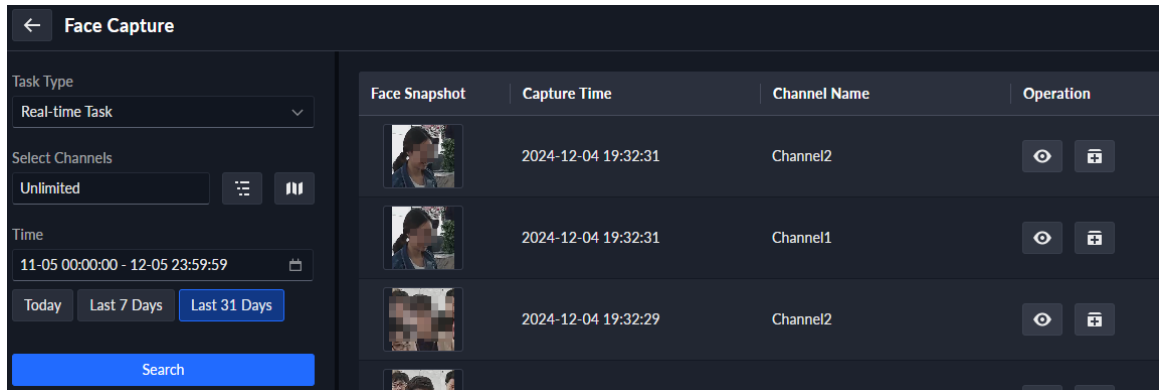
- **Case Type** : Used for categorize cases. You can click the drop-down list to select type or create new ones.
- **Status** : Select the case status from **Open** and **Close**. The Platform integrates cases under each status category.

Step 7 Add records, including face capture, body capture, license plate recognition records, access records, POS records, and MPT records.

Records of other categories are added in the same way. In this section, we take **Face Capture** as an example.

1. Click **Add** under **Face Capture**.
2. Select task type, channels, and time, and then click **Search**. You can click  to view its details.
 - The task type is **Real-time Task** by default. For recording task and local task, you need to add tasks according to "4.14 Video Analysis" before they are available.
 - When selecting channels, you can click  to select channels from the channel list, or click  to select channels from the map.

Figure 5-80 Add face capture record



3. Click  next to the record to add it to the case.
4. Click  to go back to the case adding page, you can add other type of records related to the case.

Step 8 Click , and then click **Add** under **Attachment** to upload images and videos related to the case.

- The platform supports uploading up to 20 videos, and each video cannot exceed 300 MB. Format includes .dav, .mp4, .avi, .flv and .asf.
- Up to 20 images can be uploaded. Image format includes .png, .jpg and .jpeg.



The number of all video files and images cannot be more than 20.

Step 9 Click **OK**.

Related Operations

- Delete or replace an icon

Click  on the case card, and then click edit. Click  to delete it; Drag the image file to uploading image area, or click  on the uploading area, and then upload the image file.

- Enter case name in the search box at the upper-right corner, and then press Enter or click  to search for cases.
- Click  under a temporary case to view the case details. If you need to edit the details, click **Edit** and change the information as needed.
- Click  under a temporary case to download it, or you can click **Download** in the case details page. Click **Download Progress** at the lower-left corner to check the download progress.
- Click  under a case to delete it one by one, or you can select cases, and then click **Delete** to delete them in batches.
- Click  to close the case and click it again to open the case.

5.3.7 Viewing Track of MPT Devices

Search for and view the track of an MPT device on the map within the defined period.

Prerequisites

- Configure the vector map.
- Add MPT devices to the platform. For details, see "3.1.2.4 Adding Devices".
- MPT devices upload their GPS information to the platform. For details, see their user manuals.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **DeepXplore** > **Integrated Retrieval** > .
- Step 2** Click **Single**.
- Step 3** Set the **Record Type** as **MPT Track**
- Step 4** Select an MPT device, configure the time, and then click **Search**.

The track of the MPT device will be displayed on the map.



You can only search for up to 24 hours of track in the same day. For example, 00:00 to 23:59:59, or 3:00 to 23:59:59.

5.4 Access Management

On the **Access Management** page, you can perform operations on access control, lift control, video intercom, and visitor.

5.4.1 Access Control

5.4.1.1 Viewing Access Points

Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**.

This page displays by default all the access points in the root zone and all its sub zones in card view.

Change the display mode

Click  or  on the upper-right corner to display access points in card view or on the map. Click the icon of an access point to view live videos from bound channels, unlock or lock the door, or make a call to it.

- In card view, **Event Type** supports **Exception**, **Normal** and **Alarm**.
- On the map, when an alarm occurs, the device icon on the map will be displayed in red.

View certain access points

On the top on the page, select a zone or access point type to display only door or lift control channels, or the access points in a zone and its sub zones.

View access point information

In card view, double-click an access point to view its information, including basic information, live videos from bound channels, and events. For a door channel, you can also lock or unlock the door and make a call to it.

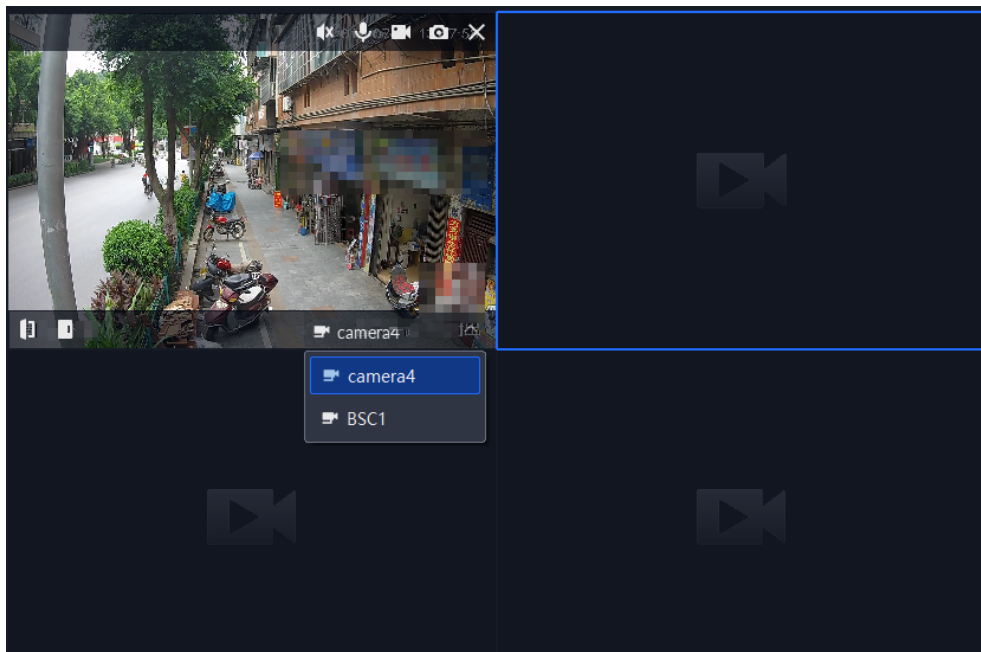
5.4.1.2 Viewing Live Video

Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**. You can view the live video of the access point (the access point device must come with a camera) or the live video of video channels bound to the access point (the channel can be bound when adding a device) in the following ways.

View live videos in card view

Click  to display access points in card view. Click  to view live videos. Each access point will only use one window. If more than 1 video channel is bound to the access point, you can click the drop-down list on the lower-right corner to switch between video channels.

Figure 5-81 Switch between video channels



View live videos in the detailed information of an access point

In card view, double-click an access point, and then live videos will be displayed in the **Related Info** section.

View live videos on the map

Click  on the upper-right corner to display access points on the map. Click the icon of an access point, and then click  to view live videos.

5.4.1.3 Locking and Unlocking Door

Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**. You can unlock or lock doors in the following ways.

Unlock or lock doors in card view

Click  to display access points in card view. Click  or  to unlock or lock a door channel.

Unlock or lock doors in the detailed information of an access point

In card view, double-click an access point, and then click **Open Door** or **Close Door**.

Unlock or lock doors on the map

Click  on the upper-right corner to display access points on the map. Click an access point, and then click  or  to unlock or lock a door channel.

5.4.1.4 Starting a Call

Support remote calling of VTO or face access control devices on the platform.

Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**. You can start a call in the following ways.

Start a call in card view

Click  to display access points in card view. Click  to start a call.

Start a call s in details of an access point

In card view, double-click an access point, and then click .

Start a call on the map

Click  on the upper-right corner to display access points on the map. Click an access point, and then click  to start a call.

5.4.1.5 Controlling Door Channels Globally

Set all door channels in a zone to normally closed, normally open modes, or restore them to the normal status in one click. Only administrators can control door channels globally.

Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**. Select a zone, and then click **Always Open**, **Restore**, or **Always Closed** to control all the door channels at the same time.

- **Always Open** : All people can pass without verifying their identifications.
- **Restore** : Restore door channels to the normal status from normally open or normally closed mode. People must verify their identifications to pass

- **Always Closed** : No person is allowed to pass.

If you perform this operation to a zone, it will also be applied to all the sub zones. When the status of the parent zone and sub zone is in conflict, the platform will resolve it in the following ways:

- When a sub zone has been set to the normally open or closed mode, operating the parent zone will override the status of the sub zone.
- When the parent zone has been set to the normally open or closed mode, and you want to set a sub zone to a mode opposite to the parent zone, the platform will prevent you from doing so, and prompt that you must restore the parent zone to the normal status before setting the sub zone.

5.4.1.6 Controlling Lift Channels Globally

Set all lift channels in a zone to no authentication, authentication, and lock modes. Only administrators can control lift channels globally.

Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**. Select a zone, and then click **No Authentication Mode**, **Authentication Mode**, or **Lock Mode** to control all the lift channels at the same time.

- **No Authentication Mode** : All people can go to any floor without verifying their identifications.
- **Authentication Mode** : People must verify their identifications to go to specified floors.
- **Lock Mode** : No person is allowed to use lifts.

If you perform this operation to a zone, it will also be applied to all the sub zones. When the status of the parent zone and sub zone is in conflict, the platform will resolve it in the following ways:

- When a sub zone has been set to the no authentication or authentication mode, operating the parent zone will override the status of the sub zone.
- When the parent zone has been set to the no authentication or authentication mode, and you want to set a sub zone to a mode opposite to the parent zone, the platform will prevent you from doing so, and prompt that you must set the parent zone to the authentication mode before setting the sub zone.

5.4.1.7 Viewing Real-Time Events

When a person passes through an access point, an event will be reported to the platform. You can view the detailed information of that event.

Prerequisites

If you want to view recorded videos and live videos of an event, you must configure the following parameters first:

- Live video: Bind video channels to access points. For details, see "3.1.3 Binding Resources".
- Recorded videos: First, bind video channels to access points ("3.1.3 Binding Resources"). Then, select either of the 2 options: Configure recording plans for the bound video channels ("3.1.4 Adding Recording Plans"), or configure an event to link the bound video channels to record videos when a person passes ("4.1 Configuring Events").

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**.

Events from all zones are displayed in the **Event** section at the bottom of the page.

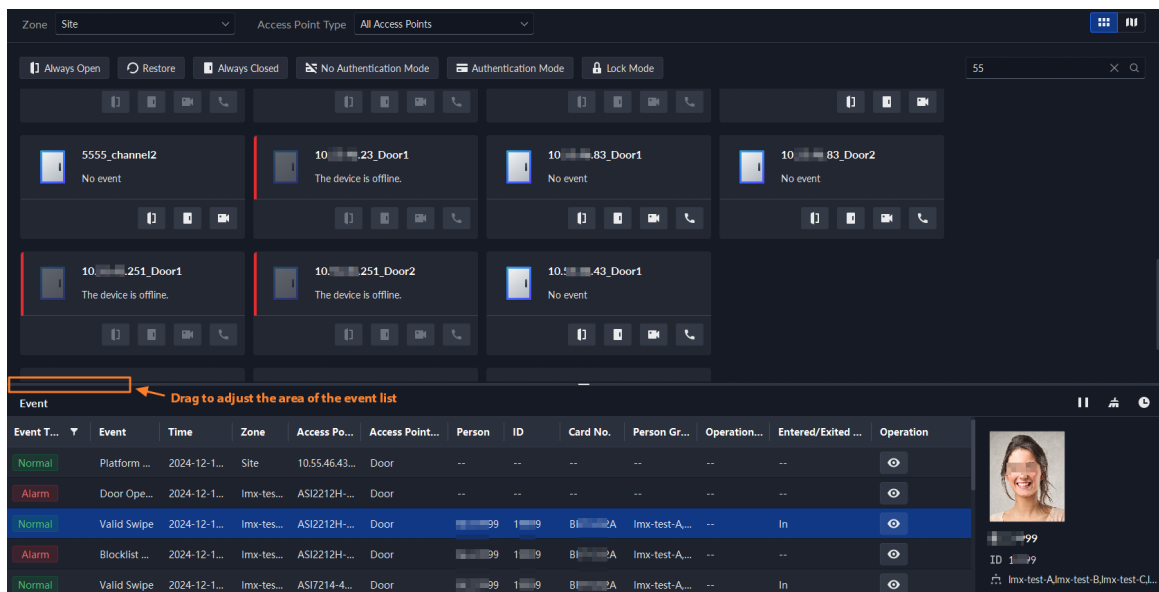
- Step 2** Select a zone and type of access points, and then the platform will display access points and real-time events of that zone and its sub zones.
- Step 3** Click , and then you can view the snapshot, recorded video, and live video of the event.
- Step 4** Locate the access point for an event.

- Click  on the upper-right corner to display access points in card view. When events are not clicked, it displays the image and information of the person in the latest event; when clicked, the corresponding access point card will be highlighted, and it will display the image and information of the person of the selected event.
- Click  on the upper-right corner to display access points on the map. When events are not clicked, the status of the access point icons on the map will change in real-time; when clicked, the event information will be displayed on the map.



- You can drag the real-time events upwards. See the following figure.
- Click the person image at the lower-right corner, and then you can view it in a larger image.

Figure 5-82 Events



Related Operations

- : Stop receiving new events. Click it again to start receiving events.
- : Clear the events on the page, but they will not be deleted.
- : View access records.

5.4.1.8 Viewing and Exporting Specified Events

View and export events in a specified zone, person group, and period.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Records** > **Event Records**.

On top of the page, the numbers of different types of events are displayed for all zones by default.

Step 2 Configure the search conditions, and then click **Search**.

Table 5-17 Parameter description

Parameter	Description
Zone	Search for events in the selected zone. You can select multiple zones at the same time.
Time	Search for events that occurred in the defined period. You can search for event within up to 1 month.
Person Group	Search for events of people that belong to the selected group.  The selected person group is empty by default. In this case, the search results will include events with no related person information, such as access by a person whose information is not on the platform, access by strangers, and alarms triggered by devices. If you want to clear the selection of a person group, click , and then no person group is selected.
Person/Person ID/ Access Point	Select an option and enter keywords to search for certain events. For example, select Access Point and enter Front Gate to search for events of access points that have Front Gate in their names.
Keywords	

Step 3 Click **Export**.

Step 4 Enter the login password, encryption password, select whether to export images and the export range, select fields to be exported, and then click **OK**.



You can configure whether to verify the password. For details, see "7.4.1 Configuring Security Parameters".

- The encryption password is used to protect the export file. It consists of 6 uppercase or lower case letters, numbers, or their combinations. You need to enter it when using the export file.
- The export range can be all or specified events that are displayed.
- Select **Export Image** to export snapshots of the events at the same time.
- The fields to be exported include **Event Type**, **Event**, **Time**, **Zone**, and more.

5.4.1.9 Acquiring Records

The platform offers 2 methods for acquiring access records, manually or automatically. For the automatic method, only records within the past 24 hours will be acquired. But, the manual method can be used to acquire records from specified period and device.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Records** > **Event Records**.

Step 2 Click **Acquire Records**.

Step 3 Enter the login password, and then click **OK**.

Step 4 Acquire records.



Select **Extract Image**, and then you can acquire images of the access records. Before using this function, you need to configure image storage. For details, see "3.3.4 Configuring Device Storage".

- **Auto Extraction** : The platform will acquire records within the past 24 hours at the defined time every day. How records are synchronized:
 - ◇ If records on a device was automatically synchronized to the platform, then the platform will synchronize all records from the time of the latest record from the last automatic synchronization to the time you set.

For example, the latest record from the last automatic synchronization was on 2024-6-18 16:00, time of automatic synchronization is set to 04:00 every day. The device was offline on 2024-6-18 18:00, and then reconnected on 2024-6-20 16:00, then the platform, on 2024-6-21 04:00, will synchronize the records generated on the device from 2024-6-18 16:00 to 2024-6-21 04:00.
 - ◇ If records on a device has not been automatically synchronized to the platform, and the device went offline and online multiple times, the platform will synchronize all the records from the time of the latest record uploaded before the first offline, to the time you set.

For example, time of synchronization is set to 04:00 every day. The device first goes offline on 2024-6-18 16:00 with the latest record uploaded on 2024-6-18 15:00. Before the time of synchronization, the device goes offline and online multiple times. Then on 2024-6-19 04:00, the platform will synchronize the records generated on the device from 2024-6-18 15:00 to 2024-6-19 04:00.
 - ◇ If records on a device has not been automatically synchronized to the platform, and records were not generated on the device and uploaded to the platform when the device is online, then on the time of synchronization, the platform will synchronize the records on the device within the past 24 hours.
- **Manual Extraction** :
 - ◇ Select **Extract Now**, and then the platform will acquire records ranging from the last time that an extraction was performed which were not extracted.

Select **Extract Image**, and then you can extract images in the access records.
 - ◇ Select **Extract by Range**, and then you can specify the time range, record type, and device.

5.4.1.10 Sending Reports

The platform supports sending reports to the specified receiver by sending now or auto send.

Prerequisites

You need to configure the email server from  > **System Parameters** > **Email Server**. For details, see "7.4.5 Configuring Email Server".

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Records** > **Event Records**.
- Step 2 Click **Send Report**, and then select **Send Now** or **Auto Send**.
 - **Send Now** : Click  to select the receiver, or enter the email address of the receiver and then press Enter, configure the email content, start from sending which record, and the total records to be sent (up to 100,000 records can be sent at a time).

- **Auto Send** : Automatically send reports to the receivers at specified time of each day or week.
 1. Enable **Daily Report** or **Weekly Report**, and then set the time.
 2. Click  to select the receiver, or enter the email address of the receiver and then press Enter.

Step 3 Click **OK**.

5.4.1.11 Viewing Access Route

View the access route of a person on a map based on events.

Step 1 Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Records** > **Event Records**.

The number of events in the root zone is displayed on the top of the page by default.

Step 2 (Optional) Select a zone, person group, and period, and then click **Search**.

You can search for event within up to 1 month.



The selected person group is empty by default. In this case, the search results will include events with no related person information, such as access trajectory of a person whose information is not on the platform, access trajectory of strangers, and alarms triggered by devices.

Step 3 (Optional) Click  to add multiple events to the temporary records.

Step 4 (Optional) Click  to go to the temporary records.

Step 5 Select the records, and then click **Generate Track** to generate the route.

The platform will play the route based on the time of events.



If events happened in multiple zones, and the maps of zones do not relate to each other as main and sub maps, the platform might not play the route normally.

5.4.1.12 Viewing and Exporting Analysis of People Entering and Exiting

When people pass through boundaries, the platform will count the number of people entering and exiting zones. You can view the number of each zone and export it to your computer.

Prerequisites

Set access points as boundaries. The platform will only count the number of people pass through boundaries. For details, see "4.5.2.5.2 Setting Boundary".

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Records** > **Analysis of People Entering and Exiting**.

Step 2 Select one or more zones, boundaries, and the start time, and then click **Search**.

The platform will display the statistics of people entering and exiting the selected zone, and related events ranging from the start time to the current time. For example, the

platform will display the statistics and events ranging from the defined start time 5-16 08:00:00 to the current time 5-17 10:00:00.

Step 3 Click **Export**.

Step 4 Enter the login password, encryption password, select whether to export images and the export range, select fields to be exported, and then click **OK**.



You can configure whether to verify the password. For details, see "7.4.1 Configuring Security Parameters".

- The encryption password is used to protect the export file. It consists of 6 uppercase or lower case letters, numbers, or their combinations. You need to enter it when using the export file.
- The export range can be all or specified events that are displayed.
- Select **Export Image** to export snapshots of the events at the same time.
- The fields to be exported include **Event Type** , **Event**, **Time**, **Zone**, and more.

Related Operations

- Manually mark the enter or exit status for people:
 - ◇ On the list of **Person Entered** , **Person Exited** or **Persons Who Did Not Exit after Entering**, click  to see all access records of a person. Click  to mark a record as invalid (the records will not be deleted). The invalid records can also be restored to be valid. The statistics and status of the person will change accordingly.
 - ◇ On the list of **Persons Who Did Not Exit after Entering**, click  to mark a person as "exited". The statistics and status of the person will change accordingly.
- You can filter the search results by **Person Group** , and also search the records by selecting **Person**, **ID**, **Access Point**, **Company**, or **Department**, and then entering the keywords.

5.4.2 Video Intercom Application

- You can call, answer, release information and view video intercom records.
- Make sure that you have configured the video intercom configuration before application. For details, see "4.6 Video Intercom". You can also click  **Video Intercom Config** to go to the video intercom configuration page.

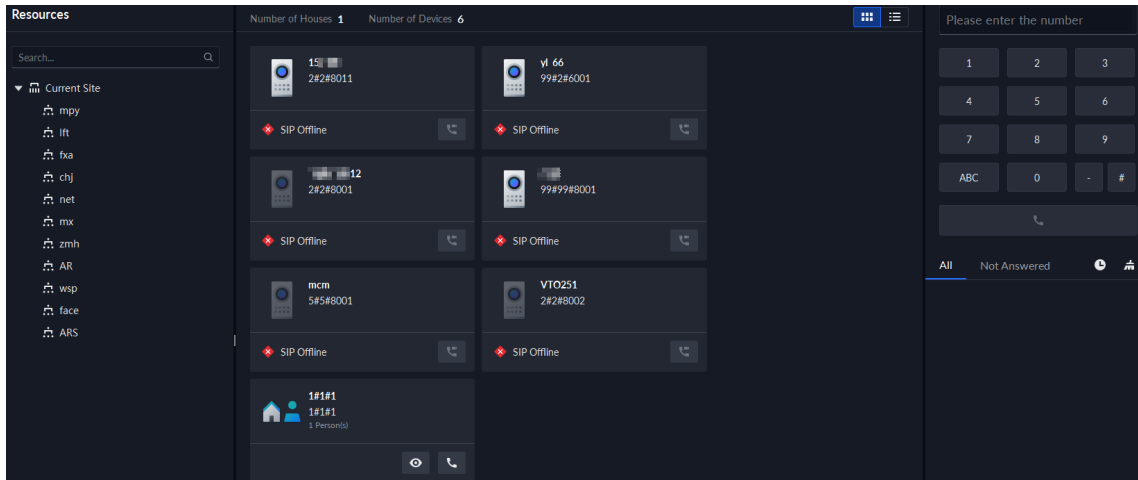
5.4.2.1 Call Center

The platform, VTOs, VTHs, second-generation door station access controllers, and second-generation fence station access controllers can call each other.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Access Management** > **Video Intercom** > **Call Center**.

Figure 5-83 Call center



Step 2 You can call different devices.

- Call from the platform to VTO

Select VTO in the device list; click  corresponding of VTO or dial a number on the dial pad to call the VTO. The system pops out call page. The following operations are supported during call.

- ◇ : If VTO is connected to lock, click this icon to unlock.
- ◇ : Click this icon to capture picture, the snapshot is saved into the default directory. To change the path, see "8.4.5 Configure File Storage Settings".
- ◇ : Click this icon to start record, click again to stop record. The video is saved in default path. To change the path, see "8.4.5 Configure File Storage Settings".
- ◇ : Click this icon to hang up.



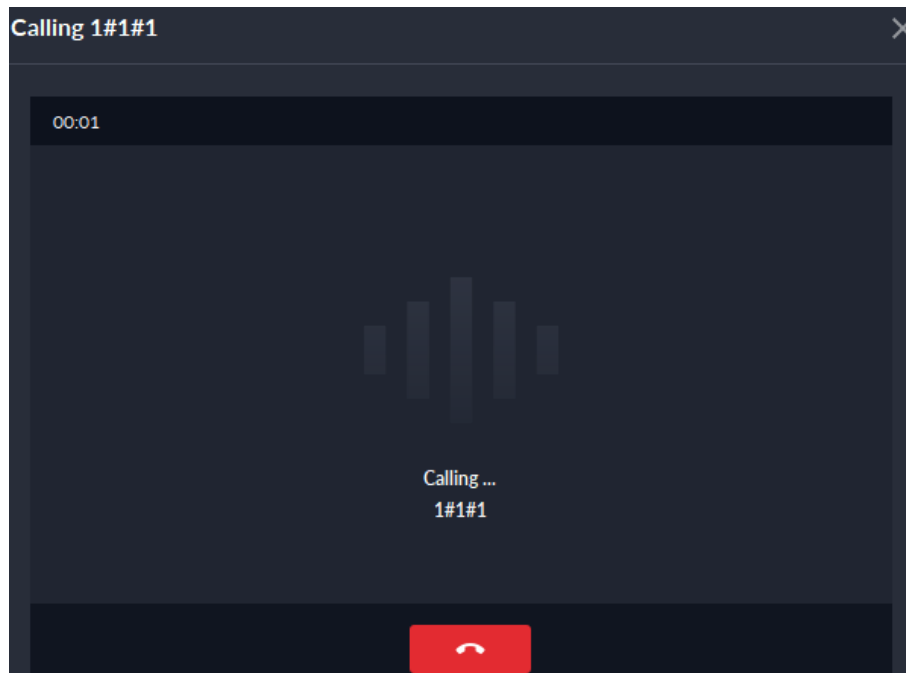
If the device supports two locks, two lock icons will appear on the page, and you can click either one to unlock corresponding door.

- Call from the platform to VTH

Select VTH from the device list, click  on the VTH or dial corresponding VTH on the right (such as 1#1#101). The system pops up the dialog box of **Calling now, please wait** There are two modes for answering the call.

- ◇ Answer by VTH, bidirectional talk between client and VTH. Press  to hang up when you answer the call.
- ◇ If VTH fails to answer in 30 s, hangs up or is busy, then it means the call is busy.

Figure 5-84 Calling



- Call from the platform to an access control device that supports video intercom

Select a device from the device list, click  on it or dial its number on the right (such as 1#1#101). The system pops up the dialog box of **Calling now, please wait ...**. There are two modes for answering the call.

- ◇ Answer by the device, bidirectional talk between client and the device. Press  to hang up when you answer the call.
- ◇ If the device fails to answer over 30 s, busy or hang up directly, then it means the call is busy.

- Call from VTO to the platform

When a VTO calls, a window pops up.

- ◇ : Unlock the door if the VTO is connected to a door.
- ◇ : Answer the call.
- ◇ : Hang up.

- When VTH is calling the platform

The client pops out the dialog box of VTH calling. Click  to talk with VTH.

- ◇ Click  to answer VTO, realize mutual call after connected.
- ◇ Click  to hang up.

- When an access control device that supports video intercom is calling the platform

The client pops out the dialog box. Click  to talk with the device.

Click  to hang up.

- Call through call records

All the call records are displayed in the **Call Record** at the lower-right corner of the page of **Video Intercom**. Click the record to call back.

5.4.2.2 Releasing Messages

Send message to VTHs.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click  > **Access Management** > **Video Intercom** > **Information Release**.
- Step 2 Click **Add New Message**, select one or more VTHs, and then configure the information you want to send.
- Step 3 (Optional) Enable **Scheduled Release**, and then configure the time.
- Step 4 Send the message.
- If no scheduled release time is configured, click **Instant Release**, or click **Save**, and then click  to send the message immediately.
 - If a scheduled release time is configured, click **Save**, and then the message will be sent on the defined time.

5.4.2.3 Video Intercom Records

Search for and view call records.

Background Information

- In a call group, only one record is generated for a call, either the call is answered or missed.
- In a call group, if one person answers, the call is considered answered. The missed records of others are not displayed.

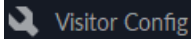
Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click  > **Access Management** > **Video Intercom** > **Video Intercom Record**.
- Step 2 Set conditions, and then click **Search**.
- The platform displays all the records according to the configured conditions.
- Step 3 (Optional) Click **Export**, and then follow the prompts to export all or partial records to your computer.

5.4.3 Visitor Application

After appointment is made on the platform, and visitor information is registered, the visitor can have access permission. Access permission is disabled after the visitor leaves or if the visitor does not leave after the appointment leaving time.

5.4.3.1 Preparations

- You have configured the deployment of the video intercom devices, access control devices, lift control devices, and entrance and exit devices. For details, see the corresponding user manual.
- You have configured the basic configuration of the platform. For details, see "3 Basic Configurations".
- Make sure that you have configured the visitor configuration before application. For details, see "4.7 Visitor Management". You can also click  to go to the video intercom configuration page.

5.4.3.2 Process

- Visits after appointment: Visitors make appointments according to "5.4.3.4 Visitor Appointment", and when they arrive on site, they can quickly access by confirming their information through **Check In** according to "5.4.3.6 Checking In".



- Visits without appointment: When visitors arrive, they need to fill out visitor information on site according to "5.4.3.6 Checking In". This will take a few minutes before they can access.



5.4.3.3 Visitor Management

You can view visitor information, and perform operations such as visitor appointment, checking-in, appointment approval, and more.

Log in to the DSS Client. On the **Home** page, click  > **Access Management** > **Visitor** > **Visitor Management**, and then you can view visitor information and perform operations.

Figure 5-85 Visitor management



Table 5-18 Visitor management description

No.	Description
1	Displays the visitors in total and the number of visitors by access status. Appointment to be Approved : Visitors must be approved before they can access, if they create appointment by themselves or are invited by host from  > Visitor > Visitor Appointment Config, and an approving role is configured. For details, see "4.7.2 Configuring Visit Settings". After being approved, the status changes to Pre-booked Appointment. Pre-booked Appointment : Appointment has been made, but not checked in yet. On Visit : Already checked in, but not exceed the appointment leaving time. Overstayed : Not checked out after the appointment leaving time.
2	Filter the visitor information by host group and time (appointment visit time, visit time, appointment leaving time, or unlimited).
3	Perform operations such as visitor registration, visit appointment and exporting visitor information. See the following sections in this chapter.

No.	Description
4	Visitor information list. Click  to select the fields that you want to display.
5	Search for visitors by host name, organization (department), or more.

5.4.3.4 Visitor Appointment

Making appointment before visitor arrive will greatly reduce the time that visitors have to wait for their information to be recorded. After appointment, the visitor status changes to **Pre-booked Appointment**.

5 ways of appointment are available:

- Appointment through the platform. For details, see "5.4.3.4.1 Appointment through the Platform".
- Create appointment by visitors. For details, see "5.4.3.4.2 Creating Appointment by Visitors".
- Invited by host. For details, see "5.4.3.4.3 Appointment Invited by Host".
- Appointment through the visitor terminal. For details, see the user manual of the visitor terminal.
- Appointment DSS Agile app. For details, see the user manual of the app.
- Invited by host through DSS Agile VDP app. For details, see the user manual of the app.

5.4.3.4.1 Appointment through the Platform

Register the information of visitors on the platform before they arrive for their visits. This will greatly reduce the time that visitors have to wait for their information to be recorded.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Access Management** > **Visitor** > **Visitor Management**.

