Micro Center Intelligent Server

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the "Intelligent micro center server" (hereinafter referred to as "the Device"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	December 2022

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.

- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

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

Transportation Requirements

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

Store the device under allowed humidity and temperature conditions.

Operation Requirements

WARNING

- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- The device is heavy and needs to be carried by several persons together to avoid personal injuries.

This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.

- Make sure that the power supply is correct before use.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drip or splash liquid onto the device, make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.
- Your configurations will be lost after performing a factory reset. Please be advised.
- Do not restart, shut down or disconnect the power to the device during an update.
- Make sure the update file is correct because an incorrect file can result in a device error occurring.
- The system cannot upgrade different types of AI modules at the same time.
- Do not frequently turn on/off the device. Otherwise, the product life might be shortened.
- Back up important data on a regular basis when using the device.
- Operating temperature: –10 °C to +55 °C (+14 °F to +131 °F).

Installation Requirements

WARNING

- Strictly comply with the local electrical safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not expose the battery to environments with extremely low air pressure, or extremely high or low temperatures. Also, it is strictly prohibited for the battery to be exposed to extremely hot

environments (such as direct sunlight or fire), and to cut or put mechanical pressure on the battery. This is to avoid the risk of fire and explosion.

- Use the standard power adapter. We will assume no responsibility for any problems caused by the use of a nonstandard power adapter.

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

Maintenance Requirements

- Make sure you use the same model when replacing the battery to avoid fire or explosion. Dispose the battery strictly following the instructions.
- Power off the device before maintenance.

- AI module does not support hot plug. If you need to install or replace the AI module, unplug the device power cord first. Otherwise, it will lead to file damage on the AI module.
- The device casing provides protection for internal components. Use a screwdriver to loosen the screws before detaching the casing. Make sure to put the casing back on and secure it in its original place before powering on and using the device.
- Clean the ventilation pipe regularly to avoid obstructions.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

Table of Contents

1 Product Overview

1.1 Product Introduction

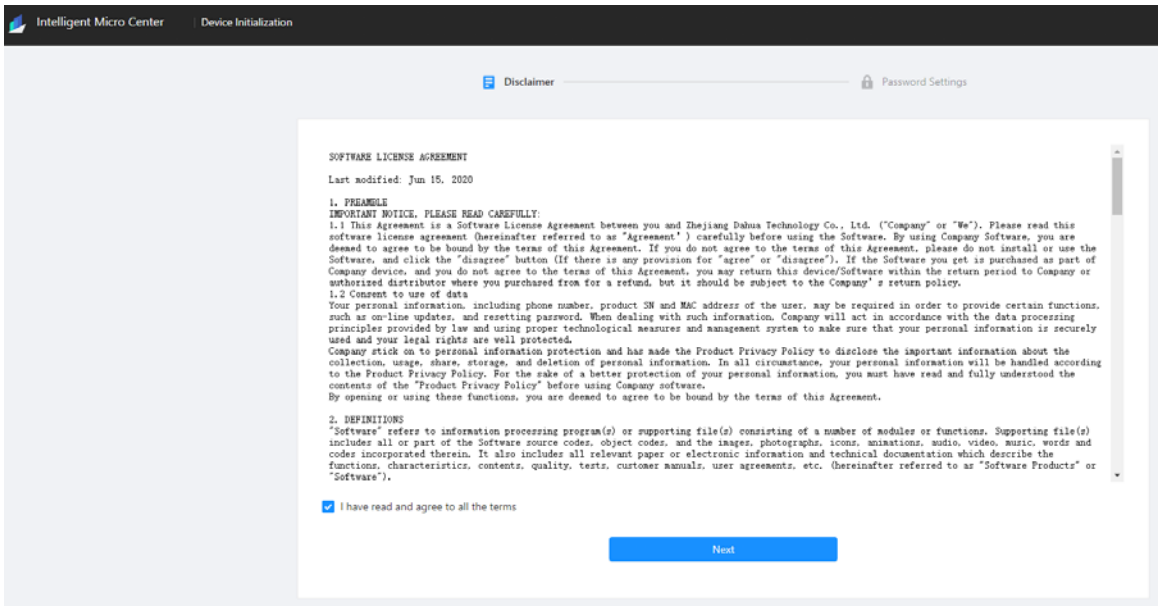
Micro Center Intelligent Server is a high-performance parsing and comparison device. It integrates AI computing chip, database, storage, web, and features abundant functions and high scalability. The server meets intelligent application needs of the various industry, such as finance and traffic. It offers functions, such as face detection, vehicle detection, human body detection, non-motor vehicle detection, face comparison, face arming and search by image. Supports multiple ways to connect to cameras and service platforms with flexibility and efficiency.

1.2 Initialization and Login

Step 1 Open the browser, and then enter "http://*server IP address*", for example, "http://192.168.1.113", and then press Enter.

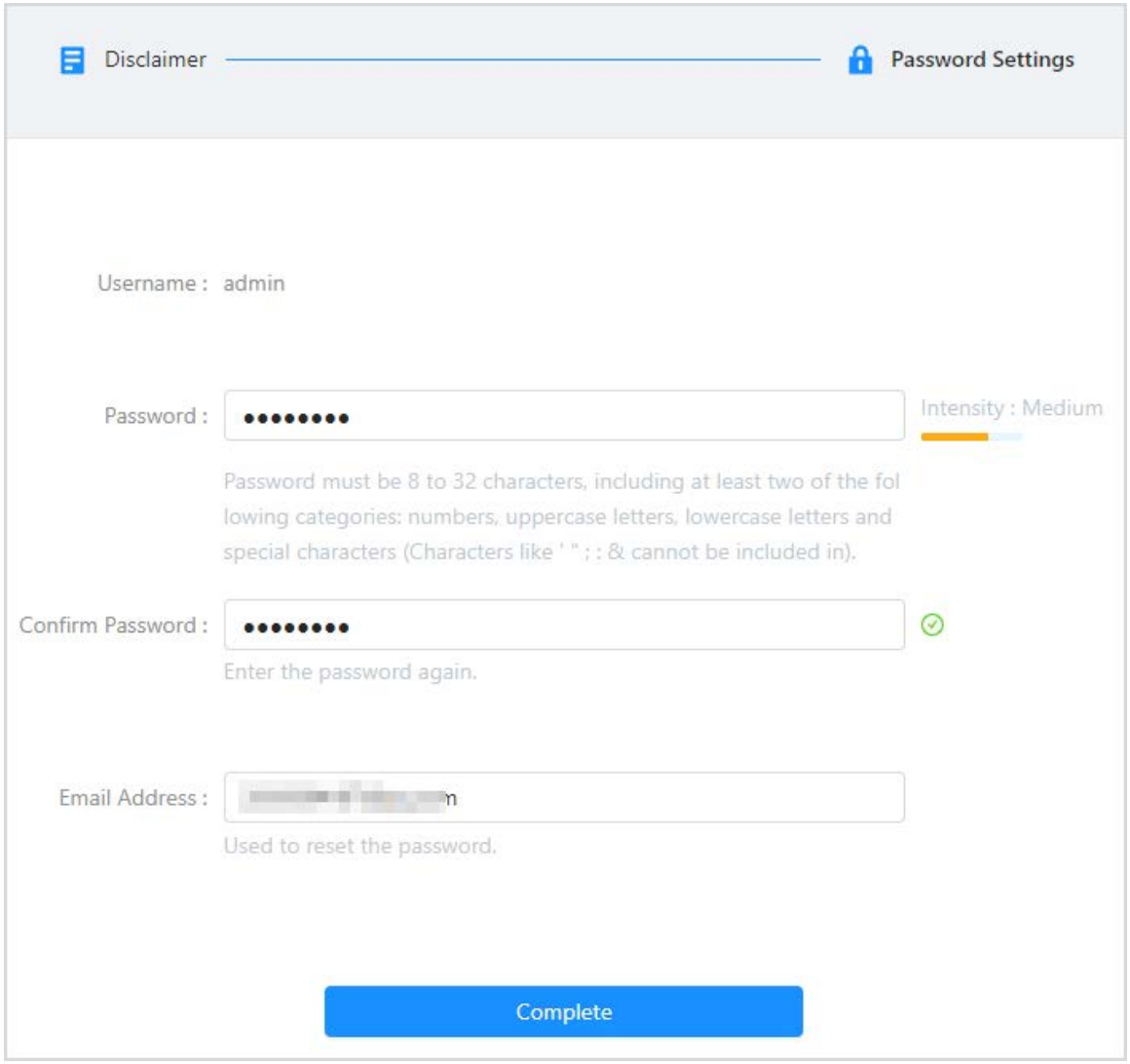
Step 2 Read the **Software License Agreement** and select **I have read and agree to all the terms**, and then click **Next**.

