DSS OneBox

User Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V8.6.0

Foreword

General

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

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

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
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

Before using and operating this device, please read and observe the following precautions carefully to avoid dangerous or illegal operations.

Transportation Requirements

Before moving the product, please unplug the AC power cord from power socket.

Installation Requirements

WARNING

Before connecting or disconnecting any signal cables, make sure that all the power cords are unplugged in advance.

Operation Requirements

- We do not recommend using the device continuously for a long time in industrial PC scenarios (such as environment with high temperature, humidity, vibration and strong electromagnetic interference).
- Please carefully read the user manual before using the product.
- To avoid damages caused by frequent start up and shutdown, please wait for at least 30 seconds before restarting the product.
- All the operations such as removal or installation shall be implemented on the electrostatic discharge (ESD) worktable, because some precision components are sensitive to electrostatic discharge.
- If there is no ESD worktable, please take the following measures to minimize possible damages from electrostatic discharge: Wear an anti-static wrist strap during operation; always touch the metal chassis of frame of the corresponding products before removal or installation of any components.
- The normal working temperature for the product is 0 °C (32 °F) to 40 °C (104 °F), and the normal working humidity is 10%–90% (RH).
- Assure good cooling and ventilation.
- There are heating hole on back cover, do not spray water to it or use damp cloth for cleaning.

Maintenance Requirements

Please call professional personnel for maintenance service.

Table of Contents

1 Overview

1.1 Introduction

DSS OneBox is an all-in-one workstation with a pre-installed license that works right out of the box, requiring no installation or deployment. It is equipped with Intel processor with decoding capability and moderate amount of storage space.

With support for multiple video channels and built-in video surveillance, event center, video intercom, attendance, and visitor management, DSS OneBox is particularly well suited for the SMB software market, such as offices, stores, and warehouses.

1.2 Highlights

- Compact

  A blend of style and practicality, seamlessly integrating into security settings.

  - ◇ Designed with aluminum and glass, offering a modern look and durability.
  - ◇ Compact design for flexible deployment in various security scenarios.
- Powerful

  A powerful core for seamless monitoring.

  - ◇ 1 TB SSD storage, expandable with an additional hard disk for image storage.
  - ◇ Integrated GPU decoding supports multiple channels of 1080P video, ensuring smooth management of multiple video streams.
  - ◇ Supports high network speeds, perfect for high-bandwidth scenario.
- Simplified

  Real-time monitoring with easy management.

  - ◇ 4-screen 4K output, providing clear and detailed views for various monitoring needs.
  - ◇ Plug-and-play with pre-installed operating system and software with relevant licenses, automatically opens the client on startup for quick access.
  - ◇ Mobile app allows for monitoring security status whether over public or local networks, enabling flexible system management.
  - ◇ Restores system default settings with one key.
- Comprehensive

  One-stop management for diverse needs.

  - ◇ Multiple video channels to suit various monitoring environments.
  - ◇ Multi-module features to meet diverse security requirements.

2 Hardware Introduction and Operations

2.1 Accessories

- 1 power cord.
- 1 power adapter.
- 1 HDMI cable.
- 1 bracket.
- 1 screw set.

2.2 Appearance

Figure 2-1 Appearance

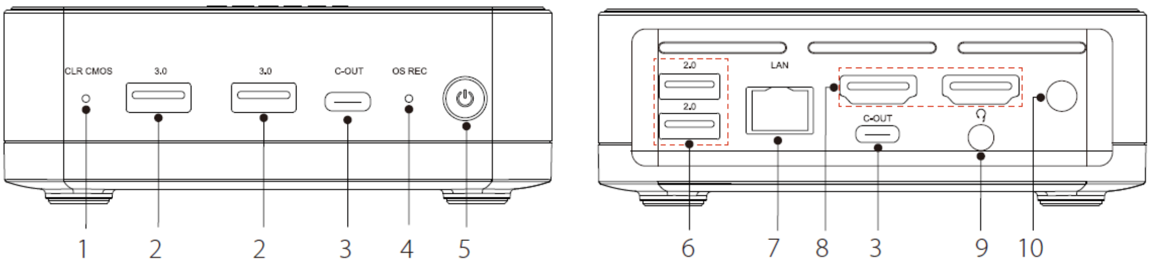


Table 2-1 Appearance description

No.	Description
1	CLR CMOS (pinhole). Used for restoring BIOS settings. Press and hold the button for 3 seconds, and the configuration takes effect.
2	3.0. Connects to USB 3.0 or USB 2.0 devices, such as USB drive, USB keyboard, and USB mouse.
3	C-OUT. Supports DP OUT, USB3.2 reversible insertion, 5 V/3 A external power supply.
4	OS REC (pinhole). System restore button. When the device is off, press and hold the button, and press the power button, until the boot screen appears. The configuration takes effect. After one-click restoration, the system will be restored to default settings, but the platform data will be kept. Please be advised.
5	Power button.

No.	Description
6	2.0. Connects to USB 2.0 devices, such as USB drive, USB keyboard, and USB mouse.
7	LAN. 2.5 Gbps network interface, connects to Ethernet.
8	HDMI OUT. High-definition multimedia signal output interface, connects to display devices with HDMI input.
9	AUDIO OUT. 3.5 mm headphone or microphone jack.
10	DC IN. 2.5 mm, 19 V power port.

2.3 Installing the Device

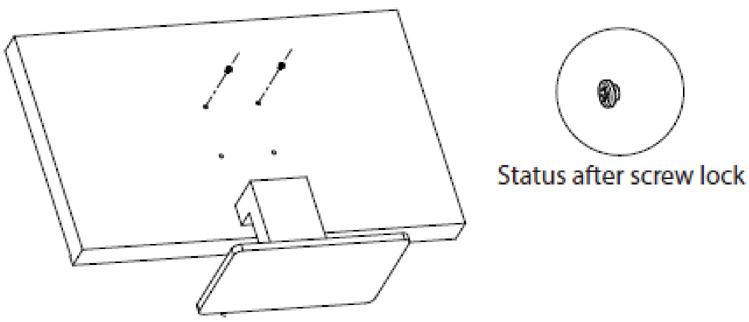
You can use the device by placing it on a desktop. If you want to install it behind a display device (such as a monitor), take the following steps.

⚠

We do not recommend using the device continuously for a long time in industrial PC scenarios (such as environment with high temperature, humidity, vibration and strong electromagnetic interference).

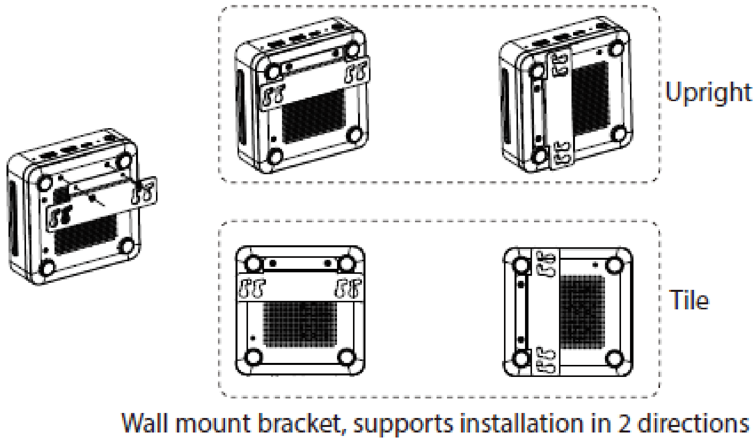
Step 1 Attach the step screws to the VESA holes of the display device.

Figure 2-2 Attach the step screws



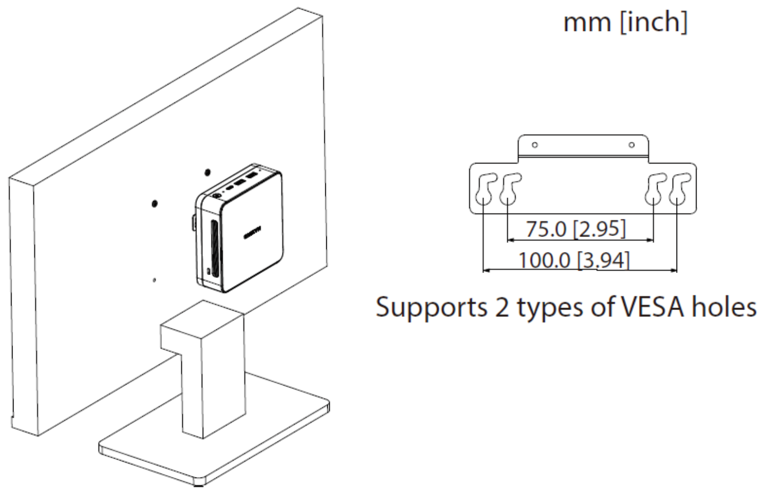
Step 2 Attach the wall mount bracket to the device.

Figure 2-3 Attach the wall mount bracket to the device



Step 3 Hang the device through the lug hole on the display device that is fixed with pre-locked step screws.

Figure 2-4 Hang the device

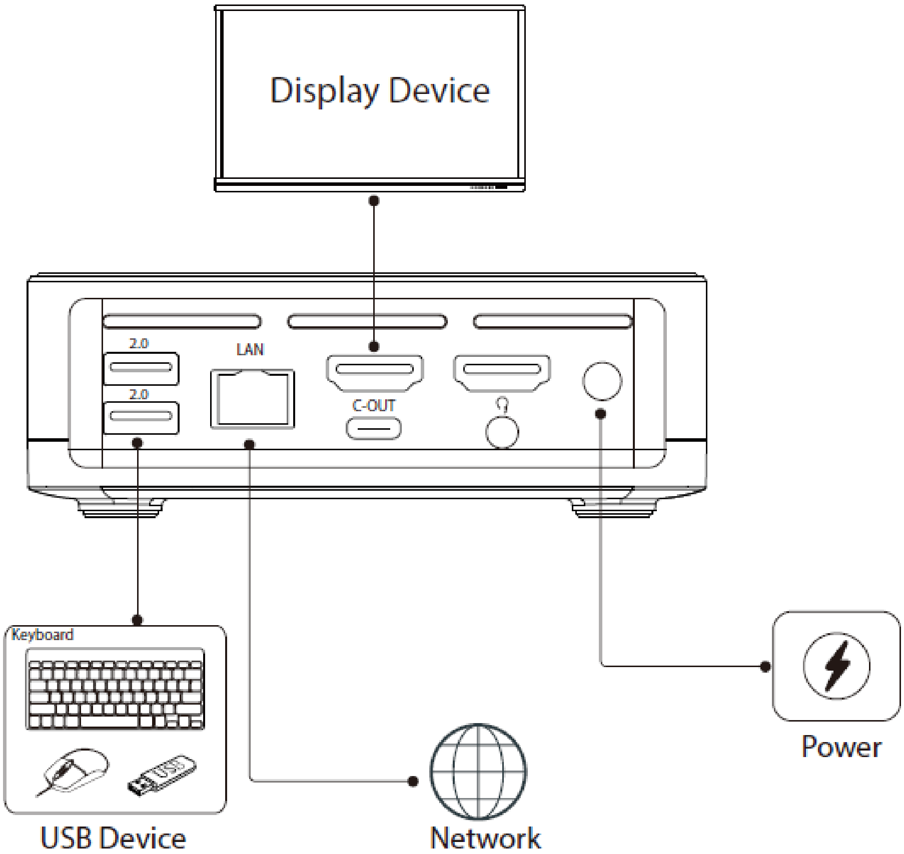


2.4 Connecting and Starting the Device

Step 1 Complete the device connection according to the illustration.

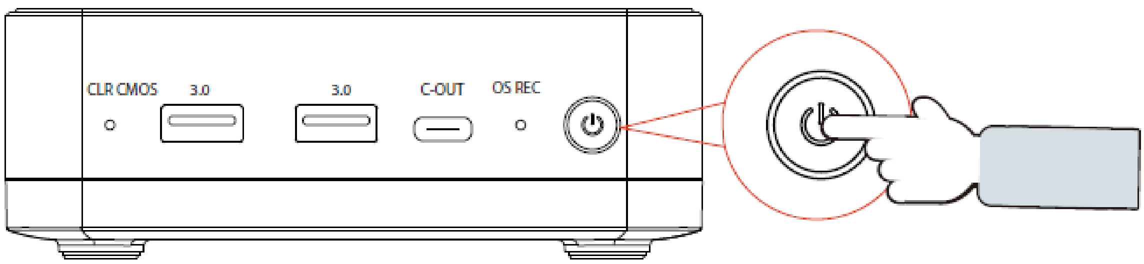
Connect the display device to the HDMI OUT or C-OUT interface of OneBox. The HDMI cable is included in the package. For the cable for connecting to the C-OUT interface, you need to purchase it separately.

Figure 2-5 Connection illustration



Step 2 Press the power button to start the device.

Figure 2-6 Start the device

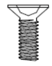
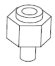
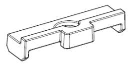


2.5 Installing Hard Drive (Optional)

Step 1 Confirm the contents of the screw package.

Table 2-2 Screw package description

Name	Image	Quantity
CM2 × 3.5 black screw		2
CM2 × 3 silver screw		1

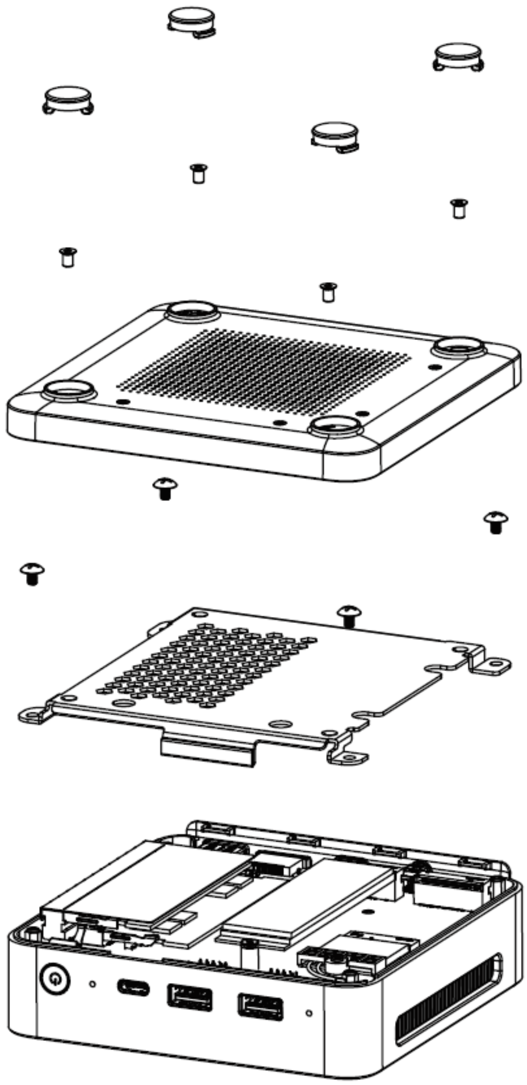
Name	Image	Quantity
Staircase screws		2
Hexagonal pillar		1
Antenna latch		1

Step 2 Invert the device.

Figure 2-7 Invert the device

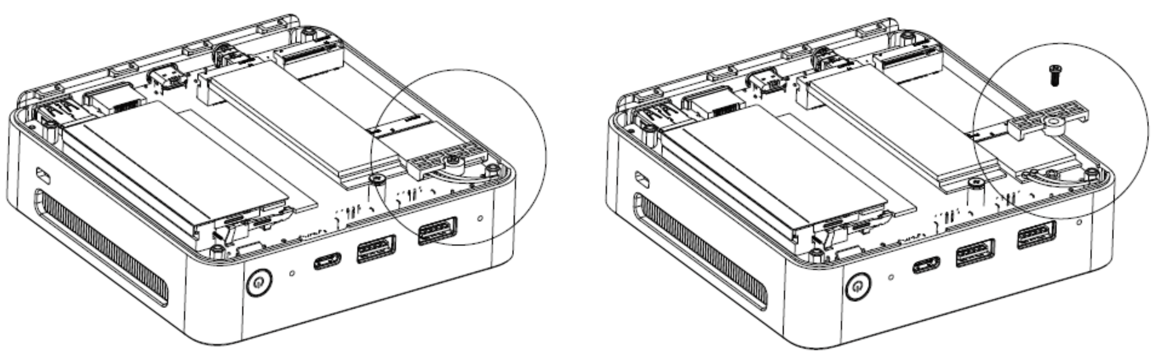
Step 3 Remove the device casing.

Figure 2-8 Remove the casing



Step 4 Disassemble the built-in latch and screws from the device.

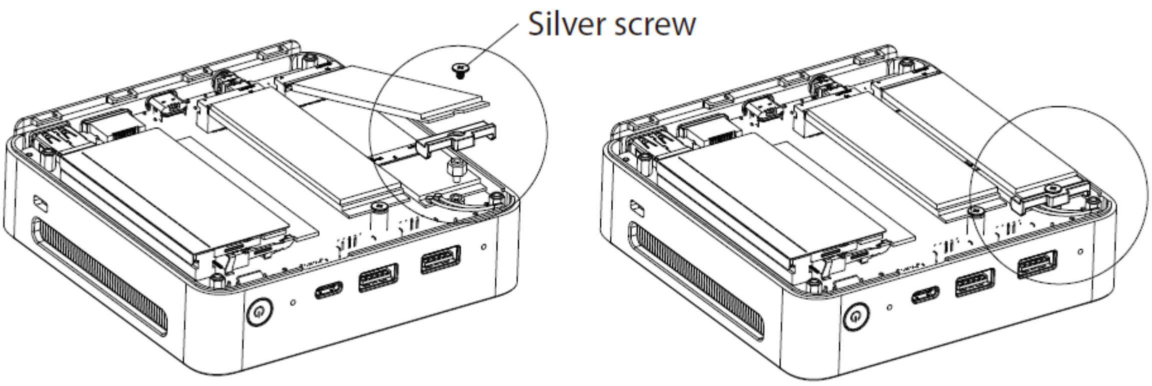
Figure 2-9 Disassemble the latch and screws



Step 5 Take out the materials from the screw package, replace and install them as shown below.

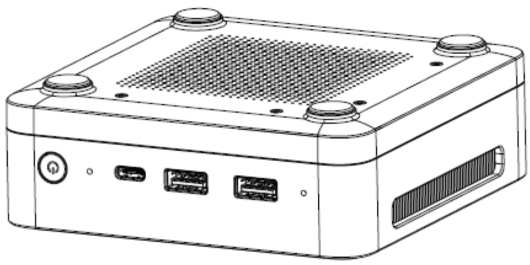
Step 6 Install the new SSD, and then securely fasten the screws.

Figure 2-10 Install SSD



Step 7 Reassemble the bottom cover of the device.

Figure 2-11 Reassemble the bottom cover



3 Management Tool

3.1 Notes

- Set the account password of your Windows operating environment in time.
    - ◇ If you enter the incorrect password 5 times consecutively, your Windows account will be locked for 5 minutes.
    - ◇ The password of the default account is set to never expire. For security reasons, we recommend setting the password to be valid within the valid period.
- The version of the current operating system will be automatically updated, and it might take a long time to restart. You can set the time of pausing updates in **Settings** > **Windows Update**.

3.2 Configuration Wizard

Procedure

Step 1 Press the power button to start the device.

Step 2 Configure the network of the Windows operating environment.

Step 3 On the **Configuration Wizard** page, configure the network parameters.

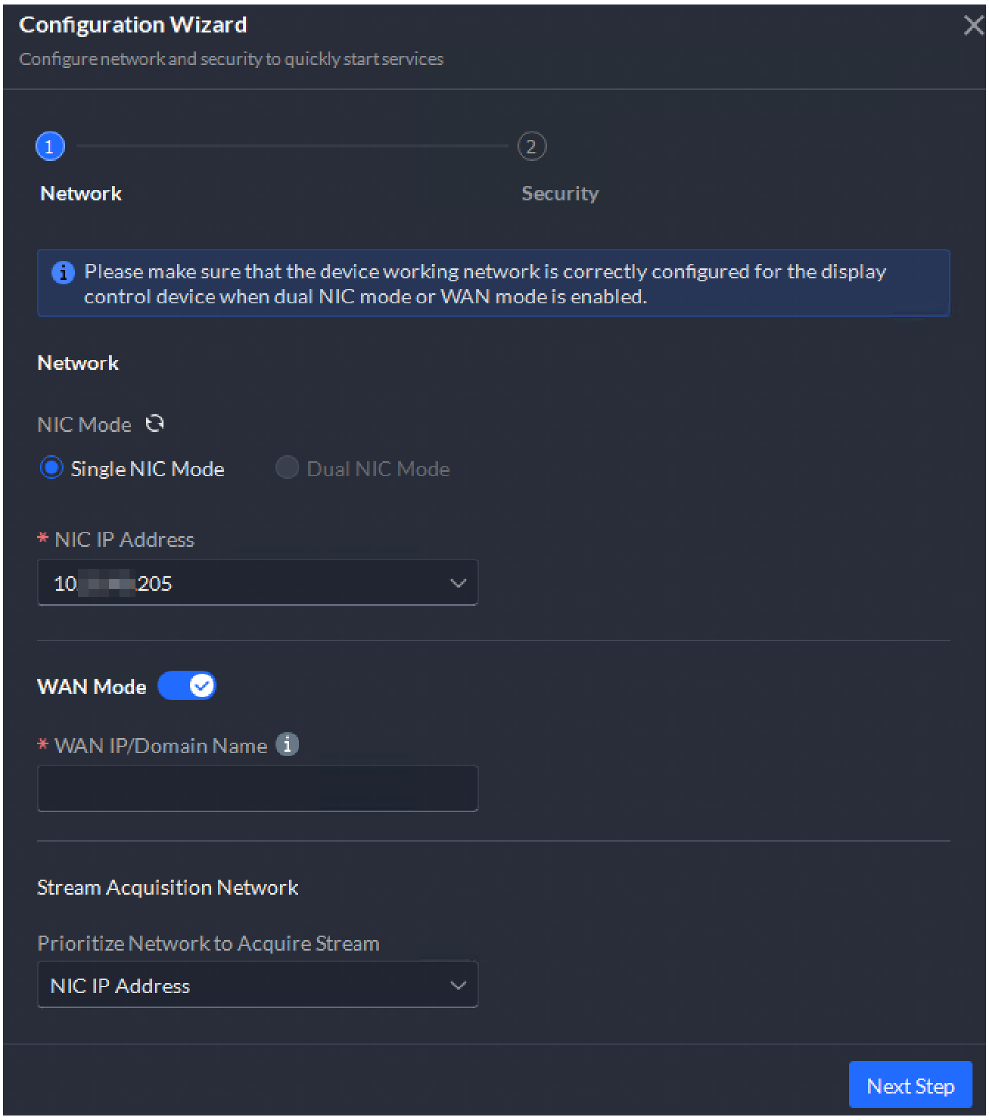
1. Configure the IP address of the network card.

    - The platform supports dual-band Wi-Fi, 2.5G wired network card and Bluetooth wireless connection.
    - When configuring 2 networks for the platform, you can either use 1 network card for accessing devices on a local area network, and 1 network card for services on the Internet; or use both network cards for accessing devices on a local area network, and then map one of them to the Internet.

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

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

Figure 3-1 Configuration wizard



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

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

   If the available RAM of the platform is less than 2 GB, you can only use basic functions related to video. If it is less than 1.5 GB, you cannot use any function.

3.3 Management Tool Introduction

The license is activated by default. If you reinstall the management tool, you need to use the activation tool to activate the license. The activation code and serial number required for activation can be found on the device. If they are lost, contact our technical support.

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

Figure 3-2 Management tool

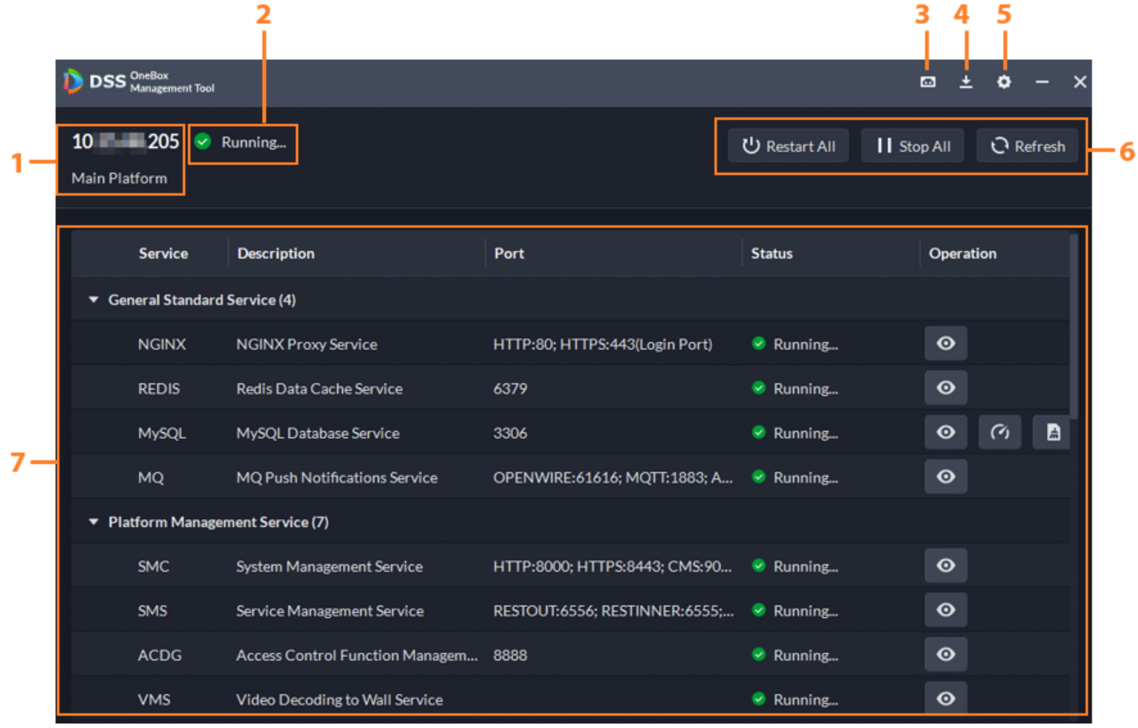


Table 3-1 Interface description

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

No.	Function	Description
5	Configurations and view information of the platform	● Network: Configure the network card mode, IP address, and the WAN mode. If the platform has 2 network cards, you can select **Dual NIC** mode, configure 2 IP addresses, and then the platform will be able to connect to two networks and access the devices on each one. If the platform is in a local network and the devices are on the internet, or you need to access the platform that is in a local network from the Internet, you can enable **WAN Mode** and map the IP address of the platform to a WAN IP address or a domain name. ● Security: Select a TLS protocol version when you access the webpage of the platform through a browser. TLS1.2 is selected by default and cannot be disabled. There are security vulnerabilities to TLS1.0 and 1.1. We strongly recommend you disable it to avoid security risks. After configuration, follow the on-screen instructions to configure the TLS protocol version in the IE browser so that you can access the webpage of the platform normally. ● Language: Select the language of the management tool. Multiple languages are supported. ● Port Self-adaption: If a port is occupied, the platform will change it automatically. After turning on or off this function, you must restart the management tool for it to be effective. ● Reset system password: Reset the password of system user. 1. Click **Export**, set the encryption password, and then export the request file. 2. Contact the technical support to get the password reset file through the request file. 3. Click **Reset** to import the reset file, and then log in the DSS client to initialize the password. ● User manual: View the user manual of the platform. ● About: View the software version information, software license agreement, and more.
6	Service management	● Click **Restart All** to restart all services. When starting the platform, if its available memory does not reach 2 GB, only the basic video services can be enabled. If the platform has less than 1.5 GB of available memory, no services are available. ● Click **Stop All** to stop all services. ● Click **Refresh** to refresh services.
7	Services	Displays all services, and their status and port numbers. Click to change the port number of a service, and then the services will restart automatically after modification.

No.	Function	Description
	Database repair	If you cannot log in to the client because the database is abnormal, you can try to repair it manually. Click of the MySQL service, and follow the instructions. Based on the items checked, the platform will determine whether repair or restoration is needed. If repair fails, you can try restoring the database. During restoration, the platform will back up the database. Please make sure that there is enough space. Otherwise, restoration will fail. Click to view all backup files. You can delete them as needed.

Uninstalling the Management Tool

To uninstall the management tool, go to "C:\DSS\DSS Server\Uninstall", double-click uninst.exe, and then follow the on-screen instructions to uninstall the program.

4 DSS Client Login

4.1 Logging in to DSS Client

First-Time Login

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

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 2 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 that you just set.

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

Log In Other than First Time

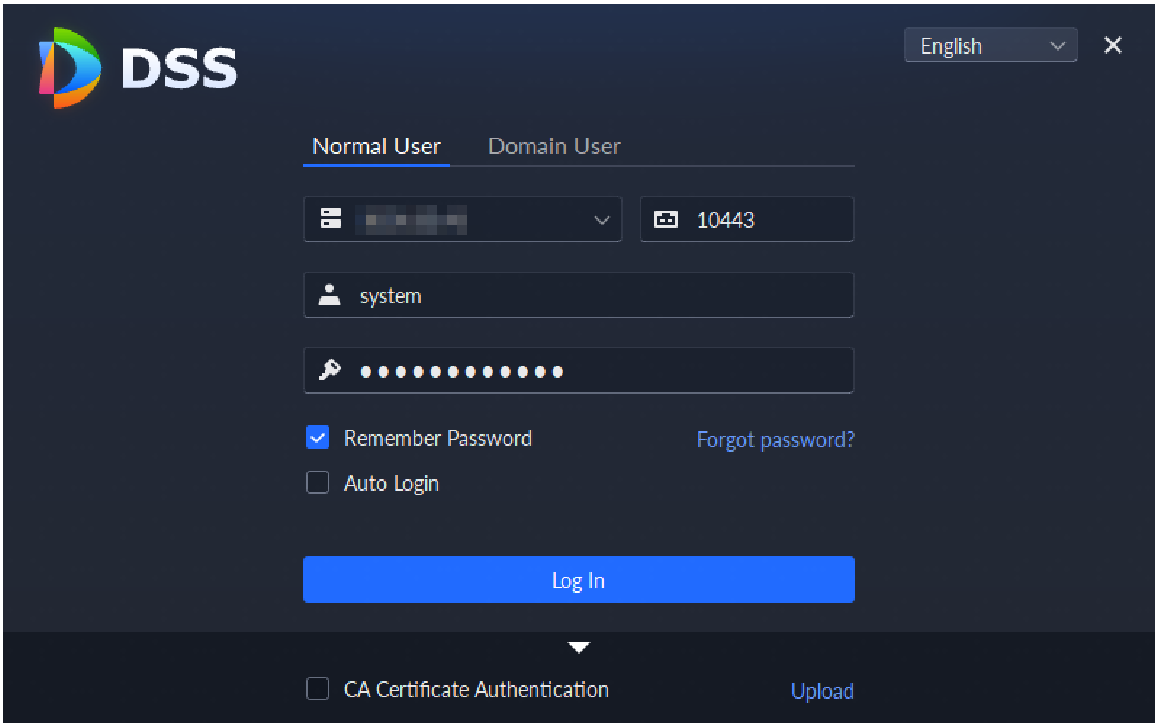
After restarting, the system automatically runs the platform management tool, and the client login window pops up automatically. Enter the username and password to log in. If you manually exit the client, log in as follows.

1. Double-click  on the desktop.
2. Select a language.
3. Enter the login username (system by default) and password (the one that you defined during initialization), and then click **Login**.

   The IP address and port are automatically filled in by default. In the drop-down list, platforms that are on the same network as your computer will be shown.

   If you log in by localhost, the platform will automatically change it to 127.0.0.1.

Figure 4-1 Login



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

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

4.2 Homepage of DSS Client

Figure 4-2 Homepage

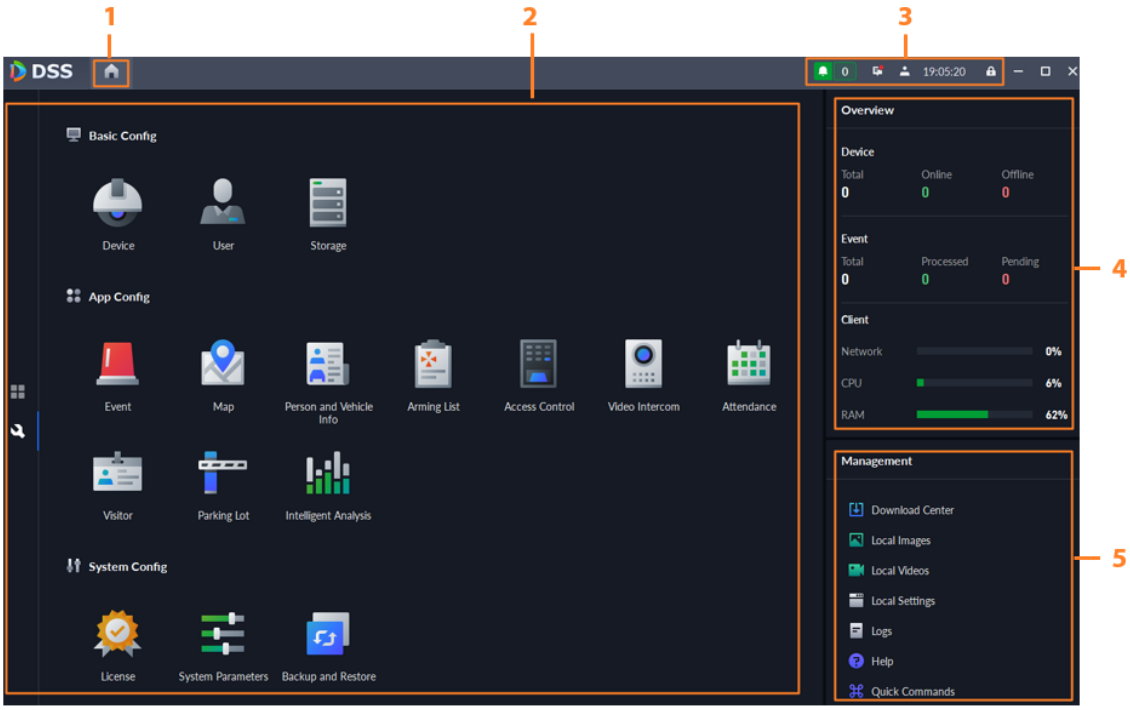


Table 4-1 Parameter description

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

No.	Name	Function
3	System settings	● : Enable or disable alarm audio. ● : Displays the number of alarms. Click the icon to go to **Event Center**. ● Click to view system messages, such as the information of a device was edited or deleted. The permissions of a user will determine what messages can be seen. For example, if user A does not have the permission of device A, then user A will not get the message when device A is deleted. ● : User information: Click the icon, and then you can log in to the webpage by clicking system IP address, change password, lock client and log out. ◇ Click platform IP address to go to the webpage. ◇ Click **Change Password** to change user password. ◇ Click **Log Out** to exit client. ◇ Click **About** to view version information. ● 19:16:50 shows the time. The image is an example. ● Click to lock the client.
4	Overview	● The number of devices in total, offline and online. ● The number of total, processed and pending events. ● The client network, CPU and RAM usage.
5	Management	● Download videos. ● Go to local storage path of pictures and view pictures. ● View local videos. ● Settings for video, snapshot, video wall, alarm, security and shortcut keys. ● View and manage logs. ● View user manual. ● Customize quick HTTP commands.

5 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.

5.1 Managing Resources

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

5.1.1 Adding Organization

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

Procedure

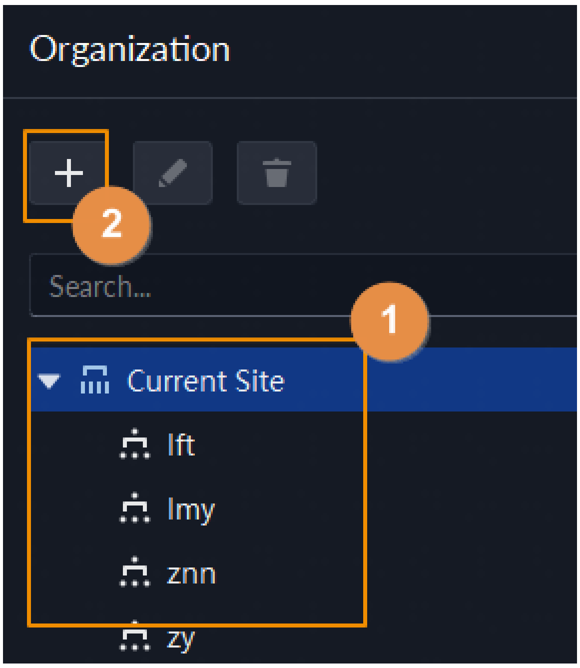
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Add an organization.

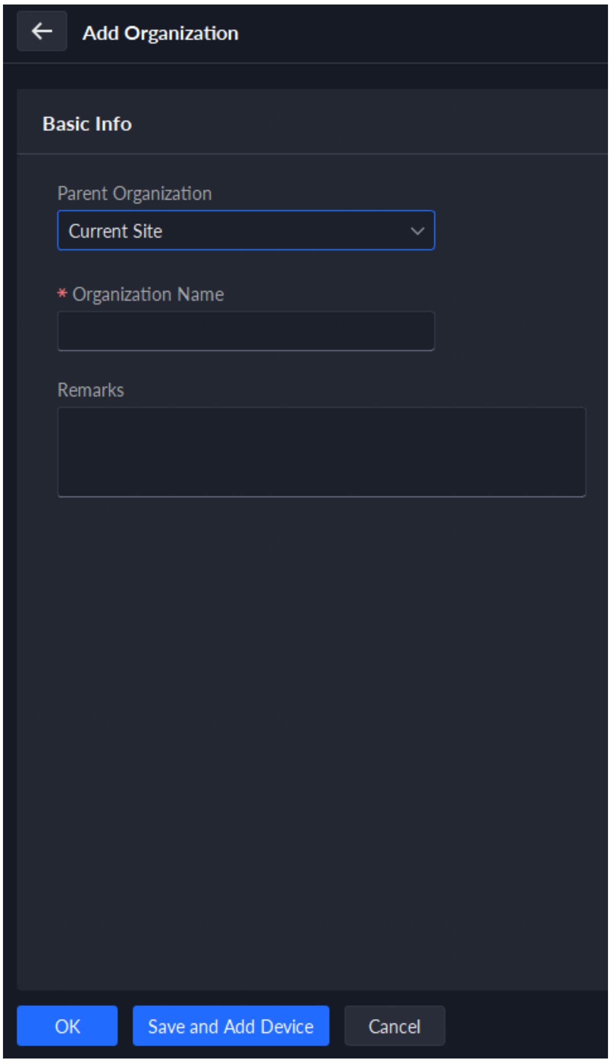
1. Select a parent organization.
2. Click .

Figure 5-1 Add an organization



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

Figure 5-2 Add an organization



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

Related Operations

- Change organization name

  Right-click the organization, and then click **Rename**.
- Delete an organization

  Organization with devices cannot be deleted.

  Select the organization, click , or right-click an organization and select **Delete**.
- Change the organization of devices

  Select one or more devices, and then click **Move To** to move them to another organization.

5.1.2 Managing Device

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

5.1.2.1 Searching for Online Devices

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

Procedure

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

Step 2 Click .

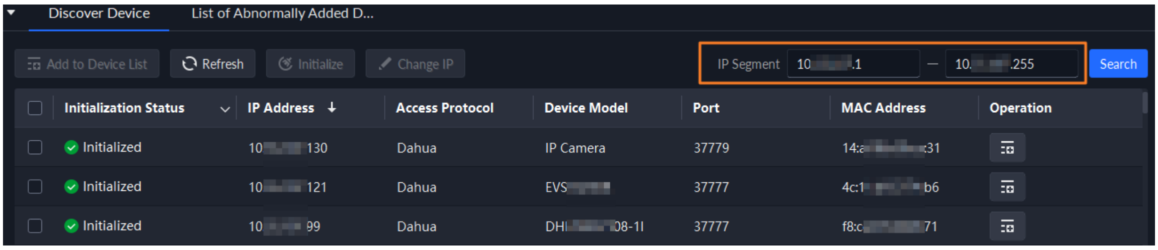
Step 3 Click **Discover Device**.

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

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

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

Figure 5-3 IP segment search



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

5.1.2.2 Initializing Devices

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

Procedure

Step 1 Search for devices. For details, see "5.1.2.1 Searching for Online Devices".

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

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

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

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

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

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

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

5.1.2.3 Changing Device IP Address

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

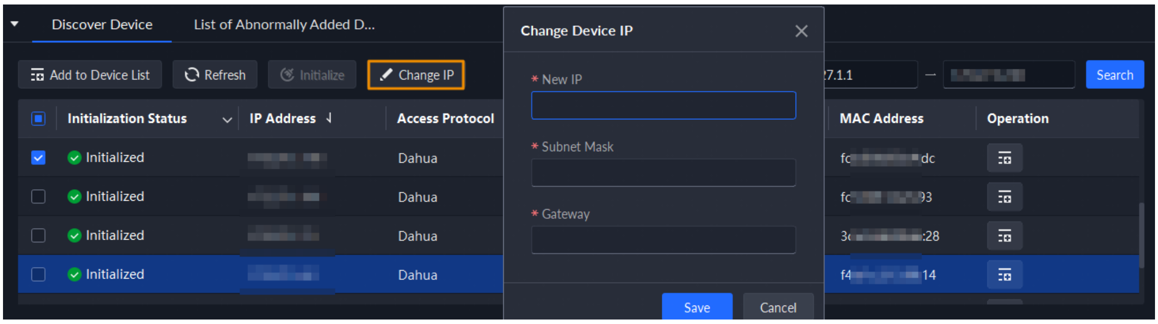
Procedure

Step 1 Search for devices. For details, see "5.1.2.1 Searching for Online Devices".

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

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

Figure 5-4 Change IP address



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

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

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

5.1.2.4 Adding Devices

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

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

5.1.2.4.1 Adding Devices One by One

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

Procedure

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

Step 2 Click .

Step 3 Click **Add**.

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

Select a mode to add the device.

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

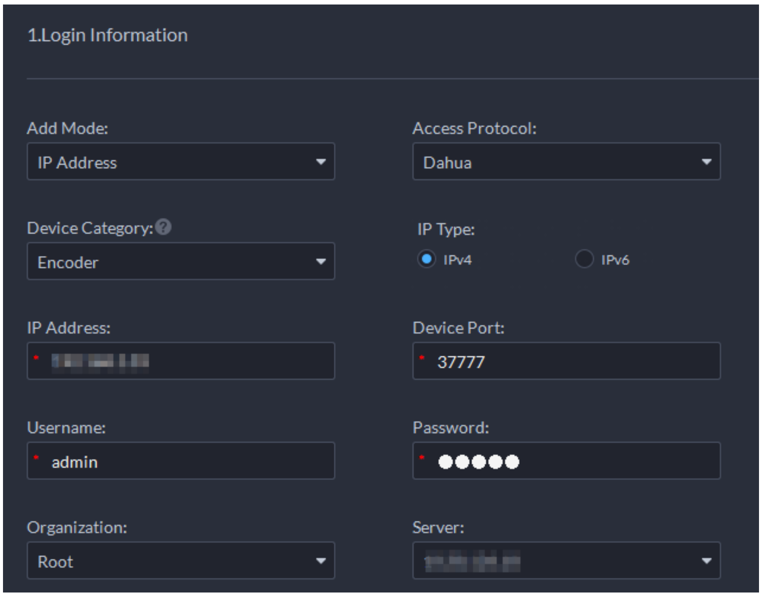
  Only **Encoder** devices support IPv6. If you want to add devices to the platform through IPv6 addresses, you must first configure an IPv6 address for the platform. Contact technical support for help.
- **IP segment** : Add multiple devices in the same segment. We recommend selecting this option when the login username and password of the multiple devices in the same segment are the same.
- **Domain Name** : We recommend selecting this option when the IP address of the device changes frequently and a domain name is configured for the device.
- **Auto Registration** : We recommend this method when the IP address of a device might change. The ID of auto register has to be in accordance with the registered ID configured on the device you want to add. The port number must be the same on the platform and on the device. The auto register port is 9500 on the platform by default. To change the auto register port number, open the configuration tool to change the port number of ARS service.

  ◇ After a device is added through auto registration, hover the mouse over its IP address on the device list, and then you can see its local IP address and the IP address it uses to connect to the platform.
  ◇ Sleep function is supported for IPCs that use 4G mobile network to communicate and are solar-powered only when they are added to the platform through automatic registration.
- **P2P** : Add devices under a P2P account to the platform. The platform must be able to access the P2P server. There is no need to apply for the dynamic domain name of the device, perform port mapping or deploy a transit server when using it.

  Before adding devices through P2P, you need to enable the P2P function from **System Parameters** > **Device Adding Config**.

- 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 5-5 Add an encoder



Step 5 Enter the device information.

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

Step 6 Click **OK**.

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

Related Operations

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

5.1.2.4.2 Adding Devices through Searching

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

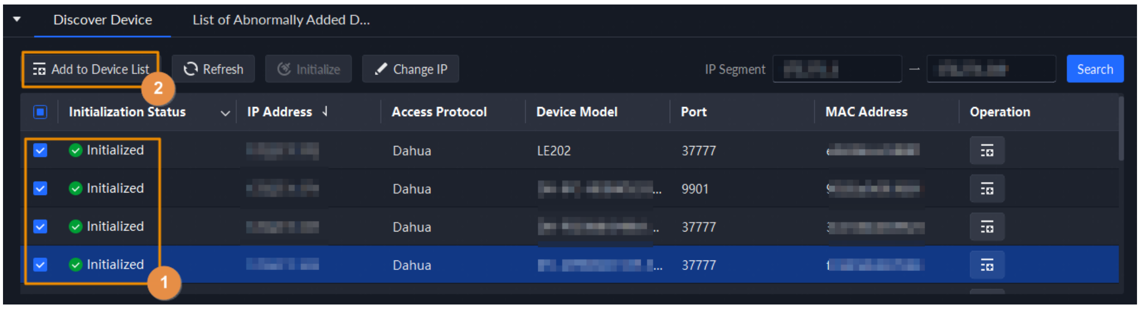
Procedure

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 5-6 Add in batches



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

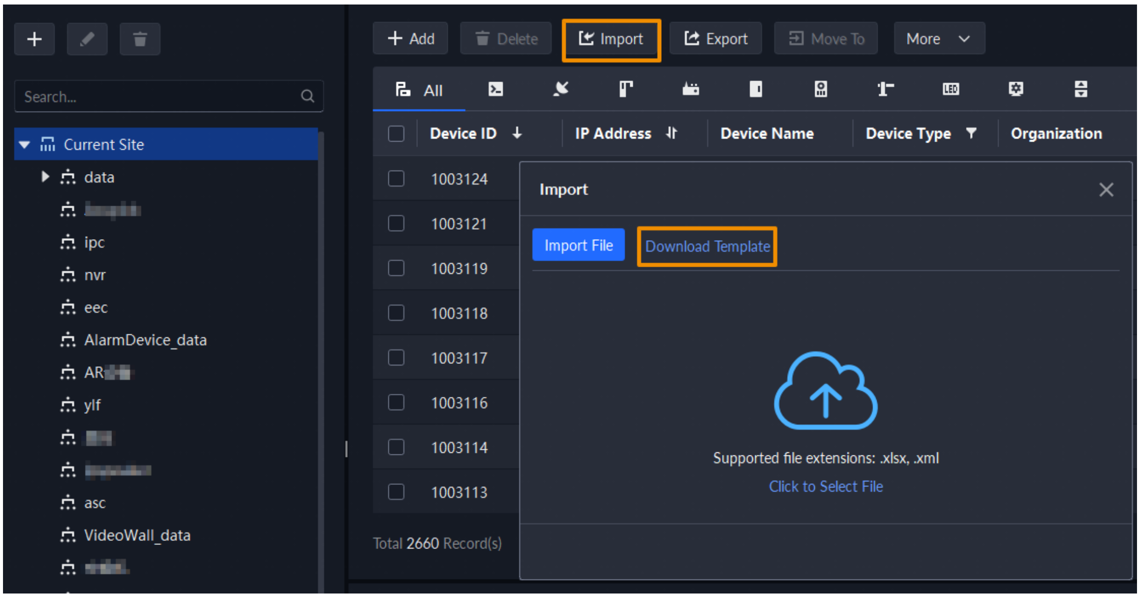
5.1.2.4.3 Importing Devices

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

Prerequisites

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

Figure 5-7 Download template



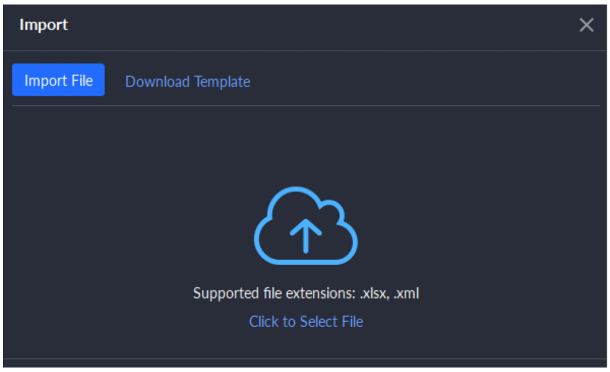
Procedure

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

Step 2 Click .

Step 3 Click **Import**.

Figure 5-8 Import devices



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

Step 5 Click **OK**.

5.1.2.5 Editing Devices

Edit the information of devices.

5.1.2.5.1 Changing IP Address

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

Procedure

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

Step 2 Click **Device Config**.

Step 3 Click of a device.

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

5.1.2.5.2 Modifying Device Information

Procedure

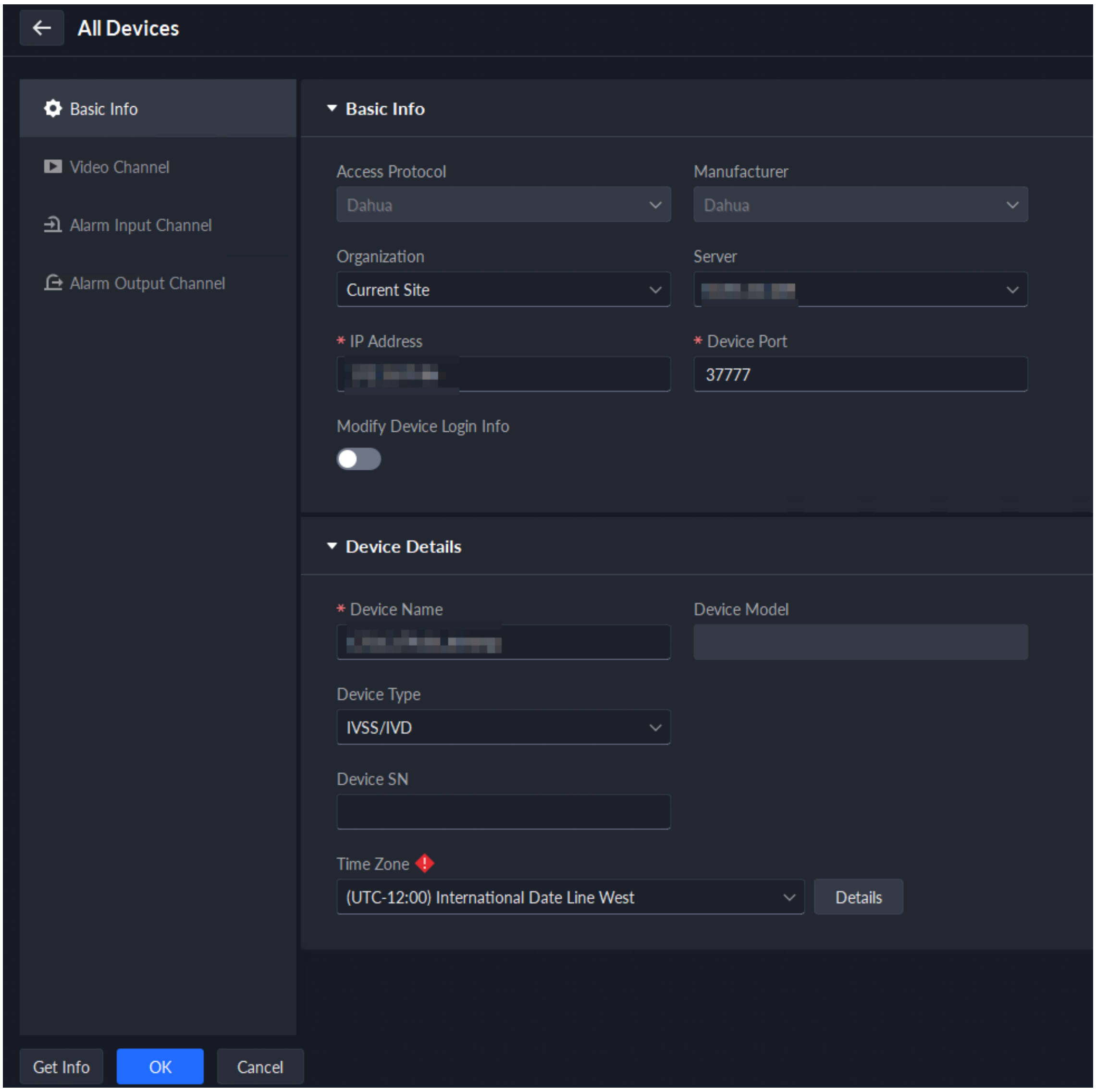
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

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

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

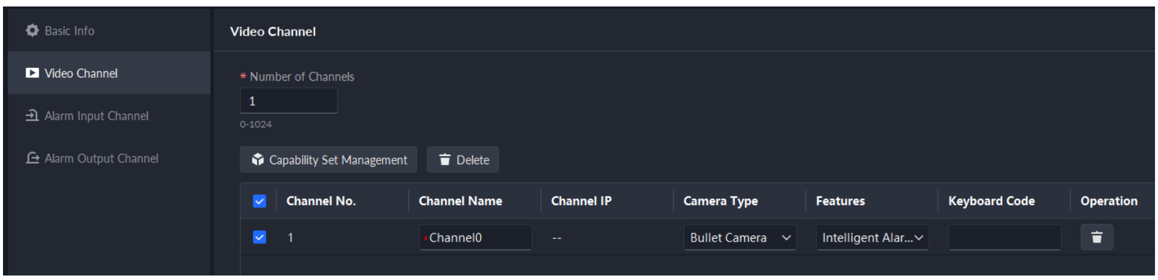
Figure 5-9 Basic information



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

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

Figure 5-10 Modify the information of video channel



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

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

- Alarm type includes 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**.

5.1.2.5.3 Getting Device Information in Batches

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

Procedure

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

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

Step 3 Select multiple devices.

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

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

Wait for the platform to finish the process.

Related Operations

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

5.1.2.5.4 Configuring Channel Features in Batches

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

Procedure

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

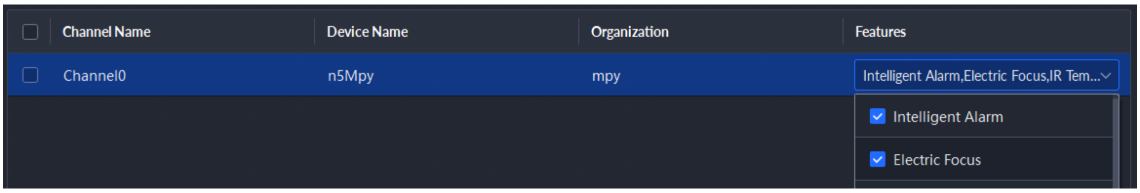
Step 2 On the top of the page, select **More** > **Capability Set Management**.

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

Step 4 Select the channels you want to configure.

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

Figure 5-11 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.

5.1.2.5.5 Modifying Device Organization

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

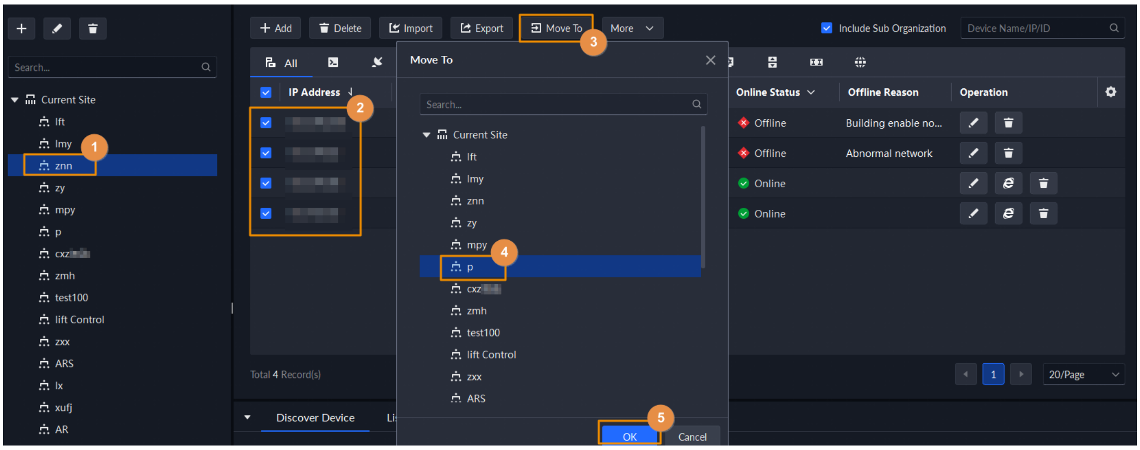
Procedure

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

Step 2 Click .

Step 3 Select a device to be moved, click **Move To** , select the target organization, and then click **OK**.

Figure 5-12 Move a device



5.1.2.5.6 Changing Device Password

You can change device usernames and passwords in batches.

Procedure

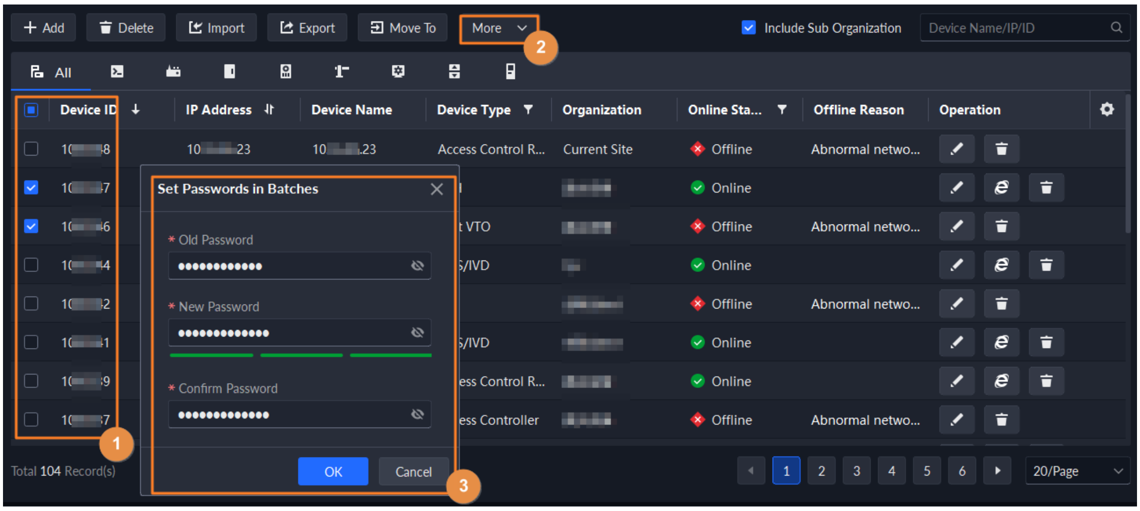
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

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

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

Figure 5-13 Change device password



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

5.1.2.6 Configuring Multicast

When multiple PC clients want to view the real-time video from the same channel, the video will be sent to the clients through the router. This will reduce the bandwidth usage.

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 Click a video channel, and then click **Modify** next to **Multicast Config**.

Step 3 Enable multicast for main stream and/or sub stream, configure the parameters, and then click **OK**.

Step 4 Enable multicast for the platform. For details, see "10.4.2 Configuring Video Settings".

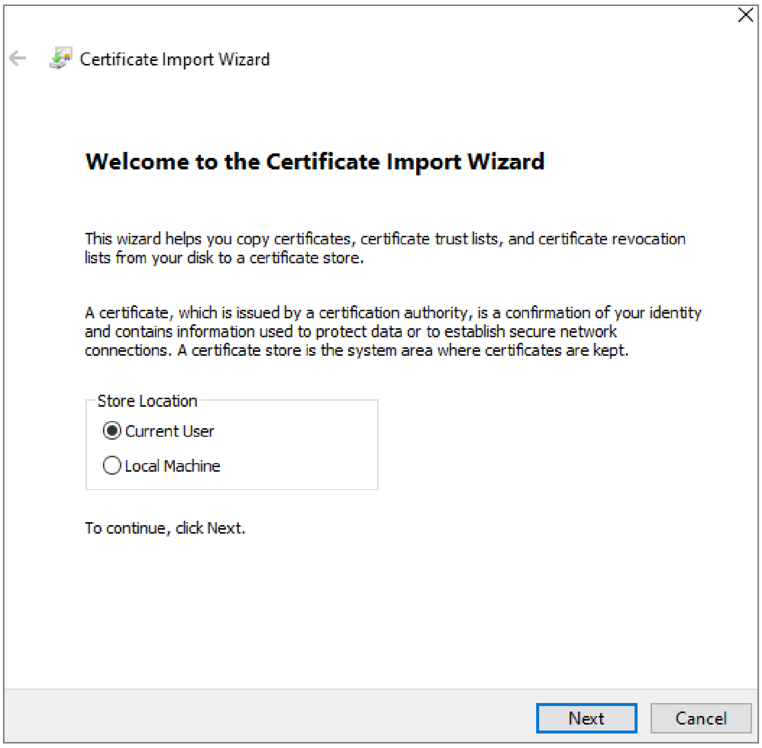
5.1.2.7 Logging in to Device Webpage

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

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

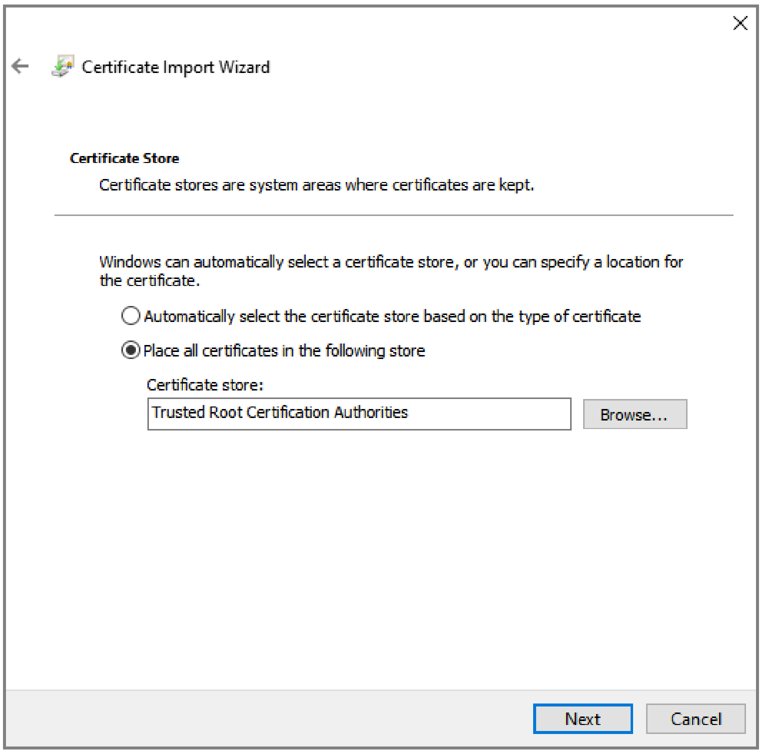
1. Log in to the webpage of the device, and then download the trusted CA root certificate.
2. Double-click the certificate, and then click **Install Certificate**.
3. Select **Current User** , and then click **Next**.

Figure 5-14 Certificate import wizard (1)



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

Figure 5-15 Certificate import wizard (2)



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

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

5.1.2.8 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 "9.2.1 Configuring Security Parameters".

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

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

5.1.2.9 Modifying Device Time Zone

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

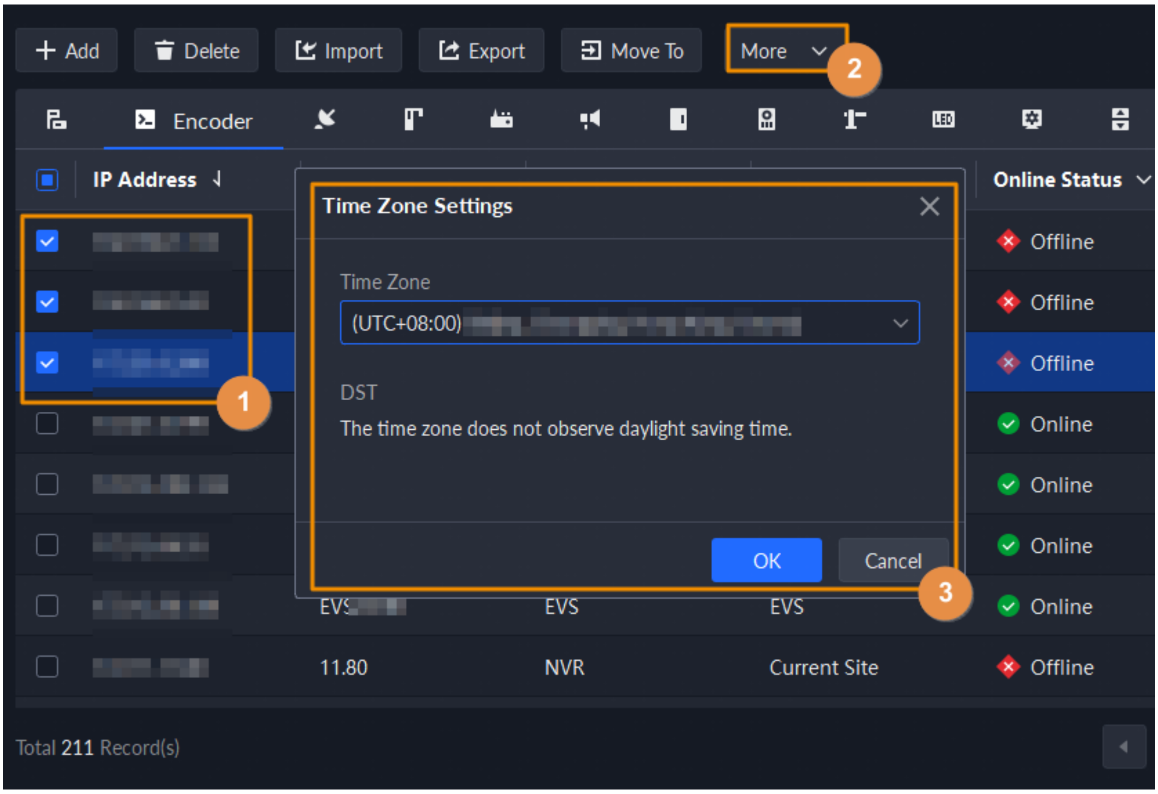
Procedure

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 device, click **More** , and then click **Time Zone Settings**.

