



General Surveillance Management Center User's Manual








Foreword

General









This user's manual introduces the functions and operations of the general surveillance management center (hereinafter referred to as "the system" or "the platform").

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

Important Safeguards and Warnings

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

Operation Requirements



A suitable operating environment is the foundation for the device to work properly. Confirm whether the following conditions have been met before use.

- Use the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the operating temperature and humidity of the device.
- Use the device on a stable base.
- Do not let any liquid flow into the device to avoid damage to internal components. When liquid flows into the device, immediately disconnect the power supply, unplug all cables connected to it, and contact after-sales service.
- Do not plug or unplug RS-232, RS-485 and other ports with the power on, otherwise, the ports will be easily damaged.
- Back up data in time during deployment and use, in an effort to avoid data loss caused by abnormal operation. The company is not liable for data security.
- The company is not responsible for damages to the device or other product problems caused by excessive use or other improper use.

Installation Requirements



DANGER

- Make sure that the power is off when you connect the cables, install or disassemble the device.
- For devices with earthing systems, make sure they are grounded to avoid being damaged by static electricity or induced voltage, and prevent electrocution from occurring.
- All installation and operations must conform to local electrical safety regulations.
- Use accessories suggested by the manufacturer, and installed by professionals.
- Do not block the ventilator of the device, and install the device in a well-ventilated place.
- Do not expose the device to heat sources or direct sunlight, such as radiator, heater, stove or other heating equipment, which is to avoid the risk of fire.
- Do not place the device in explosive, humid, dusty, extremely hot or cold sites with corrosive gas, strong electromagnetic radiation or unstable illumination.
- Avoid heavy stress, violent vibration, and immersion during installation.



WARNING

Safe and stable power supply is a prerequisite for proper operation of the device.

- Make sure that the ambient voltage is stable and meet the power supply requirements of the device.
- Prevent the power cord from being trampled or pressed, especially the plug, power socket and the junction from the device.
- For devices that can be powered by multiple supplies, do not connect them to two or more kinds of power supplies; otherwise, the device might be damaged.

- Refer to the specific user's manual for the power requirements of single device.



It is recommended to use the device with a lightning protector for better lightning-proof effect.

Transportation Requirements



- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Avoid heavy stress, violent vibration, and immersion during transportation.
- Transport the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the transporting temperature and humidity of the device.

Storage Requirements



- Store the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the storing temperature and humidity of the device.
- Avoid heavy stress, violent vibration, and immersion during storage.

Maintenance Requirements



- Contact professionals for regular inspection and maintenance of the device. Do not disassemble or dismantle the device without a professional present.
- Use accessories suggested by the manufacturer, and maintain the device by professionals.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Overview.....	1
1.1 Introduction.....	1
1.2 Highlights.....	1
2 Installation and Deployment.....	2
2.1 Configuring Single-server Deployment.....	4
2.1.1 Configuring Basic Parameters.....	4
2.1.2 Configuring Dual Network Cards.....	8
2.2 Configuring Distributed Deployment.....	9
2.2.1 Configuring Main Server.....	9
2.2.2 Configuring and Enabling Sub Servers.....	9
2.3 Configuring Hot Standby.....	10
2.4 Configuring N+M.....	12
2.5 Configuring LAN or WAN.....	13
2.5.1 Configuring Router.....	13
2.5.2 Mapping IP or Domain Name.....	14
3 Configuring Basic Settings.....	16
3.1 Login and Password Initialization.....	16
3.2 Quick Guide.....	16
3.3 Self-check.....	21
3.4 Network Config.....	21
3.4.1 NIC Config.....	21
3.4.2 Network Mode.....	23
3.4.3 Connection Detection.....	24
3.4.4 Route Setup.....	25
3.5 Mode Config.....	26
3.5.1 Configuring Main/Sub.....	26
3.5.2 Configuring Hot Standby.....	26
3.6 Security Setup.....	26
3.6.1 SSH Connection Setup.....	26
3.6.2 Enabling TLS.....	27
3.7 System Maintenance.....	27
3.7.1 Basic Maintenance.....	27
3.7.2 Database Maintenance.....	27
3.7.3 Log.....	28
3.7.4 Updating System.....	28

3.8 Basic Config	28
3.8.1 Managing Account	28
3.8.2 Time Setup	29
4 Basic Configurations	31
4.1 Preparations	31
4.1.1 Installing and Logging into DSS Client	31
4.1.2 Installing Mobile Client	33
4.2 Managing Resources	34
4.2.1 Adding Organization	34
4.2.2 Managing Device	35
4.2.3 Binding Resources	47
4.2.4 Adding Recording Plan	48
4.2.5 Adding Video Retrieval Plan	53
4.2.6 Adding Time Template	56
4.2.7 Configuring Video Retention Period	57
4.2.8 Configuring Events	57
4.2.9 Synchronizing People Counting Rules	58
4.3 Adding Role and User	59
4.3.1 Adding User Role	59
4.3.2 Adding User	60
4.3.3 Importing Domain User	61
4.3.4 Syncing Domain User	62
4.3.5 Password Maintenance	62
4.4 Configuring Storage	64
4.4.1 Configuring Network Disk	64
4.4.2 Configuring Server Disk	66
4.4.3 Configuring RAID Group	68
4.4.4 Configuring Disk Group	69
4.4.5 Configuring Device Storage	69
5 Businesses Configuration	71
5.1 Configuring Events	71
5.1.1 Configuring Event Linkage	71
5.1.2 Configuring Combined Event	75
5.1.3 Configuring Alarm Parameter	75
5.2 Configuring Map	78
5.2.1 Preparations	78
5.2.2 Adding Map	78
5.2.3 Marking Devices	82
5.3 Personnel and Vehicle Management	82
5.3.1 Adding Person and Vehicle Groups	83

5.3.2	Configuring Personnel Information.....	83
5.3.3	Vehicle Management.....	100
5.4	Watch List Configuration.....	101
5.4.1	Face Arming List.....	102
5.4.2	Vehicle Watch List.....	105
5.5	Access Control.....	107
5.5.1	Preparations.....	107
5.5.2	Configuring Zone.....	108
5.5.3	Configuring Access Rule.....	115
5.5.4	Configuring Public Passwords.....	125
5.5.5	Configuring Time Templates.....	125
5.5.6	Configuring Access Control Devices.....	126
5.5.7	Configuring Door Information.....	127
5.6	Video Intercom.....	128
5.6.1	Preparations.....	128
5.6.2	Call Management.....	129
5.6.3	Configuring Building/Unit.....	131
5.6.4	Synchronizing Contacts.....	132
5.6.5	Setting Private Password.....	132
5.6.6	App User.....	133
5.7	Visitor Management.....	133
5.7.1	Preparations.....	133
5.7.2	Configuring Visit Settings.....	134
5.8	Parking Lot.....	135
5.8.1	Preparations.....	135
5.8.2	Configuring Parking Lot.....	136
5.8.3	Managing Vehicle Group.....	142
5.9	Intelligent Analysis.....	142
5.9.1	People Counting Group.....	142
5.9.2	Scheduled Report.....	144
5.10	Maintenance Center.....	145
5.10.1	Configuring Alert Rule.....	145
5.10.2	Configuring Video Storage Detection.....	145
6	Businesses Operation.....	147
6.1	Monitoring Center.....	147
6.1.1	Main Page.....	147
6.1.2	Video Monitoring.....	149
6.1.3	Playback.....	173
6.1.4	Map Applications.....	184
6.1.5	Video Wall.....	187

6.2	Event Center	196
6.2.1	Real-time Alarms	196
6.2.2	History Alarms	199
6.2.3	Alarm Controller	200
6.3	DeepXplore	202
6.3.1	Searching for Records	202
6.3.2	Searching for People	203
6.3.3	Searching for Vehicles	206
6.4	Access Management	208
6.4.1	Access Control	208
6.4.2	Video Intercom Application	216
6.4.3	Visitor Application	221
6.5	Parking Lot	225
6.5.1	Entrance and Exit Monitoring	225
6.5.2	Searching for Records	227
6.6	Intelligent Analysis	229
6.6.1	People Counting	229
6.6.2	Heat Maps	232
6.6.3	In-area People Counting	233
6.7	Maintenance Center	234
6.7.1	Viewing System Status	234
6.7.2	Maintenance Management	234
7	General Application	236
7.1	Target Detection	236
7.1.1	Typical Topology	236
7.1.2	Preparations	236
7.1.3	Live Target Detection	237
7.1.4	Searching for Metadata Snapshots	237
7.2	ANPR	238
7.2.1	Typical Topology	238
7.2.2	Preparations	238
7.2.3	Live ANPR	239
7.2.4	Searching for Vehicle Snapshot Records	240
7.3	Face Recognition	240
7.3.1	Typical Topology	240
7.3.2	Preparations	241
7.3.3	Arming Faces	241
7.3.4	Live Face Recognition	241
7.3.5	Searching for Face Snapshots	242

8 System Configurations	243
8.1 Distributed Deployment	243
8.2 License Information	245
8.3 System Parameters	245
8.3.1 Configuring Security Parameters	245
8.3.2 Configuring Retention Period of System Data	246
8.3.3 Time Synchronization	246
8.3.4 Configuring Email Server	248
8.3.5 Configure Device Access Parameters	249
8.3.6 Remote Log	249
8.3.7 Configuring Active Directory	250
8.3.8 Configuring Push Notification for App	251
8.4 Backup and Restore	251
8.4.1 System Backup	251
8.4.2 System Restore	253
9 Management	255
9.1 Managing Logs	255
9.1.1 Operation Log	255
9.1.2 Device Log	255
9.1.3 System Log	255
9.1.4 Service Log	256
9.2 Download Center	256
9.2.1 By Timeline or File	256
9.2.2 By Tagging Record	257
9.2.3 By Locking Record	258
9.3 Configuring Local Settings	259
9.3.1 Configuring General Settings	259
9.3.2 Configuring Video Settings	260
9.3.3 Configuring Video Wall Settings	263
9.3.4 Configuring Alarm Settings	263
9.3.5 Configure File Storage Settings	264
9.3.6 Viewing Shortcut Keys	265
9.3.7 Exporting and Importing Configurations	265
9.4 Playing Local Videos	266
9.5 Quick Commands	267
Appendix 1 Service Module Introduction	269
Appendix 2 RAID	271
Appendix 3 Security Commitment and Recommendation	273

1 Overview

1.1 Introduction

DSS General Surveillance Management Center is a high-performance security management platform based on Linux OS and pre-installed DSS software, offering outstanding performance and excellent reliability. It is ideal for medium and large scenes, such as residential areas and casinos.

1.2 Highlights

- Easy to Use
 - ◇ All-in-one, plug & play and powerful.
 - ◇ Performs unified management of different devices.
- Powerful

Increase system performance through distributed deployment.
- High Storage Performance
 - ◇ 15 built-in storage disk interfaces.
 - ◇ Supports IPSAN for storage expansion.
- Stable and Reliable
 - ◇ Hot standby system design.
 - ◇ VIP Vision unique N M redundancy mode.
 - ◇ Redundant power design that makes the system more stable (only applicable to DSS7016DR-S2).

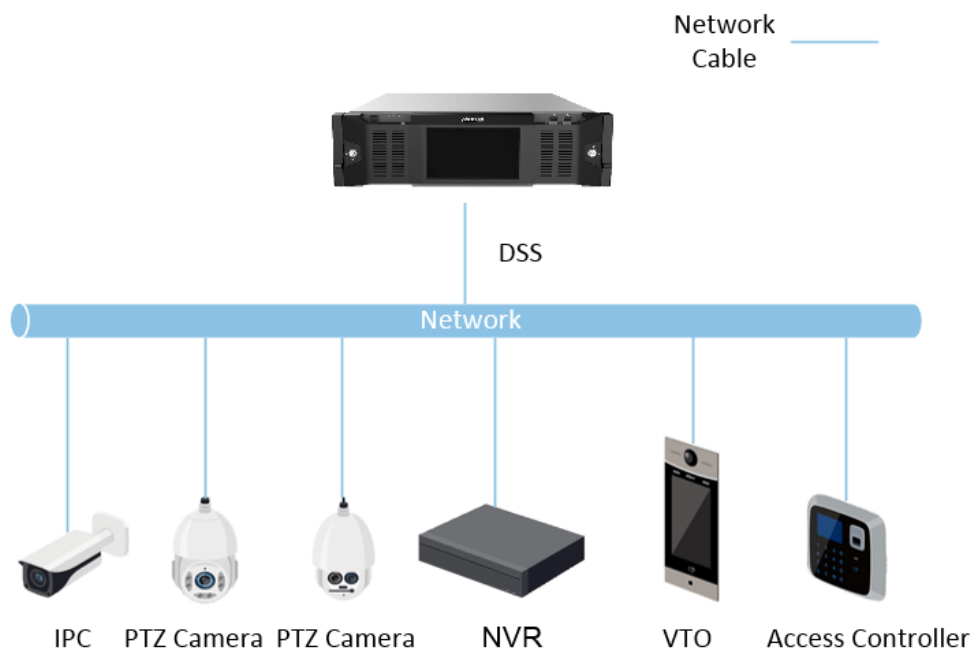
2 Installation and Deployment

The system supports standalone 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 server is required.

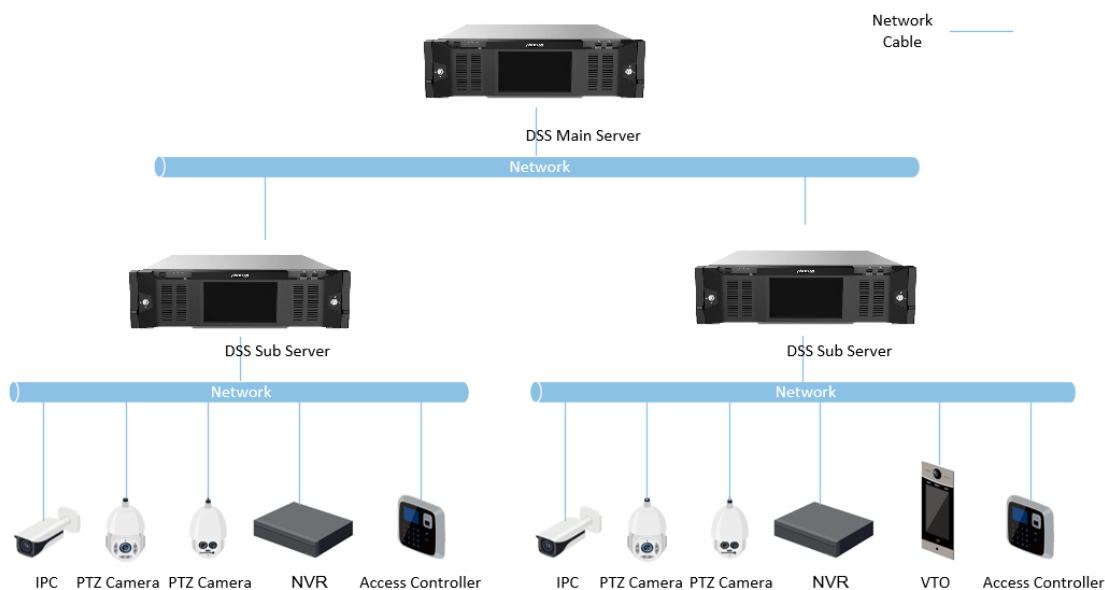
Figure 2-1 Standalone deployment



Distributed Deployment

Suitable for medium to larger 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.

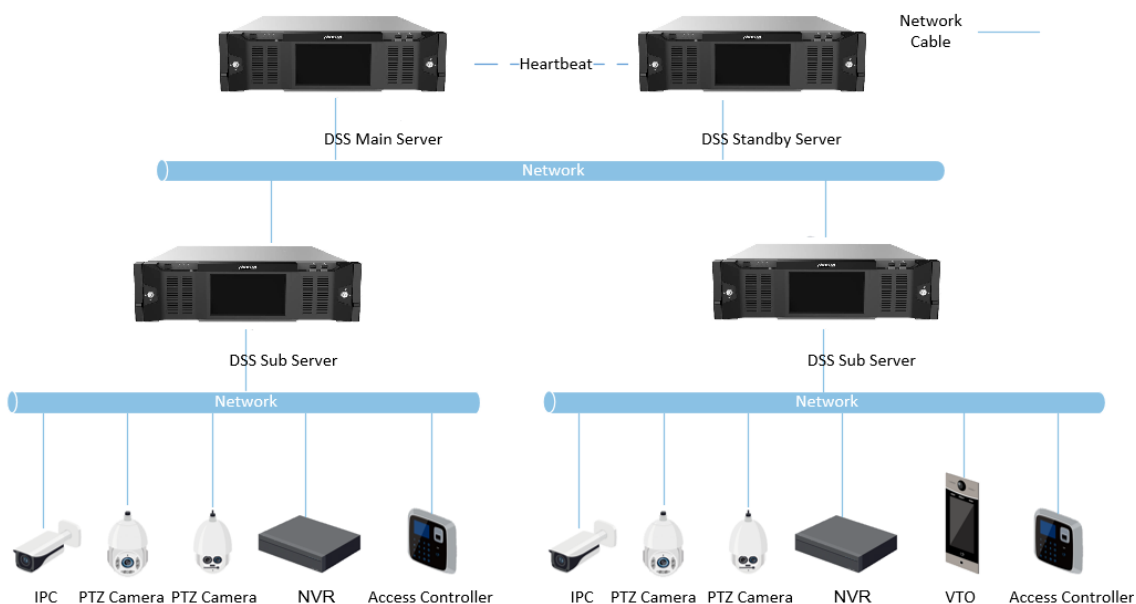
Figure 2-2 Distributed deployment



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 2-3 Hot standby

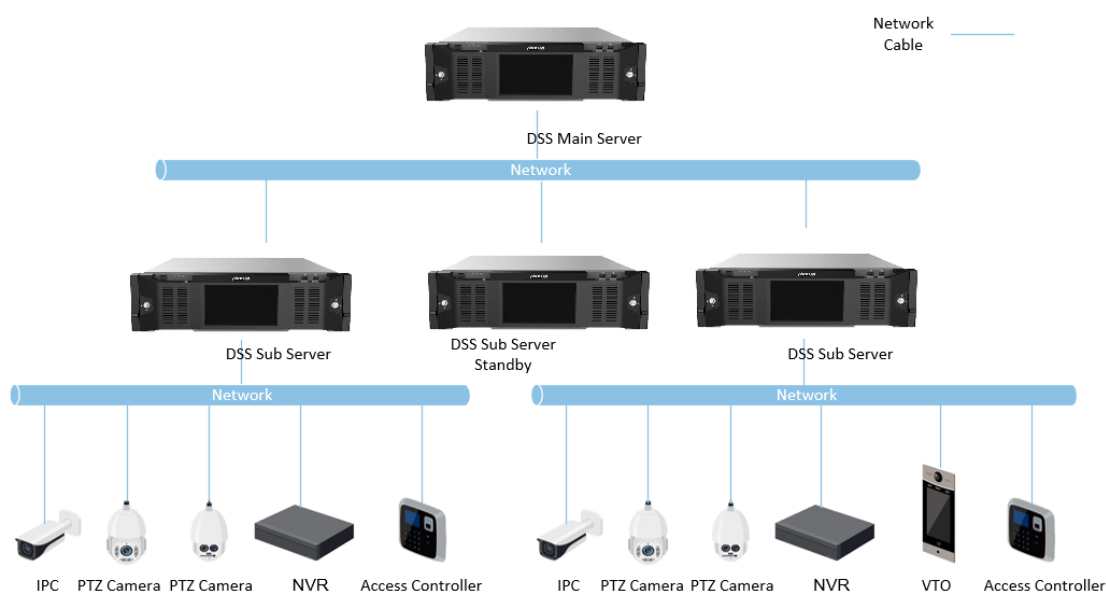


N+M

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 2-4 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 configuration system does not differentiate service LAN ports and WAN ports. Make sure that the WAN ports and LAN ports are the same.

2.1 Configuring Single-server Deployment

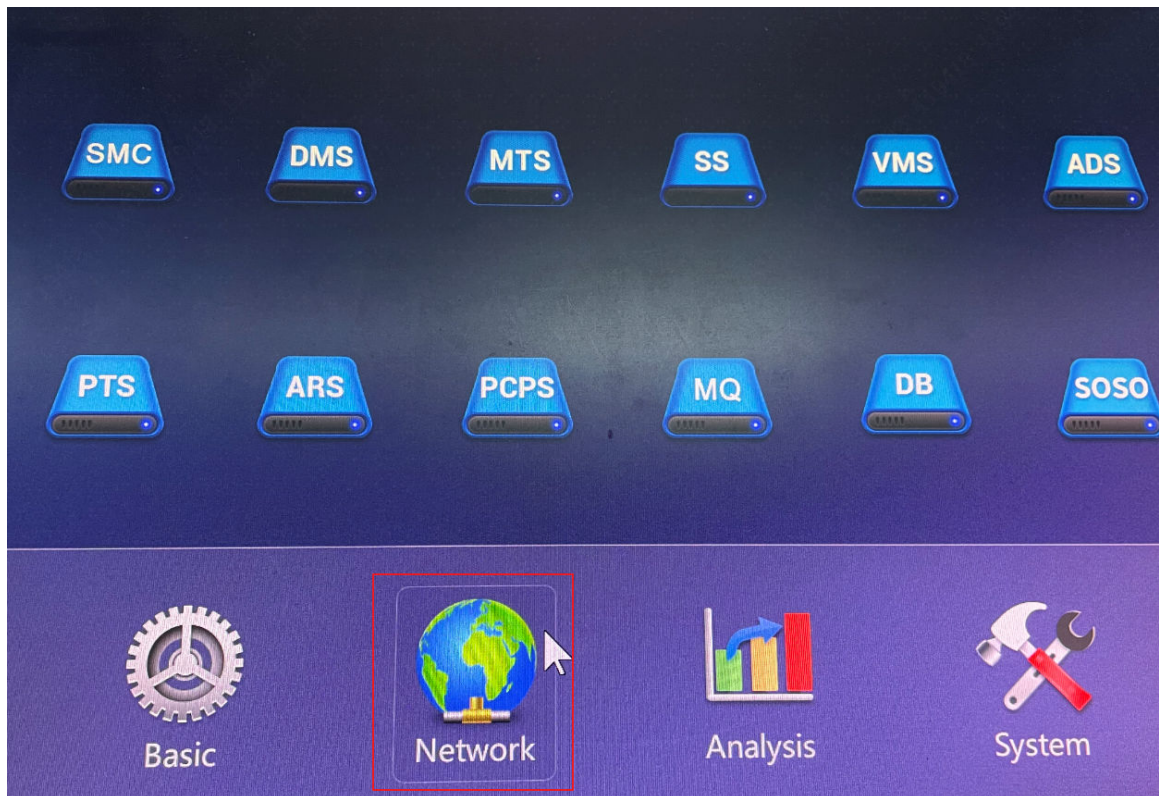
Configure the basic settings for each server before deployment.

2.1.1 Configuring Basic Parameters

Procedure

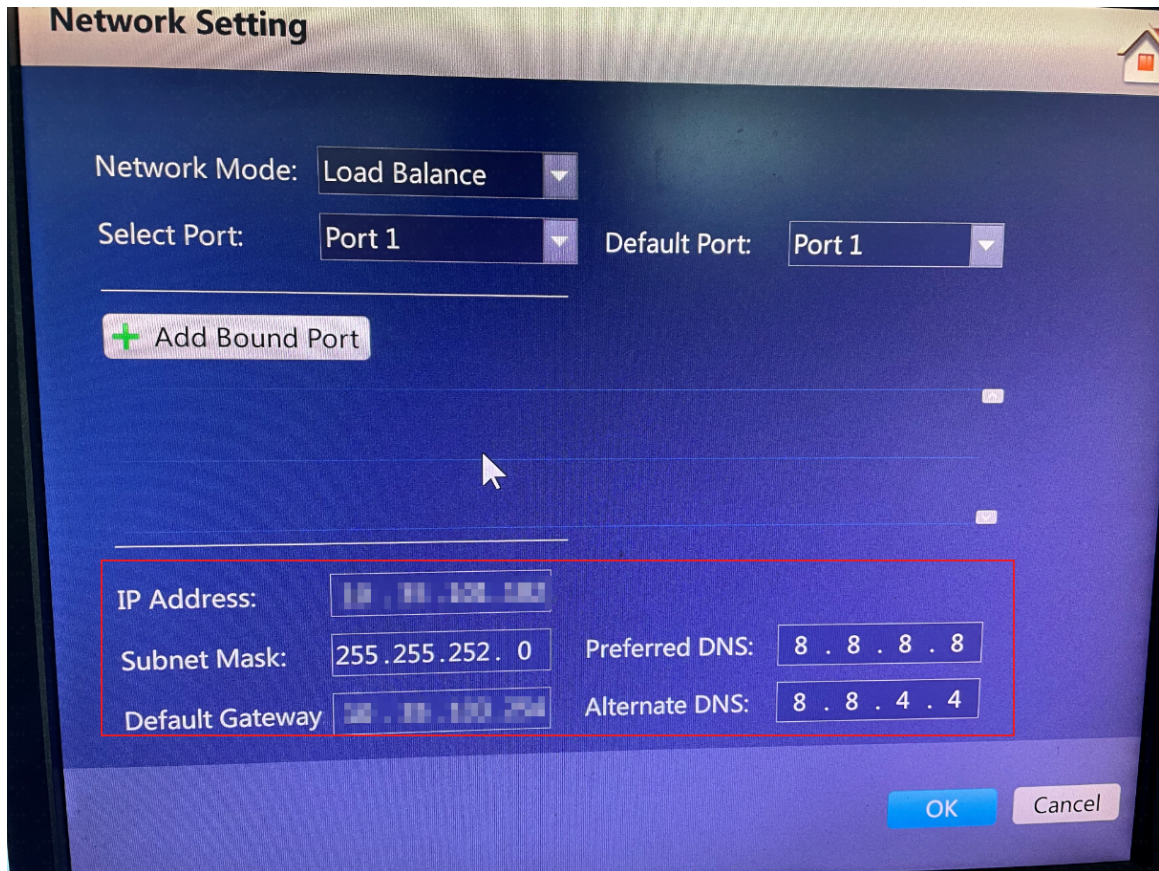
- Step 1** Turn on the platform, and then click **Network**.

Figure 2-5 Network



- Step 2** On the **Select Port** drop-down list, select the port that is connected to the network card you want to configure, and then on the **Default Port** drop-down list, select the default network card of the platform.
- Step 3** Configure the IP address, subnet mask, default gateway, and DNS, and then click **OK**.
The platform will automatically restart.

Figure 2-6 Network settings



Step 4 Go to <https://IP address that you configured/config> in the browser.



For first-time login, follow the on-screen instructions to set a password, security questions, and time zone.

Step 5 Configure network parameters.

1. Select **Quick Guide** > **NIC Config**, or **Network Config** > **NIC Config**.
2. Configure the parameters, and then click **Apply and Restart**.



Default network card and its parameters have been configured in step 2 and 3.

Table 2-1 Network card parameter description

Parameter	Description
Select NIC Mode	<ul style="list-style-type: none"> ● Multi-address Multiple network card (hereinafter referred to as NIC) mode. You can configure different network parameters for different NIC to access to multiple network segments and achieve high network reliability. For example, to configure hot standby, the NIC 2 can be used to set spare server IP. This can also be used in ISCSI storage expansion solution. When setting ISCSI storage expansion, NIC 1 can be used for communication, NIC 2 is reserved and NIC 3 and NIC 4 can be used for ISCSI storage. ● Load Balancing Multiple NICs share one IP and work at the same time to share the network load, providing greater network capacity than the single NIC mode. When one of them fails, the network load will be re-distributed among the rest NICs to ensure network stability. ● Fault-tolerant Multiple NICs share one IP. Normally, one of them works. When the working NIC fails, another one will automatically take over the job to ensure network stability. ● Link Aggregation Bind NICs so that all the bound NICs work at the same time and share network load. For example, bind two NICs and set multi-address for the other two NICs. Then the server has three IPs. The bandwidth of the two bound NICs is 2K and the other two are 2K respectively. This is applicable to stream forwarding, not storage.
Add Network Card	<p>When the NIC mode is fault tolerance, load balance or link aggregation, you need to add network card.</p> <p>Select NIC to bind. You can bind 2 NICs as needed.</p>
Network Card Config	After NIC is selected or added, its information will be displayed.
MAC Address	Displays the MAC address of the server.
IPv4	After selecting a network card, you can set its IP address, subnet mask, default gateway and DNS server address.
IPv6	Enable IPv6 and configure the parameters to connect the platform to an IPv6 network, you can add devices with IPv6 address to the platform.
Default Network Card	Select the default NIC. This NIC will be used as the default NIC to forward data package between non-consecutive network segments such as WAN or public network.

Step 6 Set server time zone and time.

1. After restart completes, log in to the configuration system again, and then select **Basic Config > Time Config**.
2. Configure the parameters, and then click **Application**.

Table 2-2 Parameters description

Parameter	Description
Time Zone	Select time zone of the server.
Date/Time	Click the box to select the date and time.
Sync PC	Click Sync PC to synchronize the time of the server with the computer you are using.

Step 7 Configure the work mode.

1. After restart completes, log in to the configuration system again, and then select **Quick Guide > Service Mode**, or select **Mode Config > Service Mode**.
2. Select **Main Server** or **Sub Server**.
 - For single-server deployment and hot standby deployment, set the work mode to **Main Server**.
 - For distributed deployment and N+M deployment, set the work mode of the main server to **Main Server**, and that of the spare servers to **Sub Server**.



If the server is set to **Sub Server**, you need to enter main server IP address and HTTPS port number.

3. Click **Apply and Restart**.

2.1.2 Configuring Dual Network Cards

2 network cards are usually used for network segmentation. For example, the platform and devices are on 2 different network segments. You can log in to the platform through the IP address of the default network card, and the platform can access devices through another network card.

Prerequisites

Set the network card mode to multi-address mode, and then configure the parameters of each network card. For details, see "2.1.1 Configuring Basic Parameters".

Background Information

Currently, only 2 network cards can be used in dual network card mode, and DSS Client needs to connect only to default network card.

Procedure

- Step 1 Go to `https://platform IP address/config` in the browser.
- Step 2 Enter the username and password, and then click **Login**.
- Step 3 Select **Network Config > Network Mode**, and then select **Dual NIC**.
- Step 4 On the **Local IP 2** drop-down box, select the IP address of the other network card, and then click **Apply and Restart**.

Figure 2-7 Dual network cards mode

The screenshot shows the 'Network Mode' configuration page. At the top, 'Dual NIC' is selected. Below, 'Local IP 1 (Default)' is set to 192.168.1.195. The 'Local IP 2' dropdown is open, showing options: 192.168.4.108, 192.168.3.108, and 192.168.2.108. The 'WAN Mapping' section shows 'Mapping IP Config' with 'Local IP' set to 192.168.1.195. The 'Service Port Config' table is as follows:

Service	Service Type	Port	Operation
NGINX(Proxy Service)	Basic Service	HTTPS 443 HTTP 80	✕
SMC(System Management Service)	Basic Service	HTTPS 8443 CMS 9000 HTTP 8000 SHUTDOWN 8006 REDIRECT 9005	✕
HRS(Platform Discovery Service)	Basic Service		
REDIS(Data Cache Service)	Basic Service	6379	

At the bottom, there is an 'Apply and Restart' button.

Related Operations

In dual network cards mode, you can configure LAN and WAN mapping for the default network card. For details, see "2.5 Configuring LAN or WAN".

2.2 Configuring Distributed Deployment

2.2.1 Configuring Main Server

Most of the parameters you need to configure for the main server are the same as single-server deployment. Among them, you must select the service mode to **Main Server**. For details, see "2.1 Configuring Single-server Deployment".

2.2.2 Configuring and Enabling Sub Servers

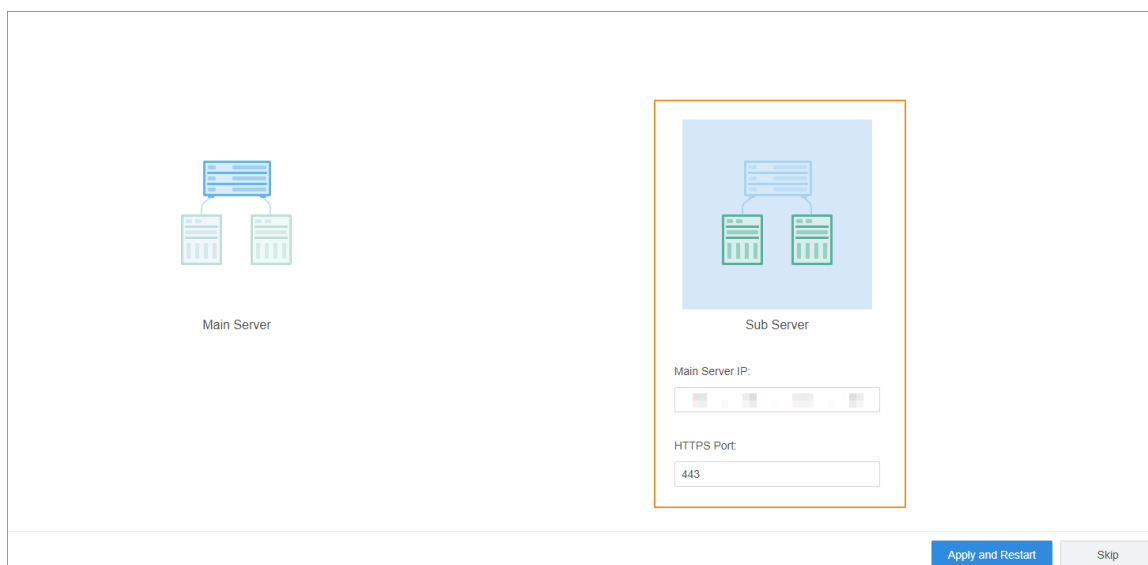
Prerequisites


- Prepare two servers and configure the basic parameters for them. For details, see "2.1 Configuring Single-server Deployment".
- One server works as the main server, and set its service mode to **Main Server**. The other one works as the sub server, and set its service mode to **Sub Server**.

Procedure

- Step 1 Go to `https://sub server IP address/config` in the browser.
- Step 2 Enter the username and password, and then click **Login**.
- Step 3 Select **Quick Guide** > **Service Mode**, or **Mode Config** > **Service Mode**, and then select **Sub Server**.
- Step 4 Enter the IP address and HTTPS port of the main server, and then click **Apply and Restart**.

Figure 2-8 Configure the sub server



Step 5 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Deployment**.






Step 6 Click  of the sub server to enable it.

Figure 2-9 Enable the sub server

Server Name	IP Address	Type	Server Status	Operation
192.168.1.1	192.168.1.1	Main Server	Running	
192.168.1.2	192.168.1.2	Sub Server	Running	  

2.3 Configuring Hot Standby

Configure hot standby server so that when the main server fails, the spare server can take over the job and ensure system stability.

Prerequisites

- Connect network cables.
 - ◇ Use network port 1 as business network port, and then configure an IP address on the business network segment for the network port 1. Connect network port 1 to the same LAN via switch, and the virtual IP address and the one of network port 1 need to be in the same segment.
 - ◇ Take network port 2 as heartbeat network port, which is used to keep data from both servers in synchronization. Configure an IP address for network port 2 that is on another network segment than network port 1, but the IP address of network port 2 of both servers need to be in the same network segment. You can check and configure the IP address of network port 2 on the config system.
- The network mode is set to multi-IP mode. For details, see "3.4.1 NIC Config".
- NTP time synchronization has been enabled on both servers. For details, see "8.3.3 Time Synchronization".
- Prepare an IP address that is not used in the business network segment. After the configuration is complete, you can access this IP address to access the platform.

- Hot standby is the synchronization of the databases of the two servers. If you need to change any configuration that does not involve the databases, such as a port number, you must make sure this port number is the same on both servers.

Procedure

Step 1 Log in to the Config system.

Step 2 Select **Mode Config > Hot standby**.


Figure 2-10 Hot standby


Step 3 Configure the parameters.



The NIC mode must be **Multi-address** for hot spare to work normally. For details, see "3.2 Quick Guide".

Table 2-3 Hot standby parameter description

Parameter	Description
Virtual IP	After setting virtual IP, it can have access to platform via the virtual IP.
Mask	It is in accordance with the mask of network port 1.
Spare IP	IP address of spare server network port 1.
Spare beat IP	IP address of spare server network port 2.
Spare config username	The login username and password of spare server Config system.
Spare config password	 <ul style="list-style-type: none"> ● The login password to Config system of the main and spare servers must be the same. ● The password cannot be changed after hot standby is configured.
One-key Check	Click One-key Check to confirm username and password.

Parameter	Description
Remove Hot Spare	<p>After clicking One-key Check and the platform indicates everything is OK, you can click this button to remove the hot spare configuration.</p> <p>If you need to completely remove the hot spare configuration, you need to click this button on the spare server first, and then on the main server.</p> <p></p> <p>For this operation, you must access the IP addresses of the servers, and not the virtual IP address.</p>

Step 4 Click **Apply and Restart**.


2.4 Configuring N+M


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


Prerequisites

- The relevant servers have been well deployed.
- The DSS client has been installed. For details, see "4.1.1 Installing and Logging into DSS Client".

Procedure

Step 1 Log in to the DSS client of the main server. 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**.

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


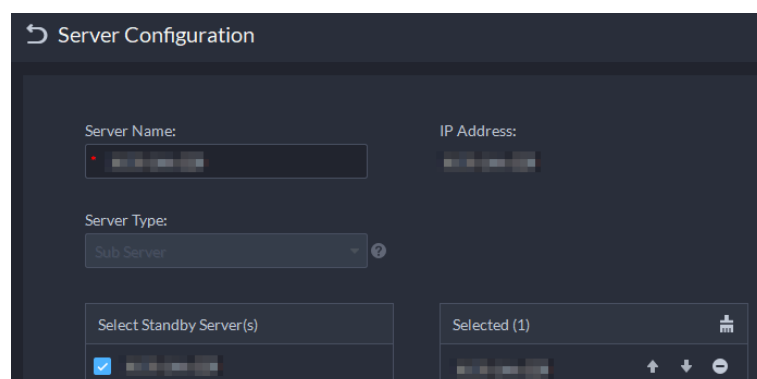


- Go to the **Configure Server** interface of the sub server to select a standby server.
 1. Click  of a sub server.
 2. On the **Select Standby Server(s)** interface, select one or more standby servers.

Figure 2-11 Select a standby server



3. Click **OK**.

- Go to the **Configure Server** interface of the standby server to select a sub server.
 1. Click  of a standby server.
 2. On the **Select Sub Server(s)** interface, select one or more sub servers.

You can click  to adjust the priority.
 3. Click **OK**.

2.5 Configuring LAN or WAN

2.5.1 Configuring Router

If the platform is in a local network, you can visit it from the public network by performing DMZ mapping. For the list of the ports to be mapped, see the table below.

Table 2-4 Port matrix

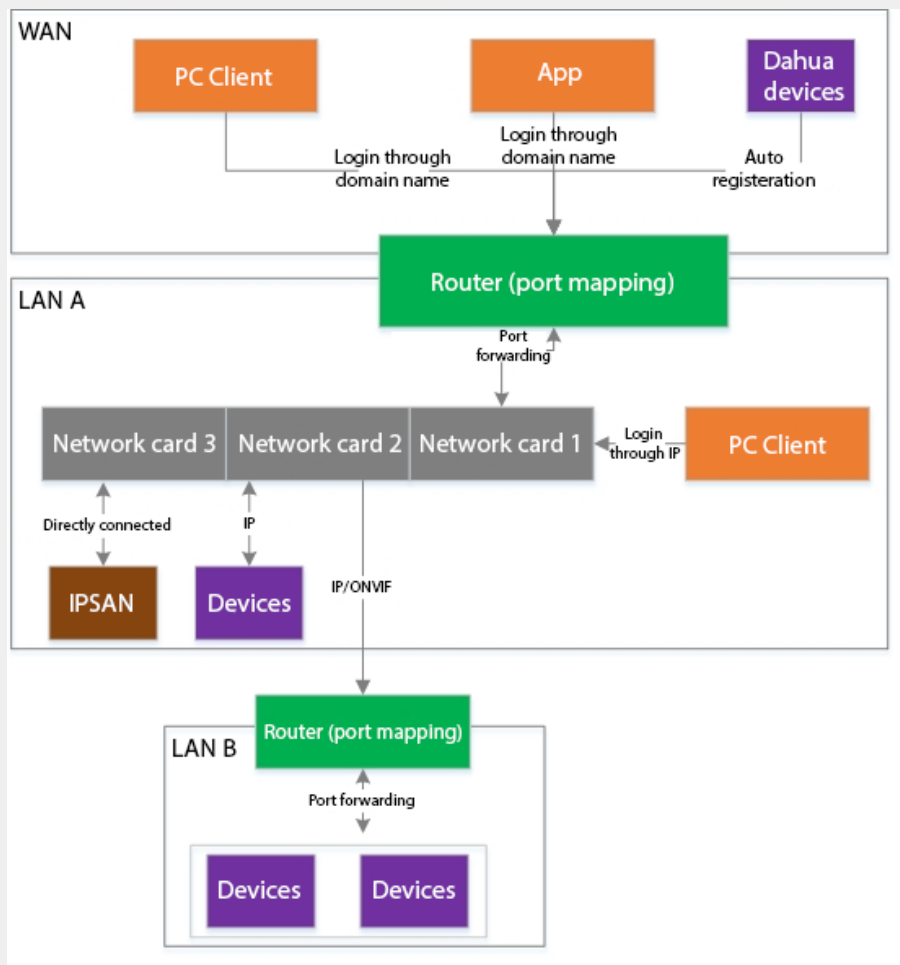
Function	Port	Service	Must be Mapped
PC client login	80 (nginx http)	HTTP	No
	443 (nginx https)	HTTPS	Yes
	1883 (MQ service mobile App connection)	MQ-mqtt (encryption)	Yes
	61616 (MQ service PC client connection)	MQ-openwire (encryption)	Yes
Live video	9100 (MTS service RTSP)	RTSP	Yes
	9102 (MTS service RTSPS)	RTSP over TLS	No
Playback	9320 (SS service RTSP)	RTSP	Yes
	9322 (SS service RTSPS)	RTSP over TLS	No
ANPR	40000-50000 (PTS image stream)	RTP	Yes
Video intercom	5080 (SC service)	SIP registration (UDP)	Yes
	20000-30000 (SC service audio stream)	Audio stream forwarding port (UDP)	Yes
Automatic registration	9005 (admin service)	Redirection of automatic registration	No
	9500 (ARS service)	Second-generation protocol	Yes



- Make sure that the number of the WAN ports is consistent with that of the LAN ports.

- You can configure LAN and WAN mapping and dual network cards mode at the same time. For how to configure dual network cards, see "2.1.2 Configuring Dual Network Cards".

Figure 2-12 Topology of deploying LAN and WAN mapping and dual networks cards



2.5.2 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.

Procedure

- Step 1 Log in to the Config system.
- Step 2 Select **Network Config** > **Network Mode**.

Figure 2-13 Network mode

Network Config > Network Mode

Network Mode

Select Network Mode

Mapping Mode Multi-IP Mode

Mapping IP Config

LAN IP Address:

Mapping IP | Domain:

Service Port Config

Service	Service Type	Port	Operation
DSS_NGINX	Basic Service	HTTPS 443 HTTP 80	
DSS_SMC	Basic Service	HTTPS 8443 CMS 9000 HTTP 8000 SHUTDOWN 8006 REDIRECT 9005	
DSS_HRS	Basic Service		
DSS_REDIS	Basic Service	6379	

Router Config

You need to configure the same service port on the router.

Step 3 Enter a fixed WAN IP address or a domain name in the **Mapping IP | Domain** box, and then click **OK**.



- If you want to use a domain name, you need to make related configurations on the domain name server.
- The DNS information of the network card must be the same as the domain name server.

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

3 Configuring Basic Settings

Log in to the Config system (configuration system) to quickly configure network parameters, basic parameters, safety parameters, and hot standby, as well as system update and self-check.

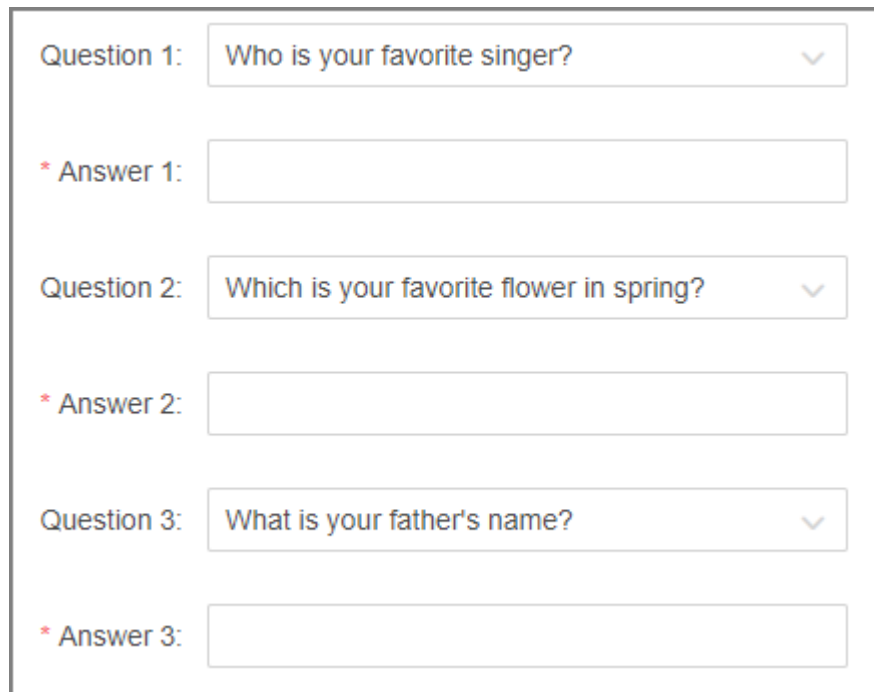
3.1 Login and Password Initialization

Procedure

Step 1 Go to `https://DSS platform IP address/config` in the browser.

The password resetting interface is displayed.

Figure 3-1 Reset password



The screenshot shows a web form for password reset. It contains three security questions, each with a dropdown menu for the question and a text input field for the answer. The questions are: 'Who is your favorite singer?', 'Which is your favorite flower in spring?', and 'What is your father's name?'. Each question is followed by an asterisk and the label 'Answer 1', 'Answer 2', or 'Answer 3' respectively.

Step 2 Enter a password and confirm it, and then click **Next**.

Step 3 Set security questions, and then click **Next**.

Step 4 Configure the time and time zone, and then click **Finish**.

Service is restarted and you need to log in to the system again.

3.2 Quick Guide

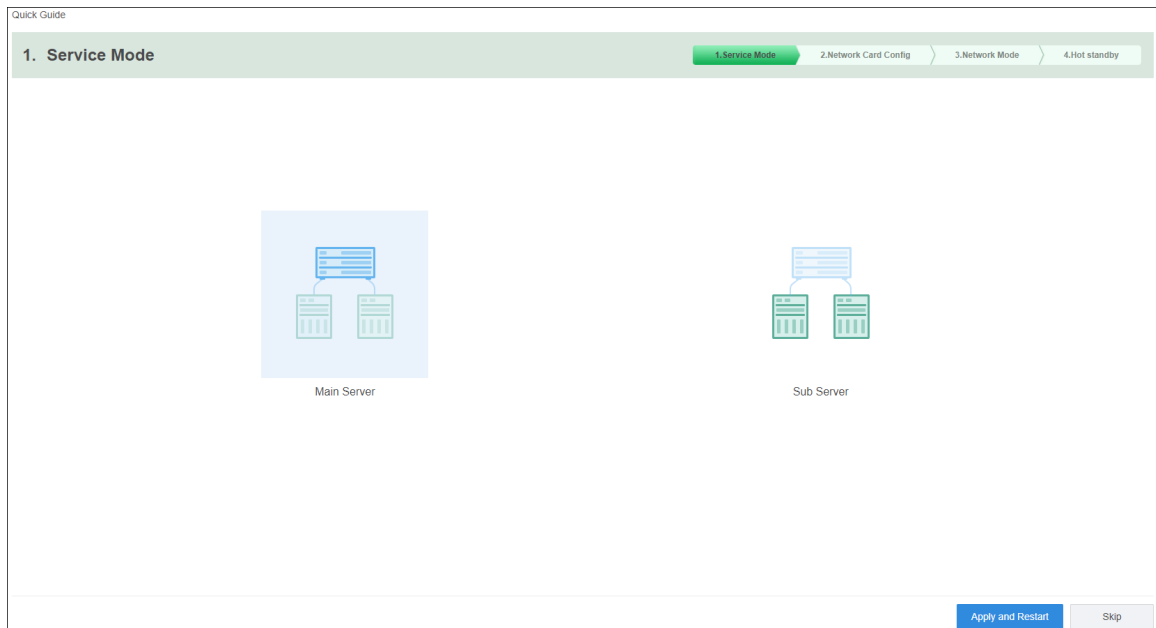
On the **Quick Guide** interface, you can quickly configure network settings, LAN to WAN mapping, and hot standby.

Procedure

Step 1 Log in to the Config system.

Step 2 Click **Quick Guide**.

Figure 3-2 Service mode



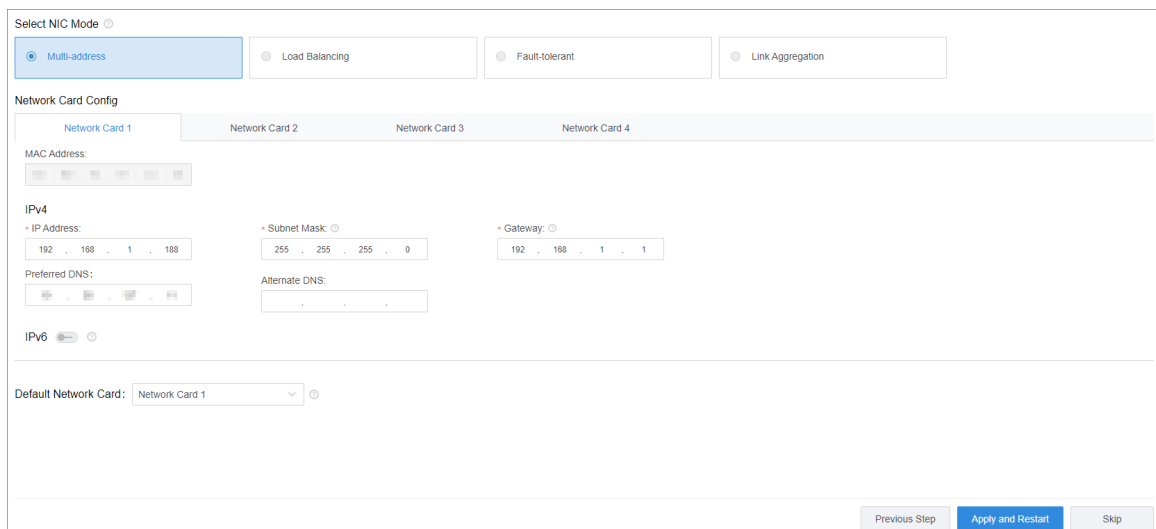
Step 3 Select **Main Server** or **Sub Server** as needed, and then click **Apply and Restart**.



If the server is set to **Sub Server**, enter the IP address and HTTPS port number of the main server.

Step 4 Log in to the Config system, and then select **Quick Guide** > **Network Card Config**.

Figure 3-3 Network card configuration



Step 5 Configure the parameters.

Table 3-1 Network card parameter description

Parameter	Description
Select NIC Mode	<ul style="list-style-type: none"> ● Multi-address Multiple network card (hereinafter referred to as NIC) mode. You can configure different network parameters for different NIC to access to multiple network segments and achieve high network reliability. For example, to configure hot standby, the NIC 2 can be used to set spare server IP. This can also be used in ISCSI storage expansion solution. When setting ISCSI storage expansion, NIC 1 can be used for communication, NIC 2 is reserved and NIC 3 and NIC 4 can be used for ISCSI storage. ● Load Balancing Multiple NICs share one IP and work at the same time to share the network load, providing greater network capacity than the single NIC mode. When one of them fails, the network load will be re-distributed among the rest NICs to ensure network stability. ● Fault-tolerant Multiple NICs share one IP. Normally, one of them works. When the working NIC fails, another one will automatically take over the job to ensure network stability. ● Link Aggregation Bind NICs so that all the bound NICs work at the same time and share network load. For example, bind two NICs and set multi-address for the other two NICs. Then the server has three IPs. The bandwidth of the two bound NICs is 2K and the other two are 2K respectively. This is applicable to stream forwarding, not storage.
Add Network Card	<p>When the NIC mode is fault tolerance, load balance or link aggregation, you need to add network card.</p> <p>Select NIC to bind. You can bind 2 NICs as needed.</p>
Network Card Config	After NIC is selected or added, its information will be displayed.
MAC Address	Displays the MAC address of the server.
IPv4	After selecting a network card, you can set its IP address, subnet mask, default gateway and DNS server address.
IPv6	Enable IPv6 and configure the parameters to connect the platform to an IPv6 network, you can add devices with IPv6 address to the platform.
Default Network Card	Select the default NIC. This NIC will be used as the default NIC to forward data package between non-consecutive network segments such as WAN or public network.

Step 6 Click **Apply and Restart**.

Step 7 Log in to the Config system, and then select **Quick Guide > Network Mode**.

Figure 3-4 Network mode

Network Mode

Single NIC Dual NIC

Local IP: 192.168.1.195

WAN Mapping

Mapping IP Config

Local IP: 192.168.1.195 WAN IP | Domain Name: []

Service Port Config

Service	Service Type	Port	Operation
NGINX(Proxy Service)	Basic Service	HTTPS 444 HTTP 81	
SMC(System Management Service)	Basic Service	HTTPS 8444 CMS 9000 HTTP 8001 SHUTDOWN 8006 REDIRECT 9006	
HRS(Platform Discovery Service)	Basic Service		

Previous Step Apply and Restart Skip

Step 8 Configure the parameters.

Table 3-2 Network mode parameter description

Mode	Parameter	Description
Network Mode	Single NIC	The platform will only use the default network card, and you can only access the platform through the IP address of this network card.
	Dual NIC	If the platform has more than one network cards, you can configure an additional one so that the platform can access more devices on another network segment. To use Dual NIC, you must set the network mode to multi-IP address mode, and then configure the parameters of the network cards.
WAN Mapping	WAN IP Domain Name	Map the LAN IP to a WAN IP, so that you can access the platform through the WAN IP. If the WAN IP changes frequently, you can map it to a domain name, and use it to access the platform.
	Service Port Config	Displays all services used by the platform and their ports. Click to change their port numbers as needed. For introduction to each service, see "Appendix 1 Service Module Introduction".

Step 9 Click **Apply and Restart**.

Step 10 Log in to the Config system, and then select **Quick Guide** > **Hot standby**.

Figure 3-5 Hot standby

Quick Guide

4. Hot standby 1. Service Mode > 2. Network Card Config > 3. Network Mode > 4. Hot standby

If you want another server to replace this main server and maintain system operation after main server finish downtime, please configure a hot spare service for this main server, fill in the following info and save.
Make sure config passwords of host and spare are identical, otherwise data sync and failure switch may fail.

Virtual IP: Mask:

Spare IP: Spare beat IP:

Spare config username: Spare config password:


Step 11 Configure the parameters.



The NIC mode must be **Multi-address** for hot spare to work normally. For details, see Step 4.


Table 3-3 Hot standby parameter description

Parameter	Description
Virtual IP	After setting virtual IP, it can have access to platform via the virtual IP.
Mask	It is in accordance with the mask of network port 1.
Spare IP	IP address of spare server network port 1.
Spare beat IP	IP address of spare server network port 2.
Spare config username	The login username and password of spare server Config system.
Spare config password	<ul style="list-style-type: none"> The login password to Config system of the main and spare servers must be the same. The password cannot be changed after hot standby is configured.
One-key Check	Click One-key Check to confirm username and password.

Parameter	Description
Remove Hot Spare	<p>After clicking One-key Check and the platform indicates everything is OK, you can click this button to remove the hot spare configuration.</p> <p>If you need to completely remove the hot spare configuration, you need to click this button on the spare server first, and then on the main server.</p> <p></p> <p>For this operation, you must access the IP addresses of the servers, and not the virtual IP address.</p>

Step 12 Click **Apply and Restart**.

3.3 Self-check

- Click **System Status**, and then select **Service Status**, **CPU Status**, **Network Status**, or **Local Disk Status** to check the different status of the platform.
- Hover the mouse over or click the icons of  at the upper left corner to check the status of the ports, IP addresses, network, CPU, and disks.

3.4 Network Config

3.4.1 NIC Config

Configure the parameters so that the platform can connect to the network.

Procedure

Step 1 Select **Network Config** > **NIC Config**.

Figure 3-6 Network card configuration

Network Card Config

Select NIC Mode

Multi-address Load Balancing Fault-tolerant Link Aggregation

Network Card Config

Network Card 1 | Network Card 2 | Network Card 3 | Network Card 4

MAC Address:

IPv4

• IP Address: • Subnet Mask: • Gateway:

Preferred DNS: Alternate DNS:

IPv6

Default Network Card:

Apply and Restart

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

Table 3-4 Network card parameter description

Parameter	Description
Select NIC Mode	<ul style="list-style-type: none"> Multi-address Multiple network card (hereinafter referred to as NIC) mode. You can configure different network parameters for different NIC to access to multiple network segments and achieve high network reliability. For example, to configure hot standby, the NIC 2 can be used to set spare server IP. This can also be used in ISCSI storage expansion solution. When setting ISCSI storage expansion, NIC 1 can be used for communication, NIC 2 is reserved and NIC 3 and NIC 4 can be used for ISCSI storage. Load Balancing Multiple NICs share one IP and work at the same time to share the network load, providing greater network capacity than the single NIC mode. When one of them fails, the network load will be re-distributed among the rest NICs to ensure network stability. Fault-tolerant Multiple NICs share one IP. Normally, one of them works. When the working NIC fails, another one will automatically take over the job to ensure network stability. Link Aggregation Bind NICs so that all the bound NICs work at the same time and share network load. For example, bind two NICs and set multi-address for the other two NICs. Then the server has three IPs. The bandwidth of the two bound NICs is 2K and the other two are 2K respectively. This is applicable to stream forwarding, not storage.

Parameter	Description
Add Network Card	When the NIC mode is fault tolerance, load balance or link aggregation, you need to add network card. Select NIC to bind. You can bind 2 NICs as needed.
Network Card Config	After NIC is selected or added, its information will be displayed.
MAC Address	Displays the MAC address of the server.
IPv4	After selecting a network card, you can set its IP address, subnet mask, default gateway and DNS server address.
IPv6	Enable IPv6 and configure the parameters to connect the platform to an IPv6 network, you can add devices with IPv6 address to the platform.
Default Network Card	Select the default NIC. This NIC will be used as the default NIC to forward data package between non-consecutive network segments such as WAN or public network.

3.4.2 Network Mode

You can set the platform to work in mapping mode or multi-IP mode. In mapping mode, you can configure LAN IP to WAN IP mapping, or LAN IP to domain name mapping, so that you can use the WAN IP or domain name to visit the platform deployed in a local network. In multi-IP mode, you can assign an IP address to the platform and use it to visit and operate the platform.

Procedure

Step 1 Select **Network Config** > **Network Mode**.

Figure 3-7 Network mode

Network Mode

Single NIC Dual NIC

Local IP: 192.168.1.195

WAN Mapping

Mapping IP Config

Local IP: 192.168.1.195 WAN IP | Domain Name: [input]



Service Port Config

Service	Service Type	Port	Operation
NGINX(Proxy Service)	Basic Service	HTTPS 444	✖
		HTTP 81	
SMC(System Management Service)	Basic Service	HTTPS 8444	✖
		CMS 9000	
		HTTP 8001	
		SHUTDOWN 8006	
HRS(Platform Discovery Service)	Basic Service	REDIRECT 9006	

Previous Step **Apply and Restart** Skip

Step 2 Configure the parameters.

Table 3-5 Network mode parameter description

Mode	Parameter	Description
Network Mode	Single NIC	The platform will only use the default network card, and you can only access the platform through the IP address of this network card.
	Dual NIC	If the platform has more than one network cards, you can configure an additional one so that the platform can access more devices on another network segment.  To use Dual NIC, you must set the network mode to multi-IP address mode, and then configure the parameters of the network cards.
WAN Mapping	WAN IP Domain Name	Map the LAN IP to a WAN IP, so that you can access the platform through the WAN IP. If the WAN IP changes frequently, you can map it to a domain name, and use it to access the platform.
	Service Port Config	Displays all services used by the platform and their ports. Click  to change their port numbers as needed. For introduction to each service, see "Appendix 1 Service Module Introduction".

