General Surveillance Management Center Web Client

User Manual



ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V8.8.0

Foreword

General

This user 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...	Search for items by keywords or specified content.
or **Delete**	Delete items one by one or in batches.
, or **Edit**	Edit the parameters of an item.
, , **Enable** , or **Disable**	Enable or disable items one by one or in batches.
or **Export**	Exported the selected content to your local computer.
or **Refresh**	Refresh the content.
*	A parameter that must be configured.

Privacy Protection Notice

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

About the Manual

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

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.

Transportation Requirements



Transport the device under allowed humidity and temperature conditions.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Installation Requirements



-  Electrical Hazard

  Preventive measures: Make sure the power is off when you put your hand into the device.
- Stability Hazard

  Possible result: The rack might fall down and cause serious personal injury.

  Preventive measures (including but not limited to):

  - Before extending the rack to the installation position, read the installation instructions.
  - When the device is installed on the slide rail, do not place any load on it.
  - Do not retract the slide rail while the device is installed on it.



- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Use the standard power adapter or cabinet power supply. We will assume no responsibility for any injuries or damages caused by the use of a nonstandard power adapter.
- Please follow the electrical requirements to power the device.
  - Following are the requirements for selecting a power adapter.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.

- ◇ We recommend using the power adapter provided with the device.
- ◇ When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.

- Rotating Fan Blades Hazard

  Avoid touching the fan blades, especially when they are moving.

- Before installation, disconnect all the power cords.

- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Install the server on a stable surface to prevent it from falling.
- Use power cords that conform to your local requirements, and are rated specifications.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- Use power cords that conform to your local requirements, and are rated specifications.
- Before connecting the power supply, make sure the input voltage matches the server power requirement.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- Install the server in an area that only professionals can access.
- Extra protection is necessary for the device casing to reduce the transient voltage to the defined range.
- If you did not push the HDD box to the bottom, then do not close the handle to avoid damage to the HDD slot.
- Install the device near a power socket for emergency disconnect.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- Affix the device securely to the building before use.

Operation Requirements

DANGER

- The device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

  Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

  Preventive measures (including but not limited to):

  - ◇ Keep new and used batteries out of reach of children.
  - ◇ If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
  - ◇ Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions

  Preventive measures (including but not limited to):

  - ◇ Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.

- ◇ Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
- ◇ Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
- ◇ Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.

WARNING

- In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- The device is heavy and needs to be carried by several persons together to avoid personal injuries.
- Place the device in a location that children cannot easily access.

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.
- Your configurations will be lost after performing a factory reset. Please be advised.
- Do not restart, shut down or disconnect the power to the device during an update.
  - ◇ Make sure the update file is correct because an incorrect file can result in a device error occurring.
  - ◇ The system cannot upgrade different types of AI modules at the same time.
- Do not frequently turn on/off the device. Otherwise, the product life might be shortened.
- Back up important data on a regular basis when using the device.
- Operating temperature: 0 °C to 45 °C (32 °F to 113 °F).
- Salt pray in the operating environment of the device might corrode its electronic components and cables. To ensure the normal operation of the device and prolong its service life, use the device in an indoor environment that is 3 kilometers away from the sea.

Maintenance Requirements

DANGER

- Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

  Preventive measures (including but not limited to):
  - ◇ Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
  - ◇ Dispose of the old batteries as instructed.
- Power off the device before maintenance to make sure that the device is disconnected from the power supply.

- AI module does not support hot plug. If you need to install or replace the AI module, unplug the device power cord first. Otherwise, it will lead to file damage on the AI module.

- The device casing provides protection for internal components. Use a screwdriver to loosen the screws before detaching the casing. Make sure to put the casing back on and secure it in its original place before powering on and using the device.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

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 7
2.2 Configuring Distributed Deployment 8
2.2.1 Configuring Main Server 8
2.2.2 Configuring and Enabling Sub Servers 8
2.3 Configuring Hot Standby 9
2.4 Configuring N+M 11
2.5 Configuring LAN or WAN 14
2.5.1 Configuring Router 14
2.5.2 Mapping IP or Domain Name 15
3 Configuring Basic Settings 17
3.1 Login and Password Initialization 17
3.2 Quick Guide 17
3.3 Self-check 22
3.4 Network Config 22
3.4.1 NIC Config 22
3.4.2 Network Mode 24
3.4.3 Connection Detection 26
3.4.4 Route Settings 26
3.4.5 802.1x 27
3.5 Mode Config 29
3.5.1 Configuring Main/Sub 29
3.5.2 Configuring Hot Standby 30
3.6 Security Config 30
3.6.1 SSH Connection Service 30
3.6.2 TLS 31
3.6.3 Trusted Verification 31
3.7 System Maintenance 31
3.7.1 Basic Maintenance 31
3.7.2 Database Maintenance 32

3.7.3 Log....32
3.7.4 Updating System and Program....33
3.8 Basic Config....34
3.8.1 User Management....34
3.8.2 Time Config....34
4 Basic Configurations....36
4.1 Preparations....36
4.1.1 Logging in to DSS Web Client....36
4.1.2 Installing Mobile Client....37
4.2 Managing Resources....37
4.2.1 Adding an Organization....37
4.2.2 Managing Devices....38
4.2.3 Binding Resources....50
4.2.4 Resource Maintenance....51
4.2.5 Adding Recording Plans....51
4.2.6 Adding Retrieval Plans....56
4.2.7 Adding Time Template....59
4.2.8 Configuring Video Retention Period....60
4.2.9 Configuring Events....60
4.2.10 Configuring Door....61
4.2.11 Synchronizing People Counting Rules....62
4.2.12 Configuring Audio Play Plan of IP Speaker....62
4.3 Adding Roles and Users....63
4.3.1 Adding a Role....63
4.3.2 Adding a User Group....65
4.3.3 Adding a User....66
4.3.4 Adding Self-Service Users....68
4.3.5 Importing Domain Users....69
4.3.6 Syncing Deleted Domain Users....70
4.3.7 Syncing Added Domain Users....70
4.3.8 Configuring Auto Synchronization....71
4.3.9 Password Maintenance....71
4.4 Configuring Storage....73
4.4.1 Configuring Network Disk....73
4.4.2 Configuring Server Disk....75
4.4.3 Configuring Disk Group....76
4.4.4 Configuring Device Storage....77
5 Businesses Configuration....79
5.1 Configuring Events....79
5.1.1 Configuring Event Linkage....79

5.1.2 Configuring Combined Event....84
5.1.3 Configuring Alarm Parameter....85
5.1.4 Configuring Generic Event....86
5.2 Configuring Map....87
5.2.1 Preparations....87
5.2.2 Adding a Map....87
5.2.3 Map Operations....90
5.2.4 Marking Devices....92
5.3 Personnel and Vehicle Management....92
5.3.1 Adding Person and Vehicle Groups....93
5.3.2 Configuring Person Information....94
5.3.3 Vehicle Management....113
5.4 Arming List....115
5.4.1 Face Arming List....115
5.4.2 Vehicle Arming List....118
5.4.3 Text-Defined Alarms....120
5.5 Access Control....122
5.5.1 Preparations....122
5.5.2 Configuring Zone....122
5.5.3 Configuring Access Rule....129
5.5.4 Configuring Public Passwords....143
5.5.5 Configuring Credential Security....143
5.5.6 Configuring Access Control Devices....145
5.6 Visitor Management....145
5.6.1 Preparations....145
5.6.2 Configuring Visitor Appointment....145
5.6.3 Configuring Visitor Registration....146
5.6.4 Configuring Registration and Appointment....147
5.6.5 WhatsApp Message Template....147
5.6.6 Configuring Visitor Access Permission and Visitor Pass....148
5.6.7 Configuring Email Template....149
5.7 Parking Lot....150
5.7.1 Preparations....150
5.7.2 Configuring Parking Lot....151
5.7.3 Vehicle Group Management....159
5.7.4 Configuring Scheduled Report....159
5.8 Intelligence Analysis....161
5.8.1 People Counting Group....161
5.8.2 Scheduled Report....162
5.8.3 Crowd Distribution Group....163

5.8.4 Vehicle Density Group 163
5.9 Maintenance Center 164
5.9.1 Configuring Alert Rule 164
5.9.2 Configuring Video Integrity 164
6 Businesses Operation 166
6.1 Monitoring Center 166
6.1.1 Main Page 166
6.1.2 Video Monitoring 167
6.1.3 Playback 181
6.1.4 Map Applications 185
6.2 Event Center 188
6.2.1 Real-Time Event 188
6.2.2 History Alarms 191
6.2.3 Event Statistics 191
6.2.4 Alarm Controller 193
6.2.5 Arming Control 196
6.3 DeepXplore 198
6.3.1 Searching for People 198
6.3.2 Searching for Vehicles 200
6.3.3 Searching for Records 202
6.3.4 Track Playback 204
6.3.5 WizSeek 205
6.4 Access Management 207
6.4.1 Access Control 207
6.4.2 Visitor Application 217
6.5 Parking Lot 229
6.5.1 Entrance and Exit Monitoring 229
6.5.2 Searching for Records 231
6.6 Intelligent Analysis 233
6.6.1 People Counting 234
6.6.2 In-Area People Counting 236
6.6.3 Crowd Distribution Analysis 237
6.6.4 Vehicle Density Analysis 237
6.6.5 Metadata Analysis 238
6.7 Maintenance Center 239
6.7.1 Viewing System Status 239
6.7.2 Maintenance Management 240
7 General Application 244
7.1 Target Detection 244
7.1.1 Typical Topology 244

7.1.2 Preparations 244
7.1.3 Live Target Detection 245
7.1.4 Searching for Metadata Snapshots 245
7.2 ANPR 245
7.2.1 Typical Topology 246
7.2.2 Preparations 246
7.2.3 Live ANPR 246
7.2.4 Searching for Vehicle Snapshot Records 247
7.3 Face Recognition 247
7.3.1 Typical Topology 247
7.3.2 Preparations 248
7.3.3 Arming Faces 248
7.3.4 Live Face Recognition 248
7.3.5 Searching for Face Snapshots 249
7.4 Lift Control 249
7.4.1 Typical Topology 250
7.4.2 Preparations 250
7.4.3 Lift Controller Maintenance 252
7.4.4 Configuring Event 254
7.4.5 Authorized Access 254
7.4.6 Calling Lift on VTO 256
7.4.7 Viewing Access Records 257
8 System Configurations 258
8.1 Distributed Deployment 258
8.2 License Information 260
8.3 System Parameters 260
8.3.1 Configuring General Parameters 260
8.3.2 Configuring Security Parameters 261
8.3.3 Configuring Data Records 262
8.3.4 Time Synchronization 262
8.3.5 WhatsApp Integration Configuration 264
8.3.6 Configuring Email Server 264
8.3.7 Configuring FTP Server 266
8.3.8 Configuring Active Directory 266
8.3.9 Configuring Device Access Parameters 267
8.3.10 Remote Logs 267
8.3.11 Configuring Mobile App 268
8.3.12 Configuring Privacy Policy 268
8.4 Backup and Restore 268
8.4.1 System Backup 269

8.4.2 System Restore....270
9 Management....271
9.1 Configuring Local Settings....271
9.1.1 Configuring General Settings....271
9.1.2 Configuring Video Settings....271
9.1.3 Configuring Alarm Settings....273
9.1.4 Configuring File Storage Settings....274
9.2 Managing Logs....275
9.2.1 Operation Log....275
9.2.2 Device Log....275
9.2.3 System Log....276
9.2.4 Service Log....276
9.3 Help....276
Appendix 1 Service Module Introduction....277

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

  Increases 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.
  - ◇ Dahua's unique N+M redundancy mode.
  - ◇ Redundant power design that makes the system more stable (only applicable to DSS7116DR).

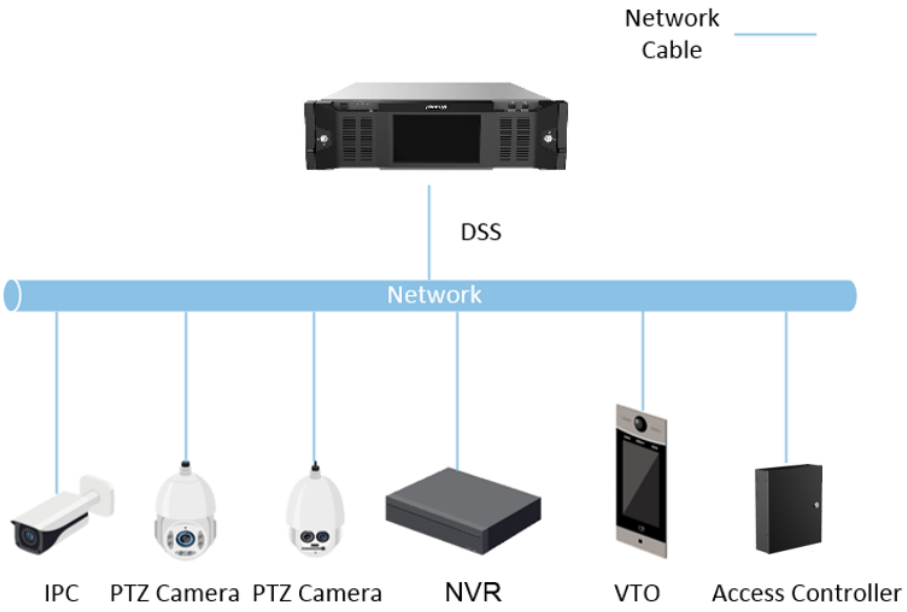
2 Installation and Deployment

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.

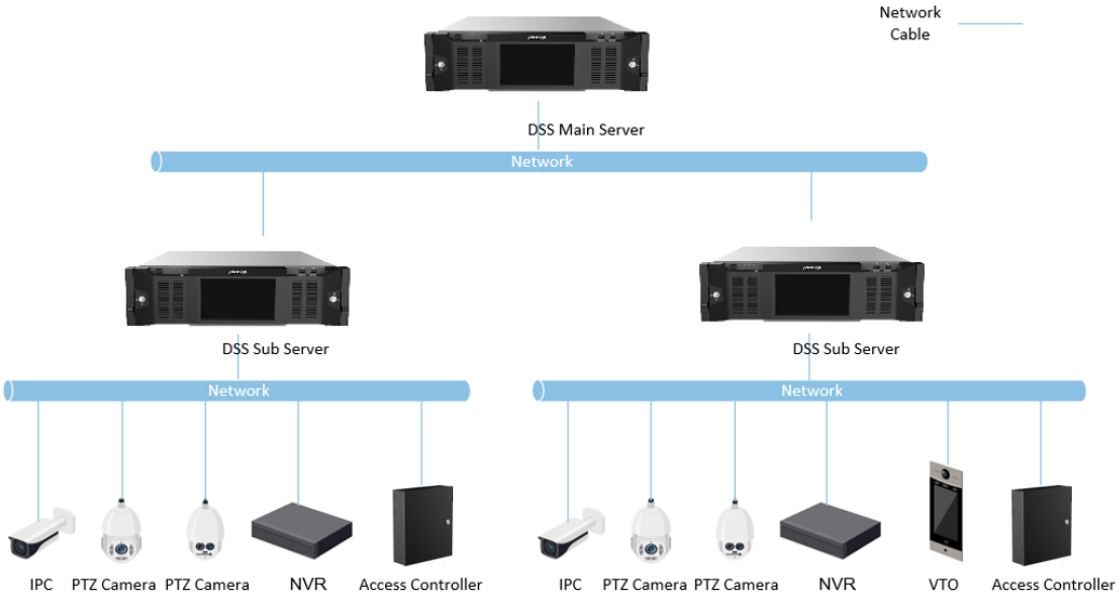
Figure 2-1 Standalone deployment



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.

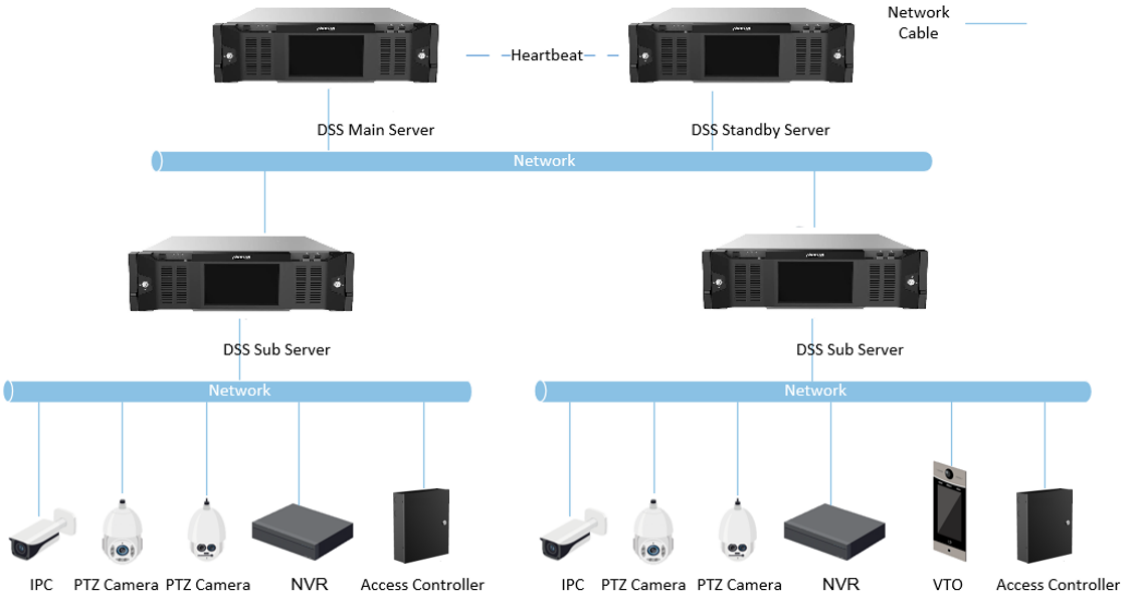
Figure 2-2 Distributed deployment



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.

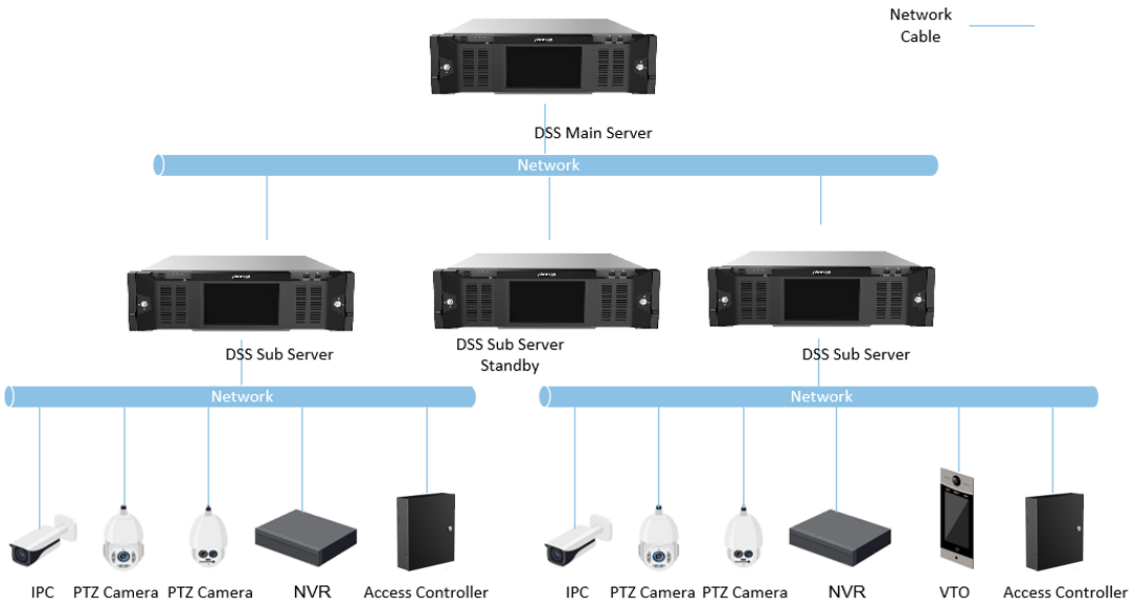
Figure 2-3 Hot standby



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 in 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**.

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.

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

The HTTPS port is 443 by default. You can modify the port from **Network Config** > **Network Mode**.

Step 5 Enter the username and password, and then click **Login**.

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

Step 6 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	• 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	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.

Parameter	Description
Mode	The mode that the system gets IP. ● **Static** : Manually configure **IP Address**, **Subnet Mask**, and **Default Gateway**. ● **DHCP** : When there is DHCP server in the network, and DHCP is enabled on the server, select **DHCP**, and the system acquires IP address automatically.
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 7 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 that you are using.

Step 8 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://*IP address that you configured:port*/config in the browser.

The HTTPS port is 443 by default. You can modify the port from **Network Config** > **Network Mode**.

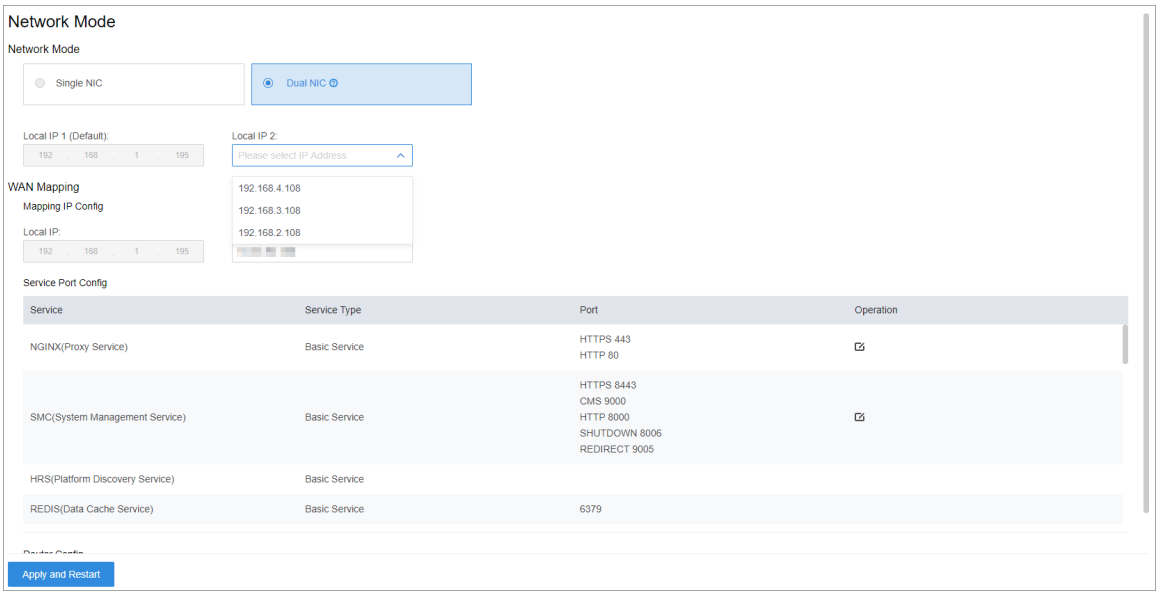
Step 2 Enter the username and password, and then click **Login**.

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

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 2-5 Dual network cards mode



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**.

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**.
- The IP addresses of the main server and the sub server must be on the same local area network.

Procedure

Step 1 Go to https://*sub server IP address:port*/config in the browser.

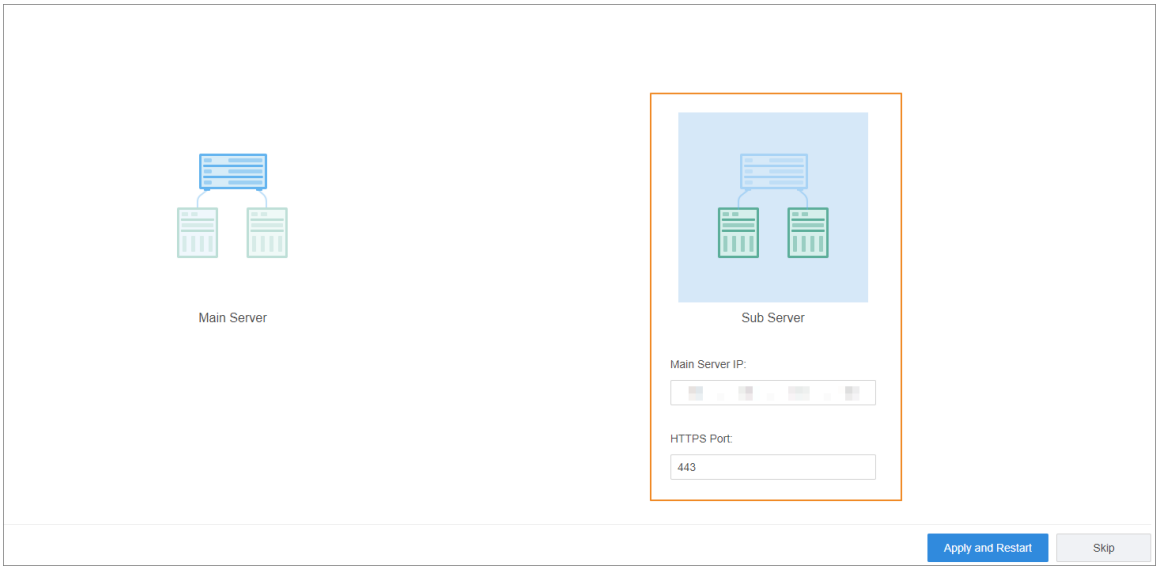
The HTTPS port is 443 by default. You can modify the port from **Network Config** > **Network Mode**.

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**.

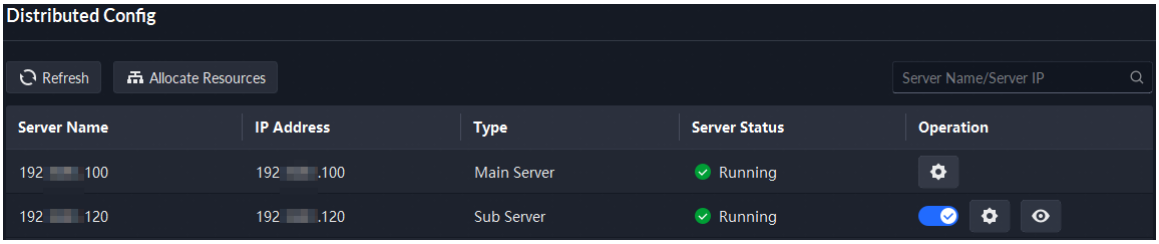
Figure 2-6 Configure the sub server



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 2-7 Enable the sub server



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

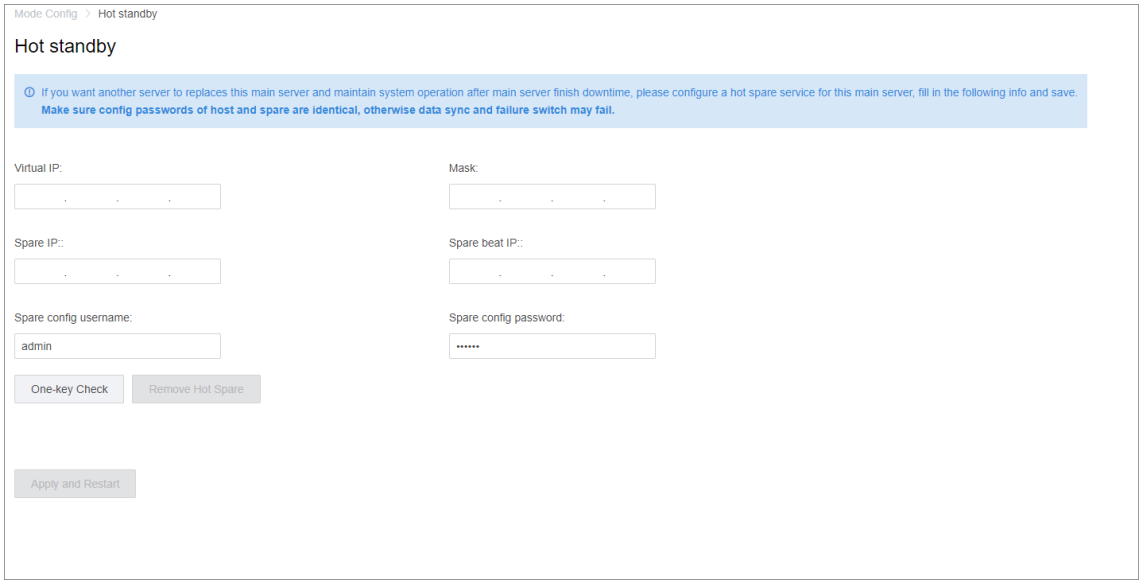
- Connect network cables.
  - Use network port 1 as business network port, and then configure an IP address on the business network segment for the network port 1. Connect network port 1 to the same LAN via switch, and the virtual IP address and the one of network port 1 need to be in the same segment.
  - 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.
- NTP time synchronization has been enabled on both servers. For details, see "8.3.4 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 2-8 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 user name and password of spare server Config system. - 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.
Spare config password	
One-key Check	Click **One-key Check** to confirm user name and password.
Remove Hot Spare	When the hot spare is ready, you can click this button to remove the hot spare configuration. 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. For this operation, you must access the IP addresses of the servers, and not the virtual IP address.

Step 4 Click **Apply and Restart**.

2.4 Configuring N+M

On the main server, enable the sub server, and then configure the N+M (primary + standby) relationship.

Prerequisites

- The relevant servers have been well deployed.
- All N+M nodes (including the central node) must be on the same network segment.

Background Information

- If the N node (active node) experiences a power outage or network disconnection, the M node (standby node) requires 60–70 seconds to complete takeover.
- If the N node experiences service failure, supports manual switching to take over the node.
- When the N node returns to normal, the system will not automatically switch to the M node. Manual switching is required.

Procedure

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

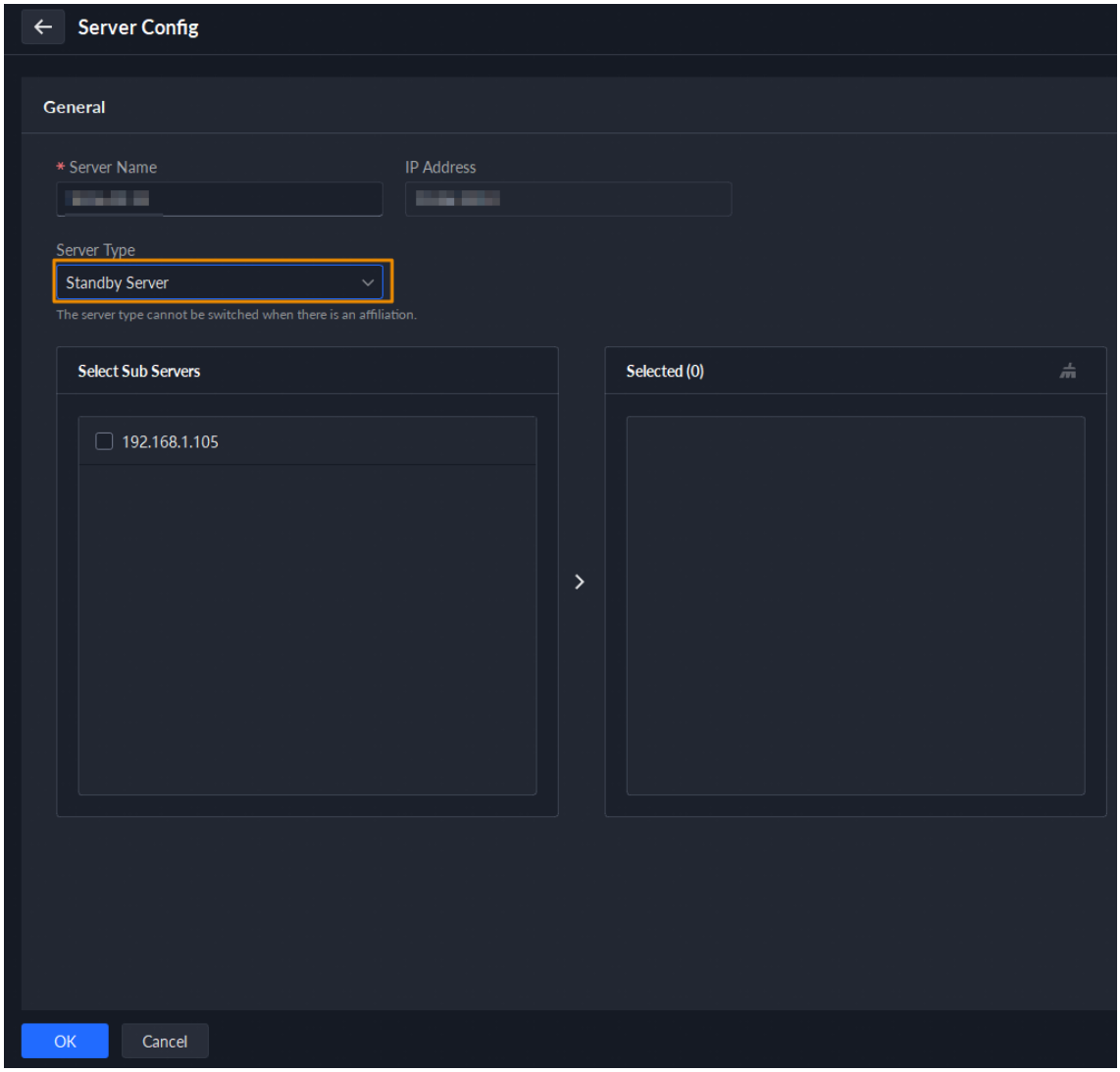
Step 2 Click .

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**.

Figure 2-9 Configure a standby server

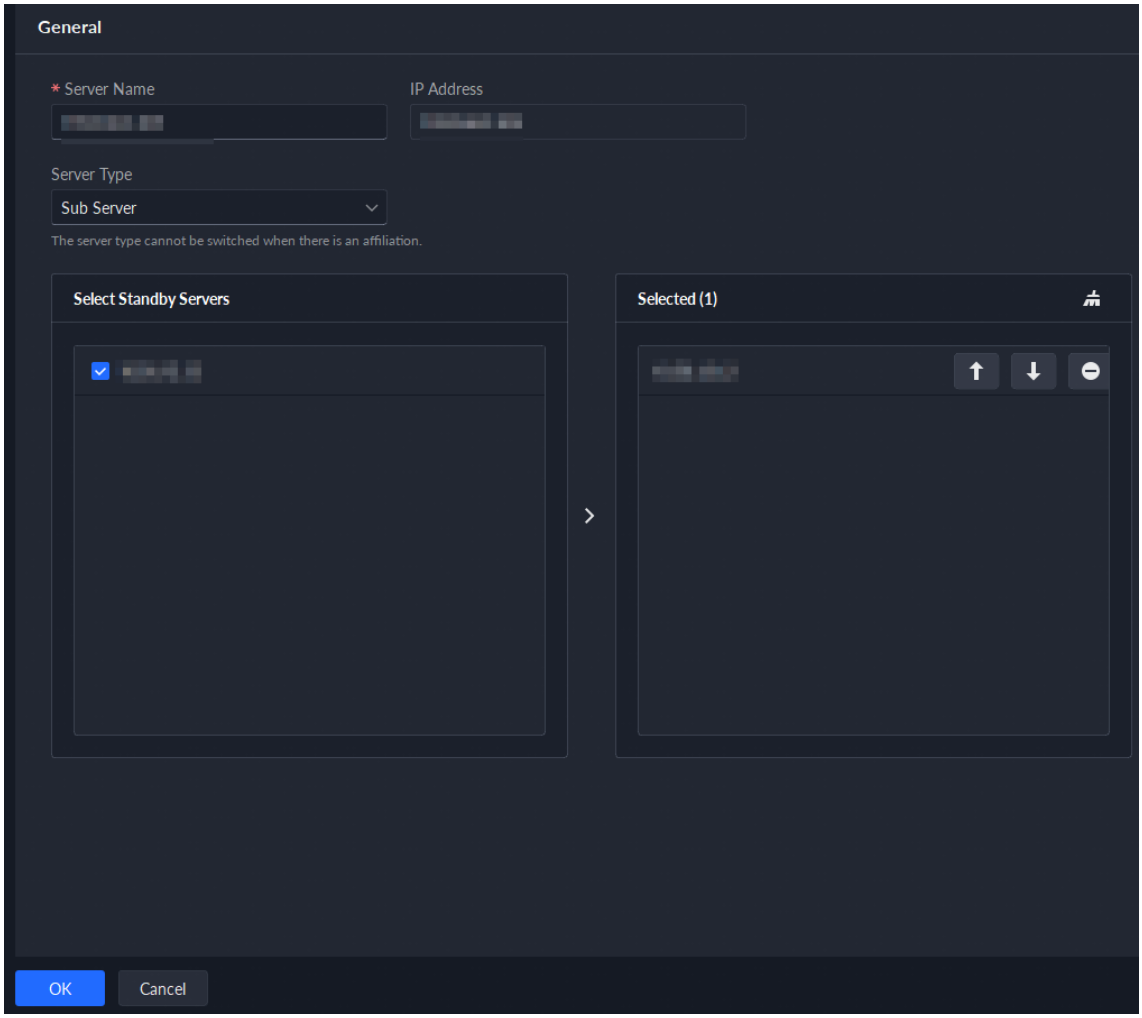


Step 5 Configure the sub-standby relationship in either of the following ways.

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

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

Figure 2-10 Select a standby server



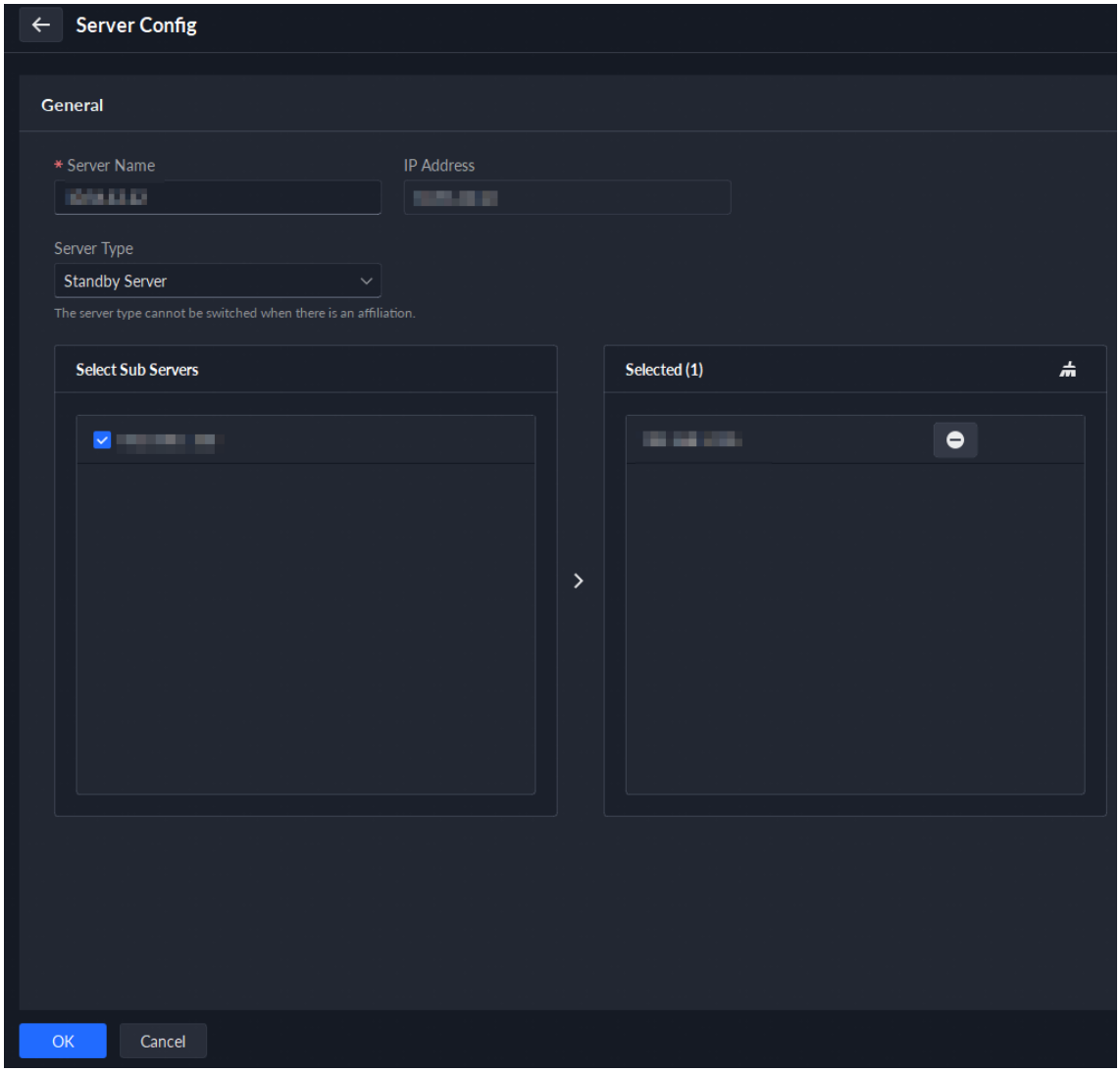
3. Click **OK**.

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

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

   You can click to adjust the priority.

Figure 2-11 Select a sub server



3. Click **OK**.

2.5 Configuring LAN or WAN

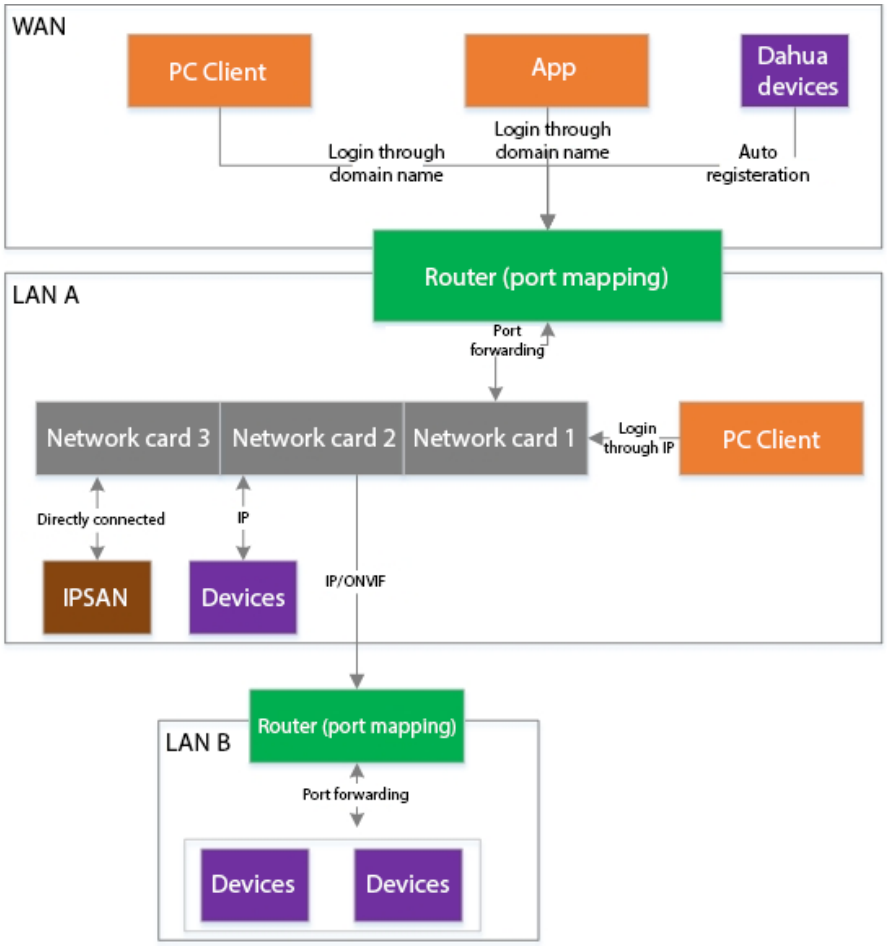
2.5.1 Configuring Router

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 *Port List*.

If there is a sub server, the sub server and the main server must be mapped to the same public IP address, but distinguished by different ports.

- 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

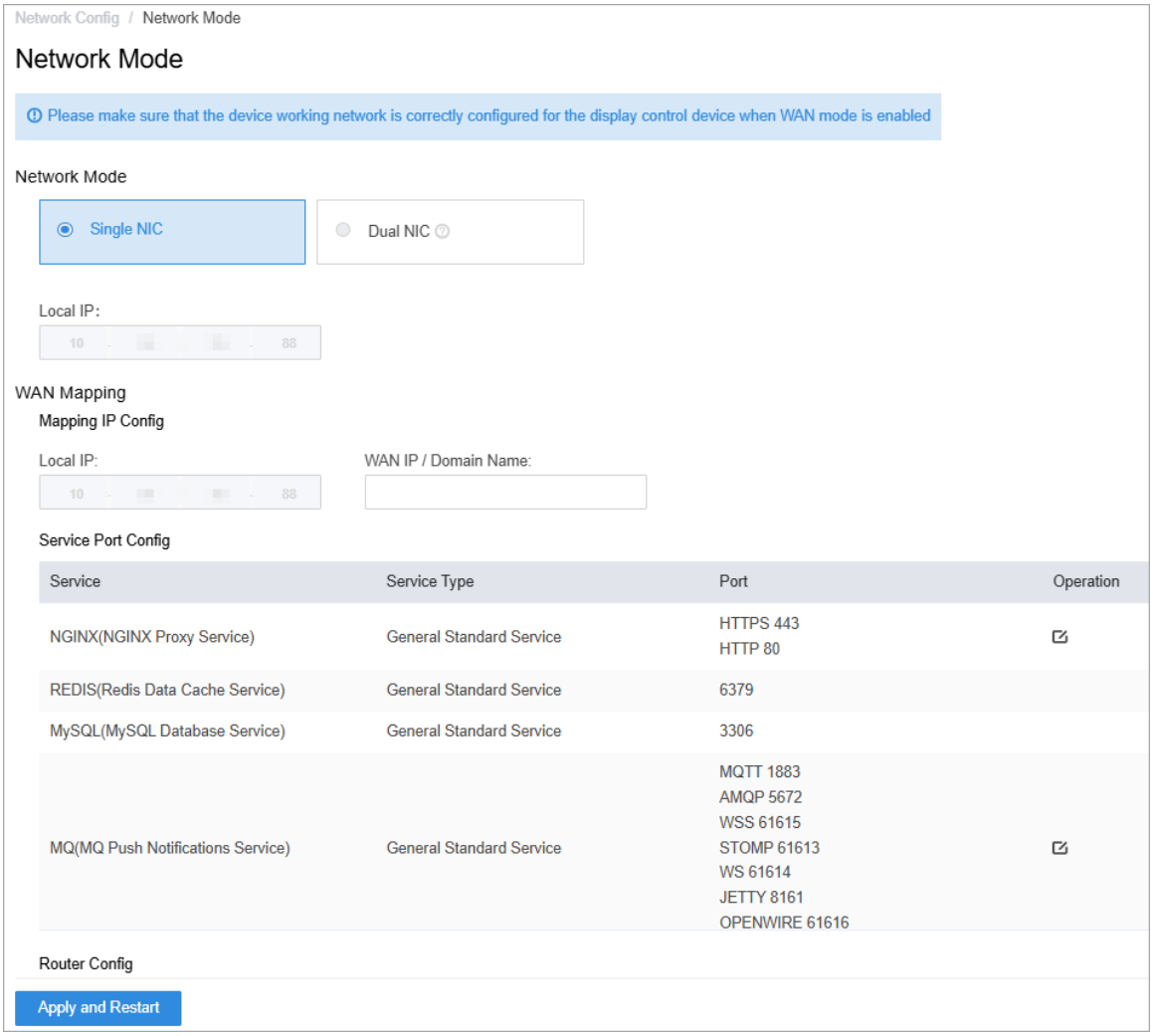
If the platform is deployed in a local network, you can map the IP address of the server to a fixed WAN IP or a domain name, and then log in to the server using the WAN IP or domain name.

Procedure

Step 1 Log in to the Config system.

Step 2 Select **Network Config** > **Network Mode**.

Figure 2-13 Network mode



Step 3 Enter a fixed WAN IP address or a domain name in the **WAN IP / Domain Name** 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.
- For distributed deployment, make sure that the external network IP of sub servers and main servers are the same, and the IP must be a public network IP.

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 page is displayed.

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

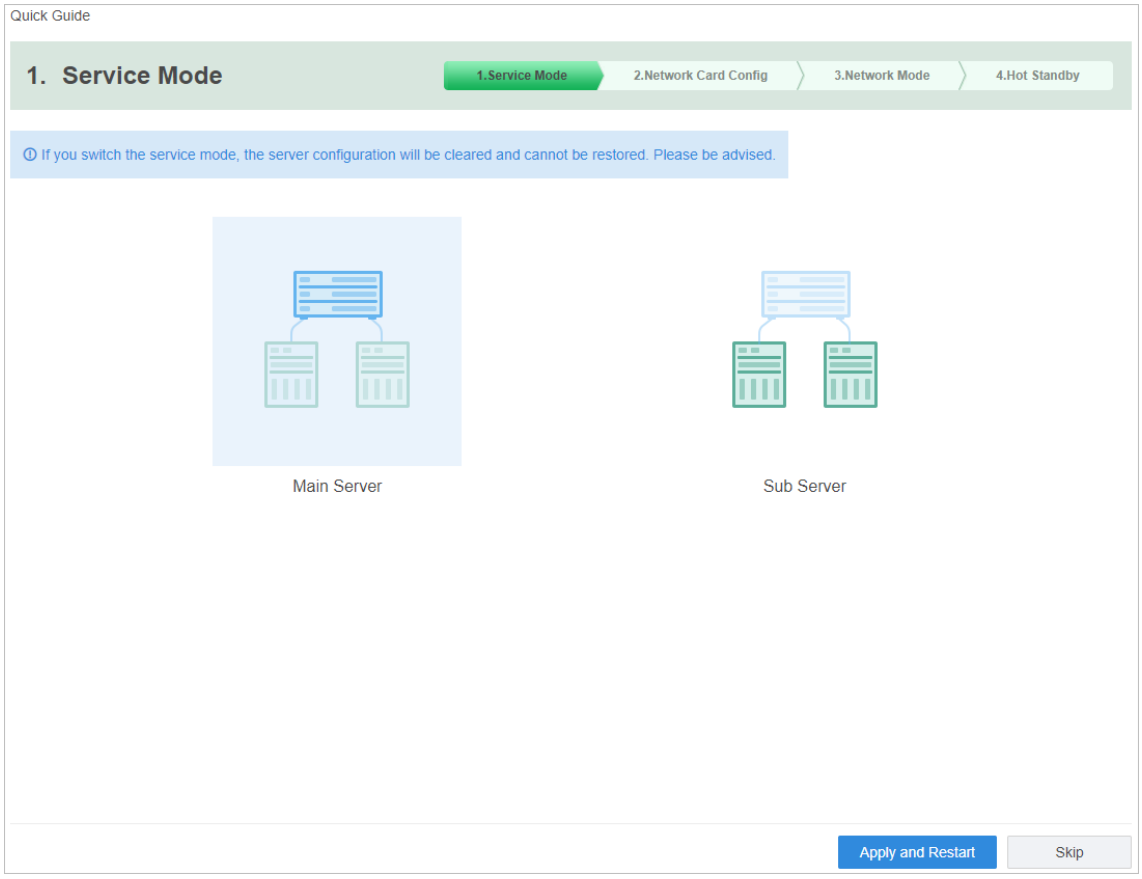
On the **Quick Guide** page, you can quickly configure network settings, LAN to WAN mapping, and hot standby.

Procedure

Step 1 Log in to the Config system.

Step 2 Click **Quick Guide**.

Figure 3-1 Service mode

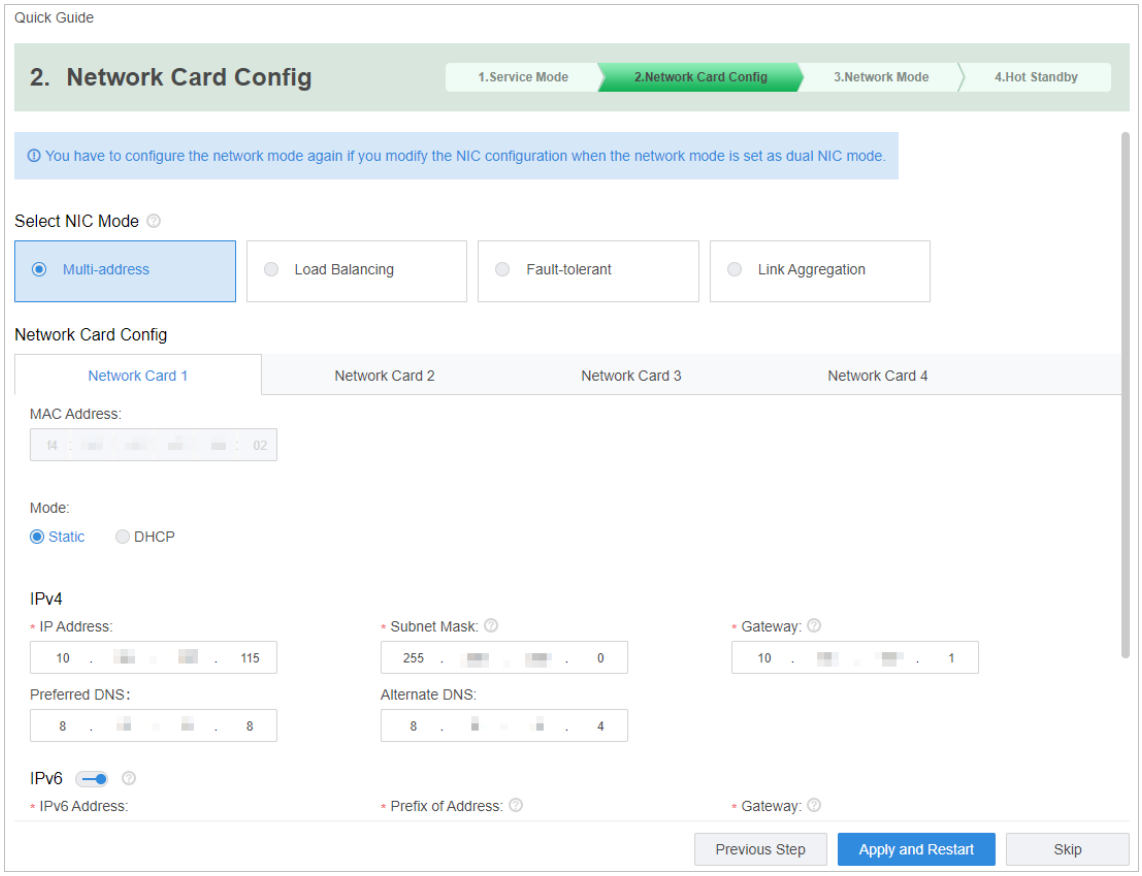


Step 3 Select **Main Server** or **Sub Server** as needed, and then click **Apply and Restart**.

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 3-2 Network card configuration



Step 5 Configure the parameters.

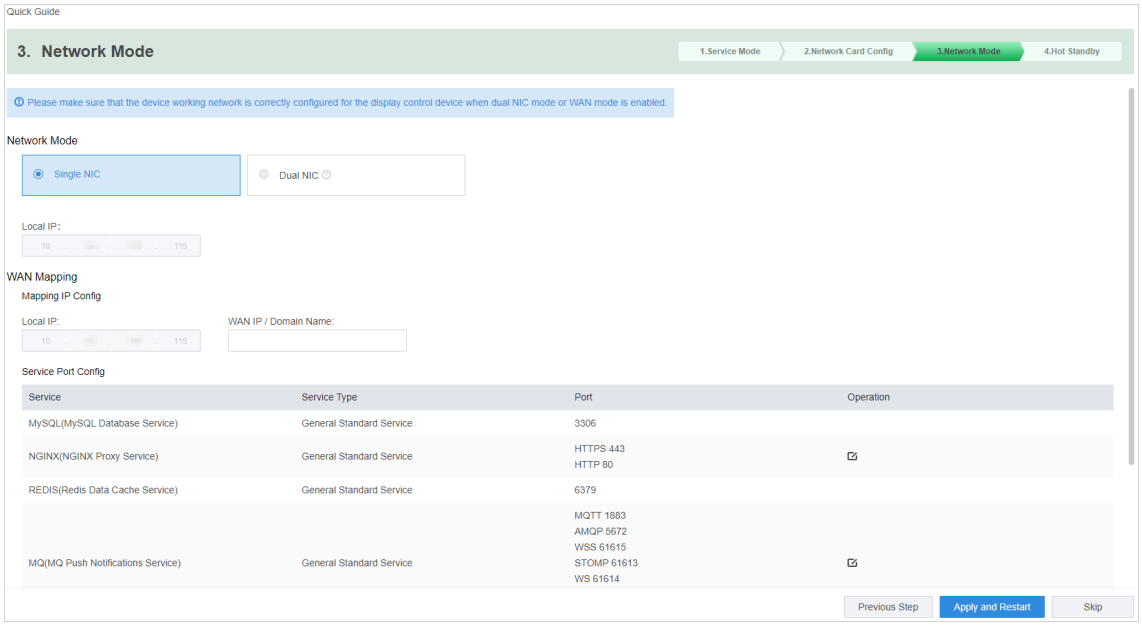
Table 3-1 Network card parameter description

Parameter	Description
Select NIC Mode	• 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	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.
Mode	The mode that the system gets IP. • **Static** : Manually configure **IP Address**, **Subnet Mask**, and **Default Gateway**. • **DHCP** : When there is DHCP server in the network, and DHCP is enabled on the server, select **DHCP**, and the system acquires IP address automatically.
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 3-3 Network mode



Step 8 Configure the parameters.

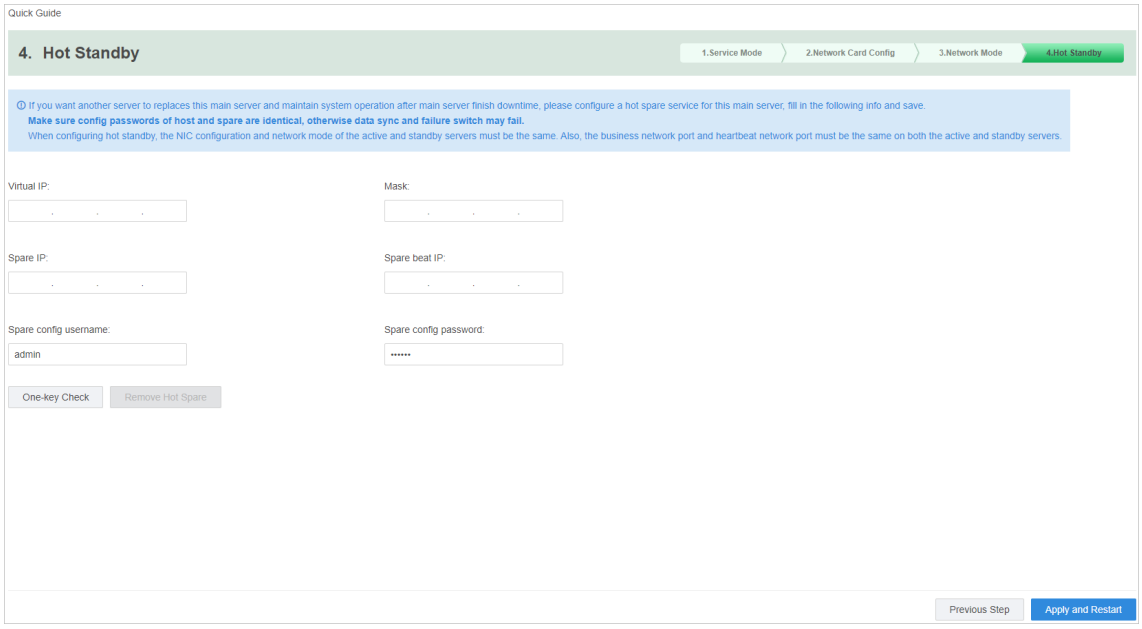
Table 3-2 Network mode parameter description

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".
Stream Acquisition Network	Prioritize Network to Acquire Stream	When selecting **Dual NIC** network mode, you can select the working network of the decoding device on the platform. When decoding to the video wall, the system will provide the corresponding IP address to the decoding device for video on wall.

Step 9 Click **Apply and Restart**.

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

Figure 3-4 Hot standby



Step 11 Configure the parameters.

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

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 network ports, IP addresses, network, CPU, and disks.

3.4 Network Config

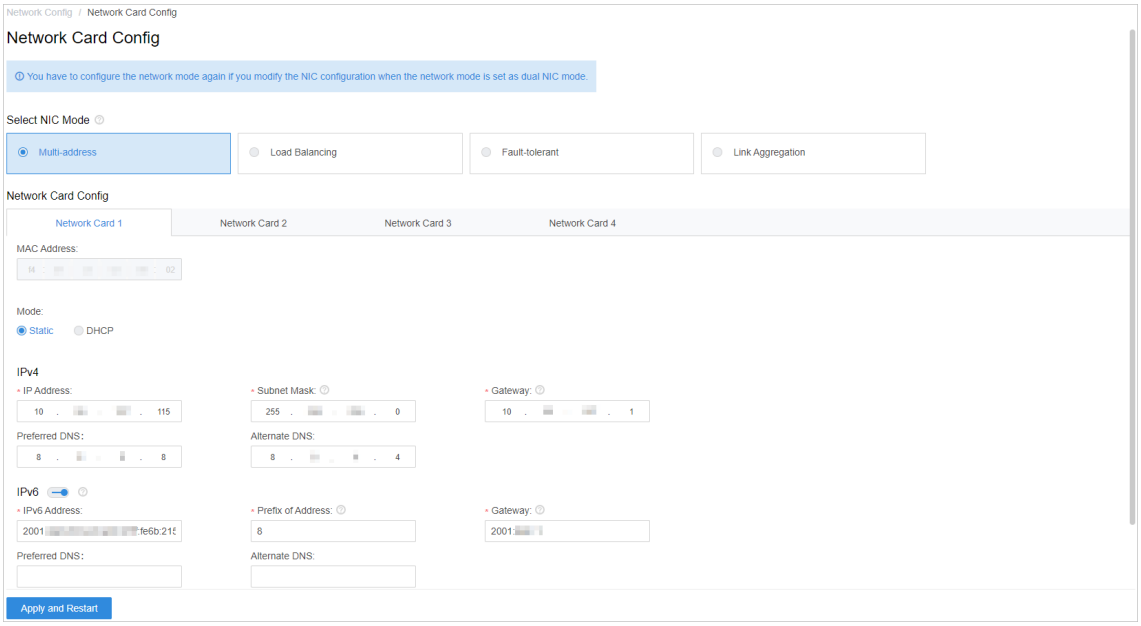
3.4.1 NIC Config

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

Procedure

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

Figure 3-5 Network card configuration



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

Table 3-3 Network card parameter description

Parameter	Description
Select NIC Mode	• 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.
Mode	The mode that the system gets IP. • **Static** : Manually configure **IP Address**, **Subnet Mask**, and **Default Gateway**. • **DHCP** : When there is DHCP server in the network, and DHCP is enabled on the server, select **DHCP**, and the system acquires IP address automatically.
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.

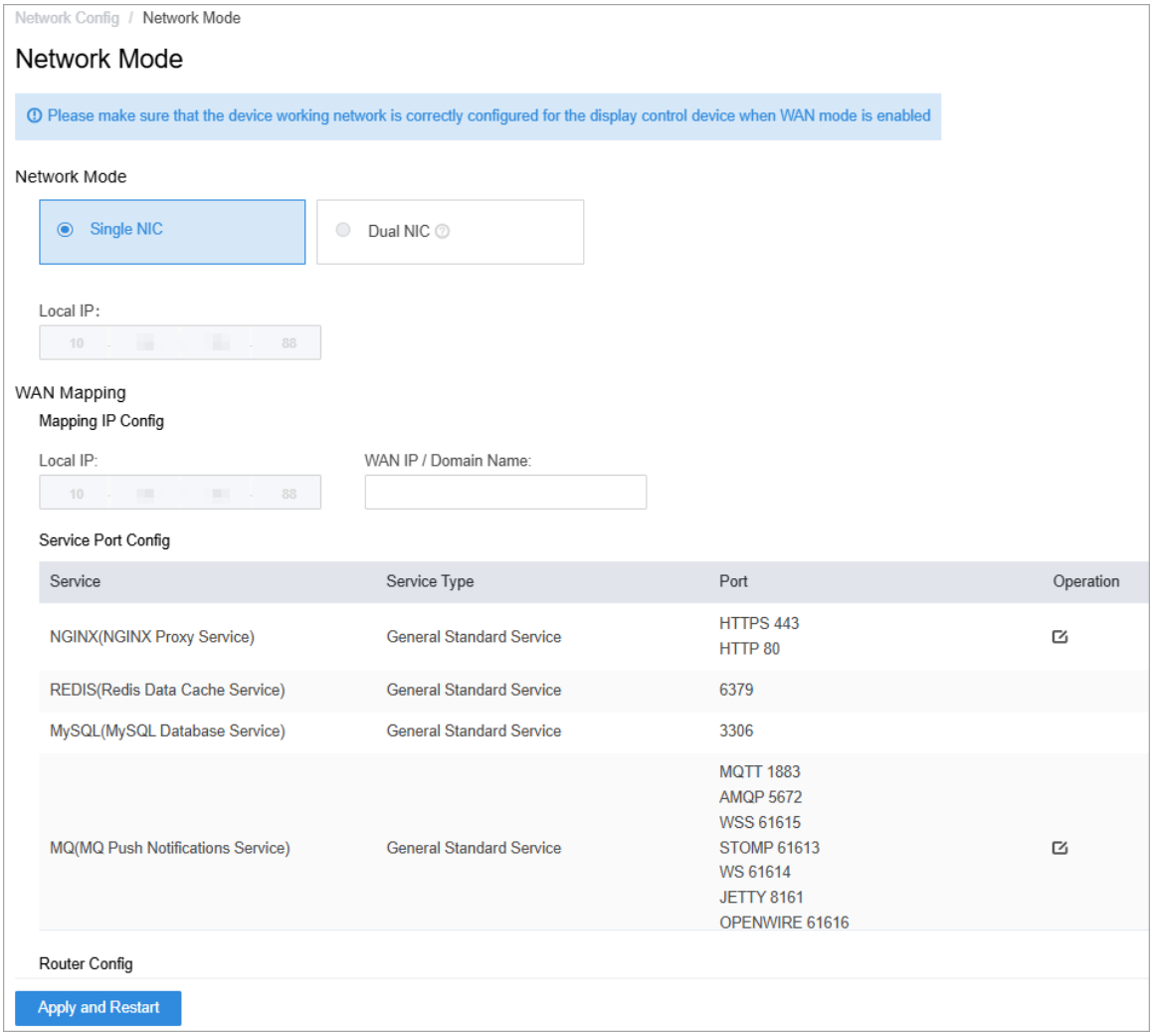
3.4.2 Network Mode

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 3-6 Network mode



Step 2 Configure the parameters.

Table 3-4 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.

Mode	Parameter	Description
	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".
Stream Acquisition Network	Prioritize Network to Acquire Stream	When selecting **Dual NIC** network mode, you can select the working network of the decoding device on the platform. When decoding to the video wall, the system will provide the corresponding IP address to the decoding device for video on wall.

Step 3 Click **Apply and Restart**.

3.4.3 Connection Detection

Check whether the IP address 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**.

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

3.4.4 Route Settings

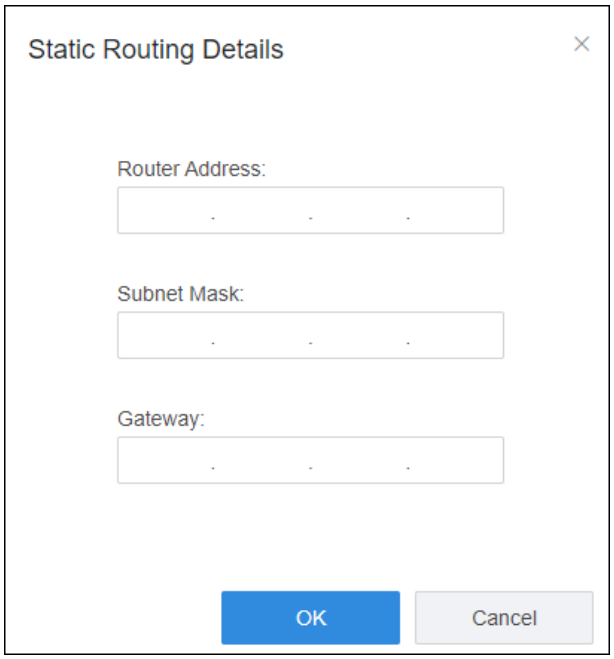
Add static route to establish access between servers in different network segments.