Figure 1-1 Initialization



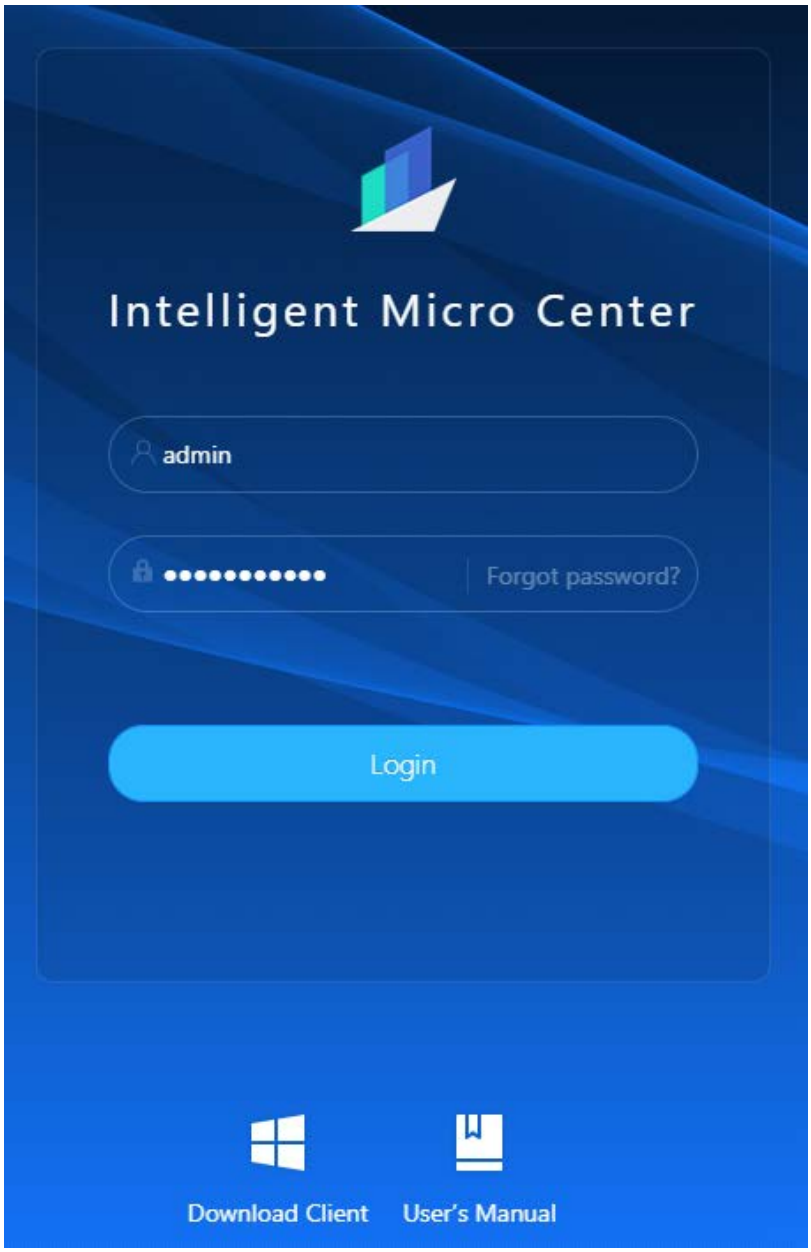
Step 3 Set and confirm the password, and then enter your email address, after that click **Complete.**

Figure 1-2 Set password



Step 4 Enter the username and password, and then click **Login** to log in to the webpage.

Figure 1-3 Login



- If you forget the password, click **Forgot password?** to reset password through the email.
- The four default IP of the server business ports are 192.168.1.113, 192.168.1.112, 192.168.1.110 and 192.168.1.109.
- Click **Download Client** to download client for live view.
- Click **User's Manual** to download user's manual.

2 Hardware Introduction

This chapter introduces the front panel and real panel of the server.

2.1 Front Panel

Figure 2-1 Front panel

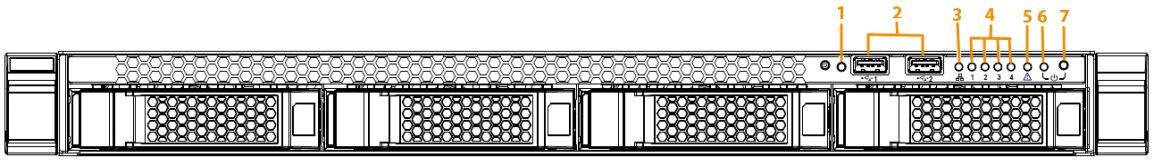


Table 2-1 Front panel description

No.	Description
1	UID switch and indicator
2	USB 3.0
3	BMC network status indicator
4	Business network status indicator
5	Alarm indicator
6	Running indicator
7	Power switch

2.2 Rear Panel

Figure 2-2 Rear panel

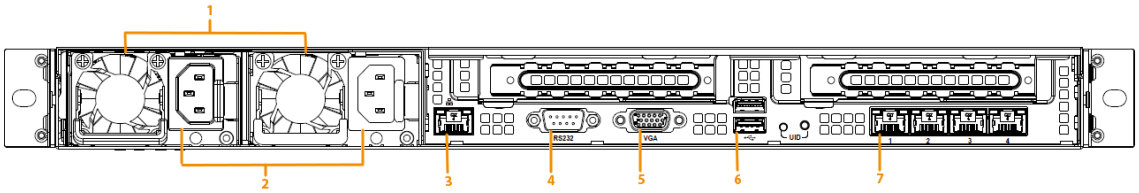


Table 2-2 Rear panel description

No.	Description
1	Fan
2	Power port
3	BMC management Ethernet port
4	Serial port
5	VGA port
6	USB 3.0

No.	Description
7	Business port

3 Functions Introduction

This chapter introduces parameters configuration of the server on the webpage.

Figure 3-1 Home page

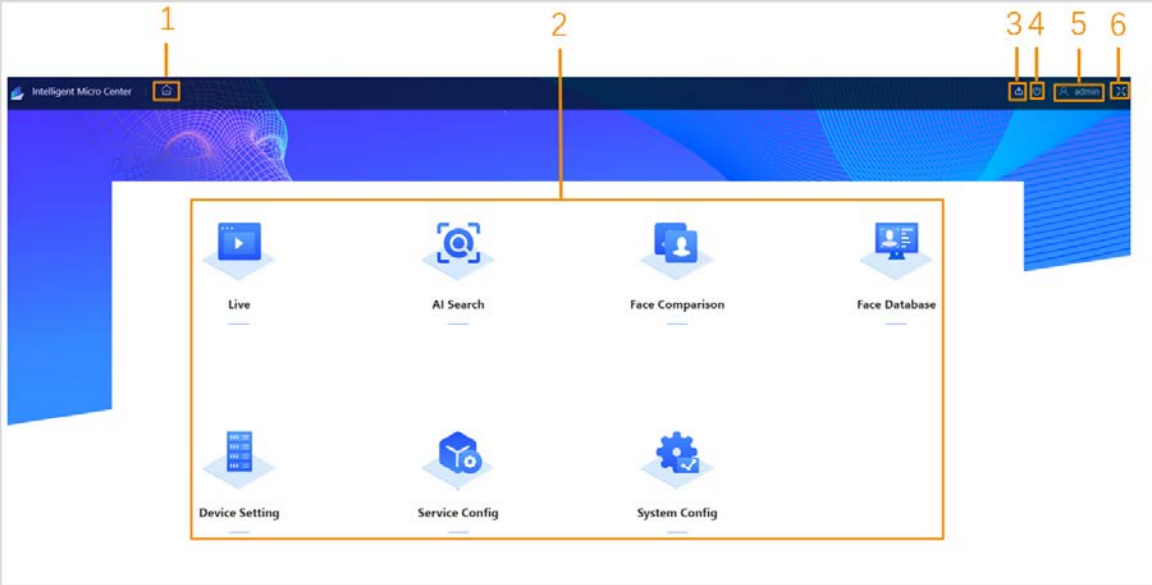


Table 3-1 Home page parameter description

No.	Parameter	Description
1	Home page	Display function modules.
2	Function menu	Click function menu to enter the operating interface.
3	Download center	Display the download progress and files.
4	Restart	Enter the password to restart the server.
5	User center	Click admin to enter the user center and the user center supports: • Change password: Click **Change Password** to set new password. • Logout: Click **Logout** to logout.
6	Screen display	Click to enter the full screen display mode. Click again or press Esc to exit full screen mode.