Step 3 Click **Apply and Restart**.

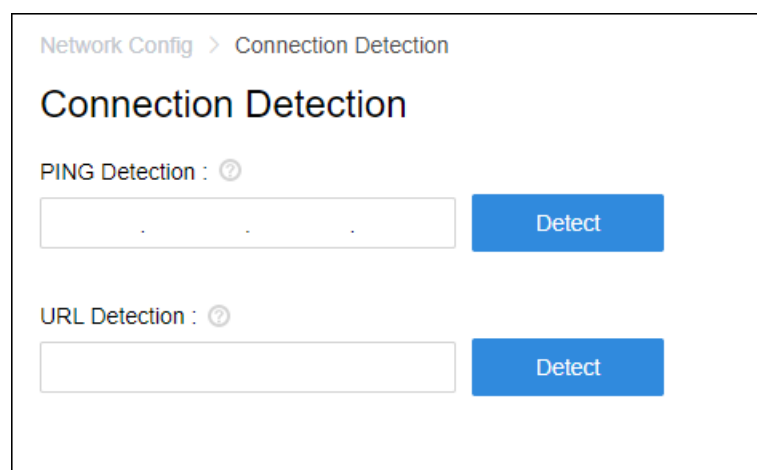
3.4.3 Connection Detection

Check whether the IP address or URL is connected normally to validate the network interconnection between servers or between the devices and the server.

Procedure


Step 1 Select **Network Config > Connection Detection**.


Figure 3-8 Connection detection



Network Config > Connection Detection

Connection Detection

PING Detection : 

URL Detection : 

Step 2 Enter IP address or URL, and then click **Detect**.

3.4.4 Route Setup

Add static route to establish access between servers in different network segments.

Procedure

Step 1 Select **Network Config** > **Routing Settings**.

Figure 3-9 Route setup



Step 2 Click **Manually Add**.

Figure 3-10 Add statistic router

Step 3 Enter router IP address, subnet mask and default gateway.

Table 3-6 Parameter description

Parameter	Description
Router Address	The IP address or the network segment of the host you want to access.
Subnet Mask	The subnet mask of the network you want to access.
Gateway	The IP address of the default gateway or the next hop.

Step 4 Click **OK**.

3.5 Mode Config

3.5.1 Configuring Main/Sub

When configuring distributed deployment or N+M deployment, set the server to be main or sub according to the actual situation.

Procedure

Step 1 Select **Quick Guide** > **Service Mode**, or select **Mode Config** > **Service Mode**.

Step 2 Select **Main Server** or **Sub Server** according to actual configuration.



If the server is set to **Sub Server**, enter IP address and HTTPS port of the main server.

Step 3 Click **Apply and Restart**.

3.5.2 Configuring Hot Standby

Configure hot standby server so that when the main server fails, the spare server can take over the job and ensure system stability. For details, see "2.3 Configuring Hot Standby".

3.6 Security Setup

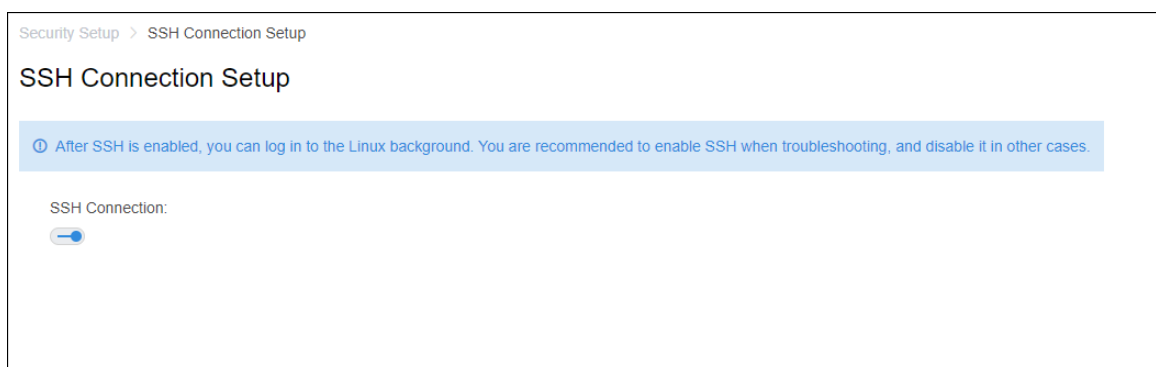
3.6.1 SSH Connection Setup

After enabling SSH connection, the debugging terminal can log in to platform server to debug device via SSH protocol.

Procedure

Step 1 Select **Security Config** > **SSH Connection Service**.

Figure 3-11 SSH connection



Step 2 Enable **SSH Connection**.



Disable **SSH Connection** after debugging.

3.6.2 Enabling TLS

By default, the platform only supports TLS1.2. You must enable TLS1.2 according to the on-screen instructions to normally access the Config system. Please be advised that TLS1.0 and TLS1.1 poses security risks. We recommend you disable TLS self-adaptive mode and enable TLS1.2 to avoid unnecessary risks to your system. If you must use TLS1.0 or TLS1.1, you must enable TLS self-adaptive mode on the platform, and then enabled the TLS version you need on the browser.

3.7 System Maintenance

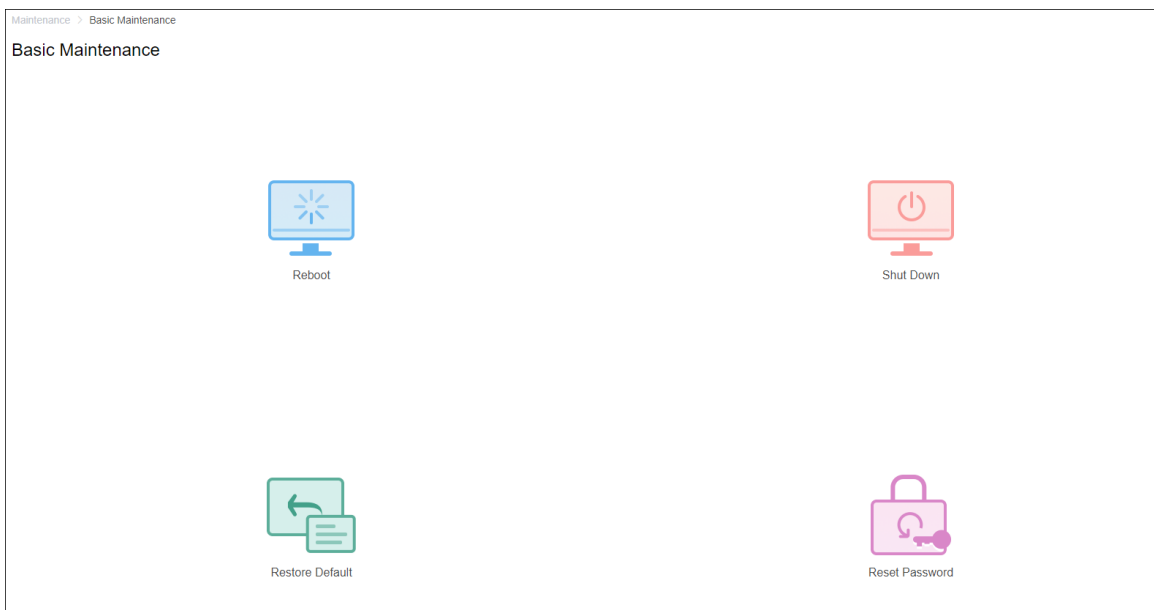
3.7.1 Basic Maintenance

Restart, shut down and reset the server. You can also reset password.

Procedure

Step 1 Select **System Maintenance** > **Basic Maintenance**.

Figure 3-12 Maintenance



Step 2 Click the icons for various functions.

- **Reboot** : Restart the server.
- **Shut Down** : Shut down the server.
- **Restore Default** : Restore the server to default settings.
- **Reset Password** : Verify your current password to reset the password. Wait for the server to restart, and then go to the config system to set a new password.

3.7.2 Database Maintenance

If you cannot log in to the client because the database is abnormal, you can try to repair it manually.

Click **Inspect Database**, and then 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.

All the backup files are displayed on the list at the bottom of the page. You can delete them as needed.



To restore the database, the platform needs to use port 3306. If a process is using the port, you need to terminate it first.

3.7.3 Log

You can download the logs of all services to your computer.


Procedure

- Step 1 Select **System Maintenance** > **Service Log**.
- Step 2 Select the date, and then click **Download** to download the logs.

3.7.4 Updating System

We recommend you update the system regularly to enjoy enhanced performance and functions. Before updating your system, contact technical support to get the update package.

Procedure

- Step 1 Select **System Maintenance** > **System Update**.
- Step 2 Select complete update or fix pack update, and then click  to select the update package.
- Step 3 Click **Update**.

3.8 Basic Config

3.8.1 Managing Account

You can change the login password of admin user.



All services will be restarted after changing the password. Check if the services have been restarted successfully during use.

Procedure

- Step 1 Select **Basic Config** > **Manage Account**.

Figure 3-13 Manage account

Basic > Manage Account

Manage Account

ⓘ All services will be restarted after you change the password.

Old Username:

Old Password:

New Password:

Confirm Password:

Apply and Restart

Step 2 Enter **Old Password** , **New Password** and **Confirm Password**.

Step 3 Click **Apply and Restart**.



It will restart all services after modifying password. Check if the services have been restarted successfully during use.

3.8.2 Time Setup

Set time zone and time where the server is located.

Procedure

Step 1 Select **Basic Config > Time Config**.

Step 2 Configure the parameters.

Table 3-7 Parameters description

Parameter	Description
Time Zone	Select time zone of the server.
Date/Time	Click the box to select the date and time.

Parameter	Description
Sync PC	Click Sync PC to synchronize the time of the server with the computer you are using.

Step 3 Click **Application**.

4 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.

4.1 Preparations

4.1.1 Installing and Logging into DSS Client

Install the DSS client before licensing it.

4.1.1.1 Installing DSS Client

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

4.1.1.1.1 DSS Client Requirements



Press the Windows key, and type **dxdiag**, and then click dxdiag Run command. 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 4-1 Hardware requirements

Parameters	Description
Recommended system requirements	<ul style="list-style-type: none"> ● 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 is reserved for the client.

4.1.1.1.2 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**.

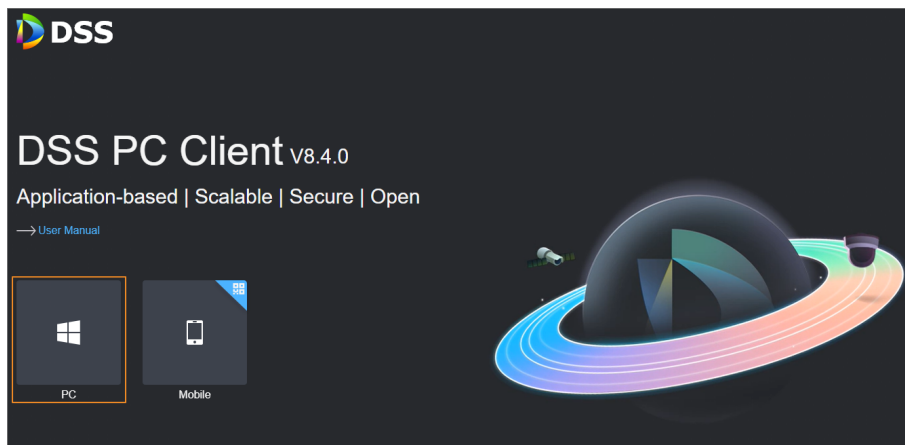


The platform also supports installation by MSI package. Please be advised that you cannot overwrite the PC client installed with an exe package, and vice versa. Also, the PC client installed with an MSI package does not support automatic update. You must download the package of the new version and install it manually.

If you save the program, go to Step 3.

If you run the program, go to Step 4.


Figure 4-1 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.

4.1.1.2 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.



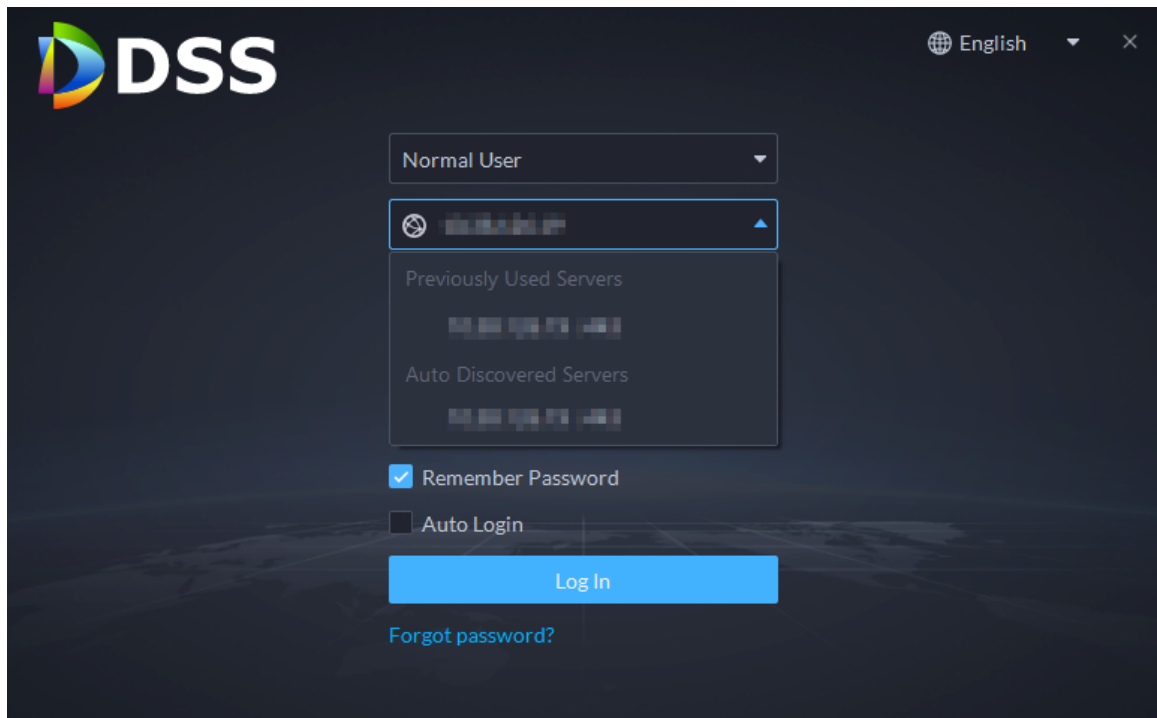
If you want to log in using a domain user account, you must import the domain user first. For details, see "4.3.3 Importing Domain User".

- 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 "2.5.2 Mapping IP or Domain Name".
- If you log in by localhost, the platform will automatically change it to 127.0.0.1.

Figure 4-2 Automatically discovered platform



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.

4.1.2 Installing Mobile Client

Procedure

Step 1 Enter IP address of the DSS in the browser and then press Enter.

Step 2 Click **Mobile**, and then scan the QR code to download the App.

4.2 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.

4.2.1 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




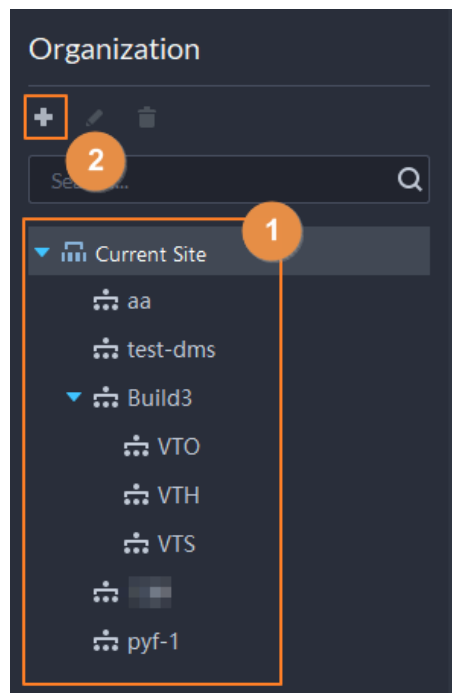
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Add an organization.
1. Select a parent organization.
 2. Click .

Figure 4-3 Add an organization




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

Figure 4-4 Add an organization



You can also right-click the root organization, and then click **Create 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.




4.2.2 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.

4.2.2.1 Searching for Online Devices

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

Procedure

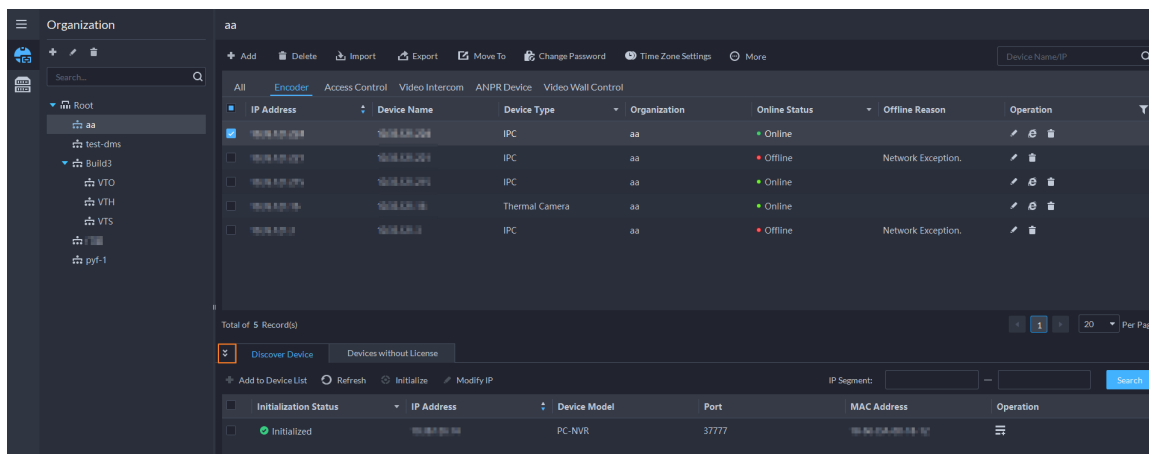
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Click .

The icon changes to  when devices are searched.



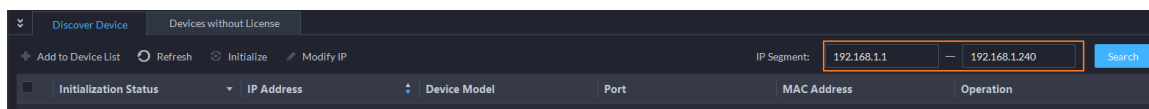
- When using the platform for the first time, the platform automatically searches for devices on the same network segment.
- If not the first time, the platform automatically searches for the devices in the network segment you configured last time.

Figure 4-5 Search for devices



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

Figure 4-6 IP segment search



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

4.2.2.2 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 "4.2.2.1 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.

4.2.2.3 Changing Device IP Address

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

Procedure

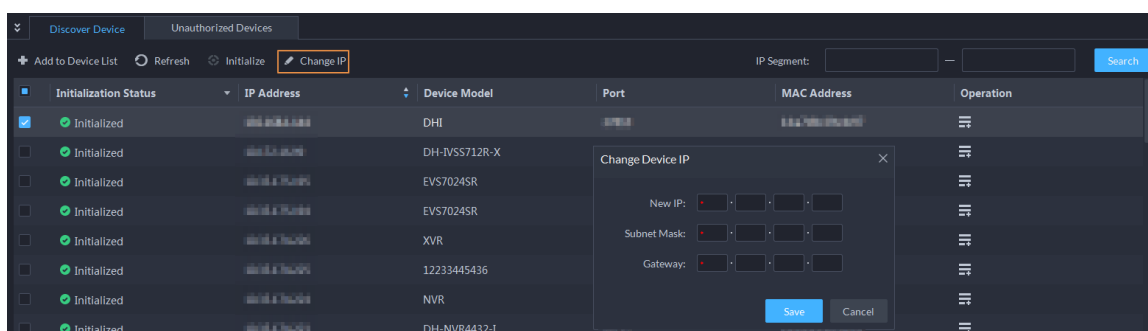
Step 1 Search for devices. For details, see "4.2.2.1 Searching for Online Devices".

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 4-7 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**.

4.2.2.4 Adding Devices

You can add different types of devices, such as encoder, decoder, ANPR device, access control, emergency assistance device, alarm box, 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**.

4.2.2.4.1 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 **Add**.

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. For details, see "3.4.1 NIC Config".

- **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, log in to the config system, select **Network Config > Network Mode**, and then change the port number of DSS_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.




The parameters vary with the selected protocols.

Figure 4-8 Add an encoder

The screenshot shows a configuration form titled "1.Login Information". It contains the following fields and options:



- Add Mode:** A dropdown menu with "IP Address" selected.
- Access Protocol:** A dropdown menu with "Dahua" selected.
- Device Category:** A dropdown menu with "Encoder" selected.
- IP Type:** Radio buttons for "IPv4" (selected) and "IPv6".
- IP Address:** A text input field containing a placeholder IP address.
- Device Port:** A text input field containing "3777".
- Username:** A text input field containing "admin".
- Password:** A password input field with masked characters.
- Organization:** A dropdown menu with "Root" selected.
- Server:** A text input field containing a placeholder server address.

- Step 5** Enter the information.
- Step 6** Click **OK**.
- To add more devices, click **Continue to add**.
 - To go to the web manager of a device, click .

4.2.2.4.2 Adding Devices through Searching

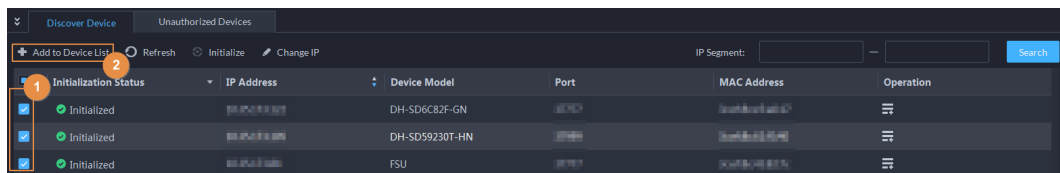
Devices on the same network with the platform server can be added using the automatic search function.

Procedure

- Step 1** Search for devices. For details, see "4.2.2.1 Searching for Online 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 4-9 Add in batches



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

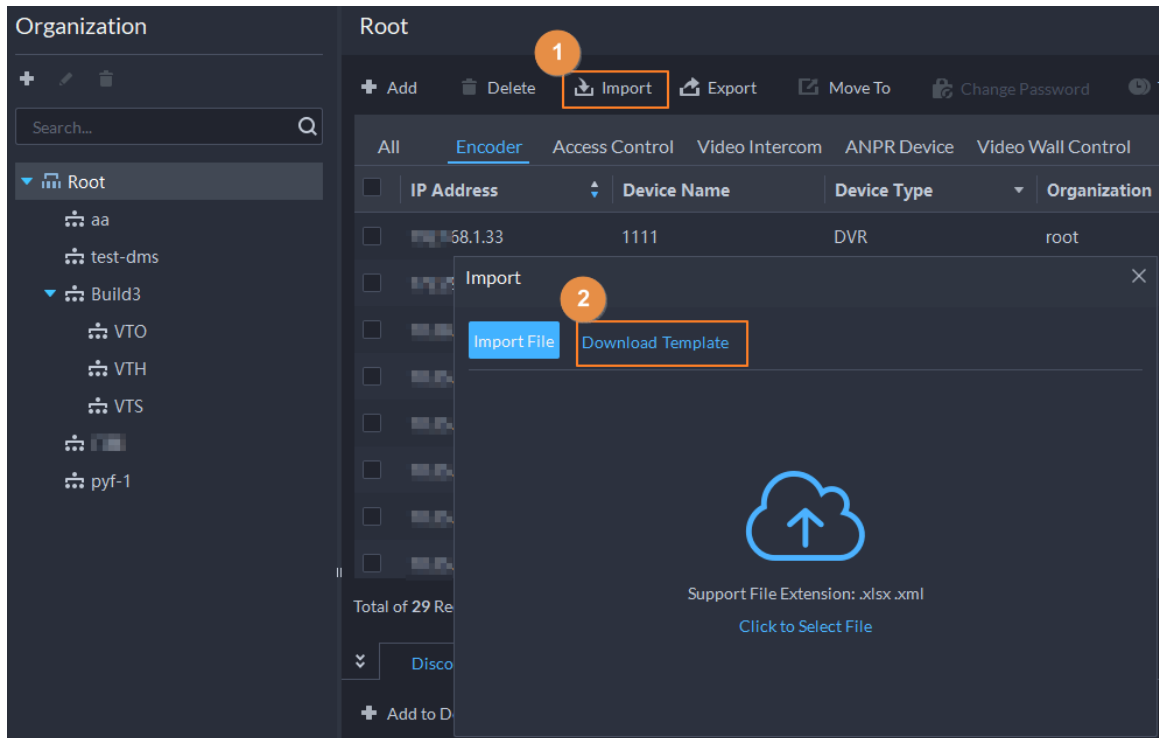
4.2.2.4.3 Importing Devices

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 4-10 Download template



Procedure



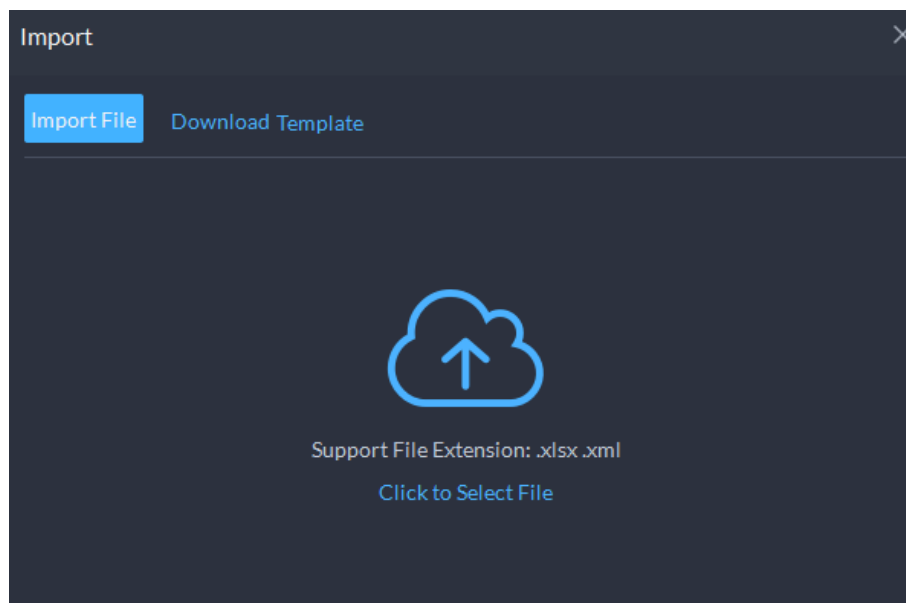
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Click **Import**.

Figure 4-11 Import devices



- Step 4** Click **Import File**, and then select the completed template.
- Step 5** Click **OK**.



4.2.2.5 Editing Devices

Edit the information of devices.

4.2.2.5.1 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**.

4.2.2.5.2 Modifying Device Information

Procedure




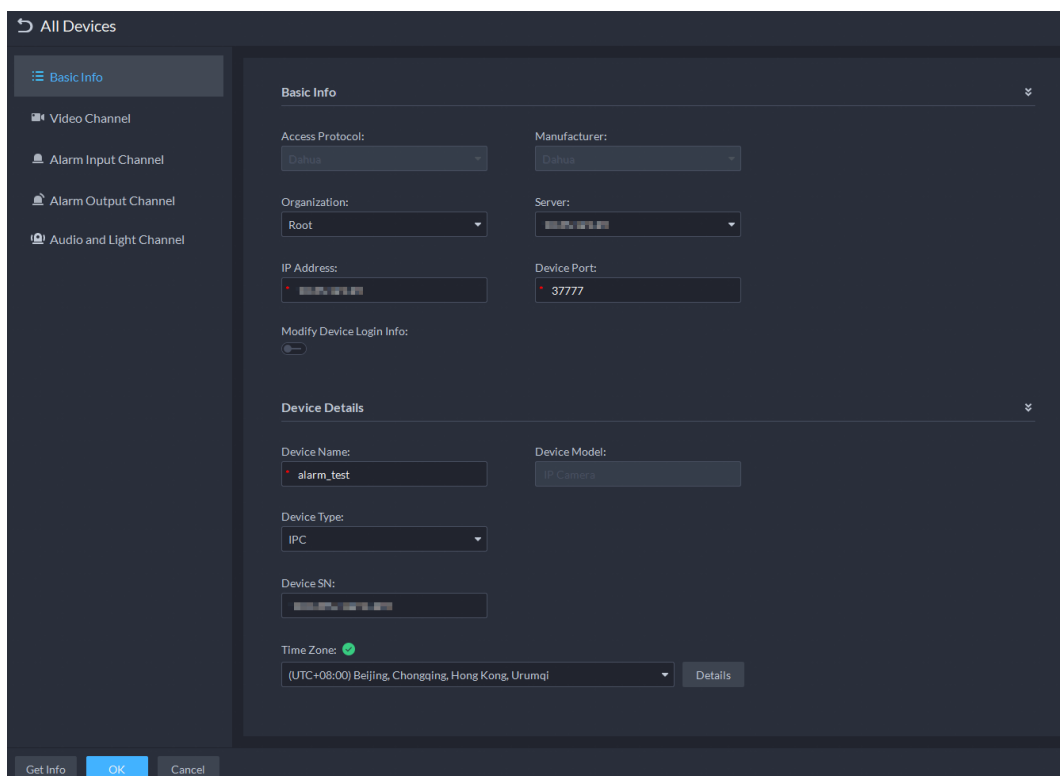
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Click  of a device, and then edit device information.
Click **Get Info** and the system will synchronize device information.

Figure 4-12 Basic information



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 it video channels.

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 number and names of alarm output channels.

Step 7 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 8 Click **OK**.

4.2.2.5.3 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**, and then click **OK**.

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.

4.2.2.5.4 Configuring Channel Features in Batches

Configure the channel features in batches so that devices can work normally. The platform also displays the number of each type of channels features allowed to be configured to help you plan the types and number of devices you will use.

Procedure


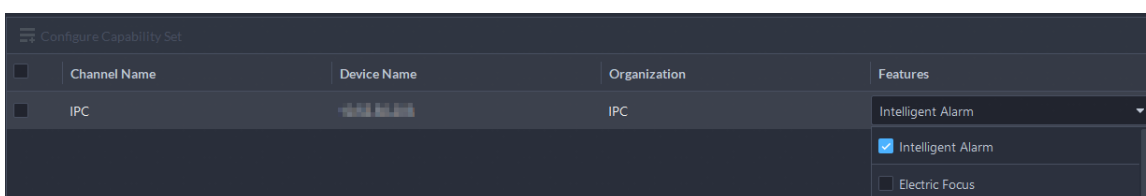
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** On the top of the page, select **More** > **Capability Set Management**.
- Step 3** In the **Capability Set Type** drop-down list, select a type, and then the platform 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 4-13 Select capability sets



- 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.

4.2.2.5.5 Modifying Device Organization

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

Procedure



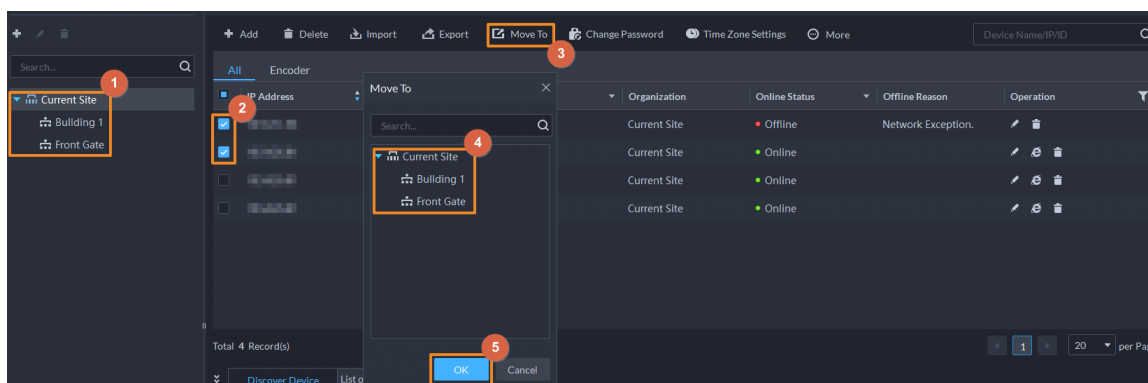
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Select a device to be moved, click **Move To**, select the target organization, and then click **OK**.

Figure 4-14 Move a device




4.2.2.5.6 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**.

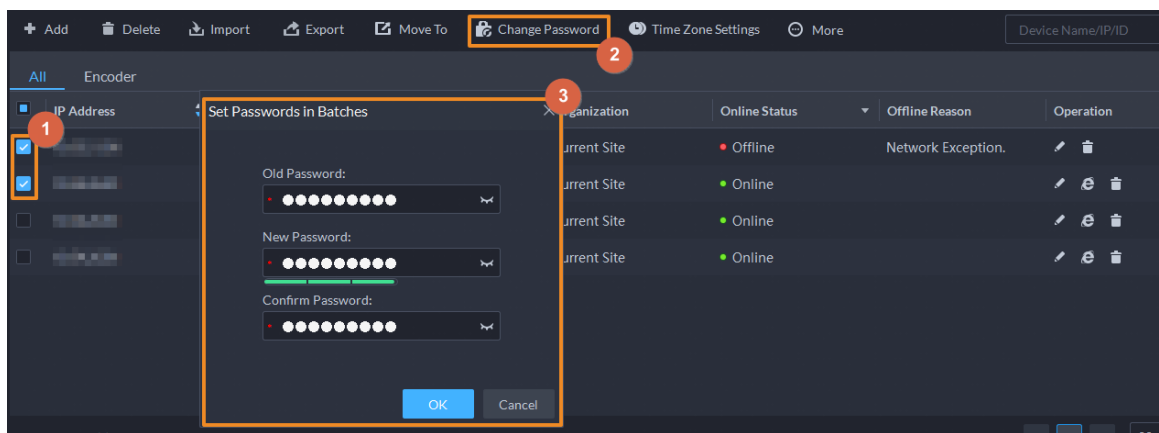
Step 2 Click .

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




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

Figure 4-15 Change device password



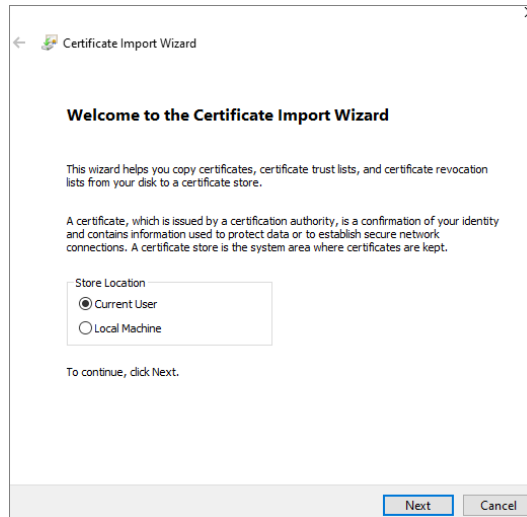
Step 4 Enter the old and new passwords, and then click **OK**.

4.2.2.6 Logging in to Device Webpage

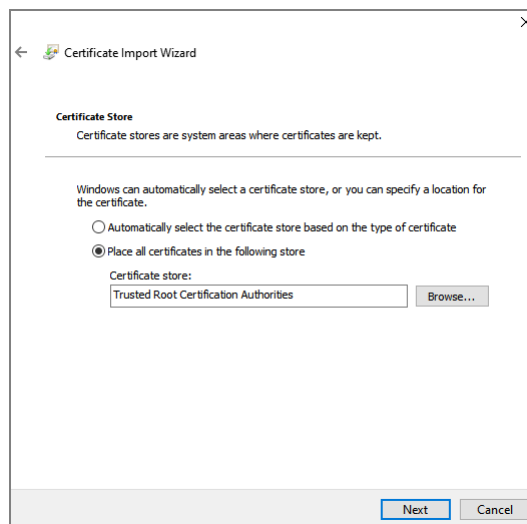
After a device is added to the platform, you can click  to go to the webpage of a device.

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**.



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



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.

4.2.2.7 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. You can export up to 100,000 devices at a time. 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 "8.3.1 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 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**.

4.2.2.8 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



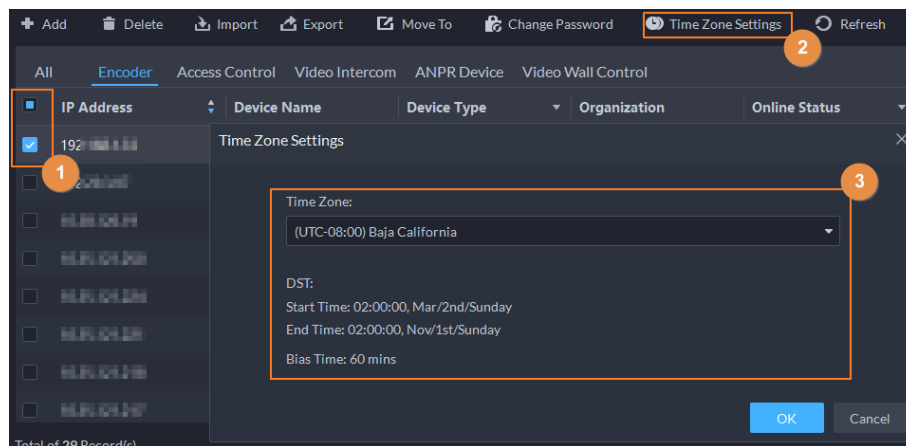
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Select a device, and then click **Time Zone Settings**.

Figure 4-16 Modify device time zone



- Step 4** Select a time zone.
- Step 5** Click **OK**.

4.2.3 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



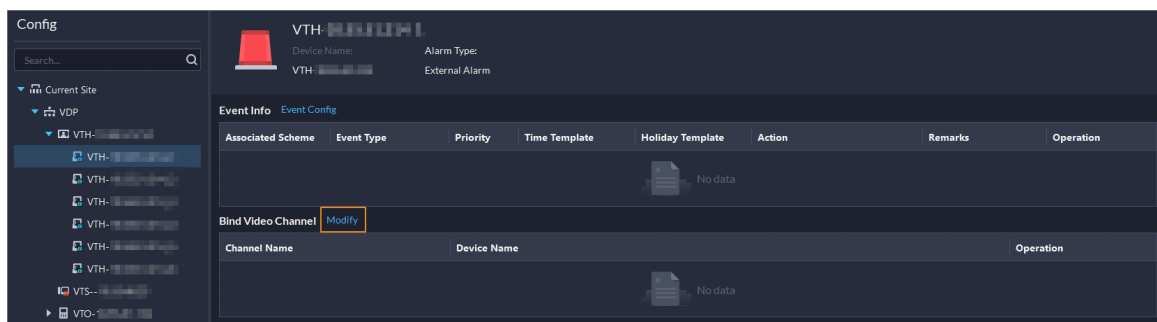
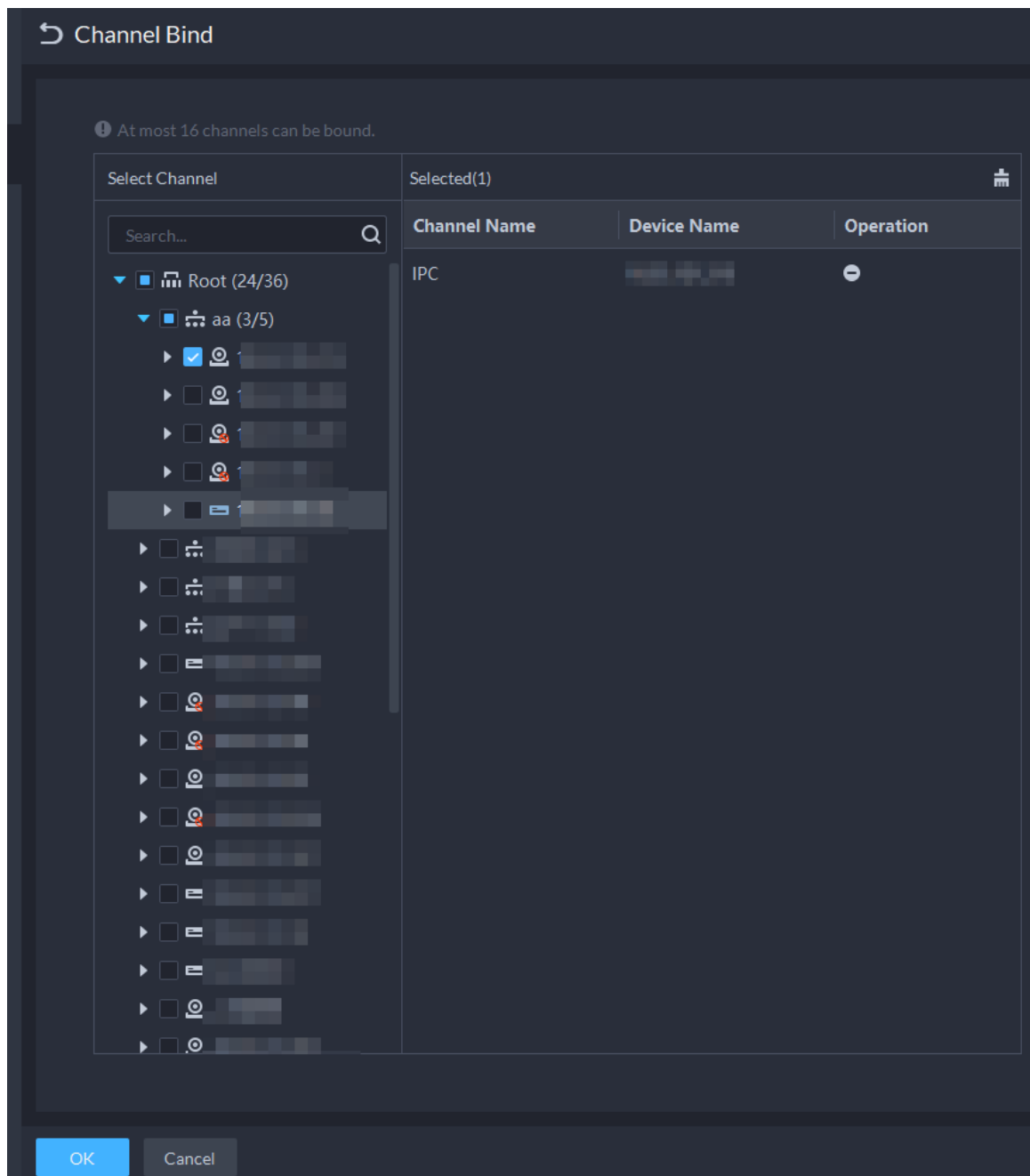
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .
- Step 3** Select a channel, and then click **Modify**.

Figure 4-17 Bind one or more channel



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

Figure 4-18 Select the channels you want to bind



Step 5 Click **OK**.

4.2.4 Adding Recording Plan

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.

4.2.4.1 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

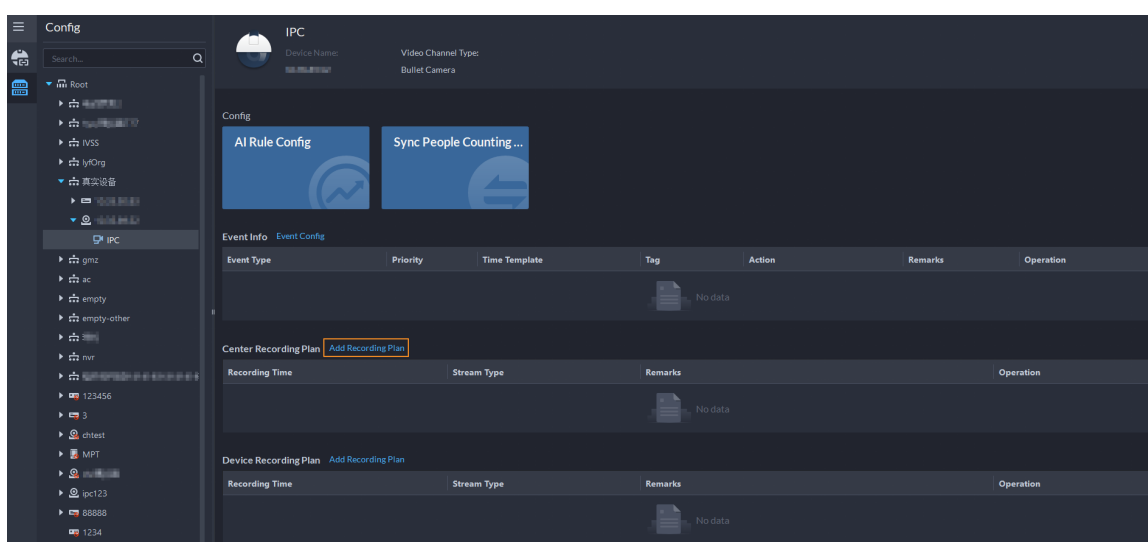
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

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 4-19 Add a center recording plan (1)



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

Table 4-2 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.
Recording Type	<ul style="list-style-type: none"> ● 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 "4.2.6 Adding Time Template".

3. Click **OK**.

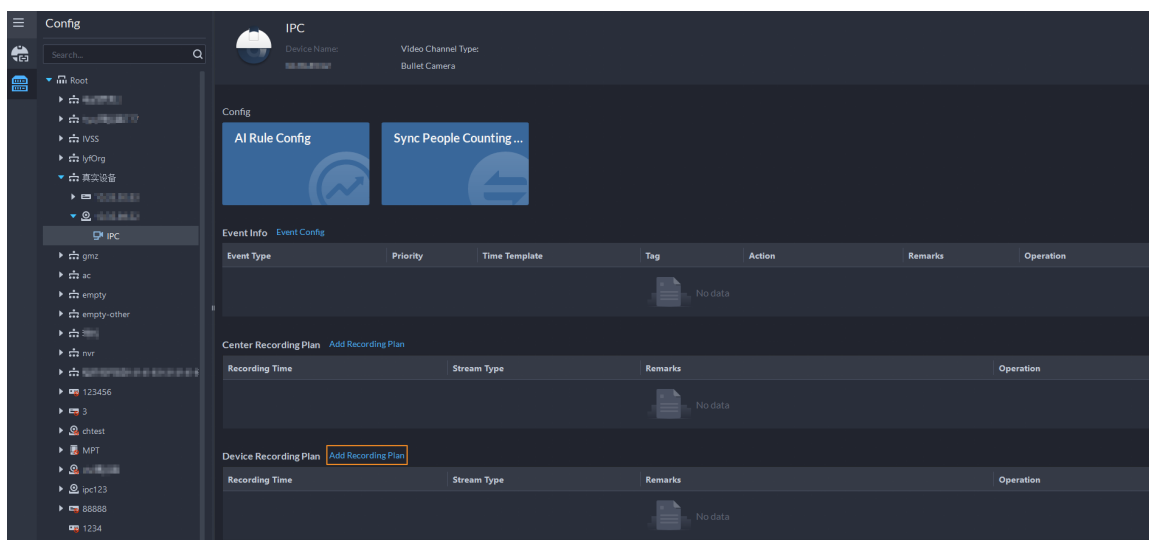
- Configure a device recording plan.



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.

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

Figure 4-20 Add a device recording plan (1)



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


Table 4-3 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 "4.2.6 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.

4.2.4.2 Adding Center Recording Plans in Batches

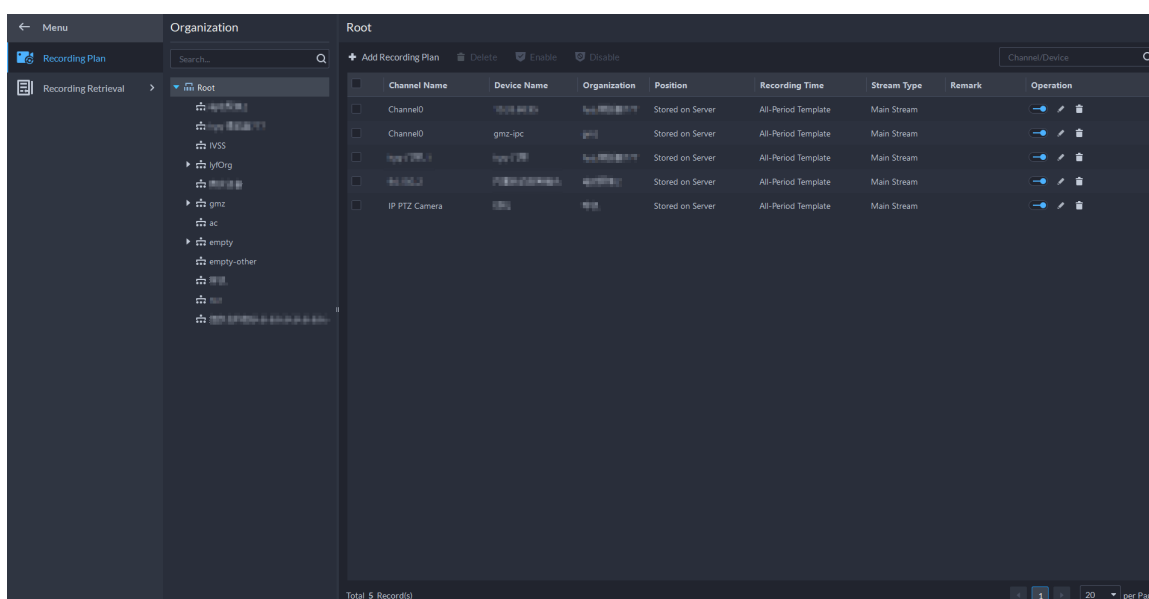
Add a center recording plan of general or motion detection videos for multiple channels at the same time.

4.2.4.2.1 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 4-21 Center recording plan



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

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

Table 4-4 Parameter description

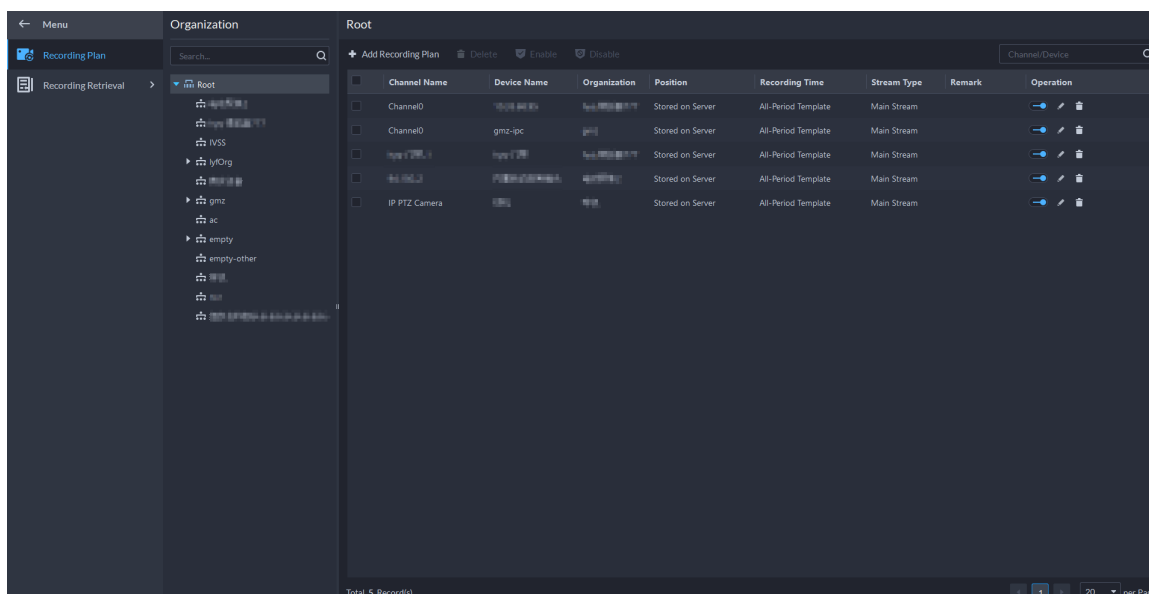
Parameter	Description
Enable	Turn on or off the recording plan.
Position	Videos will be stored on the server by default. It cannot be changed.
Stream Type	Select Main Stream , Sub Stream 1 or Sub Stream 2 . Videos recorded on the main stream will have the best quality, but they require more storage.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

4.2.4.2.2 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 4-22 Center recording plan



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








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

Table 4-5 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.
Recording Type	<ul style="list-style-type: none"> 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 "4.2.6 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.

4.2.5 Adding Video Retrieval Plan

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.

4.2.5.1 Adding Retrieval Plan One by One

Procedure



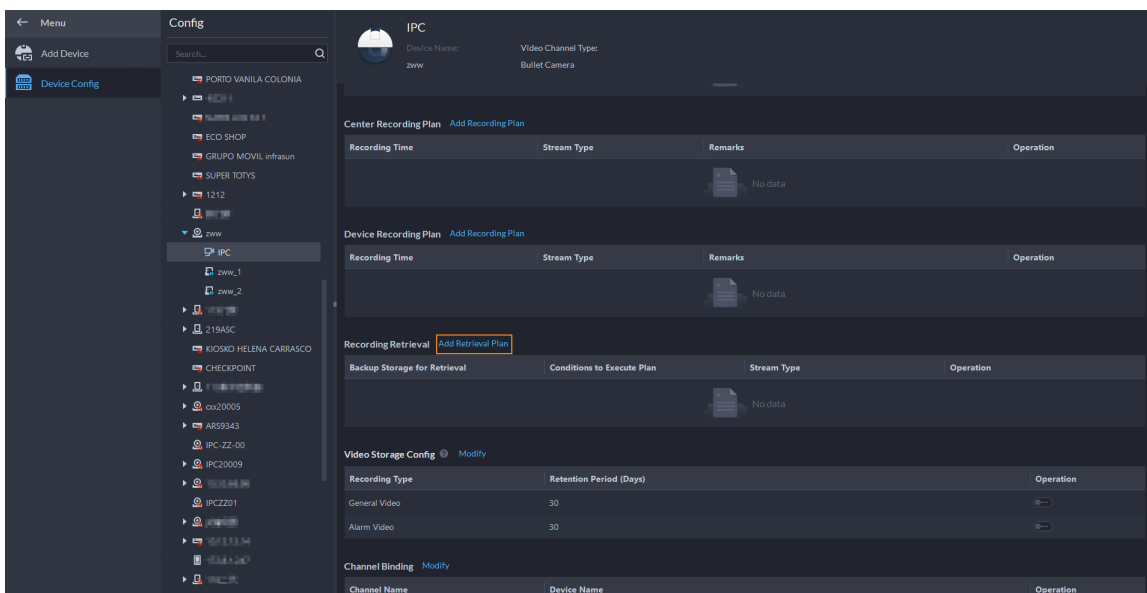
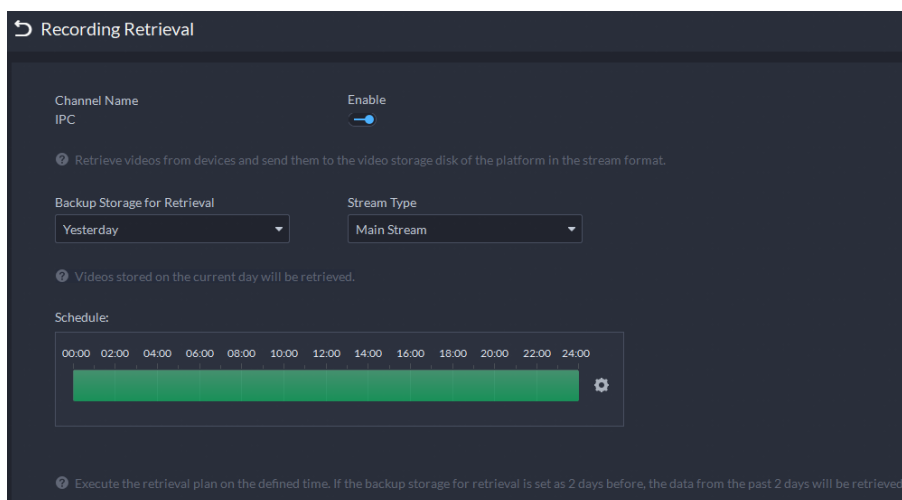
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2** Click .

Figure 4-23 Add a retrieval plan for a channel




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

Figure 4-24 Add a retrieval plan







Step 4 Configure the parameters.

Table 4-6 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.
Schedule	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

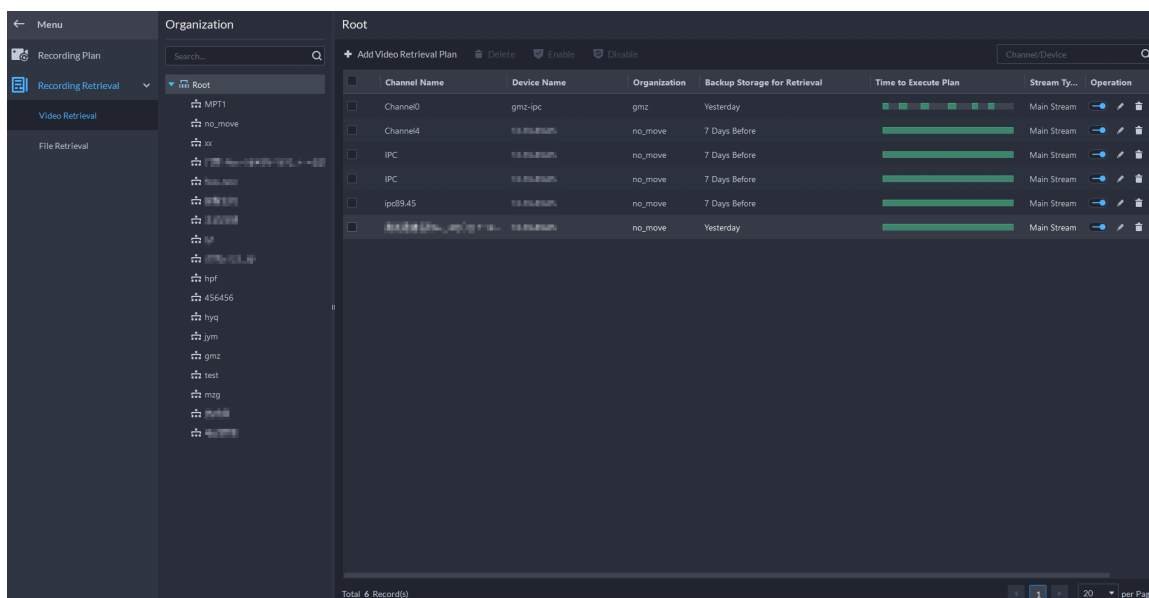
- Enable/disable retrieval plan
 -  means that the plan has been enabled. Click the icon and it becomes , and it means that the plan has been disabled.
- Edit retrieval plan
 - Click  of corresponding plan to edit the plan.
- Click  to delete recording plans one by one.