Figure 5-16 Modify device time zone



Step 4 Select a time zone.

Step 5 Click **OK**.

5.1.3 Binding Resources

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

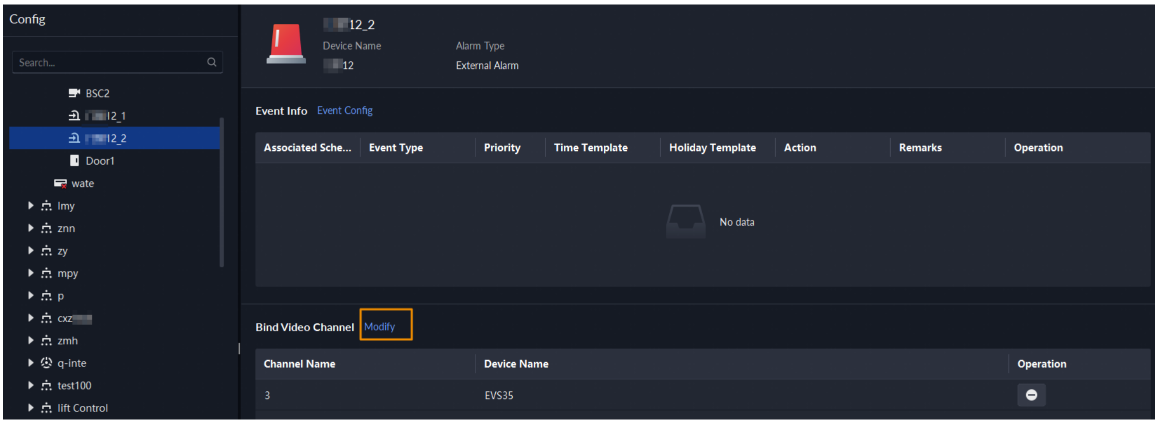
Procedure

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

Step 2 Click .

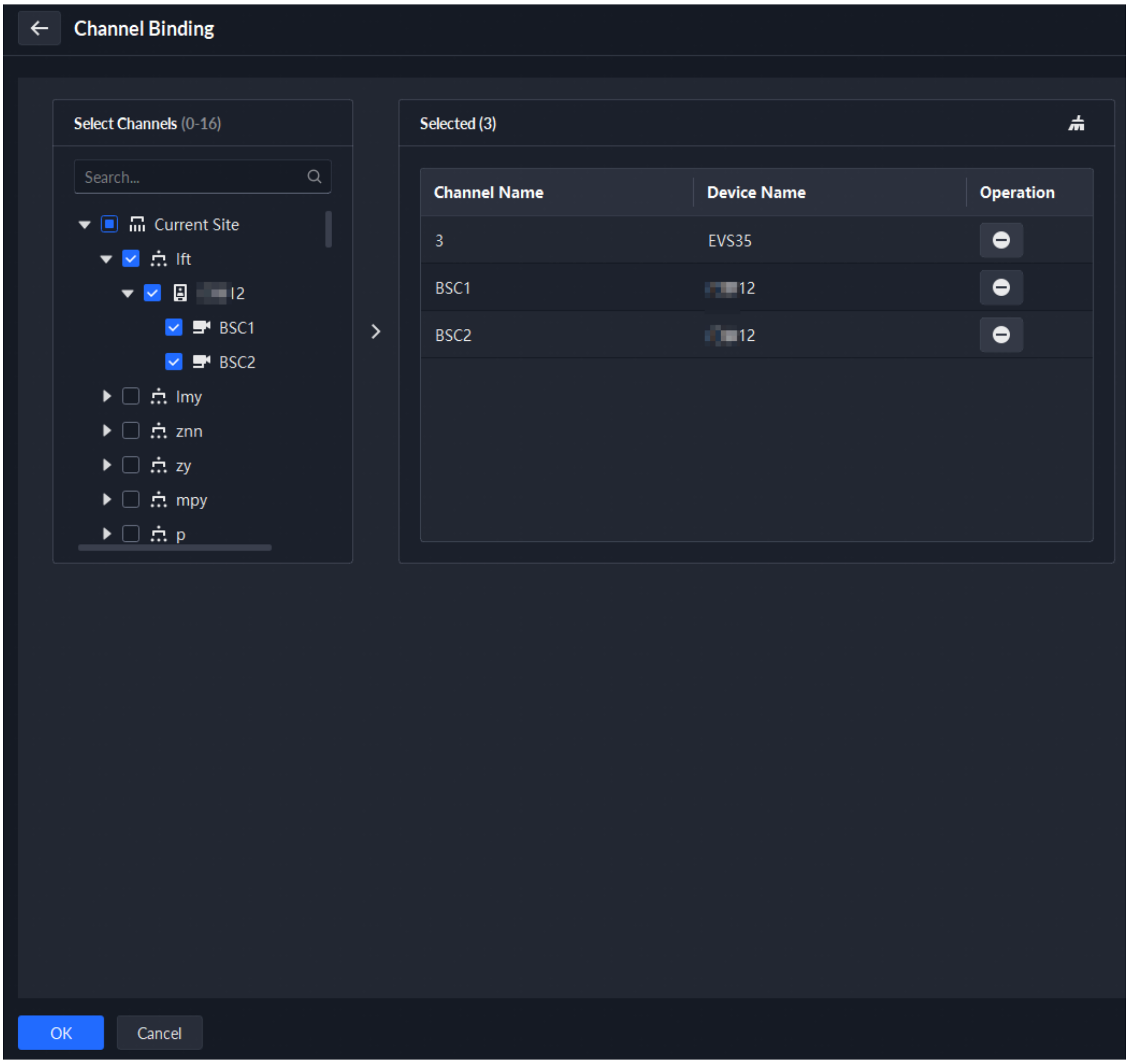
Step 3 Select a channel, and then click **Modify**.

Figure 5-17 Bind one or more channels



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

Figure 5-18 Select the channels you want to bind



Step 5 Click **OK**.

5.1.4 Adding Device Recording Plans

Configure recording plans for video channels so that they can record videos accordingly.

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 **Add Recording Plan** next to **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.

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

Table 5-1 Parameter description

Parameter	Description
Enable	Turn on or off the recording plan.
Position	Videos will be stored on the device by default. It cannot be changed.
Stream Type	The device will make recordings using the main stream by default. For channels of IVSS, you can select main stream or sub stream.
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 "5.1.5 Adding Time Template".

5.1.5 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**.

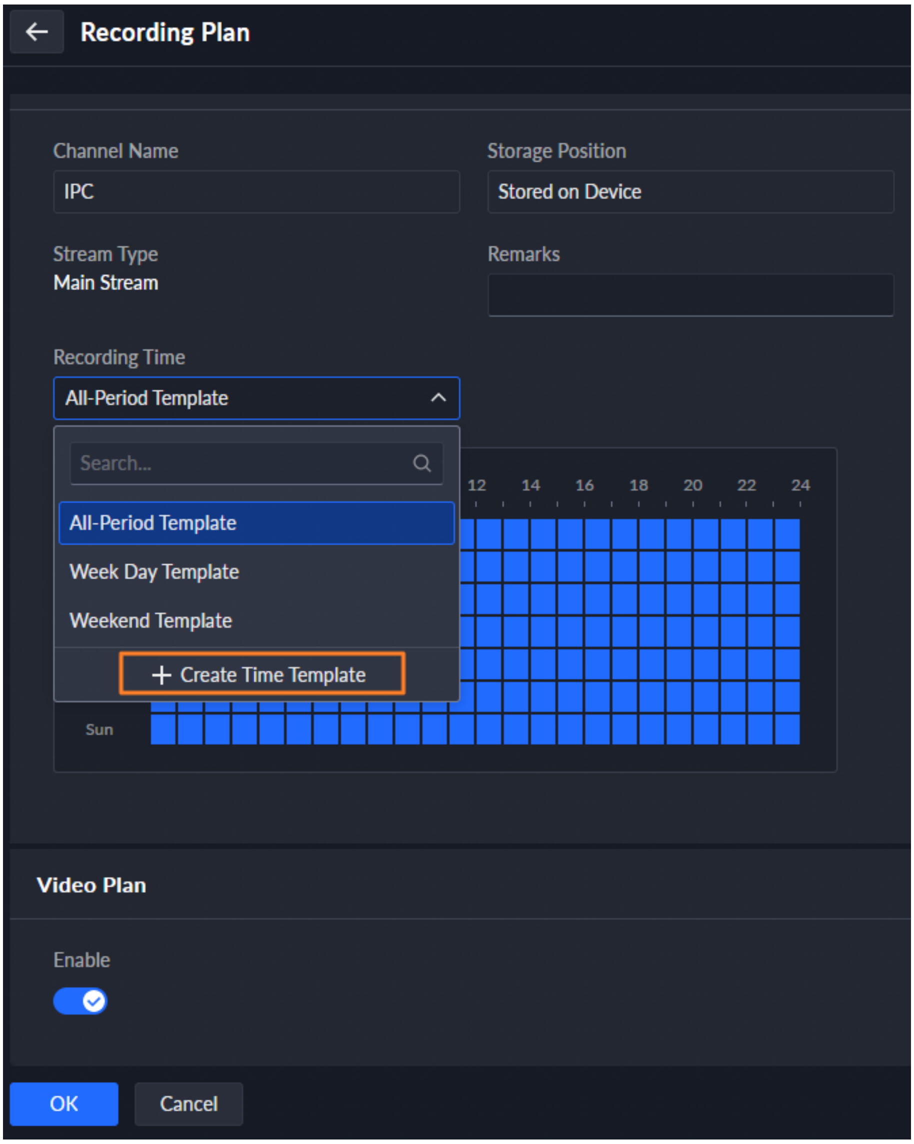
Step 2 Click .

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 5-19 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**.

5.1.6 Configuring Events

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

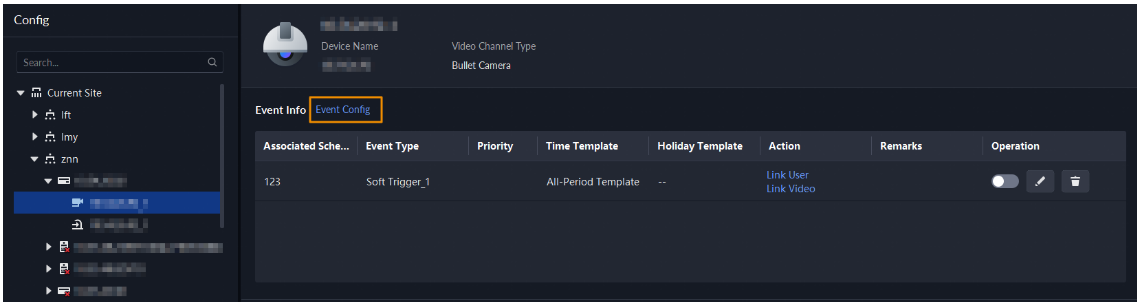
Procedure

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 5-20 Go to the event configuration



Step 3 Configure events. For details, see "6.1 Configuring Events".

5.1.7 Configuring Information Display Content

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

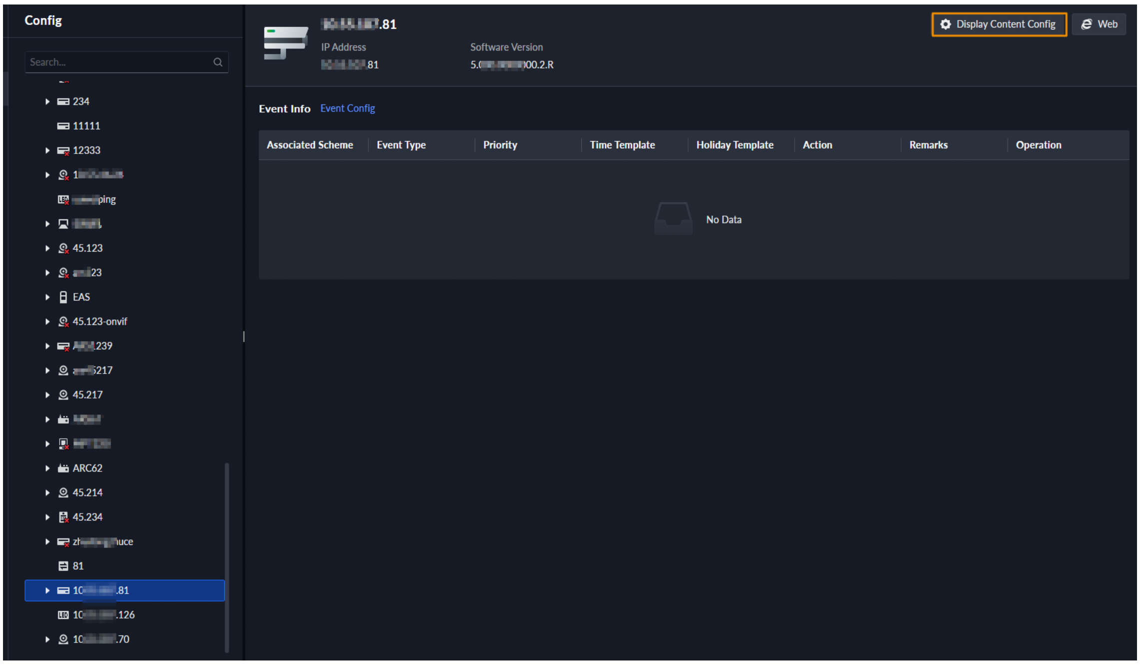
Procedure

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

Step 2 Click .

Step 3 Select the ANPR camera, and then click **Display Content Config**.

Figure 5-21 Display content configuration

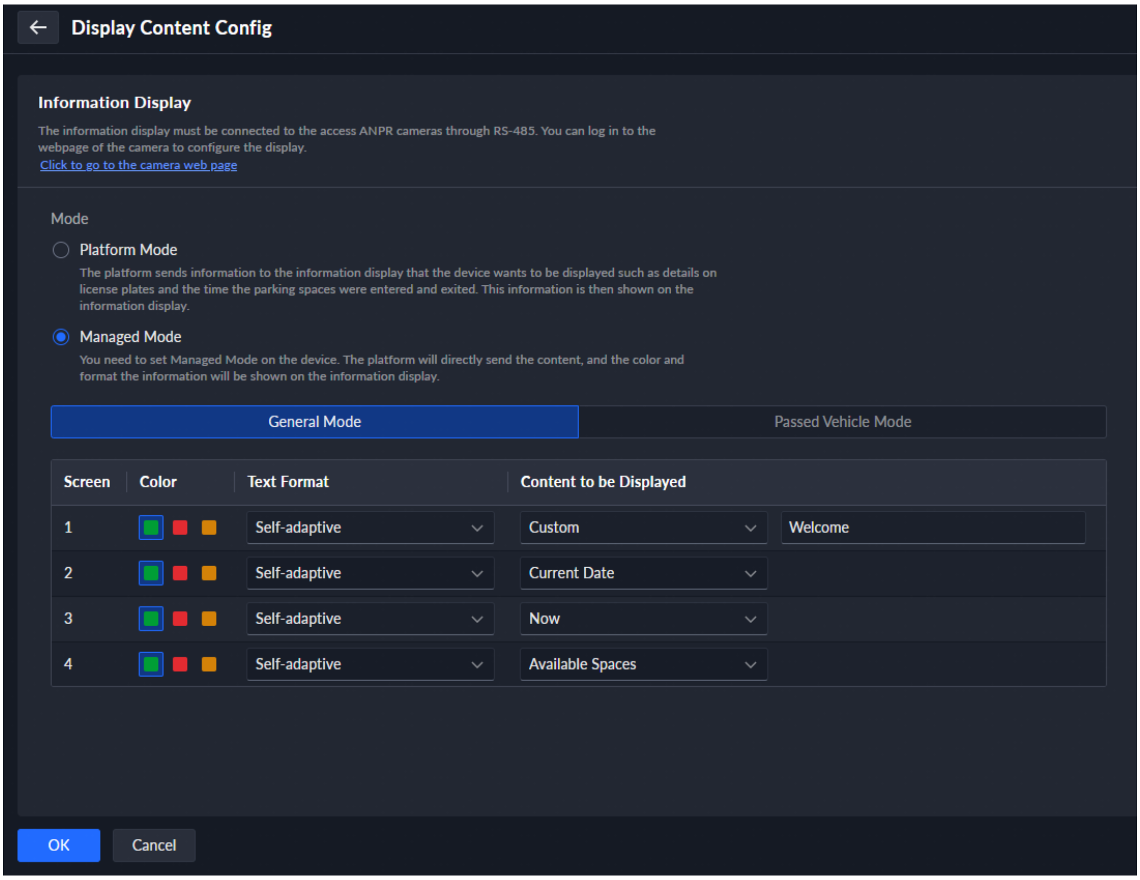


Step 4 Select **Platform Mode** or **Managed Mode**.

- **Platform Mode** : The platform sends information to the information display that the device wants to be displayed.

- **Managed Mode** : You need to set managed mode on the device. The platform will directly send the content.

Figure 5-22 Managed mode



◇ **General Mode** : The information to be displayed when no vehicles are detected passing by, including screen color, text style, content, and customized content.

◇ **Passed Vehicle Mode** : The information that needs to be displayed when a vehicle passes includes the screen color, text format, content, and customized content.

Related Operations

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

5.1.8 Configuring Door

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

Procedure

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

Step 2 Click .

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

Step 4 Configure the parameters.

Figure 5-23 Door configuration

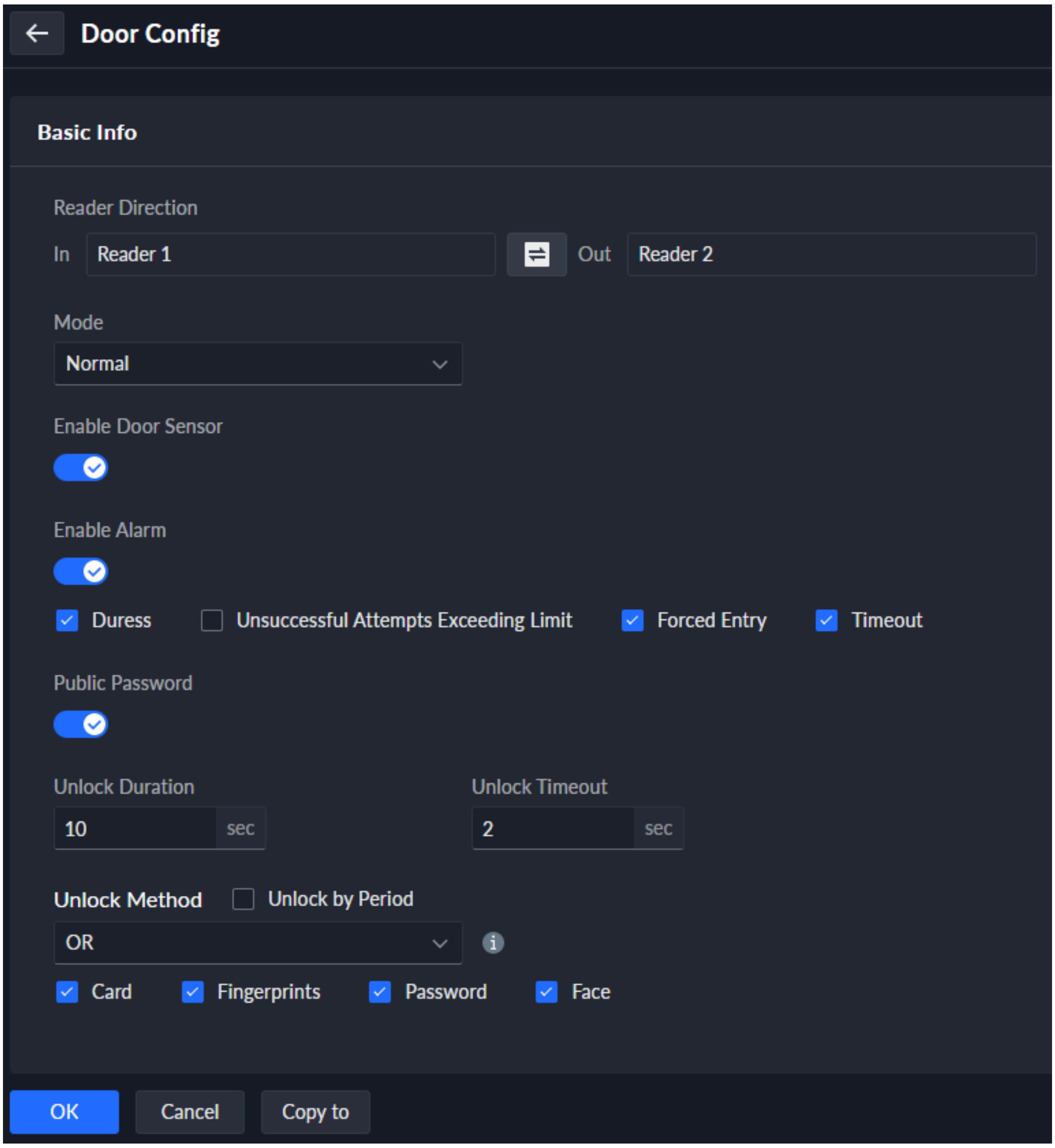


Table 5-2 Parameter description

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

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

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

Step 6 Click **OK**.

5.1.9 Synchronizing People Counting Rules

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

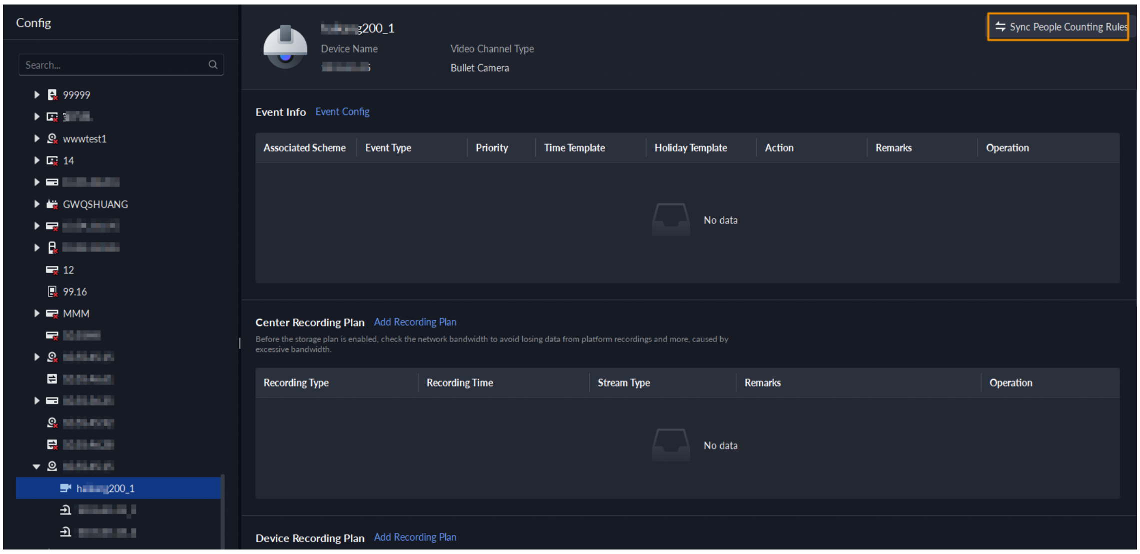
Procedure

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

Step 2 Click .

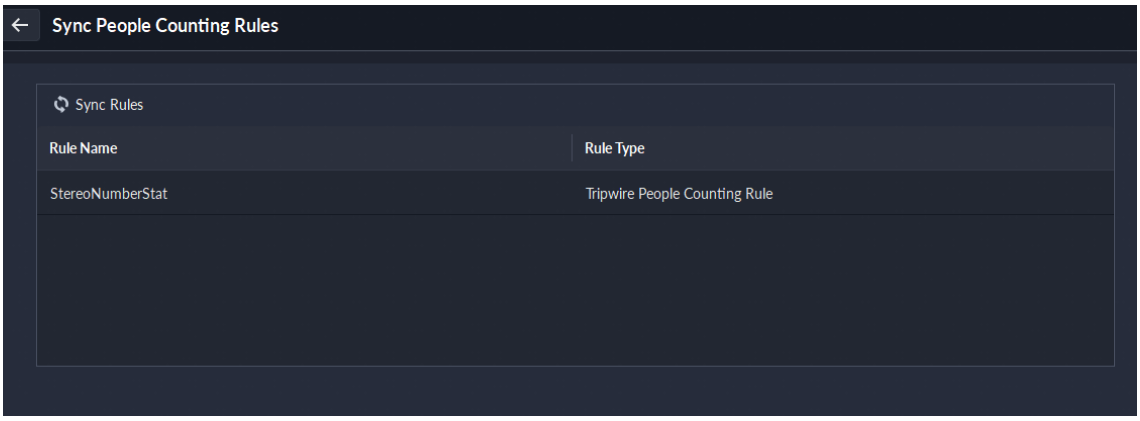
Step 3 Select a channel, and then click **Sync People Counting Rules**.

Figure 5-24 Synchronize people counting rules from the device (1)



Step 4 Click **Sync Rules**.

Figure 5-25 Synchronize people counting rules from the device (2)



5.2 Adding Roles and Users

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

5.2.1 Adding a Role

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

The following roles are available.

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

  The device and control permissions of this role cannot be edited, but its menu permissions can be edited.
- Common operator: This role has no permissions of basic configuration, storage, license, system parameters, and backup and restoring.

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

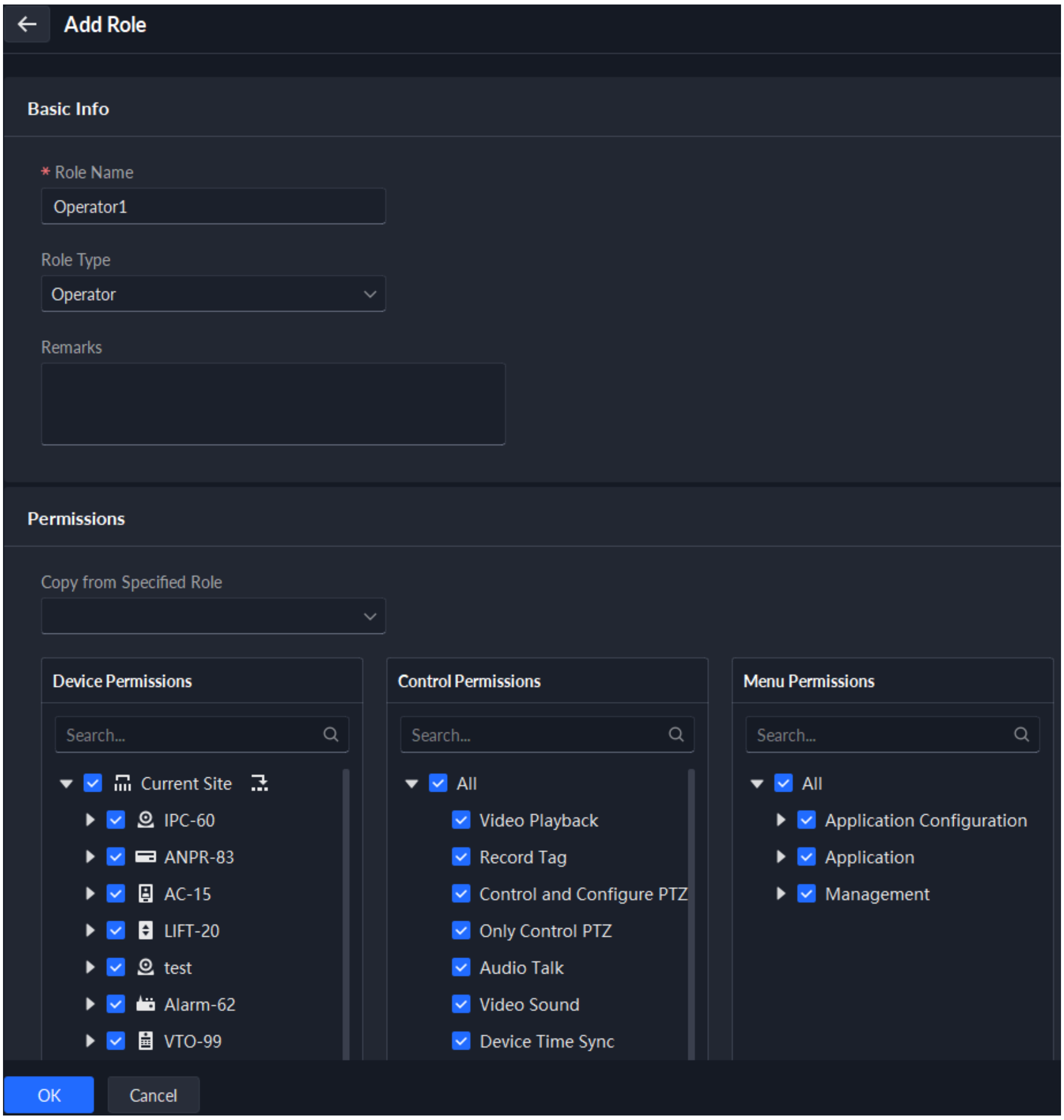
Procedure

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

Step 2 Click .

Step 3 Click **Add**, set role information, and then select device and control permissions and assign the rule to users.

Figure 5-26 Add a role



- If a device is not selected under **Device Permissions** or a menu not selected under **Menu Permissions**, all users assigned with this role will not be able to see the device or menu.
- Click of a selected organization. All permissions of subsequently added devices under this organization will also be assigned to users of this role.
- When the **Role Type** is set to **Operator**, you can copy the permissions from specified role.

Step 4 Click **OK**.

5.2.2 Adding a User

Create a user account for logging in to the platform.

Prerequisites

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

Procedure

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

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

Table 5-3 Parameter description

Parameter	Description
Username	Used to log in to the client.
Multi-client Login	Allow the user to log in to multiple clients at the same time.
Password	Used to log in to the client.
Confirm Password	
Enable Forced Password Change at First Login	The user is required to change the password at first-time login.
Enable Password Change Interval	Force the user to change the password regularly.
Enable Password Expiry Time	After the password expires, the user cannot log in to the client. If already logged in, the user will be forced to log out. The user must reset the password through email or contact the administrator.
PTZ Control Permissions	The PTZ control priority of the user. The larger the value, the higher the priority. For example, User A has a priority of 2 and User B has a priority of 3. When they operate on the same PTZ camera, which is locked, at the same time, the PTZ camera will only respond to the operations from User B.
Email Address	Used to receive emails in various situations, such as password reset, alarm messages, and visitor registration.
Bind MAC Address	Limit the user to log in from specific computers. One user can be bound to 5 MAC addresses at most.
Role	Select one or more roles to assign the user permissions, such as which devices are allowed to be operated.

Step 3 Click **OK**.

Related Operations

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

5.2.3 Adding a User Group

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

Prerequisites

You need to add users first.

Procedure

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

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

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

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

One user can be only added to one user group.

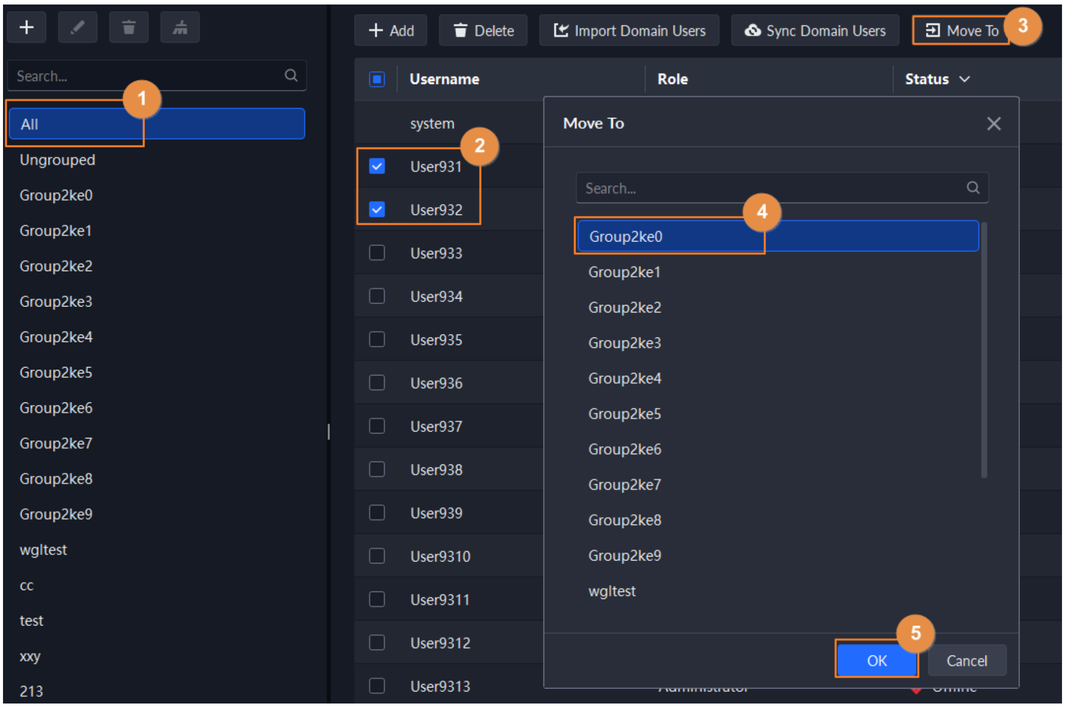


Figure 5-27 Move users to a user group

Step 5 Click **OK**.

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

Related Operations

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

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

5.2.4 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.

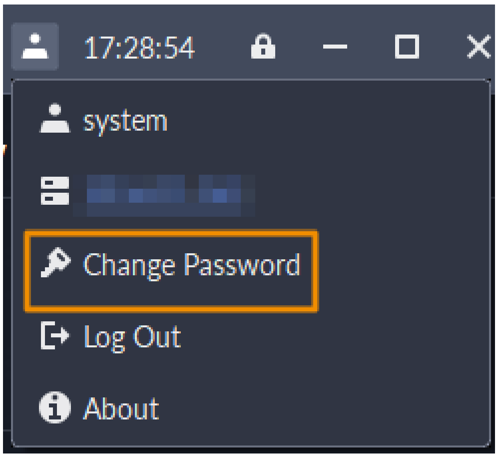
5.2.4.1 Changing Password for the Current User

We recommend changing your password regularly for account safety.

Procedure

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

Figure 5-28 Change password



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

5.2.4.2 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**.

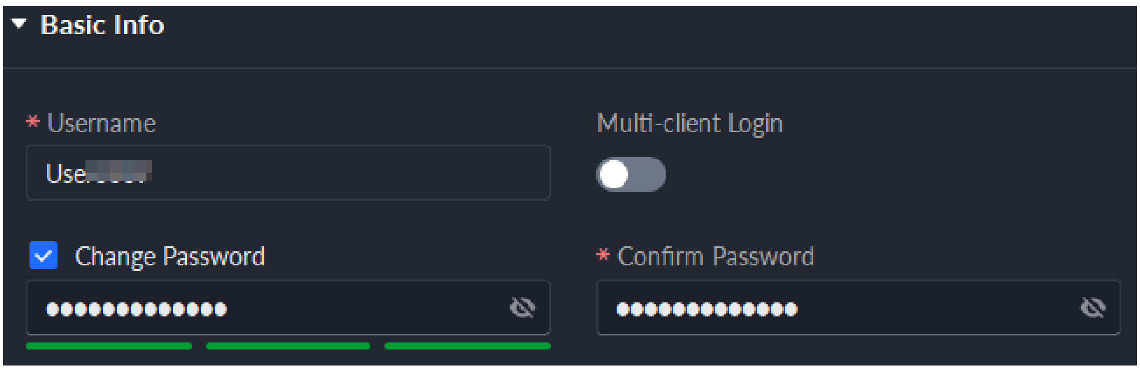
Step 2 Click .

Step 3 Select a user, and then click .

Step 4 Enable **Change Password**, and then enter the password of the current login user for password verification.

Step 5 Enter the new password, and confirm password, and then click **OK**.

Figure 5-29 Change passwords for other users



5.2.4.3 Resetting User Password

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

Procedure

Step 1 On the login page, click **Forgot password?**.

Step 2 Enter the account that you want to reset the password for, and then click **Next Step**.

Step 3 Select how you want to reset the password.

- By security questions. This is only applicable to the system user.
  1. Click **Reset Password through Security Questions**.
  2. Answer the questions, and then click **Next Step**.
- By reset file. This is only applicable to the system user.
  1. Log in to the management tool.
  2. Click , and then select **Reset System Password**.
  3. Click **Export**, set the encryption password, and then export the request file.
  4. Contact the technical support to get the password reset file through the request file.
  5. Click **Reset** to import the reset file, and then log in the DSS client to initialize the password.
- By email address. This is applicable to all accounts, but an email address must be configured first. For details, see "5.2.2 Adding a User".
  1. Click **Reset Password through Email Verification**.
  2. Click **Send Verification Code**.
  3. Enter the verification code that you received from the email address, and then click **Next Step**.

Step 4 Set a new password and confirm it, and then click **Next Step**.

The password has been reset.

5.2.4.4 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.

5.3 Configuring Storage

Manage the storage of the platform, including setting storage types to store different types of files, and setting the storage location and retention period of the images and recorded videos from devices.

5.3.1 Configuring Server Disk

Configure local disk to store different types of files, including images, and normal files. 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.

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

5.3.2 Configuring Device Storage

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 platform.

Procedure

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

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

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

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

Table 5-4 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 platform. • **Link to Images on Device** : All images produced by the channels connected to this device will be stored on the device itself. The platform will obtain images from the device.
Event Video Storage Location	**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.

6 Businesses Configuration

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

6.1 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.

6.1.1 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 6-1 Parameter description

Parameter	Description
Device, video channel, alarm input channel, subsystem, zones, access control channel, parking lot, people counting group, and lift control channel	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 "5.1.2.5.2 Modifying Device Information". ● If **Alarm Input Channel** is selected, check whether the **Triggered Event** that you select matches the channel feature of the alarm input channel you select. Otherwise, the event will not be triggered.
Soft Trigger	This is a type of event that is manually triggered. Click to customize its name and icon. When viewing the live video image of the configured channel in the **Monitoring Center**, you can click the icon to trigger an alarm manually.
Combined Event	When a combined event is triggered, the platform performs the defined linked actions. For how to configure combined events, see "6.1.2 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 "6.1.4 Configuring Generic Event".

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

Table 6-2 Parameter description

Parameter	Description
Scheme Name	Enter a name for the scheme.
Priority	The priority level is used to quickly know the urgency of the event when it is triggered.
Time Template	Select a time template for when the event can be triggered. If you want to create a new template, see "5.1.5 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**.

Parameter	Description
Alarm Storm Config	After enabled, if certain alarms are frequently triggered, you can configure an interval during which they can only be triggered once. For example, a tripwire alarm can only be triggered once in 10 seconds. This function is only available to event sources selected in the previous step. The configurations here enjoy higher priority if alarm storm for the same event is configured from **Event** > **Alarm Config** > **Alarm Storm Config**.
Remarks	Enter remarks on events.

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

Step 6 Configure alarm linkage actions.

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

Table 6-3 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 "5.1.3 Binding Resources". ◇ Select camera: Select a camera so that you can view the camera video when the associated alarm is triggered.
When an alarm is triggered, display camera live view on client	Enable this parameter, and then the platform will open the real-time video of the channel where an alarm is triggered, and play it in the defined stream type. After the event is configured, select **Local Settings** > **Alarm**, enable **Open Alarm Linkage Video** and set how the video will be opened, **As Pop-up** or **Open in Live View**. For details, see "10.4.4 Configuring Alarm Settings".
Event Recording	The platform will link device recordings when an alarm is triggered.
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.
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.

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

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

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

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

  You must add a video wall and configure its alarm on video wall mode first. For details, see "7.1.5.1 Configuring Video Wall" and "6.1.3.2 Configuring Alarm on Video Wall".

  If you set **Camera** to **Select Camera**, you can configure which channels to be displayed on the specified video wall. When the video wall you select is configured with the override mode, you can also select **Customize Alarm Window**, and then you can select which channels to be displayed on the specified windows of the video wall.
- To execute an HTTP URL command, enable **Link HTTP URL Command** . Click **Add**, and then click **New** to add a new command, or **Copy from Quick Command**. When adding a new command, you need to set the name of the command, the request method, HTTP URL, and remarks. You can click to test if the command is valid.

  When selecting **POST** or **PUT**, you can click to customize the body of HTTP URL.
- To link emails, enable **Email**, and click to add the email address, and then an email will be sent to the selected email address when an alarm is triggered. You can also manually enter an email address, but you must press Enter to make it valid.

  To configure the email template, select **Add Email Template** from the **Email Template** drop-down list.
- To link client sound, enable **Client Sound**, and then enter the audio content (up to 50 characters). When an alarm is triggered, the client will play the defined audio content.

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

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

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

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

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

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

The users will only receive notifications when they are logged in. If you need to add more users, see "5.2 Adding Roles and Users"; to add more user groups, see "5.2.3 Adding a User Group".

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

Step 9 Click **OK**.

6.1.2 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 6-4 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.

6.1.3 Configuring Alarm Parameter

6.1.3.1 Filtering Repetitive Alarm

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

Procedure

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

Step 2 Click **Add**.

Step 3 Select event sources and events, and then configure the interval.

Step 4 Click **OK**.

6.1.3.2 Configuring Alarm on Video Wall

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

Prerequisites

You must add a video wall first. For details, see "7.1.5.1 Configuring Video Wall".

Procedure

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

Step 2 Click .

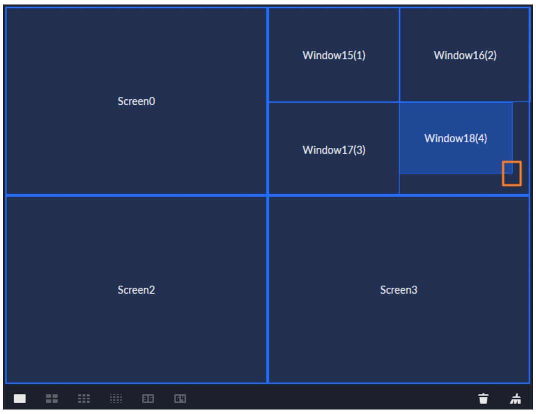
Step 3 Select a mode, and configure related parameters.

Table 6-5 Parameter description

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

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

Table 6-6 Parameter description

Parameter	Description
Set the number of windows	There is only 1 window by default. Click it, and then you can set the number of windows to 4, 9, 16, 32, or 64.
Resize a window	● Click a window, and then drag its frame near the lower-right corner to resize it.  ● Right-click a window and then select **Properties**. Configure the left margin, top margin, width, and height to resize the window.
Adjust the locations of windows	Drag the windows to adjust their locations. This operation will not change the order of the windows. The order is used to determine which window will be used to display videos first in loop mode. The number at the end of the name of a window indicates its order. For example, a window named Window (2) means that it is the second window.
Change the names of windows	● Right-click a window, and then select **Rename** to rename a window. ● Right-click a window, select **Properties** , and then rename it in **Window Name**.

Step 5 Click **OK**.

6.1.4 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 6-1 Add generic event

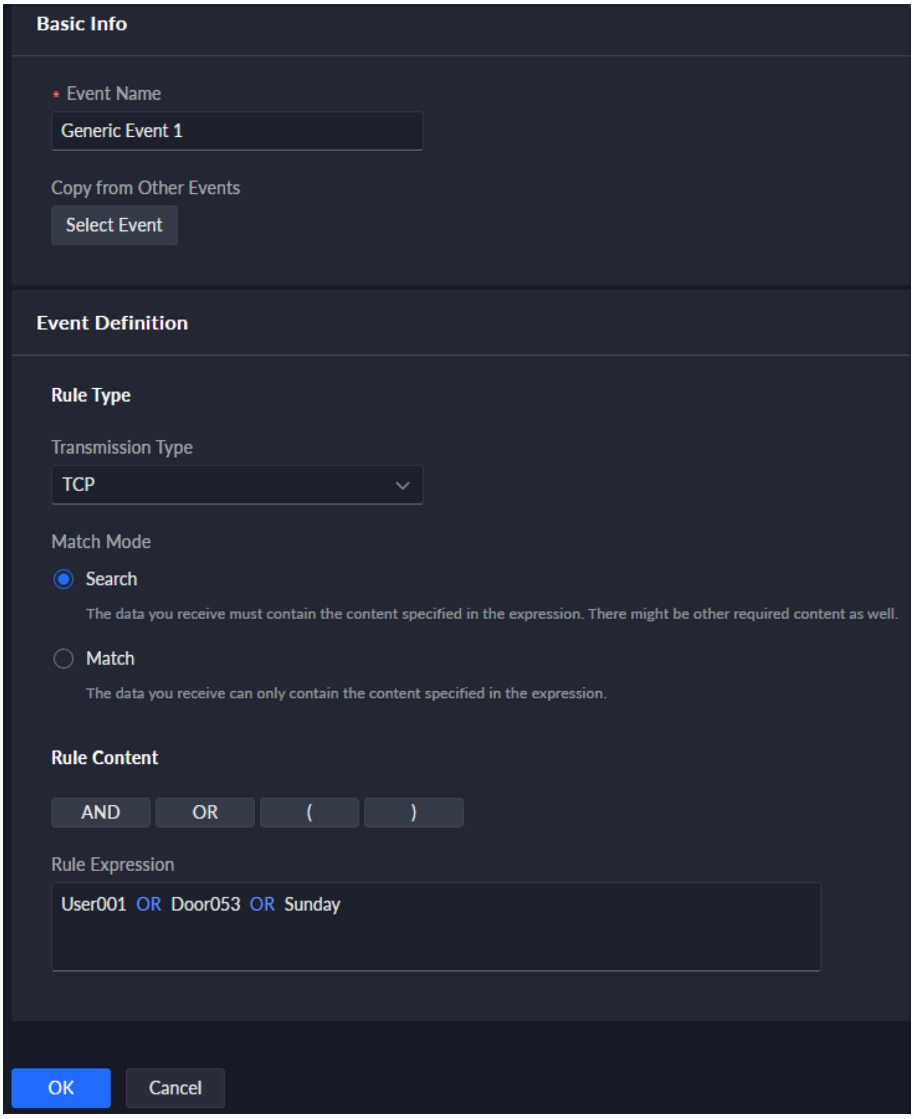


Table 6-7 Parameter description of generic event

Parameter	Description
Event Name	The name that identifies the event.
Select Event	Click **Select Event**, select from the existing generic event, and then the system automatically fills in parameters of the selected event (event name excluded).
Transmission Type	TCP, UDP, HTTP, and HTTPS are available.
Match Mode	Select **Search** or **Match** according to onscreen instructions.

Parameter	Description
Rule Content	Select **AND** , **OR**, **(,)** rules, and then set the rule expression. The system operates the expression from left to right.
Rule Expression	Select AND, OR, and ( ) operations and set the expression. The system operates on expressions from left to right. • **AND** and **OR** must be preceded and followed by characters; **(** and **)** must appear in pairs. • Rule expression supports HTTP URL, for example,http://192.168.1.1:9090/ test/Keywords/Newwords/Header/Body xxxxxxxxxxxxxxxx.

Step 3 Click **OK**.

6.2 Configuring Map

6.2.1 Preparations

- Devices are deployed. For details, see device user manuals.
- Basic configurations of the platform have been finished. For details, see "5 Basic Configurations".
- To show device alarms on the map, make sure that **Map flashes when alarm occurs** is enabled in **Home** > **Management** > **Local Settings** > **Alarm**.

6.2.2 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.

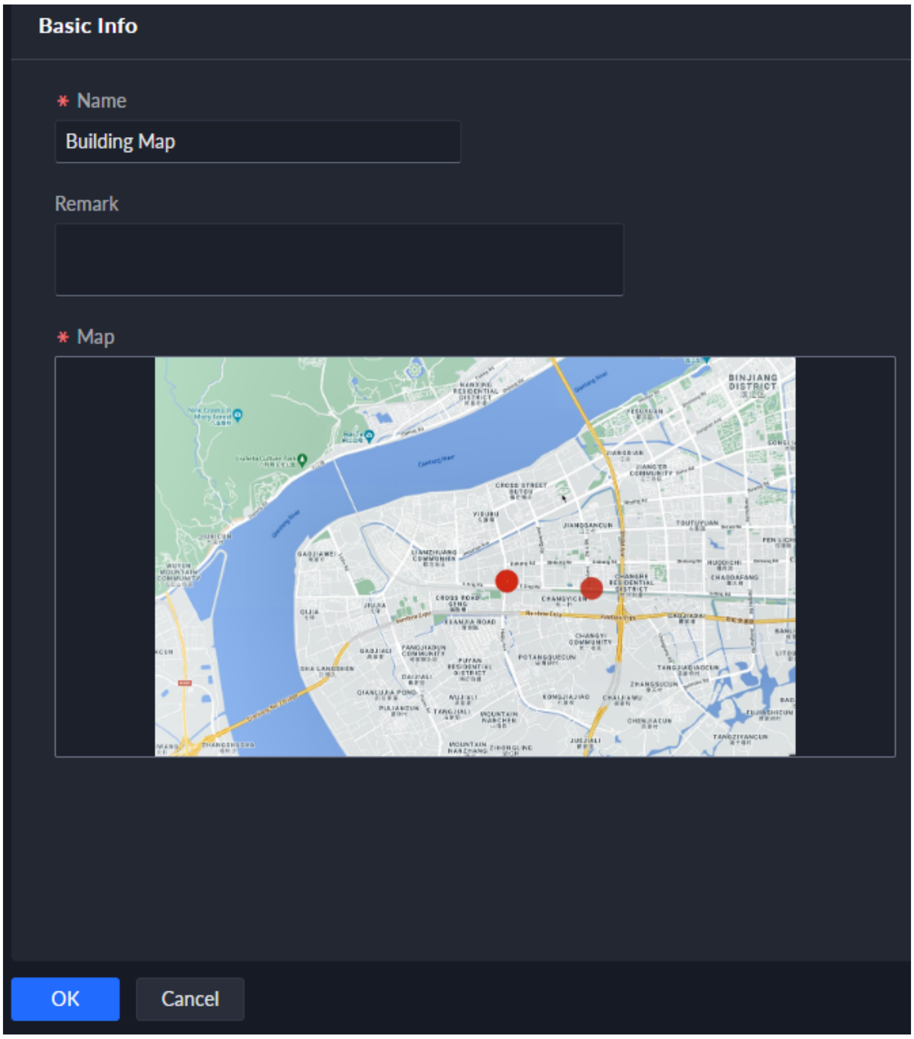
Procedure

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 picture and then click **OK**.

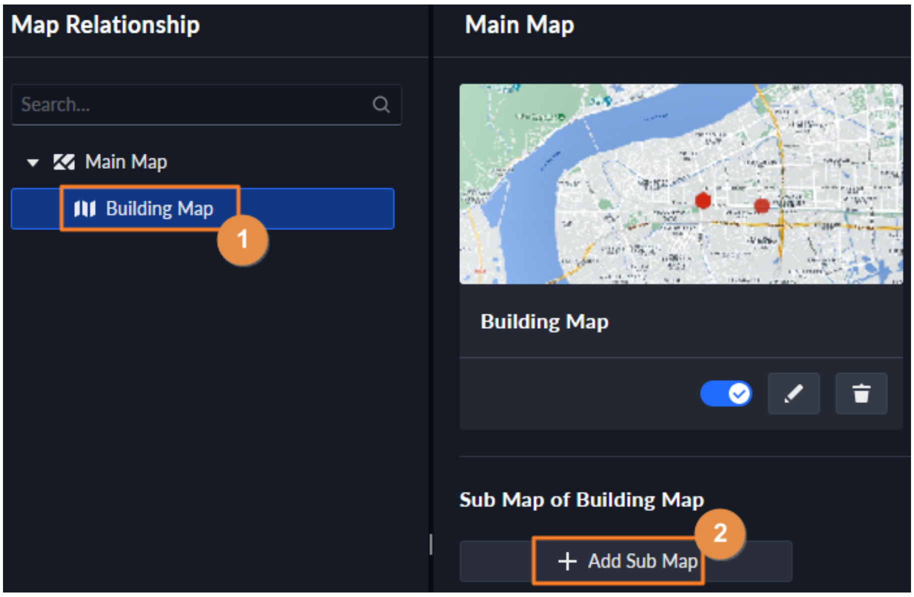
Figure 6-2 Add main map



Step 4 Add a sub map.

1. Click the added raster map, and then click **Add Sub Map**.

Figure 6-3 Add sub map



2. Enter the map name, upload the map image, and then click **Next Step**.
3. Drag the image to the desired position and click **OK**.

Related Operations

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

- View device details

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

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

  To move a device, click **Move** and then drag the device on the map.
- Configure static visible range

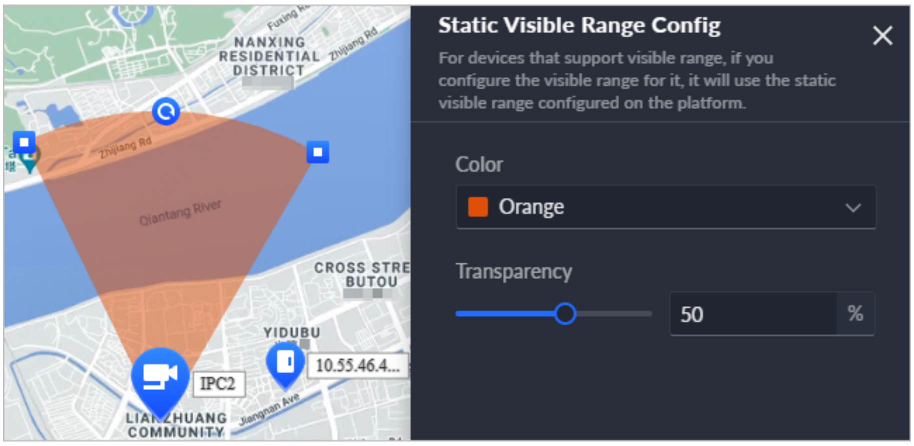
  For devices that do not support sending visible range to the platform, you can customize the visible range on the map. After that, when you monitor or track back a target, you can quickly find the monitoring devices according to the visible range.

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

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

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

  Figure 6-4 Configure static visible range



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

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

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

- Clear

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

- Add a sub map

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

  ◇ Click to edit the sub map.

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

- Length

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

- Area

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

- Add Mark

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

- Reset

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

6.2.3 Marking Devices

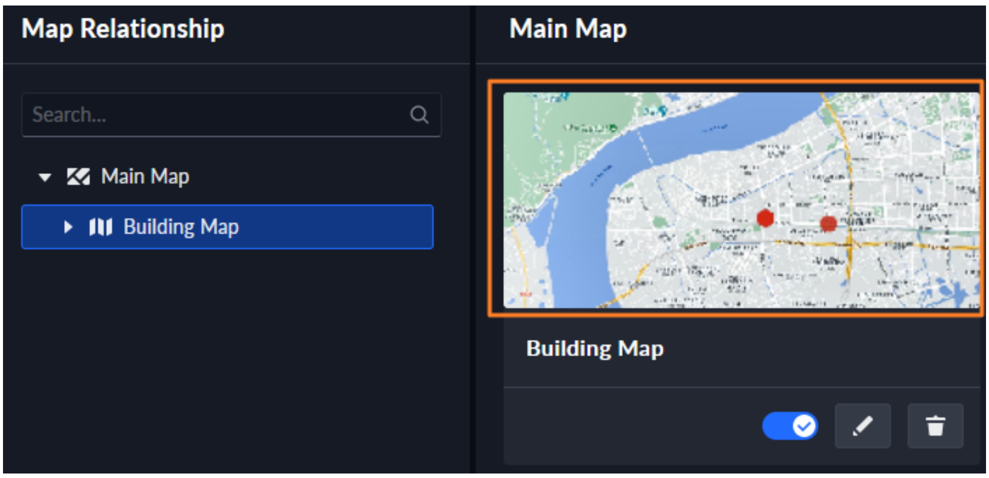
Link a device to the map by dragging it to the corresponding location on the map according to its geographical location.

Procedure

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

Step 2 Click the map.

Figure 6-5 Map



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

6.3 Personnel and Vehicle Management

Configure personnel and vehicle information for the applications of access control, vehicle control, attendance management, 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.

6.3.1 Adding Person and Vehicle Groups

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

Procedure

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

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

Step 3 Click , and then configure the parameters.

Table 6-8 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 "6.3.2 Configuring Person Information".

Related Operations

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

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

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

6.3.2 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.

- The information of a person must be the same on the platform and access control devices, such as the person ID and card number. Otherwise the attendance data of this person cannot be synchronized between the platform and access control devices.
- To collect fingerprints or card number, connect a fingerprint collector or card reader to the computer where the PC client is installed.

6.3.2.1 Extending Person Information

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

Procedure

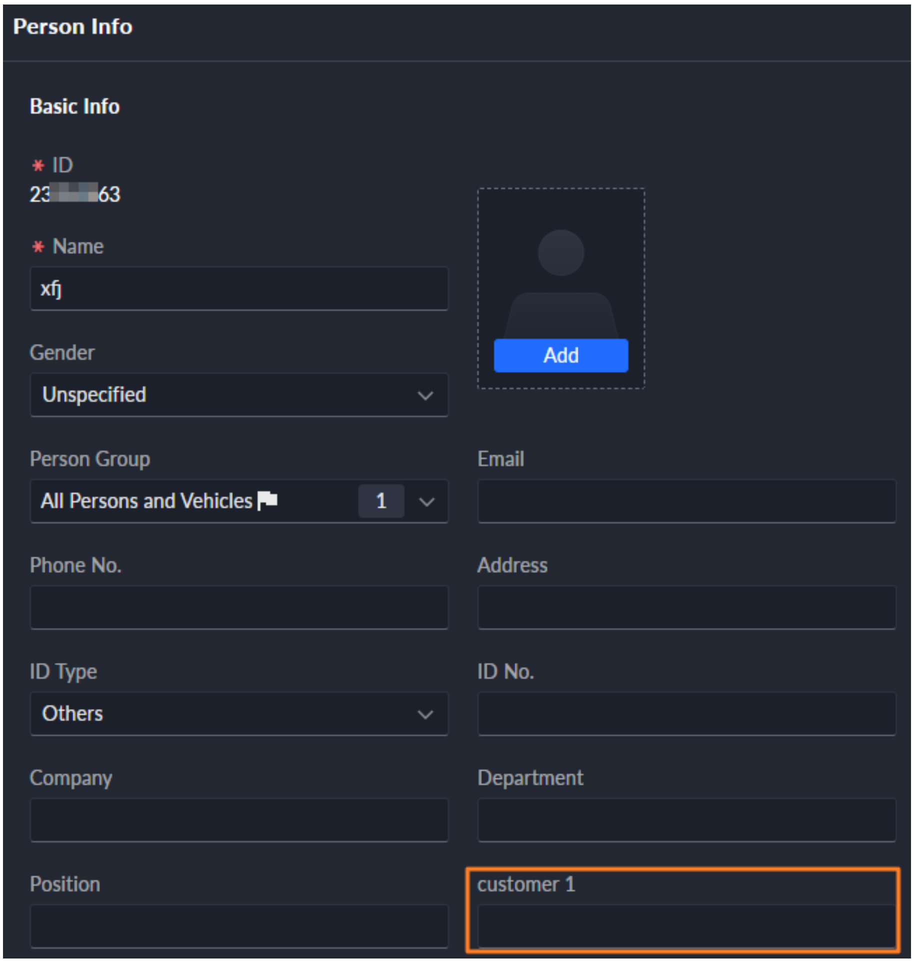
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Person and Vehicle Info**.

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

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

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

Figure 6-6 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.

6.3.2.2 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**.

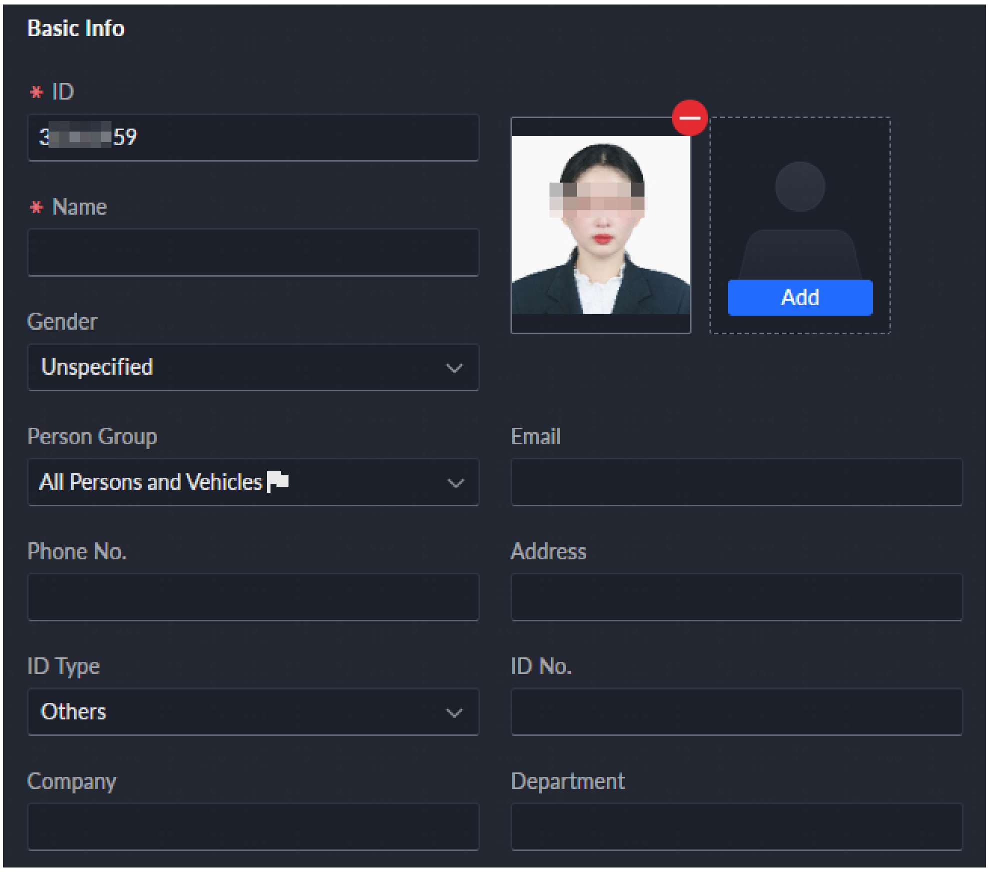
Step 2 Select **Person List** > **Persons** > **Add**.

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 6-7 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 "6.3.2.5 Importing Images of People".

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

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

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

Table 6-9 Parameter description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Card</td><td>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.</td></tr>
<tr><td>Fingerprints</td><td>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.</td></tr>
</table>

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

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

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

Table 6-10 Parameter description

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

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

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

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

     ◇ Access rules can be configured from > **Access Control** > **Access Rule** > **All Rules**.
   - VIP: When using an access point, the person is restricted by all rules except combination unlock (card, fingerprint, face, and password), multi-person unlock, and unlock by period rules.

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

     ◇ Multi-person unlock and other rules can be configured from > **Access Control** > **Access Rule** > **All Rules**.
   - Patrol: When the person uses an access point, a patrol event is reported, and the door will not open.
   - Blocklist: The person cannot use an access point. Also, a blocklist event is reported. People in blocklist are subject to the global anti-passback rules.
   - Extend time: When the person uses an access point, if the access point is a door, the door will stay unlocked for additional 5 seconds.
2. Configure validity period. The person is only effective within this period. You can modify the value to extend the validity period.
3. Select **Quote** > **Add**, and then configure the access rules.

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

Figure 6-8 Available access rules

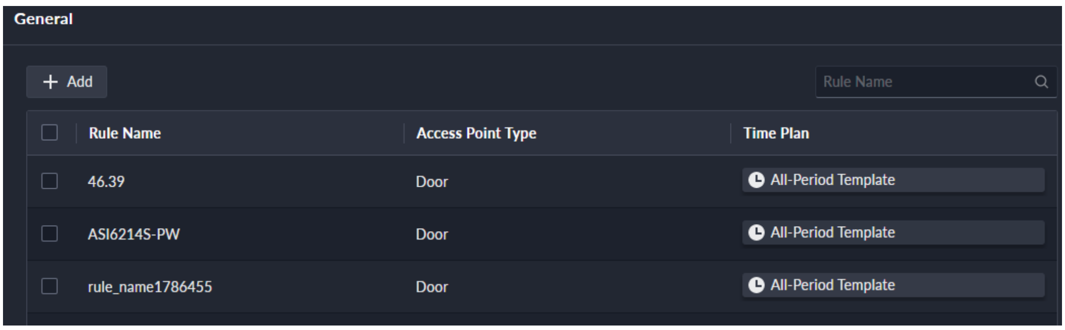
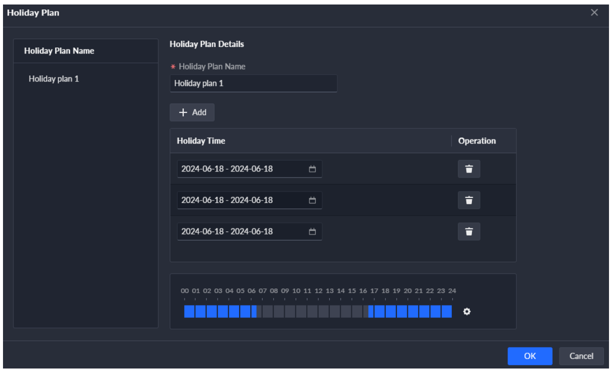


Table 6-11 Parameter description

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 "5.1.5 Adding Time Template".
Holiday Plan	Select a holiday plan when the rule will not be effective. You can add up to 4 holiday plans. Follow the steps below to create a holiday plan: **Lift** does not support holiday plans. 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 "6.5.2 Configuring Zone".
Select by Access Point	Select one or more access points. This person will have access permissions to all these access points.