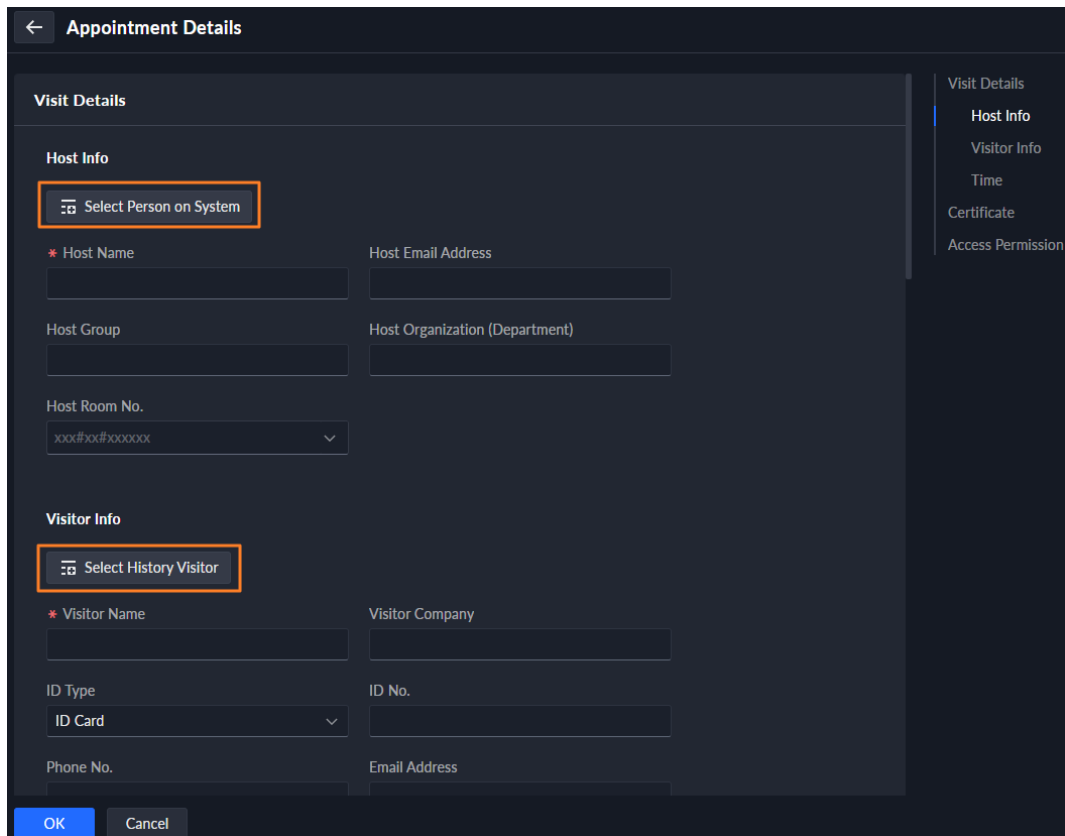
Step 2 Click **Visitor Appointment**.

Step 3 Enter the information of host and visitor.



Click **Select Person on System**, and then select a person (only person in the person group to which the current user has permission can be selected. Person group permissions can be configured when adding a person). The host information will be automatically filled in and cannot be edited; click **Select History Visitor**, and then select a history visitor. The information of this visitor will be automatically filled in and cannot be edited.

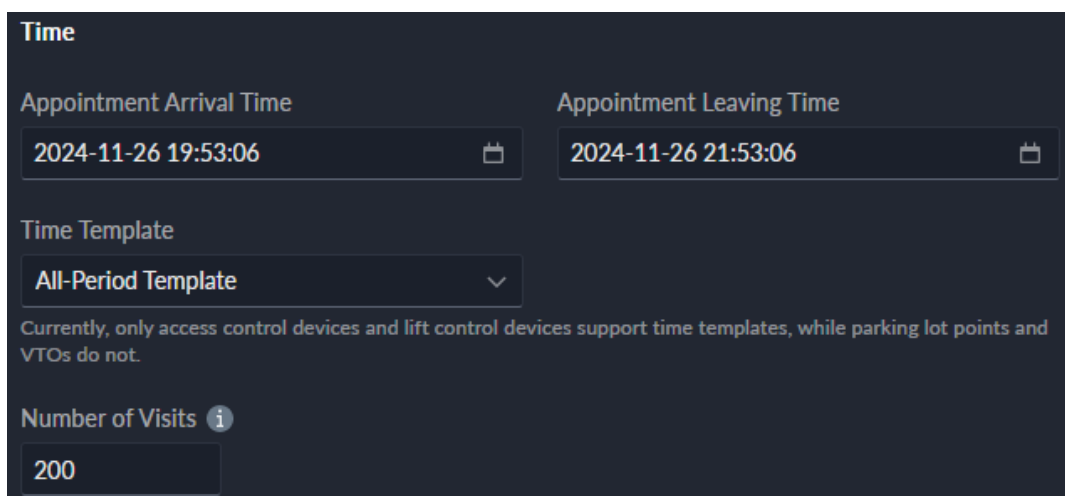
Figure 5-86 Visitor appointment



Step 4 Configure appointment arrival and leaving time, set the time template and number of visits.

- **Time Template** : All-period, week day and weekend templates are available by default. You can also click **Create Time Template** to customize visit periods from Monday to Sunday.
- **Number of Visits** : The number of visits of the selected visitor for each device.

Figure 5-87 Configure time



Step 5 In the **Certificate** section, you can issue a card to the visitor, set the visitor face image, and generate visitor pass.

Table 5-19 Certificate description

Tab	Description
Card	Issue a card to a visitor. You can issue cards by entering card number manually or by using a card reader. A card number comes with 8–16 numbers. Only second-generation access control devices support 16-digit card numbers. When a card number is less than 8 numbers, the system will automatically add zeros prior to the number to make it 8 digits. For example, if the provided number is 8004, it will become 00008004. If there are 9-16 numbers, the system will not add zero to it. ● Issue cards by entering card numbers manually: Click Add , enter the card number, and then click OK. ● Issue cards by using a card reader: Click  , select a card reader or device, and then click OK. Swipe card through the reader or device, and then a new card will be issued.
Face	Set the face image of the visitor. 1. Click Add. 2. Click Select from Local Folder to select a picture, or click Snapshot to take a photo (if a camera is detected on your computer).
Visitor Pass	Click Generate to generate a QR code for the pass. ● The QR code includes the visitor virtual ID (randomly generated by the system) and the QR code encryption information. The defined appointment period is sent to the access control device through the virtual ID. ● The QR code is valid within the defined appointment period. ● You can click Download Pass to download the QR code, or you can click Email Pass to send it to the visitor by email.

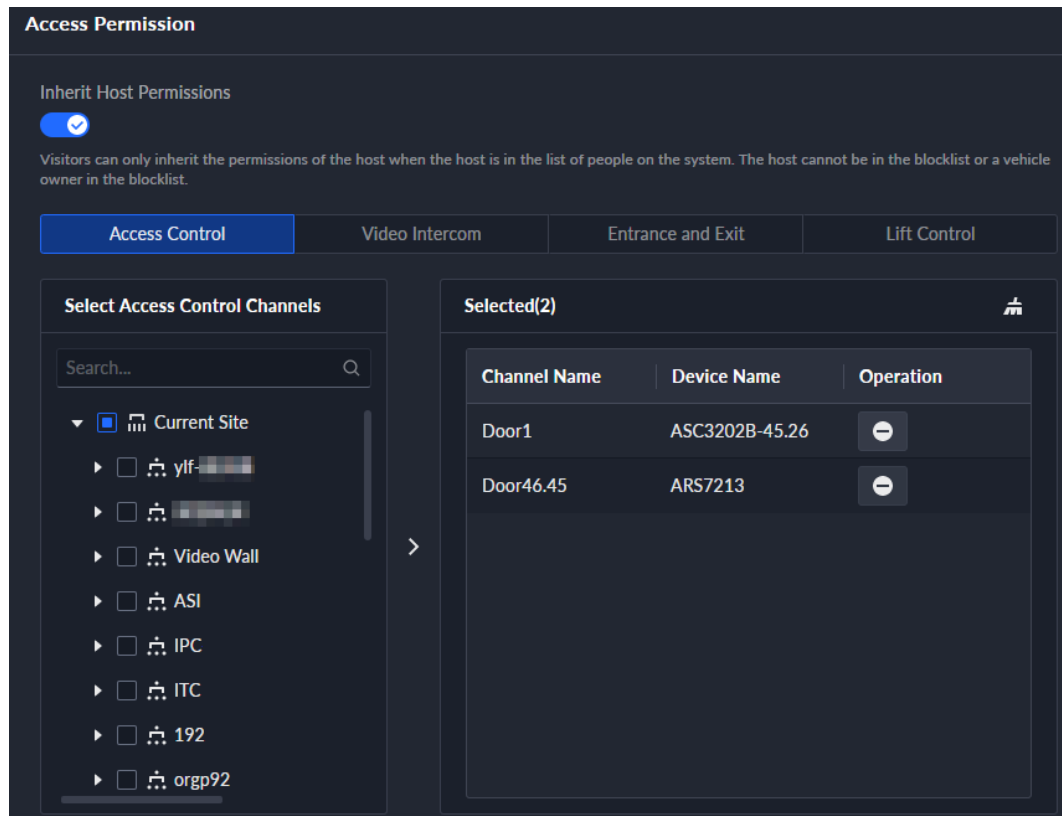
Step 6 Click the **Access Permission** tab, and then select access permissions for the visitor.



If you want to set video intercom devices and entrance and exit permissions, you must set host room number and number plate for the visitor.

By enabling **Inherit Host Permissions**, the visitor can share the access permissions with the host, but be noted that the host must be in the list of people on the system, and cannot be in the blocklist or the owner of a vehicle in the blocklist.

Figure 5-88 Access permission



Step 7 Click **OK**.

After appointment, the visitor status changes to **Pre-booked Appointment**.

Step 8 (Optional) Proceed to check in, or click  to cancel the appointment as the screen instructs.

Related Operations

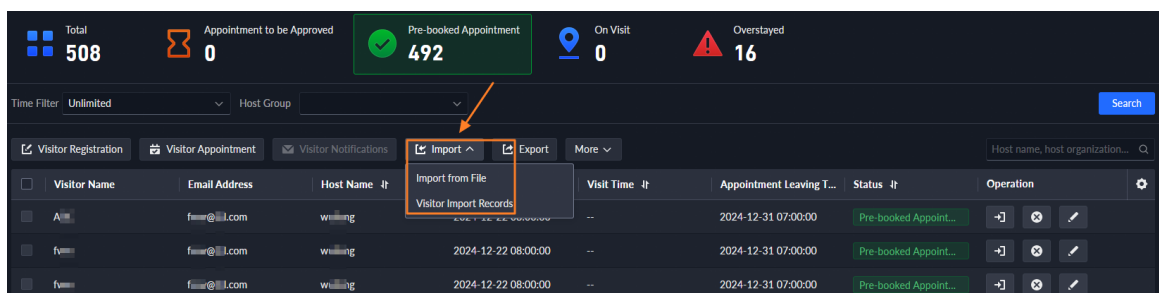
Click the **Pre-booked Appointment** tab, and then you can import the visitor appointment information in batches.

1. Select **Import** > **Import from File**.



- A imported file cannot exceed 1 GB, 1 file can be imported at a time, and a maximum of 1,000 visitors can be imported at a time.
- Click **Visitor Import Records**, and then you can view the import records.

Figure 5-89 Import visitor appointment information in batches



2. Click **Download Template**, and then fill in the information according to the template requirements.

3. Click **Import File** to import the completed template to the platform.

5.4.3.4.2 Creating Appointment by Visitors

After the platform administrator generates the visitor appointment link on the platform, visitors can access the link and fill out their appointment information. After approval, the visitor can access with the visit credential.

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Visitor**.



You can also go to the **Visitor Config** page by selecting **Access Management > Visitor**, and then clicking  at the lower-left side.

- Step 2** Select **Visitor Appointment Config > Create Appointment**.

- Step 3** (Optional) Enable **Appointment Review Config on Visitor Terminal** as needed. After being enabled, appointments made through the visitor terminal must be approved by the defined approver before the visitors can access; if not enabled, then no approval is required.

- Step 4** Select the approver.

When selecting **Host Approval**, the host will receive an email notification for approval; when selecting **Role**, the defined role will receive an approval notification in the platform's notification center at the upper right.

- Step 5** Enable **LAN Access Entry** or **WAN Access Entry**, click **Send Email**, and then set the visitor's email. The platform will send an invitation link to the visitor's email through LAN or WAN.



- Click **Regenerate** to generate a new link. The original link will be invalid.
- Click  to copy the link.

- Step 6** (Optional) Click  to download the QR code; click , and then select the printer to print the QR code.

- Step 7** Click **Save**.

- Step 8** The visitor clicks the link or scans the QR code to fill in the information, including their name, email, company (department), room number, appointment arrival time, and appointment leaving time, and the host's name, email address, license plate number, phone number, and more.



The host must be a person that has been added to the platform in  **> Person and Vehicle Info > Person List**.

Figure 5-90 Create appointment


Visitor Created Appointment System

Create Appointment

Host Info

Host Name

Host Email Address

Host Organization (Department)

Host Room No.

Please enter the room number in the following format: Building # Room No. or Building # Unit # Room No., and you can contact the host to get information on the room number.

Visit Details

Visitor Name

Email Address

Visitor Company

ID Type

ID Card

ID No.

Phone No.

Plate No.

Reason for Visit

Appointment Arrival Time

2024-06-28 12:01:08

Appointment Leaving Time

2024-06-28 14:01:08

Face


OK

Reset

Step 9 Approve the appointment.

Step 10 The visitor visits the host with the visit credential received through the email.

5.4.3.4.3 Appointment Invited by Host

After the platform administrator generates a visitor appointment link on the platform, visitors can access the link and verify the email of the host. They can then fill out their appointment information to make an appointment.

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Visitor**.



You can also go to the **Visitor Config** page by selecting **Access Management** > **Visitor**, and then clicking  at the lower-left side.

Step 2 Select **Visitor Appointment Config > Host Invitation**.

Step 3 (Optional) Enable **Approved by**, and select the approval role. The appointment must be approved by the user of the selected role before the visitor can visit; if not enabled, no approval is required.



If approval role is configured, the role can approve the appointment from **Access Management > Visitor > Visitor Management > Appointment to be Approved**. For details, see "5.4.3.5 Reviewing Appointment".

Step 4 Enable **LAN Access Entry** or **WAN Access Entry**, click **Send Email**, and then set the visitor's email. The platform will send an invitation link to the visitor's email through LAN or WAN.



- Click **Regenerate** to generate a new link. The original link will be invalid.
- Click  to copy the link.

Step 5 (Optional) Click  to download the QR code; click , and then select the printer to print the QR code.

Step 6 Click **Save**.

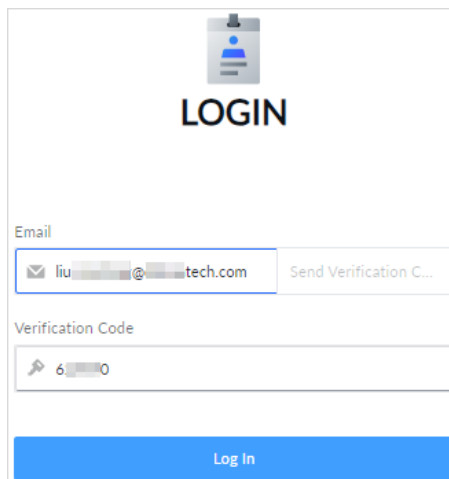
Step 7 The visitor clicks the link or scans the QR code to fill in the information.

1. Enter the email address of the host, and then the system will send a verification code to that email address.



You need to configure the person's email from **Person and Vehicle Info > Person List**; otherwise, the verification code cannot be sent.

Figure 5-91 Verify email of host



2. After entering the verification code, the visitor can select **Add Invitation** to proceed.



Click **My Invitation** to view the invitation records.

3. Fill out visitor information, including their name, email, company, reason for visit, license plate number, phone number, appointment arrival time, appointment leaving time, and more.

Figure 5-92 Host invitation


Host Invitation System

← Add Invitation

Visit Details

* Visitor Name

* Email Address

Visitor Company

Reason for Visit

ID Type

ID Card ▼

ID No.

Plate No.

Phone No.

* Appointment Arrival Time

2024-06-28 12:05:39

* Appointment Leaving Time

2024-06-28 14:05:39

OK

Cancel

4. Click **OK**.

Step 8 The approver approves the appointment (if approver has been configured).

Step 9 The visitor visits the host with the visit credential received through the email.

5.4.3.5 Reviewing Appointment

After the appointment is approved, the system will send the visit credential to the email of the visitor, and then the visitor can access through the credential.

Prerequisites

Review is enabled in **Visitor Appointment Config**. For details, see "4.7.2 Configuring Visit Settings".

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click  > **Access Management** > **Visitor** > **Visitor Management**.
- Step 2 Click the **Appointment to be Approved** tab.
- Step 3 Review the appointment.
- Click  to approve the appointment. After this, the **Status** changes to **Pre-booked Appointment**.
 - Click  to decline the appointment.
 - Click  to send the email to notify visitors configured through  > **Visitor** > **Visitor Appointment Config**.
The host will also be reminded to give their approval if **Host Approval** is enabled in  > **Visitor** > **Visitor Appointment Config** > **Create Appointment**.

5.4.3.6 Checking In

When a visitor with an appointment arrives, you need to confirm their information and give them access permission. On-site registration is supported when there is a walk-in visitor. Visitors can get access by swiping card, face recognition or scanning QR code.

- Step 1 Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Visitor** > **Visitor Management**.
- Step 2 Enter the information of the visitor.
- If a visitor has an appointment, find their visitor information, and then click .
 - If a visitor does not have an appointment, click **Visit Registration**, and then configure visitor information. For details, see "5.4.3.4 Visitor Appointment".
- Step 3 Click **OK**.
After checking in, the visitor status changes to **On Visit**.

5.4.3.7 Checking Out

When visitors are leaving, remove their access permissions.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click  > **Access Management** > **Visitor** > **Visitor Management**.
- Step 2 Click the **On Visit** tab, and then click .
- Step 3 Click **OK** to remove access permission.
If you have issued a physical card to a visitor, make sure that the visitor returns the card before leaving.

Related Operations

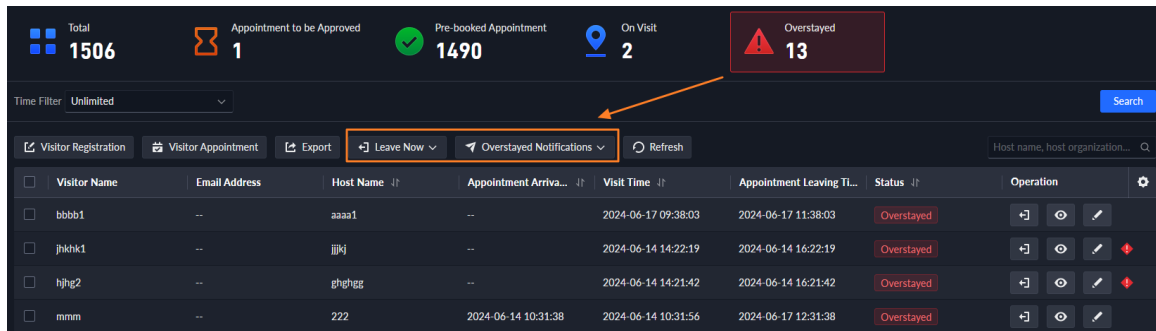
Click the **Overstayed** tab, and then you can check out visitors that are overstayed in batches and send notifications to them.

- Check out in batches: Select **Leave Now** > **Select All to Leave** to remove access permissions of all overstayed visitors; or you can select visitors first, and then select **Leave Now** > **Select to Leave** to remove access permissions of just the selected visitors.

- Send notifications: Select **Overstayed Notifications** > **Send Now/Auto Send**, select the receiver or enter the receiver's email and press Enter, and then click **OK**, to send notifications to the specified receivers.

For **Auto Send**, you need to set the time to send the email each day.

Figure 5-93 Operations related to overstayed visit



5.4.3.8 Overstayed Visit

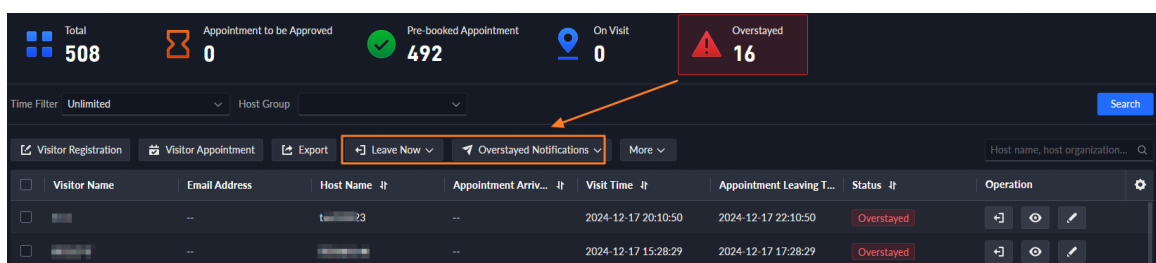
The visitor status changes to **Overstayed** if visitors do not check out within the appointment leaving time. In this case, you can check out these visitors in batches, or send them notifications to remind them of the overstayed status.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click  > **Access Management** > **Visitor** > **Visitor Management**.
- Step 2** Click the **Overstayed** tab, and then you can check out visitors that are overstayed in batches and send notifications to them.
 - Check out in batches: Select **Leave Now** > **Select All to Leave** to check out all overstayed visitors; or you can select visitors first, and then select **Leave Now** > **Select to Leave** to remove access permissions of just the selected visitors.
 - Send notifications: Select **Overstayed Notifications** > **Send Now/Auto Send**, select the receiver or enter the receiver's email and press Enter, and then click **OK**, to send notifications to the specified receivers.

For **Auto Send**, you need to set the time to send the email each day.

Figure 5-94 Operations related to overstayed visit



5.4.3.9 Visit Records

Search for visit records, and view visitor details and card swiping records.

- Step 1** Log in to the DSS Client. On the **Home** page, click  > **Access Management** > **Visitor** > **Visitor Records**.

Step 2 Set search conditions, such as visitor name, phone name, email address, card number, ID number, host name, host group, host organization (department), appointment arrival time or visit time (60 days before at most), status (unlimited, visitor left, appointment cancelled, access denied, and appointment expiration due to no arrival).

Step 3 Click **Search**.

The results are displayed.



In addition to entering the card number, you can also click , select a card reader and then get the card number by swiping card.

Step 4 Click  to view visitor details and card swiping records.

5.5 Parking Lot

You can monitor vehicles that enter and exit the parking lot in real time, view vehicle information, and search for on-site vehicles, exit vehicles and snapshot records, and manage parking lots intuitively through their different layers.

5.5.1 Statistics Dashboard

The platform automatically generates data on parking lots, including real-time data on the current day, number of vehicles entering and exiting parking lots, parking turnover rate, and rate of parking space usage.

Log in to the DSS Client. On the **Home** page, click  > **Parking Lot** > **Statistics Dashboard**. The data covers only the parking lots the current user has access to. Administrators can access all parking lots by default.

Figure 5-95 Statistics dashboard

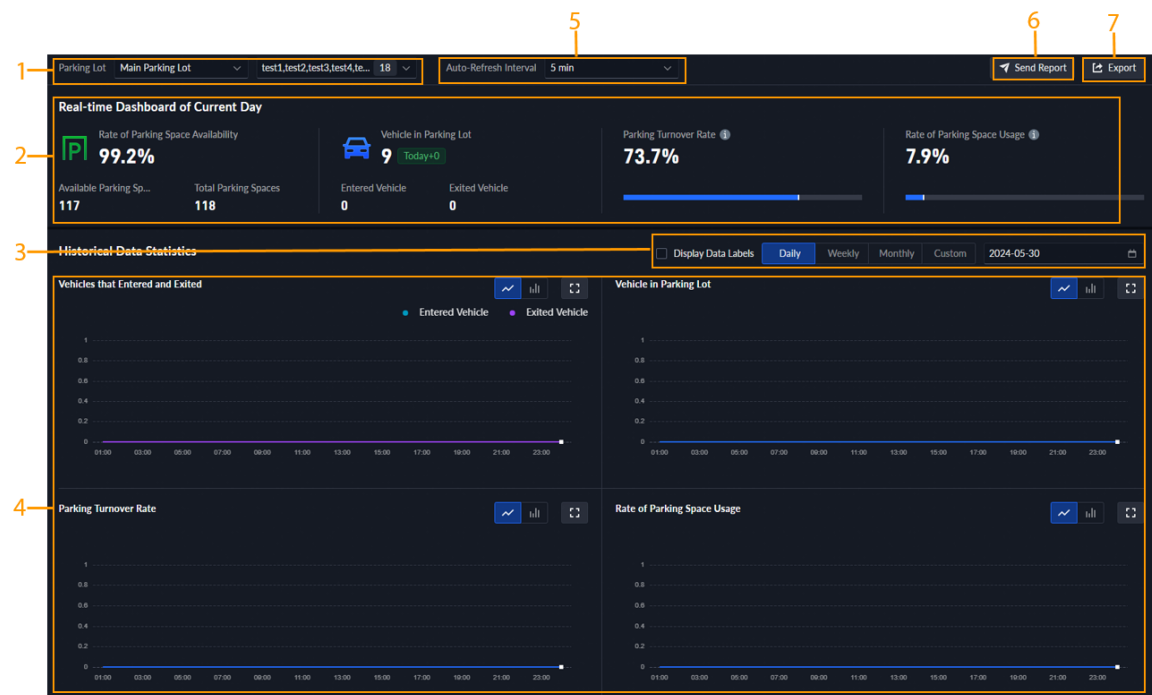


Table 5-20 Parameter description

No.	Parameter	Description
1	Parking lots	Select the parking lots you want to view data on, and the numbers of parking lots, ANPR channels, entrances, and exits.
2	Real-time data of the current day	Displays the real-time data on the parking lots you selected.
3	Counting period	Configure a period you want to view data on. The graphs will adapt accordingly.  The platform only displays the number of vehicles in parking lots for each day.
4	Different types of data presented in graphs	Displays different types of data within the counting period you configured. ● Vehicles that Entered and Exited : Vehicles that have entered and exited the parking lots. ● Vehicle in Parking Lot : Vehicles that were inside the parking lots. ● Parking Turnover Rate : Parking turnover rate = The number of vehicles that parked during the counting period/the number of parking spaces. The higher the parking turnover rate, the higher the number of vehicles parked in the parking lot. ● Rate of Parking Space Usage : Rate of Parking Space Usage = The total parking duration of all the vehicles/The number of parking spaces in the parking lot × The counting period. The higher the rate of parking space usage is, the better the parking lot is being used.
5	Auto-Refresh Interval	Select how often the data will be updated.
6	Send Report	Send the reports of statistics dashboard, entry record, exit records and parking space records to the receivers through email.
7	Export a report	Export the data of statistics dashboard, entry record, exit records and parking space records as a PDF file to your computer.

5.5.2 Entrance and Exit Monitoring

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Parking Lot** > **Entrance and Exit Monitoring**.

Step 2 Select the number of windows you want from .

Step 3 Click **Select Entrance and Exit.**, select an entrance or exit point, and then click **OK**.

The real-time video of that point will be opened in the window.

Figure 5-96 Monitor entrances and exits

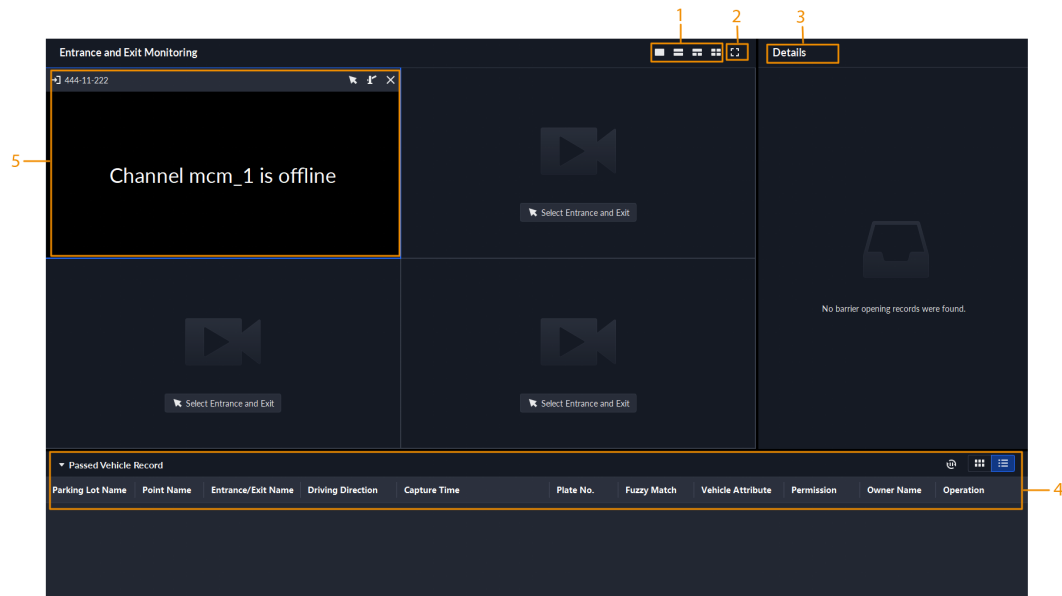


Table 5-21 Page description

No.	Description
1	Select the number of windows you want. Each window can display the real-time video of one entrance or exit point.
2	Full screen mode.
3	Displays records of barriers not opened.
4	All entrance and exit records.
5	The real-time video of an entrance or exit point. - Click  to open the real-time video of another entrance or exit point in the window. - Click  to open the barrier for vehicles. ◇ Open without Recording Plate Info : Open the barrier for vehicles without recording their plate numbers. If you select Count Parking Spaces at the same time, the number available parking spaces in the parking lot will decrease or increase depending on whether the vehicles are entering or exiting. This operation will not generate an enter or leave record.  You need to enable the parking space counting during configuration, and set the parking space counting mode as count parking spaces by entering and exiting vehicles. ◇ Open and Record Plate Info : This is applicable to when the ANPR cameras cannot recognize the number plates. You can manually enter the number plate, and a snapshot will be taken, and then the platform will generate an entrance or exit record.

5.5.3 Searching for Records

Search for entry and exit records, forced exit records, parking records, and snapshot records.

5.5.3.1 Searching for Entrance Records

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Parking Lot** > **Info Search**.

Step 2 Click the **Entrance Records** tab.

Step 3 Configure the search conditions, and then click **Search**.

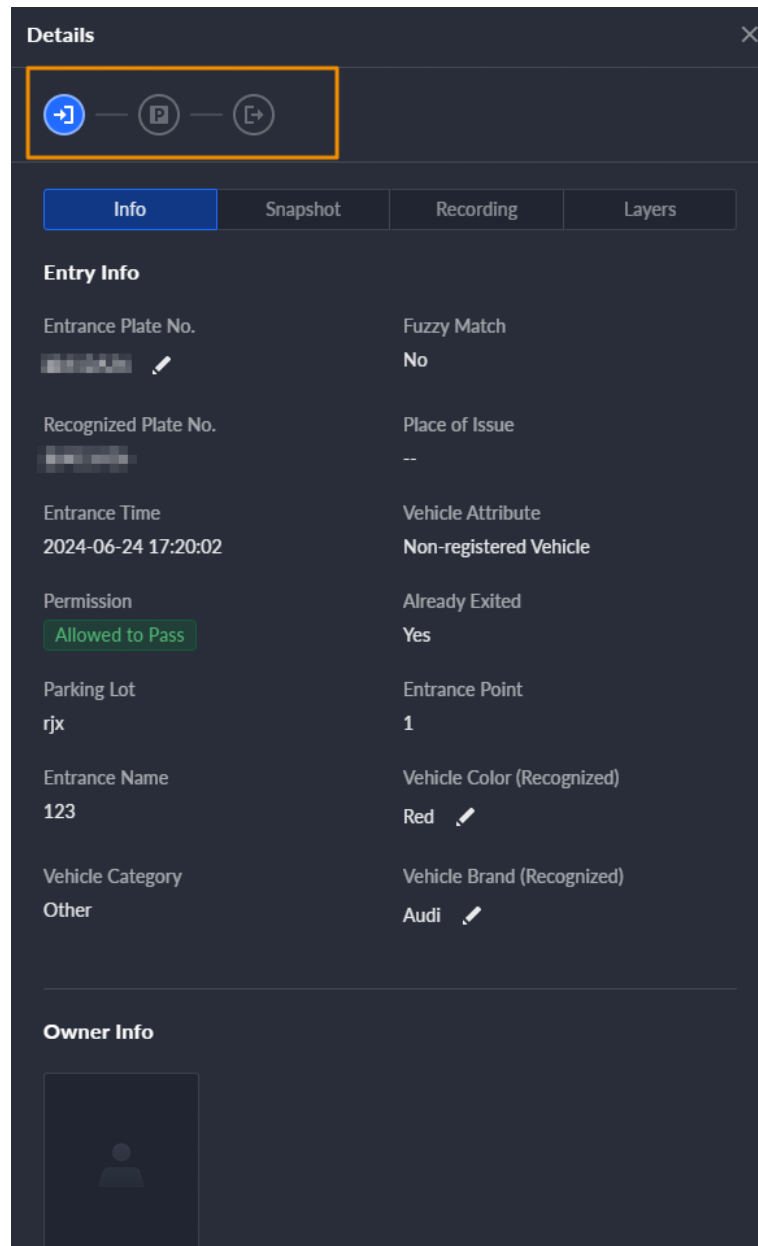


Click **Show More**, and then you can search by vehicle owner, company, person group, and more.