4.2.5.2 Adding Retrieval Plans in Batches

Procedure

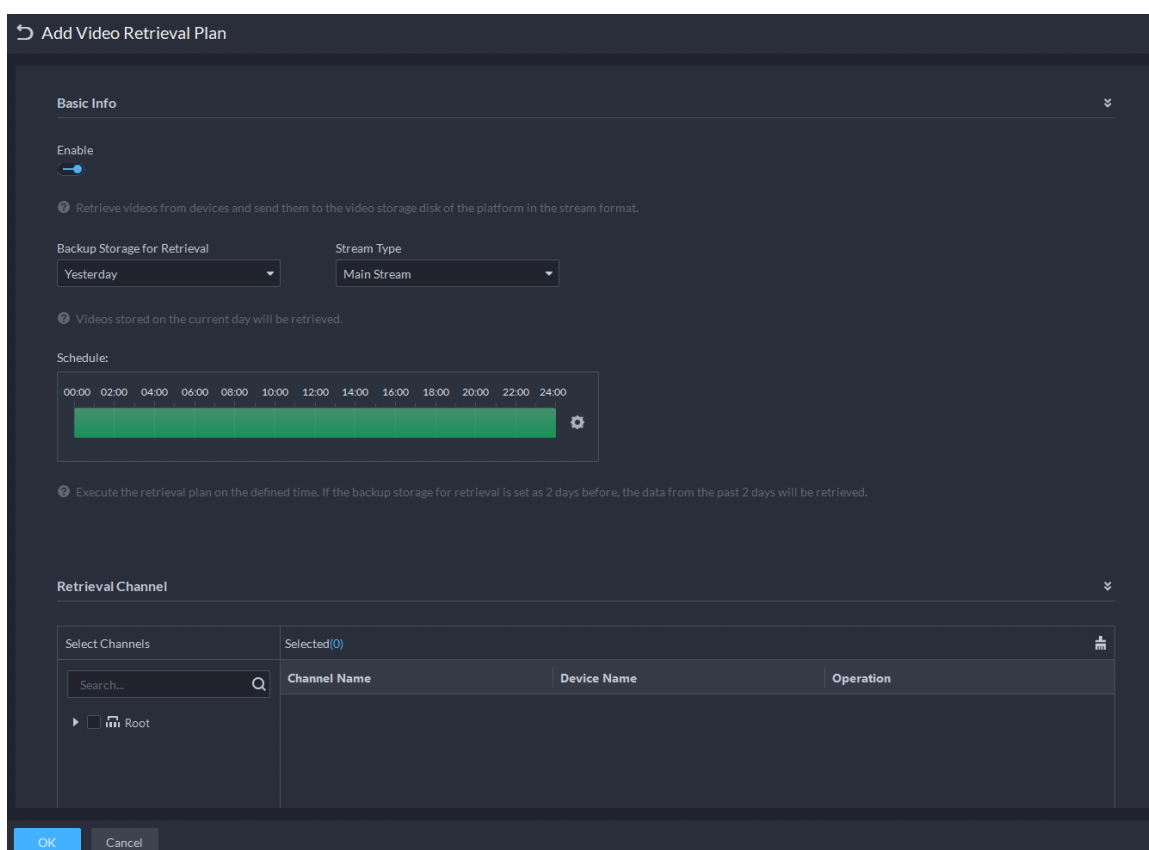
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Storage Plan** > **Recording Retrieval** > **Video Retrieval**.

Figure 4-25 Video retrieval



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


Figure 4-26 Configure a video retrieval plan



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

Table 4-7 Parameter description


Parameter	Description
Enable	Turn on or off the retrieval plan.


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

Step 4 Click **OK**.

4.2.6 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**.

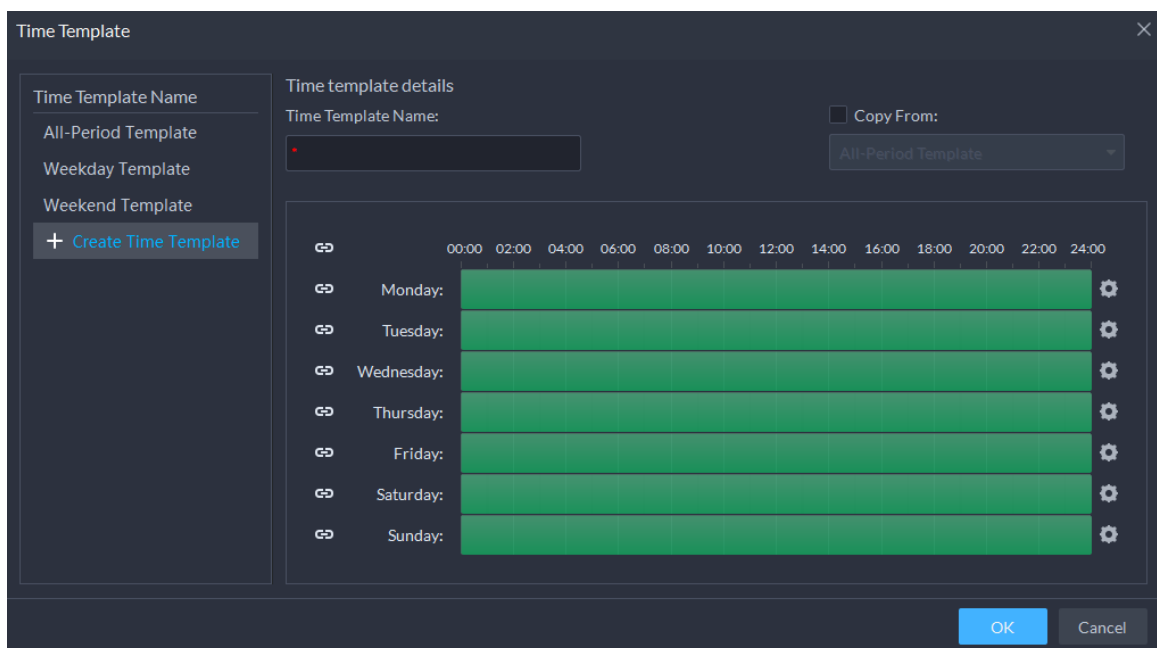
Step 2 Click .

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 4-27 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**.

4.2.7 Configuring Video Retention Period

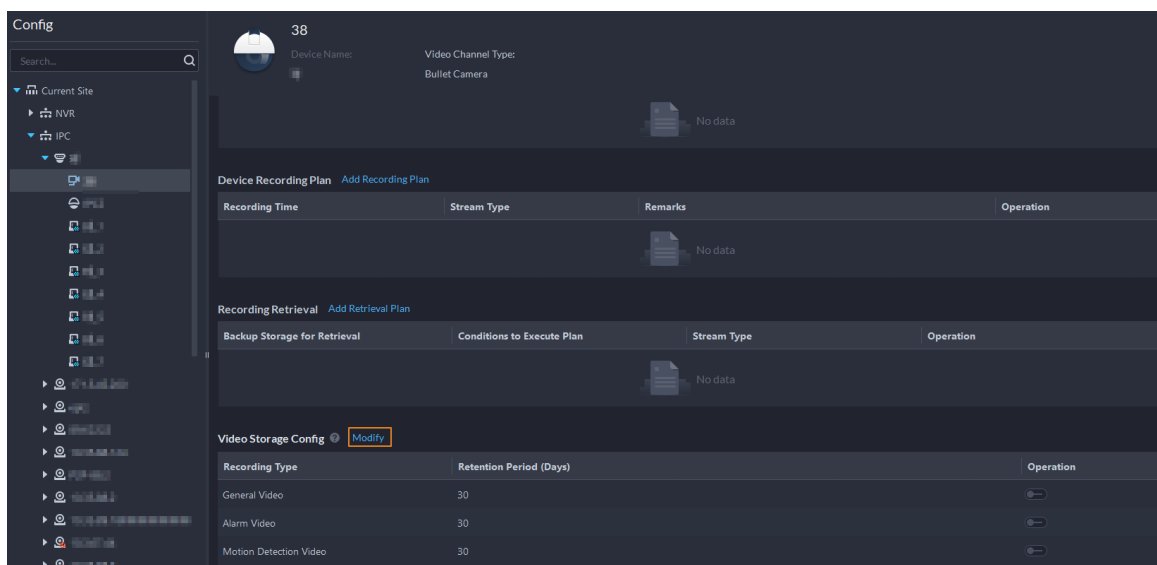
For videos stored on the platform, you can configure video retention period. When the storage space runs out, new recorded videos will cover the oldest videos automatically.

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 4-28 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**.

4.2.8 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 4-29 Go to the event configuration (device)

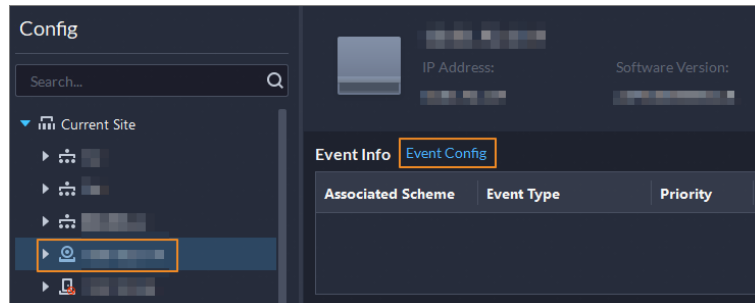
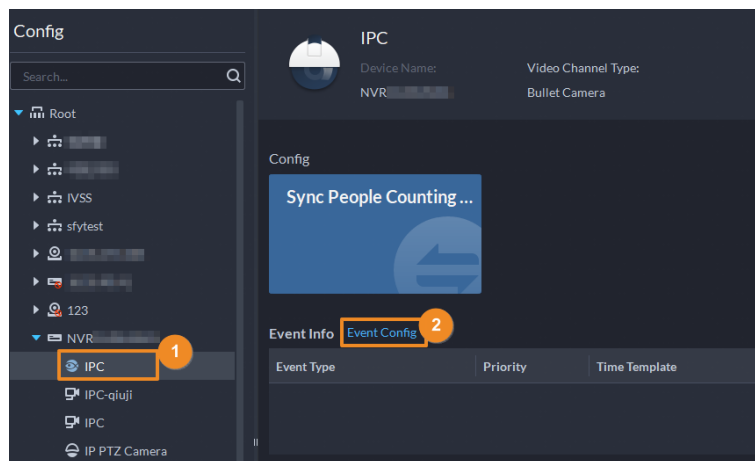


Figure 4-30 Go to the event configuration (channel)



Step 3 Configure events. For details, see "5.1 Configuring Events".

4.2.9 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



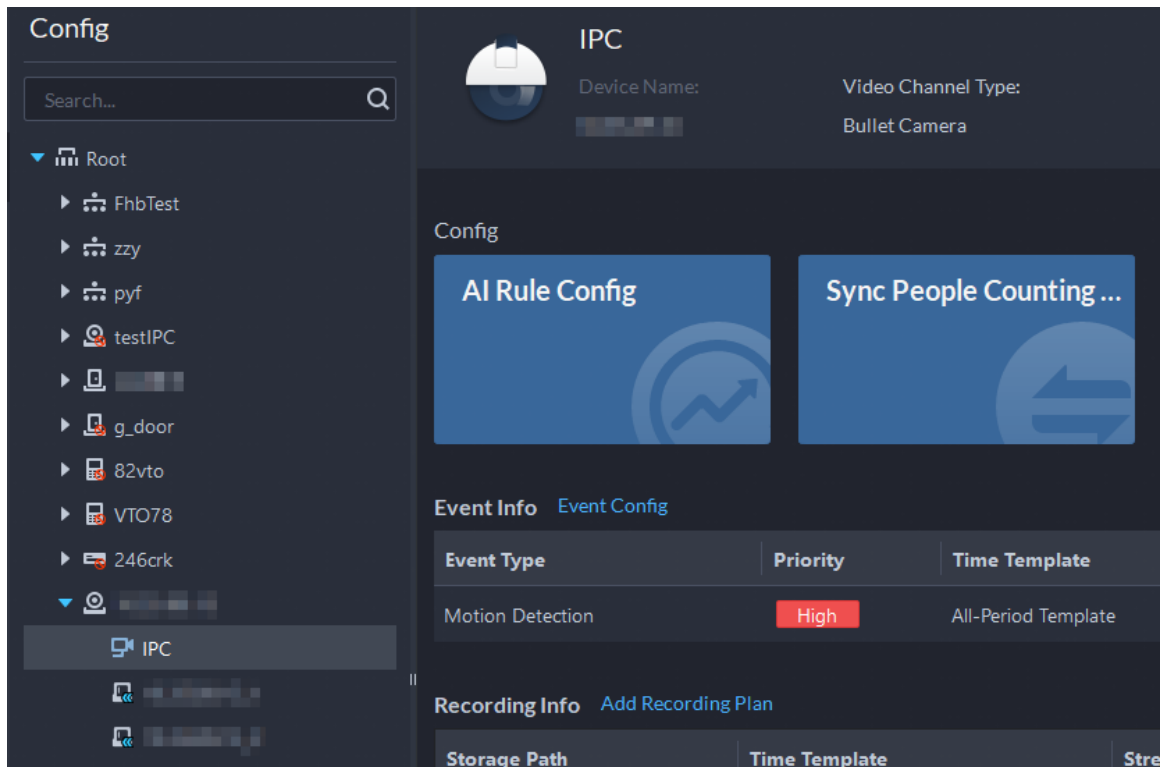
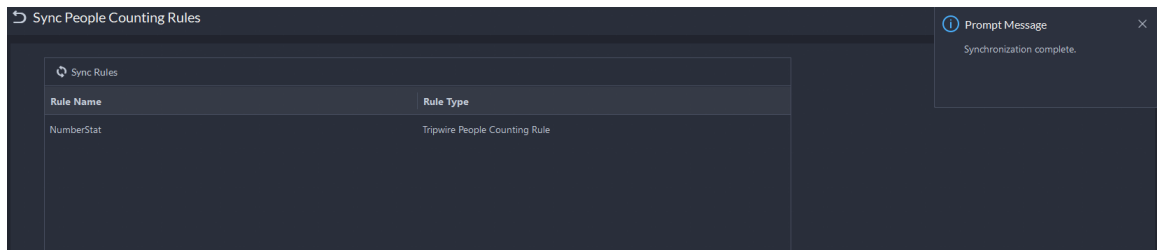
- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.
- Step 2 Click .
- Step 3 Select a channel, and then click **Sync People Counting Rules**.

Figure 4-31 Synchronize people counting rules from the device



Step 4 Click **Sync Rules**, and then the system prompts **Synchronization Complete**.

Figure 4-32 Synchronize people counting rules from the device



4.3 Adding Role and User

Users of different roles have different menus and permissions of device access and operation. When creating a user, assign a role to it to give the corresponding permissions.

4.3.1 Adding User Role

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

- Super administrator: A default rule that has the highest priority and all the permissions. This role cannot be modified. A super administrator can create administrator roles and common roles. The system supports 3 super administrators at most.
- Administrator: A default rule that cannot be modified and has no permission of authorization, backup and restoring. An administrator can only create common roles.
- Common role: A common role that has no permission of authorization, backup and restoring, user management, and device management.

Procedure



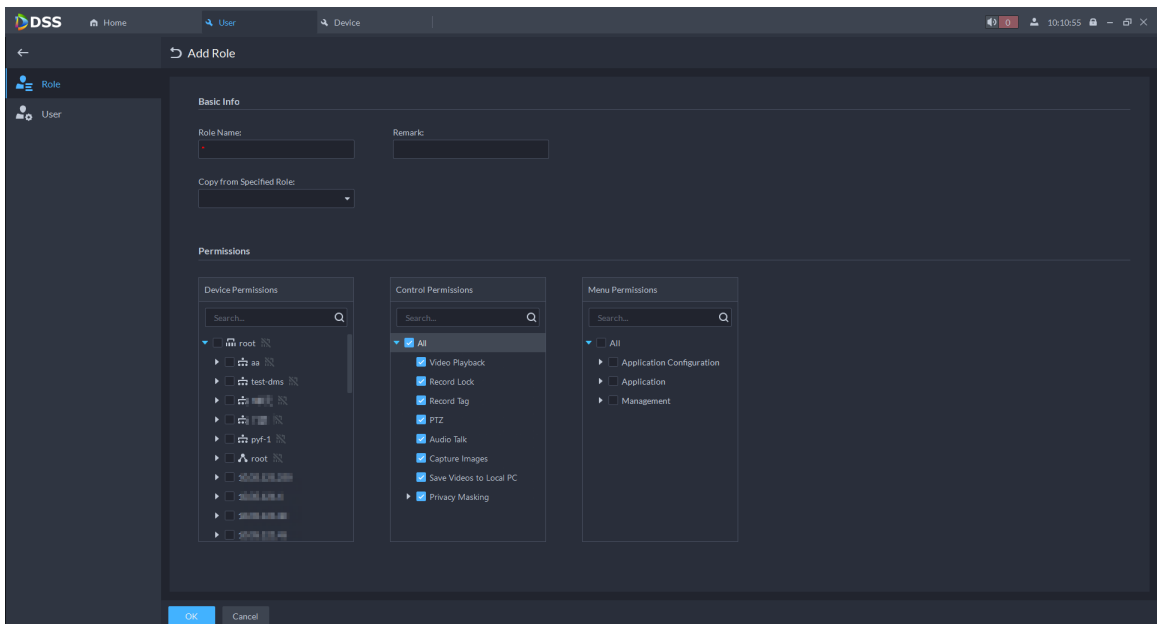

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User**.
- Step 2** Click .
- Step 3** Click **Add**, set role information, and then select device and control permissions and assign the rule to users.

Figure 4-33 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.

- Step 4** Click **OK**.

4.3.2 Adding User

Create a user account for logging in 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 **User**.
- Step 2** Click **Add**, and then configure the user information.




Table 4-8 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.

Parameter	Description
Password	Used to log in to the client.
Confirm Password	
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.
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.

4.3.3 Importing Domain User


When the users in a domain can be used as users on the platform, you can use this function to import quickly them to the platform.

Procedure

Step 1 Configure the domain information.


1. Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameter** > **Active Directory**.
2. Click  to enable the function, and then configure the parameters of the domain.
3. Click **Get DN** to automatically get the basic DN information.
4. Click **Test** to check whether the domain information is correct.
5. (Optional) Enable the automatic synchronization function and set a time. Then, the platform will automatically synchronize news users in domain 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 domain group A. The platform will synchronize new users in domain 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.

6. Click **Save**.

Step 2 Import domain users.

1. Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User > User Management**.
2. Click **Import Domain Users**.
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 and 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.

4. Click  to select a role for the users.

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

5. Click **OK**.

4.3.4 Syncing Domain User

Use this function to delete invalid domain users from the platform.

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 delete invalid domain users.

Step 3 Click **OK**.

4.3.5 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.

4.3.5.1 Changing Password for the Current User

We recommend changing your password regularly for account safety.

Procedure


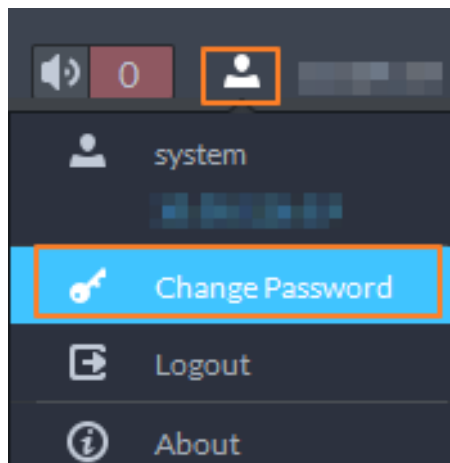
- Step 1** Log in to the DSS Client, click  at the upper-right corner, and then select **Change Password**.

Figure 4-34 Change password



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

4.3.5.2 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




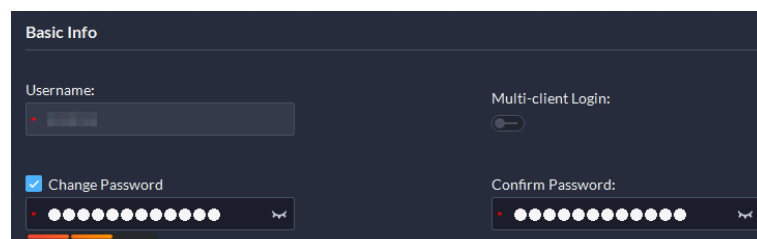
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User**.
- Step 2** Click .
- Step 3** Select a user, and then click .
- Step 4** Enable **Change Password**, enter the new password and confirm password, and then click **OK**.

Figure 4-35 Change passwords for other users



4.3.5.3 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 email address. This is applicable to all accounts, but an email address must be configured first. For details, see "4.3.2 Adding 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.

4.3.5.4 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.

4.4 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.

4.4.1 Configuring Network Disk

Do not use NAS as a network disk because it might result in data lost. We recommend using 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 disk. Check if you have backed up the data.

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 4-36 Add network disk (normal mode)

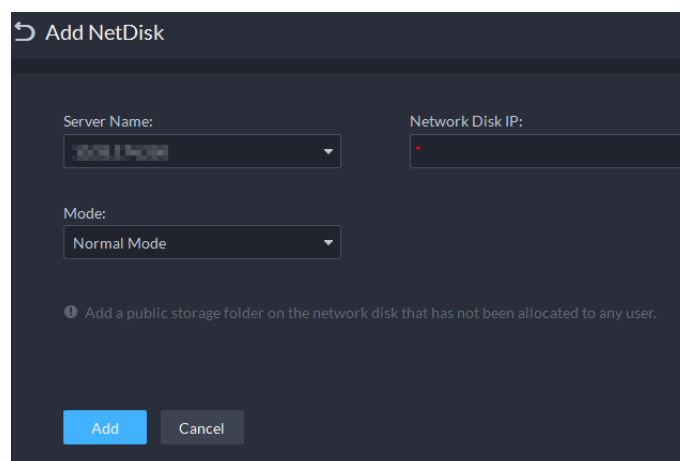
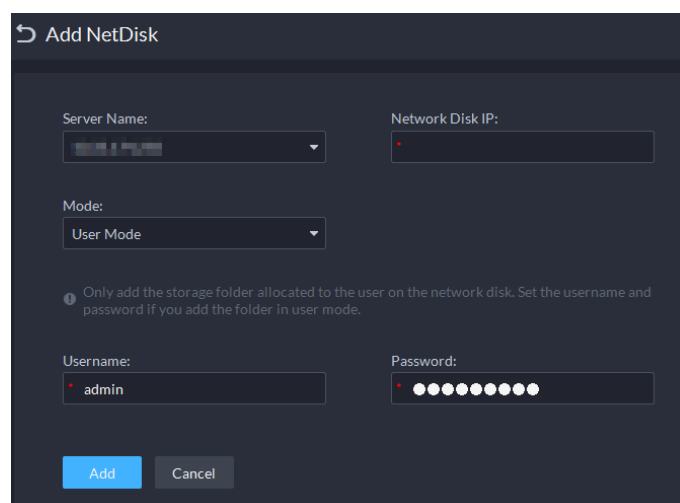


Figure 4-37 Add network disk (user mode)





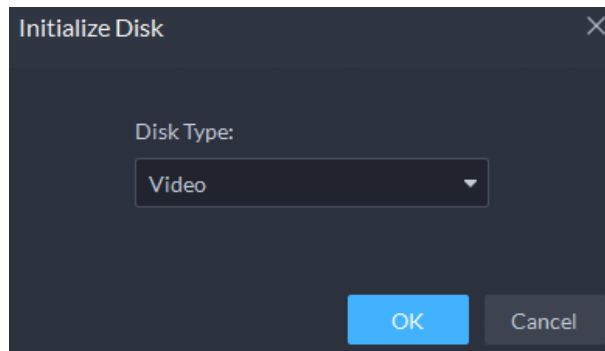


- Step 5** Select disk, and then click  to format the corresponding disk.
1. Select user volume, and then click .
 2. Select format disk type, and then click **OK**.
- **Video** : Stores videos.
 - **Image and File** : Stores all types of images.

Figure 4-38 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.

4.4.2 Configuring Server Disk

Configure local disk to store different types of files, including videos, ANPR snapshots, 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 loss.



- 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.





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 .
- Configure a hot standby disk


Select a disk, click , configure the parameters, and then click **OK**. The disk is configured as backup disk that can replace the damaged disk in the RAID group.

Figure 4-39 Configure hot standby disk

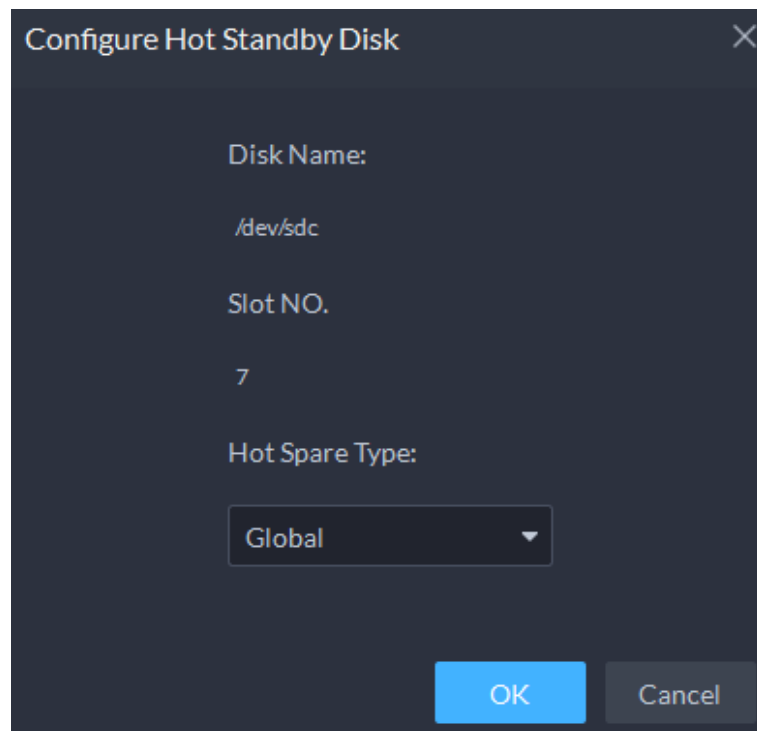



Table 4-9 Hot standby disk parameter

Parameter	Description
Hot Spare Type	<ul style="list-style-type: none"> ◇ Local Set disk as backup disk of designated RAID group. Recreate system immediately when disk error happens in the RAID group.  Local hot spare is only applicable to RAID5. ◇ Global Set disk as backup disk of all RAID groups. Recreate system immediately when disk error happens in any RAID group.

4.4.3 Configuring RAID Group

Use local disks to create RAID group for higher storage performance and data redundancy.

Procedure

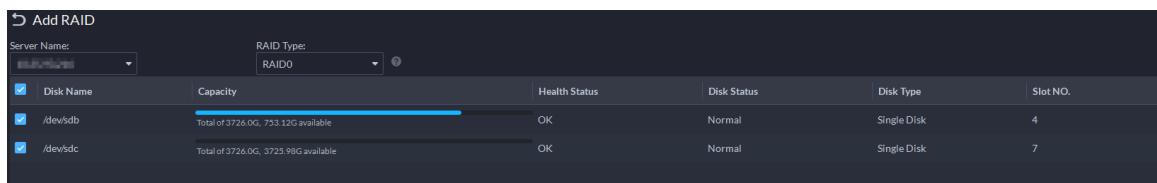
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Storage > Server Disk > Add RAID**.

Step 2 Select the server, RAID type, and the disks to be included.



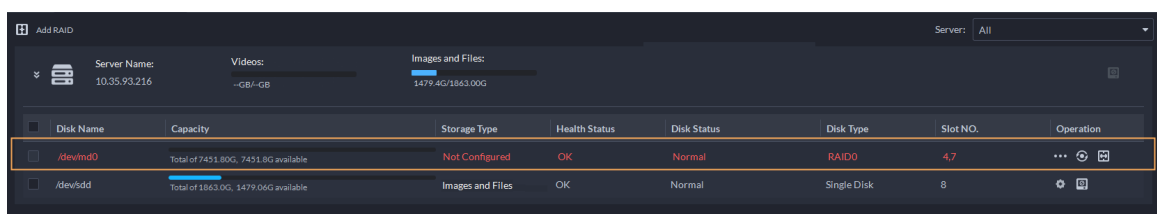
For introduction to different types of RAID, see "Appendix 1 RAID".

Figure 4-40 Add RAID






Step 3 Click **OK**.

Figure 4-41 Added RAID



Step 4 Manage RAID storage.

- : View details of the RAID.
- : Initialize RAID for normal use.
- : Divide RAID.

4.4.4 Configuring Disk Group

Allocate disk groups for video storage.

Procedure



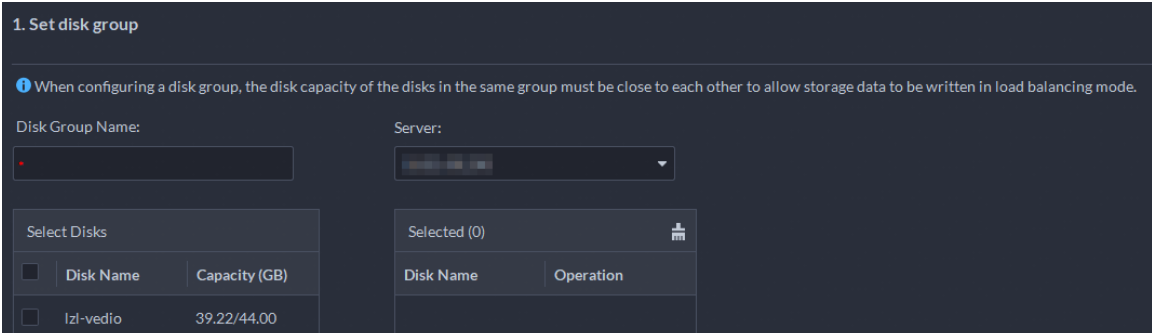
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Storage**.
- Step 2** Click .
- Step 3** Click **Add Disk Group**, enter disk group name, and then select a server and disks.

Figure 4-42 Configure disk group



1. Set disk group

When configuring a disk group, the disk capacity of the disks in the same group must be close to each other to allow storage data to be written in load balancing mode.

Disk Group Name:

Server:

Select Disks		Selected (0)	
Disk Name	Capacity (GB)	Disk Name	Operation
<input type="checkbox"/>	Izl-vedio 39.22/44.00		

- Step 4** Click **Next Step**.
- Step 5** Select devices or channels on the left.
- Step 6** Click **OK**.

4.4.5 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 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 4-10 Parameter description

Parameter	Description
Event Image Storage Location	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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.  <p>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.</p>
Retention Time of Images and Videos on Device	<p>This function is applicable to the images and videos stored on the device.</p> <p>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.</p>  <p>Deleted files cannot be recovered. Please be advised.</p>

5 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.

5.1 Configuring Events

To receive alarms triggered by devices, you need to configure them on the platform.

5.1.1 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** Configure the event source.

Table 5-1 Parameter description

Parameter	Description
Device, video channel, alarm input channel, zone, access control channel, parking lot, and people counting group,	<p>Select an event source type.</p>  <ul style="list-style-type: none"> 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 "4.2.2.5.2 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	<p>This is a type of event that is manually triggered. Click Add Soft Trigger Event Type 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.</p>
Combined Event	<p>When a combined event is triggered, the platform performs the defined linked actions. For how to configure combined events, see "5.1.2 Configuring Combined Event".</p>

Parameter	Description
Custom Alarm	<ul style="list-style-type: none"> ● DHOP event: Access events developed through Hardware Open Platform. ● Extended standard event: This is used for events that devices support, but the platform currently does not. Click Add Extended Standard Event, and then configure the parameters. <ul style="list-style-type: none"> ◇ 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.

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




Table 5-2 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 "4.2.6 Adding Time Template".
Holiday Template	<p>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.</p> <ol style="list-style-type: none"> 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.
Tag	Enter some content that is used for filtering among a large amount of events.

Step 5 Configure alarm linkage actions.

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

Table 5-3 Parameter description

Parameter	Description
Camera	<ul style="list-style-type: none"> ◇ 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 "4.2.3 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	<p>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.</p>  <p>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 "9.3.4 Configuring Alarm Settings".</p>
Event Recording	The platform will record videos when an alarm is triggered. It will be saved to the video disk of the platform.
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	<p>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.</p>  <p>For how to configure the pre-recording mode for devices in batches, see "5.1.3.3 Configuring Alarm Video Pre-recording".</p>  <ul style="list-style-type: none"> ◇ 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.

- To trigger a snapshot, enable **Trigger Snapshot**. The platform takes 2 snapshots, 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.

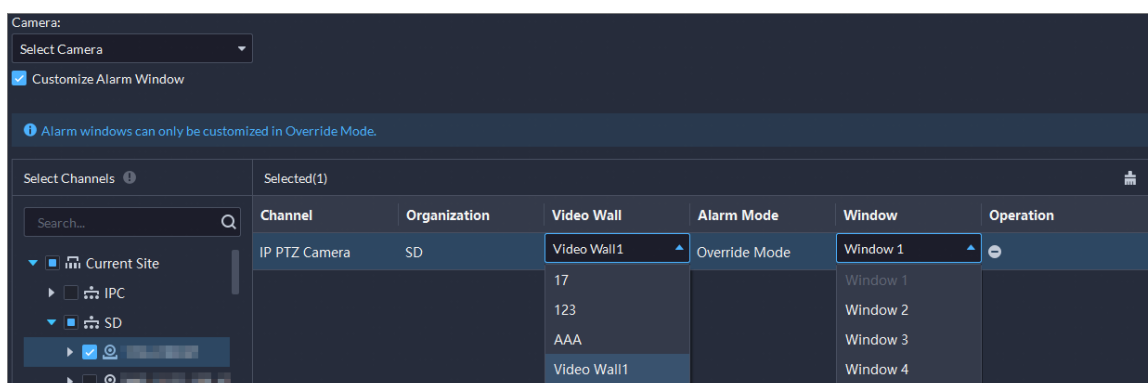
Click **Link Video Wall**, and then select the channels and video wall.





You must add a video wall and configure its alarm on video wall mode first. For details, see "6.1.5.1 Configuring Video Wall" and "5.1.3.2 Configuring Alarm on Video Wall".

If you select **Camera** to **Select Camera**, you can configure which channels to be displayed on the specified video wall. When the video wall you select is configure 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.

Figure 5-1 Display video of specified windows



- To execute an HTTP URL; command, click **Link HTTP URL Command**. Click **Add**, and then configure its request method, HTTP URL, and remarks. You can click  to test if the command is valid.
- 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.

- 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.

Step 6 Select one or more users 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 "4.3 Adding Role and User".



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 7 Click **OK**.

5.1.2 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  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 5-4 Parameter description

Parameter	Description
Name	Enter a name for the 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.

5.1.3 Configuring Alarm Parameter

5.1.3.1 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 an event, and then configure the interval.

Step 4 Click **OK**.

5.1.3.2 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 "6.1.5.1 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.

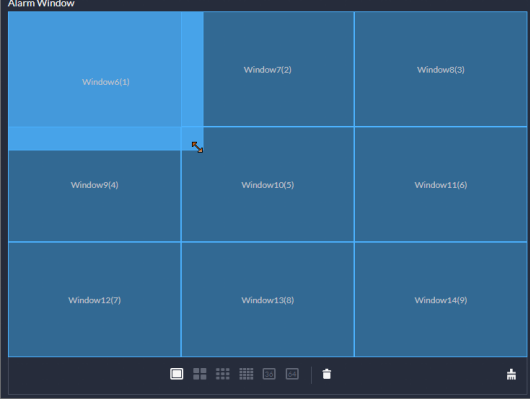
Table 5-5 Parameter description

Parameter	Description
Alarm on Video Wall Mode	<ul style="list-style-type: none"> 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	<p>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:</p> <ul style="list-style-type: none"> 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 5-6 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	<ul style="list-style-type: none"> Click a window, and then drag its frame near the lower-right corner to resize it.  <ul style="list-style-type: none"> 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	<p>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.</p> <p>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.</p>
Change the names of windows	<ul style="list-style-type: none"> 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**.

5.1.3.3 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 pre-recorded 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 Storm Config**.
- 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**.

5.2 Configuring Map

5.2.1 Preparations

- Devices are deployed. For details, see device user's manuals.
- Basic configurations of the platform have been finished. For details, see "4 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**.

5.2.2 Adding Map

5.2.2.1 Adding Vector Map

Procedure



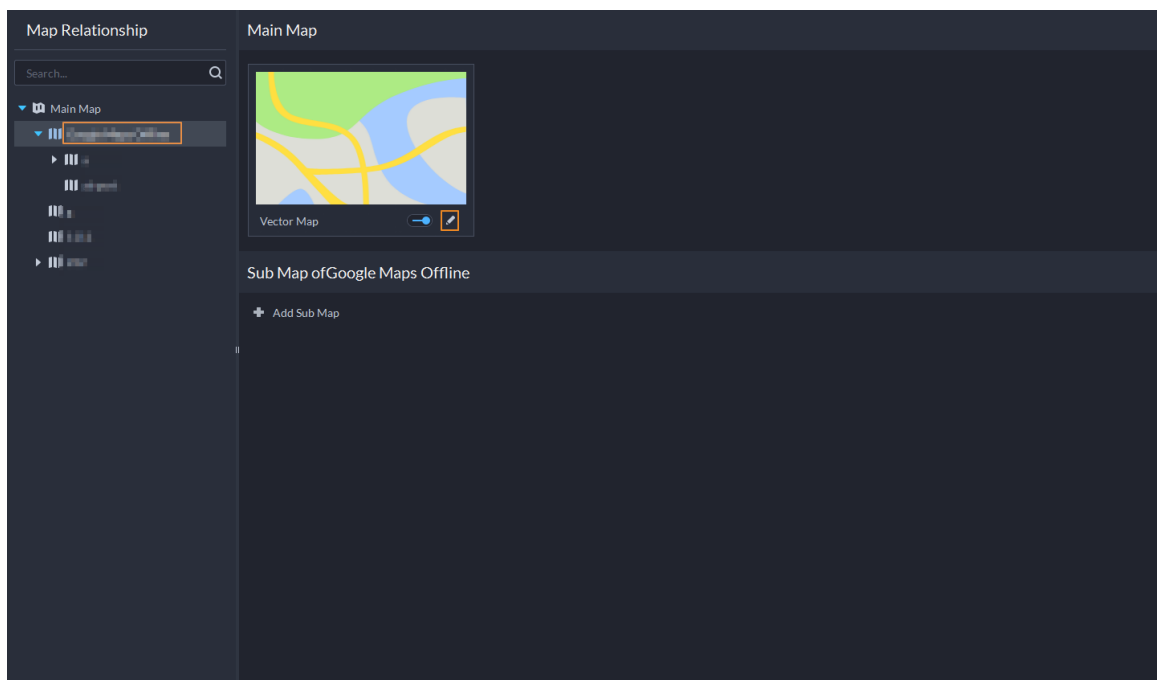
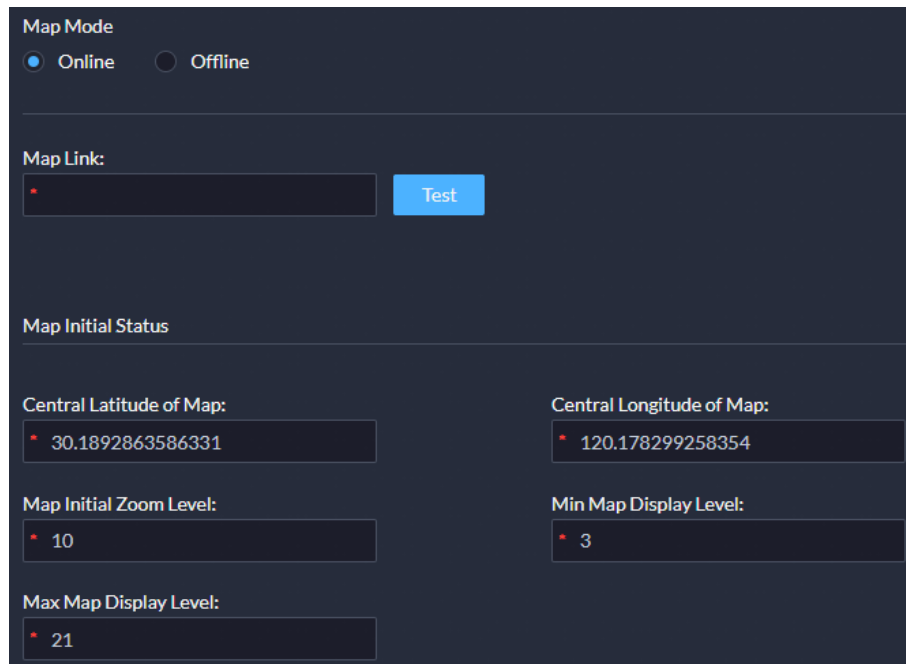
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Map**.
- Step 2** In the map list, select the vector map, and then click .

Figure 5-2 Map



- Step 3** Configure the parameters.

Figure 5-3 Map information



Map Mode

Online Offline

Map Link:

Map Initial Status

Central Latitude of Map:

Central Longitude of Map:

Map Initial Zoom Level:

Min Map Display Level:

Max Map Display Level:

- 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 5-7 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	
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.
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.

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 picture, and then click **OK**.
3. Drag the map to adjust its position, and then click **OK**.

The sub map is added.

Related Operations

- Hide Device Name

Only display the icons of devices.

- Satellite Map

View the satellite map.

- Delete Devices

To delete a device from the map, click it and then click **Delete Resource**.

- Show Device

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

- Move

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

- Select

To select one or more devices, click **Select**, and then click on the devices on the map one by one.

- Pane

To select devices in batches, you can click **Pane**, and then draw a frame on the devices to select the device.

- Clear

To clear all markings on the map, click **Clear**.

- Add 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**.

- Length

Select **Box** > **Length**, connect two 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.

5.2.2.2 Adding 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


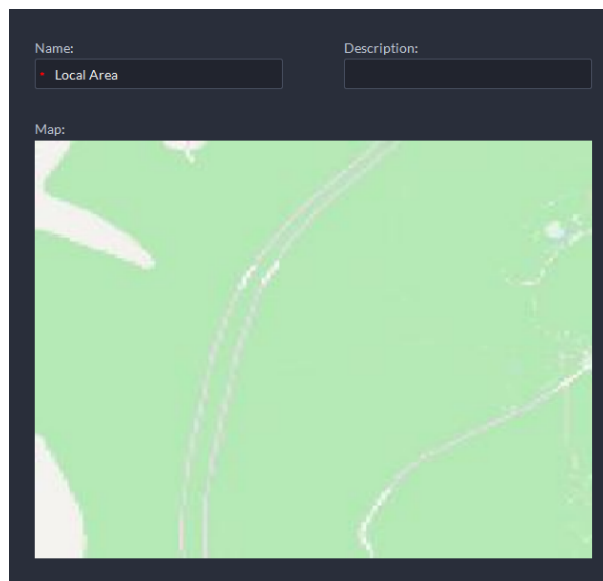
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Map**.
- Step 2** Select **Main Map**, and then click **Add Map**.
- Step 3** Enter the map name, select the picture and then click **OK**.

Figure 5-4 Add main map



- Step 4** Add a child map.
1. Click the added raster map, and then click **Add Sub Map**.
 2. Enter the map name, upload the picture, and then click **Next Step**.
 3. Drag the picture to the desired position and click **OK**.

Related Operations

- Hide Device Name
Only display the icons of devices.
- Delete Devices
To delete a device from the map, click it and then click **Delete Resource**.
- Show Device
Select which type of resources you want to display on the map.
- Move
To move a device, click **Move** and then drag the device on the map.
- Select
To select one or more devices, click **Select**, and then click on the devices on the map one by one.
- Pane
To select devices in batches, you can click **Pane**, and then draw a frame on the devices to select the device.
- Clear

To clear all markings on the map, click **Clear**.

- Add 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**.

- Map scale

Select **Map Scale** > **Configure the map scale**, draw a line on the map, and then enter its actual distance.

- Length

Select **Box** > **Length**, connect two 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.

5.2.3 Marking Devices

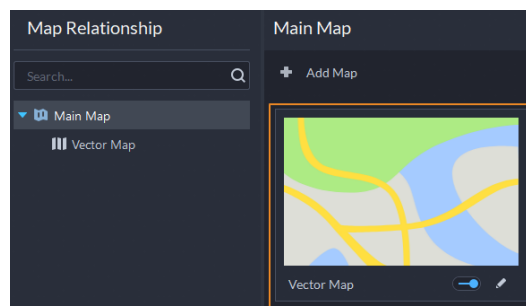
Link a device to the map by dragging it to the corresponding location on the map according to its geographical location.

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 5-5 Map



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

5.3 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 picture, 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.

5.3.1 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 **Personal and Vehicle Info**.
- Step 2** Click **Person List** or **Vehicle List**.
- Step 3** Click , and then configure the parameters.

Table 5-8 Parameter description

Parameter	Description
Parent Group	This is for permission control. For example, if a user cannot access Group A, then the user cannot access all the groups under Group A.
Group Name	Enter a name for the group.
Roles Allowed Access	<p>Only the roles and their users can view this group.</p> <p></p> <p>Click  to see the users assigned with the roles.</p>

- 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 "5.3.2 Configuring Personnel Information".

5.3.2 Configuring Personnel 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.

5.3.2.1 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 **Personal 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 **Additional Info** section of a person's information.

Figure 5-6 More information

The screenshot shows the 'Edit Person' form with the following fields:

- Phone No.
- Remarks
- Additional Info
- Nickname
- Address
- ID Type (Others)
- ID No.
- Birthday (1995 - 04 - 08)
- Region (Unknown)
- Company
- Department
- Position
- More Info 1 (highlighted with a red box)



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.

5.3.2.2 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 **Personal 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 Image** > **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 Image** > **Snapshot** to take an image.

Figure 5-7 Basic information


The screenshot shows the 'Basic Info' form with the following fields:

- ID: 00006304
- Name: John Wick
- Gender: Male
- Person Group: All Persons and Vehicles
- Email: John_Wick@gmail.com
- Profile picture: A photo of John Wick.

- 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 "5.3.2.6 Importing Images of Persons".















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 5 person groups. Click  to set one as the main person group.
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.

Table 5-9 Parameter description



Parameter	Description
Card	<ol style="list-style-type: none"> 1. Click Settings , 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.  <p>One person can have up to 5 cards. A card number is 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.</p> <ol style="list-style-type: none"> 3. Click . 4. (Optional) Click  to add more cards. You can add up to 5 cards for each person. <p>After adding a card, you can:</p> <ul style="list-style-type: none"> ◇ : 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	<ol style="list-style-type: none"> 1. Click Settings , select a fingerprint scanner, and then click OK. 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. <p>After adding a fingerprint, you can:</p> <ul style="list-style-type: none"> ◇ : 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	<p>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.</p> <p>Click , enter a password, and then click .</p> <p>After adding a password, you can:</p> <ul style="list-style-type: none"> ◇ : Change the password. ◇ : Delete the password, and then it has no access permissions.

- If the person has one or more vehicles, click **Vehicle Info** to add their information to the platform, so that you can grant access permissions to this person's vehicles later.
 - ◇ 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 5-10 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	<p>When several people live in the same room, you can set one of them as the homeowner.</p> <p>Only the homeowner can register an account on DSS Agile VDP.</p>
APP User	<p>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.</p> <p>After the person is added, the platform will send the username and password to the email address.</p> <p></p> <p>If the person does not receive the email, you can click Send Email to send a new email.</p> <p></p> <p>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.</p>

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.

- **VIP:** When the person uses an access point, a VIP event is reported.
 - **Visitor:** When the person uses an access point, a visitor event is reported. Also, the person has limited access of 200 times. After the 200 times are used up, the person cannot use an access point.
 - **Patrol:** When the person uses an access point, a patrol event is reported.
 - **Blocklist:** The person cannot use an access point. Also, a blocklist event is reported.
 - **Extend time:** When the person uses an access point, the door will stay unlocked for additional 5 seconds, and an extend time event is reported.
2. Configure the access rule validity period. The access rules are only effective within this period.
 3. Select **Add > 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 5-8 Available access rules

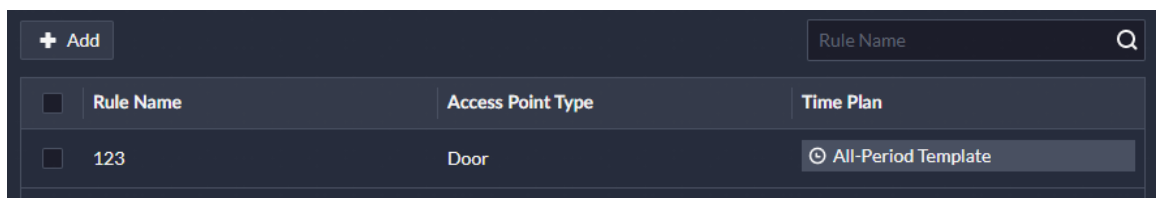

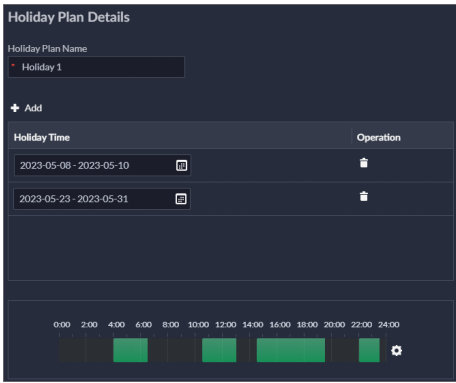






Table 5-11 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only Door is available
Time Template	Select a time template to define when the rule will be effective. For how to create a new template, see "4.2.6 Adding Time Template".

Parameter	Description
<p>Holiday Plan</p>	<p>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:</p> <ol style="list-style-type: none"> Select Add Holiday Plan in the drop-down list. Enter a name for the holiday plan. Click Add to add a holiday. <p>You can add up to 16 holidays.</p> <ol style="list-style-type: none"> Configure the effective periods for each day in the holiday. <p>You can drag on the timeline below, or click  to configure the time more accurately. You can add up to 4 periods.</p> <ol style="list-style-type: none"> Click OK. 
<p>Select by Zone</p>	<p>Click  to enable this function and select one or more zones. This person will have access permissions to all the access points in these zones.</p> <p></p> <p>For how to configure a zone, see "5.5.2 Configuring Zone".</p>
<p>Select by Access Point</p>	<p>Click  to enable this function and select one or more access points. This person will have access permissions to all these access points.</p>

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

- Click  next to **Face Arming** to enable the function.
- Select 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 "5.4.1.1 Creating Face Arming Group".

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

- Click  next to **Parking Lot** to enable the function.
- If this person has one or more parking spaces, click  to enable **Available Parking Spaces** the function, and then configure the number of the parking spaces.

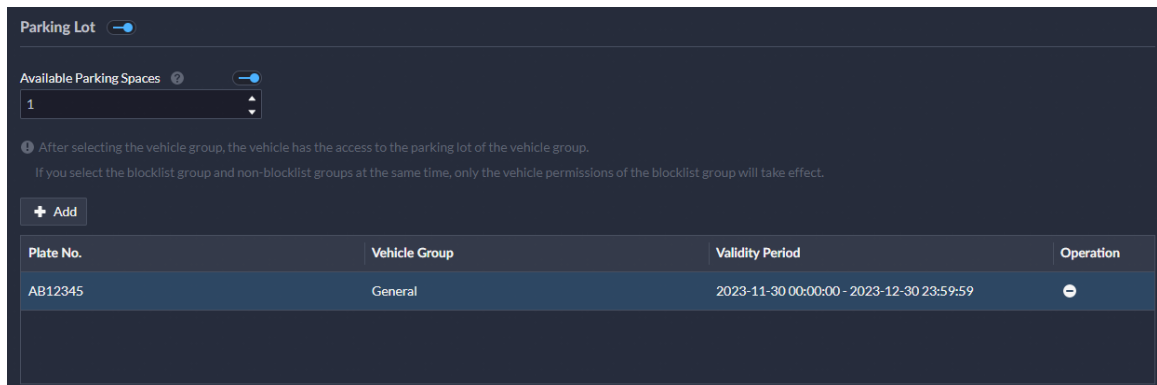
For example, if this person has 2 vehicles when there is only 1 parking space, vehicle B will not be able to enter if vehicle A is already in the parking lot.

- Click **Add** to select the vehicle of this person, and then select which one or more vehicle group it belongs to, and for how long it has access permission to the parking lot.



If there are no available vehicle groups, select **Add Group** in the drop-down list, and then to add one. For details, see "5.8.3 Managing Vehicle Group".

Figure 5-9 Parking lot vehicle group

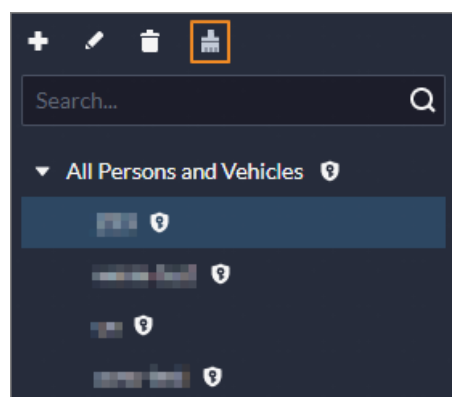


Step 8 Click **OK**.

Related Operations

- Click to edit the basic information of a person.
- To delete a person:
 - Click to delete a person and associated permissions.
 - Select multiple people, and then click **Delete** 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 5-10 Delete all persons in a group



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

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

5.3.2.3 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 larger than 1 GB.
- If a person belongs in a first-person unlock rule, set the access type of the person to **General**.

Procedure



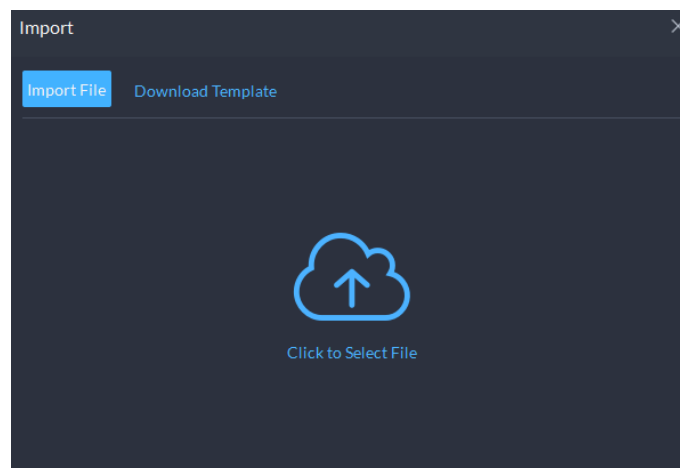
- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Personal and Vehicle Info**.
- Step 2 Click .
- Step 3 Select **Import** > **Import from File**.

Figure 5-11 Import personnel information



- Step 4 Import the personnel information file.



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

- Step 5 Click **OK**.

The following cases might occur during an import:

- 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 personnel information.

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



- Download template.

To add personnel information in batches, you can download the template, fill in the information, and then import it.

5.3.2.4 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 **Personal 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 Group** to display all the people in this group and all its sub groups.
- Step 3** Select multiple people, and then click **Move To**.
- Step 4** Select a target group, and then click **OK**.
- Step 5** Click **OK** again.

5.3.2.5 Extracting Personnel Information

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

Procedure



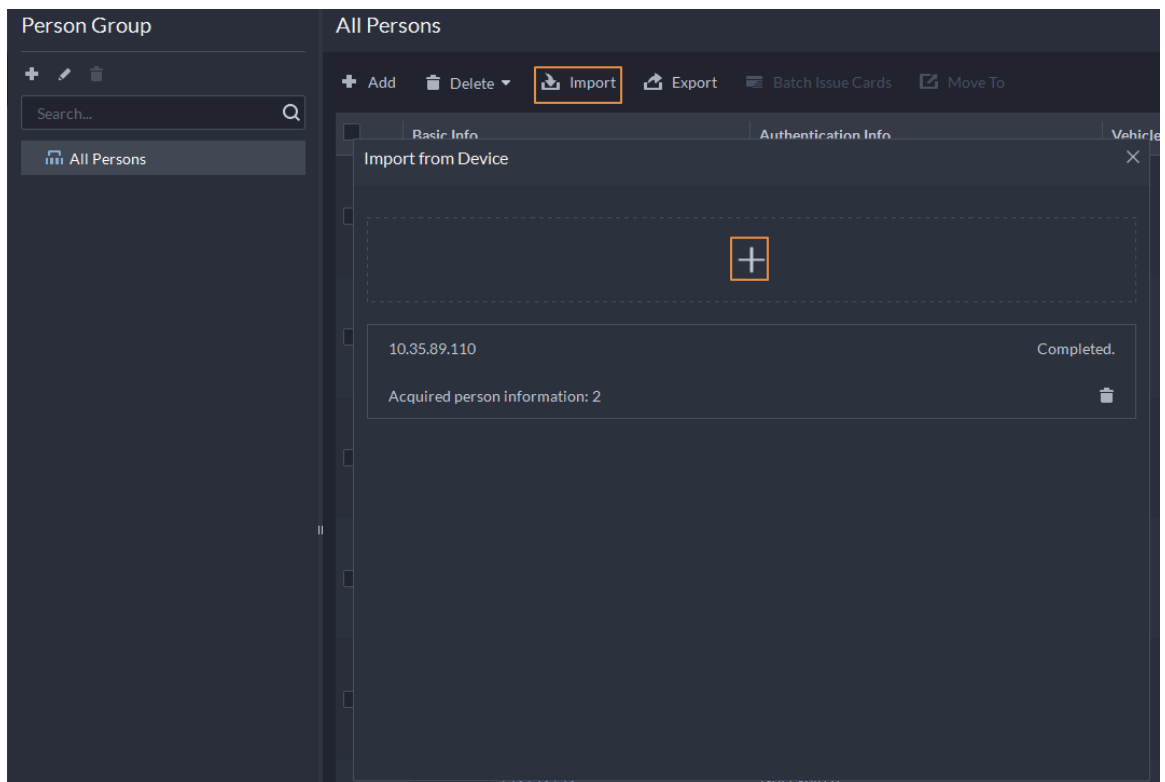
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Personal and Vehicle Info**.
- Step 2** Click .
- Step 3** Click **Import**, and then select **Import from Device**.

Figure 5-12 Import from device




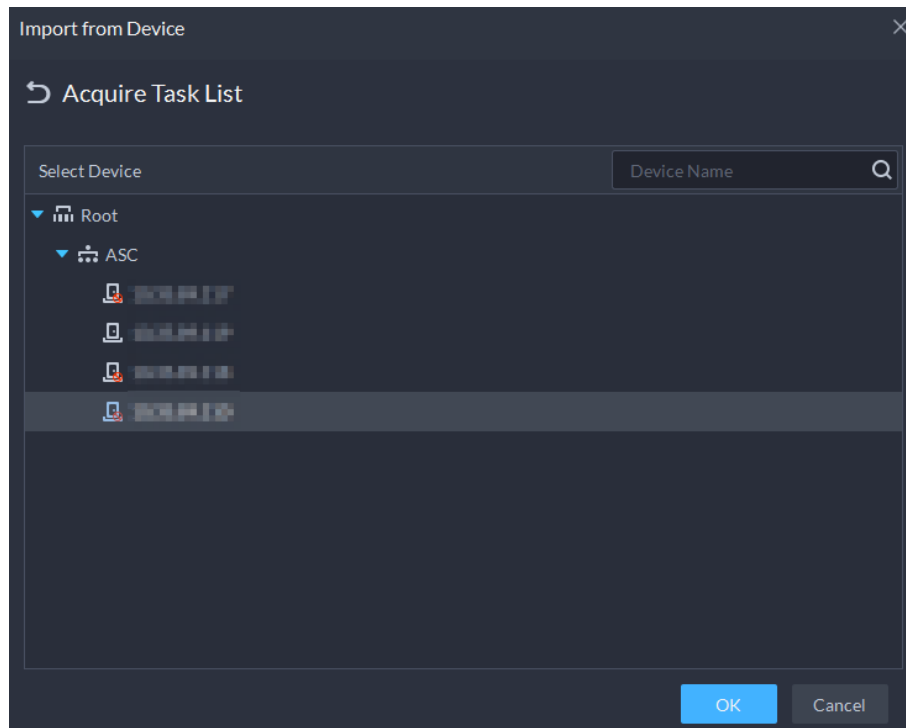
- Step 4** Click , select a channel from an access control device or door station, and then click **OK**.

Figure 5-13 Extract task list



- Step 5** Double-click a result to view the detailed information.
- Step 6** Synchronize personnel information to the platform, or export information.

Figure 5-14 Personnel extraction results

ID	Name	Access Type	Authorization Information
28848	fww4	General	X 1 X 5 X 0
13792	fww3	General	X 1 X 5 X 0
41585080	fww1	General	X 1 X 5 X 0
26568	fww2	General	X 1 X 5 X 0
26527	fww5	General	X 1 X 5 X 0
1003	[Image]	General	X 1 X 2 X 0
1001	[Image]	General	X 1 X 2 X 2
1	szt111	General	X 0 X 1 X 0
2	szt2	General	X 0 X 1 X 0

- To add all the personnel 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 you want, and then click **Export**.

5.3.2.6 Importing Images of Persons

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 face, and keep hair away from blocking it. The bear 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 **Personal and Vehicle Info > Person List > Persons**.
- Step 2** Click **Import**, and then select **Import Person Images**.
- 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.