3.1 System Configuration

Configure the system parameters of the server, such as time, user management, network configuration, network authorization, basic configuration system installation and upgrading, logs, version information and legal information.

3.1.1 Time

Set the time of the server and the server supports time synchronization with PC, time format, time zone selection.

Figure 3-2 Time settings

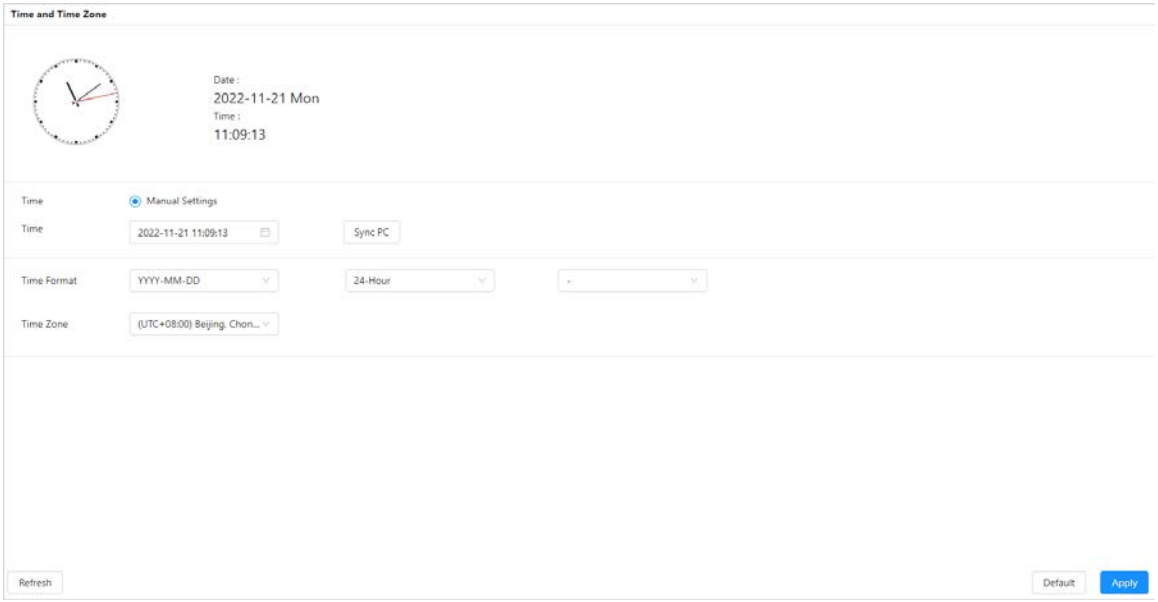


Table 3-2 Parameter description

Parameter	Description
Date and Time	Displays the current date and time of the server.
Manual Settings	Set the system time of the server. Click **Sync PC** to synchronize the time with PC.
Time Format	Select time format according to your needs.
Time Zone	Select time zone according to actual situation.

3.1.2 User Management

If you forget password, you can receive safety code with reserved email to reset password.

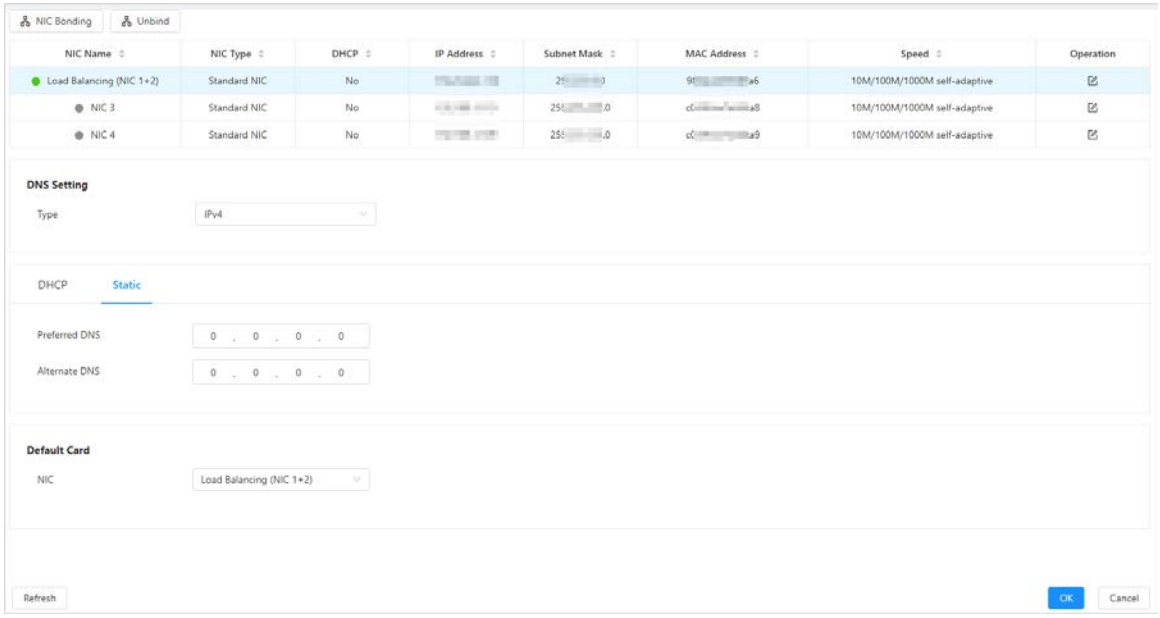
3.1.3 Network Configuration

3.1.3.1 TCP/IP

Configure TCP/IP of the server.

Click **NIC Bonding** to select the NIC card and binding mode.

Figure 3-3 NIC bonding



After bonding NIC cards, the webpage displays **Unbind** automatically. Click **Unbind** to unbind NIC cards.