Step 4 Manage the records.

- Click the image, and then a bigger one will be displayed.
- Double-click a record or click , and the detailed information is displayed on the right. Click the icon to view the corresponding detailed information. Click the play icon to play the recorded video, and then click  to download it. Click  to modify the information of the vehicle, such as the plate number, brand and color.

Figure 5-97 View details



For the dual camera mode, click each channel to view the information it captured.

Click **Snapshot** or **Recording** to view the snapshots or recordings.

Supports AcuPick that can automatically recognize targets and then search for it in DeepXplore.

- Click **Layer Info** to view the location of the channel that captured the vehicle on the layer.
- Forced exit.

If a vehicle has exited but it is displayed as inside the parking lot, click  to record it as exited the parking lot. When parking space counting by entering and exiting vehicles is enabled for the parking lot, and the vehicle will be counted for available parking space, this operation will add an available parking space to the parking lot.

- Export records.

Select the records to be exported, click **Export**, and then export them according to the on-screen instructions. You can also click **Export**, and then export all records according to the on-screen instructions.

- Click , and then select the items to be displayed.

5.5.3.2 Searching for Exit Records

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Parking Lot** > **Info Search**.

Step 2 Click the **Exit Records** tab.

Step 3 Configure the search conditions, and then click **Search**.

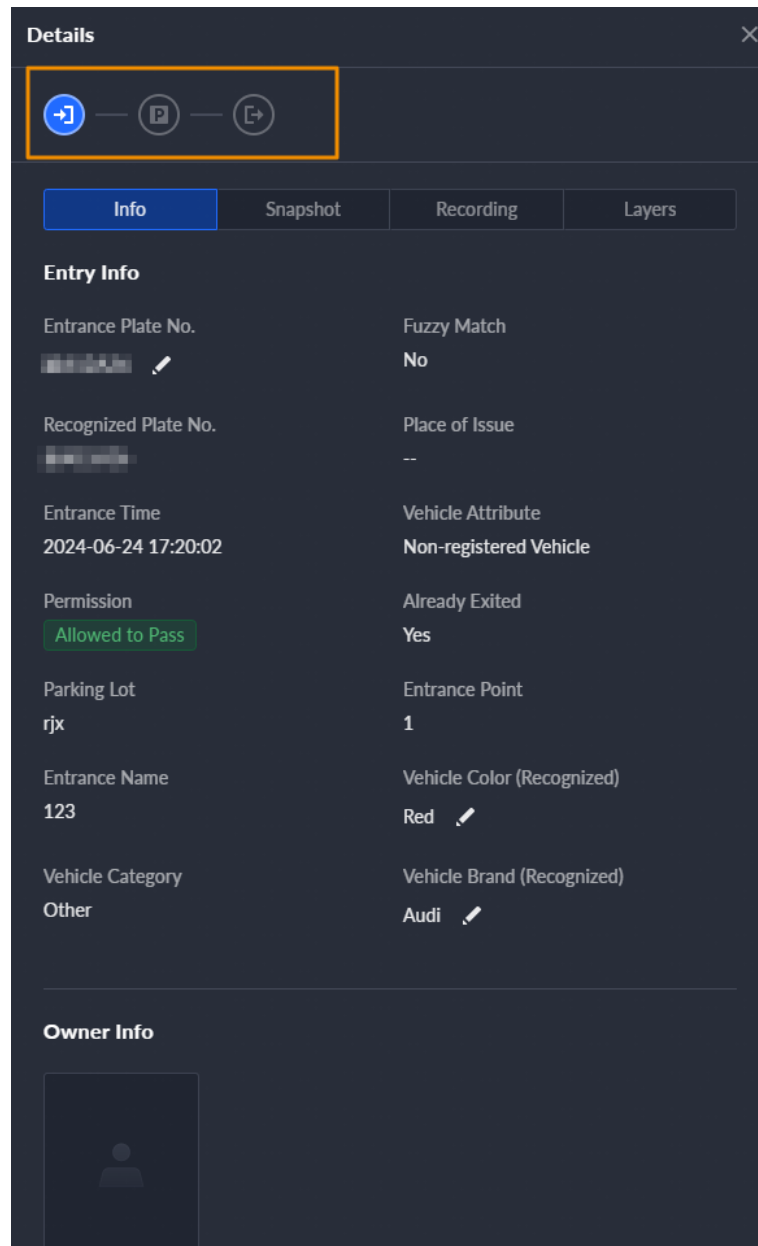


Click **Show More**, and then you can search by vehicle owner, company, person group, and more.

Step 4 Manage the records.

- Click the image, and then a bigger one will be displayed.
- Double-click a record or click , and the detailed information is displayed on the right. Click the icon to view the corresponding detailed information. Click the play icon to play the recorded video, and then click  to download it. Click  to modify the information of the vehicle, such as the plate number, brand and color.

Figure 5-98 View details



For the dual camera mode, click each channel to view the information it captured.

Click **Snapshot** or **Recording** to view the snapshots or recordings.

Supports AcuPick that can automatically recognize targets and then search for it in DeepXplore.

- Click **Layer Info** to view the location of the channel that captured the vehicle on the layer.
- Export records.

Select the records to be exported, click **Export**, and then export them according to the on-screen instructions. You can also click **Export**, and then export all records according to the on-screen instructions.

- Click , and then select the items to be displayed.

5.5.3.3 Searching for Forced Exit Records

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Parking Lot** > **Info Search**.

Step 2 Click the **Forced Exit Records** tab.

Step 3 Configure the search conditions, and then click **Search**.

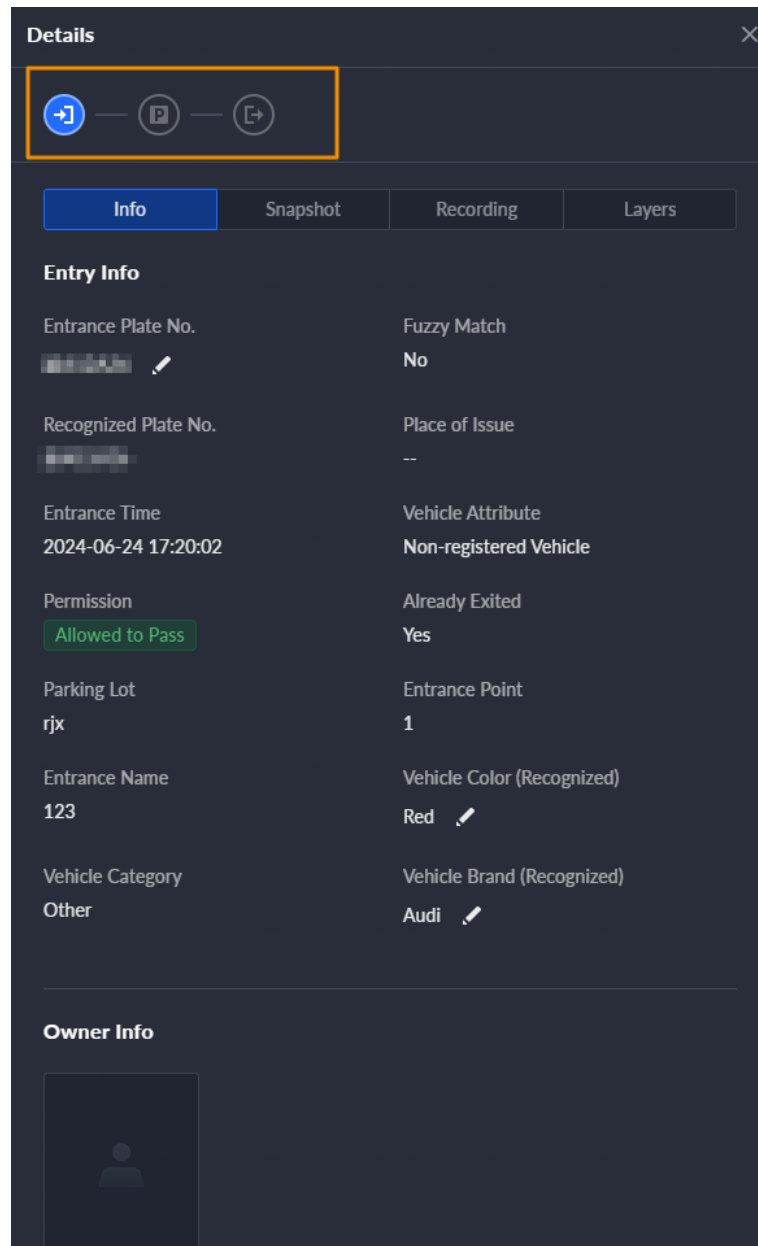


Click **Show More**, and then you can search by vehicle owner, company, person group, and more.

Step 4 Manage the records.

- Click the image, and then a bigger one will be displayed.
- Double-click a record or click , and the detailed information is displayed on the right. Click the icon to view the corresponding detailed information. Click the play icon to play the recorded video, and then click  to download it. Click  to modify the information of the vehicle, such as the plate number, brand and color.

Figure 5-99 View details



For the dual camera mode, click each channel to view the information it captured.

Click **Snapshot** or **Recording** to view the snapshots or recordings.

Supports AcuPick that can automatically recognize targets and then search for it in DeepXplore.

- Click **Layer Info** to view the location of the channel that captured the vehicle on the layer.
- If a vehicle is inside the parking lot but it is displayed as exited, click  to record it as inside the parking lot. When parking space counting by entering and exiting vehicles is enabled for the parking lot, and the vehicle will be counted for available parking space, this operation will subtract an available parking space for the parking lot.
- Export records.

Select the records to be exported, click **Export**, and then export them according to the on-screen instructions. You can also click **Export**, and then export all records according to the on-screen instructions.

- Click , and then select the items to be displayed.

5.5.3.4 Searching for Parking Records

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Parking Lot** > **Info Search**.

Step 2 Click the **Parking Records** tab.

Step 3 Configure the search conditions, and then click **Search**.



Click **Show More**, and then you can search by vehicle owner, company, person group, and more.

Step 4 Manage the records.

- Click the image, and then a bigger one will be displayed.
- Double-click a record or click , and the detailed information is displayed on the right, including entry and exit records. Click the play icon to play the recorded video, and then click  to download it.

For the dual camera mode, click each channel to view the information it captured.

- Click **Layer Info** to view the location of the channel that captured the vehicle on the layer.
- Export records.

Select the records to be exported, click **Export**, and then export them according to the on-screen instructions. You can also click **Export**, and then export all records according to the on-screen instructions.

- Click , and then select the items to be displayed.

5.5.3.5 Searching for Capture Records

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Parking Lot** > **Info Search**.

Step 2 Click the **Capture Records** tab.

Step 3 Configure the search conditions, and then click **Search**.

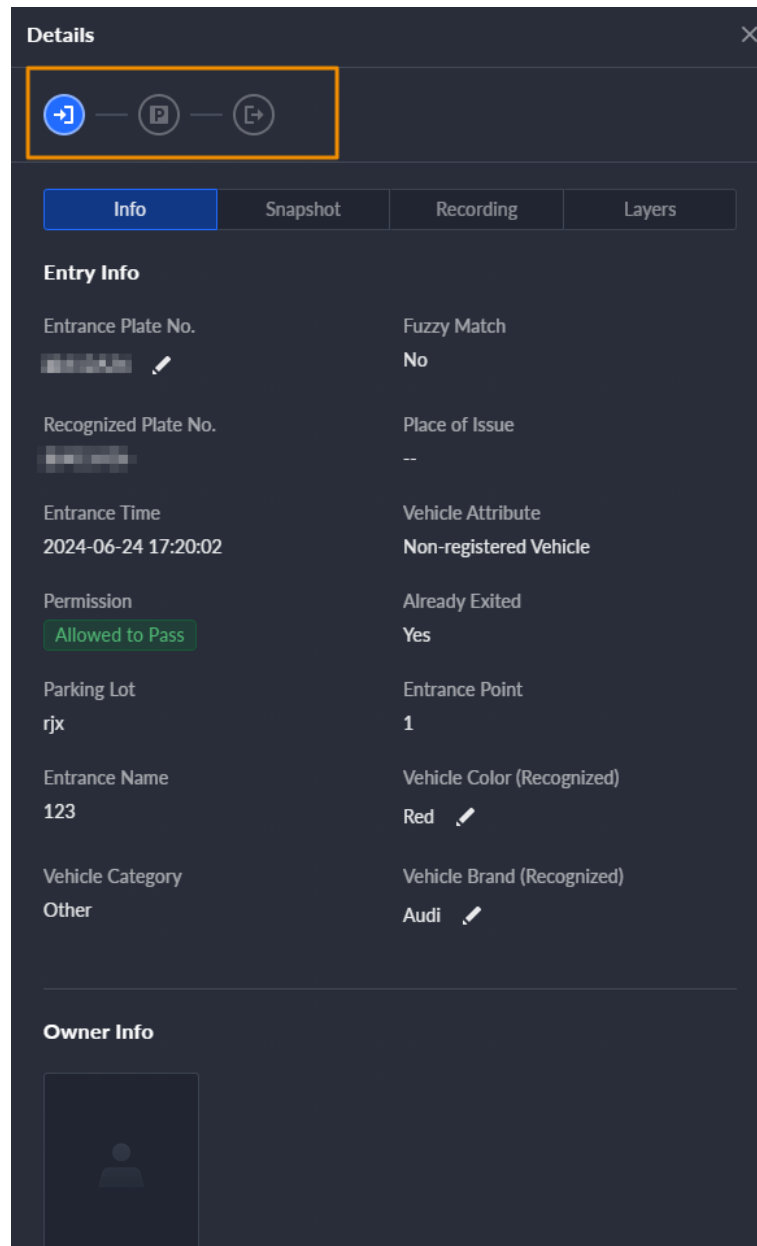


Click **Show More**, and then you can search by vehicle owner, company, person group, and more.

Step 4 Manage records.

- Click the image, and then a bigger one will be displayed.
- Double-click a record or click , and the detailed information is displayed on the right. Click the icon to view the corresponding detailed information. Click the play icon to play the recorded video, and then click  to download it. Click  to modify the information of the vehicle, such as the plate number, brand and color.

Figure 5-100 View details



For the dual camera mode, click each channel to view the information it captured.

Click **Snapshot** or **Recording** to view the snapshots or recordings.

Supports AcuPick that can automatically recognize targets and then search for it in DeepXplore.

- Restore entry.

If **Yes** is displayed under **Exited** when the vehicle is still in the parking lot, click  to change the status to **No**.

- Export records.

Select the records to be exported, click **Export**, and then export them according to the on-screen instructions. You can also click **Export**, and then export all records according to the on-screen instructions.

- Click , and then select the items to be displayed.

5.5.4 Parking Information

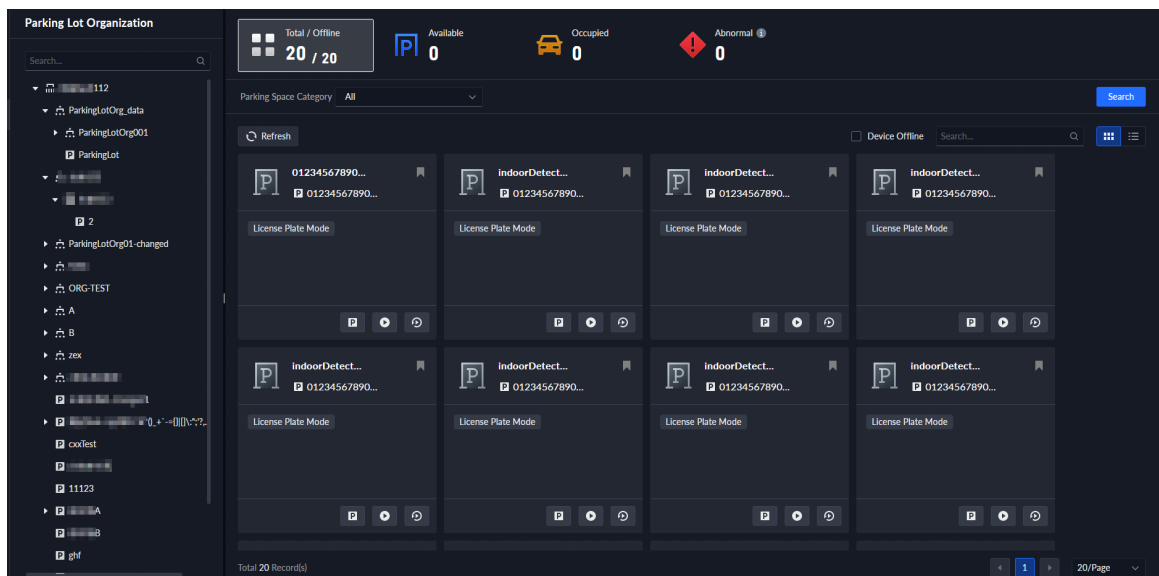
View parking space status, parking space information, and vehicle parking information.

5.5.4.1 Parking Space Status

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click  > **Parking Lot** > **Parking Info**.
- Step 2** Click **Parking Space Status**, and then select a parking organization.

Figure 5-101 Parking space status



- Step 3** Configure the search condition to view the parking space information.

Related Operations

- Click **Total/Offline**, **Available**, **Occupied**, and **Abnormal** to view the corresponding parking space.
- Click **Device Offline** to view the offline device.
- Click  to switch between list mode or card mode.
- Configure the parking space category, and then click **Search** to search for categorized or uncategorized parking spaces.
- Click  to view the video of channel.
- Click  to view the central or device recording.
- Click  to view the parking record.

5.5.4.2 Parking Information On Parking Spaces

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click  > **Parking Lot** > **Parking Info**.
- Step 2** Click **Parking Info on Parking Spaces**, and then configure the search conditions.
- Step 3** Click **Search**.

Figure 5-102 Search results

Filter

Parking Space

Unlimited

Day Type

Day

Time

2024-12-08

Parking Duration

0 - 24 H

Search

Reset

If the information on the selected parking space cannot be found, it indicates that the space did not belong to the current parking lot during the search.

Total Parking Spaces

114

Average Parking Duration

38min(s)

Longest Parking Duration

1day(s)

Shortest Parking Duration

0min(s)

Export

Send Report

Parking Space ID	Parking Space Category	Parking Lot	Organization	Total Parking Time
0123456789012345678901234567890...	Uncategorized Parki...	0123456789012345678901234567890...	0123456789012345678901234567890...	0min(s)
123153_1	Uncategorized Parki...	cooTest	112	0min(s)
123153_10	Uncategorized Parki...	cooTest	112	0min(s)
123153_11	Uncategorized Parki...	cooTest	112	0min(s)
123153_12	Uncategorized Parki...	cooTest	112	0min(s)
123153_2	Uncategorized Parki...	cooTest	112	0min(s)
123153_3	Uncategorized Parki...	cooTest	112	0min(s)
123153_4	Uncategorized Parki...	cooTest	112	0min(s)
123153_5	Uncategorized Parki...	cooTest	112	0min(s)
123153_6	Uncategorized Parki...	cooTest	112	0min(s)
123153_7	Uncategorized Parki...	cooTest	112	0min(s)
123153_8	Uncategorized Parki...	cooTest	112	0min(s)
123153_9	Uncategorized Parki...	cooTest	112	0min(s)
C01	Business	ParkingLot-TEST	ORG-TEST	0min(s)

Total 114 Record(s)

1

2

3

4

5

6

20/Page

Related Operations

- Click **Export** to export the records by following the on-screen prompts.
- Click **Send Report**, configure the subject, receivers and content, and then click **OK**.

5.5.4.3 Parking Information On Vehicles

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click  > **Parking Lot** > **Parking Info**.
- Step 2** Click **Parking Space on Vehicles**.
- Step 3** Configure the search conditions, and then click **Search**.

Figure 5-103 Parking information on vehicles

Filter		Export Send Report							
Parking Lot Organization	Unlimited								
Entrance Time	12/09 00:00:00 - 12/09 23:59:59								
Vehicle Attribute	All								
Plate No.									
☒ Complete Plate No.									
Parking Duration	Unlimited								
Place of Issue									
Show More									
		Plate No.	Parking Lot	Organization	Vehicle Attribute	Entrance Time	Exit Time	Operation	
		Unrecognized	111	112	Non-registered Vehicle	2024-12-09 18:38:15	2024-12-09		
		Unrecognized	222	112	Non-registered Vehicle	2024-12-09 18:38:15	2024-12-09		
		Unrecognized	111	112	Non-registered Vehicle	2024-12-09 18:01:20	2024-12-09		
		Unrecognized	222	112	Non-registered Vehicle	2024-12-09 18:01:20	2024-12-09		
		Unrecognized	111	112	Non-registered Vehicle	2024-12-09 17:55:09	2024-12-09		
		Unrecognized	222	112	Non-registered Vehicle	2024-12-09 17:55:09	2024-12-09		
		Unrecognized	111	112	Non-registered Vehicle	2024-12-09 16:43:45	2024-12-09		
		Unrecognized	222	112	Non-registered Vehicle	2024-12-09 16:43:45	2024-12-09		
		AB12345	yff	112	Non-registered Vehicle	2024-12-09 16:35:02	2024-12-09		
		A00002	yff	112	Non-registered Vehicle	2024-12-09 11:36:46	Did Not Exit		
		A00002	yff	112	Non-registered Vehicle	2024-12-09 11:34:12	Did Not Exit		
		A00002	yff	112	Non-registered Vehicle	2024-12-09 11:31:17	Did Not Exit		
		A00001	yff	112	Non-registered Vehicle	2024-12-09 11:31:14	Did Not Exit		
		A00001	yff	112	Non-registered Vehicle	2024-12-09 11:29:32	Did Not Exit		

Related Operations

- Click **Export** to export the records by following the on-screen prompts.
- Click **Send Report**, configure the subject, receivers and content, and then click **OK**.

5.5.5 Visualized Parking Lot

Quickly understand your parking lot by viewing the information on the layers.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click  > **Parking Lot** > **Visualized Parking Lot**.
- Step 2** Select a parking lot, and then double-click a layer.
- Step 3** View the information on the layer.

Table 5-22 Operation description

Icon/Parameter	Description
	View the total and available parking spaces on the layer.
	View all the resources on the layer.
	Displays the status of parking spaces.
	Zoom in and out on the layer.
Display Selected Layers	Select which resources you want to display on the layer.
Pane	Click and hold on the layer to select multiple devices. After you select multiple devices, you can perform the following operations: • : View the parking records from the selected devices. • : Open a video player and you can view the real-time video of each device you selected. If you are viewing the real-time video from an entrance or exit point, you can open the barrier. • : Open a video player and you can search for and view the recorded videos from the devices you selected.
Reset	Reset the layer to its default size and position.
Hide Plate No.	Hide the license plate of the vehicles parked in the parking spaces.

5.5.6 Vehicle Location

If vehicle search is configured for parking lots, vehicle owners can find where their vehicles are parked through the vehicle search system. Operations on a computer or phone are similar. This section uses a computer as an example.

Procedure

- Step 1** Go to the link of the vehicle search system in the browser.



For the links and QR codes used to access the vehicle search system, see "4.8.2.4 Vehicle Finder".

Step 2 Search for vehicles.

- Search for vehicles with license plates.

Select **Precise Search**, enter a license plate, and then click **Search** to view the location of the vehicle, including the name of the parking lot, floor number, parking space number, and layer information. If there are multiple results, click one to view its details.



To view layer information of vehicles, you must configure the layer first. For details, see "4.8.2.2 Parking Lot Layer".

- Fuzzy Search

If fuzzy search is enabled and minimum license plate characters for search is configured, enter the corresponding number of license plate, and then click **Search**. If there is only one result, the system will directly display its details. If there are multiple results, click one to view its details.

Figure 5-104 Search results

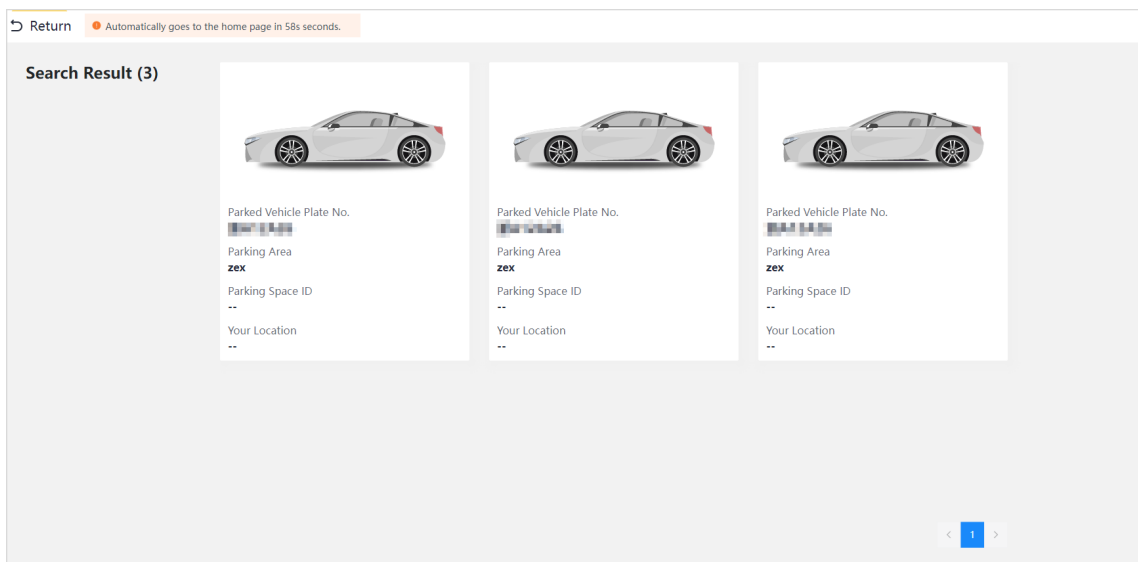
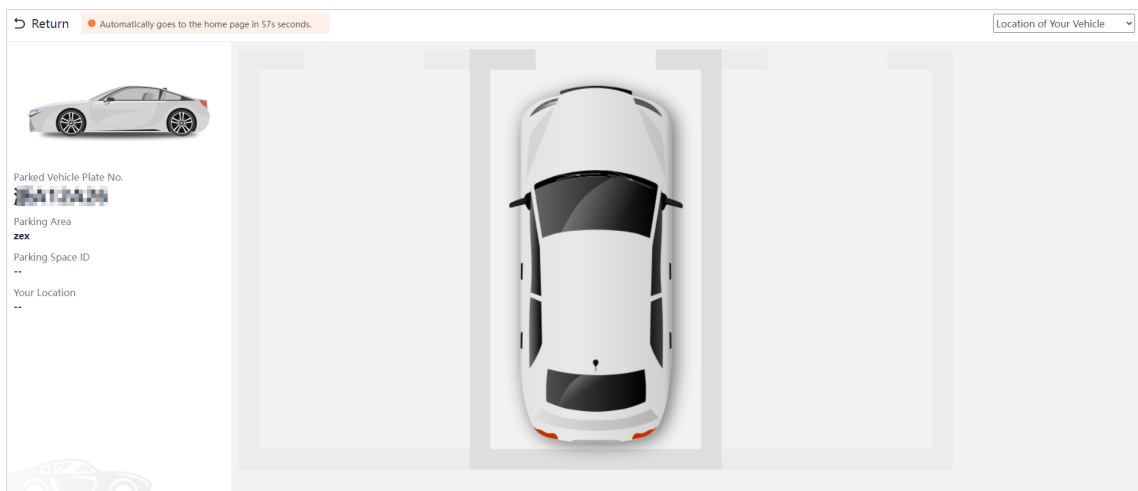


Figure 5-105 Details of search results



- Search for vehicles without license plates.

Click **Unlicensed Vehicle Search** to view all vehicles without licenses. If there is only one result, the system will directly display its details. If there are multiple results, click one to view its details.

5.6 Intelligent Analysis

View real-time and history people counting data, heat maps, number of people in an area, and metadata analysis.

5.6.1 People Counting

View the real-time and historical people count from all the devices in a people counting group.

5.6.1.1 Real-Time Count

Procedure

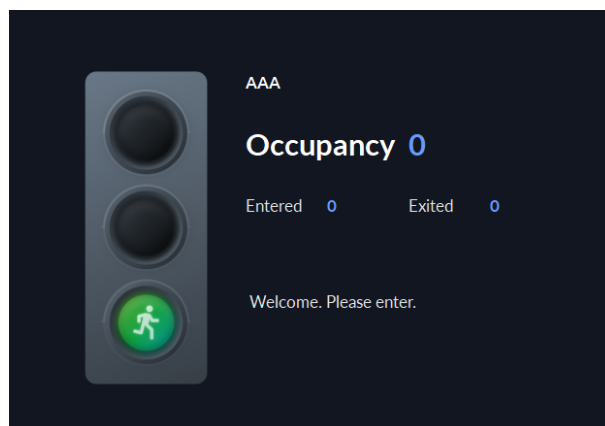
Step 1 Log in to the DSS Client. On the **Home** page, click  > **Intelligent Analysis** >  > **Real-time Count**.

Step 2 Double-click a group or drag it to a window on the right to display its real-time data.


Use the buttons  on the upper-right corner to set the number of windows and to display in full screen.

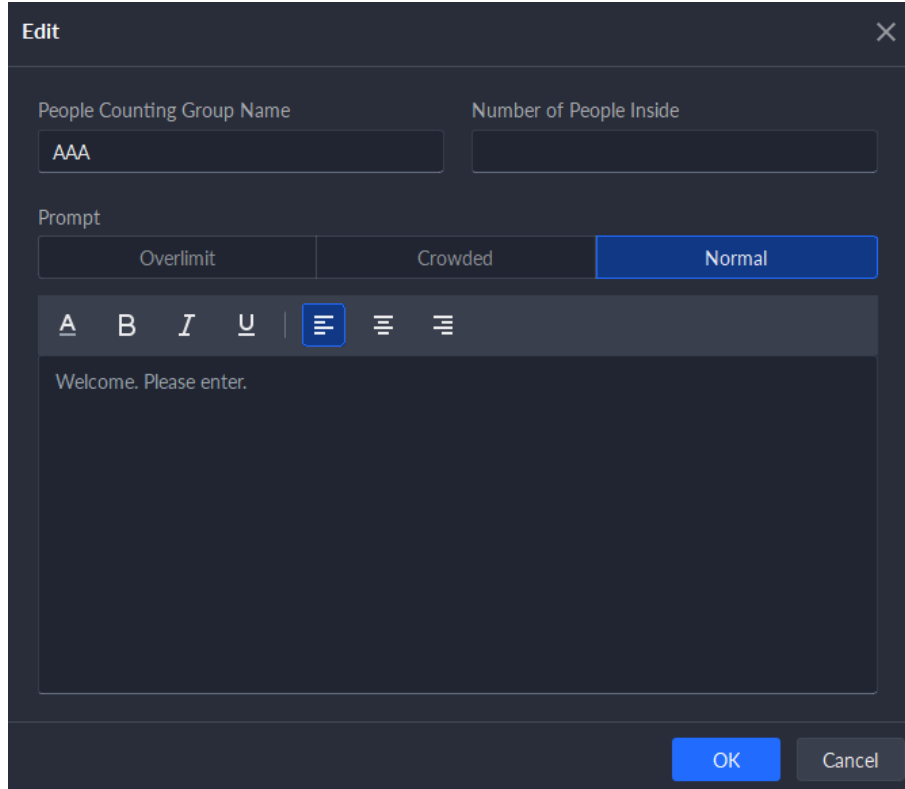
- **Occupancy** : The number of people currently inside this group, which will be reset to the defined value at the defined calibration time.
- **Entered** : The number of people entered this group, which will be reset to zero at the defined calibration time.
- **Exited** : The number of people who left this group, which will be reset to zero at the defined calibration time.
- Color of the light:
 - ◇ Red light: Occupancy $\geq$ overlmit threshold.
 - ◇ Yellow light: Crowded threshold $\leq$ occupancy < overlmit threshold.
 - ◇ Green light: Occupancy < normal threshold.