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

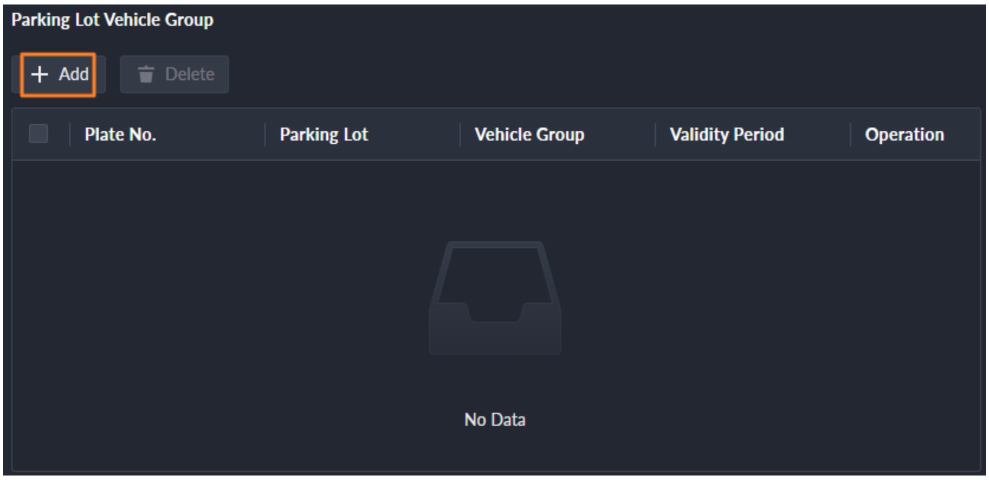
Step 6 If you want to recognize this person by face images, add the person to a face arming group.

You need to create a face arming group first. To add one, select **Add Face Arming Group** in the drop-down list. For details, see "6.4.1.1 Creating Face Arming Group".

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

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

Figure 6-9 Parking lot vehicle group



Step 8 Click **OK**.

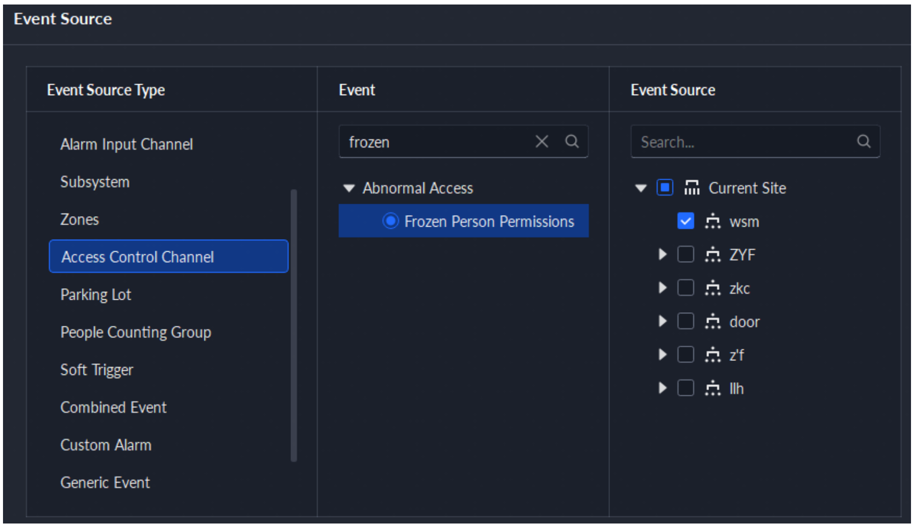
Related Operations

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

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

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

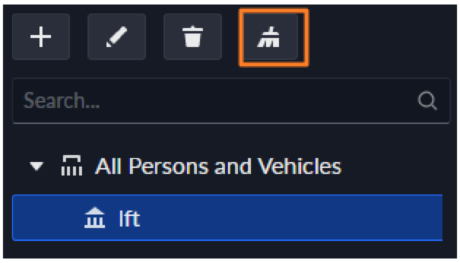
Figure 6-10 Configure frozen person permissions event



- To delete a person:
  - Click to delete a person and associated permissions.
  - Select multiple people, and then click **Delete Selected Items** to delete them and associated permissions. If you delete more than 10 persons, you must verify your login password.

◇ Select a person and vehicle group, and then click to delete all the persons and their permissions in the group. To perform this operation, you must verify your login password.

Figure 6-11 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.

6.3.2.3 Importing Multiple People

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

Prerequisites

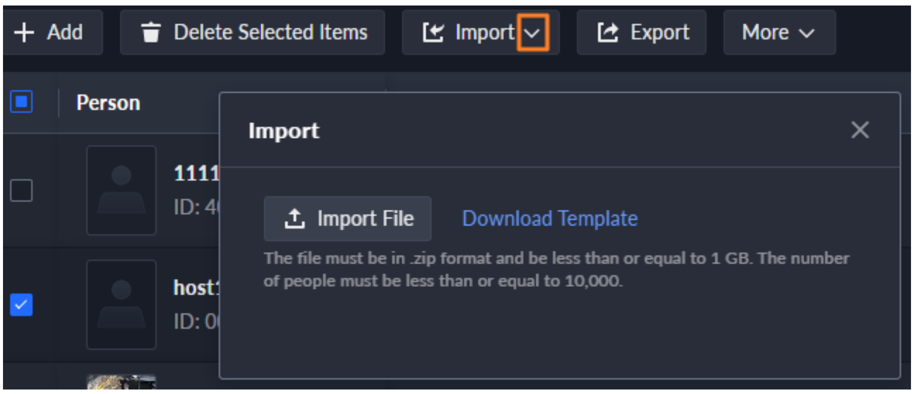
- Prepare an .xlsx file that includes the information of the people you want to import, their face images (optional), and then compress them into a .zip file. The .xlsx file can include information of up to 5,000 people. The .zip file cannot be greater than 1 GB.
- If a person belongs in a first-person unlock rule, set the access type of the person to **General**.

Procedure

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

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

Figure 6-12 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 "6.3.2.4 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**.

6.3.2.4 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.

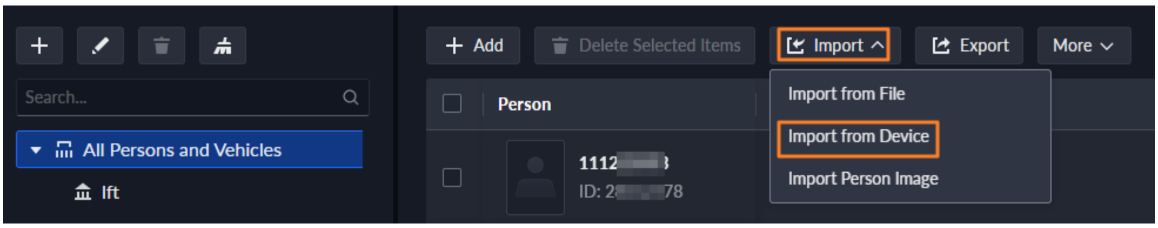
Procedure

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 6-13 Import from device

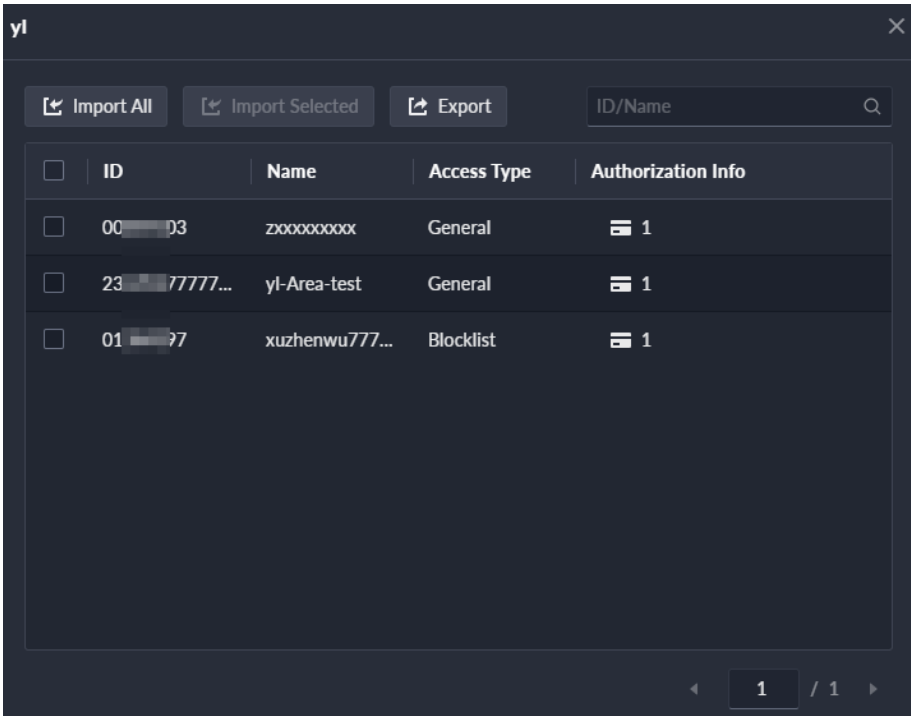


Step 4 Click , select a channel from an access control device or door station, and then click **OK**.

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

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

Figure 6-14 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**.

6.3.2.5 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:

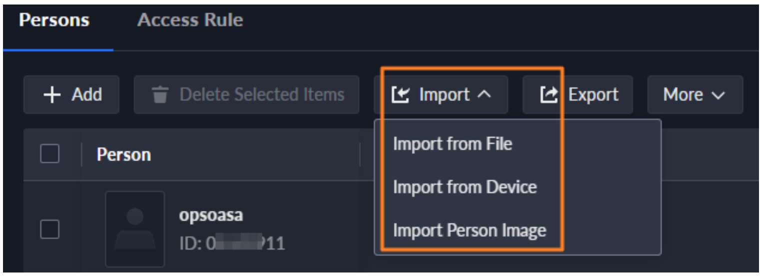
- A person can have up to 2 images, but only certain devices support recognizing people with 2 images.
- The image must be in .jpg format, and has a resolution ranging from 150 × 300 to 540 × 1080. It is preferred that it be 500 × 500. The image must not exceed 100 KB.
- Make sure that there is only 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 6-15 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.

6.3.2.6 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.

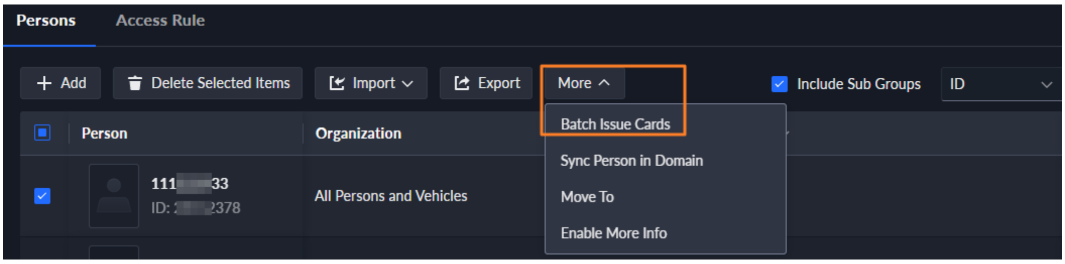
6.3.2.7 Issuing Cards in Batches

Procedure

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

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

Figure 6-16 Issue card in batches



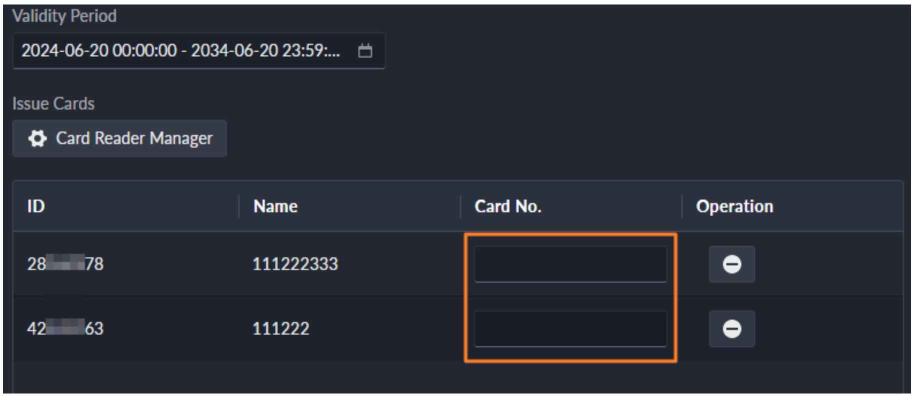
Step 3 Set validity period.

Step 4 Issue cards to personnel.

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

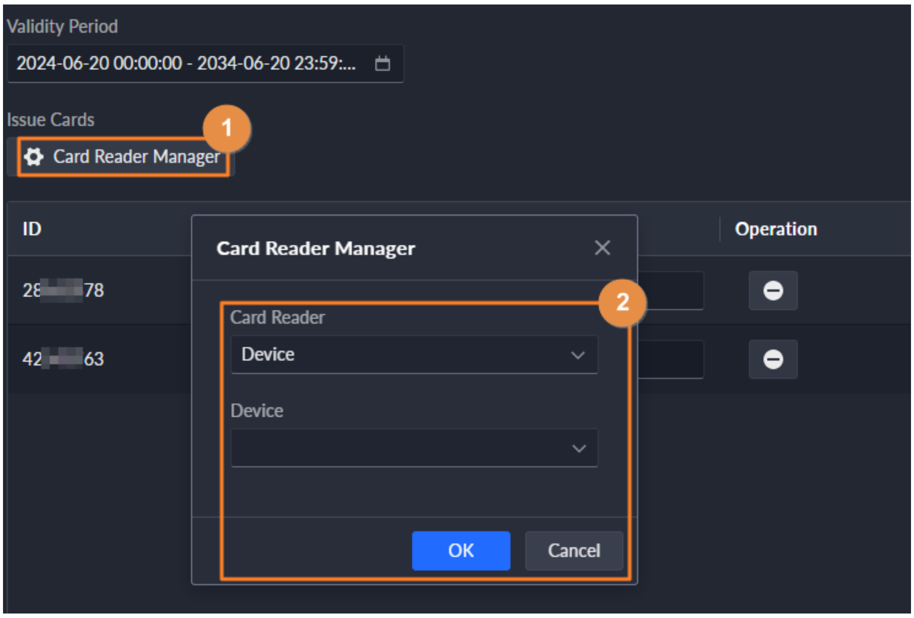
- By entering card number
  1. Double-click the **Card No.** input boxes to enter card numbers one by one.
  2. Click **OK**.

Figure 6-17 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 6-18 Reader manager



6.3.2.8 Deleting People

Notes

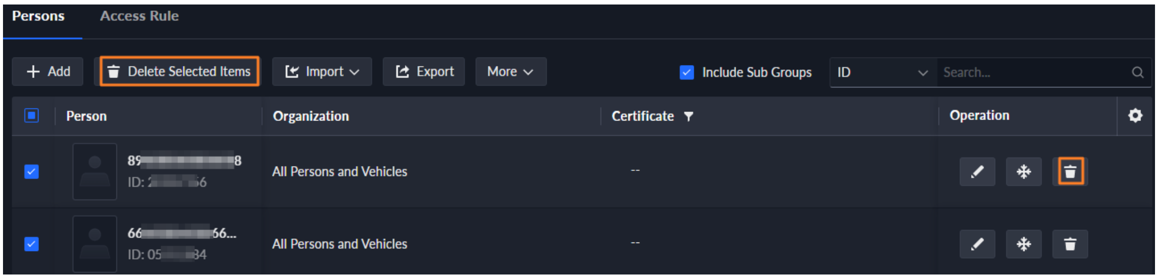
- After deleting people, their permissions (including vehicle access, person access, vehicle arming, person arming and parking lot permissions of vehicles) will also be deleted.
- After deleting people, the vehicles associated with the person will also be automatically deleted. After deleting a vehicle,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

Operations

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

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

Figure 6-19 Delete people



6.3.2.9 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 "6.3.2.2 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.

6.3.2.10 Searching for and Filtering People

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

Searching for People

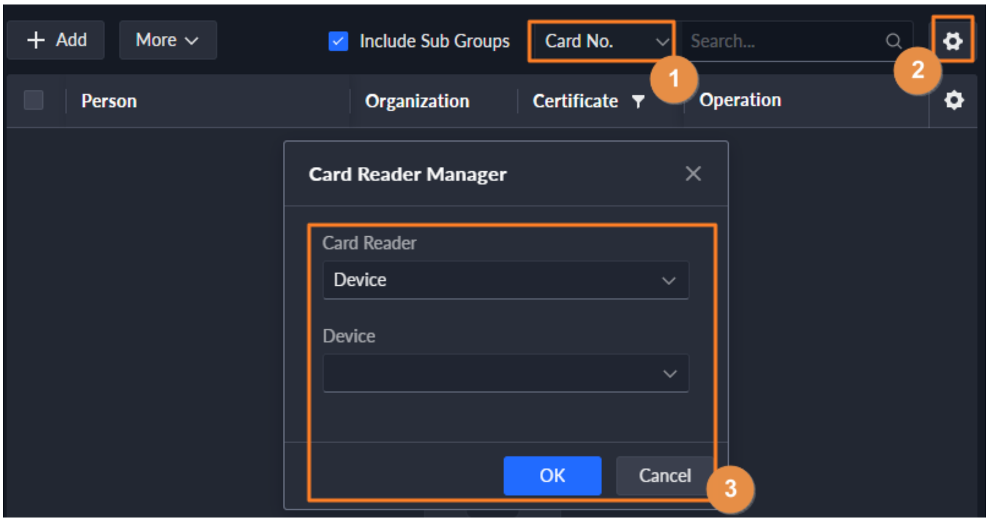
Select a person and vehicle group, enter keywords in the search area on the upper-right corner, and then click or press Enter to search for people who have that information. If **Include Sub Groups** is selected, the platform will also search for people in the sub groups of the one that you select.

Filtering People

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

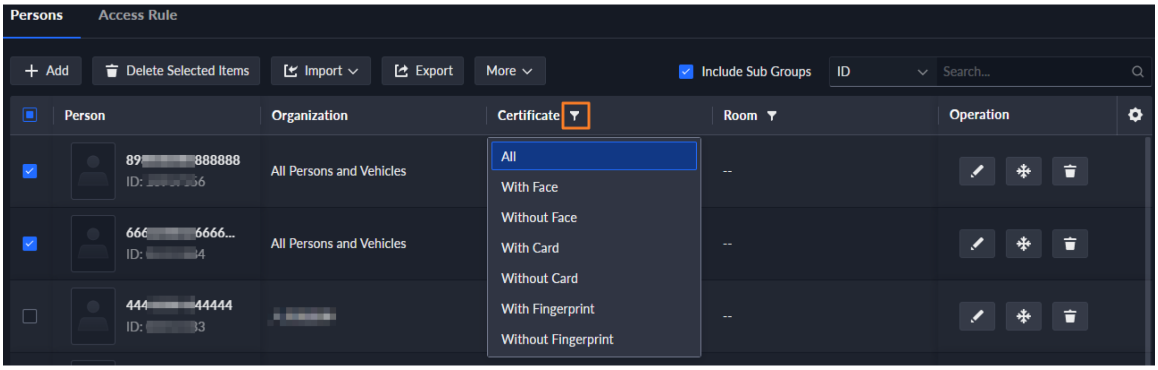
For example, when **Card No.** is selected, click , and then select swiping the card with a card reader or a device. When you swipe the card, the platform can directly read the card number and search, with no need of manually entering the card number.

Figure 6-20 Search by card number



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

Figure 6-21 Filter by certificate



6.3.2.11 Configuring Access Rule

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

Procedure

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

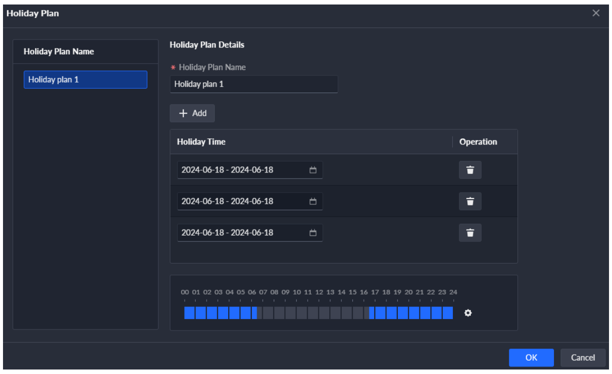
Step 2 Click a group, and then click **Access Rule**.

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

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

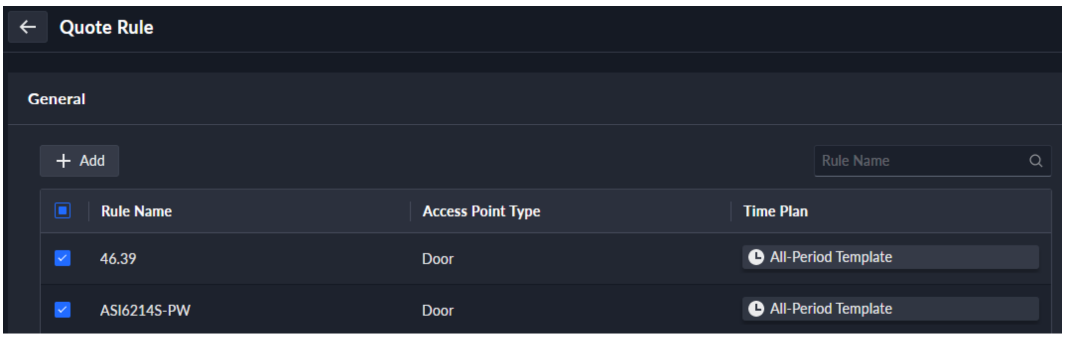
When configuring an access rule for a person and vehicle group, you can only configure general verification rules. If you want to configure other types of rules, see "6.5.3 Configuring Access Rule".

Table 6-12 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 "5.1.5 Adding Time Template".
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. Follow the steps below to create a new holiday plan: 1. Select **Add Holiday Plan** in the drop-down list. 2. Enter a name for the holiday plan. 3. Click **Add** to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click to configure the periods more precisely. You can configure up to 4 periods. 5. Click **OK**. 
Select by Zone	People can access all the access points in the selected zones.
Select by Access Point	People can access the selected access points.

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

Figure 6-22 Select access rules



6.3.3 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 "6.9.2 Configuring Parking Lot".

Procedure

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

Step 2 Add vehicles.

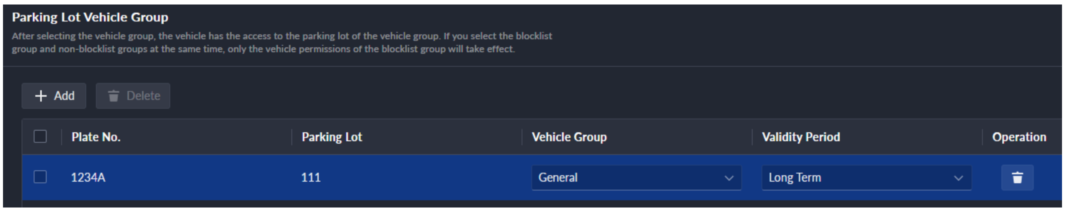
- Add vehicles one by one

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

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

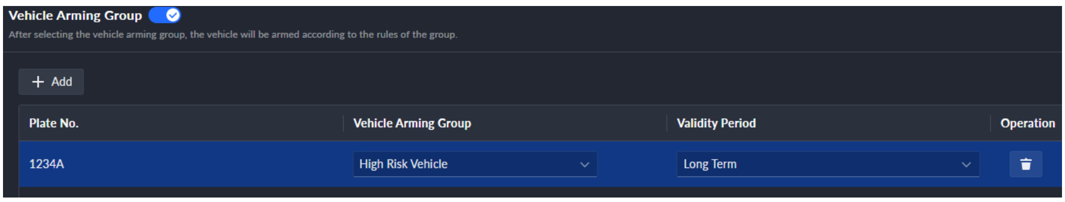
   If you have selected an owner, you can add multiple vehicles.
4. In the **Parking Lot Vehicle Group** section, click **Add**, and then you can select the plate number (the one added in the previous step) and parking lot, set the vehicle group that the vehicle belongs to, and the validity period of the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

Figure 6-23 Parking lot vehicle group



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

Figure 6-24 Vehicle arming group



For arming group details, see "6.4.2.1 Adding Vehicle Arming Group".

6. Click **OK**.

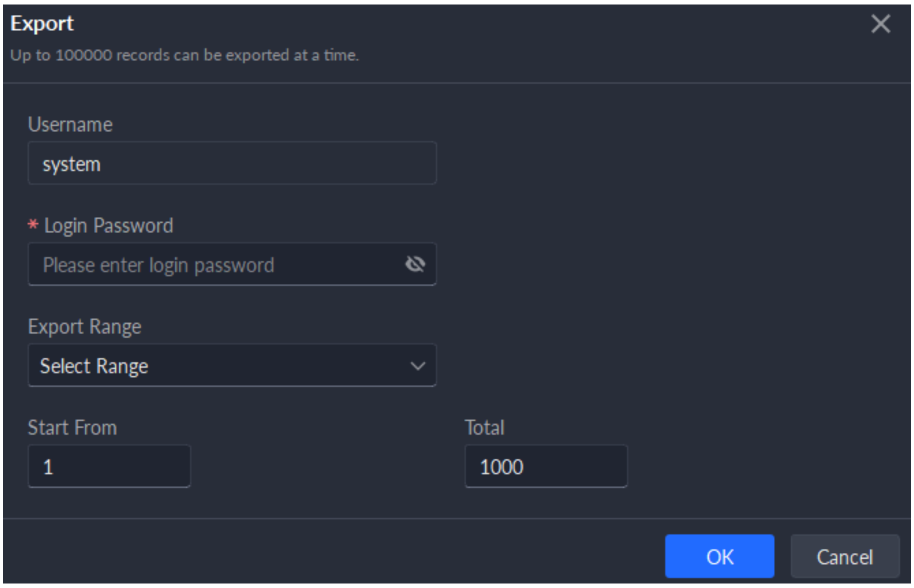
- Add vehicles in batches

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

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

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

Figure 6-25 Export vehicle information



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

Related Operations

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

6.4 Watch List Configuration

Configure face and vehicle watch list for future investigation.

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

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

6.4.1 Face Arming List

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

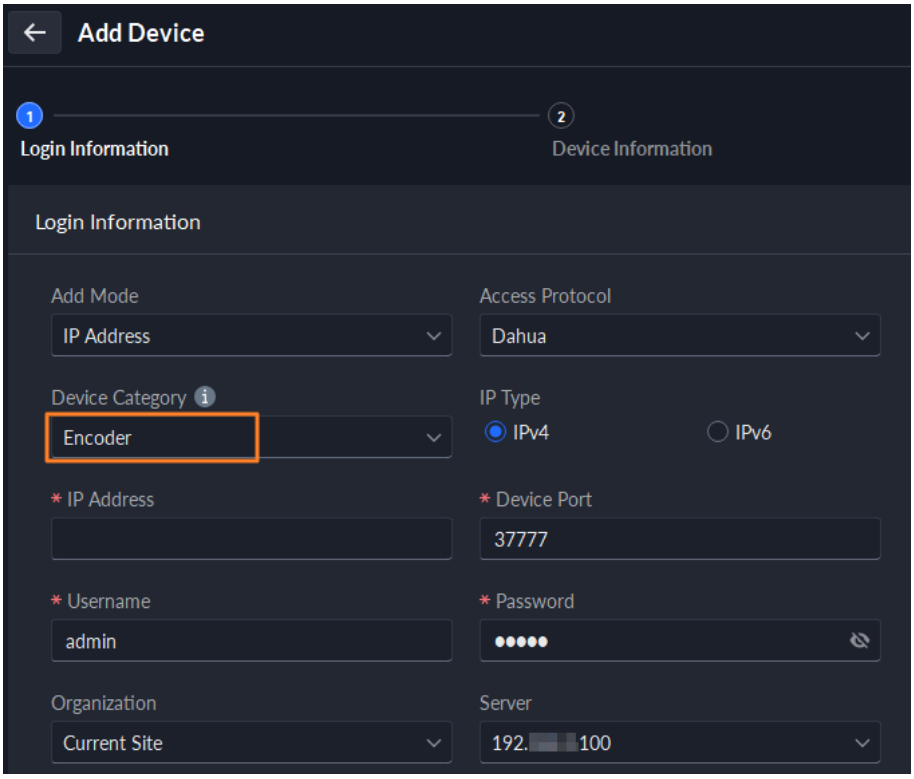
6.4.1.1 Creating Face Arming Group

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

Prerequisites

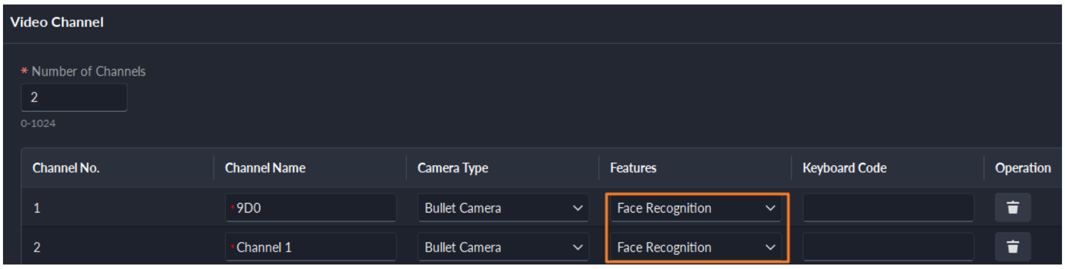
- Make sure that the devices for face recognition have been successfully configured onto the Platform.
- Make sure that the basic configuration of the Platform has completed. For details, see "5 Basic Configurations". During the configuration, you need to pay attention to following parts.
  - ◇ When adding devices on the **Device** page, set the **Device Category** to **Encoder**.

Figure 6-26 Device category



  - ◇ When adding devices like NVR or IVSS which support face recognition, set the device feature to **Face Recognition**. For details, see "5.1.2.5 Editing Devices".

Figure 6-27 Feature configuration



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

Procedure

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

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

Table 6-13 Parameter description

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

Step 3 Click **Add**.

6.4.1.2 Adding Faces

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

Procedure

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

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

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

- Add people by person groups. This is the most efficient way, provided that you have created person groups based on the access permissions. For details, see "6.3.2 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**.

6.4.1.3 Arming Faces

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

Procedure

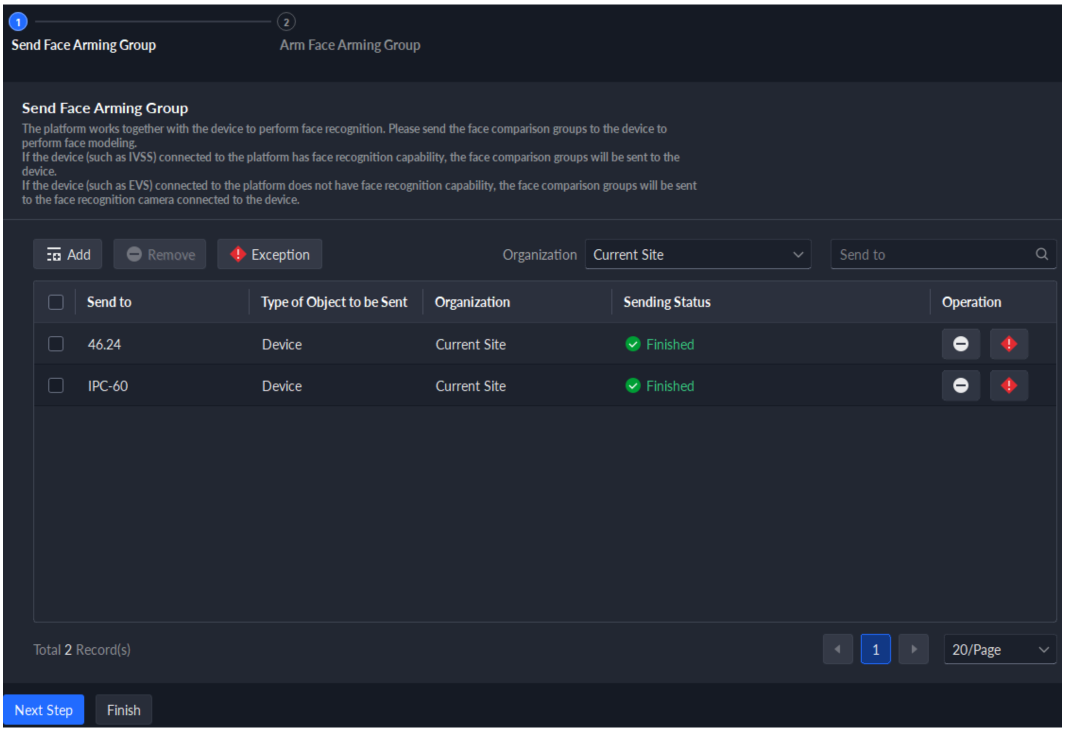
Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Arming List** > **Face Arming List**.

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

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

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

Figure 6-28 Send face arming group



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

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

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

Step 6 Click **OK**.

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

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

6.4.2 Vehicle Watch List

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

6.4.2.1 Adding Vehicle Arming Group

A vehicle arming group contains the information of multiple vehicles. When arming the group, you can arm all the vehicles inside the group at the same time. Only administrators can add, edit, and delete person and face comparison groups. You can add up to 8 vehicle arming groups.

Procedure

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

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

Table 6-14 Parameter description

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

Step 3 Click **Add**.

6.4.2.2 Adding Vehicles

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

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

Step 2 Click of a group, or double-click a group, and then click **Select from Vehicle List**.

- Add vehicles by vehicle groups. This is the most efficient way, provided that you have created vehicle groups. For details, see "6.3.2 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**.

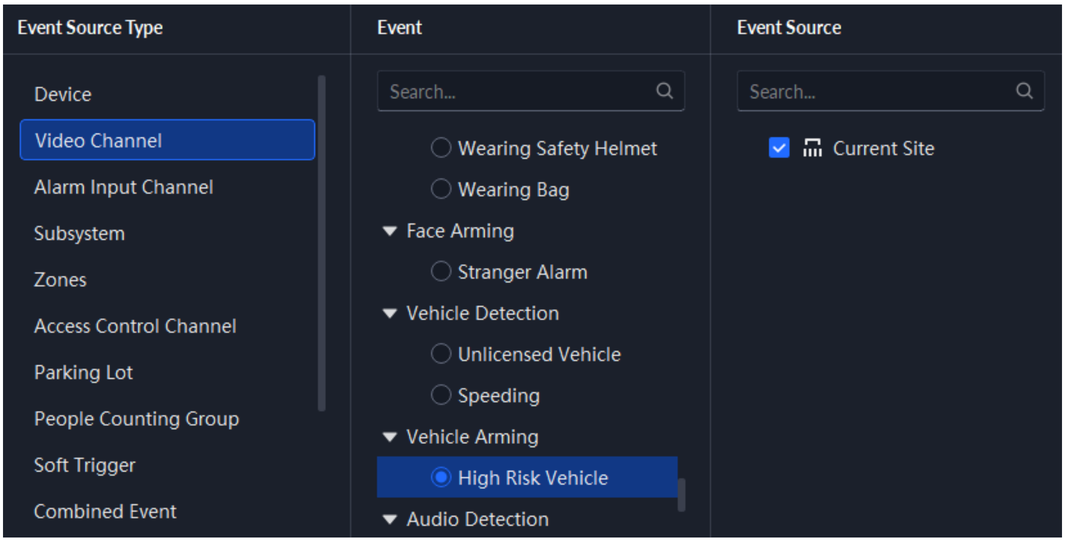
6.4.2.3 Arming Vehicles

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

Log in to the DSS Client. On the **Home** page, click , and then arm the vehicle on the **Event** page.

Click **Add** to add an event to arm a vehicle watch list. For how to configure events, see "6.1 Configuring Events".

Figure 6-29 Arm vehicle event



6.5 Access Control

6.5.1 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 "5 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 "5.1.3 Binding Resources".
  - Add persons to the platform. For details, see "6.3 Personnel and Vehicle Management".

6.5.2 Configuring Zone

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

- After adding the access control device on the **Device** page, the access point is automatically generated, and it is added to the **Unassigned** zone by default.

- The access points in the **Unassigned** zone can be moved to other zones, and you can view the details of the access points, but you cannot move access points to this zone, set them to boundaries or filter them by boundary.
- The **Unassigned** zone does not support the **Map Info** and **Access Rule** tabs, cannot be edited and deleted, and does not support adding, editing, and deleting sub zones.

6.5.2.1 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 6-15 Parameter description

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

6.5.2.2 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 6-30 Add zones in batches

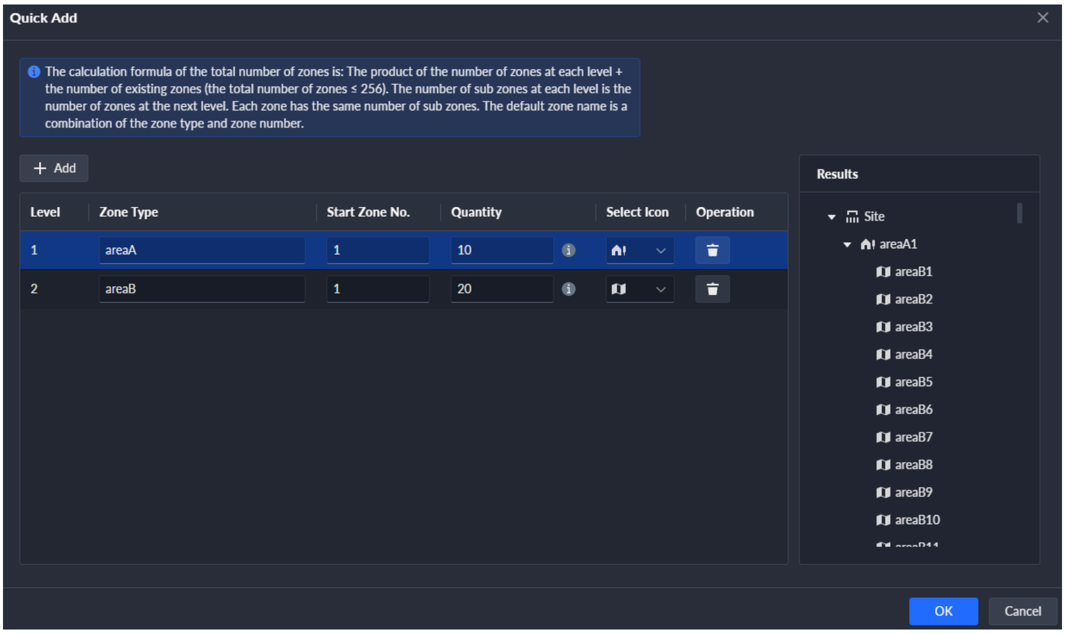


Table 6-16 Parameter description

Parameter	Description
Level	The number indicates the level of the zone. The region with a larger number is a sub zone of the region with the smaller number. For example, the level 2 zone is a sub zone of the level 1 zone.
Zone 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.

6.5.2.3 Editing and Deleting Zone

Only administrators can edit and delete zones.

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

- Click a zone and then click to edit the information of the zone, including the name, icon, and roles allowed access.

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

6.5.2.4 Moving Access Points

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

Procedure

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

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

All access points and sub zones will be displayed.

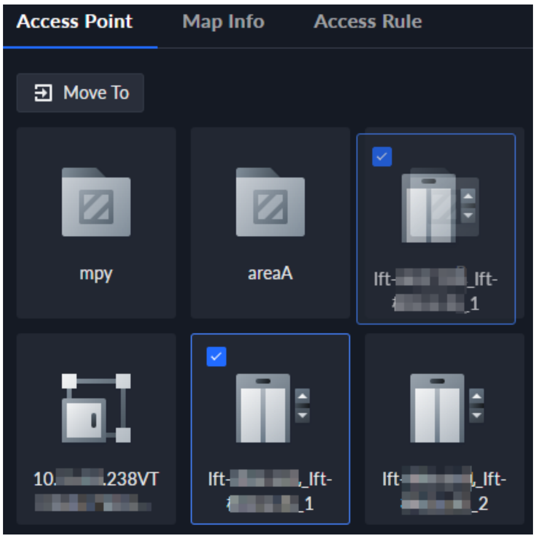
Step 3 Move the access points.

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

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

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

Figure 6-31 Move an access point

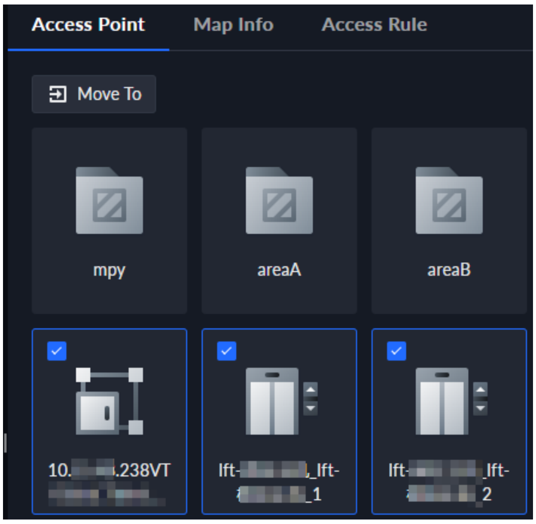


- Move multiple access points.

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

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

Figure 6-32 Move multiple access points



6.5.2.5 Configuring Access Point

6.5.2.5.1 Viewing Access Point Details

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

Procedure

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

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

Step 3 Double-click an access point to view its details.

- **Access Point Name** : The name of the access point.
- **Access Point Type** : Displays the type of the access point, door or lift.
- **Zone Name** : Displays the name of the zone the access point belongs to.
- **Linked Resources** : Displays the channel name and type of the access point, the name and type of the intercom device it belongs to, and video channels that are bound to it. If you want to bind resources to this access point, you can click **Channel Binding** to quickly go to the page. For details on channel binding, see "5.1.3 Binding Resources".
- **Access Rule** : Displays the access rules applied to this access point itself, and from the zone it belongs to. Double-click a rule to view its details. You can click **Quote** or **Remove** to add or delete the rules, but the rules from the zone cannot be deleted.

6.5.2.5.2 Setting Boundary

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

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

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

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

The icon of the access point changes to .

6.5.2.6 Configuring Access Rule for a Zone

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

Procedure

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

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

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

You can:

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

When configuring an access rule for a zone, you can only configure general verification rules for doors. If you want to configure other types of rules, see "6.5.3 Configuring Access Rule".

Table 6-17 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only **Door** is available.
Rule Type	Only **General Verification** is available. For this type of rules, doors can be unlocked by cards, fingerprints, and passwords.
Time Template	Select when this rule is effective. If you want to create a new time template, see "5.1.5 Adding Time Template".

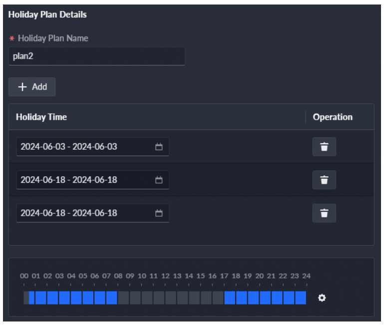
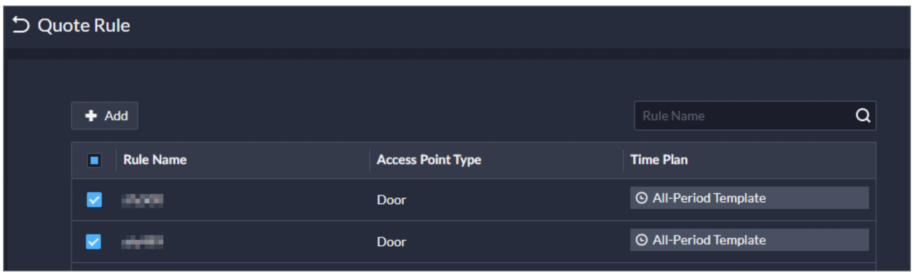
Parameter	Description
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. Follow the steps below to create a new holiday plan: 1. Select **Add Holiday Plan** in the drop-down list. 2. Enter a name for the holiday plan. 3. Click **Add** to add and configure a holiday. 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 Person Group	Select one or more person groups, and then all the persons in the groups will have permissions to access all the door channels in the zone. Select **Link Sub Node**, and then you can select a zone and all its sub zones at the same time.
Select by Person	Select one or more persons, and then they will have permissions to access all the door channels in the zone. Select **Include Sub Groups** to display all the persons in the selected group and its sub groups.

Figure 6-33 Select access rules



Step 4 Click **OK**.

6.5.2.7 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.

6.5.2.7.1 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 "6.2.2 Adding a Raster Map".

Step 4 Click **OK**.

6.5.2.7.2 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 "6.2 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.

6.5.3 Configuring Access Rule

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

6.5.3.1 Viewing Access Rule Details

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

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

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

6.5.3.2 Configuring General Verification

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

Procedure

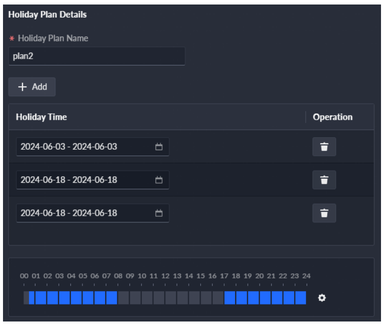
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.

Step 2 Click **Add**.

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

Table 6-18 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 "5.1.5 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	Select one or more zones, and then this rule will be applied to all access points in the zones. Select **Link Sub Node**, and then you can select a zone and all its sub zones at the same time.
Select by Access Point	Select one or more access points. Select **Include Sub Zone** to display all the access points in the selected zone and its sub zones.
Select by Person Group	Select one or more person groups, and then all the persons in the groups will have permissions to access the selected access points. Select **Link Sub Node**, and then you can select a zone and all its sub zones at the same time.
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.

6.5.3.3 Configuring Normally Open

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

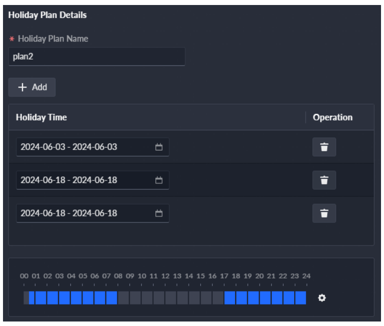
Procedure

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 6-19 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 "5.1.5 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.

Parameter	Description
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.

6.5.3.4 Configuring Normally Closed

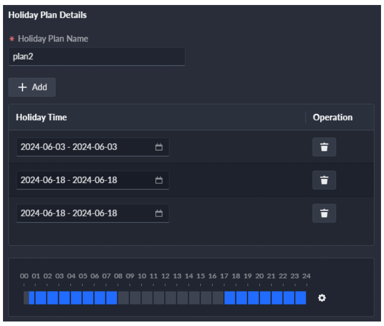
All people are not allowed to pass access points.

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 6-20 Parameter description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Rule Name</td><td>Enter a name for the rule.</td></tr>
<tr><td>Access Point Type</td><td>Only Door is available.</td></tr>
<tr><td>Rule Type</td><td>Select Remains Closed during Period.</td></tr>
<tr><td>Time Template</td><td>Select when this rule is effective. If you want to create a new time template, see "5.1.5 Adding Time Template".</td></tr>
<tr><td>Holiday Plan</td><td>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.


</td></tr>
</table>

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

6.5.3.5 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 "6.5.3.2 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 6-21 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only **Door** is available.
Rule Type	Select **First-person Unlock**.
Rule Type after Unlocked by First Person	● **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 "5.1.5 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 "6.3.2.2 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.

6.5.3.6 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 "6.5.3.2 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 6-22 Parameter description

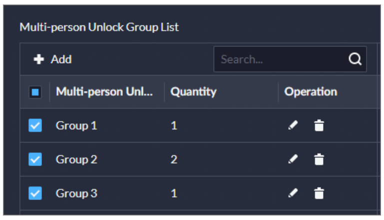
Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only **Door** is available.
Rule Type	Select **Multi-person Unlock**.
Time Template	The all-period time template is used by default and cannot be changed.
Access Point	Select one or more access points. Select **Include Sub Zone** to display all the access points in the selected zone and its sub zones.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Person</td><td>
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 "6.3.2.2 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**.
</td></tr>
</table>

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

Figure 6-34 Configure unlock methods

Step 4 Click **OK**.

6.5.3.7 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.

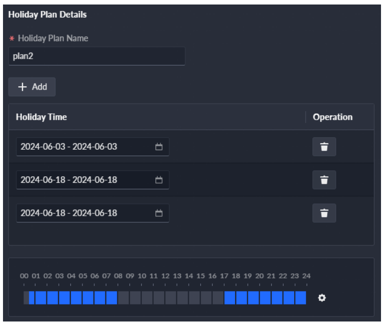
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control** > **Access Rule** > **All Rules**.

Step 2 Click **Add**.

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

Table 6-23 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only **Door** is available.
Rule Type	Select **Anti-passback**.
Anti-passback Type	For **Local Anti-passback**, you can select only the door channels of an access control device; for **Global Anti-passback**, you can select door channels from any zone (make sure that the channels support global anti-passback). If you select **Global Anti-passback**, you can configure the offline operation strategy at the same time: ● **Execute**: Offline access points will execute the anti-passback configurations. ● **Do Not Execute**: People can pass normally through offline access points.
Reset Time	If people do not pass in the defined order, they will not be allowed to pass any door within the reset time. After the reset time, they must follow the order from the beginning. The reset time can be between 1 minute and 24 hours.
Time Template	Select when this rule is effective. If you want to create a new time template, see "5.1.5 Adding Time Template".

Parameter	Description
Holiday Plan	Select when this rule is not effective. You can add up to 4 holiday plans. **Local Anti-passback** does not support holiday plan. Follow the steps below to create a new holiday plan: 1. Select **Add Holiday Plan** in the drop-down list. 2. Enter a name for the holiday plan. 3. Click **Add** to add and configure a holiday. You can add up to 16 holidays. 4. Configure the effective periods for each day in the holiday. You can drag on the timeline, or click to configure the periods more precisely. You can configure up to 4 periods. 5. Click **OK**. 
Access Point	Add doors to different groups, and then people must pass in the group order to access the doors in the last group. When setting **Anti-passback Type** to **Global Anti-passback**: ● You can add up to 32 card readers ● The platform will only display devices that support this function. ● You can select **Include Sub Zone** to display all the access points in the selected zone and its sub zones.
Person	Select the persons that will not be subject to the global anti-passback rules. You can only add up to 1,000 persons to a single rule. Make sure that the **General Verification** rule has been configured for the person. For details, see "6.5.3.2 Configuring General Verification".

6.5.3.8 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 6-24 Parameter description

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

6.5.3.9 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 6-25 Parameter description

Parameter	Description
Rule Name	Enter a name for the rule.
Access Point Type	Only **Door** is available.
Rule Type	Select **Remote Verification**.
Time Template	Select when this rule is effective. If you want to create a new time template, see "5.1.5 Adding Time Template".
Access Point	Select one or more doors. Select **Include Sub Zone** to display all the access points in the selected zone and its sub zones.

Results

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

6.5.3.10 Viewing Rule Exception

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

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

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

6.5.3.11 Verifying Consistency of Person Information

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

Prerequisites

Before using this function, you must configure an **Image and File** disk for the server where the device is added to. For details, see "5.3 Configuring Storage".

Procedure

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

Step 2 Select an access control device, and then click **Verify**.

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

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

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

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

- A person is not on the device: Send the person information from the platform to the device again.
- A person is not on the platform: On the **Person List** page, select **Import** > **Import from Device** to import the person information from the device to the platform.
- The person information is inconsistent: Send the person information from the platform to the device again.

6.5.4 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**.

6.5.5 Configuring Access Card

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

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

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

Table 6-26 Access card configuration description

Parameter	Description
Device DESFire Card	After enabled, the DESFire card can be used normally. Make sure that the device supports reading DESFire card; otherwise, the card cannot be recognized.
DESFire Card Encryption	After enabled, the DESFire card reader only shows the encrypted information.

Parameter	Description
Write to DESFire	After enabling **Device DESFire Card** and **DESFire Card Encryption**, you can click this icon, select a device that supports reading and writing DESFire cards from , enter the card number, and then the device can write the card number to the card.
Block NFC Cards	Enable **Block NFC Cards** , and then click **Apply to Device**, the devices will not recognize copied NFC cards, and people cannot use NFC cards to open doors.
Apply to Device	

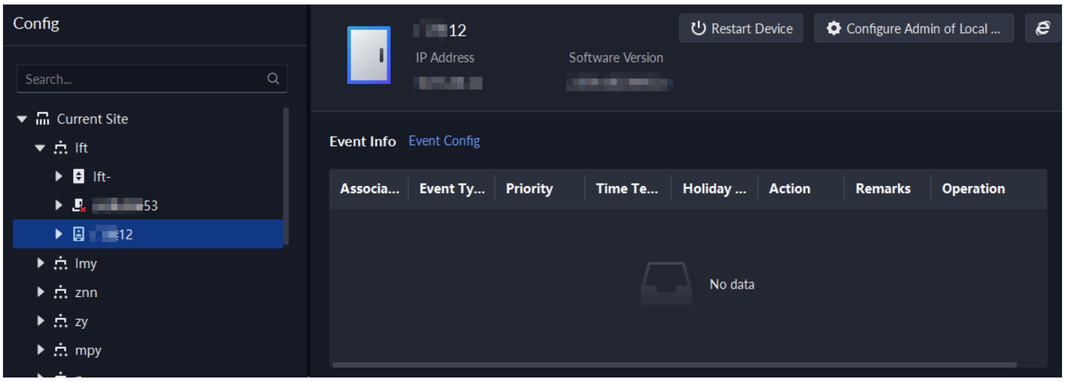
6.5.6 Configuring Access Control Devices

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 6-35 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.

6.6 Video Intercom

6.6.1 Preparations

Make sure that the following preparations have been made:

- Access control devices are correctly deployed, and the SIP server IP of the devices are filled in with IP of central servers of the platform. For details, see the corresponding user manuals.
- Basic configurations of the platform have been finished. To configure, see "5 Basic Configurations".

- ◇ When adding video intercom devices on the **Device** page, select **Video Intercom** as the device category.
- ◇ When adding access control devices that support intercom, select **Device Category** to **Access Control** in **Login Information**, and then select **Access Control Recognition Terminal**.

6.6.2 Call Management

Create call group, management group and relation group respectively and define restricted call relations. This function is only available for administrators.

Click on the page of call group, management group or relation group, the system will restore management group and relation group to their original status.

6.6.2.1 Configuring Call Group

Only devices in the same call group can call each other.

- A call group will be automatically generated after you add to the platform a VTO or access control device that supports intercom. All VTHs in the same unit will also be automatically added to the group. 2 VTHs or a VTH and VTO in the group can call each other.
- A call group will be automatically generated after you add a second confirmation station to the platform. Add the VTHs in the same house to the group, then the second confirmation station and the VTHs can call each other.
- A call group will be automatically generated after you add a fence station to the platform. All the VTHs on the platform will be automatically added to the group by default, then the fence station and the VTHs can call each other. You can also click to edit the VTHs in the group, so that the fence station can only call certain VTHs.
- After added to the platform, VTHs will be automatically added to corresponding groups if they are associated with VTOs, second confirmation stations, or fence stations, so that they can call each other.

6.6.2.2 Adding a Manager Group

Divide administrators into different groups and link them to call groups in different combinations. This is useful when certain administrators can only answer calls from certain devices. Administrators include VTS and users with permissions to use the video intercom function and operate the devices. VTS will be automatically added to the default manager group after added.

Procedure

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

Step 2 Select **Call Management** > **Manager Group Config**.

Step 3 Click .

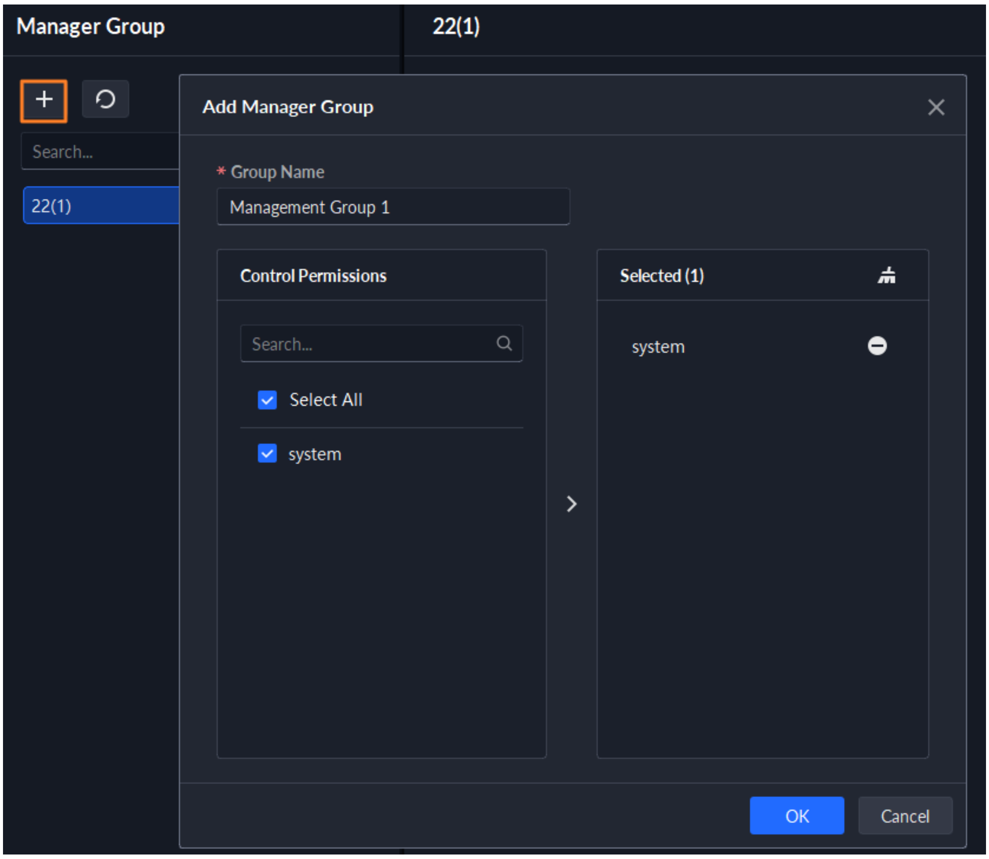
Step 4 Enter the group name, select an administrator account or VTS, and then click **OK**.

The added management group is displayed in the list.

- To transfer members, click and move the member to other groups.

- To manage group members, click ![edit] to add or delete group members.

Figure 6-36 Add a manager group



6.6.2.3 Configuring Relation Group

Link call groups and manager groups, and VTOs or VTHs in a call group can only call administrators or VTSs of a linked manager group. There are 2 types of relations:

- A call group links to 1 manager group.

  All online administrators in the manager group will receive the call when any device is calling. If an administrator answers, it will stop ringing for other administrators. The call will only be rejected if all administrators reject it.
- A call group links to multiple manager groups.

  Priorities vary for different manager groups. When any device is calling, all online administrators in the manager group with the highest priority will receive the call first. If no one answers for 30 seconds, then the call will be forwarded to the manager group with the second highest priority. If still no one answers, the device will prompt that there is no response for the call.

Procedure

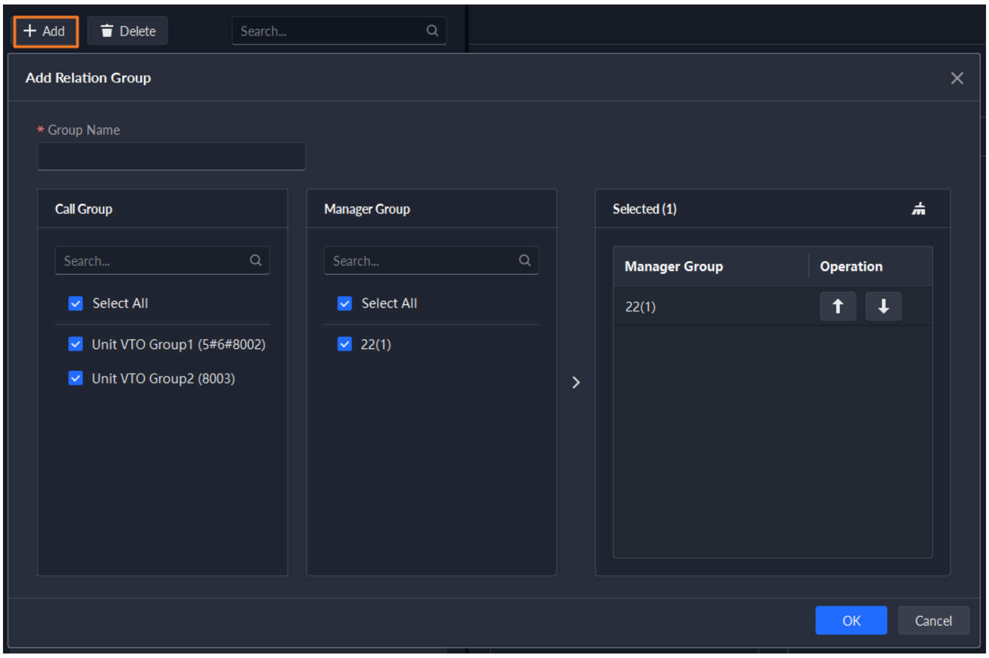
Step 1 Log in to the DSS Client. On the **Home** page, click ![icon], and then select **Video Intercom** in the **App Config** section.

Step 2 Select **Call Management** > **Relation Group Config**.

Step 3 Click ![+].

Step 4 Enter the group name, and then select one or more call groups and manager groups.

Figure 6-37 Add a relation group



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

Step 5 Click or to adjust priorities of the manager groups, and then click **OK**.

The upper manager group has the higher priority.

6.6.3 Configuring Building/Unit

Make sure the status of building and unit of the DSS client is the same as the VTO. If building and unit are enabled on the platform, they must also be enabled on the device, and vice versa; otherwise, the VTO will be offline after it is added. That also affects the dialing rule. Take room 1001 unit 2 building 1 as an example, the dialing rule is as follows:

- If building is enabled while unit is not, the room number is "1#1001".
- If building is enabled, and unit is enabled as well, the room number is "1#2#1001".
- If building is not enabled, and unit is not enabled either, the room number is "1001".

Procedure

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

Step 2 Click **Residence Config**.

Step 3 Enable or disable building and unit as required, and then click **OK**.

This configuration must be the same as the device configurations. Otherwise, information of the devices might be incorrect. For example, if only **Building** is enabled on a VTO, you must only enable **Building** on the platform.

Step 4 Click **Save**.

6.6.4 Synchronizing Contacts

Send room information to a VTO and then you can view it on the VTO or its webpage.

Procedure

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

Step 2 Click **Contacts Sync**.

Step 3 Send room information.

- Select a VTO, and then click of a room.
- Select a VTO, and then click **Send Contacts** to send all or selected rooms.

Now you can view the room information on the VTO or its webpage. If any room cannot be sent, the reason will be provided.

Related Operations

After sending room information successfully, you can delete it from the VTO, then it will not be displayed on the VTO or its webpage anymore.

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

6.6.5 Setting Private Password

Set room door passwords so that the room door can be opened by entering password on the VTO (outdoor station).

Make sure that contacts are sent to the VTO; otherwise you cannot set private password.

Procedure

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

Step 2 Click **Private Password**.

Step 3 Select a VTO, and then you can see all the VTHs linked to this VTO.

Step 4 Select a VTH and click , or select several VTHs and click **Change Password**.

Step 5 Enter password, and then click **OK.**

You can use the new password to unlock on the VTO.

Results

Use room number + private password to unlock the door. The room number consists of 6 digits. For example, a person who lives in 1001 with the private password of the VTO in the building being 123456, can enter **#001001123456#** to unlock the door.

6.6.6 App User

You can view information of App users, freeze user, modify login password and delete user.

Prerequisites

App users have registered by scanning the QR code on the VTH. For details, see the user manual of the App.

Procedure

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

Step 2 Click **App Users**.

Table 6-27 Parameter description

Operation	Description
Freeze APP user	The App user cannot log in for 300 seconds after being frozen. The account will be frozen when invalid password attempts exceeds 5 by an App user.
Change APP user login password	Click , enter a new password on the **Reset Password** page, and then click **OK**. ● The password must be 8 to 16 characters and include numbers and letters. ● Click to display password, or to mask password.
Refresh the list of App users	Click **Refresh** to display the App users that recently registered.
Delete APP user	Click to delete App users one by one, or select multiple App users, click **Delete**, and then follow the instructions to delete them. The users can no longer log in to the App. If a user is a homeowner, all App accounts in the corresponding room will be deleted, and all people in this room can no longer log in to the App.

6.7 Attendance Management

Configure attendance devices, attendance shifts and periods, so as to manage attendance records and reports.

6.7.1 Preparations

Make sure that the following preparations have been made:

- Attendance devices are correctly deployed. For details, see the corresponding user manuals.
- Basic configurations of the platform have been finished. To configure, see "5 Basic Configurations".

- When adding attendance devices on the **Device** page, select **Access Control** as the device category.
- Personnel information is added correctly. For details, see "6.3.2 Configuring Person Information".

6.7.2 Configuring Attendance Terminal

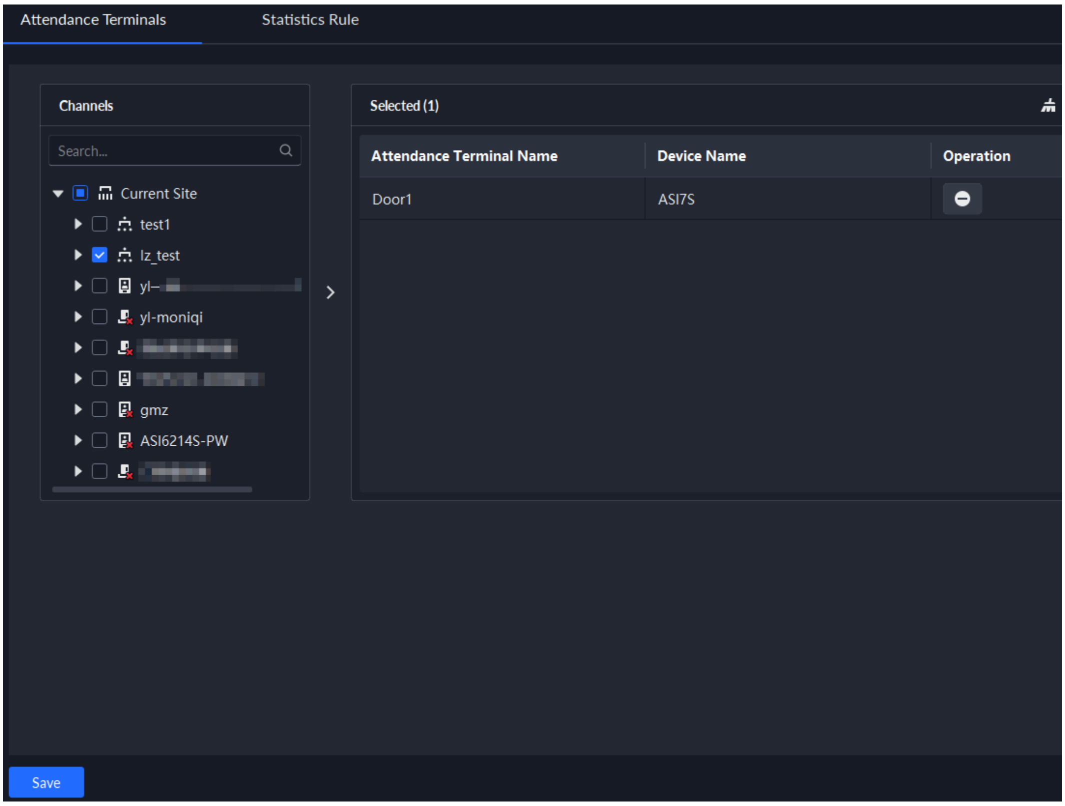
Make sure that access controller is used as the attendance device for check-in and check-out, recording attendance information, and uploading attendance data.