Editing NIC Cards

Figure 3-4 Editing the NIC card

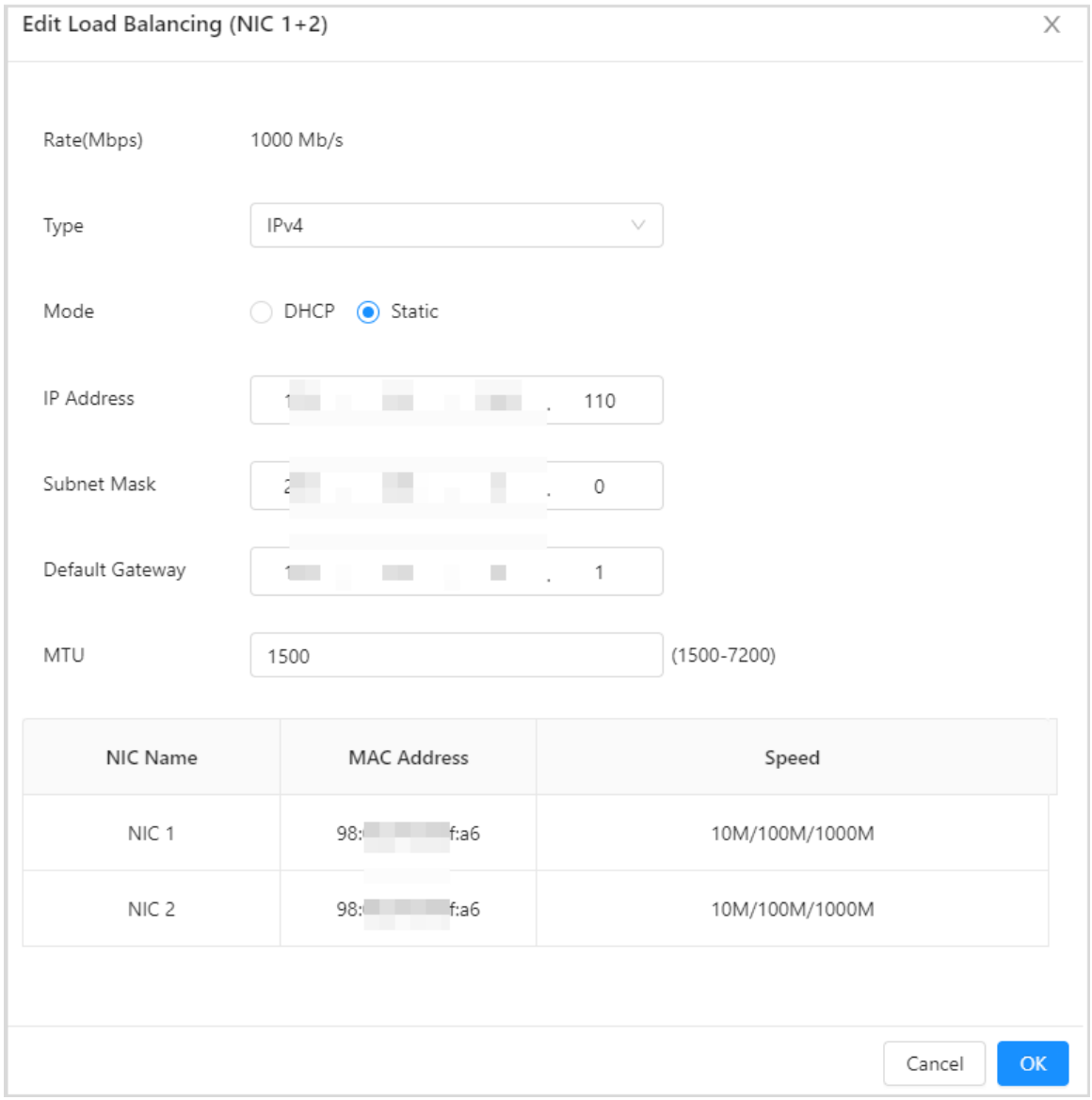


Table 3-3 Parameters description

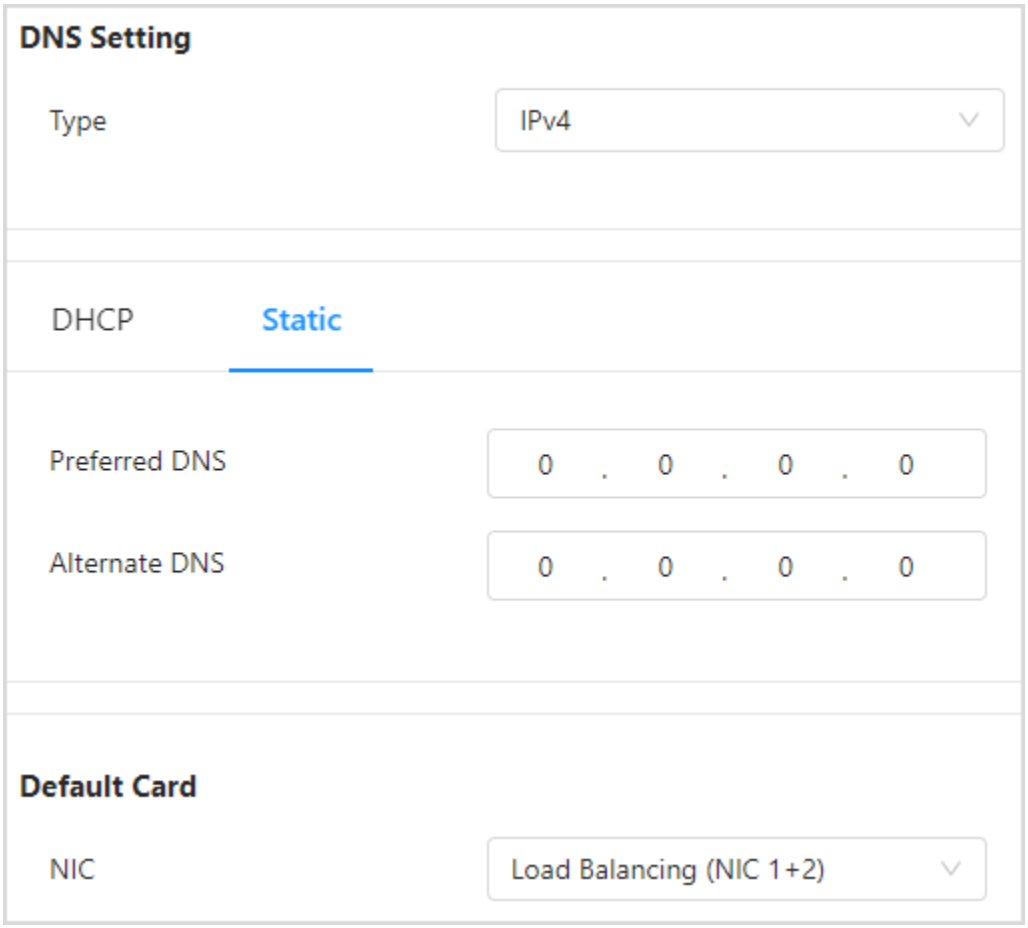
Parameter	Description
Rate	The speed of the NIC card.
Type	The type of NIC card. The default NIC card type is IPv4.
Mode	DHCP or static.
IP Address	Static mode: enter the IP address manually. DHCP mode: function reserved.
Subnet Mask	Static mode: enter the subnet mask of the IP address manually. DHCP mode: function reserved.
Default Gateway	Static mode: enter the default gateway of the IP address. DHCP mode: function reserved.

Parameter	Description
MTU	The default value is 500. Configure the MTU according to your needs.

DNS Settings

Configure the preferred or alternate DNS server address through DHCP or manually.

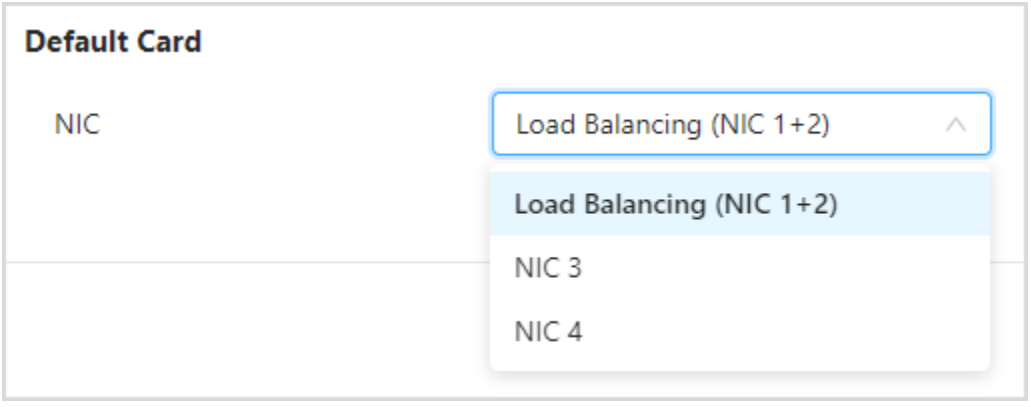
Figure 3-5 DNS settings



Default Card

Select a card online to serve as the default card.