Figure 5-106 Real-time count



- Step 3 Hover your mouse on the window displaying real-time data, and then click .
- Step 4 You can enter a number of people to overwrite the current data, and customize the content to be displayed for green, yellow and red light.

Figure 5-107 Edit the content and data



- Step 5 Click **OK**.

5.6.1.2 Historical Count

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click  > **Intelligent Analysis** > **People Counting** > **Historical Count**.
- Step 2 Select the groups you want in **Groups**, or select the channels in **Resources**.
- Step 3 Configure the search settings, and then click **Search**.
- **Groups**: Groups are people counting groups, which allow you to combine and calculate the people flow data from multiple rules across different devices and channels. You can search for historical people flow data from one or more people counting groups.
 - **Resources**: Search for historical people flow data from one or more channels. The data from all the rules of a channel will be included.

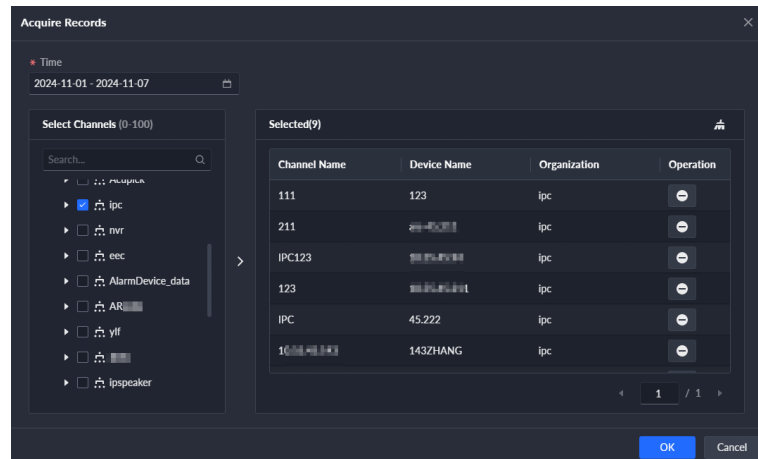


If a device is offline, it will upload all the data to the platform when it is online again.

Related Operations

- **Acquire Retention**: Click **Acquire Retention**, and then enter the login password, select the date and channels to acquire the record.

Figure 5-108 Acquire retention



A single extraction task can select up to 100 channels to extract records for 7 days.

- : Change the display format of the data.



Only daily reports displaying the number of retention.

- **Export**: Export the data into a .zip file to your computer.

5.6.2 Heat Maps

View heat maps generated by devices. A heat map shows the distribution of people flow by different colors, such as red for many people have visited an area and blue for only a few people have visited an area. The platform supports generating general heat maps and advanced heat maps. Only fisheye cameras support advanced heat maps.

Prerequisites

Configure the channel feature for either type of heat maps. For details, see "3.1.2.5.2 Modifying Device Information".

- General heat map: Select the **General Heat Map** from the channel features.
- Advanced heat map: Select the **Advanced Heat Map** from the channel features.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click  > **Intelligent Analysis** > .
- Step 2** Select a channel, and then generate a heat map.



You can generate a heat map with data from up to one month.

- Generate a general heat map.
Configure the time, and then click **Search**.
- Generate an advanced heat map.
 1. Select how you want to generate the heat map, **Number of People** or **Time**.
 2. Configure the threshold.



- When you select **Number of People**, the area with the closest number of people to the threshold will be in red.
- When you select **Time**, the area where people stay for a duration closest to the threshold will be in red.

3. Set the time, and then click **Search**.

Step 3 Click **Export** on the upper-right corner to export the heat map to your PC.

5.6.3 In-Area People Counting

View statistics on the number of in-area people.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Intelligent Analysis** > **In Area No. Analysis**.

Step 2 Select a channel and configure the search settings, and then click **Search**.

- **Report Time** : You can search for **Daily**, **Weekly** or **Monthly** reports.
- **Stay Duration** : The duration that the people stay in the area. You can select from 5 seconds, 30 seconds, 60 seconds or custom. After you select the duration, for example 60 seconds, the list displays the people stay less than 60 seconds and not less than 60 seconds in different colors.



- Custom stay duration can be configured from 0 to 1800 seconds or 0 to 30 minutes.
- If a device is offline, it will upload data within the past 24 hours to the platform when it is online again.

Related Operations

-   : Change the display format of the data.
- **Export** : Export the data to your PC.

5.6.4 Metadata Analysis

View the statistics of faces, human body, motor vehicles, and non-motor vehicles based on channels and export reports to local computer.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Intelligent Analysis** > .

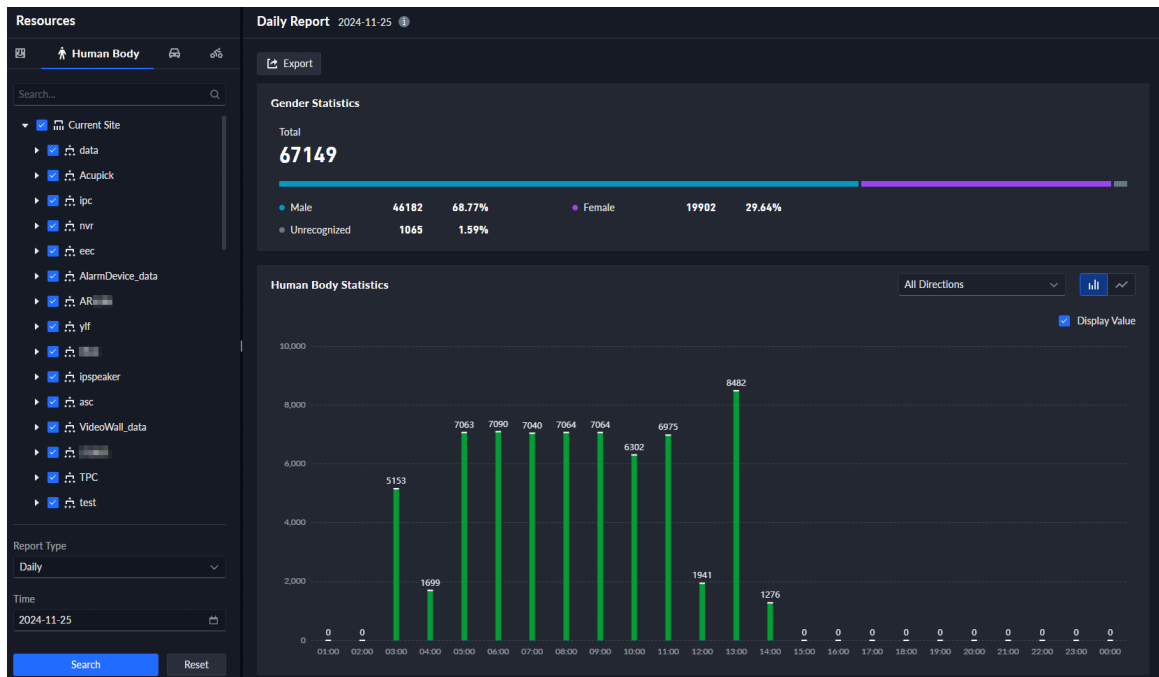
Step 2 Select a channel and configure the search settings, and then click **Search**.

- **Object**: It is **Face** by default, and you can select **Human Body**, **Motor Vehicles** or **Non-motor Vehicle**.
- **Report Type** : You can search for **Daily**, **Weekly**, **Monthly**, **Yearly** or **Custom** reports.



Custom search time can be configured for a maximum of 31 days.

Figure 5-109 Metadata Statistics



Related Operations

- : Change the display format of the data.
- **Export**: Export the data to your PC.
- Select **Display Value**, and then the specific values will be displayed on the bar chart or line chart.
- Configure search conditions such as gender and age to filter search results.

5.7 Intelligent Inspection

The platform supports regularly inspecting devices, such as electrical equipment, or areas, and collect snapshots and data. This can greatly improve inspection efficiency and reduce cost of labor.

Prerequisites

Install the plugin for intelligent inspection. For details, see "2.9 Installing Plugin".

5.7.1 Monitoring Point

View the live videos, basic information, and inspection results of points.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click  > **Intelligent Inspection** > **Point Monitoring**.
- Step 2** Double-click or drag a point to a window on the right to open its live video.
The basic information and results from the last inspection are displayed on the right.

5.7.2 Reviewing Inspection Result

Check and review inspection results.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click  > **Intelligent Inspection** > **Point Monitoring**.
- Step 2 Double-click or drag a point to a window on the right to open its live video.
The basic information and results from the last inspection are displayed on the right.
- Step 3 Click the snapshot on the right, and then the inspection results are displayed, including a snapshot, the live video, and the data collected during inspection.
- Step 4 Click **Review** to review the information, and then click **OK**.
- **Review Result** : Select from **Normal** or **Abnormal**.
 - **Reviewed By** : The name of the current user is displayed. You can change it to another name.
 - **Contact Mode** and **Approval Opinions**: Enter any content you need. These are optional parameters.

Related Operations

Click **Send Email** to send the results to specified email addresses. You can select the email addresses of users on the platform, or manually enter them (you must press Enter after entering an email address). If you want to select the email address of a user, that user must be configured with one. Also, the email server must be configured on the platform to successfully send emails. For details, see "3.2.2 Adding a User" and "7.4.5 Configuring Email Server".

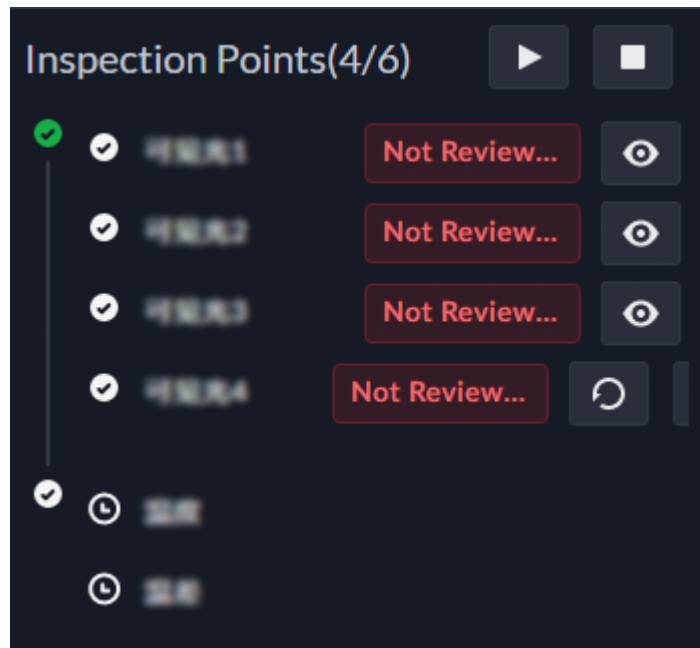
5.7.3 Viewing Real-Time Inspection

View the status of inspection plans, and the real-time videos of points in inspection plans. You can also manually execute inspection plans.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click  > **Intelligent Inspection** > **Real-time Inspection**.
- Step 2 Select an organization, and then all inspection plans under it are displayed on the right.
You can enter keywords in the search box on the upper-right corner to search for certain inspection plans.
- Step 3 Click  to view the information of an inspection plan.
The information includes the basic information, names of points, and live videos. If the inspection is in progress, the progress will also be displayed.

Figure 5-110 Inspection progress



Step 4 Click the name of a point to open its live video.



After the inspection completes, click  to view the inspection details and review the results.

Related Operations

- Click  to stop an inspection plan.
- Click  to execute an inspection plan immediately.
- Click  to pause an inspection plan.
- Click  to inspect again. Click it again to replace the snapshot, end time and inspection results.
- Click  to view snapshots and live video, and review the inspection results.

5.7.4 Searching for Inspection History

Search for and view all execution records of inspections.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Intelligent Inspection** > **Inspection History**.

Step 2 Configure the search conditions, and then click **Search**.

Table 5-23 Parameter description

Parameter	Description
Inspection Organization	Select an organization, and then only the ones in that organization are displayed.
Inspection Type	Only the selected type of inspections will be searched for.

Parameter	Description
Inspection Plans	Enter keywords to search for certain inspection plans.
Time	Only inspections executed within the defined period will be searched for.

Step 3 Click  to view inspection results of the points in an inspection plan.

Step 4 Click  of a point to view the snapshot, live video, and inspection results.

Related Operations

- Review a point

Click  to review a point at a time.

- Review multiple points

Select multiple points, and then click **Review in Batches** to review them at the same time.

- Send an email

Click  to send the results of a point to specified email addresses. You can select the email addresses of users on the platform, or manually enter them (you must press Enter after entering an email address). If you want to select the email address of a user, that user must be configured with one. Also, the email server must be configured on the platform to successfully send emails. For details, see "3.2.2 Adding a User" and "7.4.5 Configuring Email Server".

5.7.5 Searching for Data Analysis

You can view the analysis of temperature data, including temperature and temperature difference.

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Intelligent Inspection** > **Data Analysis History**.

Step 2 Configure the search conditions, and then click **Search**.

Table 5-24 Parameter description

Parameter	Description
Resources	Select one or more points. When 3 points or less are selected, the platform can generate a line chart. If more than 3 points are selected, the data can only be displayed in a list.
Data Type	Select temperature or temperature difference.
Time	Select a period.

Figure 5-111 List of data

Resources

Search...

Root

121

A

org1718952345107

org1718952345269

org1718952345433

org1718952345876

org1718952345533

org1718952345761

org1718952345532

org1718952345991

org1718952346202

org1718952346286

org1718952346352

org1718952346780

org1718952346853

org1718952346912

Data Type
Temperature Data

Time
06-21 00:00:00 - 06-21 23:59:59

Search

Temperature Report 2024-06-21 00:00 - 2024-06-21 23:59

Export

Point Name	Point Type	Inspection Ar...	Inspection O...	Inspection Or...	Inspection St...	Inspection En...	Linked Channel	Data Analysis...	Inspection An...
4	4	4		Root	2024-06-21 1...	2024-06-21 1...	Thermal	Temperature ...	39.54°C
2	2	2		Root	2024-06-21 1...	2024-06-21 1...	Thermal	Temperature ...	36.94°C
4	4	4		Root	2024-06-21 1...	2024-06-21 1...	Thermal	Temperature ...	39.86°C
2	2	2		Root	2024-06-21 1...	2024-06-21 1...	Thermal	Temperature ...	36.72°C

1
20/Page

Step 3 (Optional) Click **Export** to export the current data to your computer.

5.8 Maintenance Center

You can view the overall running status of the platform, including server, channel, and device. Clear view of alert information allows you to locate the alert source and type, and then fix it in time. You can also update the programs of devices.

5.8.1 Viewing System Status

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Maintenance Center**.

Step 2 View the status of the system.



Click **Generate Report** to generate a report, and then click **Export** to export the information on the page to your computer.

- Click **Workstation** to view the overall running status of the platform, including the status of devices on main and sub servers, alert statistics, storage and status of servers. The data is refreshed every 5 minutes.
- Select **Resource Monitoring** > **Server Status**, and then click a server or service to view its running status and history information, including alerts occurred in the last 7 days and logs generated on the current day. Click **View All** to go to corresponding pages for more information.
- Device Status

Select **Resource Monitoring > Device Status > Real-Time Status**. Click a device type, and then the status of all the devices is displayed on the right. Click  to view detailed information.

- ◇ **Channel Status Info** : Information such as the channel name, online or offline, recording days, and video integrity status.
- ◇ **Hard Disk Status Info** : If it is a storage device, you can view the information of its hard disks in this section.
- ◇ **History Info** : Displays alerts occurred in the past 7 days and logs of the current day. Click **View All** to view all information.
- ◇ Information on alarm controller peripherals: Displays name, serial number, type, program version, online status, and more of the peripherals.

Select **Resource Monitoring > Device Status > History Online and Offline Status**. Configure search conditions to search for history online and offline status of the device.



Supports searching for details for devices by organization.

- Channel Status

Select **Resource Monitoring > Channel Status > All Channels**. The channel information and status are displayed.

Select **Resource Monitoring > Channel Status > Video Channel**. The channel information and status are displayed. Click  corresponding to a channel to view detailed information.

5.8.2 Monitoring Network Status

This page displays the network topology of switches, and the devices added to them. Also, you can configure the parameters of the switches directly on the platform.

Prerequisites

- Add Dahua managed switches to the platform. For details, see "3.1.2.4 Adding Devices".
When adding the device, select **IP Address** from **Add Mode**, **Dahua** from **Access Protocol**, and **Network Device** from **Device Category**.
- Connect third-party network switches to the platform through SNMP protocol.

1. Select **System Parameters > Network Device Protocol Config**, and then upload the SNMP protocol of the network switch to the platform. For details, see "7.4.12 Configuring Network Device Protocol".
2. On the **Device** page, add the network switch to the platform. For details, see "3.1.2.4 Adding Devices".

When adding the device, select **IP Address** from **Add Mode**, **SNMP** from **Access Protocol**, and **Network Device** from **Device Category**.

Select the SNMP protocol version, and then configure **Read Community** and **Write Community**.

Set the device name, and then select the device manufacturer defined on the **Network Device Protocol Config** page.

5.8.2.1 Viewing Network Topology

View the network topology of switches and the devices added to them.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Maintenance Center > Resource Monitoring > Network Status**.

Step 2 Click **Display Settings**.

Step 3 Select the display layer and a switch, and then click **OK**.

The select switch and its devices are displayed in a network topology. Click **Device Icon** on the upper-right corner to view the icons for different types of devices in the network topology.

Related Operations

- Drag
Click and hold to drag the network topology.
- Zoom in and out
Click + and - on the lower-right corner, or rotate the wheel button to zoom in and out on the network topology.
- Hide devices
Click  below a device to hide the devices added to it.

5.8.2.2 Viewing Device Details

Log in to the DSS Client. On the **Home** page, click , and then select **Maintenance Center > Resource Monitoring > Network Status**. Click a device to view its details.

- Devices: You can view the basic information, the switches, and the alerts from the last 7 days.
- Switches: You can view their information shown below.

Table 5-25 Parameter description

Parameter		Description
Device Details	Device Details	Displays the basic information, such as the model, name, and serial number.
	Device Usage	Displays the CPU and memory usage. The information is refreshed every 10 s.
	Alert Info from Last 7 Days	Displays the alerts occurred in the past 7 days. For how to configure alerts, see "4.11.1 Configuring Alert Rule".
Port Info	PoE Power Info	Displays total PoE power at the moment, and the peak PoE power from the last 7 days. The information is refreshed every 10 s.
	Port Details	Click a port to view its details. The information is refreshed every 10 s.
	Neighbor Info	Displays the information of devices added to the selected port.

5.8.2.3 Configuring Switches

You can configure the parameters of switches directly on the platform, such as IP addresses, alarms, and port functions.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Maintenance Center > Resource Monitoring > Network Status**.
- Step 2** Click a switch, and then click  on the upper-right corner.
- Step 3** Configure the parameters you need, and then click **Apply**.

Table 5-26 Parameter description

Parameter		Description
Basic	IP Address	This information is configured manually by default. You can click Auto Obtain to enable the DHCP function so that the switch can obtain the information automatically.
	Subnet Mask	
	Gateway	
	Preferred DNS	This information is configured manually by default. You can enable the switch to automatically obtain this information after you enable it to obtain an IP address automatically.
	Alternate DNS	
Alarm Config	Loopback Alarm	An alarm is triggered when the devices added to the switch are in a loop.
	IP Conflict	When the IP addresses of the switch and the devices added to it are in conflict, an alarm is triggered.
	Port Congested	When the RX port utilization or TX Port utilization is larger than the defined threshold, an alarm is triggered.
	Port Congested Alert Threshold	The threshold ranges from 0-100, and the unit is percentage. For example, If the threshold is set to 50, the RX port utilization or TX Port utilization is larger than 50%, an alarm will be triggered.

Parameter	Description
Port Config	● Port Status : Enable or disable the port. If disabled, the port will not work. ● Network Flow Control : When the network flow received by the port is faster than the port speed, the switch will send a message to the sender. The sender will then adjust its network flow to be slower than the port speed. For example, when the sender is sending data at 90 Mbps to a 10 Mbps port, the sender will then send data slower than 10 Mbps. ● Port Speed : Configure the speed for the port to receive and send data. ● Duplex Mode : ◇ Full Duplex : The port can send and receive data at the same time. ◇ Half Duplex : The port can only send or receive data at the same time. ◇ Auto Negotiation : Automatically enable full duplex or half duplex based on available resources. ● PoE Status : After enabled, the port can power devices that support PoE. ● PD Alive : When the port cannot communicate with the devices, it will automatically check and restart the devices to ensure that they work normally. This is useful to reduce maintenance workload. ● Long-distance Transmission : The port can transmit data to devices from up to 100 m. After enabling this function, the distance is increased to 250 m, but the speed is lowered to 10 Mbps.

Related Operations

On the **Device Details** page, you can restart switch or restore its parameters.

-  : Restart the switch.
-  : Restore all parameters to their default settings, including IP address, subnet mask, DNS servers, and default gateway.

5.8.2.4 Exporting Network Information

Export the current network topology and device list to your computer.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Maintenance Center** > **Resource Monitoring** > **Network Status**.
- Step 2** Click **Export**, and then select **Export Network Topology Image** or **Export Device List**.
- Step 3** Enter the login password and configure an encryption password, and then click **OK**.

5.8.3 Maintenance Management

You can view and process alerts, view analysis reports of the system running situation, and update the programs of devices.

5.8.3.1 Viewing and Processing Alert

When alerts are triggered, you can view their information and process them. Also, notifications will be provided to inform you and quickly direct you to this page when they are triggered.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Maintenance Center > Maintenance Management > Alerts**.
- Step 2** Click an alert, and then its information is displayed on the right.
- Step 3** Process the alert.
1. Click **Accept** on the bottom of the page.
 2. Enter a name for the person who processed the alert, and the troubleshooting log, and then click **Save**.

Related Operations

- Export the details of an alert
On the bottom of the information of the alert, click **Download Report**. Enter the login password and encryption password to export the information to your computer.
- Export alert list
Click **Export** on the upper-left corner of the page, enter the login password, encryption password, and then select the export range and format to export them to your computer.
- Add an alert to favorites
Click  of an alert to add it to favorites.
- Filter the alerts
Click **Filter**, and then you can filter the alerts by time, resource type, alert type, priority, and alert status.
- Sort the alerts
Rearrange the alerts by time in the descending or ascending order.

5.8.3.2 Viewing, Downloading and Sending Analysis Report

The system will generate analysis report when it is running. You can download it to your computer, or send it immediately or at the defined time to specified email addresses

Log in to the DSS Client. On the **Home** page, click , and then select **Maintenance Center > Maintenance Management > Analysis Report**. The analysis report within the past 7 days is displayed by default.

- View analysis reports with specified content
Click **Search by Tag** on the upper-right corner of the page to generate a report by time, resource type, alert type, and alert priority. An analysis report of up to 30 days can be generated.
- Download an analysis report
Click **Download Report**, enter the login password and encryption password, and then select the content to be exported to download it to your computer.

- Send an analysis report to one or more email addresses

Click **Send Report** to send it to one or more specified email addresses immediately or at the defined time.

- ◇ **Send Now** : Send the information in **Body** and selected information to the specified email addresses immediately.
- ◇ **Auto Send** : Send the information in **Body** and selected information to the specified email addresses daily, weekly, or monthly.

Daily report: Data from yesterday will be sent to your email at a defined time. If set to 03:00:00, the data from the day before (00:00:00–23:59:59) will be sent to your email at 03:00:00 every day.

Weekly report: Data from last week will be sent to your email at a defined time. If set to 03:00:00 on Wednesday, the data from Wednesday to Tuesday of each week will be sent to your email at 03:00:00 every Wednesday.

Monthly report: Data from last month will be sent to your email at a defined time. If set to 03:00:00 on 3rd, the data from 3rd of last month to 2nd of the current month will be sent to your email at 03:00:00 on 3rd of each month.

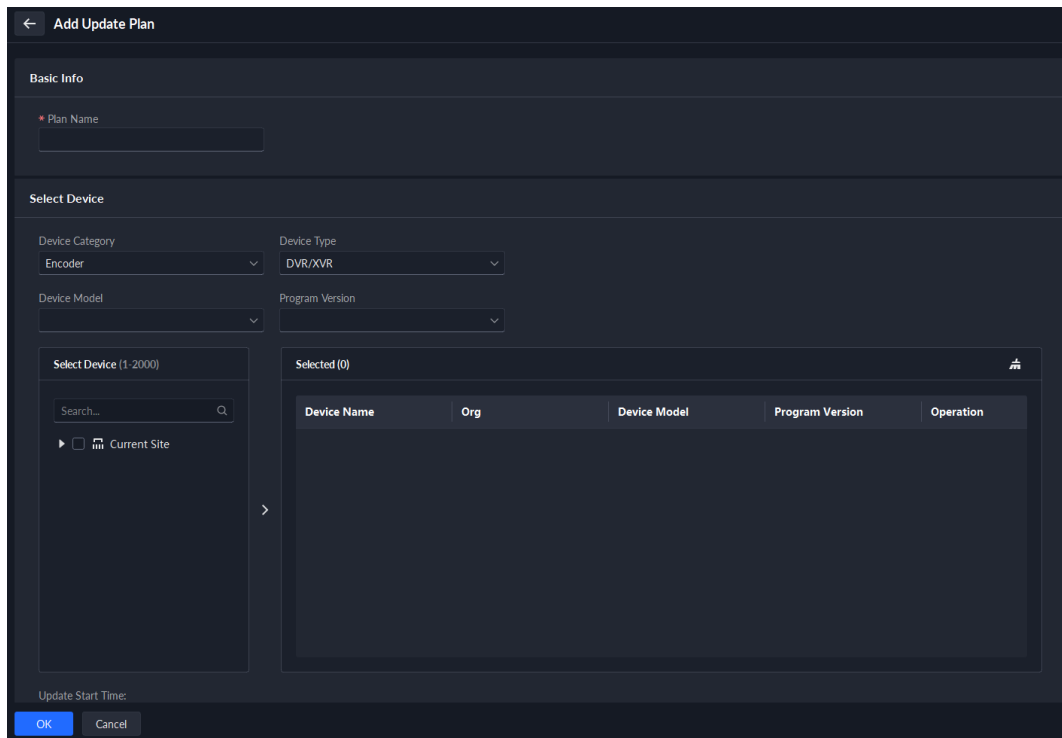
5.8.3.3 Updating Device Program

Add a plan to update the programs of selected devices in batches.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Maintenance Center > Maintenance Management > Device Update**.
- Step 2** Click **Add**.

Figure 5-112 Add an update plan



The screenshot shows the 'Add Update Plan' dialog box. It has a title bar with a back arrow and the text 'Add Update Plan'. Below the title bar, there are several sections:

- Basic Info:** Contains a text input field for 'Plan Name'.
- Select Device:** Contains four dropdown menus: 'Device Category' (set to 'Encoder'), 'Device Type' (set to 'DVR/XVR'), 'Device Model', and 'Program Version'.
- Select Device (1:2000):** A list box on the left with a search bar and a 'Current Site' button.
- Selected (0):** A table on the right showing the selected devices. The table has columns: 'Device Name', 'Org', 'Device Model', 'Program Version', and 'Operation'. It is currently empty.
- Update Start Time:** A text input field at the bottom left.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

- Step 3** Enter a name for the plan, and then select the device category, type, model, and program version.

The platform will only display corresponding devices.

Step 4 Select the devices you want to update.



Click  to cancel selecting all devices.

Step 5 Configure when to update the devices.

- **Now** : Update the devices immediately after the plan is added.
- **Custom** : Update the devices at the defined time.

Step 6 Click **Upload File** to upload the update program.



- Make sure that the uploaded program matches the models and current program versions of selected devices.
- Make sure that the network is stable and the power properly connected for all devices. Otherwise, they might not work properly.

Step 7 Click **OK**.

Related Operations

In the list of update plans, you can view the information of each plan, including name, update program, update start time, and update status.

- Click  to delete a plan one by one; select multiple plans, and then click **Delete** to delete them in batches.
- Click  to view the update status of the devices in a plan.
 - ◇ Click  to remove a device from the plan; select multiple devices, click **Delete** to remove them in batches.
 - ◇ If one or more devices failed to update, click  to update a device again one by one, or select multiple devices, and then click **Update Again** to update them in batches.

6 General Application

6.1 Target Detection

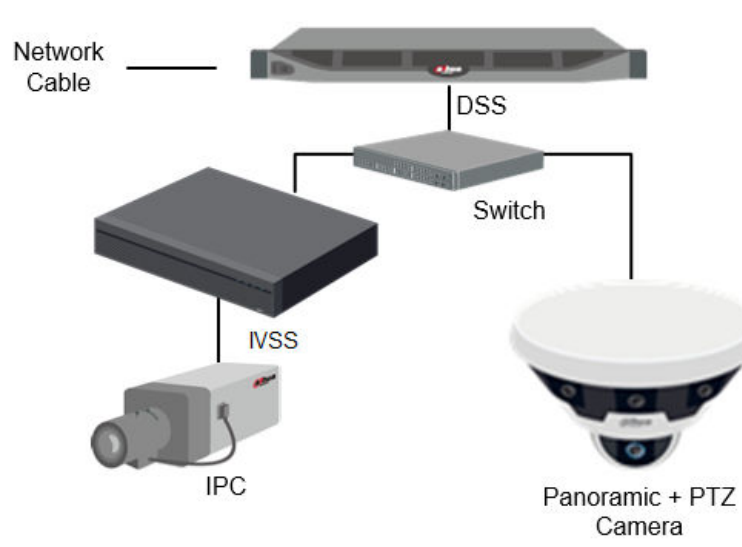
View and search for the metadata of people, vehicle, and non-motor vehicle.



Target detection can be done by video metadata cameras + a platform, or IPCs + IVSSs + platform.

6.1.1 Typical Topology

Figure 6-1 Typical topology



- General cameras record videos.
- Video metadata cameras such as panoramic + PTZ camera record videos, analyze people, motor and non-motor vehicles.
- IVSS manages cameras and analyzes people, and motor and non-motor vehicles.
- The platform centrally manages IVSS and cameras, receives analysis results from cameras and displays the reports.