Procedure

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

Step 2 Click **Manually Add**.

Figure 3-7 Add statistic router



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

Table 3-5 Parameter description

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

Step 4 Click **OK**.

3.4.5 802.1x

802.1X is a port-based access control and authentication protocol. It is used to prevent unauthorized devices or users from accessing the LAN through access ports. When 802.1X authentication is enabled on the network, devices (such as servers or user terminals) need to be authenticated by an authentication server (such as a RADIUS server), otherwise they will not be able to access network resources.

Background Information

In a multi-NIC scenario, if the switch is used as an authentication server, and 802.1x authentication is required, the corresponding aggregation port on the switch side must also enable authentication. Enabling authentication on a single physical network port will be invalid.

Procedure

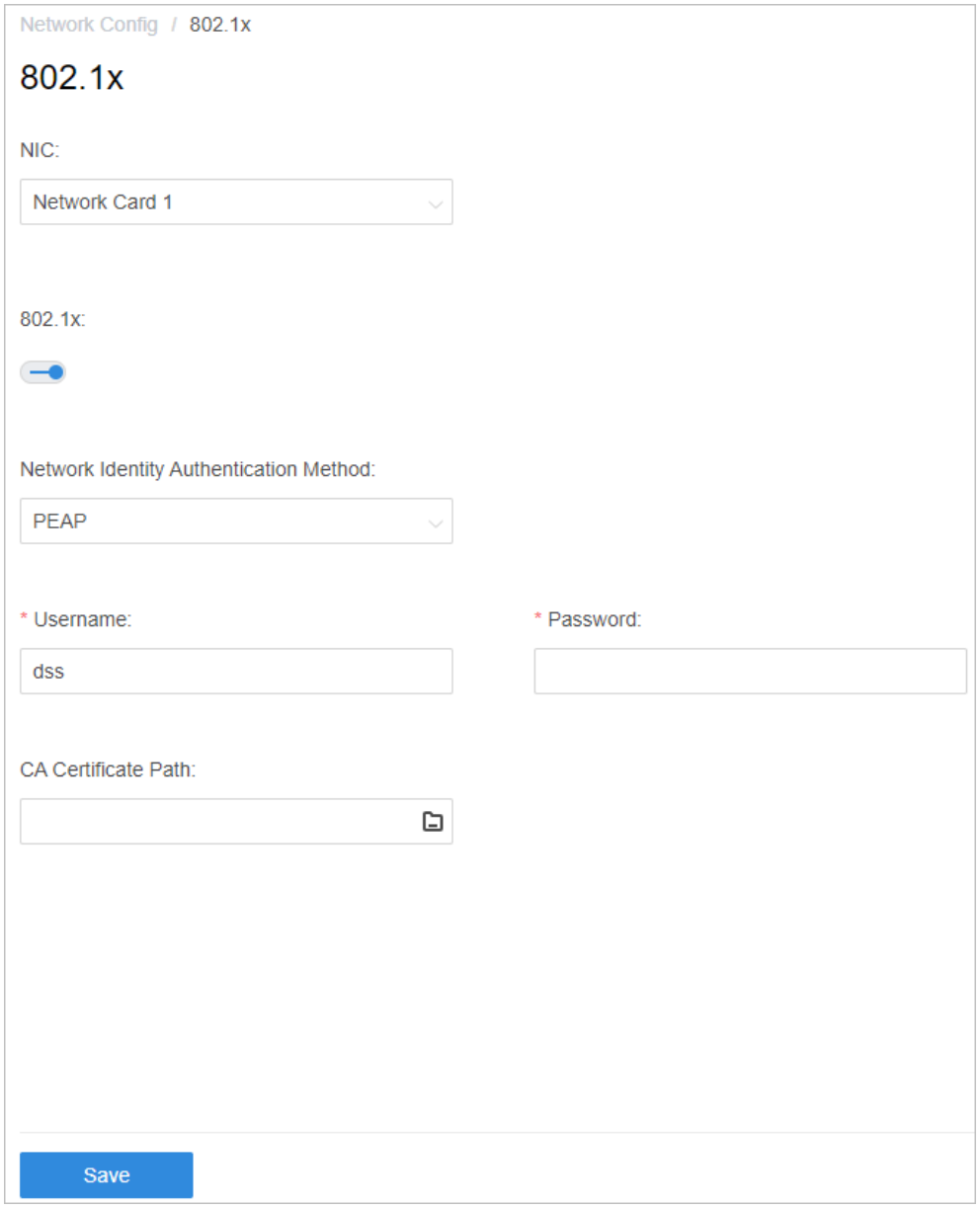
Step 1 Select **Network Config** > **802.1x**.

Step 2 Select the NIC name as needed, and click to enable 802.1x authentication.

Step 3 Select the authentication mode, and then configure parameters.

- PEAP: Protected Extensible Authentication Protocol.
  1. Select **PEAP** from the authentication mode.
  2. Enter the username and password that have been authenticated on the server (make sure that the username and password have been configured and authorized on the server).
  3. Click to select the CA certificate.

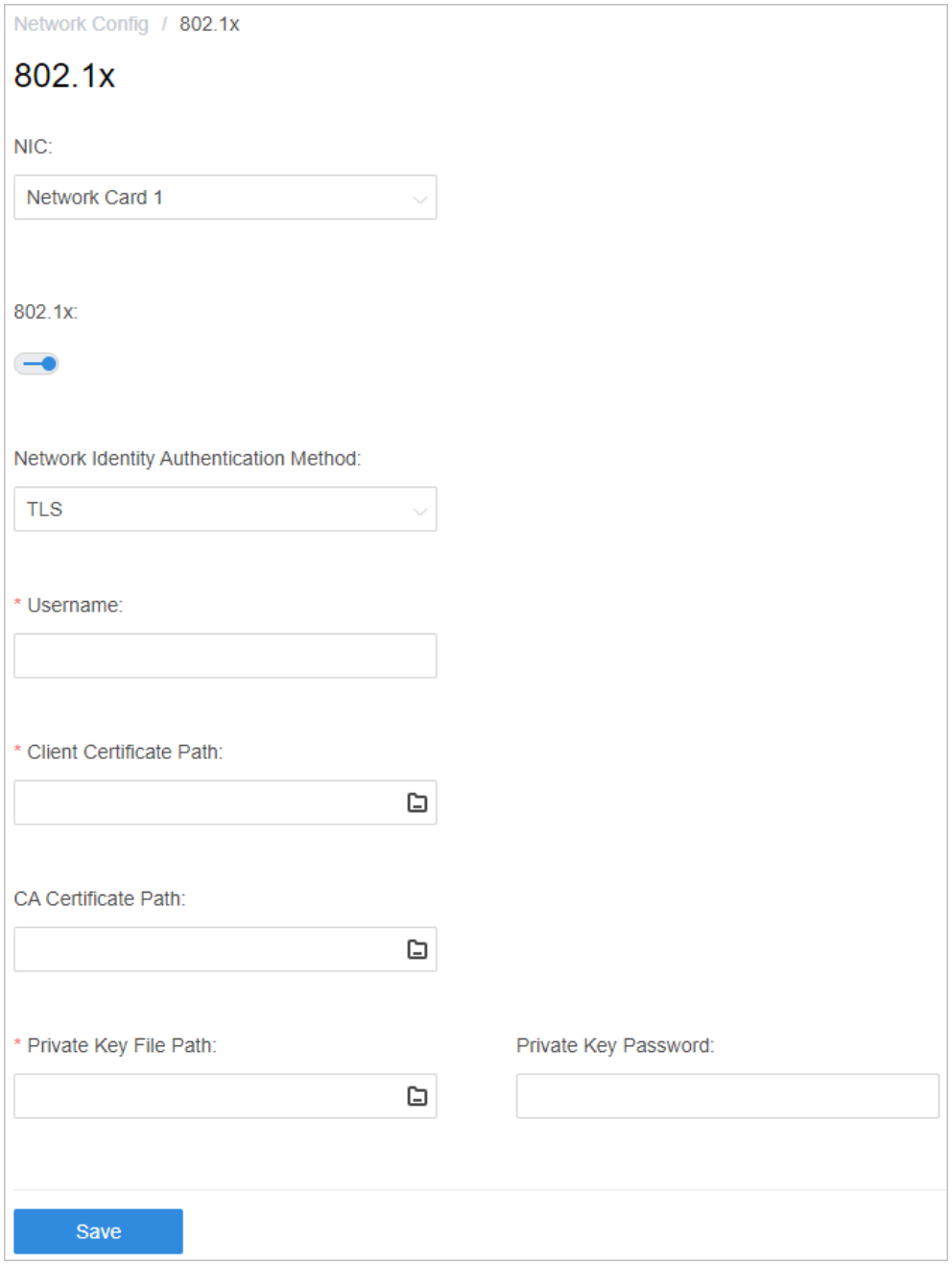
Figure 3-8 802.1x (PEAP)



- TLS: Transport Layer Security. It is applied in 2 communication application programs to ensure data security and integrity.

  1. Select **TLS** from the authentication mode.
  2. Enter the username.
  3. Click to select the client certificate, CA certificate, and private key file respectively, and set the private key password.

Figure 3-9 802.1x (TLS)



Step 4 Click **Save**.

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 Config

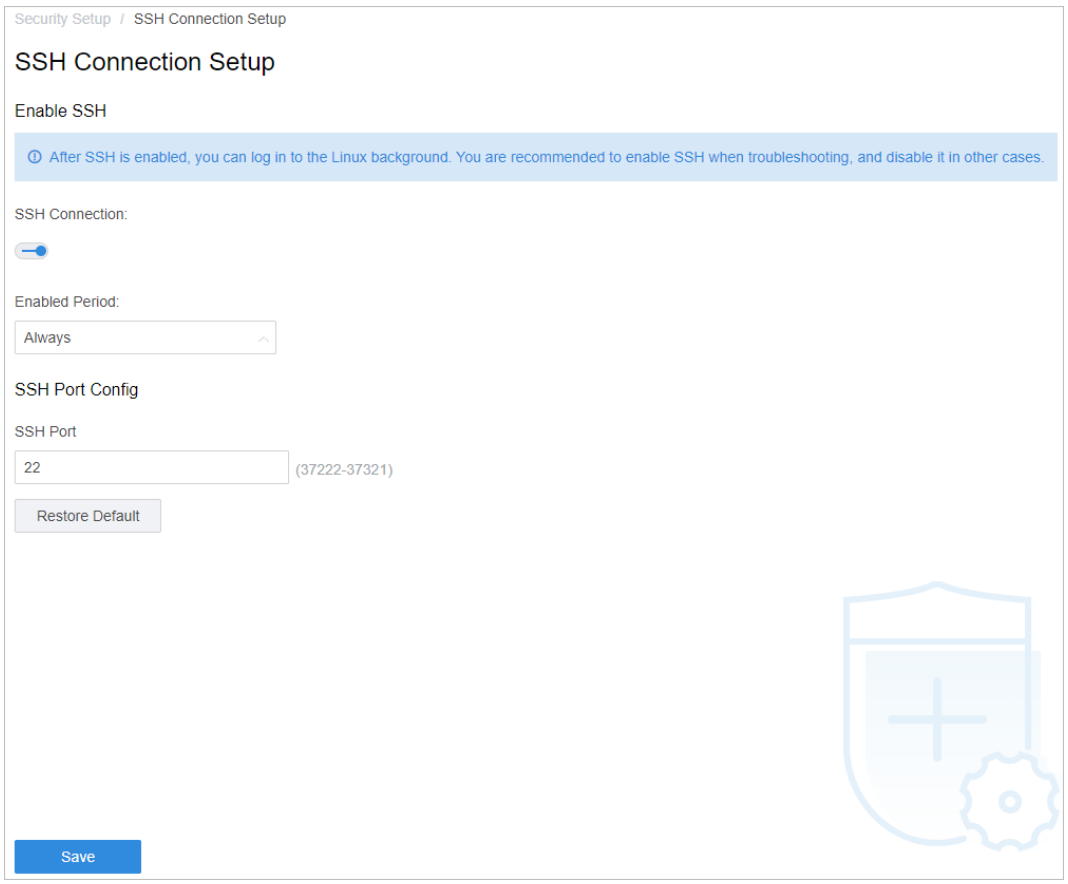
3.6.1 SSH Connection Service

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 3-10 SSH connection



Step 2 Enable **SSH Connection** , and then set the **Enabled Period** and port.

Enabled Period : You can select from **Always**, **30min**, **1h**, **2h**, **6h**, or **24h**. When the duration expires, the SSH connection will automatically stop.

Disable **SSH Connection** after debugging.

Step 3 Click **Save**.

3.6.2 TLS

For the security of system communications, only TLS 1.3 and TLS 1.2 protocols are supported. User a browser that supports TLS 1.3 or TLS 1.2.

3.6.3 Trusted Verification

After enabling trusted verification, only executable files that are correctly signed will be allowed to run normally on the platform.

Step 1 Select **Security Config** > **Trusted Verification**.

Step 2 Enable **Trusted Verification**. means enabled.

3.7 System Maintenance

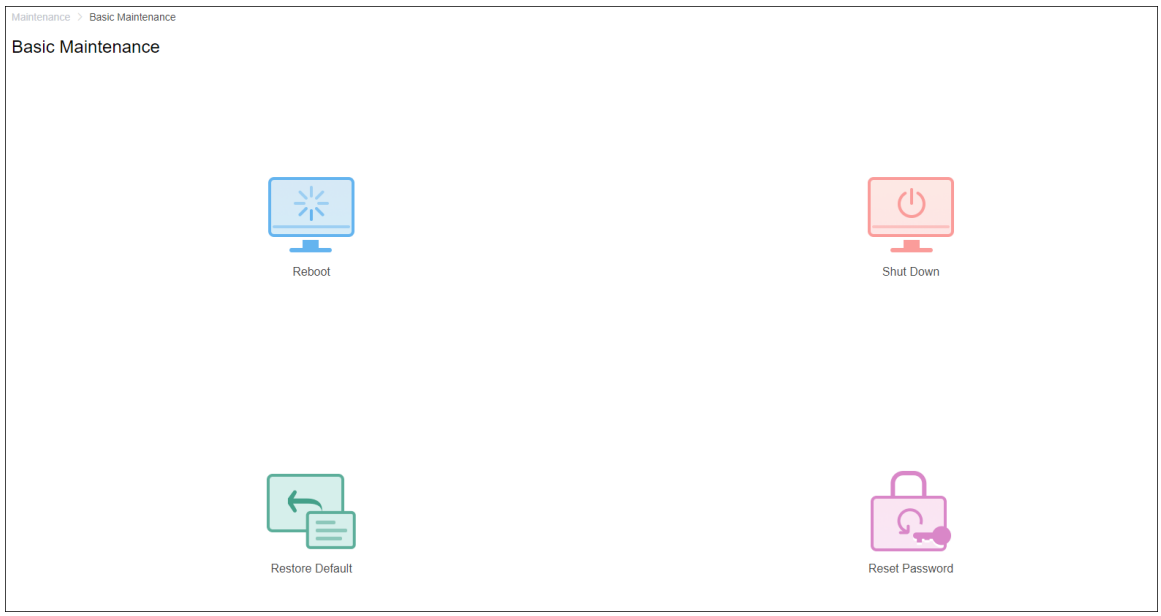
3.7.1 Basic Maintenance

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

Procedure

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

Figure 3-11 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.

Select **System Maintenance** > **Database Maintenance**, 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

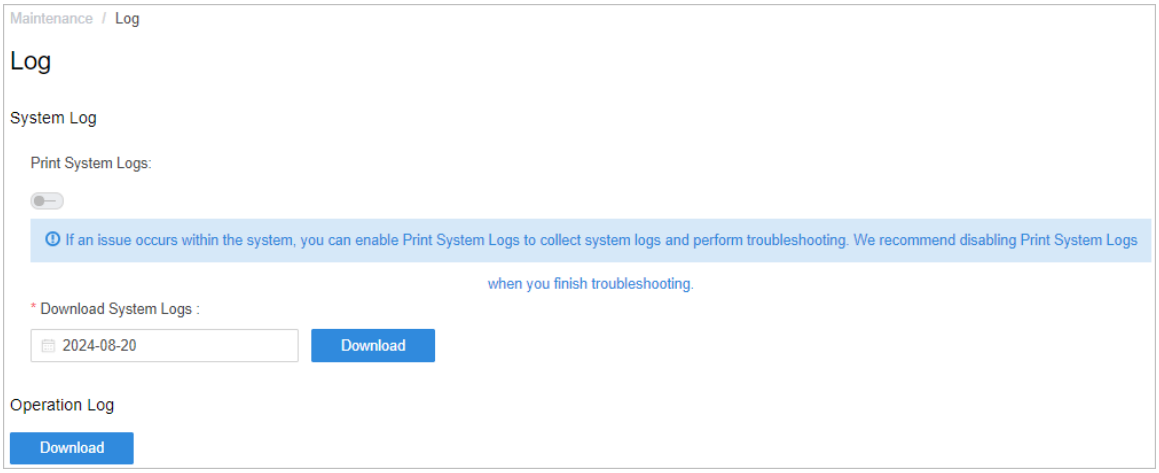
You can download system and operation logs to your computer.

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

Step 2 Download system and operation logs.

- Download system logs.
  1. Enable **Print System Logs** when there is issue with the system, so that you can collect system logs for troubleshooting. We recommend disabling it after troubleshooting.
  2. Select the date, and then click **Download** to download the system logs of the selected date.
- Download operation logs: Click **Download** of **Operation Log**.

Figure 3-12 Log



3.7.4 Updating System and Program

You can update the system and the program to enjoy enhanced performance and functions. Before updating, contact technical support to get the update package.

Procedure

Step 1 Select **System Maintenance** > **System and Program Update**.

Step 2 Update the system or the program.

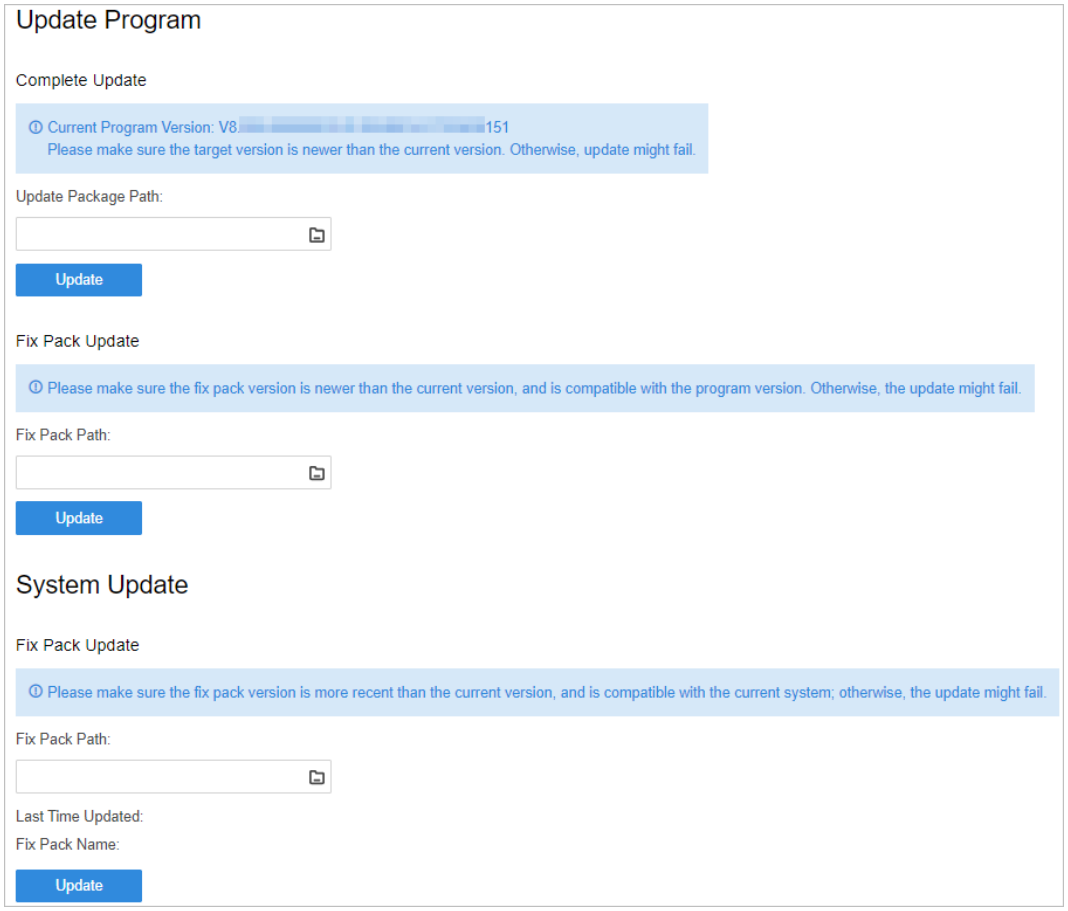
- Update the program: Select complete update or fix pack update, and then click to select the update package.

  When updating the system, you can update both the system and the trusted runtime library, or update the trusted runtime library only.

- Update the system: Select fix pack update, and then click to select the update package.

Step 3 Click **Update**.

Figure 3-13 System and program update



3.8 Basic Config

3.8.1 User Management

You can change the login password of admin user, lock the server, reset security questions, and bind IP addresses that can access the platform.

Procedure

Step 1 Select **Basic Config** > **User Management**.

Step 2 Perform the following operations.

- Change password
  1. Enable the **Reset Password** function.
  2. Enter the old password, set a high-security password according to the on-screen password setting requirements, and confirm the new password.
  3. Set the password change cycle. Seven days before the password expires, the system will remind you of the remaining expiration days on the upper-right corner of the page after you log in. If you log in after the expiration date, you will have to change your password on the login page before you can log in.

     All services will be restarted after changing the password. Check whether the services have been restarted successfully during use.
- Lock the server

  After selecting **Server Lock**, if you access the server from the LCD panel or a connected monitor, the screen will automatically lock after 5 minutes of inactivity.
- Reset security questions
  1. Click **Reset**, and then enter the login password.
  2. Reset the answers to the security questions, and then click **Save**.
- Bind IP address

  Enable **IP Address Binding**, and then add IP addresses. You can only log in to the platform using the defined IP addresses.

  A maximum of 5 IP addresses can be added.

Step 3 Click **Save**.

3.8.2 Time Config

Set time zone and time where the server is located.

Procedure

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

Step 2 Configure the parameters.

Table 3-6 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 that 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 Logging in to DSS Web Client

Procedure

Step 1 Enter https://*platform IP address* in the browser address bar, and then press Enter.

If it prompts **Your connection is not private**, select **Advanced** > **Proceed to xx.xx.xx.xxx (unsafe)** (xx.xx.xx.xxx refers to the platform IP address).

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 "4.3.5 Importing Domain Users".

Step 3 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.

- Keep the security questions and answers properly. Otherwise, your password cannot be recovered if you forget it. If you forget your password, you can click **Forgot password?** to reset it by answering your security questions.
- If you fail to log in twice consecutively, the system will display a random verification code, which is required for subsequent logins. If you fail to log in 5 times consecutively, your account will be locked.

Supports two-factor authentication, that is, a verification method that enhances account security by requiring a password (first factor) and a verification code (second factor) to log in.

a. Go to > **System Parameters** > **Security Config**, enable **Two-Factor Authentication**, and then select authentication by email or authenticator.
   - Email: Make sure that the email server is configured correctly, and the login user has configured an email address to receive the verification code.
   - Authenticator: You need to have Microsoft or Google authenticator installed on your phone.

b. Go to > **User** > **Role Users** > **User Management**, and then enable **Two-Factor Authentication** when editing the user.

c. To log in, you must enter your login password, the verification code received in your email (if email authentication is selected), or a random verification code (if authenticator authentication is selected).

   If authentication fails, you can log in by answering security questions or by resetting your system password to disable two-factor authentication.

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 App**, 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 an 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**.

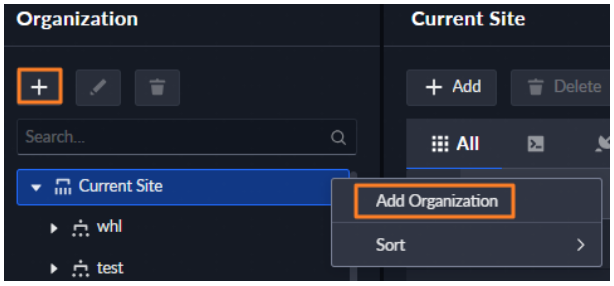
Step 2 Click .

Step 3 Add an organization.

1. Select a parent organization.
2. Click .

You can also point to the organization name, click , and then select **Add Organization** to add the organization.

Figure 4-1 Add an organization



3. Select the parent organization, enter the name of the organization, and then select the roles.
4. Click **OK**.

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**.

4.2.2 Managing Devices

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 .

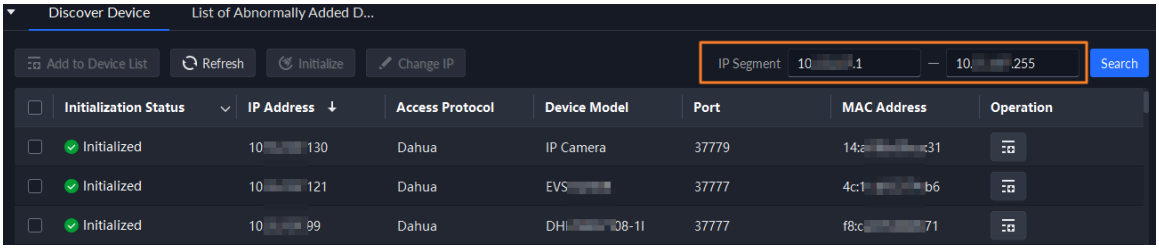
Step 3 Click **Discover Device**.

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

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

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

Figure 4-2 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.

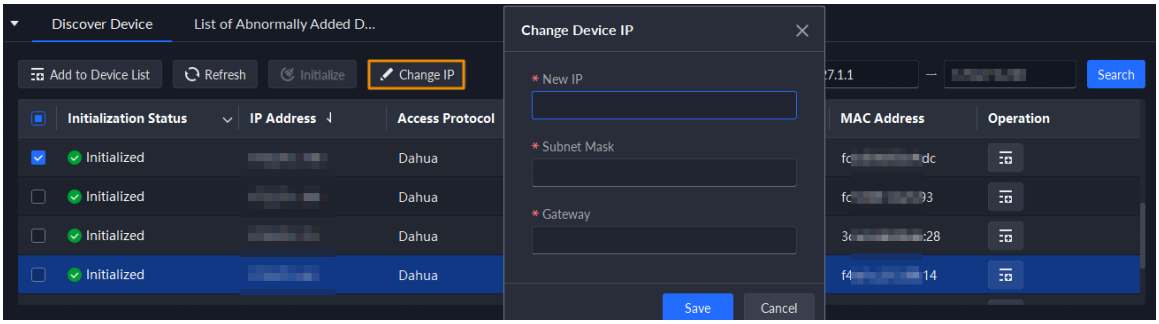
Procedure

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 4-3 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, and video intercom. This section uses 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 **Next Step**.

Select a mode to add the device.

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

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

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

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

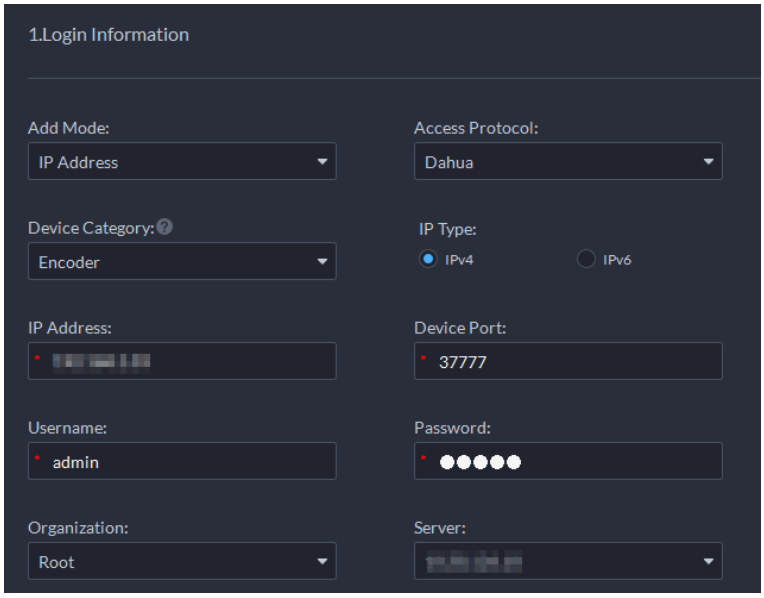
  - Before adding devices through P2P, you need to enable the P2P function from **System Parameters** > **Device Adding Config**.
  - P2P mode cannot be used to configure central recording plans when adding devices. If you need to configure central recording plans, it is recommended to select a different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

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

  - **Device Category** only supports **Encoder** and the **Access Protocol** only supports **RTSP**.
  - Only live view and playback of central recordings are supported if devices are added through this way. For details of configuring central storage plan, see "4.2.5.1 Adding Recording Plans One by One".

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

Figure 4-4 Add an encoder



Step 5 Enter the device information.

- Supports configuring device address and device owner.

  For device owner, click **Add** to add the owner's name, phone number, email address, and remarks.

  You can click to select the person that has been added to the platform.

  Supports adding 2 device owners for a device.
- When setting **Device Category** to **Alarm Controller**, you need to set the number of subsystem and zone.

Step 6 Click **OK**.

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

Related Operations

- Include Sub Organization: It is select by default. If selected, the system will display the devices of sub organization. If not selected, the system will only display the devices of the current organization.
- Click , and then you filter the device list fields to be displayed, such as device ID, IP address, device name, device manufacturer, access protocol, and more.
- Click **Online Status** , select **Online**, and then it will display devices that are **Online** or **Online (Asleep)**.

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.

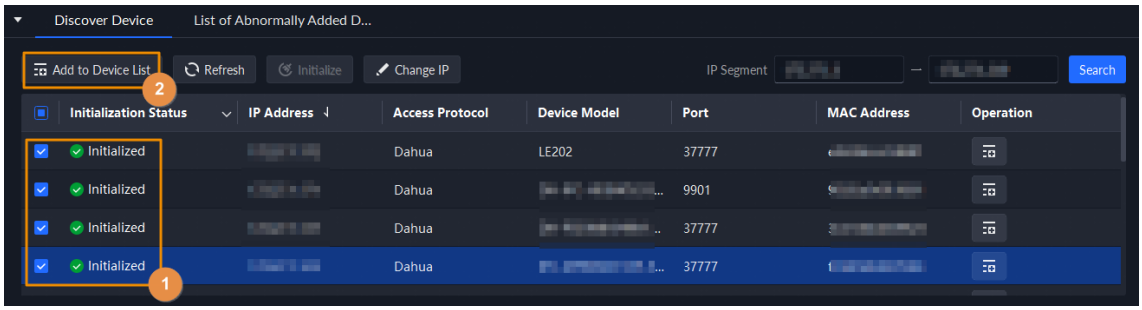
Procedure

Step 1 Search for devices.

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 4-5 Add in batches



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

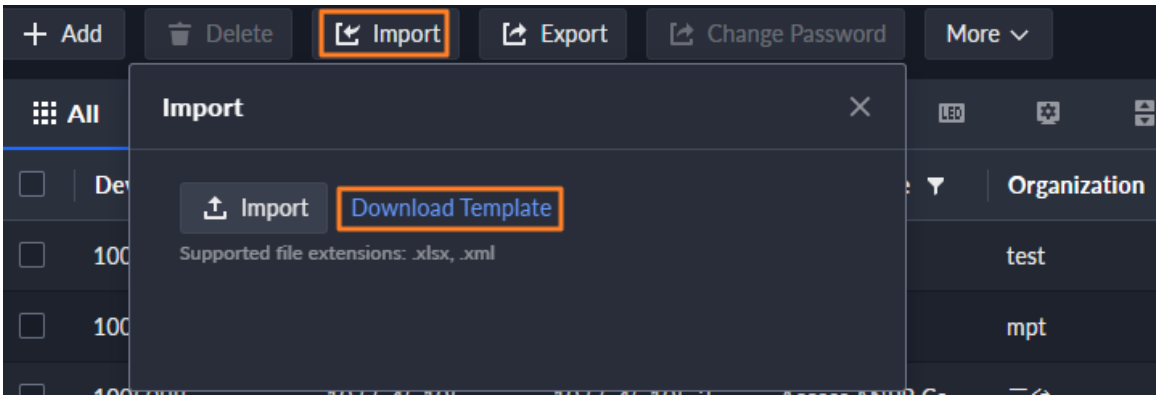
4.2.2.4.3 Importing Devices

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 4-6 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**.

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

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 SIP Information

The video intercom devices and access control terminals support the modification of SIP information, including updating SIP codes and SIP passwords.

Procedure

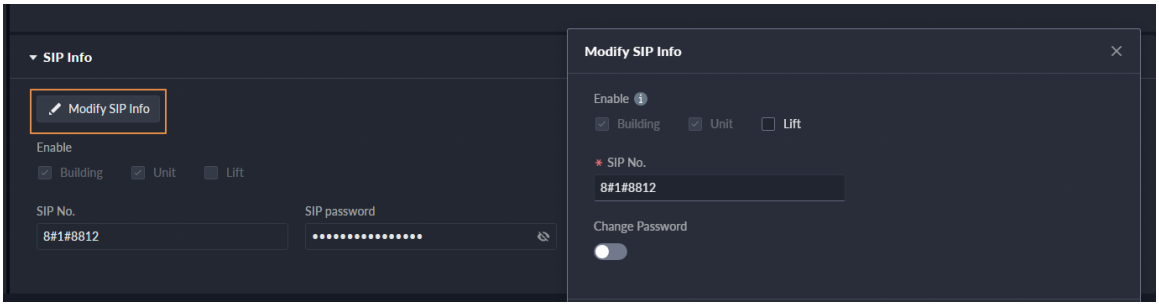
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click , and then filter the device by types.

Step 3 Click to go to device information page.

Step 4 On **SIP Info** area, click **Modify SIP Info**.

Figure 4-7 Modify the SIP information



- For the unit VTO or access control terminal that supports the video intercom function, the system automatically modifies the building and unit settings.
- Supports modifying the SIP number.
- Support the activation of the SIP password modification function, allowing the SIP password to be changed once enabled.

Step 5 Click **OK** to send the configuration to the device.

4.2.2.5.3 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 .

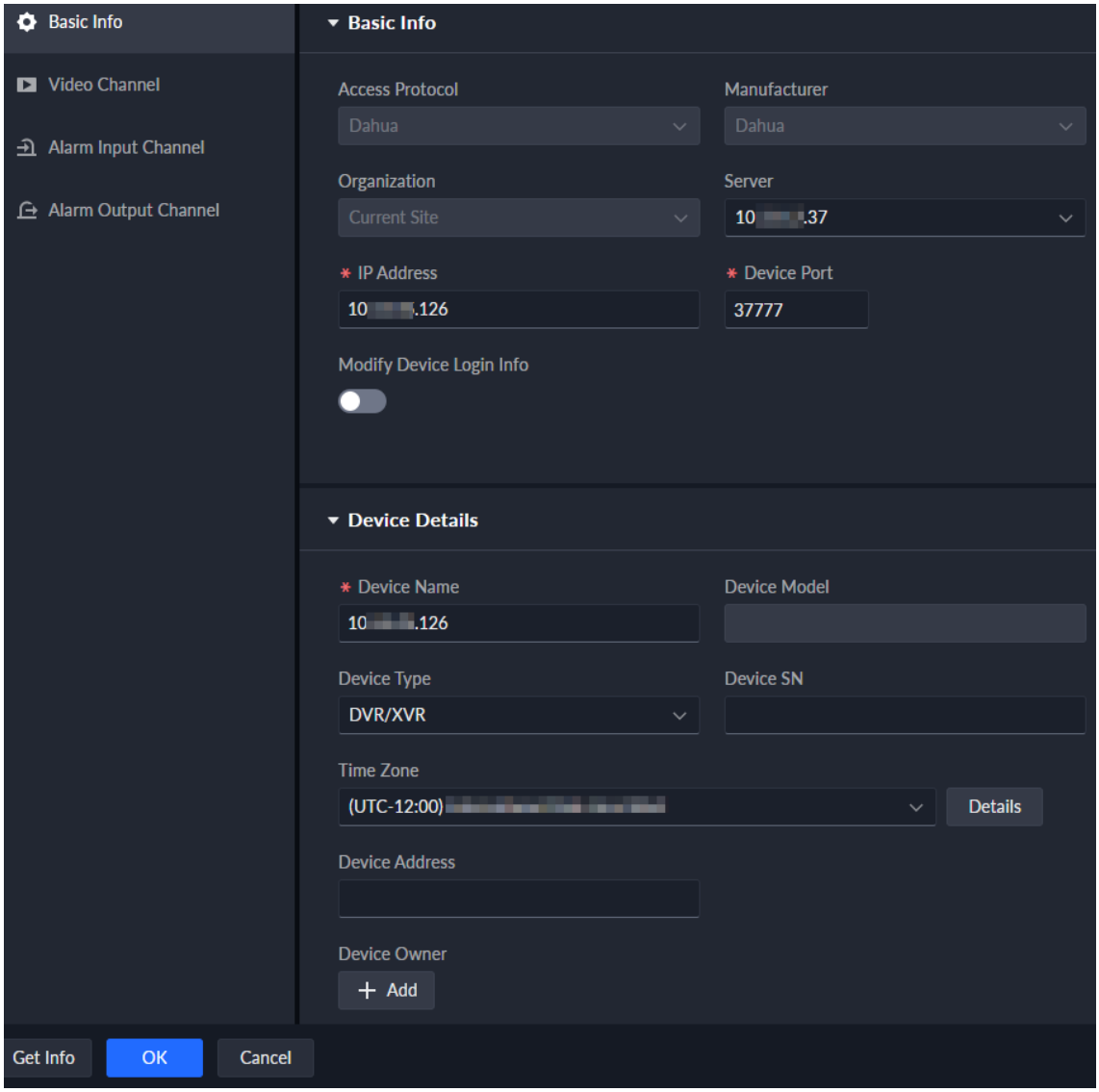
Step 3 Click of a device, and then edit device information.

- Click **Get Info** and the system will synchronize device information.
- For device owner, click **Add** to add the owner's name, phone number, email address, and remarks.

  You can click to select the person that has been added to the platform.

Supports adding 2 device owners for a device.

Figure 4-8 Basic information

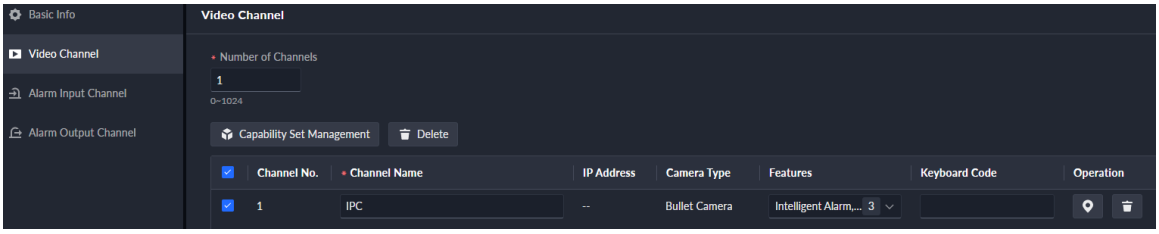


Step 4 Click **Video Channel**, and then configure the channel information, such as the channel name and channel features.

- 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 video channels.
- Select multiple channels, and then click **Capability Set Management** to configure the video channel capability in batches.

- Click  to edit the location information by entering the longitude and latitude, or marking devices on the map.
- Select multiple channels, and then click **Delete** to delete channels in batches.

Figure 4-9 Modify the information of video channel



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

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

- Alarm type includes remote external alarm, infrared detect, PIR, gas sensor, smoke sensor, glasses sensor, emergency button, stolen alarm, perimeter, preventer move, door sensor, active infrared sensor, fire alarm, duress password, water leak detection, siren, and wireless IR curtain.
- Alarm type supports custom. Select **Customize Alarm Type** in the **Alarm Type** drop-down list. Click **Add** to add new alarm type. It supports up to 30 custom alarm types.

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

Step 7 Click the **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**.

4.2.2.5.4 Getting Device Information in Batches

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

Procedure

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

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

Step 3 Select multiple devices.

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

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

Wait for the platform to finish the process.

Related Operations

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

4.2.2.5.5 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**.

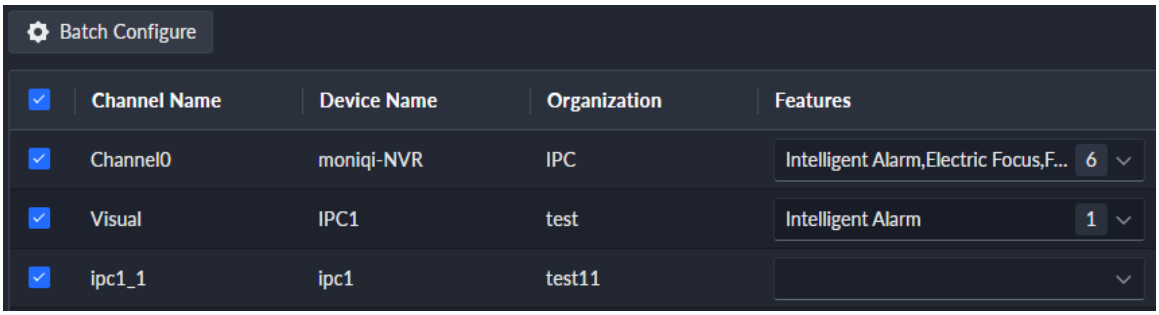
Step 3 In the **Capability Set Type** drop-down list, select a type, and then the platform will only display devices and channels that are configured with that type of capability set.

Step 4 Select the channels that you want to configure.

Step 5 Click the area below the **Features** column, and then select one or more features.

You can also select multiple channels, and then click **Batch Configure** to configure the features in batches.

Figure 4-10 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.

4.2.2.5.6 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.

Step 4 Enter the old and new passwords. The new password cannot be the same as any of the last 5 old passwords.

Step 5 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.

For devices added through P2P, you can only go to the device webpage through the platform PC client.

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.

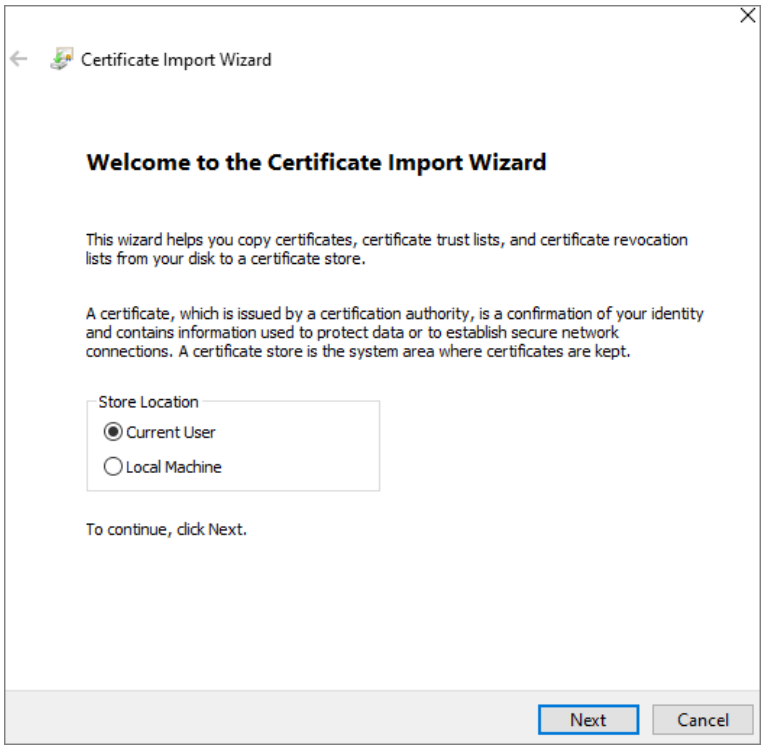
Procedure

Step 1 Log in to the webpage of the device, and then download the trusted CA root certificate.

Step 2 Double-click the certificate, and then click **Install Certificate**.

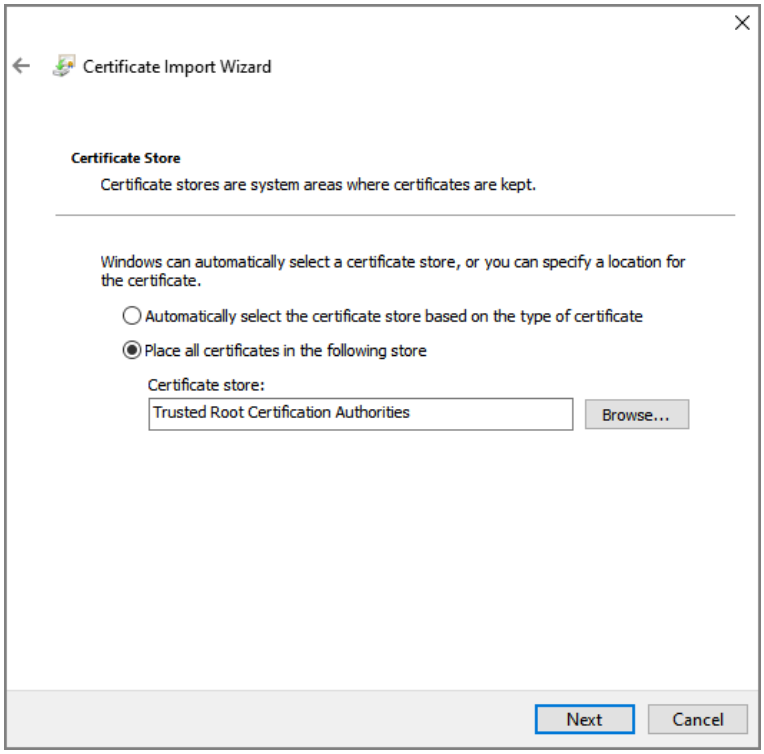
Step 3 Select **Current User** , and then click **Next**.

Figure 4-11 Certificate import wizard (1)



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

Figure 4-12 Certificate import wizard (2)



Step 5 Click **Finish**.

Step 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. 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 "8.3.2 Configuring Security Parameters".

- The encryption password is used to protect the export file. It consists of 8–32 uppercase or lowercase 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 select **More** > **Time Zone Settings**.

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.

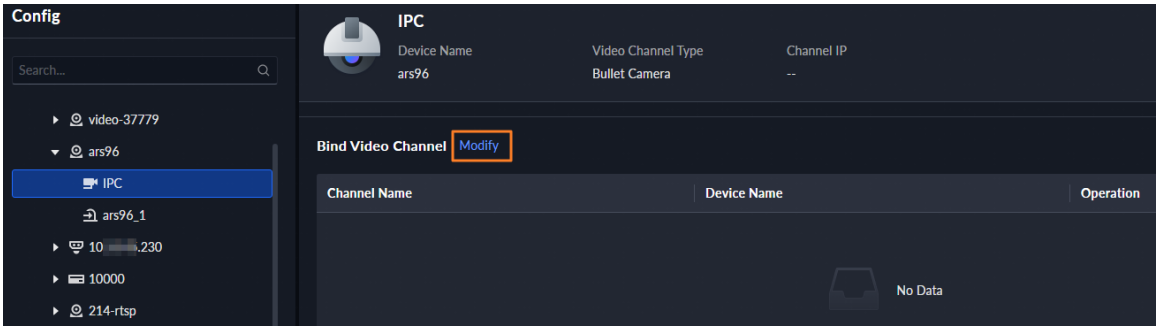
Procedure

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 4-13 Bind one or more channels



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

Step 5 Click **OK**.

4.2.4 Resource Maintenance

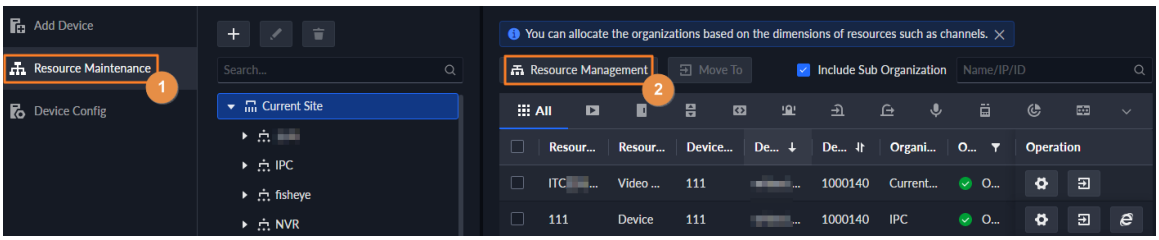
You can allocate the organizations based on the dimensions of resources such as channels.

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 **Resource Maintenance** > **Resource Management**.

Figure 4-14 Resource management



Step 3 Select the organization to be moved, the resource type (to filter the resources quickly), and the resource channels.

Step 4 Click **OK**.

Related Operations

- Move resource organization
  - Move resources one by one: Click , select **Only Devices** or **Devices and Their Channel Resources with Permissions**, select the organization that the resources will be moved to, and then click **OK**.
  - Move resources in batches: Select resources, click **Move To** , select the organization that the resources will be moved to, and then click **OK**.
- Click to go to the **Device Config** page. For details, see the following sections.
- Click to go to the device webpage. For details, see "4.2.2.6 Logging in to Device Webpage".

4.2.5 Adding Recording Plans

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

Prerequisites

Before adding a recording plan, you need to configure storage for the platform. For details, see "4.4 Configuring Storage".

4.2.5.1 Adding Recording Plans 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

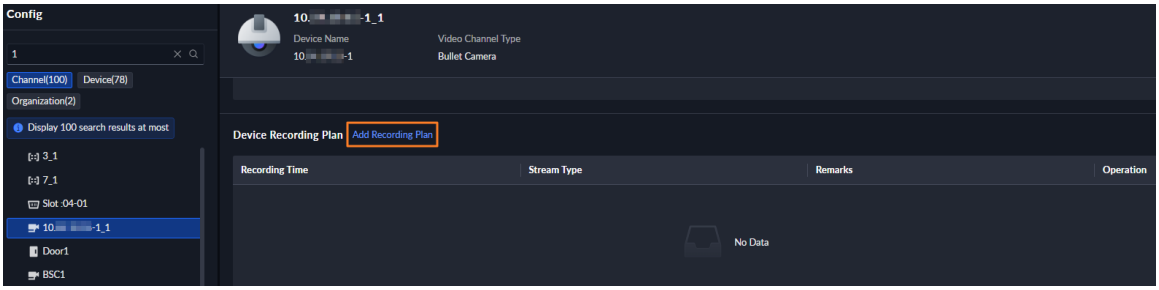
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

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 4-15 Add a center recording plan



  2. Configure the parameters.

Table 4-1 Parameter description of center recording plan

Parameter	Description
Position	Videos will be stored on the server by default. It cannot be changed.
Recording Type	◇ General recording: The device will continuously record videos within the defined periods. ◇ Motion detection recording: The device will continuously record videos within the defined periods on motion detections.
Stream Type	Select **Main Stream** , **Sub Stream 1** or **Sub Stream 2**. Videos recorded on the main stream will have the best quality, but they require more storage.
Remarks	Customizable description for the recording plan.
Recording Time	Select a default time template or click **Create Time Template** to add a new time template. See "4.2.7 Adding Time Template".

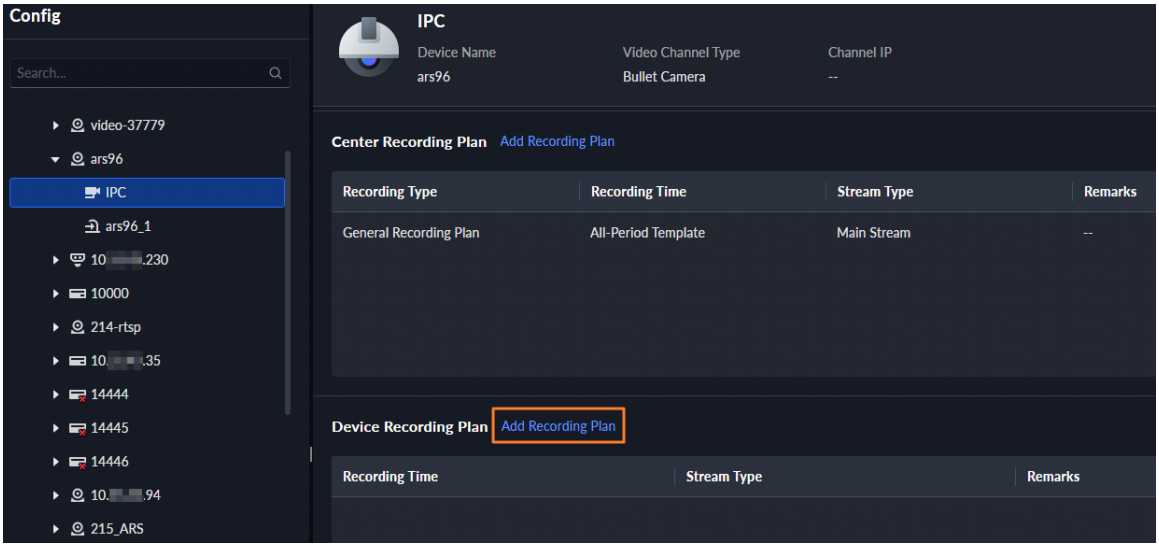
  3. Enable the recording plan as needed.
  4. Click **OK**.

- Configure a device recording plan.

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

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

Figure 4-16 Add a device recording plan



2. Configure the parameters.

Table 4-2 Parameter description of device recording plan

Parameter	Description
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 "4.2.7 Adding Time Template".

3. Enable the recording plan as needed.
4. Click **OK**.

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.

4.2.5.2 Adding Recording Plans in Batches

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

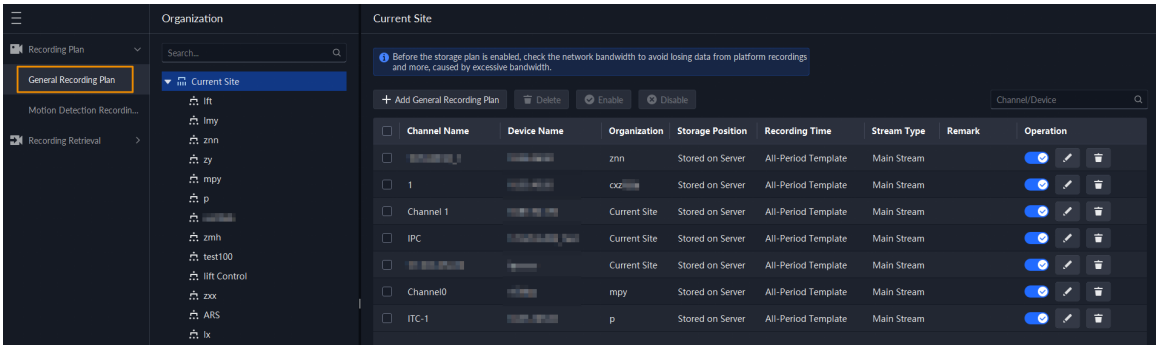
4.2.5.2.1 General Recording Plan

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**.

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

Figure 4-17 Center recording plan



Step 3 Configure the parameters.

Table 4-3 Parameter description

Parameter	Description
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. For details, see "4.2.7 Adding Time Template".
Recording Channel	Select the channels that you want to add the recording plan for.

Step 4 Enable the recording plan as needed.

Step 5 Click **OK**.

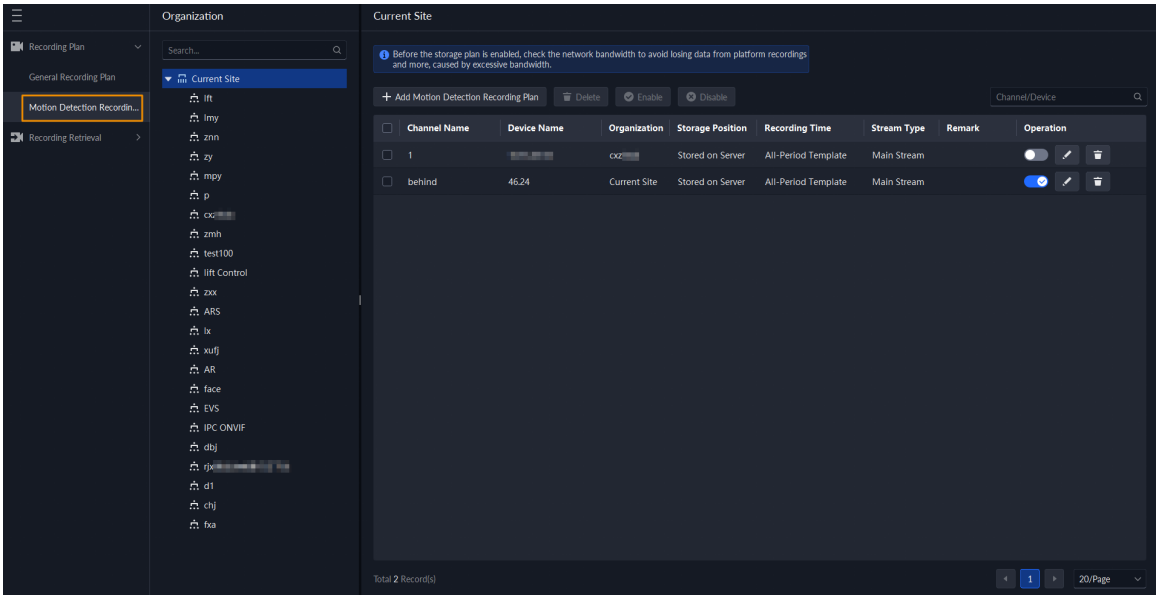
4.2.5.2.2 Motion Detection Recording Plan

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**.

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

Figure 4-18 Motion detection recording plan



Step 3 Configure the parameters.

Table 4-4 Parameter description

Parameter	Description
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 "4.2.7 Adding Time Template".
Recording Channel	Select the channels you want to add the recording plan for.

Step 4 Enable the recording plan as needed.

Step 5 Click **OK**.

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.

4.2.6 Adding Retrieval Plans

Configure retrieval plans 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 a channel one by one, or add one for multiple channels in batches.

Prerequisites

Before adding retrieval plans, you need to configure storage for the platform. For details, see "4.4 Configuring Storage".

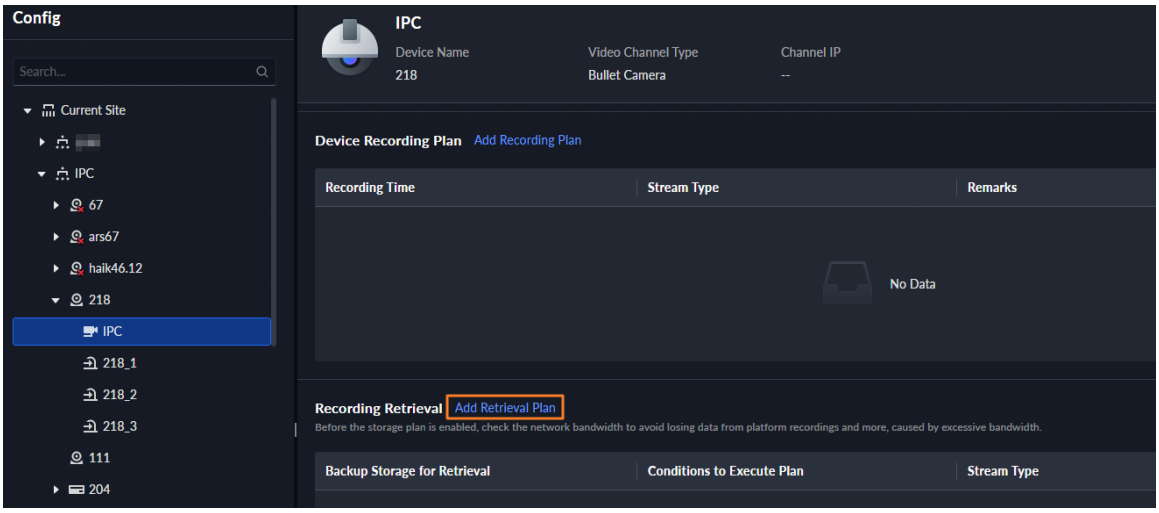
4.2.6.1 Adding Video Retrieval Plans One by One

Procedure

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

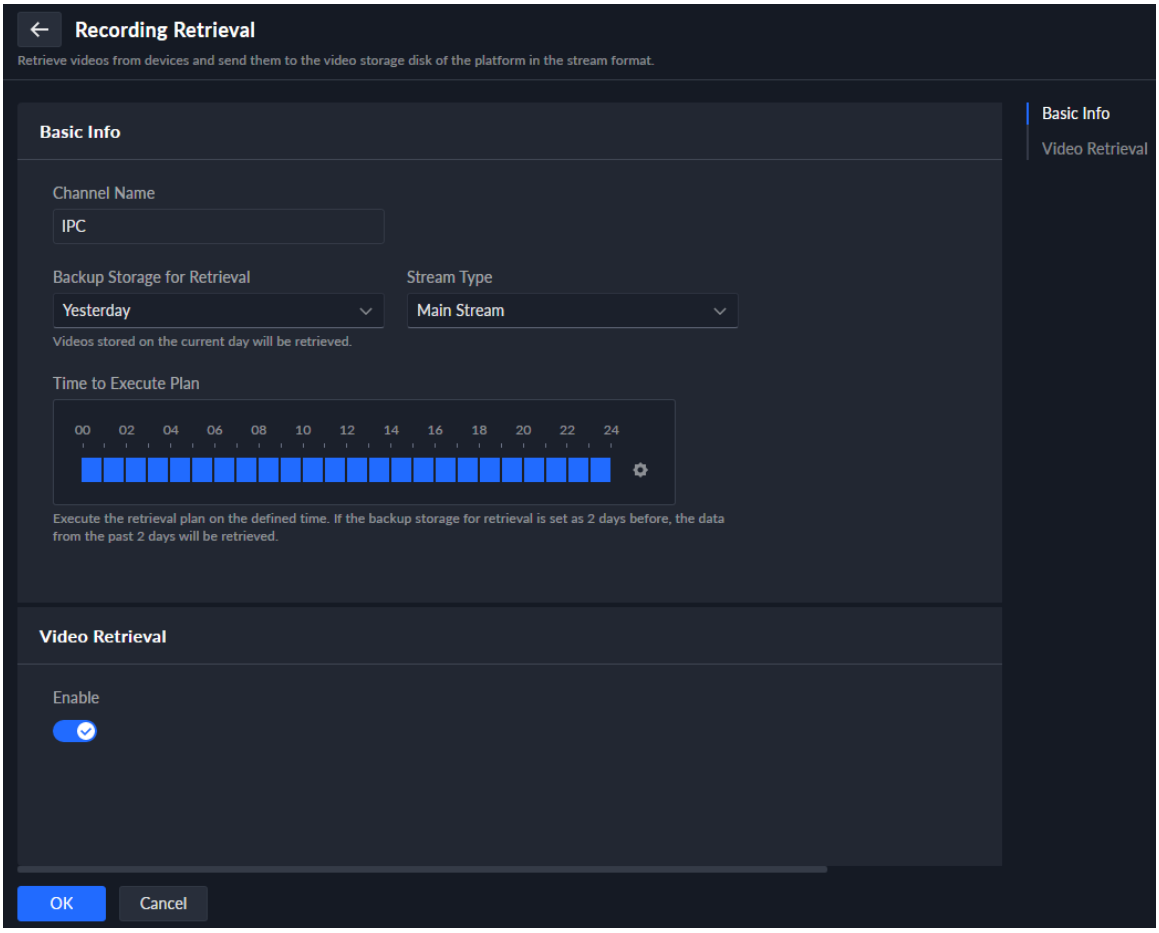
Step 2 Click **Device Config**.

Figure 4-19 Add a retrieval plan for a channel



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

Figure 4-20 Add a retrieval plan



Step 4 Configure the parameters.

Table 4-5 Parameter description

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

Step 5 (Optional) Enable the retrieval plan as needed. After being enabled, the videos stored on the device at the specified time will be automatically uploaded to the platform.

Step 6 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.

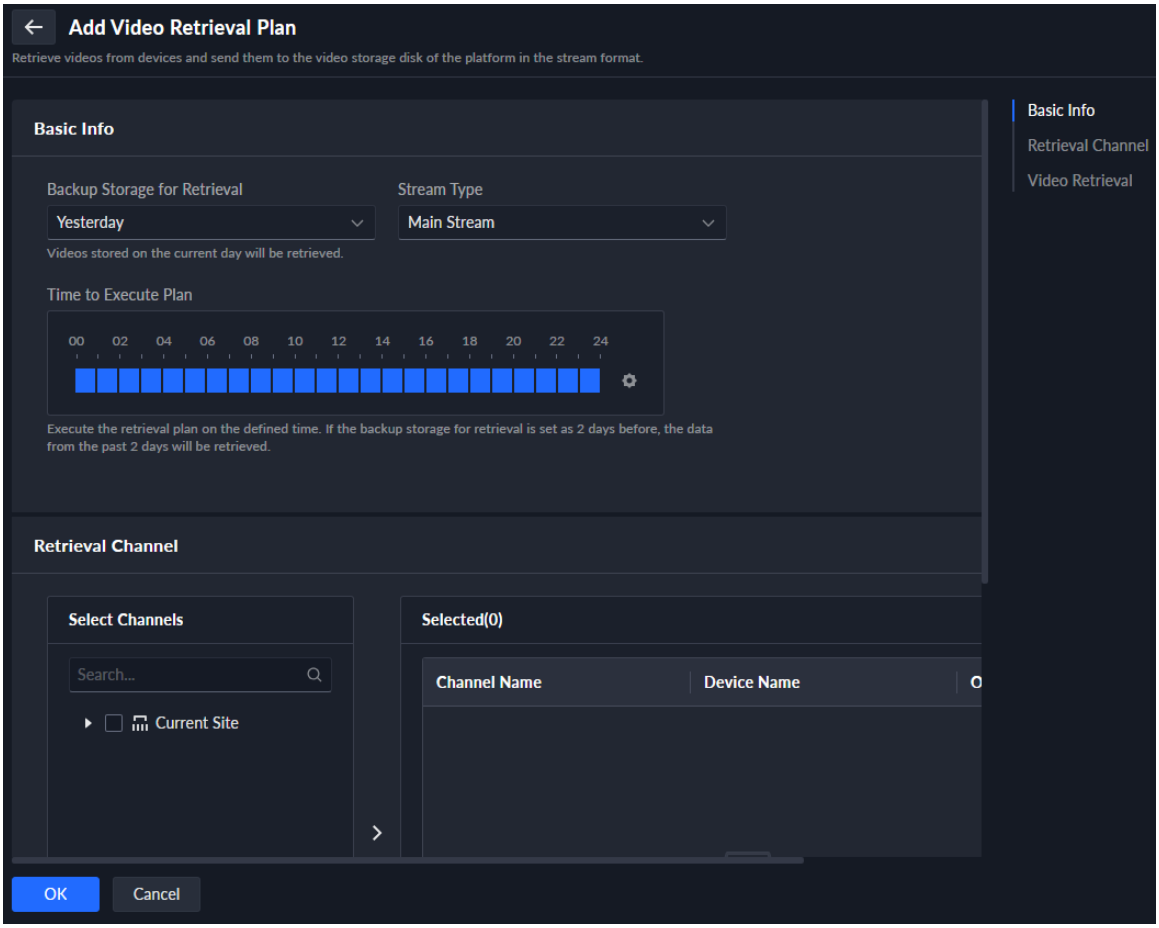
4.2.6.2 Adding Video Retrieval Plans in Batches

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**.

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

Figure 4-21 Configure a video retrieval plan



Step 3 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.