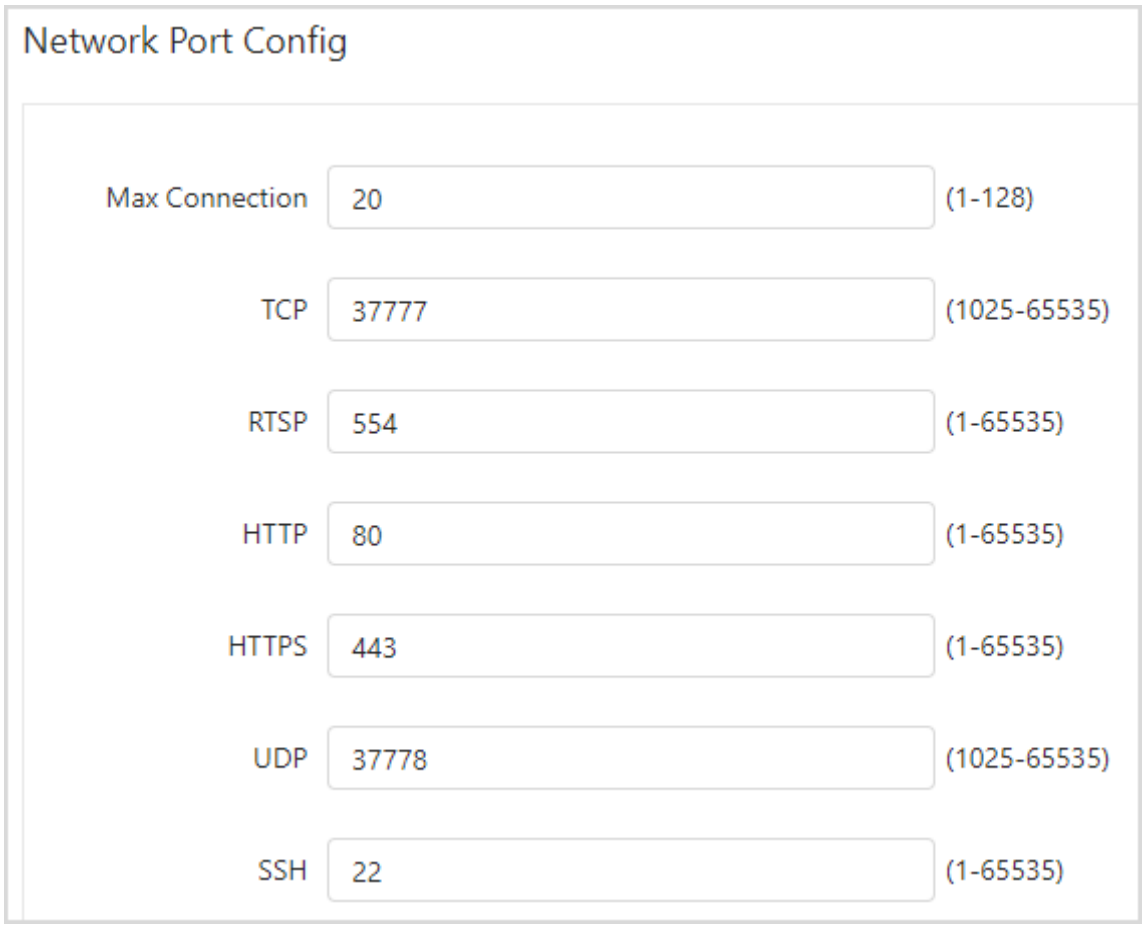
Figure 3-6 Default card



3.1.3.2 Network Port Configuration

Log in to the **Micro Intelligent Center**, and then click **System Config** > **Network Config** > **Port**.

Figure 3-7 Network port configuration



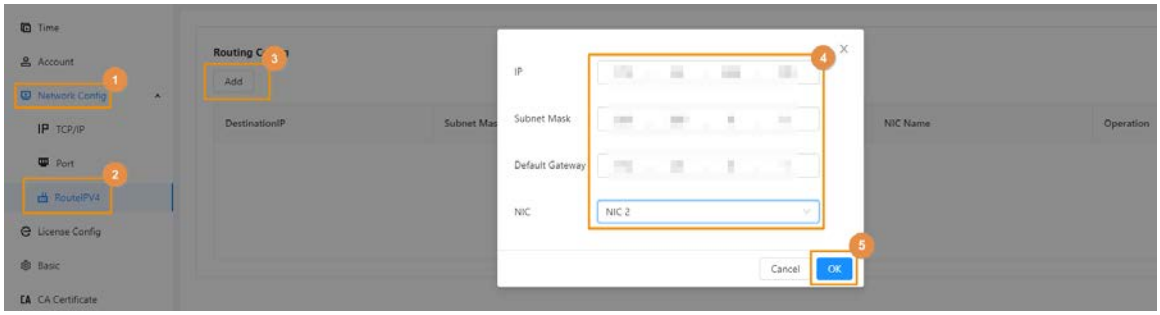
3.1.3.3 Route Configuration

Step 1 Log in to the **Intelligent Micro Center**.

Step 2 Select **System Config** > **Network Config** > **RouteIPV4**.

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

Figure 3-8 Route configuration



Step 4 Click **OK**.

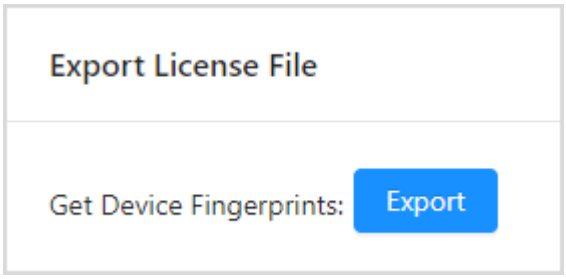
3.1.4 License Management

Support exporting and importing license files.

Exporting License Files

Click **Export** to acquire Machine Fingerprints server.dat file.
If the server inserts hardware dongle, it will export two files: Dongle information file and machine fingerprints file.

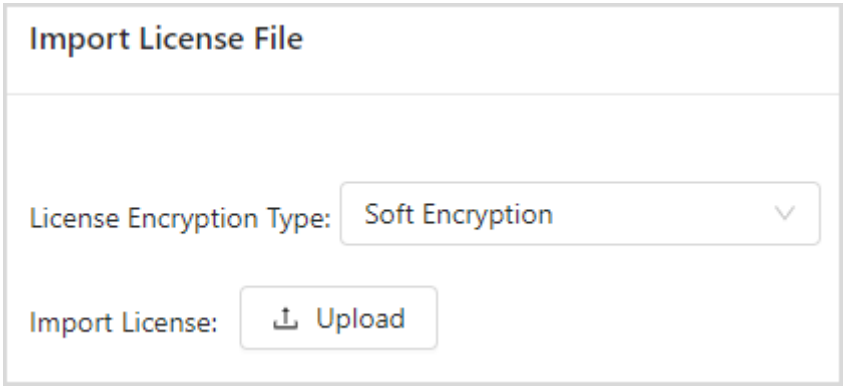
Figure 3-9 Export license file



Importing License Files

Select license encryption type, and then upload the encrypted files from local files.

Figure 3-10 Import license file



3.1.5 CA Certificate

3.1.5.1 Device Certificate Installation

Step 1 Log in to the webpage, and then select **CA Certificate** > **Device Certificate** > **Install Device Certificate**.