6.1.2 Preparations

Make sure that the following preparations have been completed:

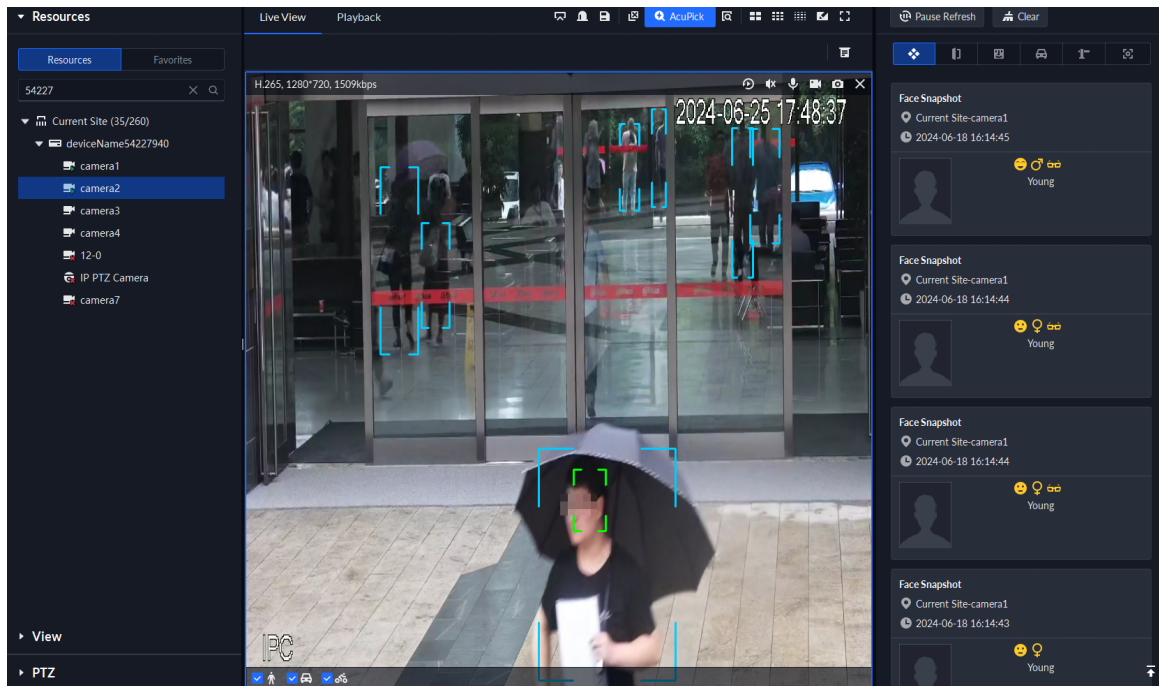
- Cameras and IVSS are correctly deployed, and video metadata is enabled on them. For details, see corresponding user manuals.
- Basic configurations of the platform have been finished. To configure the parameters, see "3 Basic Configurations".
 - ◇ When adding a camera or IVSS, select **Encoder** for device category.
 - ◇ After adding the camera or IVSS to the platform, select **Metadata Feature Report Capability** or **Metadata Attribute Report Capability** from **Features** of the device.

6.1.3 Live Target Detection

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center** > **Monitoring**.
- Step 2** Select a window, double-click the channel or drag the channel to the window.

Figure 6-2 Live view



- Step 3** Click  and then click  to view live metadata events.
- Step 4** View live video, and human body, vehicle, and non-motor vehicle information.
- Click an event record to view the event snapshot. You can play back the video of the event. Different events support different operations.
 - When playing back video, click  to download the video to a designated path.
 - Click  to play back the video before and after the snapshot.
 - Click  to delete event information.
 - Click  to view the most recent events.

6.1.4 Searching for Metadata Snapshots

Search for metadata snapshots by setting search criteria or uploading images.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **DeepXplore**.
- Step 2** Click **Integrated Retrieval**.
- Step 3** Set search criteria.

You can search for metadata snapshots in the **Record** , **Person** or **Vehicle** section. For details, see "5.3 DeepXplore".

6.2 ANPR

View automatic number plate recognition in real time or search for records. You can view the moving track of a vehicle. This is useful for road monitoring.

- Automatic number plate recognition

The platform displays vehicle snapshots and ANPR results in real time.

- Vehicle records

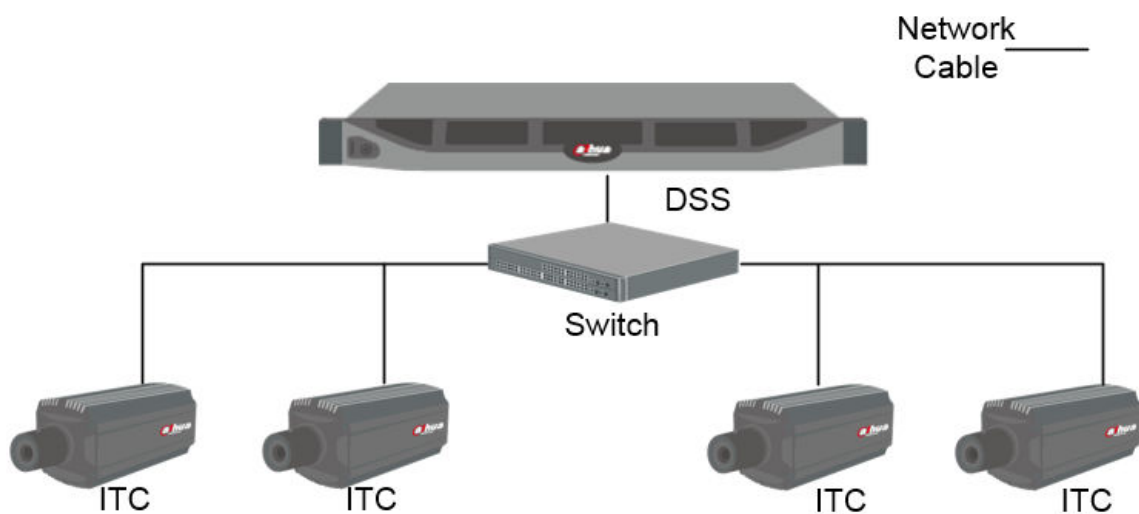
Search for vehicle records according to the filtering conditions you have set.

- Vehicle track

According to the ANPR camera locations that a vehicle has passed through, the platform displays the driving track of the vehicle on the map.

6.2.1 Typical Topology

Figure 6-3 Typical topology



- ANPR cameras (ITC camera) capture and recognize vehicles.
- DSS centrally manages ANPR cameras, receives and displays vehicle snapshots and information uploaded from the cameras.

6.2.2 Preparations

Make sure that the following preparations have been made:

- ANPR cameras are added to the platform, and the ANPR function is configured. For details, see corresponding user manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
 - ◇ When adding an ITC camera, select **ANPR Device** for device category, and then select **ANPR Device** for **Device Type**.

- ◇ ANPR snapshots are only stored on **ANPR Picture** disks. On the **Storage** page, configure at least one **ANPR Picture** disk. Otherwise vehicle pictures cannot be viewed.

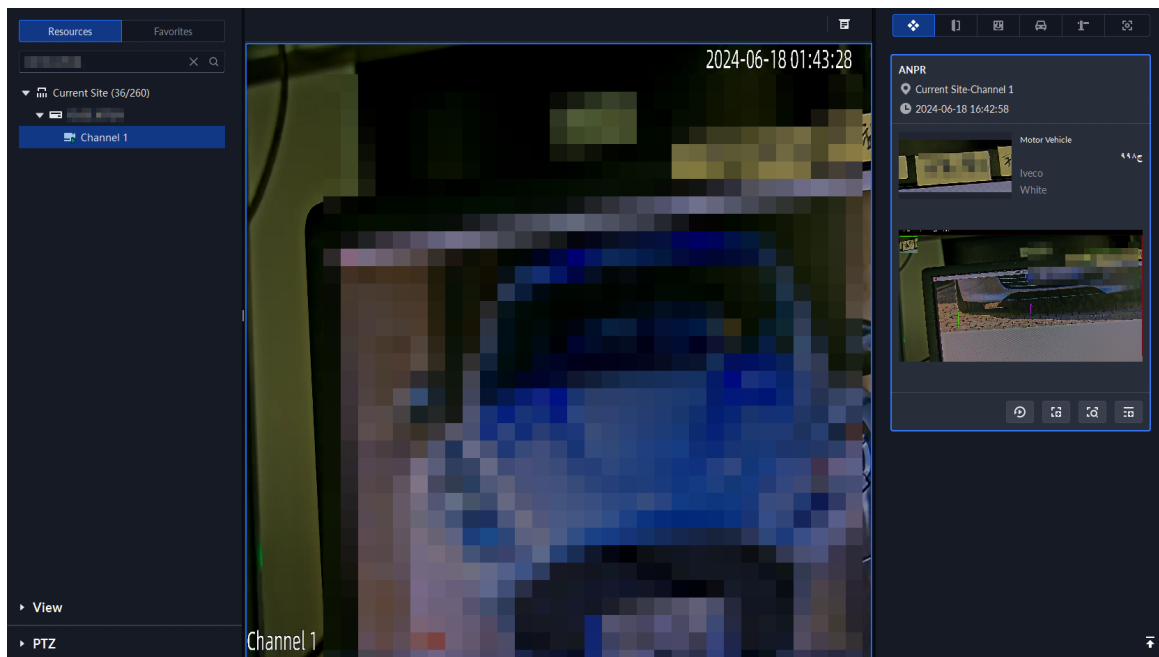
6.2.3 Live ANPR

View ANPR live video and plate snapshots.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Monitor Center** > **Monitoring**.
- Step 2** Select a window, double-click the channel or drag the channel to the window.

Figure 6-4 Live view



- Step 3** Click  and then click .

- Step 4** View live ANPR events.

- Click an event record to view event snapshots. You can also play back the video of the event. Different events support different operations.
- : This function is only available when a license plate is recognized. Click this icon to add the vehicle to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the vehicle is recognized.
- : Add the vehicle to the platform.
- When playing back a video, click  to download the video to a designated path.
- Click  to play back the video before and after the snapshot.
- Click  to delete event information.
- Click  to view the most recent events.

6.2.4 Searching for Vehicle Snapshot Records

If there are recorded videos on devices, you can view recorded videos linked to the capture records by searching for them. Each video will be 20 s long, with 10 s before and after the time of capture. When playing a video, it will start at 10 s before the time of capture.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **DeepXplore**.

Step 2 Click **Integrated Retrieval**.

Step 3 Configure the search conditions.

You can search for vehicle snapshots in the **Record** or **Vehicle** section. For details, see "5.3 DeepXplore".

6.3 Face Recognition

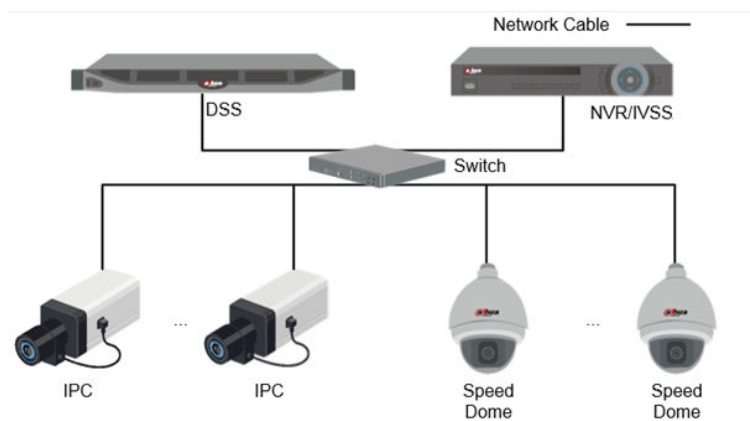
Configure face recognition settings on the device and the platform before you can view face recognition results on the platform.

6.3.1 Typical Topology

The face recognition feature is available on select models of NVR, IVSS and FR cameras.

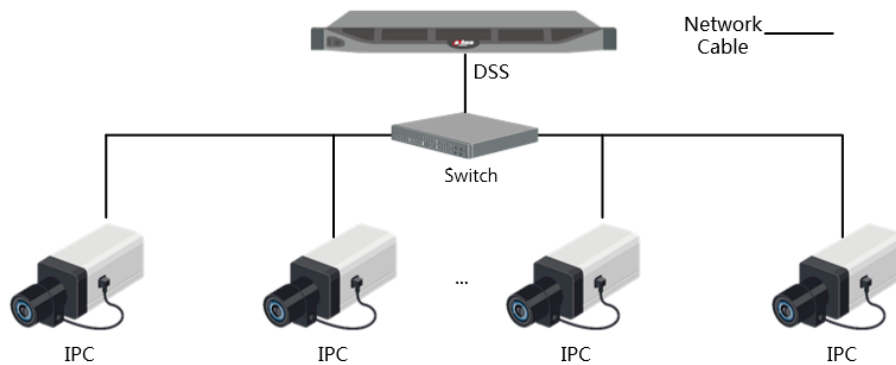
- Face recognition by NVR/IVSS

Figure 6-5 Typical topology (NVR/IVSS)



- ◇ Cameras record videos.
- ◇ NVR/IVSS is used for face recognition and storage.
- ◇ DSS centrally manages cameras, NVRs, and the face database, and provides live view and face search.
- Face recognition by camera

Figure 6-6 Typical topology (camera)



- ◇ Cameras record face videos, and detect and recognize faces.
- ◇ DSS centrally manages cameras, NVRs, and the face database, and provides live view and face search.

6.3.2 Preparations

Make sure that the following preparations have been made:

- Face recognition devices are correctly configured. For details, see corresponding user manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
 - ◇ When adding face recognition devices, select **Encoder** for device category.
 - ◇ After adding a face recognition NVR or IVSS, select **Face Recognition** for **Features** of the corresponding channels.
 - ◇ After adding face recognition cameras or face detection cameras, select **Face Recognition** or **Face Detection** for **Features**.
 - ◇ Face snapshots are stored in the **Face/Alarm and Other Pictures** disk. Configure at least one local disk for picture storage. Otherwise, the platform cannot display snapshots.

6.3.3 Arming Faces

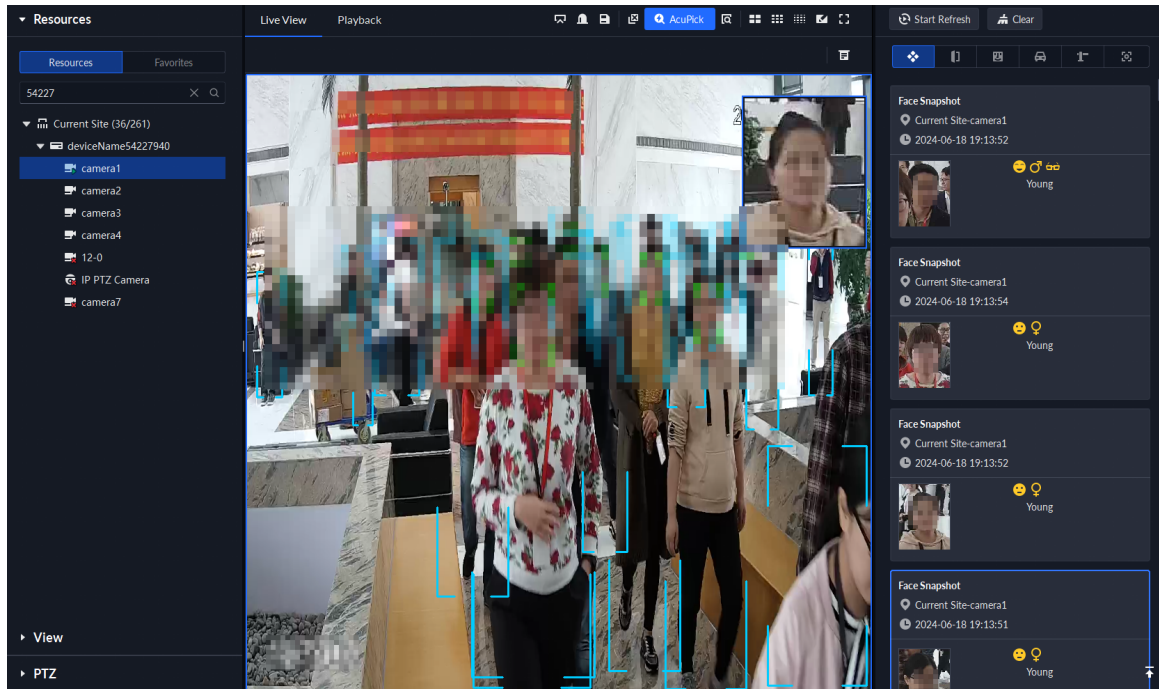
Before arming faces, you need to add the persons to the face arming group. For details, see "4.4.1 Face Arming List".

6.3.4 Live Face Recognition

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitor Center** > **Monitoring**.
- Step 2 Select a window, double-click the channel or drag the channel to the window.

Figure 6-7 Live view



Step 3 Click , and then click  to view live face recognition information.

Step 4 View live video.

- Click an event record to view event snapshots. You can play back the video of the event. Different events support different operations.
- : Add the person to the platform or add the person to an arming group. After you send the arming group to devices and configure an event, devices can trigger alarms when the face is recognized.
- When playing back video, click  to download the video to designated path.
- Click  to play back the video before and after the snapshot.
- Click  to refresh events; click  to pause refreshing.
- Click  to delete event information.
- Click  to view the most recent events.

6.3.5 Searching for Face Snapshots

Search for face snapshots by setting search criteria or uploading images.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **DeepXplore**.
- Step 2** Click **Integrated Retrieval**.
- Step 3** Configure the search conditions.

You can search for snapshots in the **Record** or **Person** section. For details, see "5.3.1 Searching for People".

6.4 POS

View POS live video and records.

- Live view

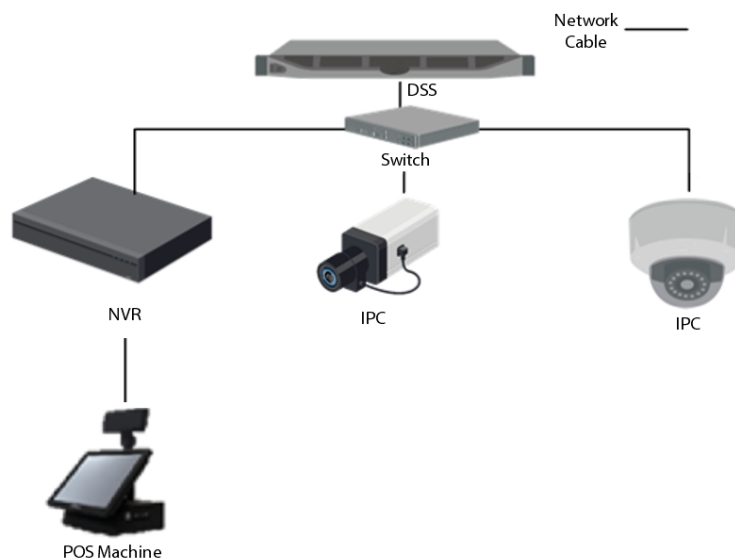
View live POS video and the transaction details overlapped on the video.

- Playback

Search for POS transaction records and play the recorded video. The POS video clip can start 10 seconds before or after the POS receipt printing.

6.4.1 Typical Topology

Figure 6-8 Typical topology



- Cameras record videos of each POS transaction.
- NVRs are connected with cameras and POS machines, and store videos.
- POS machines record transaction details and generate receipts. They connect to the platform through NVRs.
- The platform centrally manages NVRs and cameras, and provides live videos and POS transaction video records.

6.4.2 Preparations

Make sure that the following preparations have been made:

- Cameras, NVRs and POS machines are correctly configured. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
 - ◇ When adding an NVR, select **Encoder** for device category.
 - ◇ At least one POS channel is connected to NVR.
 - ◇ On the **Bind Resource** page, bind video channels to the POS channels. See "3.1.3 Binding Resources".

6.4.3 Setting POS End Sign

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.
- Step 2** Click the **POS Config** tab.
- Step 3** Set the end line of POS receipt.
- Step 4** Click **OK**.

6.4.4 POS Live View

View real-time POS transaction video and details.

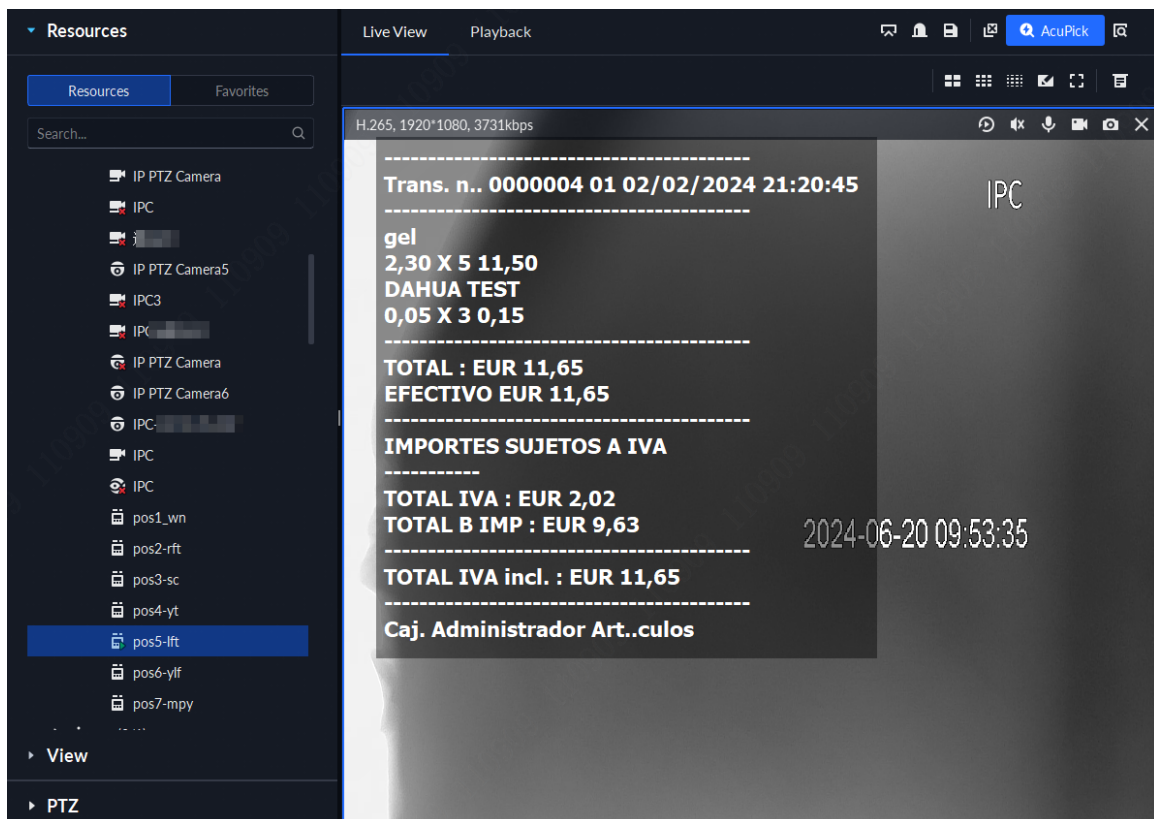
Prerequisites

Make sure that the POS channel has been bound to video channel. For details, see "6.4.4 POS Live View".

Procedure

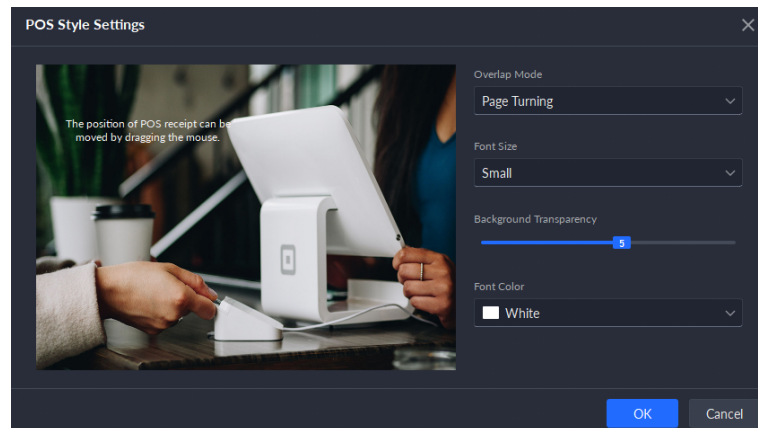
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Monitor Center** > **Monitoring**.
- Step 2** In the **POS** list in the **Resources** section, select a channel, device or organization, double-click or drag it to the window.

Figure 6-9 POS video



- Step 3** (Optional) Set POS information style.
 1. Right-click and select **Set POS Style**.

Figure 6-10 POS style setting



2. Set **Overlap Pattern** , **Font Size**, **Background Transparency** and **Font Color**.
3. Point to POS information overlay area, press mouse left button and move it to adjust POS information overlay position.
4. Click **OK**.

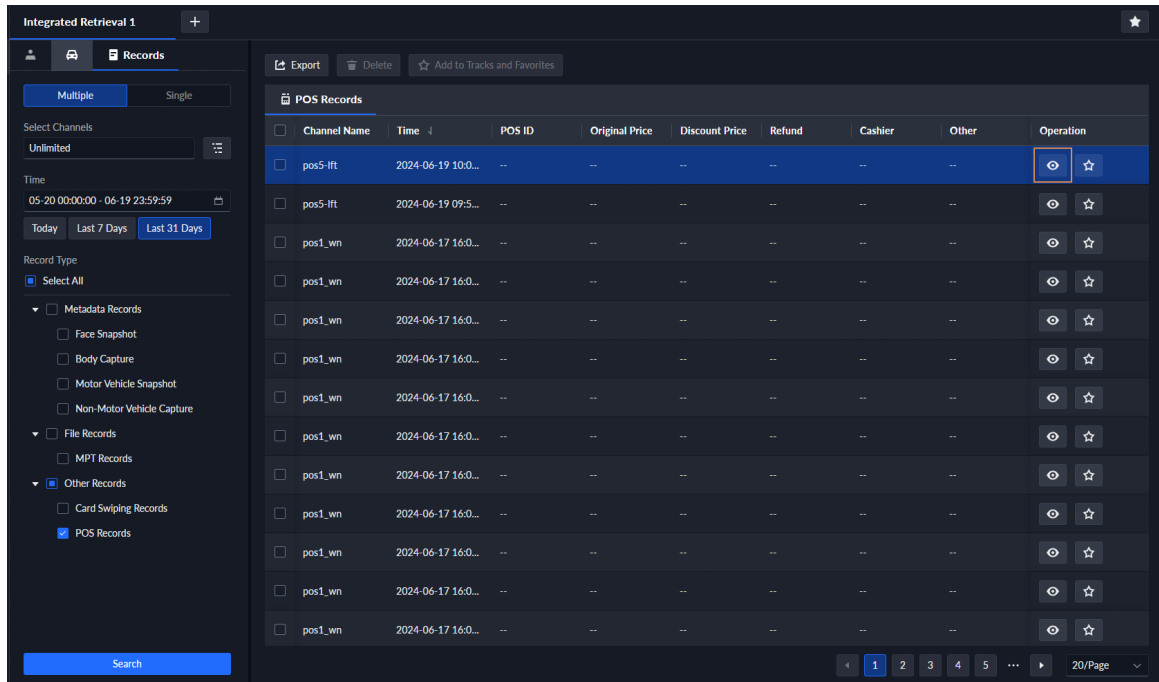
6.4.5 Searching for POS Receipts

Search for POS receipt to view related video of receipt. You can search for the video half an hour before and half an hour after the time when POS receipt is printed, and you can start to play video 10 s before the time when POS receipt is printed.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **DeepXplore**.
- Step 2 Click **Integrated Retrieval**.
- Step 3 Click . You can search for the POS records both in **Multiple** and **Single**.
- Step 4 Select channel and time, select **POS Record** for the record type, and then click **Search**.

Figure 6-11 Search for the POS records



Step 5 Click  on the operation area of the corresponding record to view its details.

- When viewing recorded videos, you can select a target manually or select one automatically recognized by AcuPick, and then search for it in DeepXplore.
- If the channel is bound to other video channels, the recorded video from the bound video channels will play automatically.

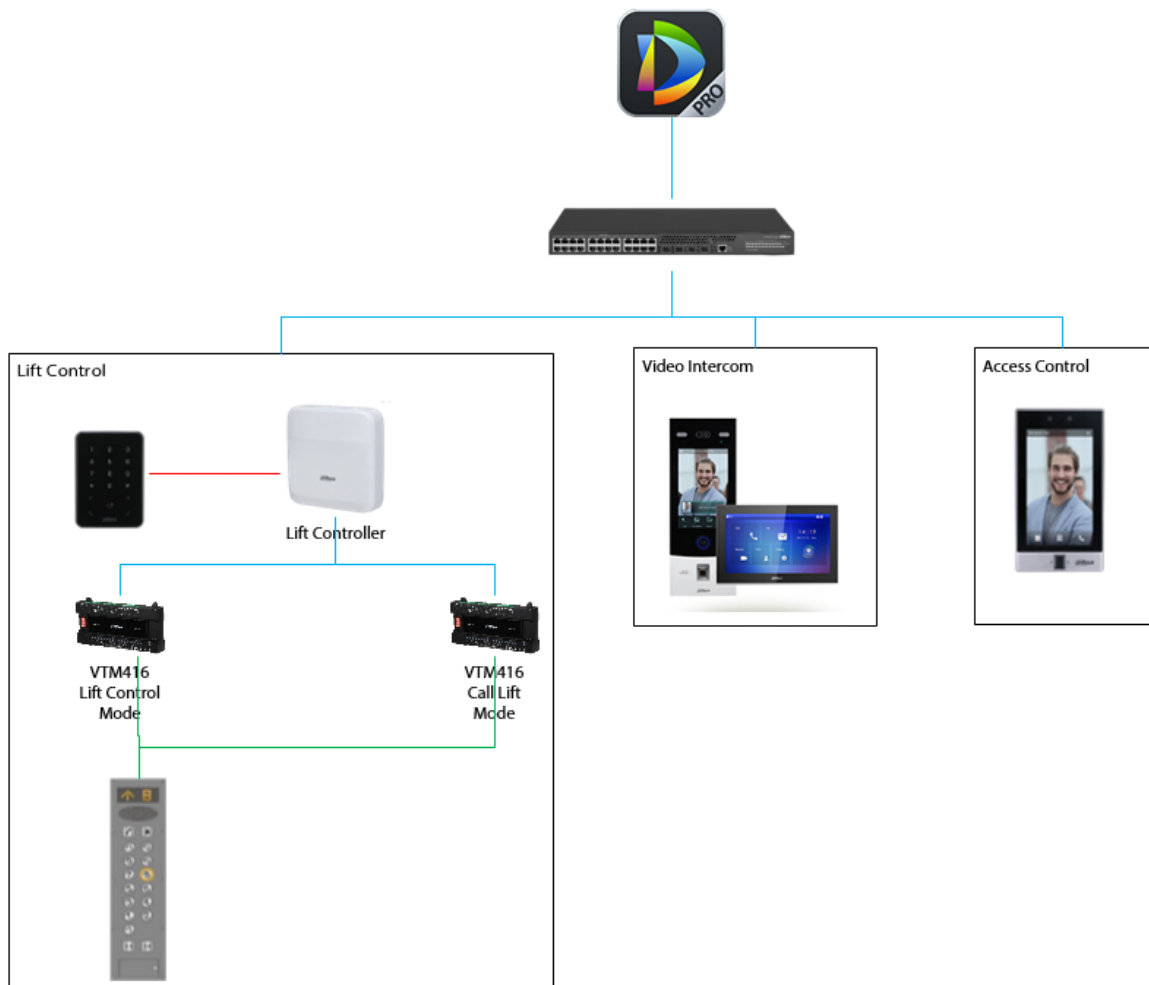
6.5 Lift Control

There are mainly 2 scenarios.

- Authorized access: After granting access permissions of corresponding floors to people, the person can go into the lift by card swiping, fingerprints, passwords, or more, and reach the floors with access permissions. For example, residents can only reach the floors they have access permissions, so as not to affect residents on other floors.
- Visitors call the lift on VTO (you need to configure visitors' VTO access permissions and floor access permissions in advance).
 - ◇ After the homeowner agrees the access on VTH or DSS Agile VDP App, the visitor can reach the floor where the homeowner is located.
 - ◇ After receiving the lift call, the platform administrator grants permissions of the specified floor to the visitor, who can then go to that floor.