Parameter	Description
Stream Type	Select the stream type of the videos that you want to upload. If the videos are recorded on sub stream 1 and **Main Stream** is configured in this retrieval plan, uploading will fail.
Time to Execute Plan	Configure when to upload videos every day. Click to configure specific periods. You can configure up to 6 periods.

Step 4 Select devices in the **Retrieval Channel** section.

Step 5 (Optional) Enable the retrieval plan as needed. After being enabled, the videos stored on the device at the specified time will be automatically uploaded to the platform.

Step 6 Click **OK**.

4.2.7 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**.

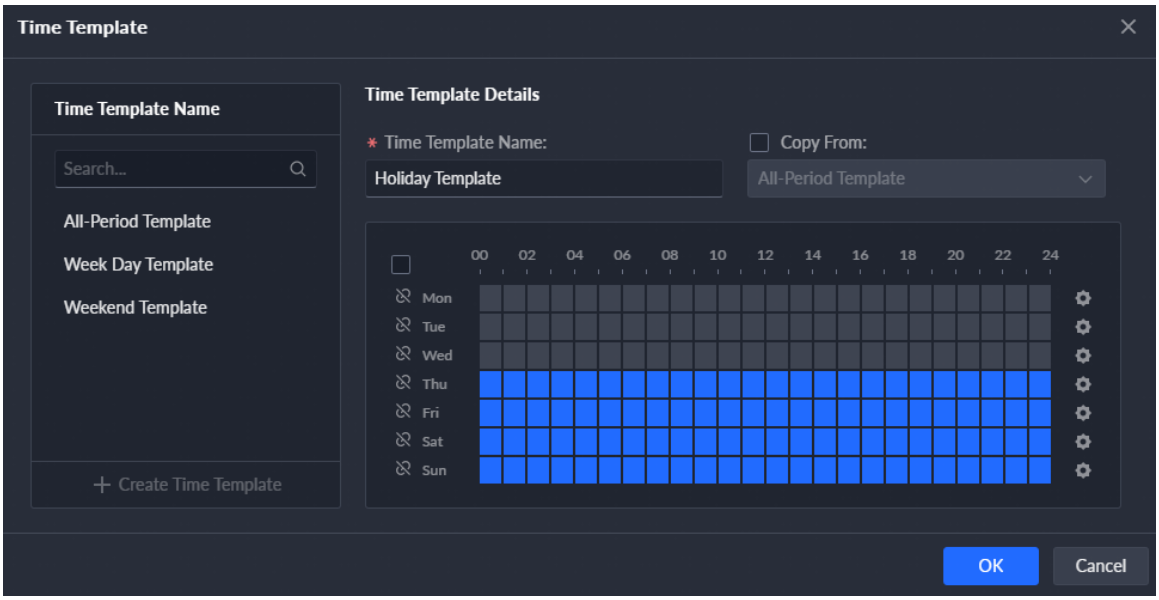
Step 2 Click .

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 4-22 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**.

4.2.8 Configuring Video Retention Period

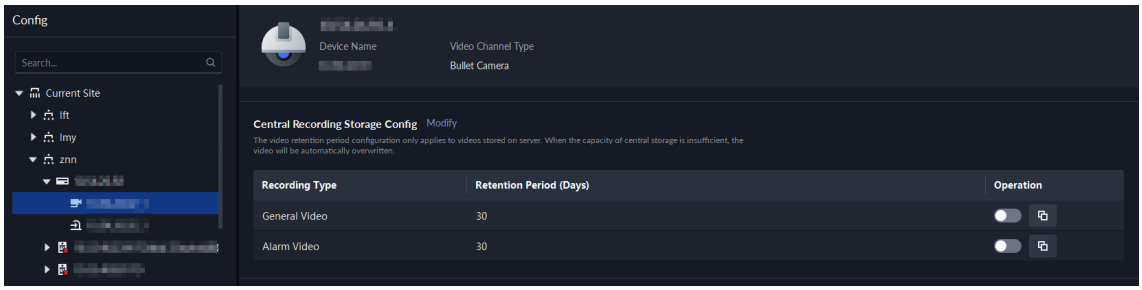
For videos stored on the platform, you can configure video retention period. When the storage space runs out, new recorded videos will cover the oldest videos automatically.

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 4-23 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.

   Channel permissions can be configured by selecting **User** > **Role Management**, and then selecting the channels in **Resource** when adding roles.
3. Click **OK**.

4.2.9 Configuring Events

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

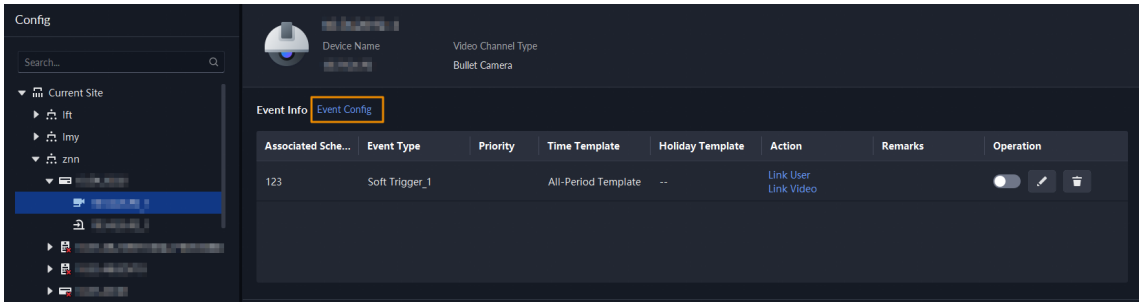
Procedure

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 4-24 Go to the event configuration



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

4.2.10 Configuring Door

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

Procedure

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

Step 2 Click .

Step 3 Select a door channel, and then click **Door Config**.

Step 4 Configure the parameters.

Table 4-7 Parameter description

Parameter	Description
Reader Direction	Click to switch the reader direction.
Mode	Select the mode of the door, including **Normal** , **Always Closed** and **Always Open**.
Enable Door Sensor	After enabling door sensor, it supports **Forced Entry** and **Timeout** alarms.
Enable Alarm	After enabling alarm, you can select uploading duress, unsuccessful attempts exceeding limit, forced entry and timeout to the platform.
Public Password	After configuring a public door password, anyone can open the door with this password.
Unlock Duration	The duration that the door opens.
Unlock Timeout	Close the door after the defined time.
Interval per Card Swipe	The card swiping within the defined interval is regarded as invalid.
Unlock Method	Supports selecting **AND** or **OR**, and selecting card, fingerprint, password, face, palm vein and Bluetooth for combined door unlock. You can also select **Unlock by Period**, and set the door unlock parameters according to time periods.

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

Step 6 Click **OK**.

4.2.11 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.

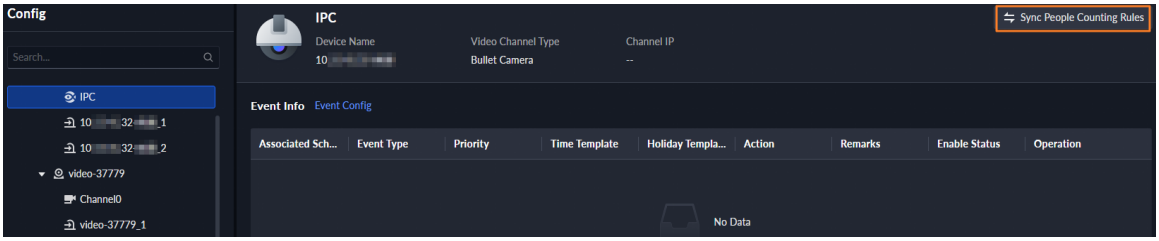
Procedure

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 **Device Config**.

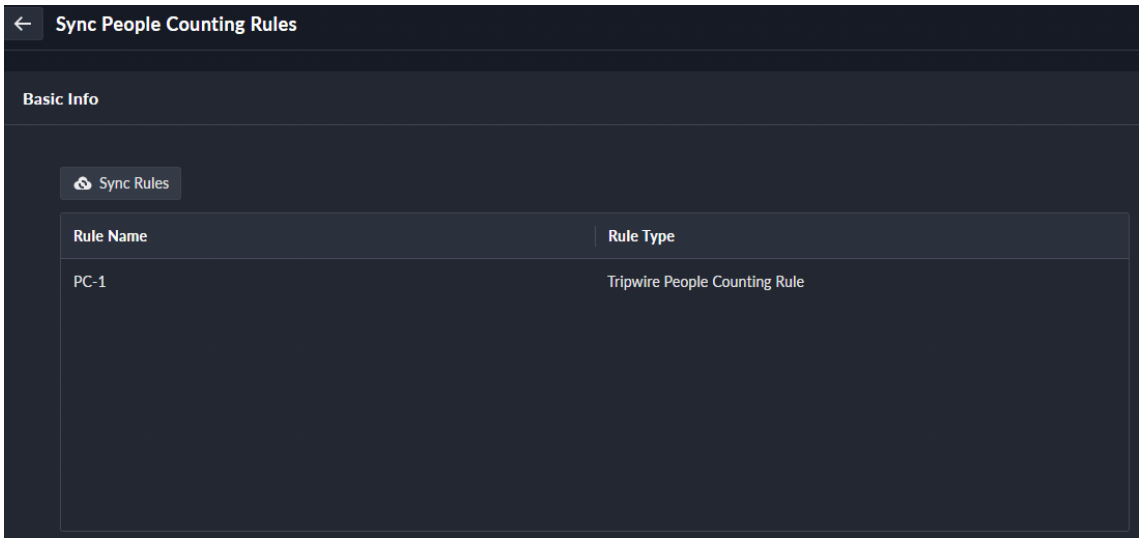
Step 3 Select a channel, and then click **Sync People Counting Rules**.

Figure 4-25 Synchronize people counting rules from the device



Step 4 Click **Sync Rules**.

Figure 4-26 Sync people counting rules



4.2.12 Configuring Audio Play Plan of IP Speaker

After configuring the plan, the IP speaker will play the corresponding audio file according to the defined configurations.

Background Information

- This function is only available for IP speakers connected through the Dahua protocol.
- Each device supports a maximum of 50 audio play plans.

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 IP speaker, and then click **Add** corresponding to **Audio Play Plan**.

Step 3 Configure plan parameters.

Table 4-8 Parameter description

Parameter	Description
Plan Name	The name that identifies the plan.
Type Start Date Start Time Loop Play End Date End Time	• Once: Select a start date, a start time, and an end time. The device will play the audio between the start and end times on that date. • Every day: Select a start date, an end date, and a daily period. Within the date range, the device will play the audio during the specified period each day. • Every week: Select a start date, an end date, a daily period, and the days of the week. Within the date range, the device will play the audio during the specified period on the selected days each week. If **Loop Play** is enabled, and the loop times is set, the audio will be played repeatedly for the configured number of times. Audio will stop at 24:00.
Audio File List	Click **Select Files** to select the audio files to be played in the plan from the device audio list. You can select up to 20 audio files for each plan.
Enable Audio Play Plan	Enabled by default.

Step 4 Click **OK** to save the settings.

Related Operations

- Click **Update** to update the audio play plans from the device to the platform.
- Click , select IP speakers, and then you can copy the audio play plan to the selected devices.

4.3 Adding Roles and Users

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

4.3.1 Adding a Role

A role is a set of permissions. Classify users of the platform into different roles so that they can have different permissions for login, resources, resource operations, and business functions.

The following roles are available.

- Super administrator: A default role that has the highest priority and all the permissions. This role cannot be modified.
- Administrator: A default role that cannot be modified. It has all the permissions of login, resources, and resource operations, and some of the business function permissions.
- General role: This role can be created as needed.

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**, and then configure role parameters.

Figure 4-27 Add a role

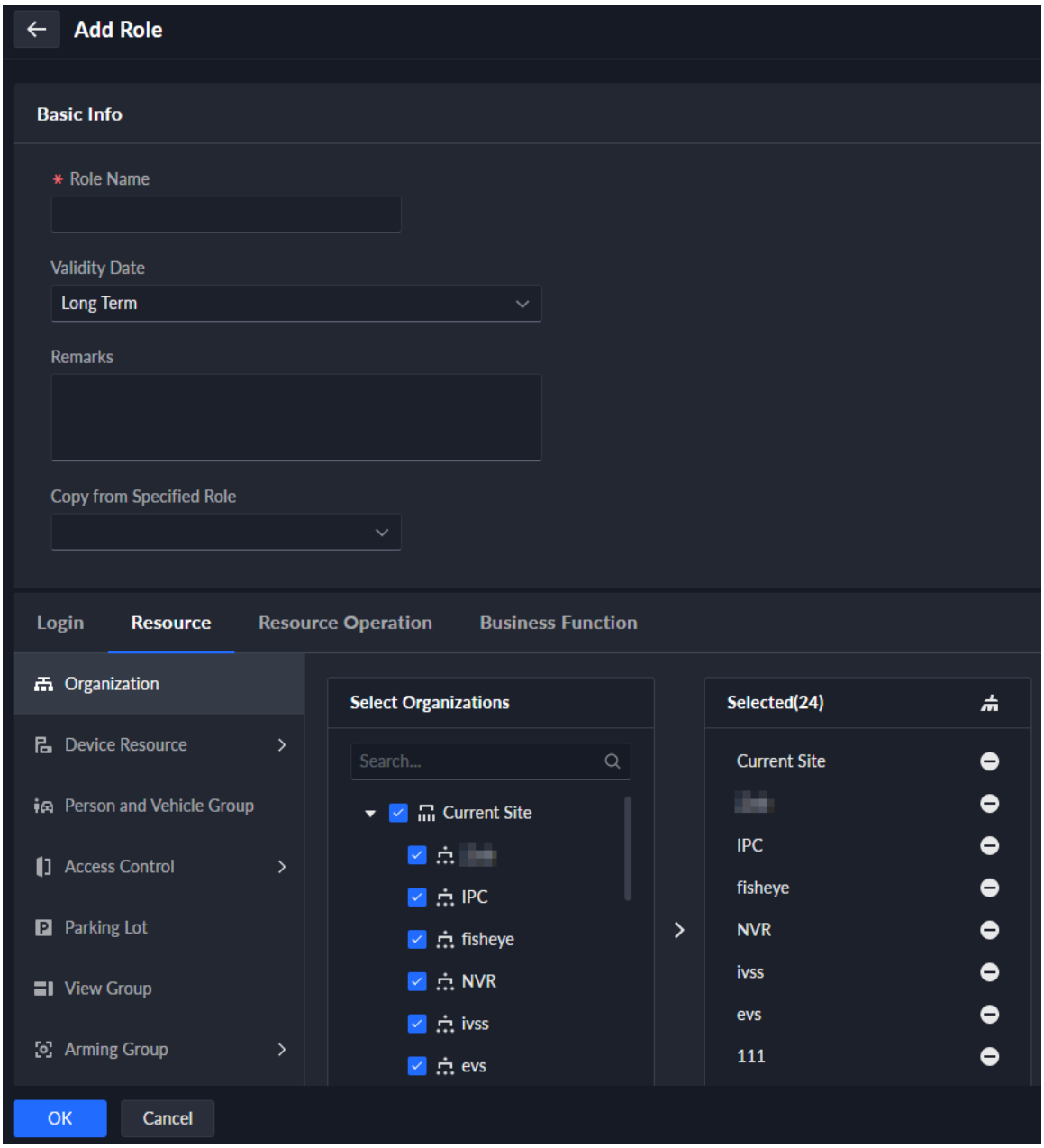


Table 4-9 Role parameters description

Parameter	Description
Role Name	The name that identifies the role.

Parameter	Description
Validity Date	The role is valid within the defined period of time. You can select from long term, one year, half a year, three months, one month, or click **Custom** to define the period that meets your needs. After the role becomes invalid, the permissions of the user of the corresponding role will be invalid.
Remarks	Remarks on the role.
Copy from Specified Role	Select a role from the drop-down box to copy the permissions of the selected role.
Login	Permissions for the role to log in to the clients, such as PC client and mobile client.
Resource	Permissions of the role to resources such as organization, devices, person and vehicle group, access control, parking lot, view group, arming group, and manage selected roles.
Resource Operation	The operation permissions of the role on the resources, such as live view, playback, PTZ, and more. • For live view, you can manage the period of permissions by selecting from all-period, weekday, or weekend template, or click **Create Time Template** to customize your period. • For video playback, you can select or customize the playback duration. • You can set the permissions of downloading videos of main stream, sub stream, or both of them. • For PTZ, it supports selecting **Operation and Config** or **Operation** as needed.
Business Function	You can select the business function permissions of different menus. For example, in the **Basic Configuration** > **Device** > **Add Device** menu, you can configure business function permissions such as adding, editing, deleting, importing, exporting, modifying IP, initializing the device, and more.

Step 4 Click **OK**.

4.3.2 Adding a User Group

Add user groups, so that you can manage users by groups later.

Procedure

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

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

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

Related Operations

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

- Click to edit user group name and remarks.

- Click to delete the user group. After this operation, users in the group will automatically be added to **Ungrouped**.
- Click to clear the user group. After this operation, users with permissions within the group will be automatically added to **Ungrouped**, while those without permissions will remain unchanged.

4.3.3 Adding a User

Create a user account for logging in to the platform.

Prerequisites

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

- The information on users, emails, and more is only stored on the server. It cannot be transmitted to external sources. The email is used for sending reports and resetting user password.
- The platform supports the following types of users.
  - Default super administrator: The default user with the super administrator role. It has the permissions of creating and managing super administrators, administrators, and general users.
  - Super administrator: A user with the super administrator role. It can create and manage administrators and general users. You can add up to 9 super administrators.
  - Administrator: A user with the administrator role. It can create and manage general users. The number of administrators is limited to the maximum number of users for the platform.
  - General user: A user with the general user role. It can create and manage general users if the user has the permissions. The number of general users is limited to the maximum number of users for 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 Select **User Management** , click **Add**, and then configure the user parameters.

Table 4-10 Parameter description

Parameter		Description
Basic Info	Username	Used to log in to the client.
	User Group	Select the group that the user belongs to.
	Password	Used to log in to the client.
	Confirm Password	
	Email Address	Used to receive emails in various situations, such as password reset, alarm messages, and visitor registration.
	Phone No.	The phone number of the user.
	Remarks	Customize the remarks on the user.

Parameter		Description
Security Strategy	Validity Period	The user can log in to the client during the validity period, and cannot log in beyond the defined period. Supports selecting all-period, week day, or weekend period. If the existing templates cannot meet your requirements, you can click **Create Time Template** to customize the time templates. Click to view the effective time period of the template.
	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.
	Two-Factor Authentication	It is a verification method that enhances account security by requiring a password (first factor) and a verification code (second factor) to log in. You need to go to > **System Parameters** > **Security Config**, enable **Two-Factor Authentication**, and then select authentication by email or authenticator. • Email: Make sure that the email server is configured correctly, and the login user has configured an email address to receive the verification code. • Authenticator: You need to have Microsoft or Google authenticator installed on your phone.
	Login Binding	Supports selecting the binding type from **IP** , **MAC**, and **IP +MAC**. You can add up to 5 addresses. **IP** : You can add up to 5 IP addresses. Supports adding, editing, and deleting IP addresses, only IPv4 is supported. **MAC** : After selecting a MAC address, you can only log in to the platform through the specific computers. One user can be bound to 5 MAC addresses at most. **IP+MAC** : Supports adding IP addresses and MAC addresses in groups. Only IPv4 is supported for IP addresses. Users can edit or delete address groups as needed.
Permissions	Multi-client Login	Allow the user to log in to multiple clients at the same time.
	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.
	Role	Select one or more roles to assign the user permissions, such as which devices are allowed to be operated.

Related Operations

- Click to lock user, and then click to unlock the user. Select users, and then click **Lock** to lock them in batches. After this, you can click **Unlock** to unlock them in batches.

  The locked user cannot log in to the DSS client and App.
- Click to modify information of a user except the user name. 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, or select users, and then click **Delete** to delete them in batches.

  You cannot delete a logged-in user.
- Move users to another group

  Select users, and then select **More** > **Move to** to move the users to another user group.

  One user can be only added to one user group.

4.3.4 Adding Self-Service Users

You can add self-service users in batches, facilitating the rapid generation of app accounts. It also supports allocating users to servers for efficient resource allocation.

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 **Self-Service Users**.

Step 3 Click **Add** , and then on the **Batch Add** page, click **Add**.

Step 4 Add self-service users from the person list, and select the applicable service application scope for them.

- Supports adding by person group or by person.

  When adding by person group, you can select **Include Sub Groups**. After selection, the platform displays people in that person group and all its subgroups.
- Service application: The service functions that the user can use. By default, it includes access and visitor services.

Step 5 Click **OK**.

Step 6 (Optional) Click **Resource Allocation** to assign self-service users to servers.

- Select **Auto Allocation** , and then click **OK** to automatically and evenly distribute all self-service users across all online servers.
- Select **Manual Allocation**, select the person group and the server, so that you can assign people in the selected person group to the specified server.

Step 7 Manage self-service users.

- Freeze/unfreeze a user

  Click to freeze the user. Click it again to unfreeze.

  Frozen users cannot log in to the client or mobile app. If the user is currently logged in, the platform will automatically log the user out when the user is frozen.

- Reset user login password

  Click , enter the new password in the pop-up window, and then click **OK**.

  - The password must be 8–32 characters, and it must contain numbers and letters.
  - indicates the password is visible; indicates password protection is enabled and the password is not visible. Click the icon to switch between the them.
- Bind/unbind person

  Click , and then select the person to bind the account; click to unbind the account from the person. After unbinding, the person information will be deleted from the account, and the permissions to open doors remotely will also be revoked.
- Send an email

  Click to send an email to the user.

  Accounts not bound to person cannot send emails.
- Delete users

  Click on a user, or select multiple users, and then click **Delete**, follow the on-screen prompts to complete the operation. After deletion, the person will no longer be able to log in to the app. If the person is the room owner, all app accounts under the room will be deleted, and all people in the room will no longer be able to log in to the app.

4.3.5 Importing Domain Users

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

Prerequisites

You need to configure domain information first from > **System Parameters** > **Active Directory**. For details, see "8.3.8 Configuring Active Directory".

Procedure

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

Step 2 Click **Import Domain Users**.

Step 3 Select how you want to import users.

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

  If you import an entire domain group after the automatic synchronization function is enabled, the platform will remember that group and automatically synchronize its new users at the defined time every day, and update the information of the users imported by manual selection at the defined time every day. For details, see the previous steps.
- **Import by Security Group** : Import all users in a security group.

Step 4 Configure the basic information for the domain user.

When synchronizing the email addresses and phone numbers of domain users, if some users lack this required information, you need to click the users and add their information after you import them.

User group: The group that the domain user belongs to. If the number of users in the group exceeds the limit of 500, the excess users will be automatically added to **Ungrouped**.

Step 5 Configure the security strategy and permissions for the user. For details, see "4.3.3 Adding a User".

Step 6 Click **OK**.

4.3.6 Syncing Deleted Domain Users

The platform supports synchronizing deleted users from domain.

Prerequisites

You need to configure domain information first in > **System Parameters** > **Active Directory**. For details, see "8.3.8 Configuring Active Directory".

Procedure

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

Step 2 Select **More** > **Sync Delete Domain User**.

Step 3 Select the invalid domain users who were deleted from the domain, and then click **Sync Deleted Users from Domain**.

Step 4 Click **OK**.

4.3.7 Syncing Added Domain Users

You can synchronize new users on the platform that were added to the domain group.

Prerequisites

You need to configure domain information first in > **System Parameters** > **Active Directory**. For details, see "8.3.8 Configuring Active Directory".

Procedure

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

Step 2 Select **More** > **Sync Add Domain User**.

Step 3 Select synchronizing **All** or **Specified** users.

When selecting **Specified**, you need to select the range of users that you want to synchronize.

Step 4 Click **OK**.

4.3.8 Configuring Auto Synchronization

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

Prerequisites

You need to configure domain information first from > **System Parameters** > **Active Directory**. For details, see "8.3.8 Configuring Active Directory".

Procedure

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

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

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

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

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

Step 4 Click **OK**.

4.3.9 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.

4.3.9.1 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**.

Step 2 Enter the old password, new password, and then confirm the new password.

Step 3 Click **OK**.

4.3.9.2 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**.

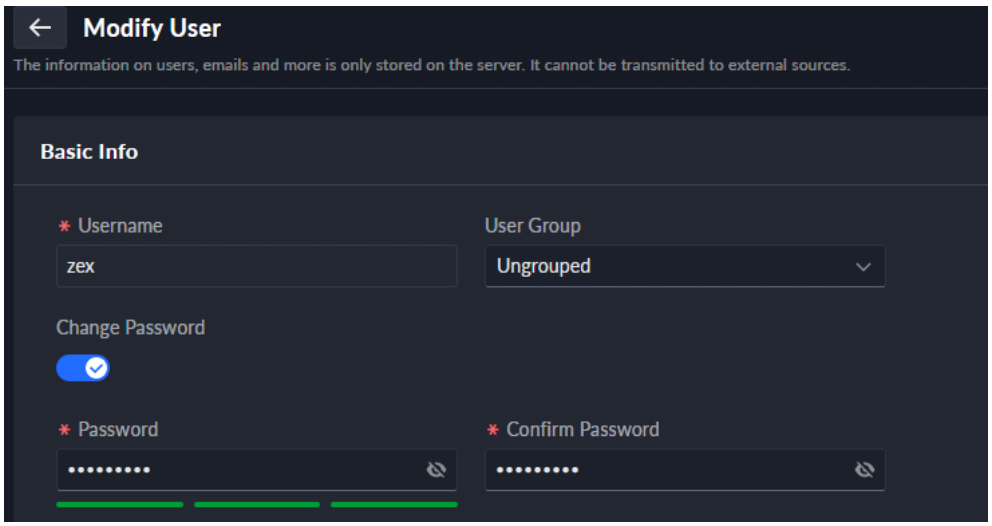
Step 2 Click .

Step 3 Select a user, and then click .

Step 4 Enable **Change Password**.

Step 5 Enter the new password, and confirm password.

Figure 4-28 Change passwords for other users



Step 6 Click **OK**.

4.3.9.3 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. Select **Security Question** verification mode.
  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 "4.3.3 Adding a User".
  1. Select **Email** verification mode.
  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.

4.3.9.4 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

We recommend using Dahua EVS devices, and the network storage server and DSS platform be directly connected through network cable, or connected to the same core switch.

Prerequisites

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

Background Information

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

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

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

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

Procedure

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

Step 2 Select .

Step 3 Click **Add**.

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

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

Figure 4-29 Add a network disk (normal mode)

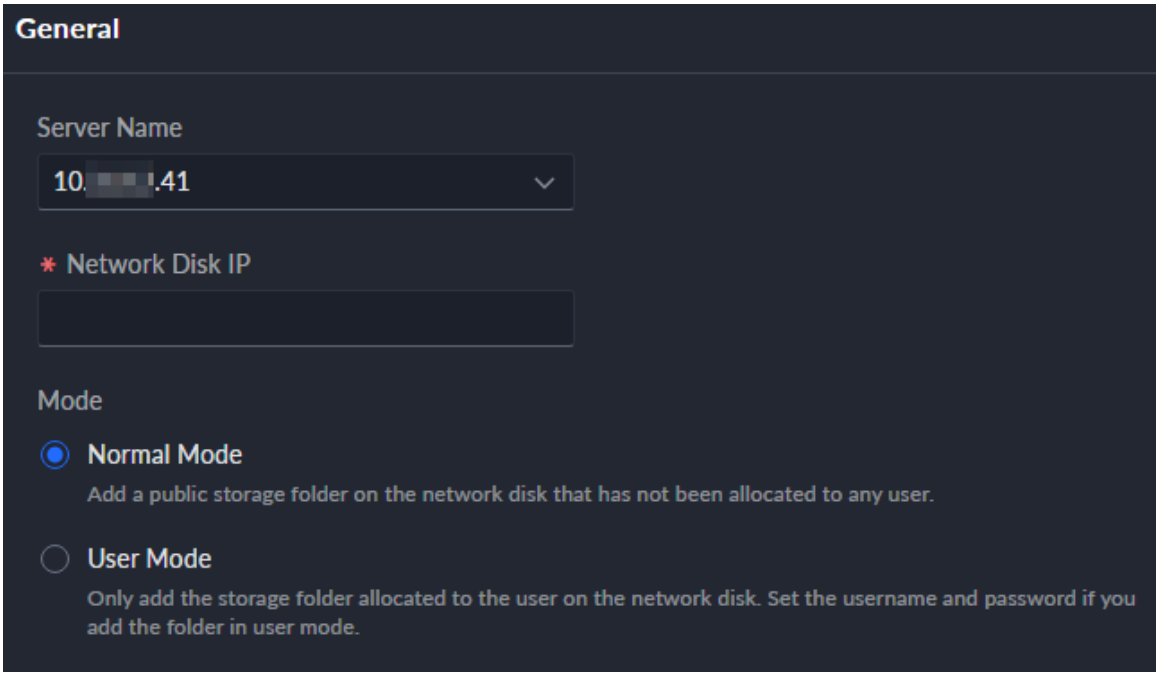
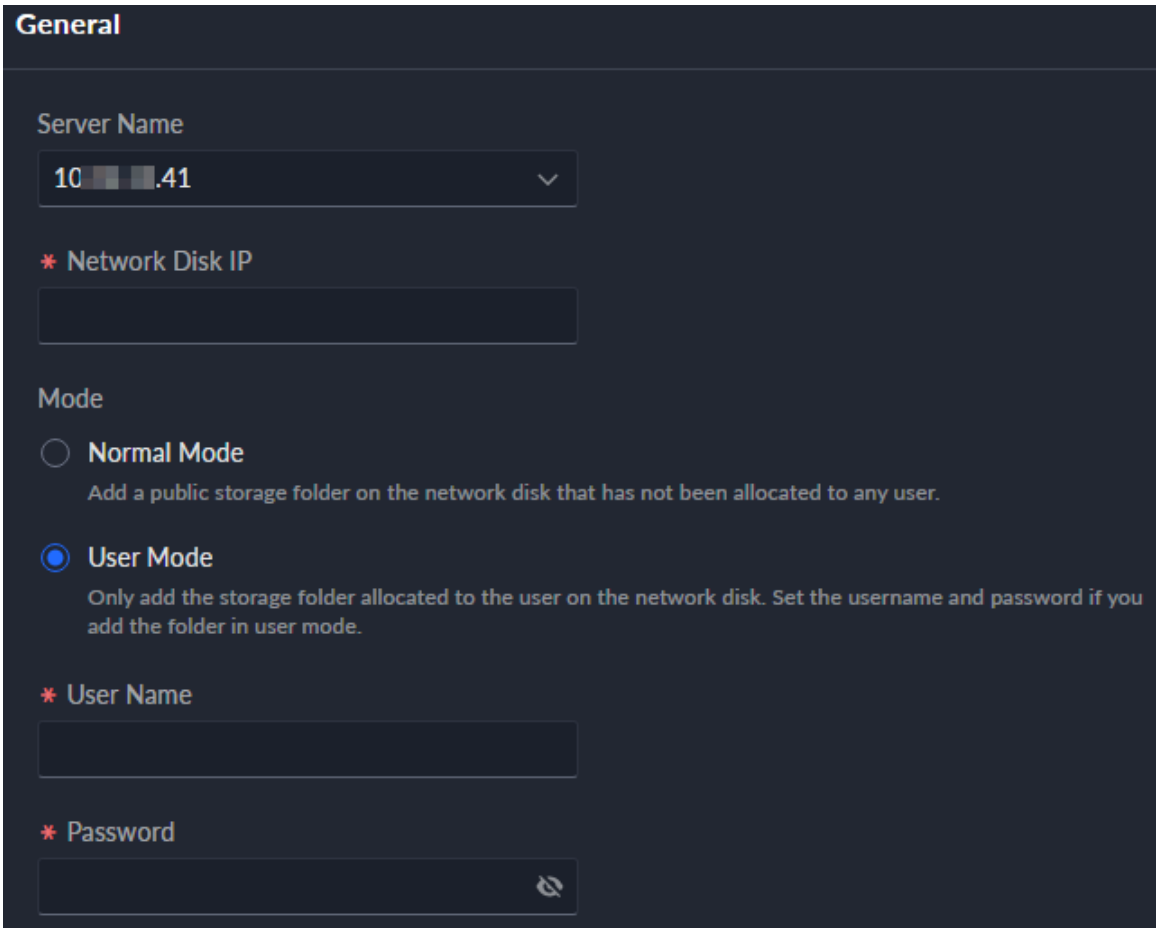


Figure 4-30 Add network disk (user mode)



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

1. Select user volume, and then click .

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

- **Video** : Stores videos.
- **Images and Files** : This is a dynamic disk. Data will be overwritten on it once it reaches full capacity. It is used to store vehicles, faces, video metadata, and alarms.

  We recommend configuring a disk with more than 100 GB available space.

For hot standby, the configurations of the file storage disks on both the active server and the standby server must be the same.

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 lost.

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

Procedure

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

Step 2 Select .

Step 3 Format a disk to set a storage type.

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

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

   - **Video** : Stores videos.
   - **Images and Files** : This is a dynamic disk. Data will be overwritten on it once it reaches full capacity. It is used to store vehicles, faces, video metadata, and alarms.

We recommend configuring a disk with more than 100 GB available space.

- For hot standby, the configurations of the file storage disks on both the active server and the standby server must be the same.
- 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 **Images and Files** 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 .

4.4.3 Configuring Disk Group

Allocate disk groups for video storage.

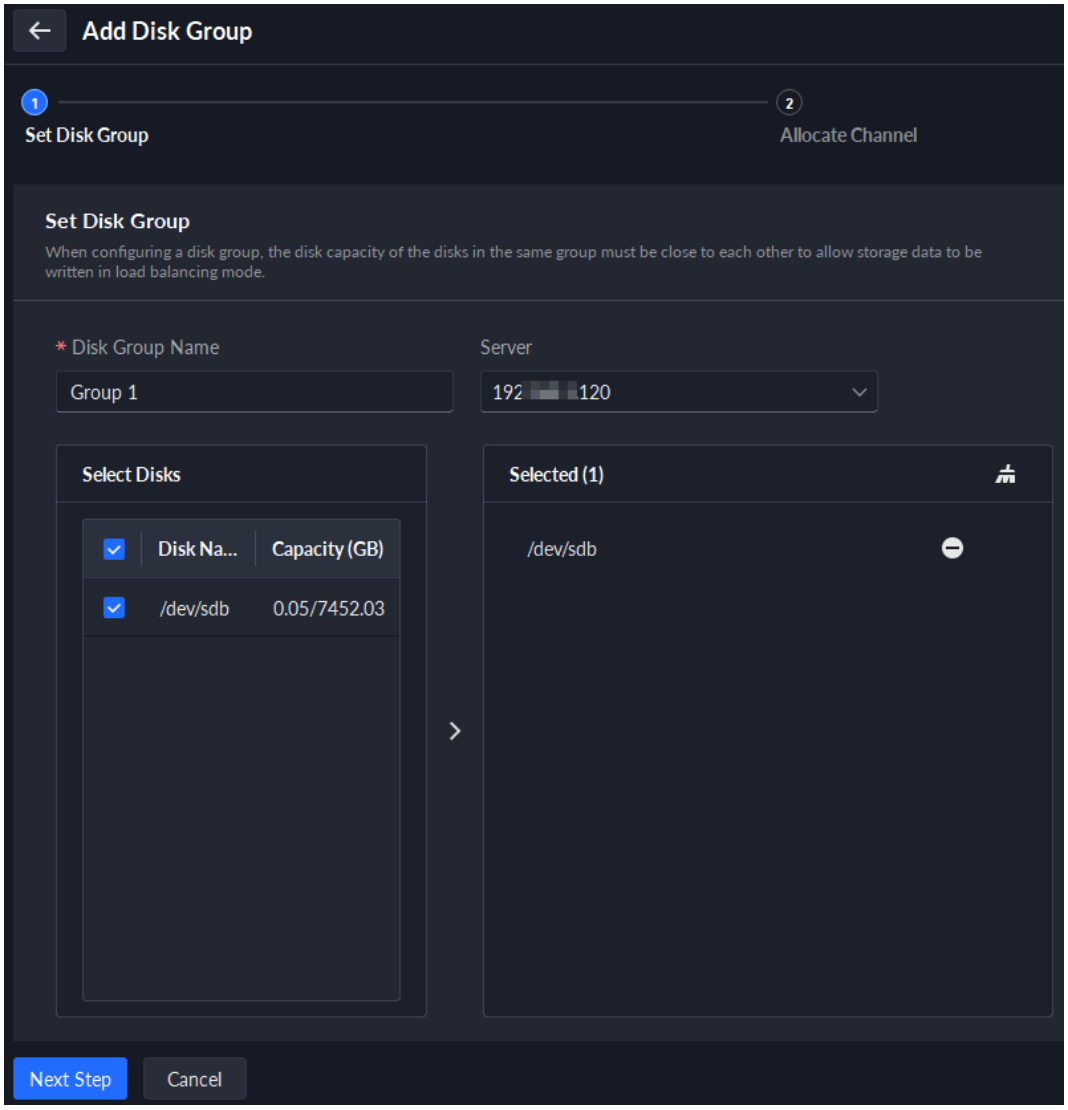
Procedure

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

Step 2 Click .

Step 3 Click **Add**, enter disk group name, and then select a server and disks.

Figure 4-31 Configure disk group



Step 4 Click **Next Step**.

Step 5 Select devices or channels on the left.

Step 6 Click **OK**.

4.4.4 Configuring Device Storage

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

Procedure

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

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

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

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

Table 4-11 Parameter description

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

Related Operations

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

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

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

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 Select the event source type, events, and event sources.

Table 5-1 Parameter description

Parameter	Description
Device, video channel, alarm input channel, subsystem, alarm control panel zone, access control channel, parking lot, people counting group, lift control channel, traffic alarm, and system	Select an event source type. • Before configuring the event, check whether the channel features match the event type; otherwise the event type cannot be selected as the alarm source. To configure channel features, see "4.2.2.5.3 Modifying Device Information". • If **Alarm Input Channel** is selected, check whether the **Triggered Event** that you select matches the channel feature of the alarm input channel you select. Otherwise, the event will not be triggered.
Soft Trigger	This is a type of event that is manually triggered. Click to customize its name and icon. When viewing the live video image of the configured channel in the **Monitoring Center**, you can click the icon to trigger an alarm manually.
Combined Event	When a combined event is triggered, the platform performs the defined linked actions. For how to configure combined events, see "5.1.2 Configuring Combined Event".

Parameter	Description
Custom Alarm	• DHOP event: Access events developed through Dahua Hardware Open Platform (DHOP). • Extended standard event: This is used for events that devices support, but the platform currently does not. Click **Add Extended Event**, and then configure the parameters. ◇ **Event Protocol** : Select the protocol of the event. ◇ **Alarm Source** : Select an event source type based of the event protocol. ◇ **Event Image** : When configuring an event for a video channel, you can choose whether to subscribe to images from the event. When subscribing to pictures, the platform will receive alarm images generated by the alarm source. However, if the alarm source does not generate alarm images, subscribing to the event images will cause the platform to not receive the alarm. ◇ **Name** , **Alarm Code**: Enter the name and code of the event.
Generic Event	Receives simple strings sent to the system by third-party hardware or software through the network, and then generates alarms or triggers corresponding linkage actions in the system. When configuring event source, select **Generic Event** from **Event Source Type** and **Event**, and select added generic events from **Event Source**. For details of add a generic event, see "5.1.4 Configuring Generic Event".

Step 4 Enable **Device Owner** as needed. After it is enabled, the device owner will be displayed in event records.

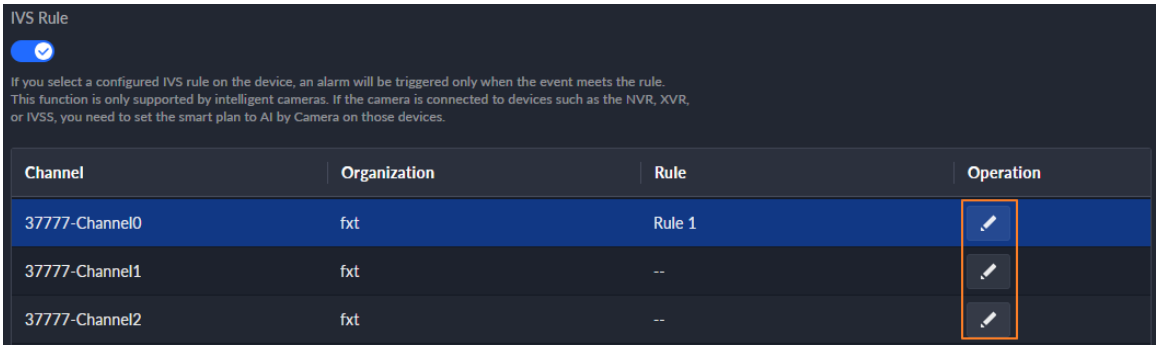
Step 5 Set IVS rules. Multiple rules can be selected when configuring specific rules for a channel corresponding to an event type (for example, tripwire). Also, other rules for that channel can still be configured for other event schemes, so that different rules on a single device can trigger different alarm actions.

This function is only available for event types such as tripwire, intrusion, fast moving, crowd gathering, loitering detection, abandoned object, missing object, stay detection, and more. Refer to the actual page.

1. Select **Video Channel** from the event source type, select the event (for example, tripwire) from **Intelligent Event** in the event list, and then select the event source.
2. Enable **IVS Rule**.
3. Click of the event source, and the system displays the configured event types and enabled IVS rules for that channel, along with the video feed.
4. Select the desired IVS rules, and then click **OK**.

   Configure the rules for each selected event source individually.

Figure 5-1 Configure IVS rule



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

Step 7 Configure alarm conditions. Alarms will be generated only when the event source generates an event and the defined conditions are met.

1. Click next to **Conditions**.
2. Enable **Alarm Input** , **Alarm Controller** and/or **Access Control Channel** as needed, select the channel and set its status.

For example, if you select access control channel A, and set its status to **Open**, an alarm will be generated only when the event source generates an event and channel A is open.

- When multiple conditions are set, alarms will be triggered only when event sources generate events and all conditions are met.
- If the event source generates an event, but the device specified in the condition is offline, no alarms will be generated.

Step 8 Click next to **Linked Action** to enable the alarm linkage function.

Step 9 Configure alarm linkage actions.

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

Table 5-3 Parameter description

Parameter	Description
Camera	◇ Event source: The camera of the alarm itself is linked when the alarm occurs. ◇ Bound camera: If the channel is bound to one or more video channels, you can view the real-time videos of the bound channel when an alarm is triggered. To bind a channel, see "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	Enable this parameter, and then the platform will open the real-time video of the channel where an alarm is triggered, and play it in the defined stream type. After the event is configured, select **Local Settings** > **Alarm**, enable **Open Alarm Linkage Video** and set how the video will be opened, **As Pop-up** or **Open in Live View**. For details, see "9.1.3 Configuring Alarm Settings".
Event Recording	The platform will record videos when an alarm is triggered. It will be saved to the video disk of the platform.
Stream Type	Available after you enable **When an alarm is triggered, display camera live view on client**. The stream type you selected will be used first. If the device does not support configuring the stream type, the main stream will be used.
Recording Time	The duration of the recorded video.

Parameter	Description
Prerecording Time	When there is recorded video that is stored on the device or platform before the alarm is triggered, the platform will take the defined duration of that video, and then add it to the alarm video. For example, when the prerecording time is set to 10 s, then the platform will add 10 s of video before the alarm is triggered to the alarm video. ◇ If the alarm video is stored on the device, we recommend you configure a 24-hour recording plan to make sure that there is prerecorded content to add to the alarm video. ◇ If the alarm video is stored on the platform, the platform will record videos and use certain input bandwidth continuously. ◇ This parameter is not applicable to alarms in parking lots and combined alarms.

- To trigger a snapshot, enable **Trigger Snapshot** . Supports selecting multiple channels, and the platform takes 1 snapshot of each selected channel, and save them to the **Images and Files** disk.
- Select a channel (supports selecting an access control 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.
- To execute an HTTP URL command, enable **Link HTTP URL Command** . Click **Add**, and then click **New** to add a new command, or **Copy from Quick Command**. When adding a new command, you need to set the name of the command, the request method, HTTP URL, and remarks. You can click to test if the command is valid.

  When selecting **POST** or **PUT**, you can click to customize the body of HTTP URL.
- To link emails, perform the following operations.

  ◇ You have configured the email server. For details, see "8.3.6 Configuring Email Server".
  ◇ The language of the email content can be set from **System Parameters** > **Email Server**. Only default content will be sent in the defined language. Any text that is manually entered will be sent in its original form.

  1. Click next to **Email**.
  2. Select an email template, or you can click **Add Email Template** from the drop-down menu to create a new email template.
  3. Select or enter an email address. After manually entering the email address, press Enter to apply the changes.
  4. Set the email subject and body, and then click **OK**.

Select **Send Alarm Image**, and configure snapshot linkage (or the alarm itself includes an image), the alarm image will be sent along with the email content.

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

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

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

Step 10 Apply an alarm protocol to help users process alarms.

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

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

Step 11 Select users or user groups who will receive the notification when an alarm is triggered.

The users will only receive notifications when they are logged in. If you need to add more users, see "4.3 Adding Roles and Users"; to add more user groups, see "4.3.2 Adding a User Group".

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

Step 12 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 **Add Combined Event Rule** to add a rule for combined events.

Step 3 Enter a name for the rule, and then configure the details.

For example, select **Event B** occurs and configure the **X** and **Y** to be 10 and 50 seconds respectively. If event B occurs during the 10 seconds to 50 seconds after event A occurs, a combined event is triggered, and then the platform will perform defined linked actions.

Step 4 Click **OK**.

The previous page displays.

Step 5 Click **Add**, and then configure the parameters of the combined event.

Table 5-4 Parameter description

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

Step 6 Click **OK**.

Related Operations

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

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 event sources and events, and then configure the interval (1–600 seconds).

Step 4 Click **OK**.

5.1.3.2 Configuring Alarm Video Pre-Recording

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

Background Information

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

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

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Event** > **Alarm Config** > **Alarm Video Pre-recording**.

Step 2 Click an organization, and then all devices and channels in that organization will be displayed on the right.

Step 3 Configure the pre-recording mode.

- Click of a channel, select a mode, and then click **OK**.
- Select multiple channels, click **Edit** , select a mode, and then click **OK**.

5.1.4 Configuring Generic Event

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

Prerequisites

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

Procedure

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

Step 2 Click **Add**, and then you can start adding the generic event.

Figure 5-2 Add generic event

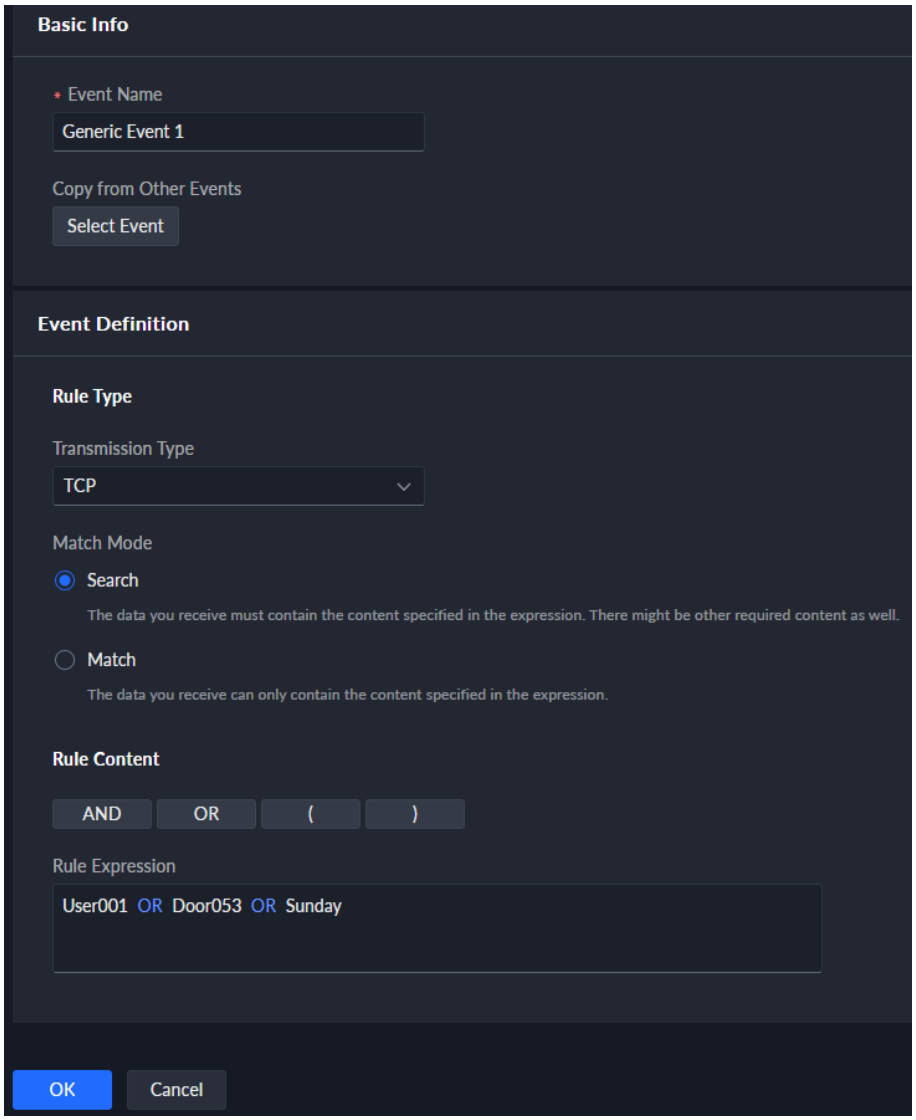


Table 5-5 Parameter description of generic event

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

Step 3 Click **OK**.

5.2 Configuring Map

5.2.1 Preparations

- Devices are deployed. For details, see device user 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 a Map

The platform supports adding raster and vector maps.

5.2.2.1 Adding a Vector Map

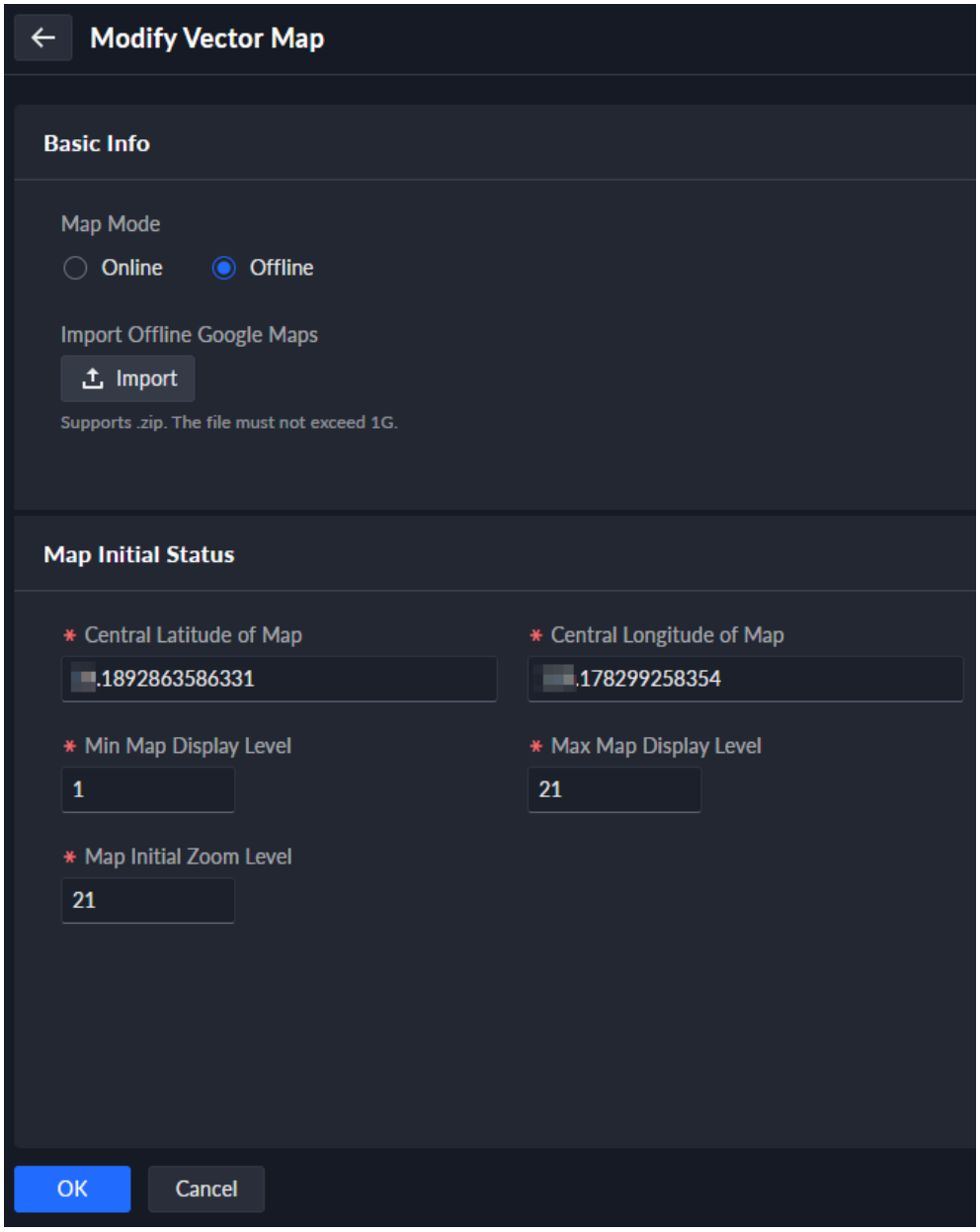
Procedure

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

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

Step 3 Configure the parameters.

Figure 5-3 Map



- 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 5-6 Parameter description

Parameter	Description
Map Link	Enter the URL of the map. Only Google Maps is supported.

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

Step 4 Add a sub map.

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

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

   The sub map is added.

5.2.2.2 Adding a Raster Map

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

Procedure

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

Step 2 Select **Main Map** , and then click **Add Map**.

Step 3 Enter the map name, select the image and then click **OK**.

Step 4 Add a sub map.

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

5.2.3 Map Operations

Click the added map, and then you can perform the following operations.

Viewing Device Details

- Click a device on the map, and then click to view device name and organization; click the icon again to hide the name and organization.
- (Optional) Click a 4G device on the map, and then click to view the battery information.

It is applicable to 4G camera scenarios without network environments.

Showing Devices

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

Moving Devices

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

Configuring Static Visible Range

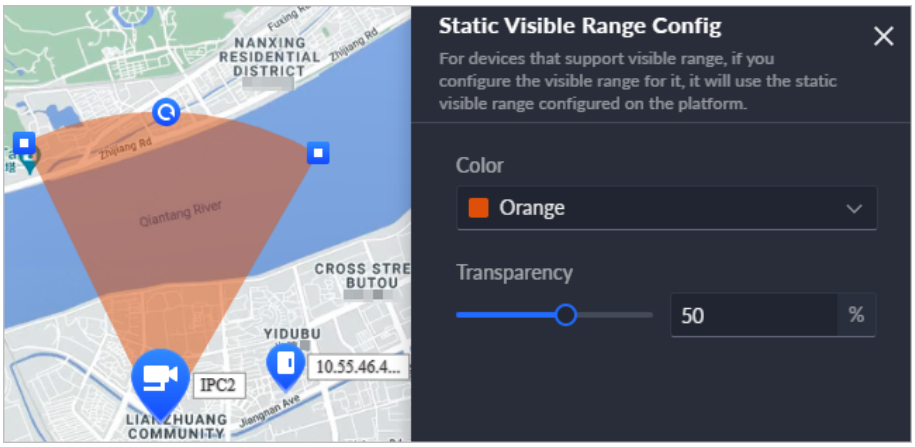
For devices that do not support sending visible range to the platform, you can customize the visible range on the map. After that, when you monitor or track back a target, you can quickly find the monitoring devices according to the visible range.

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

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

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

Figure 5-4 Configure static visible range



Deleting Devices

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

Hiding Device Names

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

Viewing Satellite Map

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

Point Clustering

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

Clearing the Map

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

Adding a Sub Map

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

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

Length

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

Area

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

Adding 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.

5.2.4 Marking Devices

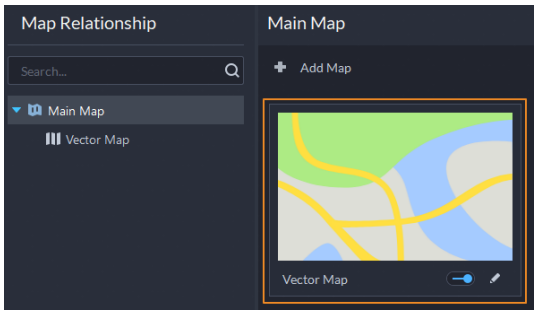
Link a device to the map by dragging it to the corresponding location on the map according to its geographical location.

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 image, and more. People bound with vehicle information will be displayed in the vehicle list.

- Vehicle information helps to confirm the entry of the vehicle into a certain area. Vehicle bound with personnel information will be displayed in the personnel list.

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.

Background Information

The permissions of person and vehicle groups can be configured by selecting **User** > **Role Management**, and then selecting the permissions in **Business Function** when adding roles.

Procedure

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

Step 2 Click **Person List** or **Vehicle List**.

Step 3 Click , and then configure the parameters.

Table 5-7 Parameter description

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

Step 4 Complete configuration.

- Click **Add** to add the group and exit the page.
- Click **Save and Add Person** to add people to the group. For details, see "5.3.2 Configuring Person Information".

Related Operations

- Edit person and vehicle group: Click to edit the group name and the roles allowed to access. Group permissions are updated after editing.

  Administrators have permissions for all groups by default. Roles without permissions can see the group in the tree on the left, but the group icon is grayed out, and the roles cannot view the people under the group.

- Delete person and vehicle group: Click , and then enter the login password. The group will be deleted.

You cannot delete the group if it has sub groups, people, or vehicles.

- Clear person and vehicle group: Select **Include Sub Groups** , click , and then enter the login password to delete people in the current group and its subgroups; if **Include Sub Groups** is not selected, only the people in the current group will be deleted. The people in the sub groups will not be affected.

5.3.2 Configuring Person Information

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

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

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. Other users can only configure information for attributes that have been added. You can add up to 10 attributes.

Procedure

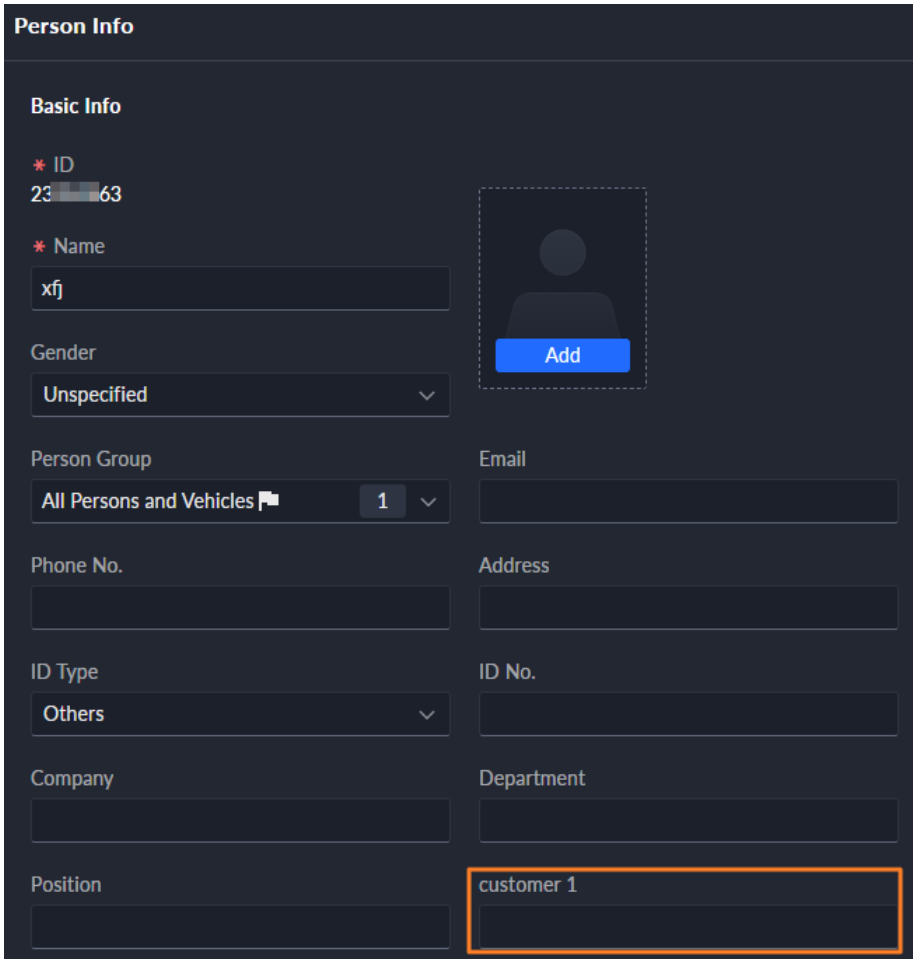
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Person and Vehicle Info**.

Step 2 Select **Person List** > **More** > **Enable More Info**.

Step 3 Click **Add** , enter a name for the attribute, and then click **OK**.

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

Figure 5-6 More information



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 **Person and Vehicle Info**.

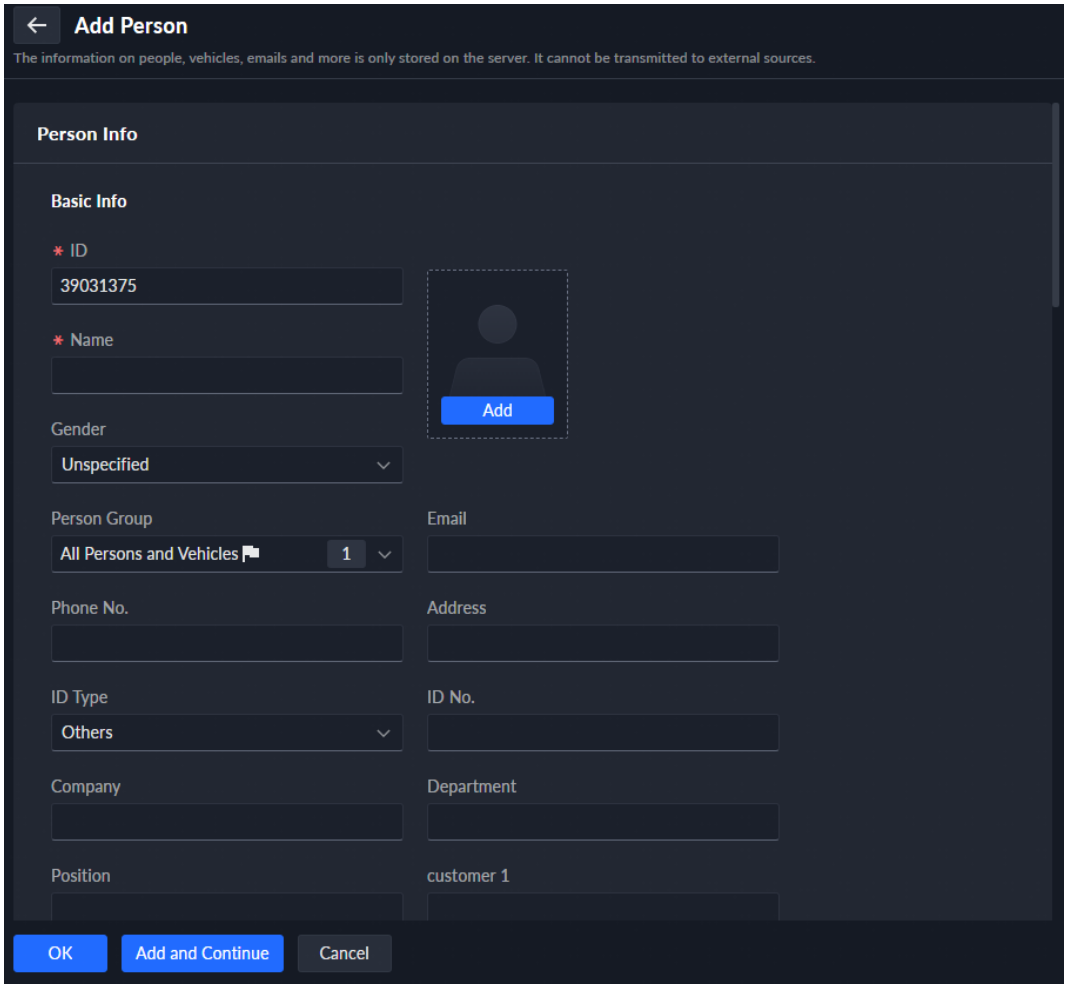
Step 2 Select **Person List** > **Persons** > **Add**.

Step 3 Click **Person Info**, and then configure the information of the person.

- Configure the basic information.

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

Figure 5-7 Basic information



- 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 "5.3.2.5 Importing Images of People".

2. Enter the information of the person as necessary.
   - The name of the person can be up to 127 characters.
   - The ID is required and must be unique. It can be up to 30 characters, and letter-number combination is also supported.
   - The person can be added to up to 20 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 or using lifts.

Table 5-8 Parameter description

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

Parameter	Description
Password	Password can be used for access control, lift control, and intercom. 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 that you are using. For the unlock by access control, if the short password is supported by the device and enabled, you can lock the door with password only. Click +, enter a password, and then click ✓. After adding a password, you can: ◇ : Change the password. ◇ : Delete the password, and then it has no access permissions.
Palm Veins	Collect the palm vein information of a person, and then the person can access through non-contact verification on the access control device that supports the palm vein function. 1. Click **Setting** to select the palm vein collection device. 2. Click **Add Left Palm Veins**, and then collect the left-hand palm vein on the device according to on-screen instructions. 3. Click **Add Right Palm Veins**, collect the right-hand palm vein on the device according to on-screen instructions. : Delete the palm vein information.
Bluetooth	Click **Add** to generate a Bluetooth card number for door access verification. Only one Bluetooth card number will be generated for one person. : Delete Bluetooth card information.

- If the person has one or more vehicles, you can set the person to the owner or linked person of the vehicle.

  A vehicle can be linked to maximum 10 people, including vehicle owner and linked person.

  - **Owner Vehicle** means that the vehicle belongs to this person. The vehicle and the person must be in the same organization, and a vehicle can only have one owner.

    If the vehicle have been added to the platform, click **Select from Vehicle List**, and then select the vehicles for this person; if not, click +, enter the plate number, and then select a color and brand.
  - **Linked Vehicle** means that the vehicle is linked to this person, for example, when a family share a vehicle.

    To link a vehicle to the person, click +, enter the plate number, and then select a color and brand.

Step 4 In the **OnePass App** area, enable **Generate App Account** as needed. After enabling it and saving the settings, an account will be automatically created. Upon first login to the

OnePass App, the account and initial password will be automatically sent to their email address for logging in to the app.

You can select the service application scope of the account, that is, the services that the account can use. By default, it includes access and visitor services.

The person can log in to OnePass App, and then go to **Me** > **My QR Code** to view the QR code. The QR code is valid for 10 minutes. After the QR code expires, the person can tap the QR code to refresh it, or exit the current menu and reopen it to automatically refresh it.

Step 5 If the person is a resident, click **Video Intercom**, and then configure the room information.

Table 5-9 Parameter description

Parameter	Description
Room Type	• None: Requires setting a SIP code, which will be used by the app for video intercom calls. • Single room: The number of the room this person lives in. It is displayed in the access records and video intercom operation records. • Multiple rooms: Supports setting a main for generating a SIP code. Also, you can select the room as the homeowner room.
Homeowner	You can enable **Homeowner** when selecting **Single Room**. There can only be one homeowner for a room. The homeowner can create sub accounts on the OnePass App.

Step 6 Click **Access Control**, and then configure the access permissions for this person.