Figure 3-11 Installing device certificate

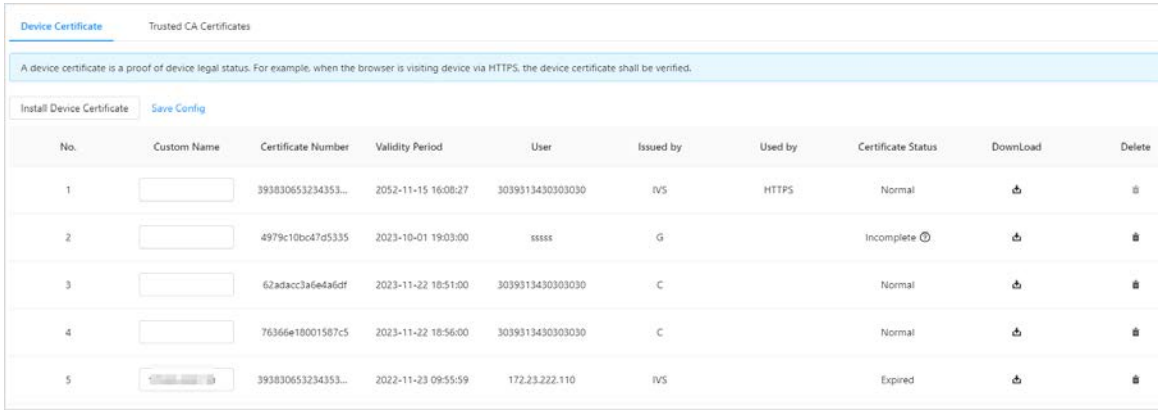
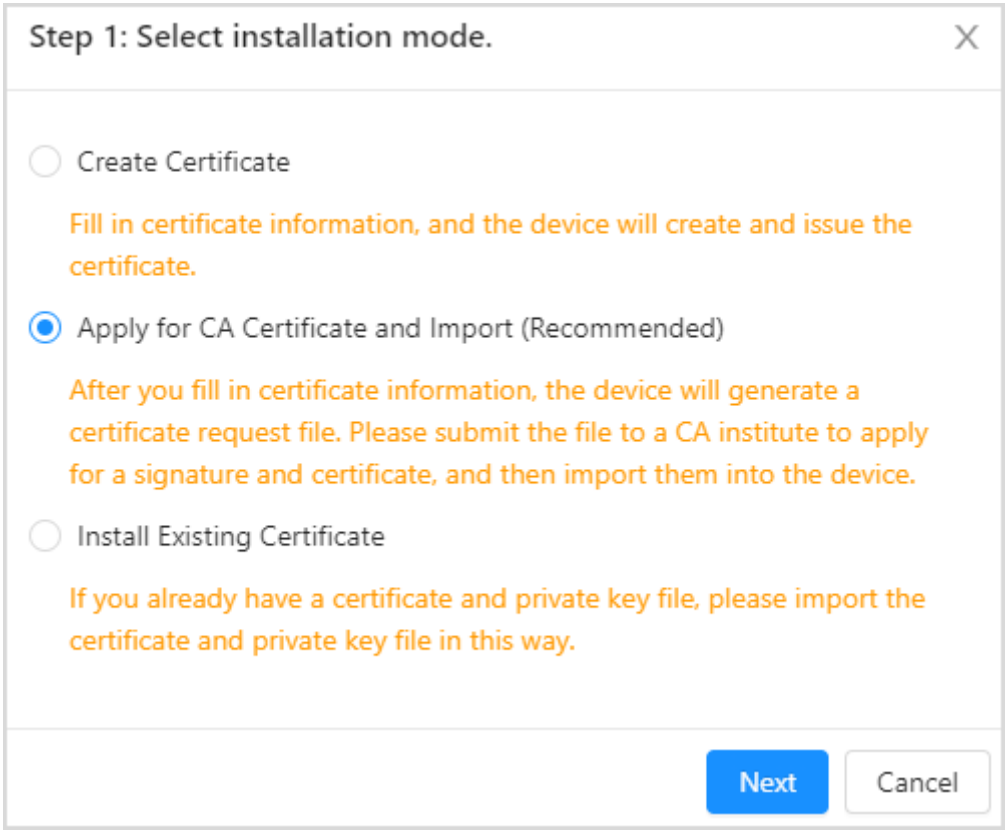


Table 3-4 Parameters description

Parameter	Description
Custom Name	Enter the customized name of the device.
Validity Period	Validity period of the certificate.
Certificate Status	Certificate status has three statues: normal, incomplete and Expired.
Download	Click to download CA certificate.
Delete	Click to delete certificate. The certificate being used by the devices cannot be deleted.

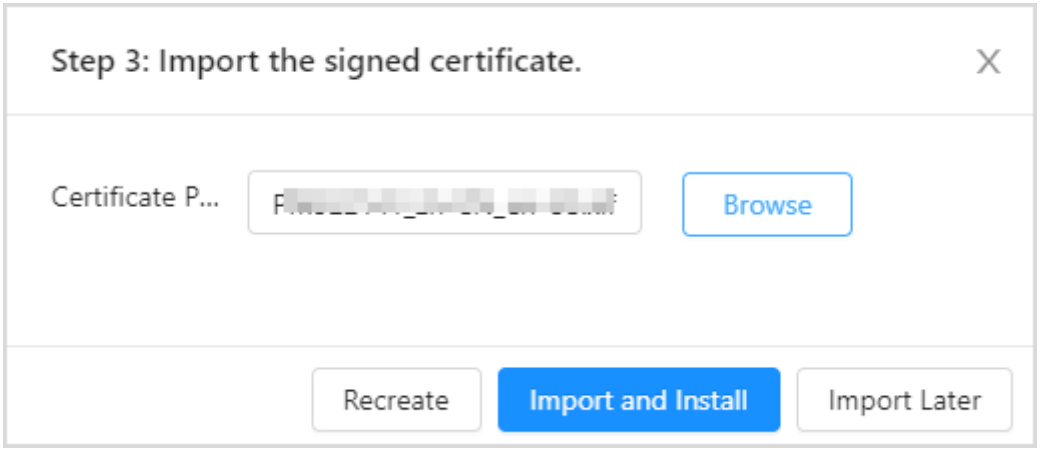
Step 2 Select installation mode, and then click **Next**.

Figure 3-12 Installation mode selection



Step 3 Click **Browse** to select certificate, and then click **Import and Install**.

Figure 3-13 Import and install



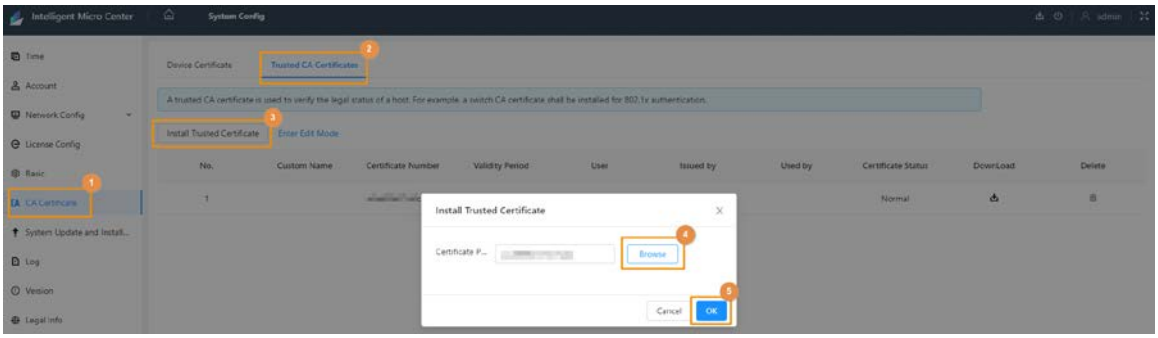
Related Operations

- Click **Enter Edit Mode** to configure the CA certificate parameters.
- Click **Save Config** to save the configuration.

3.1.5.2 Trusted CA Certificates Installation

Step 1 Log in to the webpage, select **CA Certificate** > **Trusted CA Certificates** > **Install Trusted Certificate**.

Figure 3-14 Install trusted certificate



Step 2 Click **Browse** to upload certificate files, and then click **OK**.

3.1.6 Basic

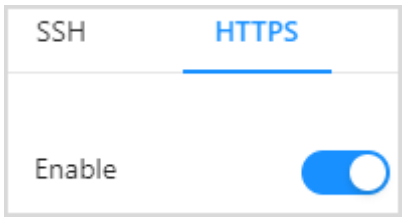
The server disables the SSH function by default to prohibit users logging in through SSH tool. After enabling SSH, users can access to the server background with SSH.

Figure3-15 SSH

HTTPS

Log in to the webpage, click **Basic** and **HTTPS**, and then click to enable HTTPS.

Figure 3-16 HTTPS

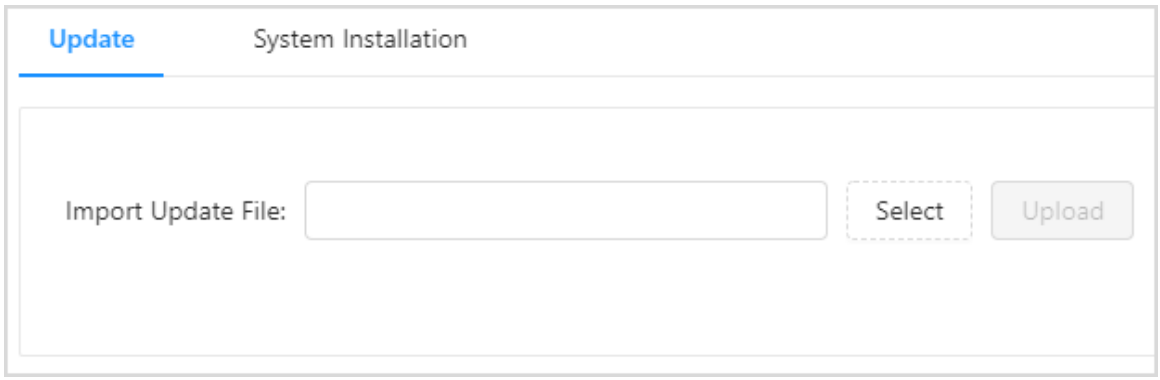


3.1.7 System Update and Installation

System update

Select **Update**, and then click **Select** to import the update file and click **Upload**.