6.5.1 Typical Topology

Figure 6-12 Typical topology



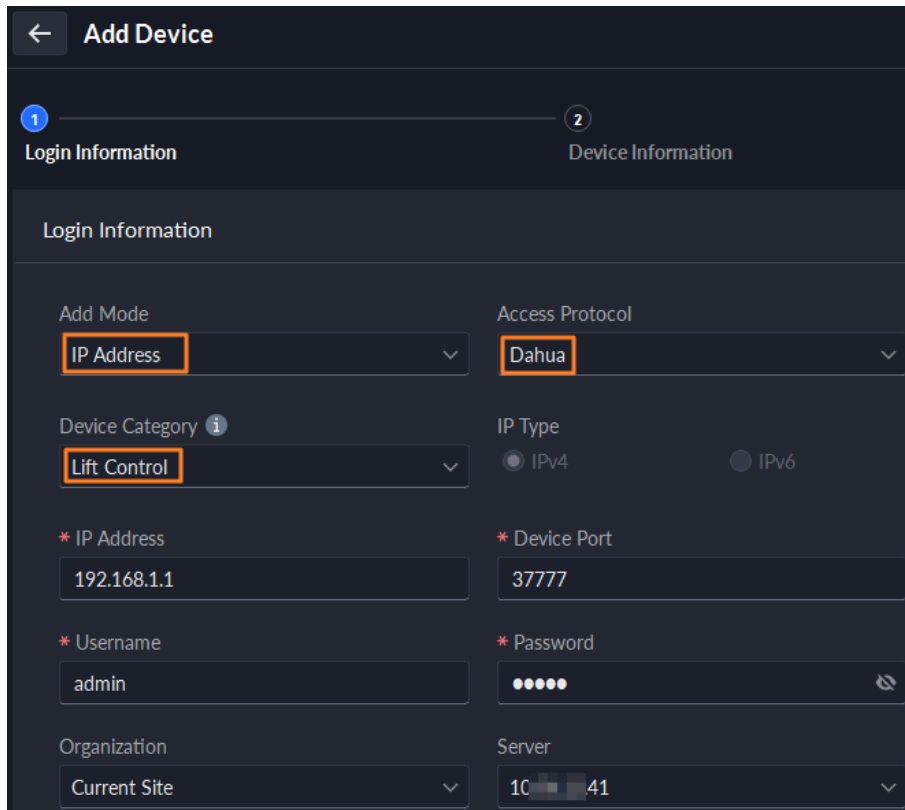
- Lift control module and lift controller: Installed on top of the elevator car or at the top of the hoistway. Connect the lift control modules to the lift controller, to manage the running of the lift.
- Card reader: Connect it to the lift controller through RS-485 or Wiegand, and supports card swiping, QR code, face recognition, and more.
- Video intercom: Visitors call VTH (indoor monitor) on the VTO (door station), and after the owner confirms, the lift comes to the floor where VTO is located.
- Access control: When people go into the lift through card swiping, fingerprint, and password on the access controller, the person can reach the floor with access permissions.
- DSS: Add and manage people, floor, lift control channels, and other information, and control the permissions.

6.5.2 Preparations

- You have installed the video intercom devices and lift control devices. For details, see device user manuals.
- You have linked the video intercom device to the lift controller on the lift controller webpage. For details, see lift controller user manual.
- You have added the video intercom devices and lift controller to the DSS platform.

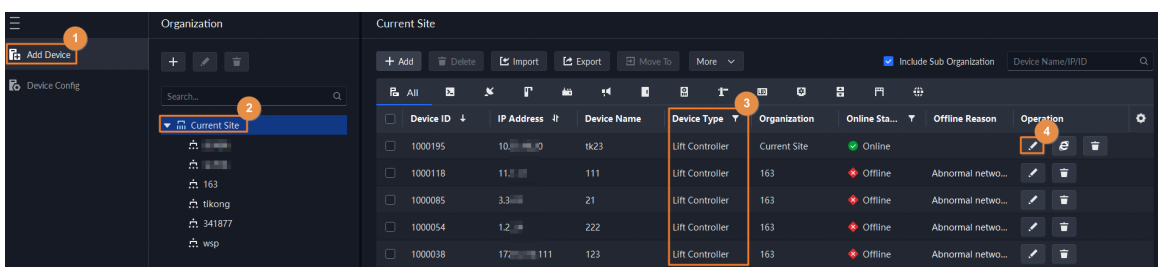
- ◇ When adding lift controller on the **Device** page, select **IP Address** or **Domain Name** from **Add Mode**, **Dahua** from **Access Protocol**, and **Lift Control** from **Device Category**,

Figure 6-13 Add lift controller



- ◇ When adding video intercom devices on the **Device** page, select **Video Intercom** from **Device Category**.
- Edit the floor name, which supports letters and numbers.

Figure 6-14 Edit floor



Device ID	IP Address	Device Name	Device Type	Organization	Online Sta...	Offline Reason	Operation
1000195	10.10.10.10	tk23	Lift Controller	Current Site	Online		
1000118	11.11.11.11	111	Lift Controller	163	Offline	Abnormal netwo...	
1000085	3.3.3.3	21	Lift Controller	163	Offline	Abnormal netwo...	
1000054	1.2.3.4	222	Lift Controller	163	Offline	Abnormal netwo...	
1000038	172.16.17.111	123	Lift Controller	163	Offline	Abnormal netwo...	

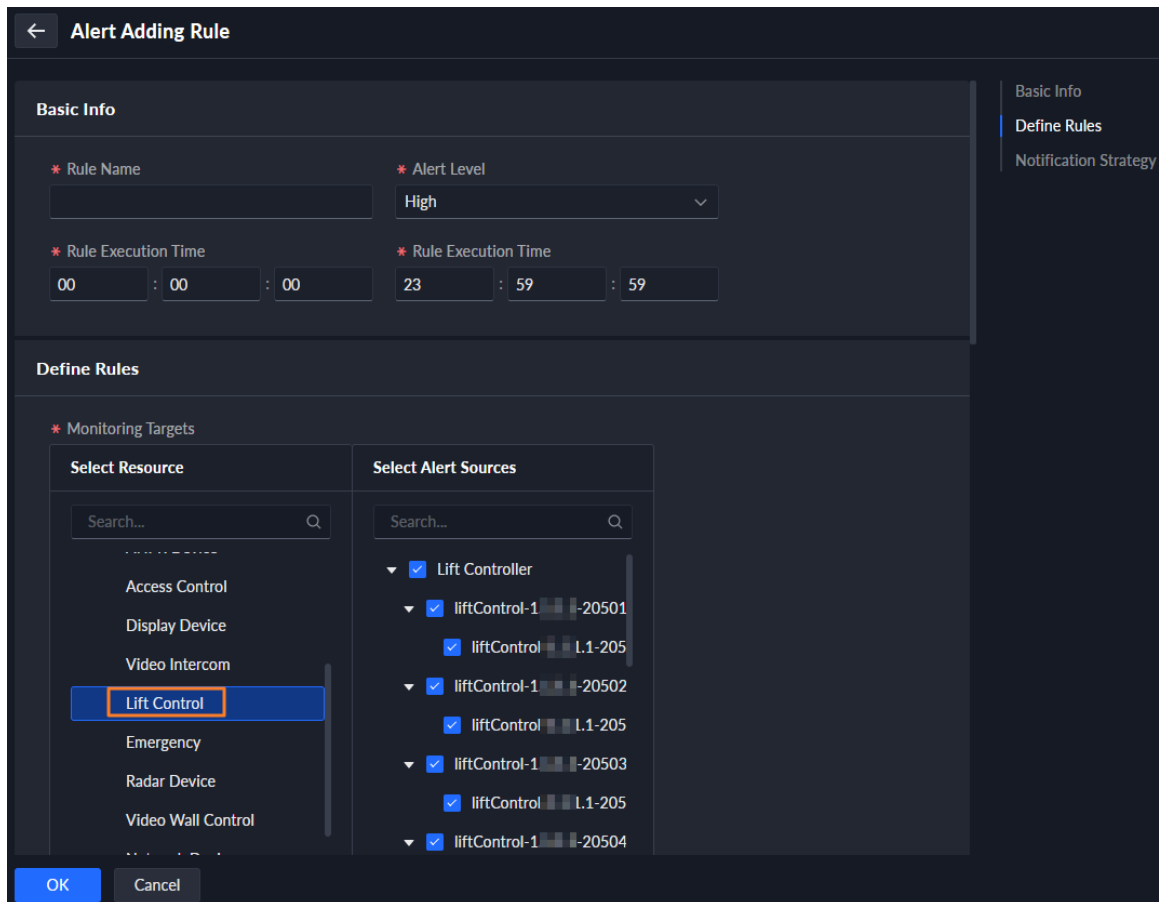
6.5.3 Lift Controller Maintenance

6.5.3.1 Configuring Alert Rule

Configure alert rules to monitor the lift controllers so that you can handle exceptions (if any) timely.

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Maintenance Center** > **Alert Rule Config**.
- Step 2** Click .
- Step 3** Configure the parameters, and then click **OK**.

Figure 6-15 Configure lift control alert rules



Alert Adding Rule

Basic Info

* Rule Name:

* Alert Level: High

* Rule Execution Time: 00 : 00 : 00

* Rule Execution Time: 23 : 59 : 59

Define Rules

* Monitoring Targets

Select Resource

Search...

Access Control

Display Device

Video Intercom

Lift Control

Emergency

Radar Device

Video Wall Control

Select Alert Sources

Search...

☒ Lift Controller

☒ liftControl-1 -20501

☒ liftControl -1.1-205

☒ liftControl-1 -20502

☒ liftControl -1.1-205

☒ liftControl-1 -20503

☒ liftControl -1.1-205

☒ liftControl-1 -20504

OK **Cancel**

Table 6-1 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule. It can be up to 50 characters.
Alert Level	Select a level for the alert. This is used to quickly know the urgency of the alert when it is triggered.
Rule Execution Time	The alert will only be triggered within the defined period.
Monitoring Targets	Targets include servers and devices. Select Lift Control from Device .
Rule Conditions	Set the threshold for device disconnection. When the value is greater than or equal to the threshold, the alert will be triggered.
Push Notifications	After enabled, you can select the users who will receive notifications when the lift controller is disconnected.
Email Notification	After enabled, you can customize the content to be sent to specified email addresses. You can configure the email addresses in the following ways: - Click + to select the email addresses of users. - Manually enter an email address, and then press Enter.

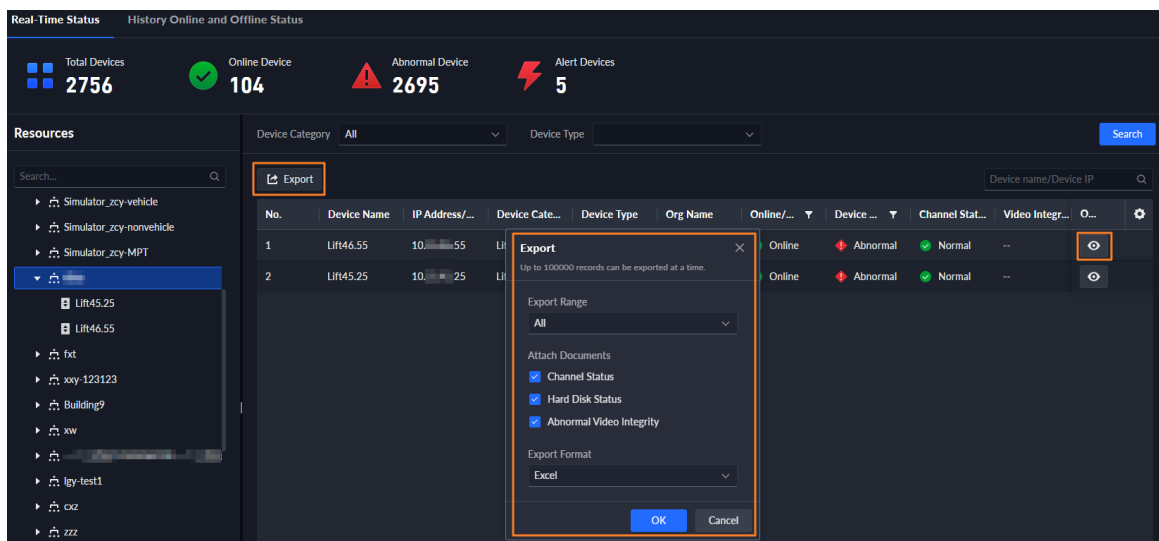
6.5.3.2 Viewing Lift Controller Status

- Step 1** Log in to the DSS Client. On the **Home** page, select  > **Maintenance Center**.
- Step 2** Select **Resource Monitoring** > **Device Status**, select the lift controller from the resource tree, and then you can view the online status, device status, and channel status of the lift controller on the right. Click  to view device details.



Click **Export**, and then you can export the records according to your settings to local.

Figure 6-16 View device status



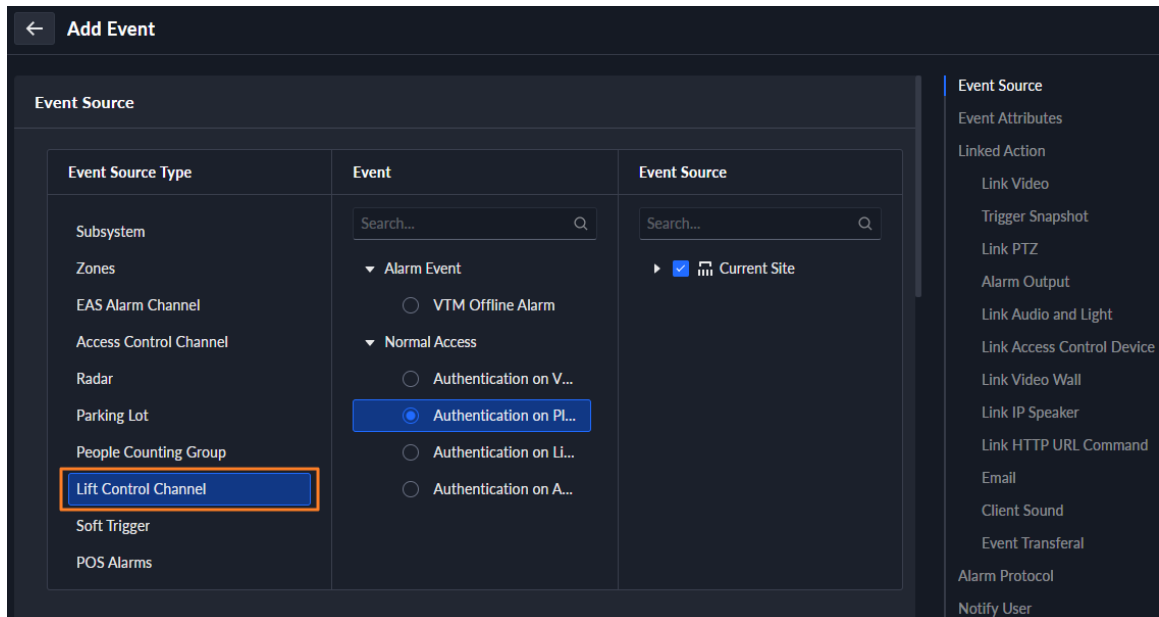
6.5.4 Configuring Event

Go to  > **Event** > **Event Config**, select **Lift Control Channel** from event source type, and then set the event, event source, and event linkage, such as taking snapshots and recording videos.

For details on configuring events, see "4.1.1 Configuring Event Linkage".

When people pass through after authentication on VTO, platform, lift controller, or access control device, the corresponding linkage action will be triggered.

Figure 6-17 Select lift control



6.5.5 Authorized Access

6.5.5.1 Adding a Person

For lift control, you need to configure the following information of a person:

- Basic information, including name, photo, and more.
- Credentials, such as passwords, cards, fingerprints, for access.
- Access control information, which is for configuring person access permissions.

You need to select **Lift** from access point type.

- Video intercom information, including room number and person identity (homeowner and app user).

When selecting **App User**, and entering the person email address. The system automatically creates a DSS Agile VDP account for the person. If a visitor comes, the person can remotely authorize the visitor on DSS Agile VDP, so that the visitor can access the floor where the person is located.

For details of adding people, see "4.3.2.2 Adding a Person".

6.5.5.2 Configuring Access Rules

Grant permissions to persons so that they can verify their identifications and access lifts within the effective periods.

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.
- Step 2** Click **Add**, and then configure the parameters.

Figure 6-18 Add an access rule

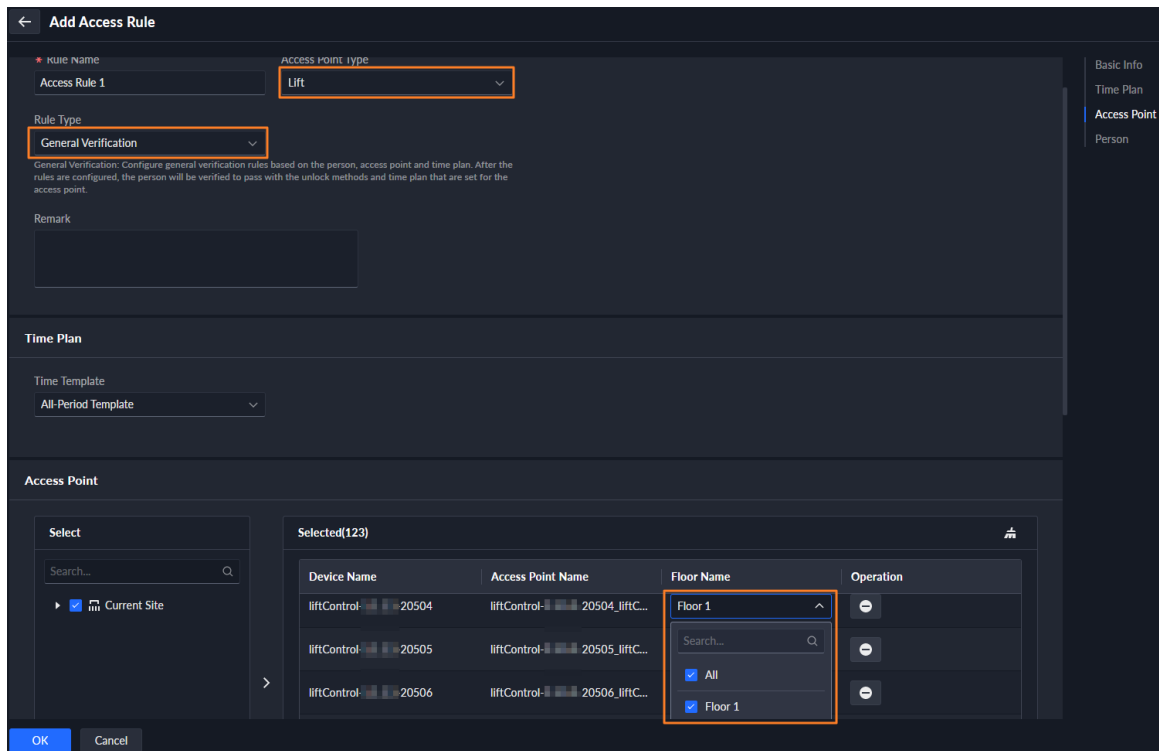


Table 6-2 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Select Lift , and then the platform will only display corresponding channels.
Rule Type	Select General Verification .
Time Template	Select when this rule is effective. If you want to create a new time template, see "3.1.6 Adding Time Template".
Access Point	Select the access point to which the access rule applies, and then select floors. The selected people will have access to the floors selected here.
Person	Select by Person Group : Select one or more person groups, and then all the persons in the groups will have permissions to access the selected access points.  Select Link Sub Node, and then you can select a zone and all its sub zones at the same time. Select by Person : Select one or more persons, and then they will have permissions to access the selected access points.  Select Include Sub Groups to display all the persons in the selected group and its sub groups.

Step 3 Click **OK**.

6.5.5.3 Controlling Lift Control Channels

Set all lift channels in a zone to no authentication, authentication, and lock modes. Only administrators can control lift channels globally.

- Step 1** Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**.
- Step 2** Select a zone, and then click **Authentication Mode**, and then people must verify their identifications to go to specified floors.



When selecting **No Authentication Mode**, all people can go to any floor without verifying their identifications; when selecting **Lock Mode**, no person is allowed to use lifts.

6.5.5.4 Accessing the Lift

People go into the lift through card swiping, fingerprints, passwords, and more, and then they can reach the floors they have access to.

6.5.6 Calling Lift on VTO

When a visitor calls the lift on VTO, the visitor can reach the floor where the homeowner is after remote authorization by the homeowner or the platform administrator.

Procedure

- Step 1** Add the visitor to the platform. For details, see "6.5.5.1 Adding a Person".
- Step 2** Configure the access rules for the visitor. For details, see "6.5.5.2 Configuring Access Rules".
- Step 3** Configure the door access rules for the visitor.
1. Click , and then in the **App Config** area, select **Access Control** > **Access Rule** > **All Rules**.
 2. Click **Add**, and then configure the parameters.

Table 6-3 Access rule parameters

Parameter	Description
Rule Name	The name that identifies the rule.
Access Point Type	Select Door .
Rule Type	Select General Verification .
Access Point	Select the access control device to which this access rule applies by zone or by access point.

Parameter	Description
Person	● Select by Person Group : Select one or more person groups, and then all the persons in the groups will have permissions to access the selected access points.  - Select Link Sub Node, and then you can select a zone and all its sub zones at the same time. ● Select by Person : Select one or more persons, and then they will have permissions to access the selected access points.  - Select Include Sub Groups to display all the persons in the selected group and its sub groups.

3. Click **OK**.

Step 4 The platform administrator configures call groups, management groups, and relationship groups to enable calls within specific groups. For details, see "4.6.2 Call Management".

Results

After the visitor calls the lift on VTO:

- After the homeowner remotely agrees the access on VTH or DSS Agile VDP app, the visitor can reach the floor where the homeowner is.
- The platform administrator grants the designated floor permissions of the homeowner to the visitor on the platform, and then the visitor can reach the floor where the homeowner is.

6.5.7 Viewing Access Records

You can view and export access events for specified zones, person groups, and time.

Step 1 Log in to the client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Records** > **Event Record**.

The number of each type of access events in all zones is displayed at the top of the page by default.

Step 2 Set search conditions, such as zone, time, person group, person, ID, access point, company, and department, and then click **Search** to view the specified access events.

Step 3 (Optional) Click **Export**.

Step 4 (Optional) Enter the login password and the encryption password of the export file, select whether to export images, set the export range and the export fields, and then click **OK**.



You can also configure not to verify the login password and set the encryption password. For details, see "7.4.1 Configuring Security Parameters".

7 System Configurations

This chapter introduces system parameters configuration, license, service management, and backup and restore.

7.1 System Deployment

The platform supports managing server information and adjusting the upper-level server of a server or device.

7.1.1 Distributed Deployment

Set the server type, and assign devices to different servers.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Deployment**.
- Step 2** Click **Distributed Config**.
- Step 3** Manage servers.
- Click  to view server details.
 - Click  corresponding to a server to define the server type. A server can be set to sub server or standby server when it is not in use.
 - Click  to enable the server.  means the server is enabled.
 - Click  to delete the server.

Figure 7-1 Servers

Refresh Allocate Resources		Server Name/Server IP		
Server Name	IP Address	Type	Server Status	Operation
192.168.12.101	192.168.12.101	Main Server	Running	
192.168.12.102	192.168.12.102	Sub Server	Offline	 
192.168.12.103	192.168.12.103	Sub Server	Running	  
192.168.12.104	192.168.12.104	Sub Server	Running	  

- Step 4** Click **Allocate Resources** to assign devices to different servers.

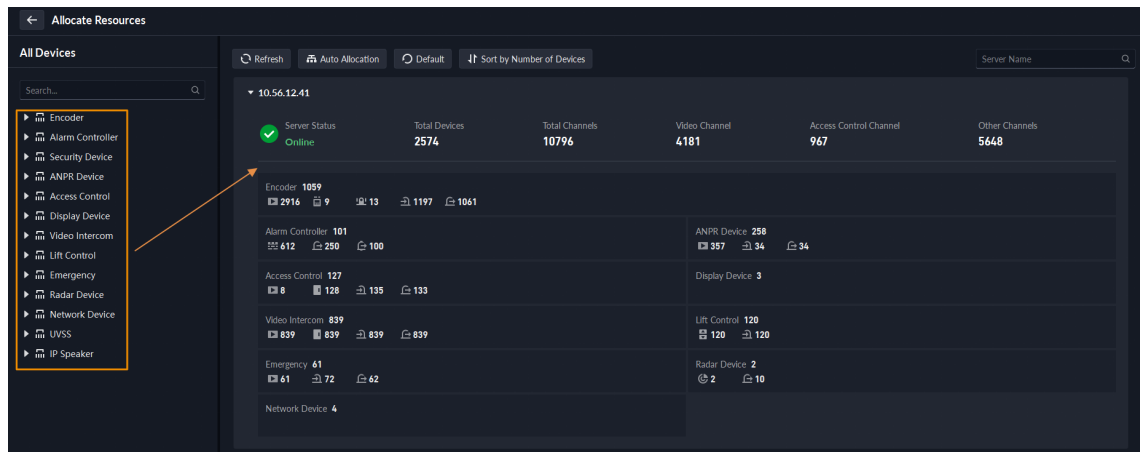
- Manually

Select devices or channels on the left side, and then drag them to the server on the right. The number of corresponding devices in the target server increases, and the devices in the original server reduces.



- Click **Default**, the servers are sorted in the order in which they were added.
- Click **Sort by Number of Devices**, the servers will be sorted by the number of devices.

Figure 7-2 Resource allocation

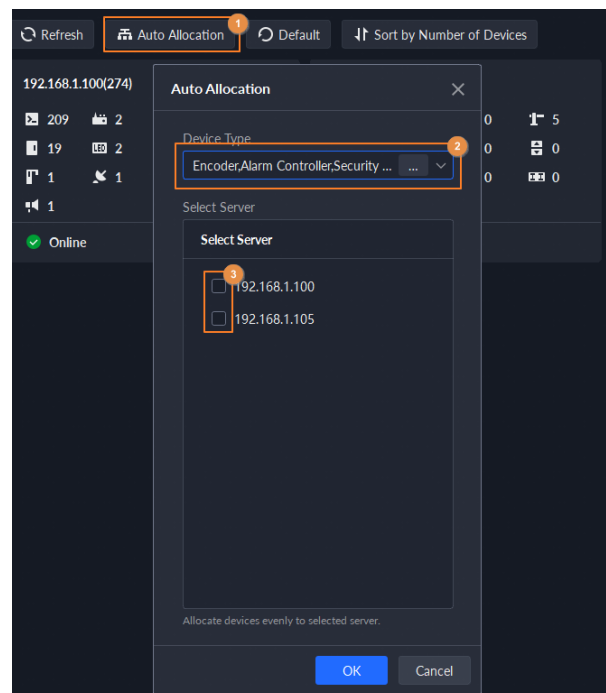


Automatic allocation

Allocate the same type of devices evenly to different servers.

1. Click **Auto Allocation**.
2. Select device type. Multiple types are supported.
3. Select the server to which the devices belong. Multiple servers can be selected.
4. Click **OK**.

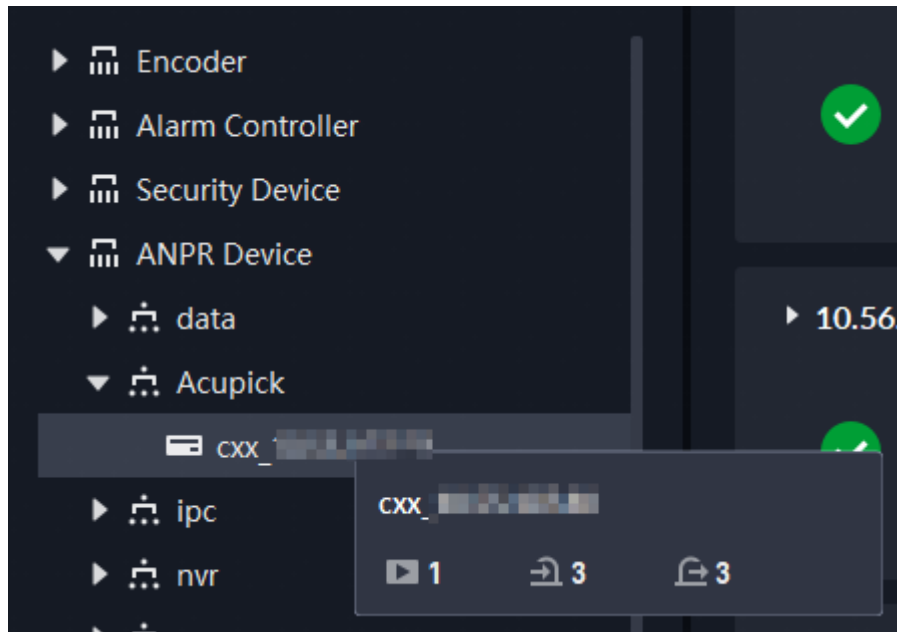
Figure 7-3 Auto allocation



Related Operations

When hovering the mouse over the device, the device name, channel type, and the number of the device will be displayed.

Figure 7-4 Information display



7.1.2 Cascade Deployment

Cascade deployment allows you to add a lower-level platform to an upper-level platform. After cascading, you can view the live video and recorded video of the lower-level platform from the upper-level platform. Also, you can display the videos on the lower-level platform on wall from the upper-level platform. 3 levels can be added at most.

Prerequisites

Make sure that the deployment of all relevant platforms has been completed.

Background Information

- You need to configure the lower-level platform information on the upper-level platform.
- Supports adding DSS Express to lower-level platform.

Procedure

- Step 1** Log in to client of the upper-level DSS platform. On the **Home** page, click , and then in the **System Config** section, select **System Deployment**.
- Step 2** Click **Cascade Config**.
- Step 3** Click **Add**, and then configure parameters.
- Step 4** After configuration, click **OK**.

Figure 7-5 Add cascade

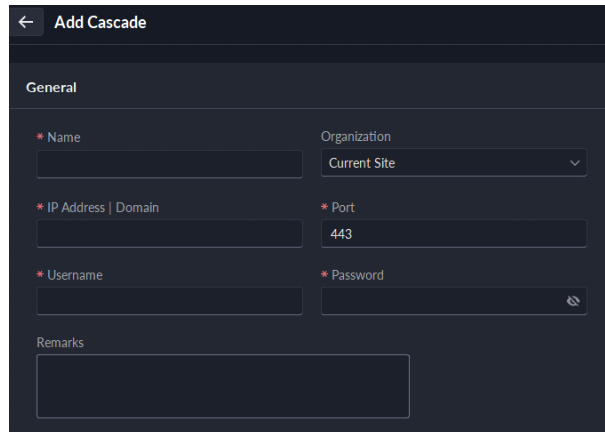


Table 7-1 Description of cascade parameters

Parameter	Description
Name	The name that identifies the platform to be added.
Organization	The organization that the added (lower-level) platform belongs to. The devices and channels of the added platform can be viewed on the upper-level platform from the organization that you have defined.
IP Address/Domain	The IP address or domain name, and the port of the added (lower-level) platform.
Port	
Username	The username and password for logging in to the added (lower-level) platform.
Password	

7.2 License Information

Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **License**.

- Click  to view the corresponding instructions.
- Click  to copy the activation code and serial number.
- Click **Export** to export the hardware information in .zip format.
- Click  of an activation code to view its details, such as time of activation and resources you can connect to the platform.

7.3 License

The system controls channel and function availability through the license. User can buy a license according to the channels and functions as needed.



The platform is unlicensed by default after being deployed.

License Types

- Trial

A trial license is limited in capacity and expires in 90 days.

- Paid

To acquire full control of the features and permanent use, you need to buy a formal license. After activating the first paid license, if you want to increase your license capacity, you can buy more license codes. For example, if you have 500 channels currently, you can buy another 600 channels. After activating the new 600 channels, you will have 600 channels.

The paid version supports the subscription licensing mode, which only supports subscribing license of video channels.

- Unlicensed

Unlicensed versions and expired versions. Lack permissions to use the system. This occurs after deactivating.