1. Select an access type.
   - General: When the person uses an access point, a general event is reported. The person is restricted by door mode, combination unlock (card, fingerprint, face, password, palm vein, and Bluetooth), unlock by period, and all types of access rules.
     - Door mode, combination unlock (card, fingerprint, face, password, palm vein, and Bluetooth) and unlock by period can be configured by selecting > **Device** > **Device Config**, clicking **Channel** to filter the access control channel, and then selecting > **Door Config**.
     - Access rules can be configured from > **Access Control** > **Access Rule** > **All Rules**.
   - VIP: When using an access point, the person is restricted by all rules except combination unlock (card, fingerprint, face, password, palm vein, and Bluetooth), multi-person unlock, and unlock by period rules.
     - Combination unlock (card, fingerprint, face, password, palm vein, and Bluetooth) and unlock by period can be configured by selecting > **Device** > **Device Config**, clicking **Channel** to filter the access control channel, and then selecting > **Door Config**.

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

- Patrol: When the person uses an access point, a patrol event is reported, and the door will not open.
- Blocklist: The person cannot use an access point. Also, a blocklist event is reported.
- Extend time: When the person uses an access point, if the access point is a door, the door will stay unlocked for additional 5 seconds.

2. Configure validity period. The person is only effective within this period. You can modify the value to extend the validity period.
3. Select **Quote** > **Add**, and then configure the access rules.

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

Figure 5-8 Available access rules

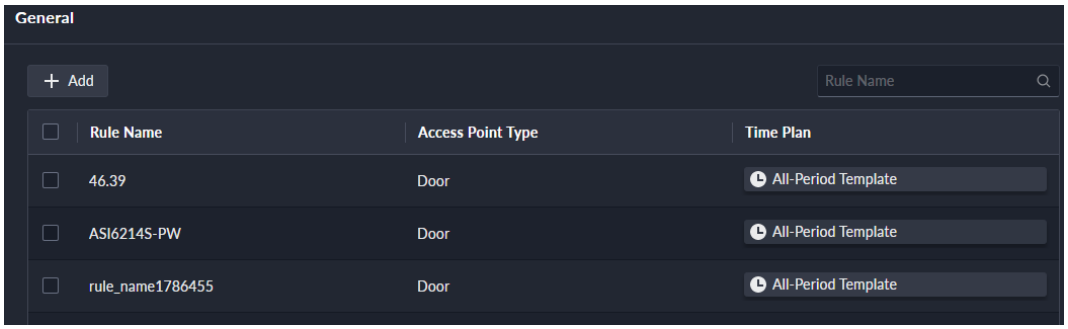
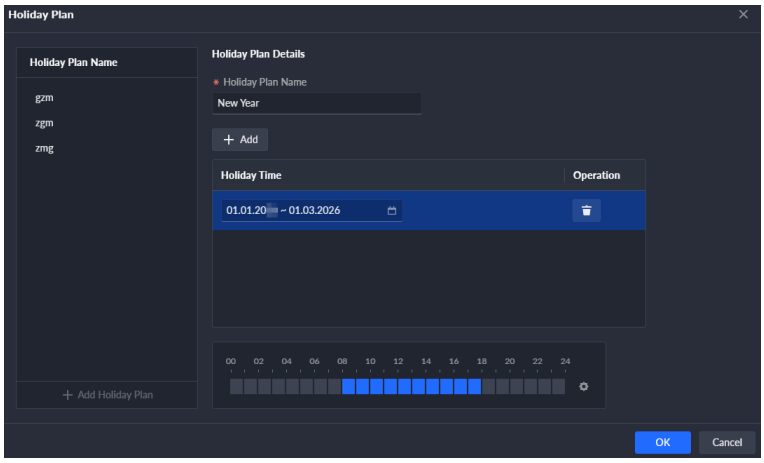


Table 5-10 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Select **Door** or **Lift**.
Time Template	Select a time template to define when the rule will be effective. For how to create a new template, see "4.2.7 Adding Time Template".

Parameter	Description
Holiday Plan	Select a holiday plan when the rule will not be effective. You can add up to 4 holiday plans. Follow the steps below to create a holiday plan: **Lift** does not support holiday plans. a. Select **Add Holiday Plan** in the drop-down list. b. Enter a name for the holiday plan. c. Click **Add** to add a holiday. You can add up to 16 holidays. d. Configure the effective periods for each day in the holiday. You can drag on the timeline below, or click to configure the time more accurately. You can add up to 4 periods. e. Click **OK**. 
Select by Zone	Select one or more zones. This person will have access permissions to all the access points in these zones. For how to configure a zone, see "5.5.2 Configuring Zone".
Select by Access Point	Select one or more access points. This person will have access permissions to all these access points.
Roles Allowed Access	Only the selected roles and their users can view and edit the rule. Click to view the users assigned with the roles.

4. Click **OK** to finish adding the rule.
5. Select one or more rules for this person, and then click **OK**.

Step 7 If you want to recognize this person by face images, add the person to a face arming group.

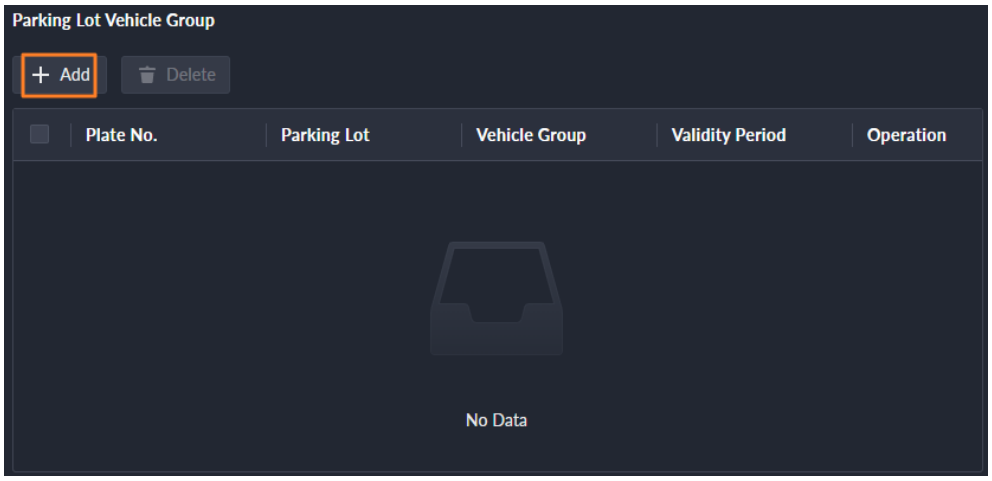
You need to create a face arming group first. To add one, select **Add Face Arming Group** in the drop-down list. For details, see "5.4.1.1 Creating Face Arming Group".

Step 8 If this person needs to enter and exit a parking lot, you can grant parking lot access permissions to them.

1. If this person has one or more parking spaces, click **Add** in the **Available Parking Spaces** section, select the parking lot, 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.
2. In the **Parking Lot Vehicle Group** section, click **Add** to select the license plate number, and then select which one or more vehicle group it belongs to.

Figure 5-9 Parking lot vehicle group



Step 9 Click **OK**.

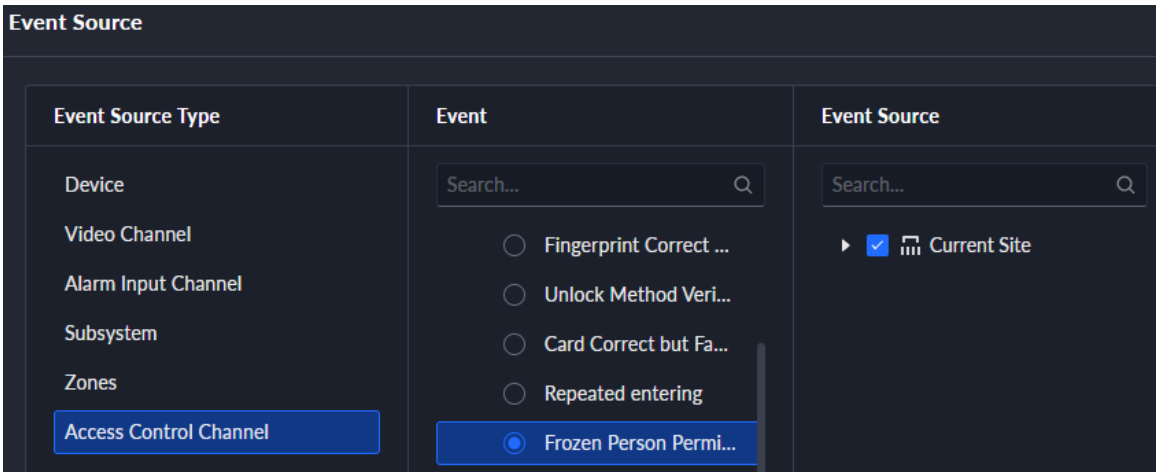
Related Operations

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

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

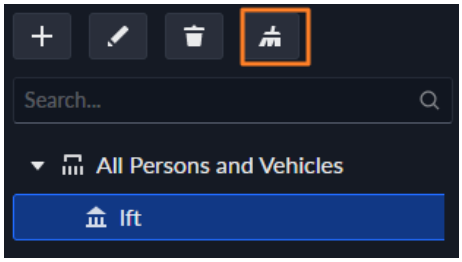
  - After canceling, if the access control device is configured with **Frozen Person Permissions** from > **Event** > **Event Config**, an alarm will be triggered if the person is detected trying to access.
  - This function is only available for access control devices (access controllers excluded).

Figure 5-10 Configure frozen person permissions eve



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

Figure 5-11 Delete all persons in a group



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

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

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

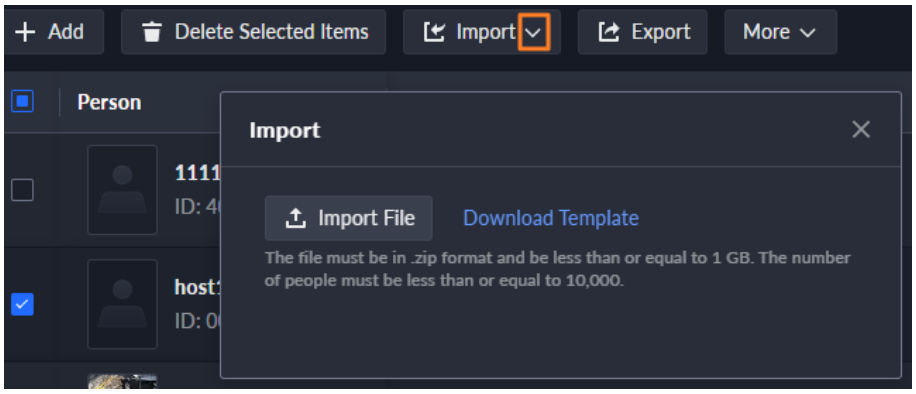
- Prepare an .xlsx file that includes the information of the people you want to import, their face images (optional), and then compress them into a .zip file. The .xlsx file can include information of up to10,000 people. The .zip file cannot be greater than 1 GB.
- If a person belongs in a first-person unlock rule, set the access type of the person to **General**.
- Existing and enabled extracting personnel information on the platform supports import.
- Existing but not enabled extracting personnel information on the platform supports import but will not be displayed.

Procedure

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

Step 2 Select **Import** > **Import from File**.

Figure 5-12 Import personnel information



Step 3 Import the person information file.

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

Step 4 Click **OK**.

The following cases might occur during an import:

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

Related Operations

- Export person information.

  Select an organization, click **Export**, and then follow the instructions on the page to save the exported information to a local disk.
- Import people from device: Select **Import** > **Import from Device**. For details, see"5.3.2.4 Extracting Person Information".
- Import person image: Select **Import** > **Import Person Image**, click **Download Template** to download the template, prepare the images according to requirements in the template, and then click **Import File**.

5.3.2.4 Extracting Person Information

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

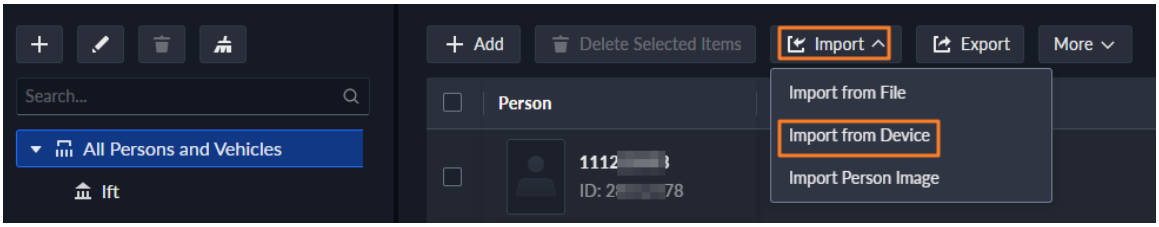
Procedure

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

Step 2 Click **Person List**.

Step 3 Click **Import** , and then select **Import from Device**.

Figure 5-13 Import from device

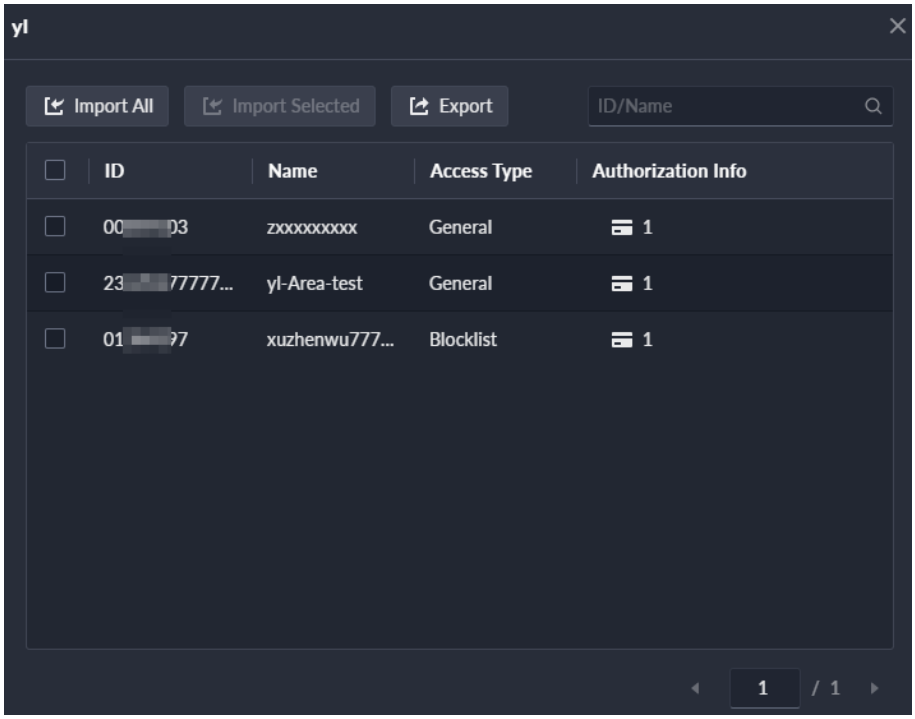


Step 4 Click , select a channel from an access control device or door station, and then click **OK**.

Step 5 Double-click a result to view the details.

Step 6 Synchronize person information to the platform, or export information.

Figure 5-14 Personnel extraction results



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

5.3.2.5 Importing Images of People

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

Prerequisites

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

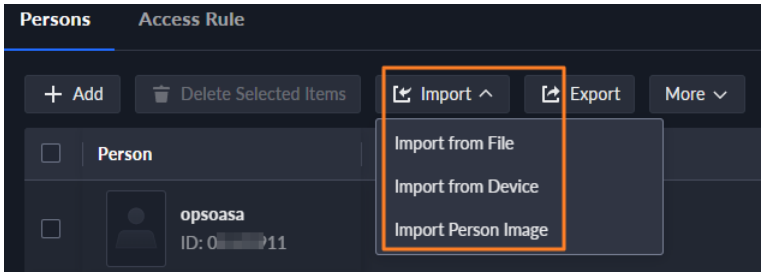
- A person can have up to 2 images, but only certain devices support recognizing people with 2 images.
- The image must be in .jpg format, and has a resolution ranging from 150 × 300 to 540 × 1080. It is preferred that it be 500 × 500. The image must not exceed 100 KB.
- Make sure that there is only 1 face in the image, with proportions between 1/3 and 2/3 of the whole image. The aspect ratio of the image must not exceed 1:2.
- Both eyes should be open with a natural expression. Expose the forehead and the face, and keep the hair away from blocking the forehead and the face. The 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 **Person and Vehicle Info** > **Person List** > **Persons**.

Step 2 Select **Import** > **Import Person Image**.

Figure 5-15 Import person image



Step 3 Click **Download Template** to save the zip file to your computer. It contains the instructions on how to prepare images, and 2 images for reference.

Step 4 Prepare images according to the requirements, and then rename them in the format of **Person ID-Person Name-1**.

1 means the first image of the person. Change it to **2** to make the second image of the person.

Step 5 Compress the images into a .zip file.

Step 6 Click **Import File**, and then open the .zip file.

The page will display the number of successes and failures. Click **Download Failure List** to see the reasons for the failures.

5.3.2.6 Synchronizing People in Domain

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

Prerequisites

Configure the information of the domain. For details, see "8.3.8 Configuring Active Directory".

Procedure

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

Step 2 Select **More** > **Sync Person in Domain**.

Step 3 Import persons in the domain to the specified person group.

Table 5-11 Parameter description

Parameter		Description
Manual Sync	Import Domain Users	Import all or certain people in the selected domain group to the selected person group on the platform. After importing the entire domain group, the group will be added to the automatic synchronization list. • **Import by Domain User** : Import selected users in a group. • **Import by User Group** : Import all users in the selected group. If you import an entire domain group after the automatic synchronization function is enabled, the platform will remember that group and automatically synchronize its new users at the defined time every day, and update the information of the users imported by manual selection at the defined time every day. For details, see the previous steps. • **Import by Security Group** : Import selected users in a security group.
	Sync Delete Domain User	When this option is selected, the platform automatically detects and displays the people that have been deleted from the domain. You can select whether to remove them from the platform.
	Sync Add Domain User	• For people imported from an entire domain group, the platform immediately imports the new people or updates the existing people's information. • For people imported by manual selection, the platform immediately updates their information.

Parameter	Description
Auto Sync Config	The list holds the domain groups that have been imported entirely. After setting the time, the platform will synchronize the new people and update the information of the existing people every day. For people imported by manual selection, the platform will update their information. Click to remove the group, the platform will not synchronize the new people, but will still update the information of the existing people.

Step 4 Click **OK**.

5.3.2.7 Moving People in Batches

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

Procedure

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

Step 2 Select a person group, and then the people in this group are displayed on the right.

Select **Include Sub Groups** to display all the people in this group and all its sub groups.

Step 3 Select multiple people, and then select **More** > **Move To**.

Step 4 Select a target group, and then click **OK**.

Step 5 Click **OK** again.

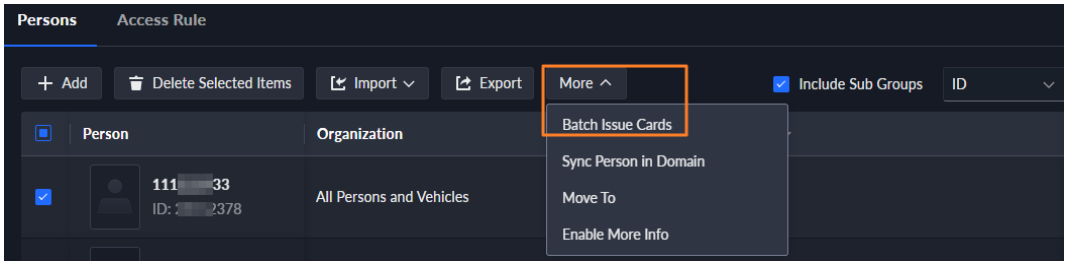
5.3.2.8 Issuing Cards in Batches

Procedure

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

Step 2 Select the people to issue card to, and then select **More** > **Batch Issue Cards**.

Figure 5-16 Issue card in batches



Step 3 Set validity period.

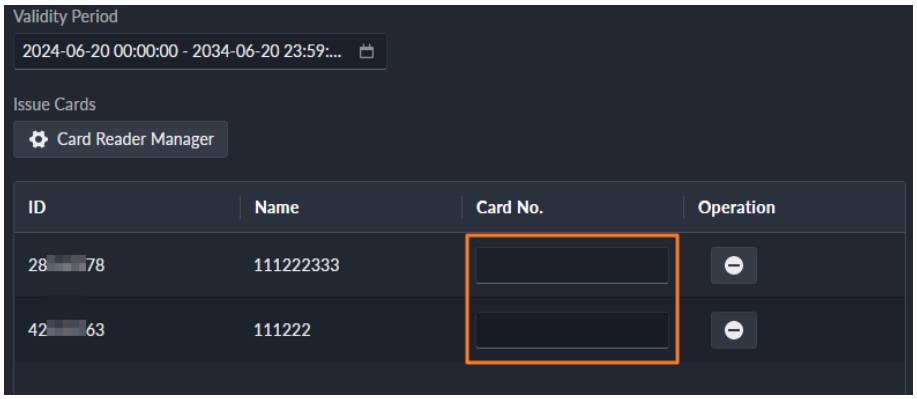
Step 4 Issue cards to personnel.

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

- By entering card number

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

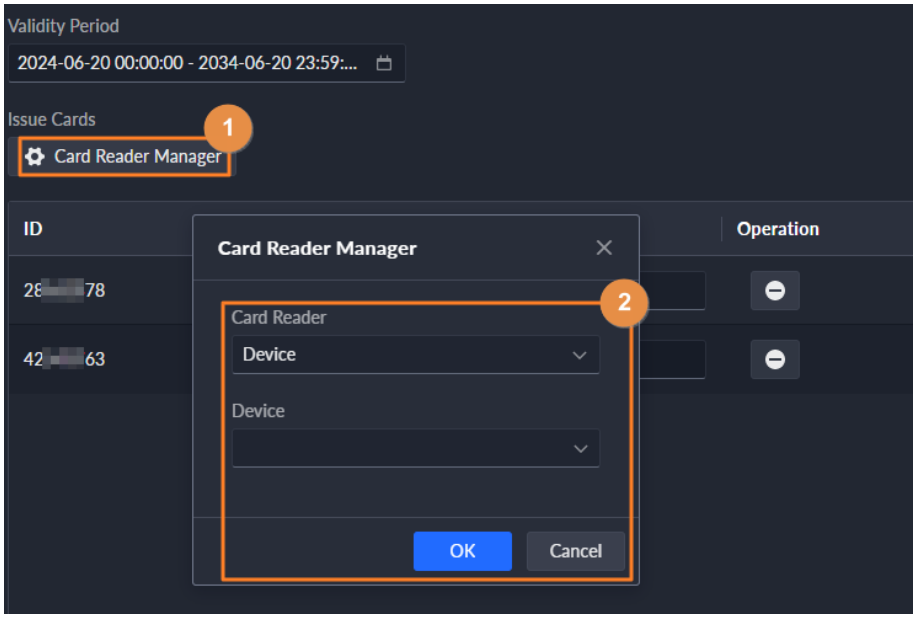
Figure 5-17 Enter card number



- By using a card reader

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

Figure 5-18 Reader manager



5.3.2.9 Deleting People

Notes

- After deleting people, their permissions (including vehicle access, person access, vehicle arming, person arming and parking lot permissions of vehicles) will also be deleted.

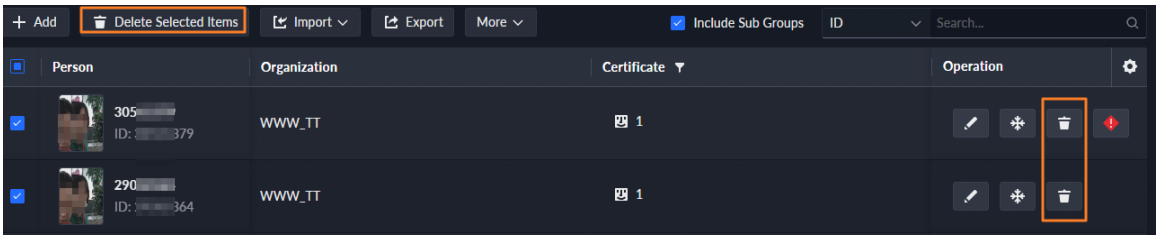
- After deleting people, the vehicles associated with the person will also be automatically deleted. After deleting a vehicle, the relationship between the person and the vehicle information will be unbound.
- If the deleted person belongs to the main person group, the person in the non-main person group will also be deleted; if the deleted person belongs to the non-main person group, the person will not be deleted in the main person group.

Operations

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

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

Figure 5-19 Delete people



5.3.2.10 Editing Person Information

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

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

Step 2 Click to edit information. For details, see "5.3.2.2 Adding a Person".

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

5.3.2.11 Searching for and Filtering People

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

Searching for People

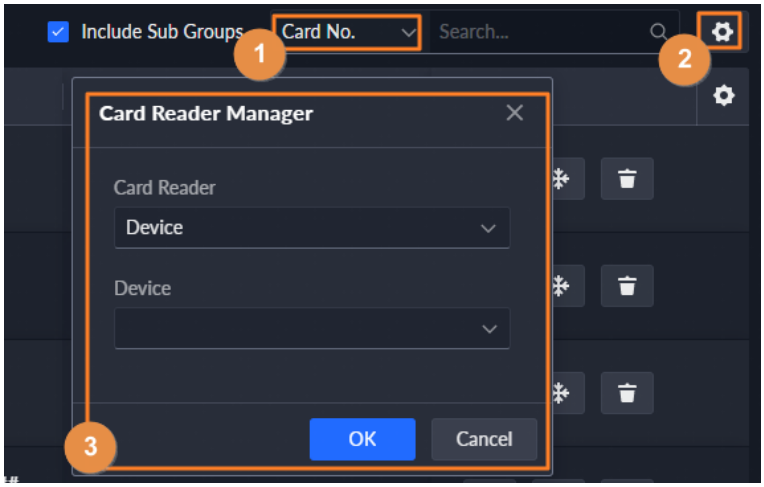
Select a person and vehicle group, enter keywords in the search area on the upper-right corner, and then click or press Enter to search for people who have that information. If **Include Sub Groups** is selected, the platform will also search for people in the sub groups of the one that you select.

Filtering People

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

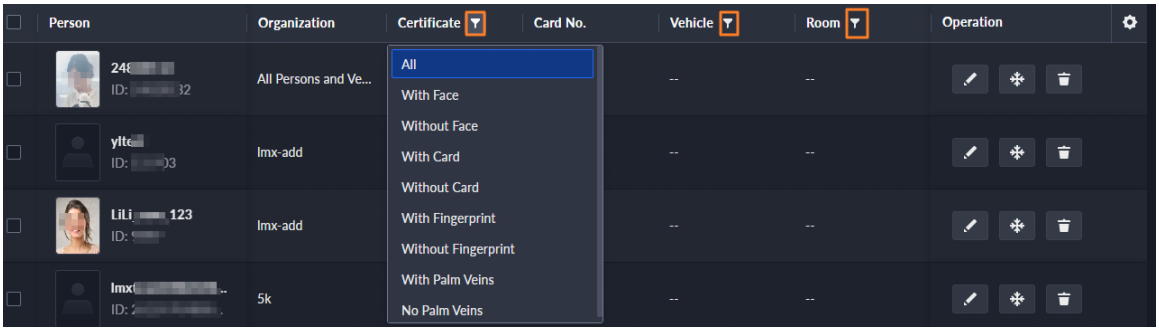
For example, when **Card No.** is selected, click , and then select swiping the card with a card reader or a device. When you swipe the card, the platform can directly read the card number and search, with no need of manually entering the card number.

Figure 5-20 Search by card number



Certificate, vehicle, and room can be used to further filter person information. For example, you can filter people with face or without face.

Figure 5-21 Filter by certificate



5.3.2.12 Configuring Access Rule

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

Background Information

The permissions of configuring access rules can be set by selecting **User** > **Role Management**, and then selecting the permissions in **Business Function** when adding roles.

Procedure

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

Step 2 Click a group, and then click **Access Rule**.

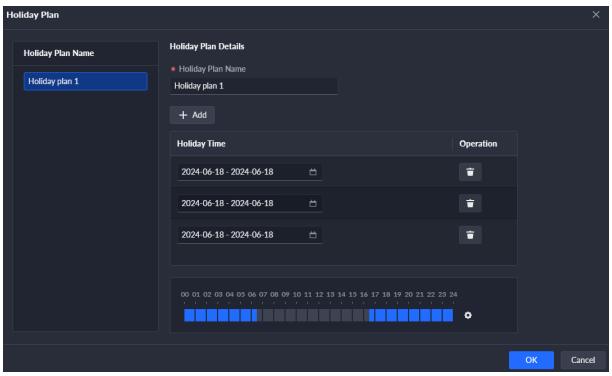
Step 3 Click **Quote**. This page displays rules that have been added. You can select and use any one of them directly.

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

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

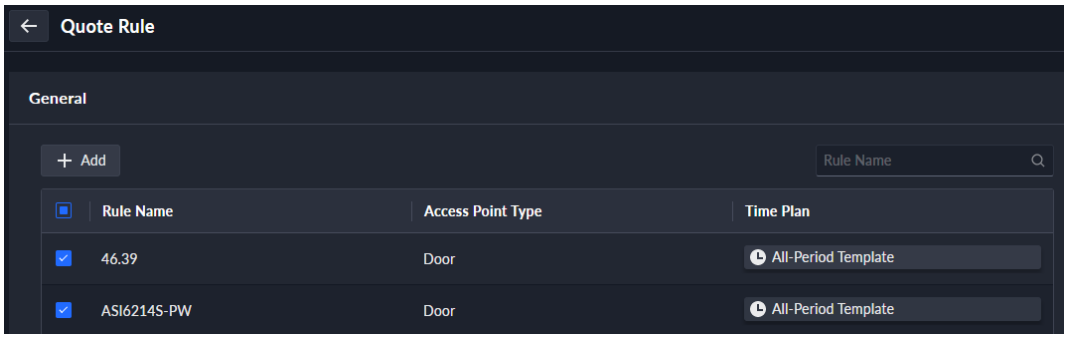
Table 5-12 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Select **Door** or **Lift**.
Rule Type	Only **General Verification** is available. For this type of rules, doors can be unlocked by face, card, fingerprint, and password.
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.7 Adding Time Template".

Parameter	Description
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. Follow the steps below to create a new holiday plan: 1. Select **Add Holiday Plan** in the drop-down list. 2. Enter a name for the holiday plan. 3. Click **Add** to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click ⚙ to configure the periods more precisely. You can configure up to 4 periods. 5. Click **OK**. 
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 5-22 Select access rules



5.3.3 Vehicle Management

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

Prerequisites

You need to add parking lot first. For details, see "5.7.2 Configuring Parking Lot".

Procedure

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

Step 2 Add vehicles.

- Add vehicles one by one

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

   When personnel and vehicles are not in the same vehicle group, the vehicle owner should be selected based on the vehicle group of the personnel.
3. Configure the information of the vehicle in the **Vehicle Info** section, such as plate number (required and unique), vehicle color, vehicle brand, and remarks.

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

   Click to display the vehicle information fields that you want to configure, including vehicle organization, vehicle organization phone number, and vehicle organization leader.
4. In the **Parking Lot Vehicle Group** section, click **Add**, and then you can select the plate number (the one added in the previous step) and parking lot, set the vehicle group that the vehicle belongs to, and the validity date of the vehicle's access permissions.

   If the owner has more vehicles than the defined parking spaces, once no parking spaces available, the owner cannot access the parking lot.
5. Click to enable **Vehicle Arming Group** , and then click **Add** to arm the vehicles that you have just added.

   For arming group details, see "5.4.2.1 Adding Vehicle Arming Group".
6. Click **OK**.

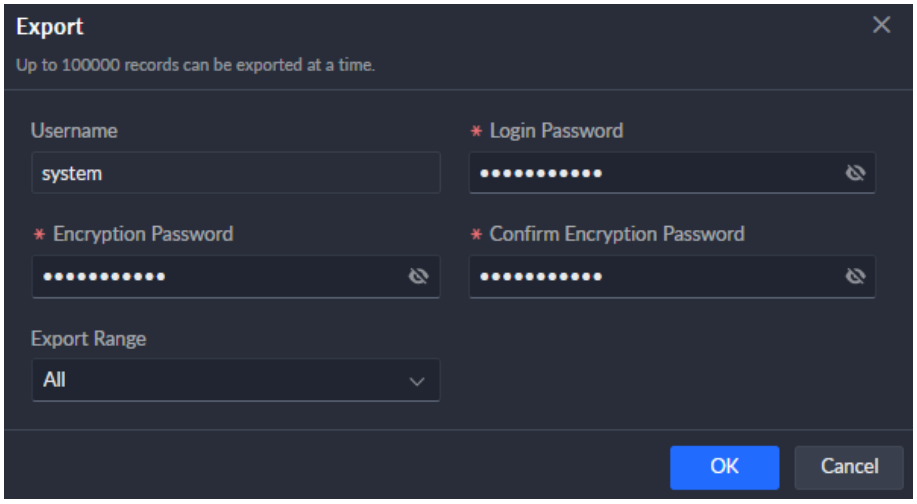
- Add vehicles in batches

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

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

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

Figure 5-23 Export vehicle information



1. Click **Export**.
2. Enter the platform login password, and set the encryption password.
3. Set **Export Range** to **All**, so that you can export all records; or set **Export Range** to **Select Range**, and then enter the start record and total records that you want to export.
4. Click **OK**.

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 Arming List

Configure face and vehicle arming list for future investigation.

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

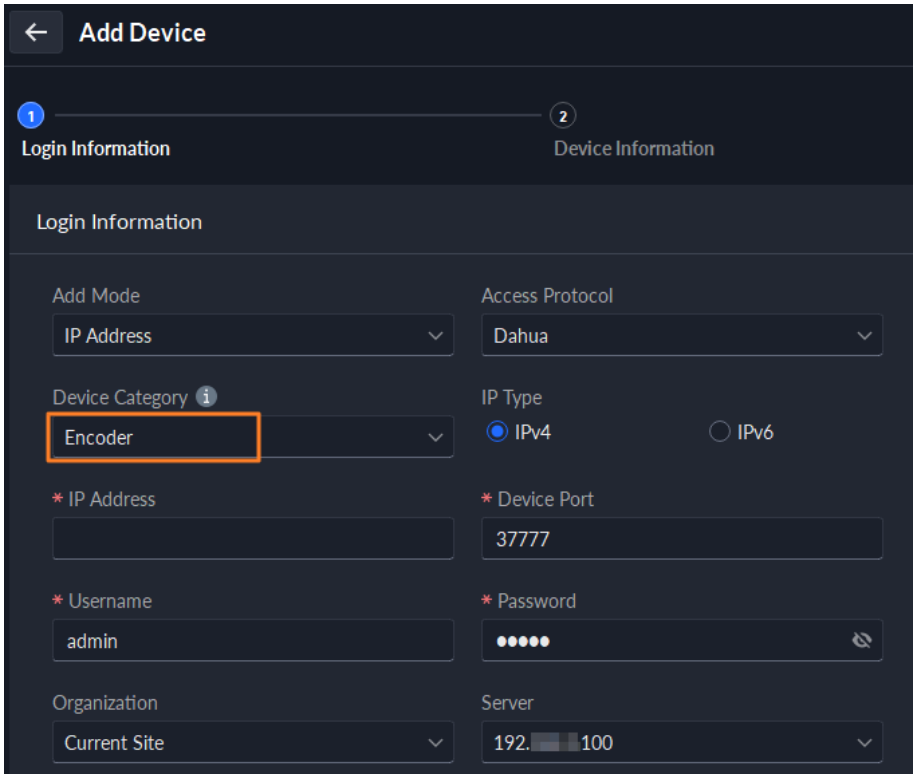
5.4.1.1 Creating Face Arming Group

Prerequisites

- The permissions of face arming group can be configured by selecting **User** > **Role Management**, and then selecting the permissions in **Business Function** when adding roles.
- Make sure that the devices for face recognition have been successfully configured on the platform.

- Make sure that the basic configuration of the platform is complete. 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



  - ◇ 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.
Arming Group Type	Only general arming is available.
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 that you want to add people to it.

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

- Add people by person groups. This is the most efficient way, provided that you have created person groups based on the access permissions. For details, see "5.3.2 Configuring Person Information".

  Click **Add by Person Group** , select one or more groups, and then click **OK**. You can also select **Include Sub Groups** to include the people in the sub groups of the groups you select.
- Select the people you want to add. This is applicable to people in different person groups have the same access permissions.

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

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

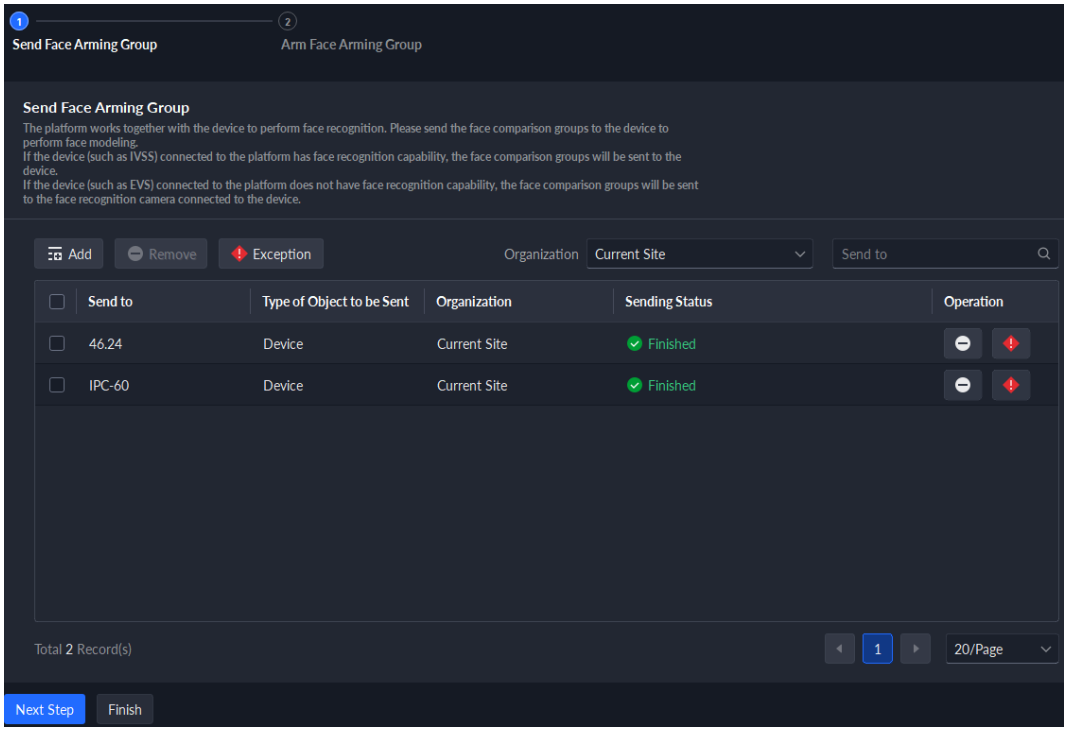
Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Arming List** > **Face Arming List**.

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

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

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

Figure 5-25 Send face arming group (device arming)



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

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

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

Step 6 Click **OK**.

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

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

5.4.2 Vehicle Arming List

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

5.4.2.1 Adding Vehicle Arming Group

A vehicle arming group contains the information of multiple vehicles. When arming the group, you can arm all the vehicles inside the group at the same time. You can add up to 16 vehicle arming groups.

Background Information

The permissions of vehicle arming group can be configured by selecting **User** > **Role Management**, and then selecting the permissions in **Business Function** when adding roles.

Procedure

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

Step 2 Click **Add**, and then configure the parameters.

Table 5-14 Parameter description

Parameter	Description
Vehicle Arming Group Name	Enter the name that identifies the group.
Arming Group Type	Only general arming is available.
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**.

5.4.2.2 Adding Vehicles

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

Step 1 Log in to the DSS Client. On the **Home** page, click , and then click **Arming List** > **Vehicle Arming 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 Person Information".

  Click **Add by Vehicle Group** , select one or more groups, and then click **OK**. You can also select **Include Sub Groups** to include the vehicles in the sub groups of the groups you select.
- Select the vehicles you want to add. This is applicable to vehicles that you want to add are in different vehicle groups.

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

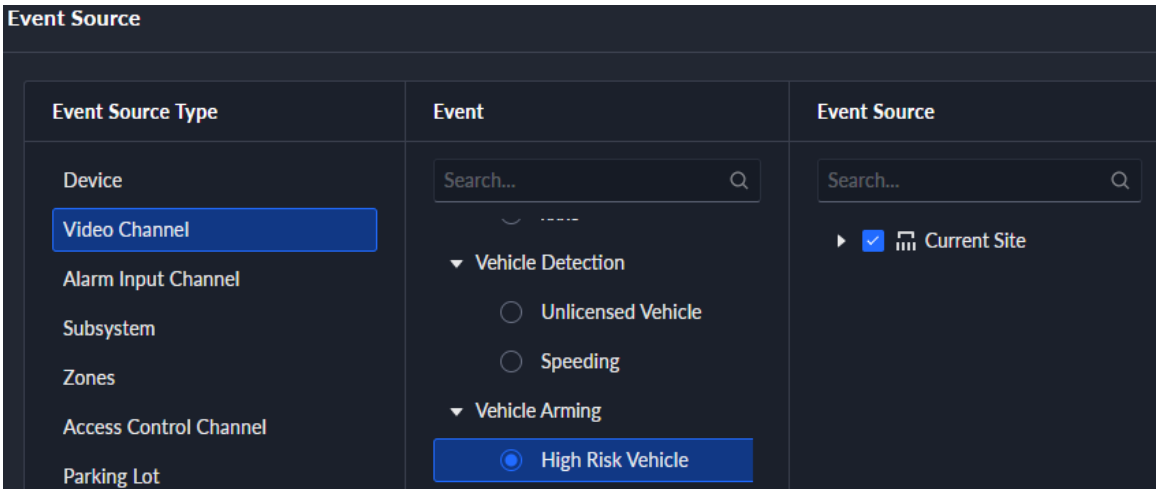
5.4.2.3 Arming Vehicles

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 arming list. For how to configure events, see "5.1.1 Configuring Event Linkage".

Figure 5-26 Arm vehicle event



5.4.3 Text-Defined Alarms

5.4.3.1 Adding Text-Defined Alarms

After adding text-defined alarm rules on the platform, they are automatically sent to the devices. The devices create text-defined alarm algorithms to detect and trigger events in real time, and the platform receives the events.

Background Information

The permissions of text-defined alarms can be configured by selecting **User** > **Role Management**, and then selecting the permissions in **Business Function** when adding roles.

Procedure

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

Step 2 Click **Add**, and then configure the parameters.

Table 5-15 Parameter description of text-defined alarms

Parameter	Description
Alarm Name (Event Name)	Enter the name of the alarm event.
Prompt	Users can set up inclusion and exclusion prompts. Users add the text-defined alarms onto the channels of the devices, and then create event plans on the server. Once the prompt rules are triggered, the server will receive the event and then send the alerts to the event center. The inclusion prompt function supports text searching and matching. The exclusion prompt function is disabled by default and can be manually enabled as needed.

Parameter	Description
Confidence Level	Set the confidence level for matching inclusion and exclusion prompts. • The confidence level for inclusion prompts is 70% by default and can be configured from 1% to 100%. • The confidence level for exclusion prompts is 70% by default and can be configured from 1% to 100%.

Related Operations

- Click  to view sending exception. Supports sending it again to update the sending results.
- Click  to view the arming texts.
- Click  to edit the arming texts.
- Click  to delete the arming texts.



When the platform modifies or deletes arming texts, it will be synchronized to the device. If the text-defined algorithm name or alarm ID is modified or deleted on the device, the platform will not subscribe to the change, and the arming status will not be updated.

5.4.3.2 Configuring Events

Only after the text-defined alarms are added and events are configured, can the platform link the Event Center and generate alarms.

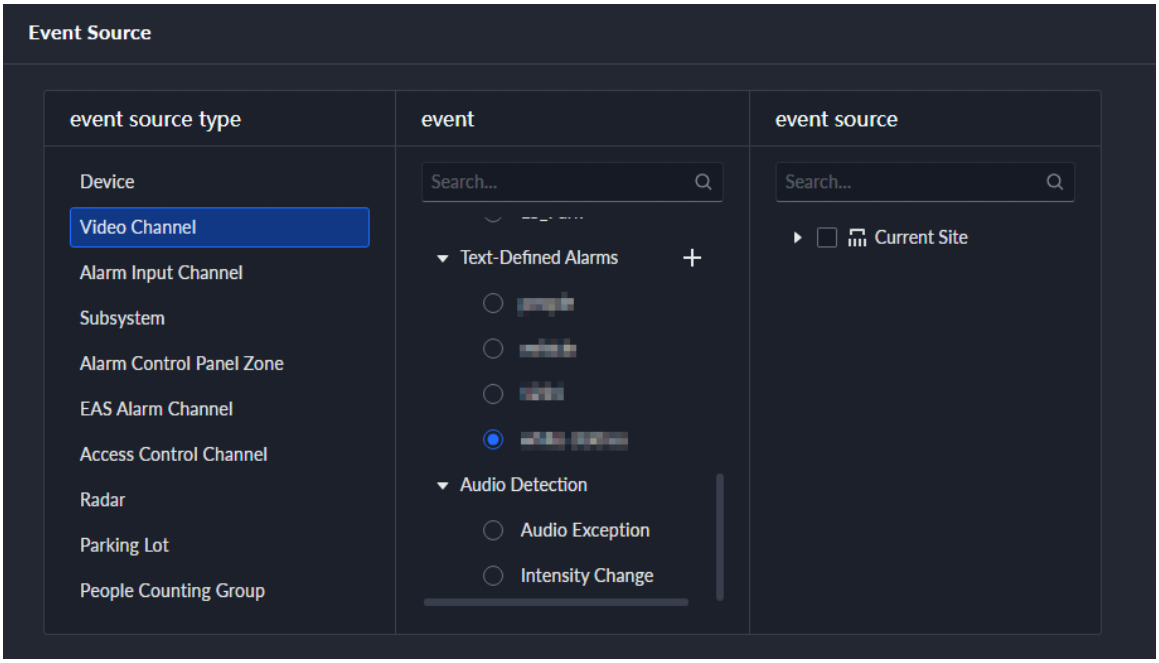
Procedure

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

Step 2 In the added text-defined alarms list, click .

Step 3 Click **Add** to add an event to arm the text. For how to configure events, see "5.1.1 Configuring Event Linkage".

Figure 5-27 Arming texts



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** from **Device Category**.
  - ◇ (Optional) You can bind video channels to access control channels, so that you can monitor the area near access control devices. For details, see "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 and lifts. Create zones to quickly define security control areas with different permissions.

- The permissions of configuring zones can be set by selecting **User** > **Role Management**, and then selecting the permissions in **Business Function** when adding roles.

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

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 5-16 Parameter description

Parameter	Description
Parent Zone	Select a parent zone for zone management.
Zone Name	Enter a name for the zone.
Icon	Select an icon for the zone. Icons are used for users to quickly identify different zones.
Select Access Point	Select access points from an existing zone. You cannot batch move the access points that have been configured with rules.
Roles Allowed Access	Only the selected roles and their users can access this zone. Click to see the users assigned with the roles.

Related Operations

Right-click the zone name, and then select **View Details** to view zone details.

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 5-28 Add zones in batches

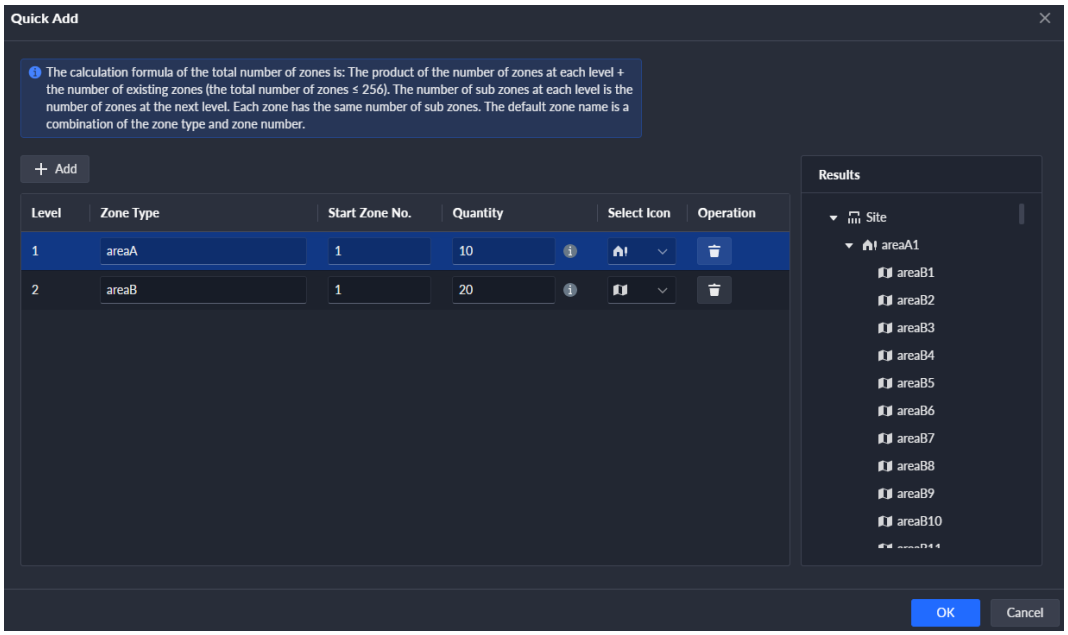


Table 5-17 Parameter description

Parameter	Description
Level	The number indicates the level of the zone. The region with a larger number is a sub zone of the region with the smaller number. For example, the level 2 zone is a sub zone of the level 1 zone.
Zone Type	Enter a name for the zone.
Start Zone No.	Enter a start number and then all the zones of this level will be automatically numbered. For example, if the start number is 1 and the quantity of zones is 3, then zones will be numbered as zone 1, zone 2, and zone 3.
Quantity	Enter a number for each zone. The number of each level of zones = upper levels × 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

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.

  You cannot delete the zone if it has access points or sub zones. If you cannot view them, go to **User** > **Role Management**, and then check whether the role has the permissions.

5.5.2.4 Moving Access Points

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

Background Information

- When you move an access point, you can move it to any zone.
- When you move access points in batches, if rules have been configured in the zone, you cannot move them; if no rules have been configured, you can move 100 access points at a 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** > **Zone Management**.

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

All access points and sub zones will be displayed.

Step 3 Move the access points.

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

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

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

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

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

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.
- **Access Point Type** : Displays the type of the access point, door or lift.
- **Zone Name** : Displays the name of the zone the access point belongs to.
- **Remark** : Supports customizing the remarks on the access point.
- **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 click **Quote** or **Remove** to add or delete the rules, but the rules from the zone cannot be deleted.

5.5.2.5.2 Setting Boundary

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

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

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

Step 3 Right-click an access point (door, not lift) and select **Set as Boundary**.

The icon of the access point changes to .

5.5.2.6 Configuring Access Rule for a Zone

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

Background Information

The permissions of configuring access rules can be set by selecting **User** > **Role Management**, and then selecting the permissions in **Business Function** when adding roles.

Procedure

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

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

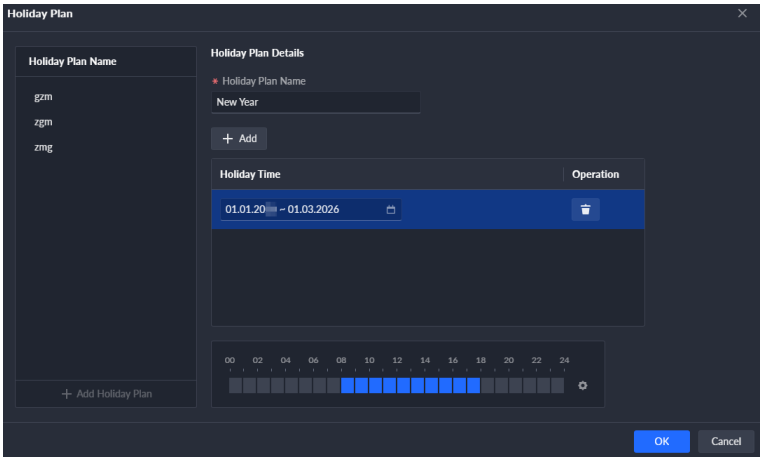
Step 3 Click **Quote**. The system displays rules that have been added.

You can:

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

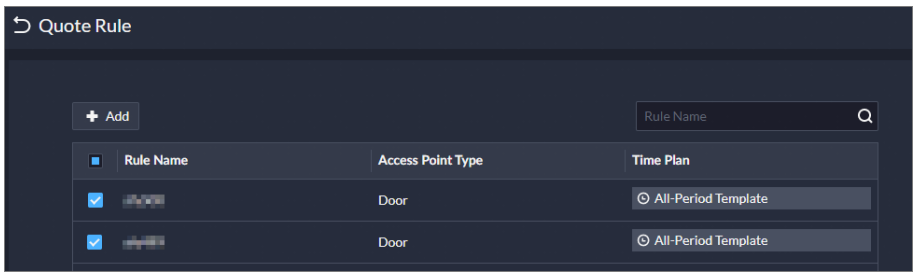
When configuring an access rule for a zone, you can only configure general verification rules for doors. If you want to configure other types of rules, see "5.5.3 Configuring Access Rule".

Table 5-18 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, passwords, palm veins, faces, and Bluetooth cards.
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.7 Adding Time Template".
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. Follow the steps below to create a new holiday plan: 1. Select **Add Holiday Plan** in the drop-down list. 2. Enter a name for the holiday plan. 3. Click **Add** to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click to configure the periods more precisely. You can configure up to 4 periods. 5. Click **OK**. 
Select by Person Group	Select one or more person groups, and then all the persons in the groups will have permissions to access all the door channels in the zone. Select **Link Sub Node**, and then you can select a zone and all its sub zones at the same time.

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.

Figure 5-29 Select access rules



Step 4 Click **OK**.

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 a Map

Procedure

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

Step 2 Click a zone, and then click **Map Info**.

Step 3 Click **Configure Map** to add a map for the zone.

- Select a map that has been added to the platform.
- Upload an image as the map. After added, the map will be added to the platform as a main map. To know more about maps, see "5.2.2 Adding a 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.

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 lift or door channels.

Background Information

The permissions of configuring access rules can be set by selecting **User** > **Role Management**, and then selecting the permissions in **Business Function** when adding roles.

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.

5.5.3.2 Configuring General Verification

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

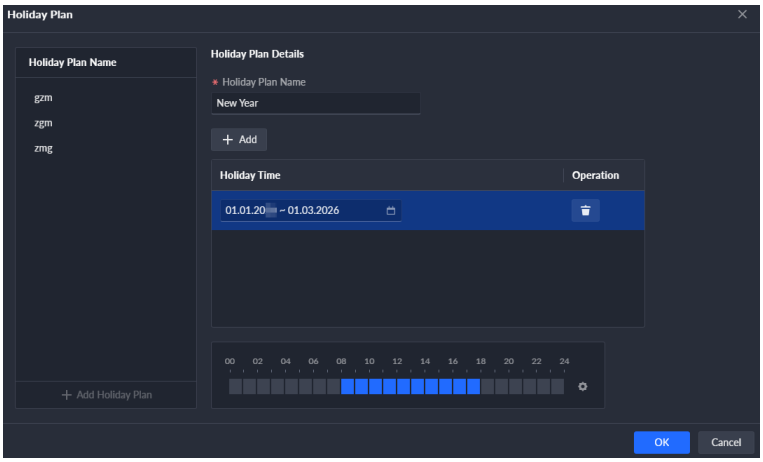
Procedure

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

Step 2 Click **Add**.

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

Table 5-19 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Select **Door** or **Lift**, and then the platform will only display corresponding channels.
Rule Type	Select **General Verification**.
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.7 Adding Time Template".
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. Follow the steps below to create a new holiday plan: 1. Select **Add Holiday Plan** in the drop-down list. 2. Enter a name for the holiday plan. 3. Click **Add** to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click ⚙ to configure the periods more precisely. You can configure up to 4 periods. 5. Click **OK**. 
Select by Zone	Select one or more zones, and then this rule will be applied to all access points in the zones. Select **Link Sub Node**, and then you can select a zone and all its sub zones at the same time.
Select by Access Point	Select one or more access points. Select **Include Sub Zone** to display all the access points in the selected zone and its sub zones.

Parameter	Description
Select by Person Group	Select one or more person groups, and then all the persons in the groups will have permissions to access the selected access points. Select **Link Sub Node**, and then you can select a zone and all its sub zones at the same time.
Select by Person	Select one or more persons, and then they will have permissions to access the selected access points. Select **Include Sub Groups** to display all the persons in the selected group and its sub groups.
Roles Allowed Access	Only the selected roles and their users can view and edit the rule. Click to view the users assigned with the roles.

5.5.3.3 Configuring Normally Open

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

Procedure

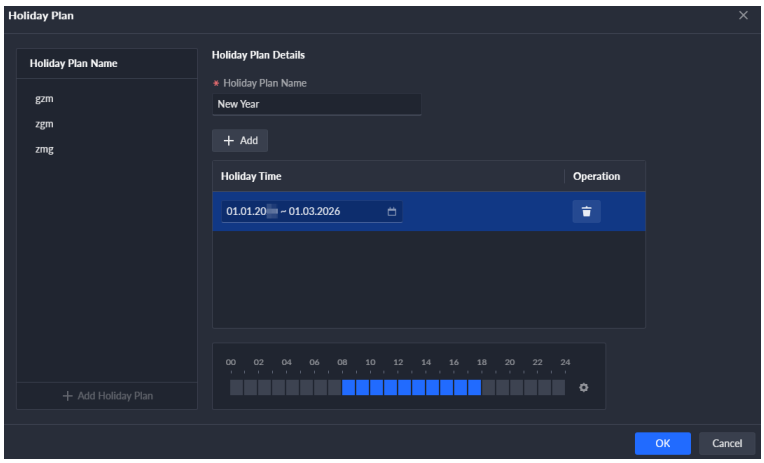
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.

Step 2 Click **Add**.

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

Table 5-20 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only **Door** is available.
Rule Type	Select **Remains Open during Period**.
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.7 Adding Time Template".

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

5.5.3.4 Configuring Normally Closed

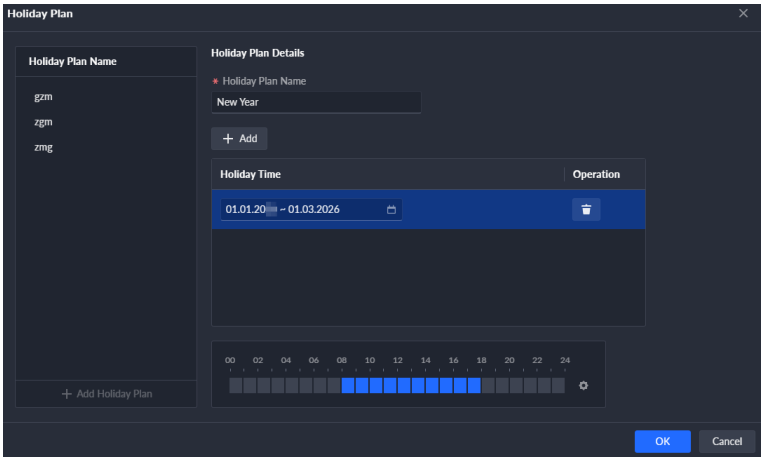
All people are not allowed to pass access points.

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

Step 2 Click **Add**.

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

Table 5-21 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only **Door** is available.
Rule Type	Select **Remains Closed during Period**.
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.7 Adding Time Template".
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. Follow the steps below to create a new holiday plan: 1. Select **Add Holiday Plan** in the drop-down list. 2. Enter a name for the holiday plan. 3. Click **Add** to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click  to configure the periods more precisely. You can configure up to 4 periods. 5. Click **OK**. 
Holiday Plan Authentication	After defining the period in holiday plan authentication, authentication is required for access within the defined period on the holiday. The operations are similar to those of adding holiday plan. You can add up to 4 plans.
Access Point	Select one or more doors. Select **Include Sub Zone** to display all the access points in the selected zone and its sub zones.

Parameter	Description
Roles Allowed Access	Only the selected roles and their users can view and edit the rule. Click to view the users assigned with the roles.

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 5-22 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only **Door** is available.
Rule Type	Select **First-person Unlock**.
Rule Type after Unlocked by First Person	• **Normal** : Other persons must verify their identifications to pass. • **Always Open** : All people can pass without verifying their identifications.
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.7 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.

Parameter	Description
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". • First-person unlock rules only support **General** access type. • People whose access types are **Patrol** will not be restricted by the rule. When no one in the first-person unlock rule unlocks the door, a patrol event for people whose access types are **Patrol**, and the door will not open.
Roles Allowed Access	Only the selected roles and their users can view and edit the rule. Click to view the users assigned with the roles.

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".

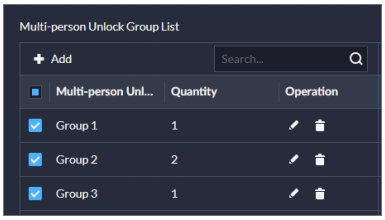
Procedure

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 5-23 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	Configure up to 4 unlock groups. Persons must verify their identifications in the group order to unlock doors. 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. ● 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". 4. Click **OK**. 5. (Optional) Repeat the steps below to add more groups. 6. Select the groups that you added, and then click **OK**.  7. Click the up or down arrows to adjust the group order, and then click **OK**.
Roles Allowed Access	Only the selected roles and their users can view and edit the rule. Click to view the users assigned with the roles.

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

Figure 5-30 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 in this order. They cannot enter building D directly.

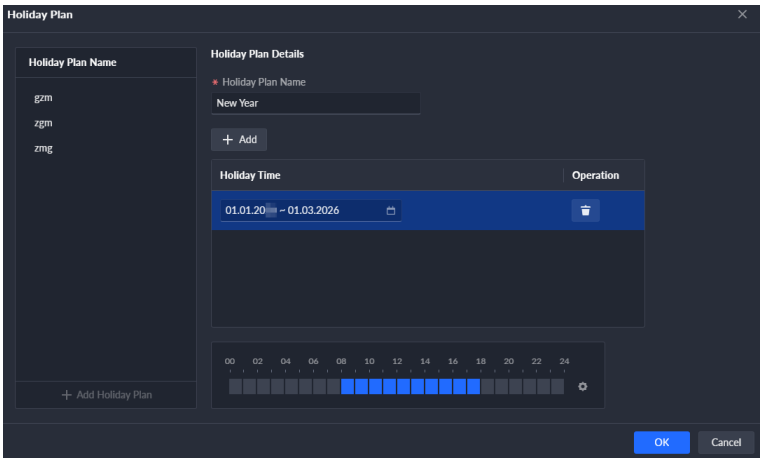
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.

Step 2 Click **Add**.

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

Table 5-24 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only **Door** is available.
Rule Type	Select **Anti-passback**.
Anti-passback Type	For **Local Anti-passback** , you can select only the door channels of an access control device; for **Global Anti-passback**, you can select door channels from any zone (make sure that the channels support global anti-passback). If you select **Global Anti-passback**, you can configure the offline operation strategy at the same time: ● **Execute** : Offline access points will execute the anti-passback configurations. ● **Do Not Execute** : People can pass normally through offline access points.
Security Scenario	When setting **Anti-passback Type** to **Global Anti-passback**, you can configure high security scenario and low security scenario. ● **High Security** : After anti-passback is triggered, all the doors configured for this rule will be locked. Only the administrator can lead the person out of the area. ● **Low Security** : After anti-passback is triggered, the person can go forward along the correct route.
Reset Time	If people do not pass in the defined order, they will not be allowed to pass any door within the reset time. After the reset time, they must follow the order from the beginning. The reset time can be between 1 minute and 24 hours.
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.7 Adding Time Template".

Parameter	Description
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. **Local Anti-passback** does not support holiday plan. Follow the steps below to create a new holiday plan: 1. Select **Add Holiday Plan** in the drop-down list. 2. Enter a name for the holiday plan. 3. Click **Add** to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click  to configure the periods more precisely. You can configure up to 4 periods. 5. Click **OK**. 
Access Point	Add doors to different groups, and then people must pass in the group order to access the last door. When setting **Anti-passback Type** to **Global Anti-passback**, pay attention to the following information. ● It supports zone anti-passback and route anti-passback. ◇ **Zone Anti-passback** : After entering the zone, the person can only exit and cannot repeatedly enter or exit. The card swiping records for boundaries can be used to determine whether a person entered or exited. You can configure the boundaries according to "5.5.2.5.2 Setting Boundary". ◇ **Route Anti-passback** : When a person opens a door in group 1, the next door the person can open is in group 2. ● The platform will only display devices that support this function. ● You can select **Include Sub Zone** to display all the access points in the selected zone and its sub zones.

Parameter	Description
Person	Select the persons that will not be subject to the global anti-passback rules. You can only add up to 1,000 persons to a single rule. Make sure that the **General Verification** rule has been configured for the person. For details, see "5.5.3.2 Configuring General Verification".
Roles Allowed Access	Only the selected roles and their users can view and edit the rule. Click to view the users assigned with the roles.

5.5.3.8 Configuring Multi-Door Interlock

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

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

Procedure

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

Step 2 Click **Add**.

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

Table 5-25 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	Select an interlock type. If you select a global interlock rule, you can configure the offline execution strategy at the same time: • **Execute** : Offline access points will execute the interlock configurations. • **Do Not Execute** : People can pass normally through offline access points. If any access point in the global interlock rule goes offline, people cannot pass through online access points, which will trigger multi-door interlock rule.
Time Template	The all-period time template is used by default and cannot be changed.
Access Point	Select an access control device, and then add its doors to different groups. When a door in any group is unlocked, people cannot pass through any other door. If remote verification is also configured at the same time, the platform will verify remote verification first. When it passes, multi-door interlock will then be verified. For example, if person A wants to open door B in group C, the remote verification will be sent to the platform. After the platform confirms that the remote verification, it will then check whether any door in other groups are opened. If any door is opened, person A cannot open door B. When configuring a global interlock rule, select **Include Sub Zone** to display all the access points in the selected zone and its sub zones.
Roles Allowed Access	Only the selected roles and their users can view and edit the rule. Click to view the users assigned with the roles.

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 5-26 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 "4.2.7 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.
Roles Allowed Access	Only the selected roles and their users can view and edit the rule. Click to view the users assigned with the roles.

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.

5.5.3.10 Permission Maintenance

After you add 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.

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** > **Permission Maintenance**.

Step 2 View and process the exceptions by tasks or by device.

- **All Tasks** : Displays the information of pending and sending tasks, and tasks with exceptions. Supports filtering tasks by access point and person.
  - Tasks that the person has no permissions will not be displayed.
  - Click person name or access point name, and it will go to the page of edit person or access point.

  For tasks with exceptions, you can hover over to view the cause of the exception. After troubleshooting, you can click to send again.
- **By Device** : Displays the pending and sending tasks, and the total number of failed devices. Supports filtering tasks by device.
  - For tasks pending sending, click **Start** to start sending the task; after that, you can click **Pause** to pause sending the task.
  - For tasks that fail to send, you can:
    - Click to view the task details.

- Click  to view the exception details (on the **Exception Details** page, click **Send Again** to send the task again).
- For devices that the task has been sent and there is exception, you can select them, and then click **Resend Abnormal Person Info** to send the tasks in batches.

5.5.3.11 Verifying Permissions

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 **Images and Files** disk for the server where the device is added to. For details, see "4.4 Configuring Storage".

Background Information

Device permission is required. If you do not have the device permissions, you cannot verify the permissions.

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** > **Permission Verification**.

Step 2 Verify the permissions. Supports **Verify Now** and **Verify by Schedule**.

- Verify now: Click **Verify Now** , select the devices to be verified, and then click **OK**.
- Verify by schedule: Verify the selected devices according to the defined schedule.
  1. Click **Verify by Schedule**.
  2. Click **Add Task**.
  3. Set the task name, verification start time (you can select executing the task by month or week), and select the devices to be verified.

     Devices included in other verification tasks will not be displayed.
  4. Click **OK**. The task is enabled by default.

The verification records are generated on the **Permission Verification** page. Wait for the verification to complete.

You can click  to verify again. The historical verification results will be overwritten.

Step 3 Process the verification results.

- If it displays **Pending Verification** , **Verifying**, or **Processing Exception**, wait for the verification or processing to finish.
- If it displays **Cancel**, no operation is required.
- If it displays **Finished Without Abnormal Info**, it means that the people on the device match those on the platform, and the device passes the verification.
- If it displays **Failed**, hover over , and then you can view the reason for the failure.
- If it displays **Abnormal** , click **Details** to view and process the exceptions.