Procedure

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

Step 2 Select **Attendance Config** > **Attendance Terminals**.

Figure 6-38 Attendance terminal



Step 3 Select access control channels, and then click **Save**.

You can enter keywords to search for devices.

6.7.3 Configuring Statistics Rule

The smallest timing unit of swiping card is minute. Seconds will be rounded up or down. For example, if you swipe your card at 09:00:01 and the rule is set to round down, then the time of you swiping the card is 09:00; if the rule is set to round up, then the time of you swiping the card it is 09:01.

Procedure

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

Step 2 Click on the left, and then select **Statistics Rule**.

Step 3 Select a rule, and then click **Save**.

6.7.4 Configuring Attendance Period

Set attendance period, which can be used as time evidence to judge if a person is late, on time, or leaves early.

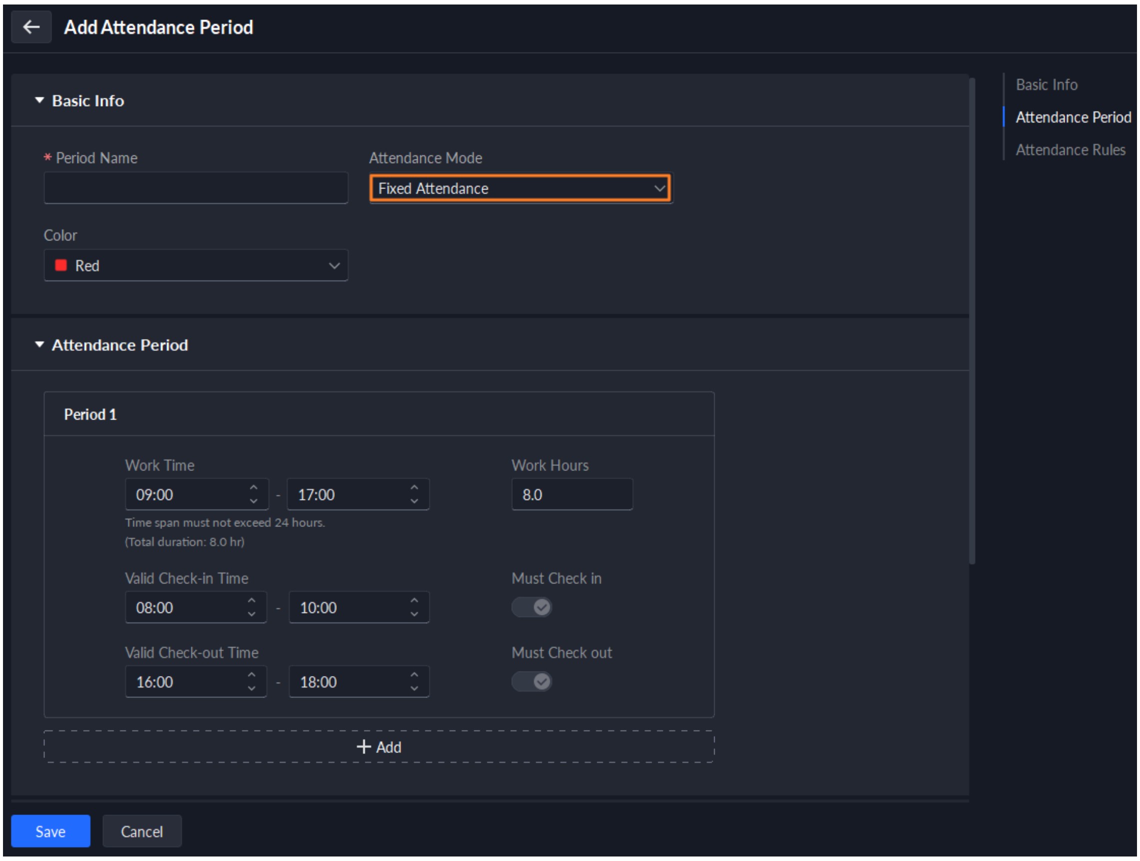
Procedure

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

Step 2 Click **Attendance Period**.

Step 3 Click at the upper-left corner of the page.

Figure 6-39 Add attendance period



Step 4 Set parameters of attendance period.

- Fixed attendance requires you to sign in and sign out during the fixed hours.

  Click to add another working period. You can set 2 working periods at most.

Table 6-28 Fixed attendance parameters

Parameter	Description
Period Name	Custom period name, used to recognize period, such as early shift and night shift.
Color	Set corresponding color of period, and corresponding color will be directly displayed on calendar when making shift for personnel, and quickly identify shift information.
Attendance Mode	Set as **Fixed Attendance**.
Work Time	Set corresponding working hour of period. Attendance time supports cross-day, but not exceeds 24 hours. One attendance period supports max two types of attendance time.
Work Hours	Fill in according to actual situation.
Valid Check-in Time	If working time is set from 09:00 to 18:00, then valid sign-in time can be set as 08:00-10:00, valid sign-out time can be set as 16:00-18:00. Configuration rules are as follows: ◇ The start time of valid sign-in time is earlier than or equal to start working time (09:00), the end time of valid sign-in time should be later than start working time (09:00), earlier than start time of valid sign-out time. If there are several sign-in records within valid sign-in time, then the earliest record is considered as sign-in time. ◇ The start time of valid sign-out time is later than the end time of valid sign-in time, earlier than end working time (18:00), the end sing-in time of valid sign-out time is later than or equal to end working time (18:00). If there are several sign-out records within valid sign-out time, then the earliest record is considered as sign-out time.
Valid Check-out Time	If working time is set from 09:00-18:00, then valid sign-in time can be set as 08:00-10:00, valid sign-out time can be set as 16:00-18:00. Configuration rules are as follows: ◇ The start time of valid sign-in time is earlier than or equal to start working time (09:00), the end time of valid sign-in time should be later than start working time (09:00), earlier than start time of valid sign-out time. If there are several sign-in records within valid sign-in time, then the earliest record is considered as sign-in time. ◇ The start time of valid sign-out time is later than the end time of valid sign-in time, earlier than end working time (18:00), the end sing-in time of valid sign-out time is later than or equal to end working time (18:00). If there are several sign-out records within valid sign-out time, then the earliest record is considered as sign-out time.
Must Check in	If you set 2 working time, then the second working time can cancel sign in, you don't have to sign in when you work at the second working time, and the start time of working time can be used as sign-in time.
Must Check out	If you set 2 working time, then the first working time can cancel sign in, you don't have to sign out when you finish work at the second working time, and the end time of working time can be used as sign-out time.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Allowed Late Check-in Time (min)</td><td rowspan="4">Define the rules for being late, absence and early leave. Take the values in the snapshot as an example.
◇ Check in on time: Check in no later than 5 minutes.
◇ Later: Check in 5 minutes later, but no later than 30 minutes.
◇ Absence: Check in 30 minutes later or check out 120 minutes earlier.
◇ Leave on time: Check out no earlier than 5 minutes.
◇ Leave earlier: Check out 5 minutes earlier, but no earlier than 120 minutes.
◇ Overtime: Check out 60 minutes later.</td></tr>
<tr><td>Allowed Early Check-out Time (min)</td></tr>
<tr><td>Absence Time
On Duty _ min later.</td></tr>
<tr><td>Absence Time
On Duty _ min earlier.</td></tr>
<tr><td>Overtime
Off Duty _ min later.</td><td>Define overtime rule.
If it is set to 120 minutes, off duty check-out time is later than end time of working time, and period >120 minutes, then it is recorded as overtime, overtime period is Period – 120 minutes.</td></tr>
</table>

- Flexible attendance just calculates whether the daily working hours of a person meets the rule according to the sign-in/out time.

Table 6-29 Flexible attendance parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Period Name</td><td>Custom period name, used to recognize period, such as flexible attendance.</td></tr>
<tr><td>Attendance Mode</td><td>Set as Flexible Attendance.</td></tr>
<tr><td>Color</td><td>Set corresponding color of period, corresponding color will be directly displayed on calendar when making shift for personnel, and quickly recognize shift information.</td></tr>
<tr><td>Work Time</td><td>Set the period you must work in a day.</td></tr>
<tr><td>Man-Hour(Hours)</td><td>Set how many hours you have to work a day. For example, if you set 8, then it means you are required to work 8 hours.</td></tr>
<tr><td>Latest Check-in Time</td><td>Sign in after restricted time is recorded as late.</td></tr>
<tr><td>Latest Check-out Time</td><td>You are required to sign out before the designated time, otherwise no sign out is recorded.</td></tr>
<tr><td>Min Overtime (hr)</td><td>For example, working hour is 8 hours a day, and if you work overtime for 2.5 hours, then it is recorded as overtime, then you can set 10.5 here.</td></tr>
<tr><td>Odd In and Even Out</td><td rowspan="2">Swipe card at odd number is recorded as check-in. For example, the first card-swiping is check-in. Swipe card at even number is recorded as check-out. For example, the second card-swiping is check-out. It is recorded swiping the card twice when the interval of two continuous card swiping is larger than the defined value.</td></tr>
<tr><td>Minimum Time Interval between Two Punches (min)</td></tr>
</table>

Step 5 Click **Save**.

If attendance period is already applied to attendance shift, then before deleting attendance period, go to **Attendance Shift**, disable the attendance period in the attendance shift, and then delete the attendance period you want.

6.7.5 Configuring Holiday Plans

Set holiday time to determine overtime type.

Procedure

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

Step 2 Click **Attendance Holiday Plan**.

Step 3 Click at the upper-left corner.

Step 4 Configure the information.

Figure 6-40 Add a holiday

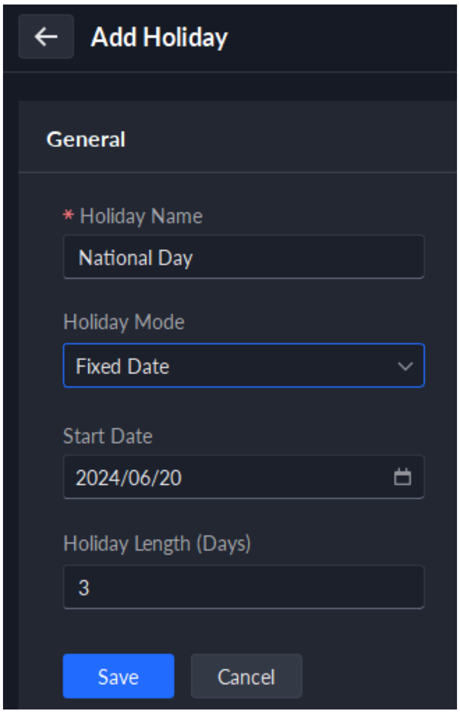


Table 6-30 Holiday parameters

Holiday Mode	Description
Fixed Date	Set some specific date as holiday. For example, set May 1, 2024 (Labor's day) as holiday, and lasts for 1 day, then set **Start Date** as May 1, 2020 and **Holiday Length (Days)** as 1.
Date Cycle	If the holiday is the fixed weekday of some week in some specific month, and it cycles according to year, which can be configured as date cycle. For example, if you want to set Mother's Day as holiday, and it lasts for 1 day, then you can set **Start Date** as the second Sunday in May, and **Holiday Length (Days)** as 1.
Yearly Cycle	If the holiday is fixed date and it cycles according to year, which can be configured as year cycle. For example, set New Year's Day as holiday, and it lasts for 1 day, then you can set **Start Date** as January 1 and **Holiday Length (Days)** as 1.

Step 5 Click **Save**.

6.7.6 Configuring Attendance Shift

Set attendance shift according to attendance period, used for department and personnel shift.

Procedure

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

Step 2 Click **Attendance Shift**.

Step 3 Click at the upper-left corner of the page.

Step 4 Set shift details, select a day, and then click **Apply** to arrange attendance period for the day.

Figure 6-41 Configure attendance shifts

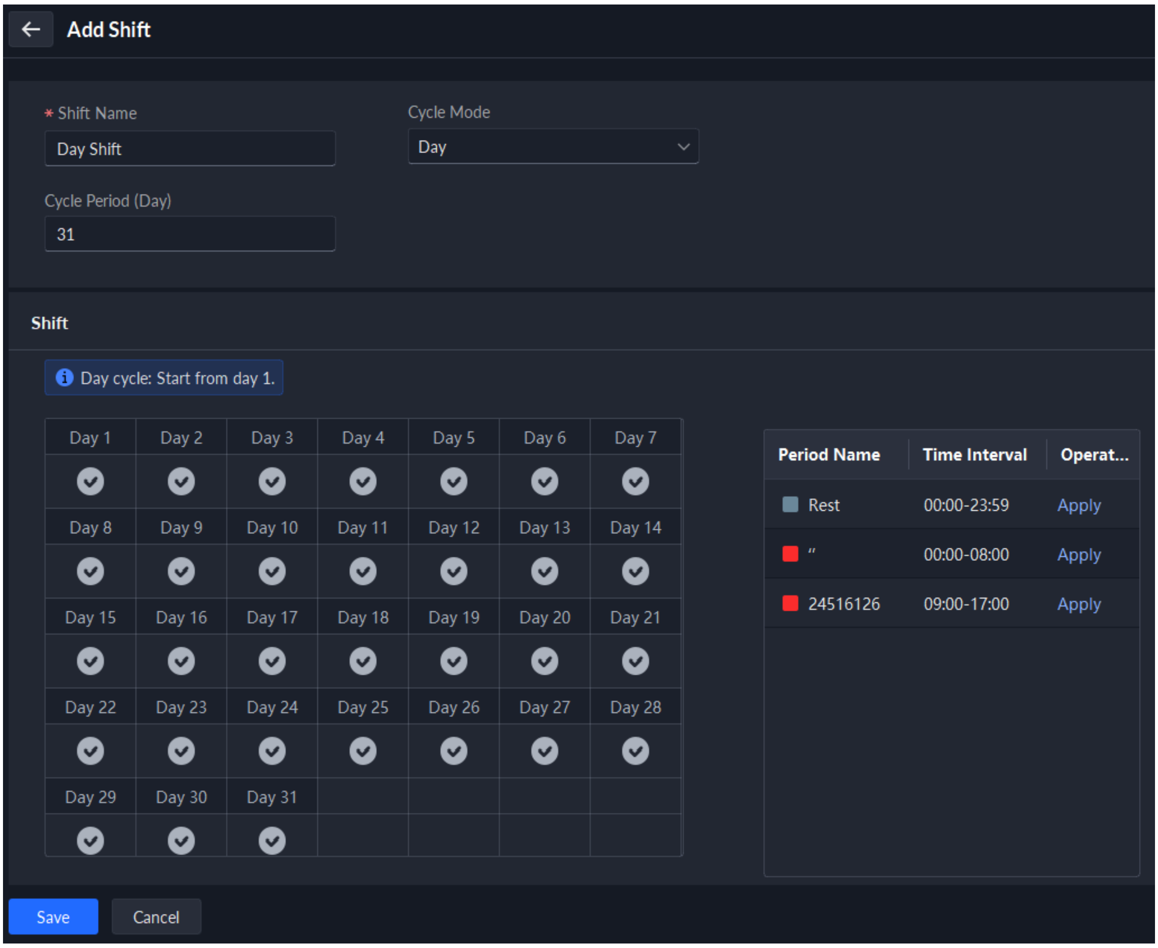


Table 6-31 Attendance shift parameters

Parameter	Description
Shift Name	Custom period name, used to recognize shift.

Parameter	Description
Cycle Mode	● **Day** : Start cycle from the first day, cycle period can be set as any number from 1 to 31 according to day. For example, if you set 2, then the cycle period is 2 days. ● **Week** : There are 7 days in a week by default, it starts cycle from Sunday, and so Sunday is required to be set as the first day. Cycle period can be set as any number from 1 to 4. For example, if you set 2, then 2 weeks can be a cycle period. ● **Month** : There are 31 days in a month by default, it starts cycle from the current day (If the date does not exist, then it will be deleted during shift arrangement), cycle period can be set as any number from 1 to 3 according to month. For example, if you set 2, then 2 months can be a cycle period.
Cycle Period (Day)	

Step 5 Click **Save**.

Delete in-use attendance shift: Go to **Shift Management** > **Person Shifts**, check if there are shifts to be deleted; if yes, remove the relation, and then delete.

6.7.7 Shift Management

Arrange shifts for personnel or department. You can also arrange temporary shift for personnel. The shift priority is temporary shift > holiday > personnel shift > department shift.

6.7.7.1 Person/Department Shift Arrangement

The operations for person shift and department shift are similar. This section takes person shift as an example.

Background Information

- If you configure department shift, then all the people of the department need to conform to the shift.
- If both person and department are configured with shift, then the latest person shift shall prevail. For example, after configuring the person shift, and the corresponding department is configured as well, then person shift is based on the latest department shift.
- If the department where new persons belong to is configured with shift, then the shift of new person should conform to department shift.

Procedure

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

Step 2 Click **Shift Management**.

Step 3 Click **Person Group Shift** at the upper-left corner of the page.

- If you need to configure shift for department, click at the upper-left corner to go to the page of department shift arrangement. The following operation is the same as person shift arrangement.
- Click next to the person and you can view the shift details.

Step 4 Select shift person, click to add shift information.

Figure 6-42 Select shifts

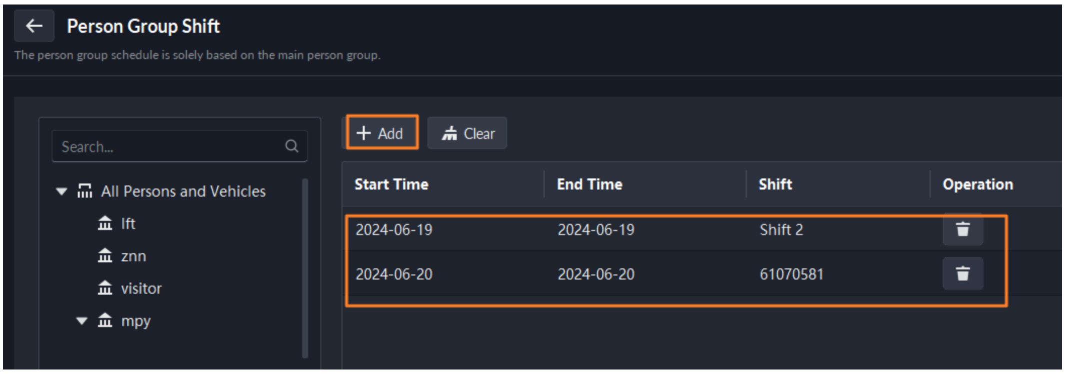


Table 6-32 Parameter description

Parameter	Description
Start Time	Set start date and end date of person shift. Click the date (for example, 2024-0619), and the calendar displays. Select the date.
End Time	
Shift	Select the one that you need. See "6.7.7.1 Person/Department Shift Arrangement".

Step 5 Click **OK**.

6.7.7.2 Temporary Shift

Arrange a temporary shift when needed.

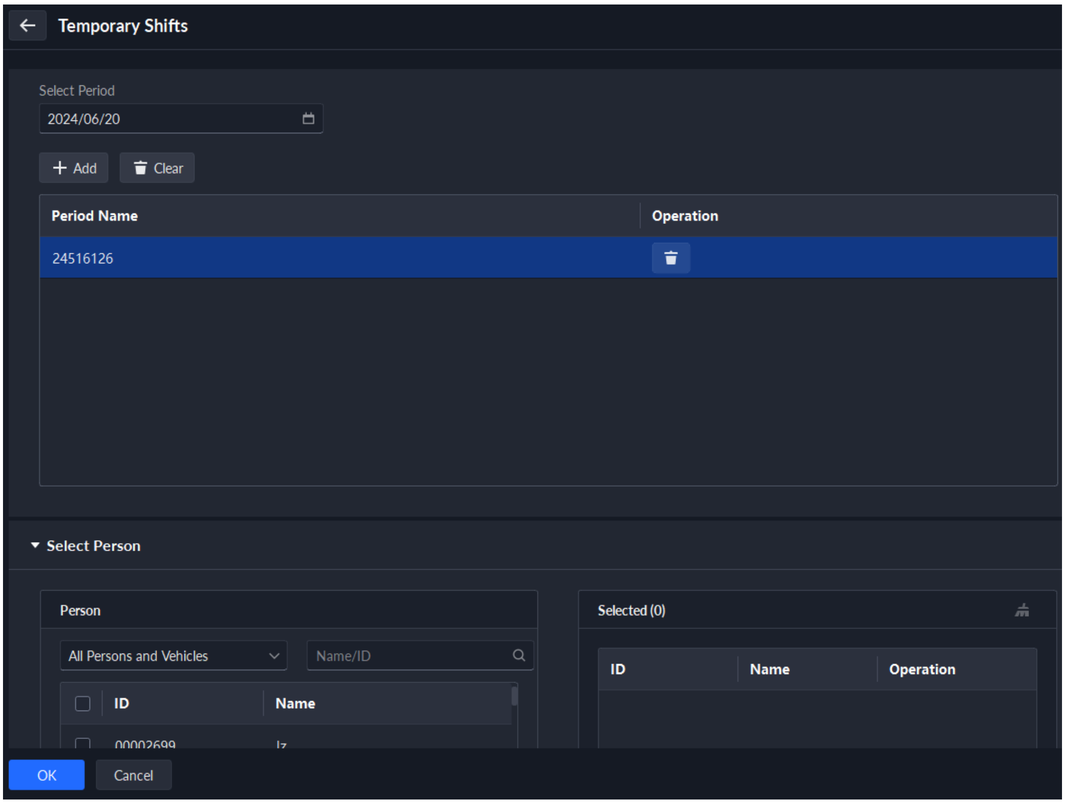
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Attendance**.

Step 2 Select **Shift Management** > **Temporary Shifts**.

Step 3 Select person and date.

Step 4 Click , and then click the **Period Name** column to select an attendance shift as needed.

Figure 6-43 Temporary shift



Step 5 Click **OK**.

Temporary shifts can be deleted: Right-click the date configured with temporary shift, and delete it according to system prompt.

6.8 Visitor Management

6.8.1 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 "5 Basic Configurations".
- Configure email server first if you want to send emails to the visitor. For details, see "9.2.4 Configuring Email Server".

6.8.2 Configuring Visit Settings

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

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

Step 2 Configure the parameters.

Table 6-33 Parameters of configuring visitor

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Create Appointment</td><td rowspan="2">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 "7.4.4.4.2 Creating Appointment by Visitors") and host invitation (see "7.4.4.4.3 Appointment Invited by Host").</td></tr>
<tr><td>Host Invitation</td></tr>
<tr><td>Appointment Expiration Config</td><td>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.</td></tr>
<tr><td>Visitor Registration</td><td>● 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.</td></tr>
</table>

Parameter	Description
Visitor Access Permission	Set the access permission group for visitors. Set the access permission group for visitors, including access control, video intercom, lift control and parking lot. Access permission control has the following 3 security levels. ● Low security level: After enabling the automatic visit access point from **Visitor** > **Visitor Registration** > **Arrival and Registration**, and selecting the channel, if the corresponding channels are also selected when adding the visitor access permission group, the visitor can be automatically authorized to enter when the visitor visits. ● Medium security level: Automatic visit and permission group are not enabled, and only automatic leave is enabled. When the visitor visits, manual registration and authorization are required, but authorization and registration are not required when leaving. ● High security level: Automatic visit and leave are disabled, and default permission group is not configured. Registration and authorization are required for both visit and leave.
Visitor Pass	Customize the content of remarks on a visitor pass.
Email Template	Click **Visitor Appointment (Visitor)** , **Visitor Appointment (Host)**, **Visitor Arrival** or **Visitor Leave** to set an email template, and then the system will automatically send emails when visitors or hosts make an appointment, visitors arrive for their appointment or end their visit. You can customize the email subject and content with the visitor information by entering information or selecting the fields such as **Visitor Name** and **Visitor Company**.

Step 3 Click **Save**.

6.9 Parking Lot

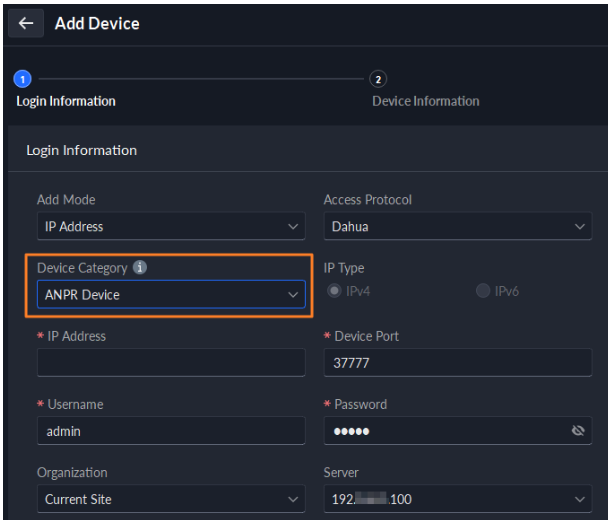
Configure entrance and exit point of the parking lot, barrier opening rules, event parameters, vehicle group, and more to realize barrier opening management, event management, and more.

6.9.1 Preparations

Make sure that the following preparations have been made:

- Devices, such as ANPR cameras, VTOs are added to the platform.
- Basic configurations of the platform have been finished. To configure, see "5 Basic Configurations".
  - ◇ When adding an ANPR camera, set **Device Category** to **Access ANPR Device**.

Figure 6-44 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 "5.1.3 Binding Resources".

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

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

◇ Select **Entrance ANPR** from **Features** for the corresponding NVR channels.

Applicable only in scenario without barrier of entrance and exit mode.

◇ When adding VTO, set **Device Category** to **Video Intercom**.

Also, you need to add the information of people and assign them permissions so that they can use the VTO normally. For details, see "6.3 Personnel and Vehicle Management".

Make sure that the configurations of building and unit on the DSS client are the same as the device. If building and unit are enabled on the platform, they must also be enabled on the device, and vice versa. Otherwise, the VTO will be offline after being added. For details, see "6.6.3 Configuring Building/Unit".

◇ Snapshots taken by ANPR cameras are stored in the **Images and Files** disks. You must configure at least one **Images and Files** disk so that snapshots of vehicles can be normally displayed. For details, see "5.3 Configuring Storage".

- If it is necessary to enable access recognition for personnel through the VTO, then personnel need to be added and authorized, and open barrier by two-factor verification should be enabled. For details, see "6.3 Personnel and Vehicle Management" and "6.9.2.1 Adding Parking Lots".

6.9.2 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.

6.9.2.1 Adding Parking Lots

Procedure

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

Step 2 Add parking lot organizations.

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

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

Only 1 main parking lot can be added.

Step 4 Configure the basic information of the parking lot, and then click **Next Step**.

Table 6-34 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 Configure the entrance and exit points, and then click **Next Step**.

The platform supports up to 4 entrances and exits.

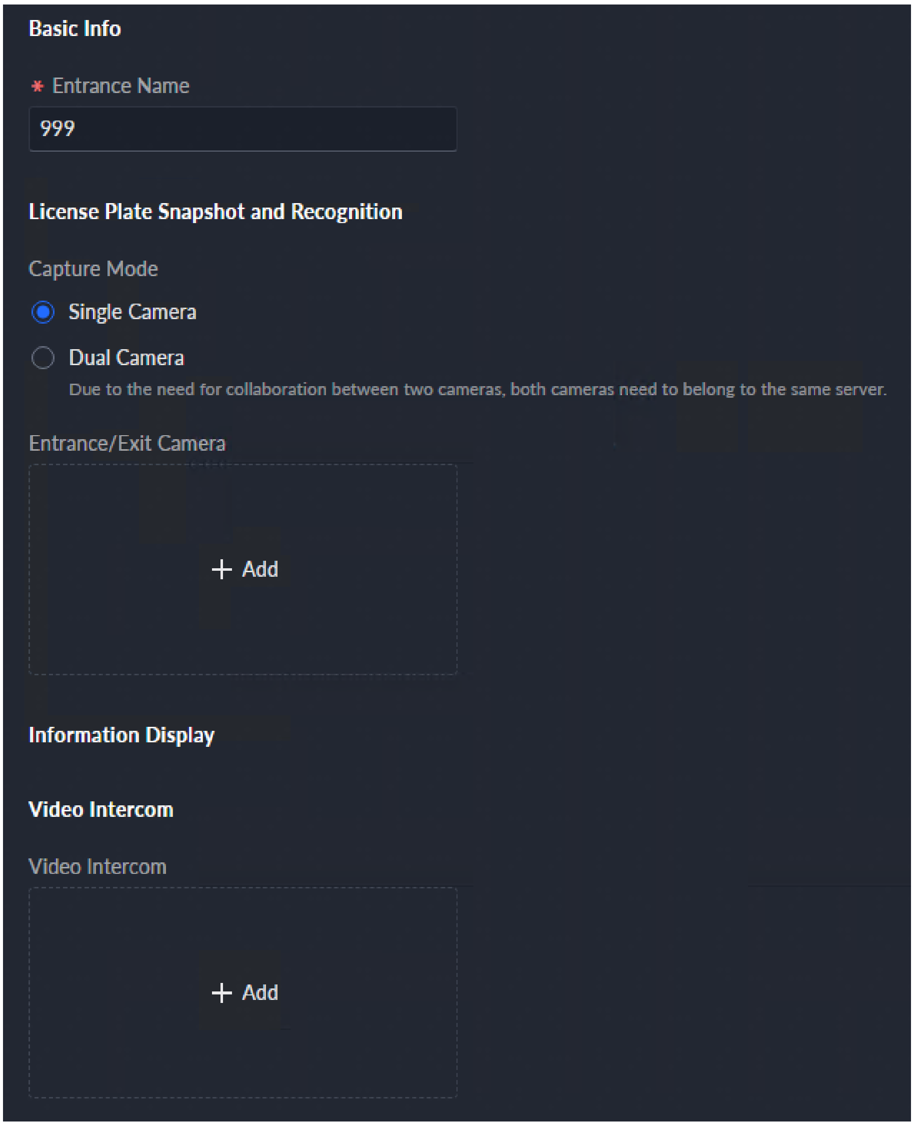
1. Click **Add Entrance and Exit Point**.
2. Enter a name (for example, south gate), and then click **OK**.
3. Select a mode for the entrance point.
    - **With Barrier** : It is generally used for managing closed parking lots, and the platform can configure entry and exit rules to determine whether vehicles need to automatically open the barrier based on these rules.
    - **Without Barrier** : It is generally used for managing open parking lots, such as gas stations, service areas, and similar scenarios, where it only records vehicle passage.

      When EVS or IVSS transparently transmits the images or videos of the events, we recommend selecting the **Without Barrier** mode.
4. If there is an entrance point, click in the **Entrance** section.
5. Enter a name for the point, select a capture mode, and then add a camera, video intercom device (optional).

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

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

Figure 6-45 Entrance point configuration



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

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

Step 6 Configure the passing rules, and then click **Save and Exit**.

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

Table 6-35 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.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Custom</td><td>
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 "5.1.5 Adding Time Template".
 Open Barrier by Verification : Configure rules, the access permission of a vehicle must be verified, and then an administrator can manually open the barrier for it.

None : No additional verification is required; barrier opens directly according to the configured passing rules.
Open Barrier by Manual Verification : The barrier opens automatically after the vehicle has been successfully verified through card or face.
Open Barrier Directly by Verification : The barrier opens automatically after the vehicle has been successfully verified through card or face.
Open Barrier by Two-Factor Verification : Configure vehicle owner or vehicle color verification.

Verification by Vehicle Owner : The barrier opens automatically after a vehicle has been successfully verified through the license plate and a verification method such as card or face.
Verification by Vehicle Color : The barrier opens automatically after a vehicle has been successfully verified through its license plate and the color of the vehicle.
You can enable Automatically opens the barrier even if the vehicle color fails to be verified, and then the barrier opens when the vehicle color fails to be verified.

 Available Parking Space Counting

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.

</td></tr>
</table>

For how to configure vehicle groups, see "6.9.3 Managing Vehicle Group".

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

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

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

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

Related Operations

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

6.9.2.2 Parking Lot Event

6.9.2.2.1 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 "6.1 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 6-36 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 "6.9.2.2.2 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.

6.9.2.2.2 Overtime Parking Rule

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

Procedure

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

Step 2 Click , and then configure the parameters.

Figure 6-46 Add rules

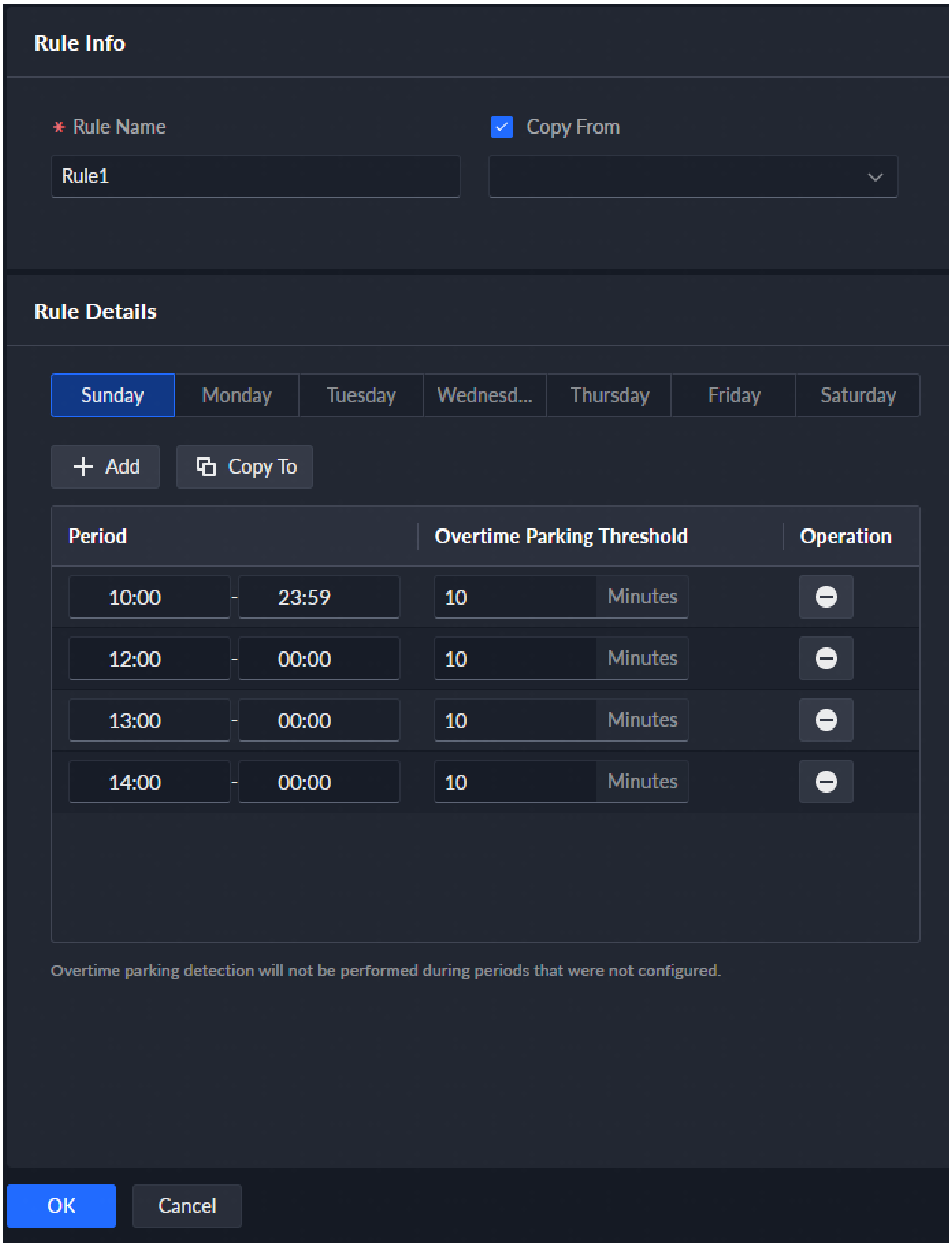


Table 6-37 Parameter description

Parameter	Description
Rule Name	Configure the rule name to differentiate it from others.
Copy From	Select the check box, and then select a rule from the drop-down list to reuse the existing rules.

Parameter	Description
Rule Details	View the rule details or add new period. Click **Add** to add overtime parking period and set over time parking threshold. Click **Copy To** to copy the configured rules to another times.

Step 3 Click **OK**.

6.9.3 Managing Vehicle Group

Add vehicles to different groups, so that you can quickly apply different parking lot functions to multiple vehicles at the same time. General, VIP, and blocklist are the default groups. If you need to use them, you can directly add vehicles to them.

Procedure

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

Step 2 Click .

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

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

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

Related Operations

Available Parking Spaces

1. Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Parking Lot** > **Vehicle Management**.
2. Select a parking lot, and then available parking space to display available parking space information.
   - **Available Parking Spaces for Person**: Display available parking space information for person.
   - **Available Parking Spaces for Vehicle Group**: Display available parking space information for vehicle.
3. Click **Add**, and then configure the parameters of the available parking space.
4. Click **OK**.

6.10 Intelligent Analysis

Before using the people counting and scheduled report functions, you must configure them first.

- People counting: Create a people counting group and add multiple people counting rules from one or more devices to it. Then, you can view the real-time and historical number of people of the group.
- Scheduled report: Configure the when to send a report with historical people counting data, the email address to send the report to, and the content of the email.

6.10.1 People Counting Group

Create a people counting group, and then add multiple people counting rules from one or more devices. In Intelligent Analysis, you can view the real-time and historical number of people of the group.

Procedure

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

Step 2 Click at the upper-left corner.

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

Figure 6-47 Add a people counting group

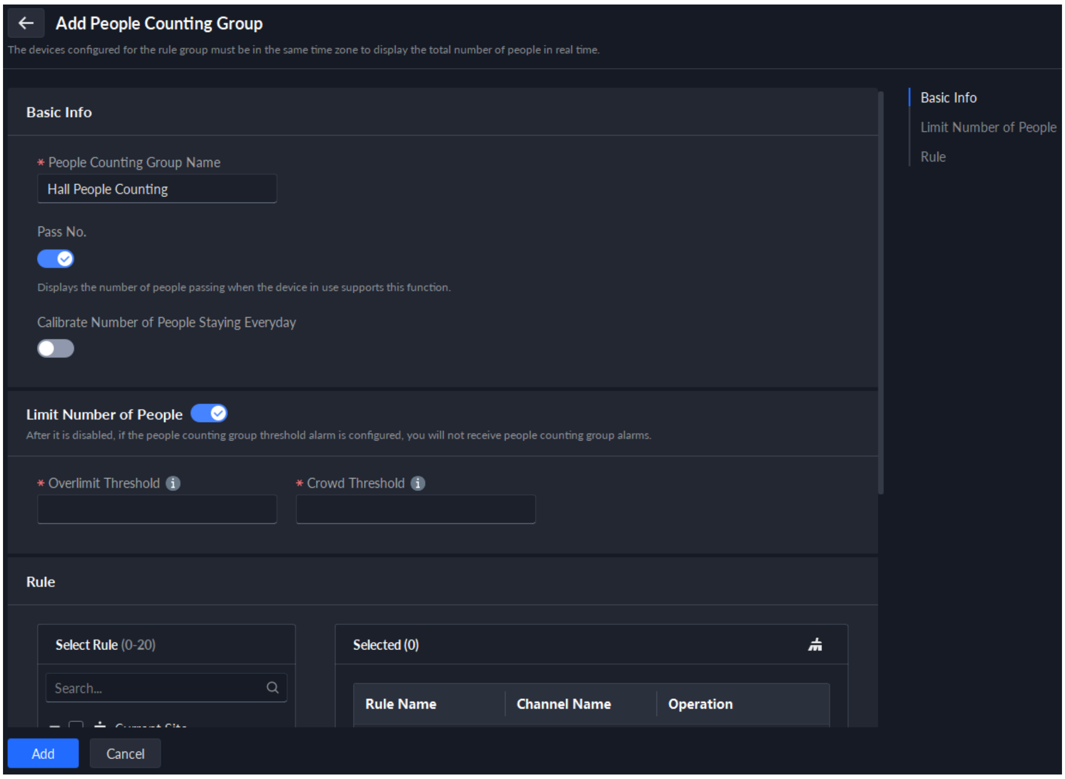


Table 6-38 Parameter description

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	

Parameter	Description
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 "6.1 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.

6.10.2 Scheduled Report

Historical data will be sent on a regular basis to one or more email address that you set on the scheduled time.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Intelligent Analysis** > **Scheduled Report Config**.

Step 2 Configure one or more types of report.

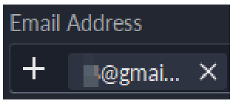
- Daily report: Data from yesterday will be sent to your email at a defined time. If set to 03:00:00, the data from the day before (00:00:00–23:59:59) will be sent to your email at 03:00:00 every day.
- Weekly report: Data from last week will be sent to your email at a defined time. If set to 03:00:00 on Wednesday, the data from Wednesday to Tuesday of each week will be sent to your email at 03:00:00 every Wednesday.
- Monthly report: Data from last month will be sent to your email at a defined time. If set to 03:00:00 on 3rd, the data from 3rd of last month to 2nd of the current month will be sent to your email at 03:00:00 on 3rd of each month.

Step 3 Configure one or more email addresses to send the report to, and the content of the email.

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

Figure 6-48 Invalid email address, you must press Enter

Figure 6-49 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.

7 Businesses Operation

7.1 Monitoring Center

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

7.1.1 Main Page

Provides frequently used functions such as video, event and alarm.

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

Prerequisites

The **Resources** and **View** menu permissions are required; otherwise, you cannot view resources, add them to favorites, and save the resources to view. Permissions can be configured from > **User** > **Role Management**.

Page Description

Figure 7-1 Monitoring center

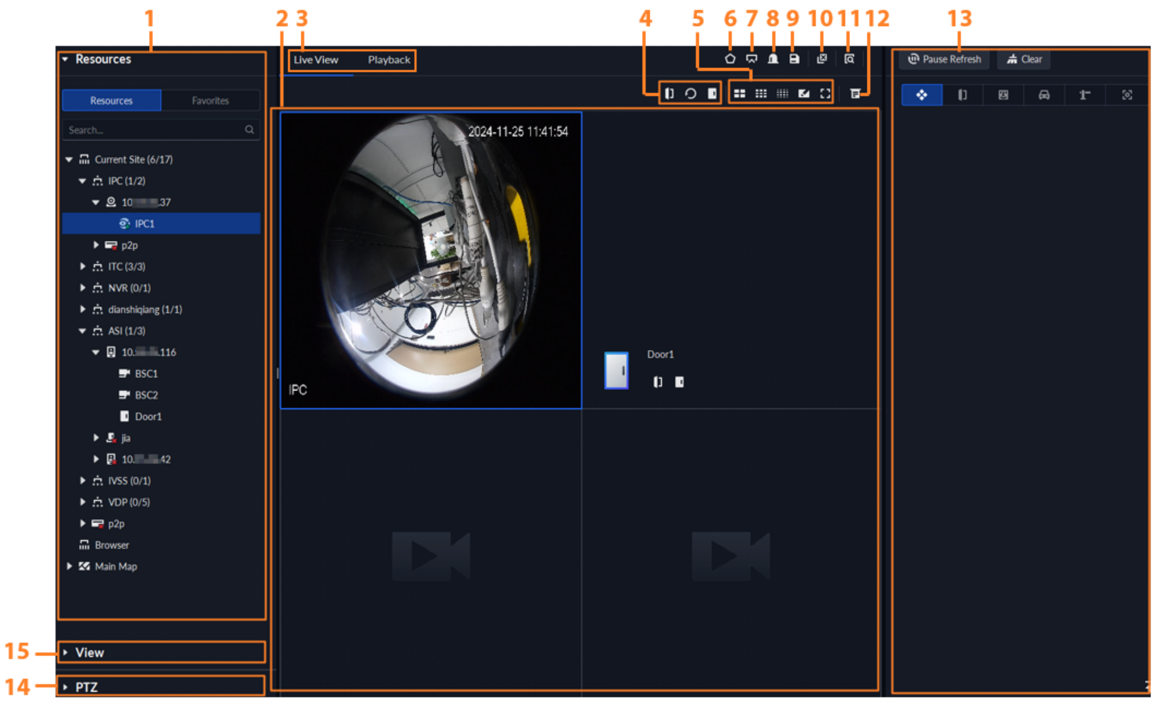


Table 7-1 Description

No.	Parameter	Description
1	Favorites and device tree	● List of resources including devices, browser, and maps. ● You can search for a device or channel in the search field. Fuzzy search is supported so that you can simply enter part of the name and then select the exact one from the provided name list. ● Add, delete or rename the favorites. You can also tour the channels in favorites.
2	Real-time videos	Drag a channel to the windows and view its real-time video.
3	Live view and playback	● Live view: View real-time videos. ● Playback: View recorded videos. For details, see Playback. Drag between the resource tree and the video window to the left, to hide the resource tree, and then the **View and Resource** selection bar will show at the top, where you can select or search the views and resources that you need, and then drag them to the window to play the video. Click to show the resource tree.
4	Control doors	For a door channel, you can configure its mode through these icons , including normally open and closed modes, and restoring it to the normal status. After restoring it to the normal status, people must verify their identifications to pass within defined periods.
5	Window split mode and full screen	● Set a window split mode. Supports 1, 4, 6, 8, 9, 13, 16, 20, 25, 36 or 64 splits, or click to set a customized split mode. If the live-view channel number is more than the number of current windows, then you can turn page(s) by clicking the buttons on the top of the page. ● Switch the video window to **Full Screen** mode. To exit **Full Screen**, you can press the Esc key or right-click on the video and select **Exit Full Screen**.
6	AI rule overlay	The function is available when **AI Rule Overlay** is turned on from **Local Settings** > **Video** > **General**. ● **Default** : Shows AI rules on the video by default. ● **Open All** : Shows the AI rules of the channels on the video, and the right-click menus of **AI Overlay** and **SMD Overlay** are also displayed. ● **Close All** : Hides the AI rules of the channels on the video, and the right-click menus of **AI Overlay** and **SMD Overlay** are also hidden.
7	Push videos to a video wall	Real-time videos that are currently opened can be quickly displayed on a video wall. You must configure a video wall before using this function. For details, see "7.1.5 Video Wall".

No.	Parameter	Description
8	Set alarm windows in batches	Set all windows as alarm windows. After selecting **Open alarm linkage video in live view** from **Local Settings** > **Alarm**, the alarm videos will be displayed on the alarm windows. If the number of alarm windows is less than that of linkage videos, the video linked to the earliest-triggered alarm will be opened.
9	Save view	Save all the channels or websites that are opened in to a view so that you can quickly open all of them later. For details, see "7.1.2.2 View".
10	Close all windows	Close all windows in live view.
11	Search for targets in the video	The platform supports manually selecting targets in the video, and then quickly searching for them in DeepXplore. For details, see "7.1.2.1 Viewing Live Video".
12	Event panel button	Displays or hides the event panel.
13	Events	Displays events from channels that you are viewing live videos from. You can: ● Click different tabs to display only that type of events. ● Click clear all the events. ● Click to go to the top of the list to view the latest events.
14	PTZ	If the channel you are viewing live video from is of a PTZ camera, you can control it through the control panel. For details, see "7.1.2.4 PTZ".
15	View	● Save the current view of window split and video channels in the live view section, and name the view. You can directly select the view from the **View** tab to display it quickly next time. ● Channels under a view or view group can be displayed by tour (in turn). You can set the tour interval to be 10 s, 30 s, 1 min, 2 min, 5 min or 10 min. ● A maximum of 100 views can be created.

7.1.2 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.

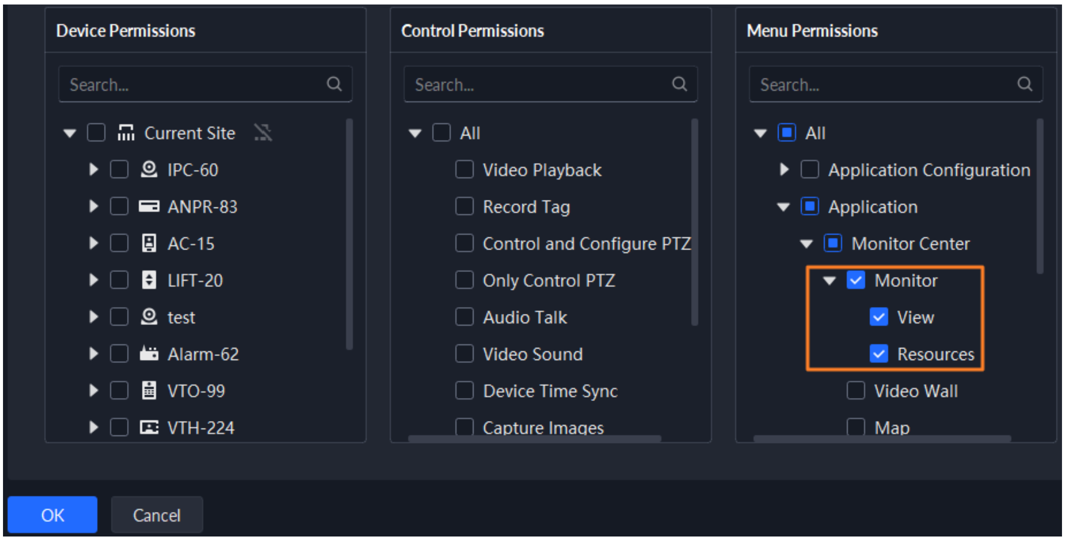
7.1.2.1 Viewing Live Video

View the live video of connected devices.

Prerequisites

The **Resources** and **View** menu permissions are required; otherwise, you cannot view resources, add them to favorites, and save the resources to view. Permissions can be configured from > **User** > **Role Management**.

Figure 7-2 Configure view and resources permissions



Background Information

This section only introduces viewing live video. For map live view, see "6.2 Configuring Map".

Procedure

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

Step 2 Click **Live View** tab.

Step 3 View real-time video.

You can view live video in the following ways:

- Double-click a channel or drag the channel from the device list on the left to one window on the right.
- Double-click a device to view all channels under the device.
- Right-click a node, select **Tour**, and then set tour interval. The channels under this node will play in turn according to the defined interval.

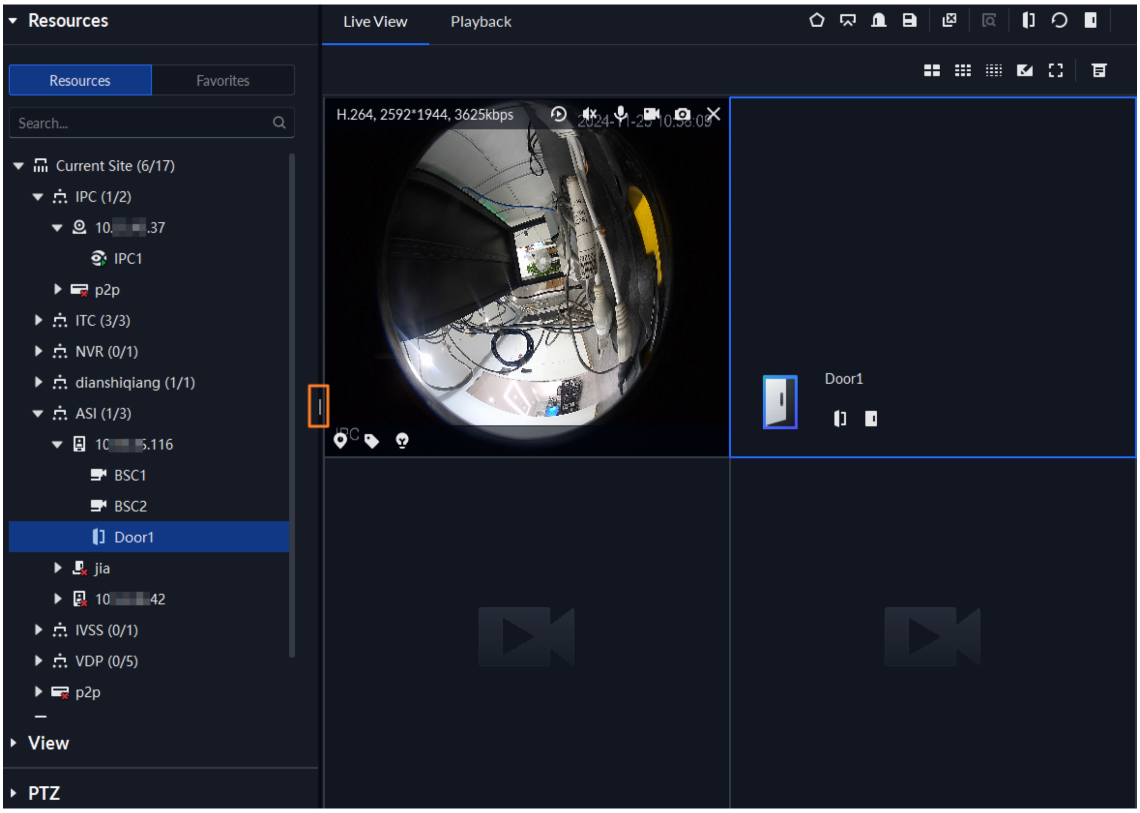
◇ Drag ▯ between the resource tree and the video window to the left, to hide the resource tree, and then the **View and Resource** selection bar will show at the top, where you can select or search the views and resources that you need, and then drag them to the window to play the video.

Click ▶ to show the resource tree.

◇ If the number of window splits is more than the number of online channels, video of all channels will be displayed in the window. Otherwise, double-click the root node, and then click ◂ 1/32 ▸ on the top of the page to turn pages.

◇ Close the on-going tour before starting live view.

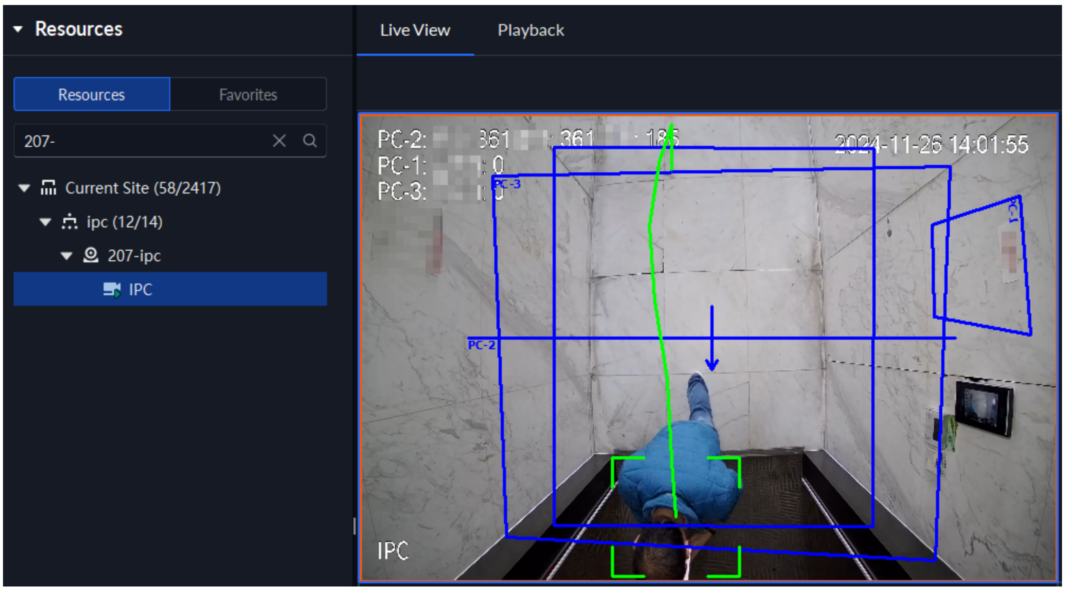
Figure 7-3 Live view



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), right-click the monitoring image, and then select **AI Overlay** > **Bounding Box Overlay**, you can view the person tracks on the monitoring image.

Figure 7-4 View person track



- Display intelligent snapshots.

  When viewing live video of face detection cameras, face recognition cameras, ANPR cameras, or target detection cameras, right-click the monitoring image, and then select **Start Picture Overlay**. The snapshot will be displayed on the upper-right corner of the live window. If no more images are captured, a snapshot will be displayed up to 5 seconds by default, and it will disappear after 5 seconds.

Point to the live window, and then select type of images to be displayed.

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

Figure 7-5 Live window

Table 7-2 Parameter description

Icon	Name	Description
	Instant playback	Turn on/off instant playback. The playback time can be defined from **Local Settings** > **Video** > **Video Playback**.
	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**.
	Audio communication	Start two-way audio with the device the channel belongs to. 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.

Icon	Name	Description
	Local record	Click it, and then the system begins to record local file and you can view the record time on the upper left. Click again, and then system stops recording and saves the file to your PC. The recorded video is saved to *C:\DSS\DSS Client\Record* by default. To change the storage path, see "10.4.5 Configure File Storage Settings".
	Snapshot	Take a snapshot. The snapshots are saved to *C:\DSS\DSS Client \Picture* by default. To change the snapshot storage path, see "10.4.5 Configure File Storage Settings".
	Close	Close the video.
	Map location	If the channel has been tagged on the map, click the icon, and then you can open the map in a new window to view the device position on the map.
	Tag	Tag the videos of interest for easy search in the future. You can search for the tagging records from **Download Center** > **Tagging Record**. **Device Permissions** and the **Record Tag** control permission are required from > **User** > **Role Management**; otherwise, you cannot tag the video.

- Sleep function is supported for IPCs that use 4G mobile network to communicate and are solar-powered.
  - When the device is asleep, you can click to wake it up.
  - The device will regularly request to sleep to save battery. When you are viewing its live video, the device will request to sleep every 2 minutes. When you are not viewing its live video, the device will request to sleep every 1 minute. You can accept or reject so that you can continue to watch live video. When rejecting the request, you can choose whether to delay the next request from the device.
- Right-click the live video, and then the shortcut menu is displayed.

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

Table 7-3 Description

Parameters	Description
Select Audio Input	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Continuous Snapshot	Take snapshots of the current image (three snapshots each time by default). The snapshots are saved to *C:\DSS\DSS Client\Picture* by default. To change the snapshot storage path, see "10.4.5 Configure File Storage Settings".

Parameters	Description
Detailed Tag	Tag the videos of interest for easy search in the future. You can set tag details such as tag name, tagging time, time before and after tag, the user who adds the tag, tag object, and more. The tagging records can be searched from **Download Center** > **Tagging Record**. ◇ **Device Permissions** and the **Record Tag** control permission are required from > **User** > **Role Management**; otherwise, you cannot tag the video. ◇ The channel that you want to tag is configured with recording plan; otherwise, no video can be searched after you adding the tag.
Stream Type	Select stream type as required. Generally, main stream requires the most bandwidth, and sub stream 2 the least. The smaller the bandwidth is required by the stream, the smoother the video image.
Play Mode	When playing videos, both fluency and real-time performance matter. To deal with network fluctuations, the platform has a set of buffer control strategies to ensure fluency and real-time performance. You can select one of the following play modes as needed. ◇ **Real-time Play Priority**: The system might lower the image quality to avoid video lag. It is suitable for special scenarios with high requirements on real-time performance. ◇ **Fluency Priority**: The system might lower the image quality and allow for lag to ensure video fluency. The higher the image quality, the lower the video fluency will be. ◇ **Balance Priority** (recommended): The system balances real-time priority and fluency priority according to the actual 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.
Video Adjustment	Adjust the brightness, contrast, saturation, and chroma of the video for video enhancement.
Digital Zoom	Click it, and then click and hold the video image to zoom in on the image. Right-click the image, and then select **Digital Zoom** again to exit zooming in.
Window Mode	Divide one window into 2 (1+1 mode), 4 (1+3 mode), and 6 (1+5 mode). One window will play the real-time video, and the others play different defined areas of the real-time video. If a device supports target tracking, you can enable this function in any window mode, the windows that play defined areas of the real-time video will follow the target when detected, until it disappears.

Parameters	Description
Stop Image Overlay	Click it, and then the snapshot information of people and vehicle metadata will be overlaid over the upper right of the video image, click it again to stop image overlay. Make sure that the device supports people and vehicle metadata snapshot.
AI Overlay	Displays rule lines, bounding box on targets, and detection area for intelligent rules, except for motion detection. After enabled, the configuration will be saved, and only works on the current channel in the live view and playback. AI overlay information is not displayed by default.
SMD Overlay	Displays the bounding box on targets. After enabled, the configuration will be saved, and only works on the current channel in the live view and playback.
Disable Privacy Masking	For a camera that supports privacy masking of human face, you can disable the masking here to view the face image.
Alarm Output Control	Turn on or turn off alarm output channels.
Audio and Light Control	You can turn on or off the audio and light channels one by one or at the same time. This function is available on select device only.
Device Intercom	For channels added through NVR, XVR/DVR, IVSS or EVS, you can select this option to talk to the NVR, XVR/DVR, IVSS or EVS.
Add to Favorites	You can add the active channel or all channels to favorites.
Time Sync	Synchronize device time with platform time. This function requires **Device Permissions** and the **Device Time Sync** control permission from > **User** > **Role Management**.
Set as Alarm Window	When selecting open alarm linkage video **In Preview** (in live window) from **Local Settings** > **Alarm**, then the video will be displayed on the window which is set to alarm window. If multiple alarms are triggered, the video linked to the latest alarm will be opened. If the number of alarm windows is fewer than the number of linkage videos, the video linked to the earliest-triggered alarm will be opened. After enabling **Set as Alarm Window**, the window frame is displayed in red.

Parameters	Description
Fisheye View	According to different installation methods, the fisheye view can be varied. ◇ In-ceiling mount: 1P+1, 2P, 1+2, 1+3, 1+4, 1P+6, 1+8. ◇ Wall mount: 1P, 1P+3, 1P+4, 1P+8. ◇ Ground mount: 1P+1, 2P, 1+3, 1+4, 1P+6, 1+8. This function is available on fisheye cameras only. When changing the video stream, the fisheye view mode will maintain the current configuration.

- To view real-time temperature of a point on the thermal camera view, hover over that point.
- If a channel supports electronic focus, you can enable electronic focus for it on the platform to adjust video definition and size.

The page might vary according to the lens types of cameras. Lens types include embedded zoom lens and external CS electronic lens. The following figure is for reference only.

Figure 7-6 Live view

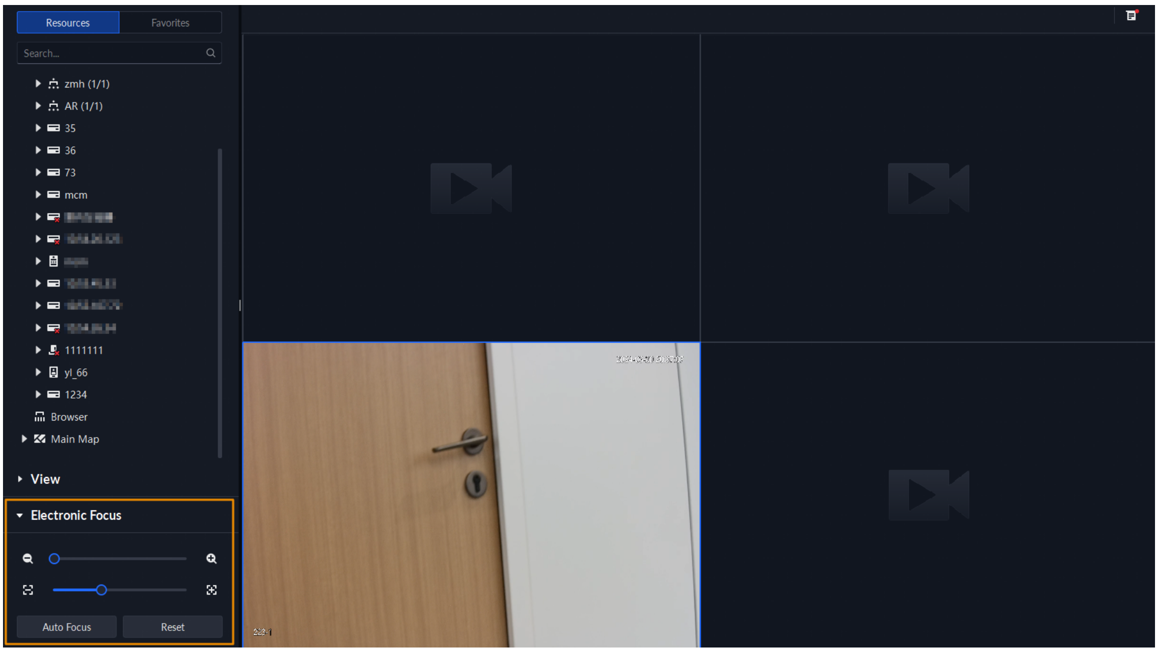


Table 7-4 Description

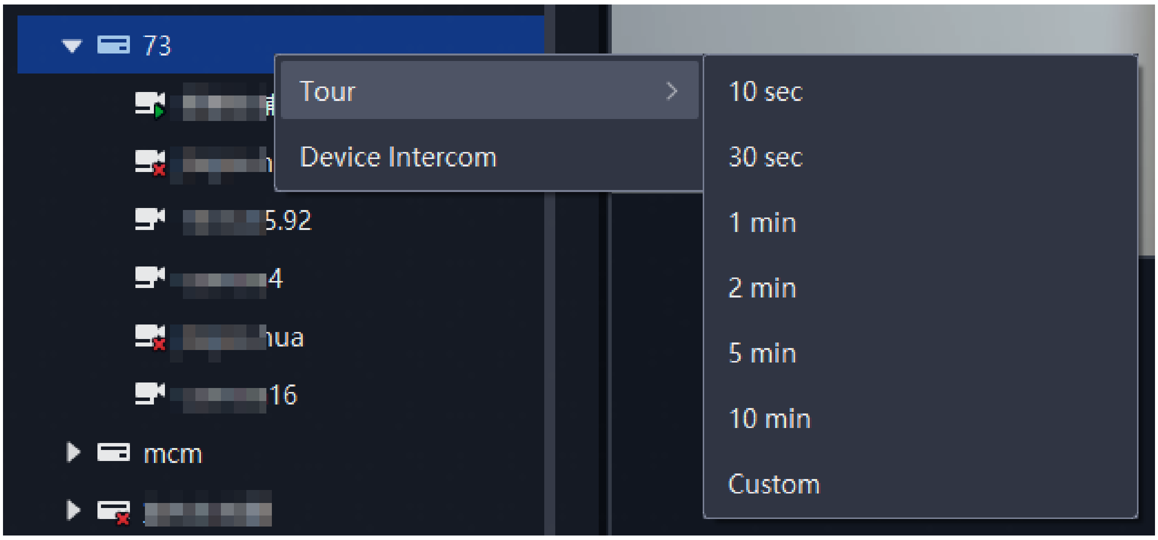
Parameters	Description
Zoom +/- (for embedded zoom lens)	Zoom in/out. Click, or click and hold or , or drag the slider to the left or right to zoom in/out.