For expired trial version and unlicensed version, all modules are displayed as unauthorized, except for the resources, license, tools, and management modules.

Activation Methods

- Normal online activation

When the platform server is connected to the Internet, it can connect to the license server, which supports online license activation by verifying the activation code.

- Normal offline activation

When the platform server is on a local area network, it cannot connect to the license server. You need to obtain the license file from a computer with Internet access, and then import the license file to the platform to activate it.

- Upgrade from DSS Express to DSS Pro

- ◇ Online activation

When the platform is upgraded from Express to DSS Pro, and the original Express has a purchased license, and the platform server has Internet access, you can activate through verifying the new activation code and Express activation code (or importing Express deactivation file).

- ◇ Offline activation

When the platform is upgraded from Express to DSS Pro, and the original Express has a purchased license, the platform server cannot visit the license server. You can activate through verifying the new activation code and Express activation code (or importing Express deactivation file) and then importing the license obtained from a computer with Internet access.

7.3.1 Activating License

You can get the desired features or number of channels only after you load the corresponding license.



The official authorization supports a subscription model, enabling users to purchase subscription licenses.

For details about activating a license, see "2.1.6.2 Activating License".

7.3.2 Deactivating License

After deactivation, the platform will be unauthorized. A deactivated license can be activated again on other servers, allowing users to change servers. The license can be deactivated with online and offline deactivation. If the server is connected to the network, use online deactivation. Otherwise use offline deactivation.

7.3.2.1 Online Deactivation

Select this method if your platform sever is connected to a network.

Background Information

When deactivating hot standby, make sure that the connection between the active and standby servers is normal; otherwise, you cannot deactivate the standby server.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **License**.

Step 2 Click **Deactivate License**, and then select **Online Deactivation**.

Step 3 Click **OK**.



The license is reusable. We recommend copying the license code by clicking  and then saving it locally.

Step 4 Click **Deactivate Now**, and then follow the onscreen instructions to finish deactivation.



Hot standby activation can only be performed after its deployment is complete.

Figure 7-6 Online deactivation

←

Deactivate Online

Please make sure that the main server has access to the Internet.

General

After deactivation, DSS will lose revoked. The deactivated license can be activated again on other servers. Please record and keep the license properly, and confirm whether deactivation is needed.

Activation Code

71 752

08 847

08 D24

Hot Spare

Active Server IP

10 35

Standby Server IP

10 40

Deactivate Now

Cancel

7.3.2.2 Offline Deactivation

Select this method if your platform server has no Internet access.

Background Information

When deactivating hot standby, make sure that the connection between the active and standby servers is normal; otherwise, you cannot deactivate the standby server.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **License**.
- Step 2 Click **Deactivate License**, and then click **Offline Deactivate License**.

Figure 7-7 Offline deactivation

Step 3 Click **Export** to export and save the license deactivation file locally.



After the license deactivation file is exported, the platform will become unauthorized, and you cannot use any function.

Step 4 Move the request file to a computer with Internet access. On that computer, open the system email that contains your license, and then click the attached URL go to the license management page.

Step 5 Select **DSS > Deactivate License**.

Step 6 Upload the license request file obtained from Step 3, and then follow on-screen instructions to finish the process.

7.3.3 Maintenance Renewal

Displays the maintenance information. You can extend the maintenance time for non-subscription paid license.

Procedure

Step 1 Log in to the client, on the main page, click .

Step 2 Select **License**.

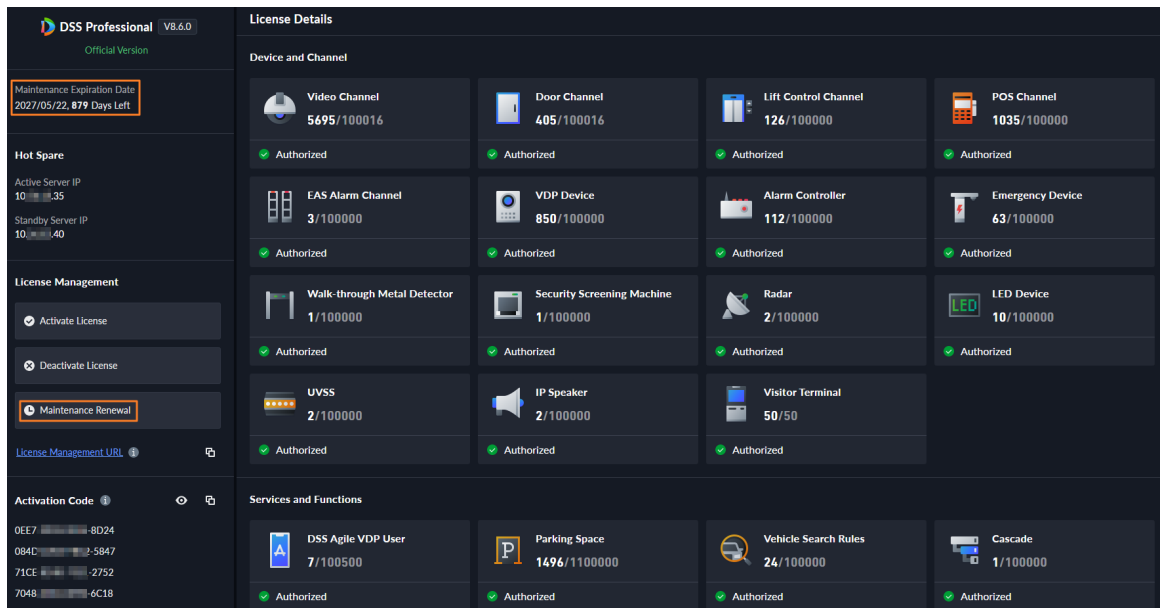


In the **Activation Code** area, you can:

- Click  to view the activation code. You can click each activation code to view the license type, activation time, maintenance expiration date, resource type and quantity involved in the license, maintenance information, and more.

- Click  to copy the activation code.

Figure 7-8 License information



License Details	
Device and Channel	
Video Channel 5695/100016 Authorized	Door Channel 405/100016 Authorized
Lift Control Channel 126/100000 Authorized	POS Channel 1035/100000 Authorized
EAS Alarm Channel 3/100000 Authorized	VDP Device 850/100000 Authorized
Alarm Controller 112/100000 Authorized	Emergency Device 63/100000 Authorized
Walk-through Metal Detector 1/100000 Authorized	Security Screening Machine 1/100000 Authorized
Radar 2/100000 Authorized	LED Device 10/100000 Authorized
UVSS 2/100000 Authorized	IP Speaker 2/100000 Authorized
Visitor Terminal 50/50 Authorized	
Services and Functions	
DSS Agile VDP User 7/100500 Authorized	Parking Space 1496/1100000 Authorized
Vehicle Search Rules 24/100000 Authorized	Cascade 1/100000 Authorized

License Management

- Activate License
- Deactivate License
- Maintenance Renewal

Hot Spare

Active Server IP: 10.10.10.35
Standby Server IP: 10.10.10.40

Activation Code

0EE7-8D24
084C-5847
71CE-2752
7048-6C18

Step 3 The version information and maintenance expiration date and activation code are displayed.

Step 4 (Optional) You can extend the maintenance time, when it expires.

- Online maintenance renewal.
 - Enter the maintenance activation code. Supports entering multiple activation code.
 - Select the function resource activation code to be maintained.
 - Click **Activate Now**.

Figure 7-9 Online maintenance renewal

Online Maintenance Renewal

Step 1: Enter the maintenance activation code

Maintenance Activation Code

+

-

-

Step 2: Select the function resource activation code to be maintained

Maintenance renewal will extend the maintenance period of the activation code for the function license. Please make sure that the number of maintenance resources for the selected function license activation code is the same as the number of maintenance resources for the maintenance activation code.

☒	Activation Code	Maintenance Resources
☒	5 5	1300032
Total		1300032

Activate Now

Cancel

- Offline maintenance renewal.
 1. Enter the maintenance activation code. Supports entering multiple activation codes.
 2. Select the function resource activation code to be maintained.
 3. Click **Export** to export offline license request file.
 4. Click **DSS License Management** to open the license management webpage or click  to copy the license management address and then open it through a browser.
 5. Click  to upload the request file, and then click **Activate**.

Figure 7-10 Offline maintenance renewal

Offline Maintenance Renewal

Maintenance renewal will extend the maintenance period of the activation code for the function license. Please make sure that the number of maintenance resources for the selected function license activation code is the same as the number of maintenance resources for the maintenance activation code.

☐	Activation Code	Maintenance Resources
☐	XXXXXXXXXX	1300032
Total		0

Export offline license request file

Export

Step 3:Upload Request File
Open the license management webpage of DSS on a computer with Internet access, and then upload the offline license application file that was exported.

[DSS License Management](#)

Step 4:Activate
Import the activation file that you obtained.

File Path

7.4 System Parameters

Configure security parameters, storage retention duration, email server, time sync, remote log, login method, and more.

7.4.1 Configuring Security Parameters

Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameter** > **Security Parameter**, and then configure the parameters.

Table 7-2 Parameter description

Parameter	Description
Certificate Management	A CA certificate is used to validate the legitimacy of the platform. When accessing the platform through a browser, the browser will validate the certificate. If the certificate is installed in the browser, the browser will consider the platform as secure, and will grant it access. If the certificate is not installed in the browser, the browser will not consider the platform as secure, and will not grant it access. You can create, import, and download certificates on the platform. ● Create a certificate: After creating a certificate, import it to the computer that will access the platform. ● Import a certificate: You can import a certificate that has been created to the platform.
File Security Policies	Protect your data by verifying login password when download or export information, and encrypting the export files. ● File Export or Download Password Authentication : ◇ You need to enter the password of the current account to export or download files. ◇ For all users that log in to the platform, they do not need to enter the password when exporting or downloading files. ● File Export and Download Encryption : You need to set an encryption password for files to be exported or downloaded. When anyone uses the files, they need to verify the encryption password.
HTTP Allowlist	After the firewall of the server is enabled, you need to add the IP address of the computer where the DSS Client is installed to the HTTP allowlist so that it can access the server.
RTSP Redirecting Allowlist	After the firewall of the server is enabled, only the IP addresses in the RSTP allowlist can request video stream through the media gateway service. The IP addresses of decoders will be added automatically. If there are other IP addresses that need to request video stream through media gateway service, you need to manually add them to the RSTP allowlist.
Generic Event Allowlist	Click Add , and then add the IP address for receiving generic events from third-party system or device to the allowlist. This helps ensure system security.
Synthesis Allowlist	Click Add , and then add the IP addresses of third-party systems to the allowlist of DSS before they can be integrated with DSS through Modbus, BACnet, and SNMP protocols.

7.4.2 Configuring Retention Period of System Data

Set the retention periods for various types of records. The expired records will be automatically deleted.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.
- Step 2 Click **Message Retention Period**.
- Step 3 Double-click a number to change its value.

Step 4 Click **Save**.

7.4.3 Time Synchronization

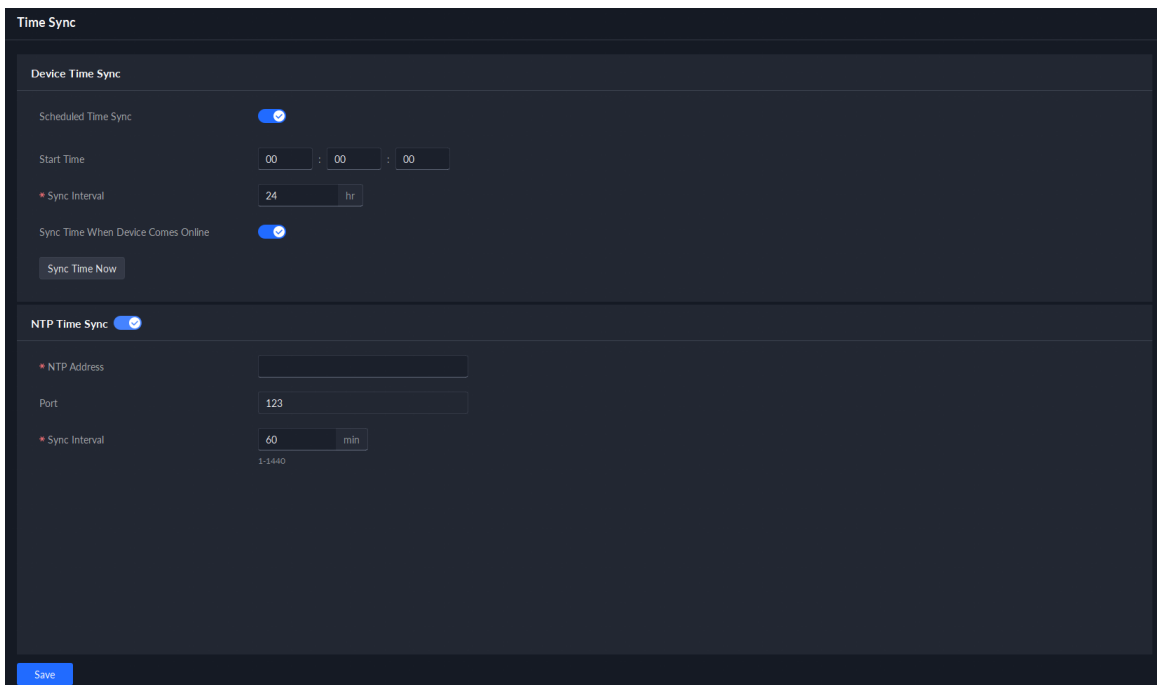
Synchronize the system time of all connected devices, PC client, and the server. Otherwise the system might malfunction. For example, video search might fail. The platform supports synchronizing the time of multiple devices, which have the same time zone as the platform. You can synchronize the time manually or automatically.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.

Step 2 Click the **Time Sync** tab, enable the sync methods, and then set parameters.

Figure 7-11 Enable time synchronization



- **Scheduled Time Sync** : Enable the function, enter the start time in time sync for each day, and the interval.
- **Sync Time When Device Comes Online** : Syncs device time when the device goes online.
- **NTP Time Sync** : If there is an NTP server in the system, you can enable this function so that the system can synchronize its time with the NTP server.

Step 3 Click **Save**.

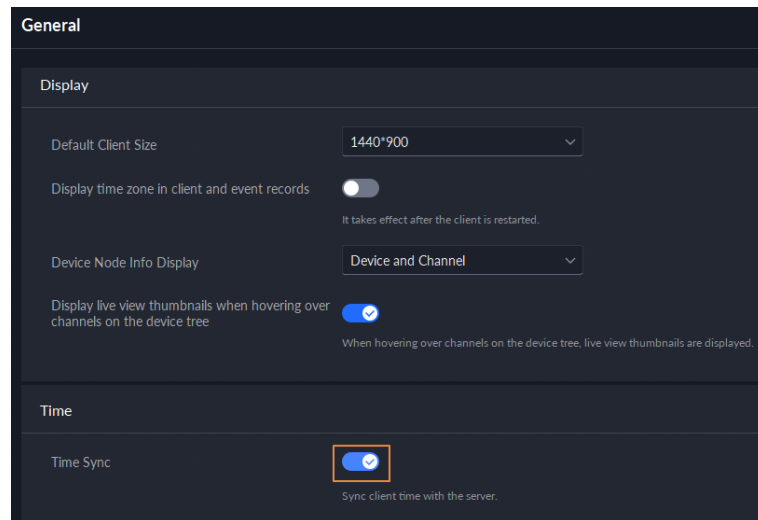
Step 4 Enable time synchronization on DSS Client.

1. Log in to the DSS Client, and then in the **Management** section, click **Local Settings**.
2. Click the **General** tab, select the check box next to **Time Sync**, and then click **Save**.



The system immediately synchronizes the time after you restart the client to keep the time of the server and the PC client the same.

Figure 7-12 Enable time sync



3. Restart the client for the configuration to take effect.

7.4.4 Configuring Central Intelligent Server

Configure the parameters of AcuPick, and select the central intelligence server, so that the AcuPick and video analysis functions can work normally.

Prerequisites

Purchase a license with the AcuPick function, and then activate the license. For details, see "2.1.6 Licensing".

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.
- Step 2** Click the **Central Intelligent Server** tab.
- Step 3** Enable or disable the AcuPick central intelligence comparison function. If it is enabled, you need to configure the parameters as shown in the following table.
 - Disabled: Only device comparison can be used.
 - Enabled: Both central intelligence comparison and device comparison can be used.

Table 7-3 Parameter description

Parameter	Description
IP/Domain Name	• Get the VIP automatically when the system is hot standby deployment. ◇ When the AcuPick parameter is not modified, displays the IP address as 127.0.0.1 by default. ◇ After manually modify the AcuPick IP and save it, the modified IP address will be displayed. • When the system deployment methods are standalone deployment and configuring LAN or WAN, displays the IP address as 127.0.0.1 by default.
Port	Enter the port number of the server deployed with the AcuPick algorithms.

Parameter	Description
Identity Certificate	Click  to copy the identity certificate and secret key, and then configure them to the DSS server. For details, see "2.1.4 Management Tool".
Secret Key	Click  to generate a new secret key.
Test AcuPick Function	Click the button to check if the function is working normally. If not, address the issue prompted by the platform, and then check again. Repeat the steps until it can work normally.

Step 4 Select devices to be used as the central intelligence server.

Step 5 Click **Save**.

7.4.5 Configuring Email Server

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.

Step 2 Click the **Email Server** tab, enable **Email Server**, and then configure parameters as required.

Table 7-4 Description of email server parameters

Parameter	Description
SMTP Server Type	Select according to the type of SMTP server to be connected. The types include Yahoo , Gmail , Hotmail , and UserDefined .
Sender Email Address	The sender displayed when an email is sent from DSS.
SMTP Server	IP address, password, and port number of the SMTP server.
Password	
Port	
Encryption Method	Supports no encryption, TLS encryption, and SSL encryption.
Test Recipient	Set the recipient, and then click Email Test to test whether the mailbox is available.
Email Test	

Step 3 Click **Save**.

7.4.6 Configuring Active Directory

Before importing domain users, you need to configure domain, including domain name/IP, port, username and password.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameter** > **Active Directory**.

Step 2 Click  to enable the function, and then configure the parameters of the domain, including SSL private key, domain name/IP, port, username and password.



Click **Change Password** to change the domain password.

Step 3 Click **Get DN** to automatically get the basic DN information.

Step 4 Click **Test** to check whether the domain information is correct.

Step 5 Enable the automatic synchronization function and set a time. The platform will automatically synchronize new users in user groups that you have imported previously, and update the information of the users imported by manual selection at the defined time every day.

For example, you have imported the entire user group A. The platform will synchronize new users in user group A every day at the defined time. Click  to remove a group on the list, and then it will not be synchronized. For users imported by manual selection, the platform will check their information, and update if anything changes.

Step 6 Click **Save**.

7.4.7 Configure POS Parameters

You can configure the sign that prompts the end of a POS receipt, the duration of related video when you search for the POS records in **DeepXplore**, and POS fields for the POS receipts.

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.

Step 2 Click the **POS Config** tab, and then configure the POS parameters.

- **POS End Sign** : The sign that prompts the end of a POS receipt.
- **POS Video Config** : The duration of POS-related videos that can be viewed when searching for POS records on the **DeepXplore** page. For example, when it is set to 1 minute, you can watch 30 seconds of related videos before and after the POS record.
- **POS Field Config** : Configure POS fields for the POS receipts, and then click  to enable them. The POS fields that you have configured will be used to search for certain information in the transactions. For example, the POS field for original price is TOTAL, then the platform will obtain the number for TOTAL and return the results.

The configuration is effective for all POS records.

Figure 7-13 POS end sign

POS Config

POS End Sign

* POS End Sign

Thank You!

POS Video Config

POS Video Config

1min

POS Field Config

Receipt Field	POS Field	Operate
POS ID		☐
Original Price	TOTAL	☒
Discounted Price		☐
Refund		☐
Cashier		☐
Other		☐

Save

Step 3 Click **Save**.

7.4.8 Configure Device Access Parameters

To ensure that you can safely use the devices, we recommend using the security mode if devices support this mode to avoid security risks. The platform also supports enabling and disabling adding devices through P2P.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameter** > **Device Adding Config**.
- Step 2 Select a device login mode, and then click **Save**.
- Step 3 Enable or disable the P2P function.
- If disabled, you cannot add devices to the platform through P2P.

7.4.9 Remote Logs

To ensure safe use of the platform, the system sends administrator and operator logs to the log server for backup at 3 am every day.

Procedure

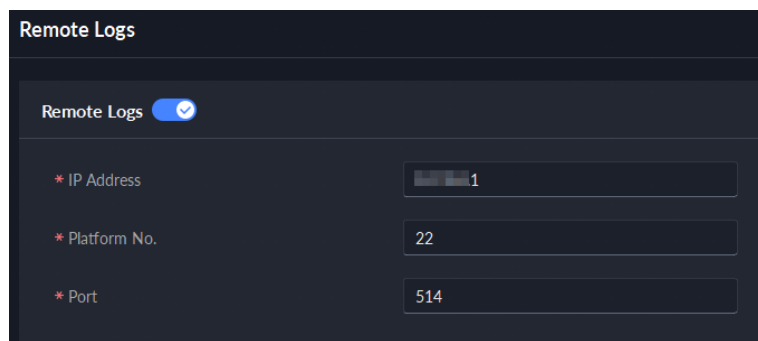
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.

Step 2 Click the **Remote Logs** tab.

Step 3 Enable the function, and then set parameters as required.

The **Platform No.** must be the same on the remote server and the platform.

Figure 7-14 Enable remote logs



Step 4 Click **Save**.

7.4.10 Configuring Independent Database

The platform supports connecting to an independent database and storing data in it, including face images, video metadata, events, and ANPR information. Only official licenses support this function.

Prerequisites

- You have prepared a ready-to-run database.
- You need to select the type of the independent database, and configure the database information on DSS, so that DSS has the authority to create databases and tables for the external independent database.

After configuring the database, DSS has a special script to automatically create databases and tables, and you do not have to manually create databases and tables again.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.

Step 2 Click the **Independent Database Deployment** tab.

Step 3 Click  to enable the function, and then configure the parameters.

Table 7-5 Parameter description

Parameter	Description
Database Type	Supports MySQL, SQL Server 2016, and SQL Server 2022.
IP Address	Enter the IP address of the database.

Parameter	Description
Port	Enter the port of the database.
Username	Enter the username and password used to log in to the database.
Password	

Step 4 Click **Save**.



An independent database can only connect to one platform.

Results

After an independent database is deployed, face images, video metadata, events, and ANPR information will only be stored in the independent database, and will not be stored in the local database anymore. Also, when you search for these 4 types of data, the platform will only search the independent database. The data that was previously generated in the local database will not be available for the search.

7.4.11 Configuring Push Notification for App

If you need to send messages to App, you must enable this function. After enabled, messages will be sent to App through the servers of push notification providers. Data related to these messages will not be sent back to us.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters** > **Mobile App Config**.

Step 2 Enable or disable push notification.

If disabled, the app will not receive any offline push notifications, such as offline alarms and offline calls.

7.4.12 Configuring Network Device Protocol

When adding a third-party network device that supports the SNMP protocol (such as a switch), you must upload the SNMP protocol of the network device to the DSS platform first.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.

Step 2 Click **Network Device Protocol Config**, and then click **Add**.

Step 3 On the **Upload Protocol** page, enter the name of the device manufacturer.

Step 4 Click **Download Template** to download the Excel template.

Step 5 In the template, enter the corresponding OID number in the SNMP protocol function supported by the network device.



The OID number must be filled in correctly to ensure that the switch connected through the SNMP protocol works properly.

Step 6 Click **Upload File**, upload the SNMP protocol MIB file, and then click **OK**.

- Click  to delete the uploaded protocol file.

- Click  to download the protocol file.

Step 7 Click  to enable SNMP trap configuration, and then you can configure the trap information of the network device connected by SNMP protocol. This ensure that the third-party network device can send alarms to the platform normally.



SNMP trap configuration is only applicable to network devices that accesses the platform through SNMP V3 version.

- **User Name** : Username of SNMP trap.
- **Authentication Type** : You can select from **None**, **MD5** and **SHA**. When selecting **MD5** or **SHA**, you need to set the authentication password.
- **Encryption Type** : You can select from **None**, **CBC-DES**, and **CFB-AES**. When selecting **CBC-DES** or **CFB-AES**, you need to set the encryption password.

Step 8 Click **Save**.

7.4.13 Configuring Privacy Policy

You can select enable or disable **Store Face Snapshot Records** as needed. When it is disabled (default), the platform will not display or store face snapshot records that do not include comparison records.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.

Step 2 Click **Privacy Policy**.

Step 3 Enable or disable **Store Face Snapshot Records** as needed (disabled by default).

When it is disabled, the platform will not display or store face snapshot records that do not include comparison records.

If you enable this function, the face snapshot records will be saved, and the prompt of **Only displays the face comparison records. If you want to display the face snapshot records, please enable Store Face Snapshot Records in System Parameters and Privacy Policy** will be displayed on the pages of face recognition records in **Monitoring Center**, and face capture records in **DeepXplore**, and the pages of adding recording task and local task in **Video Analysis** . Use this function ethically and securely in accordance with applicable laws.

7.5 Backup and Restore

The platform supports backing up configuration information and saving it to a computer or server, so that you can use the backup file for restoring settings.

7.5.1 System Backup

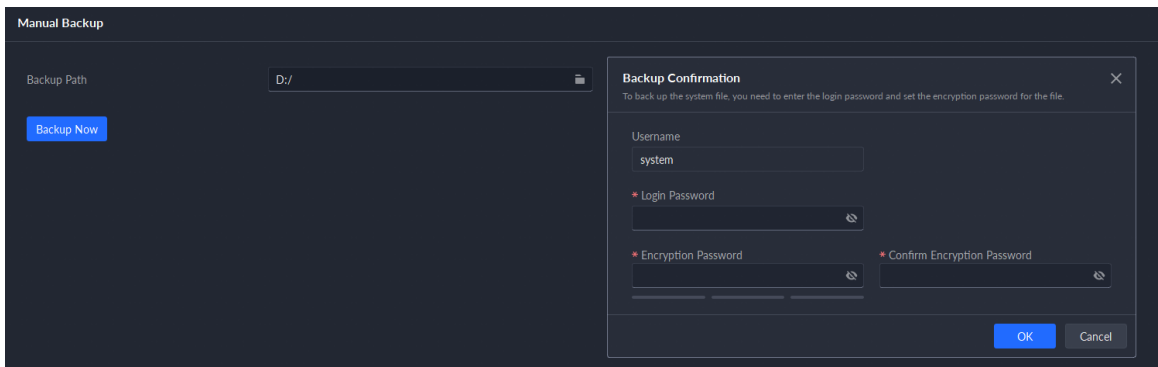
Use the data backup function to ensure the security of user information. Data can be manually or automatically backed up.

- **Manual backup**: Manually back up the data, and the DSS platform will save it locally.
- **Automatic backup**: The DSS platform automatically backs up the data at a defined time, and saves it to the installation path of the platform server.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **Backup and Restore**.
- Step 2** Click the **Backup** tab.
- Step 3** Back up data.
 - Manual backup: In the **Manual Backup** section, select the data saving path, click **Backup Now**. The **Login Password** is the same as the system user's. Create an **Encryption Password** to protect data.

Figure 7-15 Manual backup

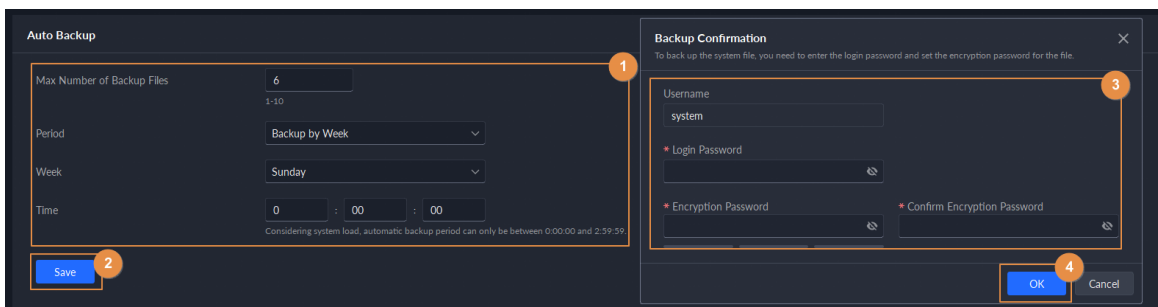


- Auto backup: In the **Auto Backup** section, configure backup parameters, and then click **OK**. The **Login Password** is the same as the system user's. Create an **Encryption Password** to protect the data. The platform automatically backs up data according to the defined time and period. The backup path is the installation path of the platform server by default.



Max Number of Backup Files means you can only save defined number of backup files in the backup path.

Figure 7-16 Auto backup



7.5.2 System Restore

Restore the data of the most recent backup when the database becomes abnormal. It can quickly restore your DSS system and reduce loss.

- Local Restore: Import the backup file locally.
- Server Restore: Select the backup file from the server.

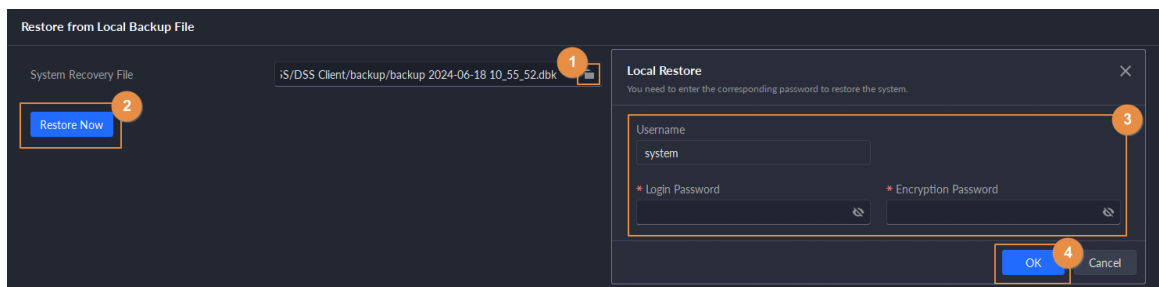


- Users must not use the platform when you are restoring the configurations.
- Restoring the configurations will change the data on the platform. Please be advised.

Procedure

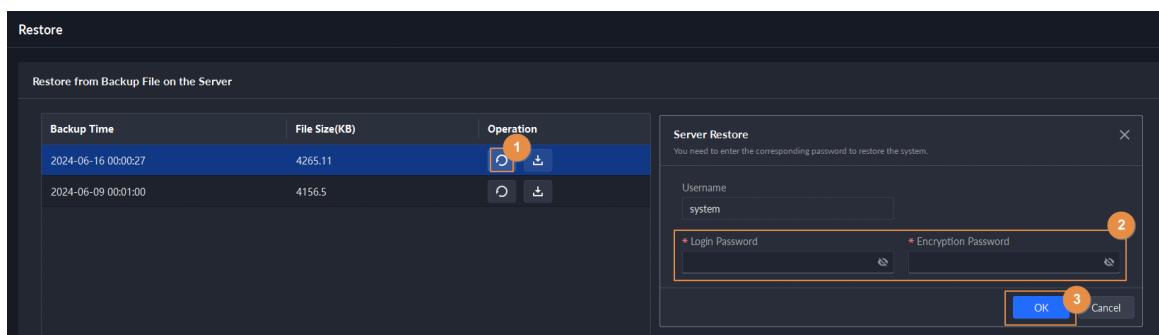
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **Backup and Restore**.
- Step 2** Click the **Restore** tab.
- Step 3** Restore data.
- Restore from local backup file: In the **Restore from Local Backup File** section, select the backup file path, click **Restore Now**, and then enter the passwords (the **Password** is the same as the system user's. The **Encryption Password** is the one created when the file was backed up).

Figure 7-17 Local restore



- Restore from backup file on the server: In the **Restore from Backup File on the Server** section, click , enter the passwords (the **Password** is the same as the system user's. The **Encryption Password** is the one created when the file was backed up), and then click **OK**. After restoration, the platform will automatically restart.