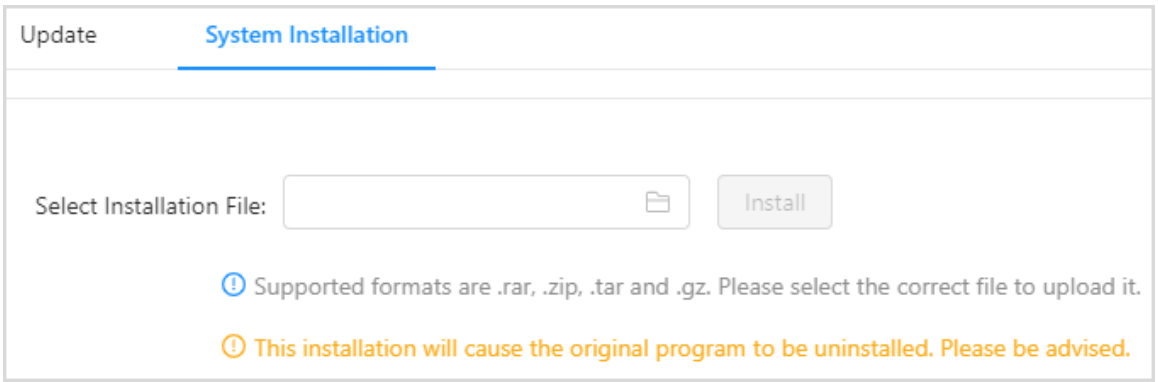
Figure 3-17 Update



System Installation

Select **System Installation** to select installation file, and then click **Install**.

Figure 3-18 System installation

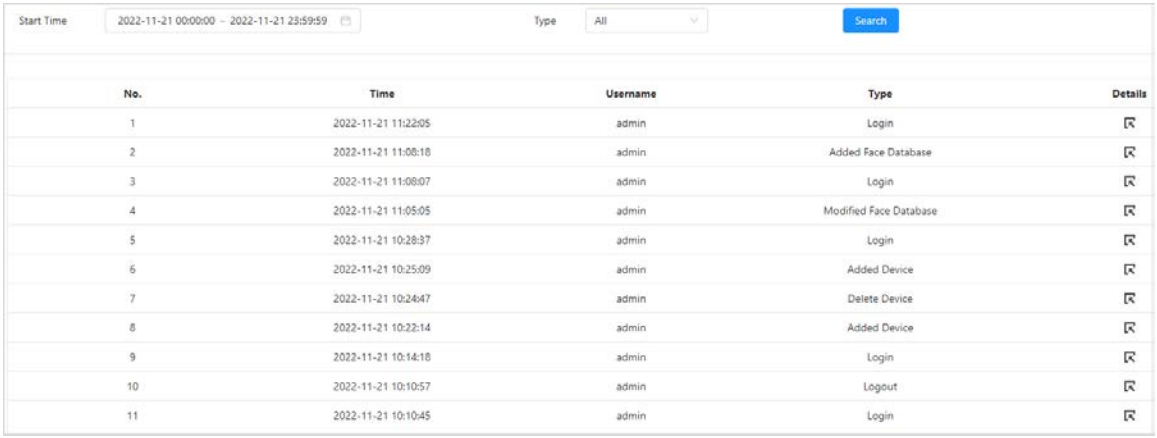


3.1.8 Logs

Logs record and save operations of users and device status. You can set search conditions to search for the specified logs.

Log in to the webpage, select **System Config** and **Log**.

Figure 3-19 Logs

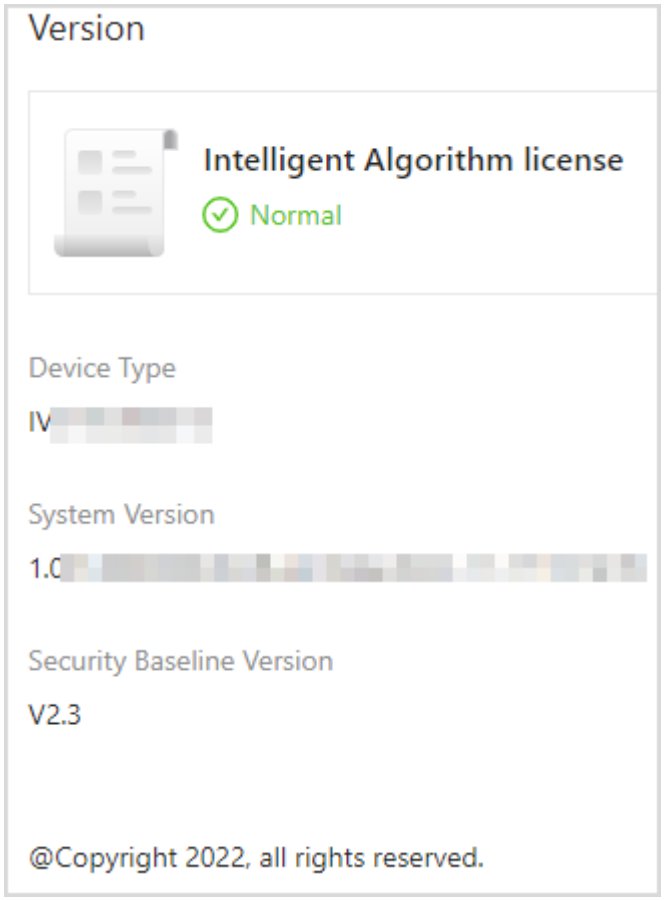


Click to view the log details.

3.1.9 Version

Click **Version** to view the device details.

Figure 3-20 Version



3.1.10 Legal Information

Click **Legal Info** to view **Software License Agreement** and **Open Source Software Notice**.

3.2 Service Configuration

Log in to the webpage, select **Service Config** to modify video stream channels, static face database, armed face database and storage period, and then click **Save.**

Figure 3-21 Business configuration

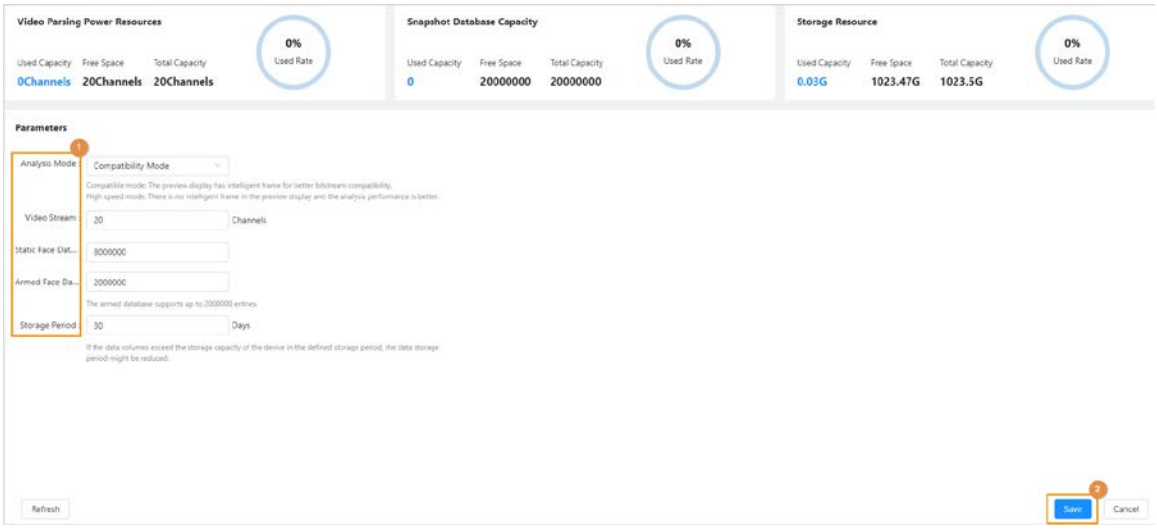


Table 3-5 Parameter description

Parameter	Description
Video Stream	The number of channels must be multiples of 20. The maximum is 60 and the minimum is 0.
Static Face Database	The summation of static face database capacity, snapshot database capacity and armed face database capacity is 30,000,000. The maximum of armed face database is 2,000,000. When you change the capacity of static face database, the snapshot database capacity will change as well and the total capacity will be kept as 30,000,000.
Armed Face Database	
Storage Period	Within the storage period, if the data reaches the limitation of the storage capacity, the server will recycle capacity in advance. It depends on the actual device capacity.