Parameters	Description
Focus +/-	Adjust camera focus to achieve the best video definition. Click or click and hold or , or drag the slider to the left or right to adjust focus.
Auto Focusing (for embedded zoom lens)	Adjust image definition automatically. Other focusing operations are unavailable during auto focusing.
ABF (auto back focusing, for external CS electronic lens)	
Reset	When image definition is imperfect, or after many times of zooming or focusing operations, you can click **Reset** to reset the lens, so as to eliminate lens deviation.

- Tour

  On the live view page, right-click a device or node, select **Tour**, and then select an interval. The channels under this device or node will be played in turn at the pre-defined interval. You can also customize the interval.

Figure 7-7 Start tour



  - ◇ To view remaining time of a channel during tour, check .
  - ◇ To pause, click .
  - ◇ To exit tour play, click .
- Region of interest (RoI)

  A window can be divided into 4 or 6 regions during live view. One area is used to play live video and other regions are used to zoom in regional image.

  On the live view page, right-click the window, select **Window Mode**, and then select a mode. For example, select a 1+3 mode.

  To exit the **Window Mode**, right-click the window and then select .

Figure 7-8 Split mode

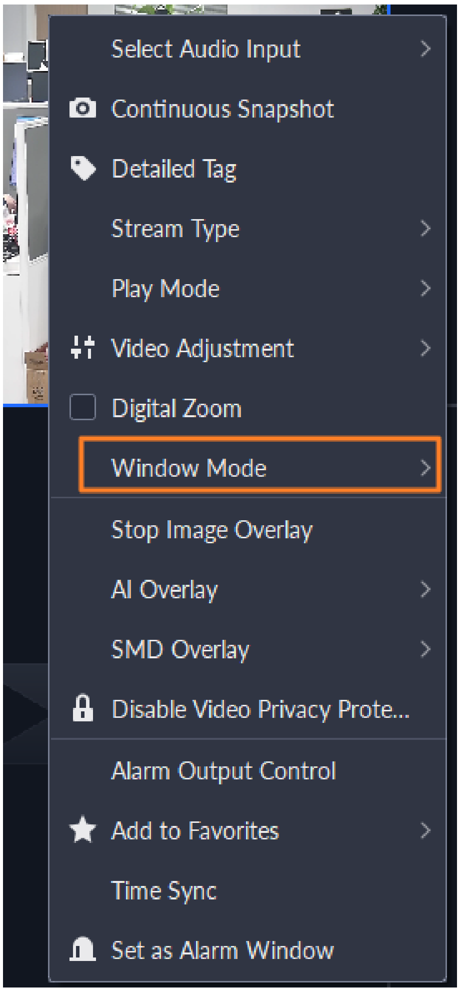
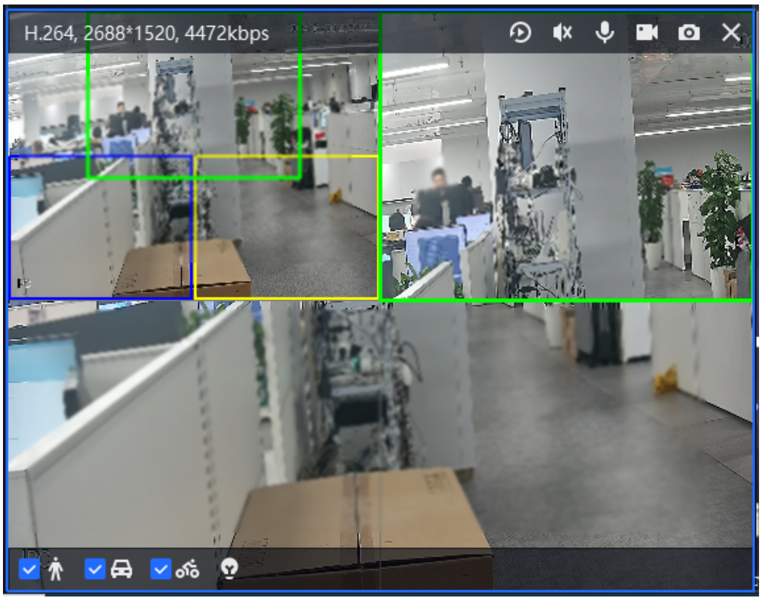


Figure 7-9 1+3 mode



- Search for targets in the video.

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

Figure 7-10 Select a target

- View real-time events.

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

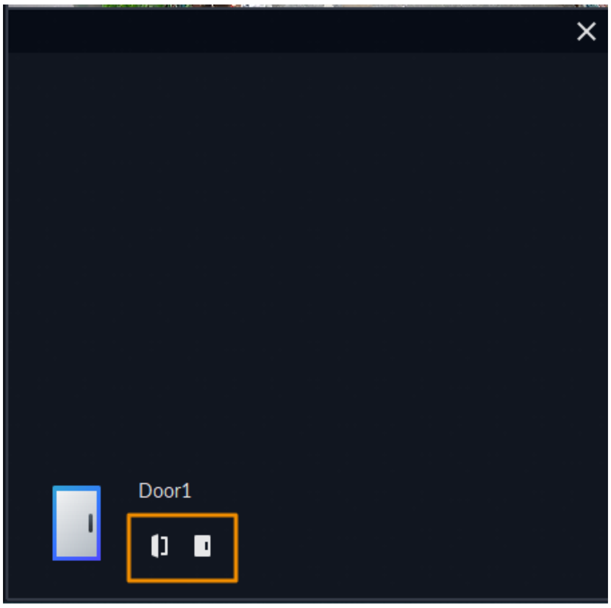
  - ◇ Click the event type on the top of the event panel to view the corresponding event.
  - ◇ Click event record to view the snapshot. Video playback is also supported. Operations related to different events might be different.
  - ◇ : Refreshes events in real time. : Stops refreshing.
  - ◇ Click to clear the events in the event panel.
  - ◇ Click to quickly view the latest events.
  - ◇ : View the recorded video of the event.
  - ◇ : Go to DeepXplore to search for the target.
  - ◇ : This function is only available when a license plate is recognized. Click this icon to add the vehicle to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the vehicle is recognized.
  - ◇ : Add the vehicle to the platform.
  - ◇ : Add the person to the platform.
  - ◇ : Add the face to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the face is recognized.
- Remotely unlock the door.

  When viewing the access control channel, you can remotely control the status of the door on the upper-right corner: Normally open (), normally closed (), or normal status (). You need to enter the login password of the current user before operation.

Restore the door to normal status first, and then the door can be opened and closed according to defined period or through face recognition.

In the video window of the access control channel, you can remotely lock or unlock the door.

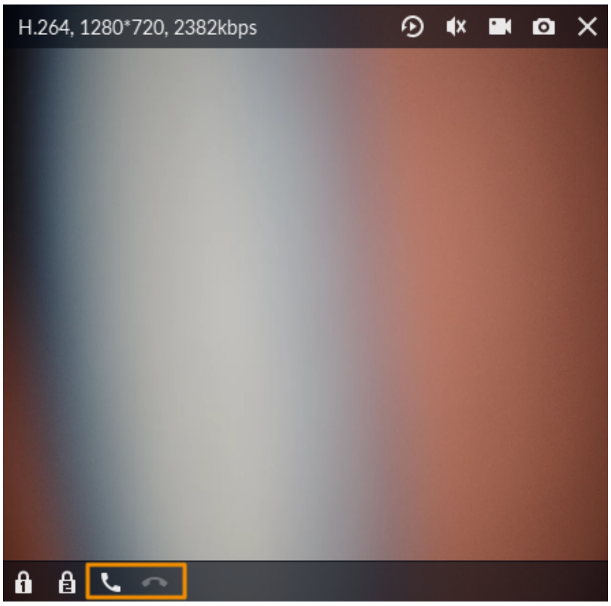
Figure 7-11 Lock/unlock the door



- Video intercom.

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

Figure 7-12 Video intercom



7.1.2.2 View

The current layout and resources can be saved as a view to be quickly played next time.

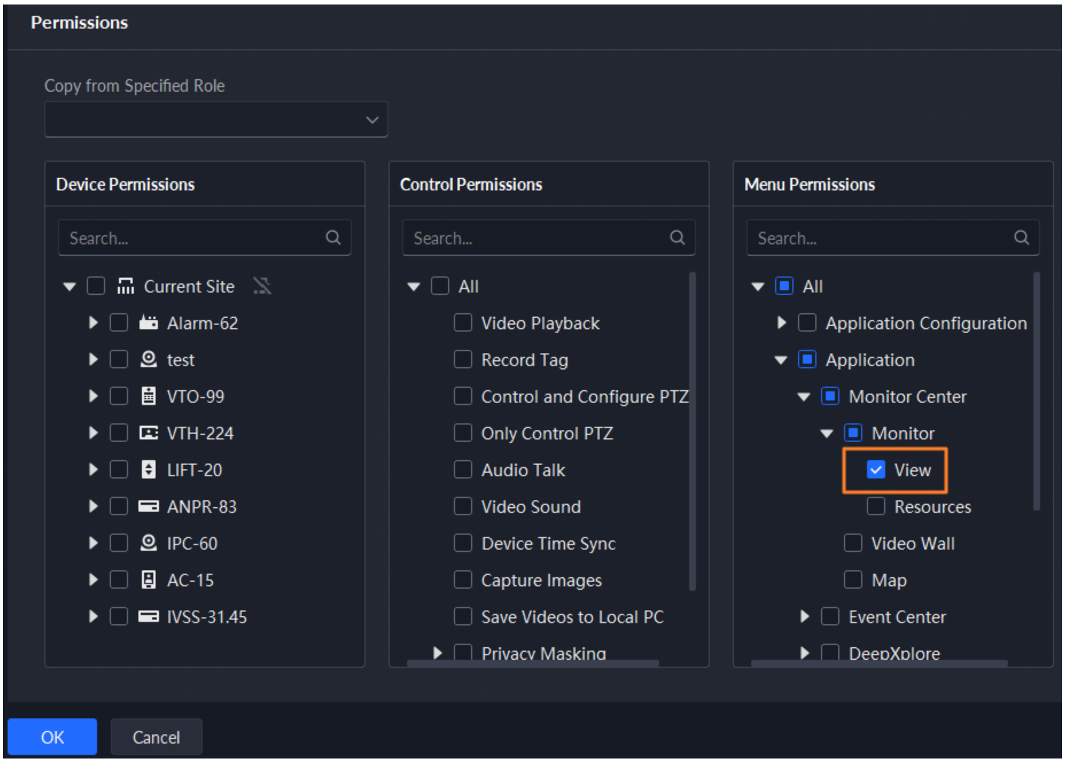
Views can be categorized as public views and private views. Only administrators are allowed to configure public views, and the users specified by them can access certain public views. Private views are configured and owned by users themselves. They can share private views with other users.

Views are categorized into different groups, which include three levels: First-level root node, second-level grouping and third-level view. Tour is supported for first-level root node and second-level grouping. The tour time can be 10 seconds, 30 seconds, 1 minutes, 2 minutes, 5 minutes, 10 minutes, or customized (5 seconds–120 minutes). You can create up to 1000 views.

Prerequisites

The **View** menu permission is required; otherwise, you cannot save the resources to view. The permission can be configured from > **User** > **Role Management**.

Figure 7-13 Configure view permission



7.1.2.2.1 Creating a Public View Group

Public view groups are used to organize public views. There is the default root group of the Public View. You can only create one level of sub groups. Only administrators are allowed to create public view groups.

Background Information

By default, all users are allowed to access **Public View** and its views. If you want to control access, create groups that can be accessed by specified roles and their users, and save views to the groups.

Procedure

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

Step 2 Click **View**.

Step 3 Right-click **Public View** , and then select **Create View Group**.

Step 4 Enter a name for the group, and then select the roles that are allowed to access this group.

Click to view the users of a selected role.

Step 5 Click **OK**.

7.1.2.2.2 Creating a Private View Group

Private view groups are used to organize private views. There is the default group of the Private View. You can only create one level of sub groups. Private views are configured and owned by users themselves. They can share private views with other users.

Procedure

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

Step 2 Click **View**.

Step 3 Right-click **Private View** , and then select **Create View Group**.

Step 4 Enter a name for the group, and then click **OK**.

7.1.2.2.3 Creating a View

Views are categorized into public or private view groups. They are used to quickly apply different resources and settings. For example, a view can contain the configurations of multiple live video, split mode, alarm windows, and more. When you open the view, these configurations will be applied at the same time, and you do not need to configure them again.

Procedure

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

Step 2 Configure the split mode, and then drag channels, maps, and the browser to the windows.

Step 3 Click on the upper-right corner to save the current layout.

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

Table 7-5 Parameter description

Parameter	Description
View Type	Select a type for the view. Only administrators can create a public view. If the view is saved to **Public View**, all users can access it.
View Name	Enter a name for the view. It can be the same as other groups or views.
View Group	Select a group for the view based on its type.

7.1.2.2.4 Updating a View

When you need to change the resources or settings in a view, you can update them directly without creating a view.

Procedure

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

Step 2 Click **View**.

Step 3 Double-click or drag a view to a window to open it.

Step 4 Change the resources or settings, such as the split mode, number of channels and alarm windows, and the locations of the channels.

Step 5 Click on the upper-right corner to update the view.

7.1.2.2.5 Viewing a View

- Live view

  Double-click or drag a view to a window to view its resources.
- Tour

  Right-click a view group, select **Tour** and set the tour period.

  - To view remaining time for a view, check 00:05.
  - To pause, click .
  - To exit tour, click .

7.1.2.2.6 Sharing a Private View

Privates views can be shared with other users.

Procedure

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

Step 2 Click **View**.

Step 3 Right-click a private view, and then select **Share View**.

Step 4 Select a user and enter a message in remarks, and then click **OK**.

The view will be saved to **Private View** of the user.

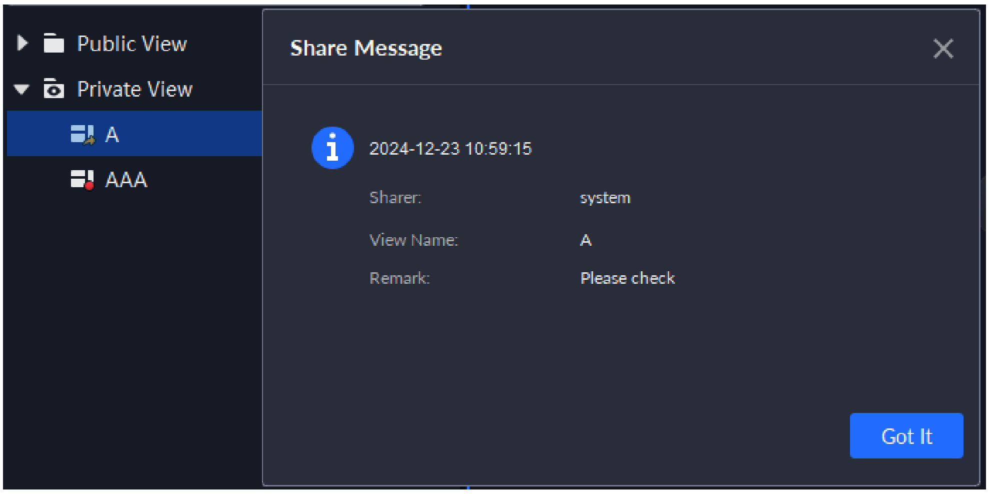
It will fail to share if the user's view groups or views reach the limit. You can share again after the user deletes a group or view.

Results

The user who receives the shared view can right-click a view, and then click **View Details** to check the details of the shared view.

indicates read, and indicates unread.

Figure 7-14 Check the shared view



7.1.2.2.7 Related Operations

- Change the group a view belongs to

  Drag a view to other groups. You can only do so for private views. You cannot drag a private view to a public view group, or a public view to a private view group.
- View the details of a public view group or a view

  Right-click a public view group, and then select **View Details** to check the roles and users that are allowed to access it.

  Right-click a public view group, and then select **Resources Details** to check the information of the channels, including the name, type, and organization.
- Edit the information of a public view group

  Right-click a public view group, and then select **Edit** to change its name and the roles and users that are allowed to access it.
- Rename a view

  Right-click a view, and then select **Rename** to change its name.
- Delete a group or view

  Right-click a group or view, and then select **Delete** to delete it. If there are multiple views in the group, they will also be deleted.

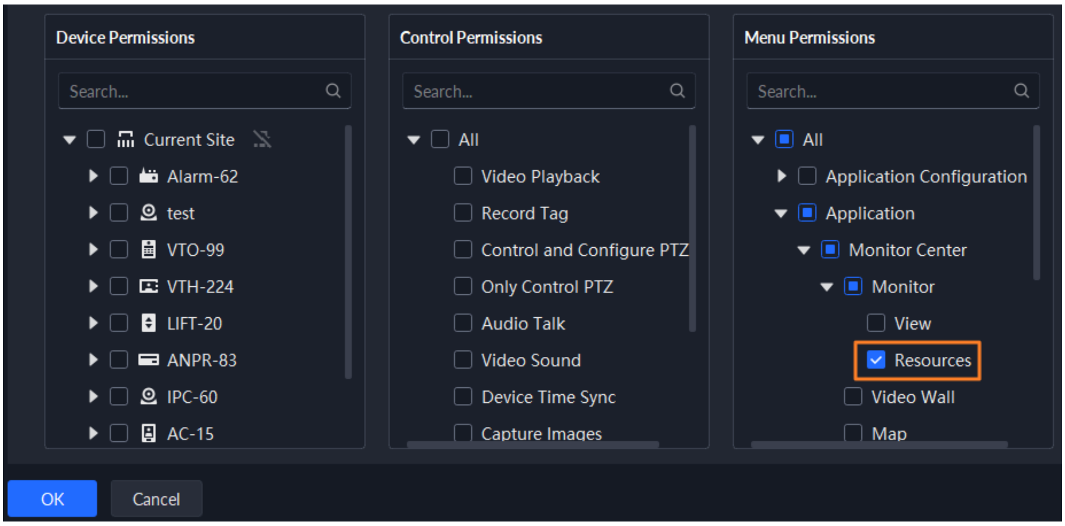
7.1.2.3 Favorites

Add frequently used channels to favorites so that you can quickly locate and use them. You can also share your favorites with other users.

Prerequisites

The **Resources** menu permission is required; otherwise, you cannot view resources, add them to favorites, and save the resources to view. Permissions can be configured from > **User** > **Role Management**.

Figure 7-15 Configure view and resources permissions



7.1.2.3.1 Creating Favorites Folder

Each user can create up to 999 favorites folders. The number of channels in all favorites folders can be up to 2,000.

Procedure

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

Step 2 Click **Favorites**.

Step 3 Click a folder and click +, or right-click a folder and select **Add a Favorites**.

Step 4 Select a parent node, enter a name for the folder, select the channels to be added to the folder, and then click **OK**.

The favorites folder is added as a sub folder under the parent node you selected. The maximum level of a favorites folder can be up to 10.

7.1.2.3.2 Editing or Deleting Favorites Folder

Log in to the DSS Client. On the **Home** page, click ⊞, and then select **Monitoring** > **Favorites**.

- Edit a folder: Click a folder and click ✎, or right-click a folder and select **Edit**, and then you can edit the name and channels of the folder.
- Delete a folder: Click a folder and click 🗑, or right-click a folder and select **Delete**, and then you can delete the folder, its sub folders and all channels.

  You can also right-click a channel and select **Delete** to remove it from a folder.

7.1.2.3.3 Sharing Favorites Folder

You can share a folder and its channels with other users. For permission control, if users have permission to access certain channels, or do not have any permission to access the channels, they will receive a folder with only the channels they have permission to, or an empty folder.

Procedure

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

Step 2 Click **Favorites**.

Step 3 Right-click a folder, and then select **Share the Favorites**.

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

The folder, its sub folders, and all the channels will be shared with the users you selected. But if any of the follow situation occurs with the users you are sharing with, this operation will fail:

- They have more than 999 folders.
- They have 2,000 channels in all folders.
- The levels of their folders have reached 10.

7.1.2.3.4 Viewing Favorites Folder

- Live view

  On the **Monitoring** page, and then click **Favorites** to open list of favorites folders. Double-click or drag a folder or channel to the window on the right to view live videos.
- Tour

  On the **Monitoring** page, and then click **Favorites** to open list of favorites folders. Right-click a folder and select **Tour**, and then select a duration. The platform plays live videos of all the channels in the folder and its sub folders in a loop.

  ◇ To view remaining time of a channel during tour, click .

  ◇ To pause, click .

  ◇ To exit tour play, click .

7.1.2.4 PTZ

Operate PTZ cameras during live view on the DSS Client.

Background Information

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

7.1.2.4.1 Configuring Preset

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

Procedure

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

Step 2 Click .

Step 3 Click .

Step 4 Add a preset.

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

Related Operations

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

7.1.2.4.2 Configuring Tour

Set the tour parameters so that a camera can go back and forth among different presets. Set tour to enable camera to automatically go back and forth between different presets.

Prerequisites

You have added at least 2 presets.

Procedure

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

Step 2 Click .

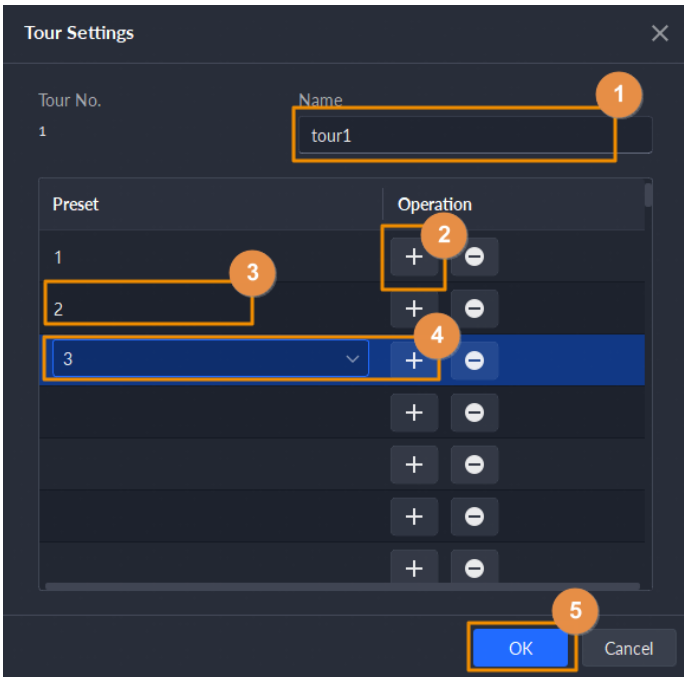
Step 3 Click .

Step 4 Click .

Step 5 Add tours.

1. Enter tour name, and click .
2. Select a preset from the drop-down list on the left.
3. Repeat the previous 2 steps to add more presets.
4. Click **OK**.

Figure 7-16 Add tours (2)



Related Operations

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

7.1.2.4.3 Configuring Pattern

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

Procedure

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

Step 2 Click .

Step 3 Click .

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

Step 5 Click .

Related Operations

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

7.1.2.4.4 Enabling/Disabling Pan

On the **Monitoring Center** page, open the video of a PTZ camera. Click , and then click . PTZ rotates 360° at a specified speed. Click to stop camera rotation.

7.1.2.4.5 Enabling/Disabling Wiper

Enable/disable the PTZ camera wiper. Make sure that the camera supports wiper function.

On the **Monitoring Center** page, open the video of a PTZ camera. Click , and then click to turn on wiper. Click to turn off wiper.

7.1.2.4.6 Enabling/Disabling Light

Turn on/off camera light. Make sure that the camera supports light.

On the **Monitoring Center** page, open the video of a PTZ camera. Click , and then click to turn on light. After enabling light, click to turn off light.

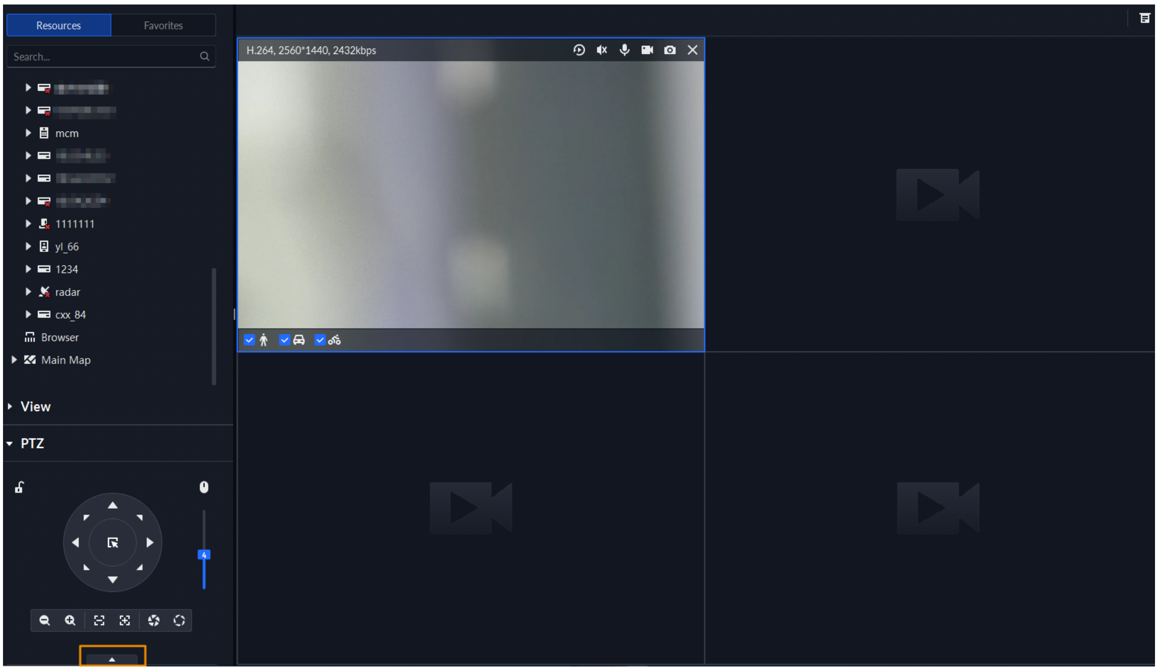
7.1.2.4.7 Configuring Custom Command

Procedure

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

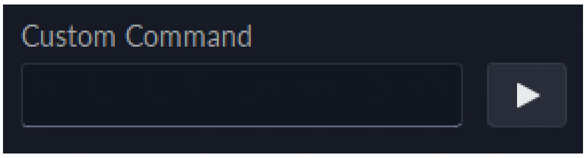
Step 2 Click .

Figure 7-17 Go to PTZ control



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

Figure 7-18 Custom command



Step 4 Click ▶ to show the command functions.

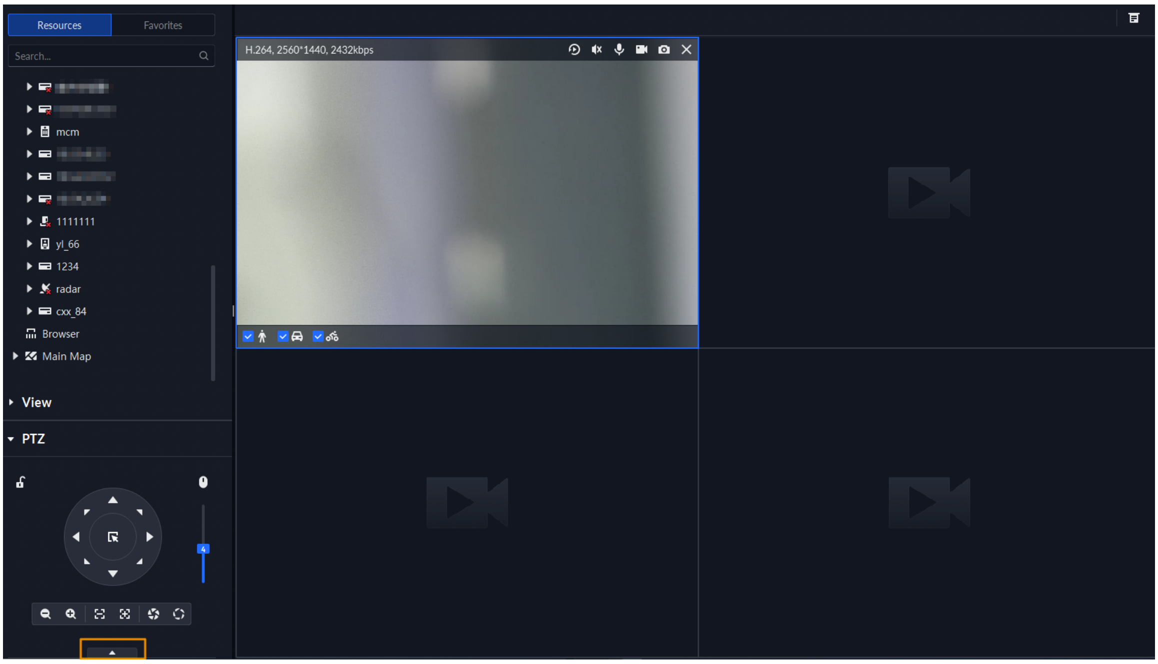
7.1.2.4.8 PTZ Menu

Procedure

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

Step 2 Click ▲.

Figure 7-19 Go to PTZ control panel



Step 3 Click .

Step 4 Click .

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

Figure 7-20 Go to PTZ menu configuration page

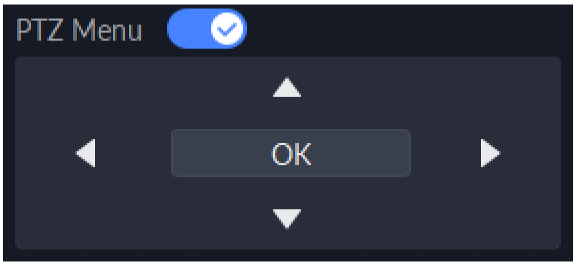


Table 7-6 PTZ menu description

Parameters	Description
/	Up/down.
/	Left/right. Point to set parameters.
	Click to enable PTZ menu function. System displays main menu on the monitor window.
	Click to close PTZ menu function.
OK	It is the confirm button. It has the following functions. ● If the main menu has the sub-menu, click **OK** to enter the sub-menu. ● Point to **Back** and then click **OK** to go to go back to the previous menu. ● Point to **Exit** and then click **OK** to exit the menu.

Parameters	Description
Camera	Point to **Camera** and then click **OK** to enter camera settings sub-menu page. Set camera parameters. It includes picture, exposure, backlight, day/night mode, focus and zoom, defog, and default.
PTZ	Point to **PTZ** and then click **OK** to go to PTZ sub-menu page. Set PTZ functions. It includes preset, tour, scan, pattern, rotation, PTZ restart, and more.
System	Point to **System** and then click **OK** to go to system sub-menu page. Set PTZ simulator, restore camera default settings, video camera software version and PTZ version.
Return	Point to the **Return** and then click **OK** to go back to the previous menu.
Exit	Point to the **Exit** and then click **OK** to exit PTZ menu.

7.1.2.5 Fisheye-PTZ Smart Track

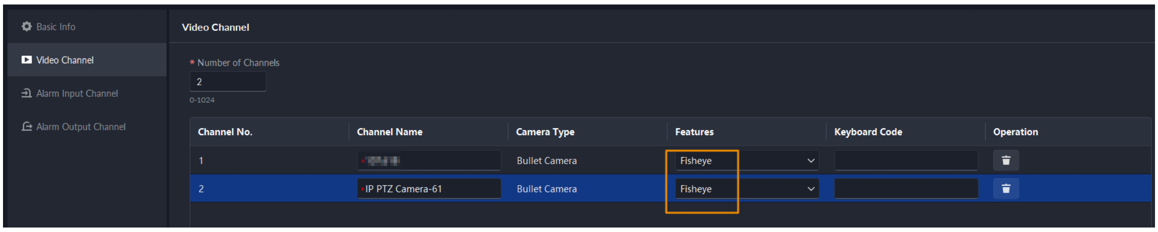
Link a PTZ camera to a fisheye camera so that when the fisheye camera detects a target, the PTZ camera automatically rotates to it and track.

7.1.2.5.1 Preparations

Make sure the following preparations have been completed:

- Fisheye camera and PTZ camera are well deployed. For details, see corresponding user manuals.
- Basic configurations of the platform have been finished. For details, see "5 Basic Configurations".
  - ◇ When adding cameras, select **Encoder** from **Device Category**.
  - ◇ The **Features** of a fisheye camera is set to **Fisheye**. For details, see "5.1.2.5.2 Modifying Device Information".

Figure 7-21 Set the feature to Fisheye



7.1.2.5.2 Configuring Fisheye-PTZ Smart Track

Procedure

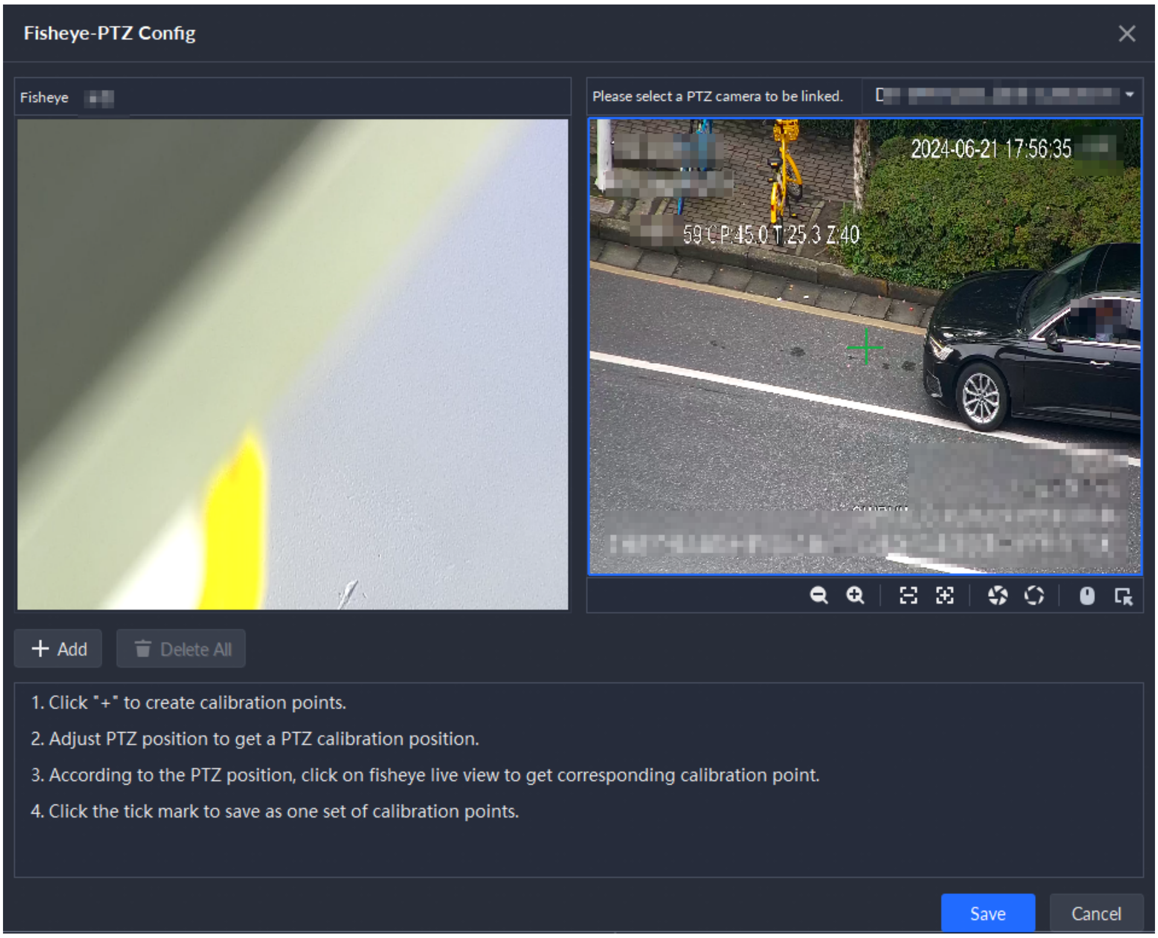
Step 1 Log in to the DSS Client. On the **Home** page, click , and then click **Monitoring Center**.

Step 2 Click .

Step 3 In the device tree on the left, right-click a fisheye camera, and then select **Modify Smart Track**.

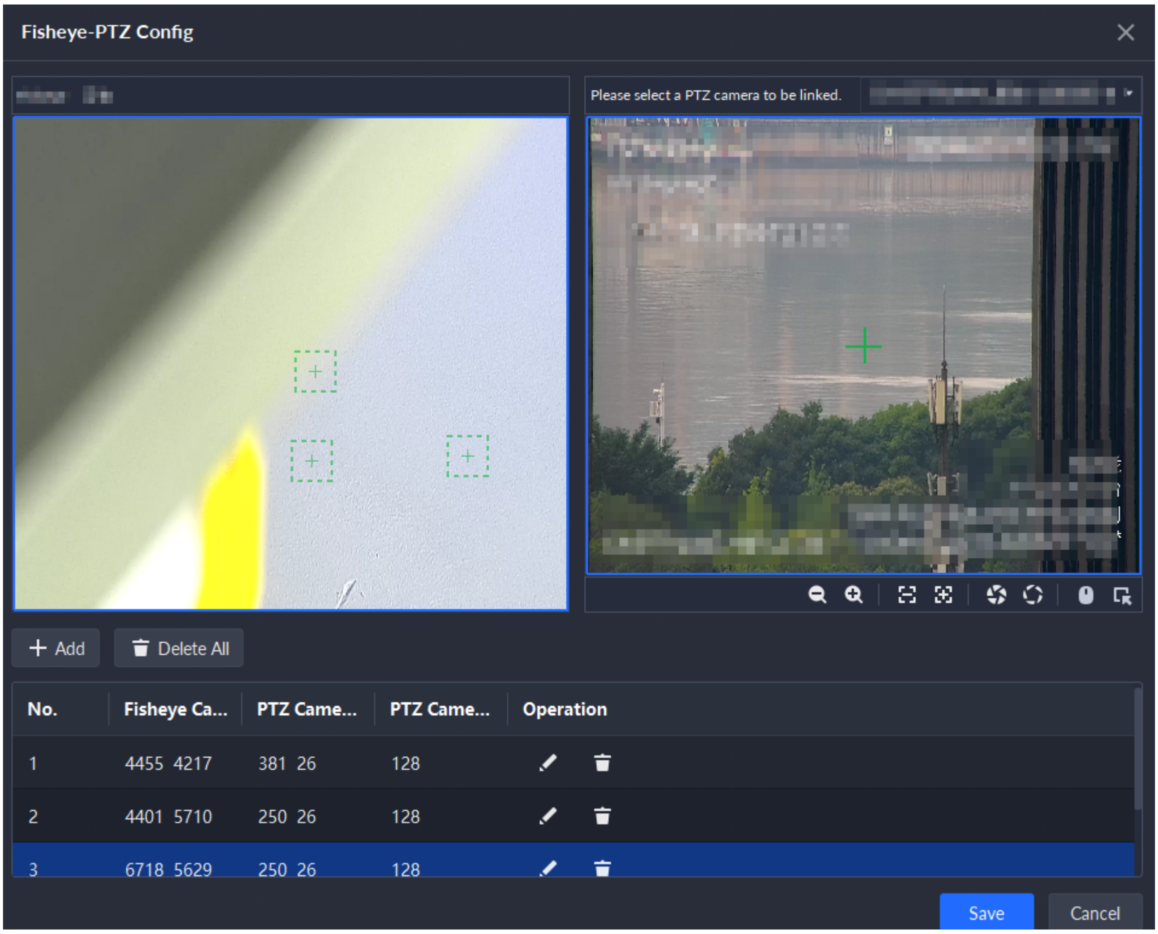
Step 4 Click next to **Please select a PTZ camera to link**, and then select a PTZ camera.

Figure 7-22 Set smart track rules (1)



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

Figure 7-23 Set smart track rules (2)



- Select 3-8 mark points on fisheye camera.
- When you find mark point on the right side of the PTZ camera, click to zoom out PTZ.
- Click to 3D position, and when you click a certain point on the left side of PTZ camera, it will automatically move to the center.

Step 6 Click to save the calibration point.

See above steps to add at least three calibration points. These three points shall not be on the same straight line.

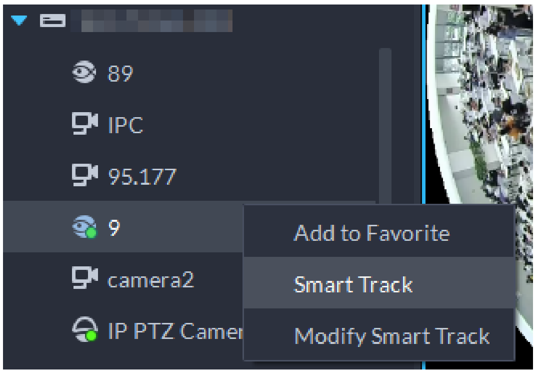
Step 7 Click **Save**.

7.1.2.5.3 Applying Fisheye-PTZ Smart Track

Procedure

Step 1 Log in to the DSS Client. On the **Monitoring Center** page, select the fisheye camera on the device tree and then right-click to select **Smart Track**.

Figure 7-24 Select a smart track channel



Step 2 Click any point on the left of fisheye, PTZ camera on the right will automatically rotate to corresponding position.

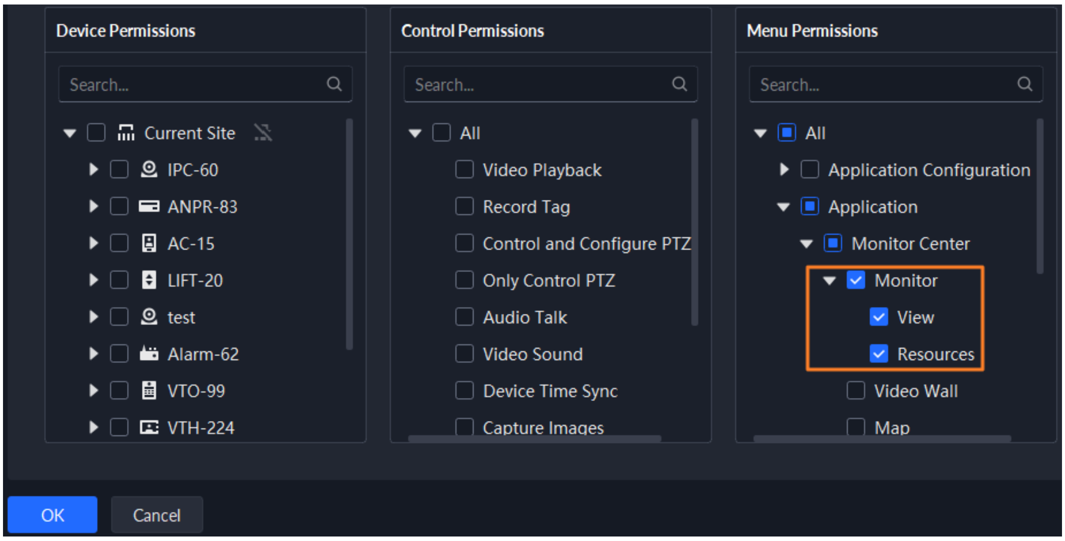
7.1.3 Playback

Play back recorded videos.

Prerequisites

The **Resources** and **View** menu permissions are required; otherwise, you cannot view resources, add them to favorites, and save the resources to view. Permissions can be configured from > **User** > **Role Management**.

Figure 7-25 Configure view and resources permissions



7.1.3.1 Page Description

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

Drag between the resource tree and the video window to the left, to hide the resource tree, and then the **View and Resource** selection bar will show at the top, where you can select or search the views and resources that you need, and then drag them to the window to play the video.

Click to show the resource tree.

Figure 7-26 Playback page

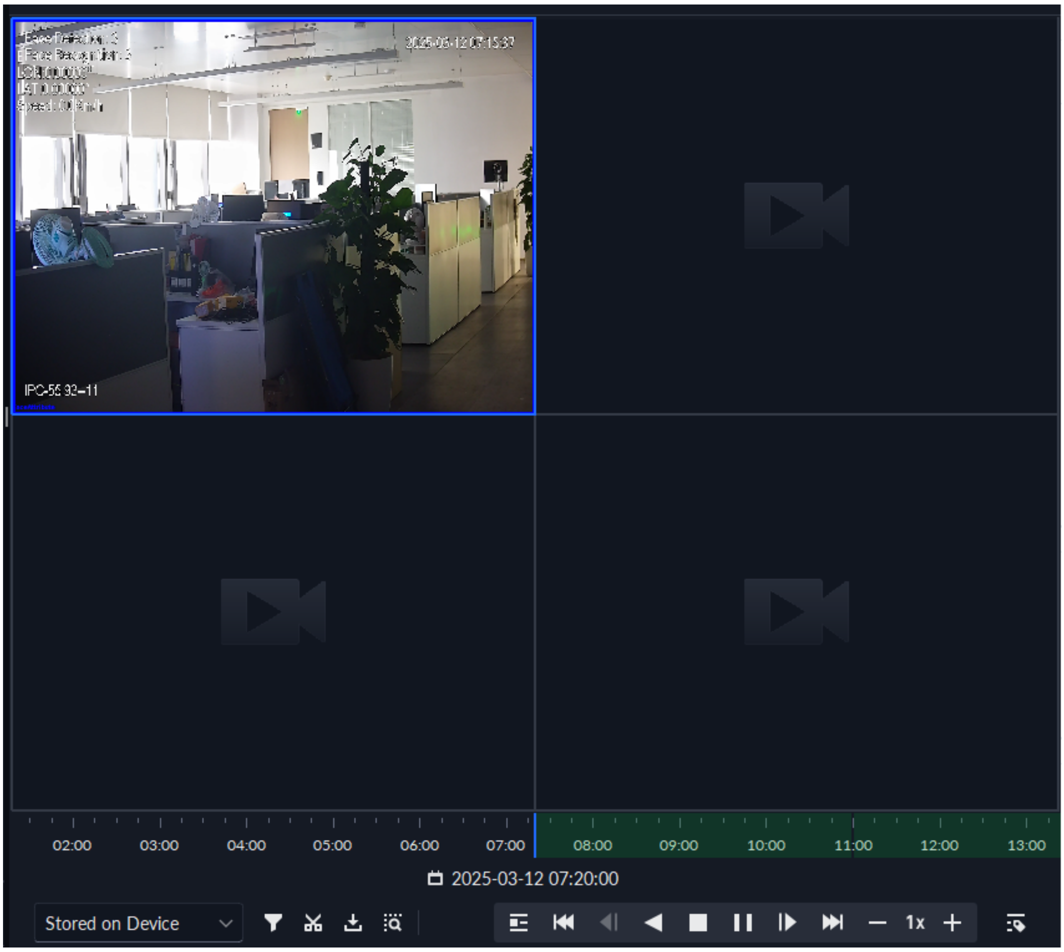
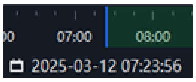


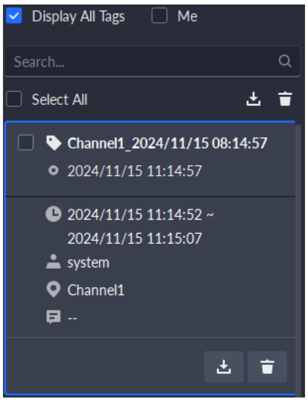
Table 7-7 Function description

Icon	Description
	Filter video according to record type.
	Select and download a duration of video on the progress bar.
	Download the video.

Icon	Description
	Make dynamic detection analysis over some area of the record image, and it only plays back the video with dynamic image in the detection area.
	Play multiple recorded videos from the same time. For example, you are playing recorded videos from 3 channels at the same time. Select channels, configure when you want to play the recorded video from, and then click this icon. All 3 channels will play recorded videos from the same time.
	Play the previous or next video clip of the most recent time. For example, when searching for videos, if you do not remember the exact event time, and there is no video clip at the time that you search, you can try to play the previous or next video of the most recent time, to track the event. This function is not available when  is enabled.
	Play back or forward by frame.
	Play the video backwards.
	Stop or pause the video.
	Fast forward or slow down the video to up to 64 times. When playing a video backwards or forwards alternately, the play speed will not be changed.
	Click  to select the date to view the video. The time period of the video is displayed on the timeline. During playback, you can drag time progress bar to play back video at the specific time. Stay your mouse on the time progress bar, and then the system displays the video thumbnail of that time, which makes it easy to determine whether it is the video that you want to view.
	Select the storage location of the video to be searched.

<table>
<tr><th>Icon</th><th>Description</th></tr>
<tr><td></td><td>
Open the tag to view the tag records. You can also:

- Select **Display All Tags** or **Me** to view all tags or tags added by you.
- Double-click a tag record to play the video related to the tag.
- Click to view tag details, such as the time before and after tagging, the user who added the tag, the channel name, remarks, and more.
- Download the records one by one or in batches. When downloading, you need to set an encryption password to encrypt the tag records.
- Delete the tags one by one or in batches.



</td></tr>
</table>

7.1.3.2 Playing Back Video

Procedure

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

Step 2 Click the **Playback** tab.

Step 3 Double-click or drag a channel to a window on the right.

> Drag between the resource tree and the video window to the left, to hide the resource tree, and then the **View and Resource** selection bar will show at the top, where you can select or search the views and resources that you need, and then drag them to the window to play the video.
>
> Click to show the resource tree.

Step 4 Select the storage path of recorded video from **Stored on Device**, and then click to select the date.

> - Dates with blue dots means there are videos.
> - After selecting a date, the platform will search for videos on that date from other channels. If you switch to the **Live View** page, or close the page or the PC client, the date will be reset.

Step 5 Click to play the video.

Step 6 Hover over the video, and then the icons appear. You can perform the following actions.

Figure 7-27 Video playback

Table 7-8 Function description

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. The saving path is C:\DSS\DSS Client\Record\ by default.
	Take a snapshot on the device	Take a snapshot of the current image and save it locally. The saving path is *C:\DSS\DSS Client\Picture* by default.
	Close	Close the window.
	Map location	If the device has been marked on the map, click the icon to open the map in a new window to display map location of the device.
	Search by snapshot	Capture the target in the playback window. Click to select the search method, and then the system goes to the page with search results. More operations: ● Place the mouse on the selected area, and then drag to move the selection area. ● Place the mouse to the upper-left, upper-right, and lower-left corner of the selected area, drag to adjust the size of the selection area. ● Right-click to exit search by snapshot.

Icon	Name	Description
	Tag	Tag the videos of interest for easy search in the future. You can search for the tagging records from **Download Center** > **Tagging Record**. **Device Permissions** and the **Record Tag** control permission are required from > **User** > **Role Management**; otherwise, you cannot tag the video.

Right-click the video, and then you can perform the following actions. The menu might vary, depending on the devices that you use.

Figure 7-28 Shortcut menu

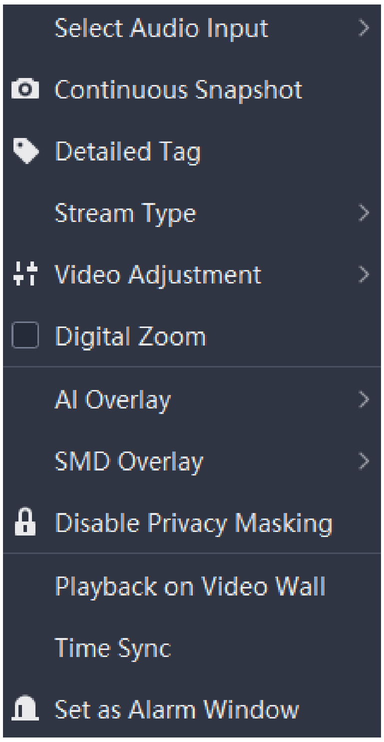


Table 7-9 Description

Parameters	Description
Select Audio Input	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Continuous Snapshot	Take snapshots of the current image (three snapshots each time by default). The snapshots are saved to *C:\DSS\DSS Client\Picture* by default. To change the snapshot saving path, see "10.4.5 Configure File Storage Settings".

Parameters	Description
Detailed Tag	Tag the videos of interest for easy search in the future. You can set tag details for that tag such as its name, time, the moment before and after it, the user who created it, and its object. You can also search for the tag records in **Download Center** > **Tagging Record**. ● You must gain control permission in **Device Permissions** and the **Record Tag**. Go to > **User** > **Role Management** to set them, otherwise, you will not be able to tag the video. ● The channel that you want to tag must be configured with recording plan, otherwise you will not be able to search for videos after you add tags.
Stream Type	Select **Main Stream**, **Sub Stream 1** or **Sub Stream 2**. Videos recorded on the main stream will have the best quality, but they require more storage. This function is available for recordings stored on device only.
Video Adjustment	Adjust the brightness, contrast, saturation, and chroma of the video for video enhancement.
Digital Zoom	Click it, and then double-click the video image to zoom in the image. Double-click the image again to exit zooming in.
AI Overlay	The client does not show rule lines over live video by default. When needed, you can click **AI Overlay** , enable **Rule Overlay** and **Bounding Box Overlay**, and then the live video shows rule lines if the AI detection rules are enabled on the device. This configuration is effective with the current selected channel both in live video and playback.
SMD Overlay	Enable **SMD Overlay** to show target bounding box over live video. When SMD is enabled on the device, you can enable **SMD Overlay** for the device channel, and then the live video will display dynamic target bounding boxes. This configuration is effective with the current selected channel both in live video and playback.
Disable Privacy Masking	For cameras that support privacy masking for human faces, you can disable the masking here to view the face image.
Playback on Video Wall	Play the video of the current channel on video wall. Make sure that video wall is configured (see "7.1.5 Video Wall").
Time Sync	Synchronize the device time with platform time. This function requires that you gain control permission in **Device Permissions** and the **Device Time Sync**. Go to > **User** > **Role Management**.

Parameters	Description
Set as Alarm Window	When selecting open alarm linkage video **In Preview** (in live window) from **Local Settings** > **Alarm**, then the video will be displayed on the window which is set to alarm window. If multiple alarms are triggered, the video linked to the latest alarm will be opened. If the number of alarm windows is fewer than the number of linkage videos, the video linked to the earliest-triggered alarm will be opened. After enabling **Set as Alarm Window**, the window frame is displayed in red.

7.1.3.3 Tagging Videos

You can tag records of interest for quick search.

Procedure

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

Step 2 Click the **Playback** tab.

Step 3 Double-click or drag a channel to a window.

Step 4 Select the storage path from Store on Server where the recorded videos are stored, and then click to select the date.

The search results are displayed.

Dates with blue dot means there are video recordings.

Figure 7-29 Playback page

Step 5 Point to the window, and then click .

Step 6 Enter a name for the tag, and then click **OK**.

Related Operations

Click on the lower-right corner to view all the tags in the current recorded video. Double-click a tag to play the recorded video from the time of the tag. You can search for tags by their names.

7.1.3.4 Filtering Recording Type

Filter video according to record type, record type includes scheduled recording, alarm video, motion detection video, and videos recorded in main or sub stream.

Procedure

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

Step 2 Click the **Playback** tab.

Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

Step 4 Click , select one or more types, and then click **OK**.

The platform only displays videos of the selected types in different colors on the timeline.

Filtering videos by video stream is only supported when you are viewing a video stored on a device, and the search type of device video stream is set to main and sub streams. For details, see "10.4.2 Configuring Video Settings".

7.1.3.5 Searching for Targets

When playing back a video, you can manually select a target, and then search for it in DeepXplore.

Procedure

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

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

Step 3 Select the storage path of recorded video from Stored on Device, and then click to select the date.

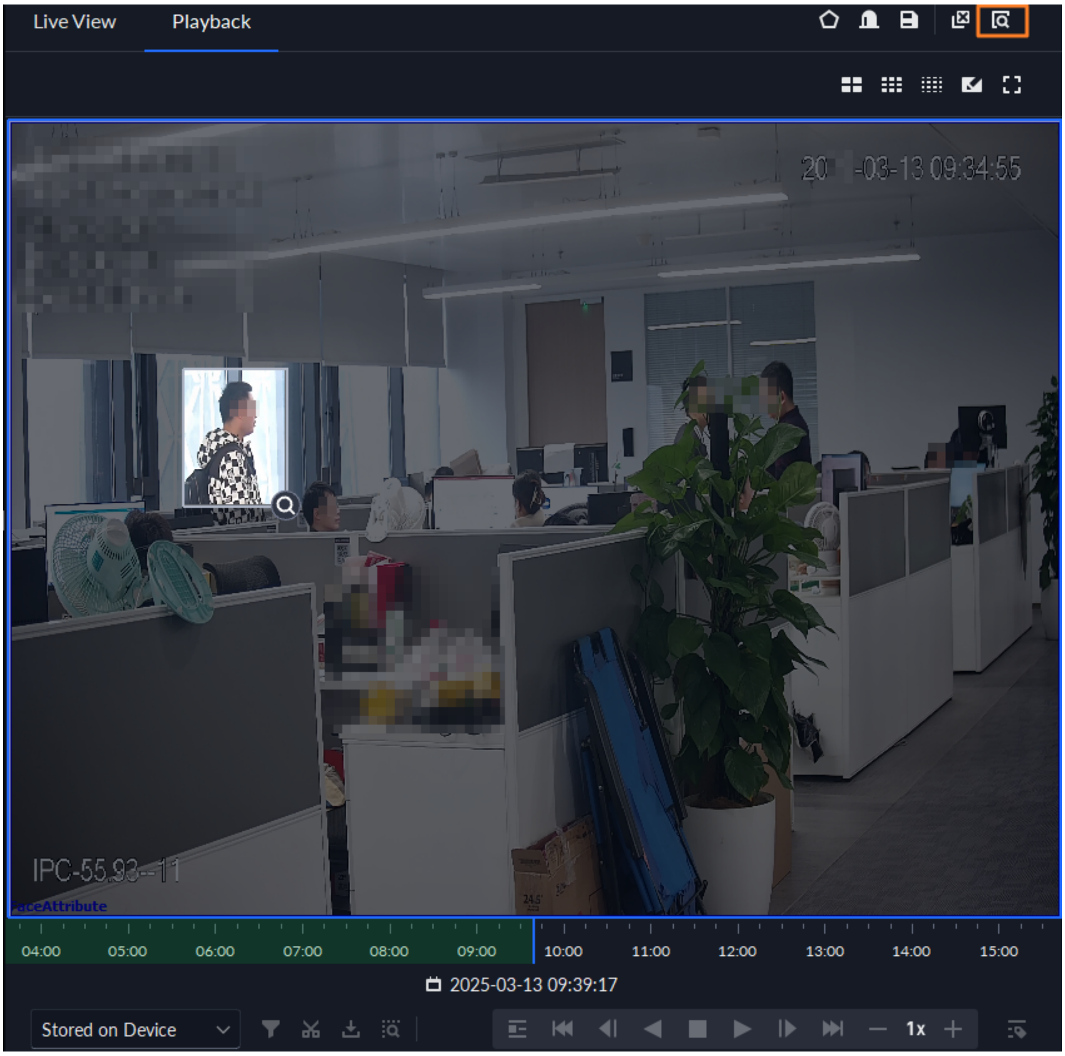
Dates with blue dot means there are recordings.

Step 4 Click on the bottom of the page.

Step 5 Drag on the video to select a target.

Right-click to exit this function.

Figure 7-30 Select a target



Step 6 (Optional) Adjust the area of selection.

- Place the mouse on the selected area, and then drag to move the area to any location.
- Place the mouse to the upper-left, upper-right and lower-left corner of the selected area, and then drag to resize the area.

Step 7 Click and select a type for the target, and then you are directed to DeepXplore to search for it. For details, see "7.3 DeepXplore".

7.1.3.6 Clipping Videos

Download a video by selecting a period on the timeline.

Procedure

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

Step 2 Click the **Playback** tab.

Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

Step 4 Select the storage path of videos from Stored on Device, and then click to select the date.

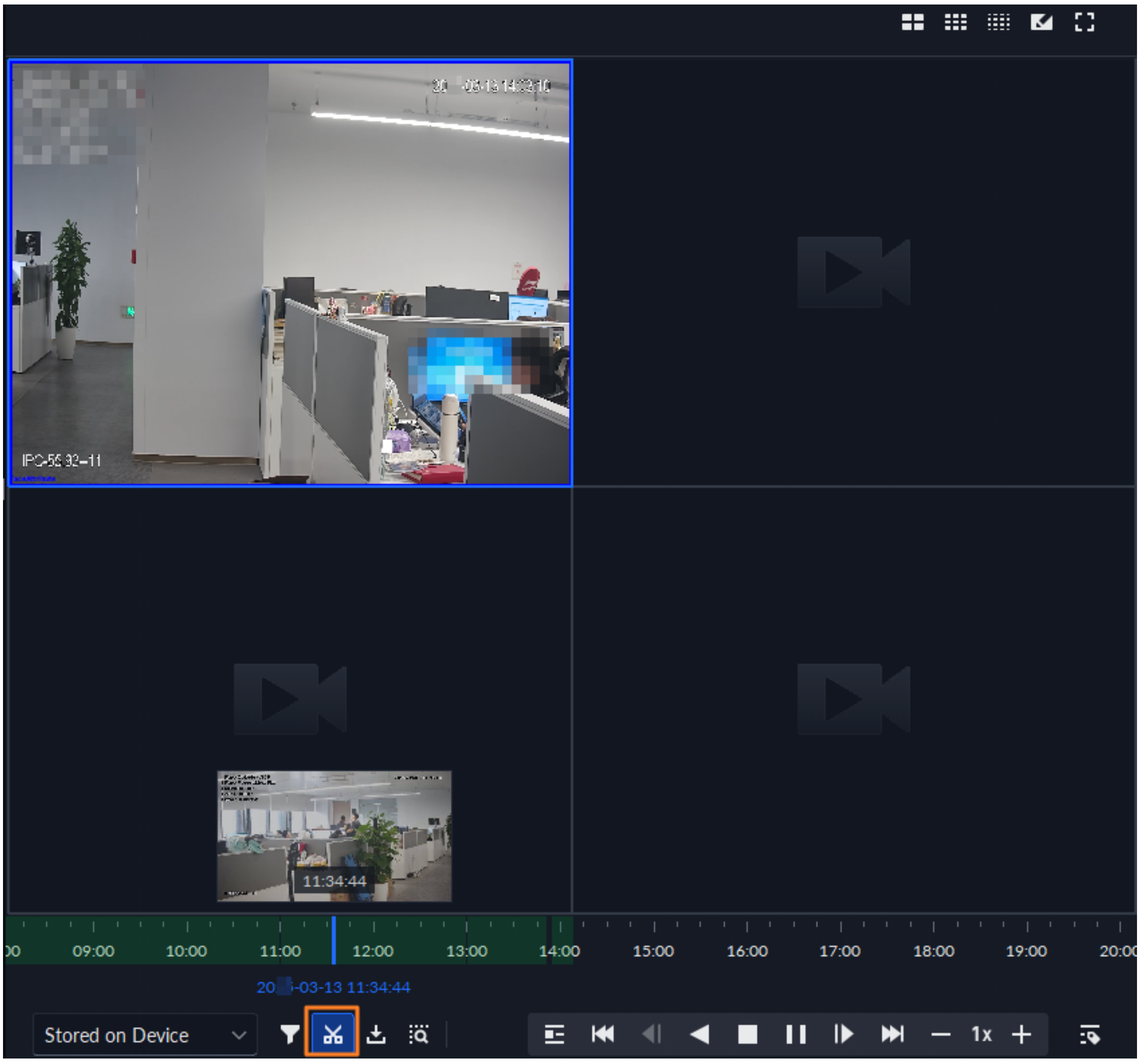
The search results are displayed.

Dates with blue dot means there are videos.

Step 5 Select a date with video recordings, and then click .

Step 6 On the timeline, click the point with green shade to start clipping, drag your mouse, and then click again to stop.

Figure 7-31 Select a period



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

You need to verify your password by default before downloading. You can configure whether to verify the password. For details, see "9.2.1 Configuring Security Parameters".

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

The video will be downloaded to the default path configured in the local settings. For details, see "10.4.5 Configure File Storage Settings".

Table 7-10 Parameter description

Parameter	Description
Start Time	The start and end time represents the length of video you selected. You can adjust it more specifically here.
End Time	
Transcode	The format is .dav by default. Other formats include .avi, .mp4, and .asf.
File Format	
Storage Path	Configure the storage path for the recordings. Click to edit the name of the recording file and select the local storage path.
Privacy Masking	If disabled, faces in the video will not be blurred. Make sure that the device supports the privacy masking function, and the function on the device is enabled.

7.1.3.7 Smart Search

With the smart search function, you can select a zone of interest on the video image to view motion records within this section. The relevant camera is required to support Smart Search; otherwise the search result will be empty.

Procedure

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

Step 2 Click the **Playback** tab.

Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

Step 4 Select the storage path of recorded video from Stored on Device or, and then click to select the date.

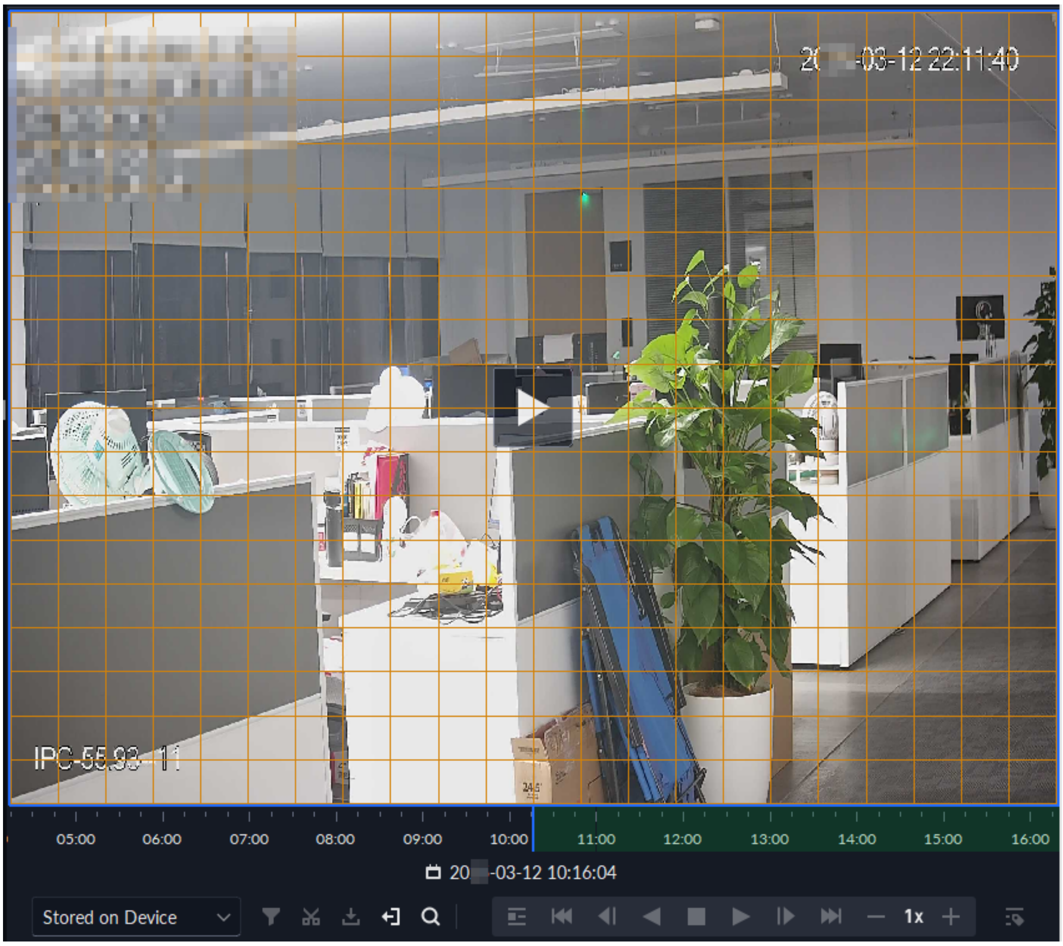
The search results are displayed.