Table 5-27 Exceptions and how to process them

Exception	How to Process
Person Not on Platform	◇ Click **Delete** to remove person information from the device. ◇ Click **Extract** to extract the person from the device to the platform. The system will automatically go to the **Import from Device** page. For details, see "5.3.2.4 Extracting Person Information".
Person Not on Device	Click **Resend** to send the person information to the device. The original information of the person on the device will be overwritten.
Inconsistent Person Info between Platform and Device	◇ Click **Resend** to send the person information to the device. The original information of the person on the device will be overwritten. ◇ Click **Extract** to extract the person from the device to the platform. The system will automatically go to the **Import from Device** page. For details, see "5.3.2.4 Extracting Person Information".
Permissions Not Matched	Click **Delete** to remove person information from 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 in the platform, and up to 500 passwords for a single device.

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

Step 2 Click .

Step 3 Enter a name for the password, configure the password, and then select the door channels from access control and video intercom devices that the password will be applied to.

Step 4 Click **Save**.

Step 5 (Optional) If exceptions occur, click to view details. Handle the exceptions according to the reasons provided by the platform, and then click **Send Again**.

5.5.5 Configuring Credential Security

You can enable **Device DESFire Card** , **Block NFC Cards**, or fingerprint uniqueness verification as needed.

5.5.5.1 Configuring Access Card

You can enable **Device DESFire Card** or **Block NFC Cards** as needed. After enabling DESFire card, the platform can issue cards to people by DESFire card reader, and then people can access by using DESFire cards; by enabling **Block NFC Cards**, the device will not recognize copied NFC cards, and people cannot use NFC cards to open doors.

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

Step 2 Enable **DESFire card** and **Block NFC Cards** as needed.

Table 5-28 Access card configuration description

Parameter	Description
Device DESFire Card	After enabled, the DESFire card can be used normally. Make sure that the device supports reading DESFire card; otherwise, the card cannot be recognized.
DESFire Card Encryption	After enabled, the DESFire card reader only shows the encrypted information.
Block NFC Cards Apply to Device	Enable **Block NFC Cards** , and then click **Apply to Device**, the devices will not recognize copied NFC cards, and people cannot use NFC cards to open doors.
Write to DESFire	After enabling **Device DESFire Card** and **DESFire Card Encryption**, you can click this icon, select a device that supports reading and writing DESFire cards from , enter the card number, and then the device can write the card number to the card.

5.5.5.2 Configuring Fingerprint

You can enable **Verify Fingerprint Uniqueness** as needed. After enabling it, the platform will verify the uniqueness of fingerprints when it sends fingerprint credentials to devices.

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

Step 2 Enable **Verify Fingerprint Uniqueness** as needed, and then click **Apply to Device** to apply the settings to devices that support the above capability.

5.5.5.3 Configuring Short Password Access

Access control supports unlocking the door with the short passwords. Once the feature is enabled, personnel can enter only the short password to unlock the 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** > **Basic Config** > **Credential Security Config** > **Short Password Config**.

Step 2 Enable the function of short password access.

Step 3 Click **Apply to Device** , read and confirm the prompt, and then click **OK**.

The PIN code for unlocking the door with the password is consistent with the unlocking password configured when adding personnel in the **Person and Vehicle Info**. For details, see "5.3.2.2 Adding a Person".

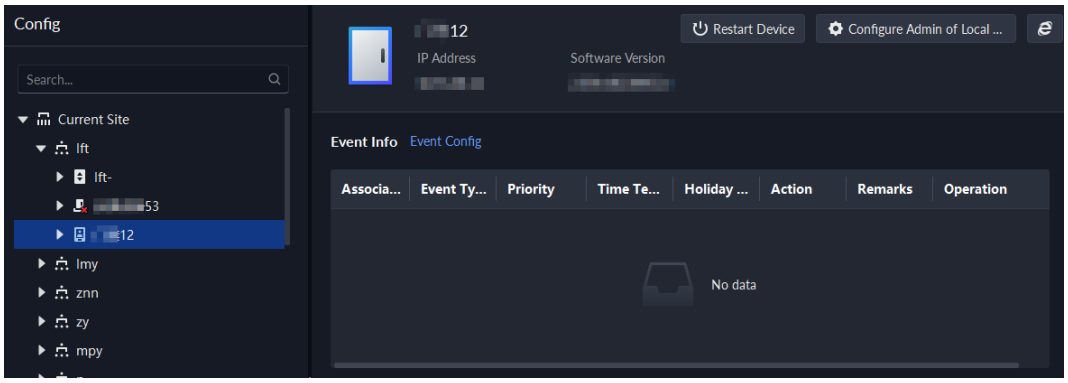
5.5.6 Configuring Access Control Devices

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.

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 5-31 Select an access control device



Step 3 Configure the access control device.

- Click **Restart Device** to restart the device.
- Click **Configure Admin of Local Device** and add people from person groups. Then, the people can use their usernames and passwords to log in to the configuration page of the device.
- Click at the upper-right corner to go to the webpage of the device.

5.6 Visitor Management

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

5.6.1 Preparations

- Access control devices and lift control devices have been added to the platform.
- Basic configurations of the platform have been finished. For details, see "4 Basic Configurations".
- Configure email server first if you want to send emails to the visitor. For details, see "8.3.6 Configuring Email Server".

5.6.2 Configuring Visitor Appointment

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

You can also go to the **Visitor Config** page by selecting **Access Management** > **Visitor** > **Visitor Management/Visitor Records**, and then clicking at the lower-left side.

Step 2 Click **Visitor Appointment Config**, and then configure the parameters.

Table 5-29 Parameters of visitor appointment

Parameter	Description
Create Appointment	The platform administrator can configure visitor appointment information and send the link to visitors' emails or provide QR codes. Visitors can enter the link or scan the QR code to fill out their visitor information. After approval, visitors will receive an access pass via email. The system supports creating appointment by visitors (see "6.4.2.4.2 Creating Appointment by Visitors") and host invitation (see "6.4.2.4.3 Appointment Invited by Host"). Make sure that LAN and WAN mapping is configured. For details, see "2.5 Configuring LAN or WAN".
Host Invitation	
Appointment Expiration Config	Enable **Configure Appointment Expiration Time**, and then set the timeout period. If the visitor does not visit within the defined period after the appointment, the appointment will automatically expire. For example, if the visitor's appointment arrival and leaving time are set to 9:00 am and 9:00 pm respectively, and the expiration time is set to 1 hour, the appointment will be invalid if the visitor does not arrive at 10:00 am; if the expiration time is set to 13 hours, then the appointment will be invalid at 9:00 pm. • The appointment will expire after the appointment leaving time expires. • The appointment will expire if the appointment is not approved after the appointment leaving time. • The visitor status will be automatically updated at the defined time of each day. It is 2:00 am each day by default.

Step 3 Click **Save**.

5.6.3 Configuring Visitor Registration

Configure automatic arrival and leave points. Visitors with appointment can verify their identities on the selected arrival points without registering, and visitors who are visiting can verify their identities on the selected leave points to end their visits automatically.

Procedure

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

You can also go to the **Visitor Config** page by selecting **Access Management** > **Visitor** > **Visitor Management/Visitor Records**, and then clicking at the lower-left side.

Step 2 Click **Visitor Registration**, and then configure the parameters.

- Arrival and registration: Enable the function, and then select the channels as needed. Visitors with appointment can verify their identities on the selected channels without registering.
- Leave registration:
  - Enable the function, and then select the channels as needed. Visitors who are visiting can verify their identities on the selected channels to end their visits automatically.
  - Set the visitor on-site notification time (10 am every day by default). When a visitor has not left after the visit time, the platform sends notifications to users with permissions of the visitor management menu to remind them of the number of visitors that overstayed.

Step 3 Click **Save**.

5.6.4 Configuring Registration and Appointment

Supports customizing visitor registration and appointment fields, which can be used for filling in information on the visitor appointment and registration pages.

Procedure

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

You can also go to the **Visitor Config** page by selecting **Access Management** > **Visitor** > **Visitor Management/Visitor Records**, and then clicking at the lower-left side.

Step 2 Click **Registration and Appointment Config**.

Step 3 Click **Add**.

Step 4 Set the field name, and then select the services.

Step 5 Set the field attributes, including required or not, display or not.

- If the field is required, it must be displayed.
- Inherent fields of the platform cannot change the name and cannot be deleted.

Step 6 Click **Save**.

5.6.5 WhatsApp Message Template

Integrating WhatsApp allows for visitor appointment scheduling, notifications, credential issuance, and real-time communication. It supports custom WhatsApp message templates and Meta templates for sending messages related to visitor appointments, approvals, and more.

Prerequisites

You have completed the WhatsApp integration configuration. For details, see "8.3.5 WhatsApp Integration Configuration".

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 Click **WhatsApp Message Template**.

Step 3 Add the templates. The templates include custom template and meta template.

- Custom template: Supports the templates for visitor appointment, approve, review failures, review search, 23-hour reminder and service overview. The configuration method for templates of different purposes is similar. Takes the visitor appointment template as an example.
  1. Click **Add Custom Template**.
  2. Enter the template name, and then select the template usage as **Visitor Appointment**.
  3. Configure keywords to trigger the corresponding message template. A minimum of 1 keyword and a maximum of 3 keywords are required. Click to delete or add the keywords.

     Only **Visitor Appointment** and **Review Search** supports configuring the keywords.
  4. Configure the template content, supporting the inclusion of platform-defined terms or links.
- Meta template: Only supports the templates for approve and review failure. The main content displays only text information; detailed information needs to be checked on the Meta official website. Click **Add Meta Template** to add a Meta template, and the platform will retrieve and display the Meta template's name and quotations, allowing users to correspond with the platform's quotations by selection.

Step 4 Select whether enable the template.

If not enable immediately, the corresponding template can still be enabled later from the template list page.

Multiple templates can be created for each purpose, and can be enabled at the same time. The system prioritizes sending Meta templates.

Step 5 Click **OK**.

Related Operations

- Click **QR Code** to open the QR code of the WhatsApp account. Users scan the QR code to follow the business account.
- The platform has configured default test message templates and query failure message templates. Users can modify the content but cannot delete these templates.

5.6.6 Configuring Visitor Access Permission and Visitor Pass

Configure visitor access control, lift control, and entrance and exit. You can also customize visitor pass remarks.

Procedure

Step 1

Step 2 Click **Visitor Access Permission** , and then click **Add** to start adding the permission group.

1. Set a name for the group.
2. Set the access permission group for visitors, including access control and entrance and exit.

   Access permission control has the following 3 security levels.

   - Low security level: After enabling the automatic visit access point from **Visitor** > **Visitor Registration** > **Arrival and Registration**, and selecting the channel, if the corresponding channels are also selected when adding the visitor access permission group, the visitor can be automatically authorized to enter when the visitor visits.
   - Medium security level: Automatic visit and permission group are not enabled, and only automatic leave is enabled. When the visitor visits, manual registration and authorization are required, but authorization and registration are not required when leaving.
   - High security level: Automatic visit and leave are disabled, and default permission group is not configured. Registration and authorization are required for both visit and leave.

   After sending visitor access permissions to the devices, you can check the status of the status in the visitor access permission list. If it is failed, supports resending the configuration.
3. Select the roles to allow access. Only users corresponding to the selected roles can view this access permission group.
4. Click **Save**.

Step 3 Click **Visitor Pass** , customize the content, and then click **Save**. The content will be displayed in the remarks of the visitor pass.

5.6.7 Configuring Email Template

Except the platform appointments, other appointment methods support the use of custom email templates. The corresponding email templates can be created and modified on the platform, including general templates, create appointment templates, host invitation templates, and platform appointment templates. The email template configuration method is similar; below is an example of configuring the general template for visitor arrivals.

Prerequisites

- The email server has been configured. For the details, see "8.3.6 Configuring Email Server".
- The email address of the visitors and hosts has been set.

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 Select **General** > **Visitor Arrival**.

Step 3 Enable the email template. Once enabled, the system will send emails to visitors or hosts according to the specified email template.

The create appointment templates and the host invitation templates are enabled by default and cannot be turned off.

Step 4 Configure the email subject, such as visiting message.

Step 5 Configure the email content.

The platform has created the key words for the template, such as visitor name, visitor company, ID type, and more.

Step 6 Click **Save**.

5.7 Parking Lot

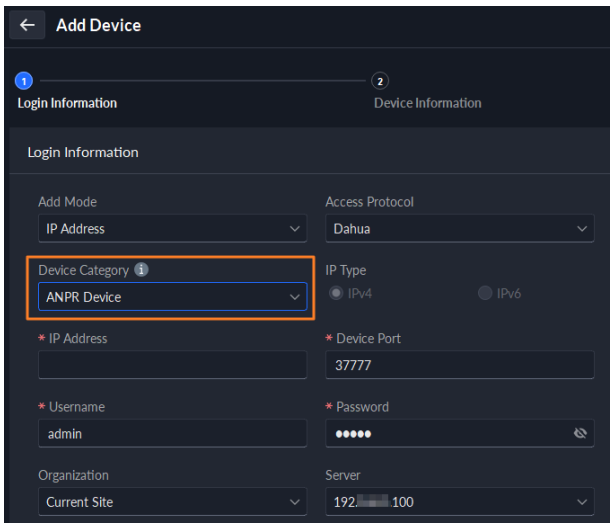
Configure entrance and exit point of the parking lot, barrier opening rules, event parameters, vehicle group, and more to realize barrier opening management, event management, and more.

5.7.1 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. For details, see "4 Basic Configurations".
  - ◇ When adding an ANPR camera, set **Device Category** to **Access ANPR Device**.

Figure 5-32 Set device category



After you have added ANPR cameras, you can bind video channels to their channels. This is available when you have installed other cameras at the entrance to view and record videos of the entire scene, not just the vehicle. You can view the video from the bound camera when checking the alarm details. For how to bind channels, see "4.2.3 Binding Resources".

  - ◇ When adding an NVR, set **Device Category** to **Encoder**.

NVR devices are used for transparent transmission of ANPR camera events, as well as for storing images and videos.

  - ◇ Select **Entrance ANPR** from **Features** for the corresponding NVR channels.
  - ◇ When adding VTO or access control device, set **Device Category** to **Video Intercom** or **Access Control**.

    - ○ You need to add the information of people, set the room (required when VTO is used), 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 configurations of building and unit on the DSS client are the same as the device. If building and unit are enabled on the platform, they must also be enabled on the device, and vice versa. Otherwise, the VTO will be offline after being added.
- Snapshots taken by ANPR cameras are stored in the **Images and Files** disk. 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".

- If it is necessary to enable access recognition for people through the VTO, then you need to add and authorize people, and enable opening barrier by two-factor verification. For details, see "5.3 Personnel and Vehicle Management" and "5.7.2.1 Adding a Parking Lot".

5.7.2 Configuring Parking Lot

A parking lot includes parking spaces, entrances and exits, barrier control rules and other information. Link an ANPR camera for recognizing license plates, and a VTO for abnormal situation call.

5.7.2.1 Adding a Parking Lot

5.7.2.1.1 Configuring 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 Add parking lot organizations.

1. Click , and then configure the organization name, parent organization and roles allowed to access.
2. Click **OK**.

Step 3 Select a parking lot organization, and then click to add a parking lot.

Up to 8 main parking lots can be added. Every main parking lot can add up to 16 sub parking lots.

Step 4 Configure the basic information of the parking lot.

Table 5-30 Parameter description

Parameter	Description
Parking Lot Name	To differentiate from other parking lots.
Parking Lot Organization	Select the organization to which the parking lot belongs.
Parking Lot Mode	**Entrance and Exit Mode** : The parking lot has access management.
Enable Parking Space Counting	Configure the total parking spaces and available ones. • 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
Reset Available Parking Space	In the entrance and exit mode, enable **Enable Parking Space Counting** before configuring **Reset Available Parking Space**. ● For reset type, you can select **Reset to Total Parking Space** , **Auto Calculate Available Parking Spaces Based on Vehicles in Parking Lot** and **Reset to Specified Available Parking Spaces**. ◇ **Reset to Total Parking Space** : You can enable or disable the function of clearing vehicles in parking lot automatically. After the function is enabled, the platform automatically clears the vehicles in the parking lot at the specified time and reset the available parking spaces to the total parking spaces. After the function is disabled, the platform automatically reset the available parking spaces to the total parking spaces. ◇ **Auto Calculate Available Parking Spaces Based on Vehicles in Parking Lot** : The available parking spaces will be automatically calculated based on the currently present vehicles. ◇ **Reset to Specified Available Parking Spaces** : you can configure the available spaces and the vehicles in the parking lot will not be cleared. ● Reset time: The default reset time is at midnight each day. You can customize the reset time.
Fuzzy Match of Entrance & Exit Plate No. Snapshot	● First Character Rule ◇ 1 character added to the front of the plate number: It will still be considered as a match when an additional character is added to the plate number. For example, AB12345 is recognized as AAB12345. ◇ Missing the first character of the plate number: It will still be considered as a match when the first character is missing from the plate number. For example, AB12345 is recognized as B12345. ● Last Character Rule ◇ 1 character added to the end of the plate number: It will still be considered as a match when an additional character is added to the end of the plate number. For example, AB12345 is recognized as AB123455. ◇ Missing the last character of the plate number: It will still be considered as a match when the last character is missing from the plate number. For example, AB12345 is recognized as AB1234. ● Misread Character Rule: It will still be considered as a match if a character is recognized incorrectly, but the number of characters is correct. For example, AB12345 is recognized as AB12B45.  When you enable multiple rules, the platform will check if each rule is satisfied. Only when one or more rules are satisfied will platform consider it to be a match. For example, 1 character added to the front of the plate number, and missing the first character of the plate number are both enabled. When the plate number AB12345 is recognized as AAB12345, it satisfied 1 character added to the front of the plate number, but not missing the first character of the plate number. This will be considered as a match. If the plate number AB12345 is recognized as AB112345, it does not satisfy both rules. This will not be considered as a match.

Parameter	Description
Auto overwrite when captured vehicle has not exited	If a vehicle entered the parking lot but has not exited, a new entry record will be generated when the vehicle is recognized to have entered again. The original entry recorded will be changed to a forced exit record. After enabled, when there are 0 available parking spaces in the parking lot for authorized vehicles on site, 0 remaining parking spaces for personnel, and 0 remaining parking spaces for vehicle groups, access is still permitted.
Filter Invalid Access Records	Click to enable the function, and then set the time range. Vehicles with multiple access records within the set period, only after their first access record will be retained. All the others will be filtered out.

Step 5 Click **Next Step**.

5.7.2.1.2 Configuring Entrance and Exit Points

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

Procedure

Step 1 Click **Add Entrance and Exit Point**.

Step 2 Enter a name (for example, south gate), and then click **OK**.

Step 3 Select a mode for the entrance point.

- **With Barrier** : It is generally used for managing closed parking lots, and the platform can configure entry and exit rules to determine whether vehicles need to automatically open the barrier based on these rules.
- **Without Barrier** : It is generally used for managing open parking lots, such as gas stations, service areas, and similar scenarios, where it only records vehicle passage.

  When EVS or IVSS transparently transmits the images or videos of the events, we recommend selecting the **Without Barrier** mode.

Step 4 If there is an entrance point, click in the **Entrance** section.

Step 5 Enter a name for the point, select a capture mode, and then add a camera, access control or video intercom device (optional).

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

In **Dual Camera** mode, the vehicles captured by the 2 cameras within the defined **Dual Camera Coordinative Time** will be considered as the same one. You must configure the time properly according to the installation positions of the cameras and the distance between them.

The 2 cameras must be added to the same server.

Step 6 If there is an exit point, click in the **Exit** section, and then configure the parameters.

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

When both the entrance and exit are in **Without Barrier** mode, the same camera can be selected for the entrance and exit at the same location.

Step 7 Click **Next Step**.

5.7.2.1.3 Configuring Passing Rules

Procedure

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

Table 5-31 Parameter description

Parameter	Description
Registered Vehicles	**Allow Passage When Available Space is 0** : After being enabled, vehicles are allowed to enter the parking lot even if there are no available parking spaces. Click to enable this function for an entrance point. This function is available only when parking space counting is enabled and the parking space counting mode is **Count parking spaces by entering and exiting vehicles** for the parking lot.
All Vehicles	All vehicles can enter the parking lot. • **Allow Passage When Available Space is 0** : After being enabled, vehicles are allowed to enter the parking lot even if there are no available parking spaces. • **Allow Unlicensed Vehicles to Enter** : Vehicles with no license plates can also enter the parking lot. • **Allow Vehicles on the Blocklist to Enter** : Vehicles on the blocklist are also allowed to enter the parking lot.

Parameter	Description
Custom	You can customize the passing rule for the entrance. A more flexible direction rule configuration allows users to set passing rules based on their specific needs for certain special scenarios. • **Registered Vehicles Access Rule** Click **Add** , and then select **By Parking Lot** or **By Point**. By parking lot: The vehicle groups will be added to all entrance and exit points of the parking lot, and the vehicles in these group can enter and exit through any entrance or exit. By point: You can add different vehicle groups to different entrance or exit points. For example, vehicle group is added to the east entrance but not the south entrance, then the vehicles in the group can only enter the parking lot through the east entrance. • Click  to enable **Allow Passage When Available Space is 0**, and then the vehicle groups will be synchronized. When the available space is 0, the vehicles in these added groups can enter and exit the parking lot. • **All Vehicles** : Select a default time template or create a new one, and then any vehicle can enter the parking lot within the specified duration. For how to create a new time template, see "4.2.7 Adding Time Template". • **Open Barrier by Verification** : Configure rules, the access permission of a vehicle must be verified, and then an administrator can manually open the barrier for it. ◇ **None** : No additional verification is required; barrier opens directly according to the configured passing rules. ◇ **Open Barrier by Manual Verification** : The vehicles with access permissions will not be released automatically, and they can be released manually only after manual verification. ◇ **Open Barrier Directly by Verification** : The barrier opens automatically after the vehicle has been successfully verified through card or face. ◇ **Open Barrier by Two-Factor Verification** : Configure vehicle owner or vehicle color verification. ○ **Verification by Vehicle Owner** : The barrier opens automatically after a vehicle has been successfully verified through the license plate and a verification method such as card or face. ○ **Verification by Vehicle Color** : The barrier opens automatically after a vehicle has been successfully verified through its license plate and the color of the vehicle. You can enable **Automatically opens the barrier even if the vehicle color fails to be verified**, and then the barrier opens when the vehicle color fails to be verified.

Parameter	Description
	• **Available Parking Space Counting** ◇ **Count each vehicle as an occupied parking space** : The number of parking spaces decreases after a vehicle enters. ◇ **Count each unregistered vehicle as an occupied parking space** : The number of parking spaces decreases only after vehicles that are not added to the vehicles groups of the current parking lot enter. ◇ **Custom** : Configure the vehicle groups that do not need to calculate available parking spaces, while all other vehicles need to calculate available parking spaces.

For how to configure vehicle groups, see "5.7.3 Vehicle Group Management".

Step 2 Select a vehicle exit rule, and then configure the parameters.

The exit rule supports enabling **Overtime Vehicle Access**. After it is enabled, vehicles parking overtime are allowed to exit the parking lot.

Other parameters are similar to the ones in the entrance. See the previous step.

Step 3 Enable **Send Plate No. to Devices**, and then add vehicle groups to the allowlist and blocklist.

Devices can use this information to determine which vehicles to let in when the platform is offline.

Step 4 Click **Save and Exit**.

5.7.2.2 Quick Configuration of Release Rules

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 of the corresponding parking lot, and then you can edit the release rules.

For details, see "5.7.2.1.3 Configuring Passing Rules".

5.7.2.3 Parking Lot Event

5.7.2.3.1 Event Parameter

For certain parking lot events, such as parking over time, it is necessary to initialize and configure the corresponding event parameters in order to perform anomaly detection.

Procedure

Step 1 Configure an event, and you need to select **Parking Lot** as the type of event source. For how to configure an event, see "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, 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 5-32 Parameter description

Parameter	Description
Overtime Parking in Parking Lot	• **Overtime Parking Rule** : Select the overtime parking rule from the drop-down list, and then overtime parking detection will be performed according to the rule. For the detailed information of overtime parking rule, see "5.7.2.3.2 Overtime Parking Rule". • **Detection Interval** : How long the platform will check which vehicles have parked overtime. For example, select 5 minutes, then the platform will check whether there are vehicles that have parked overtime in the parking lot. If yes, then an alarm will be triggered. • **Vehicles to Trigger Alarms** : ◇ **All Vehicles** : All vehicles will trigger alarms if they park overtime, but VIP vehicles are not included. If you enable **Include VIP Vehicles**, VIP vehicles will also trigger alarms when they park overtime. ◇ **Non-registered Vehicle and Vehicle in the Blocklist** : The vehicles whose information is not registered to the platform will trigger alarms when they park overtime. ◇ **Custom** : Enable **Non-registered Vehicle**, and then the vehicles whose information is not registered to the platform will trigger alarms when they park overtime; enable **Registered Vehicle** and add vehicle groups, and then the vehicles in these groups will trigger alarms when they park overtime. You can enable **Non-registered Vehicle** and **Registered Vehicle** at the same time.
No Entry and Exit Record	• **No Entrance/Exit Record Duration** : The unit is day. When there are entrance/exit records and no new entrance/exit records exist within the duration after the last record, it is determined that there are no entrance/exit records. • **Statistical Time Point** : The platform will start calculating the duration of a vehicle that has not entered or exited the parking lot on the defined time. • **Entrance and Exit Vehicle Group of Interest** : Only calculate the duration for the vehicles in the vehicle groups that are added.

5.7.2.3.2 Overtime Parking Rule

The overtime rules can be configured across days, or to have different overtime durations for various time periods each day, while no overtime detection is performed during other times. You can configure up to 6 overtime parking rules for each day.

Procedure

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

Step 2 Click +, and then configure the parameters.

Select **Copy From** , and then copy the general, working day, or weekend overtime rule from the drop-down list to save your configuration time. It is suitable for scenarios where rules are configured **By Week**.

Figure 5-33 Add rules

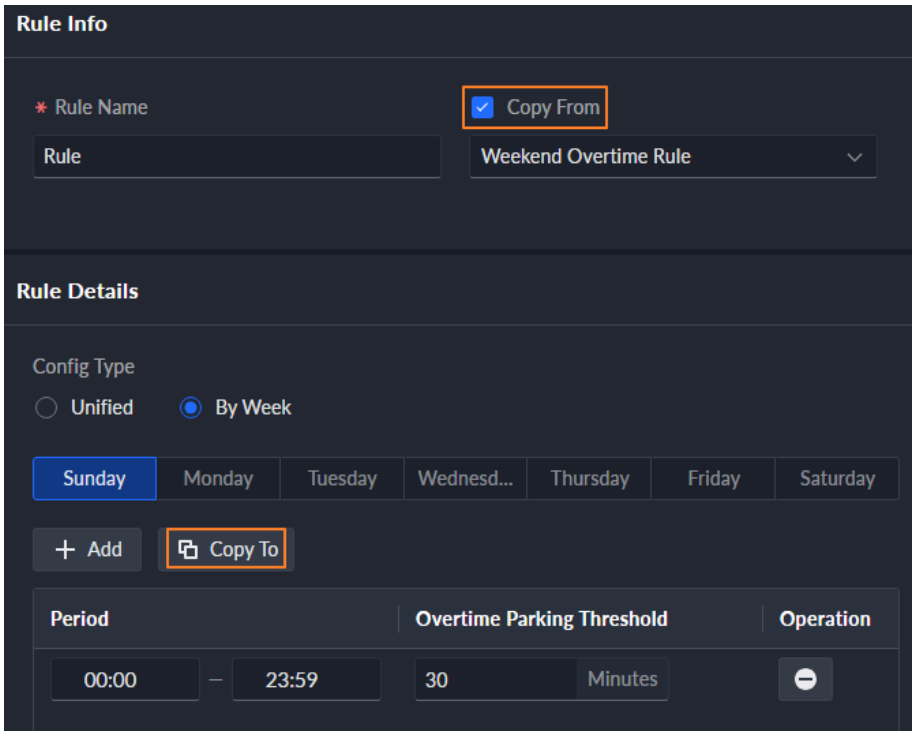


Table 5-33 Parameter description

Parameter	Description
Rule Name	Configure the rule name to differentiate it from others.
Copy From	Select the check box, and then select a rule from the drop-down list to reuse the existing rules.
Rule Details	• Unified: Set the overtime parking threshold by minute, hour, or day, ranging from 10 minutes to 180 days. • By week: Click **Add** to add overtime parking period and set over time parking threshold. Click **Copy To** to copy the configured rules to other days.

Step 3 Click **OK**.

5.7.3 Vehicle Group Management

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.

5.7.3.1 Managing Vehicle Groups

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Parking Lot** > **Vehicle Management** > **Vehicle Group**.

Step 2 Click .

Step 3 Enter a name, select a color for the group, and then select the parking lot that the vehicle group belongs to.

Step 4 Click of a group, and click **Select from Vehicle List** , select the vehicles that you want to add to the group, and then click **OK**.

Select **Vehicle List** , configure the search conditions and then the results will be displayed on the right. Click **Select from Vehicle List** to add vehicles.

5.7.3.2 Configuring Available Parking Spaces

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Parking Lot** > **Vehicle Management**.

Step 2 Select a parking lot, and then available parking space to display available parking space information.

- **Available Parking Spaces for Person** : Display available parking space information for person.
- **Available Parking Spaces for Vehicle Group** : Display available parking space information for vehicle.

Step 3 Click **Add**, and then configure the parameters of the available parking space.

Step 4 Click **OK**.

5.7.4 Configuring Scheduled Report

Procedure

Step 1 Log in to the client. On the **Home** page, click , and then in the **APP Config** section, select **Parking Lot** > **Scheduled Report Config**.

Step 2 Click .

Step 3 Configure the parameters of the basic information and email information.

Figure 5-34 Configure the information

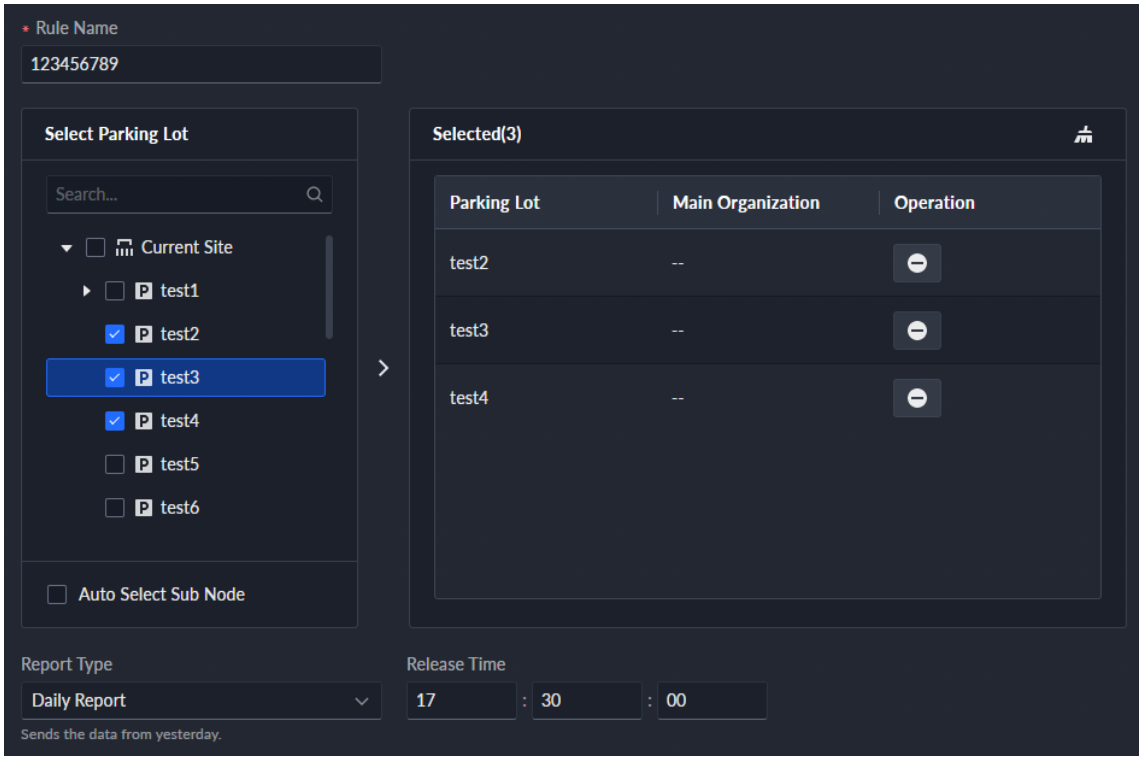
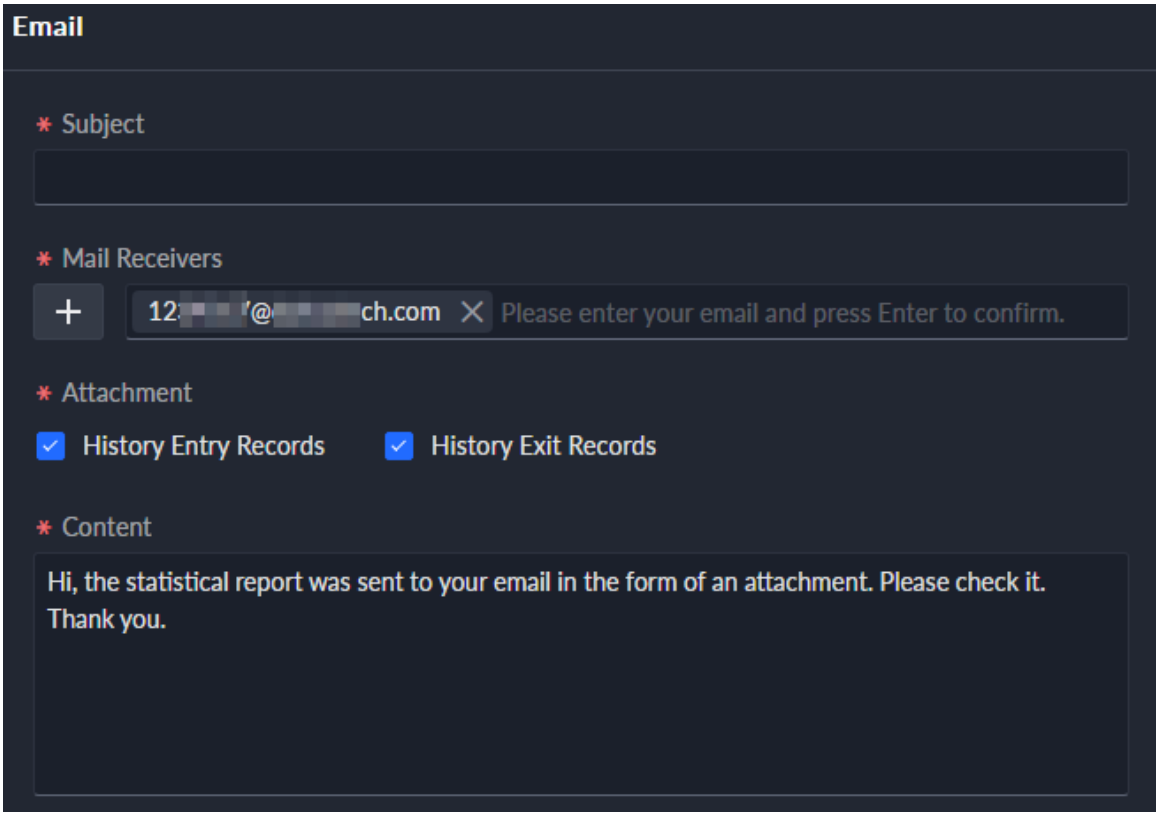


Figure 5-35 Configure email



Step 4 Click **OK**.

The added emails will be displayed in the list. Select the email to view the detailed information.

Related Operations

The added emails are enabled by default, you can click to disable it.

5.8 Intelligence 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.

5.8.1 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 **Intelligence Analysis** > **People Counting Group Config**.

Step 2 Click at the upper-left corner.

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

Figure 5-36 Add a people counting group

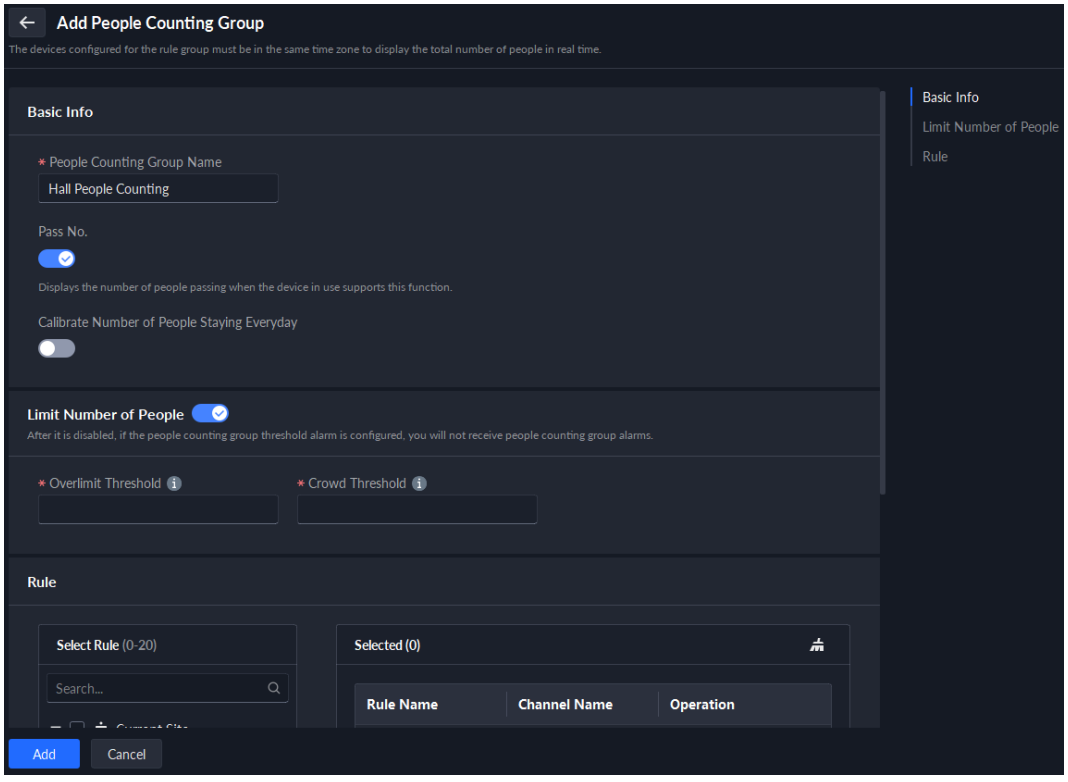


Table 5-34 Parameter description

Parameter	Description
People Counting Group Name	Name of the people counting group.
Pass No.	The calibration time can only be configured on the hour. It is the start of a counting cycle. ● After **Pass No.** is enabled, the number of people pass by will be displayed. The value will be set to 0 every day on the calibration time by default. ● The number of people entered but did not exit will be set to the defined value every day on the calibration time.
Calibrate Number of People Staying Everyday	
Calibration Time	
Calibrated Number of People	
Limit Number of People	When enabled, you can configure the crowd and overlimit thresholds of the people in the group. If an alarm is configured at the same time, alarms will be triggered when the number of people reach the thresholds. For details, see "5.1 Configuring Events". ● When the number of people in the group reaches the defined overlimit threshold, the light will turn red. ● When the number of people in the group reaches the defined crowd threshold but smaller than the overlimit threshold, the light will turn yellow.
Overlimit Threshold	
Crowd Threshold	
Rule	Select the devices whose people counting rules you want to include in the group, and then their data will be combined together.

5.8.2 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 **Intelligence 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 5-37 Invalid email address, you must press Enter

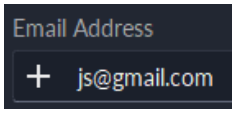
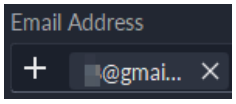


Figure 5-38 Valid email address



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.

5.8.3 Crowd Distribution Group

Add crowd distribution groups, and then you can search for the crowd distribution data by groups from > **Intelligent Analysis**.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Intelligence Analysis** > **Crowd Distribution Group Config**.

Step 2 Click **Add**.

Step 3 Enter a group name, select the rules that will be managed in the group, and then click **Add**.

The rules are obtained from the devices when adding them to the platform, or manually synchronized from devices in **Device Config**.

5.8.4 Vehicle Density Group

Add vehicle density groups, and then you can search for the vehicle density data by groups from > **Intelligent Analysis**.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Intelligence Analysis** > **Vehicle Density Group Config**.

Step 2 Click **Add**.

Step 3 Enter a group name, select the rules that will be managed in the group, and then click **Add**.

The rules are obtained from the devices when adding them to the platform, or manually synchronized from devices in **Device Config**.

5.9 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.

5.9.1 Configuring Alert Rule

Configure alert rules to monitor servers and devices so that you can handle them timely.

Procedure

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

Step 2 Click .

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

Table 5-35 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule. It can be up to 50 characters.
Alert Level	Select a level for the alert. This is used to quickly know the urgency of the alert when it is triggered.
Rule Execution Time	The alert will only be triggered within the defined period.
Monitoring Targets	Targets include servers and devices. You can select different alert sources for each of them.
Rule Conditions	Set the threshold for each condition. When the value is greater than or equal to the threshold, the alert will be triggered.
Push Notifications	After enabled, you can select the users who will receive notifications when the alert is triggered.
Email Notification	After enabled, you can customize the content to be sent to specified email addresses. You can configure the email addresses in the following ways: • Click to select the email addresses of users. • Manually enter an email address, and then press Enter.

5.9.2 Configuring Video Integrity

The platform will continue to check the duration and integrity of the videos. You will be prompted if the one of them is abnormal. For example, 30 days of duration and video integrity have been configured for channel A. If there are only 24 days of video, or the video does not last for 24 hours on any day, the platform will give corresponding prompts.

Prerequisites

Recording plans have been configured for channels and videos have been recorded.

Procedure

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

Step 2 Click .

Step 3 Configure consecutive storage days, and then select the channels for detection.

Step 4 Click **OK**.

Results

Select > **Maintenance Center** > **Resource Monitoring** > **Device Status**, and then click of the device configured with storage detection.

If the duration of video is not enough, the number of days will be displayed in red. If the duration of video for a day is less than 24 hours, the integrity status will be abnormal and displayed in red.

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, video playback, emap, 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

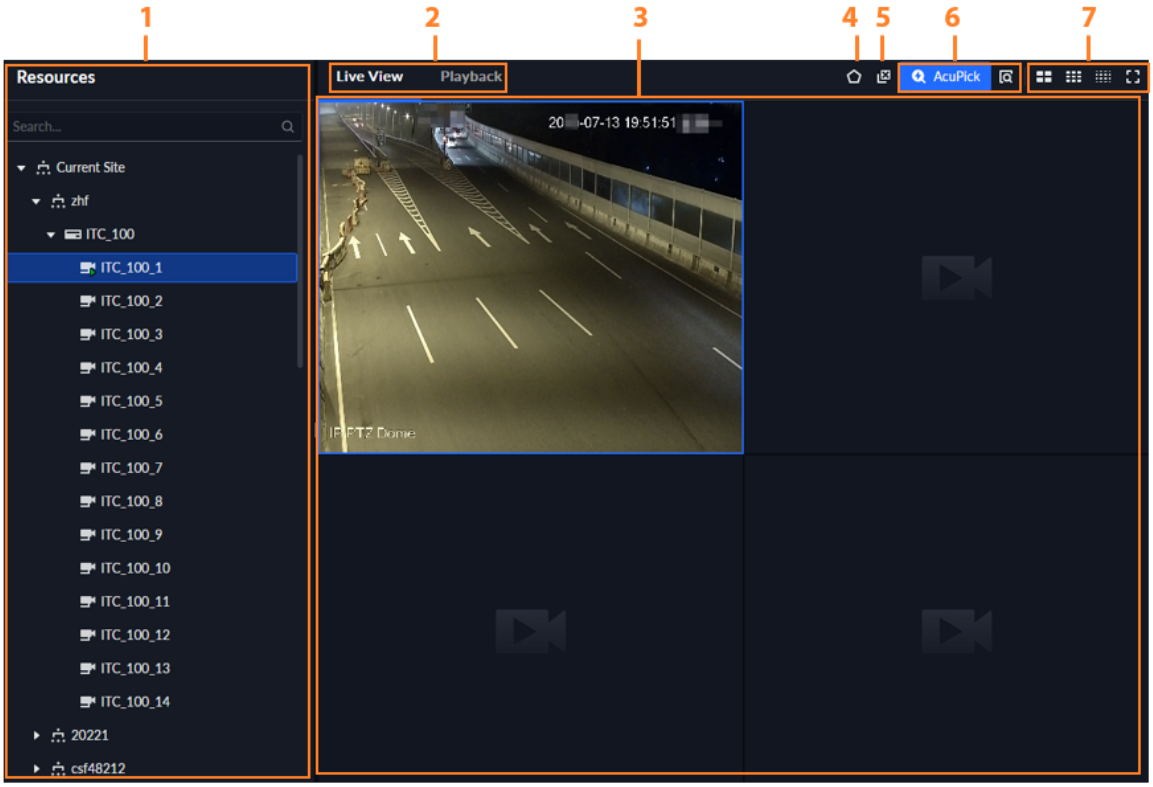


Table 6-1 Monitoring center description

No.	Parameter	Description
1	Resource list	• Double-click the organization, device or channel in the device list, and then the window will display the live video. • 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.
2	Live view and playback	• Live view: View real-time videos. • Playback: View recorded videos. For details, see "6.1.3 Playback".

No.	Parameter	Description
3	Real-time videos	Double-click a channel to the windows and view its real-time video. You can drag between the resource tree and the video window to the left, to hide the resource tree, and then click to show the resource tree.
4	AI rule overlay	• **Default** : Shows AI rules on the video by default. • **Open All** : Shows the AI rules of the channels on the video, and video menus of **AI Overlay** and **SMD Overlay** (by clicking the video, and then selecting > **AI Overlay**) are also displayed. • **Close All** : Hides the AI rules of the channels on the video, and video menus of **AI Overlay** and **SMD Overlay** (by clicking the video, and then selecting > **AI Overlay**) are also hidden.
5	Close all windows	Close all windows in live view.
6	Search for targets in the video	The platform supports manually selecting targets and automatically recognizing targets in the video, and then quickly searching for them in DeepXplore. For details, see Selecting and Searching for Target Manually andAcuPick.
7	Window split mode and full screen	• Set a window split mode. Supports 4, 9, or 16 splits. If the live-view channel number is more than the number of current windows, you need to change the split mode, or close some windows. • 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**.

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.

Background Information

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 the **Live View** tab.

Step 3 View real-time video.

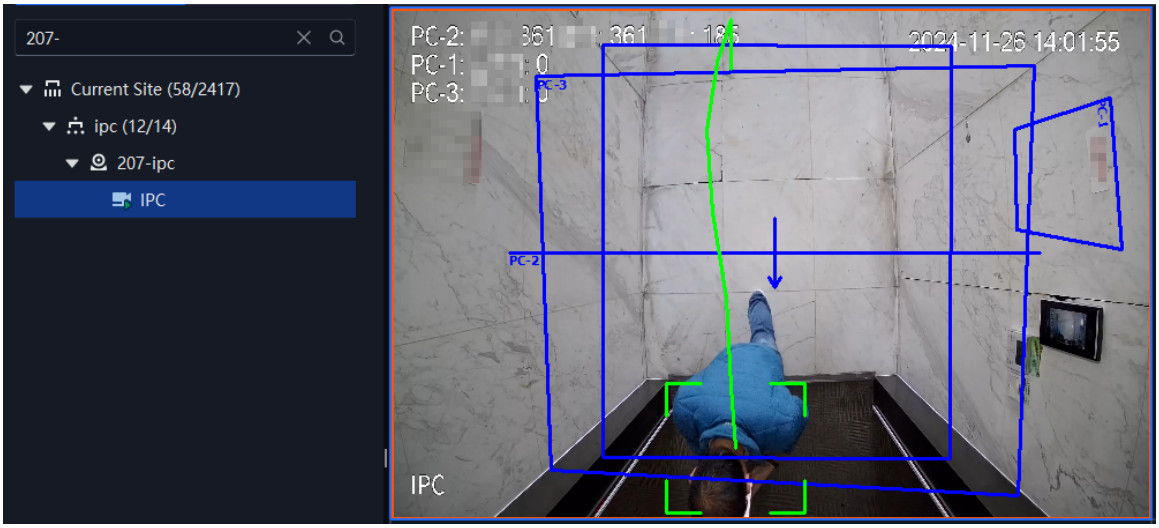
You can view live video in the following ways:

- Double-click a channel to one window on the right.
- Double-click a device to view all channels under the device.

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

- When viewing live video of people counting cameras (make sure that the people counting function is enabled on the camera), click the video image, and then select > **AI Overlay** > **Bounding Box Overlay**, you can view the person tracks on the monitoring image.

Figure 6-2 View person track



- Point to the video window, and then you can see the shortcut menu at the upper right.

Table 6-2 Live window icon description

Icon	Name	Description
	PTZ control	Click the icon, and then you can zoom in and out the PTZ device, lock PTZ, perform 3D positioning, configure presets, tour, pattern, scan, pan, wiper, light, and more. For details, see "6.1.2.3 PTZ". This function is only available for PTZ devices.
	Audio	Turn on/off the audio of the channel. The audio is not enabled by default. To enable the audio function, the **Video Sound** permission is required from > **User** > **Role Management**.

Icon	Name	Description
	Audio communication	Start two-way audio with the device the channel belongs to. This function is only available when logging in to the web client through HTTPS. The audio communication is not enabled by default. To enable this function, you need to add the audio talk permission on the role management page.
	Local record	Click it, and then the system begins to record local file and you can view the record time on the upper left. Click it again, and then system stops recording and saves the file to your computer. The recorded video is saved to the default download path of the browser.
	Snapshot	Take a snapshot. The snapshots are saved to the default download path of the browser.
	Close	Close the video.

- Click the video image, and then select . You can perform the following operations.

  The menu varies depending on the functions supported by the device you are operating on.

Table 6-3 Right-click menu description

Parameter	Description
Select Audio Input	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Start Remote Recording	Record the audio and video in the current window. ◇ If a channel already has a center recording plan, you cannot start remote recording. ◇ If a video storage disk is configured on the platform, the videos will be saved to the platform server.
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.

Parameter	Description
Play Mode	When playing videos, both fluency and real-time performance matter. To deal with network fluctuations, the platform has a set of buffer control strategies to ensure fluency and real-time performance. You can select one of the following play modes as needed. ◇ **Real-time Play Priority** : The system might lower the image quality to avoid video lag. It is suitable for special scenarios with high requirements on real-time performance. ◇ **Fluency Priority** : The system might lower the image quality and allow for lag to ensure video fluency. The higher the image quality, the lower the video fluency will be. ◇ **Balance Priority** (recommended): The system balances real-time priority and fluency priority according to the actual network performance.
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.
AI Overlay	Select **AI Overlay**, and then you can select: ◇ **Start Image Overlay** : Overlay the snapshot information of people and vehicle metadata over the upper right of the video image, click it again to stop image overlay. Make sure that: ○ The device supports people and vehicle metadata snapshot. ○ **Image Overlay** is enabled from **Local Settings** > **Video**. ◇ **Rule Overlay** , **Area Overlay**, **Bounding Box Overlay**, and **SMD Bounding Box Overlay**: Displays rule lines, detection area for intelligent rules, bounding box on targets, and motion detection bounding box on targets. After enabled, the configurations will be saved, and only works on the current channel in the live view and playback. Make sure that **AI Rule Overlay** is enabled from **Local Settings** > **Video**.
Alarm Output Control	Turn on or turn off alarm output channels.
Audio and Light Control	You can turn on or off the audio and light channels one by one or at the same time. This function is available on select device only.
Device Intercom	For channels added through NVR, XVR/DVR, IVSS or EVS, you can select this option to talk to the NVR, XVR/DVR, IVSS or EVS.

Parameter	Description
Time Sync	Synchronize device time with server time. This function requires **Device Permissions** and the **Device Time Sync** control permission from > **User** > **Role Management**.

- To view real-time temperature of a point on the thermal camera view, hover over that point.
- Search for targets in the video.

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

Figure 6-3 Select a target



6.1.2.1.1 Selecting and Searching for Target Manually

Manually select a target in the video and quickly search for it in DeepXplore.

Procedure

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

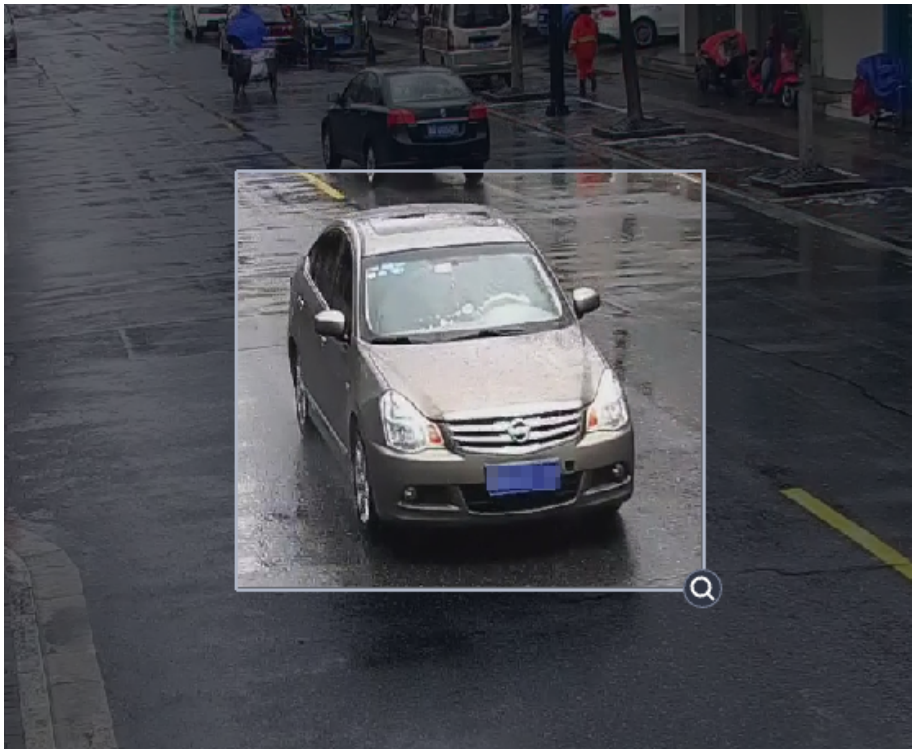
Step 2 Double-click a channel.

Step 3 Click on the upper-right corner.

Step 4 Drag on the video to select a target.

Right-click to exit this function.

Figure 6-4 Select a target



Step 5 (Optional) Adjust the area of selection.

- Move the selection box: Place the mouse cursor over the selected area, click the left button, and the drag the mouse.
- Resize the selection box: Place the mouse cursor over the top-left, bottom-left, or top-right corner of the selected area. Click the left mouse button and drag it to adjust the size accordingly.

Step 6 Click and select a type for the target, and then you are directed to DeepXplore to search for it. For details, see "6.3 DeepXplore".

6.1.2.1.2 AcuPick

The platform can automatically recognize different types of objects in the video by using the AcuPick object recognition function of devices. You can select a target and then quickly search for it in DeepXplore.

Prerequisites

Make sure that the device to which the channel belongs (for example, NVR, IVSS) supports the AcuPick object recognition function.

Procedure

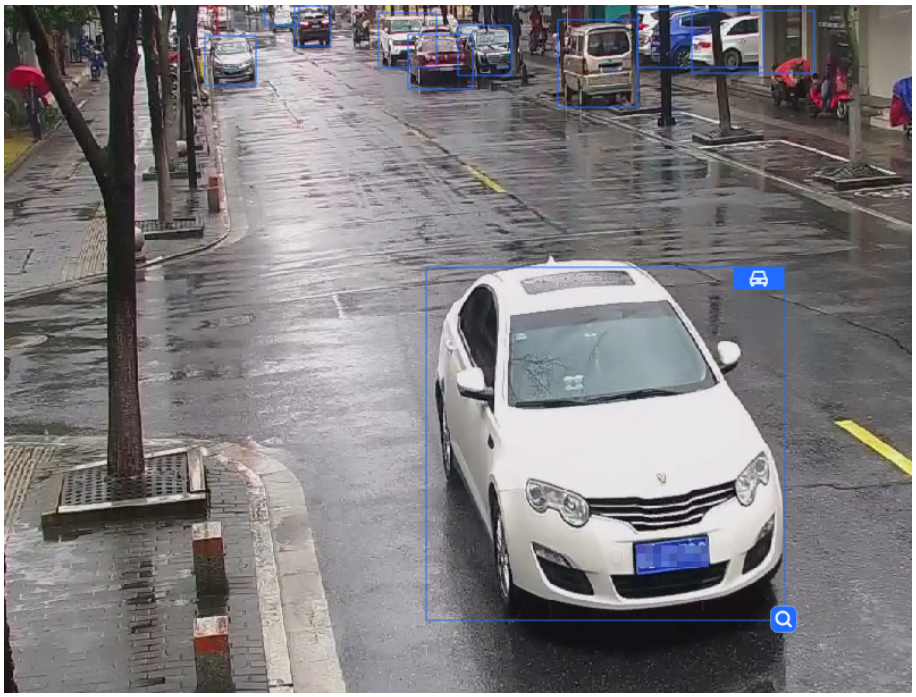
Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center** > **Monitoring**.

Step 2 Double-click a channel.

Step 3 Click AcuPick on the bottom of the page to automatically recognize targets in the video, including faces, human bodies, and vehicles.

Click to exit this function.

Figure 6-5 Automatically recognize targets



Step 4 Hover over the recognized target, and then click of a target to search for it in DeepXplore. For details, see "6.3 DeepXplore".

If certain targets are not recognized, you can click to manually select one. For details, see "6.1.2.1.1 Selecting and Searching for Target Manually".

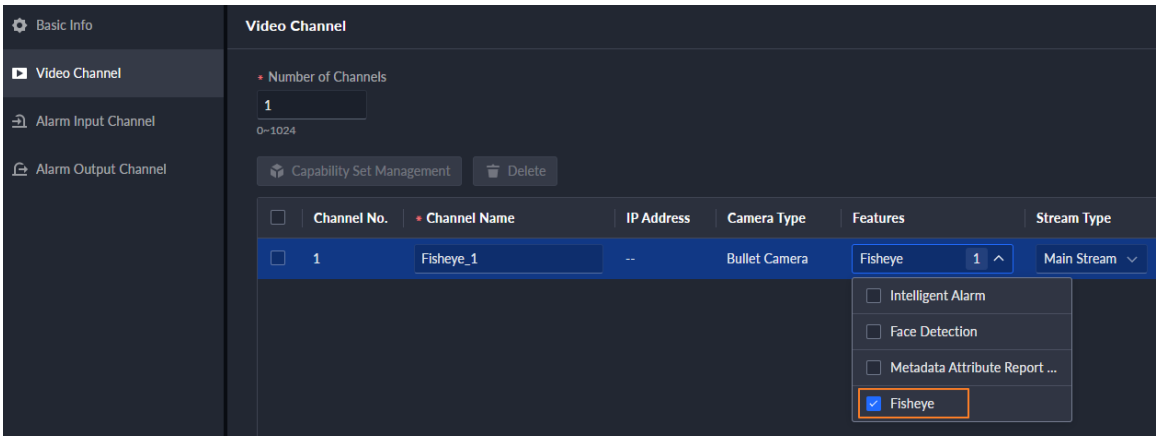
6.1.2.2 Dewarped Live View of Fisheye Camera

Configure center calibration, and then you can view dewarped live view of a fisheye camera on the platform.

Prerequisites

Add the fisheye camera to the platform through ONVIF protocol first, and then set its feature to **Fisheye**.

Figure 6-6 Set features of the fisheye camera



Background Information

Dewarping refers to making the image look closer to the normal effect by eliminating or reducing the distortion at the edge of video image of a fisheye camera.

Procedure

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

Step 2 Double-click or drag the fisheye channel to the window on the right.

Step 3 Point to the top of the video image, and then click to start center calibration.

1. Move or adjust the dotted blue rectangle in the video to calibrate the center of the camera view as desired.

   Operate the calibration with proper scope; otherwise, the calibration will fail.

2. Click **OK**.

Figure 6-7 Center calibration



Step 4 Right-click the live view of the fisheye camera, select **Install Mode** , and then select **Ceiling Mount** or **Ground Mount** from **Installation Mode**.

Step 5 Right-click the live view of the fisheye camera, select **Fisheye View**, and then select the view that you want. means 1 panorama and 1 fisheye view, means 2 small panoramas.

To perform the center calibration again, you need to right-click the live view of the fisheye camera, and then cancel selecting the installation mode.

6.1.2.3 PTZ

Operate PTZ cameras during live view on the DSS Client.

Background Information

If you want to configure PTZ control, you need to add **PTZ Operation and Configuration** permission on role management page. If you want to call the PTZ functions, you need to add **PTZ Operation** permission on the role management page.

6.1.2.3.1 Opening PTZ

Procedure

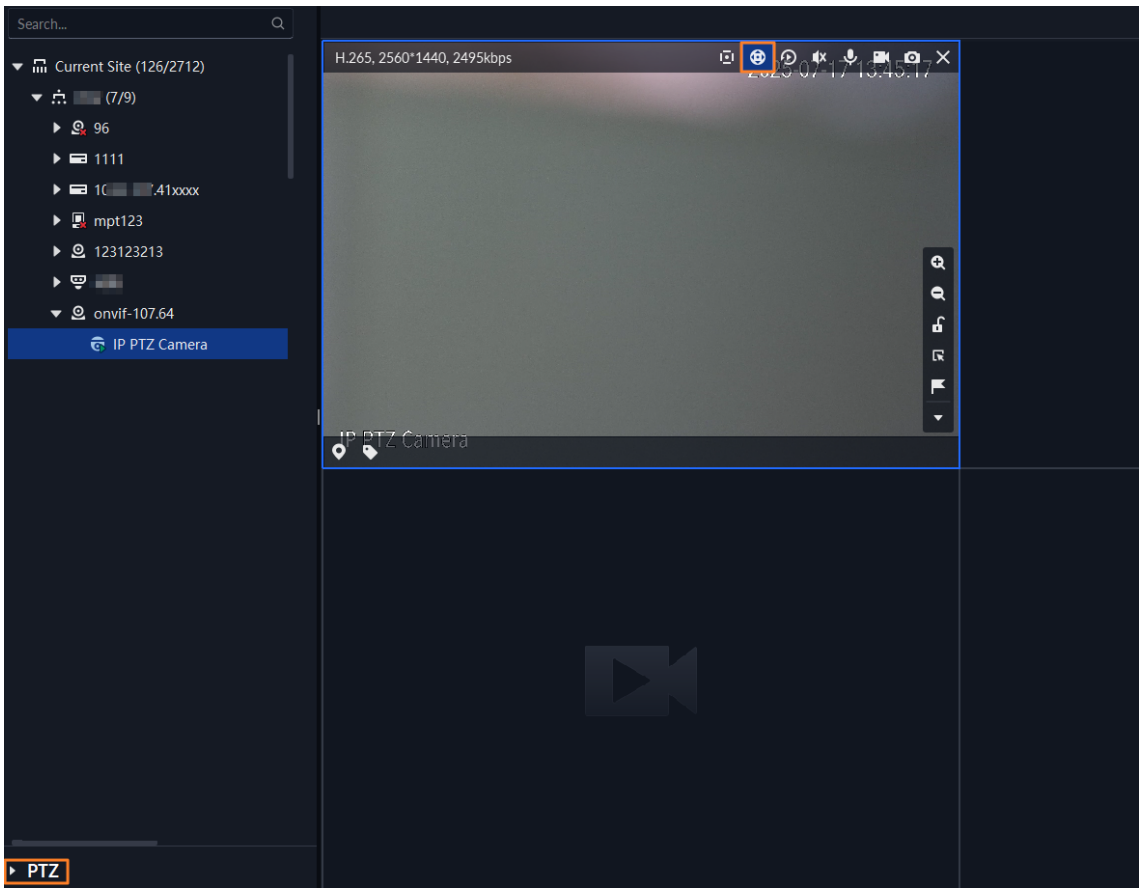
Step 1 Log in to the DSS Client. On the **Home** page, click , and then click **Monitoring Center** > **Monitoring**.

Step 2 Click **Resources**, and then select a channel with PTZ.

Step 3 Click **PTZ** at the lower left to open the PTZ panel, or click in the video image of the PTZ channel, and you will see the PTZ icons.

The following sections use the PTZ panel operations as the example.

Figure 6-8 Open PTZ



6.1.2.3.2 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 **PTZ**.

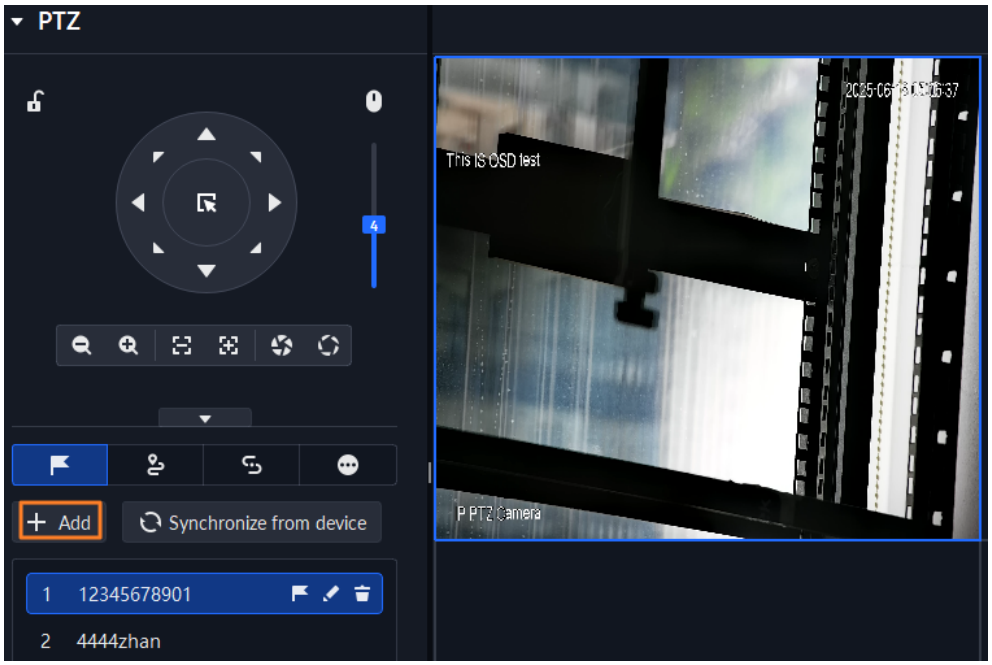
Step 3 Click .

Step 4 Add a preset.

Click **Synchronize from device** to obtain presets configured on the PTZ device.

1. Rotate the PTZ camera to a specific point.
2. Click **Add** , enter the preset name, and then click **OK**.

Figure 6-9 Add a preset



6.1.2.3.3 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.