5.3.2.7 Issuing Cards in Batches

Procedure



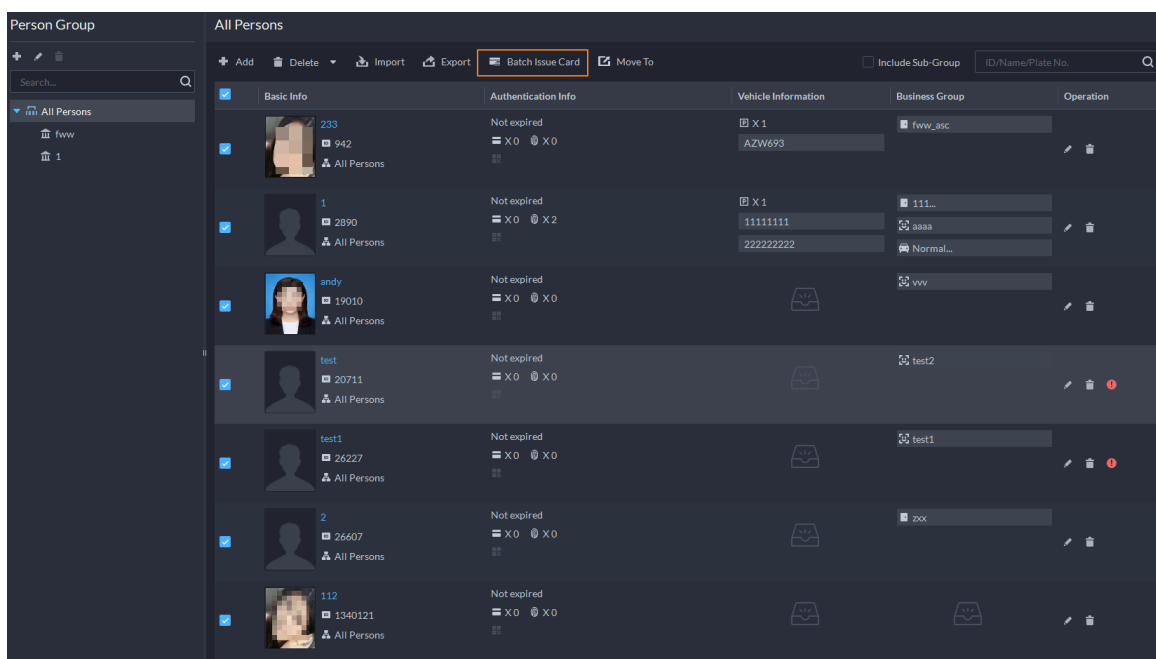
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Personal and Vehicle Info**.
- Step 2** Click .
- Step 3** Select the people to issue card to, and then click **Batch Issue Card**.

Figure 5-15 Issue card in batches



- Step 4** Set term of validity.

Step 5 Issue cards to personnel.

Step 6 Support issuing cards by entering card number or by using a card reader.

- By entering card number

Figure 5-16 Enter card number

Batch Issue Card

Effective Period:
2021/04/13 00:00:00-2031/04/13 23:59:59

Issue Card

ID	Name	Card No.	Operation
942	233		
2890	1		
19010	andy		
20711	test		
26227	test1		
26607	2		
1340121	112		
6754227	z1		
10020001	ZhangSan1	10020001	
10020002	ZhangSan2	10020002	
10020003	ZhangSan3	10020003	
10020004	ZhangSan4	10020004	
10020005	ZhangSan5	10020005	
10020006	ZhangSan6	10020006	
10020007	ZhangSan7	10020007	
10020008	ZhangSan8	10020008	

Save Cancel

1. Double-click the **Card No.** input boxes to enter card numbers one by one.

2. Click **OK**.

- By using a card reader


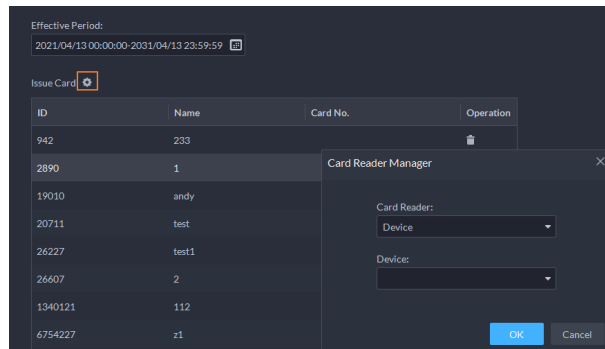
1. Click .
2. Select a card reader or device, and then click **OK**.

Figure 5-17 Reader manager




3. Select people one by one and swipe cards respectively until everyone has a card number.
4. Click **OK**.

5.3.2.8 Viewing Certain People and Information

View certain people and their information by searching for keywords or filtering the type of information to be displayed, such as ID, name, license plate, and access permission status.

Search for Certain 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 you select.

Filter person information


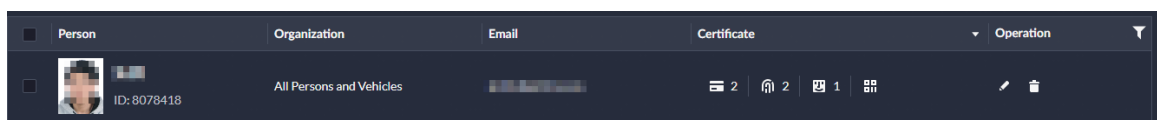
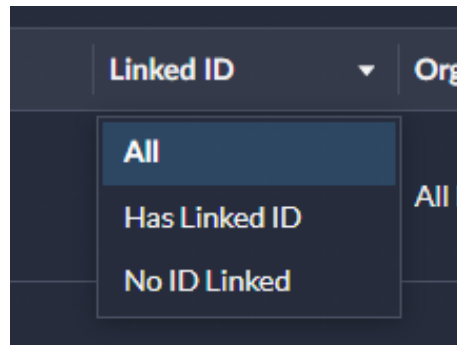
Click  on the upper-right corner to select which information to be displayed. For example, when **Email** is selected, the email addresses of the people in the list will be displayed.

Figure 5-18 Display email addresses



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




Figure 5-19 Filter by linked ID



5.3.2.9 Editing Person Information

Modify personnel information including basic information, authentication details, and authorization. Person ID cannot be modified.


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 .
- Step 3** Click  to edit information. For details, see "5.3.2.2 Adding a Person".

5.3.2.10 Configuring Access Rule

An access rule defines the permission and effective time of that permission to 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


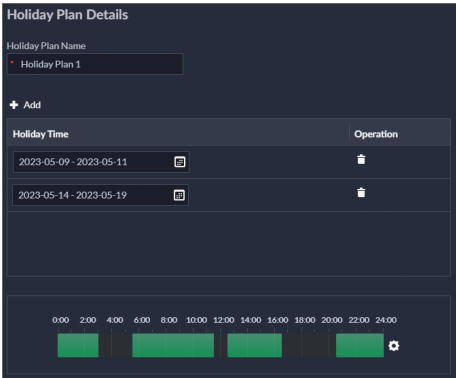
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Personal and Vehicle Info > Person List**.
- Step 2** Click a group, and then click **Access Rule**.
- Step 3** Click **Add**. This page displays rules that have been added. You can select 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 "5.5.3 Configuring Access Rule".

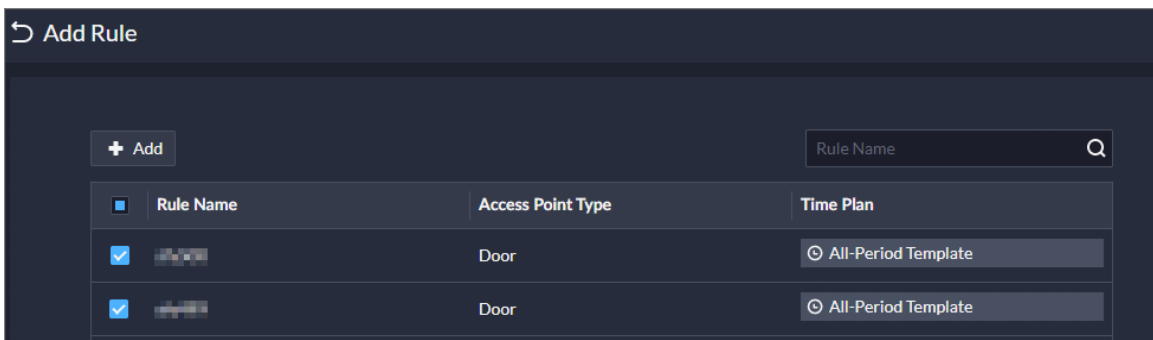
Table 5-12 Parameter description

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.

Parameter	Description
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.6 Adding Time Template".
Holiday Plan	<p>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:</p> <ol style="list-style-type: none"> 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 5-20 Select access rules



5.3.3 Vehicle Management

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

Procedure




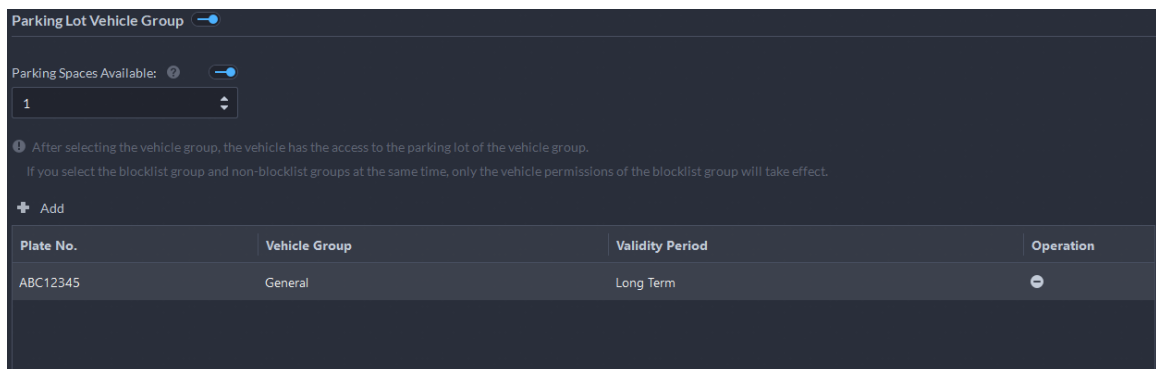
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Personal and Vehicle Info**.
- Step 2** Click .
- Step 3** Add vehicles.
- Add vehicles one by one
 1. Click **Add**.
 2. In the **Owner Info** section, click **Select from Person List** to select the owner of the vehicle.
 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. Click  to enable **Parking Lot Vehicle Group**, and then you can set the available parking spots for the selected person, and grant access permissions by adding vehicles into entrance and exit vehicle groups.

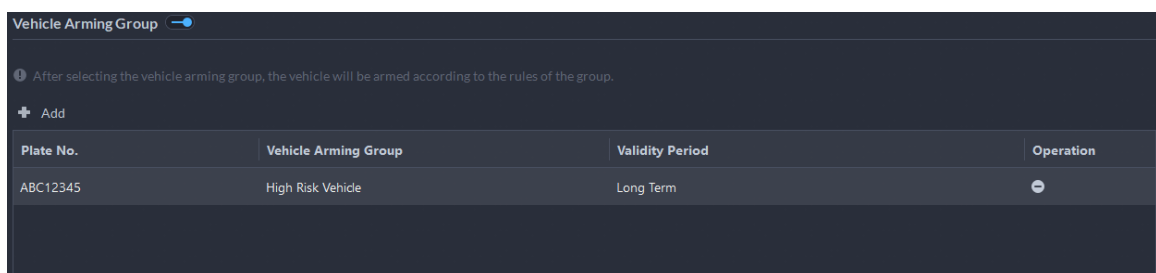
Figure 5-21 Parking lot vehicle group



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

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

Figure 5-22 Vehicle arming group





For arming group details, see "5.4.2.1 Creating Vehicle Arming Group".

6. Click **OK**.

- Add vehicles in batches

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





The platform supports downloading files that failed to import for you to check and fix.

Step 4 (Optional) Export vehicle information to local storage as needed.

Figure 5-23 Export vehicle information

- Click **Export** and then enter required information, such as passwords for login and encryption, to export all the items.
- Select vehicles, and then click **Export** to export only the selected information.

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.

5.4 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.

5.4.1 Face Arming List

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

5.4.1.1 Creating Face Arming Group

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

Prerequisites

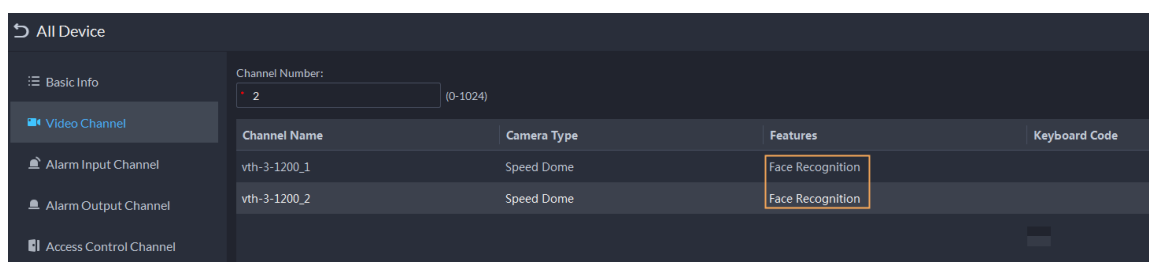
- Make sure that the devices for face recognition have been successfully configured onto the Platform.
- Make sure that the basic configuration of the Platform has completed. For details, see "4 Basic Configurations". During the configuration, you need to pay attention to following parts.
 - ◇ When adding devices on the **Device** page, set the **Device Category** to **Encoder**.

Figure 5-24 Device category

The screenshot shows the 'Add Device' configuration interface. The 'Device Category' dropdown menu is highlighted with a red box and contains the value 'Encoder'. Other fields include 'Add Mode' (IP Address), 'Access Protocol' (Dahua), 'IP Address', 'Device Port' (3777), 'Username' (admin), 'Password', 'Organization' (Root), and 'Server'.

- ◇ When adding devices like NVR or IVSS which support face recognition, set the device feature to **Face Recognition**. For details, see "4.2.2.5 Editing Devices".

Figure 5-25 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 5-13 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**.

5.4.1.2 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.

- 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 "5.3.2 Configuring Personnel 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**.

5.4.1.3 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**.


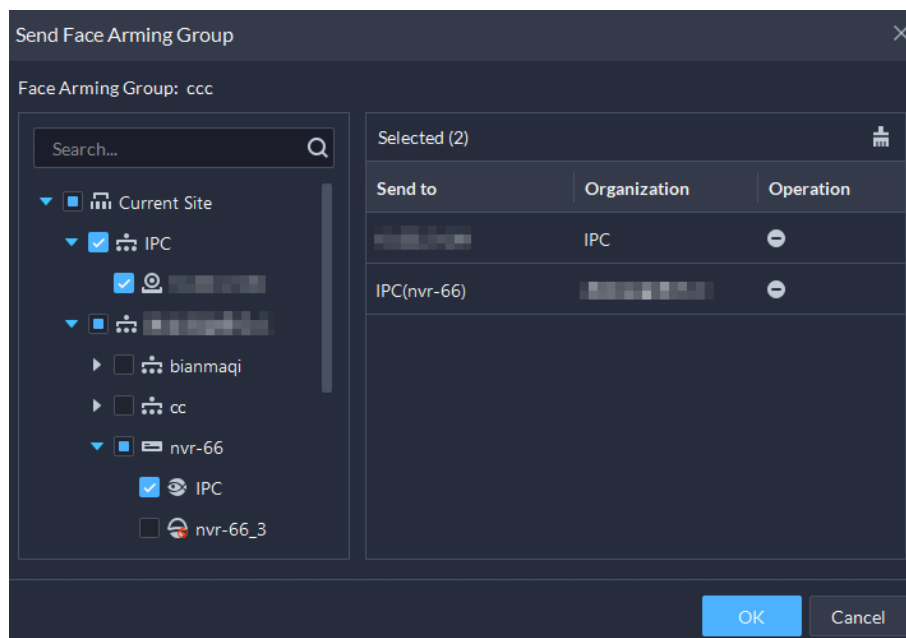
The platform will send the information of the face arming group to the devices and channels you selected, and display the progress. If exceptions occur, you can click  to see the reason.

Figure 5-26 Send face arming group



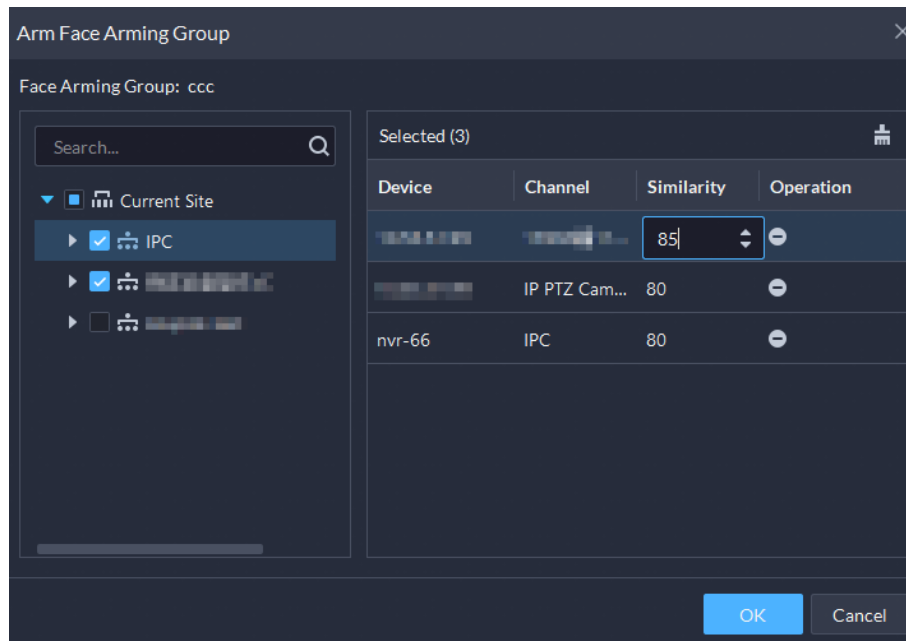
Step 4 After the face arming group is successfully sent, click **Next Step**.

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.

Figure 5-27 Arm face arming group



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 **Send Again** to arm the face arming group again.

5.4.2 Vehicle Watch List

Create a vehicle comparison group and add vehicles to it. After a vehicle comparison group is sent to cameras for recognition, alarms will be triggered if the vehicles in the group are captured and recognized.

5.4.2.1 Creating 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 16 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 5-14 Parameter description

Parameter	Description
Vehicle 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.


Parameter	Description
Roles Allowed Access	<p>Only the roles and their users can view this group.</p>  <p>Click  to see the users assigned with the roles.</p>


Step 3 Click **Add**.

5.4.2.2 Adding Vehicles

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

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  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 "5.3.2 Configuring Personnel 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**.

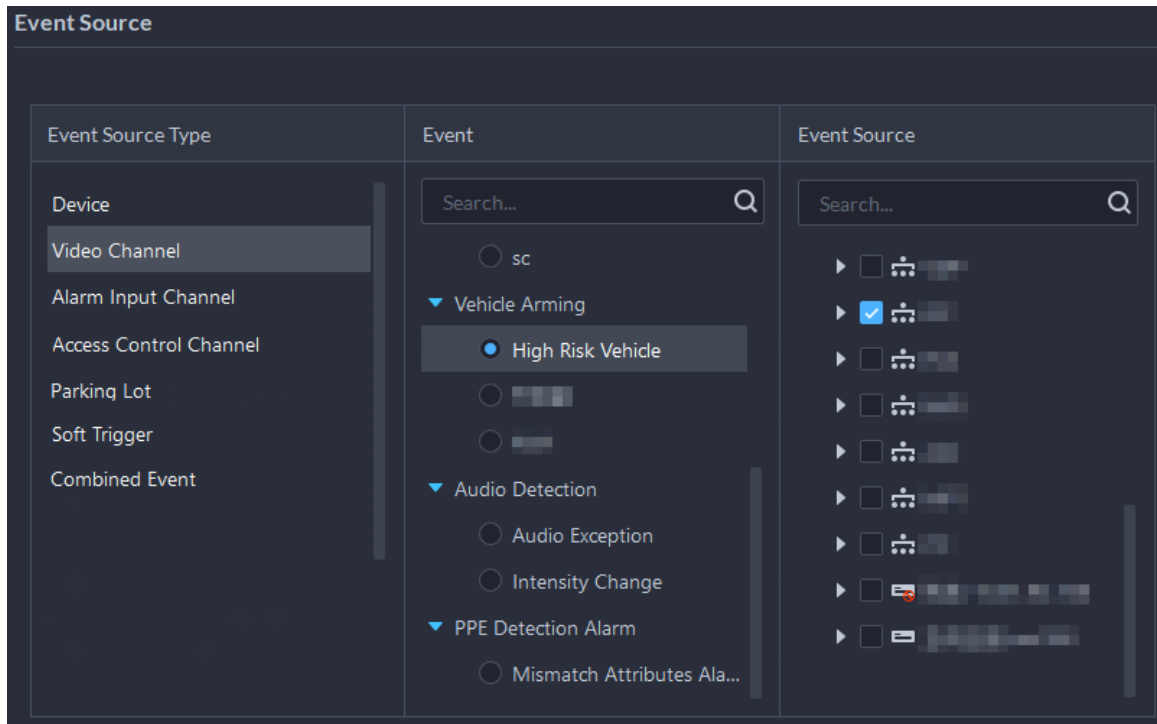
5.4.2.3 Arming Vehicles

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 "5.1 Configuring Events".

Figure 5-28 Arm vehicle event



5.5 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.

5.5.1 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 "4 Basic Configurations" for details.
 - ◇ When adding access control devices, select **Access Control** as the 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 "4.2.3 Binding Resources".
 - ◇ Add persons to the platform For details, see "5.3 Personnel and Vehicle Management".

5.5.2 Configuring Zone

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

5.5.2.1 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 5-15 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.
Roles Allowed Access	Only the selected roles and their users can access this zone.  Click  to see the users assigned with the roles.

5.5.2.2 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 5-29 Add zones in batches

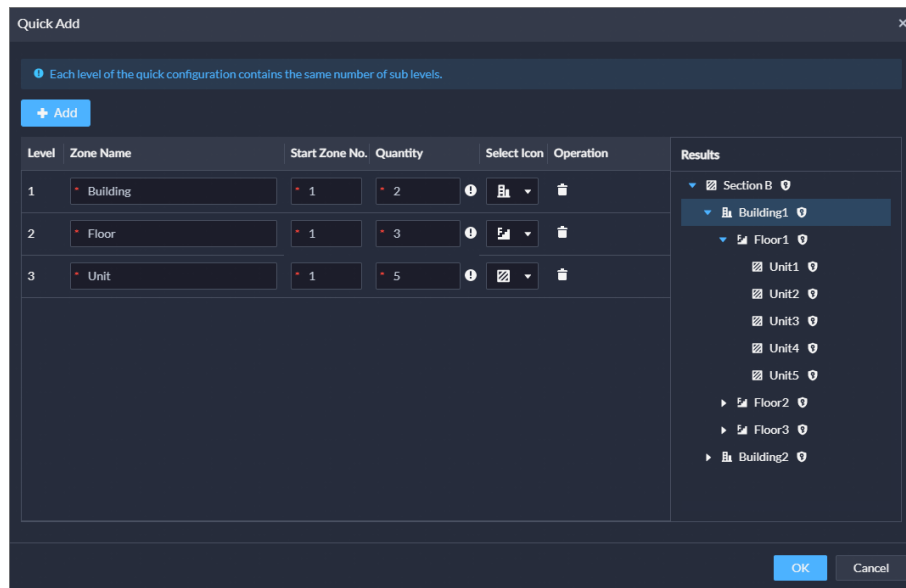


Table 5-16 Parameter description

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 Name	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 × 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 = 1×2×3 = 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.

5.5.2.3 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.

5.5.2.4 Moving Access Point

The access points in a zone can be moved to other zones. After you add access control devices and video intercom devices with access control functions, access points of door channels will be generated and added to the root 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.

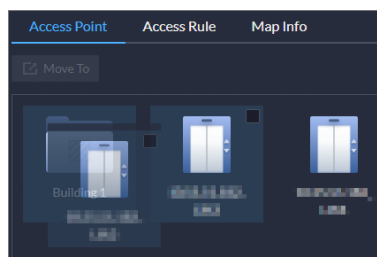
After moving the access points, access rules of the current zones will not be applied to them, and their information on the map will also be deleted. The access rules of the target zone will apply to them.



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

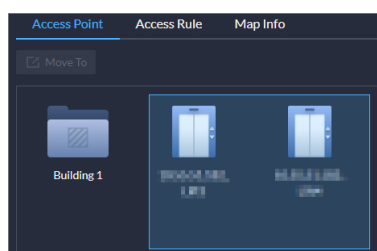
- Move an access point.
 - ◇ Drag an access point to a sub zone.

Figure 5-30 Move an access point



- ◇ Right-click an access point, select **Move To**, and then select a zone.
- Move multiple access points.
 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.

Figure 5-31 Drag 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.




You can also drag to select access points in the search result.

5.5.2.5 Configuring Access Point

5.5.2.5.1 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 that can be changed.
 - **Access Point Type** : Displays the type of the access point.
 - **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 "4.2.3 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 add or delete the rules, but the rules from the zone cannot be deleted.


5.5.2.5.2 Setting Boundary

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

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 Right-click an access point and select **Set as Boundary**.




 will be displayed on the lower-right corner of the icon of the access point.

5.5.2.6 Configuring Access Rule for a Zone

An access rule defines the permission and effective time of that permission to 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**.


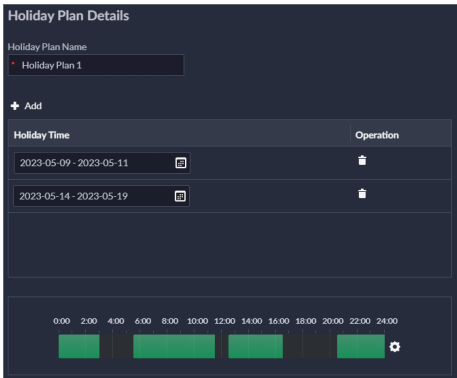

Step 3 Click **Quote**. This page displays rules that have been added. You can select and use any one of them directly.


Step 4 Click **Add**, and then configure the parameters of the new access rule.



When configuring an access rule for a zone, you can only configure general verification rules. If you want to configure other types of rules, see "5.5.3 Configuring Access Rule".

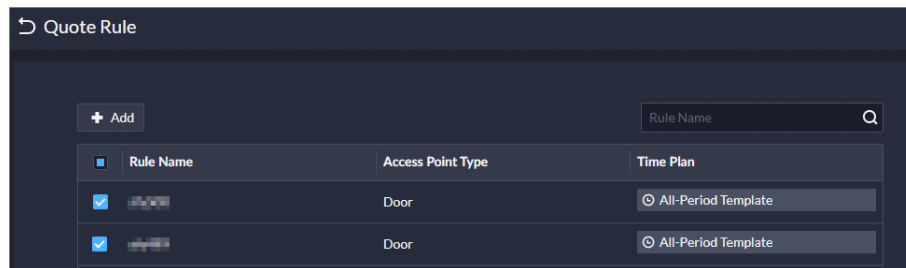
Table 5-17 Parameter description

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 "4.2.6 Adding Time Template".
Holiday Plan	<p>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:</p> <ol style="list-style-type: none"> 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. <ul style="list-style-type: none"> You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. <p>You can drag on the timeline, or click  to configure the periods more precisely. You can configure up to 4 periods.</p> 5. Click OK. 
Select by Person Group	<p>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.</p>  <p>Select Link Sub Node, and then you can select a zone and all its sub zones at the same time.</p>

Parameter	Description
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.

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

Figure 5-32 Select access rules



5.5.2.7 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.

5.5.2.7.1 Adding 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 "5.2.2 Adding Map".

Step 4 Click **OK**.

5.5.2.7.2 Marking Access Point and Sub Zone

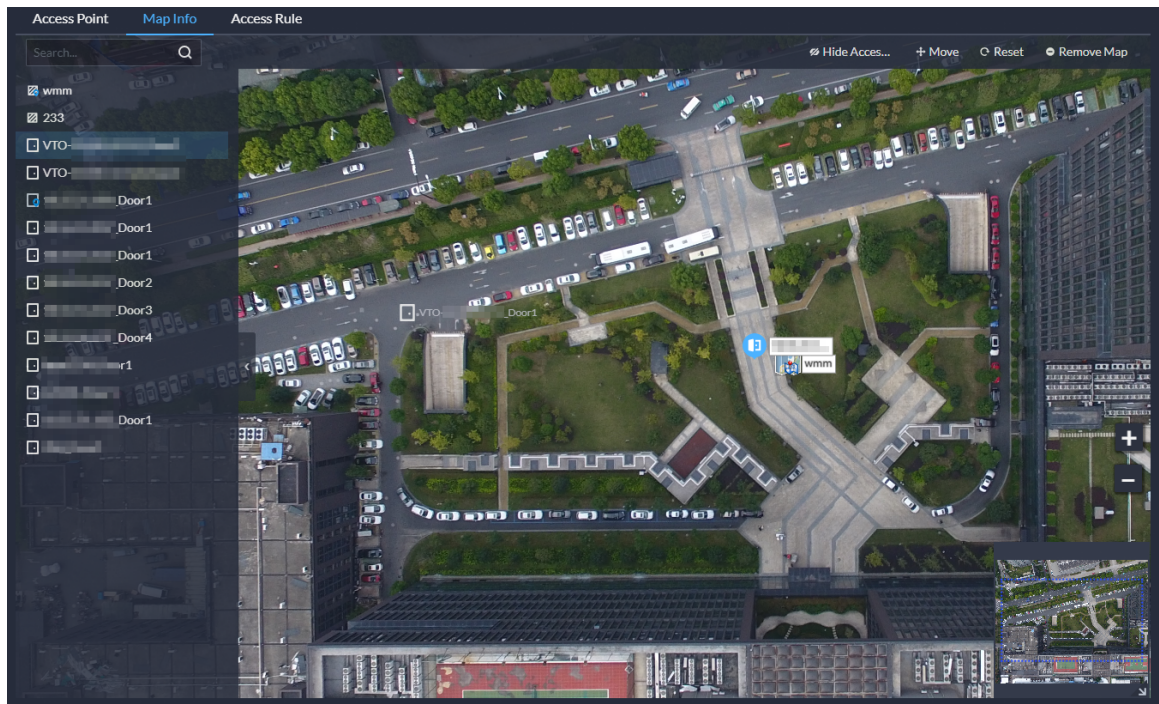
Procedure

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.

Figure 5-33 Drag and mark



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 "5.2 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.



5.5.3 Configuring Access Rule

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

5.5.3.1 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.

5.5.3.2 Configuring General Verification

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

Procedure



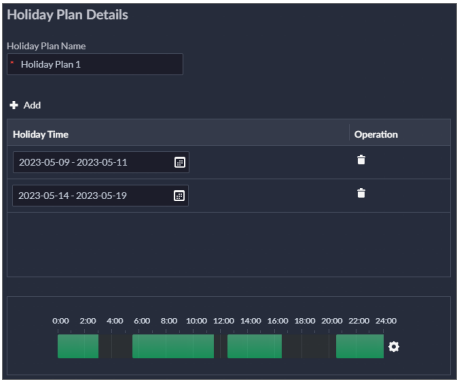




- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.
- Step 2 Click **Add**.
- Step 3 Configure the parameters, and then click **OK**.

Table 5-18 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Select Door .
Rule Type	Select General Verification .
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.6 Adding Time Template".

Parameter	Description
Holiday Plan	<p>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:</p> <ol style="list-style-type: none"> 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. <p>You can add up to 16 holidays.</p> <ol style="list-style-type: none"> 4. Configure the effective periods for each day in the holiday. <p>You can drag on the timeline, or click  to configure the periods more precisely. You can configure up to 4 periods.</p> <ol style="list-style-type: none"> 5. Click OK. 
Select by Zone	<p>Select one or more zones, and then this rule will be applied to all access points in the zones.</p>  <p>Select Link Sub Node, and then you can select a zone and all its sub zones at the same time.</p>
Select by Access Point	<p>Select one or more access points.</p>  <p>Select Include Sub Zone to display all the access points in the selected zone and its sub zones.</p>
Select by Person Group	<p>Select one or more person groups, and then all the persons in the groups will have permissions to access the selected access points.</p>  <p>Select Link Sub Node, and then you can select a zone and all its sub zones at the same time.</p>
Select by Person	<p>Select one or more persons, and then they will have permissions to access the selected access points.</p>  <p>Select Include Sub Groups to display all the persons in the selected group and its sub groups.</p>

5.5.3.3 Configuring Normally Open

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

Procedure



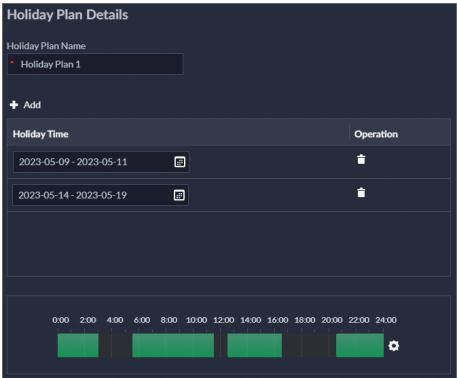

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.
- Step 2** Click **Add**.
- Step 3** Configure the parameters, and then click **OK**.

Table 5-19 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only Door is available.
Rule Type	Select Normally Open .
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.6 Adding Time Template".
Holiday Plan	<p>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:</p> <ol style="list-style-type: none"> 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. <p>You can add up to 16 holidays.</p> <ol style="list-style-type: none"> 4. Configure the effective periods for each day in the holiday. <p>You can drag on the timeline, or click  to configure the periods more precisely. You can configure up to 4 periods.</p> <ol style="list-style-type: none"> 5. Click OK. 
Access Point	<p>Select one or more doors.</p>  <p>Select Include Sub Zone to display all the access points in the selected zone and its sub zones.</p>

5.5.3.4 Configuring Normally Closed

All people are not allowed to pass access points.

Procedure



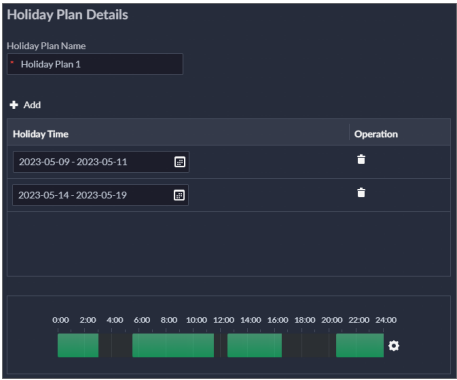

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.
- Step 2** Click **Add**.
- Step 3** Configure the parameters, and then click **OK**.

Table 5-20 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only Door is available.
Rule Type	Select Normally Closed .
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.6 Adding Time Template".
Holiday Plan	<p>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:</p> <ol style="list-style-type: none"> 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. <p>You can add up to 16 holidays.</p> <ol style="list-style-type: none"> 4. Configure the effective periods for each day in the holiday. <p>You can drag on the timeline, or click  to configure the periods more precisely. You can configure up to 4 periods.</p> <ol style="list-style-type: none"> 5. Click OK. 
Access Point	<p>Select one or more doors. </p> <p>Select Include Sub Zone to display all the access points in the selected zone and its sub zones.</p>

5.5.3.5 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 "5.5.3.2 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 5-21 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	<ul style="list-style-type: none"> ● Normal : Other persons must verify their identifications to pass. ● Normally 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 "4.2.6 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 "5.3.2.2 Adding a Person". <ul style="list-style-type: none"> ● 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, People whose access types are Patrol can still unlock it.

5.5.3.6 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 "5.5.3.2 Configuring General Verification".

Procedure



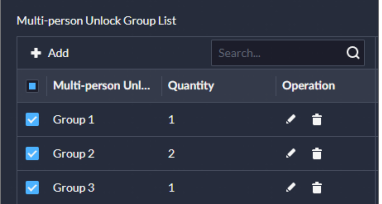
- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.
- Step 2 Click **Add**, and then configure the parameters.

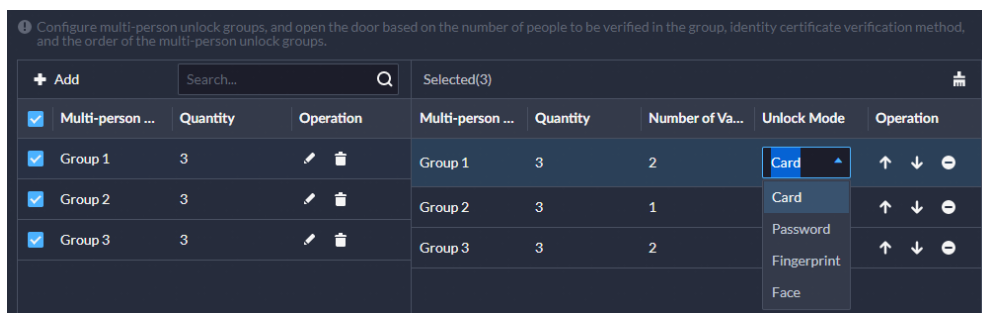
Table 5-22 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
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.

Parameter	Description
Person	<p>Configure up to 4 unlock groups. Persons must verify their identifications in the group order to unlock doors.</p> <ol style="list-style-type: none"> 1. Click Add. 2. Enter a name for the group. 3. 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. <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <ul style="list-style-type: none"> ● 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 "5.3.2.2 Adding a Person". </div> 4. Click OK. 5. (Optional) Repeat the steps below to add more groups. 6. Select the groups you added, and then click OK. <div style="text-align: center; margin: 10px 0;">  </div> <ol style="list-style-type: none"> 7. 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 5-34 Configure unlock methods



Step 4 Click **OK**.

5.5.3.7 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. They cannot enter building D directly.

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 5-23 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	Only local anti-passback is supported. You can select the door channels of an access control device.
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 5 minutes and 24 hours.
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.6 Adding Time Template".
Anti-passback Group	Add doors to different groups, and then people must pass in the group order to access the doors in the last group.

5.5.3.8 Configuring Multi-door Interlock

When a door in any group is unlocked, people cannot pass through any other door.

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 5-24 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 .

Parameter	Description
Interlock Type	Only local interlock is supported. You can configure the door access points of 1 device. 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.
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.

5.5.3.9 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**.

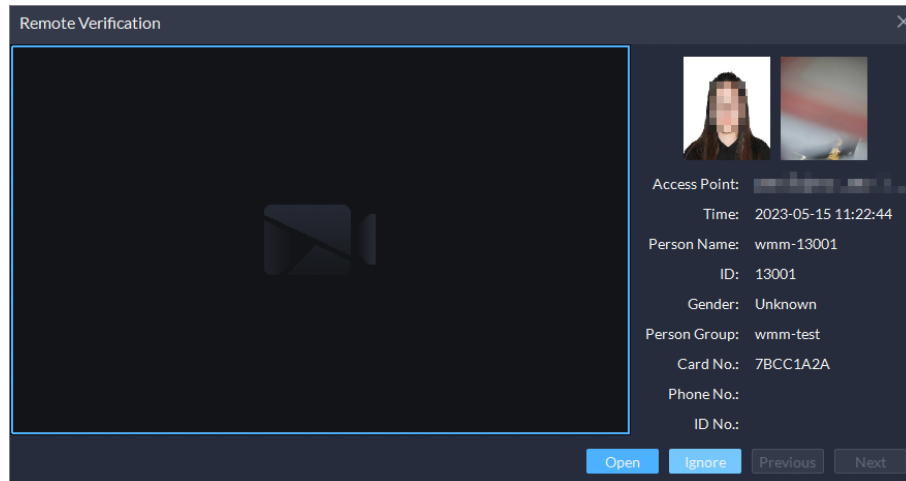
Table 5-25 Parameter description

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 "4.2.6 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.

Figure 5-35 Remote verification



5.5.3.10 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.


5.5.3.11 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 "4.4 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 **Verification**.

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: The person will be added to the device.
- A person is not on the platform: The person will be deleted from the device.
- The information of a person on the device is not the same as the platform: Update the information on the device.

5.5.4 Configuring Public Passwords

For a door, any person with the public password can unlock it. You can configure up to 1,500 passwords.


Procedure

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

Step 2 Click **Add**.

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**.

5.5.5 Configuring Time Templates

Configure time templates for different access control strategies. For example, employees can only gain access to their offices during work time.

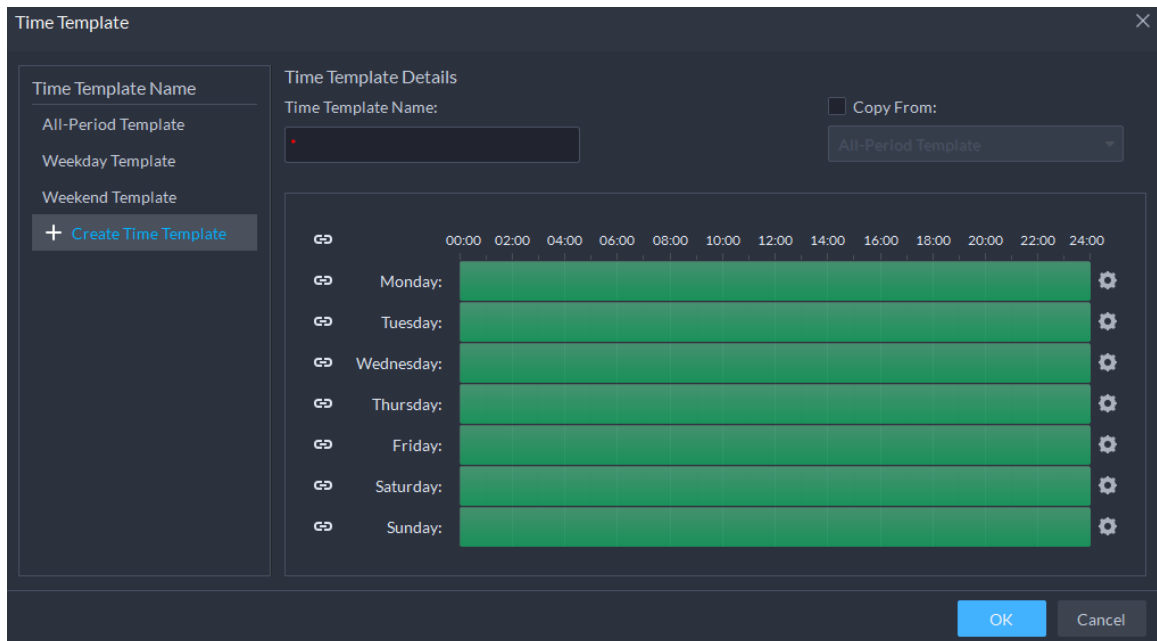
Procedure

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

Step 2 Click .


Step 3 Click **Create Time Template** from the **Time Template** drop-down list when adding or editing a door group.

Figure 5-36 Time template



Step 4 Enter the template name, set time periods, and then click **OK**.

There are two ways to set time periods:

- Drag your mouse cursor on the time bars to select time sections. To remove a selected time section, click on the time bar and drag.
- Click , and then set time periods in the **Period Setup** dialog box.



- You can add up to 6 periods for each day.
- To use an existing template, select the **Copy From** check box and then select a template in the drop-down list.

5.5.6 Configuring Access Control Devices

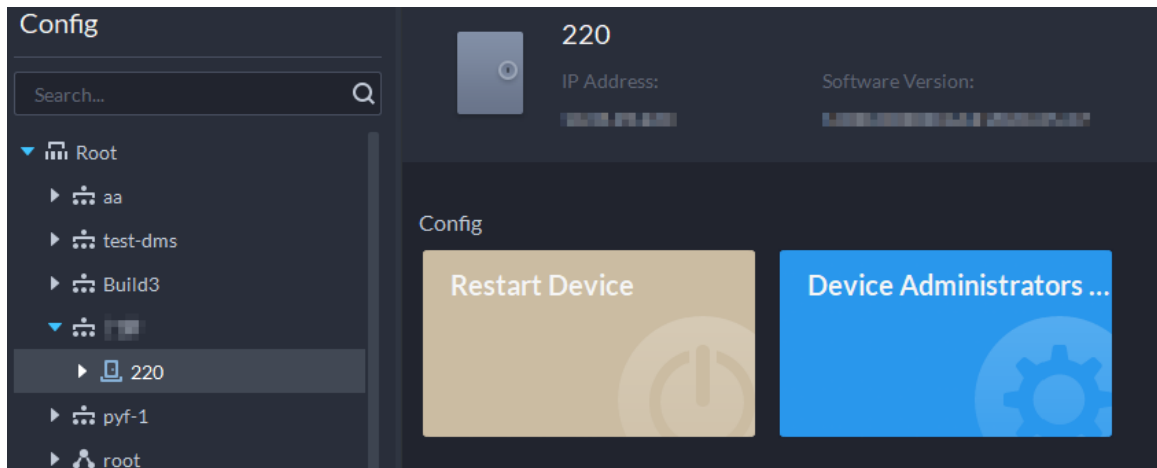
If an access control device is online, you can restart it, and synchronize its time with the platform. Also, you can set a person as the administrator, and then the person can log in to the configuration page of the access control device to configure parameters.

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 an access control device from the device tree.

Figure 5-37 Select an access control device



Step 3 Configure the access control device.

- Click **Restart Device** to restart the device.
- Click **Device Administrators Config** 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 web page of the device.

5.5.7 Configuring Door Information

You can configure door status, modes, alarms 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** Select a door channel in the device tree, and then click **Door Config** on the right.
- Step 3** Configure door information, and then click **OK**.

Figure 5-38 Door configuration

Reader Direction:
In ⇌ Out

Mode:

Enable Door Sensor:

Enable Alarm:

Duress Unsuccessful Attempts Exceeding Limit

Public Password:

Unlock Duration: sec Unlock Timeout: sec

Unlock Method: Unlock by Period

Card Fingerprints Password



The page is only for reference, and might vary with different access control devices.

Table 5-26 Parameter description

Parameter	Description
Reader Direction	Indicates the in/out reader based on the wiring of ACS.
Mode	Set access control status to Normal , Normally Open , or Normally Closed .
Enable Door Sensor	You can only enable forced entry and timeout alarms when the door sensor is enabled.
Enable Alarm	<ul style="list-style-type: none"> • Duress: Entry with the duress card, duress password, or duress fingerprint triggers a duress alarm. • Unsuccessful Attempts Exceeding Limit: If failed to unlock the door for certain times, an alarm will be triggered. • Forced Entry: If the door is unlocked by methods you have not configured, the door contact is split and triggers an intrusion alarm. • Timeout: Unlock duration timeout triggers a timeout alarm.
Public Password	Enable this function, and then you can use a public password to unlock the door. For how to configure a public password, see "5.5.4 Configuring Public Passwords".
Unlock Duration	Sets up for how long the door will unlock. The door locks automatically after the duration.
Unlock Timeout	Unlock duration exceeding the Unlock timeout triggers a timeout alarm.
Unlock Method	<p>You can use any one of the methods, card, fingerprint, face, and password, or their combinations to unlock the door.</p> <ul style="list-style-type: none"> • Select And, and select unlock methods. You can only open the door using all the selected unlock methods. • Select Or and select unlock methods. You can open the door in one of the ways that you configured.
Unlock by Period	<p>For each day of the week, you can set up to 4 periods, and the unlock method for each period. For example, card is set for Monday 08:00-12:00, then people can only use their cards to open the door every Monday from 08:00 to 12:00.</p> <p>Use the Copy to function to quickly apply the current configurations to one or more days.</p>

5.6 Video Intercom

5.6.1 Preparations

Make sure that the following preparations have been made:


- Access control devices are correctly deployed. For details, see the corresponding user's manuals.

- Basic configurations of the platform have been finished. To configure, see "4 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**.

5.6.2 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.

5.6.2.1 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.

5.6.2.2 Adding 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 in the **App Config** section, select **Video Intercom**.
- Step 2** Click .
- Step 3** Click **Manager Group Config**.
- Step 4** Click **Add Group**.
- Step 5** Enter group name, select administrator account or VTS, and click **OK**.
The added management group is displayed in the list.





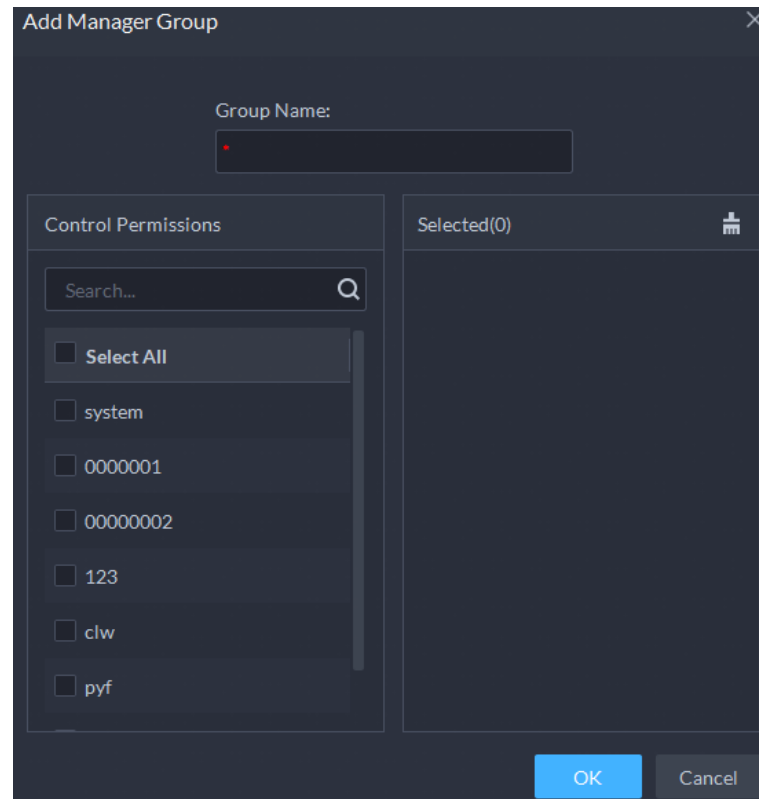
- To transfer members, click  and move the member to other groups.
- To manage group members, click  to add or delete group members.

Figure 5-39 Edit manager group



5.6.2.3 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 in the **App Config** section, select **Video Intercom**.
- Step 2** Click .
- Step 3** Click **Relation Group Config**.
- Step 4** Click **Add**.

Step 5 Enter the group name, and then select one or more call groups and manager groups.

Figure 5-40 Add a group relation



Because only up to 2 manager groups will receive a call, we recommend you select no more than 2 manager groups.

Step 6 Click or to adjust priorities of the manager groups, and then click **OK**.

The upper manager group has higher priority.

5.6.3 Configuring Building/Unit

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".

Procedure

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

Step 2 Click .

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 Click **Save**.

5.6.4 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 in the **App Config** section, select **Video Intercom**.

Step 2 Click .


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  delete one room at a time.
- Click **Delete Contacts** to delete all or selected rooms.

5.6.5 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 in the **App Config** section, select **Video Intercom**.

Step 2 Click .

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.

5.6.6 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 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 in the **App Config** section, select **Video Intercom**.

Step 2 Click .

Table 5-27 Parameter description

Operation	Description
Freeze APP user	The App user cannot log in for 600 s after being frozen. The account will be frozen when invalid password attempts exceeds 5 by an App user.
Change APP user login password	Click  and enter a new password on the Reset Password page, and then click OK .  <ul style="list-style-type: none"> 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.

5.7 Visitor Management


After visitor information is registered, the visitor can have access permission. Access permission is disabled after the visitor leaves.

5.7.1 Preparations

- Access control devices have been added into the platform.
- Basic configurations of the platform have been finished. To configure, see "4 Basic Configurations".

5.7.2 Configuring Visit Settings

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Visitor**.
- Step 2** Configure the parameters.
- **Automatic visit**

Enable the function, and then select the channels as needed. Visitors with appointment can verify their identities on the selected channels without registering.
 - **Automatic leave**
 - ◇ 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.
 - ◇ Sign out regularly: Expired visits will be automatically ended at the defined time point.
 - ◇ Daily sign-out time: For visitors who do not arrive for their appointment before the daily sign-out time, their appointment will be canceled.
 - ◇ Sign out now: For visitors who missed their appointment when you click this button, their appointment will be canceled.
 - **Default visitor permissions:** Set the default access permissions for visitors.
 - **Email template:** You can set up an email template and automatically send emails when visitors make an appointment, arrive for their appointment, and end their visit. You can customize the email subject and content with the visitor information, such as visitor's name and ID number.
 - **Visitor pass remarks:** Customize the content of remarks on a visitor pass.

Figure 5-41 Customize visitor pass remarks

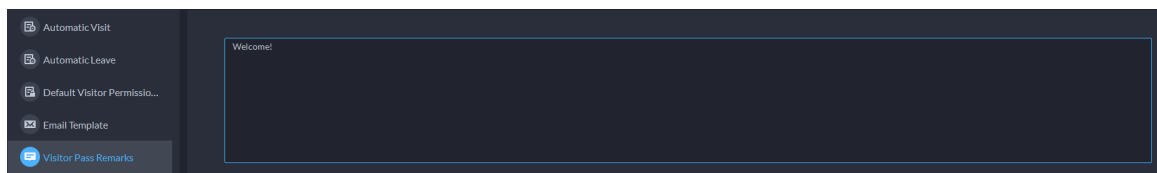
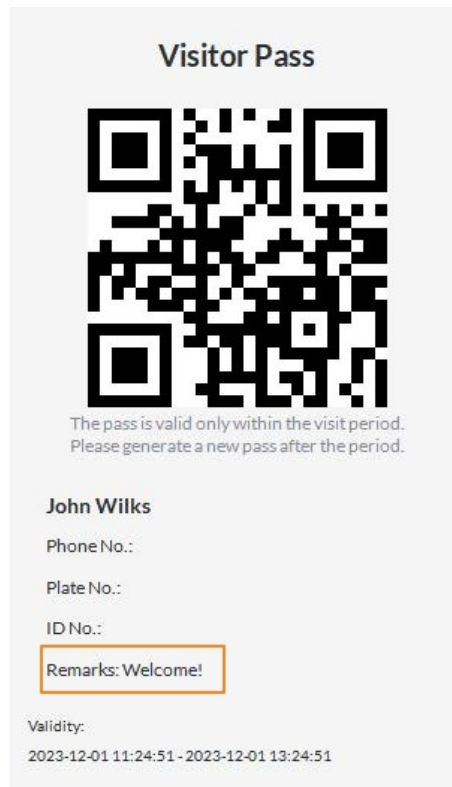


Figure 5-42 Visitor pass remarks



Step 3 Click **Save**.

5.8 Parking Lot

Control vehicle entrance and exit control with the functions such as ANPR, alarm, and search. In case the vehicle is not recognized by the ANPR camera, visitors can use VTO to call the management center, and then the management center can remotely open the barriers after verifying the identity of the visitor.

5.8.1 Preparations

Make sure that the following preparations have been made:

- Devices, such as ANPR cameras, VTOs, are added to the platform.
- Basic configurations of the platform have been finished. To configure, see "4 Basic Configurations".
 - ◇ When adding an ANPR camera, select **Access ANPR Device** as the device category.

After you have added ANPR cameras, you can bind video channels to their channels. This is useful 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 video from the bound camera when checking the alarm details. For how to bind channels, see "4.2.3 Binding Resources".

- ◇ When adding an NVR, select **Encoder** as the device category.
- ◇ Select **Entrance ANPR** from **Features** for the corresponding NVR channels.
- ◇ When adding VTO, select **Video Intercom** as the device category.

Also, you need to add the information of people and assign them permissions so that they can use the VTO normally. For details, see "5.3 Personnel and Vehicle Management".



Make sure that the configuration of building and unit on the DSS client is 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 "5.6.3 Configuring Building/Unit".


- ◇ 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 "4.4 Configuring Storage".

5.8.2 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 verifying identities.

5.8.2.1 Basic Information

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 Click the root node, and then click **Add**.




Up to 8 parking lots can be added.

Step 3 Configure the basic information of the parking lot, and then click **Next Step**.

Table 5-28 Parameter description



Parameter	Description
Parking Lot Name	To differentiate from other parking lots.
Enable Parking Space Counting	Configure the total parking spaces and available ones. <ul style="list-style-type: none"> ● Total Parking Spaces: The total number of parking spaces in the parking lot. ● Available Parking Spaces: The number of parking spaces in the parking lot that are not in use.

Parameter	Description
Fuzzy Match of Entrance & Exit Plate No. Snapshot	<ul style="list-style-type: none"> ● First Character Rule <ul style="list-style-type: none"> ◇ 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 <ul style="list-style-type: none"> ◇ 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. <p></p> <p>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.</p>
Auto overwrite when captured vehicle has not existed	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.

Step 4 Configure the entrance and exit points, and then click **Next Step**.



The platform supports up to 16 entrances and exits from all parking lots.

1. Click  or **Add Entrance and Exit Point**.
2. Enter a name, and then click **OK**.
3. If there is an entrance point, click  next to **Entrance**.
4. Enter a name for the point, select a capture mode, and then add a camera, video intercom device (optional), or information display (optional).

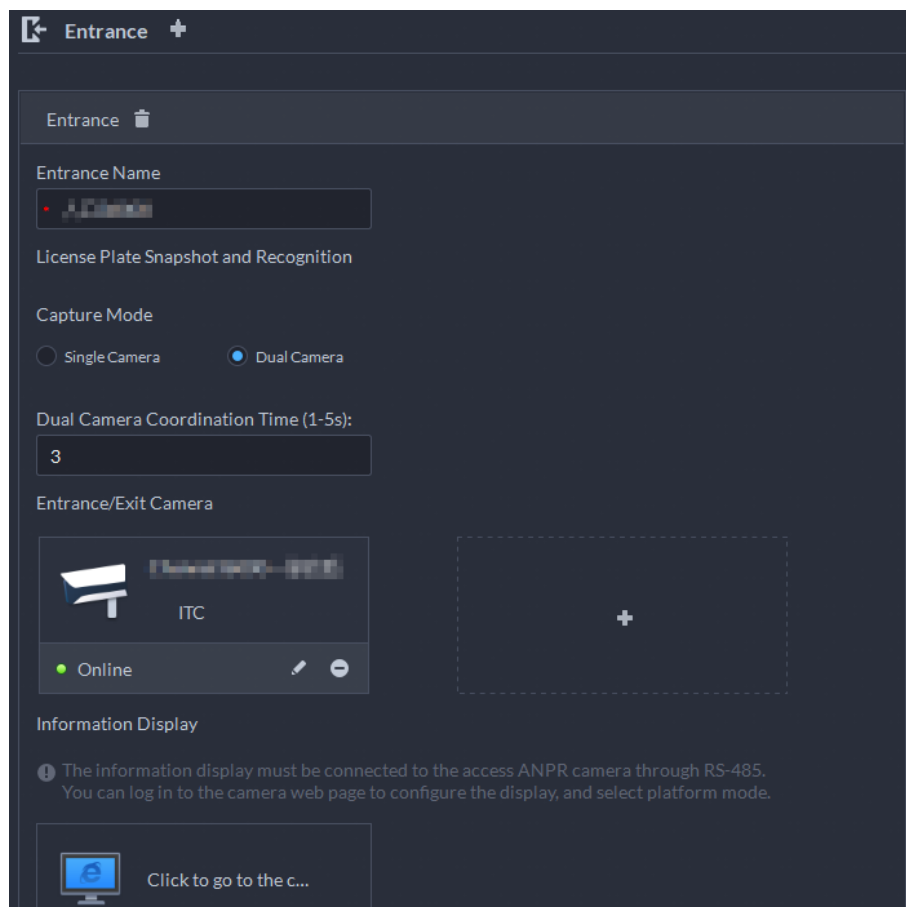
If limited by the surroundings, you can install two cameras for this point, and then set **Capture Mode** to **Dual Camera** to improve the successful rate of recognition number plates.

In **Dual Camera** mode, the vehicles captured by the two cameras within the defined **Dual Camera Coordination 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.

Figure 5-43 Entrance point configuration







5. If there is an exit point, click  next to **Exit**, and then configure the parameters.



The parameters are similar to the ones in **Entrance**. For details, see the steps above.

Step 5 Configure the passing rules, and then click **Save and Exit**.

1. Select a vehicle entrance rule, and then configure the parameters.

Table 5-29 Parameter description

Parameter	Description
Registered Vehicles	<ul style="list-style-type: none"> ● 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 East entrance but not South entrance, then the vehicles in the group can only enter the parking lot through East entrance. ● Allow Passage When Available Space is 0 : After enabled, vehicles are allowed to enter the parking lot even if there are no available parking space. Click  to enable this function for an entrance point.  This function is available only when parking space counting is enabled for the parking lot.
All Vehicles	<p>All vehicles can enter the parking lot.</p> <ul style="list-style-type: none"> ● Allow Unlicensed Vehicles to Enter : Vehicles with no license plates can also enter the parking lot. ● Vehicles on the Blocklist to Enter : Vehicles on the blocklist are also allowed to enter the parking lot. ● Allow Passage When Available Space is 0 : After enabled, vehicles are allowed to enter the parking lot even if there are no available parking space. Click  to enable this function for an entrance point.  This function is available only when parking space counting is enabled for the parking lot.