Dates with blue dot means there are video recordings.

Step 5 Select a window that has videos, click , and then select a type.

The smart search page is displayed, with 22 × 18 squares in the window.

Figure 7-32 Smart search



Step 6 Click the squares and select detection areas.

- Select a detection area: Point to image, click and drag to select a square.
- For the selected area, click again or select square to cancel it.

Step 7 Click to start smart search analysis.

- If there are search results, the time progress bar will become purple and display dynamic frame.
- It will prompt that the device does not support smart search if the device you selected does not support the function.

Click to select the detection area again.

Step 8 Click button on the image.

- : The system only plays back the retrieved results, which are indicated by purple frames on the timeline bar.
- : Plays back the whole video.

Step 9 Click to exit smart search.

7.1.4 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 "6.2 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 7-11 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. 
Hide device name	Select **Display Settings** > **Hide Device Name**, and then only displays the icons of devices or channels.
View device details	Click a device on the map, and then click to view device name and organization; Click the icon again to hide the name and organization.
View live video	● View live videos in batches: Click **Rectangle**, select devices on the map, and then click . ● View the live video of a device: Click a device on the map, and then click . PTZ control and presets are supported when viewing the live video. Make sure that the device supports the PTZ function.

Function	Description
Playback	● View videos in batches: Click **Rectangle**, select devices on the map, select the time and storage type (device recordings), and then click . ● View the video of a device: Click a device on the map, select the time and storage type (device recordings), 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.
Cancel alarms	Click a device on the map, and then select . The alarm will also be automatically canceled after 30 seconds.
Monitor a radar	● The alarm area and detection area are displayed on the map by default. If a target is detected, its real-time location will be displayed in these areas. ● Click a radar channel, you can view its information and use the following functions: ◇ : View the raster map on the radar. You can use this function to check if the maps on the radar and the platform are consistent. ◇ : View the real-time videos of the linked PTZ cameras. ◇ : Search for and view recordings of the linked PTZ cameras. ◇ : View the real-time videos of the channels bound to the radar. You can use this function to monitor the area around the radar. ◇ : If the alarm area and detection area of the radar are keeping you from operating other channels, you can click this icon to hide these areas.
Show devices	Click **Show Device**, and then select the types of devices and channels that you want to display on the map. You can click an alarm output channel to control whether it will output alarm signals.
Clear	To clear all markings on the map, click **Clear**.
Add marks	Select **Box** > **Add Mark**, and then mark information on the map.
Reset	Select **Box** > **Reset** to restore the map to its initial position and zoom level.
Sub maps	Click to view the information of the sub map.

Function	Description
	Double-click , and then the platform will go to the sub map, where you can view the resources on it.

7.1.5 Video Wall

A video wall, which consists of multiple video screens, is used for displaying videos on the wall, instead of small PC displays.

Complete video wall settings before you can view videos on the wall.

7.1.5.1 Configuring Video Wall

7.1.5.1.1 Page Description

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

Figure 7-33 Video wall

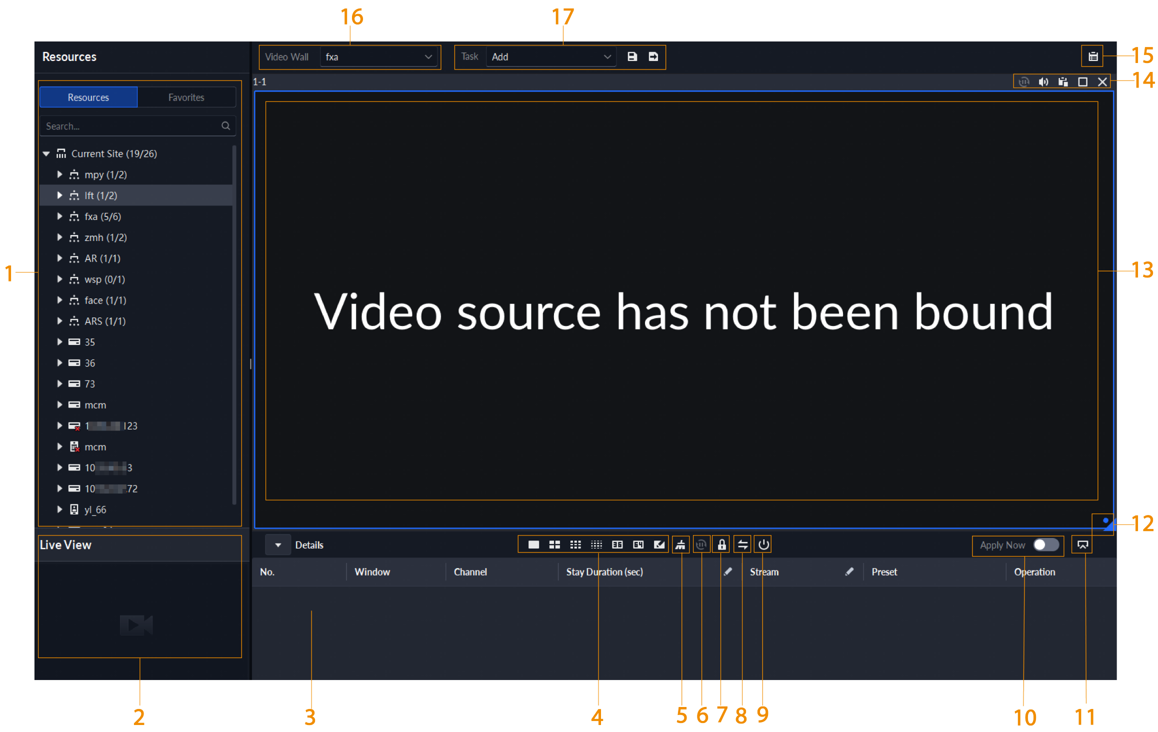


Table 7-12 Page description

No.	Function	Description
1	Device tree	If you have selected **Device and Channel** in **Local Settings** > **General**, the device tree will display all devices and their channels. Otherwise, it will only display all channels. Click to view channels that you have saved to favorites. You can enter keywords in to search for the channels you want.
2	Live view	View live videos from channels.
3	Detailed information	View the channel information in a screen of the video wall. ● Click and view the live video of the channel in **Live View** on the lower-left corner. This can be helpful when you need to make sure whether it is the channel you want. ● Click to adjust the order of channels. ● Click to delete the channel from the screen. ● Click **Stay Duration (sec)** or to define for how long the live video of the channel will be displayed during each tour. ● Click **Stream** or to change the video stream of the channel.
4	Window split	Select how you want the window to split.
5	Clear screen	Clear all the screens.
6	Stopping or starting all tours	Stop or start all tours.
7	Lock window	If multiple screens in a video wall are configured to be a combined screen, then you can perform video roaming on the window that has been locked.
8	Display mode	Displays the real-time video, or a snapshot of the real-time video every 10 minutes of the bound channel in the screen. If nothing happens after operation, you can just click another screen, then click the screen you want, and then it should work properly.
9	Turning on or off screens	Turn on or off the screens configured for the currently selected video wall.
10	Decoding to wall immediately after configuration	When a task has been configured, the platform will immediately decode channels to the video wall.
11	Decoding to wall	Manually decode channels to the video wall.
12	Video wall layout	Click to view the layout of the current video wall.
13	Video wall display area	The display area for video walls.

No.	Function	Description
14	Screen operations	Includes stopping tour for the screen, muting, pasting, maximizing or restoring the screen, and closing the screen.
15	Video wall plan	Configure a timed or tour plan for the video wall.
16	Video wall selection	Select the video wall you want to configure.
17	Display task management	Add, save, and delete tasks.

7.1.5.1.2 Preparations

To display video on the wall, make sure that:

- Cameras, decoders and video wall are well deployed. For details, see the corresponding user manuals.
- Basic configurations of the platform have been finished. For details, see "5 Basic Configurations". During configuration, make sure that:
  - ◇ When adding a camera, select **Encoder** from **Device Category**.
  - ◇ When adding a decoder, select **Video Wall Control** from **Device Category**.

7.1.5.1.3 Adding Video Wall

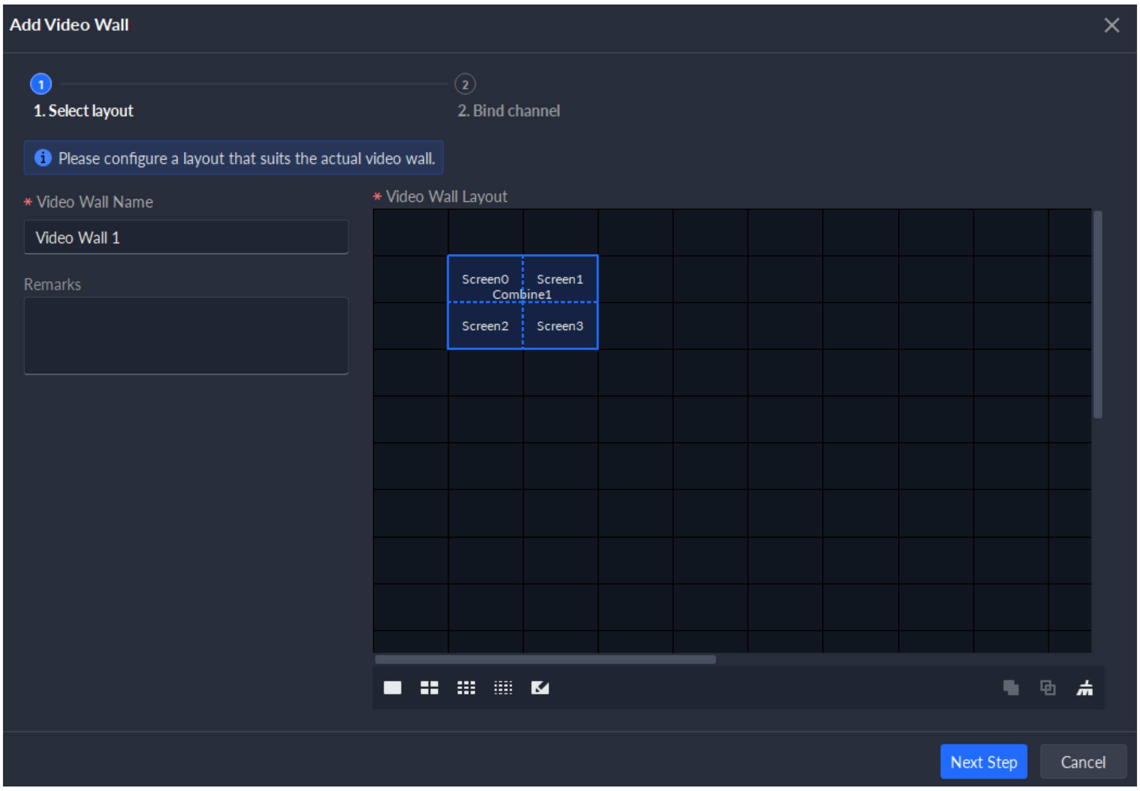
Add a video wall layout on the platform.

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

Step 2 From the **Video Wall** drop-down list, select **Add Video Wall**.

Step 3 Enter video wall name, and then select a window splicing mode.

Figure 7-34 Add a video wall



- The video wall name cannot consist of special characters including < > % & = " ' and /.
- Select a splicing mode from among 1 × 1, 2 × 2, 3 × 3, 4 × 4 or set a custom mode by clicking .
- A multi-screen splicing mode is a combined screen by default. You can perform video roaming on it. For example, with a 2×2 combined screen, if you close 3 of them, the other one will be spread out on the combined screen. To cancel combination, click the combined screen, and then click .
- To create a combined screen, press and hold Ctrl, select multiple screens, and then click .
- To clear the created screen, click .

Step 4 Click **Next Step**.

Step 5 Select the encoders which need to be bound in the device tree, and drag it to the corresponding screen.

- You can set whether to show ID in the screen, means that the screen ID is disabled; click the icon and it becomes , which means that screen ID is enabled.
- Each screen in a combined screen must be bound with a decoding channel.

Step 6 Click **Finish**.

7.1.5.1.4 Configuring Video Wall Display Tasks

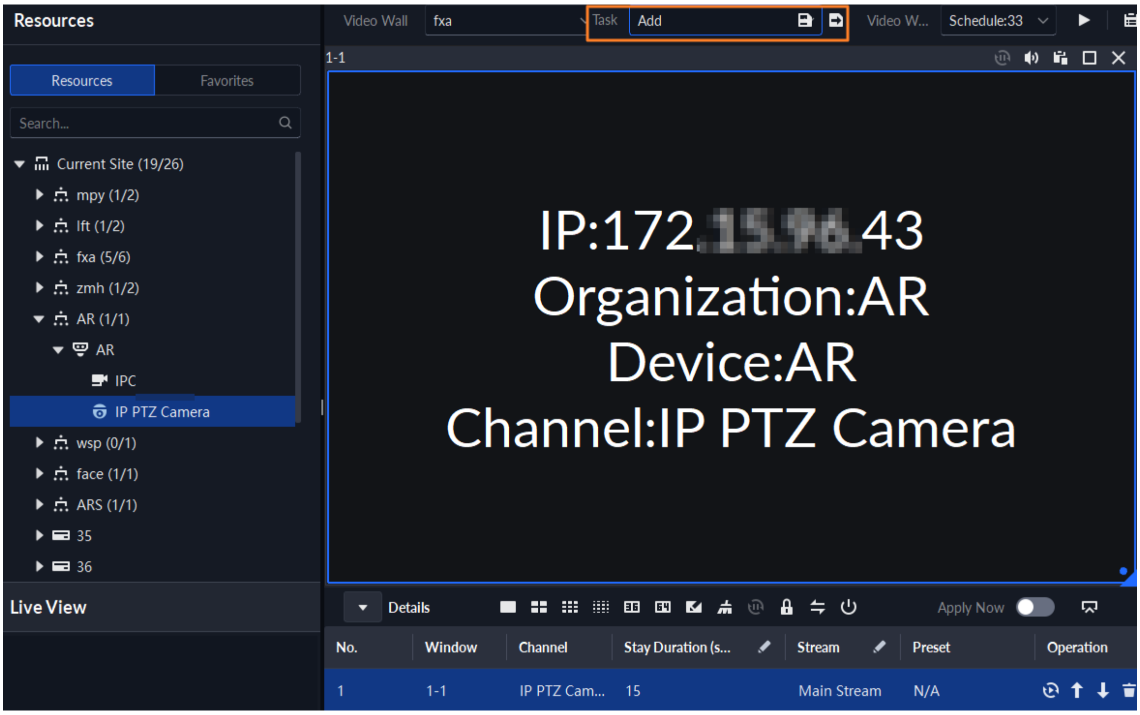
Displays videos on the wall manually or in accordance with the pre-defined configuration.

Procedure

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

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

Figure 7-35 Add a video wall task



Step 3 From the device tree, select a camera, and then drag it to a screen, or select a window, drag the camera to the **Details** section.

If you do not close video wall display in advance, this action will delete the bound camera and play the selected camera on the wall.

Step 4 Click .

If you have selected an existing task in the **Task** drop-down list, after dragging the video channel to the window, click to save it as a new task, which will be played on the wall immediately.

Step 5 Name the task, and then click **OK**.

- During video wall display of a task, if you have rebound the video channel, click to start video wall display manual.
- During video wall display, click or to stop or start tour display.

Step 6 Click to start video wall display.

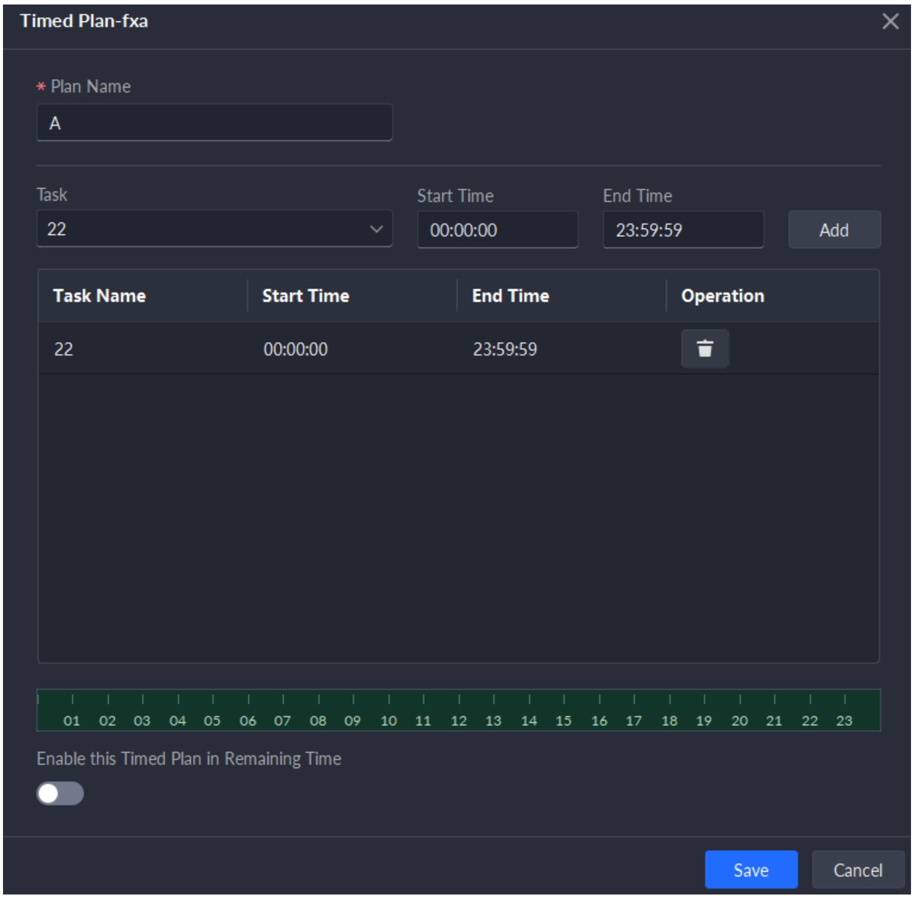
7.1.5.1.5 Configuring Timed Plans

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

Step 2 Click on the upper-right corner.

Step 3 Hover over , and then select **Timed**.

Figure 7-36 Set timed plan



Step 4 Enter the plan name.

Step 5 Select a video task, set start time and end time, and then click **Add**.

Repeat this step to add more tasks. The start time and the end time of tasks cannot be repeated.

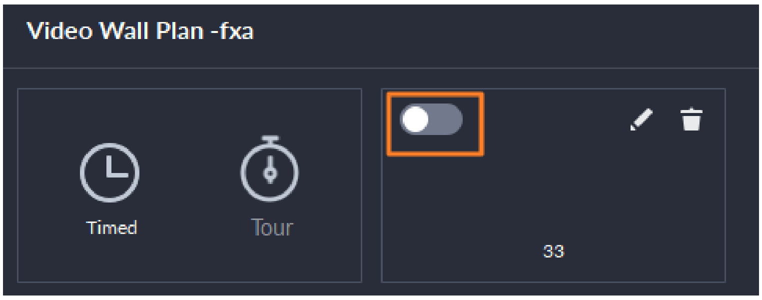
Select the **Enable This Timed Plan in Remaining Time** check box, and then set the task. The video wall displays the selected task during the remaining period.

Step 6 Click **Save**.

Step 7 Click to start the plan.

You cannot display multiple plans on the wall at the same time. When a plan is enabled, the previous plan on the wall is automatically terminated.

Figure 7-37 Enable timed plan



7.1.5.1.6 Configuring Tour Plans

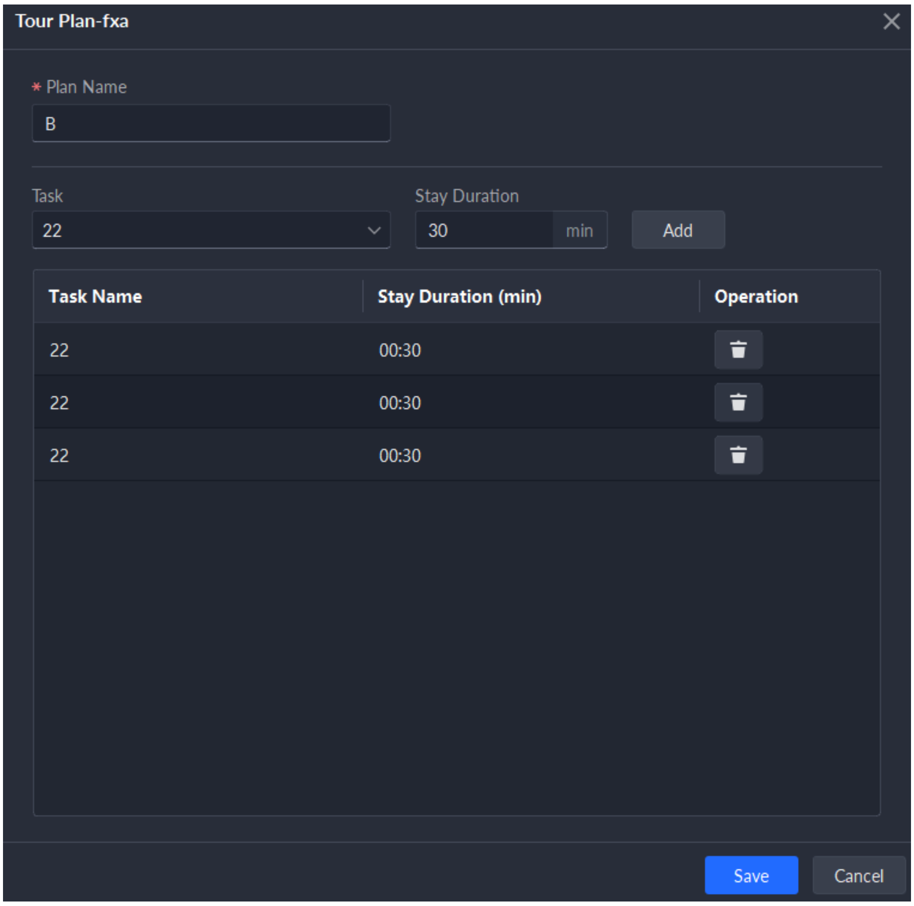
After setting video wall tasks, you can configure the sequence and interval of tasks so that they can automatically play in turn on the wall.

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

Step 2 Click  on the upper-right corner.

Step 3 Hover over , and then select **Tour**.

Figure 7-38 Tour plan



Step 4 Enter task name, select a video task and then set stay time. Click **Add**.

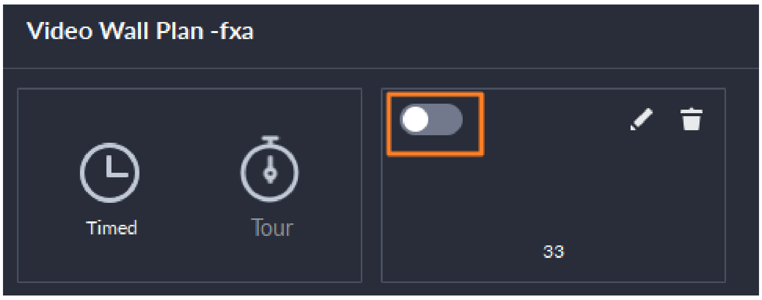
Repeat this step to add more tasks.

Step 5 Click **Save**.

Step 6 Click to start the tour plan.

You cannot display multiple plans on the wall at the same time. When a plan is enabled, the previous plan on the wall is automatically terminated.

Figure 7-39 Enable tour plan



7.1.5.2 Video Wall Applications

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

7.1.5.2.1 Instant Display

Drag a camera to the video wall screen for instant display on the wall.

The video wall display task is configured. For details, see "7.1.5.1.4 Configuring Video Wall Display Tasks".

Procedure

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

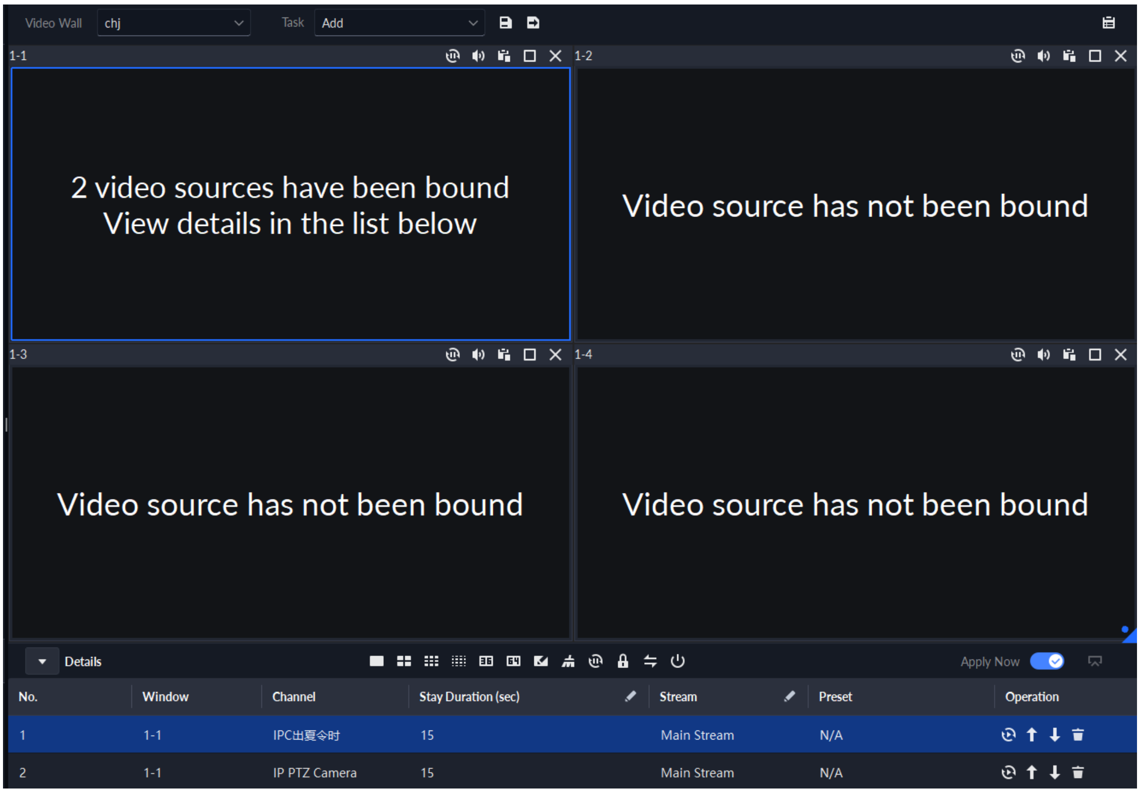
Step 2 In the **Video Wall** drop-down list, select a video wall.

Step 3 Click to start video wall display.

Step 4 Drag a camera from the device tree to a screen, or select a window and drag the camera to the **Details** section.

- A window can be bound to multiple video channels.
- The binding mode, which includes **Tour**, **Tile**, and **Ask Every Time**, can be set in **Local Settings** > **Video Wall**. For details, see "10.4.3 Configuring Video Wall Settings".
- For a fisheye camera, right-click it to select the installation mode for fisheye dewarping.

Figure 7-40 Bind video channel



Step 5 Select a screen, and then click **Details** to view detailed information about the screen and channel, including stream type, preset and display sequence.

- Click to view live video of the current channel on the lower left.
- Click to adjust sequence.
- Click to delete the video channel on the current window.

7.1.5.2.2 Video Wall Task Display

Displays a pre-defined task on video wall.

Step 1 Log in to the DSS Client, and on the **Home** page, select **Tools** > **Video Wall**.

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

Step 3 Operations available.

- After changing the video channel that is being displayed, click at the lower-right corner before you can see the effect on video wall.
- Click / to pause or stop.
- Select a screen, and then click **Details** to view detailed information about the screen and channel, including stream type, preset and display sequence.

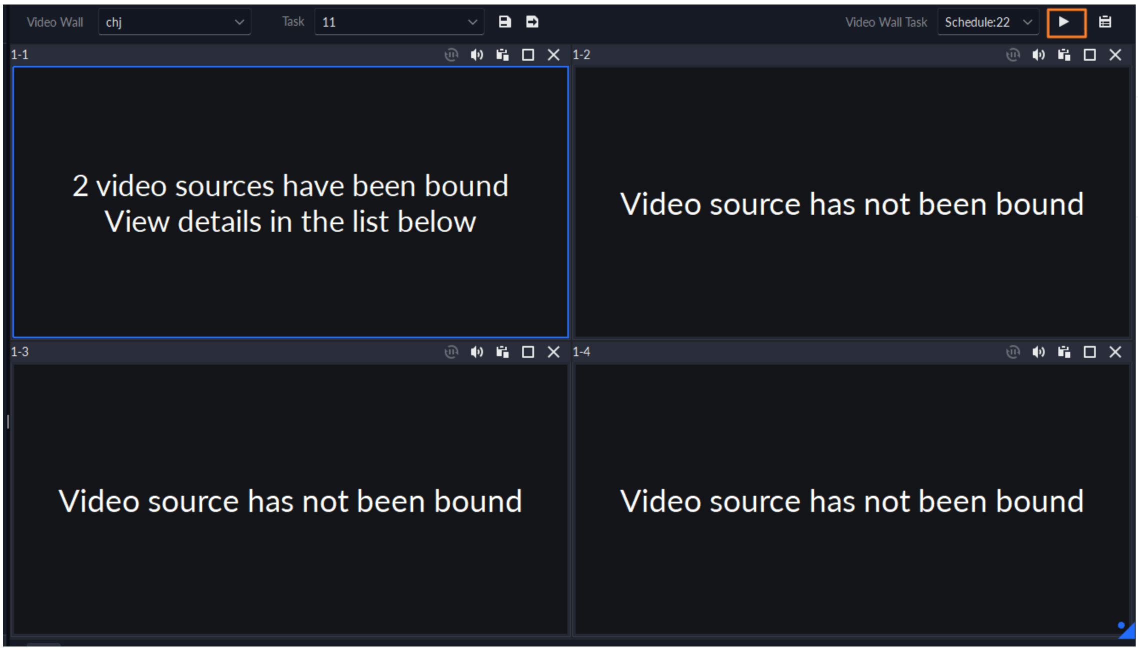
7.1.5.2.3 Video Wall Plan Display

Display a pre-defined plan on video wall.

Make sure that there are pre-defined plans.

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

Figure 7-41 Display video wall plan



7.2 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 "6.1 Configuring Events".

7.2.1 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**.

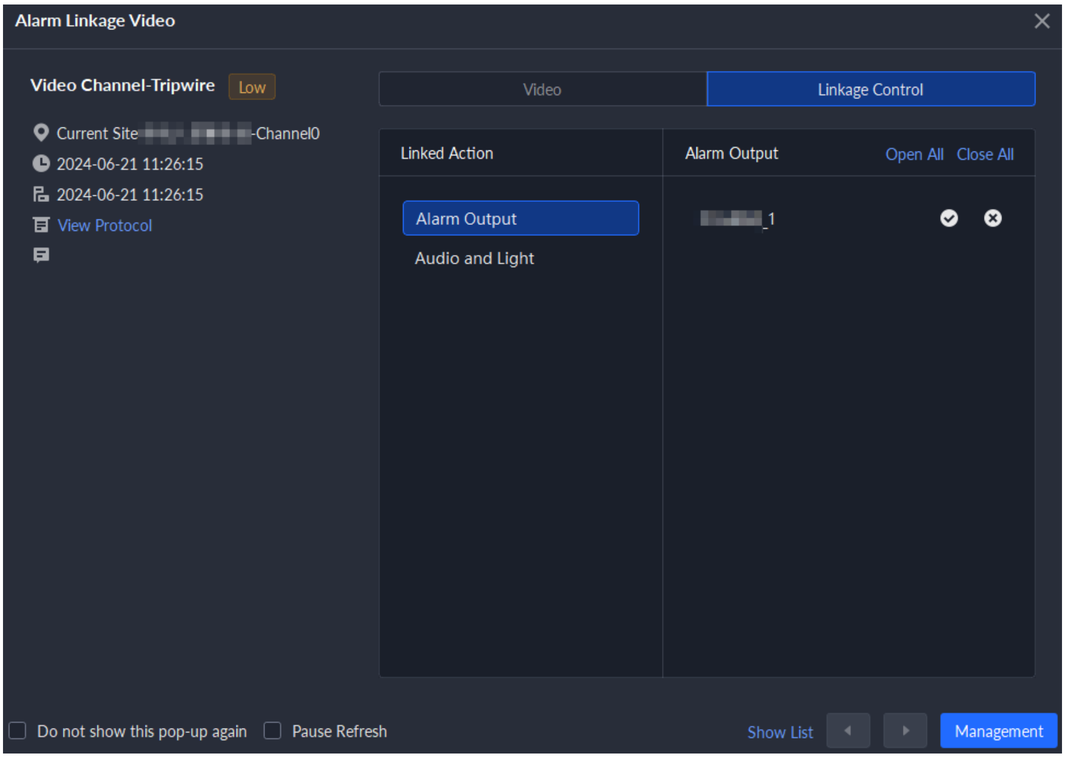
The alarm list is refreshed in real time. To stop refreshing, click **Pause Refresh** . To continue receiving alarms, click **Start Refresh**.

Alarm pops up when **Open Alarm Linkage Video** is set to **As Pop-up** from **Management** > **Local Settings** > **Alarm**. You can click the **Video**, **Linkage Control** or **Map** tab to view the video, 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.

  You can adjust the volume of audio in **Audio and Light**, or click **Open All** or **Close All** to open or close the alarm.

Figure 7-42 Alarm pop-up



Step 3 Click to claim an alarm.

After an alarm has been claimed, the username of your account will be displayed under the **Processed by** column.

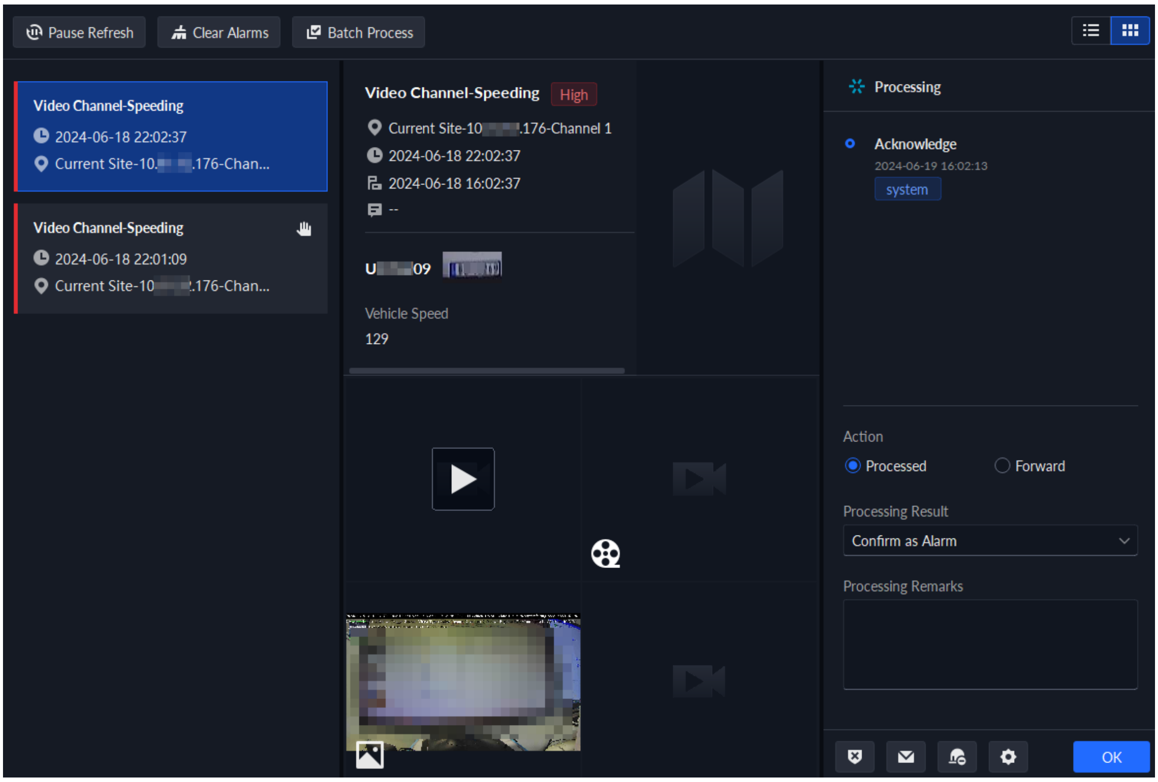
Step 4 Process alarms.

You can use the up and down arrow keys on the keyboard to quickly select other alarms.

1. Click or double-click the alarm to view the claimed alarm.

   Alarms related to vehicles also display vehicle information such as plate number, speed, and more.

Figure 7-43 Alarm details



2. The middle area displays the time when the alarm was triggered, name and location of the alarm source, alarm type, and the live video images of linked channels, alarm videos, and alarm snapshots.

   Double-click a window to view them in larger size. Click to go back.
3. On the right side, select how to process the alarm, enter some comments, and then click **OK**.

   Forward allows you to forward the alarm to another user who will process it.
4. (Optional) Click to disarm the alarm. You can disarm for a period, or disarm until the defined time.

   After disarming, all users will not receive this alarm within the defined time; and after the defined time, if the alarm is not eliminated, it will continue to alarm.
5. (Optional) Click to send the alarm information to other users as an email. Events that are processed or forwarded can also be sent as emails.
6. Click and configure the parameters related to the processing comments, and then click **OK**.
   - **Require Processing Remarks to be Entered** : After enabled, users must enter some content in the processing comments to successfully process alarms.
   - **Pre-processing Remarks** : Configure the predefined comments for each processing status. The content will be automatically filled in when users select different status for alarms.

Related Operations

- The platform also supports processing alarms in batches. Click **Batch Process**, select multiple alarms, and then you can process them in batches.
- When viewing the recorded videos, you can select a target manually, and then search for it in DeepXplore.

7.2.2 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 "7.2.1 Real-Time Event".

You can use the up and down arrow keys on the keyboard to quickly select other alarms.

Related Operations

When viewing the recorded videos and snapshots, you can select a target manually, and then search for it in DeepXplore.

7.2.3 Alarm Controller

You can monitor and manage alarm controllers.

Prerequisites

Alarm controllers are added to the platform. For details, see "5.1.2 Managing Device".

Background Information

- Arm and disarm
  - Home arm: An arming mode when a user is within the zone of the alarm system. In this mode, zones around the system, such as outdoor perimeter detectors, balcony curtain detectors, are armed, while zones inside the system, typically indoor infrared detectors, are bypassed by the system. People can move in this area without triggering alarms. If there are internal zones within a subsystem, they will be disarmed.
  - Away arm: An arming mode when all users have left the zones of the alarm system. In this mode, all zones are armed.
  - Disarm: Cancel arming.
- Bypass

  When detectors connected to the alarm controller malfunction or there is movement within specific zones, the normal arming operations within the system will be affected. In this case, the system allows users to bypass these zones.
  - Unbypass: Restores bypassed zones to the enabled status.
  - Bypass: The zone is temporarily disabled during the arm, and it automatically returns to the enabled status when the system is disarmed.
  - Isolate: The zone is permanently disabled. When the system is disarmed and then armed again, the isolated zone remains disabled.

Procedure

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

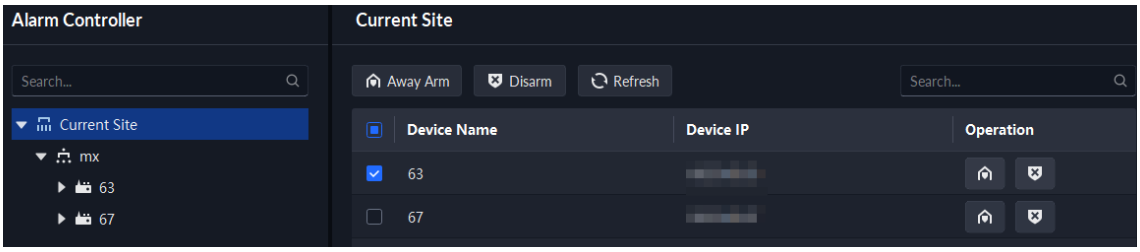
Step 2 Click **Alarm Controller**.

Step 3 In the device tree, click an organization.

All alarm controllers under this organization will be displayed on the right. You can select one or more alarm controllers, and then click (**Away Arm**) or (**Disarm**) to arm or disarm the alarm controllers you selected.

If arming failed, you can click **Force Arm** on the prompt window to arm again.

Figure 7-44 Alarm controller organization

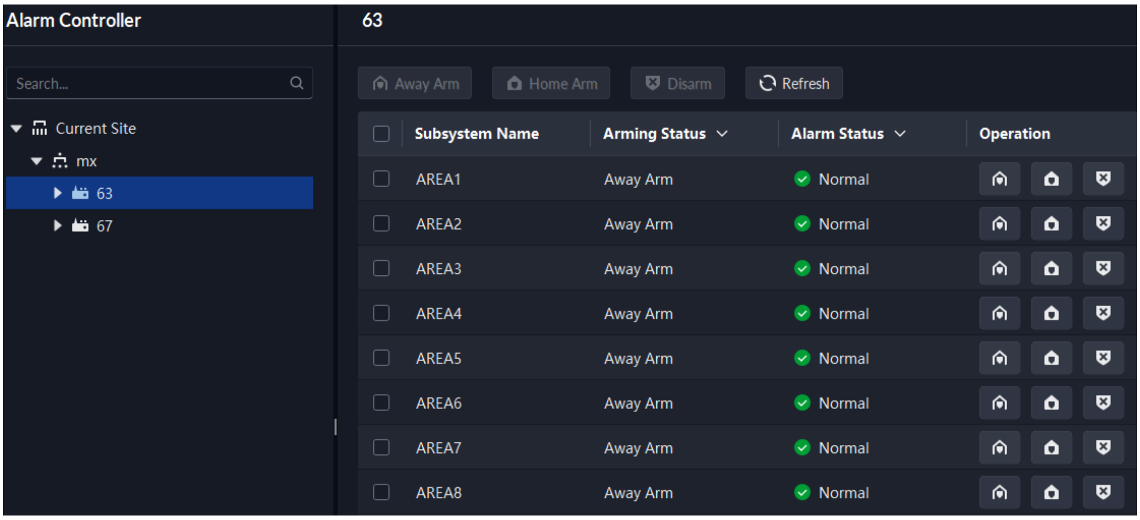


Step 4 In the device tree, click an alarm controller.

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 7-45 Subsystems



Step 5 Arm or disarm subsystems.

- 

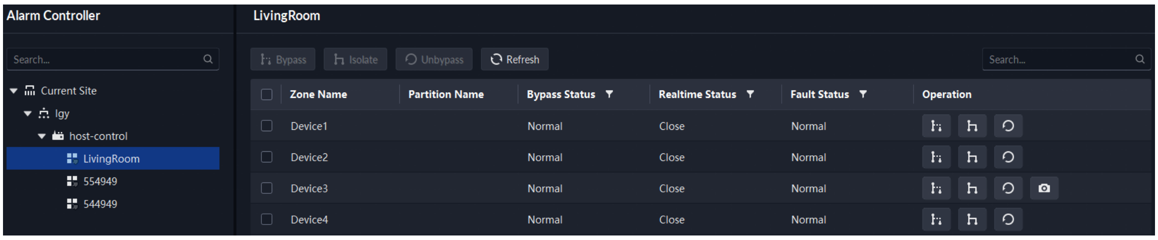
: Operate on multiple subsystems.
- : Operate on one system.

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

Step 6 In the device tree, click a subsystem of the alarm controller.

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

Figure 7-46 Zone



Step 7 Bypass, isolate, or unbypass zones.

- Bypass Isolate Unbypass: Operate on multiple zones.
- : Operate on one zone.
- : Operate on one zone.

◇ The snap function ( ) is available only when the alarm controller is online, and PIR camera is connected to the corresponding zone.

◇ The snapshot can be downloaded to local in .jpg format.

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

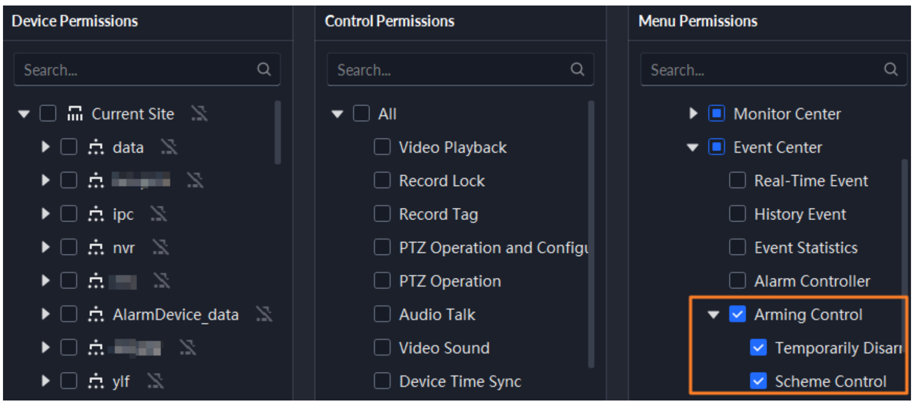
7.2.4 Arming Control

You can edit or cancel temporary disarming on the platform to avoid unnecessary alarms, and enable or disable event schemes to with one click.

Prerequisites

The **Arming Control** menu permission is required. The permission can be configured from > **User** > **Role Management**.

Figure 7-47 Configure arming control permission



7.2.4.1 Temporary Disarming

You can edit or cancel temporary disarming to avoid unnecessary alarms. For example, if an industrial park holds a celebration activity, it can temporarily disarm the park or some zones as needed.

Prerequisites

You need to configure temporary disarming on the **Real-Time Event** or **Event History** page.

Procedure

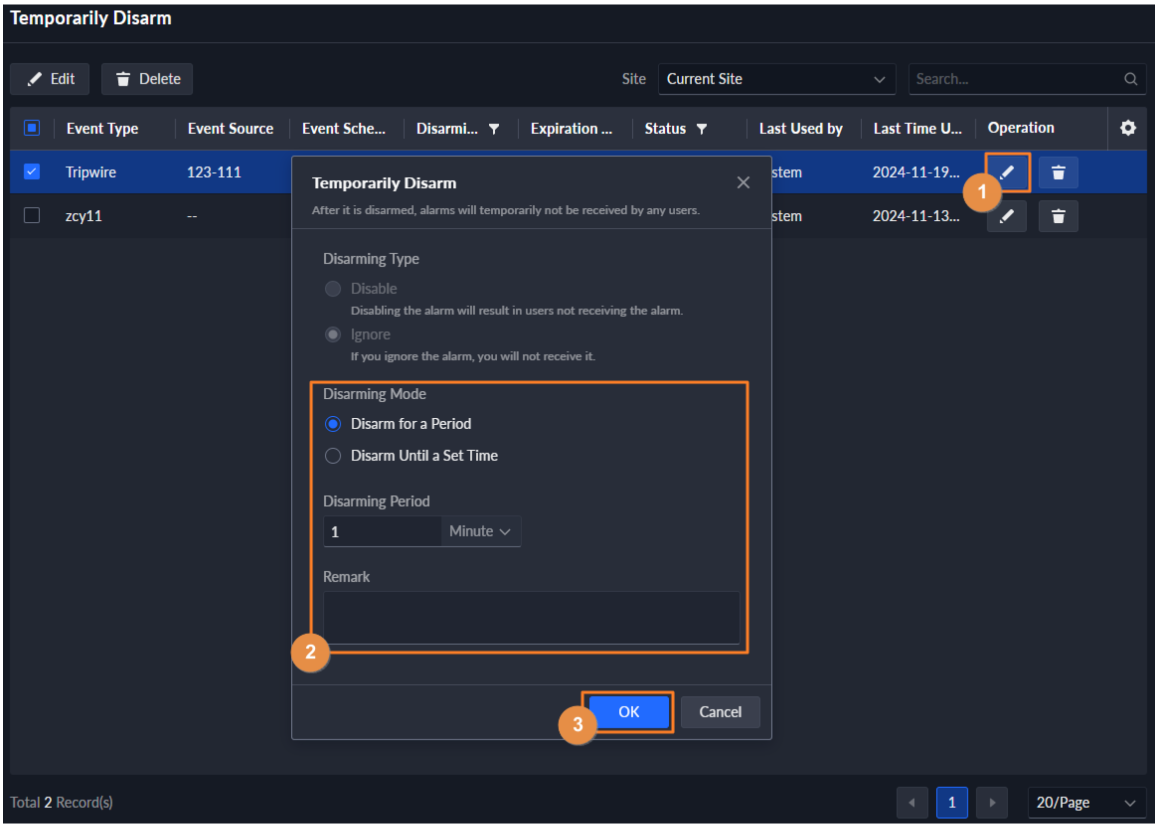
Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Event Center**.

Step 2 Select **Arming Control** > **Temporarily Disarm**, and then click corresponding to a disarming record to edit the disarming period.

> Select several disarming records, and then click **Edit** to edit the disarming periods in batches.

You can set disarming for a period, or disarming until the defined time. After disarming, all users will not receive this alarm within the defined time; and after the defined time, if the alarm is not eliminated, it will continue to alarm.

Figure 7-48 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.

7.2.4.2 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.

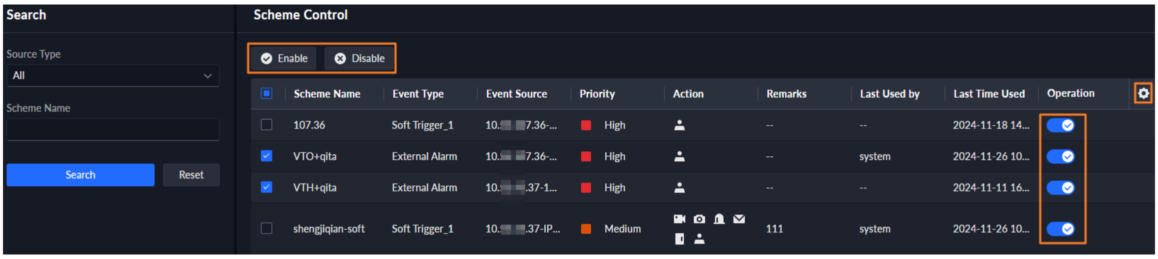
Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Event Center**.

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 7-49 Scheme control



7.3 DeepXplore

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

7.3.1 Searching for People

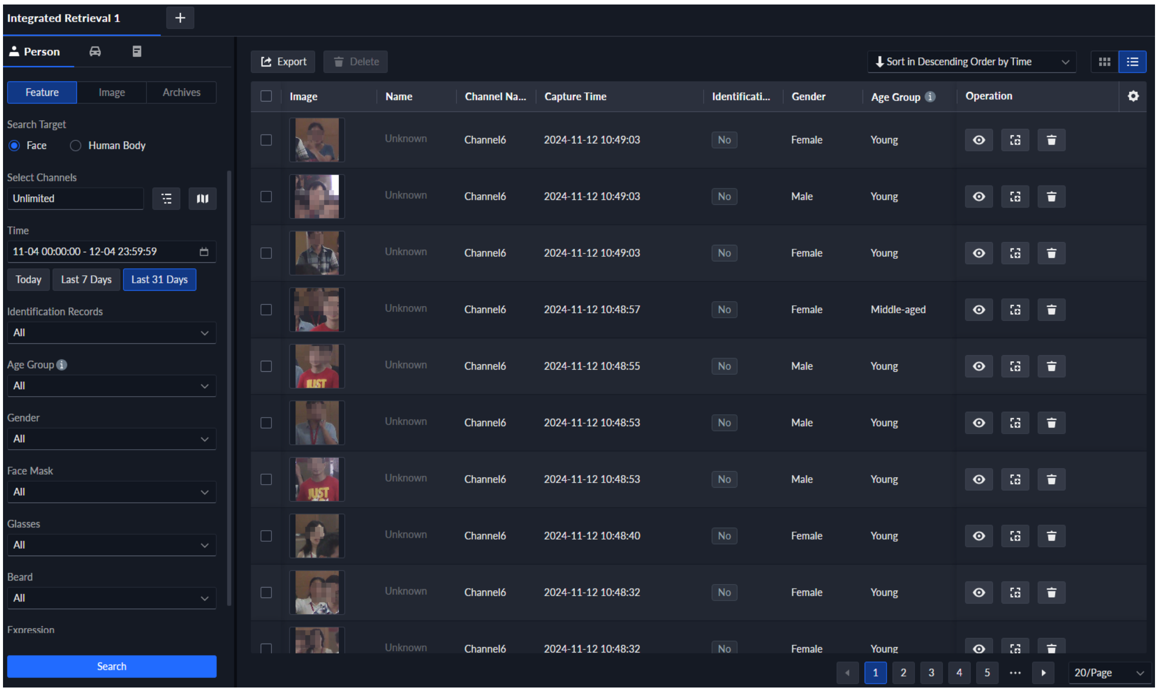
Based on the defined search conditions, you can view capture records of faces, bodies and other information.

Procedure

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

Step 2 Click **Integrated Retrieval**, and then click .

Figure 7-50 Person search



- Search type
  - ◇ **Feature** : Search for records by the defined features, including age, gender, face mask, glasses, beard, expression, and more.

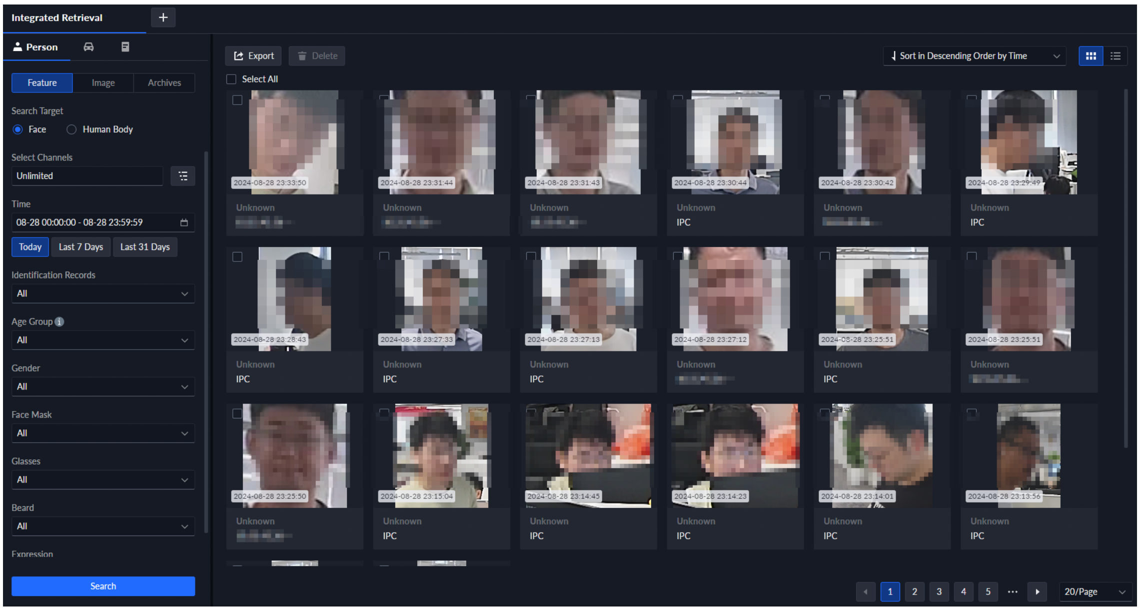
    When selecting whether to search for identification records, the difference is that, besides the age and gender, identification records will also show the similarity between the captured face and those in the arming lists.
  - ◇ **Image** : The platform compares the image you upload to capture records on 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.

    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 7-51 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).
- When viewing recorded videos and snapshots, you can select a target manually, and then search for it in DeepXplore.
- If the channel is bound to other video channels, the recorded video from the bound video channels will play automatically.
- Click to add the person to a face arming group. After you send the group to devices and configure an event, devices can trigger alarms when the face is recognized.
- Click to delete it one by one.

  You cannot delete the records of searching by image on devices.
- For the archives searching, double click the searching results or click to view the details. You can see the face capture, vehicle capture, access records and other information of the corresponding person.

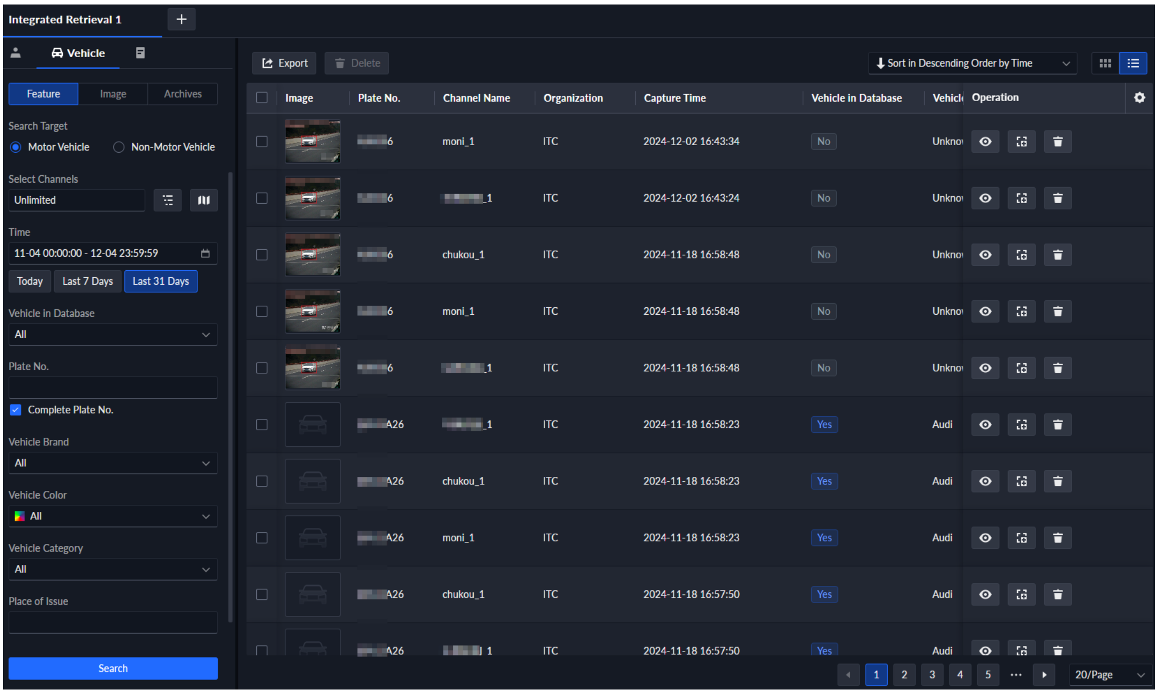
7.3.2 Searching for Vehicles

Procedure

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

Step 2 Click **Integrated Retrieval**, and then click .

Figure 7-52 Vehicle search



- Search type
  - ◇ **Feature** : Search for records by the defined attributes, including vehicle in database, plate number, vehicle brand, vehicle color, vehicle category, place of issue, and more.
  - ◇ **Image** : The platform compares the image you upload to 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).

- 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.
- If a license plate is recognized, click to add the vehicle to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the vehicle is recognized.
- Click to delete it one by one.

  The records of searching by image on devices, access records cannot be deleted.
- For vehicle archives, double-click a record to view recognition records of a license plate.

7.3.3 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**.

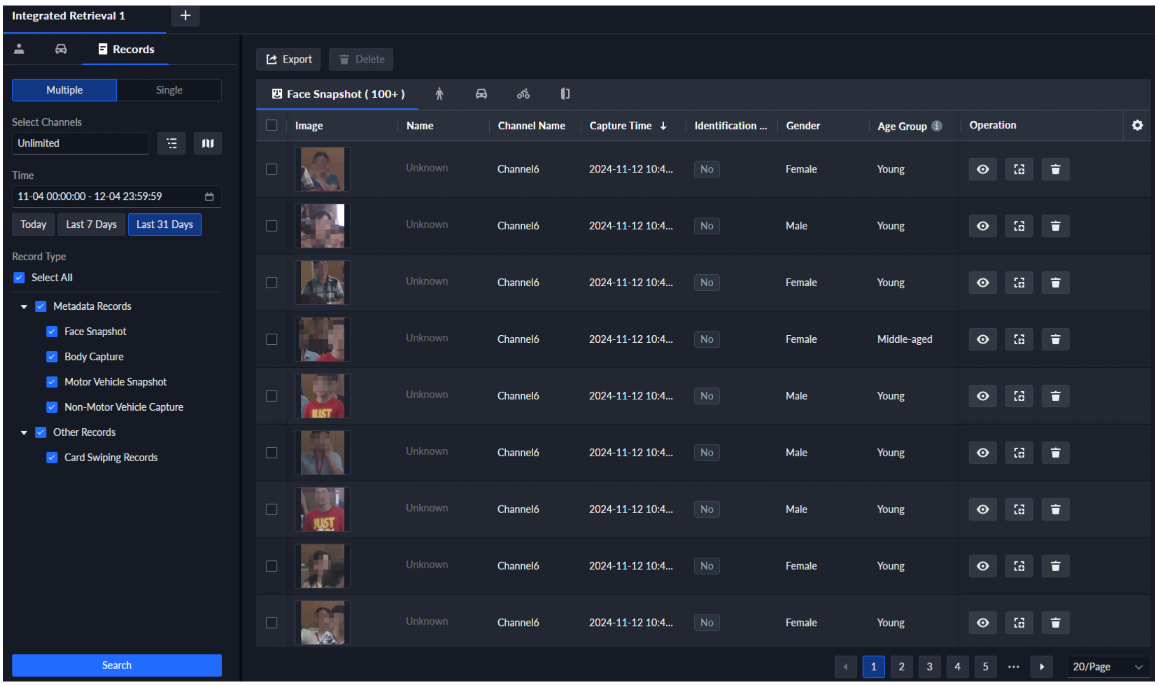
Step 2 Click **Integrated Retrieval**.

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 7-53 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.

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

- View details on records

  Select a record, and then click to view its details on the right, including snapshots, recorded videos (can be downloaded to your computer), and targets that can be further searched for (manually select a target).
- When viewing recorded videos and snapshots, you can select a target manually, and then search for it in DeepXplore.
- If the channel is bound to other video channels, the recorded video from the bound video channels will play automatically.
- 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.
- If a license plate is recognized, click to add the vehicle to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the vehicle is recognized.
- Click to delete it one by one.

  The access records cannot be deleted.

7.4 Access Management

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

7.4.1 Access Control

7.4.1.1 Viewing Access Points

Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Access Control** > **Access Control Panel**.

This page displays by default all the access points in the root zone and all its sub zones in card view.

Change the display mode

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

- In card view, **Event Type** supports **Exception**, **Normal** and **Alarm**.
- On the map, when an alarm occurs, the device icon on the map will be displayed in red.

View certain access points

On the top on the page, select a zone or access point type to display only door or lift control channels, or the access points in a zone and its sub zones.

View access point information

In card view, double-click an access point to view its information, including basic information, live videos from bound channels, and events. For a door channel, you can also lock or unlock the door and make a call to it.

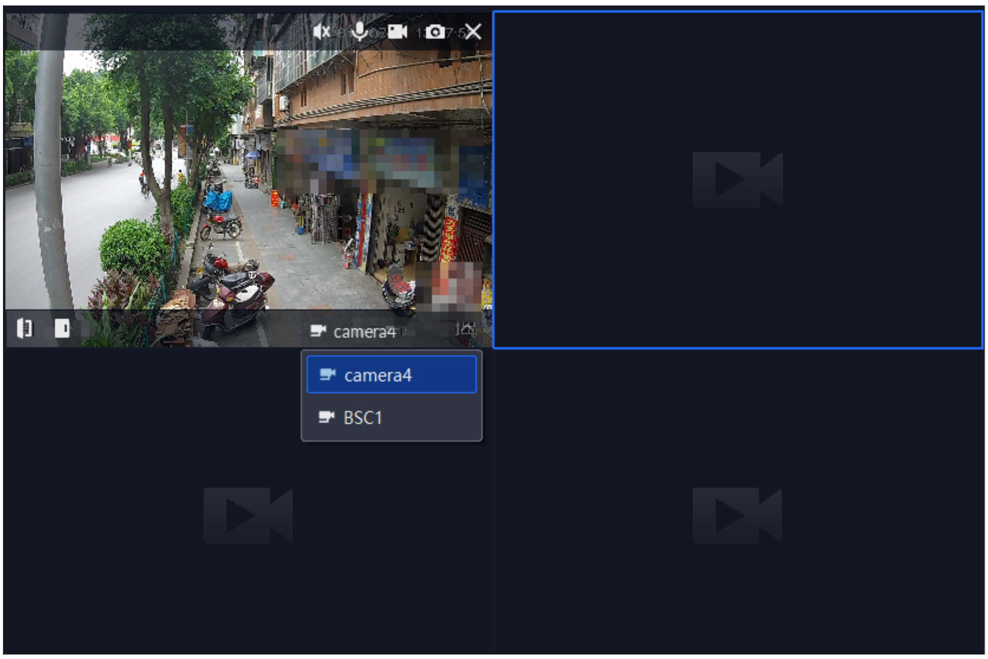
7.4.1.2 Viewing Live Video

Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Access Control** > **Access Control Panel**. You can view the live video of the access point (the access point device must come with a camera) or the live video of video channels bound to the access point (the channel can be bound when adding a device) in the following ways.

View live videos in card view

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

Figure 7-54 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.

7.4.1.3 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.

7.4.1.4 Starting a Call

Support remote calling of VTO or face access control devices on the platform.

Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Access Control** > **Access Control Panel**. You can start a call in the following ways.

Start a call in card view

Click to display access points in card view. Click to start a call.

Start a call s in details of an access point

In card view, double-click an access point, and then click .