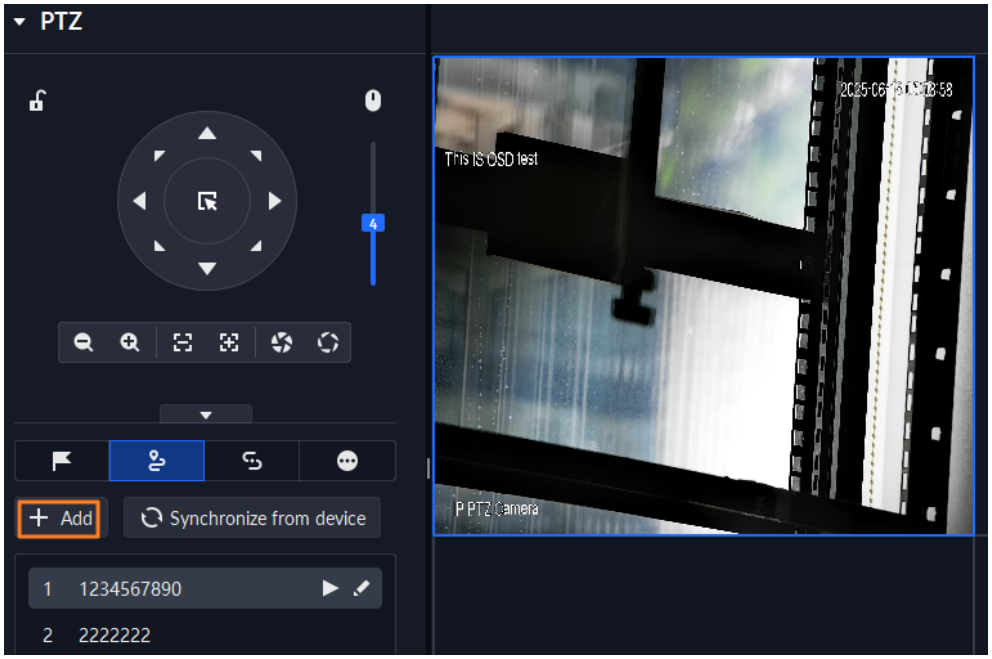
Step 2 Click **PTZ**.

Step 3 Click .

Step 4 Click **Add**.

Click **Synchronize from device** to obtain the tour data configured on the PTZ device.

Figure 6-10 Add tours



Step 5 Add tours.

1. Enter tour name, and then click **Add**.
2. Select a preset from the drop-down list.
3. Repeat the previous 2 steps to add more presets.
4. Click **OK**.

Related Operations

- To start tour, click , and then camera goes back and forth among the presets.
- Edit tour: Click .

6.1.2.3.4 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 **PTZ**.

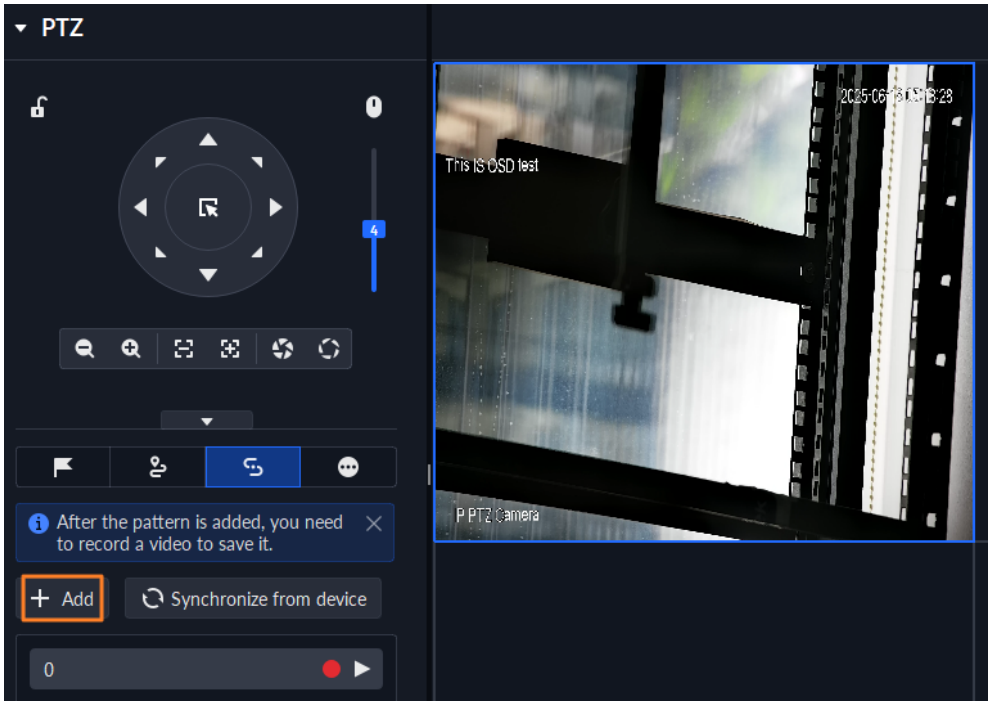
Step 3 Click .

Step 4 Click **Add**.

Step 5 Click , and then operate the 8 PTZ buttons to set pattern.

Click **Synchronize from device** to obtain the patterns configured on the PTZ device.

Figure 6-11 Set pattern



Step 6 Click to stop pattern recording.

Related Operations

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

6.1.2.3.5 Enabling or Disabling Pan

1. On the **Monitoring Center** page, open the video of a PTZ camera.
2. Click **PTZ**, and then click .
3. Click . The PTZ rotates 360° at a specified speed. Click to stop camera rotation.

6.1.2.3.6 Enabling or Disabling Wiper

Enable or disable the PTZ camera wiper. Make sure that the camera supports wiper function.

1. On the **Monitoring Center** page, open the video of a PTZ camera.
2. Click **PTZ**, and then click .
3. Click to turn on the wiper. Click to turn off the wiper.

6.1.2.3.7 Enabling or Disabling Light

Turn on or off the camera light. Make sure that the camera supports light.

1. On the **Monitoring Center** page, open the video of a PTZ camera.
2. Click **PTZ**, and then click .
3. Click to turn on the light. After enabling the light, click to turn off the light.

6.1.2.3.8 Configuring Custom Command

Procedure

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

Step 2 Click **PTZ**, and then click .

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

Step 4 Click to show the command functions.

6.1.2.3.9 PTZ Menu

Procedure

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

Step 2 Click **PTZ**, and then click .

Step 3 Click .

Step 4 Use the panel to go to the menu configuration page.

Figure 6-12 Go to PTZ menu configuration page

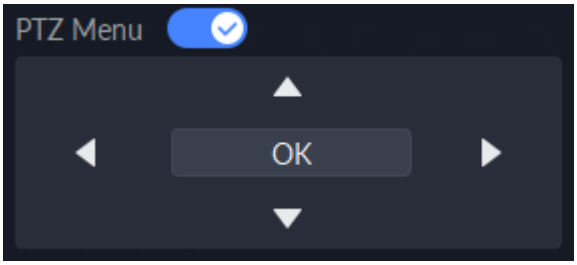


Table 6-4 PTZ menu description

Parameters	Description
/	Up/down.
/	Left/right. Point to set parameters.
	Click to enable PTZ menu function. The system displays main menu on the monitoring window.
	Click to close PTZ menu function.
OK	It is the confirm button. It has the following functions. ● If the main menu has the sub-menu, click **OK** to enter the sub-menu. ● Point to **Back** and then click **OK** to go to go back to the previous menu. ● Point to **Exit** and then click **OK** to exit the menu.
Camera	Point to **Camera** and then click **OK** to go to the 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.

Parameters	Description
System	Point to **System** and then click **OK** to go to system sub-menu page. Set PTZ simulator, restore camera default settings, video camera software version and PTZ version.
Return	Point to the **Return** and then click **OK** to go back to the previous menu.
Exit	Point to the **Exit** and then click **OK** to exit PTZ menu.

6.1.3 Playback

Play back recorded videos.

Background Information

- The playback duration of recorded videos can be controlled through the **Resource Operation** permissions when adding a role. Searching for recordings beyond the specified duration will result in a message indicating insufficient permissions.
- The system automatically plays the recordings after you search recordings, drag the timeline to a specific time to play the recording, and search for recordings of a specific time through the calendar on the **Playback** page.

  You can turn off the **Auto Play Videos** function from **Local Settings** > **Video** > **Video Playback**.

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.

Drag between the resource tree and the video window to the left, to hide the resource tree. Select a window, and then double-click the resource to play the video.

Click to show the resource tree.

Figure 6-13 Playback page

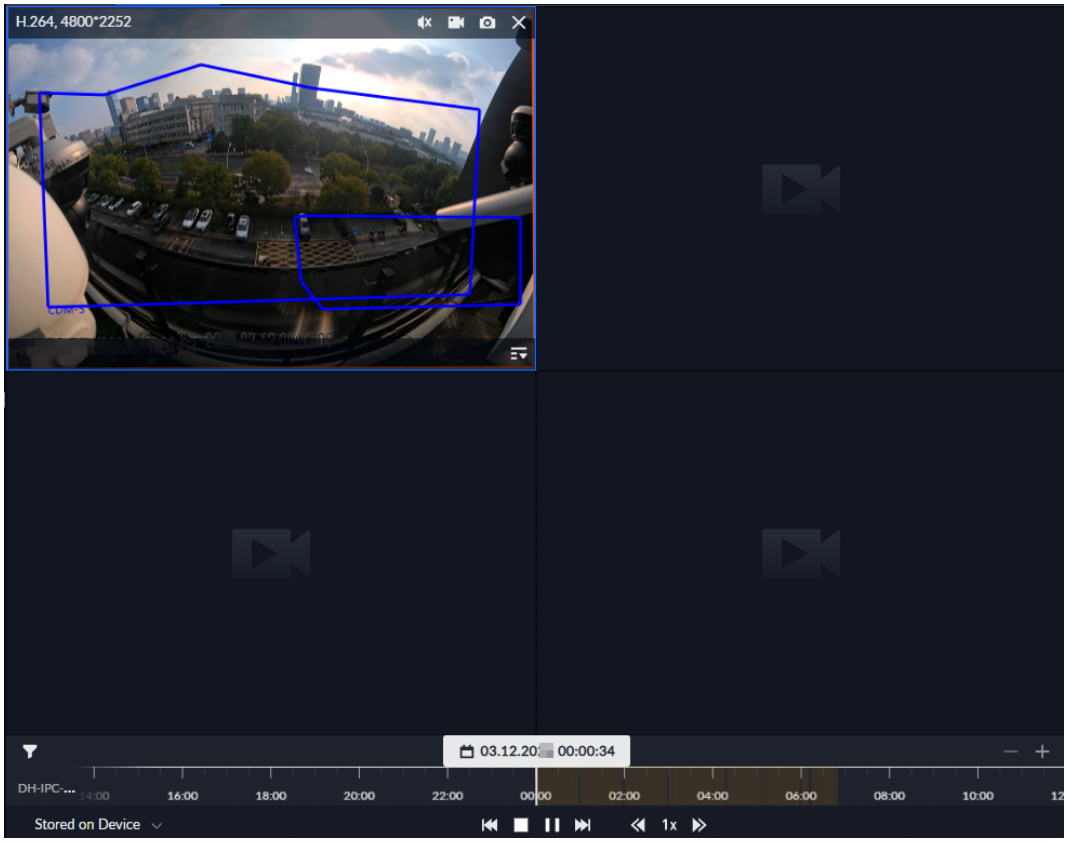
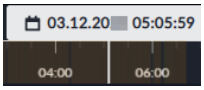
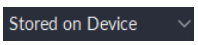


Table 6-5 Function description

Icon	Description
	Filter video recordings according to video type and stream type.
	Timeline. ● Click to select the date to view the video. The time period of the video is displayed on the timeline. ● During playback, you can drag time progress bar to play back video at the specific time.
	Click + or -, or use your mouse wheel to conveniently zoom in and out of the timeline.
	Select the storage location of the video to be searched. Supports searching for the video on the platform server or storage device.
	Play the previous or next video clip of the most recent time. For example, when searching for videos, if you do not remember the exact event time, and there is no video clip at the time that you search, you can try to play the previous or next video of the most recent time, to track the event. This function is not available when is enabled.

Icon	Description
,	Stop or pause the video.
1x	Fast forward or slow down the video to up to8 times. When playing a video backwards or forwards alternately, the play speed will not be changed. When fast forwarding or slowing down the video, you can click to pause playback and adjust the speed. After adjusting, click to play the video at the adjusted speed.

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** > **Monitoring**.

Step 2 Click the **Playback** tab.

Step 3 Double-click to open the video of a channel.

Drag between the resource tree and the video window to the left, to hide the resource tree. Click to show the resource tree.

Step 4 Select the storage path of recorded video from **Stored on Server**, and then click to select the date.

- Dates with blue dots means there are videos.
- After selecting a date, the platform will search for videos on that date from other channels. If you switch to the **Live View** page, or close the page or the PC client, the date will be reset.

Step 5 Click to play the video.

Step 6 Hover over the video, and then the icons appear. You can perform the following actions.

Table 6-6 Function description

Icon	Name	Description
	Visual tracking	Click to turn on visual tracking, and then you can click the shape over the video image to view the video of associated channels, so that you can track the area or location where the target passes through.

Icon	Name	Description
	Audio	Turn on/off the audio of the channel.  The audio is not enabled by default. To enable the audio function, the **Video Sound** permission is required from  > **User** > **Role Management**.
	Take a recording on the device	Click it to start recording. The recorded video is stored locally.
	Take a snapshot on the device	Take a snapshot of the current image and save it locally.
	Close	Close the window.

Click the video image, and select . You can perform the following operations.

Table 6-7 Shortcut menu description

Parameter	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.
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.
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	When enabled, the platform displays rule lines, detection area for intelligent rules, bounding box on targets, and motion detection bounding box on targets if the AI detection rules are enabled on the device. This configuration is effective with the current selected channel both in live video and playback.  Make sure that **AI Rule Overlay** is enabled from **Local Settings** > **Video**.
Disable Privacy Masking	For cameras that support privacy masking for human faces, you can disable the masking here to view the face image.
Time Sync	Synchronize the device time with server time.  This function requires that you gain control permission in **Device Permissions** and the **Device Time Sync**. Go to  > **User** > **Role Management**.

6.1.3.3 Filtering Recording Type and Stream Type

Filter videos 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.

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 device recordings or central recordings, and the search type of device video stream is set to main and sub streams. For details, see "9.1.2 Configuring Video Settings".

6.1.3.4 Searching for Targets

When playing back a video, you can manually select a target, or select one automatically recognized by AcuPick, and then search for it in DeepXplore. For details, see "6.1.2.1.1 Selecting and Searching for Target Manually" and "6.1.2.1.2 AcuPick".

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 6-8 Function description

Function	Description
Zoom in and out on the map	Rotate the wheel or click + and − to zoom in and out on the map. Select **Display Settings** > **Point Clustering**, and then when you zoom out on the map, the same type of devices or channels will be merged together if they are near each other. 
Satellite map	Select **Display Settings** > **Satellite Map**, and then if you are using an online map, you can view its satellite map. This function is only available on GIS maps.
Hide device name	Select **Display Settings** > **Hide Device Name**, and then only displays the icons of devices or channels.
View device details	Click a device on the map, and then click to view device name and organization; click again to hide the name and organization.
View live video	• View live videos in batches: Click **Selected** > **Rectangle**, or click **Selected** > **Polygon**, select devices on the map, and then click . • View the live video of a device: Click a device on the map, and then click . PTZ control and presets are supported when viewing the live video. Make sure that the device supports the PTZ function.
Playback	• View videos in batches: Click **Selected** > **Rectangle**, or click **Selected** > **Polygon**, select devices on the map, select the time and storage type (either device or central recordings can be selected), and then click . • View the video of a device: Click a device on the map, select the time and storage type (either device or central recordings can be selected), and then click . Drag the timeline to quickly locate the recorded video at the corresponding time and play it.
View alarms	Click to view all alarms that are triggered. Click an alarm and the map will zoom in to the location of the device that triggered the alarm. Alarms will be automatically canceled after 30 seconds.

Function	Description
Cancel alarms	Click a device on the map, and then select . The alarm will also be automatically canceled after 30 seconds.
Talk	Click a device on the map, and then click  to start talk. This function is available on select devices.
Show devices	Click **Show Device**, and then select the types of devices and channels that you want to display on the map. You can click an alarm output channel to control whether it will output alarm signals.
Visual range	• For devices that do not support sending the visual range to the platform, after you configure static visual range from  > **Map**, you can view the monitoring area of the device on the map. • If a device supports visual range, click **Dynamic Visual Range**, and then double-click a device on the map to show its monitoring area. ◇ For devices that support dynamic visible range (for example, PTZ camera), if static visible range is configured at the same time, refer to the static visible range. ◇ This function is only available on GIS maps.
Initial angle	If a device supports initial angle, click **Initial Angle** and double-click a device on the map to show the initial angle. This function is only available on GIS maps.
Measure distance	Select **Box** > **Length**, connect 2 points with a line on the map (double-click to finish drawing), and then the distance between the points is shown. This function is only available on GIS maps.
Measure area	Select **Box** > **Area**, select a region on the map (double-click to finish drawing), and then the area is measured. This function is only available on GIS maps.
Clear	Clear all markings on the map.
Add marks	Select **Box** > **Add Mark**, and then mark information on the map.
Reset	Select **Box** > **Reset** to restore the map to its initial position and zoom level.
Sub maps	Click  to view the information of the sub map.

Function	Description
	Double-click , and then the platform will go to the sub map, where you can view the resources on it.

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 Event

View and process real-time alarms.

Background Information

After you log in, the system displays up to 1,000 unprocessed events in the past 7 days by default.

Procedure

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

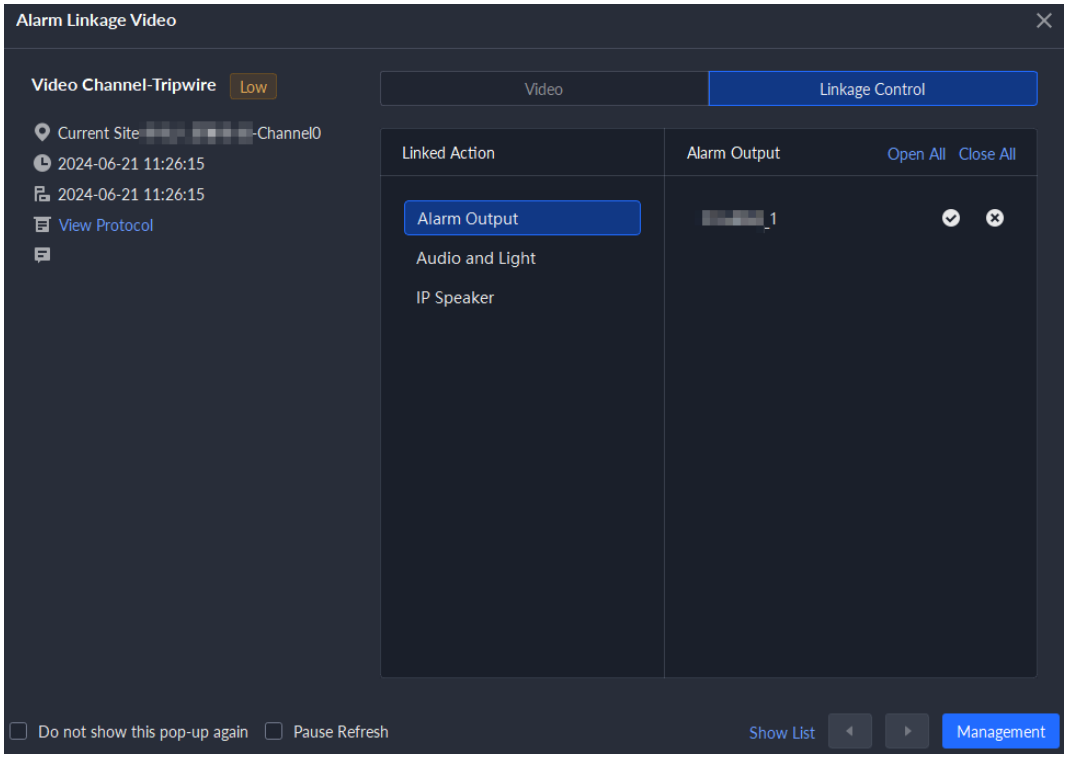
Step 2 Click **Real-time Event**.

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

Alarm pops up when **Open Alarm Linkage Video** is set to **As Pop-up** from **Management** > **Local Settings** > **Alarm**. You can click the **Video**, **Snapshot**, **Linkage Control** or **Map** tab to view the video or snapshot, open or close alarms manually, or view the location of the device on the map.

- The **Map** tab displays after you set **Related Content** to **Link Video and Map** from **Local Settings** > **Alarm**.
- The **Linkage Control** tab supports alarm output, audio and light, and IP speaker.
  - ◇ You can adjust the volume of audio in **Audio and Light**.
  - ◇ For IP speaker, you can start talking or broadcasting, play the specified audio file, and adjust the volume of speaker and microphone.
  - ◇ For alarm output, you can click **Open All** or **Close All** to open or close the alarm.

Figure 6-14 Alarm pop-up



Step 3 Click to claim an alarm.

After an alarm has been claimed, the user name of your account will be displayed under the **Processed by** column.

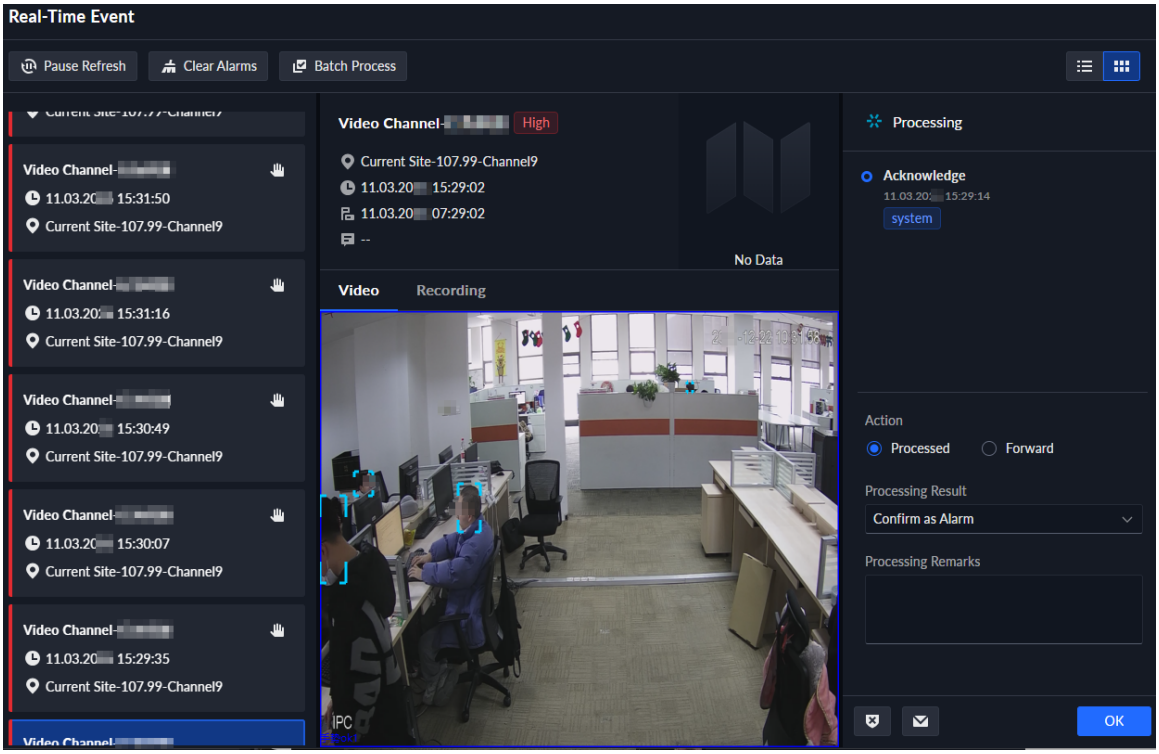
Step 4 Process alarms.

You can use the up and down arrow keys on the keyboard to quickly select other alarms.

1. Click or double-click the alarm to view the alarm details.

   - Alarms related to vehicles also display vehicle information such as plate number, speed, and more.
   - For animal intrusion, animal tripwire, and animal fast moving events, the animal type will be displayed, such as cat, dog, and bird.

Figure 6-15 Alarm details



2. The middle area displays the time when the alarm was triggered, name and location of the alarm source, alarm type, and the live video images of linked channels, alarm videos, and alarm snapshots.

   Double-click a window to view them in larger size. Click to go back.
3. On the right side, select **Processed** , and then enter the comments to handle the alarm by the current user, or select **Forward** to forward the alarm to another user or user group for handling.
4. (Optional) Click to disarm the alarm. You can disarm for a period, or disarm until the defined time.

   If disarming type is set to disable, then all users will not receive this alarm within the defined time. If disarming type is set to ignore, then only the user who claim the alarm will not receive this alarm within the defined time.

   After the defined time, if the alarm is not eliminated, it will continue to alarm.
5. (Optional) Click to send the alarm information to other users as an email. Events that are processed or forwarded can also be sent as emails.

   The emails here are sent by the user through the client, and their language is consistent with the client language.

Related Operations

- The platform also supports processing alarms in batches. Click **Batch Process**, select multiple alarms, and then you can process them in batches.
- When viewing the recorded videos, you can select a target manually or select one automatically recognized by AcuPick, and then search for it in DeepXplore.

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 **Event History**.

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

In the **Processing Remarks** section, you can search for events by entering remarks that are defined when processing or forwarding the event.

Step 4 Claim and process alarms. For details, see "6.2.1 Real-Time Event".

You can use the up and down arrow keys on the keyboard to quickly select other alarms.

Step 5 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. This function is only available for super administrator and administrator.
- **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

When viewing the recorded videos and snapshots, you can select a target manually or select one automatically recognized by AcuPick, and then search for it in DeepXplore.

6.2.3 Event Statistics

With alarms being triggered and processed, statistics are generated to give you a clear picture of what is happening in your area, such as the number of alarms that were processed, and the type of alarms that are triggered most frequently.

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

Figure 6-16 Alarm overview

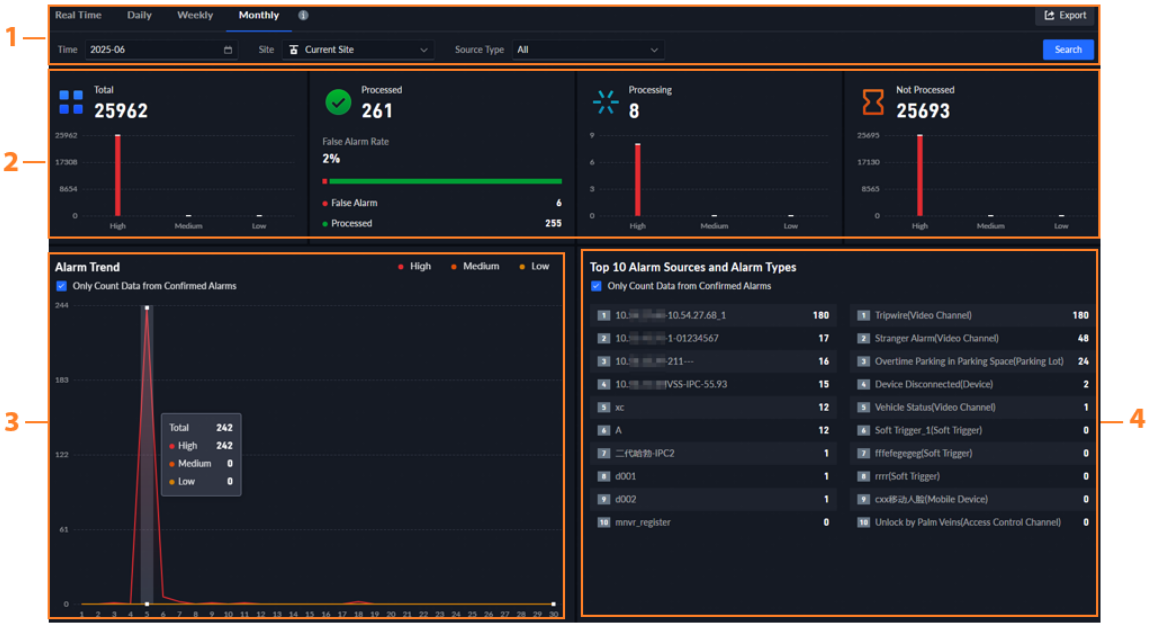


Table 6-9 Alarm overview description

No.	Parameter	Description
1	Search conditions and export records	• To view real-time alarm overview, click **Real Time**, select a site (if any), an organization, and refresh frequency. • To view daily alarm overview, click **Daily** , configure the time, select a site, an organization, and then click **Search**. • To view weekly alarm overview, click **Weekly** , configure the time, select a site, an organization, and then click **Search**. • To view monthly alarm overview, click **Monthly** , configure the time, select a site, an organization, and then click **Search**. If the time zone of the server is not the same as the DSS client, statistics will be generated based on the time zone of the server. For example, daily statistics will be generated from 00:00 to 24:00 based on the time zone of the server. • Export: Export the page of the current search results to local.
2	Alarm Overview	Statistics is generated based on the alarms that the current user has access to. The number and proportion of alarm events that are pending, processed, or not processed are displayed. The data will only refresh in real-time when you are viewing daily statistics.
3	Alarm Trend	Displays trend of alarms of all priorities.

No.	Parameter	Description
4	Top 10 Alarm Sources and Alarm Types	Top 10 alarm sources and alarm types that the current user has access to are sorted by the number of alarms. The data will only refresh in real-time when you are viewing daily statistics. You can click high, medium, or low to not include the number of certain alarms. For example, if you click **High**, the number of the alarms in this priority will not be counted.

6.2.4 Alarm Controller

You can monitor and manage alarm controllers.

Prerequisites

Alarm controllers are added to the platform. For details, see "4.2.2 Managing Devices".

Background Information

- Arm and disarm
  - Home arm: An arming mode when a user is within the zone of the alarm system. In this mode, zones around the system, such as outdoor perimeter detectors, balcony curtain detectors, are armed, while zones inside the system, typically indoor infrared detectors, are bypassed by the system. People can move in this area without triggering alarms. If there are internal zones within a subsystem, they will be disarmed.
  - Away arm: An arming mode when all users have left the zones of the alarm system. In this mode, all zones are armed.
  - Disarm: Cancel arming.
- Bypass

  When detectors connected to the alarm controller malfunction or there is movement within specific zones, the normal arming operations within the system will be affected. In this case, the system allows users to bypass these zones.
  - Unbypass: Restores bypassed zones to the enabled status.
  - Bypass: The zone is temporarily disabled during the arm, and it automatically returns to the enabled status when the system is disarmed.
  - Isolate: The zone is permanently disabled. When the system is disarmed and then armed again, the isolated zone remains disabled.

Procedure

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

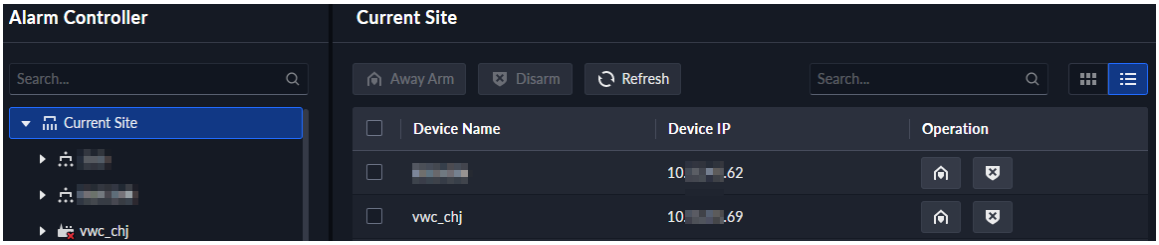
Step 2 Click **Alarm Controller**.

Step 3 In the device tree, click an organization.

All alarm controllers under this organization will be displayed on the right. You can select one or more alarm controllers, and then click (**Away Arm**) or (**Disarm**) to arm or disarm the alarm controllers you selected.

If arming failed, you can click **Force Arm** on the prompt window to arm again.

Figure 6-17 Alarm controller organization

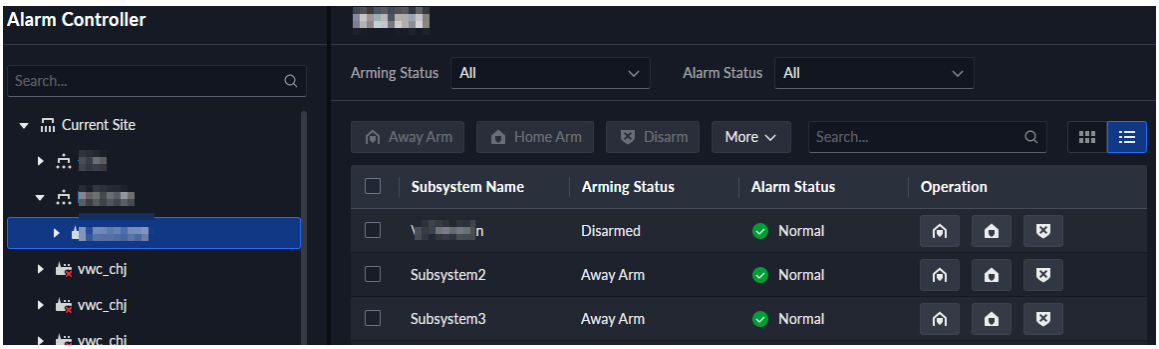


Step 4 In the device tree, click an alarm controller.

All subsystems under this alarm controller will be displayed on the right.

You can right-click an alarm controller, and then click **Update Alarm Controller** to update its information.

Figure 6-18 Subsystems



Step 5 Arm or disarm subsystems.

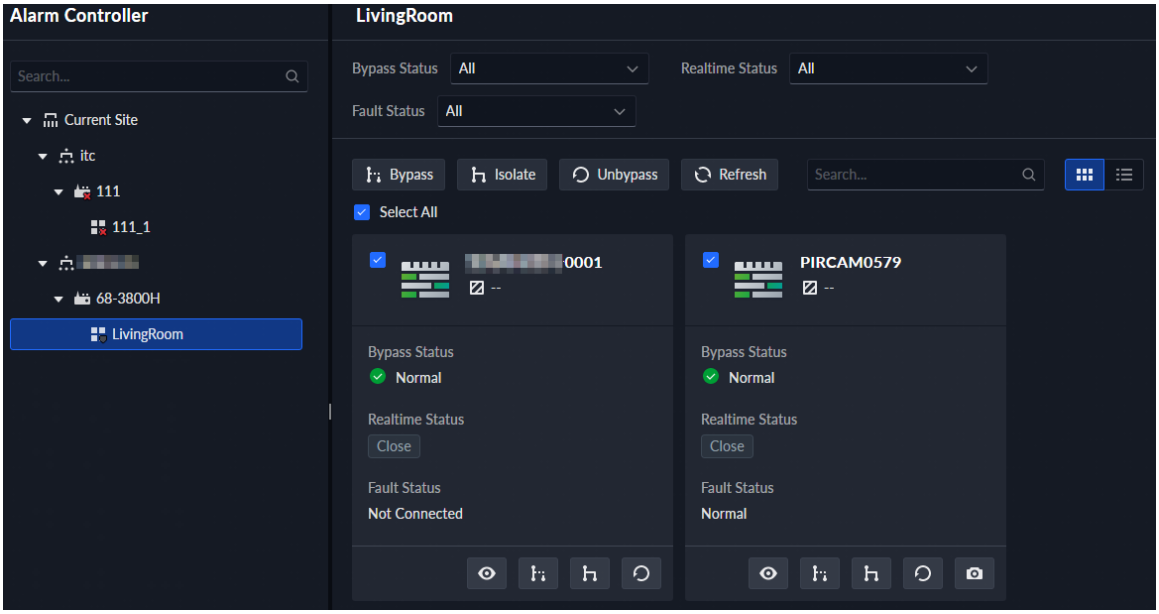
- Away Arm Home Arm Disarm: Operate on multiple subsystems.
- : Operate on one system.

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

Step 6 In the device tree, click a subsystem of the alarm controller.

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

Figure 6-19 Zone



Step 7 Bypass, isolate, or unbypass zones.

- Bypass Isolate Unbypass: Operate on multiple zones.
- : Operate on one zone. You can view details, bypass, isolate, unbypass, and take a snapshot respectively.

  - The snap function ( ) is available only when the alarm controller is online, and PIR camera is connected to the corresponding zone.
  - The snapshot can be downloaded to local in .jpg format.

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

Related Operations

Right-click the alarm controller, and then you can:

- Click **Update Alarm Controller** to update device information.
- Click **Alarm Output Control** , and then click or to open or close the alarm output of device, or you can select devices, and then click **Open** or **Close** to open or close alarm output of devices in batches.
- Click **Siren Control** , and then click or to open or close siren, or you can select sirens, and then click **Open** or **Close** to open or close them in batches.

6.2.5 Arming Control

You can edit or cancel temporary disarming on the platform to avoid unnecessary alarms, and enable or disable event schemes to with one click.

6.2.5.1 Temporary Disarming

You can edit or cancel temporary disarming to avoid unnecessary alarms. For example, if an industrial park holds a celebration activity, it can temporarily disarm the park or some zones as needed.

Prerequisites

You need to configure temporary disarming on the **Real-Time Event** or **Event History** page.

Procedure

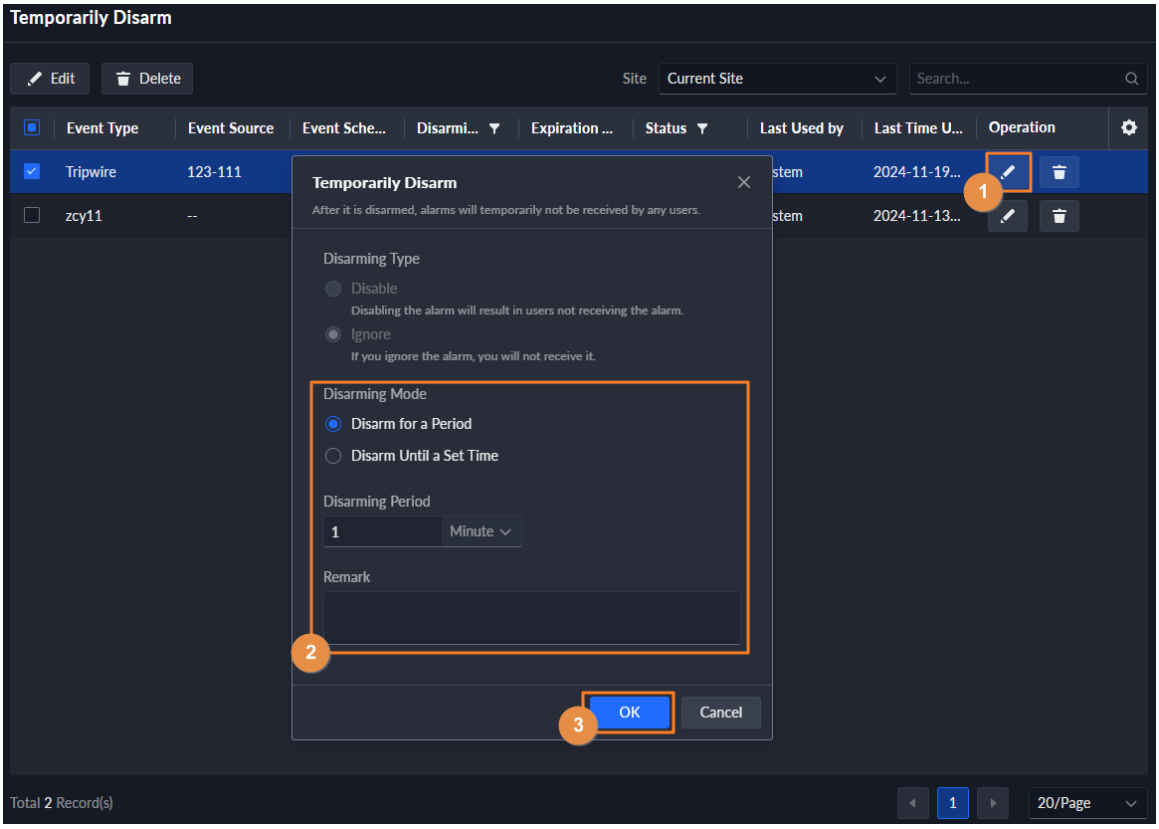
Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Event Center**.

Step 2 Select **Arming Control** > **Temporarily Disarm**, and then click corresponding to a disarming record to edit the disarming period.

Select several disarming records, and then click **Edit** to edit the disarming periods in batches.

You can set disarming for a period, or disarming until the defined time. If disarming type is set to disable, then all users will not receive this alarm within the defined time. If disarming type is set to ignore, then only the user who claim the alarm will not receive this alarm within the defined time. After the defined time, if the alarm is not eliminated, it will continue to alarm.

Figure 6-20 Edit temporary disarming



Step 3 Click **OK**.

Related Operations

Click corresponding to a disarming record to cancel disarming and delete the record.

Select several disarming records, and then click **Delete** to cancel disarming and delete the records in batches.

6.2.5.2 Scheme Control

The platform provides ease of enabling or disabling event schemes with one click. For example, when a device generates events frequently, you can disable it, so that no such events will be received.

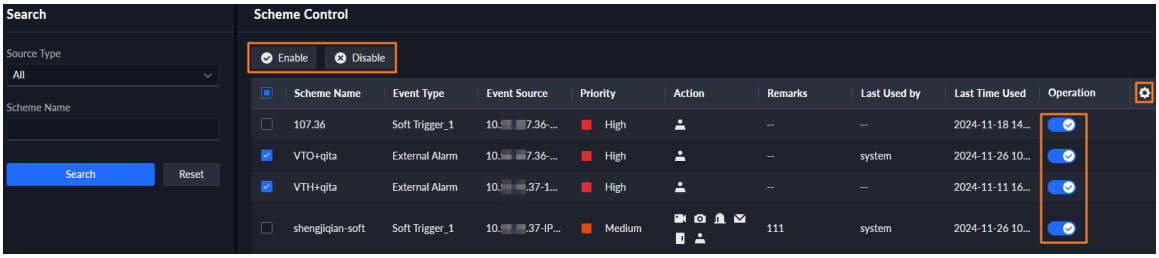
Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Event Center**.

Step 2 Select **Arming Control** > **Scheme Control**, and then enable or disable event schemes.

- Enable or disable schemes one by one: Click corresponding to a scheme to enable it, and then the icon changes to ; click to disable the scheme.
- Enable or disable schemes in batches: Select the schemes that you want to enable or disable, and then click **Enable** or **Disable**.

- You can filter schemes by **Source Type**, or search for schemes by the name.
- Click , and then you can select the fields to be displayed on the page.

Figure 6-21 Scheme control



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 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 **Target Search**, and then click .

- Search type
  - **Feature** : Search for records by the defined features, including age, gender, face mask, glasses, beard, and more.

    When selecting whether to search for identification records, the difference is that, besides the age and gender, identification records will also show the similarity between the captured face and those in the arming lists.
  - **Image** : The platform compares the image you upload to capture records on the selected devices. If the similarity between a captured image on the platform and the one you upload equals to or higher than the defined value, the platform will display the result. For body images, the platform can only compare them to records on one device.

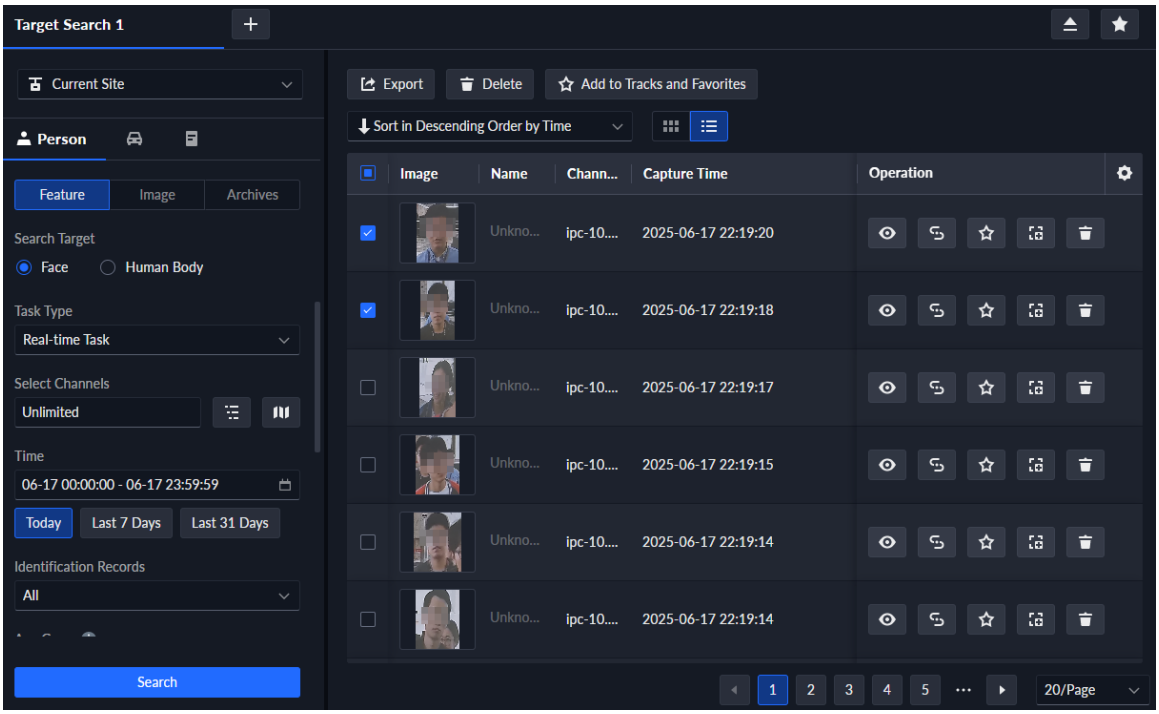
    Only new versions of IVSS devices support displaying similarity.
  - **Archives** : Search for records in the person information database.
- Search target
  - **Face** : Search for records in the face capture database.
  - **Human Body** : Search for records in the body capture database.
  - Search channel: Select device channels of the records by clicking **Selected Channel**.
  - Search time: Select time period of the records from **Today** , **Last 7 Days** and **Last 31 Days**.

    Only available for face and body capture records.

- Search conditions: Set search conditions such as age, gender, top color, ID, name and more to search for specific records.

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

Figure 6-22 Search results



Step 4 Manage the results.

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

- View details on records

  Select a record, and then click . Its details are displayed on the right, including snapshots, recorded videos (can be downloaded to your computer), and targets that can be further searched for (manually select a target or use AcuPick to automatically recognize targets).
- When viewing recorded videos and snapshots, you can select a target manually or select one automatically recognized by AcuPick, and then search for it in DeepXplore.
- If the channel is bound to other video channels, the recorded video from the bound video channels will play automatically.
- You can select a record, and then click to view the track playback. Perform searching by image using the current captured snapshot, with the search criteria defaulting to the current retrieval conditions. You can click on the track playback page, and then configure the conditions to search again.
- Generate tracks

  Click to add a record to the temporary records, and then click at the upper-right corner to view all records in the temporary records. Select multiple records, and then click **Generate Track** to generate a track.
- Click to add the person to a face arming group. After you send the group to devices and configure an event, devices can trigger alarms when the face is recognized.
- Click to delete it one by one.

You cannot delete the records of searching by image on devices.

- For the archives searching, double-click the search results or click to view the details. You can see the face capture, vehicle capture, access records and other information of the corresponding person.
- Extract records: When NVR and IVSS go online again after offline, the records of faces, human bodies, motor vehicles, and non-motor vehicles captured when they are offline can be uploaded to the platform.

  Click at the upper right, and then enter the platform login password. The **Resume Upload when Offline** page is displayed.

  - ◇ Auto extraction: Set the extraction time, and then the system automatically extracts the snapshot records 24 hours before the defined time. To extract records prior to 24-hour period, you need to perform manual extraction.
  - ◇ Manual extraction: Set the extraction time (up to 24 hours), select the type of record that you want to extract, select the device source for extraction (multiple channels of one device can be selected), and then click **OK**.

    The system extracts records according to the configuration.

    1. Select the search record to be exported as needed, and then click **Export**.
    2. Select the record type, set the export range, and then select the image checkbox.
    3. Click **OK** to export the record.

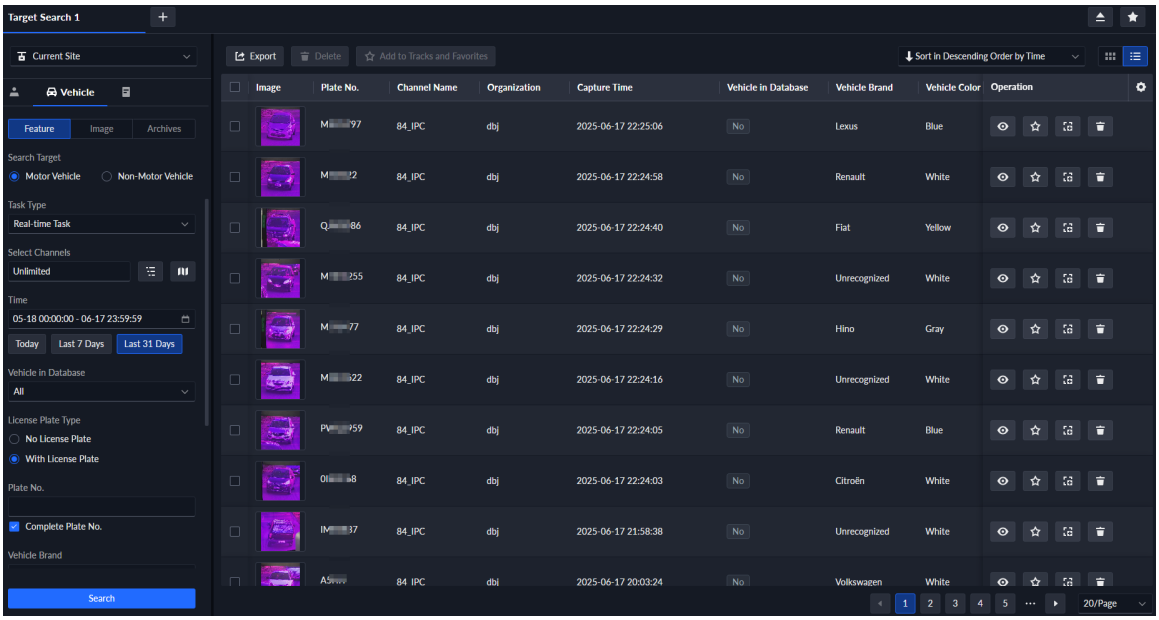
6.3.2 Searching for Vehicles

Procedure

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

Step 2 Click **Target Search**, and then click .

Figure 6-23 Vehicle search



- Search type
  - **Feature** : Search for records by the defined attributes, including vehicle in database, vehicles with or without license plate, vehicle brand, vehicle color, vehicle category, place of issue, confidence level, license plate length, area code, plate type, and more.

    Confidence level: Quantifies the probability that the recognized license plate number is accurate. Higher confidence represents more accurate recognition than lower confidence.
  - **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.
  - **Archives** : Search for records in vehicle information database.
- Search target
  - **Vehicle** : Search for records in vehicle capture database.
  - **Non-Motor Vehicle** : Search for records in non-motor vehicle capture database.
  - Search channel: Select device channels of the records by clicking **Selected Channel**.
  - Search time: Select time period of the records from **Today** , **Last 7 Days** and **Last 31 Days**.

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

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

For the search results, you can perform following operations.

- View details on records

  Select a record, and then click to view its details on the right, including snapshots, recorded videos (can be downloaded to your computer), and targets that can be further searched for (manually select a target or use AcuPick to automatically recognize targets).
- If the license plate is incorrectly or cannot be recognized, you can correct it manually. Then, it can be added to an arming group.
- If the channel is bound to other video channels, the recorded video from the bound video channels will play automatically.
- You can select a record, and then click to view the track playback. Perform searching by image using the current captured snapshot, with the search criteria defaulting to the current retrieval conditions. You can click on the track playback page, and then configure the conditions to search again.
- Generate tracks

  Click to add a record to the temporary records, and then click at the upper-right corner to view all records in the temporary records. Select multiple records, and then click **Generate Track** to generate a track.
- If a license plate is recognized, click to add the vehicle to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the vehicle is recognized.

- Only mobile arming tasks can be sent to devices. General arming tasks cannot be sent to devices.
- Non-motor vehicle, human body, card swiping, cannot be added to the arming group.

- Click to delete it one by one.

The records of searching by image on devices, access records cannot be deleted.

- For vehicle archives, double-click a record to view recognition records of a license plate.
- Extract records: When NVR and IVSS go online again after offline, the records of faces, human bodies, motor vehicles, and non-motor vehicles captured when they are offline can be uploaded to the platform.

  Click at the upper right, and then enter the platform login password. The **Resume Upload when Offline** page is displayed.

  - Auto extraction: Set the extraction time, and then the system automatically extracts the snapshot records 24 hours before the defined time. To extract records prior to 24-hour period, you need to perform manual extraction.
  - Manual extraction: Set the extraction time (up to 24 hours), select the type of record that you want to extract, select the device source for extraction (multiple channels of one device can be selected), and then click **OK**.

    The system extracts records according to the configuration.

    1. Select the search record to be exported as needed, and then click **Export**.
    2. Select the record type, set the export range, and then select the image checkbox.
    3. Click **OK** to export the record.

6.3.3 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**.

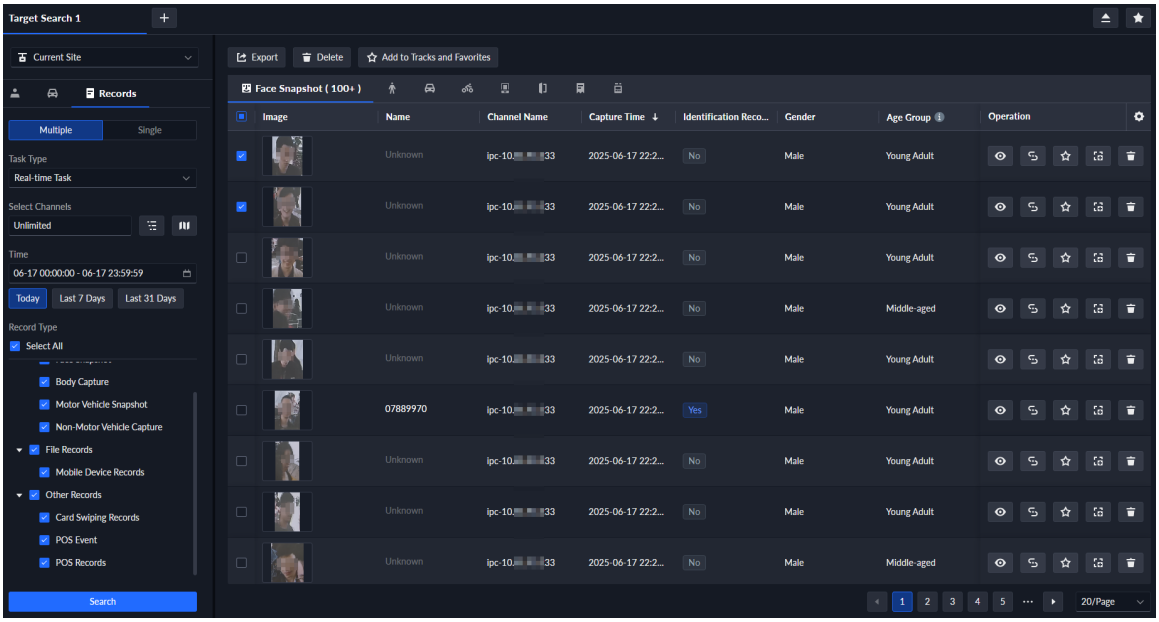
Step 2 Click **Target Search**.

Step 3 Click .

- **Multiple** : you can search for the records of multiple types. Select channel and time, and then click **Search**.

  When selecting channels, you can click to select channels from the channel list, or click to select channels from the map.

Figure 6-24 Records search



- **Single** : You can search for the records of a single type, including card swiping records. Set information such as channel, and time, and then click **Search**.

Step 4 Manage the results.

You can perform the following operations.

- View details on records

  Select a record, and then click to view its details on the right, including snapshots, recorded videos (can be downloaded to your computer), map, and targets that can be further searched for (manually select a target or use AcuPick to automatically recognize targets).
- When viewing recorded videos and snapshots, you can select a target manually or select one automatically recognized by AcuPick, and then search for it in DeepXplore.
- If the channel is bound to other video channels, the recorded video from the bound video channels will play automatically.
- Generate tracks

  Click to add a record to the temporary records, and then click at the upper-right corner to view all records in the temporary records. Select multiple records, and then click **Generate Track** to generate a track.
- You can also click to add it to a face arming group. After you send the group to devices and configure an event, devices can trigger alarms when the face is recognized.
- For the face snapshot and body capture, you can select a record, and then click to view the track playback. Perform searching by image using the current captured snapshot, with the search criteria defaulting to the current retrieval conditions. You can click on the track playback page, and then configure the conditions to search again.
- If a license plate is recognized, click to add the vehicle to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the vehicle is recognized.
- Click to delete it one by one.

- Extract records: When NVR and IVSS go online again after offline, the records of faces, human bodies, motor vehicles, and non-motor vehicles captured when they are offline can be uploaded to the platform.

  Click  at the upper right, and then enter the platform login password. The **Resume Upload when Offline** page is displayed.

  - ◇ Auto extraction: Set the extraction time, and then the system automatically extracts the snapshot records 24 hours before the defined time. To extract records prior to 24-hour period, you need to perform manual extraction.
  - ◇ Manual extraction: Set the extraction time (up to 24 hours), select the type of record that you want to extract, select the device source for extraction (multiple channels of one device can be selected), and then click **OK**.

    The system extracts records according to the configuration.

    1. Select the search record to be exported as needed, and then click **Export**.
    2. Select the record type, set the export range, and then select the image checkbox.
    3. Click **OK** to export the record.

6.3.4 Track Playback

The search results of face or body captured images support track playback, allowing for the playback and display of target trajectories on a map.

Prerequisites

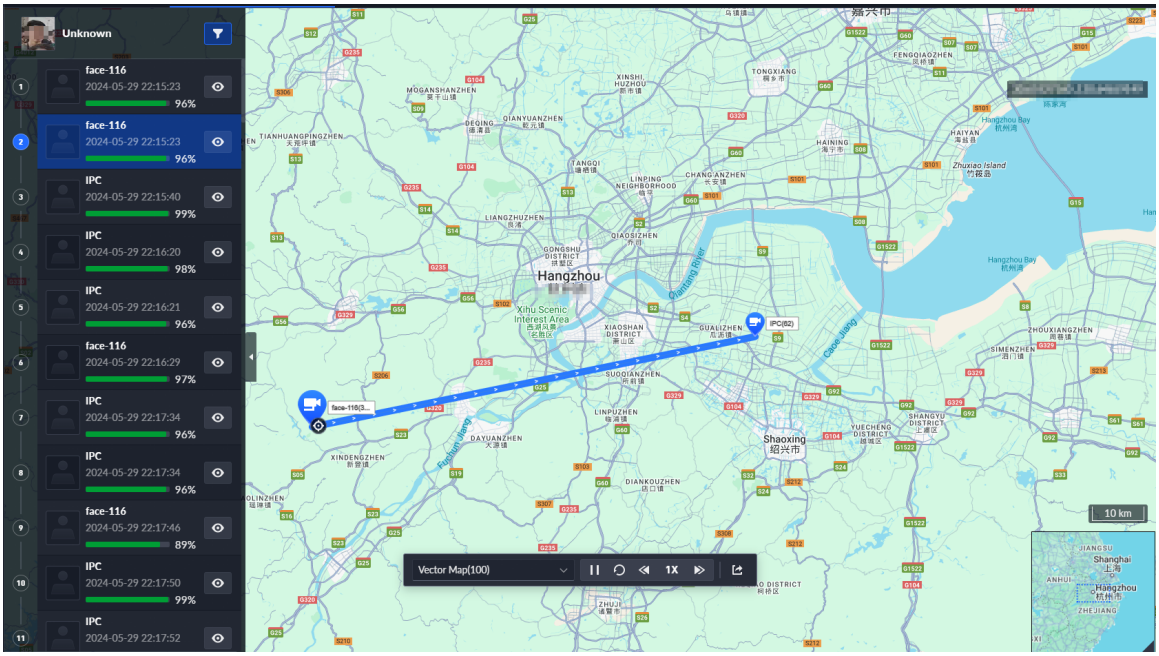
- The devices support structured feature reporting.
- You have configured the map.

Procedure

Step 1 On the person searching result page, or on the face snapshot or body capture searching result page of archives searching, select a result, and then click  to view the track playback. Perform searching by image using the current captured snapshot, with the search criteria defaulting to the current retrieval conditions.

Step 2 (Optional) You can click  on the track playback page, and then configure the conditions to search again.

Figure 6-25 Track playback



Step 3 Displays and plays the track in time order. Click on the snapshot card in the list to view the details.

Step 4 On the track playback page, the following operations are supported.

Table 6-10 The operation instruction of track playback

Icon	Description
Vector Map(100)	Switch the map. If the first location is within a subgraph, the system will automatically switch to the subgraph and start playing the trajectory. However, it does not support switching the map.
	Stop playing.
	Replay.
1X	Control the speed of track playback.
	Export the trajectory.

6.3.5 WizSeek

Supports searching for records by time, channel, data source, event type and similarity, and fast arming, and you can perform operations such as viewing details and adding records to favorites.

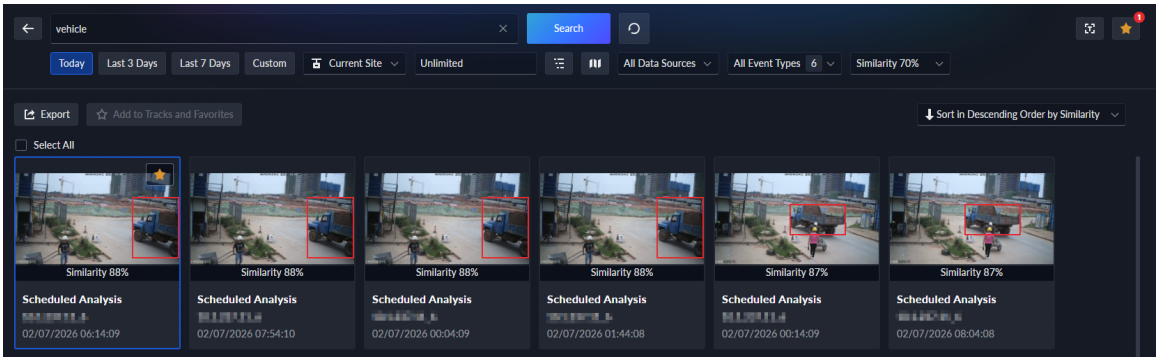
Procedure

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

Step 2 Click the **WizSeek** tab.

Step 3 Set the search conditions, including time, channel, data source, event type and similarity, and then click **Search**. After the search is complete, the page will display search progress 100%.

Figure 6-26 WizSeek



Step 4 Perform the operations.

Table 6-11 Operation description

Operation	Description
View large image	Click the image for a larger view.
Add to tracks and favorites	Hover over the image, and then click to add the record to tracks and favorites, or select records, and then click **Add to Tracks and Favorites** to add the selected records to tracks and favorites in batches. Click at the upper right, and then you can view the records added to the tracks and favorites.
Generate track	In the tracks and favorites, select the snapshot record, and then click **Generate Track**. The system will go to the track page and display the track information.
View record details	Hover over the image, and then click to view the record details. ● Click the **Snapshot** tab to view the snapshot. ◇ Click **AcuPick** , the platform automatically recognizes different types of targets in the video. You can select a target, and then quickly search for it on the **Target Search** page in DeepXplore. ◇ Click , drag on the video to select a target (right-click to exit), click , and then select **Search Face Image by Image** , **Search Human Body Image by Image** or **Search Vehicle Image by Image**. You can quickly search for it on the **Target Search** page in DeepXplore. ○ Move the selection box: Place the mouse cursor over the selected area, click the left button, and the drag the mouse. ○ Resize the selection box: Place the mouse cursor over the top-left, bottom-left, or top-right corner of the selected area. Click the left mouse button and drag it to adjust the size accordingly. ● Click the **Recording** tab to play back the recorded video. ● Click the **Map** tab to view the position of the target on the map.

Operation	Description
Export the records	1. Click **Export**. 2. Enter the platform login password, and set the encryption password. 3. Select **All** to export all the records, or select **Select Range**, set the record that you want to start from and the total number of records, to export the records according to your settings. 4. Enable **Export Image** as needed. 5. Click **OK**. The records will be exported to local in .zip format. You need to decompress the file with the encryption password before you can view the records.
Fast arming	1. Click  at the upper right of the search result page, and then configure the text-defined alarms. For details, see "5.4.3.1 Adding Text-Defined Alarms". 2. Click **OK**, and then the platform will automatically send the arming and configure the event plan.

6.4 Access Management

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

6.4.1 Access Control

6.4.1.1 Access Control Panel

Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**.

This page displays by default all the access points in the root zone and all its sub zones in card view.

Change the display mode

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

- In card view, it supports displaying the latest event information, device online or offline status, and door open or closed status.
- On the map, when an alarm occurs, the device icon on the map will be displayed in red.

View certain access points

On the top on the page, select a zone or access point type to display only door or lift control channels, or the access points in a zone and its sub zones.

View access point information

In card view, double-click an access point to view its information, including basic information, live videos from bound channels, and events. You can also lock or unlock the door and make a call to it.

Batch Operation

Supports batch operations for devices to set them to normally open, restore, normally closed, no authenticated mode, authenticated mode, and locked mode. All batch operations are similar; the following introduces the batch operation for setting access control devices to **Normally Open** as an example.

- Normally open all the doors: Click **Normally Open** , select **Keep All Always Open**, and then confirm the operation.
- Normally open the selected doors: Select multiple devices, select **Normally Open** > **Keep Selected Always Open**, and then confirm the operation.

Filtering the Device

Supports filtering by device status, with filter criteria including always open, normal, always closed, without authentication, with authentication, and lock. By default, all conditions are selected for filtering.

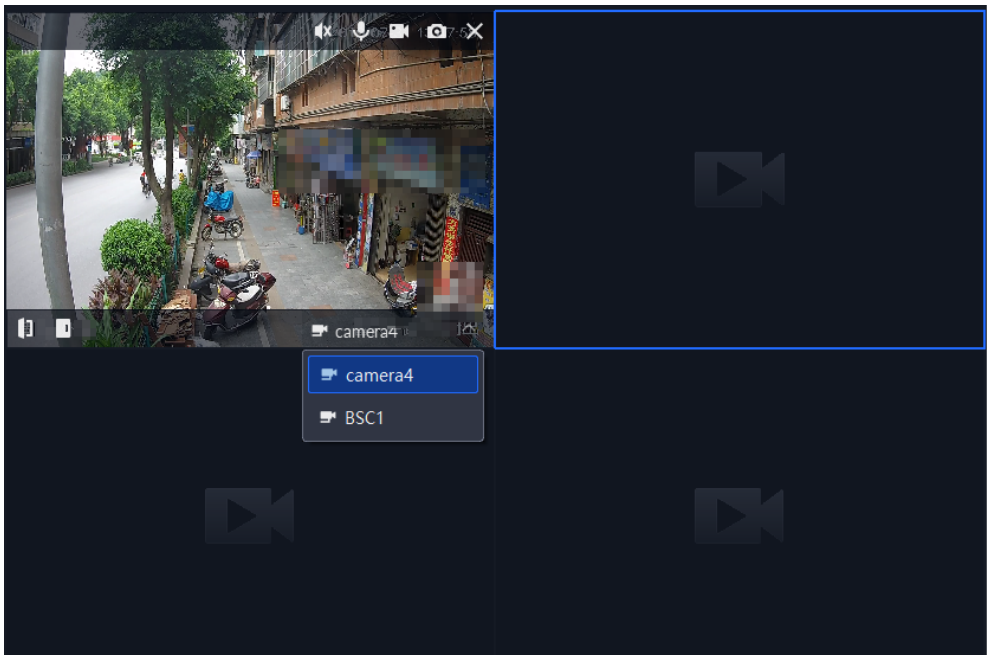
6.4.1.2 Viewing Live Video

Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**. You can view the live video of video channels bound to the access point (the channel can be bound when adding a device, or you can bind the video channel of the access control device) in the following ways.

View live videos in card view

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

Figure 6-27 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 Locking and Unlocking Door

Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Access Control** > **Access Control Panel**. You can unlock or lock doors in the following ways.

Unlock or lock doors in card view

Click to display access points in card view. Click or to unlock or lock a door channel.

Unlock or lock doors in the detailed information of an access point

In card view, double-click an access point, and then click **Open Door** or **Close Door**.

Unlock or lock doors on the map

Click  on the upper-right corner to display access points on the map. Click an access point, and then click  or  to unlock or lock a door channel.

6.4.1.4 Controlling Door Channels Globally

Set door channels in a zone to normally closed, normally open modes, or restore them to the normal status with one click.

1. Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**.
2. Select a zone, and then click **Always Open** , **Restore**, or **Always Closed** to control the door channels at the same time.
   - **Always Open** : People can pass without verifying their identifications.
   - **Restore** : Restore door channels to the normal status from normally open or normally closed mode. People must verify their identifications to pass
   - **Always Closed** : People cannot pass.

The always open, restore, and always closed operations are only for the access points of the current zone and its sub zones (that is, access points displayed on the console when no search operation is performed), not following the operations of the parent zone.

If the parent zone is set to always open or closed, the sub zones can be set to other states. If the device is offline when the rules are sent, it will not automatically change to the status of the corresponding zone after it goes online. You need to configure the status manually.

6.4.1.5 Controlling Lift Channels Globally

Set lift channels in a zone to no authentication, authentication, and lock modes.

1. Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Access Control** > **Access Control Panel**.
2. Select a zone, and then click **No Authentication Mode** , **Authentication Mode**, or **Lock Mode** to control the lift channels at the same time.
   - **No Authentication Mode** : People can go to any floor without verifying their identifications.
   - **Authentication Mode** : People must verify their identifications to go to specified floors.
   - **Lock Mode** : People cannot use lifts.

The no authentication mode, authentication mode, and lock mode are only for the lift control access points of the current zone and its sub zones (that is, lift control access points displayed on the console when no search operation is performed), not following the operations of the parent zone.

If the parent zone is set to no authentication mode, the sub zones can be set to other modes. If the device is offline when the rules are sent, it will not automatically change to the status of the corresponding zone after it goes online. You need to configure the status manually.

6.4.1.6 Viewing Real-Time Events

When a person passes through an access point, an event will be reported to the platform. You can view the detailed information of that event.

Prerequisites

If you want to view recorded videos and live videos of an event, you must configure the following parameters first:

- Live video: Bind video channels to access points. For details, see "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 ("4.2.5 Adding Recording Plans"), or configure an event to link the bound video channels to record videos when a person passes ("5.1 Configuring Events").
- Snapshot: Enable the snapshot function on the device side, and configure an event to link the bound video channels to take snapshots 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.

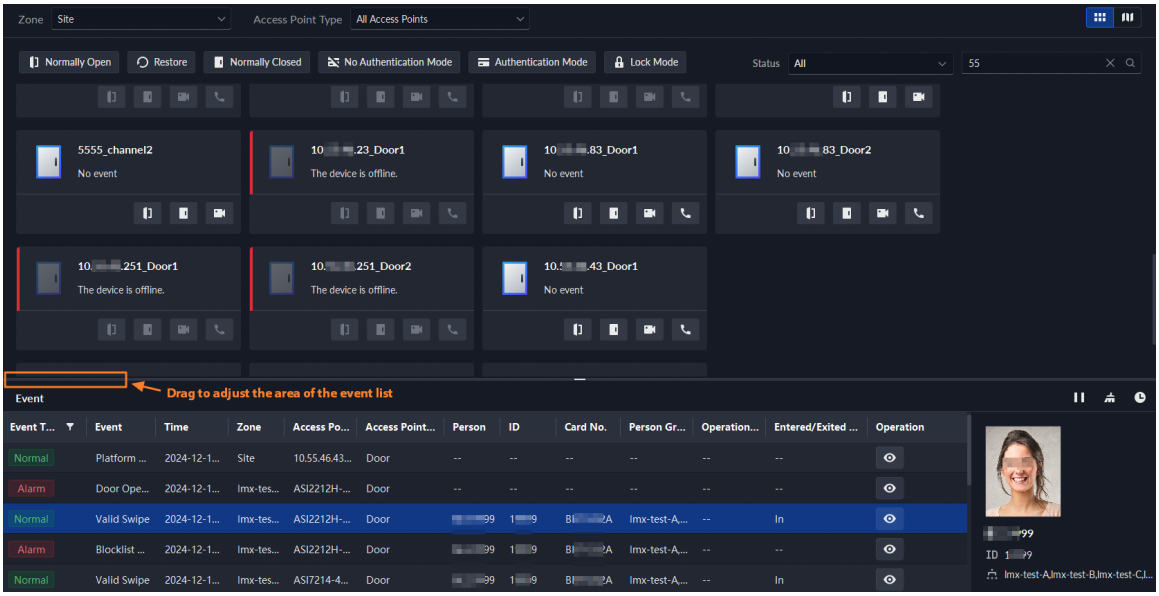
Step 3 Click , and then you can view the snapshot, recorded video, and live video of the event.

Step 4 Locate the access point for an event.

- Click on the upper-right corner to display access points in card view. When events are not clicked, it displays the image and information of the person in the latest event; when clicked, the corresponding access point card will be highlighted, and it will display the image and information of the person of the selected event.
- Click on the upper-right corner to display access points on the map. When events are not clicked, the status of the access point icons on the map will change in real time; when clicked, the event information will be displayed on the map.

- You can drag the real-time events upwards. See the following figure.
- Hover over the person image at the lower-right corner, and then you can view it in a larger image.

Figure 6-28 Events



Related Operations

- You can filter events by **Status**.
- : Stop receiving new events. Click it again to start receiving events.
- : Clear the events on the page, but they will not be deleted.
- : View access records.
- : Select the fields that you want to display or hide.
- For anti-passback alarms, you can click to reset the anti-passback time. After resetting, the person can re-enter the start point of the anti-passback route.

  This function only applies to global anti-passback rules.

6.4.1.7 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 6-12 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.

Parameter	Description
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/ID/Access Point/ Access Point/Company/ Department/Card No.	Select an option and enter keywords to search for certain events. For example, select **Access Point** and enter Front Gate to search for events of access points that have Front Gate in their names.
Keywords	

Step 3 (Optional) Export records.

1. Click **Export**.
2. Enter the login password, encryption password, select whether to export images and the export range, select fields to be exported, and then click **OK**.

   You can configure whether to verify the password. For details, see "8.3.2 Configuring Security Parameters".

   - The encryption password is used to protect the export file. It consists of 6 uppercase or lower case letters, numbers, or their combinations. You need to enter it when using the export file.
   - The export range can be all or specified events that are displayed.
   - Select **Export Image** to export snapshots of the events at the same time.
   - The fields to be exported include **Event Type** , **Event**, **Time**, **Zone**, and more.

Related Operations

- Click **Total** , **Alarm Event**, **Abnormal Access**, or **Normal Access**, and then you can view the events of the corresponding status.
- Click to select the field that you want to show or hide.
- Click to view the access record details.
- For anti-passback alarms, you can click to reset the anti-passback time. After resetting, the person can re-enter the start point of the anti-passback route.

  This function only applies to global anti-passback rules.
- Click to delete the access record.
- Click to add a record to the movement path.

  After that, you can click to view the movement path, where you can select the records, and then click **Generate Track** to view track information.

6.4.1.8 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. You can manually acquire the records from specified period and device.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Access Control** > **Access Records** > **Event Records**.

Step 2 Click **Acquire Records**.

Step 3 Enter the login password, and then click **OK**.

Step 4 Acquire records.

Select **Extract Image**, and then you can acquire images of the access records. Before using this function, you need to configure image storage. For details, see "4.4.4 Configuring Device Storage".

- **Auto Extraction** : The platform automatically synchronizes offline records from the previous 24 hours at a scheduled time each 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 that you set.

    For example, the latest record from the last automatic synchronization was on 2026-3-18 16:00, time of automatic synchronization is set to 04:00 every day. The device was offline on 2026-3-18 18:00, and then reconnected on 2026-3-20 16:00, then the platform, on 2026-3-21 04:00, will synchronize the records generated on the device from 2026-3-18 16:00 to 2026-3-21 04:00.
  - If records on a device have 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 2026-3-18 16:00 with the latest record uploaded on 2026-3-18 15:00. Before the time of synchronization, the device goes offline and online multiple times. Then on 2026-3-19 04:00, the platform will synchronize the records generated on the device from 2026-3-18 15:00 to 2026-3-19 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 offline records ranging from the last time that an extraction was performed which were not extracted.

    Select **Extract Image**, and then you can extract images in the access records.
  - Select **Extract by Range**, and then you can specify the time range, record type, and device.

6.4.1.9 Sending Reports

The platform supports sending reports to the specified receiver by sending now or auto send.

Prerequisites

You need to configure the email server from > **System Parameters** > **Email Server**. For details, see "8.3.6 Configuring Email Server".

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Access Control** > **Access Records** > **Event Records**.

Step 2 Click **Send Report** , and then select **Send Now** or **Auto Send**.

- **Send Now** : Click to select the receiver, or enter the email address of the receiver and then press Enter, configure the email content, start from sending which record, and the total records to be sent (up to 100,000 records can be sent at a time).
- **Auto Send** : Automatically send reports to the receivers at specified time of each day or week.
  1. Enable **Daily Report** or **Weekly Report**, and then set the time.
  2. Click to select the receiver, or enter the email address of the receiver and then press Enter.

Step 3 Click **OK**.

6.4.1.10 Viewing Access Route

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

Step 1 Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Access Control** > **Access Records** > **Event Records**.

The number of events in the root zone is displayed on the top of the page by default.

Step 2 (Optional) Select a zone, person group, and period, and then click **Search**.

You can search for event within up to 1 month.

The selected person group is empty by default. In this case, the search results will include events with no related person information, such as access trajectory of a person whose information is not on the platform, access trajectory of strangers, and alarms triggered by devices.

Step 3 (Optional) Click to add multiple events to the temporary records.

Step 4 (Optional) Click to go to the temporary records.

Step 5 Select the records, and then click **Generate Track** to generate the route.

The platform will play the route based on the time of events.

If events happened in multiple zones, and the maps of zones do not relate to each other as main and sub maps, the platform might not play the route normally.

6.4.1.11 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 (Optional) Export records.

1. Click **Export**.
2. Enter the login password, encryption password, select the export range, select fields to be exported, and then click **OK**.

You can configure whether to verify the password. For details, see "8.3.2 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.
- The fields to be exported include **Event Type** , **Event**, **Time**, **Zone**, and more.

Related Operations

- Manually mark the enter or exit status for people:
  - On the list of **Person Entered** , **Person Exited** or **Persons Who Did Not Exit after Entering**, click to see all access records of a person. Click to mark a record as invalid (the records will not be deleted). The invalid records can also be restored to be valid. The statistics and status of the person will change accordingly.
  - On the list of **Persons Who Did Not Exit after Entering**, click to mark a person as "exited". The statistics and status of the person will change accordingly.
- You can filter the search results by **Person Group** , and also search the records by selecting **Person**, **ID**, **Access Point**, **Company**, or **Department**, and then entering the keywords.
- Force clear: Supports force clearing the person in batches or force clear all the person who did not exit after entering.
  - Force clear in batches: Click **Persons Who Did not Exit after Entering** tab, select multiple person, and then click **Force Clear** > **Force Clear Selected**.
  - Force clear all: Click **Persons Who Did not Exit after Entering** , and then select **Force Clear** > **Force Clear All**.

Up to 10,000 people can be cleared at one time.

6.4.2 Visitor Application

After visitor information is registered, the visitor can have access permission. Access permission is disabled after the visitor leaves or if the visitor does not after the appointment leaving time.

6.4.2.1 Preparations

- You have configured the deployment of the video intercom devices, access control devices, lift control devices, and entrance and exit devices. For details, see the corresponding user manual.
- You have configured the basic configuration of the platform. For details, see "4 Basic Configurations".
- Make sure that you have configured the visitor configuration before application. For details, see "5.6 Visitor Management". You can also click Visitor Config to go to the video intercom configuration page.

6.4.2.2 Process

- Visits after appointment: Visitors make appointments according to "6.4.2.4 Visitor Appointment", and when they arrive on site, they can quickly access by confirming their information through **Check In** according to "6.4.2.6 Checking In".



- Visits without appointment: When visitors arrive, they need to fill out visitor information on site according to "6.4.2.6 Checking In". This will take a few minutes before they can access.



6.4.2.3 Visitor Management

You can view visitor information, and perform operations such as visitor appointment, checking-in, appointment approval, and more.

Log in to the DSS Client. On the **Home** page, click > **Access Management** > **Visitor** > **Visitor Management**, and then you can view visitor information and perform operations.

Figure 6-29 Visitor management

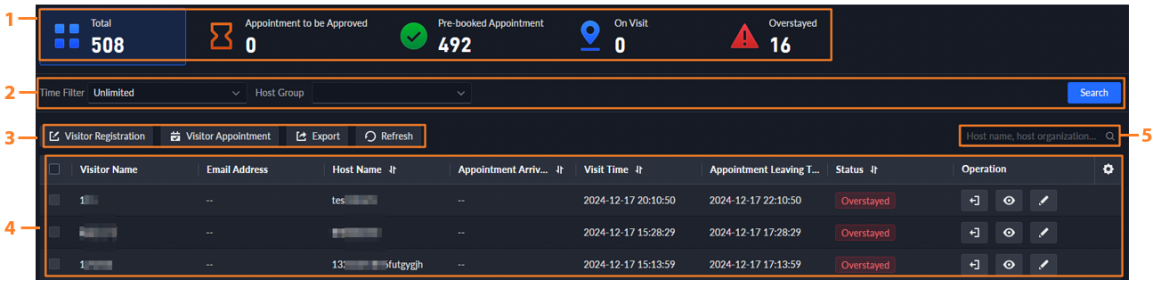


Table 6-13 Visitor management description

No.	Description
1	Displays the visitors in total and the number of visitors by access status. • **Appointment to be Approved** : Visitors must be approved before they can access, if they create appointment by themselves or are invited by host from > **Visitor** > **Visitor Appointment Config**, and an approving role is configured. For details, see "5.6.2 Configuring Visitor Appointment". After being approved, the status changes to **Pre-booked Appointment**. • **Pre-booked Appointment** : Appointment has been made, but not checked in yet. • **On Visit** : Already checked in, but not exceed the appointment leaving time. • **Overstayed** : Not checked out after the appointment leaving time.
2	Filter the visitor information by host group and time (appointment visit time, visit time, appointment leaving time, or unlimited).
3	Perform operations such as visitor registration, visit appointment and exporting visitor information. See the following sections in this chapter.
4	Visitor information list. Click to select the fields that you want to display.
5	Search for visitors by host name, organization (department), or more.

6.4.2.4 Visitor Appointment

Making appointment before visitor arrive will greatly reduce the time that visitors have to wait for their information to be recorded. After appointment, the visitor status changes to **Pre-booked Appointment**.

6 ways of appointment are available:

- Appointment through the platform. For details, see "6.4.2.4.1 Appointment through the Platform".
- Create appointment by visitors. For details, see "6.4.2.4.2 Creating Appointment by Visitors".
- Invited by host. For details, see "6.4.2.4.3 Appointment Invited by Host".
- Appointment through the visitor terminal. For details, see the user manual of the visitor terminal.
- Appointment DSS Agile app. For details, see the user manual of the app.
- Invited by host through OnePass App. For details, see the user manual of the app.

6.4.2.4.1 Appointment through the Platform

Register the information of visitors on the platform before they arrive for their visits. This will greatly reduce the time that visitors have to wait for their information to be recorded.

Procedure

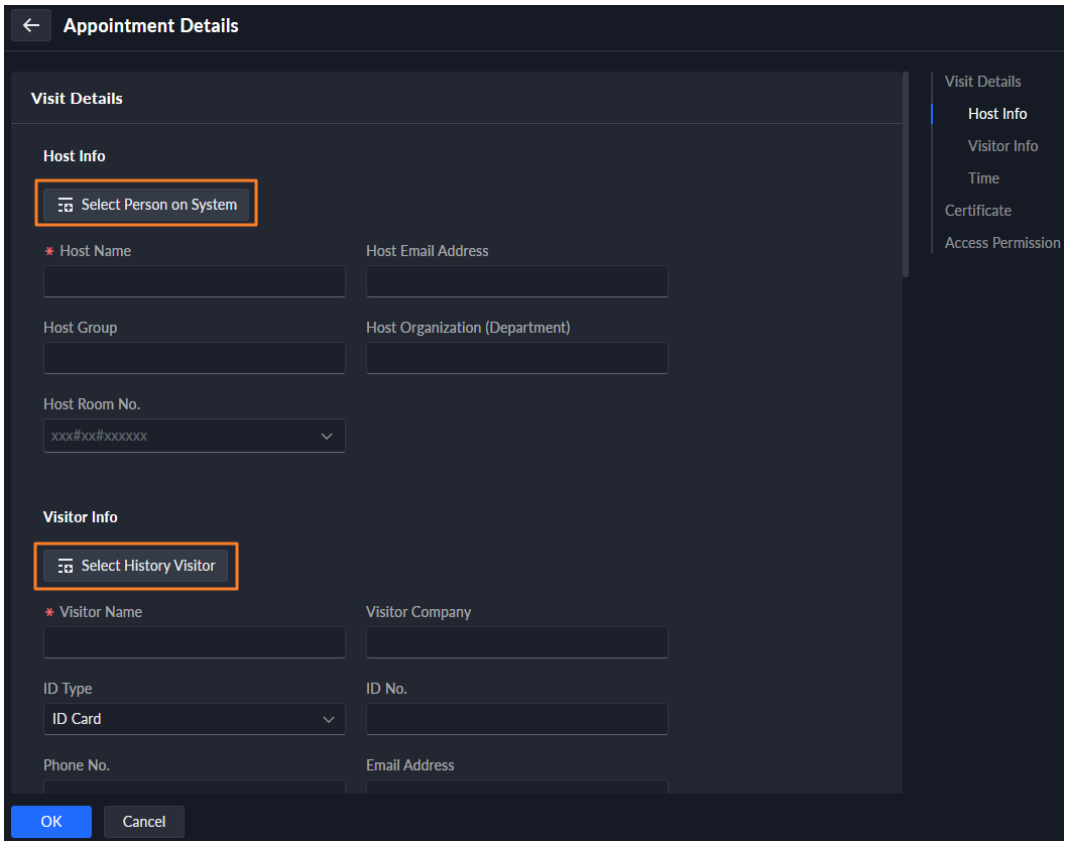
Step 1 Log in to the DSS Client. On the **Home** page, click > **Access Management** > **Visitor** > **Visitor Management**.

Step 2 Click **Visitor Appointment**.

Step 3 Enter the information of host and visitor.

Click **Select Person on System** , and then select a person (only person in the person group to which the current user has permission can be selected. Person group permissions can be configured when adding a person). The host name and group information will be automatically filled in and cannot be edited, but the other information can be modified. Click **Select History Visitor**, and then select a history visitor. The information of this visitor will be automatically filled in and can be edited.

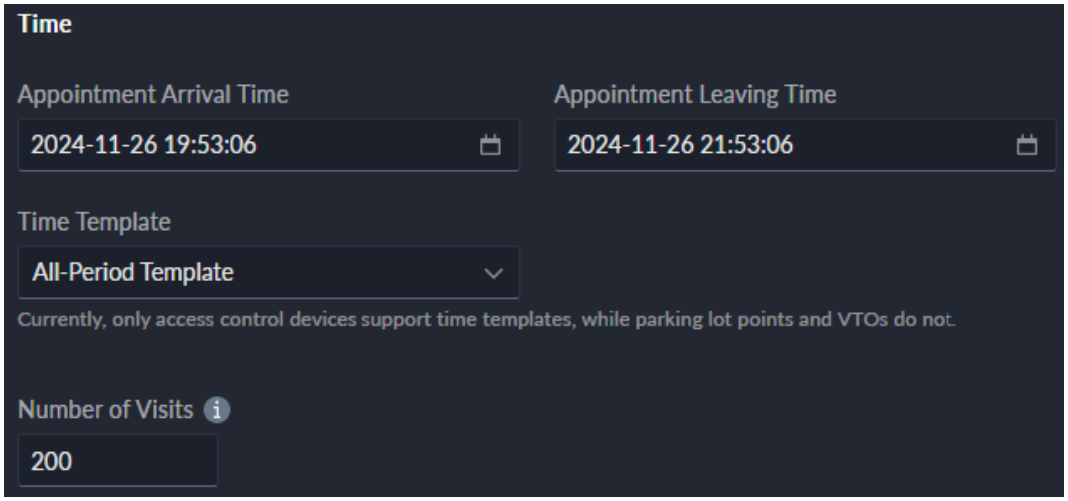
Figure 6-30 Visitor appointment



Step 4 Configure appointment arrival and leaving time, set the time template and number of visits.

- **Time Template** : All-period, week day and weekend templates are available by default. You can also click **Create Time Template** to customize visit periods from Monday to Sunday.
- **Number of Visits** : The number of visits of the selected visitor for each device.

Figure 6-31 Configure time



Step 5 In the **Certificate** section, you can issue a card to the visitor, set the visitor face image, and generate visitor pass.

Table 6-14 Certificate description

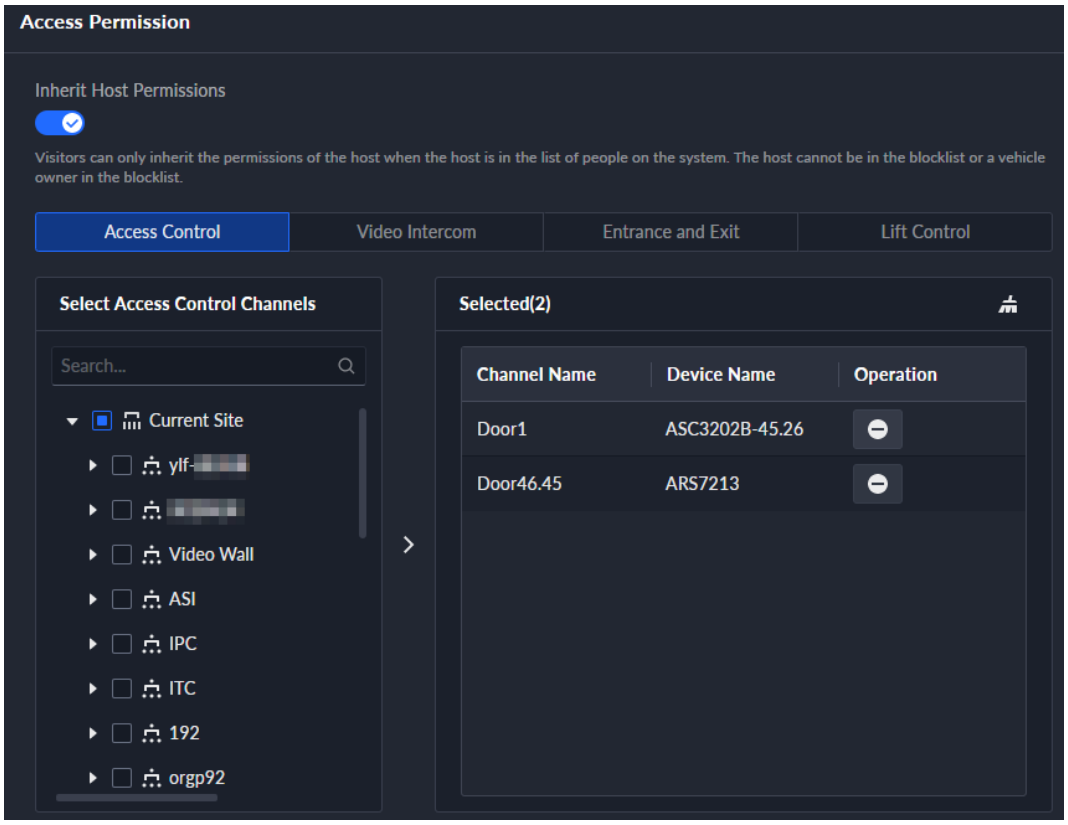
Tab	Description
Card	Issue a card to a visitor. You can issue cards by entering card number manually or by using a card reader. A card number comes with 8–16 numbers. Only second-generation access control devices support 16-digit card numbers. When a card number is less than 8 numbers, the system will automatically add zeros prior to the number to make it 8 digits. For example, if the provided number is 8004, it will become 00008004. If there are 9-16 numbers, the system will not add zero to it. • Issue cards by entering card numbers manually: Click **Add** , enter the card number, and then click **OK**. • Issue cards by using a card reader: Click , select a card reader or device, and then click **OK**. Swipe card through the reader or device, and then a new card will be issued.
Face	Set the face image of the visitor. 1. Click **Add**. 2. Click **Select from Local Folder** to select a picture, or click **Snapshot** to take a photo (if a camera is detected on your computer).
Visitor Pass	Click **Generate** to generate a QR code for the pass. • The QR code is valid within the defined appointment period. • You can click **Download Pass** to download the QR code, or you can click **Email Pass** to send it to the visitor by email.

Step 6 Click the **Access Permission** tab, and then select access permissions for the visitor.

If you want to set video intercom devices and entrance and exit permissions, you must set host room number and number plate for the visitor.

By enabling **Inherit Host Permissions**, the visitor can share the access permissions with the host, but be noted that the host must be in the list of people on the system, and cannot be in the blocklist or the owner of a vehicle in the blocklist.

Figure 6-32 Access permission



Step 7 Click **OK**.

After appointment, the visitor status changes to **Pre-booked Appointment**.

Step 8 (Optional) Proceed to check in, or click to cancel the appointment as the screen instructs.

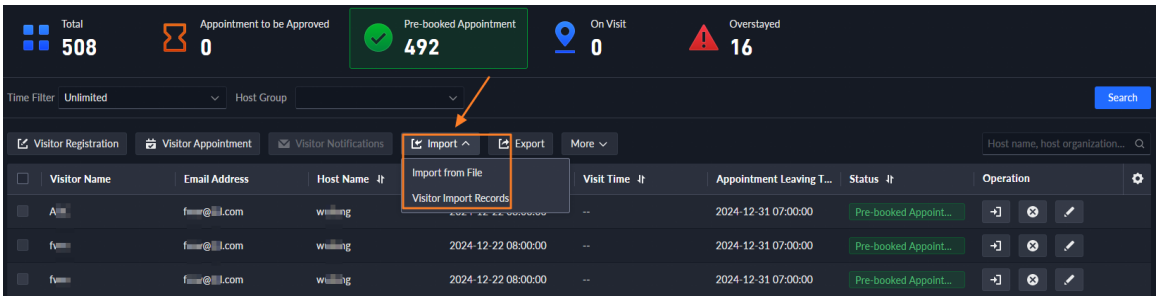
Related Operations

Click the **Pre-booked Appointment** tab, and then you can import the visitor appointment information in batches.

1. Select **Import** > **Import from File**.

- A imported file cannot exceed 1 GB, 1 file can be imported at a time, and a maximum of 1,000 visitors can be imported at a time.
- Click **Visitor Import Records**, and then you can view the import records.

Figure 6-33 Import visitor appointment information in batches



2. Click **Download Template**, and then fill in the information according to the template requirements.
3. Click **Import File** to import the completed template to the platform.

6.4.2.4.2 Creating Appointment by Visitors

After the platform administrator generates the visitor appointment link on the platform, visitors can access the link and fill out their appointment information. After approval, the visitor can access with the visit credential.

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

You can also go to the **Visitor Config** page by selecting **Access Management** > **Visitor**, and then clicking at the lower-left side.

Step 2 Select **Visitor Appointment Config** > **Create Appointment**.

Step 3 (Optional) Enable **Appointment Review Config on Visitor Terminal** as needed. After being enabled, appointments made through the visitor terminal must be approved by the defined approver before the visitors can access; if not enabled, then no approval is required.

Step 4 Select the approver.

When selecting **Host Approval** , the host will receive an email notification for approval; when selecting **Role**, the defined role will receive an approval notification in the platform's notification center at the upper right.

Step 5 (Optional) Enable **Inherit Host Permission**. After being enabled, visitors have the same access permissions as the host they are visiting.

If visitor appointment review is not enabled, or if the review is enabled but the approval role is selected as the visitors, then inheriting the host permissions is not supported.

Step 6 Enable **LAN Access Entry** or **WAN Access Entry**, click **Send Email**, and then set the visitor's email. The platform will send an invitation link to the visitor's email through LAN or WAN.

- Click **Regenerate** to generate a new link. The original link will be invalid.
- Click to copy the link.

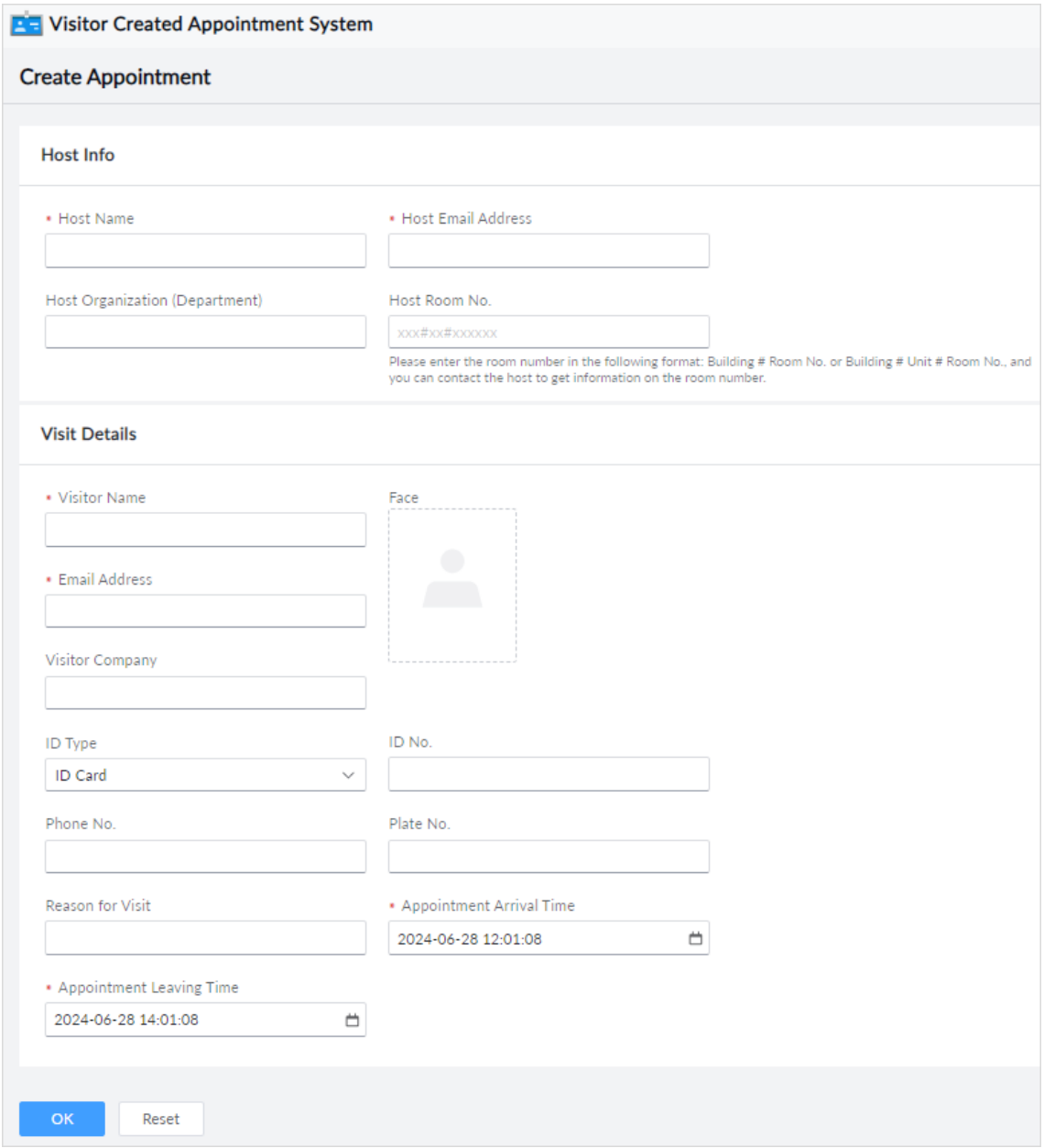
Step 7 (Optional) Click to download the QR code; click , and then select the printer to print the QR code.

Step 8 Click **Save**.

Step 9 The visitor clicks the link or scans the QR code to fill in the information, including their name, email, company (department), room number, appointment arrival time, and appointment leaving time, and the host's name, email address, license plate number, phone number, and more.

The host must be a person that has been added to the platform in > **Person and Vehicle Info** > **Person List**.

Figure 6-34 Create appointment



Step 10 Approve the appointment.

Step 11 The visitor visits the host with the visit credential received through the email.

6.4.2.4.3 Appointment Invited by Host

After the platform administrator generates a visitor appointment link on the platform, visitors can access the link and verify the email of the host. They can then fill out their appointment information to make an appointment.

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

You can also go to the **Visitor Config** page by selecting **Access Management** > **Visitor**, and then clicking at the lower-left side.

Step 2 Select **Visitor Appointment Config** > **Host Invitation**.

Step 3 (Optional) Enable **Approved by**, and select the approval role. The appointment must be approved by the user of the selected role before the visitor can visit; if not enabled, no approval is required.

If approval role is configured, the role can approve the appointment from **Access Management** > **Visitor** > **Visitor Management** > **Appointment to be Approved**. For details, see "6.4.2.5 Reviewing Appointment".

Step 4 (Optional) Enable **Inherit Host Permission**. After being enabled, visitors have the same access permissions as the host they are visiting.

If visitor appointment review is not enabled, or if the review is enabled but the approval role is selected as the visitors, then inheriting the host permissions is not supported.

Step 5 Enable **LAN Access Entry** or **WAN Access Entry**, click **Send Email**, and then set the visitor's email. The platform will send an invitation link to the visitor's email through LAN or WAN.

- Click **Regenerate** to generate a new link. The original link will be invalid.
- Click to copy the link.

Step 6 (Optional) Click to download the QR code; click , and then select the printer to print the QR code.

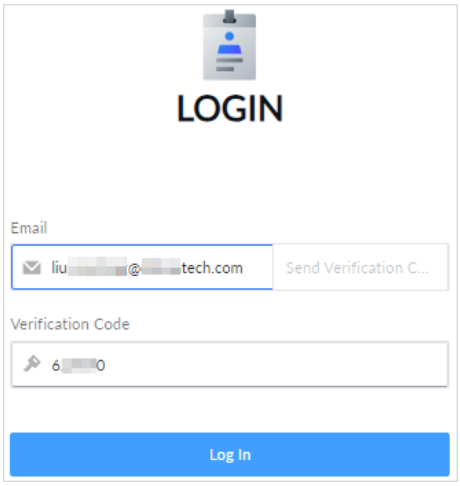
Step 7 Click **Save**.

Step 8 The visitor clicks the link or scans the QR code to fill in the information.

1. Enter the email address of the host, and then the system will send a verification code to that email address.

   You need to configure the person's email from **Person and Vehicle Info** > **Person List**; otherwise, the verification code cannot be sent.

Figure 6-35 Verify email of host

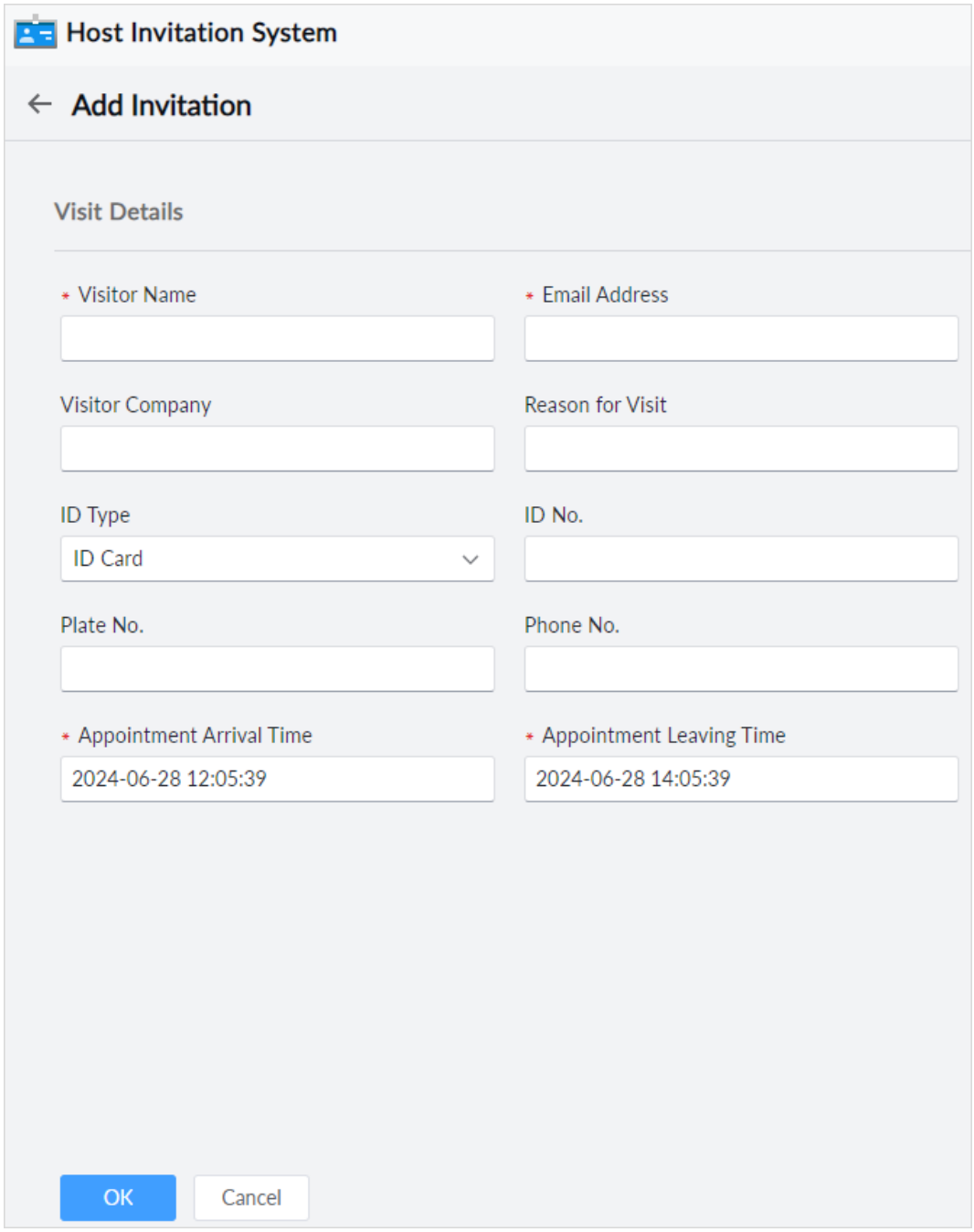


2. After entering the verification code, the visitor can select **Add Invitation** to proceed.

   Click **My Invitation** to view the invitation records.

3. Fill out visitor information, including their name, email, company, reason for visit, license plate number, phone number, appointment arrival time, appointment leaving time, and more.

Figure 6-36 Host invitation



4. Click **OK**.

Step 9 The approver approves the appointment (if approver has been configured).

Step 10 The visitor visits the host with the visit credential received through the email.

6.4.2.5 Reviewing Appointment

After the appointment is approved, the system will send the visit credential to the email of the visitor, and then the visitor can access through the credential.

Prerequisites

Review is enabled in **Visitor Appointment Config**. For details, see "5.6.2 Configuring Visitor Appointment".

Procedure

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

Step 2 Click the **Appointment to be Approved** tab.

Step 3 Review the appointment.

- Click to approve the appointment. After this, the **Status** changes to **Pre-booked Appointment**.
- Click to decline the appointment.
- Click to send the email to notify visitors configured through > **Visitor** > **Visitor Appointment Config**.

  The host will also be reminded to give their approval if **Host Approval** is enabled in > **Visitor** > **Visitor Appointment Config** > **Create Appointment**.
- Supports enabling **Inherit Host Permission**. After being enabled, visitors have the same access permissions as the host they are visiting.

6.4.2.6 Checking In

When a visitor with an appointment arrives, you need to confirm their information and give them access permission. On-site registration is supported when there is a walk-in visitor. Visitors can get access by swiping card, face recognition or scanning QR code.

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

Step 2 Enter the information of the visitor.

- If a visitor has an appointment, find their visitor information, and then click .
- If a visitor does not have an appointment, click **Visit Registration**, and then configure visitor information. For details, see "6.4.2.4 Visitor Appointment".

Step 3 Click **OK**.

After checking in, the visitor status changes to **On Visit**.

6.4.2.7 Checking Out

When visitors are leaving, remove their access permissions.

Procedure

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

Step 2 Click the **On Visit** tab, and then click .

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

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

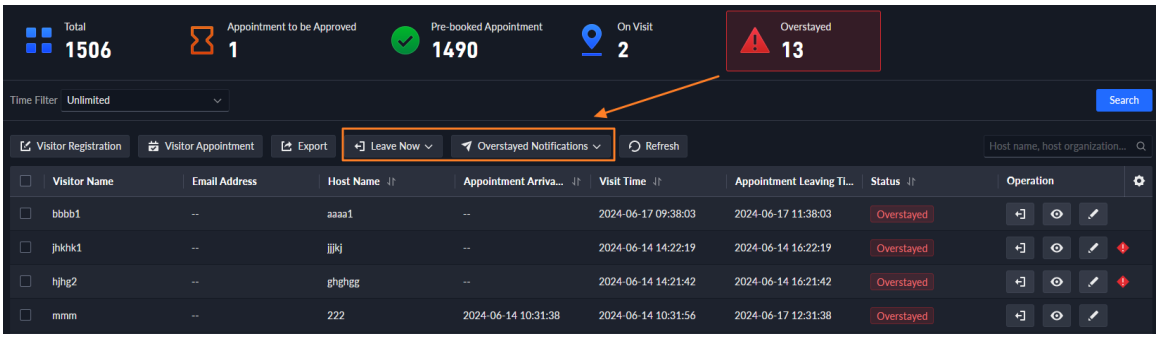
Related Operations

Click the **Overstayed** tab, and then you can check out visitors that are overstayed in batches and send notifications to them.

- Check out in batches: Select **Leave Now** > **Select All to Leave** to remove access permissions of all overstayed visitors; or you can select visitors first, and then select **Leave Now** > **Select to Leave** to remove access permissions of just the selected visitors.
- Send notifications: Select **Overstayed Notifications** > **Send Now/Auto Send**, select the receiver or enter the receiver's email and press Enter, and then click **OK**, to send notifications to the specified receivers.

  For **Auto Send**, you need to set the time to send the email each day.

Figure 6-37 Operations related to overstayed visit



6.4.2.8 Overstayed Visit

The visitor status changes to **Overstayed** if visitors do not check out within the appointment leaving time. In this case, you can check out these visitors in batches, or send them notifications to remind them of the overstayed status.

Procedure

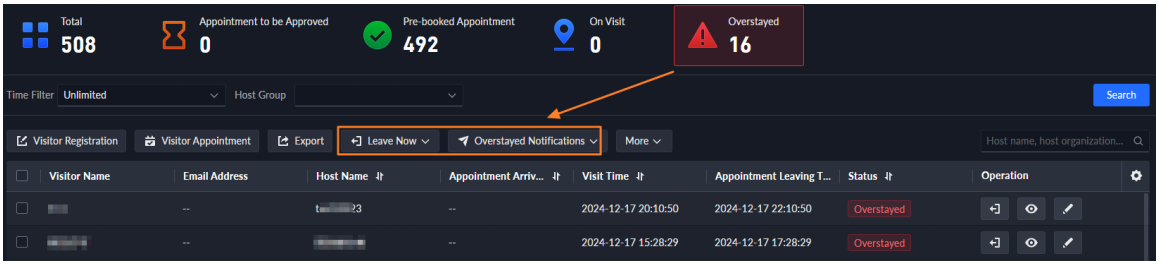
Step 1 Log in to the DSS Client. On the **Home** page, click ⊞ > **Access Management** > **Visitor** > **Visitor Management**.

Step 2 Click the **Overstayed** tab, and then you can check out visitors that are overstayed in batches and send notifications to them.

- Check out in batches: Select **Leave Now** > **Select All to Leave** to check out all overstayed visitors; or you can select visitors first, and then select **Leave Now** > **Select to Leave** to remove access permissions of just the selected visitors.
- Send notifications: Select **Overstayed Notifications** > **Send Now/Auto Send**, select the receiver or enter the receiver's email and press Enter, and then click **OK**, to send notifications to the specified receivers.

  For **Auto Send**, you need to set the time to send the email each day.

Figure 6-38 Operations related to overstayed visit



6.4.2.9 Visit Records

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

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

Step 2 Set search conditions, such as visitor name, phone name, email address, card number, ID number, host name, host group, host organization (department), appointment arrival time or visit time (60 days before at most), status (unlimited, visitor left, appointment cancelled, access denied, and appointment expiration due to no arrival).

Step 3 Click **Search**.

The results are displayed.

In addition to entering the card number, you can also click , select a card reader and then get the card number by swiping card.

Step 4 Click to view visitor details and card swiping records.

6.5 Parking Lot

You can monitor vehicles that enter and exit the parking lot in real time, view vehicle information, and search for enter and exit vehicles 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 **Select Entrance and Exit.** , select an entrance or exit point, and then click **OK**.

The real-time video of that point will be opened in the window.

Figure 6-39 Monitor entrances and exits

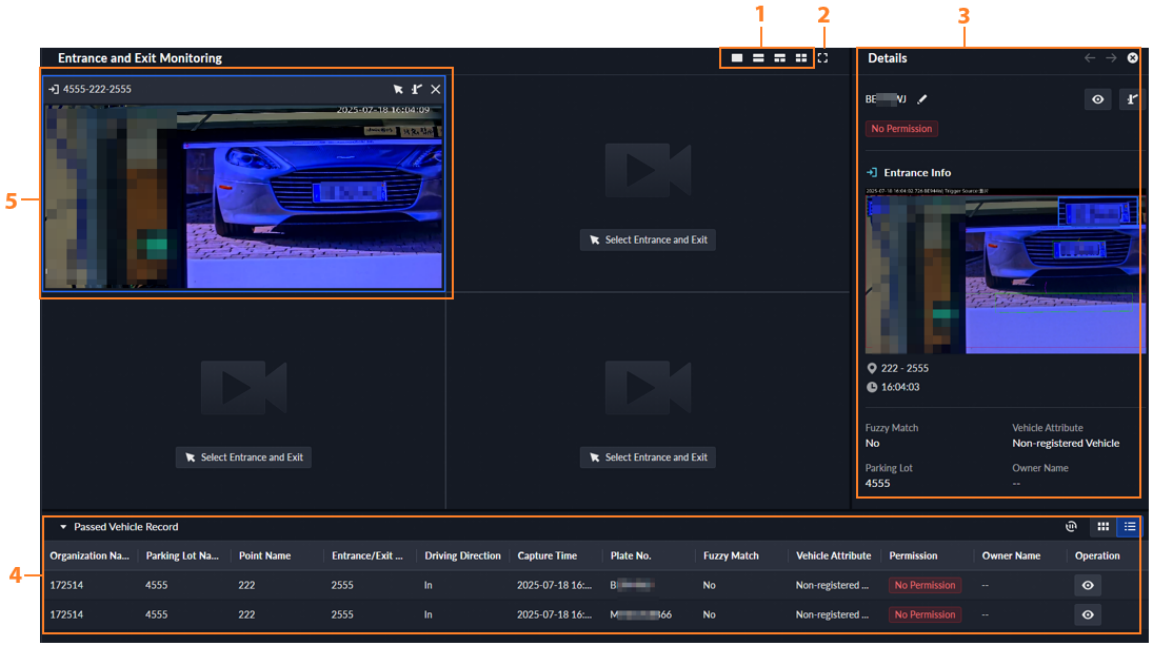


Table 6-15 Page description

No.	Description
1	Select the number of windows you want. Each window can display the real-time video of one entrance or exit point.
2	Full screen mode.
3	Displays records of barriers not opened.
4	Display the vehicle passing records captured by entrance and exit channels that have been opened in the video window.
5	The real-time video of an entrance or exit point. ● Click to open the real-time video of another entrance or exit point in the window. ● Click to open the barrier for vehicles. ◇ **Open without Recording Plate Info** : Open the barrier for vehicles without recording their plate numbers. If you select **Count Parking Spaces** at the same time, the number available parking spaces in the parking lot will decrease or increase depending on whether the vehicles are entering or exiting. This operation will not generate an enter or leave record. You need to enable the parking space counting during configuration, and set the parking space counting mode as count parking spaces by entering and exiting vehicles. ◇ **Open and Record Plate Info** : This is applicable to when the ANPR cameras cannot recognize the number plates. You can manually enter the number plate, and a snapshot will be taken, and then the platform will generate an entrance or exit record.

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 then you can search by vehicle owner, company, person group, and more.

Step 4 Manage the records.

- Click the image, and then a bigger one will be displayed.
- Double-click a record or click , and the detailed information is displayed on the right. Click the icon to view the corresponding detailed information. Click the play icon to play the recorded video, and then click to download it. Click to modify the information of the vehicle, such as the plate number, brand and color.

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

  Click **Snapshot** or **Recording** to view the snapshots or recordings.
- 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, or you can select multiple vehicles, and then click **Force Exit** to record them as exited the parking lot in batches.
- 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.

6.5.2.2 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 then you can search by vehicle owner, company, person group, and more.

Step 4 Manage the records.

- Click the image, and then a bigger one will be displayed.

- Double-click a record or click , and the detailed information is displayed on the right. Click the icon to view the corresponding detailed information. Click the play icon to play the recorded video, and then click to download it. Click to modify the information of the vehicle, such as the plate number, brand and color.

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

  Click **Snapshot** or **Recording** to view the snapshots or recordings.
- 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.

6.5.2.3 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 then you can search by vehicle owner, company, person group, and more.

Step 4 Manage the records.

- Click the image, and then a bigger one will be displayed.
- Double-click a record or click , and the detailed information is displayed on the right. Click the icon to view the corresponding detailed information. Click the play icon to play the recorded video, and then click to download it. Click to modify the information of the vehicle, such as the plate number, brand and color.

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

  Click **Snapshot** or **Recording** to view the snapshots or recordings.
- If a vehicle is inside the parking lot but it is displayed as exited, click to record it as inside the parking lot. When parking space counting by entering and exiting vehicles is enabled for the parking lot, and the vehicle will be counted for available parking space, this operation will subtract an available parking space for the parking lot.
- Export records.

  Select the records to be exported, click **Export** , and then export them according to the on-screen instructions. You can also click **Export**, and then export all records according to the on-screen instructions.
- Click , and then select the items to be displayed.

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 then you can search by vehicle owner, company, person group, and more.

Step 4 Mange records.

- Click the image, and then a bigger one will be displayed.
- Double-click a record or click , and the detailed information is displayed on the right. Click the icon to view the corresponding detailed information. Click the play icon to play the recorded video, and then click to download it. Click to modify the information of the vehicle, such as the plate number, brand and color.

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

  Click **Snapshot** or **Recording** to view the snapshots or recordings.
- 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, number of people in an area, crowd distribution analysis, vehicle density analysis, metadata analysis, and hydrological analysis.

You can click **Intelligent Analysis Config** at the lower left to go to corresponding page and configure the parameters.

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 People Counting

Procedure

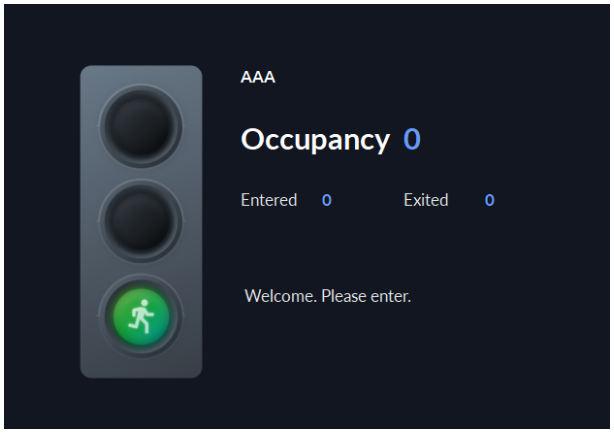
Step 1 Log in to the DSS Client. On the **Home** page, click > **Intelligent Analysis** > > **Real-time People No.**

Step 2 Double-click a group 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 ≥ overlimit threshold.
  - Yellow light: Crowded threshold ≤ occupancy < overlimit threshold.
  - Green light: Occupancy < normal threshold.

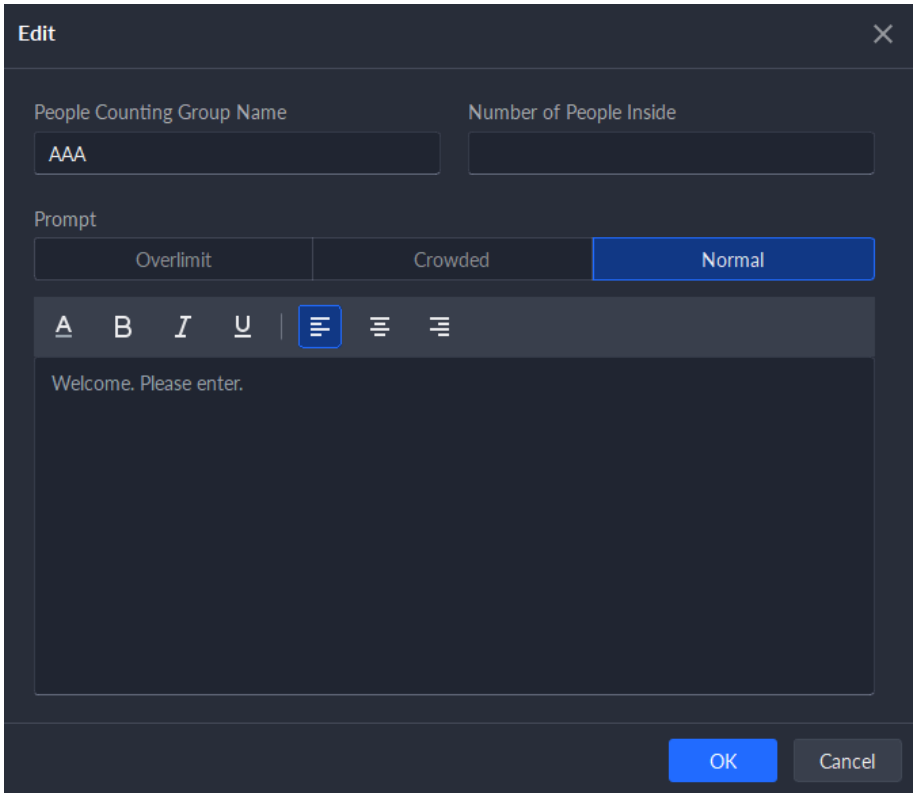
Figure 6-40 Real-time count



Step 3 Hover your mouse on the window displaying real-time data, and then click .

Step 4 Enter a number of people to overwrite the current data, and customize the content to be displayed for green, yellow and red light.

Figure 6-41 Edit the content and data



Step 5 Click **OK**.

6.6.1.2 Historical People Counting

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click > **Intelligent Analysis** > **People Counting** > **Historical People No.**.

Step 2 Select the groups that you want in **Groups** , or select the channels in **Resources**.

Step 3 Configure the search settings, and then click **Search**.

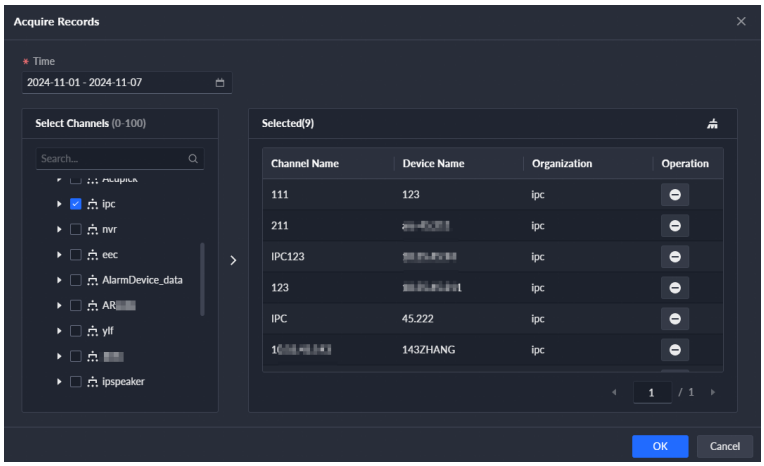
- **Groups** : Groups are people counting groups, which allow you to combine and calculate the people flow data from multiple rules across different devices and channels. You can search for historical people flow data from one or more people counting groups.
- **Resources** : Search for historical people flow data from one or more channels. The data from all the rules of a channel will be included.

If a device is offline, it will upload all the data to the platform when it is online again.

Related Operations

- **Acquire Retention** : Click **Acquire Retention**, and then enter the login password, select the date and channels to acquire the record.

Figure 6-42 Acquire retention



A single extraction task can select up to 100 channels to extract records for 7 days.

- : Change the display format of the data.

Only daily reports displaying the number of retention.

- **Export** : Export the data into a .zip file to your computer.

6.6.2 In-Area People Counting

View statistics on the number of in-area people.

Procedure

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

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

- **Report Time** : You can search for **Daily**, **Weekly** or **Monthly** reports.
- **Stay Duration** : The duration that the people stay in the area. You can select from 5 seconds, 30 seconds, 60 seconds or custom. After you select the duration, for example 60 seconds, the list displays the people stay less than 60 seconds and not less than 60 seconds in different colors.

- Custom stay duration can be configured from 0 to 1800 seconds or 0 to 30 minutes.
- If a device is offline, it will upload data within the past 24 hours to the platform when it is online again.

Related Operations

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

6.6.3 Crowd Distribution Analysis

View the statistics of crowd distribution by groups or resources, and export reports to local computer.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select > **Intelligent Analysis** > **Crowd Distribution Analysis**.

Step 2 Click **Groups** or **Resources**, and then select the crowd distribution groups or resources respectively.

Step 3 Select the report type (daily, weekly, monthly, or yearly), and then select the time.

Step 4 Click **Search**.

Related Operations

- : Change the display format of the data.
- **Export** : Export the data to your computer.
- Select **Display Value**, and then the specific values will be displayed on the bar chart or line chart.
- Configure search conditions such as gender and age to filter search results.

6.6.4 Vehicle Density Analysis

View the statistics of vehicle density by groups or resources, and export reports to local computer.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select > **Intelligent Analysis** > **Vehicle Density Analysis**.

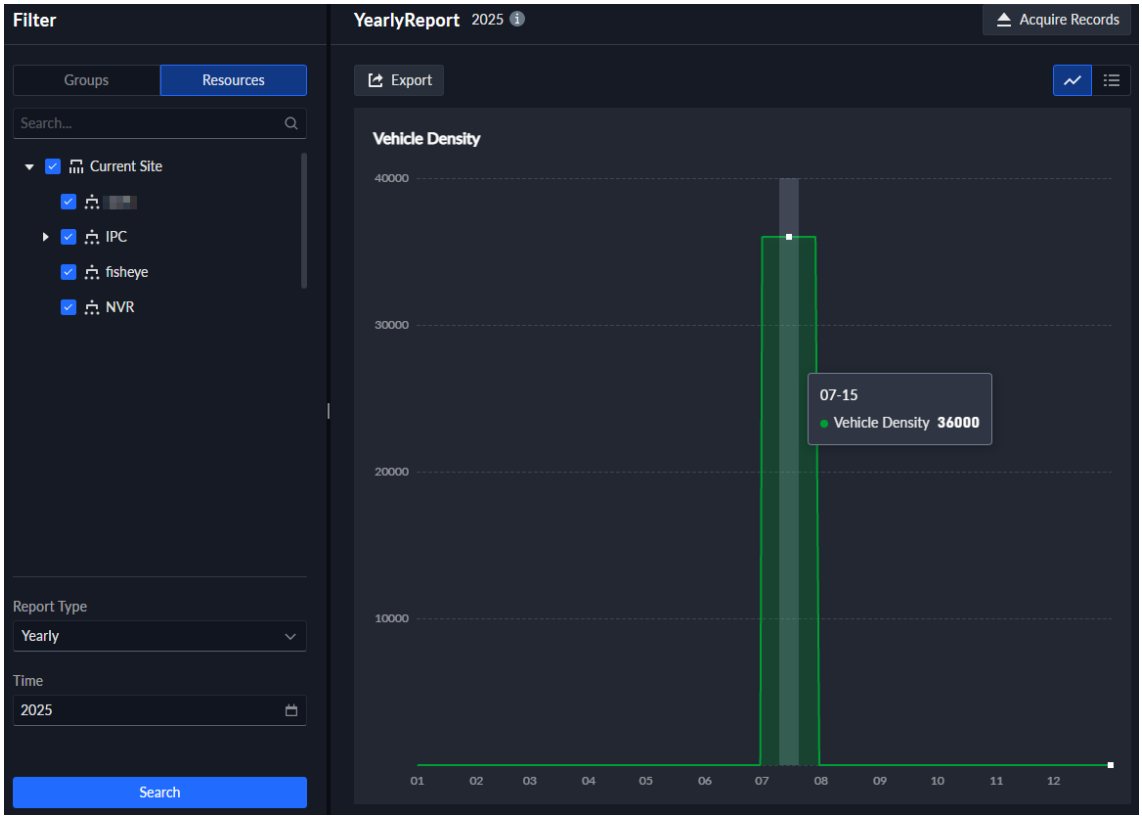
Step 2 Click **Groups** or **Resources**, and then select the vehicle density groups or resources respectively.

Step 3 Select the report type (daily, weekly, monthly, or yearly), and then select the time.

Step 4 Click **Search**.

Hover over the chart, and then you can view the data of the specific day.

Figure 6-43 Vehicle density analysis



Related Operations

- : Change the display format of the data.
- **Export** : Export the data to your computer in .zip format.

6.6.5 Metadata Analysis

View the statistics of faces, human body, motor vehicles, and non-motor vehicles based on channels and export reports to local computer.

Procedure

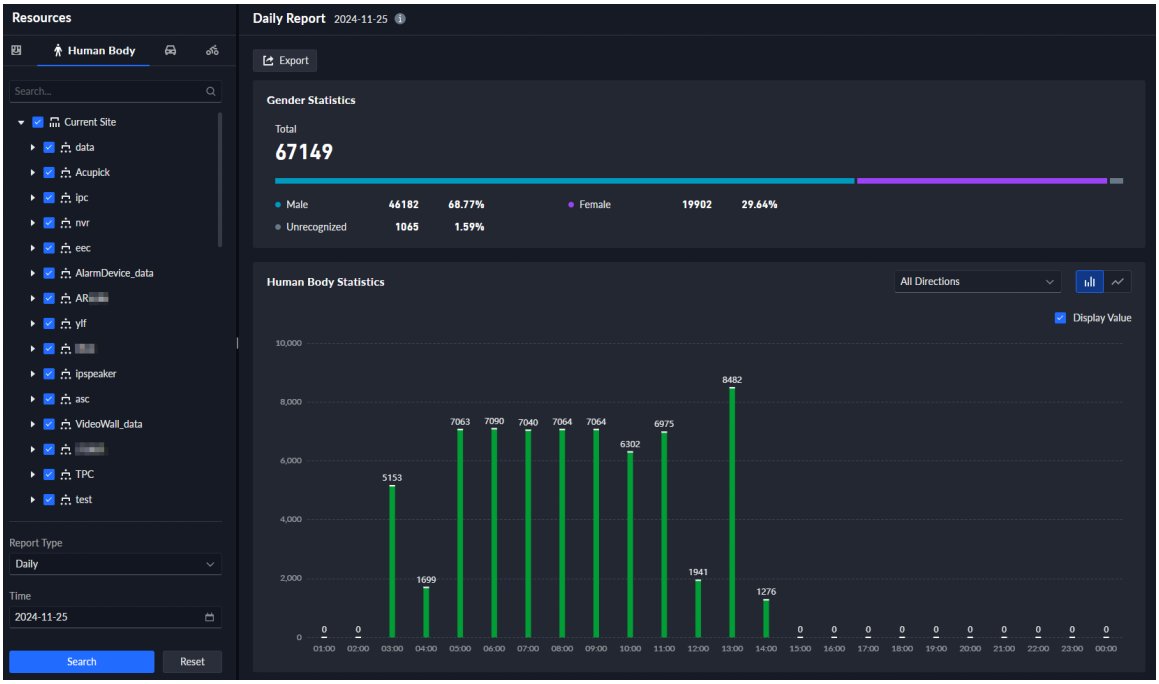
Step 1 Log in to the DSS Client. On the **Home** page, click > **Intelligent Analysis** > .

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

- Object: It is **Face** by default, and you can select **Human Body**, **Motor Vehicles** or **Non-motor Vehicle**.
- **Report Type** : You can search for **Daily**, **Weekly**, **Monthly**, **Yearly** or **Custom** reports.

Custom search time can be configured for a maximum of 31 days.

Figure 6-44 Metadata statistics



Related Operations

- : Change the display format of the data.
- **Export** : Export the data to your computer.
- Select **Display Value**, and then the specific values will be displayed on the bar chart or line chart.
- Configure search conditions such as gender and age to filter search results.

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** to generate a report, and then click **Export** to export the information on the page to your computer.

- Click **Workstation** to view the overall running status of the platform, including the status of devices on main and sub servers, alert statistics, storage and status of servers. The data is refreshed every 5 minutes.
- Select **Resource Monitoring** > **Server Status**, and then click a server or service to view its running status and history information, including alerts occurred in the last 7

days and logs generated on the current day. Click **View All** to go to corresponding pages for more information.

- Device Status

  Select **Resource Monitoring** > **Device Status** > **Real-Time Status**. It displays the total number of devices, online devices, and more. The devices in online (asleep) status are counted as online devices. Click a device type, and then the status of all the devices is displayed on the right. Click to view detailed information.

  - **Channel Status Info** : Information such as the channel name, online or offline, video integrity status, and recording days.
  - **Hard Disk Status Info** : If it is a storage device, you can view the information of its hard disks in this section.
  - **Battery Charge Statistics** : If it is a 4G device with battery, you can view the information of the battery charge statistics.
  - **Disk Storage Records** : If it is an NVR device, you can view the storage records of the device. It displays **Start Time** and **End Time** by the device time.
  - **History Info** : Displays alerts occurred in the past 7 days and logs of the current day. Click **View All** to view all information.
  - Information on alarm controller peripherals: Displays name, serial number, type, program version, online status, and more of the peripherals.

  Select **Resource Monitoring** > **Device Status** > **History Online and Offline Status**. Configure search conditions to search for history online and offline status of the device.

  Supports searching for details for devices by organization.

- Channel Status

  Select **Resource Monitoring** > **Channel Status** > **All Channels**. The channel information and status are displayed.

  Select **Resource Monitoring** > **Channel Status** > **Video Channel**. The channel information and status are displayed. Click corresponding to a channel to view detailed information.

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. In the filter conditions, set **Encoder** as the resource type, and then select **Battery Fault** as the alert type. The corresponding alert details will display specific alert type, battery status, and more.
- 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.