Parameter	Description
Custom	<p>You can customize the passing rule for the entrance.</p> <ul style="list-style-type: none"> For how to configure Registered Vehicles Access Rule and Allow Passage When Available Space is 0, see the content above. 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 "4.2.6 Adding Time Template". Open Barrier by Verification : After enabled, the access permission of a vehicle must be verified, and then an administrator can manually open the barrier for it. If Open Barrier by Card Swiping After Verification is also enabled, the driver can swipe a card, and then the barrier will automatically open if the can verify the driver to be the owner of the vehicle. Open Barrier by Card Swiping Without Verification : The barrier will automatically open if the card has access permission. <p></p> <p>You can enable Open Barrier by Verification or Open Barrier by Card Swiping Without Verification at the same time.</p> <ul style="list-style-type: none"> Available Parking Space Counting :  <p>You must enable parking space counting and select Count parking spaces by entering and exiting vehicles.</p> <ul style="list-style-type: none"> ◇ 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 a vehicle that is not registered to the platform enters. ◇ Custom : Configure which vehicles in the vehicle groups will be used to calculate parking spaces.



For how to configure vehicle groups, see "5.8.3 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.

Related Operations


- : Edit the passing rules of the parking lot.
- : Edit the available parking space of the parking lot.
- : Edit the information of the parking lot.
- : Delete the parking lot.

5.8.2.2 Event Parameter

Configure events for a parking lot so that you can receive notifications when alarms are triggered.

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 "5.1 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, the events that were configured will be displayed on the right.



Blocklist alarm will not be displayed because there are no additional parameters to be configured.



Step 4 Click  to configure an event.



Table 5-30 Parameter description

Parameter	Description
Parking Overtime	<ul style="list-style-type: none"> ● Overtime Parking Threshold : The unit is minute. Alarm will be triggered if a vehicle has parked for longer than the defined value. ● 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 : <ul style="list-style-type: none"> ◇ 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. <p> You can enable Non-registered Vehicle and Registered Vehicle at the same time.</p>
No Entry and Exit Record	<ul style="list-style-type: none"> ● No Entrance/Exit Record Duration : The unit is day. If a vehicle has not entered or exited the parking lot for longer than the defined duration, then an alarm will be triggered. ● 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.

5.8.3 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 Groups**.
- Step 2 Click **Add**.
- Step 3 Enter a name and select a color for the group, and then click **Add**.
- Step 4 Click  of a group, or double-click a group and click **Select from Vehicle List**, select the vehicles that you want to add to the group, and then click **OK**.

5.9 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.

5.9.1 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 **Add** at the upper-left corner.

Figure 5-44 Add a 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:

Pass No. ⓘ Displays the number of people passing when the device in use supports this function.

Calibrate Number of People Staying Everyday

ⓘ The calibration will be done according to the time zone of the first device in the rule group.

Calibration Time:
 : :

Calibrated Number of People:

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 ⓘ

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


Table 5-31 Parameter description

Parameter	Description
People Counting Group Name	Name of the people counting group.
Pass No.	<p>The calibration time can only be configured on the hour. It is the start of a counting cycle.</p> <ul style="list-style-type: none"> 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	<p>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 "5.1 Configuring Events".</p> <ul style="list-style-type: none"> When the number of people in the group reaches the defined crowd threshold but smaller than the overlimit threshold, the light will turn yellow. When the number of people in the group reaches the defined overlimit threshold, the light will turn red.
Crowd Threshold	
Overlimit Threshold	
Rule	Select the devices whose people counting rules you want to include in the group, and then their data will be combined together.

5.9.2 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.


1. Click  to select the users that have been configured email addresses, or enter an email address, and then press Enter.

Figure 5-45 Invalid email address, you must press Enter

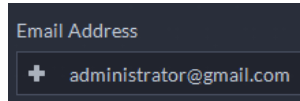
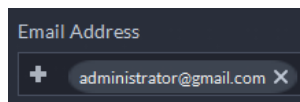


Figure 5-46 Valid email address



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.

5.10 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.

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

Table 5-32 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 Notification	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: <ul style="list-style-type: none"> Click  to select the email addresses of users. Manually enter an email address, and then press the Enter key.


5.10.2 Configuring Video Storage Detection

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 **Add**.
- Step 3** Configure consecutive storage days, and then select the channels for detection.
- Step 4** Click **OK**.

Related Operations

You can view the detection results when viewing the detailed information of a device in **Maintenance Center**. 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.

Figure 5-47 Video duration and integrity status

Channel Name	Channel Type	Channel Online/...	Chanel ...	Recording ...	Video Integ...	Storage ...	Latest Status Change
48-onvif_1	Video Channel	Online	Normal	5	⊙	Centre Storage	2022-11-15 14:59:19
48-onvif_2	Video Channel	Online	Normal	2	⊙	-	2022-11-15 14:59:19
48-onvif_3	Video Channel	Online	Normal	-	⊙	Centre Storage	2022-11-15 14:59:19

6 Businesses Operation

6.1 Monitoring Center

The monitoring center provides integrated real-time monitoring applications for scenarios such as CCTV center. The platform supports live video, license plate recognition, target detection, access control, emp, snapshots, events, video playback, video wall, and more.

6.1.1 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**.

Figure 6-1 Monitoring center

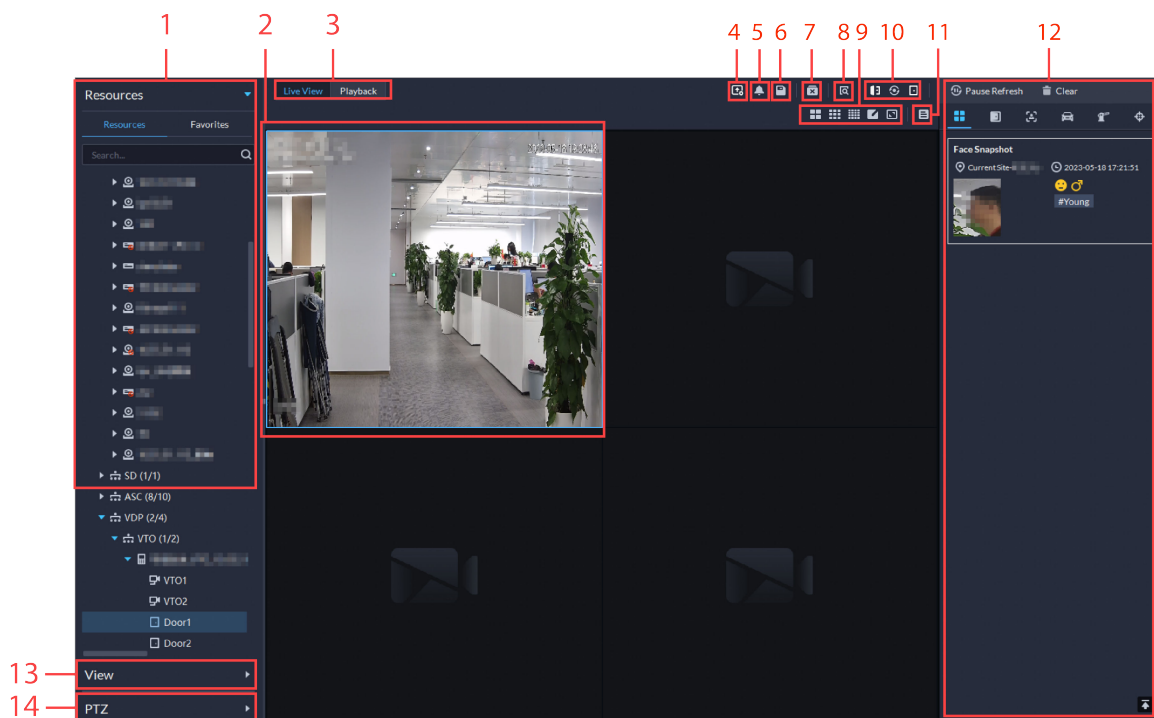




Table 6-1 Page description

No.	Parameter	Description
1	Favorites and device tree	<ul style="list-style-type: none"> 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.

No.	Parameter	Description
3	Live view and playback	<ul style="list-style-type: none"> ● Live view: View real-time videos. ● Playback: View recorded videos. For details, see Playback.
4	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 "6.1.5 Video Wall".
5	Set alarm windows in batches	<p>Set all windows as alarm windows.</p> <p>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.</p>
6	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.
7	Close all windows	Close all windows in live view.
8	Search for targets in the video	The platform supports manually selecting targets in the video, and then quickly searching for them in DeepXplore. For details, see Viewing Live Video.
9	Window split mode and full screen	<ul style="list-style-type: none"> ● 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. <p>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.</p> <ul style="list-style-type: none"> ● 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.
10	Control doors	For a door channel, you can configure its mode, 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.
11	Event panel button	Display or hide the event panel.
12	Events	<p>Displays events from channels that you are viewing live videos from. You can:</p> <ul style="list-style-type: none"> ● 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
13	View	<ul style="list-style-type: none"> ● 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. Maximum 100 views can be created.
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.

6.1.2 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.

6.1.2.1 Viewing Live Video

View the live video of connected devices.



This section only introduces viewing live video. For map live view, see "5.2 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.




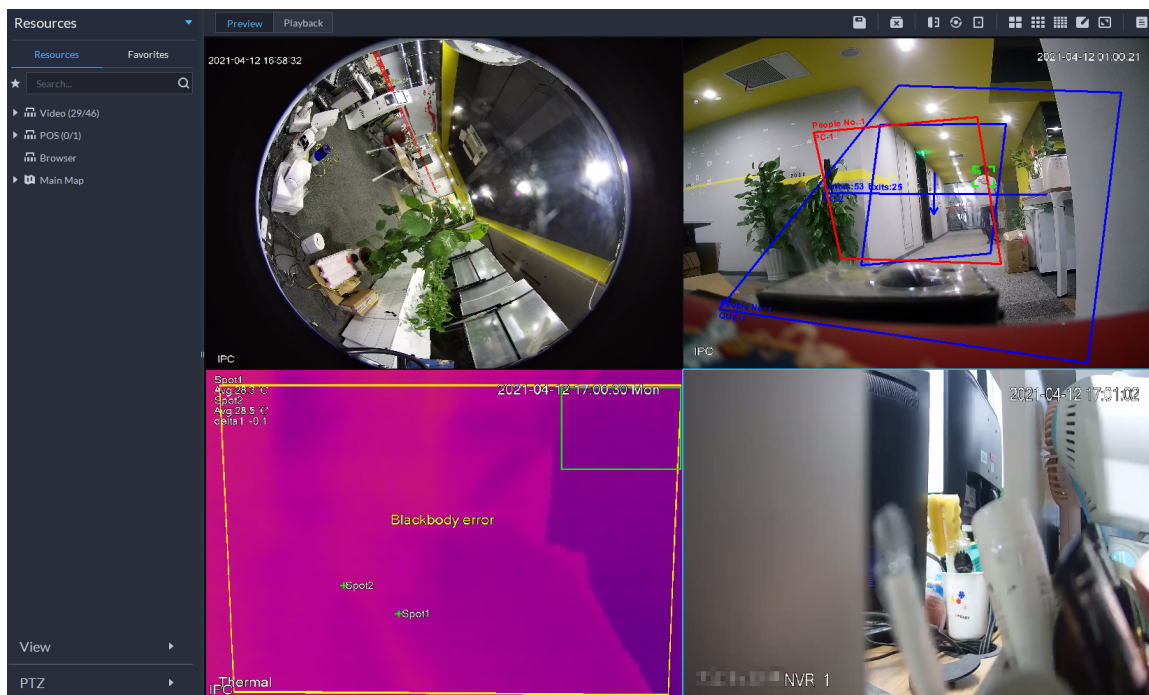
- ◇ If the number of splits in the window is more than the number of online channels, video of all channels will be displayed in the window. Otherwise, click  on the top of the page to turn pages.
- ◇ Close the on-going tour before starting live view.

Figure 6-2 Live view



Step 4 You can perform the following operations during live view.

- 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 s by default, and it will disappear after 5 s.

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 on the upper-right corner.

Figure 6-3 Live window

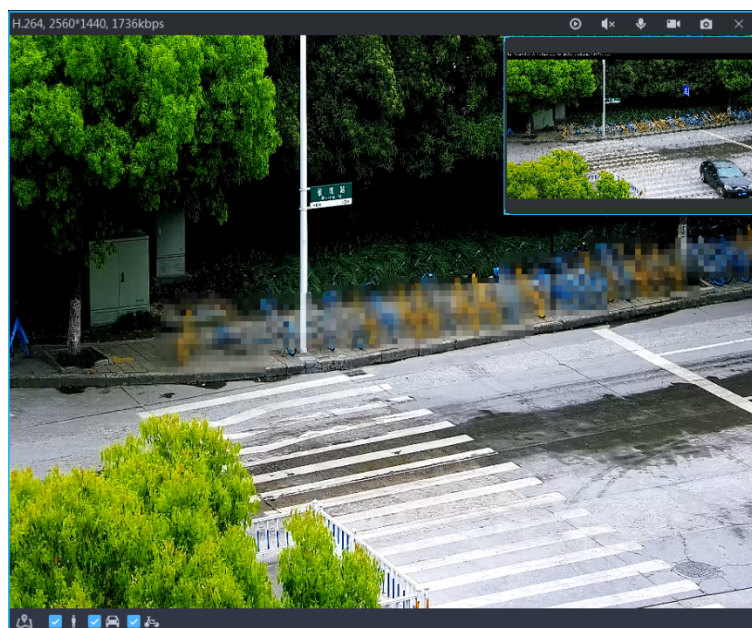








Table 6-2 Parameter description

Icon	Name	Description
	Instant playback	Open/close instant playback.
	Audio	Open/close audio.
	Audio communication	Start two-way audio with the device the channel belongs to.
	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 <code>..\DSS\DSS Client\Record</code> by default. To change the storage path, see "9.3.5 Configure File Storage Settings".
	Snapshot	Take a snapshot. The snapshots are saved to <code>..\DSS\DSS Client\Picture</code> by default. To change the snapshot storage path, see "9.3.5 Configure File Storage Settings".
	Close	Close the video.


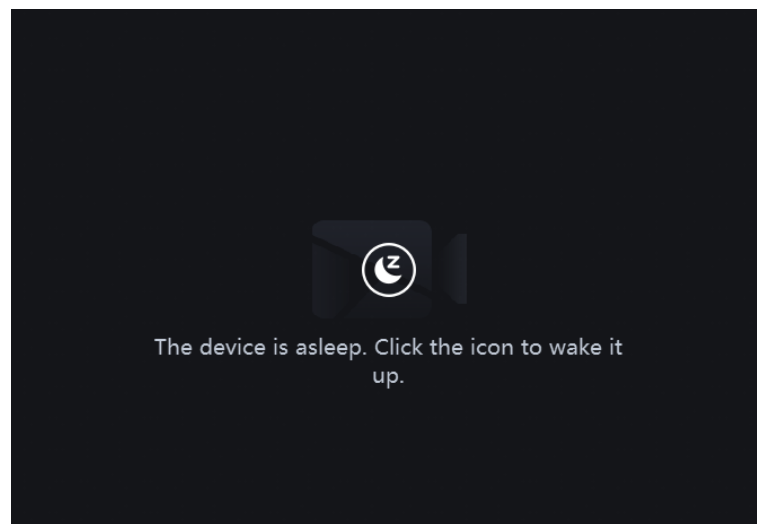
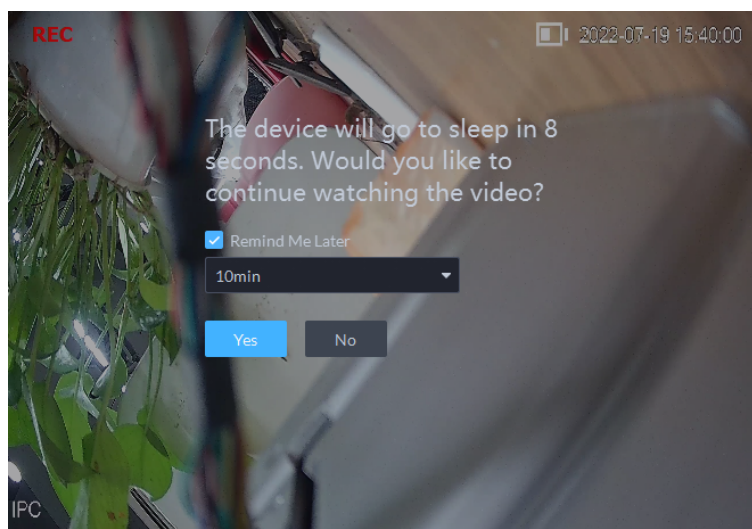
- Sleep function is supported for IPCs that use 4G mobile network to communicate and are solar-powered.
 - ◇ When the device is asleep, you can click  to wake it up.

Figure 6-4 Wake up the device



- ◇ 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.

Figure 6-5 Request to sleep 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 6-3 Description

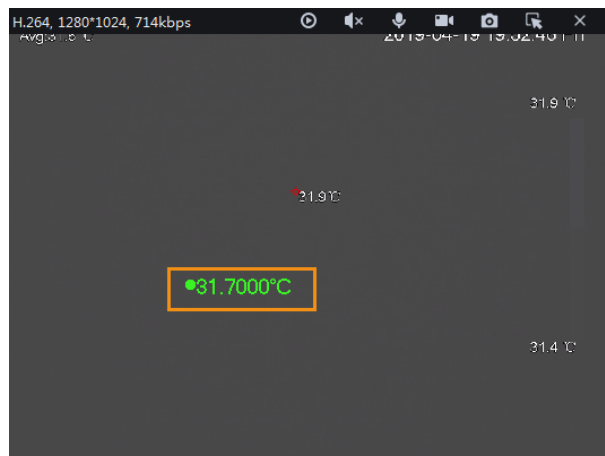
Parameters	Description
Audio Input Selection	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Start Remote Recording	Record the audio and video in the current window. If a channel already 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 "9.3.5 Configure File Storage Settings".
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	<ul style="list-style-type: none"> ◇ Real-Time Priority: The video is in real-time, but video quality might be reduced. ◇ Fluency Priority: The video is fluent, but video lagging might occur. ◇ Balance Priority: Real-time priority or fluency priority, depending on actual conditions. ◇ Custom: Configure the video buffer time from Local Settings > Video. The larger the value, the more stable the video quality.

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	<p>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.</p> <p>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.</p>
AI Overlay	<p>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.</p>  <p>AI overlay information is not displayed by default.</p>
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.
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 Favorite	You can add the active channel or all channels into Favorite.
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.

Parameters	Description
Fisheye View	<p></p> <p>This function is available on fisheye cameras only. When changing the video stream, the fisheye view mode will maintain the current configuration.</p> <p>According to different installation methods, the fisheye view can be varied.</p> <ul style="list-style-type: none"> ◇ 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.

- To view real-time temperature of a point on the thermal camera view, hover over that point.

Figure 6-6 View temperature



- 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 6-7 Live view

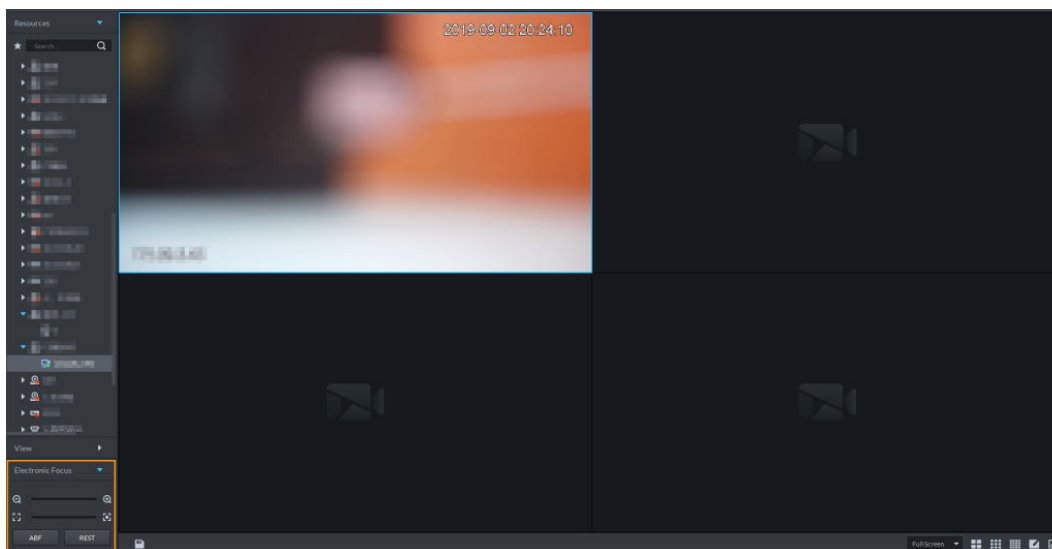









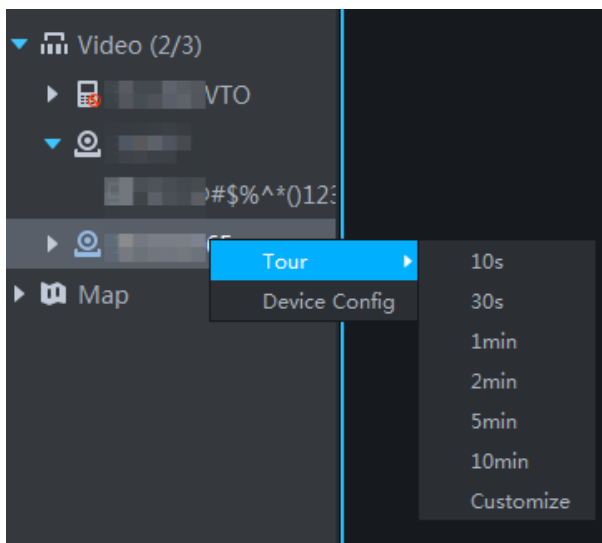
Table 6-4 Description




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 6-8 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 6-9 Split mode

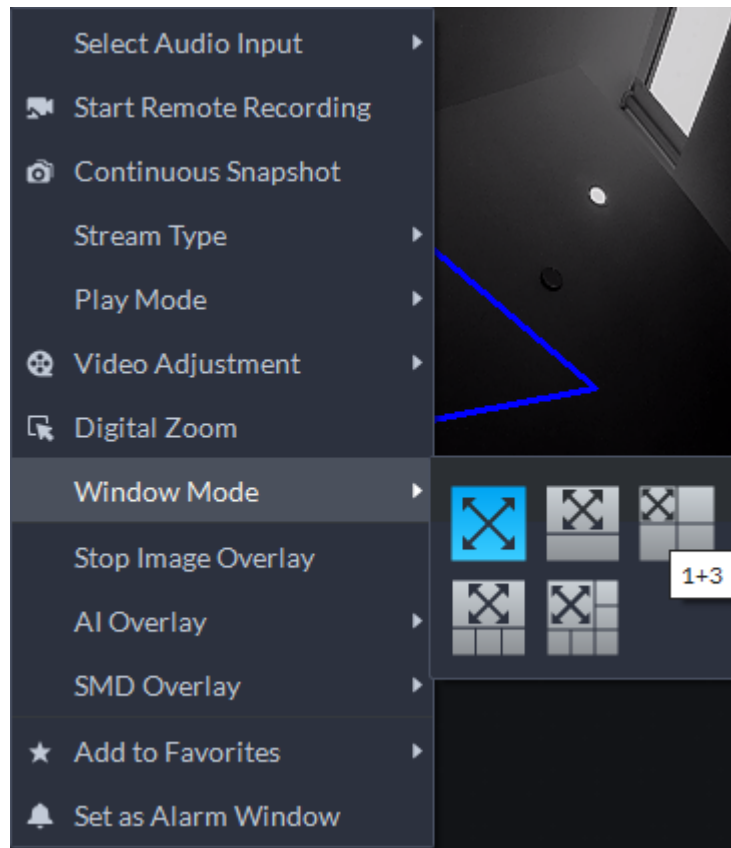
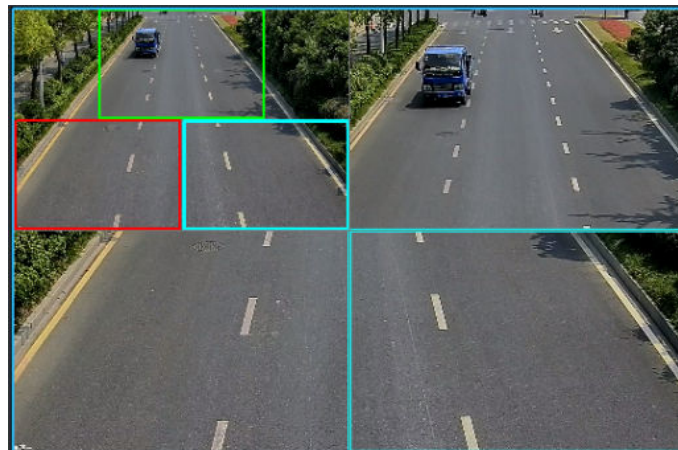


Figure 6-10 1+3 mode




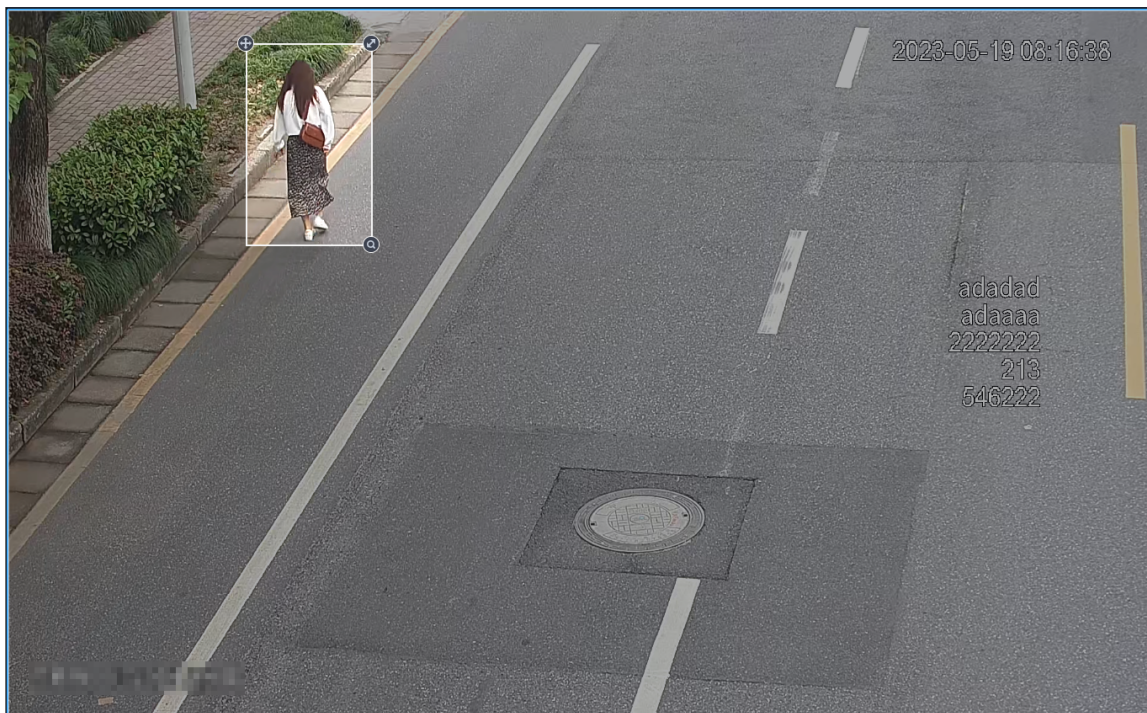











- Search for targets in the video.
Click  on the upper-right corner to select and search for the target in DeepXplore.

Figure 6-11 Select a target






- View real-time events.

Click  to open the event panel, which displays the real-time alarm events of opened channels.

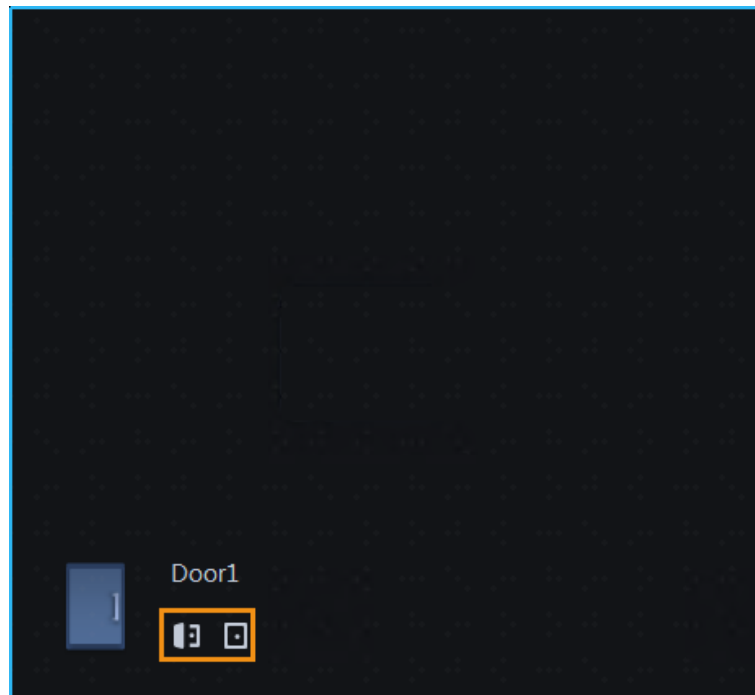
- ◇ Click the event type on the top of the event panel to view the corresponding event.
- ◇ Click event record to view the snapshot. Video playback is also supported. Operations related to different events might be different.
- ◇ : Refreshes events in real time. : Stops refreshing.
- ◇ Click  to clear 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.

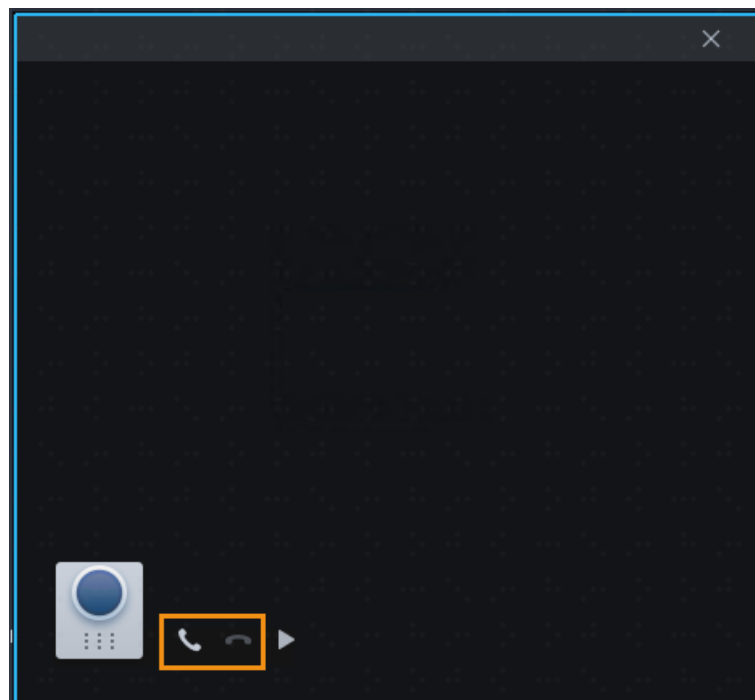
Figure 6-12 Lock/unlock the door



- Video intercom.

When viewing the video intercom channel, you can answer or hang up the call.

Figure 6-13 Video intercom



6.1.2.2 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.


6.1.2.2.1 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**.

6.1.2.2.2 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**.

6.1.2.2.3 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 6-5 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.




6.1.2.2.4 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.

6.1.2.2.5 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  00:02.
 - ◇ To pause, click .
 - ◇ To exit tour, click .

6.1.2.2.6 Sharing a Private View

Private 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 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.

6.1.2.2.7 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.

6.1.2.3 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.


6.1.2.3.1 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.

6.1.2.3.2 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.

6.1.2.3.3 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.




6.1.2.3.4 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 .

6.1.2.4 PTZ

Operate PTZ cameras during live view on the DSS Client.

6.1.2.4.1 Configuring Preset

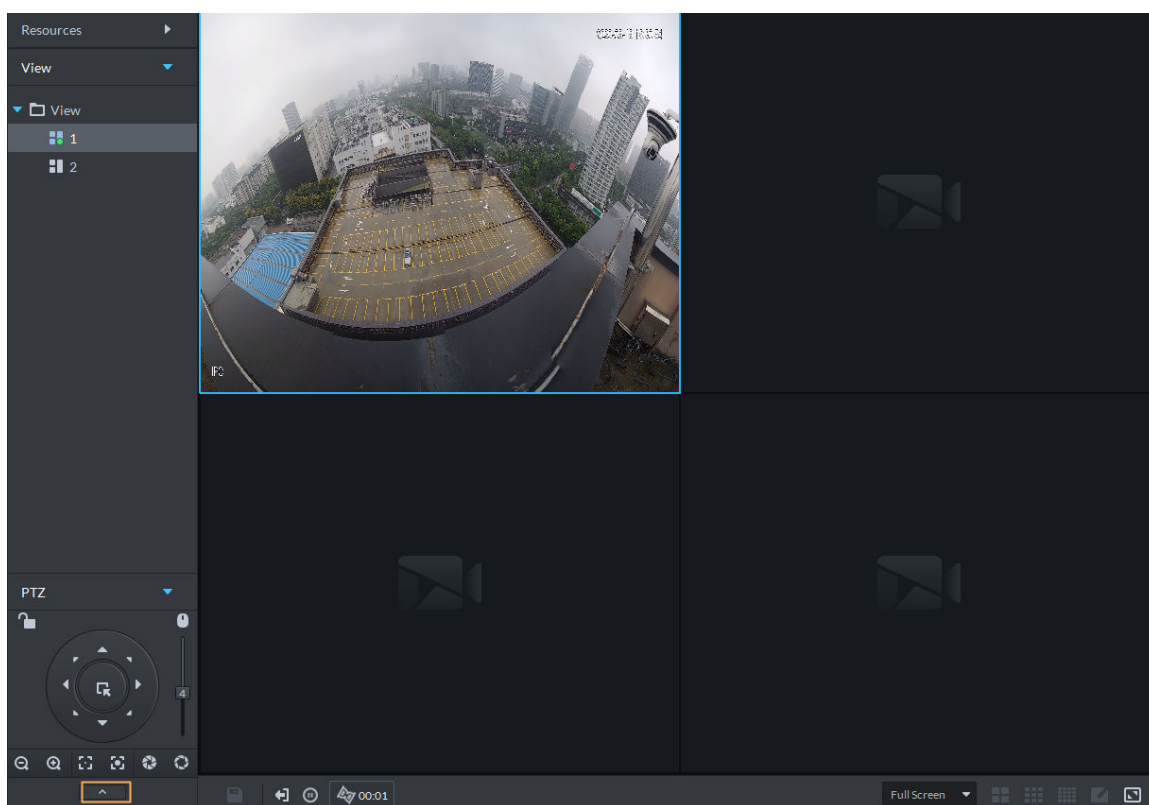
A preset is a set of parameters involving PTZ direction and focus. By calling a preset, you can quickly rotate the camera to the pre-defined position.


Procedure

Step 1 On the **Monitoring Center** page, open the video of a PTZ camera.



Step 2 Click .

Figure 6-14 Go to PTZ control panel




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 .

Related Operations

Call a preset: Click  of a specific preset, and then camera will rotate to the related position.

6.1.2.4.2 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

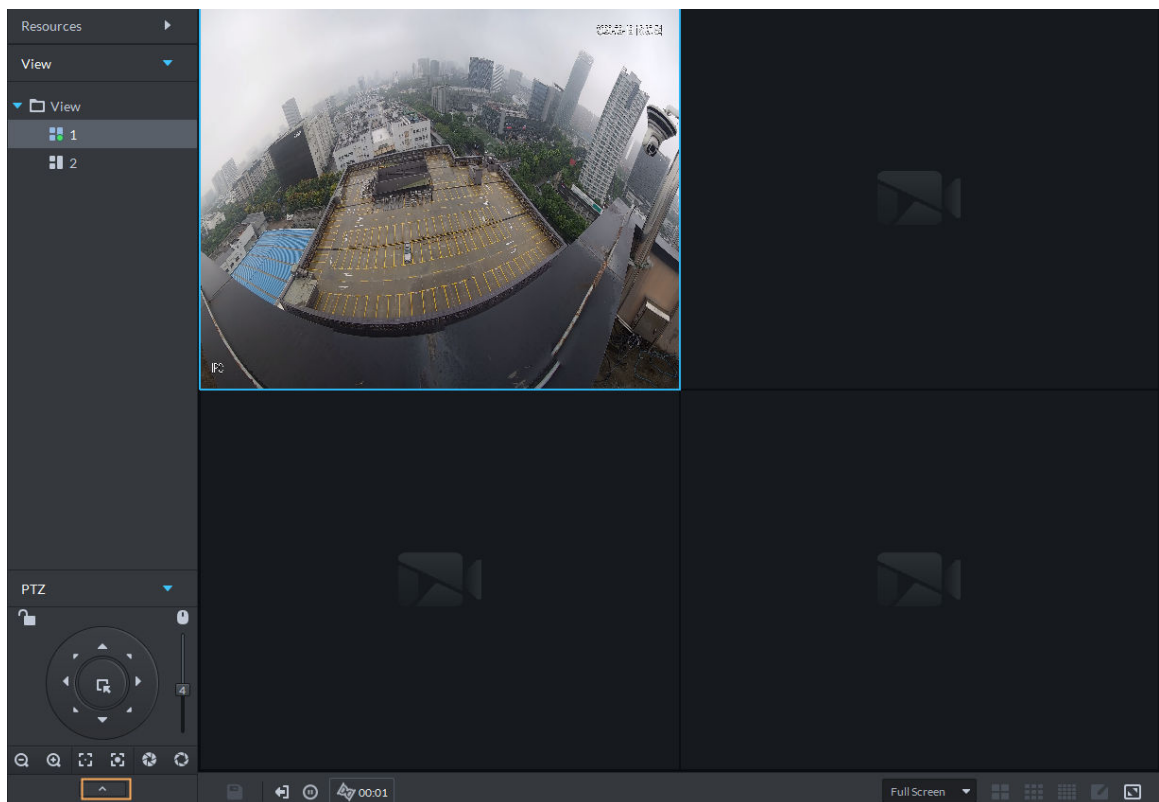
You have added at least 2 presets.

Procedure


Step 1 On the **Monitoring Center** page, open the video of a PTZ camera.

Step 2 Click .


Figure 6-15 Go to PTZ control panel



Step 3 Click .

Step 4 Click .

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**.

Related Operations

To start tour, click , then camera goes back and forth among the presets.

6.1.2.4.3 Configuring Pattern

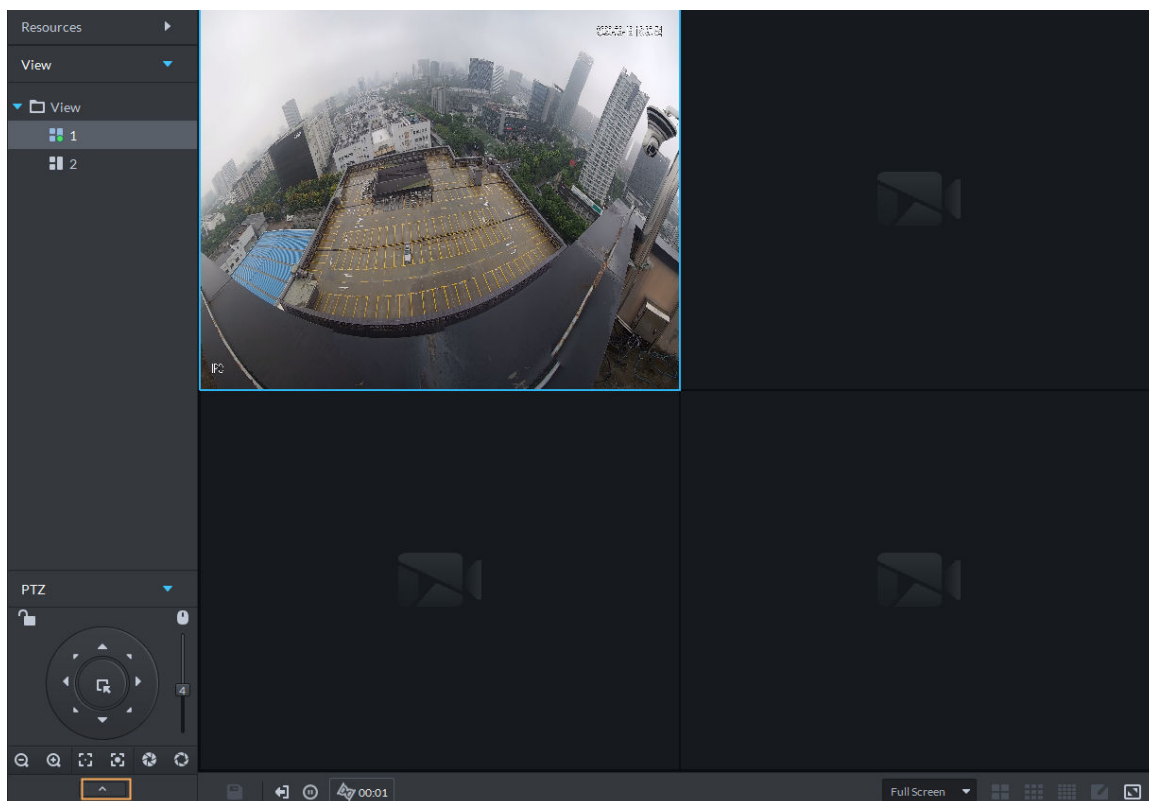
A pattern is a record of a consecutive series of PTZ operations. You can select a pattern to repeat the corresponding operations quickly. See pattern configuration instructions as follows.

Procedure


Step 1 On the **Monitoring Center** page, open the video of a PTZ camera.


Step 2 Click .

Figure 6-16 Go to PTZ control panel




Step 3 Click .




Step 4 Click , and then operate the 8 PTZ buttons of PTZ to set pattern.

Step 5 Click .

Related Operations




Call pattern: Click , and then the camera will automatically repeat the pattern that you have configured.

6.1.2.4.4 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.




6.1.2.4.5 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.

6.1.2.4.6 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.

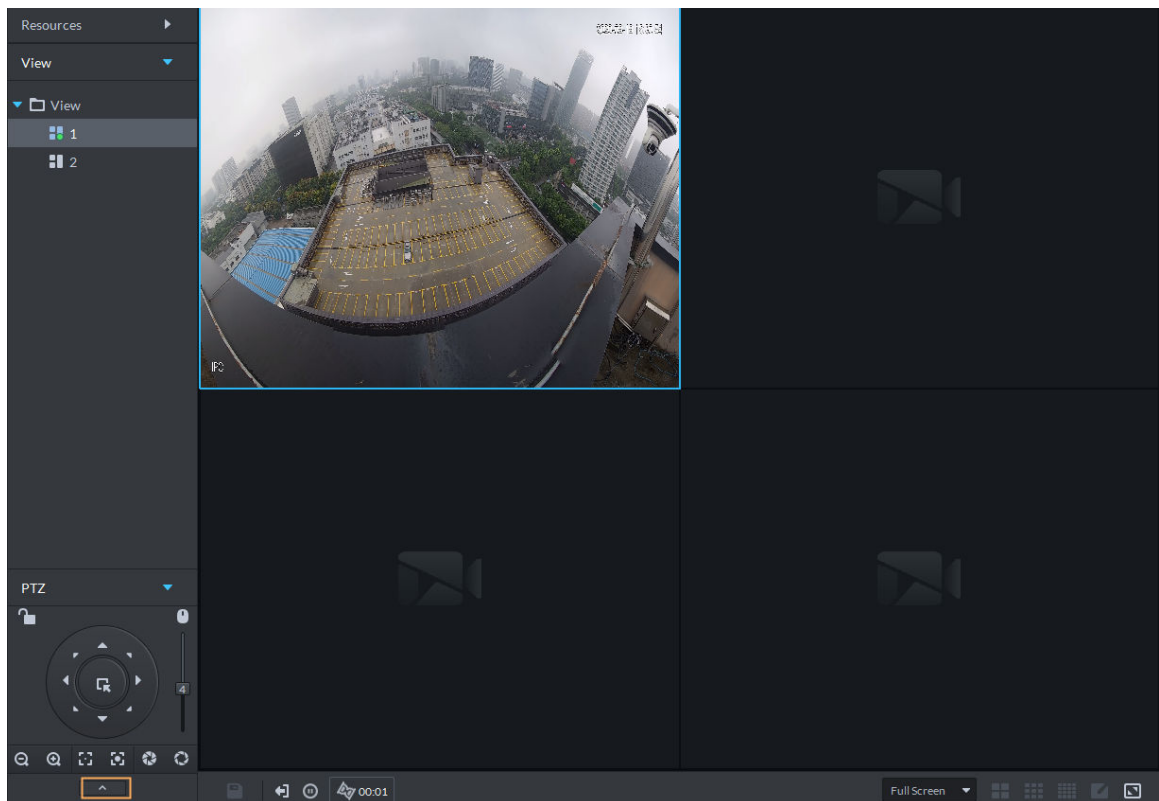
6.1.2.4.7 Configuring Custom Command

Procedure

Step 1 On the **Monitoring Center** page, open the video of a PTZ camera.

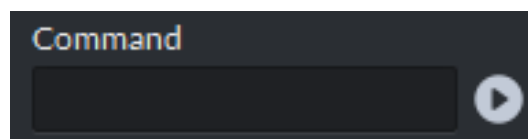
Step 2 Click .


Figure 6-17 Go to PTZ control panel



Step 3 Enter your command in the **Command** box.

Figure 6-18 Custom command



Step 4 Click  to show the command functions.

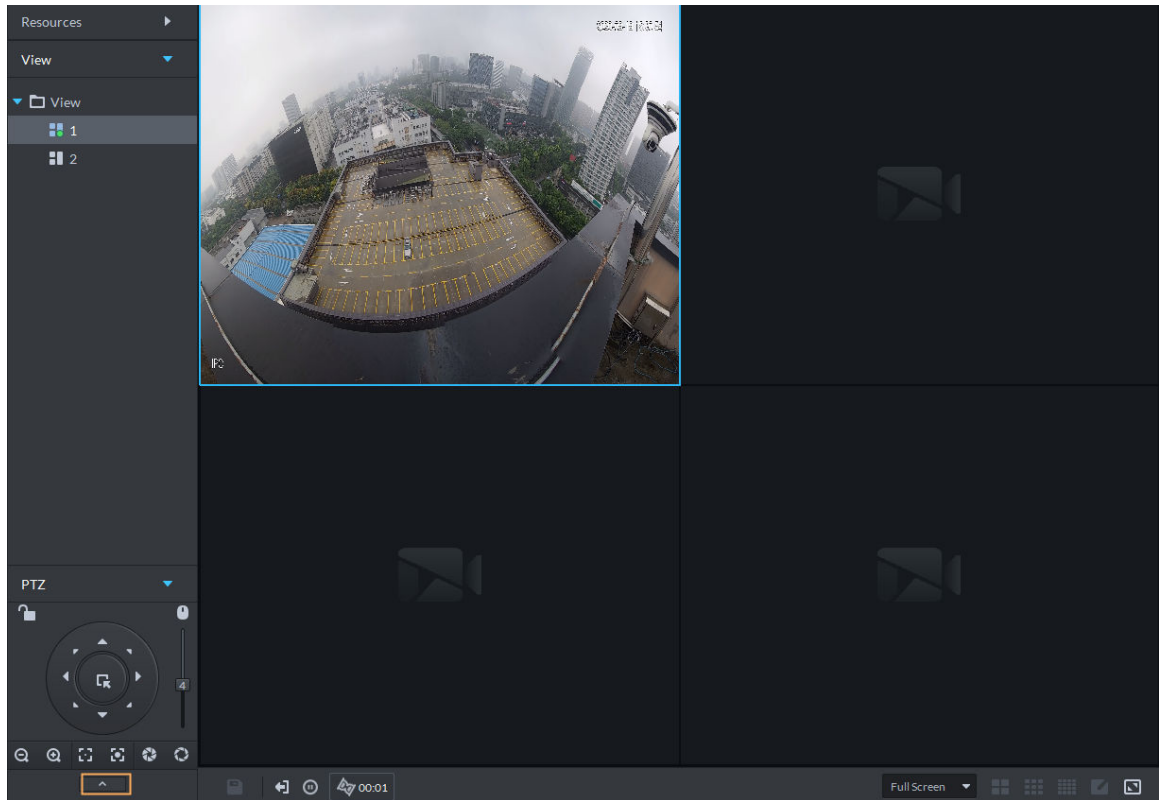
6.1.2.4.8 PTZ Menu

Procedure

Step 1 On the **Monitoring Center** page, open the video of a PTZ camera.

Step 2 Click .

Figure 6-19 Go to PTZ control panel



Step 3 Click .

Step 4 Click .

Step 5 Use the panel to go to the menu configuration page.

Figure 6-20 Go to PTZ menu configuration page

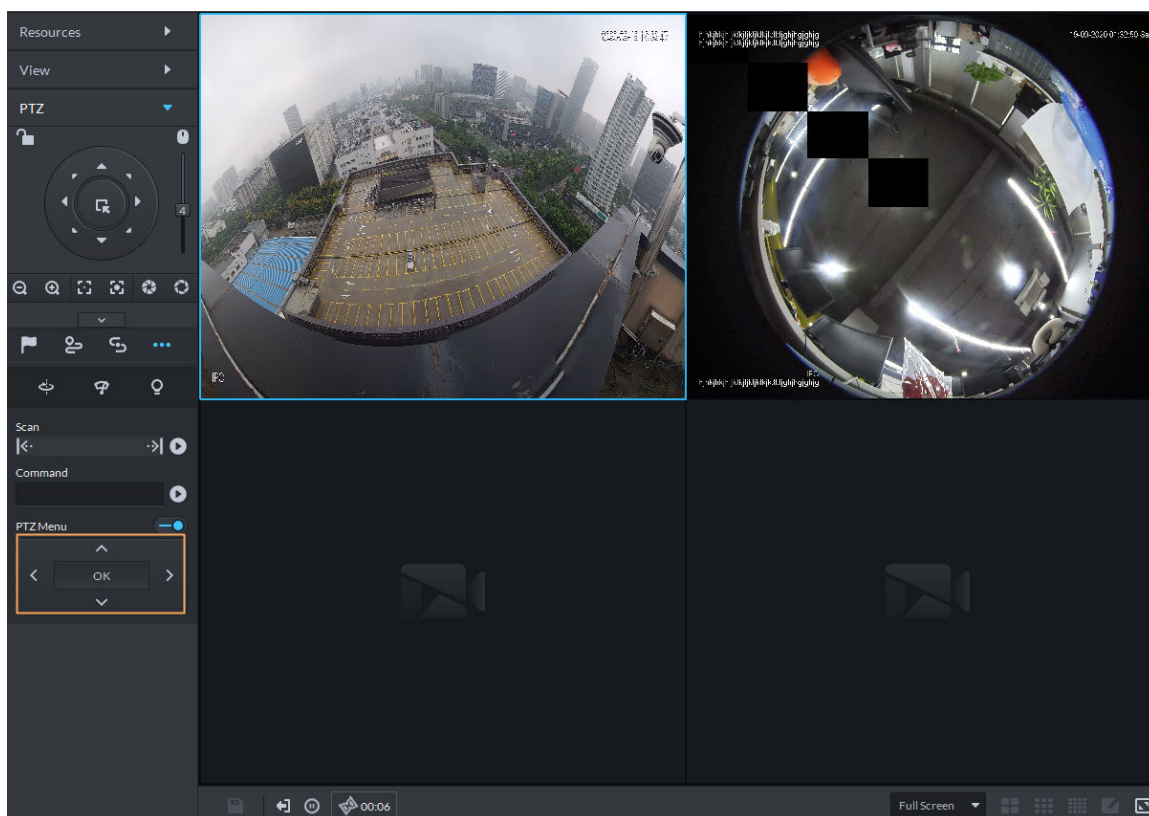








Table 6-6 PTZ menu description

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. <ul style="list-style-type: none"> ● If the main menu has the sub-menu, click OK to enter the sub-menu. ● Point to Back and then click OK to go back to the previous menu. ● Point to Exit and then click OK to exit the menu.
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.

Parameters	Description
Exit	Point to the Exit and then click OK to exit PTZ menu.

6.1.2.5 Fisheye-PTZ Smart Track

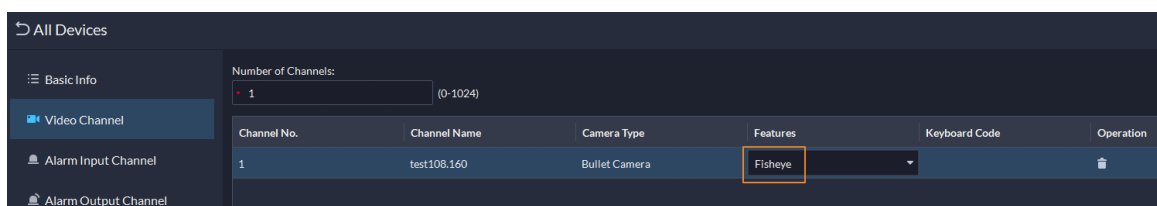
Link a PTZ camera to a fisheye camera so that when the fisheye camera detects a target, the PTZ camera automatically rotates to it and track.

6.1.2.5.1 Preparations

Make sure the following preparations have been completed:

- Fisheye camera and PTZ camera are well deployed. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. For details, see "4 Basic Configurations".
 - ◇ When adding cameras, select **Encoder** from **Device Category**.
 - ◇ The **Features** of a fisheye camera is set to **Fisheye**. For details, see "4.2.2.5.2 Modifying Device Information".

Figure 6-21 Set the feature to Fisheye



6.1.2.5.2 Configuring Fisheye-PTZ Smart Track

Procedure




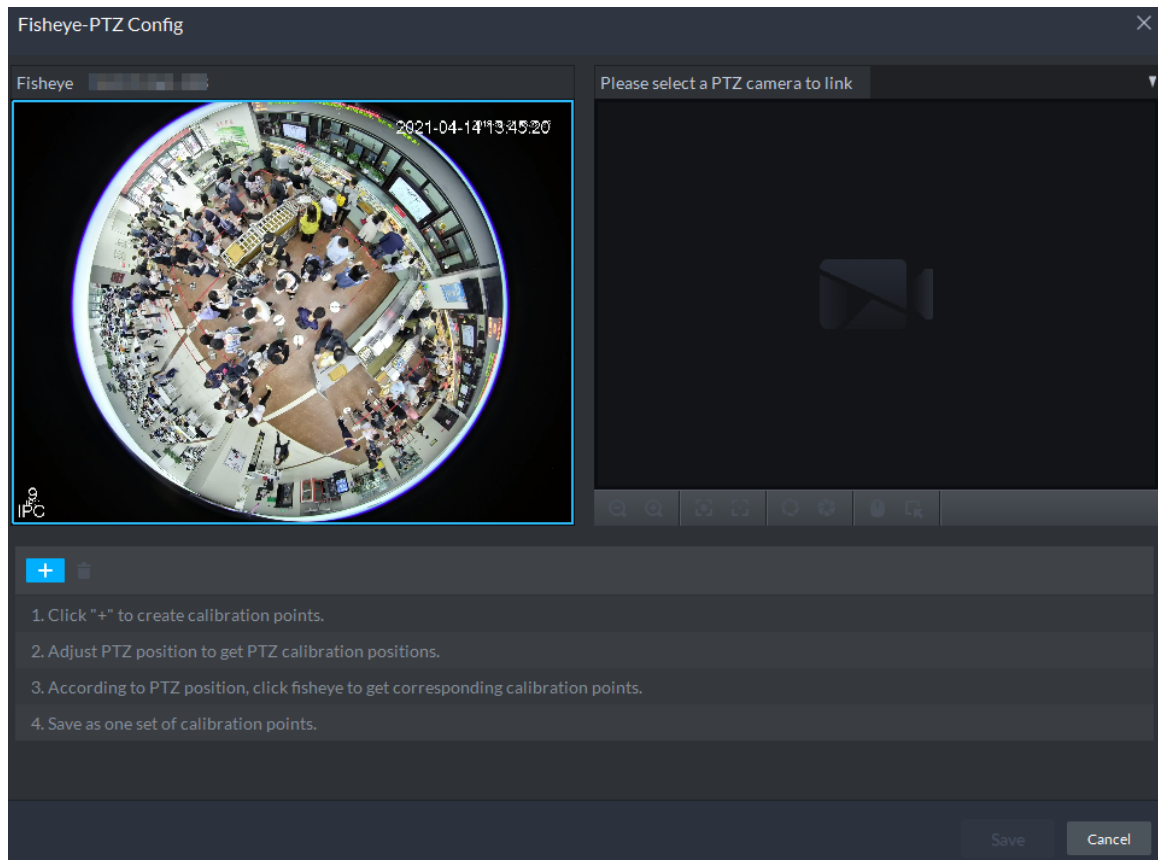
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then click **Monitoring Center**.
- Step 2** Click .
- Step 3** In the device tree on the left, right-click a fisheye camera, and then select **Modify Smart Track**.
- Step 4** Click  next to **Please select a PTZ camera to link**, and then select a PTZ camera.

Figure 6-22 Set smart track rules (1)






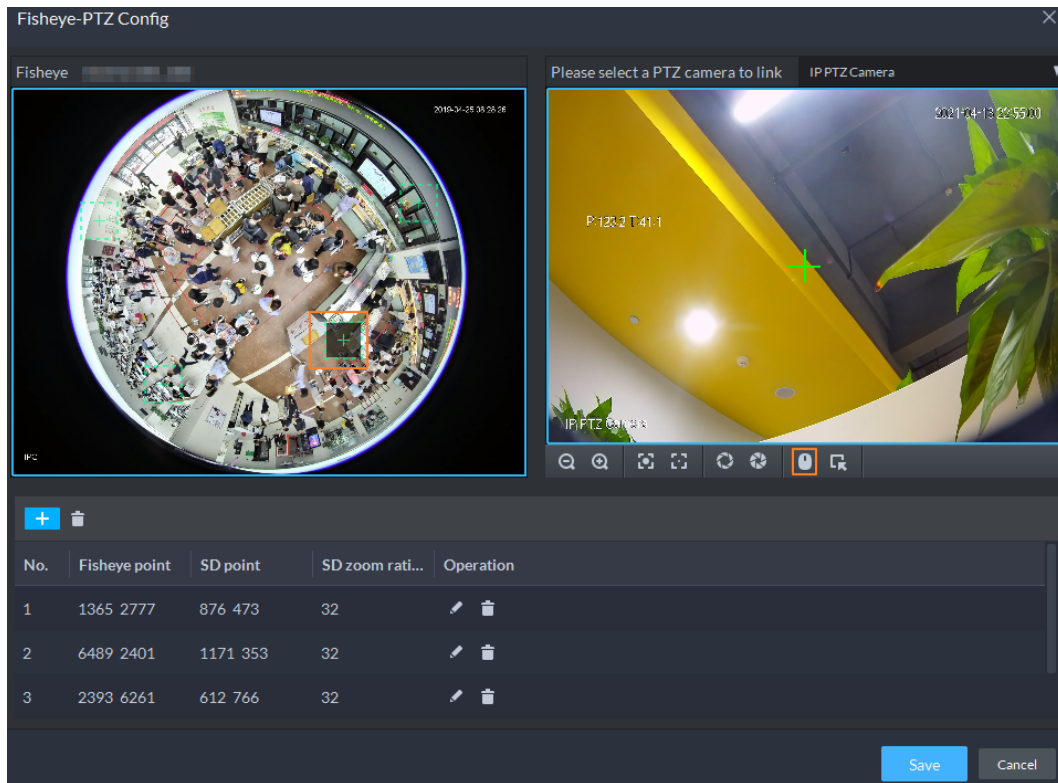
Step 5 Click  and then move the  of the fisheye on the left to select a position. Click  of the PTZ camera to find the position. Adjust the PTZ camera to find the position and move the PTZ to the center position (The green cross on the image).

Figure 6-23 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.