Start a call on the map

Click on the upper-right corner to display access points on the map. Click an access point, and then click to start a call.

7.4.1.5 Controlling Door Channels Globally

Set all door channels in a zone to normally closed, normally open modes, or restore them to the normal status in one click. Only administrators can control door channels globally.

Log in to the DSS Client. On the **Home** page, select ⊞ > **Access Management** > **Access Control** > **Access Control Panel**. Select a zone, and then click **Always Open**, **Restore**, or **Always Closed** to control all the door channels at the same time.

- **Always Open** : All people can pass without verifying their identifications.
- **Restore** : Restore door channels to the normal status from normally open or normally closed mode. People must verify their identifications to pass
- **Always Closed** : No person is allowed to pass.

If you perform this operation to a zone, it will also be applied to all the sub zones. When the status of the parent zone and sub zone is in conflict, the platform will resolve it in the following ways:

- When a sub zone has been set to the normally open or closed mode, operating the parent zone will override the status of the sub zone.
- When the parent zone has been set to the normally open or closed mode, and you want to set a sub zone to a mode opposite to the parent zone, the platform will prevent you from doing so, and prompt that you must restore the parent zone to the normal status before setting the sub zone.

7.4.1.6 Controlling Lift Channels Globally

Set all lift channels in a zone to no authentication, authentication, and lock modes. Only administrators can control lift channels globally.

Log in to the DSS Client. On the **Home** page, select ⊞ > **Access Management** > **Access Control** > **Access Control Panel**. Select a zone, and then click **No Authentication Mode**, **Authentication Mode**, or **Lock Mode** to control all the lift channels at the same time.

- **No Authentication Mode** : All people can go to any floor without verifying their identifications.
- **Authentication Mode** : People must verify their identifications to go to specified floors.
- **Lock Mode** : No person is allowed to use lifts.

If you perform this operation to a zone, it will also be applied to all the sub zones. When the status of the parent zone and sub zone is in conflict, the platform will resolve it in the following ways:

- When a sub zone has been set to the no authentication or authentication mode, operating the parent zone will override the status of the sub zone.
- When the parent zone has been set to the no authentication or authentication mode, and you want to set a sub zone to a mode opposite to the parent zone, the platform will prevent you from doing so, and prompt that you must set the parent zone to the authentication mode before setting the sub zone.

7.4.1.7 Viewing Real-Time Events

When a person passes through an access point, an event will be reported to the platform. You can view the detailed information of that event.

Prerequisites

If you want to view recorded videos and live videos of an event, you must configure the following parameters first:

- Live video: Bind video channels to access points. For details, see "5.1.3 Binding Resources".

- Recorded videos: First, bind video channels to access points ("5.1.3 Binding Resources"). Then, select either of the 2 options: Configure recording plans for the bound video channels ("5.1.4 Adding Device Recording Plans"), or configure an event to link the bound video channels to record videos when a person passes ("6.1 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.

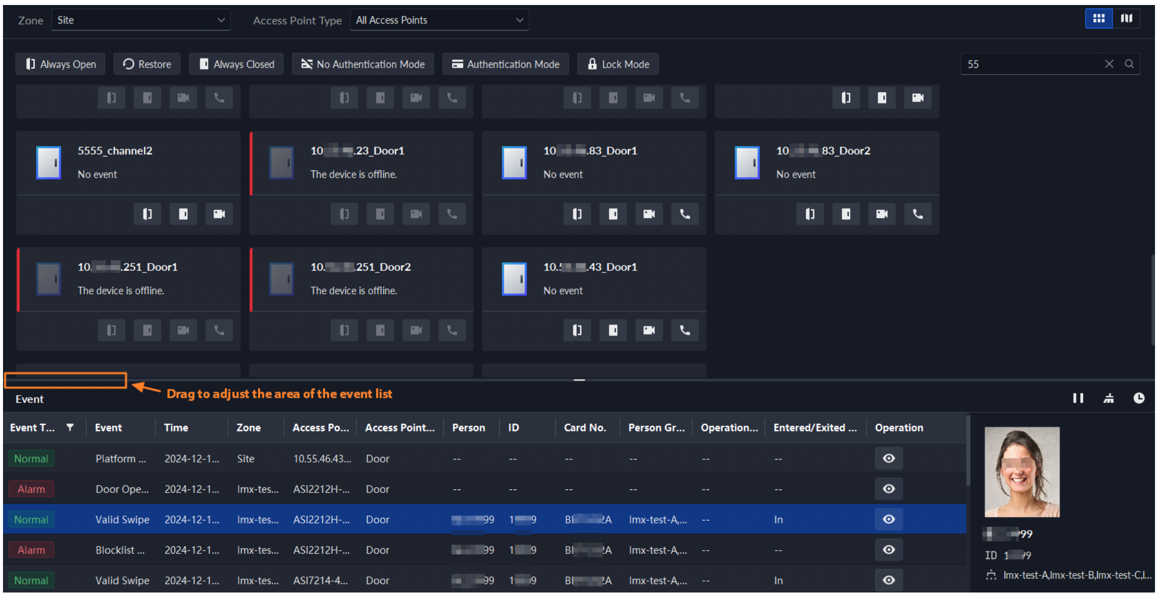
Step 3 Click , and then you can view the snapshot, recorded video, and live video of the event.

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.
- Click the person image at the lower-right corner, and then you can view it in a larger image.

Figure 7-55 Events



Related Operations

- : Stop receiving new events. Click it again to start receiving events.
- : Clear the events on the page, but they will not be deleted.
- : View access records.

7.4.1.8 Viewing and Exporting Specified Events

View and export events in a specified zone, person group, and period.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select ⊞ > **Access Management** > **Access Control** > **Access Records** > **Event Records**.

On top of the page, the numbers of different types of events are displayed for all zones by default.

Step 2 Configure the search conditions, and then click **Search**.

Table 7-13 Parameter description

Parameter	Description
Zone	Search for events in the selected zone. You can select multiple zones at the same time.
Time	Search for events that occurred in the defined period. You can search for event within up to 1 month.
Person Group	Search for events of people that belong to the selected group. The selected person group is empty by default. In this case, the search results will include events with no related person information, such as access by a person whose information is not on the platform, access by strangers, and alarms triggered by devices. If you want to clear the selection of a person group, click ⊠, and then no person group is selected.
Person/Person ID/ Access Point	Select an option and enter keywords to search for certain events. For example, select **Access Point** and enter Front Gate to search for events of access points that have Front Gate in their names.
Keywords	

Step 3 Click **Export**.

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

You can configure whether to verify the password. For details, see "9.2.1 Configuring Security Parameters".

- The encryption password is used to protect the export file. It consists of 6 uppercase or lower case letters, numbers, or their combinations. You need to enter it when using the export file.
- The export range can be all or specified events that are displayed.
- Select **Export Image** to export snapshots of the events at the same time.
- The fields to be exported include **Event Type** , **Event**, **Time**, **Zone**, and more.

7.4.1.9 Acquiring Records

The platform offers 2 methods for acquiring access records, manually or automatically. For the automatic method, only records within the past 24 hours will be acquired. But, the manual method can be used to acquire records from specified period and device.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Access Control** > **Access Records** > **Event Records**.

Step 2 Click **Acquire Records**.

Step 3 Enter the login password, and then click **OK**.

Step 4 Acquire records.

Select **Extract Image**, and then you can acquire images of the access records. Before using this function, you need to configure image storage.

- **Auto Extraction** : The platform will acquire records within the past 24 hours at the defined time every day. How records are synchronized:
  - ◇ If records on a device was automatically synchronized to the platform, then the platform will synchronize all records from the time of the latest record from the last automatic synchronization to the time you set.

    For example, the latest record from the last automatic synchronization was on 2024-6-18 16:00, time of automatic synchronization is set to 04:00 every day. The device was offline on 2024-6-18 18:00, and then reconnected on 2024-6-20 16:00, then the platform, on 2024-6-21 04:00, will synchronize the records generated on the device from 2024-6-18 16:00 to 2024-6-21 04:00.
  - ◇ If records on a device has not been automatically synchronized to the platform, and the device went offline and online multiple times, the platform will synchronize all the records from the time of the latest record uploaded before the first offline, to the time you set.

    For example, time of synchronization is set to 04:00 every day. The device first goes offline on 2024-6-18 16:00 with the latest record uploaded on 2024-6-18 15:00. Before the time of synchronization, the device goes offline and online multiple times. Then on 2024-6-19 04:00, the platform will synchronize the records generated on the device from 2024-6-18 15:00 to 2024-6-19 04:00.
  - ◇ If records on a device has not been automatically synchronized to the platform, and records were not generated on the device and uploaded to the platform when the device is online, then on the time of synchronization, the platform will synchronize the records on the device within the past 24 hours.
- **Manual Extraction** :
  - ◇ Select **Extract Now**, and then the platform will acquire records ranging from the last time that an extraction was performed which were not extracted.

    Select **Extract Image**, and then you can extract images in the access records.
  - ◇ Select **Extract by Range**, and then you can specify the time range, record type, and device.

7.4.1.10 Sending Reports

The platform supports sending reports to the specified receiver by sending now or auto send.

Prerequisites

You need to configure the email server from > **System Parameters** > **Email Server**. For details, see "9.2.4 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**.

7.4.1.11 Viewing Access Route

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

Step 1 Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Access Control** > **Access Records** > **Event Records**.

The number of events in the root zone is displayed on the top of the page by default.

Step 2 (Optional) Select a zone, person group, and period, and then click **Search**.

You can search for event within up to 1 month.

The selected person group is empty by default. In this case, the search results will include events with no related person information, such as access trajectory of a person whose information is not on the platform, access trajectory of strangers, and alarms triggered by devices.

Step 3 (Optional) Click to add multiple events to the temporary records.

Step 4 (Optional) Click to go to the temporary records.

Step 5 Select the records, and then click **Generate Track** to generate the route.

The platform will play the route based on the time of events.

If events happened in multiple zones, and the maps of zones do not relate to each other as main and sub maps, the platform might not play the route normally.

7.4.1.12 Viewing and Exporting Analysis of People Entering and Exiting

When people pass through boundaries, the platform will count the number of people entering and exiting zones. You can view the number of each zone and export it to your computer.

Prerequisites

Set access points as boundaries. The platform will only count the number of people pass through boundaries. For details, see "6.5.2.5.2 Setting Boundary".

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select ⊞ > **Access Management** > **Access Control** > **Access Records** > **Analysis of People Entering and Exiting**.

Step 2 Select one or more zones, boundaries, and the start time, and then click **Search**.

The platform will display the statistics of people entering and exiting the selected zone, and related events ranging from the start time to the current time. For example, the platform will display the statistics and events ranging from the defined start time 5-16 08:00:00 to the current time 5-17 10:00:00.

Step 3 Click **Export**.

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

You can configure whether to verify the password. For details, see "9.2.1 Configuring Security Parameters".

- The encryption password is used to protect the export file. It consists of 6 uppercase or lower case letters, numbers, or their combinations. You need to enter it when using the export file.
- The export range can be all or specified events that are displayed.
- Select **Export Image** to export snapshots of the events at the same time.
- The fields to be exported include **Event Type** , **Event**, **Time**, **Zone**, and more.

Related Operations

- Manually mark the enter or exit status for people:
  - On the list of **Person Entered** , **Person Exited** or **Persons Who Did Not Exit after Entering**, click to see all access records of a person. Click to mark a record as invalid (the records will not be deleted). The invalid records can also be restored to be valid. The statistics and status of the person will change accordingly.
  - On the list of **Persons Who Did Not Exit after Entering**, click to mark a person as "exited". The statistics and status of the person will change accordingly.
- You can filter the search results by **Person Group** , and also search the records by selecting **Person**, **ID**, **Access Point**, **Company**, or **Department**, and then entering the keywords.

7.4.2 Video Intercom Application

- You can call, answer, release information and view video intercom records.
- Make sure that you have configured the video intercom configuration before application. For details, see "6.6 Video Intercom". You can also click Video Intercom Config to go to the video intercom configuration page.

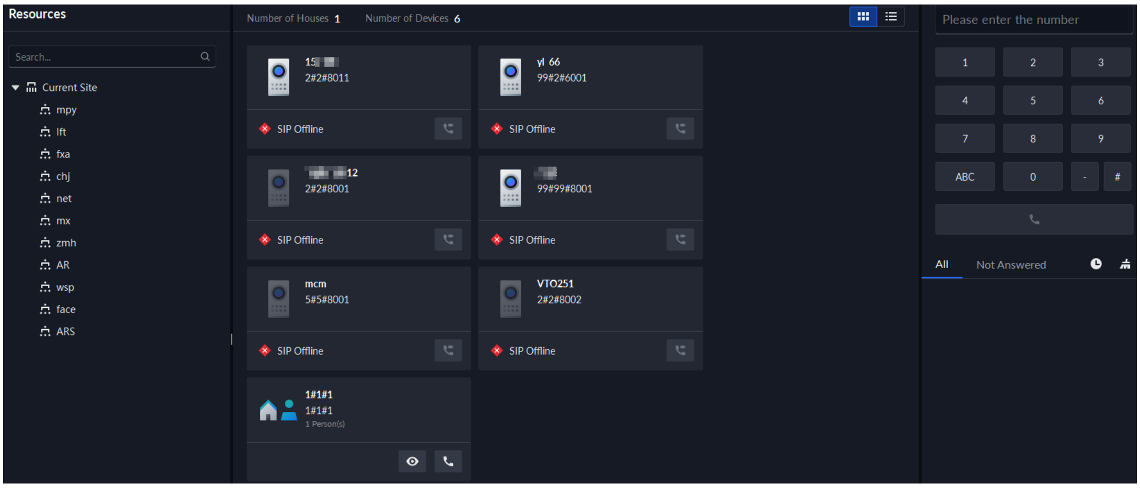
7.4.2.1 Call Center

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

Procedure

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

Figure 7-56 Call center



Step 2 You can call different devices.

- Call from the platform to VTO

  Select VTO in the device list; click corresponding of VTO or dial a number on the dial pad to call the VTO. The system pops out call page. The following operations are supported during call.

  ◇ : If VTO is connected to lock, click this icon to unlock.
  ◇ : Click this icon to capture picture, the snapshot is saved into the default directory. To change the path, see "10.4.5 Configure File Storage Settings".
  ◇ : Click this icon to start record, click again to stop record. The video is saved in default path. To change the path, see "10.4.5 Configure File Storage Settings".
  ◇ : Click this icon to hang up.

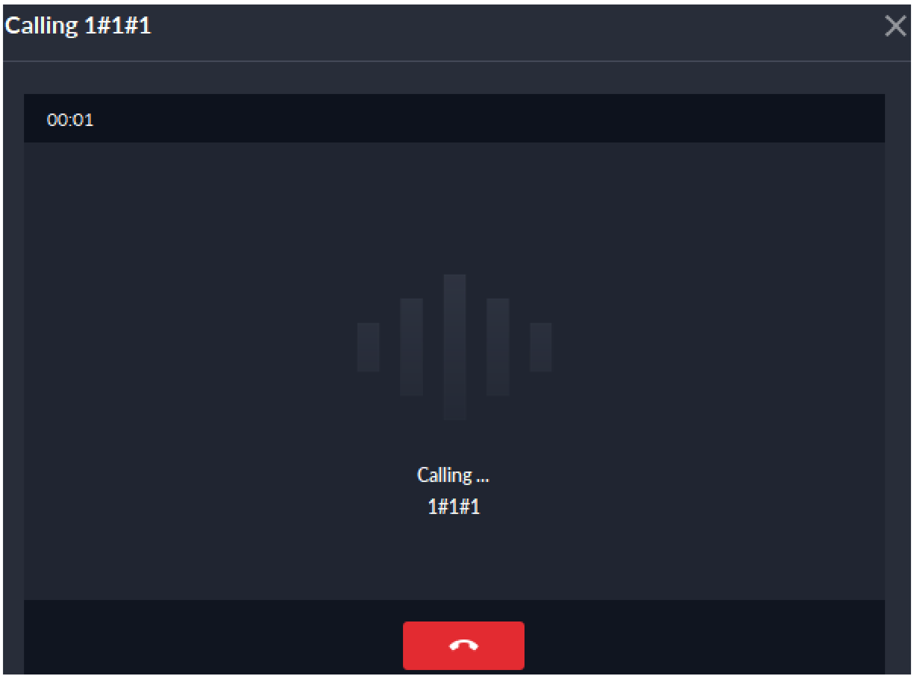
  If the device supports two locks, two lock icons will appear on the page, and you can click either one to unlock corresponding door.

- Call from the platform to VTH

  Select VTH from the device list, click on the VTH or dial corresponding VTH on the right (such as 1#1#101). The system pops up the dialog box of **Calling now, please wait ...**. There are two modes for answering the call.

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

Figure 7-57 Calling



- Call from the platform to an access control device that supports video intercom

  Select a device from the device list, click on it or dial its number on the right (such as 1#1#101). The system pops up the dialog box of **Calling now, please wait ….** There are two modes for answering the call.

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

- Call from VTO to the platform

  When a VTO calls, a window pops up.

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

- When VTH is calling the platform

  The client pops out the dialog box of VTH calling. Click to talk with VTH.

  - ◇ Click to answer VTO, realize mutual call after connected.
  - ◇ Click to hang up.

- When an access control device that supports video intercom is calling the platform

  The client pops out the dialog box. Click to talk with the device.

  Click to hang up.

- Call through call records

  All the call records are displayed in the **Call Record** at the lower-right corner of the page of **Video Intercom**. Click the record to call back.

7.4.2.2 Releasing Messages

Send message to VTHs.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click > **Access Management** > **Video Intercom** > **Information Release**.

Step 2 Click **Add New Message**, select one or more VTHs, and then configure the information you want to send.

Step 3 (Optional) Enable **Scheduled Release**, and then configure the time.

Step 4 Send the message.

- If no scheduled release time is configured, click **Instant Release** , or click **Save**, and then click to send the message immediately.
- If a scheduled release time is configured, click **Save**, and then the message will be sent on the defined time.

7.4.2.3 Video Intercom Records

Search for and view call records.

Background Information

- In a call group, only one record is generated for a call, either the call is answered or missed.
- In a call group, if one person answers, the call is considered answered. The missed records of others are not displayed.

Procedure

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

Step 2 Set conditions, and then click **Search**.

The platform displays all the records according to the configured conditions.

Step 3 (Optional) Click **Export**, and then follow the prompts to export all or partial records to your computer.

7.4.3 Viewing Attendance Data

View attendance data, displayed in the form of report, including card swiping record table, attendance report, abnormality table, overtime table and away table. This section uses **Card-swiping Record** as an example.

Prerequisites

You have configured the attendance parameters before application. For details, see "6.7 Attendance Management". You can also click **Attendance Config** to go to the attendance configuration page.

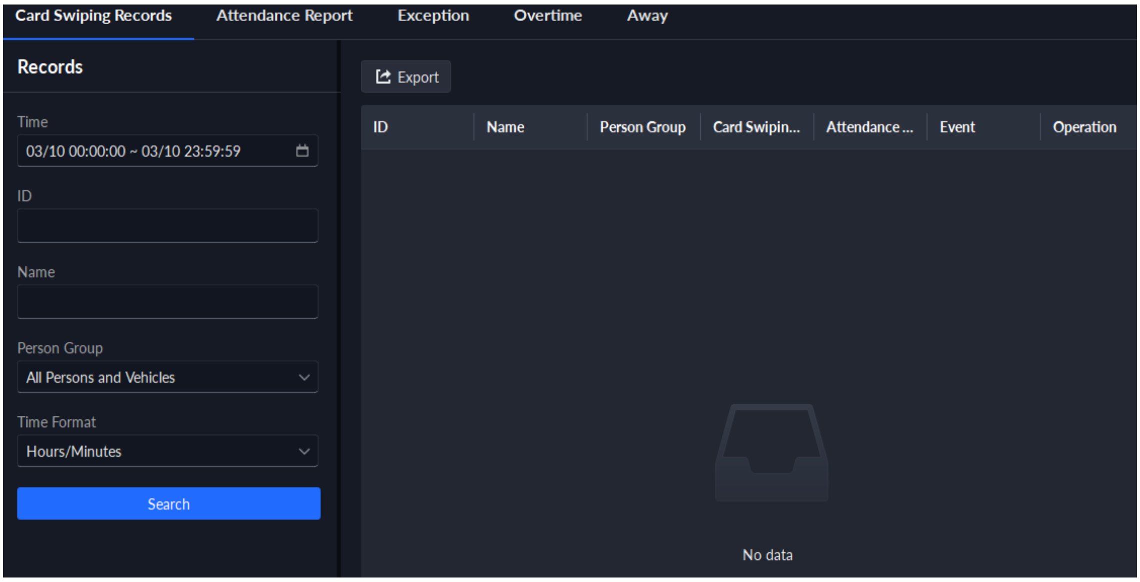
Procedure

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

Step 2 Click corresponding tab, set search condition, and then click **Search**.

For the data in **Attendance Report** , **Overtime**, and **Away**, you can set the time format to minutes or hours+minutes.

Figure 7-58 Attendance



Step 3 Manage search results.

- Click **Export** at the upper-left corner of the page, and then export records as the screen instructs.
- When card swiping records are displayed in list, click to view the details of the corresponding user.

7.4.4 Visitor Application

After appointment is made on the platform, and visitor information is registered, the visitor can have access permission. Access permission is disabled after the visitor leaves or if the visitor does not leave after the appointment leaving time.

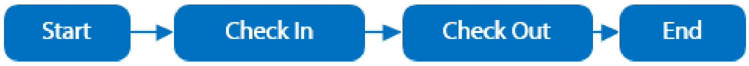
7.4.4.1 Preparations

- 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 "5 Basic Configurations".
- Make sure that you have configured the visitor configuration before application. For details, see "6.8 Visitor Management". You can also click Visitor Config to go to the video intercom configuration page.

7.4.4.2 Process

- Visits after appointment: Visitors make appointments according to "7.4.4.4 Visitor Appointment", and when they arrive on site, they can quickly access by confirming their information through **Check In** according to "7.4.4.6 Checking In".

- Visits without appointment: When visitors arrive, they need to fill out visitor information on site according to "7.4.4.6 Checking In". This will take a few minutes before they can access.



7.4.4.3 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 7-59 Visitor management

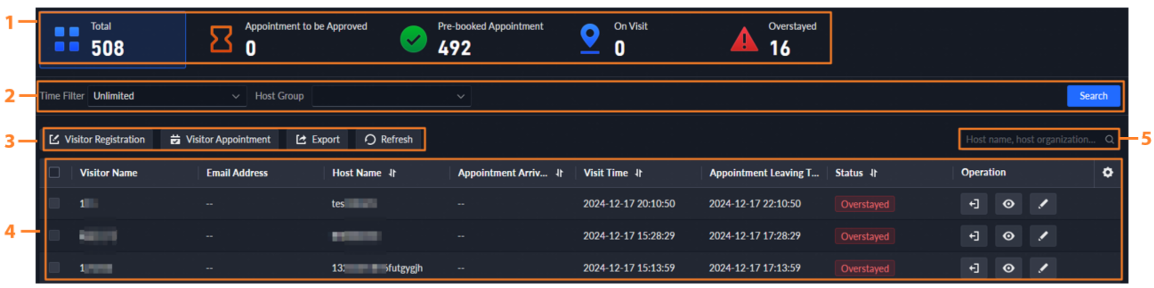


Table 7-14 Visitor management description

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 "6.8.2 Configuring Visit Settings". After being approved, the status changes to **Pre-booked Appointment**. ● **Pre-booked Appointment** : Appointment has been made, but not checked in yet. ● **On Visit** : Already checked in, but not exceed the appointment leaving time. ● **Overstayed** : Not checked out after the appointment leaving time.
2	Filter the visitor information by host group and time (appointment visit time, visit time, appointment leaving time, or unlimited).
3	Perform operations such as visitor registration, visit appointment and exporting visitor information. See the following sections in this chapter.
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.

7.4.4.4 Visitor Appointment

Making appointment before visitor arrive will greatly reduce the time that visitors have to wait for their information to be recorded. After appointment, the visitor status changes to **Pre-booked Appointment**.

5 ways of appointment are available:

- Appointment through the platform. For details, see "7.4.4.4.1 Appointment through the Platform".
- Create appointment by visitors. For details, see "7.4.4.4.2 Creating Appointment by Visitors".
- Invited by host. For details, see "7.4.4.4.3 Appointment Invited by Host".
- Appointment through the visitor terminal. For details, see the user manual of the visitor terminal.
- Appointment DSS Agile app. For details, see the user manual of the app.
- Invited by host through DSS Agile VDP app. For details, see the user manual of the app.

7.4.4.4.1 Appointment through the Platform

Register the information of visitors on the platform before they arrive for their visits. This will greatly reduce the time that visitors have to wait for their information to be recorded.

Procedure

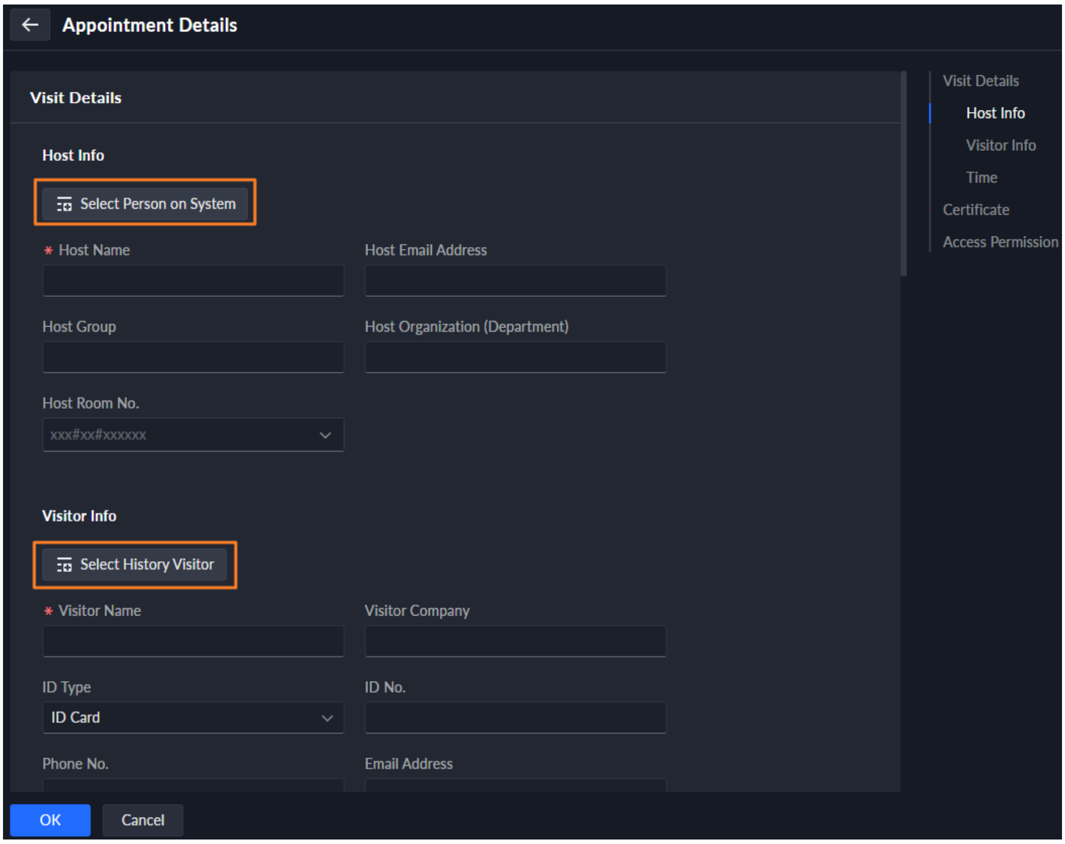
Step 1 Log in to the DSS Client. On the **Home** page, click ⊞ > **Access Management** > **Visitor** > **Visitor Management**.

Step 2 Click **Visitor Appointment**.

Step 3 Enter the information of host and visitor.

Click **Select Person on System** , and then select a person (only person in the person group to which the current user has permission can be selected. Person group permissions can be configured when adding a person). The host information will be automatically filled in and cannot be edited; click **Select History Visitor**, and then select a history visitor. The information of this visitor will be automatically filled in and cannot be edited.

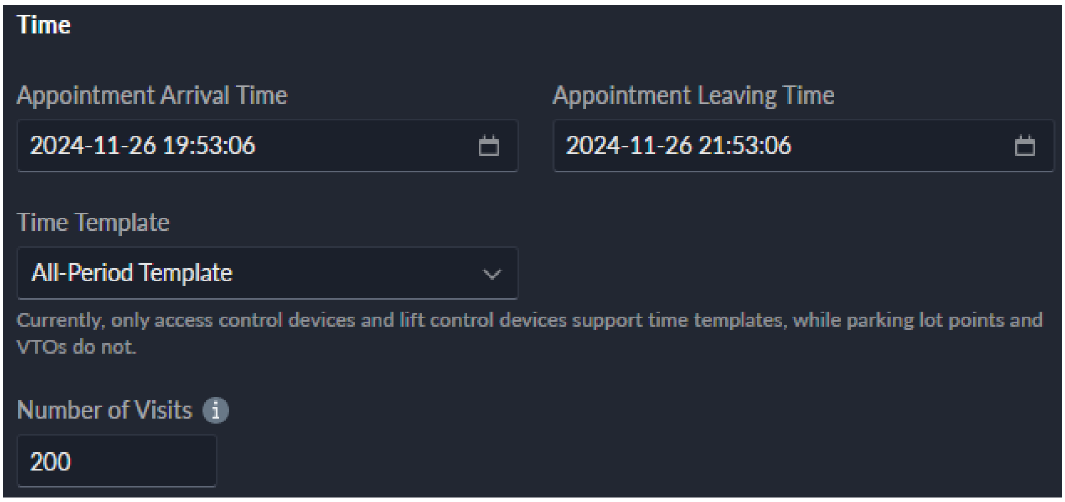
Figure 7-60 Visitor appointment



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 7-61 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 7-15 Certificate description

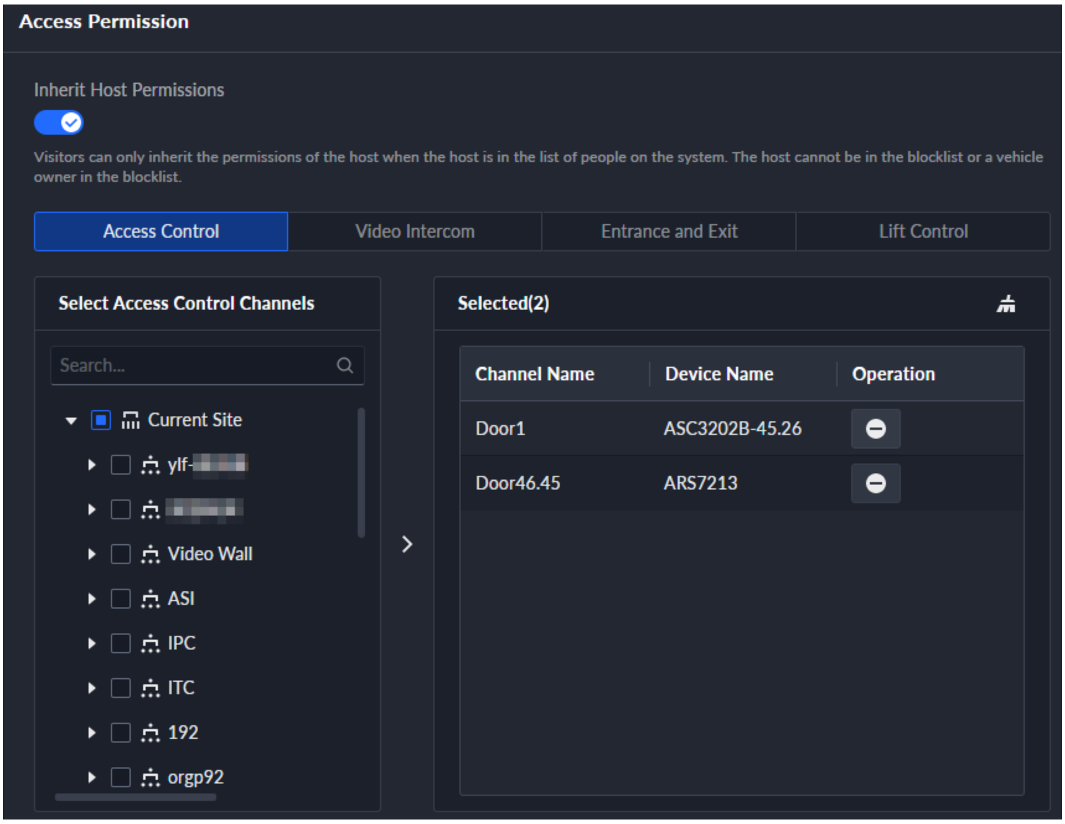
Tab	Description
Card	Issue a card to a visitor. You can issue cards by entering card number manually or by using a card reader. A card number comes with 8–16 numbers. Only second-generation access control devices support 16-digit card numbers. When a card number is less than 8 numbers, the system will automatically add zeros prior to the number to make it 8 digits. For example, if the provided number is 8004, it will become 00008004. If there are 9-16 numbers, the system will not add zero to it. ● Issue cards by entering card numbers manually: Click **Add** , enter the card number, and then click **OK**. ● Issue cards by using a card reader: Click , select a card reader or device, and then click **OK**. Swipe card through the reader or device, and then a new card will be issued.
Face	Set the face image of the visitor. 1. Click **Add**. 2. Click **Select from Local Folder** to select a picture, or click **Snapshot** to take a photo (if a camera is detected on your computer).
Visitor Pass	Click **Generate** to generate a QR code for the pass. ● The QR code includes the visitor virtual ID (randomly generated by the system) and the QR code encryption information. The defined appointment period is sent to the access control device through the virtual ID. ● The QR code is valid within the defined appointment period. ● You can click **Download Pass** to download the QR code, or you can click **Email Pass** to send it to the visitor by email.

Step 6 Click the **Access Permission** tab, and then select access permissions for the visitor.

If you want to set video intercom devices and entrance and exit permissions, you must set host room number and number plate for the visitor.

By enabling **Inherit Host Permissions**, the visitor can share the access permissions with the host, but be noted that the host must be in the list of people on the system, and cannot be in the blocklist or the owner of a vehicle in the blocklist.

Figure 7-62 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.

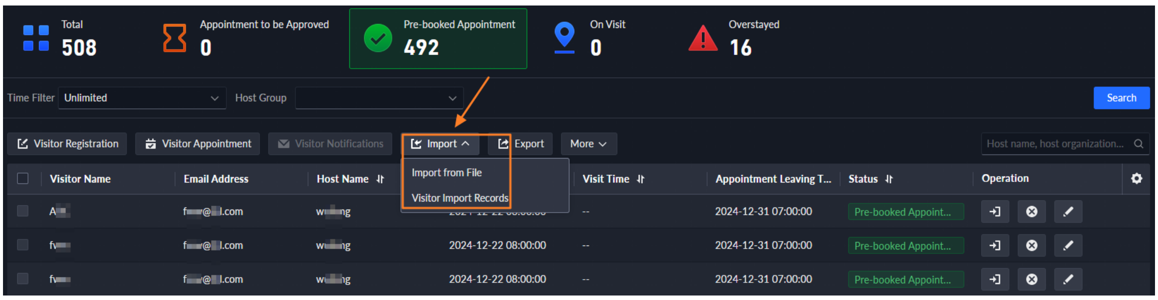
Related Operations

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 7-63 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.

7.4.4.4.2 Creating Appointment by Visitors

After the platform administrator generates the visitor appointment link on the platform, visitors can access the link and fill out their appointment information. After approval, the visitor can access with the visit credential.

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

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

Step 2 Select **Visitor Appointment Config** > **Create Appointment**.

Step 3 (Optional) Enable **Appointment Review Config on Visitor Terminal** as needed. After being enabled, appointments made through the visitor terminal must be approved by the defined approver before the visitors can access; if not enabled, then no approval is required.

Step 4 Select the approver.

When selecting **Host Approval**, the host will receive an email notification for approval; when selecting **Role**, the defined role will receive an approval notification in the platform's notification center at the upper right.

Step 5 Enable **LAN Access Entry** or **WAN Access Entry**, click **Send Email**, and then set the visitor's email. The platform will send an invitation link to the visitor's email through LAN or WAN.

- Click **Regenerate** to generate a new link. The original link will be invalid.
- Click to copy the link.

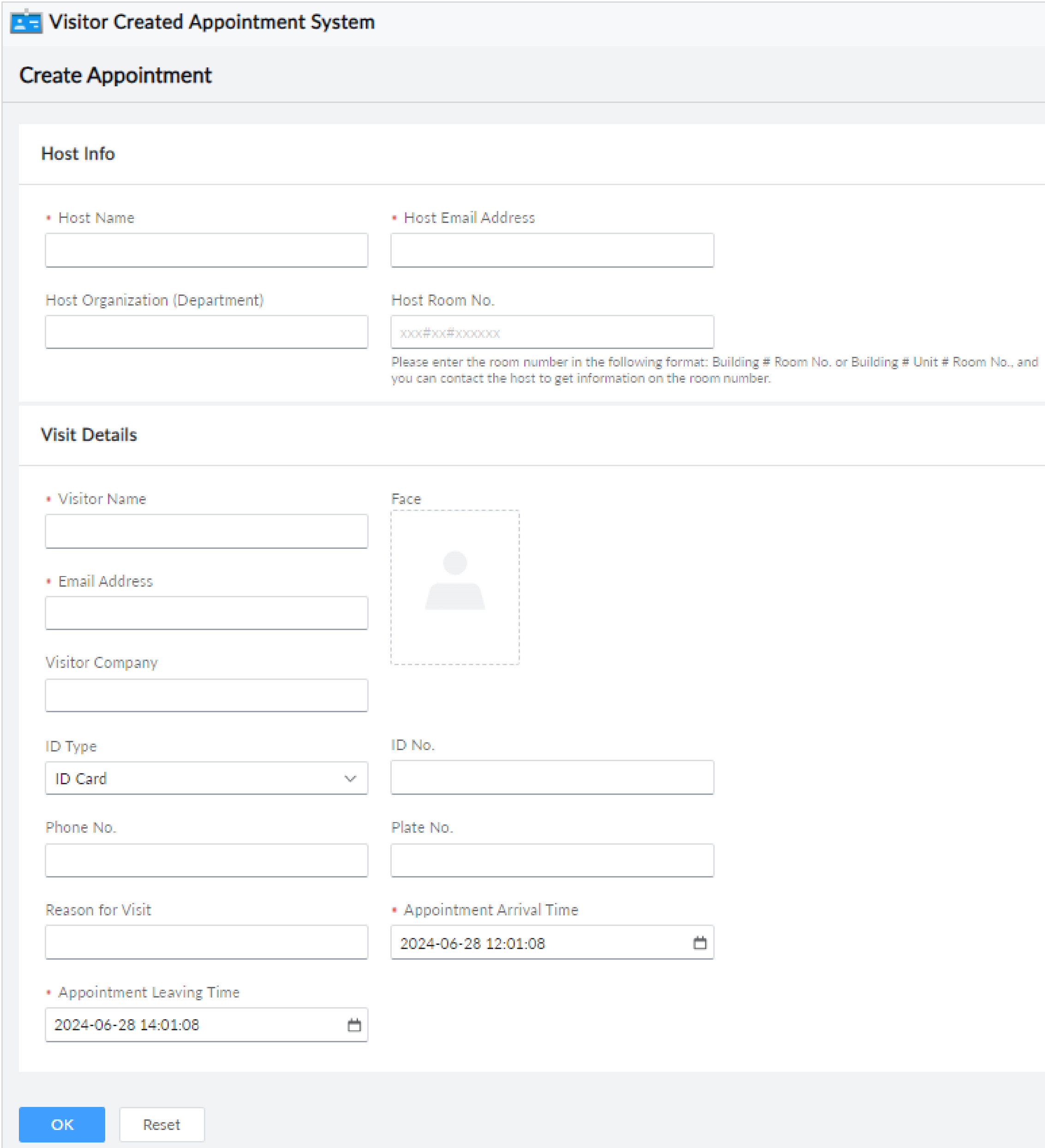
Step 6 (Optional) Click to download the QR code; click , and then select the printer to print the QR code.

Step 7 Click **Save**.

Step 8 The visitor clicks the link or scans the QR code to fill in the information, including their name, email, company (department), room number, appointment arrival time, and appointment leaving time, and the host's name, email address, license plate number, phone number, and more.

The host must be a person that has been added to the platform in > **Person and Vehicle Info** > **Person List**.

Figure 7-64 Create appointment



Step 9 Approve the appointment.

Step 10 The visitor visits the host with the visit credential received through the email.

7.4.4.4.3 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 "7.4.4.5 Reviewing Appointment".

Step 4 Enable **LAN Access Entry** or **WAN Access Entry**, click **Send Email**, and then set the visitor's email. The platform will send an invitation link to the visitor's email through LAN or WAN.

- Click **Regenerate** to generate a new link. The original link will be invalid.
- Click to copy the link.

Step 5 (Optional) Click to download the QR code; click , and then select the printer to print the QR code.

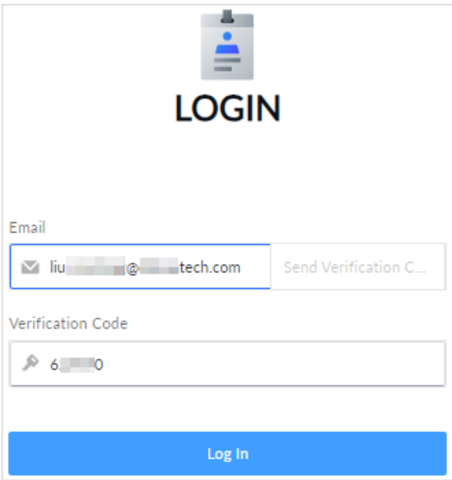
Step 6 Click **Save**.

Step 7 The visitor clicks the link or scans the QR code to fill in the information.

1. Enter the email address of the host, and then the system will send a verification code to that email address.

   You need to configure the person's email from **Person and Vehicle Info** > **Person List**; otherwise, the verification code cannot be sent.

   Figure 7-65 Verify email of host

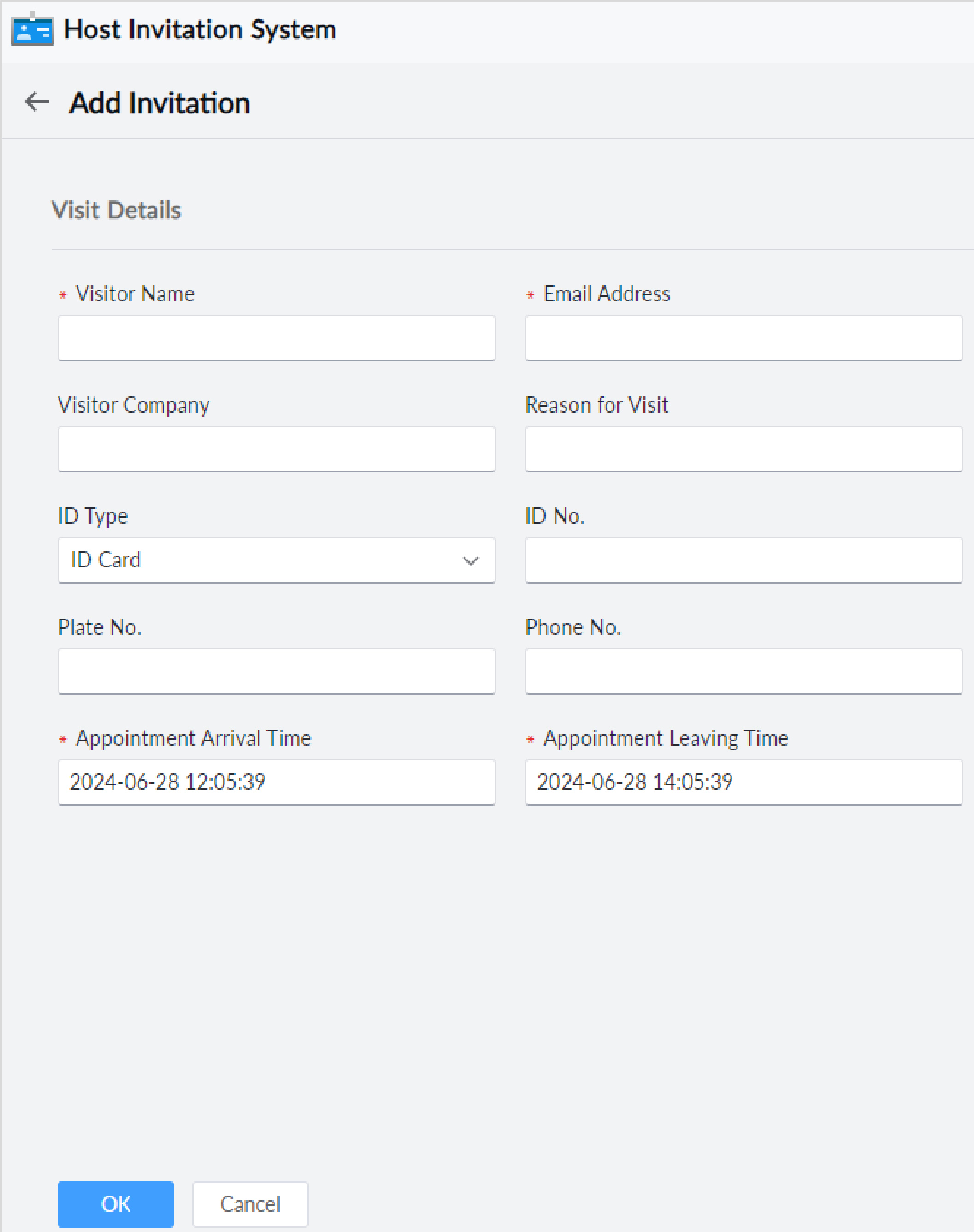
   

2. After entering the verification code, the visitor can select **Add Invitation** to proceed.

   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 7-66 Host invitation



4. Click **OK**.

Step 8 The approver approves the appointment (if approver has been configured).

Step 9 The visitor visits the host with the visit credential received through the email.

7.4.4.5 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 "6.8.2 Configuring Visit Settings".

Procedure

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

Step 2 Click the **Appointment to be Approved** tab.

Step 3 Review the appointment.

- Click to approve the appointment. After this, the **Status** changes to **Pre-booked Appointment**.
- Click to decline the appointment.
- Click to send the email to notify visitors configured through > **Visitor** > **Visitor Appointment Config**.

  The host will also be reminded to give their approval if **Host Approval** is enabled in > **Visitor** > **Visitor Appointment Config** > **Create Appointment**.

7.4.4.6 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 "7.4.4.4 Visitor Appointment".

Step 3 Click **OK**.

After checking in, the visitor status changes to **On Visit**.

7.4.4.7 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

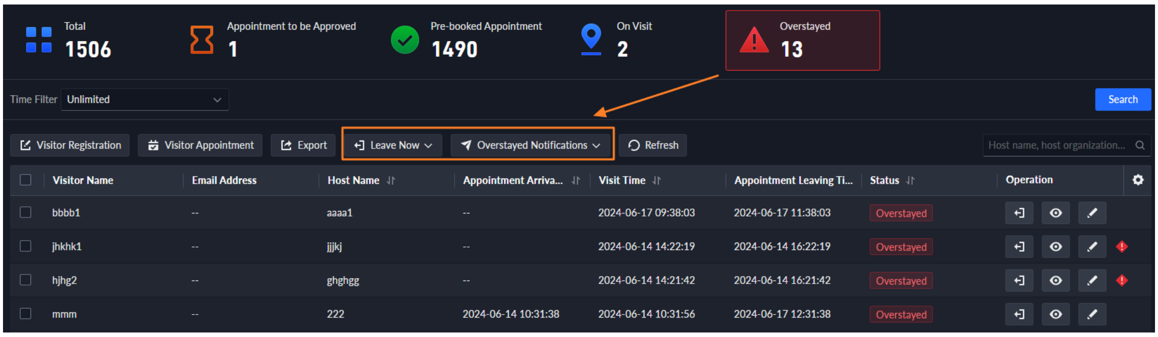
Click the **Overstayed** tab, and then you can check out visitors that are overstayed in batches and send notifications to them.

- 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 7-67 Operations related to overstayed visit



7.4.4.8 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

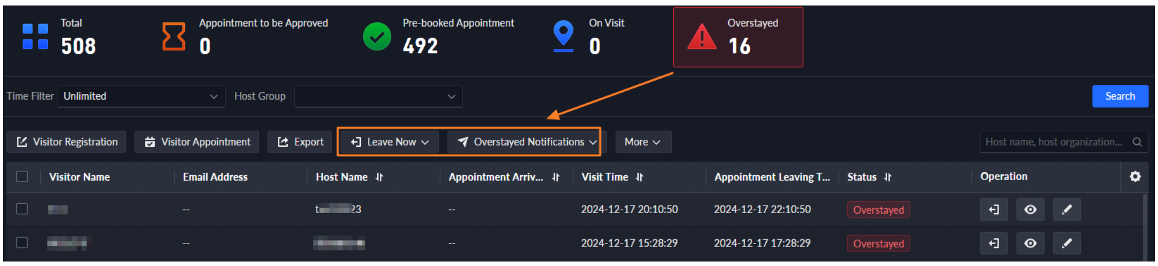
Step 1 Log in to the DSS Client. On the **Home** page, click > **Access Management** > **Visitor** > **Visitor Management**.

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 7-68 Operations related to overstayed visit



7.4.4.9 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.

7.5 Parking Lot

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

7.5.1 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 7-69 Monitor entrances and exits

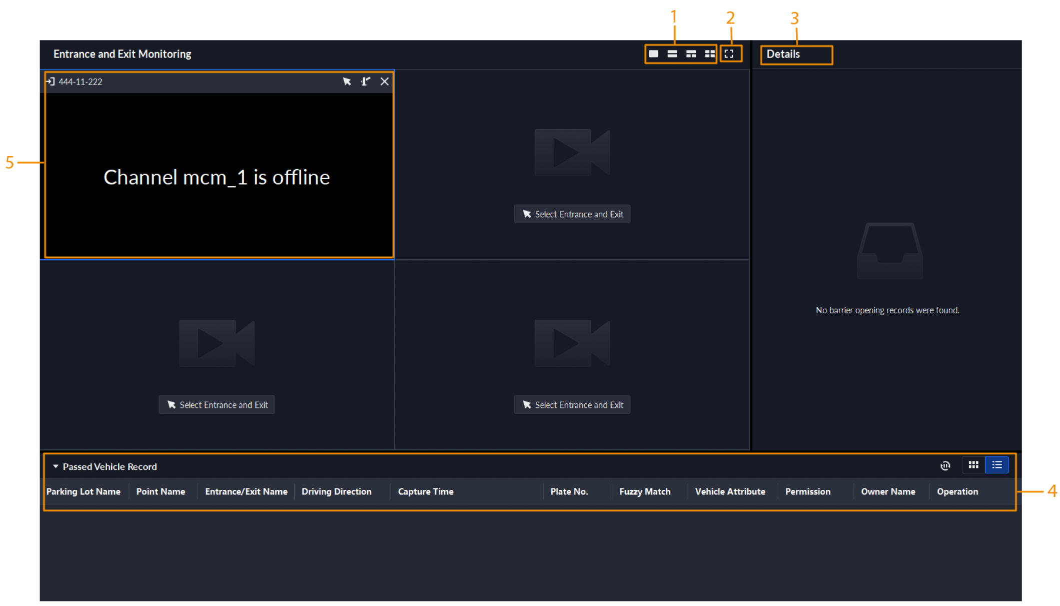


Table 7-16 Page description

No.	Description
1	Select the number of windows you want. Each window can display the real-time video of one entrance or exit point.
2	Full screen mode.
3	Displays records of barriers not opened.
4	All entrance and exit records.
5	The real-time video of an entrance or exit point. ● Click to open the real-time video of another entrance or exit point in the window. ● Click to open the barrier for vehicles. ◇ **Open without Recording Plate Info** : Open the barrier for vehicles without recording their plate numbers. If you select **Count Parking Spaces** at the same time, the number available parking spaces in the parking lot will decrease or increase depending on whether the vehicles are entering or exiting. This operation will not generate an enter or leave record. You need to enable the parking space counting during configuration, and set the parking space counting mode as count parking spaces by entering and exiting vehicles. ◇ **Open and Record Plate Info** : This is applicable to when the ANPR cameras cannot recognize the number plates. You can manually enter the number plate, and a snapshot will be taken, and then the platform will generate an entrance or exit record.

7.5.2 Searching for Records

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

7.5.2.1 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.

- 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.

7.5.2.2 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.

7.5.2.3 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.

7.5.2.4 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.

7.6 Intelligent Analysis

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

7.6.1 People Counting

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

7.6.1.1 Real-Time Count

Procedure

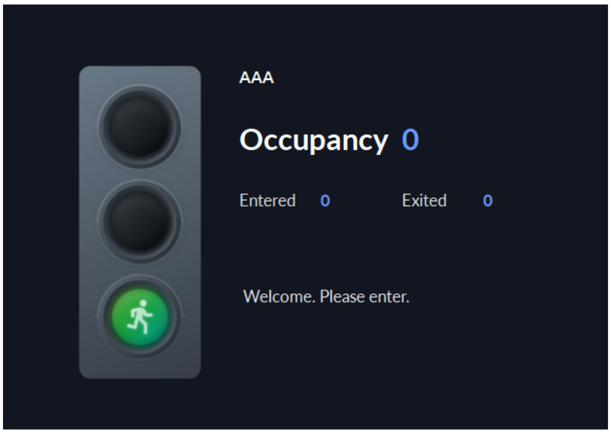
Step 1 Log in to the DSS Client. On the **Home** page, click > **Intelligent Analysis** > > **Real-time Count**.

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

Use the buttons on the upper-right corner to set the number of windows and to display in full screen.

- **Occupancy** : The number of people currently inside this group, which will be reset to the defined value at the defined calibration time.
- **Entered** : The number of people entered this group, which will be reset to zero at the defined calibration time.
- **Exited** : The number of people who left this group, which will be reset to zero at the defined calibration time.
- Color of the light:
  - Red light: Occupancy ≥ overlimit threshold.
  - Yellow light: Crowded threshold ≤ occupancy < overlimit threshold.
  - Green light: Occupancy < normal threshold.

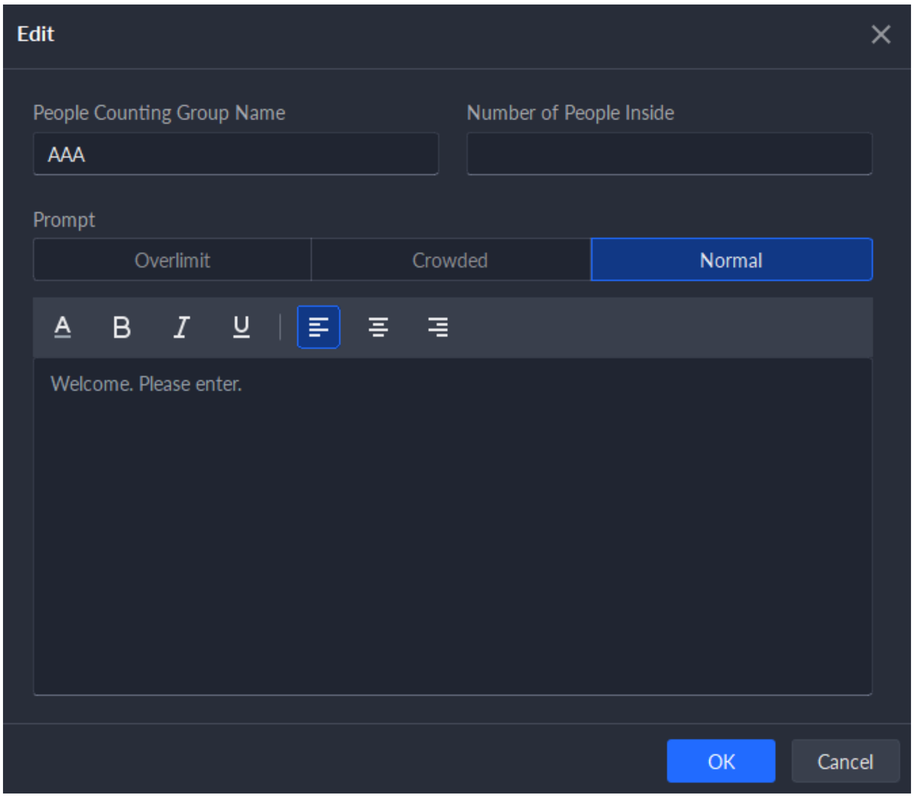
Figure 7-70 Real-time count



Step 3 Hover your mouse on the window displaying real-time data, and then click .

Step 4 You can enter a number of people to overwrite the current data, and customize the content to be displayed for green, yellow and red light.

Figure 7-71 Edit the content and data



Step 5 Click **OK**.

7.6.1.2 Historical Count

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, click > **Intelligent Analysis** > **People Counting** > **Historical Count**.

Step 2 Select the groups you want in **Groups** , or select the channels in **Resources**.

Step 3 Configure the search settings, and then click **Search**.

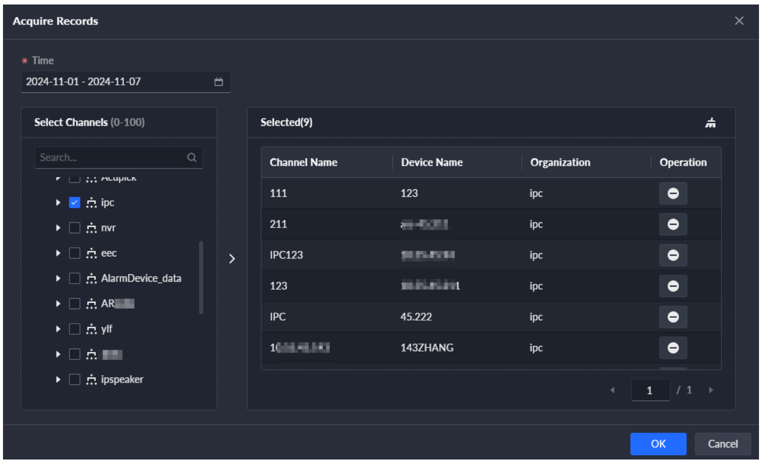
- **Groups** : Groups are people counting groups, which allow you to combine and calculate the people flow data from multiple rules across different devices and channels. You can search for historical people flow data from one or more people counting groups.
- **Resources** : Search for historical people flow data from one or more channels. The data from all the rules of a channel will be included.

If a device is offline, it will upload all the data to the platform when it is online again.

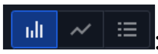
Related Operations

- **Acquire Retention** : Click **Acquire Retention**, and then enter the login password, select the date and channels to acquire the record.

Figure 7-72 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.

7.6.2 Heat Maps

View heat maps generated by devices. A heat map shows the distribution of people flow by different colors, such as red for many people have visited an area and blue for only a few people have visited an area. The platform supports generating general heat maps and advanced heat maps. Only fisheye cameras support advanced heat maps.

Prerequisites

Configure the channel feature for either type of heat maps. For details, see "5.1.2.5.2 Modifying Device Information".

- General heat map: Select the **General Heat Map** from the channel features.
- Advanced heat map: Select the **Advanced Heat Map** from the channel features.

Procedure

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

Step 2 Select a channel, and then generate a heat map.

You can generate a heat map with data from up to one month.

- Generate a general heat map.

  Configure the time, and then click **Search**.
- Generate an advanced heat map.

1. Select how you want to generate the heat map, **Number of People** or **Time**.
2. Configure the threshold.

   - When you select **Number of People**, the area with the closest number of people to the threshold will be in red.
   - When you select **Time**, the area where people stay for a duration closest to the threshold will be in red.
3. Set the time, and then click **Search**.

Step 3 Click **Export** on the upper-right corner to export the heat map to your PC.

7.6.3 In-Area People Counting

View statistics on the number of in-area people.

Procedure

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

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

- **Report Time** : You can search for **Daily**, **Weekly** or **Monthly** reports.
- **Stay Duration** : The duration that the people stay in the area. You can select from 5 seconds, 30 seconds, 60 seconds or custom. After you select the duration, for example 60 seconds, the list displays the people stay less than 60 seconds and not less than 60 seconds in different colors.

- Custom stay duration can be configured from 0 to 1800 seconds or 0 to 30 minutes.
- If a device is offline, it will upload data within the past 24 hours to the platform when it is online again.

Related Operations

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

7.6.4 Metadata Analysis

View the statistics of faces, human body, motor vehicles, and non-motor vehicles based on channels and export reports to local computer.

Procedure

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

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

- Object: It is **Face** by default, and you can select **Human Body**, **Motor Vehicles** or **Non-motor Vehicle**.
- **Report Type** : You can search for **Daily**, **Weekly**, **Monthly**, **Yearly** or **Custom** reports.

Custom search time can be configured for a maximum of 31 days.

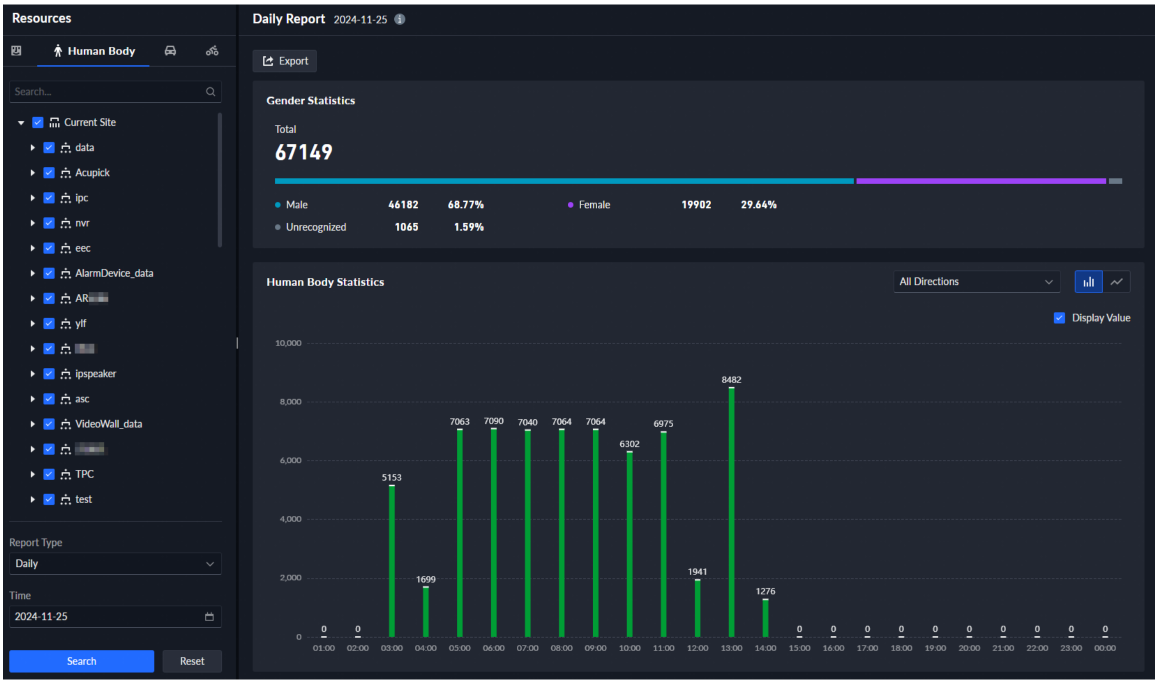


Figure 7-73 Metadata Statistics

Related Operations

- : Change the display format of the data.
- **Export** : Export the data to your PC.
- Select **Display Value**, and then the specific values will be displayed on the bar chart or line chart.
- Configure search conditions such as gender and age to filter search results.

7.7 Maintenance Center

You can view the overall running status of the platform, including channel and device.

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, and storage and status of the platform. The data is refreshed every 5 minutes.
- Select **Resource Monitoring** > **Server Status**, and then click a service to view its running status and history information, including logs generated on the current day. Click **View All** to go to corresponding pages for more information.
- Device Status

  Select **Resource Monitoring** > **Device Status** > **Real-Time Status**. Click a device type, and then the status of all the devices is displayed on the right. Click to view detailed information.

  - ◇ **Channel Status Info** : Information such as the channel name, online or offline 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.
  - ◇ **History Info** : Displays 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.

8 General Application

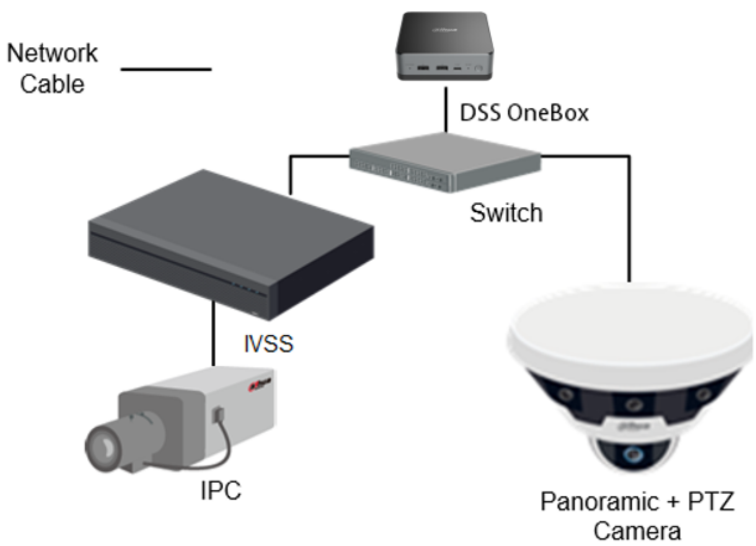
8.1 Target Detection

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.

8.1.1 Typical Topology

Figure 8-1 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.

8.1.2 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 "5 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.

8.1.3 Live Target Detection

Procedure

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

Step 2 Select a window, double-click the channel or drag the channel to the window.

Step 3 Click and then click to view live metadata events.

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

- Click an event record to view the event snapshot. You can play back the video of the event. Different events support different operations.
- When playing back video, click to download the video to a designated path.
- Click to play back the video before and after the snapshot.
- Click to delete event information.
- Click to view the most recent events.

8.1.4 Searching for Metadata Snapshots

Search for metadata snapshots by setting search criteria or uploading images.

Procedure

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

Step 2 Click **Integrated Retrieval**.

Step 3 Set search criteria.

You can search for metadata snapshots in the **Record** , **Person** or **Vehicle** section. For details, see "7.3 DeepXplore".

8.2 ANPR

View automatic number plate recognition in real time or search for records.