Figure 7-18 Restore from backup files on the server



You can click  to download the backup file.

8 Management

8.1 Download Center

You can download videos stored on the server or the device. They can be saved in are in .dav (default), .avi, .mp4, or .asf formats. For H.265 videos, they can only be saved in .dav formats. To download a video, you can:

- Select a duration on the timeline.
- Download videos by files. The system will generate files every 30 minutes from the time the video starts. If the video does not start on the hour or the half hour, the first file will start from the earliest start time to the half hour or the hour. For example, if a video starts from 4:15, the first file will be from 4:15 to 4:30.
- Download a period before and after a tag.
- Download a video defined by a locking record.

The maximum size of a video file is 1024 MB by default. You can change it to control how many files will be generated when you download a video by timeline or tag. For details, see "8.4.5 Configure File Storage Settings".

8.1.1 By Timeline or File

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Download Center** > **Download Video**.

Step 2 Configure the search conditions, and then click **Search**.

Step 3 Download videos.



By default, you need to verify your password and configure an encryption password before download. You can configure whether to verify the password. For details, see "7.4.1 Configuring Security Parameters".

- Download a video by selecting a duration on the timeline.



If you set the **Search Type of Device Video Stream** to **Main Stream and Sub Stream 1**, you can download videos recorded in main stream or sub stream for videos stored on devices. For details, see "8.4.2 Configuring Video Settings".

1. Click the **Timeline** tab, and then select a period on the timeline.
 2. On the pop-up page, adjust the length of the video.
 3. (Optional) Click  to select a format of the video. If this function is not enabled, the video will be saved in .dav format by default.
 4. Click **OK**.
- Download a video by file.

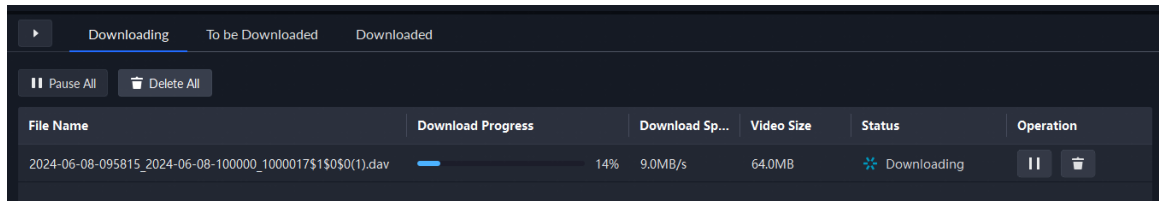
Click the **File** tab, and then click  to download a file.

You can also select multiple files, and then click **Download Selected File** on the upper-left corner to download them at the same time.

Related Operations

- You can pause, resume, and delete a download task.

Figure 8-1 Download progress



- After download completes, click **Open Folder** to go to the path where the video is saved to, or click **Open** in the prompt on the upper-right corner to play the video directly in **Local Video**. For details, see "8.3 Playing Local Videos".

8.1.2 By Tagging Record

Search for tagging records on the platform and download relevant videos.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Download Center** > **Tagging Records**.
- Step 2 Configure the search conditions, and then click **Search**.

Table 8-1 Parameter description

Parameter	Description
Site	If you have logged in to multiple sites, you can select which one you want to search for tags from.
Select Channels	The platform displays channels in the site you selected. Select one or more channels to search for tags from. Unlimited: The platform will search all channels. : Manually select channels.
Time	Configure the time to search for tags within it.

- Step 3 Click to download one video at a time, or select more tags, and then click **Download Selected Tagged File** to download multiple videos at the same time.
- Step 4 Verify the login password and configure the encryption password, and then click **OK**.

By default, you need to verify your password and configure an encryption password before download. You can configure whether to verify the password. For details, see "7.4.1 Configuring Security Parameters".
- Step 5 Configure the length of the video, whether you want to convert the video format, and then click **OK**.

Related Operations

Click to delete a tag, or select more tags, and then click **Download Selected Tagged File** to delete them in batches. This operation will only delete the tags. It will not delete the videos.

8.1.3 By Locking Record

Search for locking records on the platform and download relevant videos.

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, select **Management** > **Download Center** > **Locking Records**.
- Step 2** Configure the search conditions, and then click **Search**.

Table 8-2 Parameter description

Parameter	Description
Site	If you have logged in to multiple sites, you can select which one you want to search for locked videos from.
Select Channels	The platform displays channels in the site you selected. Select one or more channels to search for locked videos from. Unlimited : The platform will search all channels. : Manually select channels.
Time	Configure the time to search for locked videos within it.

- Step 3** Click  to download one video at a time, or select more records, and then click **Download Selected Locked Video** to download multiple videos at the same time.
- Step 4** Verify the login password and configure the encryption password, and then click **OK**.

By default, you need to verify your password and configure an encryption password before download. You can configure whether to verify the password. For details, see "7.4.1 Configuring Security Parameters".
- Step 5** Configure the length of the video, whether you want to convert the video format, and then click **OK**.

Related Operations

Click  to unlocked a video, or select more records, and then click **Unlocked Video** to unlock them in batches. After unlocked, the videos can be overwritten or deleted.

8.2 Viewing Local Images

You can view snapshots taken by clicking  on the video image from the monitoring center.

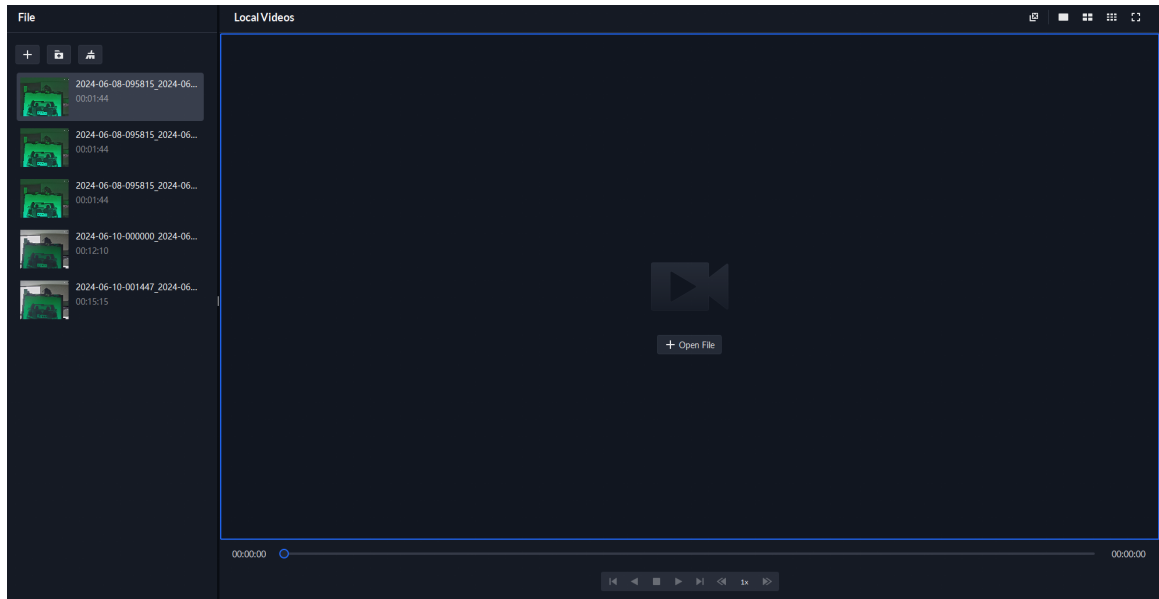
8.3 Playing Local Videos

You can play local videos directly on the platform.

Procedure

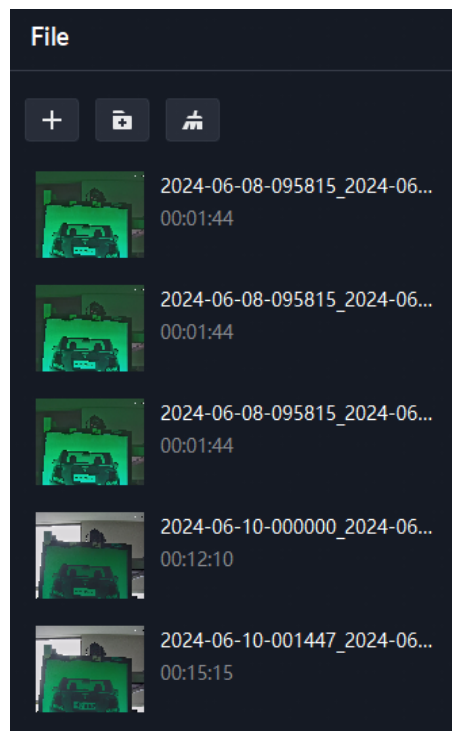
- Step 1** Log in to the DSS Client. On the **Home** page, select **Management** > **Local Video**.

Figure 8-2 Local video



Step 2 Click  to select one or more files, or  to open all files in a folder.

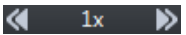
Figure 8-3 Play list



Step 3 Drag a file to the window on the right or right click it to play.

Related Operations

Table 8-3 Interface operation

Icon/Function	Description
Right-click menu	• Continuous Snapshot : Take snapshots of the current image (2 snapshots each time by default). The snapshots are saved to <code>..\DSS\DSS Client\Picture</code> by default. To change the snapshot saving path, see "8.4.5 Configure File Storage Settings". • Video Adjustment : Adjust the brightness, contrast, saturation, and chroma of the video for video enhancement. • Digital Zoom : Click and hold to select an area to zoom in on it. Double-click the image again to exit zooming in.  You can also scroll to zoom in and out.
	Close all playing videos.
	Split the window into multiple ones and play a video in full screen.
	Take a snapshot of the current image and save it locally. The path is <code>C:\DSS\DSS Client\Picture\</code> by default.
	Close the window.
	Stop/pause the video.
	Fast/slow playback. Max. supports 64X or 1/64X.
	Frame by frame playback/frame by frame backward.
	Capture the target in the playback window. Click  to select the search method, and then the system goes to the page with search results. More operations: • Move the selection area: Hover over the selection area, and then left-click to move. • Adjust the size of the selection area: Hover over the upper-right, upper-left and lower-left corner of the selection area, and then left-click to adjust. • Right-click to exit search by snapshot.

8.4 Configuring Local Settings

After logging in to the client for the first time, you need to configure the following fields under system parameters: Basic settings, video parameters, record playback, snapshot, recording, alarm, video wall, security settings and shortcut keys.

8.4.1 Configuring General Settings

Configure client language, client size, time, and more.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **General**, and then configure the parameters.

Table 8-4 Parameter description

Parameters	Description
Default Client Size	The size of the client when it is not maximized. Select a proper resolution according to your screen.
Display time zone in client and event records	When selected, the client and the time of alarms will show both the time and time zone.
Device Node Info Display	Select that the device tree displays devices and their channels or only channels.
Display live view thumbnails when hovering over channels on the device tree	When selected, you can hover the mouse over a channel in the device tree in Monitoring Center and a snapshot of its live video image will be displayed.
Time Sync	If enabled, the client starts to synchronize network time with the server to complete time synchronization.
Auto run at startup	● If Remember Password has been selected on the Login page, select Auto restart after reboot, and the system will skip the login page and directly open the homepage after you restart the PC next time. ● If Remember Password is not selected on the Login page, select Auto restart after reboot, the client login page will appear after you restart the PC.
Auto Login	Enable the system to skip the login page and directly open the homepage when logging in next time. ● If Remember Password and Auto Login have been selected on the Login page, the function is already enabled. ● If Remember Password has been selected while Auto Login is not selected on the Login page, select Auto Login on the Basic page to enable this function. ● If neither Remember Password nor Auto Login has been selected on the Login page, select Auto Login on the Basic page and you then to enter the password when logging in next time to enable the function.
CPU Alarm Threshold	The user will be asked to confirm whether to open one more video when the CPU usage exceeds the defined threshold.
Audio and video transmission encryption	Encrypt all audio and video to ensure information security.
Client Inactive Status Config	If no operation is performed for the defined period, the client will be automatically locked or logged out. If you are logged out, all the tasks on the client will be suspended.
Self-adaptive audio talk parameters	If enabled, the system automatically adapts to the device sampling frequency, sampling bit, and audio format for audio talk.

Parameters	Description
Access Card Input and Display Mode	Select a mode for the platform to use and display access cards. For example, when you manually issue a card to a person, you can enter A-F and numbers in the card number if Hex is selected, but you can only enter 0-9 if Decimal is selected.
Joystick Sensitivity	Select the sensitivity for when you operate the joystick. The higher the sensitivity, the more frequent joystick commands are sent, and the greater the possibility that operations will be delayed due to poor performance of PTZ cameras.
Use Thousand Separator	Configure a separator for thousands. This will apply to all numbers on the PC client.
Decimal Separator	Select a separator for decimals. This will apply to all numbers on the PC client.

Step 3 Click **Save**.

8.4.2 Configuring Video Settings

Configure window split, display mode, stream type and play mode of live view, and instant playback length.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **Video**, and then configure the parameters.

Table 8-5 Parameter description

Parameters	Description
Default Window Split	Set split mode of the video window.
Window Display Scale	Select from Original Scale and Full Screen .
Stream Acquisition Mode	When the device and clients are properly connected to the network, direct acquisition can reduce the use of the platform's forwarding bandwidth. If too many clients are acquiring video streams from a channel, acquisition might fail due to insufficient performance of the device. At this time, video streams can be set to be forwarded to clients by the platform. ● Streaming Service Forwarding : Video streams will be forwarded to clients by the platform. ● Acquire directly from the device : Clients will acquire video streams directly from the channel. If direct acquisition fails, the platform will forward the video streams to clients.

Parameters	Description
Decoding Mode	● Software Decoding by CPU : All videos will be decoded by the CPU. When you are viewing live videos from large amount of channels, it will take up too much resources of the CPU that affects other functions. ● Hardware Decoding by GPU : All videos will be decoded by the GPU. The GPU is better at concurrent operation than the CPU. This configuration will free up resources of the CPU significantly. ● Performance Mode (CPU First) : All videos will be decoded by the CPU first. When selecting this mode, you need to set the CPU threshold. When the resources of the CPU are taken up to the defined threshold, the platform will use the GPU to decode videos.
CPU Threshold	
Video Toolbar Icon Size	Set the icon size on the toolbar when viewing real-time and recorded videos.
Visual Tracking Mode	Visual tracking of targets in single or multiple windows on the Live View and Playback pages.
AI Rule Overlay	After turning it on, when viewing live video or playing recordings, right-click the video window, the AI Overlay and SMD Overlay menu will be displayed. If you turn it off, these menus, the  icon on the live view and playback pages, and the overlaid information on the video image will not be displayed.
Close videos being played after long period of inactivity	The system closes live view or playback automatically after inactivity for a pre-defined period of time. Supports up to 30 minutes.
Inactivity Time	
Stream Switching Rule	When the number of window splits is greater than the defined value, the live video will switch from the main stream type to sub stream type.
Switches to Main Stream when Window Maximized	If selected, you can double-click a video window to maximize it and switch from sub stream to main stream. Double-click again to restore the window size, and then the system will switch it back to sub stream.
Display the previous live view after restart	If selected, the system displays the last live view automatically after you restart the client.

Parameters	Description
Play Mode	When playing videos, both fluency and real-time performance matter. To deal with network fluctuations, the platform has a set of buffer control strategies to ensure fluency and real-time performance. You can select one of the following play modes as needed. ● Real-time Play Priority : The system might lower the image quality to avoid video lag. It is suitable for special scenarios with high requirements on real-time performance. ● Fluency Priority : The system might lower the image quality and allow for lag to ensure video fluency. The higher the image quality is, the lower the video fluency will be. ● Balance Priority (recommended): The system balances real-time priority and fluency priority according to the actual server and network performance. ● Custom : The system adjusts video buffering and lowers the impact on video quality caused by unstable network. The bigger the value, the more stable the video quality will be.
Display Recording Status	You can select displaying or not displaying an icon on the upper-left corner of the window when recording is performed. Different icons will be displayed when you select Device Video , Central Recording or Simultaneous Display. By selecting Simultaneous Display, when device recording is performed, the  icon will be displayed; when central recording is performed, the  icon will be displayed; and when both device recording and central recording are performed, the  icon will be displayed.
Enable Multicast	Enable this function and configure the multicast parameters for video channels. When multiple PC clients want to view the real-time video from the same channel, the video will be sent to the clients through the router. This will reduce the bandwidth usage of the server.
Instant Playback Time	Click  on the live view page to play the video of the previous period. The period can be user-defined. For example, if you set 30 seconds, the system will play the video of the previous 30 seconds.
Search Type of Device Video Stream	Select a default stream type when you play back recordings from a device.  If Only Sub Stream 2 is selected, but the device does not support sub stream 2, then recordings of sub stream 1 will be played.
Play Priority	Select a default location for recorded videos when you play them, including Prioritize Device Recording for playing recorded videos stored on devices, and Prioritize Central Recording for playing recorded videos stored on the platform.

Parameters	Description
Frame Extraction Mode	Frame extraction helps ensure that the video runs smoothly and the pressure on decoding, bandwidth and forwarding is minimal when playing high-definition videos. When frame extraction is enabled, certain frames will be skipped. ● Do Not Extract : Frame extraction will not be enabled in any situation. ● Self-adaptive : The platform will enable frame extraction based on the resolution and the play speed. ● By Split Window : Some frames will be extracted when the number of split windows is greater than the defined split windows. No frames will be extracted when the window is maximized. ● Force : Frame extraction is always enabled.
Time Limit of Visual Tracking	The duration of video that the platform pulls when switching to the next linked channel during visual tracking. It ranges from 0 to 10 seconds, and is 2 seconds by default. For example, if you set the time limit as 2 seconds, when you switch to the next linked video, the platform will pull 2 seconds of the video from the linked channel before opening the video, so that you can smoothly switch to the video.
Continuous Snapshot Interval	Set the number of snapshots and the interval between each one. For example, if the Continuous Snapshot Interval is 10 seconds and the Number of Continuous Snapshots is 4, when you right-click on the live or recorded video and select Snapshot, 4 snapshots will be taken every 10 seconds.
Number of Continuous Snapshots	

Step 3 Click **Save**.

8.4.3 Configuring Video Wall Settings

Configure the default binding mode and stream type of video wall.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **Video Wall**, and then configure the parameters.

Table 8-6 Parameter description

Parameter	Description
Default Stream Type	Select Main Stream , Sub Stream 1 , Sub Stream 2 or Local Signal as the default stream type for video wall display.
Stream Switching Rule	When the number of window splits is greater than the defined value, the live video will switch from the main stream type to sub stream type.

Parameter	Description
Double-click on the video to maximize the window and switch to main stream	Double-click the video to maximize the window, and then its stream type will switch to main stream.
Video Source Play Duration	Set the default time interval between the channels for tour display. For example, if 5 seconds is configured and you are touring 3 video channels, the live video image of each channel will be played 5 seconds before switching to the next channel.
Mode of Video Decoding to Wall	● Tour : Multiple video channels switch to decode in one window by default. ● Tile : Video channels are displayed in the windows by tile by default. ● Ask Every Time : When dragging a channel to the window, the system will ask you to select tour or tile mode.

Step 3 Click **Save**.

8.4.4 Configuring Alarm Settings

Configure the alarm sound and alarm display method on the client.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **Alarm**, and then configure the parameters.

- Alarm sound

Table 8-7 Alarm sound parameter description

Parameter	Description
Custom	◇ Default : All types of alarms will use the same default alarm sound when triggered. ◇ Custom : Click Modify Alarm Sound, and then you can change the alarm sound and its play mode of each type of alarm. ◇ Play Audio Defined in Scheme : When an alarm is triggered, the platform plays the sound defined in  > Event > Event Config. For details, see "4.1.1 Configuring Event Linkage".
Play Config	When you select Play Audio Defined in Scheme, you can select Prioritize playing the audio configured for the event schemes, or Only play the audio configured for the event schemes.  The platform will play the default audio if no audio content is configured in Event Config.
Alarm Type	All Event Source Types by default, and cannot be modified.
Play Mode	Play Once by default, and cannot be modified.

Parameter	Description
Sound	Click , and then you can test playing the audio content.  This parameter is available when Prioritize playing the audio configured for the event schemes is selected.

- Mode of opening alarm linkage videos

Table 8-8 Parameter description of opening alarm linkage videos

Parameter	Description
Open alarm linkage video when alarm occurs	If selected, the platform will automatically open linked video(s) when an alarm occurs.  For this function to work properly, you must enable When an alarm is triggered, display camera live view on client when configuring an event. For details, see "4.1 Configuring Events".
Open Alarm Linkage Video	Configure how the platform plays the video when an alarm is triggered. ◇ As Pop-up : The alarm video will be played in a pop-up window. You can set how long the pop-up windows will be displayed, whether to display the pop-up windows and the client on the top of the screen, and link video only or link video and map. ○ Link Video: When an alarm is triggered, you can view the real-time video of the alarm channel in the pop-up window. ○ Link Video and Map: When an alarm is triggered, you can click the Video or Map tab to switch viewing the real-time video or the map information. ◇ Open in Live View : The alarm video will be played in a window in Monitoring Center. You can set how long the video will play, and whether to open the monitoring menu when alarm is triggered (Monitoring Center > Monitoring).  If Open Monitoring Menu When Alarm is Triggered is not enabled, when a channel set as an alarm window triggers an alarm, the platform will still open the monitoring menu and play the real-time video of that channel.

- Map flashes

Table 8-9 Parameter description related to map flashing

Parameter	Description
Device on the map flashes when alarm occurs	Set one or more alarm types for alarm notification on the map. When an alarm occurs, the corresponding device will flash on the map.
Alarm Type	

Parameter	Description
Map Flash Duration	Set the duration that the device flashes on the map when an alarm is triggered. You can select from 20 s , 40 s , 1 min , 5 min , 10 min , Always , or click Custom to customize the duration.

Step 3 Click **Save**.

8.4.5 Configure File Storage Settings

Configure the storage path, naming rule, file size, and format of recordings and snapshots.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **File Storage**, and then configure the parameters.

Table 8-10 Parameter description

Parameters	Description
Video Naming Rule	Select a naming rule for manual recordings.
Video Storage Path	Set a storage path of manual recordings during live view or playback. The default path is C:\Users\Public\DSS Client\Record.
Video File Size	Configure the maximum size of a video file. If you download a video that is larger than the defined size, the platform will divide it into multiple files. The maximum size can be up to 4 GB for 32-bit operating systems, and 1024 GB for 64-bit operating systems.
Image Format	Select a format for snapshots.
Image Naming Rule	Select a naming rule for snapshots.
Image Storage Path	Set a storage path for snapshots. The default path is C:\Users\Public\DSS Client\Picture.

Step 3 Click **Save**.

8.4.6 Viewing Shortcut Keys

View shortcut keys for operating the client quickly.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **Shortcut Key** to view shortcut keys of the PC keyboard and USB joystick.

8.4.7 Exporting and Importing Configurations

For the parameters in local settings configured by the user currently logged in to the PC client, they can be exported and imported to another PC client. This is helpful that the user does not need to configure the parameters again when using a new platform.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **Export/Import Configurations** on the lower-right corner.

Step 3 Export or import configurations.

- Export configurations.



The parameters of **Alarm Sound** and **Map Flashes** will not be included in the exported configurations.

1. Click **Export Configurations**.
2. Select **Export to File**, and then export the configurations to the specified path of your computer. Or select **Send by Email**, and send the configurations to the specified email address.
3. Click **OK**.

- Import configurations.

1. Click **Import Configurations**.
2. Click , and then open the exported file of configurations.
3. Click **OK**.

8.5 Managing Logs

View and export operator logs, device logs and system logs, and enable the service log debug mode for troubleshooting.

8.5.1 Operation Log

View and export logs that record users' operations, such as viewing the real-time video of a channel.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, select **Management > Logs > Operation Logs**.
- Step 2 Select one or more types of logs.
- Step 3 Specify the time and keywords, and then click **Search**.
Up to 1 month of logs can be searched for at a time.
- Step 4 To export the logs, click **Export** and follow the on-screen instructions.

8.5.2 Device Log

View and export logs generated by devices.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, select **Management > Logs > Device Logs**.
- Step 2 Select a device and time, and then click **Search**.
- Step 3 To export the logs, click **Export** and follow the on-screen instructions.

8.5.3 System Log

View and export logs on how the platform has been running, such as a system error.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Logs** > **System Logs**.
- Step 2 Select a type of logs.
- Step 3 Specify the time, and then click **Search**.
Up to 1 month of logs can be searched for at a time.
- Step 4 (Optional) Click **Export** and follow the on-screen instructions.

8.5.4 Service Log

Services will generate logs when they are running. These logs can be used for troubleshooting. If you need even more detailed logs, enable the debug mode so that the platform will generate detailed logs.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Logs** > **Extract Service Logs**.
- Step 2 Click  to download the logs of the service within a specified period to your computer.
- Step 3 (Optional) Click  to enable the debug mode of a service, and then click  to download the detailed logs within a specified period to your computer.



After the debug mode is enabled, the platform will generate a large amount of logs that occupy more disk space. We recommend you disable the debug mode after you have finished troubleshooting.

8.6 Help

Click **Help** to view the user manual of the platform.

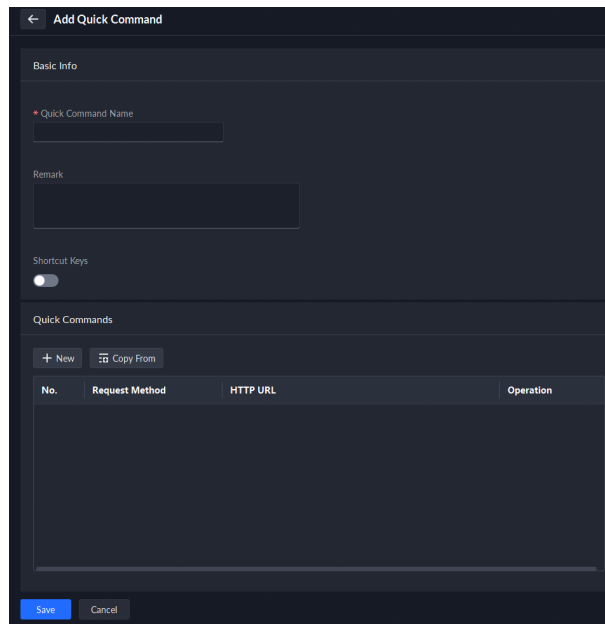
8.7 Quick Commands

Customize HTTP commands and execute them quickly. Request methods of GET, POST, PUT and DELETE are supported.

Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Quick Commands**.
- Step 2 Click **Config**, and then click **Add**.

Figure 8-4 Add a quick command



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

Table 8-11 Quick command parameter description

Parameter	Description
Quick Command Name	The name that identifies the quick command.
Remark	Remarks on the quick command.
Shortcut Keys	After enabling Shortcut Keys , you can set a single key or a combination of 2 keys as the shortcut key.
Enter Shortcut Keys	 The shortcut keys set here take effect globally on the client.
Add	Click Add, and then select New or Copy From to add a new quick command, or copy from an existing quick command or event plan. When you select New, you need to set the request method (GET by default, and you can also select POST, PUT, and DELETE), and HTTP URL address.  - When selecting POST or PUT, you can click  to customize the body of HTTP URL. - Click    in sequence to move up, move down, or delete the request. - Up to 20 requests can be added to 1 quick command.

Parameter	Description
Execute in Order	• When it is enabled, the system will execute the quick command in order of the added requests, and the next request can be executed only after the previous request is successfully executed. • When it is not enabled, the requests will be executed at the same time if multiple requests are added to 1 quick command.

Step 4 Press the defined shortcut keys or click  to execute a quick command.

Appendix 1 Service Module Introduction

Appendix Table 1-1 Service module introduction

Service Name		Function Description
NGINX Proxy Service	NGINX	Provides access to the platform.
System Management Service	SMC	Manages services and provides access to various functions.
Redis Data Cache Service	REDIS	Stores data that is frequently accessed.
MySQL Database Service	MySQL	Stores data for a long time.
System Config Service	CFGS	Monitors system resources and synchronizes configurations across the distributed environment.
MQ Push Notifications Service	MQ	Pushes messages among clients and platforms.
Media Gateway Service	MGW	Acquires video streams for video walls.
Protocol Conversion Proxy Service	PCPS	Accesses third-party video devices.
Device Management Service	DMS	Accesses video devices.
Device Auto Registration Service	ARS	Accesses devices added through automatic registration.
Alarm Controller and LED Device Access Service	MCD	Accesses alarm controllers and LED devices.
Device Search Service	SOSO	Searches for and obtains configurations from devices in local networks.
Device Update Service	DUS	Updates devices.
AcuPick Algorithm Service	AcuPick	Searches for bodies and vehicles by images.
Video Intercom Service	SCS	Manages audio talks among PC clients and app, and video intercom devices.
Service Management Service	SMS	Manages BSMS, POC and SCS.
Business Session Management Service	BSMS	Downloads files from devices, manages the sleep and wake status of low-power consumption cameras that uses 4G network, and redirects to the webpage of devices added through automatic registration.
Group Talk Service	POC	Manages the group talk among MPT devices.
Access Control Management Service	ACDG	Manages ACMS.

Service Name		Function Description
Access Control Management Service	ACMS	Accesses access control devices.
Video Storage Service	SS	Stores and forwards recorded videos on the platform.
Video Decoding to Wall Service	VMS	Accesses decoders outputs videos to video walls.
Object Storage Service	OSS	Stores files of the platform.
Media Forwarding Service	MTS	Forwards real-time video streams.
Third-party Plug-in Management System	TPMS	Service for managing third-party protocols.
License Management Service	LAMS	Service for managing licenses.

Appendix 2 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") places great emphasis on cybersecurity and privacy protection. We continuously allocate special funds to enhance employees' awareness and capabilities in security, and ensure sufficient security protection for our products. Dahua has established a professional security team to provide comprehensive security empowerment and control throughout the entire product lifecycle, including design, development, testing, production, delivery, and maintenance. Dahua products adhere to the principle of minimum necessary data collection, service minimization, strict prohibition of backdoors, and the disabling of unnecessary and insecure services (such as Telnet). We continuously introduce innovative security technologies to bolster the security capabilities of our products. Additionally, we go above and beyond by providing global users with security alarm and 24/7 security emergency response services. This approach ensures that we are better safeguarding their security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report potential risks or vulnerabilities to the Dahua PSIRT. They can do so by visiting the cybersecurity section on the Dahua website.

The security of software platforms not only relies on the continuous attention and efforts from manufacturers throughout R & D, production, and delivery, but also requires active participation from users. Users should remain attentive to the environment and methods to ensure its secure operation. To this end, we suggest users to safely use the software platform, including but not limited to:

Account Management

1. Use Strong Passwords

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

2. Change Password Regularly

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

3. Assign Accounts and Permissions Reasonably

According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

4. Enable Account Lock

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

5. Set and Update Passwords Reset Information Timely

The platform supports password reset function. To reduce the risk of being attacked, please set up related information for password reset in time. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

6. Enable Account Binding IP/MAC

It is recommended to enable the account binding IP/MAC mechanism to further improve access security.

Service Configuration

1. **Enable HTTPS**

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

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

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

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

- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.

Network Configuration

1. **Enable Firewall Allowlist**

We suggest you to enable allowlist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the allowlist.

2. **Network Isolation**

The network should be isolated by partitioning the video monitoring network and the office network on the switch and router to different VLANs. This prevents attackers from using the office network to launch Pivoting attacks on the video monitoring network.

Security Auditing

1. **Check Online Users**

It is recommended to check online users irregularly to identify whether there are illegal users logging in.

2. **View the Platform Log**

By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

Physical Protection

We suggest that you perform physical protection to the device that has installed the platform. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware.

Perimeter Security

We suggest that you deploy perimeter security products and take necessary measures such as authorized access, access control, and intrusion prevention to protect the software platform security.

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188