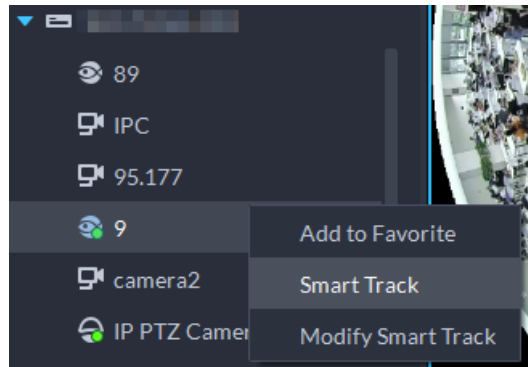
Step 7 Click **Save**.

6.1.2.5.3 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 6-24 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.

6.1.3 Playback

Play back recorded videos.

6.1.3.1 Page Description


Log in to the DSS Client. On the **Home** page, click , and then click **Monitoring**. Click the **Playback** tab.

Figure 6-25 Playback page

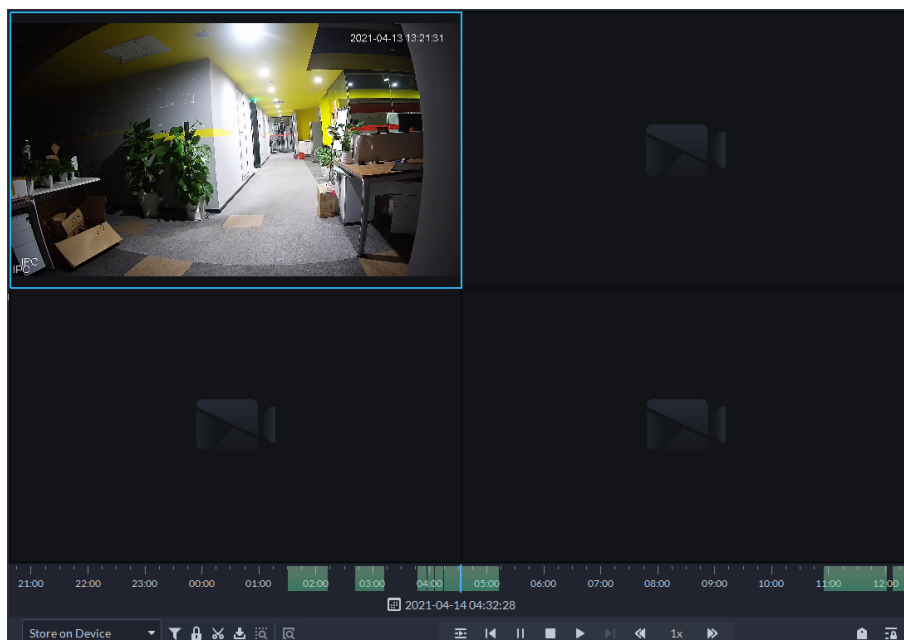










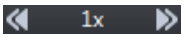
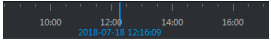
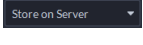





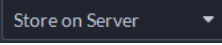

Table 6-7 Function description

Icon	Description
	Filter video according to record type.

Icon	Description
	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.
	Manually select a target in the video and quickly search for it in DeepXplore.
	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.
	Play the video backwards or forwards.
	Stop/pause the video.
	Play back or forward frame by frame. Click and hold to play continuously.
	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.
	During playback, you can drag time progress bar to play back record at the specific time.
	Select the storage location of the video to be searched. Supports searching for the video on the platform server or storage device.
	Tag records.
	Lock records.

6.1.3.2 Playing Back Video

Procedure

- Step 1** Log in to the DSS Client. On the **Home** page, click  and then select **Monitoring Center**.
- Step 2** Click the **Playback** tab.
- Step 3** Double-click or drag a channel to a window on the right.
- Step 4** Select the storage path of recorded video from , 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 6-26 Video playback



Table 6-8 Function description

Icon	Name	Description
	Take a recording on the device	Click this icon 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: <ul style="list-style-type: none"> • : Move the selection area. • : 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.

Right-click the video, and then you can perform the following actions.

Figure 6-27 Shortcut menu

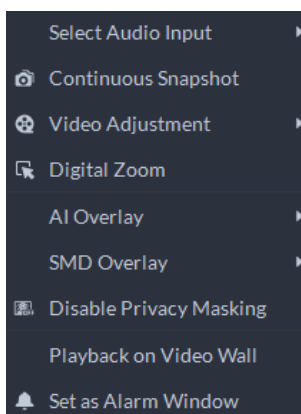


Table 6-9 Description


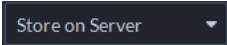

Parameters	Description
Select Audio Input	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Continuous Snapshot	Take snapshots of the current image (three snapshots each time by default). The snapshots are saved to <code>..\DSS\DSS Client\Picture</code> by default. To change the snapshot saving path, see "9.3.5 Configure File Storage Settings".
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 and 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 view 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 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.
Playback on Video Wall	Play the video of the current channel on video wall. Make sure that video wall is configured (see "6.1.5 Video Wall").

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.

6.1.3.3 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.

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.


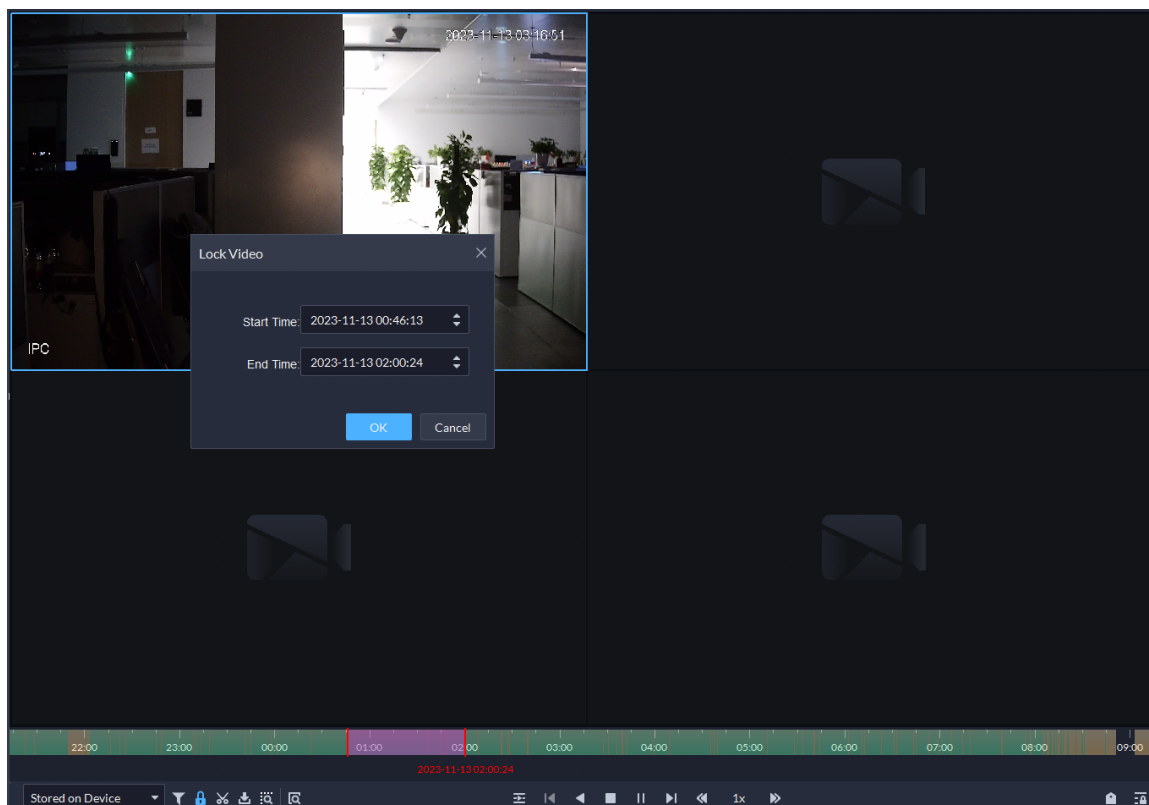

- Step 5 Select a window that has recorded video, and then click  on the bottom of the page, and then click on the timeline to mark the start point and end point of the video clip you need.

Figure 6-28 Lock record



Step 6 Confirm the start and end time, and then click **OK**.


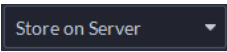

Related Operations

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.

6.1.3.4 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 6-29 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.

6.1.3.5 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 "9.3.2 Configuring Video Settings".

6.1.3.6 Searching for Targets

When playing back a video, you can manually select a target, and then 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 **Store on Server**, and then click  to select the date.



Dates with blue dot means there are recordings.

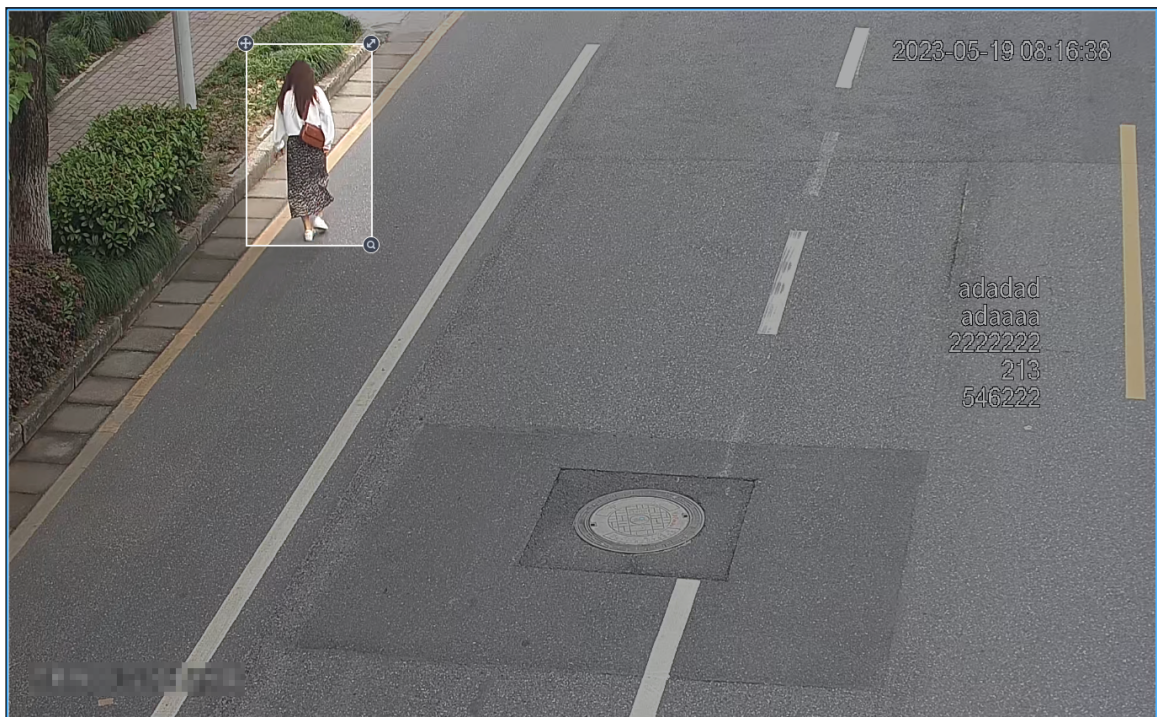
Step 4 Click  on the bottom of the page.

Step 5 Drag on the video to select a target.






Right-click to exit this function.

Figure 6-30 Select a target



Step 6 (Optional) Adjust the area of selection.

- Drag  to move the area to any location.
- Drag  to resize the area.

Step 7 Click  and select a type for the target, and then you are directed to DeepXplore to search for it. For details, see "6.3 DeepXplore".

6.1.3.7 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 **Store on Server**, and then click  to select the date.

The search results are displayed.

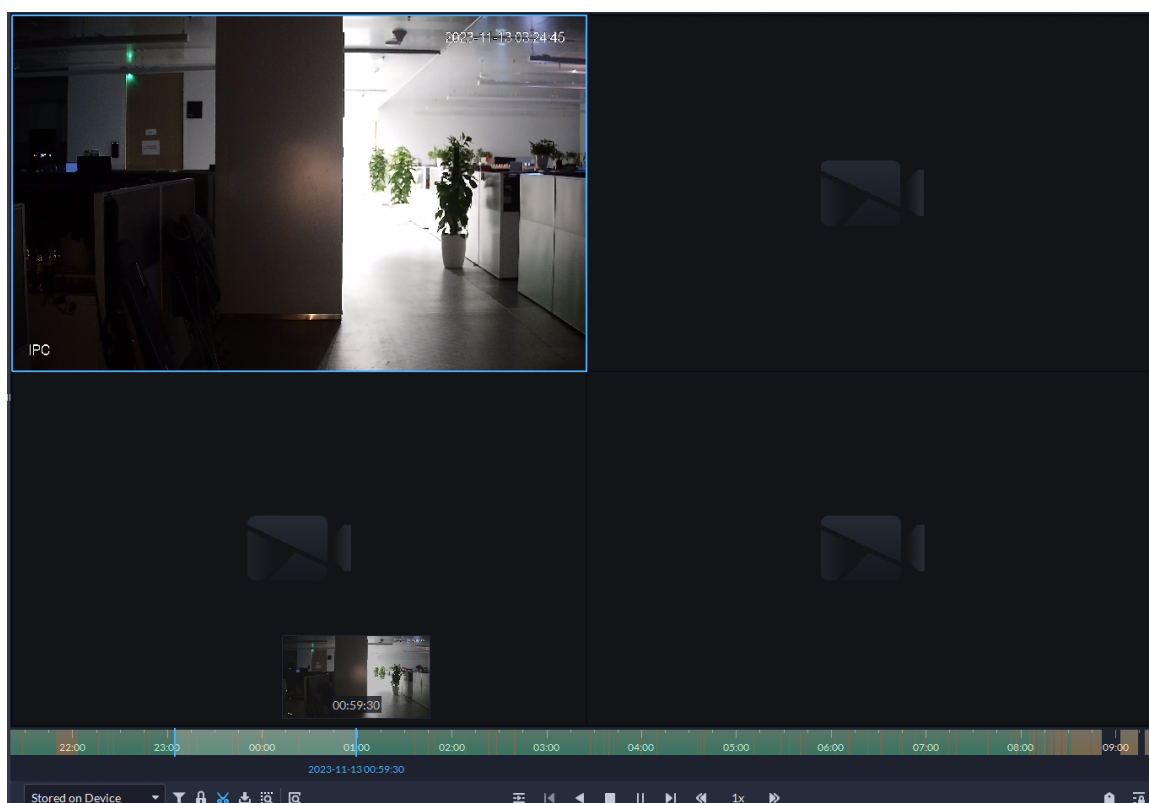


Dates with blue dot means there are videos.

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 6-31 Select a period



Step 7 Enter the password and encryption password, and then click **OK**.



You need to verify your password by default before download. You can configure whether to verify the password. For details, see "8.3.1 Configuring Security Parameters".

Step 8 Configure the parameters of the video, and then click **OK** to start the download.



The video will be downloaded to the default path configured in the local settings. For details, see "9.3.5 Configure File Storage Settings".

Table 6-10 Parameter description


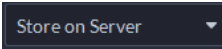

Parameter	Description
Start Time	The start and end time represents the length of video you selected. You can adjust it more specifically here.
End Time	

Parameter	Description
Transcode	The default format is .dav. You can select another format for the video.
File Format	
Select Stream	Select a stream for the video. For the same period, the main stream provides clearer image, but uses more disk space, while it is the opposite for the sub stream.
Privacy Masking	If disabled, faces in the video will not be blurred.

6.1.3.8 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

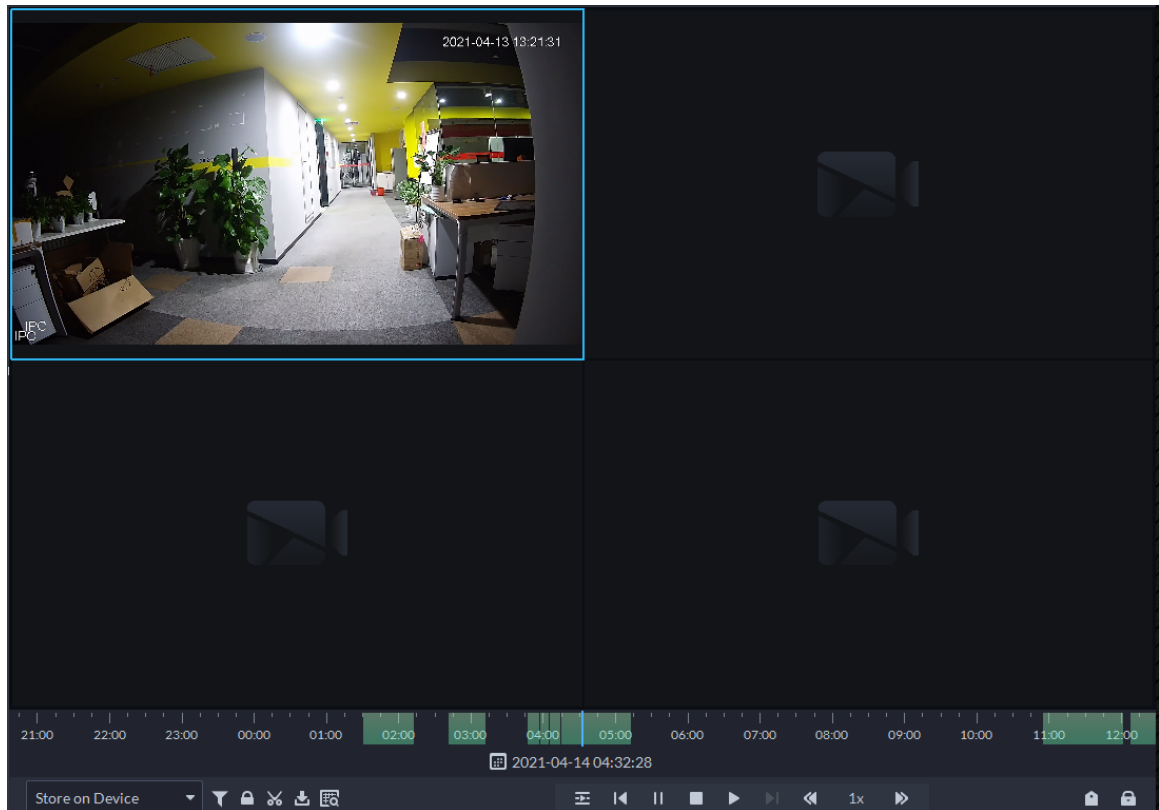
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center**.
- Step 2** Click the **Playback** tab.
- Step 3** Select a channel from the device tree, and then double-click it, or drag it to the window.
- Step 4** Select the storage path of recorded video from , and then click  to select the date.

The search results are displayed.



Dates with blue dot means there are video recordings.

Figure 6-32 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 6-33 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 the play button on the image or control bar.

The system plays search results, which are marked purple on the timeline.

Step 9 Click  to exit smart search.


6.1.4 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 "5.2 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 6-11 Function description

Function	Description
Hide Device Name	Only displays the icons of devices or channels.
Zoom in and out on the map	<p>Rotate the wheel or click  and  to zoom in and out on the map. When zooming out on the map, the same type of devices or channels will be merged together if they are near each other.</p> 
Satellite Map	If you are using an online map, you can view its satellite map.
View live video	Click Pane , select devices on the map, and then click  to view videos in batches; or click  on the map, and then select to view videos.
Playback	Click Pane , select devices on the map, and then click  to view videos in batches; or click  on the map, and then select to view videos.
View alarms	<p>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.</p> <p>Alarms will be automatically canceled after 30 s.</p>
Cancel alarms	<p>Click a device on the map, and then select .</p> <p>The alarm will also be automatically canceled after 30 s.</p>

Function	Description
Monitor a radar	<ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> ◇ : 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	<p>Select the types of devices and channels you want to display on the map.</p>  <p>You can click an alarm output channel to control whether it will output alarm signals.</p>
Visual area	<p>If a device supports visual area, click Visual Area and double-click a device on the map to show its monitoring area.</p>  <p>This function is only available on GIS maps.</p>
Initial angle	<p>If a device supports initial angle, click Initial Angle and double-click a device on the map to show the initial angle.</p>  <p>This function is only available on GIS maps.</p>
Measure distance	<p>Select Box > Length, connect two points with a line on the map (double-click to finish drawing), and then the distance between the points is shown.</p>  <p>This function is only available on GIS maps.</p>
Measure area	<p>Select Box > Area, select a region on the map (double-click to finish drawing), and then the area is measured.</p>  <p>This function is only available on GIS maps.</p>
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.

Function	Description
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.

6.1.5 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.

6.1.5.1 Configuring Video Wall

6.1.5.1.1 Page Description

Before using the video wall function, you should get familiar with what you can do on the video wall page.

Figure 6-34 Video wall

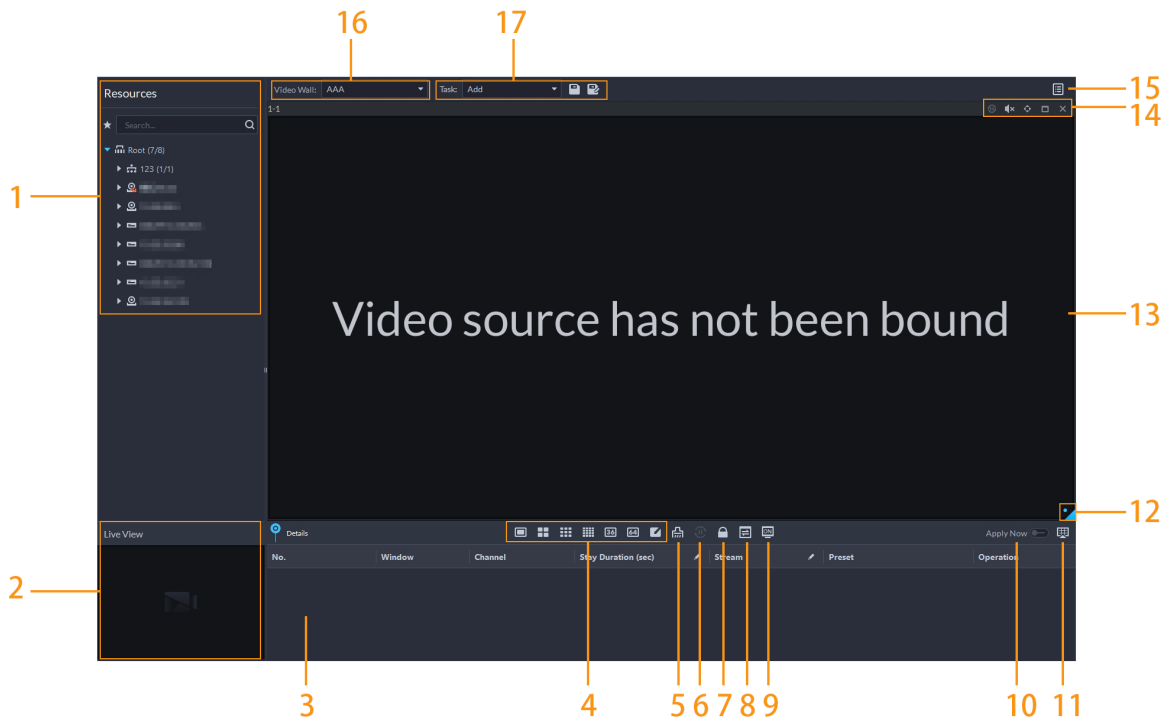









Table 6-12 Page description

No.	Function	Description
1	Device tree	<p>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.</p> <p>Click  to view channels that you have saved to favorites.</p> <p>You can enter keywords in  to search for the channels you want.</p>
2	Live view	View live videos from channels.
3	Detailed information	<p>View the channel information in a screen of the video wall.</p> <ul style="list-style-type: none"> • 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	<p>Display the real-time video, or a snapshot of the real-time video every 10 minutes of the bound channel in the screen.</p> <p>If nothing happens after operation, you can just click another screen, then click the screen you want, and then it should work properly.</p>
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.

No.	Function	Description
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.

6.1.5.1.2 Preparations

To display video on the wall, make sure that:

- Cameras, decoders and video wall are well deployed. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. For details, see "4 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**.

6.1.5.1.3 Adding Video Wall

Add a video wall layout on the platform.

Procedure


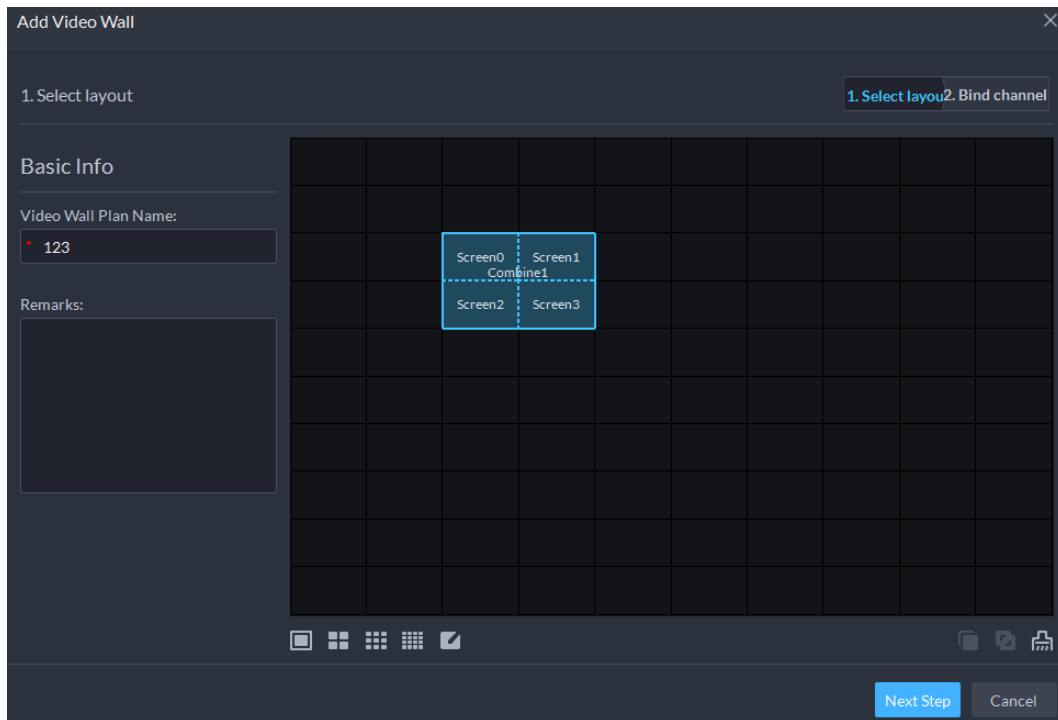




- Step 1 Log in to the DSS Client, and on the **Home** page, select **Monitoring Center** > .
- Step 2 From the **Video Wall** drop-down list, select **Add New Video Wall**.
- Step 3 Enter **Video Wall Name**, and then select a window splicing mode.

Figure 6-35 Add a video wall





- 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**.

6.1.5.1.4 Configuring Video Wall Display Tasks

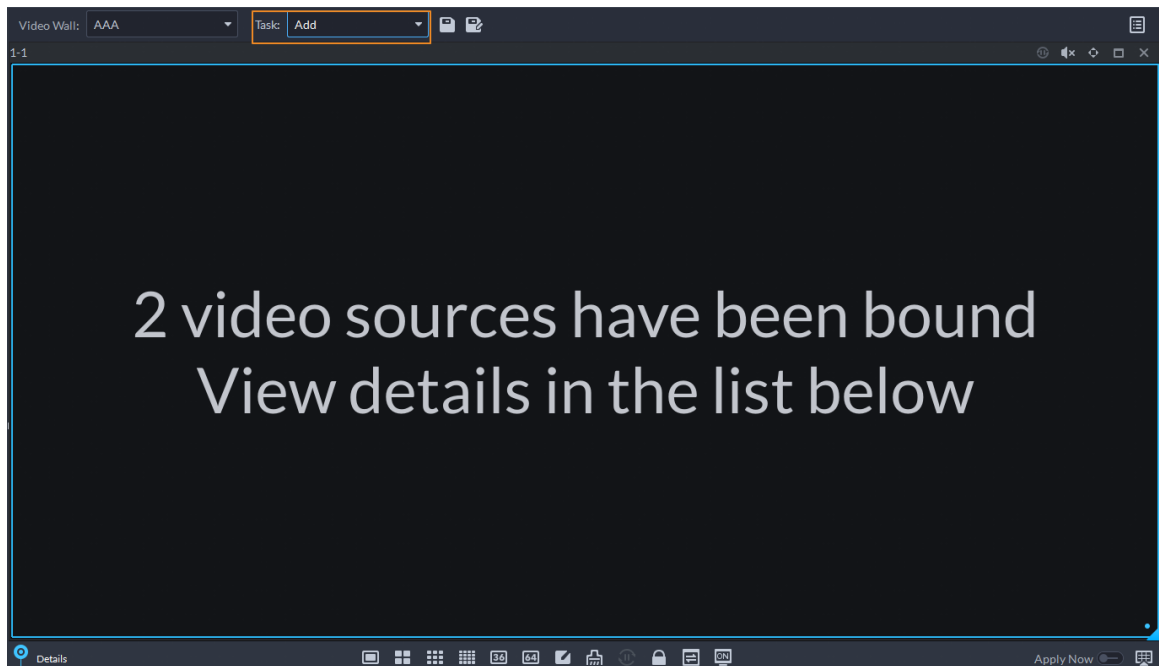
Display videos on the wall manually or in accordance with the pre-defined configuration.

Procedure

Step 1 Log in to the DSS Client, and on the **Home** page, select **Monitoring Center** > .

Step 2 In the **Task** drop-down list, select **Add**.

Figure 6-36 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 **Detail** 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.

6.1.5.1.5 Configuring Timed Plans

Procedure

Step 1 Log in to the DSS Client, and on the **Home** page, select **Monitoring Center** > .

Step 2 Click  on the upper-right corner.

Step 3 Hover over , and then select .

Figure 6-37 Set timed plan

Task Name	Start Time	End Time	Operation
25	00:00:00	23:59:59	

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.

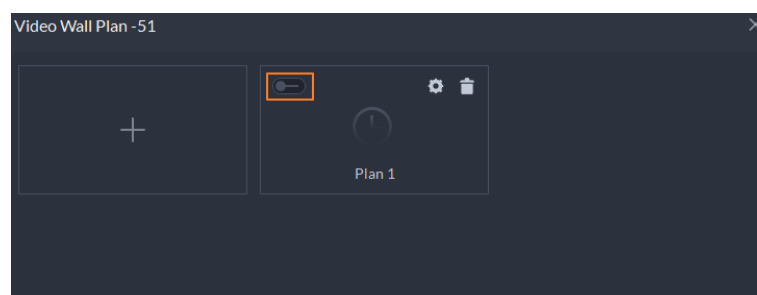
Step 6 Click **Save**.

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 6-38 Enable timed plan



- Modify plan:

- Delete plan: 

6.1.5.1.6 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.

Procedure





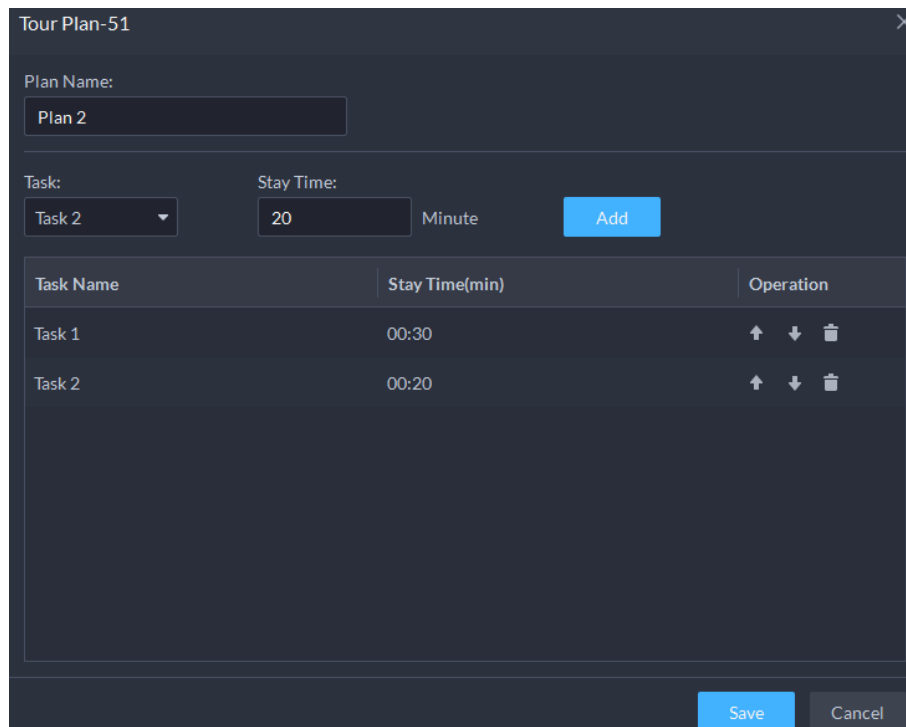
- Step 1 Log in to the DSS Client, and on the **Home** page, select **Monitoring Center** > .
- Step 2 Click  on the upper-right corner.
- Step 3 Hover over , and then select .

Figure 6-39 Tour plan



- Step 4 Enter task name, select a video task and then set stay time. Click **Add**. Repeat this step to add more tasks.





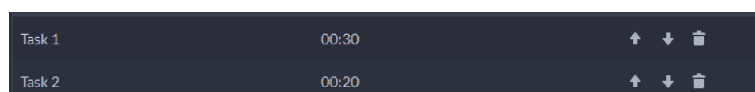

Click  to adjust task sequence; click  to delete a task.

Figure 6-40 Tour information

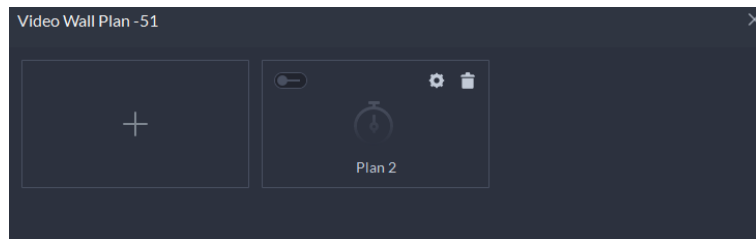




- Step 5 Click **Save**.
- Step 6 Click  to start the tour plan.



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 6-41 Enable tour plan



- Modify plan: Click .
- Delete plan: Click .

6.1.5.2 Video Wall Applications


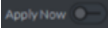
Before using the video wall function, make sure that display devices are properly connected to video wall screens.

6.1.5.2.1 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 "6.1.5.1.4 Configuring Video Wall Display Tasks".

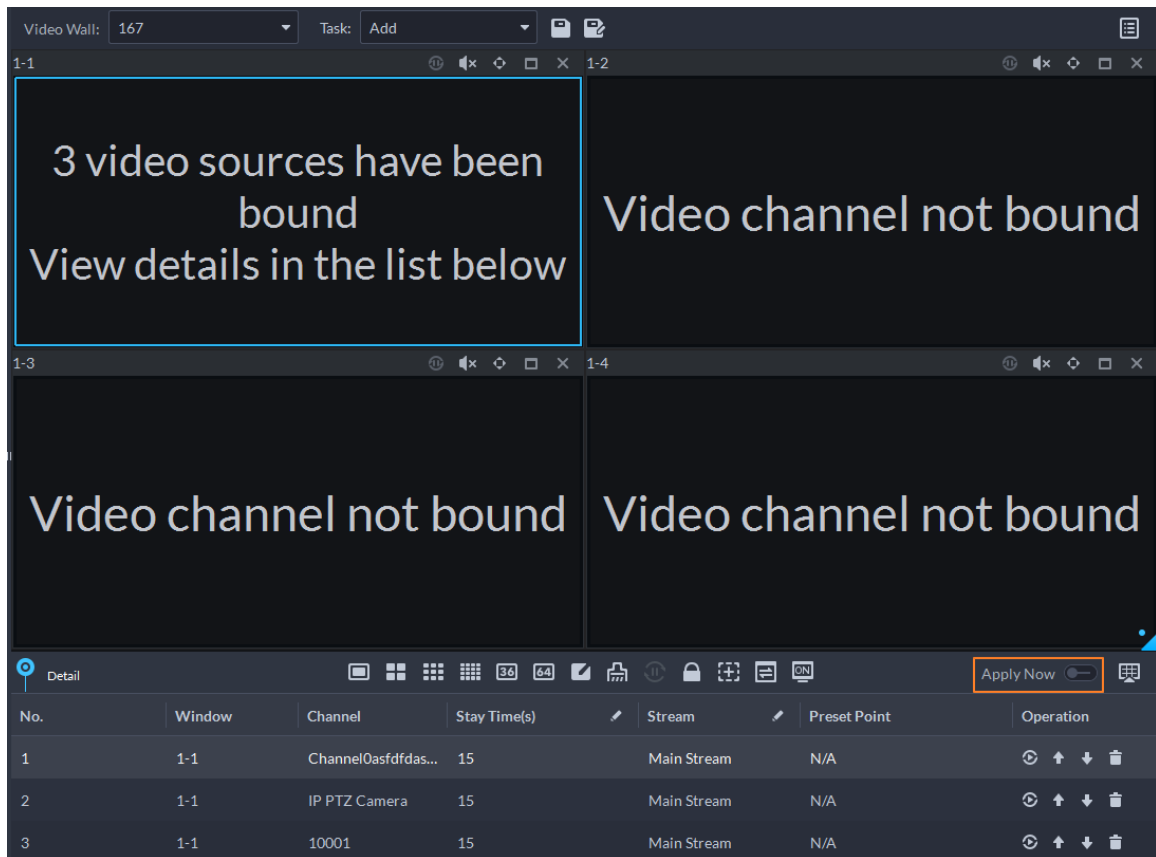
Procedure

- Step 1 Log in to the DSS Client, and on the **Home** page, select **Monitoring Center** > .
- Step 2 In the **Video Wall** drop-down list, select a video wall.
- Step 3 Click **Apply Now**  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 **Detail** section.






- A window can be bound to multiple video channels.
- The binding mode, which includes **Tour**, **Tile**, and **Inquiry**, can be set in **Local Settings** > **Video Wall**. For details, see "9.3.3 Configuring Video Wall Settings".
- For a fisheye camera, right-click it to select the installation mode for fisheye dewarping.

Figure 6-42 Bind video channel



Step 5 Select a screen, and then click **Detail** 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.

6.1.5.2.2 Video Wall Task Display




Display a pre-defined task on video wall.

Procedure

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 **Detail** to view detailed information about the screen and channel, including stream type, preset and display sequence.

6.1.5.2.3 Video Wall Plan Display

Display a pre-defined plan on video wall.



Make sure that there are pre-defined plans.




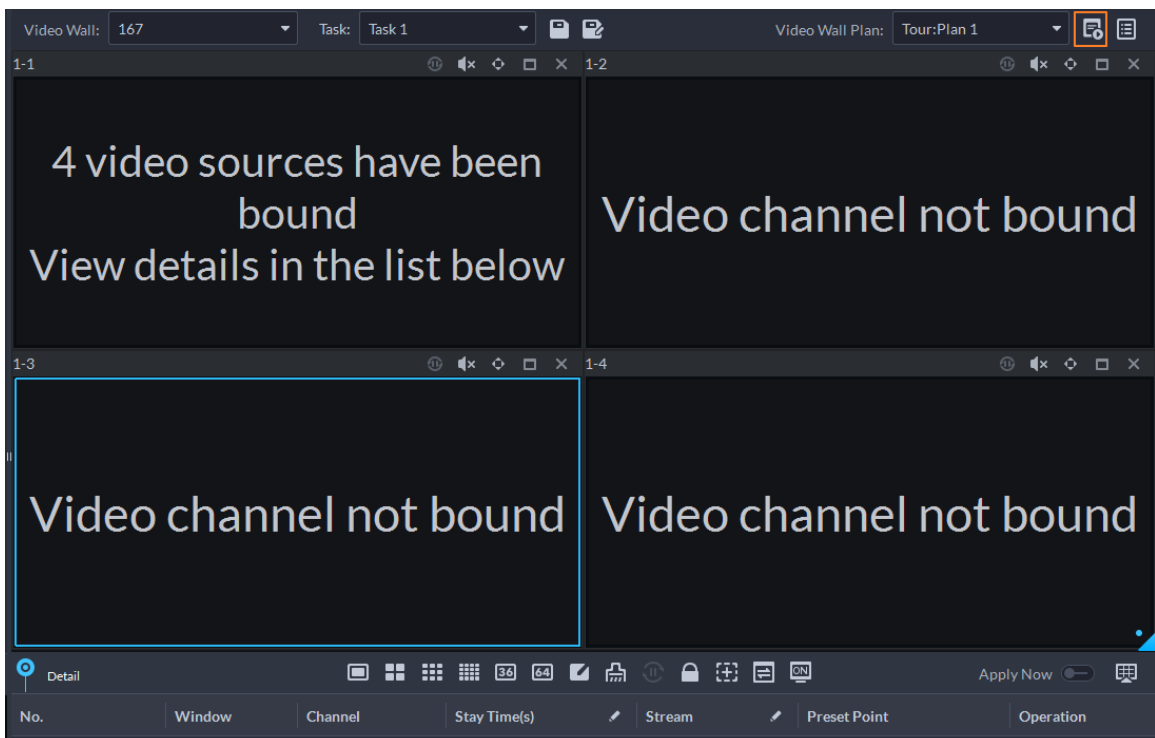
The video wall automatically works as the plans have been configured. To stop the current plan, click  on the upper-right corner of the **Video Wall** page, and then it changes to . Click  to start displaying video on wall again.

Figure 6-43 Display video wall plan



6.2 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.

Make sure that you have configured and enabled alarm events. To configure, see "5.1 Configuring Events".

6.2.1 Real-time Alarms

View and process real-time alarms.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Event Center**.

Step 2 Click .



The alarm list is refreshed in real time. To stop refreshing, click **Pause Refresh**. To continue receiving alarms, click **Start Refresh**.

Figure 6-44 Real-time alarms

Alarm Time	Alarm Category	Alarm Type	Alarm Source	Priority	Processed by	Operation
2022-07-13 18:51:41	Soft Trigger	Soft Trigger_1	jym-Channel0	High		
2022-07-13 18:51:41	Soft Trigger	Soft Trigger_1	jym-Channel0	High		
2022-07-13 18:51:41	Soft Trigger	Soft Trigger_1	jym-Channel0	High		
2022-07-13 18:51:41	Soft Trigger	Soft Trigger_1	jym-Channel0	High		
2022-07-13 18:51:41	Soft Trigger	Soft Trigger_1	jym-Channel0	High		
2022-07-13 18:51:40	Soft Trigger	Soft Trigger_1	jym-Channel0	High		
2022-07-13 18:51:40	Soft Trigger	Soft Trigger_1	jym-Channel0	High		

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.


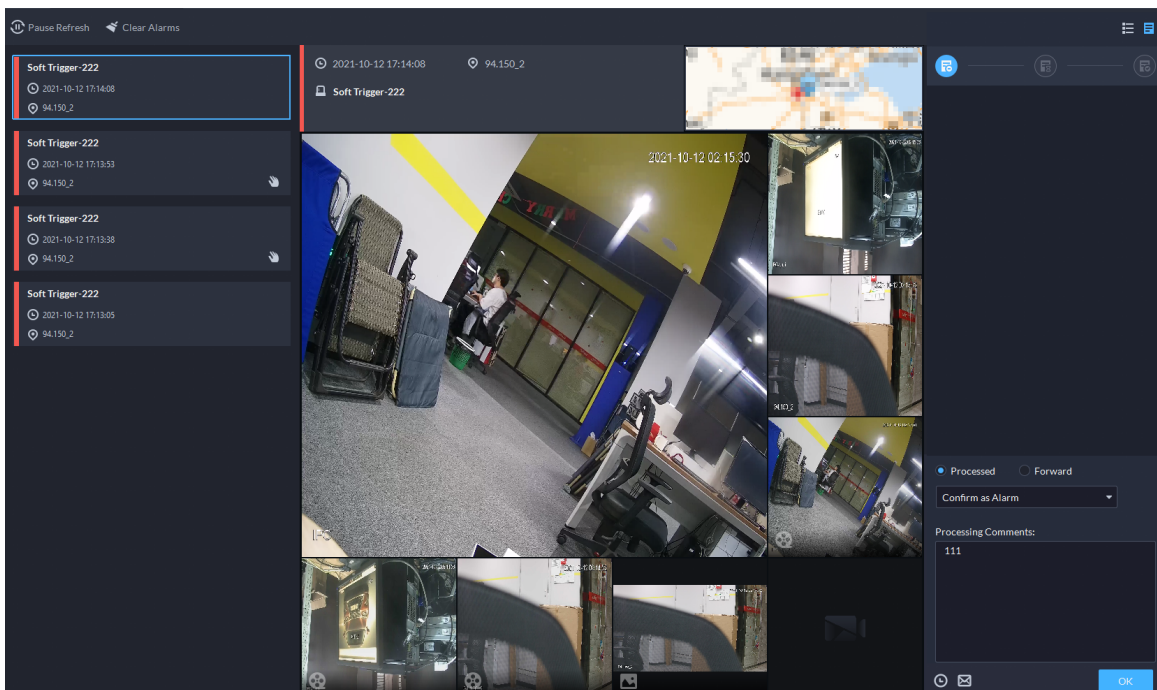
1. Click  or double-click the alarm.

Figure 6-45 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.


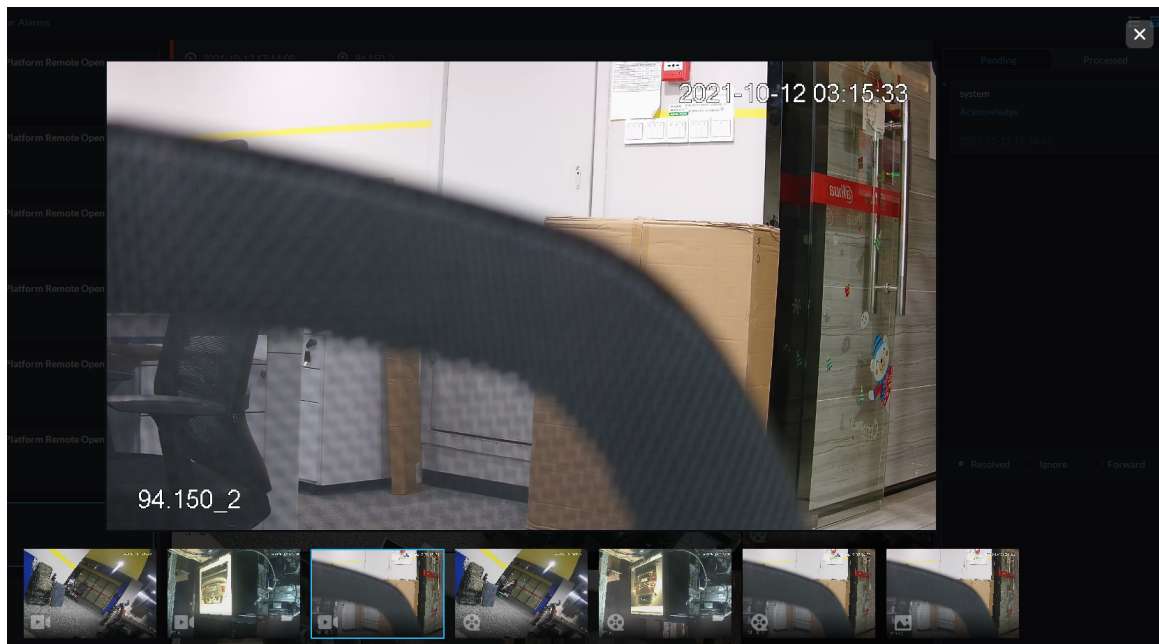
Double-click a window to view them in larger size. Click  to go back.

Figure 6-46 Alarm linkage media



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.



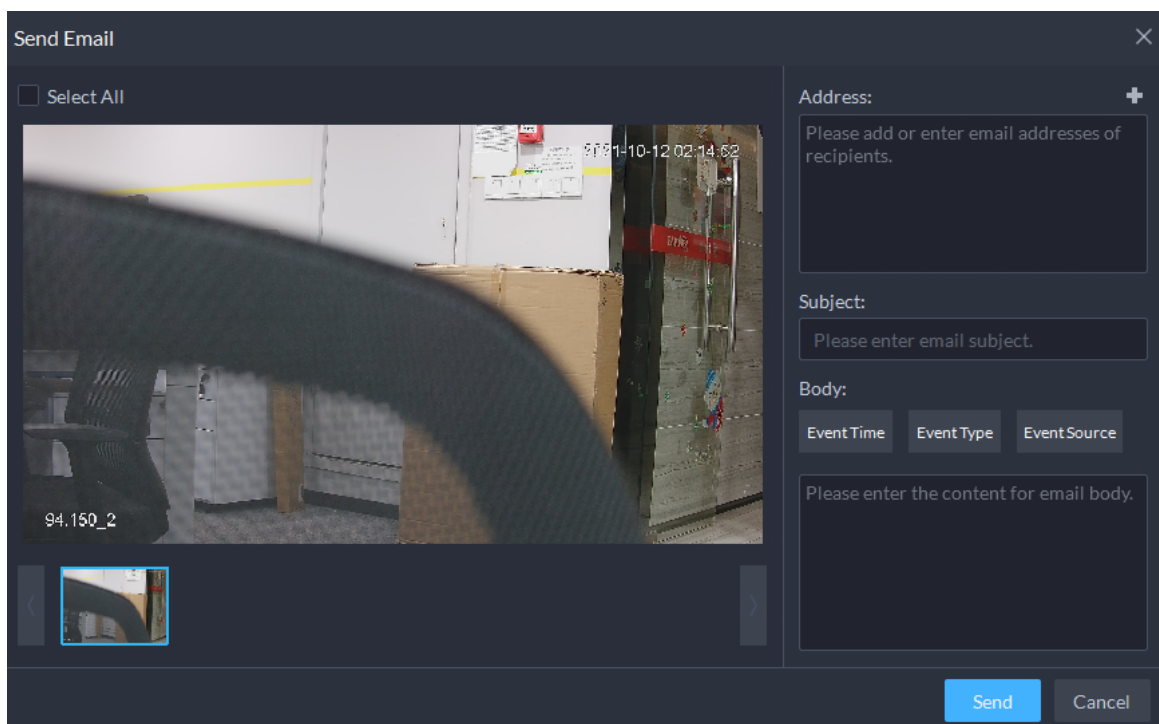

4. (Optional) Click  to disarm the alarm. This alarm will not be triggered within the defined period.
5. (Optional) Click  to send the alarm information to other users as an email. Events that are processed or forwarded can also be sent as emails.

Figure 6-47 Send email



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, and then search for it in DeepXplore.

6.2.2 History Alarms

Search for and process history alarms.

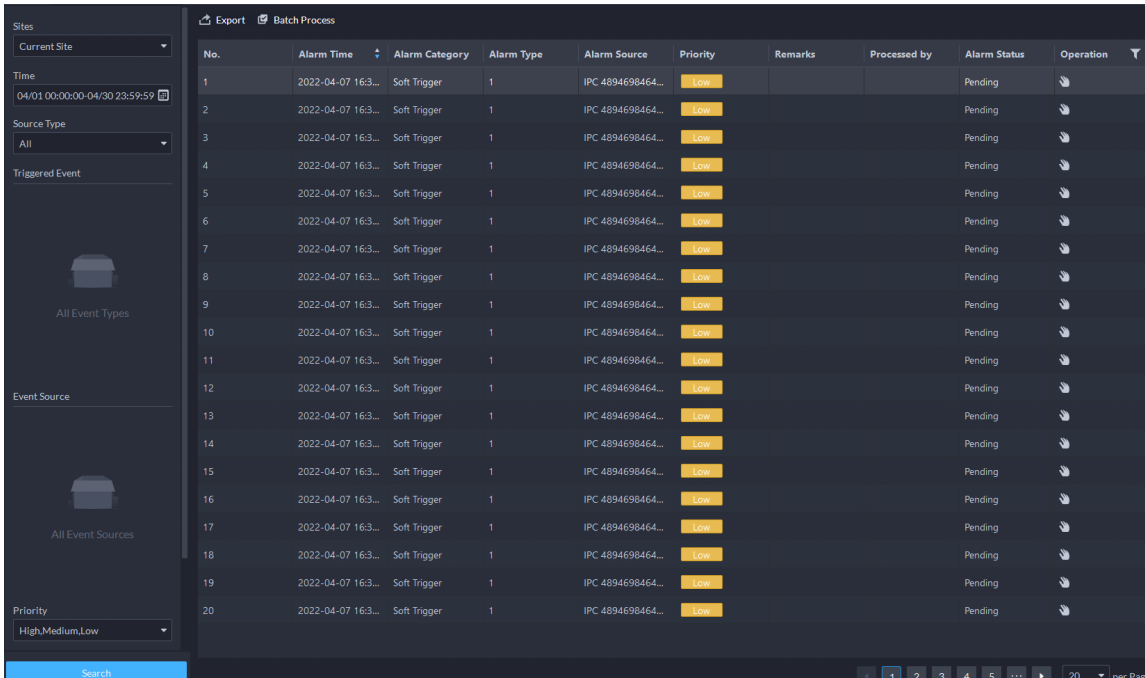
Procedure





















Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Event Center**.

Step 2 Click .

Step 3 Set search conditions, and then click **Search**.

Figure 6-48 History alarms



No.	Alarm Time	Alarm Category	Alarm Type	Alarm Source	Priority	Remarks	Processed by	Alarm Status	Operation
1	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
2	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
3	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
4	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
5	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
6	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
7	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
8	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
9	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
10	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
11	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
12	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
13	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
14	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
15	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
16	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
17	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
18	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
19	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	
20	2022-04-07 16:3...	Soft Trigger	1	IPC 4894698464...	Low			Pending	

Step 4 Claim and process alarms. For details, see "6.2.1 Real-time Alarms".



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, and then search for it in DeepXplore.

6.2.3 Alarm Controller

You can monitor and manage alarm controllers.

Prerequisites

Alarm controllers are added to the platform. See "4.2.2 Managing Device".

Procedure

Step 1 Click .

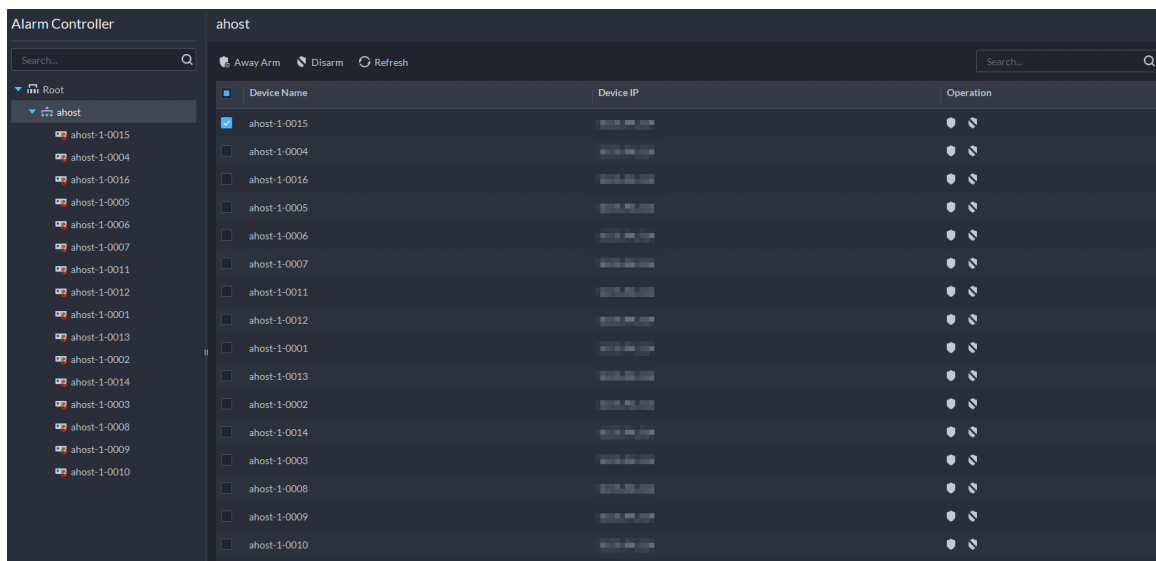
Step 2 In the device tree, click an organization.

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 6-49 Alarm controller organization



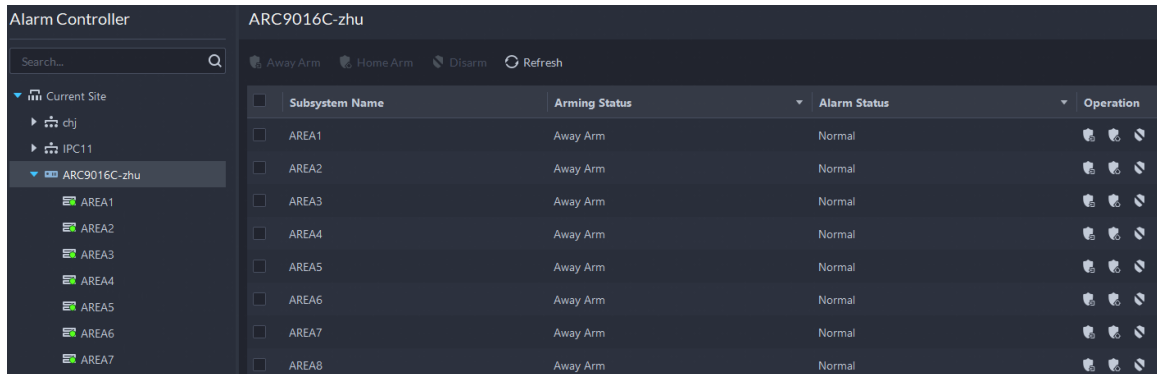
Step 3 In the device tree, click an alarm controller.

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 6-50 Subsystems



Step 4 Arm or disarm subsystems.

- : Operate on multiple subsystems.
- : Operate on one system.

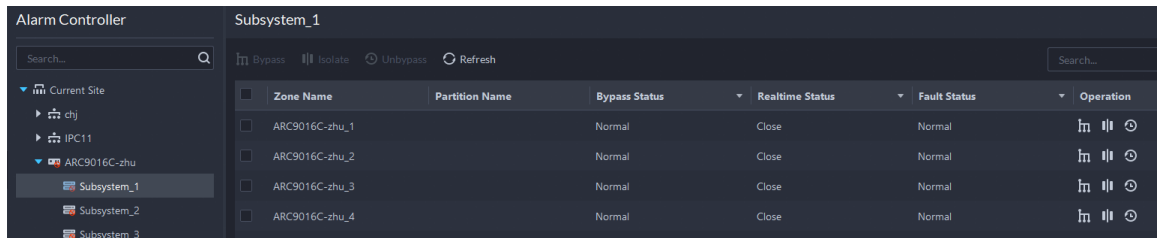


- See the user manual of the alarm controller for detailed description on each function.
- If arming failed, you can click **Force Arm** on the prompt window to arm again.

Step 5 In the device tree, click a subsystem of the alarm controller.

All zones under this subsystem will be displayed on the right.

Figure 6-51 Zone



Step 6 Bypass, isolate, or unbypass zones.

- : Operate on multiple zones.
- : Operate on one zone.



- 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.

6.3 DeepXplore

You can set multiple search conditions to view records of people, vehicle snapshots and access that you are interested in.

6.3.1 Searching for Records

In this section, you can view integrated records of people, vehicle, and access control.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **DeepXplore**.