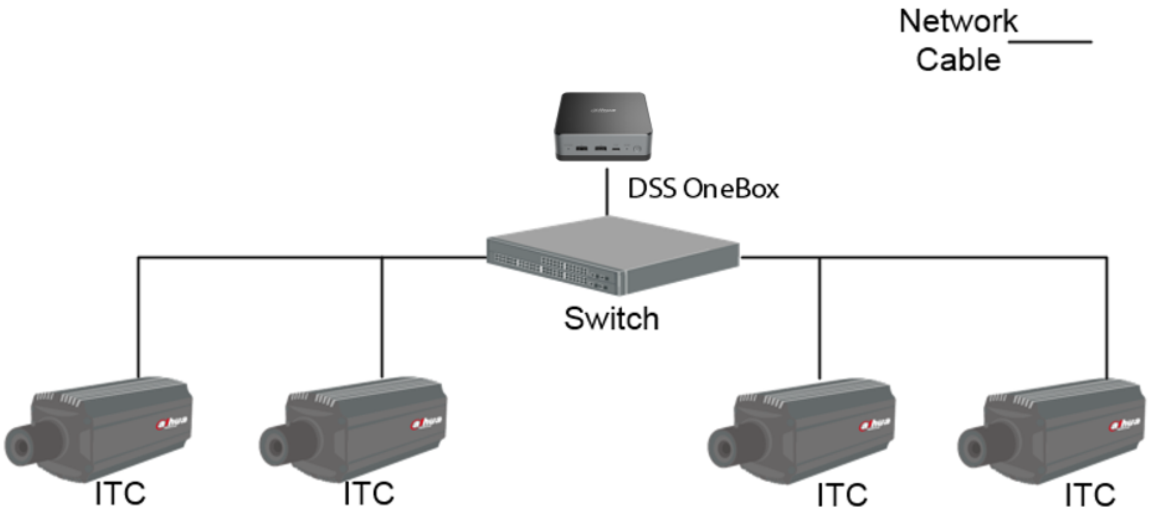
- Automatic number plate recognition

  The platform displays vehicle snapshots and ANPR results in real time.
- Vehicle records

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

8.2.1 Typical Topology

Figure 8-2 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.

8.2.2 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 "5 Basic Configurations".
  - ◇ When adding an ITC camera, select **ANPR Device** for device category, and then select **ANPR Device** for **Device Type**.
  - ◇ ANPR snapshots are only stored on **ANPR Picture** disks. On the **Storage** page, configure at least one **ANPR Picture** disk. Otherwise vehicle pictures cannot be viewed.

8.2.3 Live ANPR

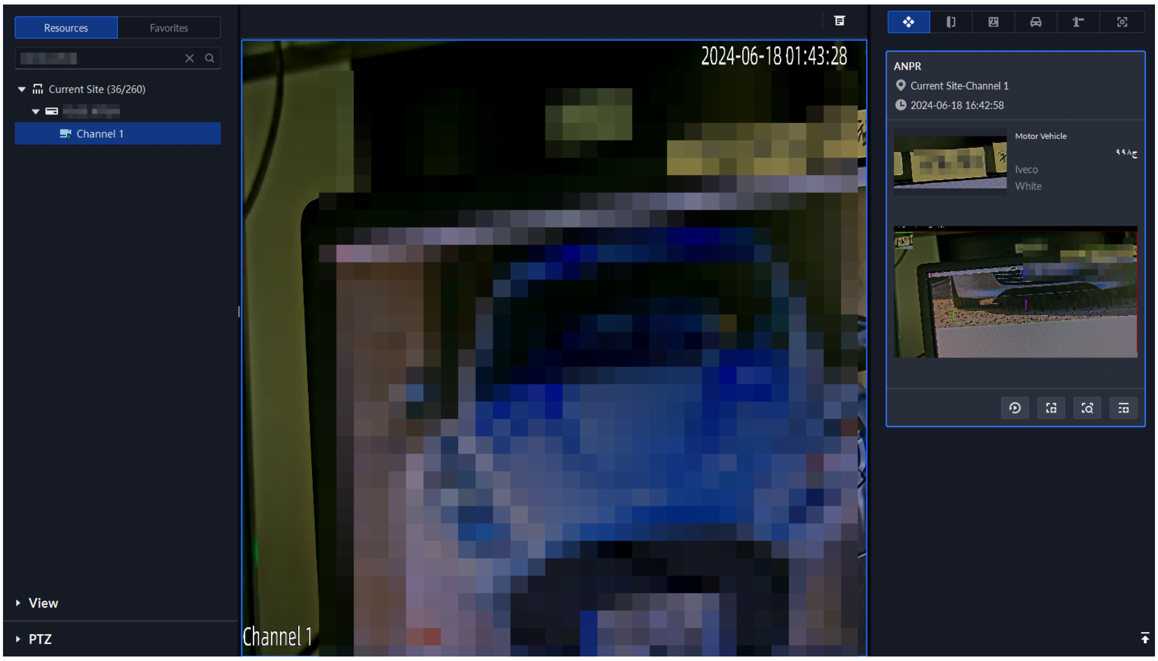
View ANPR live video and plate snapshots.

Procedure

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

Step 2 Select a window, double-click the channel or drag the channel to the window.

Figure 8-3 Live view



Step 3 Click and then click .

Step 4 View live ANPR events.

- Click an event record to view event snapshots. You can also play back the video of the event. Different events support different operations.
- : This function is only available when a license plate is recognized. Click this icon to add the vehicle to an arming group. After you send the group to devices and configure an event, devices can trigger alarms when the vehicle is recognized.
- : Add the vehicle to the platform.
- When playing back a video, click to download the video to a designated path.
- Click to play back the video before and after the snapshot.
- Click to delete event information.
- Click to view the most recent events.

8.2.4 Searching for Vehicle Snapshot Records

If there are recorded videos on devices, you can view recorded videos linked to the capture records by searching for them. Each video will be 20 s long, with 10 s before and after the time of capture. When playing a video, it will start at 10 s before the time of capture.

Procedure

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

Step 2 Click **Integrated Retrieval**.

Step 3 Configure the search conditions.

You can search for vehicle snapshots in the **Record** or **Vehicle** section. For details, see "7.3 DeepXplore".

8.3 Face Recognition

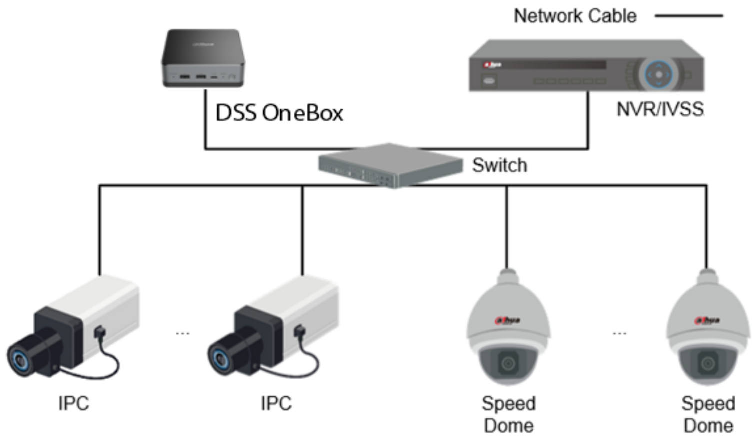
Configure face recognition settings on the device and the platform before you can view face recognition results on the platform.

8.3.1 Typical Topology

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

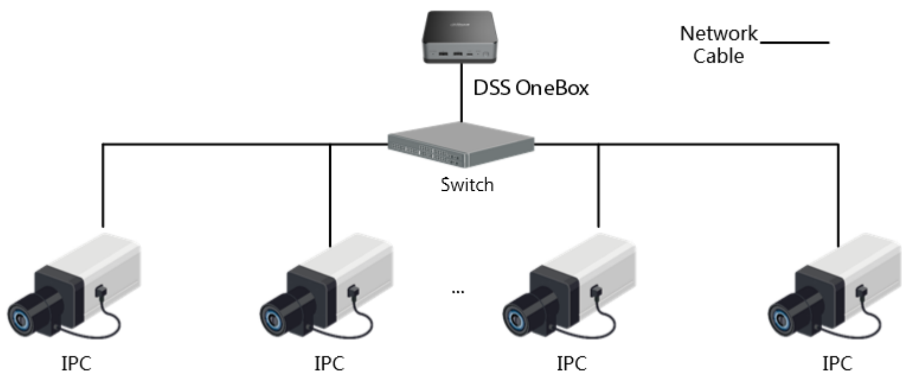
- Face recognition by NVR/IVSS

Figure 8-4 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 8-5 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.

8.3.2 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 "5 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.

8.3.3 Arming Faces

Before arming faces, you need to add the persons to the face arming group. For details, see "6.4.1 Face Arming List".

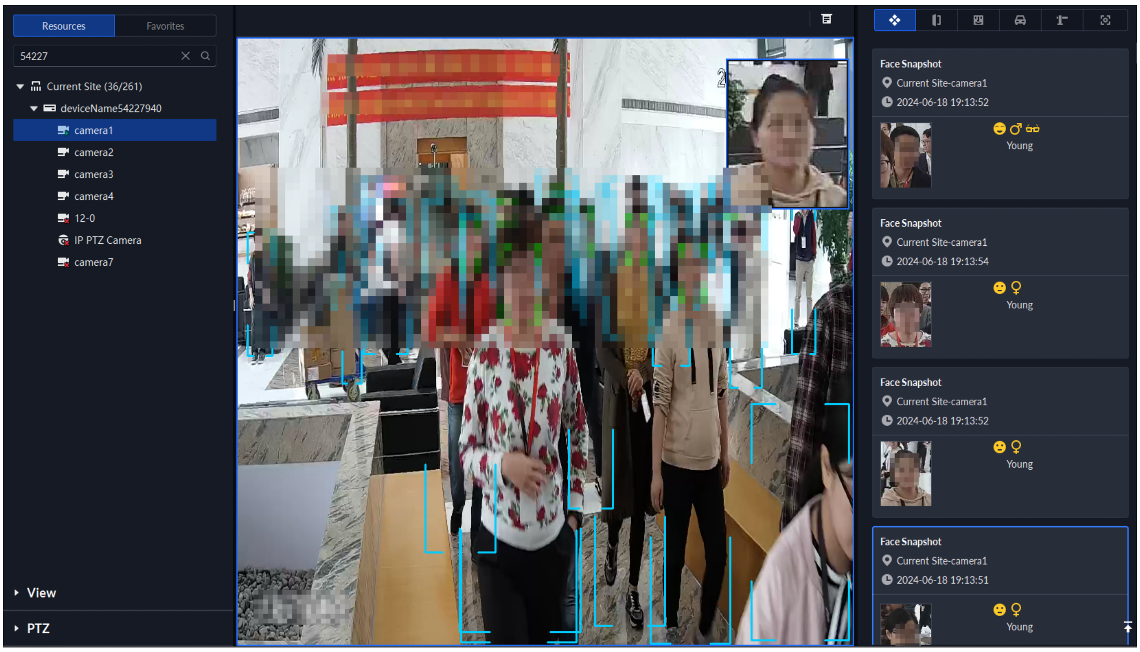
8.3.4 Live Face Recognition

Procedure

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

Step 2 Select a window, double-click the channel or drag the channel to the window.

Figure 8-6 Live view



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

Step 4 View live video.

- Click an event record to view event snapshots. You can play back the video of the event. Different events support different operations.

- : Add the person to the platform or add the person to an arming group. After you send the arming group to devices and configure an event, devices can trigger alarms when the face is recognized.
- When playing back video, click to download the video to designated path.
- Click to play back the video before and after the snapshot.
- Click to refresh events; click to pause refreshing.
- Click to delete event information.
- Click to view the most recent events.

8.3.5 Searching for Face Snapshots

Search for face snapshots by setting search criteria or uploading images.

Procedure

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

Step 2 Click **Integrated Retrieval**.

Step 3 Configure the search conditions.

You can search for snapshots in the **Record** or **Person** section. For details, see "7.3.1 Searching for People".

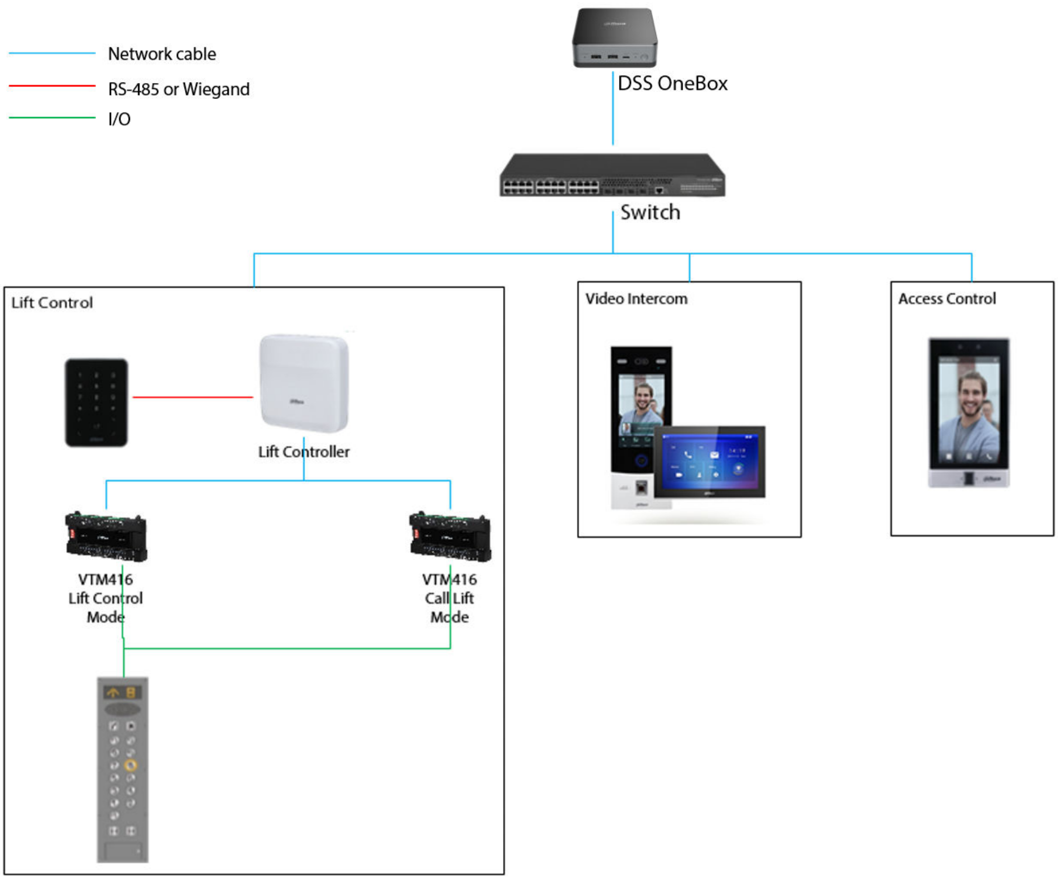
8.4 Lift Control

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 DSS Agile VDP App, the visitor can reach the floor where the homeowner is located.
  - ◇ After receiving the lift call, the platform administrator grants permissions of the specified floor to the visitor, who can then go to that floor.

8.4.1 Typical Topology

Figure 8-7 Typical topology



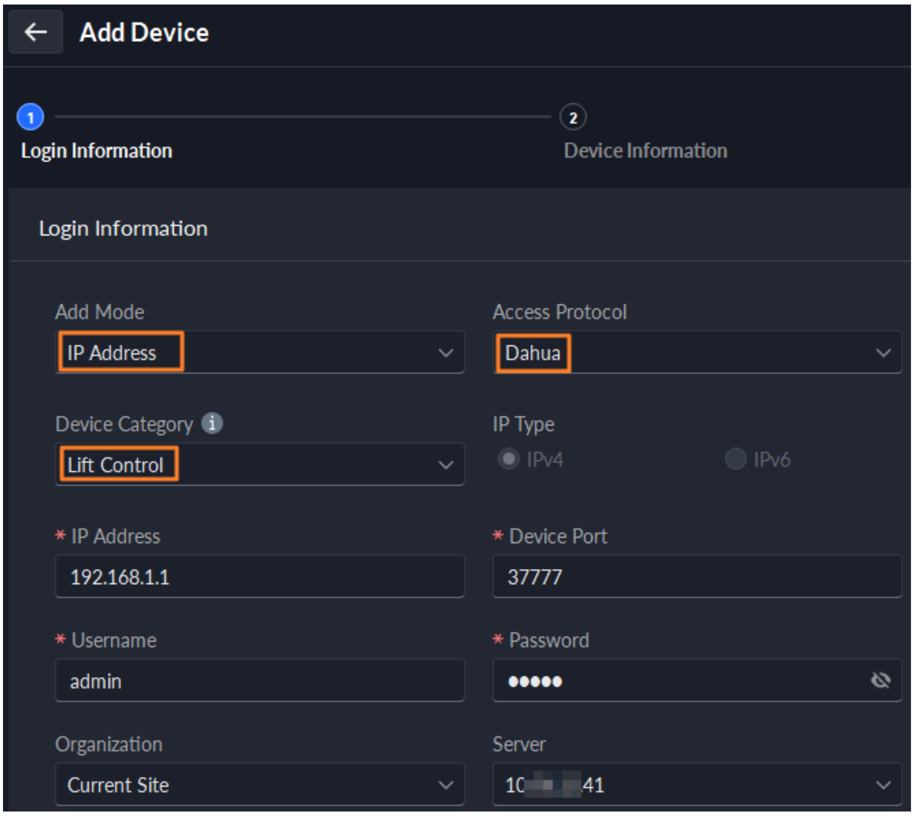
- Lift control module and lift controller: Installed on top of the elevator car or at the top of the hoistway. Connect the lift control modules to the lift controller, to manage the running of the lift.
- Card reader: Connect it to the lift controller through RS-485 or Wiegand, and supports card swiping, 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.

8.4.2 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**,

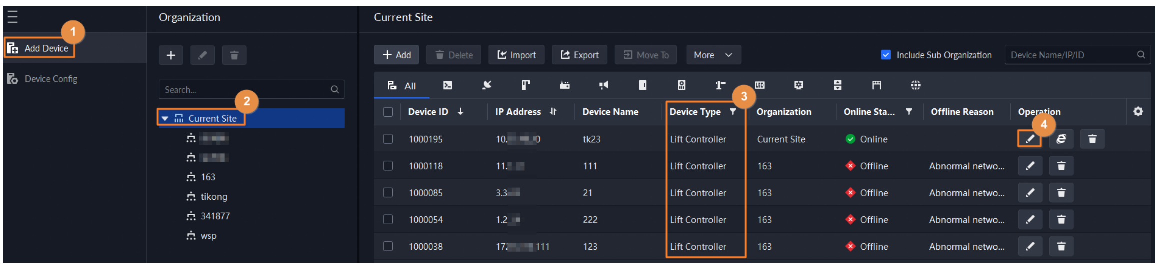
Figure 8-8 Add lift controller



◇ 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 8-9 Edit floor



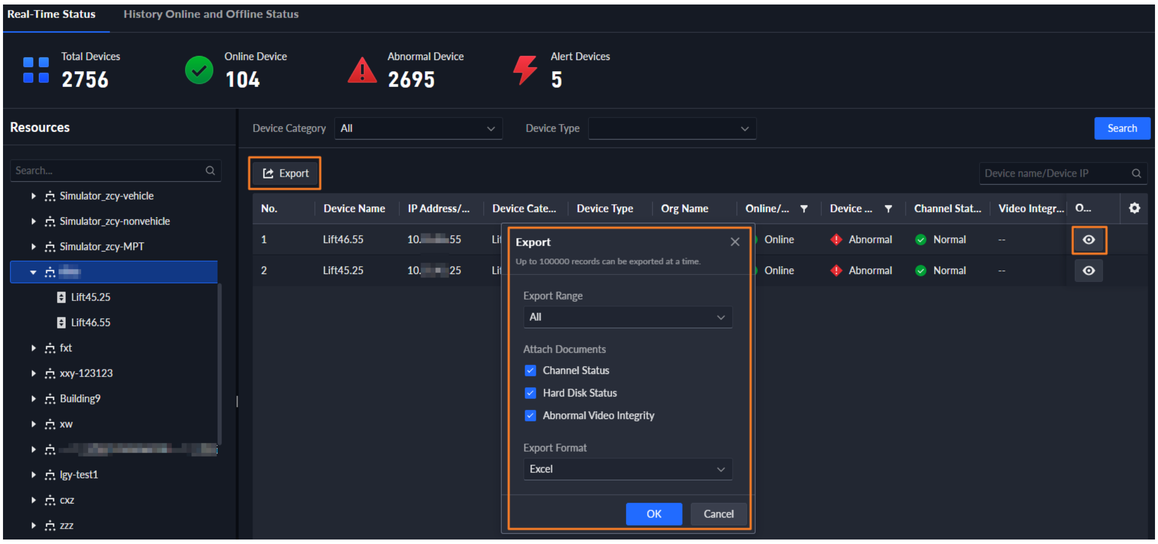
8.4.3 Viewing Lift Controller Status

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 8-10 View device status



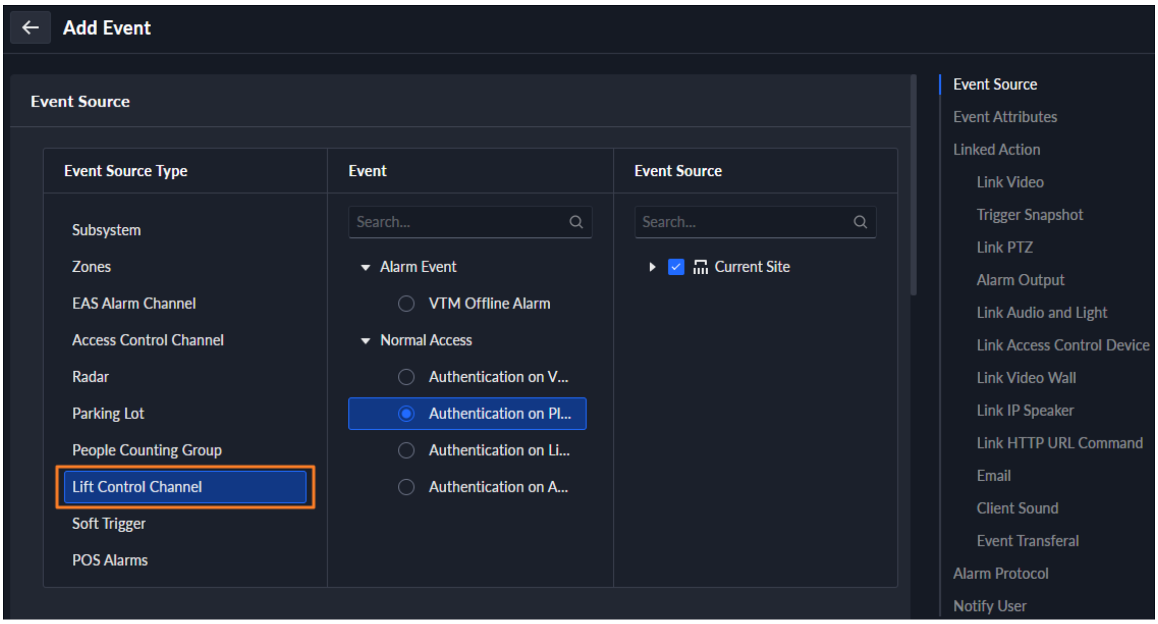
8.4.4 Configuring Event

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 "6.1.1 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 8-11 Select lift control



8.4.5 Authorized Access

8.4.5.1 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 DSS Agile VDP account for the person. If a visitor comes, the person can remotely authorize the visitor on DSS Agile VDP, so that the visitor can access the floor where the person is located.

For details of adding people, see "6.3.2.2 Adding a Person".

8.4.5.2 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 8-12 Add an access rule

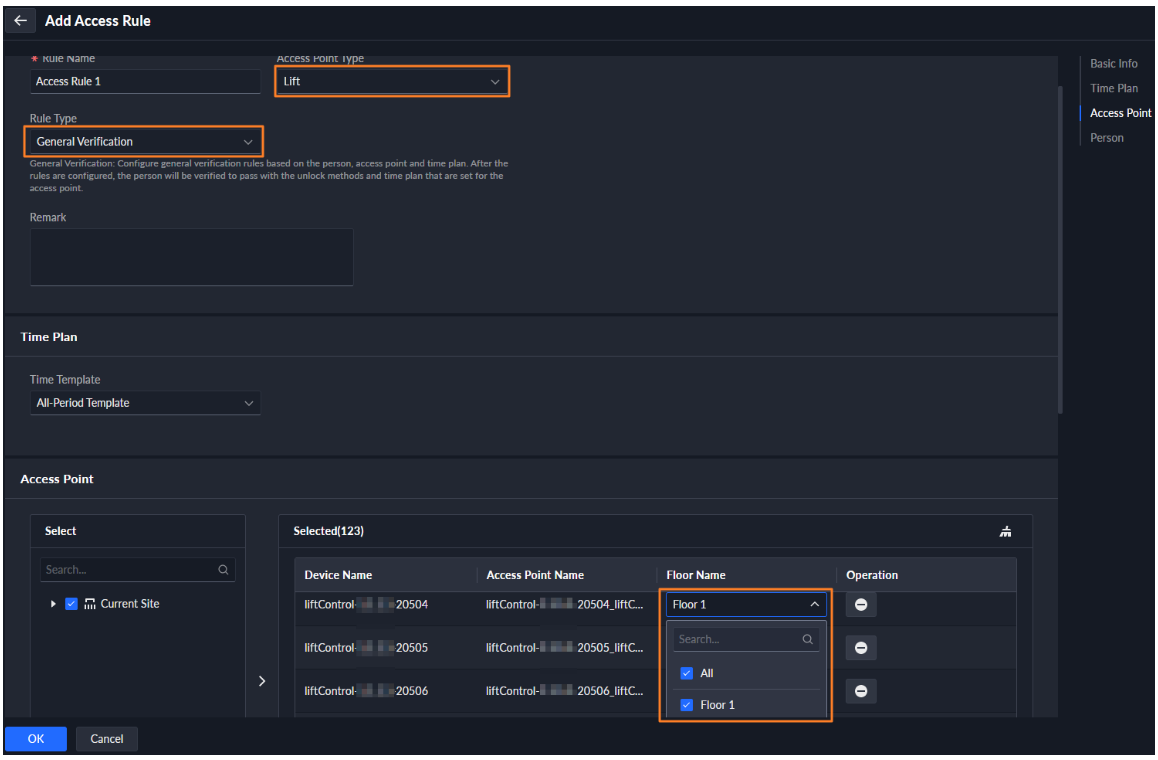


Table 8-1 Parameter description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Rule Name</td><td>Enter a name for the rule.</td></tr>
<tr><td>Access Point Type</td><td>Select Lift, and then the platform will only display corresponding channels.</td></tr>
<tr><td>Rule Type</td><td>Select General Verification.</td></tr>
<tr><td>Time Template</td><td>Select when this rule is effective. If you want to create a new time template, see "5.1.5 Adding Time Template".</td></tr>
<tr><td>Access Point</td><td>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.</td></tr>
<tr><td>Person</td><td>

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.

</td></tr>
</table>

Step 3 Click **OK**.

8.4.5.3 Controlling Lift Control Channels

Set all lift channels in a zone to no authentication, authentication, and lock modes. Only administrators can control lift channels globally.

Step 1 Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Access Control** > **Access Control Panel**.

Step 2 Select a zone, and then click **Authentication Mode**, and then people must verify their identifications to go to specified floors.

When selecting **No Authentication Mode** , all people can go to any floor without verifying their identifications; when selecting **Lock Mode**, no person is allowed to use lifts.

8.4.5.4 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.

8.4.6 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 "8.4.5.1 Adding a Person".

Step 2 Configure the access rules for the visitor. For details, see "8.4.5.2 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 8-2 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. For details, see "6.6.2 Call Management".

Results

After the visitor calls the lift on VTO:

- After the homeowner remotely agrees the access on VTH or DSS Agile VDP app, the visitor can reach the floor where the homeowner is.
- The platform administrator grants the designated floor permissions of the homeowner to the visitor on the platform, and then the visitor can reach the floor where the homeowner is.

8.4.7 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 "9.2.1 Configuring Security Parameters".

9 System Configurations

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

9.1 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.

9.2 System Parameters

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

9.2.1 Configuring Security Parameters

Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameter** > **Security Parameter**, and then configure the parameters.

Table 9-1 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. ● 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.

Parameter	Description
File Security Policies	Protect your data by verifying login password when download or export information, and encrypting the export files. ● **File Export or Download Password Authentication** : ◇ You need to enter the password of the current account to export or download files. ◇ For all users that log in to the platform, they do not need to enter the password when exporting or downloading files. ● **File Export and Download Encryption** : You need to set an encryption password for files to be exported or downloaded. When anyone uses the files, they need to verify the encryption password.
HTTP Allowlist	After the firewall 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 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.

9.2.2 Configuring Retention Period of System Data

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

Procedure

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

Step 2 Click **Message Retention Period**.

Step 3 Double-click a number to change its value.

Step 4 Click **Save**.

9.2.3 Time Synchronization

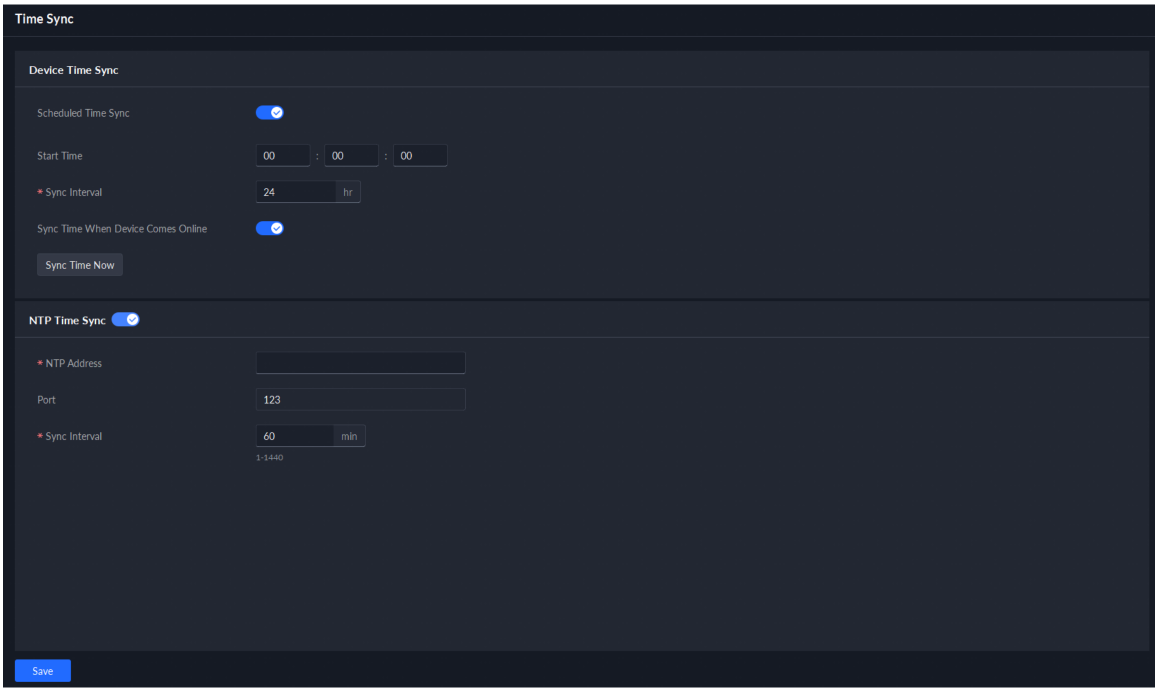
Synchronize the system time of all connected devices, PC client, and the platform. Otherwise the system might malfunction. For example, video search might fail. The platform supports synchronizing the time of multiple devices, which have the same time zone as the platform. You can synchronize the time 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 9-1 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.

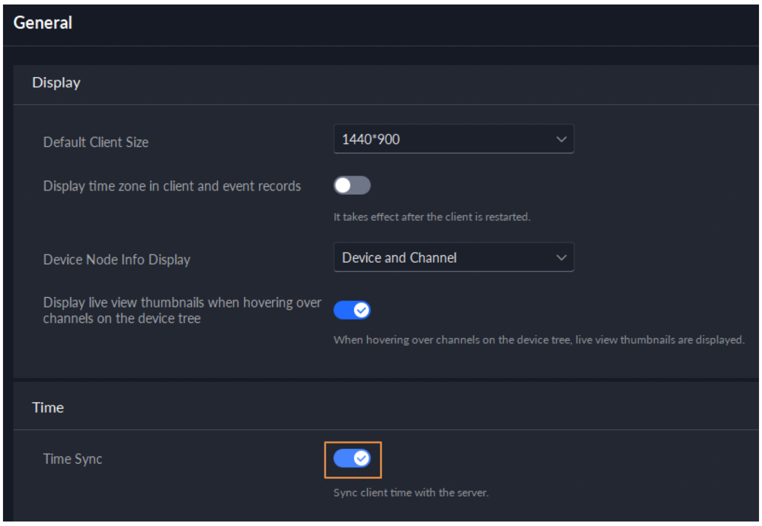
Step 3 Click **Save**.

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 platform and the PC client the same.

Figure 9-2 Enable time sync



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

9.2.4 Configuring Email Server

Procedure

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

Step 2 Click the **Email Server** tab, enable **Email Server**, and then configure parameters as required.

Table 9-2 Description of email server parameters

Parameter	Description
SMTP Server Type	Select according to the type of SMTP server to be connected. The types include **Yahoo** , **Gmail**, **Hotmail**, and **UserDefined**.
Sender Email Address	The sender displayed when an email is sent from DSS.
SMTP Server	IP address, password, and port number of the SMTP server.
Password	
Port	
Encryption Method	Supports no encryption, TLS encryption, and SSL encryption.
Test Recipient	Set the recipient, and then click **Email Test** to test whether the mailbox is available.
Email Test	

Step 3 Click **Save**.

9.2.5 Configure Device Access Parameters

To ensure that you can safely use the devices, we recommend using the security mode if devices support this mode to avoid security risks. The platform also supports enabling and disabling adding devices through P2P.

Procedure

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

Step 2 Select a device login mode, and then click **Save**.

Step 3 Enable or disable the P2P function.

If disabled, you cannot add devices to the platform through P2P.

9.2.6 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

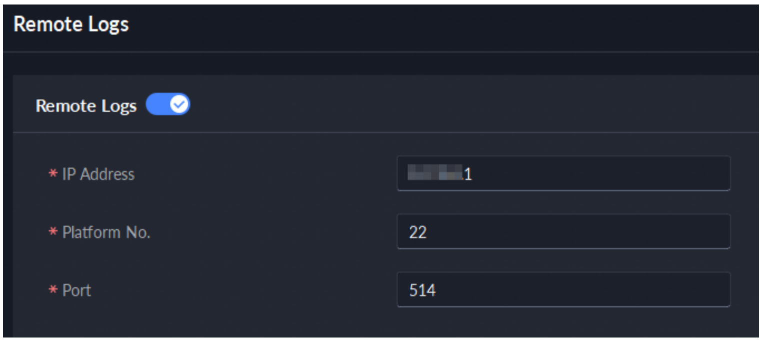
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.

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 9-3 Enable remote logs



Step 4 Click **Save**.

9.2.7 Configuring Mobile App

You can enable push notifications if you need to send messages to the app. In addition, when there is no fixed public IP or domain for the platform, you can enable easy linkage to use basic functions of the platform on the app.

Procedure

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

Step 2 (Optional) Enable or disable push notification.

If disabled, the app will not receive any offline push notifications, such as offline alarms and offline calls.

Step 3 (Optional) Enable or disable easy linkage.

- When there is no fixed public IP or domain for the platform, you can enable the easy linkage function, so that you can access the platform on the app using the public network, and perform basic operations such as login, subscribing to alarms, viewing live videos, playing back recordings, and viewing alarm images.

  In easy linkage mode, you will not be able to use video intercom on the app, and the video stream might not be stable.

  1. Scan the QR code corresponding to **Download App** to download the app.
  2. Use the app to scan the QR code corresponding to **Easy Linkage**, and then enter the username and password to log in to the app.
- When easy linkage is disabled, make sure that the network of the platform and the app can be connected; otherwise the app cannot log in successfully.
  1. Scan the QR code corresponding to **Download App** to download the app.
  2. 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 username and password.

9.2.8 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.

9.3 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.

9.3.1 System Backup

Use the data backup function to ensure the security of user information. Data can be manually or automatically backed up.

- Manual backup: Manually back up the data, and the DSS platform will save it locally.
- Automatic backup: The DSS platform automatically backs up the data at a defined time, and saves it to the installation path of the platform.

Procedure

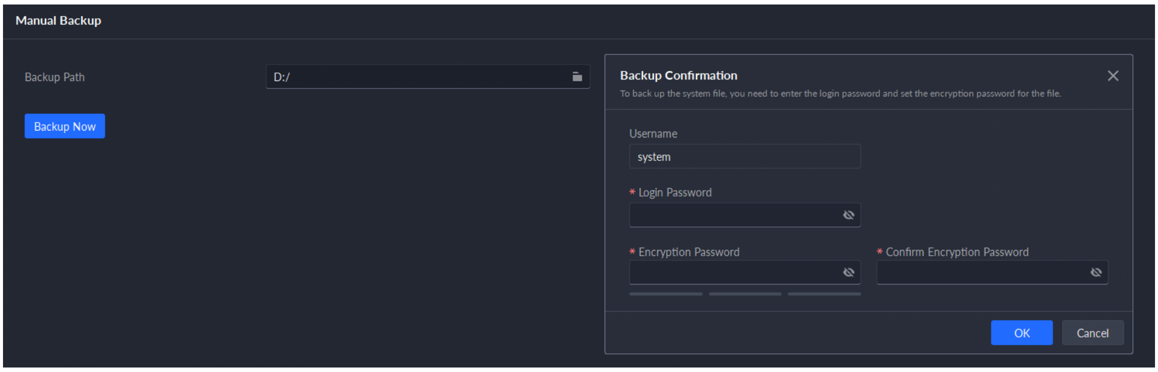
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **Backup and Restore**.

Step 2 Click the **Backup** tab.

Step 3 Back up data.

- Manual backup: In the **Manual Backup** section, select the data saving path, click **Backup Now**. The **Login Password** is the same as the system user's. Create an **Encryption Password** to protect data.

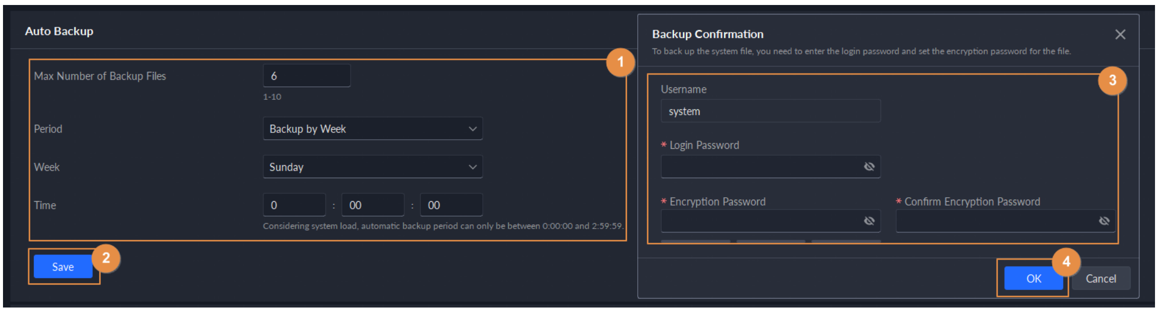
Figure 9-4 Manual backup



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

Max Number of Backup Files means you can only save defined number of backup files in the backup path.

Figure 9-5 Auto backup



9.3.2 System Restore

Restore the data of the most recent backup when the database becomes abnormal. It can quickly restore your DSS system and reduce loss.

- Local Restore: Import the backup file locally.

- Server Restore: Select the backup file from the platform.

⚠

- Users must not use the platform when you are restoring the configurations.
- Restoring the configurations will change the data on the platform. Please be advised.

Procedure

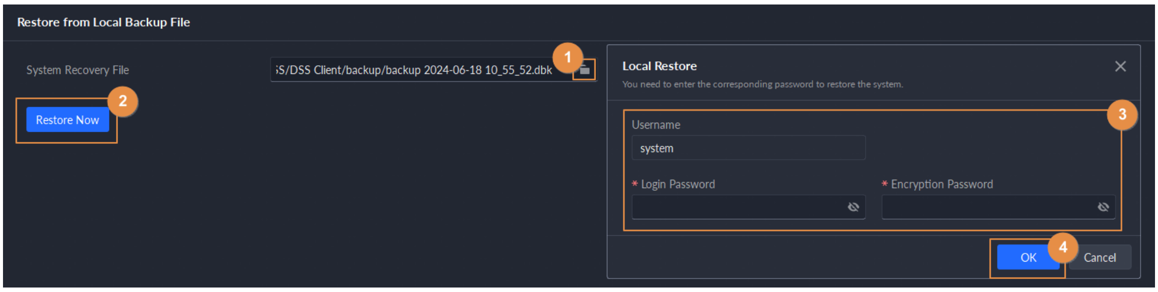
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **Backup and Restore**.

Step 2 Click the **Restore** tab.

Step 3 Restore data.

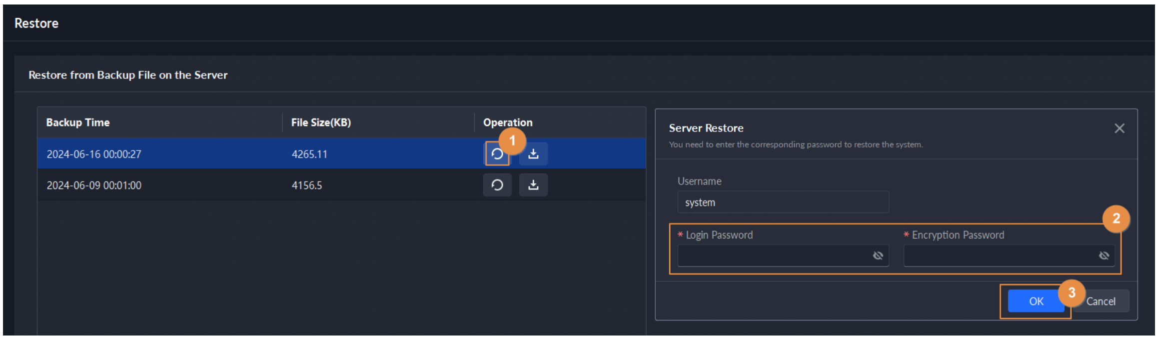
- Restore from local backup file: In the **Restore from Local Backup File** section, select the backup file path, click **Restore Now**, and then enter the passwords (the **Password** is the same as the system user's. The **Encryption Password** is the one created when the file was backed up).

Figure 9-6 Local restore



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

Figure 9-7 Restore from backup files on the server



You can click to download the backup file.

10 Management

10.1 Download Center

You can download videos stored on the platform or the device. They can be saved in are in .dav (default), .avi, .mp4, or .asf formats. For H.265 videos, they can only be saved in .dav formats. To download a video, you can:

- Select a duration on the timeline.
- Download videos by files. The system will generate files every 30 minutes from the time the video starts. If the video does not start on the hour or the half hour, the first file will start from the earliest start time to the half hour or the hour. For example, if a video starts from 4:15, the first file will be from 4:15 to 4:30.
- Download a period before and after a tag.

The maximum size of a video file is 1024 MB by default. You can change it to control how many files will be generated when you download a video by timeline or tag. For details, see "10.4.5 Configure File Storage Settings".

10.1.1 By Timeline or File

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Download Center** > **Download Video**.

Step 2 Configure the search conditions, and then click **Search**.

Step 3 Download videos.

By default, you need to verify your password and configure an encryption password before download. You can configure whether to verify the password. For details, see "9.2.1 Configuring Security Parameters".

- Download a video by selecting a duration on the timeline.

  If you set the **Search Type of Device Video Stream** to **Main Stream and Sub Stream 1**, you can download videos recorded in main stream or sub stream for videos stored on devices. For details, see "10.4.2 Configuring Video Settings".

  1. Click the **Timeline** tab, and then select a period on the timeline.
  2. On the pop-up page, adjust the length of the video.
  3. (Optional) Click to select a format of the video. If this function is not enabled, the video will be saved in .dav format by default.
  4. Click **OK**.
- Download a video by file.

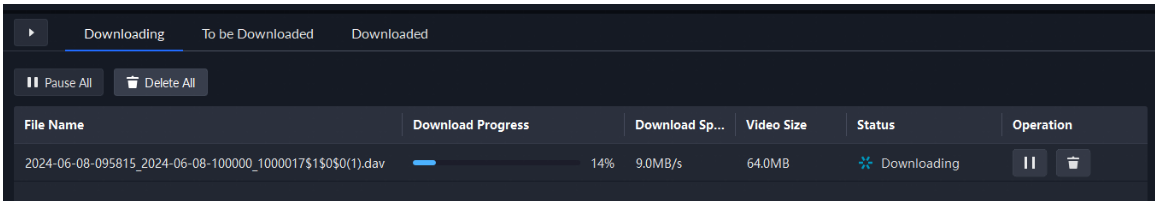
  Click the **File** tab, and then click to download a file.

  You can also select multiple files, and then click **Download Selected File** on the upper-left corner to download them at the same time.

Related Operations

- You can pause, resume, and delete a download task.

Figure 10-1 Download progress



- After download completes, click **Open Folder** to go to the path where the video is saved to, or click **Open** in the prompt on the upper-right corner to play the video directly in **Local Video**. For details, see "10.3 Playing Local Videos".

10.1.2 By Tagging Record

Search for tagging records on the platform and download relevant videos.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Download Center** > **Tagging Records**.

Step 2 Configure the search conditions, and then click **Search**.

Table 10-1 Parameter description

Parameter	Description
Select Channels	Select one or more channels to search for tags from. ● **Unlimited** : The platform will search all channels. ● : Manually select channels.
Time	Configure the time to search for tags within it.

Step 3 Click to download one video at a time, or select more tags, and then click **Download Selected Tagged File** to download multiple videos at the same time.

Step 4 Verify the login password and configure the encryption password, and then click **OK**.

By default, you need to verify your password and configure an encryption password before download. You can configure whether to verify the password. For details, see "9.2.1 Configuring Security Parameters".

Step 5 Configure the length of the video, whether you want to convert the video format, and then click **OK**.

Related Operations

Click to delete a tag, or select more tags, and then click **Download Selected Tagged File** to delete them in batches. This operation will only delete the tags. It will not delete the videos.

10.2 Viewing Local Images

You can view snapshots taken by clicking on the video image from the monitoring center.

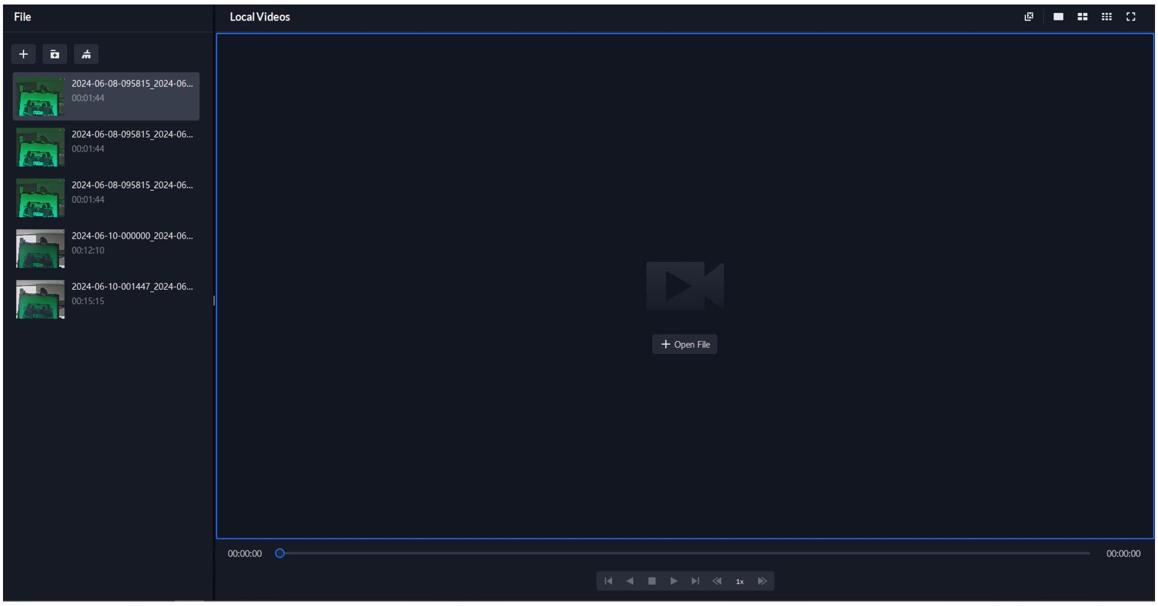
10.3 Playing Local Videos

You can play local videos directly on the platform.

Procedure

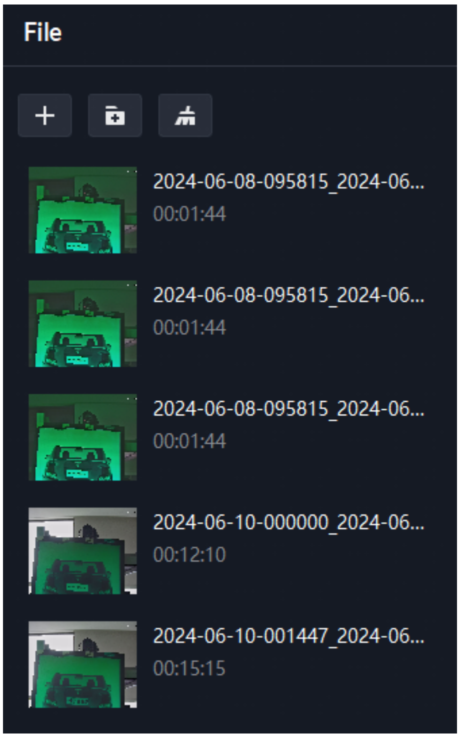
Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Video**.

Figure 10-2 Local video



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

Figure 10-3 Play list



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

Related Operations

Table 10-2 Interface operation

Icon/Function	Description
Right-click menu	● **Continuous Snapshot** : Take snapshots of the current image (2 snapshots each time by default). The snapshots are saved to *C:\DSS \DSS Client\Picture* by default. To change the snapshot saving path, see "10.4.5 Configure File Storage Settings". ● **Video Adjustment** : Adjust the brightness, contrast, saturation, and chroma of the video for video enhancement. ● **Digital Zoom** : Click and hold to select an area to zoom in on it. Double-click the image again to exit zooming in.  You can also scroll to zoom in and out.
	Close all playing videos.
	Split the window into multiple ones and play a video in full screen.
	Take a snapshot of the current image and save it locally. The path is C:\DSS \DSS Client\Picture\ by default.
	Close the window.
	Stop/pause the video.
	Fast/slow playback. Max. supports 64X or 1/64X.
	Frame by frame playback/frame by frame backward.
	Capture the target in the playback window. Click  to select the search method, and then the system goes to the page with search results. More operations: ● Move the selection area: Hover over the selection area, and then left-click to move. ● Adjust the size of the selection area: Hover over the upper-right, upper-left and lower-left corner of the selection area, and then left-click to adjust. ● Right-click to exit search by snapshot.

10.4 Configuring Local Settings

After logging in to the client for the first time, you need to configure the following fields under system parameters: Basic settings, video parameters, record playback, snapshot, recording, alarm, video wall, security settings and shortcut keys.

10.4.1 Configuring General Settings

Configure client language, client size, time, and more.

Procedure

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

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

Table 10-3 Parameter description

Parameters	Description
Default Client Size	The size of the client when it is not maximized. Select a proper resolution according to your screen.
Display time zone in client and event records	When selected, the client and the time of alarms will show both the time and time zone.
Device Node Info Display	Select that the device tree displays devices and their channels or only channels.
Display live view thumbnails when hovering over channels on the device tree	When selected, you can hover the mouse over a channel in the device tree in **Monitoring Center** and a snapshot of its live video image will be displayed.
Time Sync	If enabled, the client starts to synchronize network time with the platform to complete time synchronization.
Auto run at startup	● If **Remember Password** has been selected on the **Login** page, select **Auto restart after reboot**, and the system will skip the login page and directly open the homepage after you restart the PC next time. ● If **Remember Password** is not selected on the **Login** page, select **Auto restart after reboot**, the client login page will appear after you restart the PC.
Auto Login	Enable the system to skip the login page and directly open the homepage when logging in next time. ● If **Remember Password** and **Auto Login** have been selected on the **Login** page, the function is already enabled. ● If **Remember Password** has been selected while **Auto Login** is not selected on the **Login** page, select **Auto Login** on the **Basic** page to enable this function. ● If neither **Remember Password** nor **Auto Login** has been selected on the **Login** page, select **Auto Login** on the **Basic** page and you then to enter the password when logging in next time to enable the function.
CPU Alarm Threshold	The user will be asked to confirm whether to open one more video when the CPU usage exceeds the defined threshold.
Audio and video transmission encryption	Encrypt all audio and video to ensure information security.
Client Inactive Status Config	If no operation is performed for the defined period, the client will be automatically locked or logged out. If you are logged out, all the tasks on the client will be suspended.
Self-adaptive audio talk parameters	If enabled, the system automatically adapts to the device sampling frequency, sampling bit, and audio format for audio talk.

Parameters	Description
Access Card Input and Display Mode	Select a mode for the platform to use and display access cards. For example, when you manually issue a card to a person, you can enter A-F and numbers in the card number if **Hex** is selected, but you can only enter 0-9 if **Decimal** is selected.
Joystick Sensitivity	Select the sensitivity for when you operate the joystick. The higher the sensitivity, the more frequent joystick commands are sent, and the greater the possibility that operations will be delayed due to poor performance of PTZ cameras.
Use Thousand Separator	Configure a separator for thousands. This will apply to all numbers on the PC client.
Decimal Separator	Select a separator for decimals. This will apply to all numbers on the PC client.

Step 3 Click **Save**.

10.4.2 Configuring Video Settings

Configure window split, display mode, stream type and play mode of live view, and instant playback length.

Procedure

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

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

Table 10-4 Parameter description

Parameters	Description
Default Window Split	Set split mode of the video window.
Window Display Scale	Select from **Original Scale** and **Full Screen**.
Stream Acquisition Mode	When the device and clients are properly connected to the network, direct acquisition can reduce the use of the platform's forwarding bandwidth. If too many clients are acquiring video streams from a channel, acquisition might fail due to insufficient performance of the device. At this time, video streams can be set to be forwarded to clients by the platform. ● **Streaming Service Forwarding**: Video streams will be forwarded to clients by the platform. ● **Acquire directly from the device**: Clients will acquire video streams directly from the channel. If direct acquisition fails, the platform will forward the video streams to clients.

Parameters	Description
Decoding Mode CPU Threshold	• **Software Decoding by CPU** : All videos will be decoded by the CPU. When you are viewing live videos from large amount of channels, it will take up too much resources of the CPU that affects other functions. • **Hardware Decoding by GPU** (default): All videos will be decoded by the GPU. The GPU is better at concurrent operation than the CPU. This configuration will free up resources of the CPU significantly. • **Performance Mode (CPU First)** : All videos will be decoded by the CPU first. When selecting this mode, you need to set the CPU threshold. When the resources of the CPU are taken up to the defined threshold, the platform will use the GPU to decode videos.
Video Toolbar Icon Size	Set the icon size on the toolbar when viewing real-time and recorded videos.
AI Rule Overlay	After turning it on, when viewing live video or playing recordings, right-click the video window, the **AI Overlay** and **SMD Overlay** menu will be displayed. If you turn it off, these menus, the icon on the live view and playback pages, and the overlaid information on the video image will not be displayed.
Close videos being played after long period of inactivity Inactivity Time	The system closes live view or playback automatically after inactivity for a pre-defined period of time. Supports up to 30 minutes.
Stream Switching Rule	When the number of window splits is greater than the defined value, the live video will switch from the main stream type to sub stream type.
Switches to Main Stream when Window Maximized	If selected, you can double-click a video window to maximize it and switch from sub stream to main stream. Double-click again to restore the window size, and then the system will switch it back to sub stream.
Display the previous live view after restart	If selected, the system displays the last live view automatically after you restart the client.

Parameters	Description
Play Mode	When playing videos, both fluency and real-time performance matter. To deal with network fluctuations, the platform has a set of buffer control strategies to ensure fluency and real-time performance. You can select one of the following play modes as needed. ● **Real-time Play Priority** : The system might lower the image quality to avoid video lag. It is suitable for special scenarios with high requirements on real-time performance. ● **Fluency Priority** : The system might lower the image quality and allow for lag to ensure video fluency. The higher the image quality is, the lower the video fluency will be. ● **Balance Priority** (recommended): The system balances real-time priority and fluency priority according to the actual server and network performance. ● **Custom** : The system adjusts video buffering and lowers the impact on video quality caused by unstable network. The bigger the value, the more stable the video quality will be.
Display Recording Status	You can select displaying or not displaying an icon on the upper-left corner of the window when recording is performed.
Enable Multicast	Enable this function and configure the multicast parameters for video channels. When multiple PC clients want to view the real-time video from the same channel, the video will be sent to the clients through the router. This will reduce the bandwidth usage of the platform.
Instant Playback Time	Click on the live view page to play the video of the previous period. The period can be user-defined. For example, if you set 30 seconds, the system will play the video of the previous 30 seconds.
Search Type of Device Video Stream	Select a default stream type when you play back recordings from a device. If **Only Sub Stream 2** is selected, but the device does not support sub stream 2, then recordings of sub stream 1 will be played.
Frame Extraction Mode	Frame extraction helps ensure that the video runs smoothly and the pressure on decoding, bandwidth and forwarding is minimal when playing high-definition videos. When frame extraction is enabled, certain frames will be skipped. ● **Do Not Extract** : Frame extraction will not be enabled in any situation. ● **Self-adaptive** : The platform will enable frame extraction based on the resolution and the play speed. ● **By Split Window** : Some frames will be extracted when the number of split windows is greater than the defined split windows. No frames will be extracted when the window is maximized. ● **Force** : Frame extraction is always enabled.

Parameters	Description
Continuous Snapshot Interval	Set the number of snapshots and the interval between each one. For example, if the **Continuous Snapshot Interval** is 10 seconds and the **Number of Continuous Snapshots** is 4, when you right-click on the live or recorded video and select **Snapshot**, 4 snapshots will be taken every 10 seconds.
Number of Continuous Snapshots	

Step 3 Click **Save**.

10.4.3 Configuring Video Wall Settings

Configure the default binding mode and stream type of video wall.

Procedure

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

Step 2 Click **Video Wall**, and then configure the parameters.

Table 10-5 Parameter description

Parameter	Description
Default Stream Type	Select **Main Stream** , **Sub Stream 1**, **Sub Stream 2** or **Local Signal** as the default stream type for video wall display.
Stream Switching Rule	When the number of window splits is greater than the defined value, the live video will switch from the main stream type to sub stream type.
Double-click on the video to maximize the window and switch to main stream	Double-click the video to maximize the window, and then its stream type will switch to main stream.
Video Source Play Duration	Set the default time interval between the channels for tour display. For example, if 5 seconds is configured and you are touring 3 video channels, the live video image of each channel will be played 5 seconds before switching to the next channel.
Mode of Video Decoding to Wall	● **Tour** : Multiple video channels switch to decode in one window by default. ● **Tile** : Video channels are displayed in the windows by tile by default. ● **Ask Every Time** : When dragging a channel to the window, the system will ask you to select tour or tile mode.

Step 3 Click **Save**.

10.4.4 Configuring Alarm Settings

Configure the alarm sound and alarm display method on the client.

Procedure

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

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

- Alarm sound

Table 10-6 Alarm sound parameter description

Parameter	Description
Custom	◇ **Default** : All types of alarms will use the same default alarm sound when triggered. ◇ **Custom** : Click **Modify Alarm Sound**, and then you can change the alarm sound and its play mode of each type of alarm. ◇ **Play Audio Defined in Scheme** : When an alarm is triggered, the platform plays the sound defined in > **Event** > **Event Config**. For details, see "6.1.1 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 10-7 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 "6.1 Configuring Events".

Parameter	Description
Open Alarm Linkage Video	Configure how the platform plays the video when an alarm is triggered. ◇ **As Pop-up** : The alarm video will be played in a pop-up window. You can set how long the pop-up windows will be displayed, whether to display the pop-up windows and the client on the top of the screen, and link video only or link video and map. ○ Link Video: When an alarm is triggered, you can view the real-time video of the alarm channel in the pop-up window. ○ Link Video and Map: When an alarm is triggered, you can click the **Video** or **Map** tab to switch viewing the real-time video or the map information. ◇ **Open in Live View** : The alarm video will be played in a window in **Monitoring Center**. You can set how long the video will play, and whether to open the monitoring menu when alarm is triggered (**Monitoring Center** > **Monitoring**). If **Open Monitoring Menu When Alarm is Triggered** is not enabled, when a channel set as an alarm window triggers an alarm, the platform will still open the monitoring menu and play the real-time video of that channel.

- Map flashes

Table 10-8 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**.

10.4.5 Configure File Storage Settings

Configure the storage path, naming rule, file size, and format of recordings and snapshots.

Procedure

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

Step 2 Click **File Storage**, and then configure the parameters.

Table 10-9 Parameter description

Parameters	Description
Video Naming Rule	Select a naming rule for manual recordings.
Video Storage Path	Set a storage path of manual recordings during live view or playback. The default path is C:\Users\Public\DSS Client\Record.

Parameters	Description
Video File Size	Configure the maximum size of a video file. If you download a video that is larger than the defined size, the platform will divide it into multiple files. The maximum size can be up to 4 GB for 32-bit operating systems, and 1024 GB for 64-bit operating systems.
Image Format	Select a format for snapshots.
Image Naming Rule	Select a naming rule for snapshots.
Image Storage Path	Set a storage path for snapshots. The default path is C:\Users\Public\DSS Client\Picture.

Step 3 Click **Save**.

10.4.6 Viewing Shortcut Keys

View shortcut keys for operating the client quickly.

Procedure

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

Step 2 Click **Shortcut Key** to view shortcut keys of the PC keyboard and USB joystick.

10.4.7 Exporting and Importing Configurations

For the parameters in local settings configured by the user currently logged in to the PC client, they can be exported and imported to another PC client. This is helpful that the user does not need to configure the parameters again when using a new platform.

Procedure

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

Step 2 Click **Export/Import Configurations** on the lower-right corner.

Step 3 Export or import configurations.

- Export configurations.

The parameters of **Alarm Sound** and **Map Flashes** will not be included in the exported configurations.

1. Click **Export Configurations**.
2. Select **Export to File**, and then export the configurations to the specified path of your computer. Or select **Send by Email**, and send the configurations to the specified email address.
3. Click **OK**.

- Import configurations.

1. Click , and then open the exported file of configurations.
2. Click **Import Configurations**.
3. Click **OK**.

10.5 Managing Logs

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

10.5.1 Operation Log

View and export logs that record users' operations, such as viewing the real-time video of a channel.

Procedure

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

Step 2 Select one or more types of logs.

Step 3 Specify the time and keywords, and then click **Search**.

Up to 1 month of logs can be searched for at a time.

Step 4 To export the logs, click **Export** and follow the on-screen instructions.

10.5.2 Device Log

View and export logs generated by devices.

Procedure

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

Step 2 Select a device and time, and then click **Search**.

Step 3 To export the logs, click **Export** and follow the on-screen instructions.

10.5.3 System Log

View and export logs on how the platform has been running, such as a system error.

Procedure

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

Step 2 Select a type of logs.

Step 3 Specify the time, and then click **Search**.

Up to 1 month of logs can be searched for at a time.

Step 4 (Optional) Click **Export** and follow the on-screen instructions.

10.5.4 Service Log

Services will generate logs when they are running. These logs can be used for troubleshooting. If you need even more detailed logs, enable the debug mode so that the platform will generate detailed logs.

Procedure

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Logs** > **Extract Service Logs**.

Step 2 Click to download the logs of the service within a specified period to your computer.

Step 3 (Optional) Click to enable the debug mode of a service, and then click to download the detailed logs within a specified period to your computer.

After the debug mode is enabled, the platform will generate a large amount of logs that occupy more disk space. We recommend you disable the debug mode after you have finished troubleshooting.

10.6 Help

Click **Help** to view the user manual of the platform.

10.7 Quick Commands

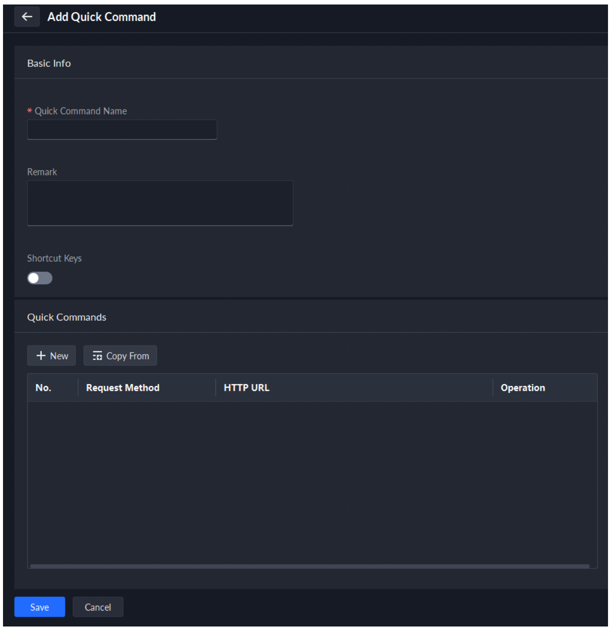
Customize HTTP commands and execute them quickly. Request methods of GET, POST, PUT and DELETE are supported.

Procedure

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

Step 2 Click **Config**, and then click **Add**.

Figure 10-4 Add a quick command



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

Table 10-10 Quick command parameter description

Parameter	Description
Quick Command Name	The name that identifies the quick command.
Remark	Remarks on the quick command.

Parameter	Description
Shortcut Keys	After enabling **Shortcut Keys**, you can set a single key or a combination of 2 keys as the shortcut key. The shortcut keys set here take effect globally on the client.
Enter Shortcut Keys	
Add	Click **Add** , and then select **New** or **Copy From** to add a new quick command, or copy from an existing quick command or event plan. When you select **New**, you need to set the request method (GET by default, and you can also select POST, PUT, and DELETE), and HTTP URL address. ● When selecting **POST** or **PUT**, you can click to customize the body of HTTP URL. ● Click in sequence to move up, move down, or delete the request. ● Up to 20 requests can be added to 1 quick command.
Execute in Order	● When it is enabled, the system will execute the quick command in order of the added requests, and the next request can be executed only after the previous request is successfully executed. ● When it is not enabled, the requests will be executed at the same time if multiple requests are added to 1 quick command.

Step 4 Press the defined shortcut keys or click to execute a quick command.

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