6.7.2.3 Updating Device Program

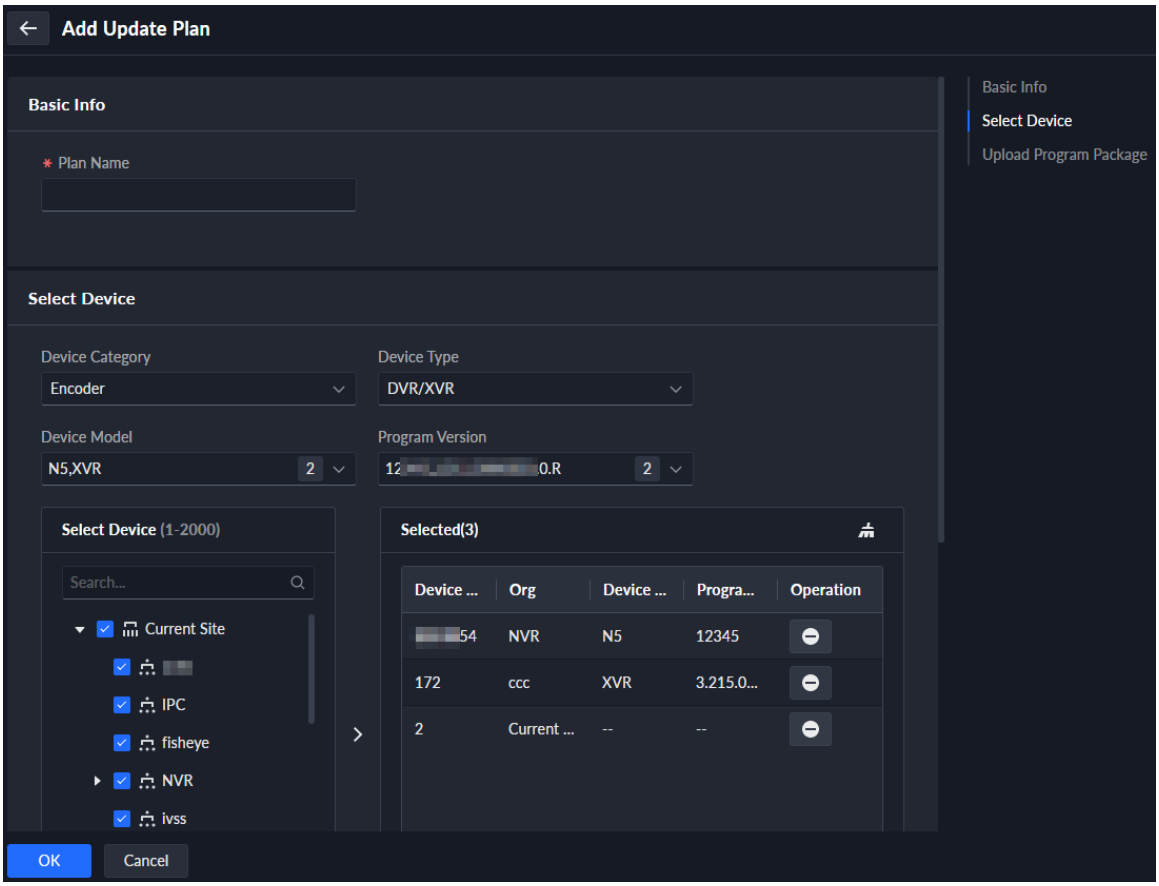
Add a plan to update the programs of selected devices in batches.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Maintenance Center** > **Maintenance Management** > **Device Update** > **Device Update**.

Step 2 Click **Add**.

Figure 6-45 Add an update plan



Step 3 Enter a name for the plan, and then select the device category, type, model, and program version.

The platform will only display corresponding devices.

Step 4 Select the devices you want to update.

Click to cancel selecting all devices.

Step 5 Configure when to update the devices.

- **Now** : Update the devices immediately after the plan is added.
- **Custom** : Update the devices at the defined time.

Step 6 Click **Upload File** to upload the update program.

- Make sure that the uploaded program matches the models and current program versions of selected devices.

- Make sure that the network is stable and the power properly connected for all devices. Otherwise, they might not work properly.

Step 7 Click **OK**.

Related Operations

In the list of update plans, you can view the information of each plan, including name, update program, update start time, and update status.

- Click to delete a plan one by one; select multiple plans, and then click **Delete** to delete them in batches.
- Click to view the update status of the devices in a plan.
  - Click to remove a device from the plan; select multiple devices, click **Delete** to remove them in batches.
  - If one or more devices failed to update, click to update a device again one by one, or select multiple devices, and then click **Update Again** to update them in batches.

7 General Application

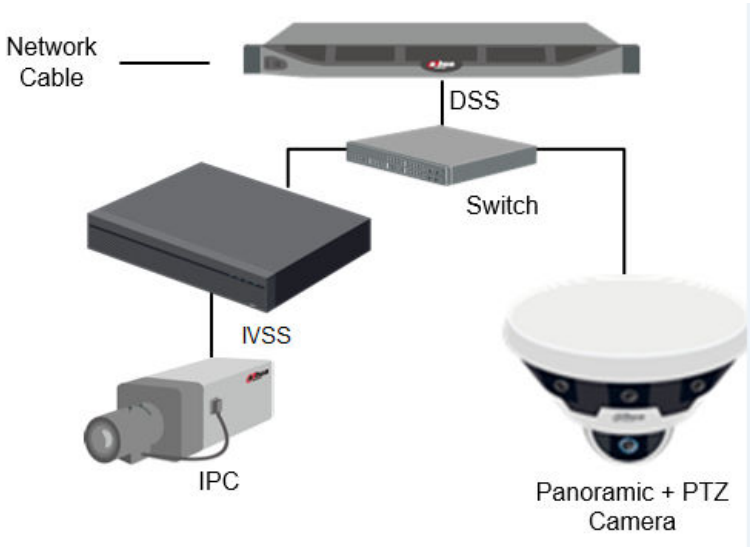
7.1 Target Detection

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, analyze people, motor and non-motor vehicles.
- IVSS manages cameras and analyzes people, and motor and non-motor vehicles.
- The platform centrally manages IVSS and cameras, receives analysis results from cameras and displays the reports.

7.1.2 Preparations

Make sure that the following preparations have been completed:

- Cameras and IVSS are correctly deployed, and video metadata is enabled on them. For details, see corresponding user manuals.
- Basic configurations of the platform have been finished. To configure the parameters, see "4 Basic Configurations".
  - When adding a camera or IVSS, select **Encoder** for device category.
  - After adding the camera or IVSS to the platform, select **Metadata Attribute Report Capability** 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** > **Monitoring**.

Step 2 Select a window, and then double-click the channel.

You can view the live video. If people, motor vehicles, or non-motor vehicles are detected, captured images will be displayed in the upper-right corner of the window.

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 **Target Search**.

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.

- Automatic number plate recognition

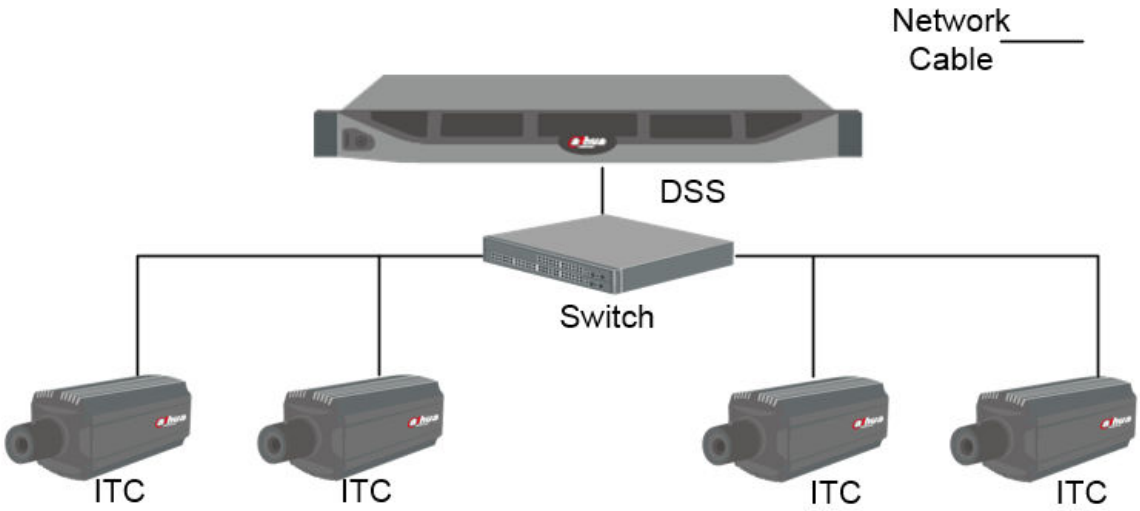
  The platform displays vehicle snapshots and ANPR results in real time.
- Vehicle records

  Search for vehicle records according to the filtering conditions that 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 7-2 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 manuals.
- Basic configurations of the platform have been finished. To configure, see "4 Basic Configurations".
  - ◇ When adding an ITC camera, select **ANPR Device** for device category, and then select **ANPR Device** for **Device Type**.
  - ◇ ANPR snapshots are only stored in the **Images and Files** disk. On the **Storage** page, configure at least one **Images and Files** disk. Otherwise vehicle images 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** > **Monitoring**.

Step 2 Select a window, and then double-click the channel.

You can view the live video. If vehicles are detected, captured images are displayed in the upper-right corner of the window.

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 **Target Search**.

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

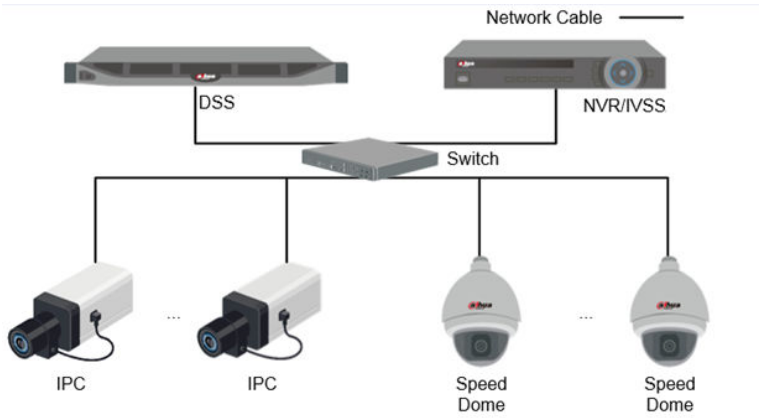
Configure face recognition settings on the device and the platform before you can view face recognition results on the platform.

7.3.1 Typical Topology

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

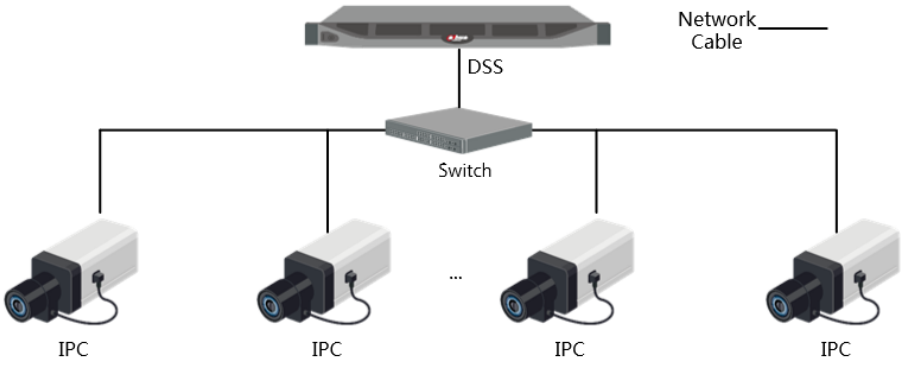
- Face recognition by NVR/IVSS

Figure 7-3 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 7-4 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 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 the face arming 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** > **Monitoring**.

Step 2 Select a window, and then double-click the channel.

You can view the live video. If faces are detected, captured images are displayed in the upper-right corner of the window.

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 **Target Search**.

Step 3 Configure the search conditions.

You can search for snapshots in the **Record** or **Person** section. For details, see "6.3.1 Searching for People".

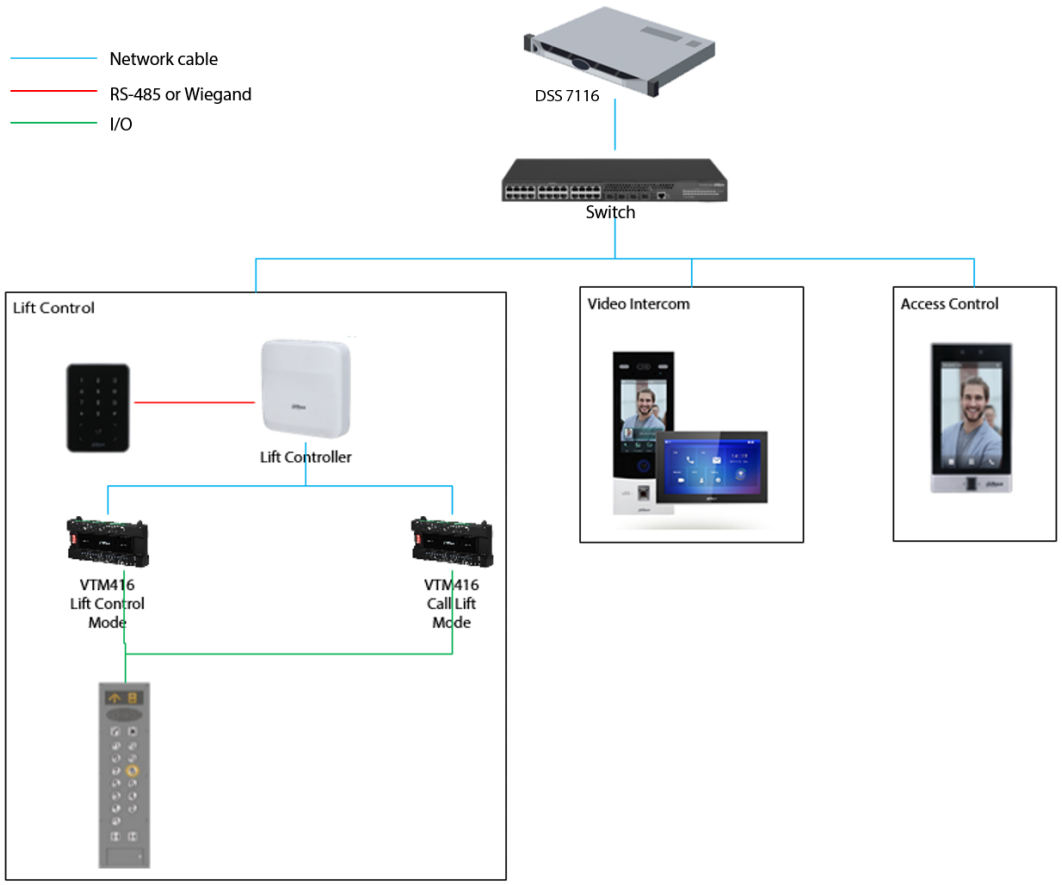
7.4 Lift Control

There are mainly 2 scenarios.

- Authorized access: After granting access permissions of corresponding floors to people, the person can go into the lift by card swiping, fingerprints, passwords, or more, and reach the floors with access permissions. For example, residents can only reach the floors they have access permissions, so as not to affect residents on other floors.
- Visitors call the lift on VTO (you need to configure visitors' VTO access permissions and floor access permissions in advance).
  - ◇ After the homeowner agrees the access on VTH or OnePass App, the visitor can reach the floor where the homeowner is located.
  - ◇ After receiving the lift call, the platform administrator grants permissions of the specified floor to the visitor, who can then go to that floor.

7.4.1 Typical Topology

Figure 7-5 Typical topology



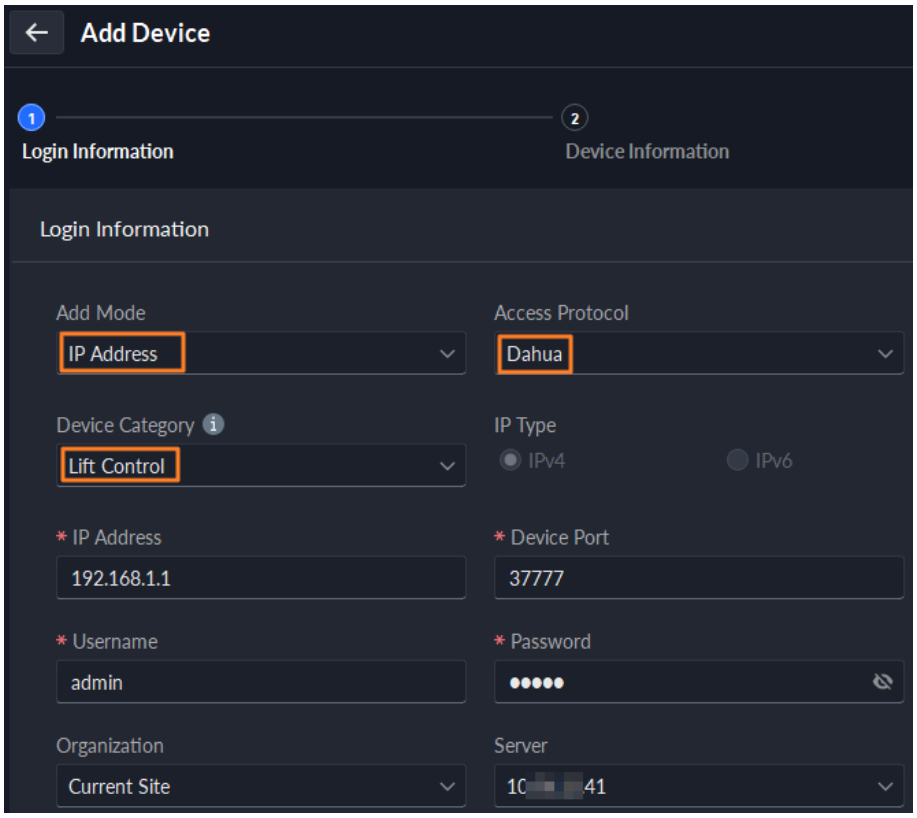
- Lift control module and lift controller: Installed on top of the elevator car or at the top of the hoistway. Connect the lift control modules to the lift controller, to manage the running of the lift.
- Card reader: Connect it to the lift controller through RS-485 or Wiegand, and supports card swiping, QR code, face recognition, and more.
- Video intercom: Visitors call VTH (indoor monitor) on the VTO (door station), and after the owner confirms, the lift comes to the floor where VTO is located.
- Access control: When people go into the lift through card swiping, fingerprint, and password on the access controller, the person can reach the floor with access permissions.
- DSS: Add and manage people, floor, lift control channels, and other information, and control the permissions.

7.4.2 Preparations

- You have installed the video intercom devices and lift control devices. For details, see device user manuals.
- You have linked the video intercom device to the lift controller on the lift controller webpage. For details, see lift controller user manual.
- You have added the video intercom devices and lift controller to the DSS platform.

◇ When adding lift controller on the **Device** page, select **IP Address** or **Domain Name** from **Add Mode**, **Dahua** from **Access Protocol**, and **Lift Control** from **Device Category**,

Figure 7-6 Add lift controller



◇ When adding video intercom devices on the **Device** page, select **Video Intercom** from **Device Category**.

- Edit the floor name, which supports letters and numbers.

Figure 7-7 Select lift controller

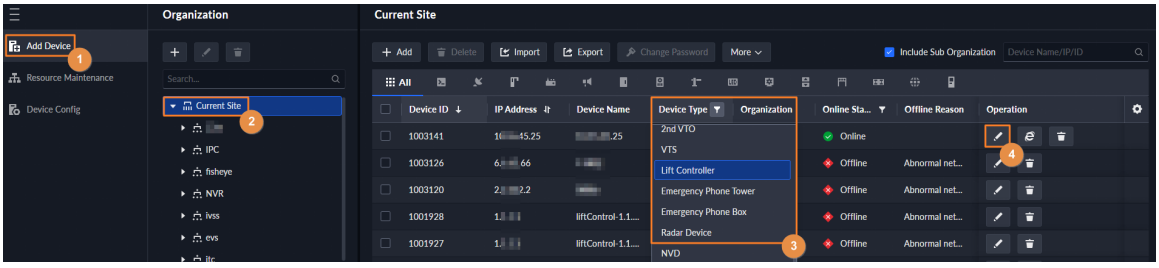
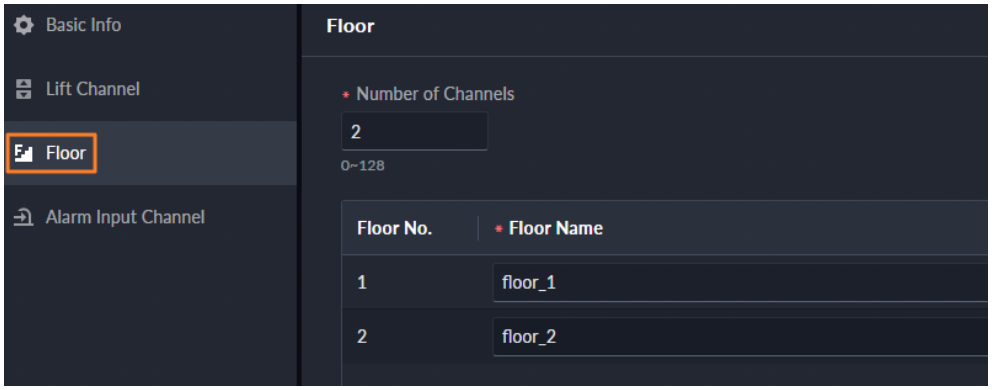


Figure 7-8 Edit floor



7.4.3 Lift Controller Maintenance

7.4.3.1 Configuring Alert Rule

Configure alert rules to monitor the lift controllers so that you can handle exceptions (if any) timely.

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

Step 2 Click .

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

Figure 7-9 Configure lift control alert rules

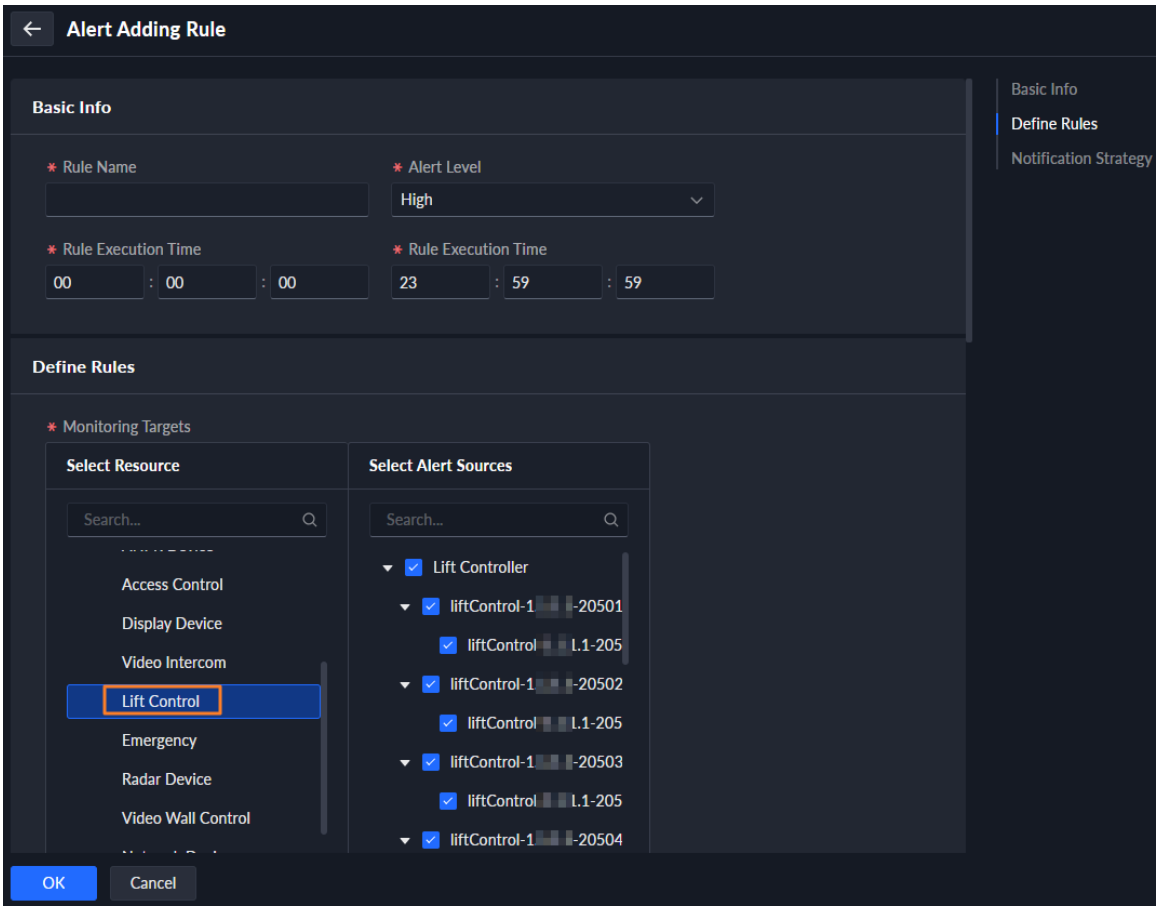


Table 7-1 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule. It can be up to 50 characters.
Alert Level	Select a level for the alert. This is used to quickly know the urgency of the alert when it is triggered.
Rule Execution Time	The alert will only be triggered within the defined period.
Monitoring Targets	Targets include servers and devices. Select **Lift Control** from **Device**.
Rule Conditions	Set the threshold for device disconnection. When the value is greater than or equal to the threshold, the alert will be triggered.
Push Notifications	After enabled, you can select the users who will receive notifications when the lift controller is disconnected.
Email Notification	After enabled, you can customize the content to be sent to specified email addresses. You can configure the email addresses in the following ways: ● Click to select the email addresses of users. ● Manually enter an email address, and then press Enter.

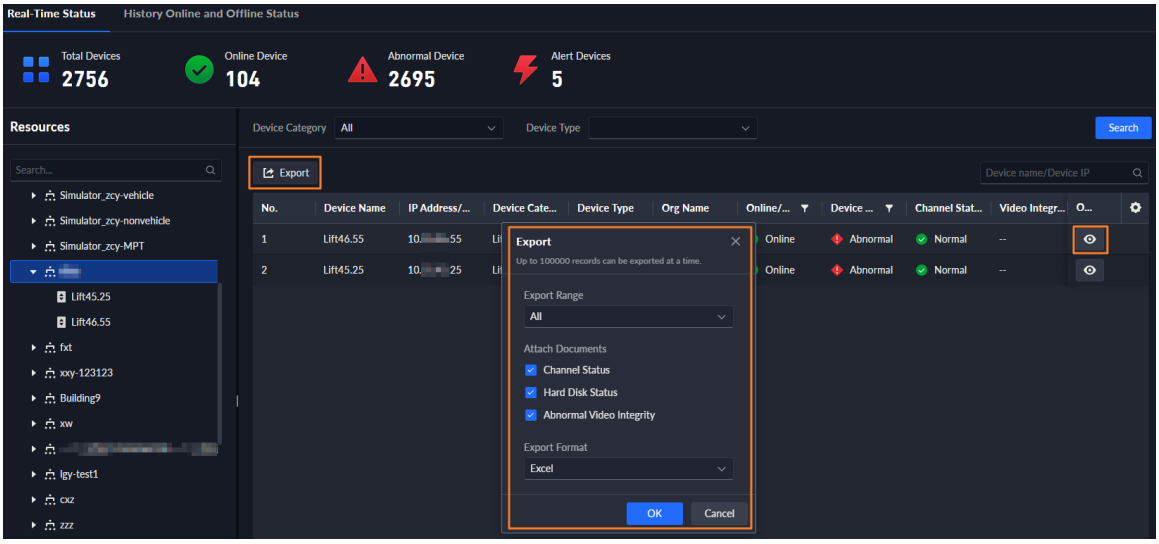
7.4.3.2 Viewing Lift Controller Status

Step 1 Log in to the DSS Client. On the **Home** page, select > **Maintenance Center**.

Step 2 Select **Resource Monitoring** > **Device Status**, select the lift controller from the resource tree, and then you can view the online status, device status, and channel status of the lift controller on the right. Click to view device details.

Click **Export**, and then you can export the records according to your settings to local.

Figure 7-10 View device status



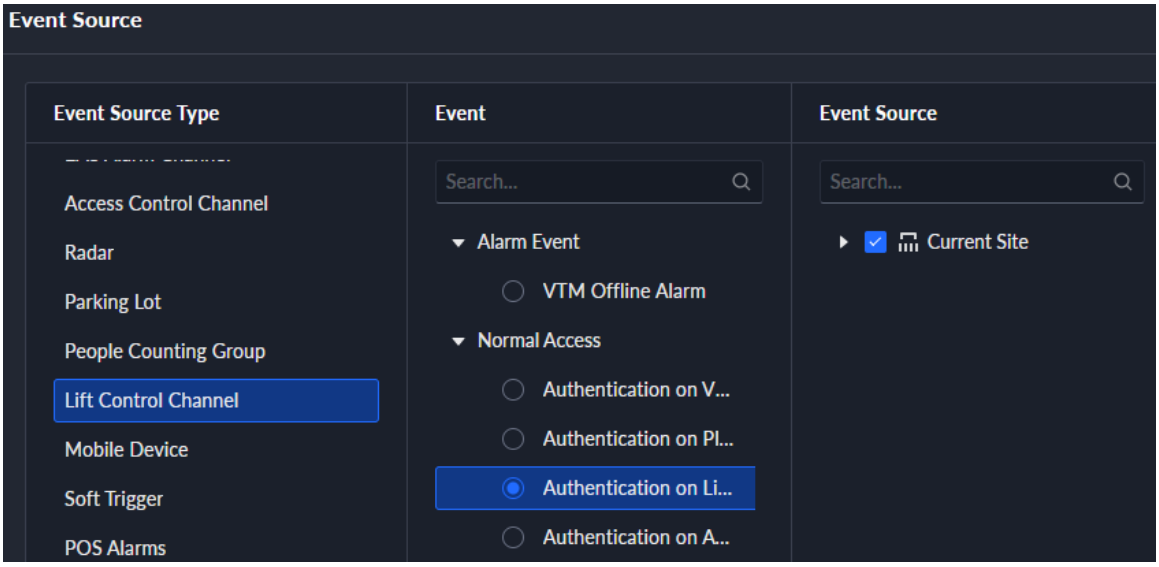
7.4.4 Configuring Event

Go to > **Event** > **Event Config**, select **Lift Control Channel** from event source type, and then set the event, event source, and event linkage, such as taking snapshots and recording videos.

For details on configuring events, see "5.1.1 Configuring Event Linkage".

When people pass through after authentication on VTO, platform, lift controller, or access control device, the corresponding linkage action will be triggered.

Figure 7-11 Select lift control



7.4.5 Authorized Access

7.4.5.1 Adding a Person

For lift control, you need to configure the following information of a person:

- Basic information, including name, photo, and more.
- Credentials, such as passwords, cards, fingerprints, for access.
- Access control information, which is for configuring person access permissions.

  You need to select **Lift** from access point type.
- Video intercom information, including room number and person identity (homeowner and app user).

  When selecting **App User**, and entering the person email address. The system automatically creates a OnePass App account for the person. If a visitor comes, the person can remotely authorize the visitor on OnePass App, so that the visitor can access the floor where the person is located.

For details of adding people, see "5.3.2.2 Adding a Person".

7.4.5.2 Configuring Access Rules

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

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

Step 2 Click **Add**, and then configure the parameters.

Figure 7-12 Add an access rule

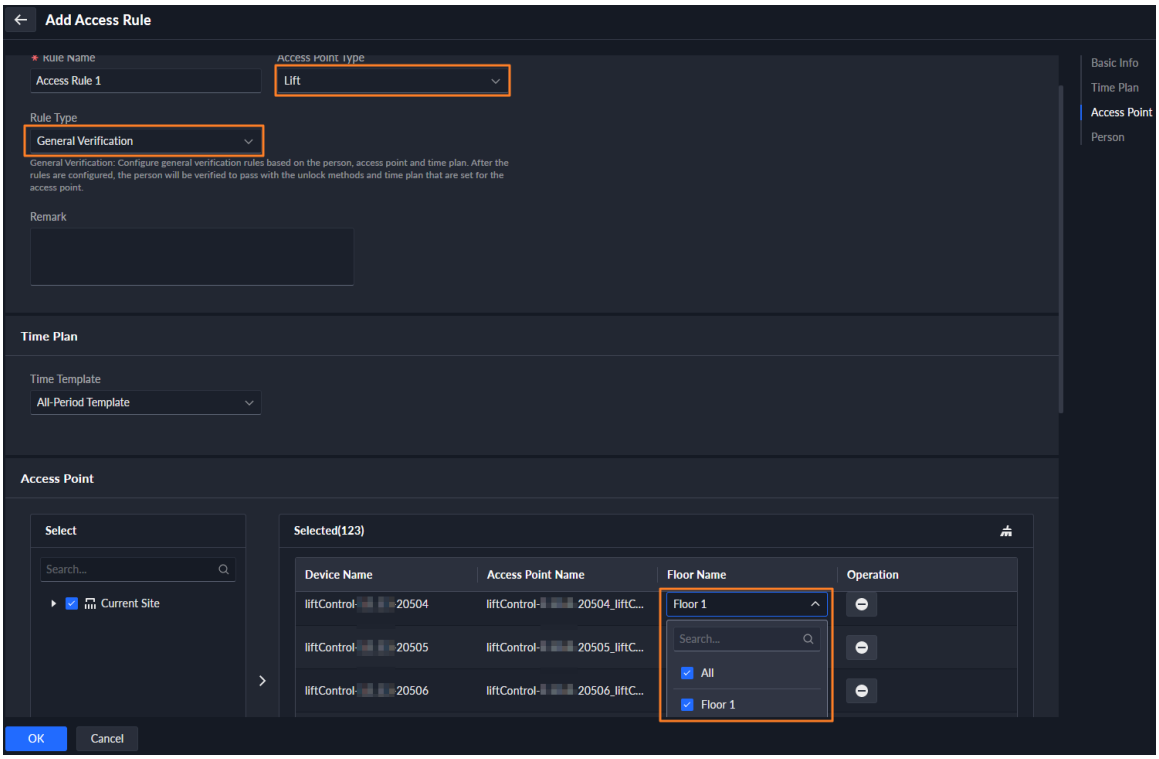


Table 7-2 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Select **Lift**, and then the platform will only display corresponding channels.
Rule Type	Select **General Verification**.
Time Template	Select when this rule is effective. If you want to create a new time template, see "4.2.7 Adding Time Template".
Access Point	Select the access point to which the access rule applies, and then select floors. The selected people will have access to the floors selected here.

Parameter	Description
Person	• **Select by Person Group** : Select one or more person groups, and then all the persons in the groups will have permissions to access the selected access points. Select **Link Sub Node**, and then you can select a zone and all its sub zones at the same time. • **Select by Person** : Select one or more persons, and then they will have permissions to access the selected access points. Select **Include Sub Groups** to display all the persons in the selected group and its sub groups.

Step 3 Click **OK**.

7.4.5.3 Controlling Lift Control Channels

Set all lift channels in a zone to no authentication, authentication, and lock modes.

Step 1 Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Access Control** > **Access Control Panel**.

Step 2 Select a zone, and then click **Authentication Mode**, and then people must verify their identifications to go to specified floors.

When selecting **No Authentication Mode** , all people can go to any floor without verifying their identifications; when selecting **Lock Mode**, no person is allowed to use lifts.

7.4.5.4 Accessing the Lift

People go into the lift through card swiping, fingerprints, passwords, and more, and then they can reach the floors they have access to.

7.4.6 Calling Lift on VTO

When a visitor calls the lift on VTO, the visitor can reach the floor where the homeowner is after remote authorization by the homeowner or the platform administrator.

Procedure

Step 1 Add the visitor to the platform. For details, see "7.4.5.1 Adding a Person".

Step 2 Configure the access rules for the visitor. For details, see "7.4.5.2 Configuring Access Rules".

Step 3 Configure the door access rules for the visitor.

1. Click , and then in the **App Config** area, select **Access Control** > **Access Rule** > **All Rules**.
2. Click **Add**, and then configure the parameters.

Table 7-3 Access rule parameters

Parameter	Description
Rule Name	The name that identifies the rule.
Access Point Type	Select **Door**.
Rule Type	Select **General Verification**.
Access Point	Select the access control device to which this access rule applies by zone or by access point.
Person	• **Select by Person Group** : Select one or more person groups, and then all the persons in the groups will have permissions to access the selected access points. Select **Link Sub Node**, and then you can select a zone and all its sub zones at the same time. • **Select by Person** : Select one or more persons, and then they will have permissions to access the selected access points. Select **Include Sub Groups** to display all the persons in the selected group and its sub groups.

3. Click **OK**.

Step 4 The platform administrator configures call groups, management groups, and relationship groups to enable calls within specific groups.

Results

After the visitor calls the lift on VTO:

- After the homeowner remotely agrees the access on VTH or OnePass App, the visitor can reach the floor where the homeowner is.
- The platform administrator grants the designated floor permissions of the homeowner to the visitor on the platform, and then the visitor can reach the floor where the homeowner is.

7.4.7 Viewing Access Records

You can view and export access events for specified zones, person groups, and time.

Step 1 Log in to the client. On the **Home** page, select > **Access Management** > **Access Control** > **Access Records** > **Event Record**.

The number of each type of access events in all zones is displayed at the top of the page by default.

Step 2 Set search conditions, such as zone, time, person group, person, ID, access point, company, and department, and then click **Search** to view the specified access events.

Step 3 (Optional) Click **Export**.

Step 4 (Optional) Enter the login password and the encryption password of the export file, select whether to export images, set the export range and the export fields, and then click **OK**.

You can also configure not to verify the login password and set the encryption password. For details, see "8.3.2 Configuring Security Parameters".

8 System Configurations

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

8.1 Distributed Deployment

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

Procedure

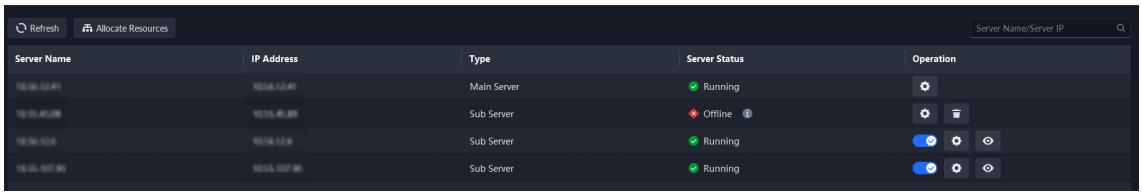
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Deployment**.

Step 2 Click **Distributed Config**.

Step 3 Manage servers.

- Click to view server details.
- Click corresponding to a server to define the server type. A server can be set to sub server or standby server when it is not in use.
- Click to enable the server. means the server is enabled.
- Click to delete the server.

Figure 8-1 Servers



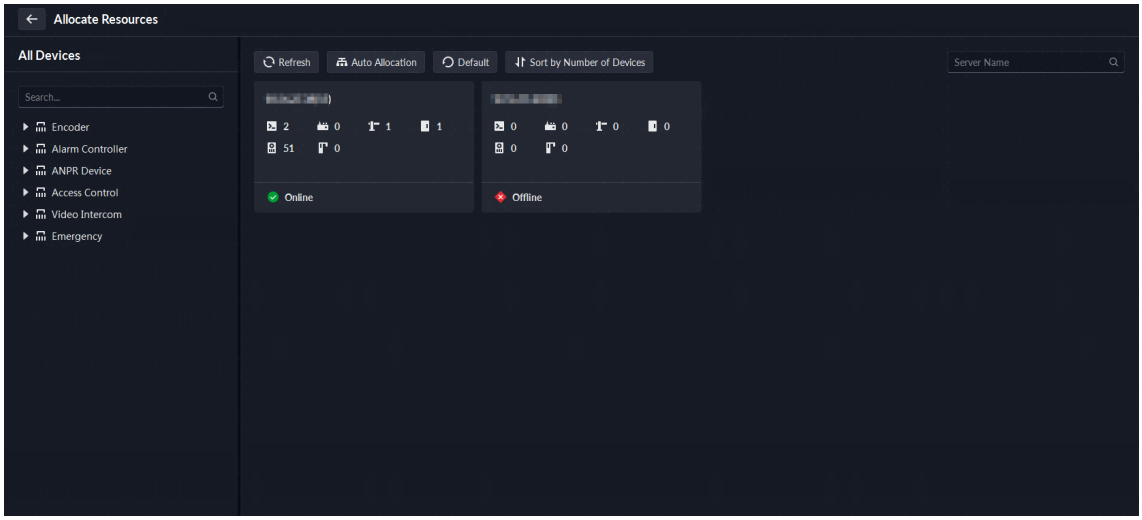
Step 4 Click **Allocate Resources** to assign devices to different servers.

- Manually

  Select devices or channels on the left side, and then drag them to the server on the right. The number of corresponding devices in the target server increases, and the devices in the original server reduces.

  ◇ Click **Default**, the servers are sorted in the order in which they were added.
  ◇ Click **Sort by Number of Devices**, the servers will be sorted by the number of devices.

Figure 8-2 Resource allocation

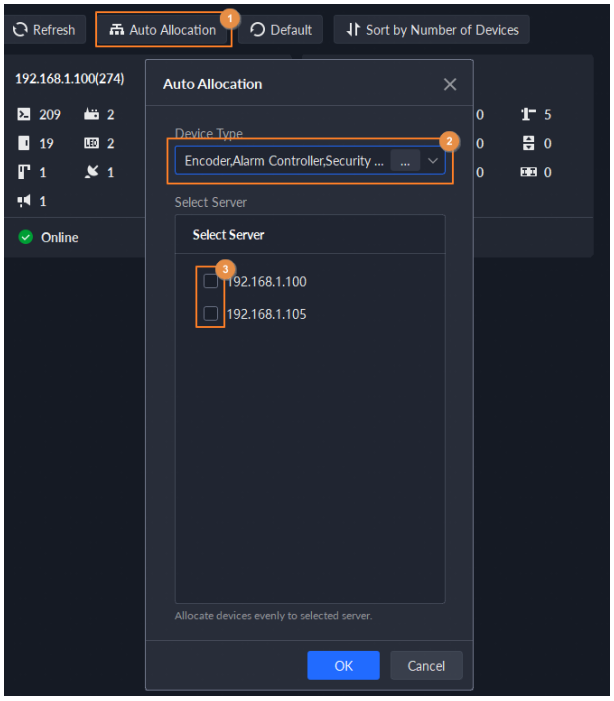


- Automatic allocation

  Allocate the same type of devices evenly to different servers.

  1. Click **Auto Allocation**.
  2. Select device type. Multiple types are supported.
  3. Select the server to which the devices belong. Multiple servers can be selected.
  4. Click **OK**.

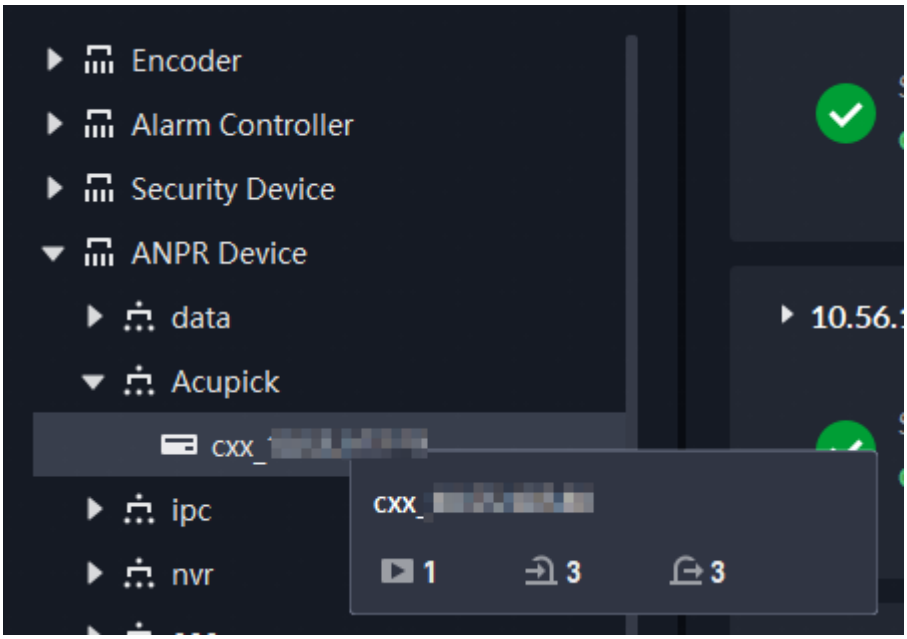
Figure 8-3 Auto allocation



Related Operations

When hovering the mouse over the device, the device name, channel type, and the number of the device will be displayed.

Figure 8-4 Information display



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.

- Click to view the corresponding instructions.
- Click to copy the activation code and serial number.
- Click **Export** to export the hardware information in .zip format.

8.3 System Parameters

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

8.3.1 Configuring General Parameters

You can set the date and number formats based on your country or region. The settings will take effect after you open the page again or log in to the client again.

Procedure

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

Step 2 Click **General**.

Step 3 Select the date and number formats based on your country or region.

Step 4 Click **Save**.

8.3.2 Configuring Security Parameters

Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters** > **Security Config**, and then configure the parameters.

Table 8-1 Parameter description

Parameter	Description
Certificate Management	A CA certificate is used to validate the legitimacy of the platform. When accessing the platform through a browser, the browser will validate the certificate. If the certificate is installed in the browser, the browser will consider the platform as secure, and will grant it access. If the certificate is not installed in the browser, the browser will not consider the platform as secure, and will not grant it access. You can create, import, and download certificates on the platform. Supports installing the certificate in the following methods. ● 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.
Two-Factor Authentication	After enabling two-factor authentication, you can combine password authentication with email, Microsoft Authenticator, or Google Authenticator to improve your account security. You need to enable **Two-Factor Authentication** when adding or editing a user from > **User** > **Role Users** > **User Management**.
File Security Policies	Protect your data by verifying login password when download or export information, and encrypting the export files. ● **File Export or Download Password Authentication** : ◇ You need to enter the password of the current account to export or download files. ◇ For all users that log in to the platform, they do not need to enter the password when exporting or downloading files. ● **File Export and Download Encryption** : You need to set an encryption password for files to be exported or downloaded. When anyone uses the files, they need to verify the encryption password.

Parameter	Description
Watermark Management	You can configure watermarks for viewing live videos, playing back recorded videos, and downloading videos. Set the watermark content, font size and color, transparency, line spacing, application scope, and then click **Save**. The settings take effect immediately. • This function is only available on the client. You cannot add watermarks to videos or webpages that are called by third-party systems, or snapshots (such as vehicle snapshots). • The client needs to transcode the downloaded video to add the watermark, which will increase the time when downloading the video.
HTTP Allowlist	After the firewall of the server is enabled, you need to add the IP address of the computer where the DSS Client is installed to the HTTP allowlist so that it can access the platform.
RTSP Redirecting Allowlist	After the firewall of the server is enabled, only the IP addresses in the RSTP allowlist can request video stream through the media gateway service. The IP addresses of decoders will be added automatically. If there are other IP addresses that need to request video stream through media gateway service, you need to manually add them to the RSTP allowlist.
Generic Event Allowlist	Click **Add**, and then add the IP address for receiving generic events from third-party system or device to the allowlist. This helps ensure system security.

8.3.3 Configuring Data Records

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

Procedure

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

Step 2 Click **Message Retention Period**.

Step 3 Double-click a number to change its value.

Step 4 Click **Save**.

8.3.4 Time Synchronization

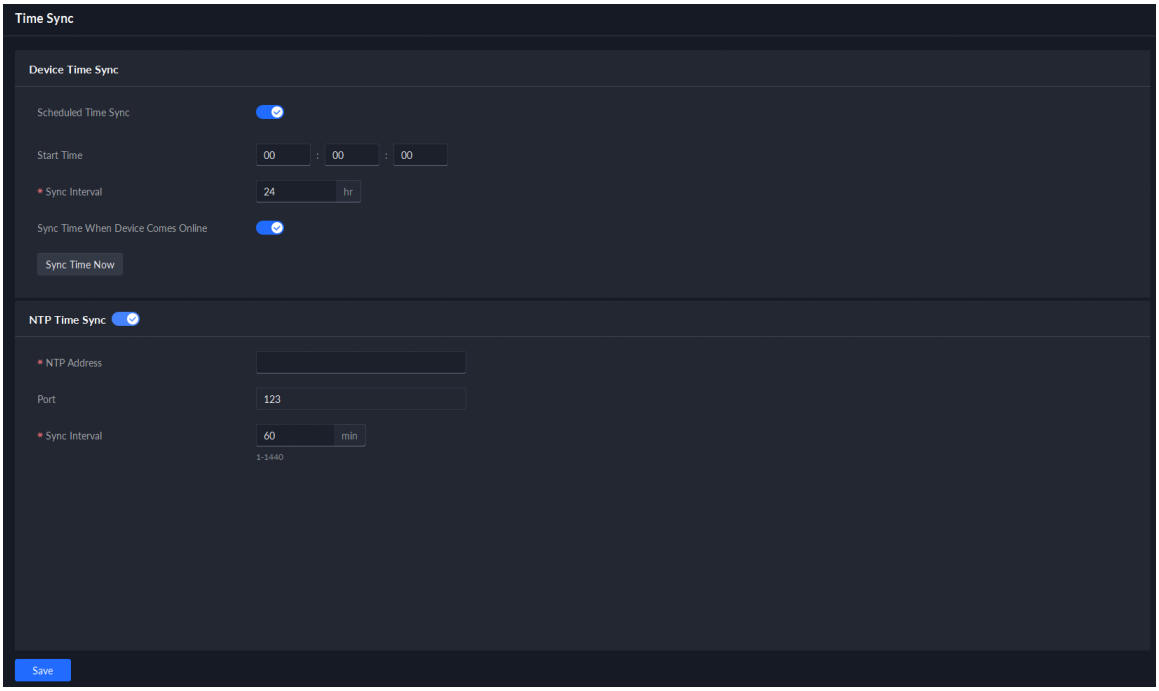
Synchronize the system time of all connected devices, PC client, and the server. Otherwise the system might malfunction. For example, video search might fail. The platform supports synchronizing the time of multiple devices, which have the same time zone as the platform. You can synchronize the time manually or automatically.

Procedure

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

Step 2 Click the **Time Sync** tab, enable the sync methods, and then set parameters.

Figure 8-5 Enable time synchronization



- **Scheduled Time Sync** : Enable the function, enter the start time in time sync for each day, and the interval.
- **Sync Time When Device Comes Online** : Syncs device time when the device goes online.
- **NTP Time Sync** : If there is an NTP server in the system, you can enable this function so that the system can synchronize its time with the NTP server.

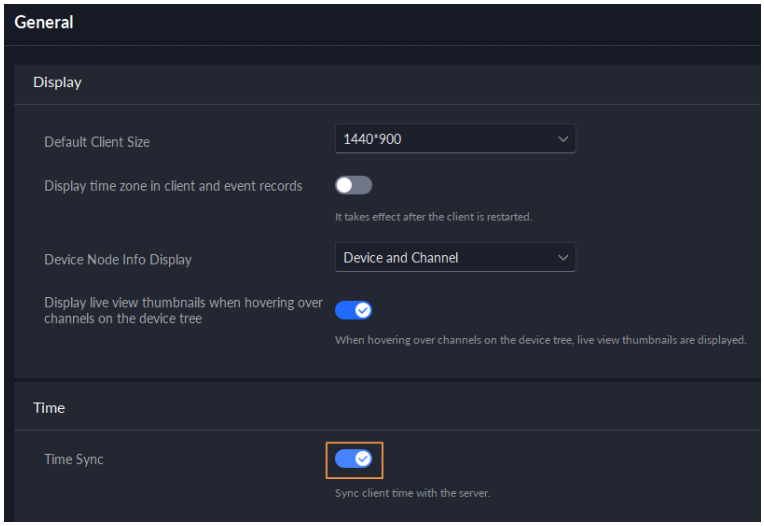
Step 3 Click **Save**.

Step 4 Enable time synchronization on DSS Client.

1. Log in to the DSS Client, and then in the **Management** section, click **Local Settings**.
2. Click the **General** tab, select the check box next to **Time Sync**, and then click **Save**.

The system immediately synchronizes the time after you restart the client to keep the time of the server and the PC client the same.

Figure 8-6 Enable time sync



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

8.3.5 WhatsApp Integration Configuration

Supports API integration with the system to enable automated message sending, configuring template, and more.

Procedure

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

Step 2 Click **WhatsApp Integration Config**.

Step 3 Enable **WhatsApp Integration Config**, and then configure the parameters.

Configure the parameters, including WhatsApp business account ID, phone number, telephone number, application number; If **Modify WhatsApp Authentication Parameters** is enabled, set the application key, verification password and access password. After configuration, users cannot view the application key, verification password, and access password.

View the help document on the interface to learn more about how to set the parameters.

Step 4 Click **Save**.

8.3.6 Configuring Email Server

Procedure

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

Step 2 Click the **Email Server** tab, enable **Email Server**, and then configure parameters as required.

Table 8-2 Description of email server parameters

Parameter	Description
Authentication Mode	The following 2 methods are available for mail server login authentication. ● Username or password: Verify user identity and log in to the mail server using user name and password. Supports Yahoo, Outlook/ Hotmail, Gmail, and custom mail servers. ● OAuth 2.0: Allows authorization for the platform to access the user mailbox without providing a password. When using OAuth 2.0 authentication, only Outlook (default) and Gmail mail service providers are supported. OAuth 2.0 authentication supports API and SMTP protocol types.
Mail Service Provider	
Sender Email Address	The sender displayed when an email is sent from DSS.
SMTP Server	Configure the SMTP server address, password, and port number. ● When selecting the **OAuth 2.0** checkbox, the SMTP server is smtp.office365.com. If it displays the email address is unavailable, you can modify it into smtp-mail.outlook.com. ● This parameter is not required when selecting **OAuth 2.0** authentication mode and **API** protocol type. ● After initial setup, you can click **Change Password** to change the SMTP server password.
Password	
Port	
Encryption Method	Supports no encryption, TLS encryption (default), and SSL encryption.
Email Language	Select the language for the email content. ● Emails sent by the client will use the client language, such as emails sent when forwarding events. ● Emails of the following types will be sent in the configured language: emails linked in **Event Config** , emails triggered by alarm rules in **Maintenance Center**, and immediate emails from the access control and visitor functions in **Access Control**. Pay attention that only default content will be output in the configured language. Any text that is manually entered will be sent in its original form.
Test Recipient	Set the recipient, and then click **Test Email** to test whether the mailbox is available.
Test Email	

Step 3 (Optional) When selecting **OAuth 2.0** mode, you need to perform email authorization.

- Outlook
  1. Get the client ID, and then enter the ID. For details, see **Help Document**.
  2. Click **Get** to get the user authorization code.
  3. Click the authorization URL or scan the QR code to complete the account authorization in 15 minutes. After the authorization is complete, the authorization status will be displayed.

- Gmail

  1. Get the client ID and key, and then enter them. For details, see **Help Document**.
  2. Click **Get Authorization URL**, and then the page will display the authorization link.
  3. Click the authorization URL, and then it will go to the browser for account authorization. After the authorization is complete, the authorization status will be displayed.

Step 4 Click **Save**.

8.3.7 Configuring FTP Server

FTPS is used for remote backup and IP speakers. The system supports built-in FTPS and independent FTPS. You need to enable and configure the FTP server before you can use the function.

Procedure

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

Step 2 Click the **FTP Server Config** tab, and then enable **FTP Server Config** as needed (leave it disabled if you are not using FTPS-related services).

Step 3 Select FTPS type from **Built-In FTPS** or **Independent FTPS**.

- It is built-in FTPS by default. When you switch to an independent FTP server, you need to manually migrating historical data to the external independent server.
- For an independent FTPS, you need to configure FTP server IP address, port, user name, and then click **Change Password** to set the password.

  After configuration, you can click **Test** to test whether the FTP server connection is successful.

Step 4 Click **Save**.

8.3.8 Configuring Active Directory

Before importing domain users, syncing deleted domain users, syncing added domain users, or performing other operations related to domain users according to "4.3 Adding Roles and Users", you need to configure domain, including domain name/IP, port, user name and password.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameter** > **Active Directory**.

Step 2 Click to enable the function, and then configure the parameters of the domain, including SSL private key, domain name/IP, port, username and password.

Click **Change Password** to change the domain password.

Step 3 Click **Get DN** to automatically get the basic DN information.

Step 4 Click **Test** to check whether the domain information is correct.

Step 5 Enable the automatic synchronization function and set a time. The platform will automatically synchronize new users in user groups that you have imported previously, and update the information of the users imported by manual selection at the defined time every day.

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

Step 6 Click **Save**.

8.3.9 Configuring 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 (Optional) Enable or disable the P2P function.

If disabled, you cannot add devices to the platform through P2P.

Step 4 Enable the **Device Info Retrieval Timeout**, and then set the timeout limit.

Step 5 Click **Save**.

8.3.10 Remote Logs

To ensure safe use of the platform, the system sends administrator and operator logs to the log server for backup at 3 am every day.

Procedure

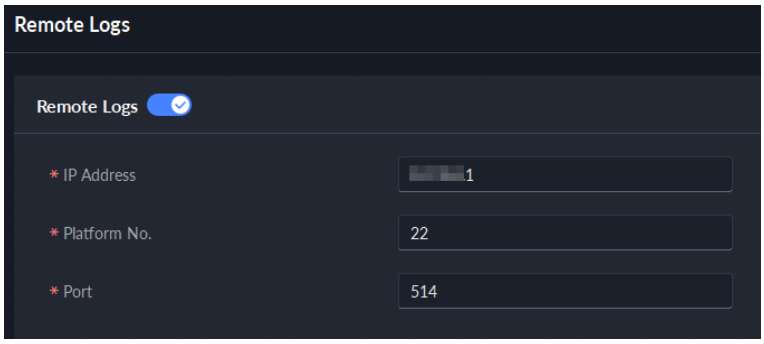
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.

Step 2 Click the **Remote Logs** tab.

Step 3 Enable the function, and then set parameters as required.

The **Platform No.** must be the same on the remote server and the platform.

Figure 8-7 Enable remote logs



Step 4 Click **Save**.

8.3.11 Configuring Mobile App

You can enable push notifications if you need to send messages to the app. In addition, you can download the app and log in to the app through this page.

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**.

Step 2 (Optional) Enable or disable push notification.

If enabled, the platform will connect to the cloud server which is required for push notifications; if disabled, the app will not receive any offline push notifications, such as offline alarms and offline calls.

Step 3 (Optional) Scan the QR code corresponding to **Download App** to download the app.

Step 4 (Optional) After downloading and installing the app, use the app to scan the QR code corresponding to **Log Into App**, and the app will automatically obtain the platform IP address and port. You can log in to the app after entering the user name and password.

Related Operations

Click , and then you can download the QR code as a JPG file.

8.3.12 Configuring Privacy Policy

You can select enable or disable **Store Face Snapshot Records** as needed. When it is disabled (default), the platform will not display or store face snapshot records that do not include comparison records.

Procedure

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

Step 2 Click **Privacy Policy**.

Step 3 Enable or disable **Store Face Snapshot Records** as needed (disabled by default).

When it is disabled, the platform will not display or store face snapshot records that do not include comparison records.

If you enable this function, the face snapshot records will be saved, and the prompt of **Only displays the face comparison records. If you want to display the face snapshot records, please enable Store Face Snapshot Records in System Parameters and Privacy Policy** will be displayed on the pages of face recognition records in **Monitoring Center**, and face capture records in **DeepXplore**. Use this function ethically and securely in accordance with applicable laws.

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.

- Automatic backup
  - **Basic Config** : The server automatically performs backups at set times to back up basic data such as device, user, and event configurations, and to save it to the server.
  - **Function Data** : The server backs up the function data including face data, structured data, and event data of the previous day at set times.
- Manual backup
  - **Basic Config** : The server manually performs backups to back up basic data such as device, user, and event configurations, and to save it locally.
  - **Function Data** : Click **Back Up Now** to back up the function data to the latest data. Service data backup files can only be saved on the server and cannot be exported.

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
  1. Click the **Manual Backup** tab.
  2. Click **Back Up Now**.
     - **Basic Config** : Users can download and upload backup files. To ensure security, users must create an encryption password to protect the data. Accessing any backup file requires password verification.
     - **Function Data** : Backup files cannot be downloaded. These backup files can only be restored locally.
- Auto backup: Click the **Auto Backup** tab, configure backup parameters, and then click **OK**. 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 server by default.
  - **Basic Config** : The user can set defined number of backup files of devices, users, event configurations, and more, to the backup path according to the defined period and time.
  - **Function Data** : After **Backup Retention Period** is set, the server will save the backup files of the function data.
  - **General** : Enable FTP backup and set the FTP backup path. After local backup, the backup file will be uploaded to the defined path to make another backup.

    - Only data through auto backup can be uploaded through FTP. Data through manual backup cannot be uploaded to FTP.
    - Enable FTP server from **System Parameters** > **FTP Server Config**, and make sure that the FTP server can be connected normally.
    - The FTP backup path cannot exceed 50 characters, and only characters, numbers, _, -, and / are allowed.

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.

- Restore from Backup File on the Server
  - **Basic Config** : Supports selecting backup files from the server and restoring data to that at the time of backup.
  - **Function Data** : Supports selecting the function data and period, and restoring data to that at the time of backup.
- Restore from Local Backup File

  Basic Config : If a backup file has already been obtained, the server supports importing the file and restoring the data to that at the time of the backup.

- 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.
- Restoring data will delete the data within the specified time range. Data outside the backup time range will be retained.

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 backup file on the server
  1. Click **Restore from Backup File on the Server** tab.
  2. Restore from backup files.
     - **Basic Config** : Click , and then enter the passwords. The **Password** is the same as the current user's, and the **Encryption Password** is the one created when the file was backed up).
     - **Function Data** : Select the function data and period to be restored. Click **Restore Now**, and then click **OK** to restore from the backup files.
  3. Click **OK**. After restoration, the platform will automatically restart.

  You can click to download the backup file.
- Restore from local backup file
  1. Click the **Restore from Local Backup File** tab.
  2. Click **Restore Now**.
  3. Enter the password, which is the same as the current user's.
  4. Select the backup file path, and then enter the **Encryption Password**, which is the one created when the file was backed up.

     After restoration, the platform will automatically restart.

9 Management

9.1 Configuring Local Settings

After logging in to the client, you can manage default settings, and configure the parameters including basic settings, video parameters, record playback, snapshot, recording, alarm, video wall, security settings and shortcut keys.

9.1.1 Configuring General Settings

Configure whether to display time zone in records, client inactive status, self-adaptive audio talk parameters, 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 9-1 Parameter description

Parameters	Description
Display Time Zone in Record	When selected, the client and the time of alarms will show both the time and time zone.
Client Inactive Status Config	If no operation is performed for the defined period, the client will be automatically logged out. If you are logged out, all the tasks on the client will be suspended.
Auto Lockout Config	
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.

Step 3 Click **Save**.

9.1.2 Configuring Video Settings

Configure parameters relating to live view and playback, such as window split, display mode, stream switching rules, play mode, and more.

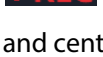
Procedure

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 9-2 Parameter description

Parameters	Description
Default Window Split	Set split mode of the video window.
Window Display Scale	Select from **Original Scale** and **Full Screen**.

Parameters	Description
AI Rule Overlay	After turning it on, when viewing live video or playing recordings, right-click the video window, the **AI Overlay** menu will be displayed. If you turn it off, the menu, the  icon on the live view and playback pages, and the overlaid information on the video image will not be displayed.
Stream Switching Rule	When the number of window splits is greater than the defined value, the live video (when you select **Effective for Live Video**) or live video and playback (when you select **Effective for Live Video and Playback**) will switch from the main stream to sub stream.
Switches to Main Stream when Window Maximized	If selected, you can double-click a live video window (when you select **Effective for Live Video**), or a live video or playback window (when you select **Effective for Live Video and Playback**) 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.
Play Mode	When playing videos, both fluency and real-time performance matter. To deal with network fluctuations, the platform has a set of buffer control strategies to ensure fluency and real-time performance. You can select one of the following play modes as needed. • **Real-time Play Priority** : The system might lower the image quality to avoid video lag. It is suitable for special scenarios with high requirements on real-time performance. • **Fluency Priority** : The system might lower the image quality and allow for lag to ensure video fluency. The higher the image quality is, the lower the video fluency will be. • **Balance Priority** (recommended): The system balances real-time priority and fluency priority according to the actual server and network performance. • **Custom** : The system adjusts video buffering and lowers the impact on video quality caused by unstable network. The bigger the value, the more stable the video quality will be.
Display Recording Status	You can select displaying or not displaying an icon on the upper-left corner of the window when recording is performed. Different icons will be displayed when you select **Device Video** , **Central Recording** or **Simultaneous Display**. By selecting **Simultaneous Display**, when device recording is performed, the  icon will be displayed; when central recording is performed, the  icon will be displayed; and when both device recording and central recording are performed, the  icon will be displayed.
Search Type of Device Video Stream	Select a default stream type when you play back recordings from a device. If **Only Sub Stream 2** is selected, but the device does not support sub stream 2, then recordings of sub stream 1 will be played.

Parameters	Description
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.
Auto Play Videos	After enabling this function, the system will automatically play the recordings after you search and find recordings, drag the timeline to a specific time to play the recording, and search for recordings of a specific time through the calendar on the **Playback** page.

Step 3 Click **Save**.

9.1.3 Configuring Alarm Settings

Configure the alarm sound and alarm display method on the client.

Procedure

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

Step 2 Click **Alarm**, and then configure the parameters.

- Alarm sound

Table 9-3 Alarm sound parameter description

Parameter	Description
Method	◇ **Default** : All types of alarms will use the same default alarm sound when triggered. ◇ **Custom** : Click **Modify Alarm Sound**, and then you can change the alarm sound and its play mode of each type of alarm. ◇ **Play Audio Defined in Scheme** : When an alarm is triggered, the platform plays the sound defined in > **Event** > **Event Config**. For details, see "5.1.1 Configuring Event Linkage".
Play Config	When you select **Play Audio Defined in Scheme** , you can select **Prioritize playing the audio configured for the event schemes**, or **Only play the audio configured for the event schemes**. The platform will play the default audio if no audio content is configured in **Event Config**.
Alarm Type	**All Event Source Types** by default, and cannot be modified.
Play Mode	**Play Once** by default, and cannot be modified.
Sound	Click , and then you can test playing the audio content. This parameter is available when **Prioritize playing the audio configured for the event schemes** is selected.

- Mode of opening alarm linkage videos

Table 9-4 Parameter description of opening alarm linkage videos

Parameter	Description
Open alarm linkage video when alarm occurs	If selected, the platform will automatically open linked video(s) when an alarm occurs. For this function to work properly, you must enable **When an alarm is triggered, display camera live view on client** when configuring an event. For details, see "5.1 Configuring Events".
Pop-up Display Duration	Set how long the pop-up windows will be displayed when alarms are triggered. You can select from fixed time options, or click **Custom** to customize the duration.
Related Content	Link video only or link video and map when alarms are triggered. ◇ Link Video: When an alarm is triggered, you can view the real-time video of the alarm channel in the pop-up window. ◇ Link Video and Map: When an alarm is triggered, you can click the **Video** or **Map** tab to switch viewing the real-time video or the map information.

- Map flashes

Table 9-5 Parameter description related to map flashing

Parameter	Description
Device on the map flashes when alarm occurs	Set one or more alarm types for alarm notification on the map. When an alarm occurs, the corresponding device will flash on the map.
Alarm Type	
Map Flash Duration	Set the duration that the device flashes on the map when an alarm is triggered. You can select from **20 s** , **40 s**, **1 min**, **5 min**, **10 min**, **Always**, or click **Custom** to customize the duration.

Step 3 Click **Save**.

9.1.4 Configuring File Storage Settings

Configure the naming rule and file size 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 9-6 Parameter description

Parameter	Description
Video Naming Rule	Select a naming rule for manual recordings.

Parameter	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 size ranges from 10 MB to 200 MB, and it is 100 MB by default.
Image Naming Rule	Select a naming rule for snapshots.

Step 3 Click **Save**.

9.2 Managing Logs

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

9.2.1 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 In the search results list, select the log checkbox as needed, and then click **Integrity Check**. After the check is completed, it will display the check results and the time of the last check.

- If the check result displays **Intact** (green), it indicates that the log file is intact and has not been tampered with.
- If the check result displays **Compromised** (red), it indicates that the log file has been tampered with.

Step 5 To export the logs, click **Export** and follow the on-screen instructions.

Check results and check time are not included in the exported files.

9.2.2 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.

9.2.3 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.

9.2.4 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.

9.3 Help

Click **Help** to view the user manual of the platform.

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.
Device Auto Registration Service	ARS	Accesses devices added through automatic registration.
Alarm Controller Management Service	ARCMS	Accesses alarm controllers.
Device Search Service	SOSO	Searches for and obtains configurations from devices in local networks.
Video Intercom Service	SCS	Manages audio talks among PC client and app, and video intercom devices.
Service Management Service	SMS	Manages BSMS, POC and SCS.
Business Session Management Service	BSMS	Downloads files from devices, manages the sleep and wake status of low-power consumption cameras that uses 4G network, and redirects to the webpage of devices added through automatic registration.
Access Control Management Service	ACDG	Manages ACMS.

Service Name		Function Description
Access Control Management Service	ACMS	Accesses access control devices.
Video Storage Service	SS	Stores and forwards recorded videos on the platform.
Video Decoding to Wall Service	VMS	Accesses decoders outputs videos to video walls.
Object Storage Service	OSS	Stores files of the platform.
Media Forwarding Service	MTS	Forwards real-time video streams.

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188