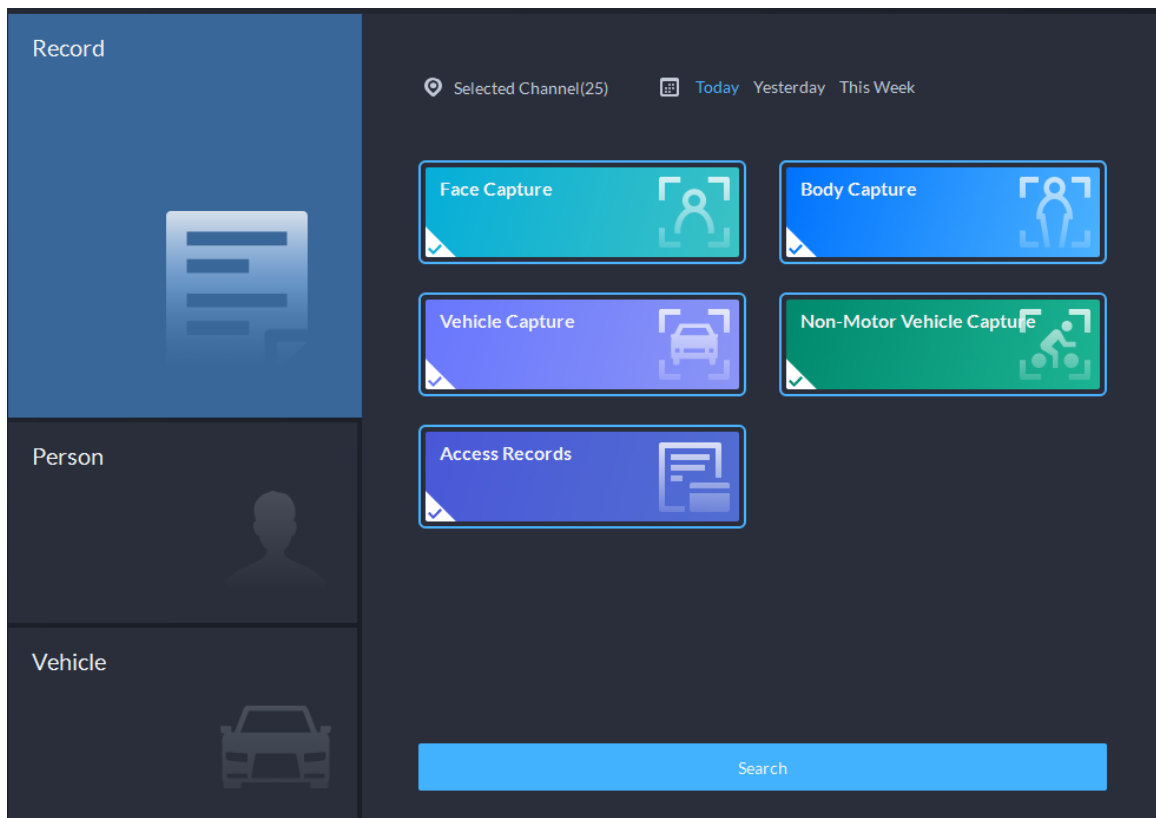
Step 2 Click , and then select **Record**.

Figure 6-52 Record search




Step 3 Set the search object, channel and time, and then click **Search**.


For the search result, you can perform the following operations.

- View details on records

Select a record, and then its details are displayed on the right, including snapshots (hover the mouse to zoom in on a portion of the snapshot), recorded videos (can be downloaded to your computer), and targets that can be further searched for (manually select a target).

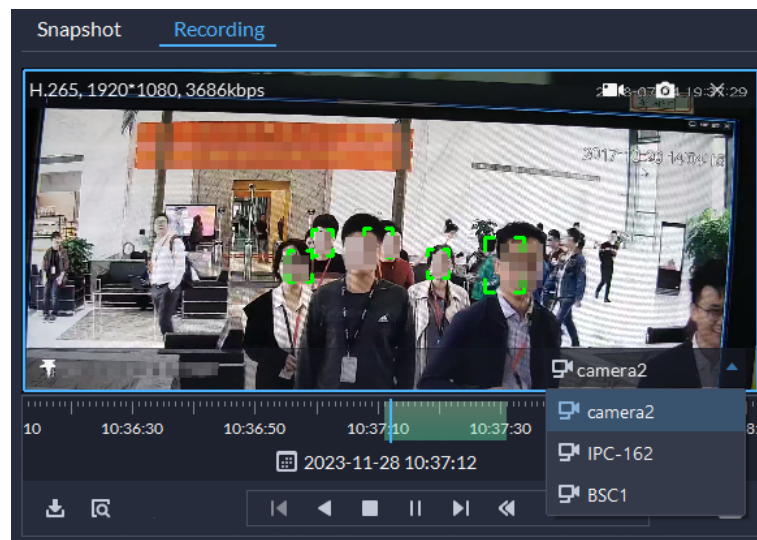
- For face images, you can hover the mouse over the small image on the right, and then click  to search for images similar to this one. The platform will compare the image you upload to the records on the selected devices, and then return results based on


the defined similarity. For body and vehicle images, the platform can only compare them to records on one device.


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.

- When viewing recorded videos and snapshots, you can select a target manually, and then search for it in DeepXplore.
- If the channel is bound to other video channels, hover the mouse on the video to view the recorded video from the bound video channels.

Figure 6-53 View recorded videos from bound video channels






- 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.



Access records cannot be deleted.

- 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  to generate a track.

6.3.2 Searching for People

Based on the defined search conditions, you can view capture records of faces, bodies and other information.

Procedure



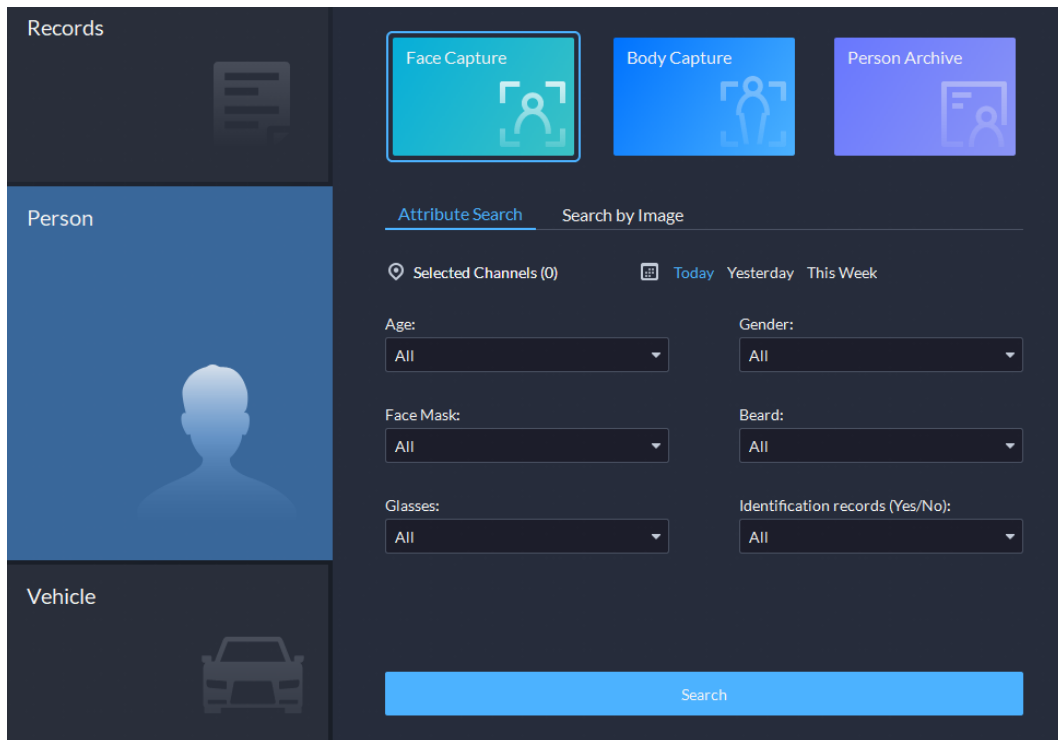
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **DeepXplore**.
- Step 2** Click , and then select **Person**.

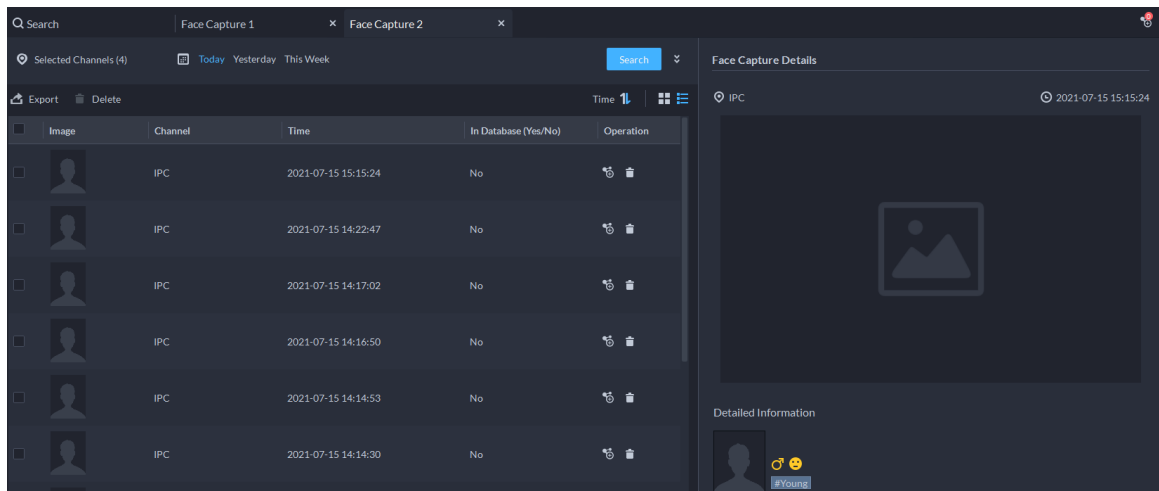
Figure 6-54 Person search



- Search object
 - ◇ **Face Capture** : Search for records in the face capture database.
 - ◇ **Body Capture** : Search for records in the body capture database.
 - ◇ **Person Archive** : Search for records in the person information database.
- Search type
 - ◇ **Attribute Search** : Search for records by the defined features such as age, gender, color of clothes, ID 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.
 - ◇ **Search by 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. For body images, the platform can only compare them to records on one device.
 - 📖
 - Only new versions of IVSS devices support displaying similarity.
 - ◇ Search channel: Select device channels of the records by clicking **Selected Channel**.
 - ◇ Search time: Select time period of the records from **Today** , **Yesterday** and **This Week**.
 - 📖
 - 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 6-55 Search results



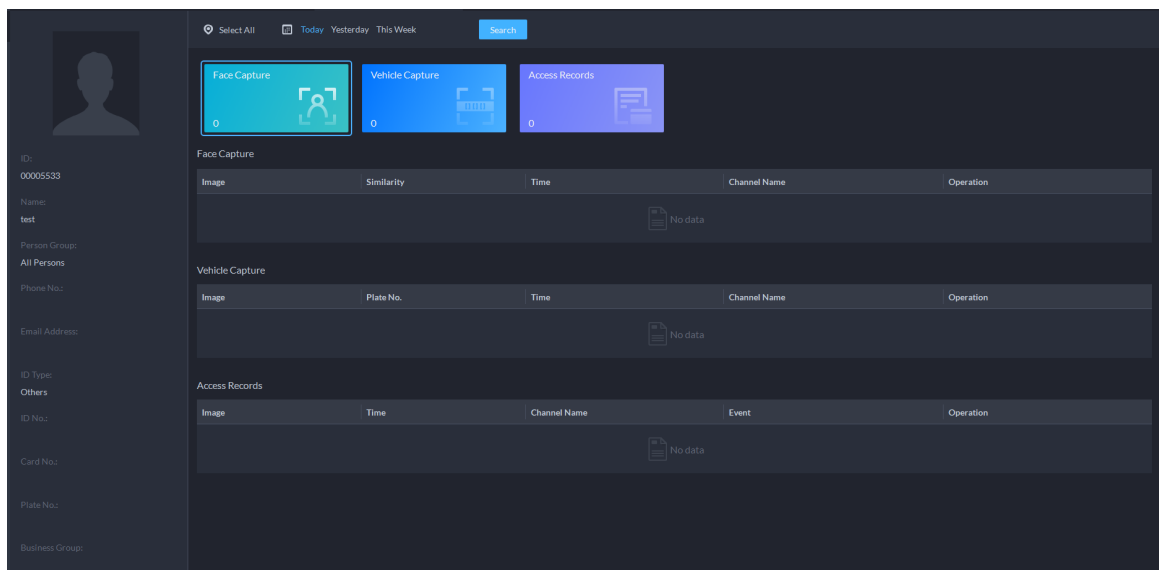
Step 4 Go back to Searching for People, and then click **Person Archive**.

Step 5 Enter the ID, name or card number of the person you want to search for.

Step 6 Double-click the record.

You can see the face capture, vehicle capture, access records and other information of the corresponding person.


Figure 6-56 Person information




For the search result, you can perform the following operations.

- View details on records

Select a record, and then its details are displayed on the right, including snapshots (hover the mouse to zoom in on a portion of the snapshot), recorded videos (can be downloaded to your computer), and targets that can be further searched for (manually select a target).

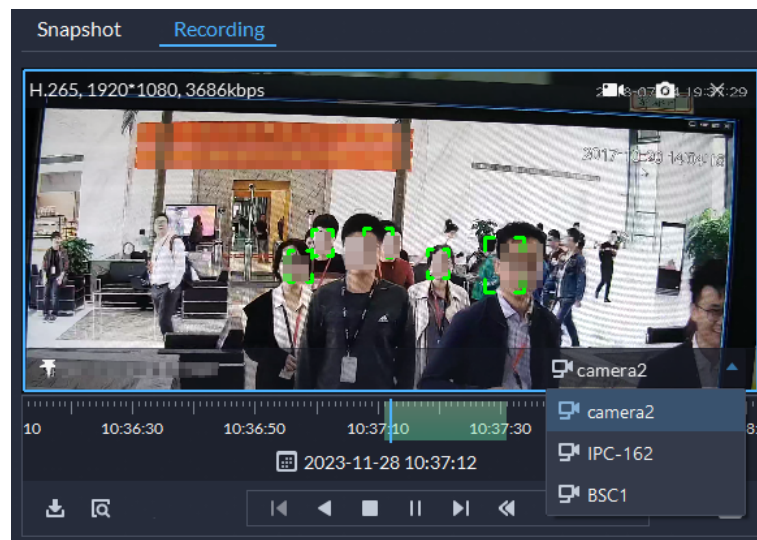
- For face images, you can hover the mouse over the small image on the right, and then click  to search for images similar to this one. The platform will compare the image you upload to the records on the selected devices, and then return results based on


the defined similarity. For body and vehicle images, the platform can only compare them to records on one device.




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.

- When viewing recorded videos and snapshots, you can select a target manually, and then search for it in DeepXplore.
- If the channel is bound to other video channels, hover the mouse on the video to view the recorded video from the bound video channels.

Figure 6-57 View recorded videos from bound video channels



- Click  to delete it one by one.
- 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  to generate a track.

6.3.3 Searching for Vehicles

Procedure



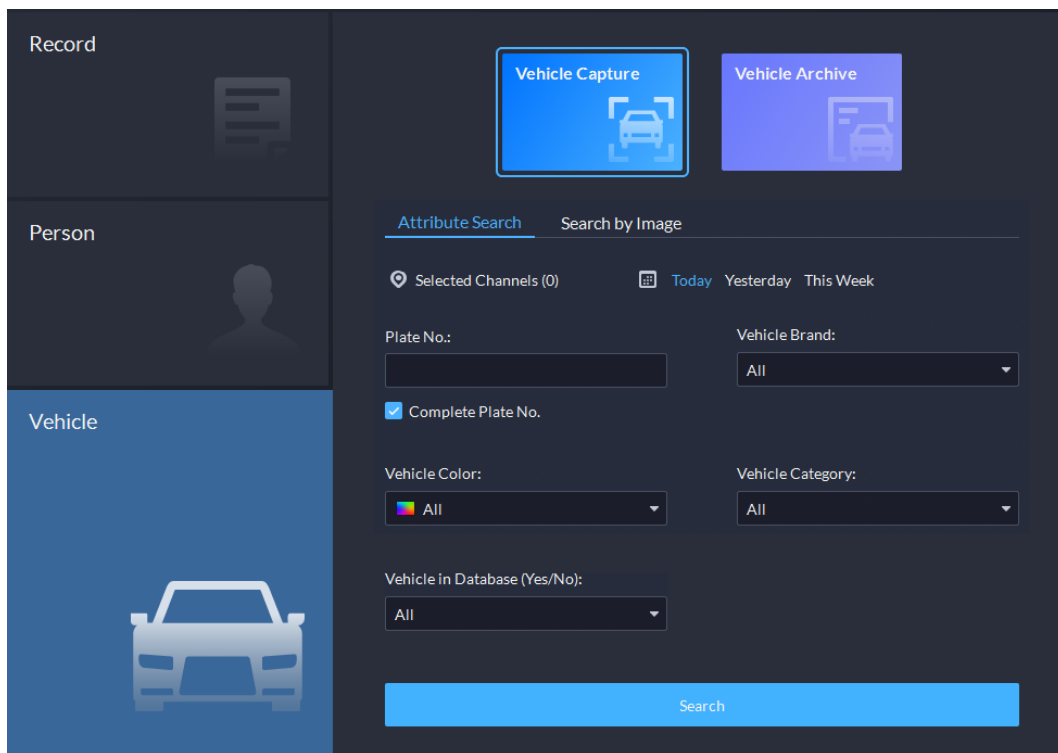
- Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **DeepXplore**.
- Step 2 Click , and then select **Vehicle**.

Figure 6-58 Vehicle search



- Search object
 - ◇ **Vehicle Capture** : Search for records in vehicle capture database.
 - ◇ **Vehicle Archive** : Search for records in vehicle information database.
- Search type
 - ◇ **Attribute Search** : Search for records by the defined attributes such as vehicle color and brand.
 - ◇ **Search by Image** : The platform compares the image you upload to the records on one device. 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.
 - ◇ Search channel: Select device channels of the records by clicking **Selected Channel**.
 - ◇ Search time: Select time period of the records from **Today** , **Yesterday** and **This Week**.



Only available for vehicle capture records.

- Search conditions: Set search conditions such as plate number (full plate number optional), vehicle brands, owner name and more to search for specific records.
- **Vehicle in Database (Yes/No)** : Select whether to search for capture records of vehicles in arming groups.

Step 3 Set the search conditions, and then click **Search**.

For the search result, you can perform following operations.

- View details on records

Select a record, and then its details are displayed on the right, including snapshots (hover the mouse to zoom in on a portion of the snapshot), recorded videos (can be

downloaded to your computer), and targets that can be further searched for (manually select a target).


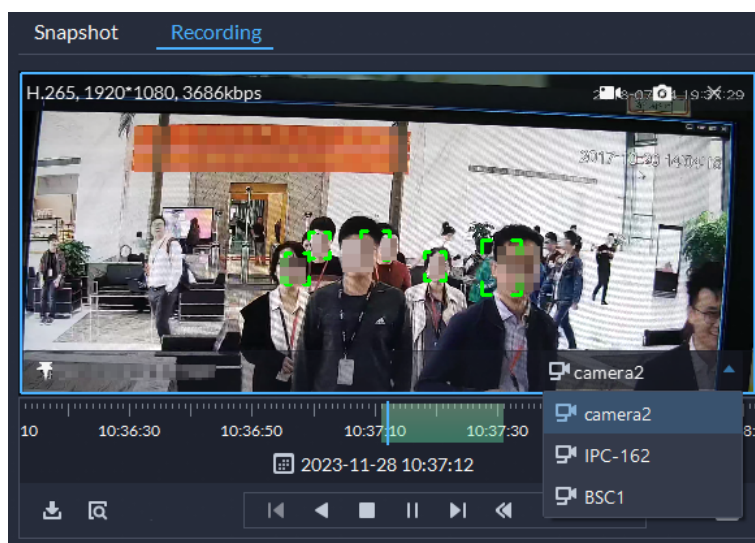





- If a license plate is recognized, click  to add the vehicle to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the vehicle is recognized.
- If the license plate is incorrectly or cannot be recognized, you can correct it manually. Then, it can be added to an arming group.
- If the channel is bound to other video channels, hover the mouse on the video to view the recorded video from the bound video channels.

Figure 6-59 View recorded videos from bound video channels




- Click  to delete it one by one.

- Access records cannot be deleted.
- 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  to generate a track.
- For vehicle archives, double-click a record to view recognition records of a license plate.

6.4 Access Management

On the **Access Management** page, you can perform operations on access control, video intercom, and visitor.

6.4.1 Access Control

6.4.1.1 Viewing Access Point

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



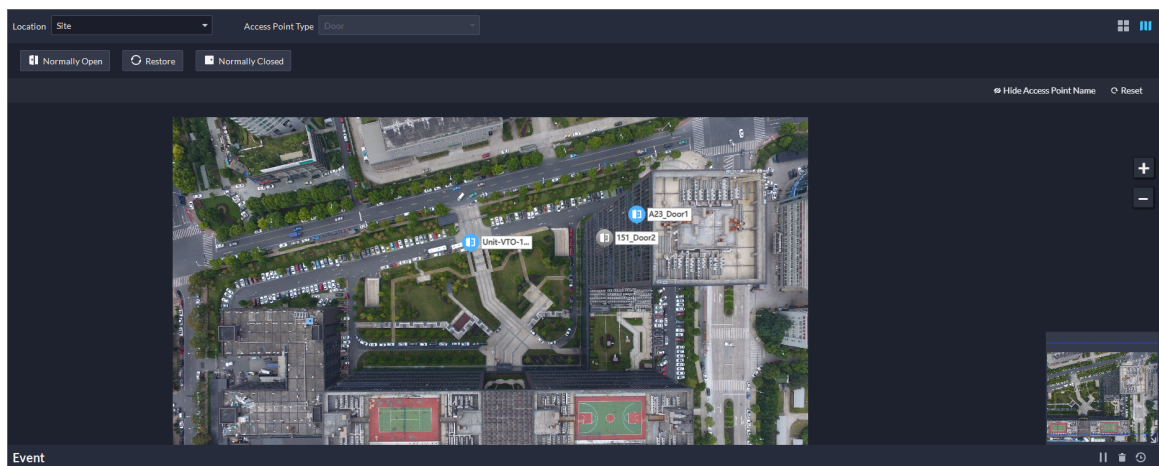
Click  or  on the upper-right corner to display access points in card view or on the map. Click the icon of an access point to view live videos from bound channels, unlock or lock the door, or make a call to it.

Figure 6-60 Access points on a map




View certain access points

On the top on the page, select a zone or access point type to display 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. You can also lock or unlock the door and make a call to it.

6.4.1.2 Viewing Live Video from Bound Channel

Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**. You can view live videos from bound channels in the following ways.

View live videos in card view



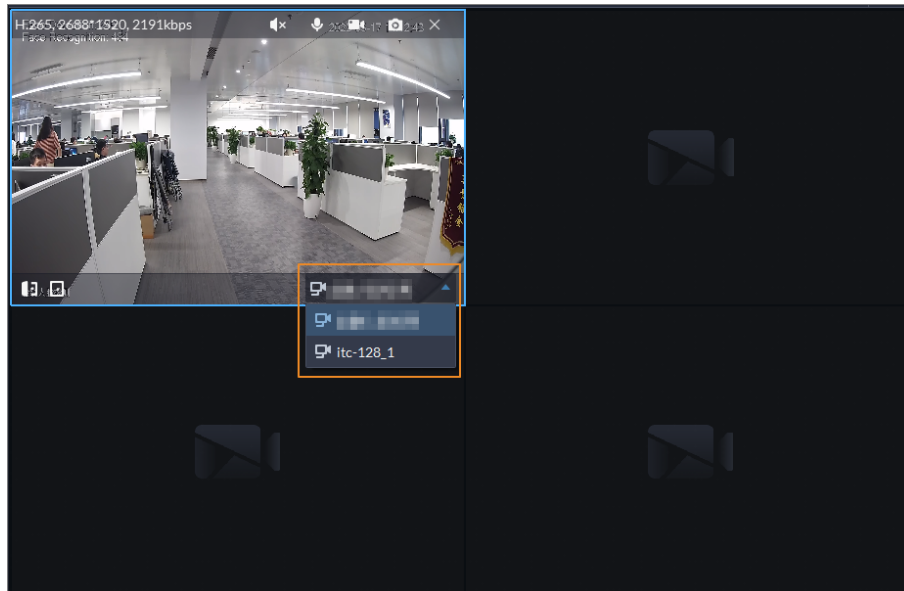
Click  to display access points in card view. Click  to view live videos. Each access point will only use one window. If more than 1 video channel is bound to the access point, you can click the drop-down list on the lower-right corner to switch between video channels.



Figure 6-61 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.

6.4.1.3 Unlocking and Locking 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  or  to unlock or lock a door channel.

6.4.1.4 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 **Normally Open**, **Restore**, or **Normally Closed** to control all the door channels at the same time.

- **Normally 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
- **Normally 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.

6.4.1.5 Viewing Real-time Event

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 "4.2.3 Binding Resources".
- Recorded videos: First, bind video channels to access points ("4.2.3 Binding Resources"). Then, select either of the 2 options: Configure recording plans for the bound video channels ("4.2.4 Adding Recording Plan"), or configure an event to link the bound video channels to record videos when a person passes ("5.1 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 the platform will display 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.


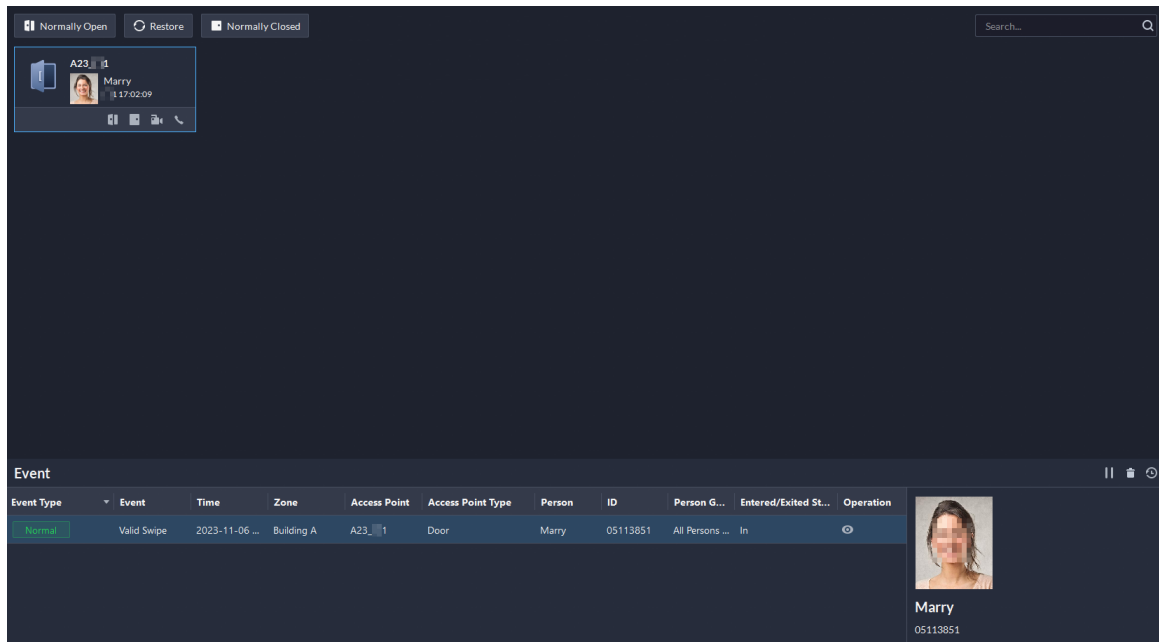
- Click  on the upper-right corner to display access points in card view. Click an event, and then its access point will be highlighted.

Figure 6-62 Highlighted access point




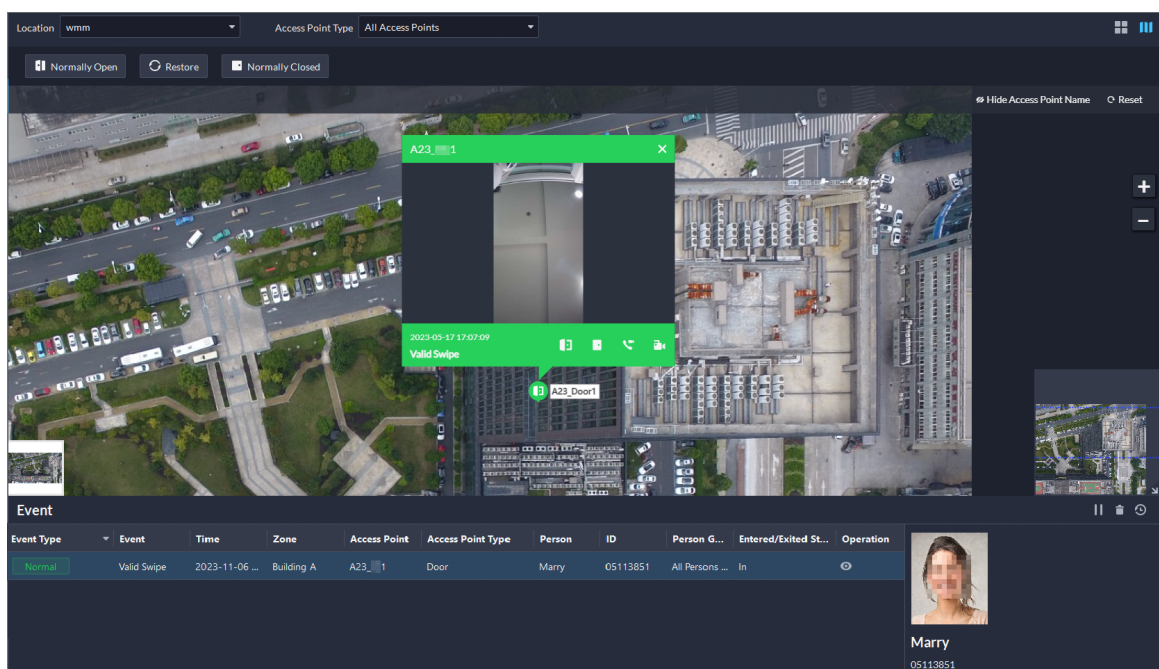



- Click  on the upper-right corner to display access points on the map. Click an event, and then its information is displayed on the map.

Figure 6-63 Highlighted on the map



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.
- : Go to the **Access Records** page.

6.4.1.6 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 6-13 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.
Key words	

Step 3 Click **Export**.

Step 4 Enter the login password, encryption password, and select whether to export images and the export range, and then click **OK**.



You can configure whether to verify the password. For details, see "8.3.1 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.

6.4.1.7 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.

- **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 2022-10-18 16:00, time of automatic synchronization is set to 04:00 every day. The device was offline on 2022-10-18 18:00, and then reconnected on 2022-10-20 16:00, then the platform, on 2022-10-21 04:00, will synchronize the records generated on the device from 2022-10-18 16:00 to 2022-10-21 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 2022-10-18 16:00 with the latest record uploaded on 2022-10-18 15:00. Before the time of synchronization, the device goes offline and online multiple times. Then on 2022-10-19 04:00, the platform will synchronize the records generated on the device from 2022-10-18 15:00 to 2022-10-19 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 by Range**, and then you can specify the time range, record type, and device.

6.4.1.8 Viewing Access Route

View the access route of a person on a map based on events.

Procedure

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 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 by a person whose information is not on the platform, access by strangers, and alarms triggered by devices.

Step 3 Click to add multiple events to the temporary records.

Step 4 Click to go to the temporary records.

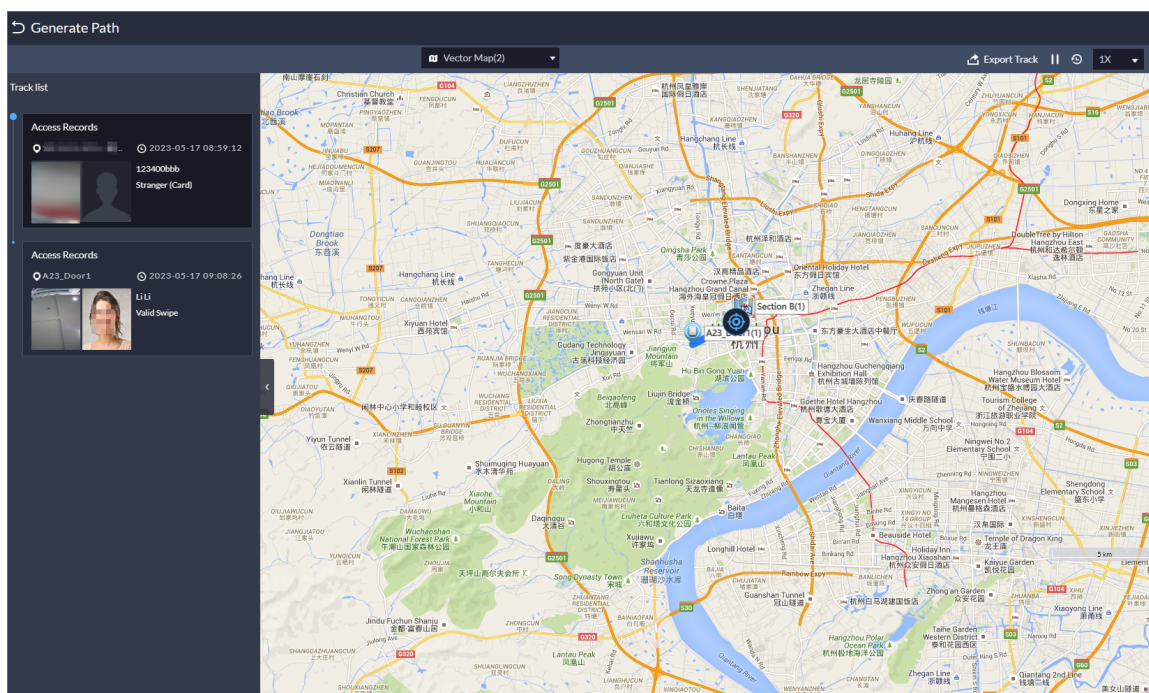
Step 5 Select the events, and then click to generate the route.

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.

Figure 6-64 Route



6.4.1.9 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 "5.5.2.5.2 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, and select whether to export images and the export range, and then click **OK**.






You can configure whether to verify the password. For details, see "8.3.1 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.

Related Operations

Manually mark the enter or exit status for people:

- On the list of person entered, exited or entered but did not exit, click  to see all access records of a person. Click  to mark a record as invalid. The invalid records can also be restored to be valid. The statistics and status of the person will change accordingly.
- On the list of person who did not exit after entering, click  to mark a person as "exited". The statistics and status of the person will change accordingly.

6.4.2 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 "5.6 Video Intercom". You can also click  to go to the video intercom configuration page.

6.4.2.1 Call Center

The platform, VTOs, VTHs, second-generation door station access controllers, and second-generation fence station access controllers can call each other.

Procedure


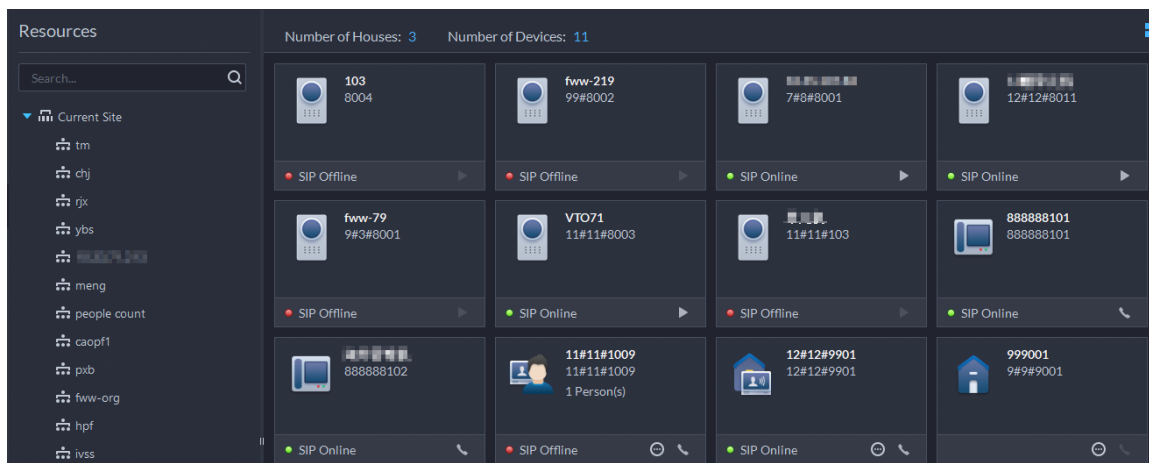

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Access Management** >  > **Call Center**.

Figure 6-65 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.





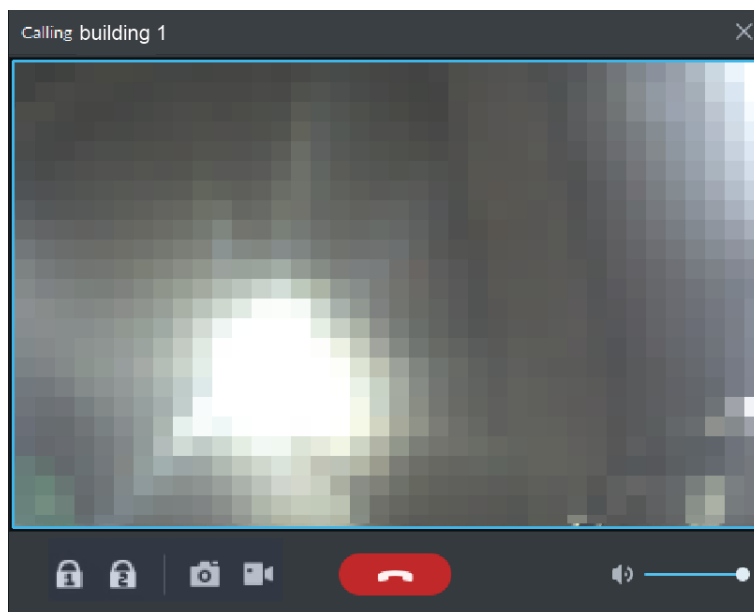

- ◇ : If VTO is connected to lock, click this icon to unlock.
- ◇ : Click this icon to capture picture, the snapshot is saved into the default directory. To change the path, see "9.3.5 Configure File Storage Settings".
- ◇ : Click this icon to start record, click again to stop record. The video is saved in default path. To change the path, see "9.3.5 Configure File Storage Settings".
- ◇ : Click this icon to hang up.

Figure 6-66 Call



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.


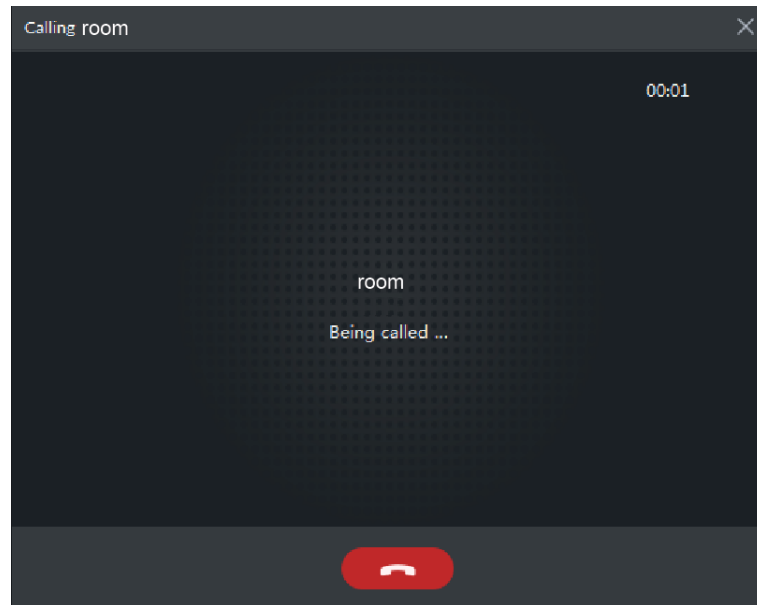

- ◇ Answer by VTH, bidirectional talk between client and VTH. Press  to hang up when you answer the call.
- ◇ If VTH fails to answer in 30 s, hangs up or is busy, then it means the call is busy.

Figure 6-67 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.


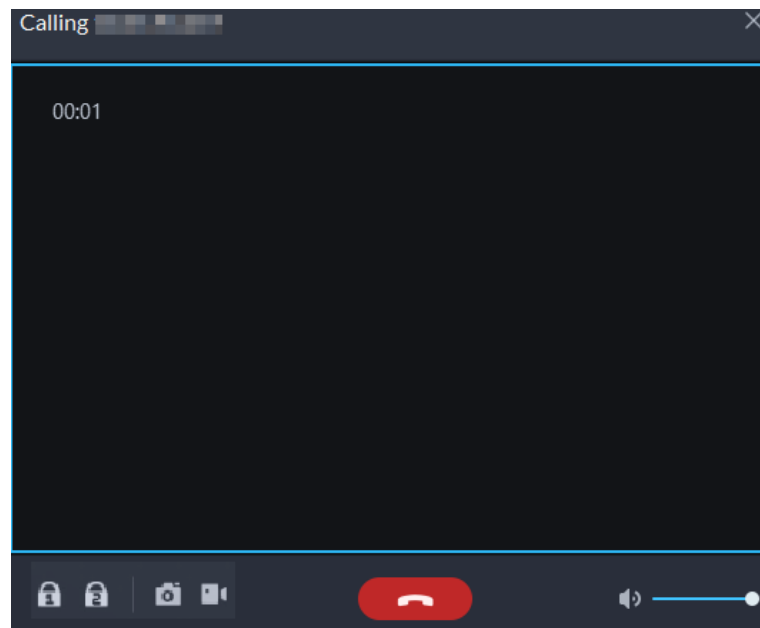
- ◇ Answer by the device, bidirectional talk between client and the device. Press  to hang up when you answer the call.
- ◇ If the device fails to answer over 30 s, busy or hang up directly, then it means the call is busy.

Figure 6-68 Calling



- Call from VTO to the platform

When a VTO calls, a window pops up.




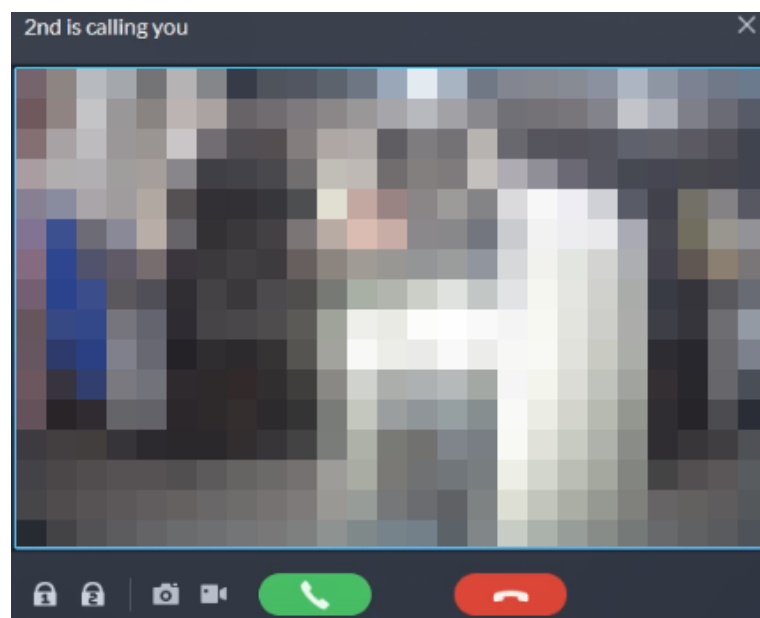


- ◇ : Unlock the door if the VTO is connected to a door.
- ◇ : Answer the call.
- ◇ : Hang up.

Figure 6-69 VTO Call



- 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.



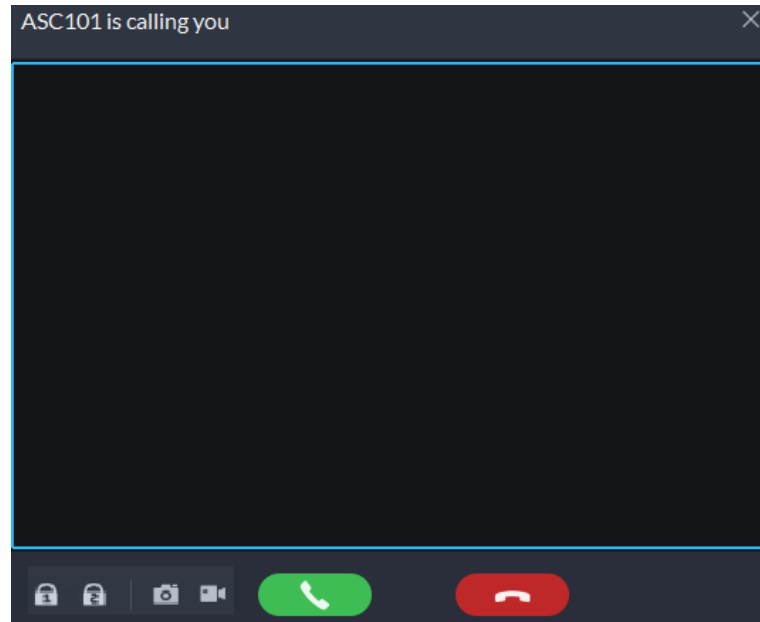
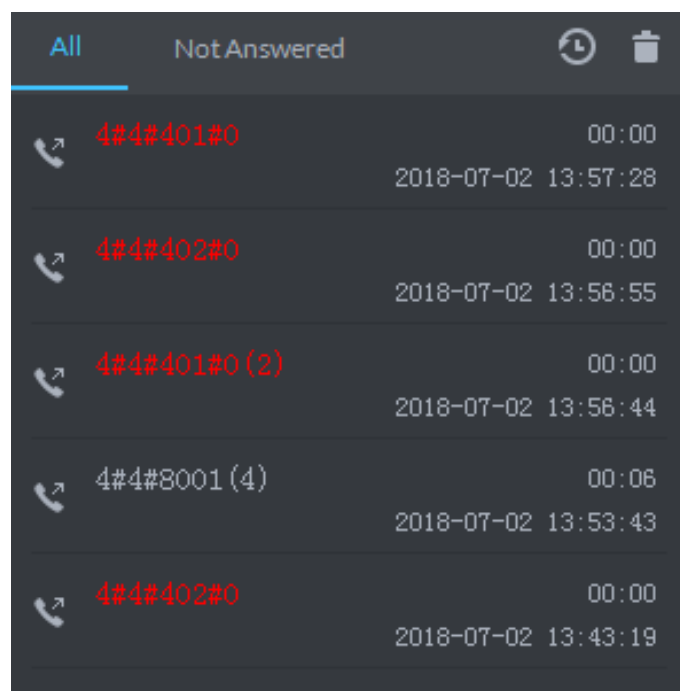
- When an access control device that supports video intercom is calling the platform
The client pops out the dialog box. Click  to talk with the device.
Click  to hang up.

Figure 6-70 Call from an access control device that supports video intercom



- 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.



Figure 6-71 Call records



6.4.2.2 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 **Schedule 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.

6.4.2.3 Video Intercom Records

Search for and view call records.


Procedure

- Step 1 Log in to the DSS Client. On the **Home** page, click  > **Access Management** >  > **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.

6.4.3 Visitor Application

After visitor information is registered, the visitor can have access permission. Access permission is disabled after the visitor leaves.

6.4.3.1 Preparations

- You have configured the deployment of the video intercom devices, access control devices and entrance and exit device. For details, see the corresponding user's manual.
- You have configured the basic configuration of the platform. For details, see "4 Basic Configurations".
- Make sure that you have configured the visitor configuration before application. For details, see "5.7 Visitor Management". You can also click  **Visitor Configuration** to go to the video intercom configuration page.

6.4.3.2 Visitor Appointment

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



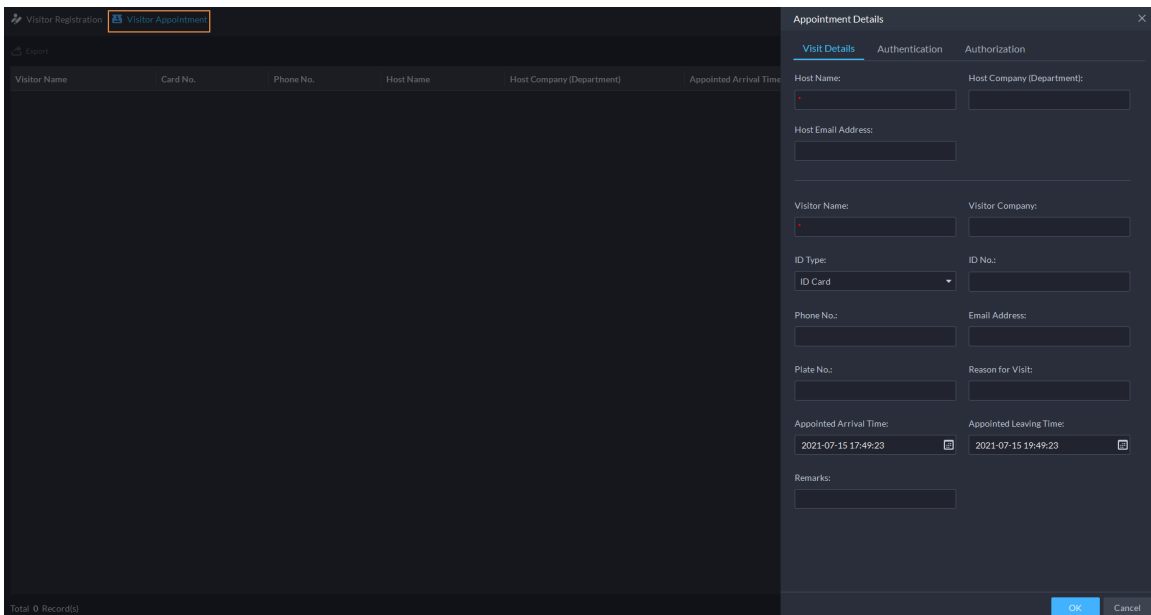



- Step 1** Log in to the DSS Client. On the **Home** page, click  > **Access Management** >  > **Visitor Management**.
- Step 2** Click **Visitor Registration**.
- Step 3** Click the **Visitor Details** tab, enter the information of the visitor and the one to be visited.

Figure 6-72 Visitor details




Click  in the appointment list to enter the **Visitor Details** tab.

- Step 4** (Optional) Click the **Authentication** tab, select the room number to be visited, and then click **Generate** to generate the QR code of the pass.



You can click  to download the QR code, and click  to send it to the visitor by email.

- Step 5** Click **OK**.

6.4.3.3 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 card swipe or face recognition.

Procedure

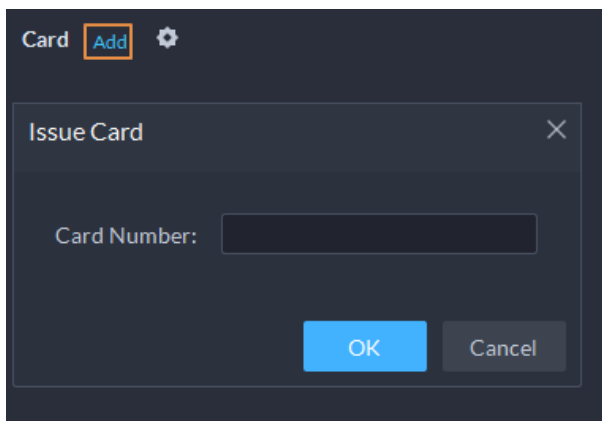
- Step 1** Log in to the DSS Client. On the **Home** page, select  > **Access Management** >  > **Visitor Management**.
- Step 2** (Optional) Click the **Authentication** tab, and then set authorization information.
1. Select the room number.
 2. Issue cards.

You can issue cards by entering card number manually or by using a card reader. A card number is 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** next to **Card**, enter the card number, and then click **OK**.

Figure 6-73 Issue card



- Issue card by using a card reader


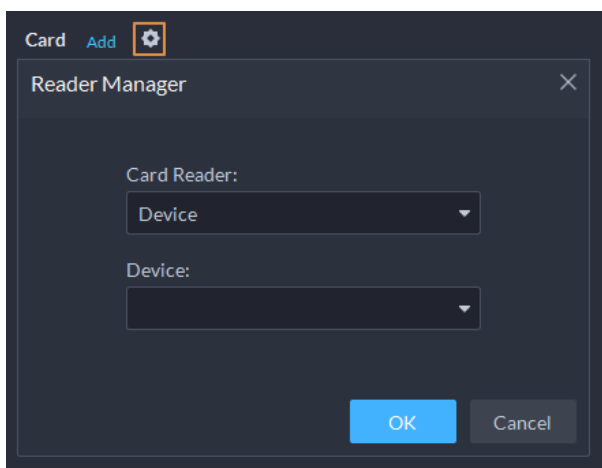
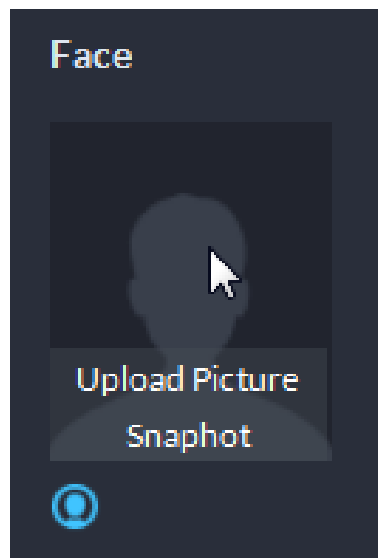
Click , select a card reader or device, and then click **OK**. Swipe card through the reader or device, and then a new card will be issued.

Figure 6-74 Reader manager





3. Set face picture. Position your face in the snapshot area, and click **Upload Picture** to select a picture or click **Snapshot** to take a photo.

Figure 6-75 Take a face photo



4. Click **Generate** to generate a QR code for the pass.

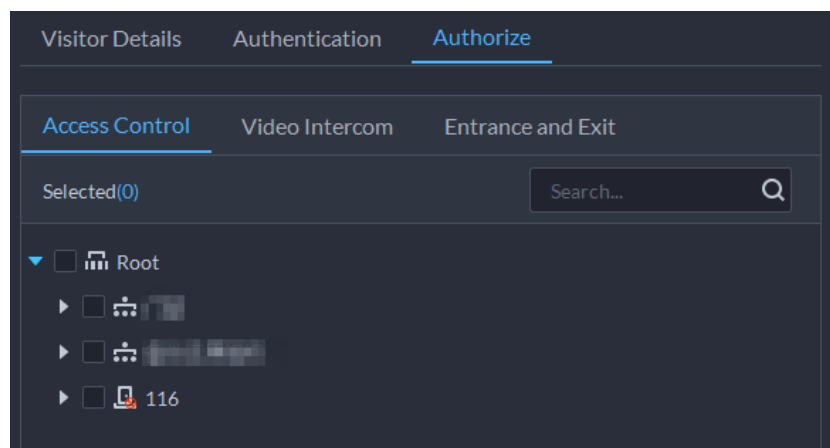
You can click  to download the QR code, and click  to send it to the visitor by email.

- Step 3** Click the **Authorize** 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.


Figure 6-76 Authorize



- Step 4** Click **OK**.

Related Operations


- End the visit.

Click  to end a visit.

- View card swiping records.

Click the **Card-swiping Record** tab, or click  in visitor record to view visitor card swiping records.



- Cancel the appointment.

Click , and cancel the appointment as the screen instructs.

6.4.3.4 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 Management**.

Step 2 Find the appointment record of the visitor, and then click .

Step 3 Click **OK** to remove access permission.

If you have issued a card to a visitor, make sure the visitor returns the card before leaving.

6.4.3.5 Visit Records

Search for visit records, and view visitor details and card swiping records.


Procedure


Step 1 Log in to the DSS Client. On the **Home** page, click  > **Access Management** >  > **Visitor Record**.

Step 2 Set search conditions, and then 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 3 Click  to view visitor details and card swiping records.

6.5 Parking Lot

You can monitor vehicles that enter and exit in real time, view vehicle information, and search for on-site vehicle, exit vehicle and snapshot records.

6.5.1 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 **Please click to select the 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 6-77 Monitor entrances and exits

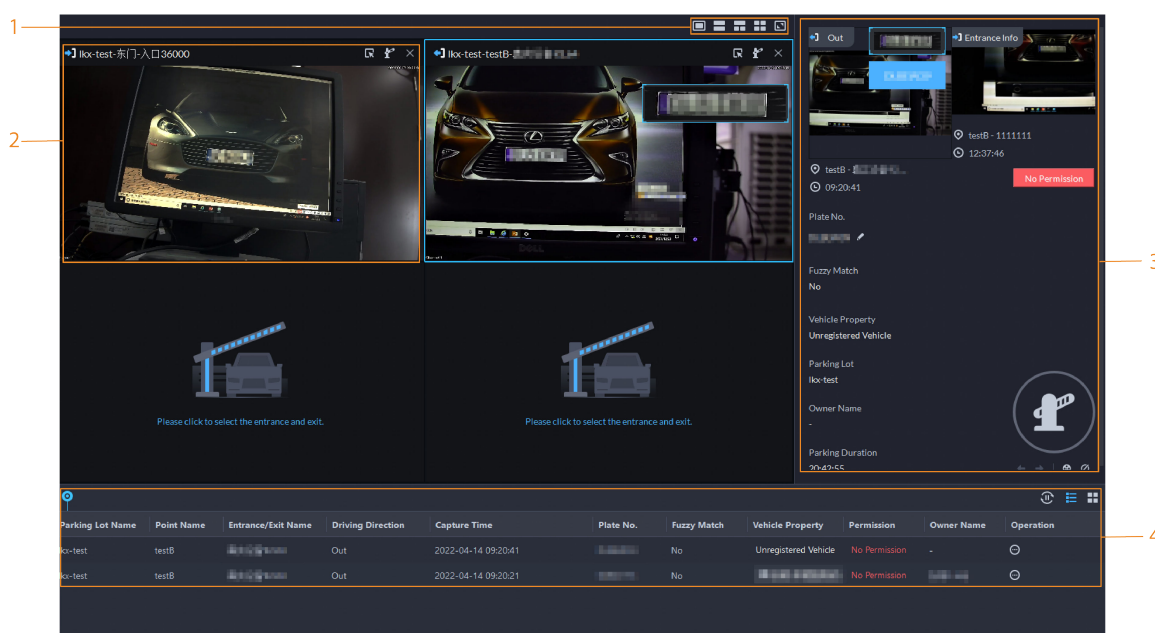









Table 6-14 Page description

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	<p>The real-time video of an entrance or exit point.</p> <ul style="list-style-type: none"> Click  to open the real-time video of another entrance or exit point in the window. Click  to open the barrier for vehicles. <ul style="list-style-type: none"> ◇ 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 leaving. This operation will not generate an enter or leave record. ◇ 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.
3	<p>Displays records of barriers not opened.</p> <ul style="list-style-type: none"> Click  to open the barrier for the vehicle. If the plate number is incorrect, you can click  to manually edit it. Click  to view the recorded video from the corresponding channel.

No.	Description
4	<p>All entrance and exit records.</p> <ul style="list-style-type: none"> • : Pause or resume refreshing the entrance and exit records. • : View the details and recorded video of a record.

6.5.2 Searching for Records

Search for entry and exit records, forced exit records, and snapshot records.

6.5.2.1 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 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 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.
- For the dual camera mode, click each channel to view the information it captured.
- 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 the then export all records according to the on-screen instructions.
- Click  and then select the items to be displayed.

6.5.2.2 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 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 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.

For the dual camera mode, click each channel to view the information it captured.

- 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 the then export all records according to the on-screen instructions.
- Click  and then select the items to be displayed.

6.5.2.3 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 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 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.

For the dual camera mode, click each channel to view the information it captured.

- 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 the then export all records according to the on-screen instructions.
- Click  and then select the items to be displayed.

6.5.2.4 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 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 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. For the dual camera mode, click each channel to view the information it captured.
- 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.

6.6 Intelligent Analysis



View real-time and history people counting data, heat maps, and number of people in an area.

6.6.1 People Counting

View the real-time and historical people count from all the devices in a people counting group.


6.6.1.1 Real-time Count

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click  > **Intelligent Analysis** >  > **Real-time Count**.

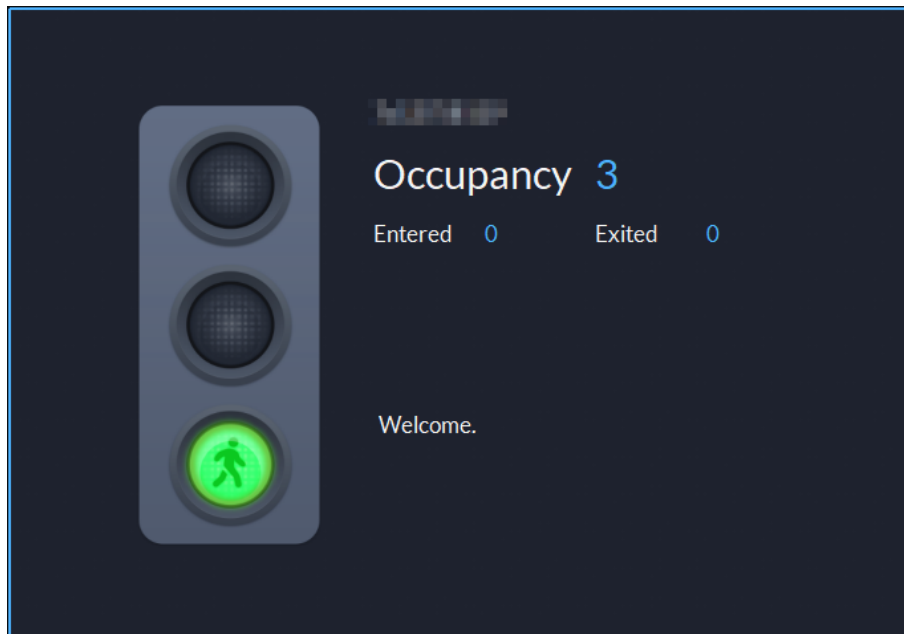
Step 2 Double-click a group or drag it to a window on the right to display its real-time data.




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 overlimit threshold.
 - ◇ Yellow light: Crowded threshold \leq occupancy $<$ overlimit threshold.
 - ◇ Green light: Occupancy $<$ normal threshold.

Figure 6-78 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 6-79 Edit the content and data

Step 5 Click **OK**.

6.6.1.2 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.

Figure 6-80 Historical people counting data



Related Operations

- 

: 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.

6.6.2 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 "4.2.2.5.2 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 week.

- 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.

6.6.3 In-area People Counting

View statistics on the number of in-area people.

Procedure

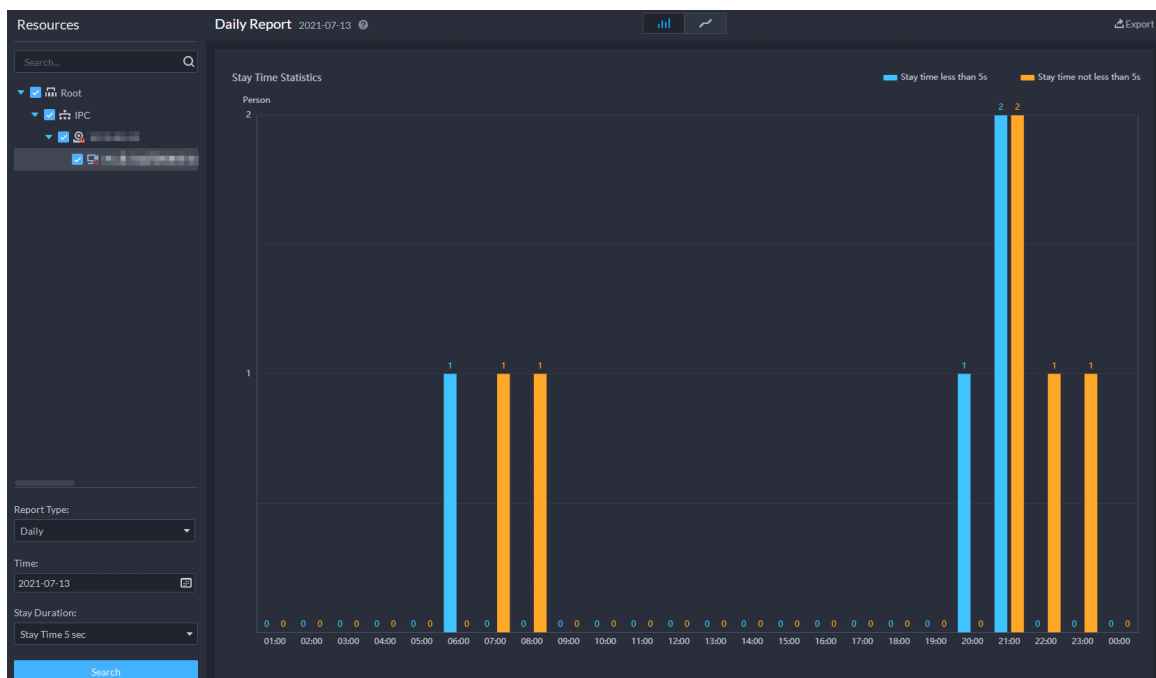
Step 1 Log in to the DSS Client. On the **Home** page, click  > **Intelligent Analysis** > **In Area No. Analysis**.

Step 2 Select a channel and configure the search settings, and then click **Search**.



If a device is offline, it will upload data within the past 24 hours to the platform when it is online again.

Figure 6-81 In-area people number statistics



Related Operations




- **Change the display format of the data.**
- **Export** : Export the data to your PC.

6.7 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.

6.7.1 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** or **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 jump to corresponding pages for more information.
- Select **Resource Monitoring > Device Status**. Click a device type, and then the status of all the devices are 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. Click  to view the RAID information of the hard disks.
 - ◇ **History Info** : Displays alerts occurred in the past 7 days and logs of the current day. Click **View All** to view all information.

6.7.2 Maintenance Management

You can view and process alerts, and analysis reports of the system running situation.

6.7.2.1 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.

6.7.2.2 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.

7 General Application

7.1 Target Detection

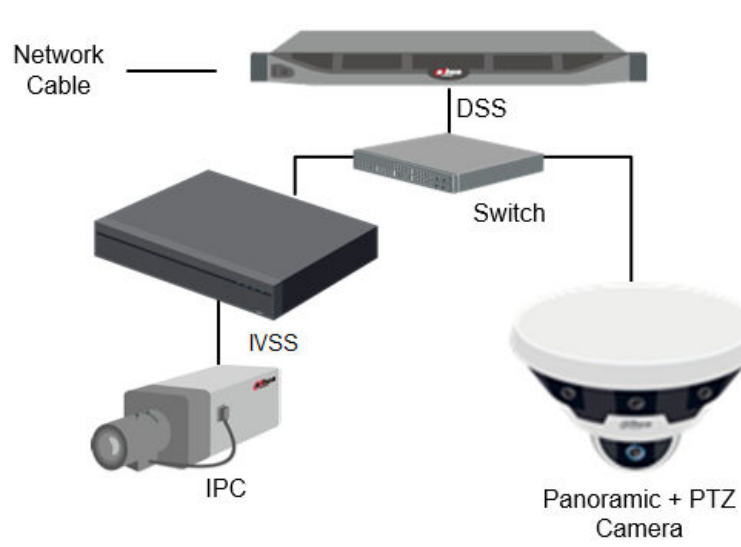
View and search for the metadata of people, vehicle, and non-motor vehicle.



Target detection can be done by video metadata cameras + a platform, or IPCs + IVSSs + platform.

7.1.1 Typical Topology

Figure 7-1 Typical topology



- General cameras record videos.
- Video metadata cameras such as panoramic + PTZ camera record videos and analyze people, and 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.

7.1.2 Preparations

Make sure the following preparations have been completed:

- Cameras and IVSS are correctly deployed, and video metadata is enabled on them. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure the parameters, see "4 Basic Configurations".
 - ◇ When adding a camera or IVSS, select **Encoder** for device category.
 - ◇ After adding the camera or IVSS to the platform, select **Target Detection** from **Features** of the device.

7.1.3 Live Target Detection

Procedure


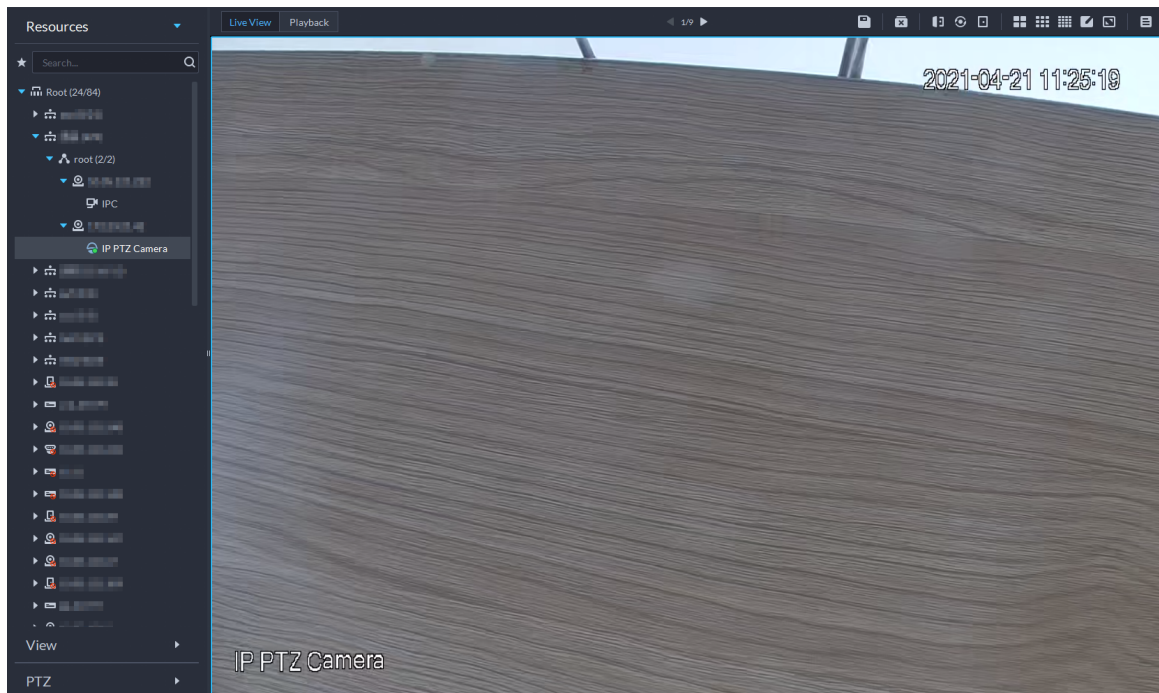






- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center > Monitor**.
- Step 2** Select a window, double-click the channel or drag the channel to the window.

Figure 7-2 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.

7.1.4 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 .
- Step 3** Set search criteria.

You can search for metadata snapshots in the **Record** , **Person** or **Vehicle** section. For details, see "6.3 DeepXplore".

7.2 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

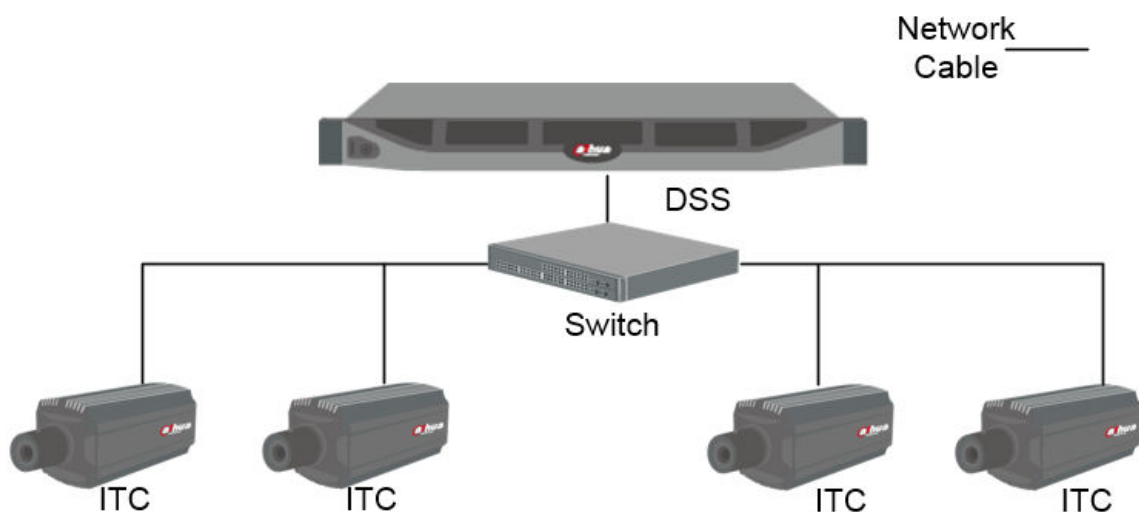
Search for vehicle records according to the filtering conditions you have set.

- 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.

7.2.1 Typical Topology

Figure 7-3 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.

7.2.2 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's manuals.
- Basic configurations of the platform have been finished. To configure, see "4 Basic Configurations".
 - ◇ When adding an ITC camera, select **ANPR** 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.

7.2.3 Live ANPR

View ANPR live video and plate snapshots.

Procedure


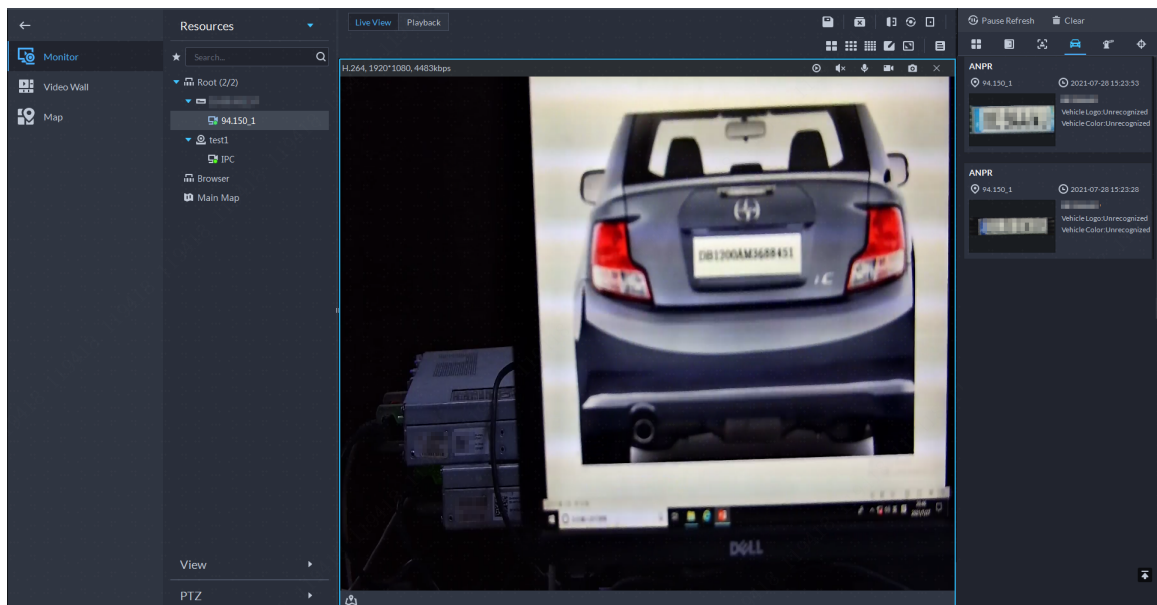






- Step 1** Log in to the DSS Client. On the **Home** page, click , and then select **Monitor Center** > **Monitor**.
- Step 2** Select a window, double-click the channel or drag the channel to the window.

Figure 7-4 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.

7.2.4 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 .

Step 3 Configure the search conditions.

You can search for vehicle snapshots in the **Record** or **Vehicle** section. For details, see "6.3 DeepXplore".

7.3 Face Recognition

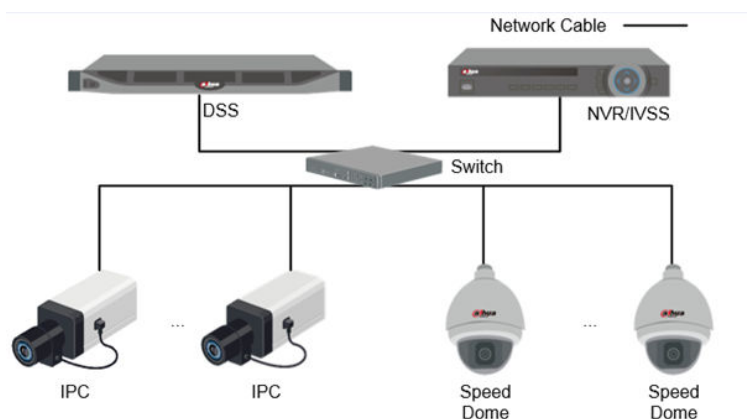
Configure face recognition settings on the device and the platform before you can view face recognition results on the platform.

7.3.1 Typical Topology

The face recognition feature is available on select models of NVR, IVSS and FR cameras.

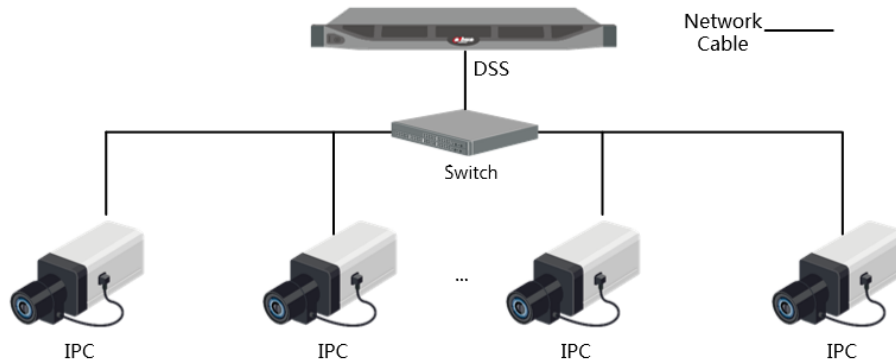
- Face recognition by NVR/IVSS

Figure 7-5 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 7-6 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.

7.3.2 Preparations

Make sure that the following preparations have been made:

- Face recognition devices are correctly configured. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "4 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.

7.3.3 Arming Faces

Before arming faces, you need to add the persons to face recognition group. For details, see "5.4.1 Face Arming List".

7.3.4 Live Face Recognition

Procedure


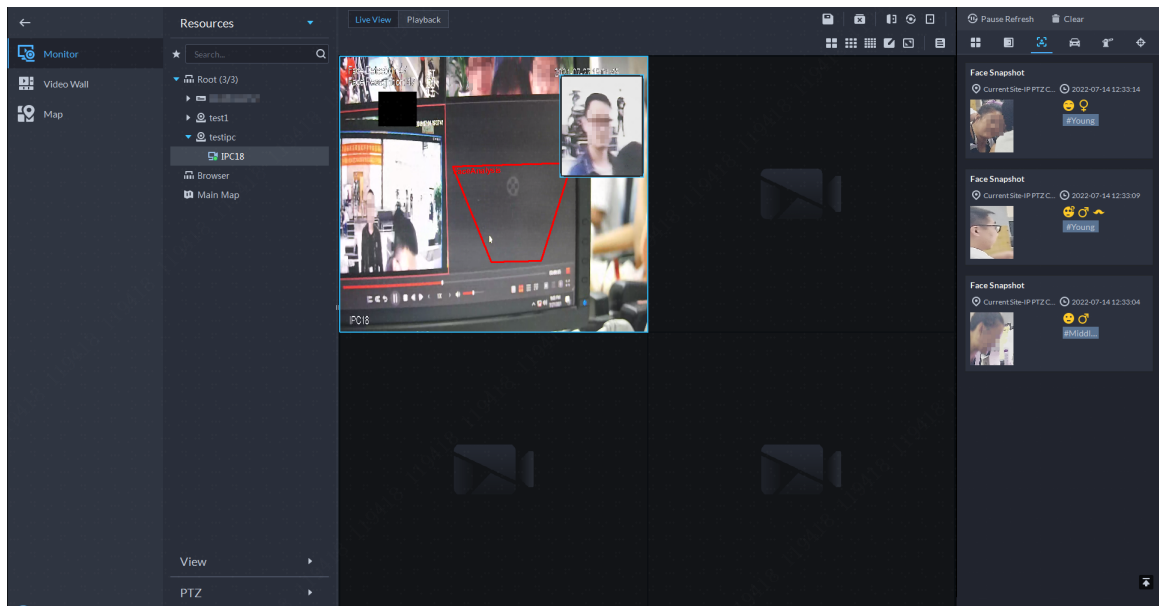










- Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitor Center** > **Monitor**.
- Step 2 Select a window, double-click the channel or drag the channel to the window.

Figure 7-7 Live view



Step 3 Click  and then click  to view live face recognition information.

Step 4 View live video, and human body, vehicle, and non-motor vehicle information.

- 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.
- : 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.
- 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.

7.3.5 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 .

Step 3 Configure the search conditions.

You can search for vehicle snapshots in the **Record** or **Person** section. For details, see "6.3 DeepXplore".

8 System Configurations

This chapter introduces system parameters configuration, license information, service management, and backup and restore.

8.1 Distributed Deployment

Background Information

Set the server type, and assign devices to different servers.

Procedure








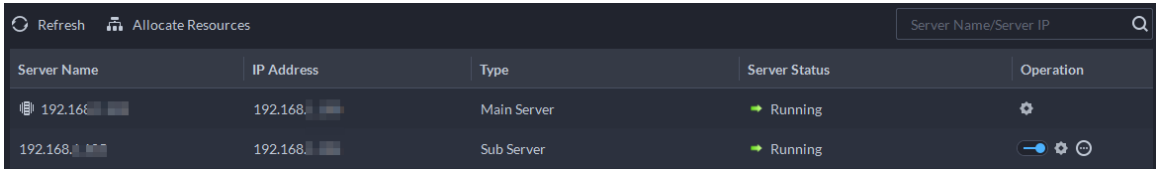




- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Deployment**.
- Step 2** Click .
- Step 3** Manage servers.
- Click  to view server details.
 - Click  corresponding to a server to define the server type. A server can be set 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 8-1 Servers



Server Name	IP Address	Type	Server Status	Operation
192.168.1.1	192.168.1.1	Main Server	Running	
192.168.1.2	192.168.1.2	Sub Server	Running	  

Step 4 Assign devices to different servers.

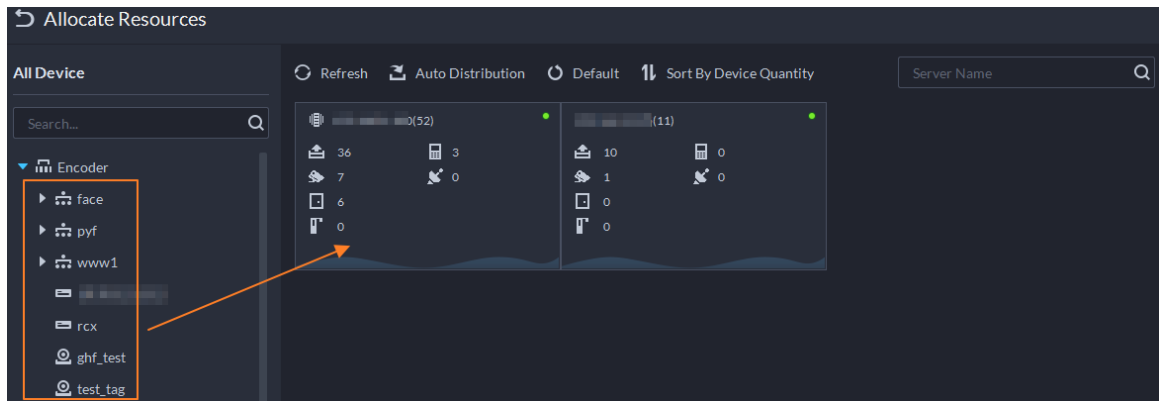
- Manually

Click **Allocate Resources**, and then select devices or channels on the left side, and 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 Device Quantity**, the servers will be sorted by the number of devices.

Figure 8-2 Resource allocation

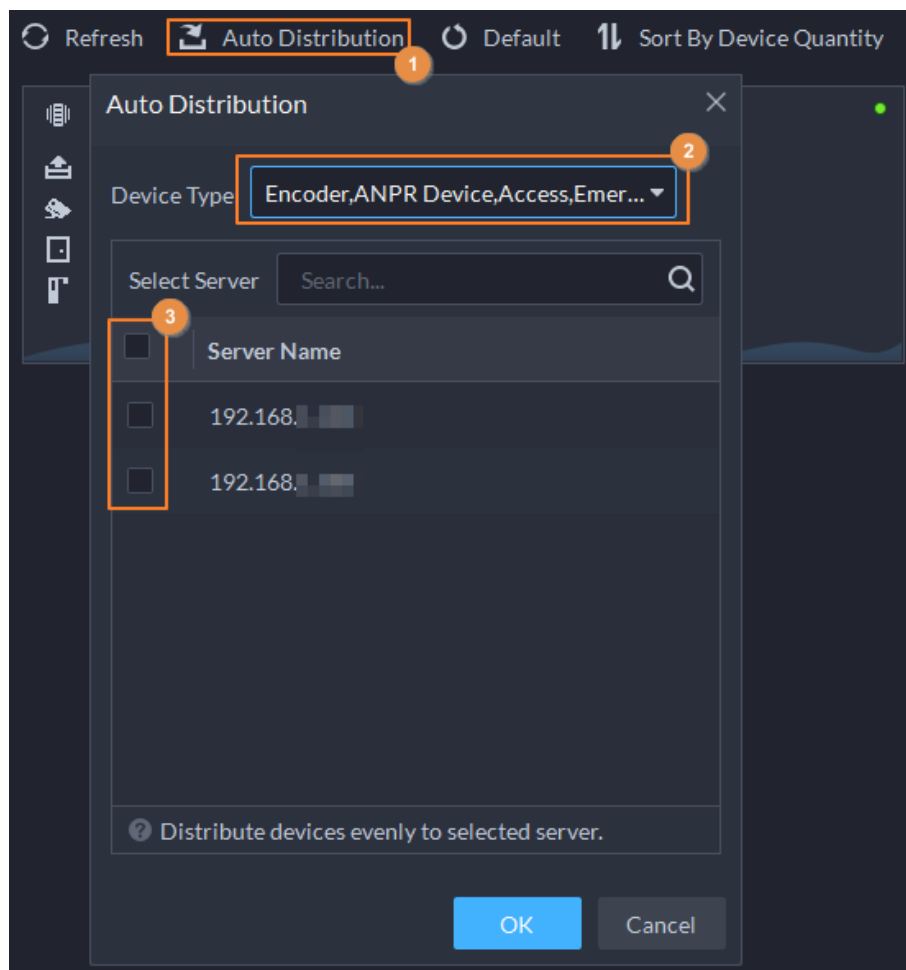


- Automatic allocation


Allocate the same type of devices evenly to different servers.

1. Click **Auto Distribution**.
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 8-3 Auto allocation



8.2 License Information

Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **License**.

On this page, you can view the types of devices and the number of channels that can be connected to the platform, and the number of App users that can be registered.

8.3 System Parameters

Configure security parameters, storage retention duration, email server, time sync, remote log, login method, and more.

8.3.1 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 8-1 Parameter description

Parameter	Description
Certificate Management	<p>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.</p> <ul style="list-style-type: none"> ● 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	<p>Protect your data by verifying login password when download or export information, and encrypting the export files.</p> <ul style="list-style-type: none"> ● File Export or Download Password Authentication : <ul style="list-style-type: none"> ◇ 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	<p>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.</p>

Parameter	Description
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.

8.3.2 Configuring Retention Period of System Data

Set the retention periods for various types of records. The expired records will be automatically deleted.

Procedure


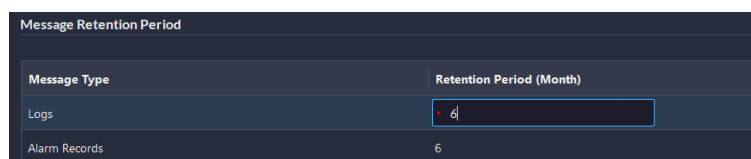
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameter**.
- Step 2** Click **Message Retention Period**.
- Step 3** Double-click a number to change its value.

Figure 8-4 Change the retention period



- Step 4** Click **Save**.

8.3.3 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 Parameter**.
- Step 2** Click the **Time Sync** tab. Enable the sync methods, and then set parameters.

Figure 8-5 Enable time synchronization

The screenshot shows the 'Time Sync' configuration page. It includes a 'Device Time Sync' toggle, a 'Scheduled Time Sync' toggle, a 'Start Time' field set to 00:00:00, and a 'Sync Interval' field set to 24 Hour(s). Below these is a 'Sync Time When Device Comes Online' toggle and a 'Sync Time Now' button. The 'NTP Time Sync' section has a toggle, an empty 'NTP Address' field, a 'Port' field set to 123, and a 'Sync Interval' field set to 60 Min(s) (1-1440). A 'Save' button is located at the bottom left of the form.

- **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**.

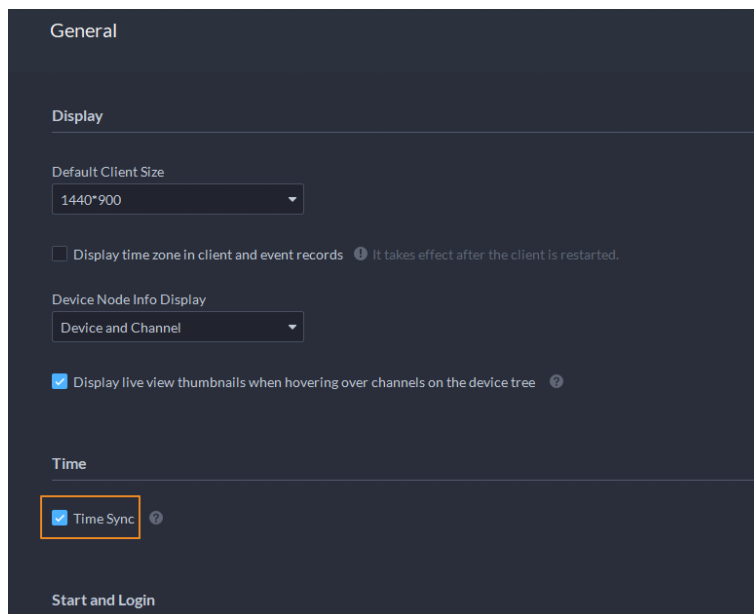
Step 4 (Optional) Enable time synchronization on DSS Client.

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 8-6 Enable time sync



The screenshot shows the 'General' configuration page. Under the 'Display' section, there are three settings: 'Default Client Size' set to '1440*900', 'Display time zone in client and event records' (unchecked), and 'Device Node Info Display' set to 'Device and Channel'. Under the 'Time' section, the 'Time Sync' checkbox is checked and highlighted with a red box. At the bottom, there is a 'Start and Login' button.

3. Restart the client for the configuration to take effect.

8.3.4 Configuring Email Server

Procedure


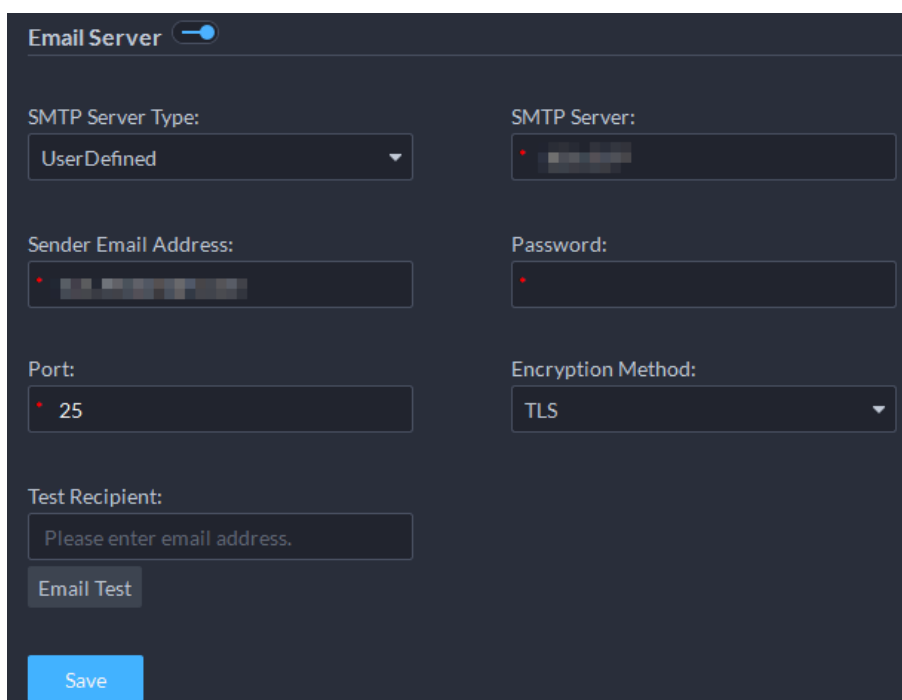
- Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameter**.
- Step 2 Click the **Email Server** tab, enable **Email Server**, and then configure parameters as required.

Figure 8-7 Set email server



The screenshot shows the 'Email Server' configuration page. At the top, there is a toggle switch for 'Email Server' which is turned on. Below this, there are several configuration fields: 'SMTP Server Type' (dropdown menu set to 'UserDefined'), 'SMTP Server' (text input field), 'Sender Email Address' (text input field), 'Password' (text input field), 'Port' (text input field set to '25'), and 'Encryption Method' (dropdown menu set to 'TLS'). At the bottom, there is a 'Test Recipient' field with the placeholder text 'Please enter email address.', an 'Email Test' button, and a 'Save' button.

Table 8-2 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**.

8.3.5 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.

8.3.6 Remote Log

To ensure safe use of the platform, the system sends administrator and operator logs to the log server for backup at 3 A.M. 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 Parameter**.

Step 2 Click the **Remote Log** 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 8-8 Enable remote log



Step 4 Click **Save**.


8.3.7 Configuring Active Directory

When the users in a domain can be used as users on the platform, you can use this function to import quickly them to the platform.

Procedure


Step 1 Configure the domain information.

1. Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameter** > **Active Directory**.
2. Click  to enable the function, and then configure the parameters of the domain.
3. Click **Get DN** to automatically get the basic DN information.
4. Click **Test** to check whether the domain information is correct.
5. (Optional) Enable the automatic synchronization function and set a time. Then, the platform will automatically synchronize news users in domain 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 domain group A. The platform will synchronize new users in domain 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.

6. Click **Save**.

Step 2 Import domain users.


1. Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User** > **User Management**.
2. Click **Import Domain Users**.
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 and 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. For details, see the previous steps.

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

4. Click  to select a role for the users.

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

5. Click **OK**.

8.3.8 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 messages, such as alarms and calls.

8.4 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.

8.4.1 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

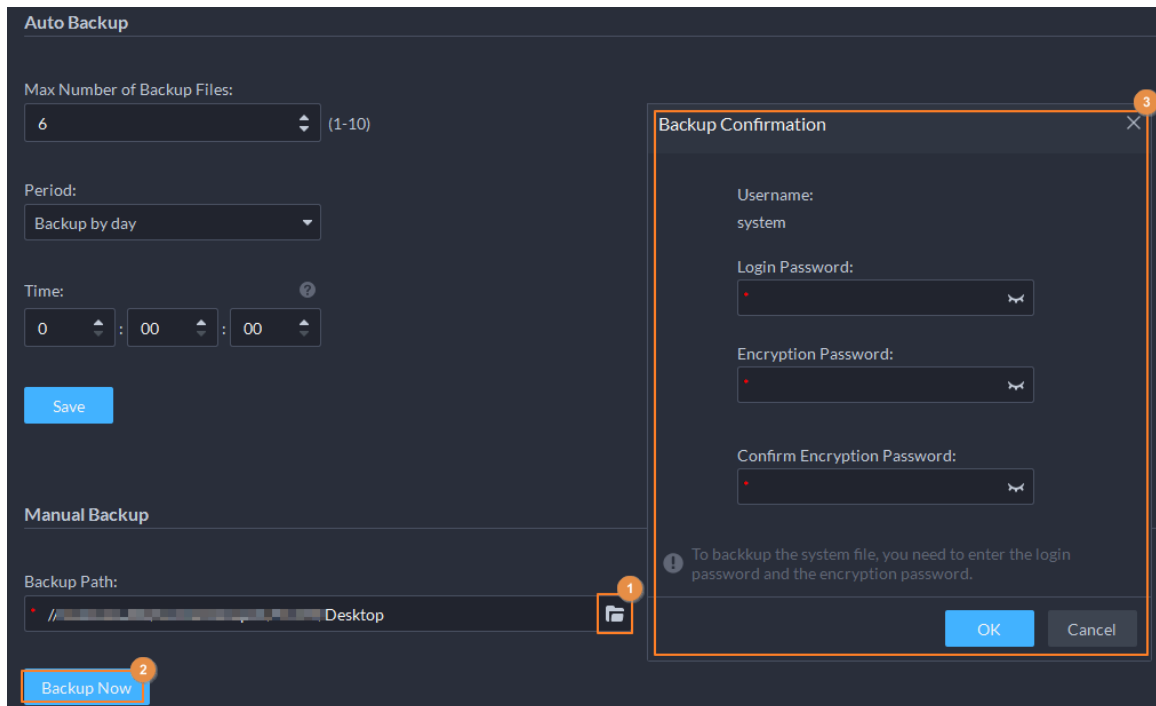
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **Backup and Restore**.

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 8-9 Manual backup

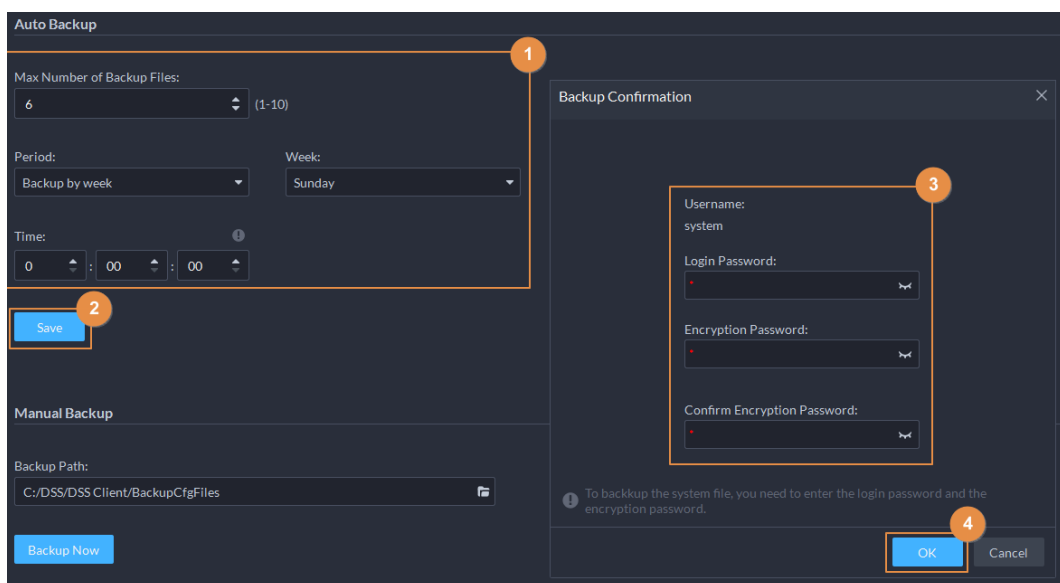


- Auto backup: In the **Auto Backup** section, configure backup parameters, and then click **OK**. The **Login Password** is the same as the system user's. Create an **Encryption Password** to protect the data. The platform automatically backs up data according to the defined time and period. The backup 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 8-10 Auto backup



8.4.2 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


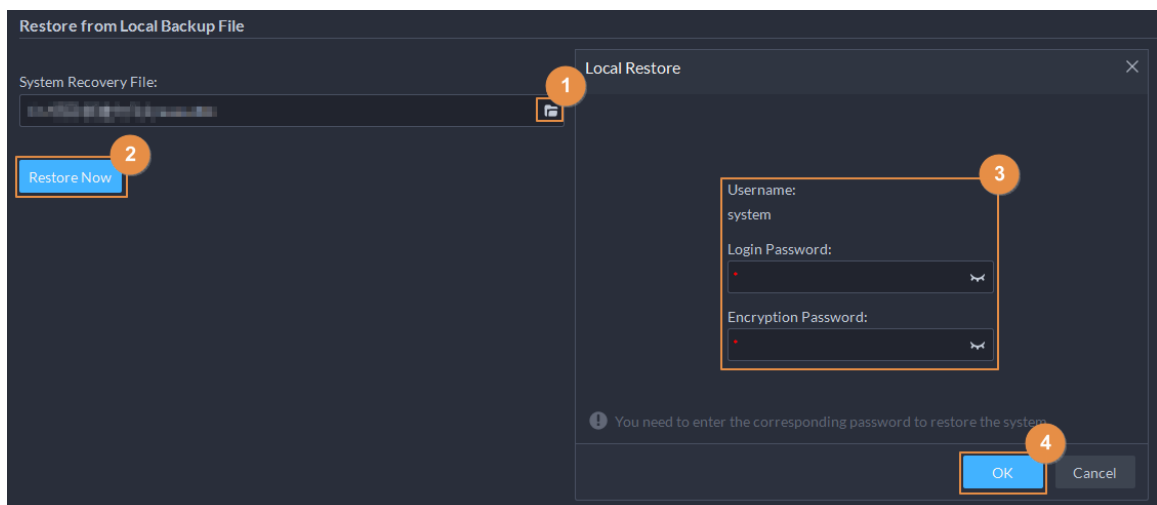
- Step 1** Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **Backup and Restore**.
- Step 2** Click the **Restore** tab.
- Step 3** Restore data.
- Restore from local backup file: In the **Restore from Local Backup File** section, select the backup 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 8-11 Local restore




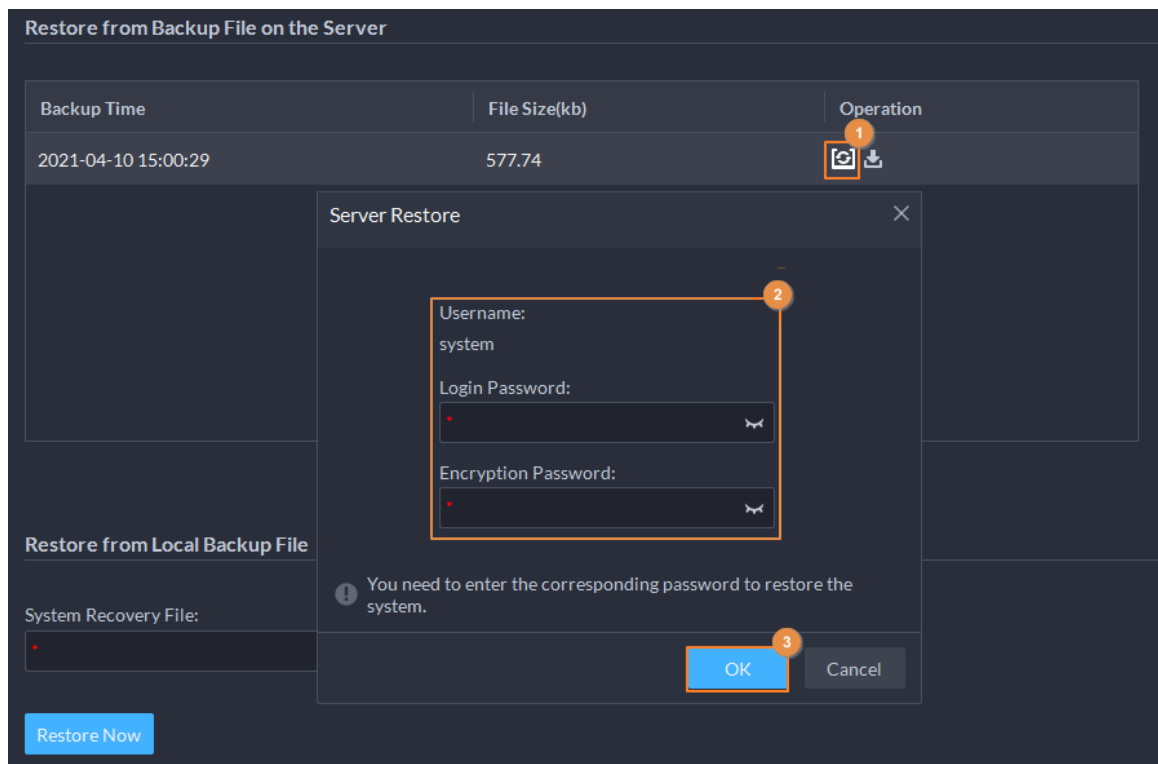

- Restore from backup file on the server: In the **Restore from Backup File on the Server** section, click , enter the passwords (the **Password** is the same as the system user's. The **Encryption Password** is the one created when the file was backed up), and then click **OK**. After restoration, the platform will automatically restart.

Figure 8-12 Restore from backup files on the server



You can click  to download the backup file.

9 Management

9.1 Managing Logs

View and export operator logs, device logs and system logs, and enable the service log debug mode for troubleshooting.

9.1.1 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.

9.1.2 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.

9.1.3 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.

9.1.4 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.

9.2 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 "9.3.5 Configure File Storage Settings".

9.2.1 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 "8.3.1 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 "9.3.2 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.

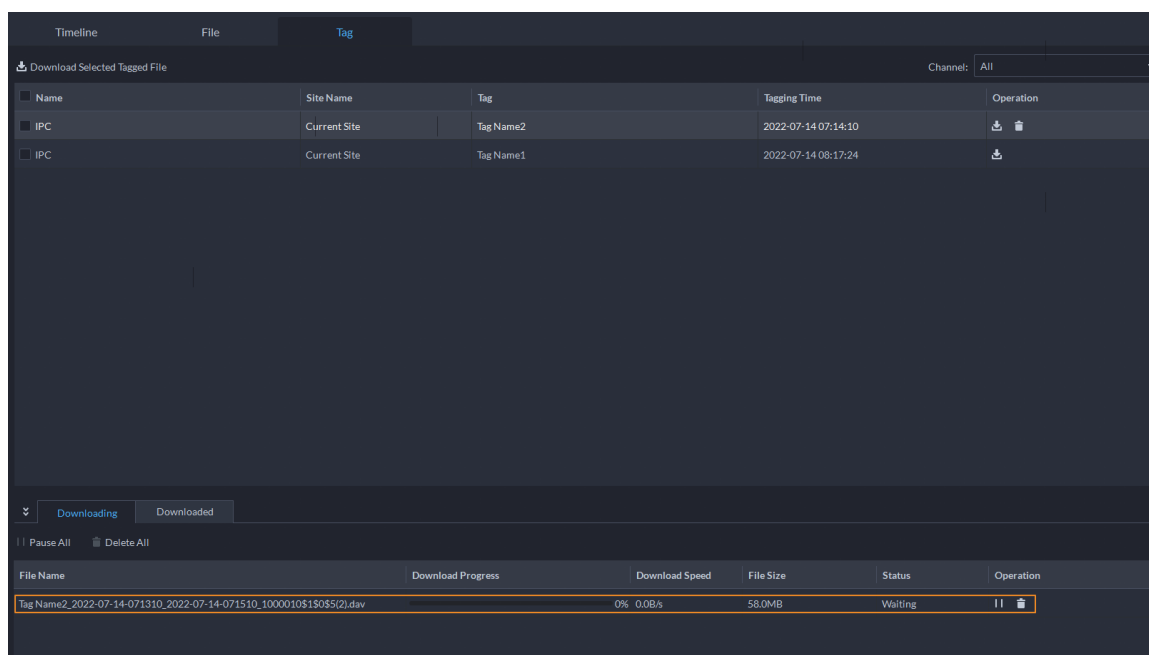
Click the **File** tab, and then click  to download a file.



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 9-1 Download progress



- After download completes, click  to go to the path where the video is saved to, or click  in the prompt on the upper-right corner to play the video directly in **Local Video**. For details, see "9.4 Playing Local Videos".


9.2.2 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 9-1 Parameter description

Parameter	Description
Select Channels	Select one or more channels to search for tags from. <ul style="list-style-type: none"> ● Unlimited : The platform will search all channels. ● : Manually select channels.
Time	Configure the time to search for tags within it.
Storage Position	Select where the videos are stored.

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 "8.3.1 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.

9.2.3 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 9-2 Parameter description

Parameter	Description
Select Channels	Select one or more channels to search for locked videos from. <ul style="list-style-type: none"> ● 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 "8.3.1 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 unlock 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.

9.3 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.

9.3.1 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 9-3 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	<ul style="list-style-type: none"> 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.

Parameters	Description
Auto Login	<p>Enable the system to skip the login page and directly open the homepage when logging in next time.</p> <ul style="list-style-type: none"> • 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.
Auto Lock Client	<p>If no operation is performed for the defined period, the client will be automatically locked, and you cannot perform any operation. Click Click to Unlock Client and verify the password of the current account to unlock the client.</p>  <p>The period can be 5 to 60 minutes.</p>
Self-adaptive audio talk parameters	If enabled, the system automatically adapts to the device sampling frequency, sampling bit, and audio format for audio talk.
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	<p>Select the sensitivity for when you operate the joystick.</p> <p>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.</p>
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**.

9.3.2 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 9-4 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	<p>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.</p> <ul style="list-style-type: none"> ● 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.
Decoding Mode	<ul style="list-style-type: none"> ● 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. ● Software 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 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.
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.
Double-click on the video to maximize the window and switch to main stream	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.

Parameters	Description
Play Mode	<ul style="list-style-type: none"> ● Real-time Priority The system might lower the image quality to avoid video lag. ● 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 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 previous live view after restart	If selected, the system displays the last live view automatically after you restart the client.
Close videos being played after long period of inactivity	The system closes live view automatically after inactivity for a pre-defined period of time. Supports up to 30 minutes.
Inactivity Time	
Display Device Video Status	After enabled, if the device is recording a video, an icon will be displayed on the upper-left corner of the window.
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	<p>Select a default stream type when you play back recordings from a device.</p>  <p>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.</p>
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.
Frame Extraction Mode	<p>Frame extraction is useful to guarantee fluency and lower the pressure on decoding, bandwidth and forwarding when playing back high-definition videos. When frame extraction is enabled, certain frames will be skipped.</p> <ul style="list-style-type: none"> ● 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. ● Force : Frame extraction is always enabled.

Parameters	Description
Continuous Snapshot Interval	Set the number and interval between each snapshot.
Number of Continuous Snapshots	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/playback video and select Snapshot , 4 images will be taken every 10 seconds.

Step 3 Click **Save**.

9.3.3 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 9-5 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.
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	<ul style="list-style-type: none"> • 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**.

9.3.4 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.

Table 9-6 Parameter description

Parameters	Description
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.
Open alarm linkage video when alarm occurs	If selected, the platform will automatically open linked video(s) when an alarm occurs.
Open Alarm Linkage Video	<ul style="list-style-type: none"> ● As Pop Up : The alarm video will be played in a pop-up window. ● Open in Live View : The alarm video will be played in a window in Monitoring Center.  <p>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 "5.1 Configuring Events".</p>
Pop-up Display Duration	
When an alarm is triggered, the alarm pop up window and the client will be displayed on the top of the screen.	When you configure the alarm videos to be displayed as pop-up windows, you can select for how long the pop-up windows will be displayed, and whether to display the pop-up windows and the client on the top of the screen.
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.

Step 3 Click **Save**.

9.3.5 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 9-7 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.

Parameters	Description
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**.

9.3.6 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.

9.3.7 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**.

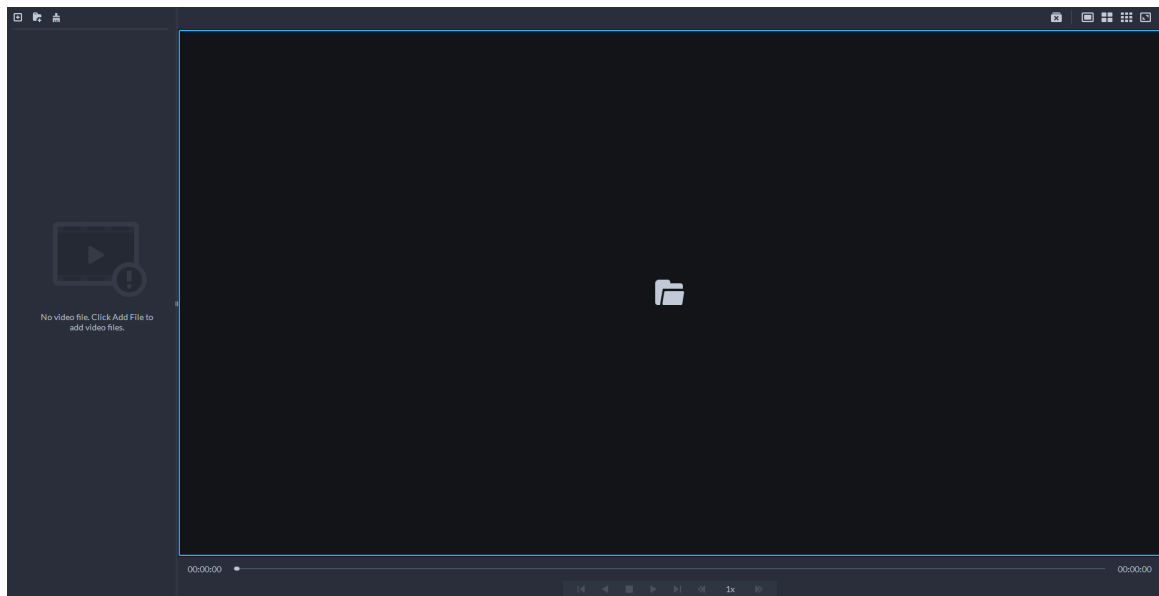
9.4 Playing Local Videos

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 9-2 Local video





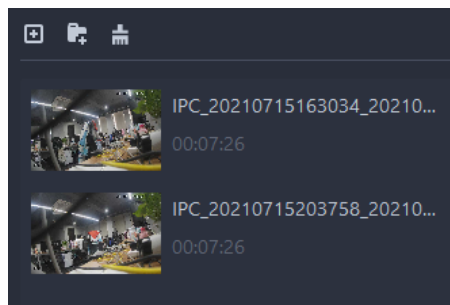
Step 2 Click  to select one or more files, or  to open all files in a folder.







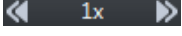





Figure 9-3 Play list



Step 3 Drag a file to the window on the right or right click it to play.

Related Operations

Table 9-8 Interface operation

Icon/Function	Description
Right-click menu	<ul style="list-style-type: none"> ● Continuous Snapshot : Take snapshots of the current image (2 snapshots each time by default). The snapshots are saved to <i>..\DSS\DSS Client\Picture</i> by default. To change the snapshot saving path, see "9.3.5 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 <i>C:\DSS\DSS Client\Picture\</i> 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: <ul style="list-style-type: none"> ● : Move the selection area. ● : Adjust the size of the selection area. ● Right-click to exit search by snapshot.

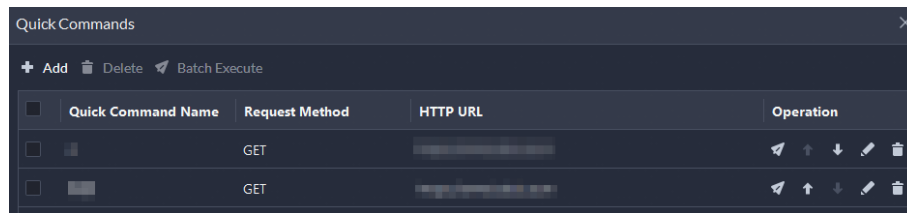
9.5 Quick Commands

Customize HTTP commands and execute them quickly. Request methods of GET, POST, PUT and DELETE are supported.

Procedure

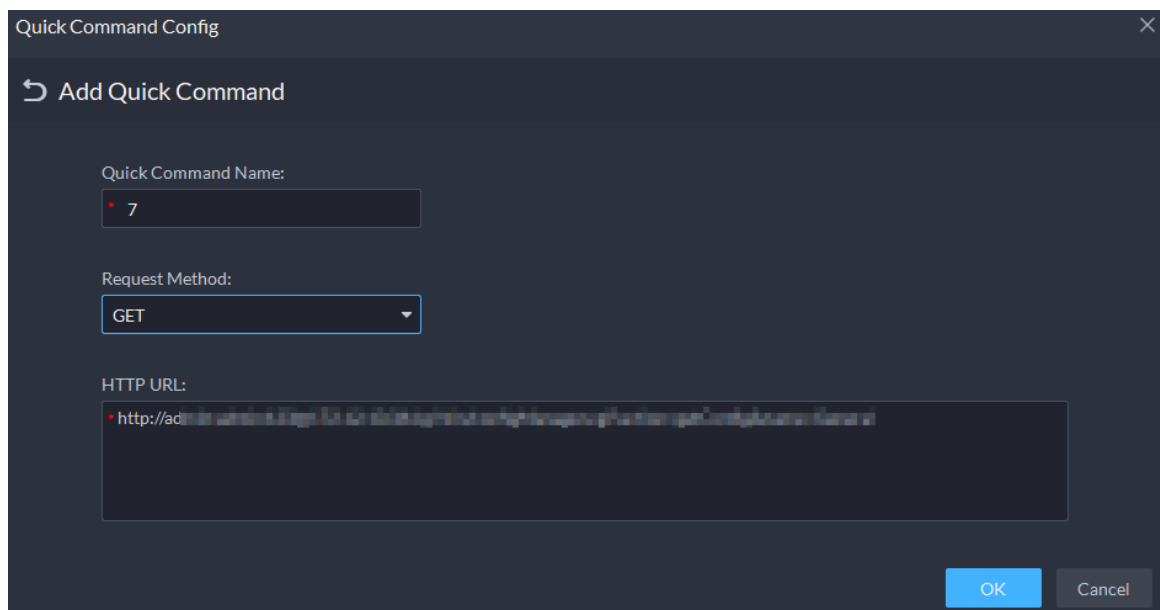
Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Quick Commands**.

Figure 9-4 Quick commands



Step 2 Click **Add**.

Figure 9-5 Add a quick command





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

Step 4 Execute commands.

- Click  to execute one command.
- Select multiple commands, and then click **Batch Execute** to execute them in batches.



Before batch execution, use  and  to adjust the order of the commands. The platform will execute them in this order.

Appendix 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.
Alarm Distribution Service	ADS	Filters and distributes alarms from devices.
Device Auto Registration Service	ARS	Accesses devices added through automatic registration.
Image Transmission Service	PTS	Accesses ANPR devices and transfers images between the devices and the platform.
Alarm Controller Access Service	MCD	Accesses alarm controllers.
Device Search Service	SOSO	Searches for and obtains configurations from devices in local networks.
Video Intercom Service	SC	Manages audio talks among PC clients and app, and video intercom devices.
DA Management Service	DAMS	Manages DA_BSID.
Link Management Service	DA_BSID	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.

Service Name		Function Description
Access Control Management Service	ACDG	Manages MCDDOOR.
Access Control Connection Service	MCDDOOR	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.

Appendix 2 RAID

RAID is an abbreviation for Redundant Array of Independent Disks. It is to combine several independent HDDs (physical HDD) to form a HDD group (logic HDD).

Comparing with one HDD, RAID provides more storage capacity and data redundancy. The different redundant arrays have different RAID level. Each RAID level has its own data protection, data availability and performance degree.

RAID Level

RAID Level	Description	Min. HDD Needed
RAID 0	RAID 0 is called striping. RAID 0 is to save the continued data fragmentation on several HDDs. It can process the read and write at the same time, so its read/write speed is N (N refers to the HDD amount of the RAID 0) times as many as one HDD. RAID 0 does not have data redundant, so one HDD damage might result in data loss that cannot be restored.	2
RAID 1	It is also called mirror or mirroring. RAID 1 data is written to two HDDs equally, which guarantee the system reliability and can be repaired. RAID 1 read speed is almost close to the total volume of all HDDs. The write speed is limited by the slowest HDD. At the same time, the RAID 1 has the lowest HDD usage rate. It is only 50%.	
RAID 5	RAID 5 is to save the data and the corresponding odd/even verification information to each HDD of the RAID 5 group and save the verification information and corresponding data to different HDDs. When one HDD of the RAID 5 is damaged, system can use the rest data and corresponding verification information to restore the damaged data. It does not affect data integrity.	3
RAID 6	Based on the RAID 5, RAID 6 adds one odd/even verification HDD. The two independent odd/even systems adopt different algorithms to ensure high data reliability. Even when two HDDs are broken at the same time, there is no data loss risk. Comparing to RAID 5, the RAID 6 needs to allocate larger HDD space for odd/even verification information, so its read/write is even worse.	4
RAID 10	RAID 10 is a combination of the RAID 1 and RAID 0. It uses the extra high speed efficient of the RAID 0 and high data protection and restoring capability of the RAID 1. It has high read/write performance and security. However, the RAID 10 HDD usage efficiency is as low as RAID 1.	

RAID Capacity

See the sheet for RAID space information.

Capacity N refers to the mini HDD amount to create the corresponding RAID.

RAID Level	Total Space of the N HDD
RAID 0	$N \times \text{minN}$
RAID 1	minN
RAID 5	$(N-1) \times \text{minN}$
RAID 6	$(N-2) \text{minN}$
RAID 10	$(N/2) \times \text{minN}$

Appendix 3 Security Commitment and Recommendation

VIP Vision 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. VIP Vision 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. VIP Vision 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, VIP Vision encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report potential risks or vulnerabilities to the VIP Vision PSIRT. They can do so by visiting the cybersecurity section on the VIP Vision 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.

Achieve more than security with VIP Vision

VIP Vision

Address: 8A Precision Place, Mulgrave, NSW, 2756, Australia

website: www.vipvision.au

Ph: 02 4502 8671

Email: sales@vipvision.au