3.3 Device Management

3.3.1 Adding Devices

Add remote devices to the server, including IPC, NVR, DVR and more.
You can add devices one by one or in batches.

3.3.1.1 Adding Devices Manually

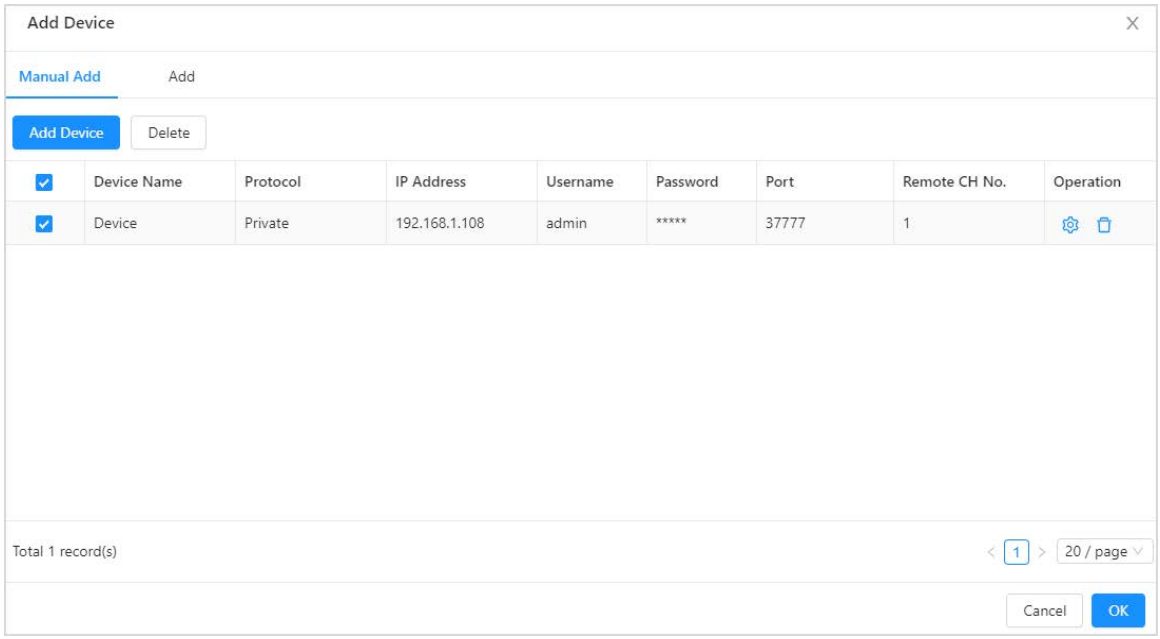
Step 1 Log in to the webpage.

Step 2 Select **Device Setting**, and then click **Add**.

Step 3 Click **Add Device**, and then configure the parameters according to your needs. Click **OK**.

When **RTSP** protocol is selected, the channel type will be video stream and cannot be changed. To change it, you need to enter the RTSP address on the channel configuration page.

Figure 3-22 Manual add



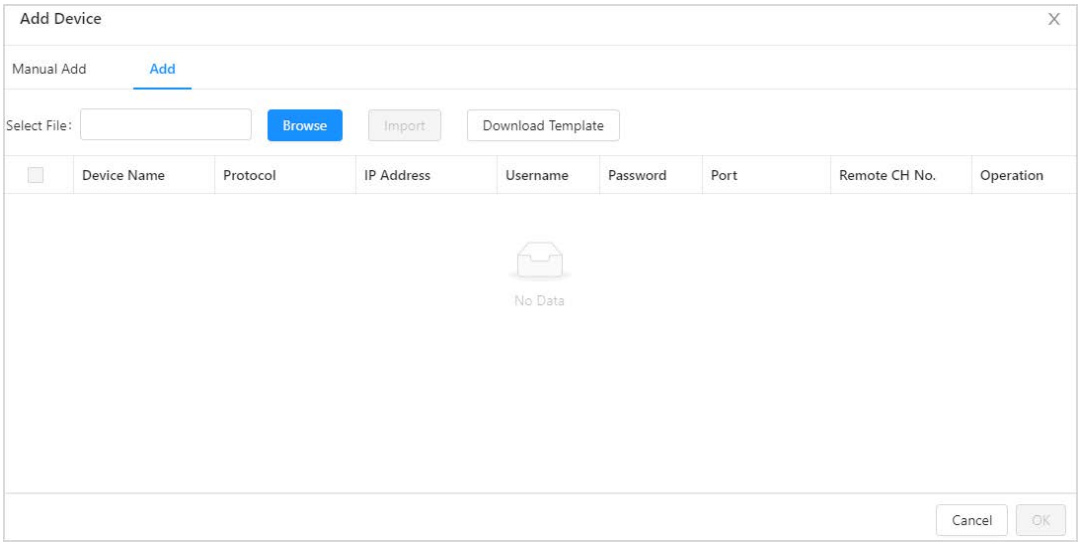
Step 4 Click **OK**.

3.3.1.2 Adding Device in Batches

Step 1 Log in to the webpage.

Step 2 Select **Device Setting**, and then click **Add**.

Figure 3-23 Add device in batches



Step 3 Click **Download Template** to download remote device template to your local computer.

Step 4 Complete the template and then save it.

Step 5 On the **Add Device** page, click **Browse** to select the template, and then click **Import**.

Step 6 Click **OK**.

If you want to add more devices, click **Add More**.

Related Operations

- If the remote device has many channels, click to enter the total number of and the system will display the channel list. You can edit channel name, and select and add channels. When you are finished, click **OK**.
- Click **Delete** to delete remote devices.

  On the channel list page, select channels, and then click **Delete** or in the operation bar to delete channels.

3.3.2 Editing Channel Information

After adding channels, you can click table to edit channels.

- When the protocol is private, you can change the name, type of the channel, and the analysis type.
- When the protocol is RTSP, you can change the channel name, analysis type and RTSP address.

Changing Channel Name

Click channel name to edit it.

Changing Channel Type

- Click the channel type of the device, and then select **Video Stream** or **Image Stream** from the channel type list.
- Select channels, and then click **Change Channel Type** to change the channel type in batches.

Changing Analysis Type

When the channel type is video stream, you can change the analysis type. But when the channel type is image stream, you cannot change the analysis type.

- Click the analysis type of the video stream channels to delete the types that do not need
- You can select multiple video stream channels, and select the analysis type from the list on the right of the **Change Analysis Type**.

Searching for Channels

You can search for channels by name, IP address or RTSP. For channels, fuzzy search is also supported.

Filtering Attributes

Click **Filter** in the upper right corner to change the attributes being displayed in the list.

Enabling/Disabling Analysis

- On the analysis status list,  means analysis enabled, and  means analysis disabled.
- Select multiple channels, click **Start Analysis** or **Stop Analysis** to start or stop analyzing in batches. When debugging, we recommend not analyzing channels. You should view the logs.

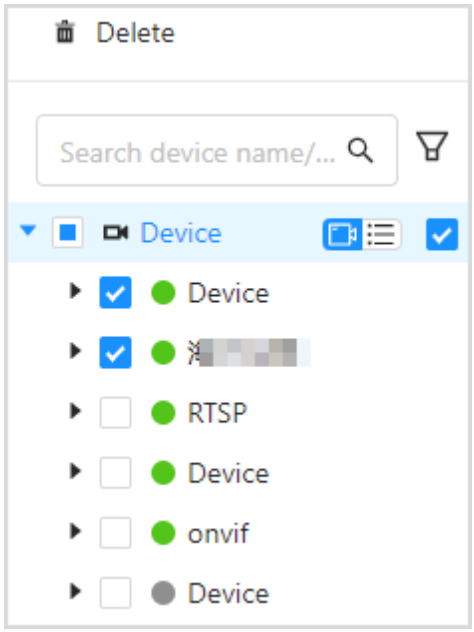
Export Channel Information

Select channels, and then click **Export** to export channel information to Excel.

Device Tree Operations

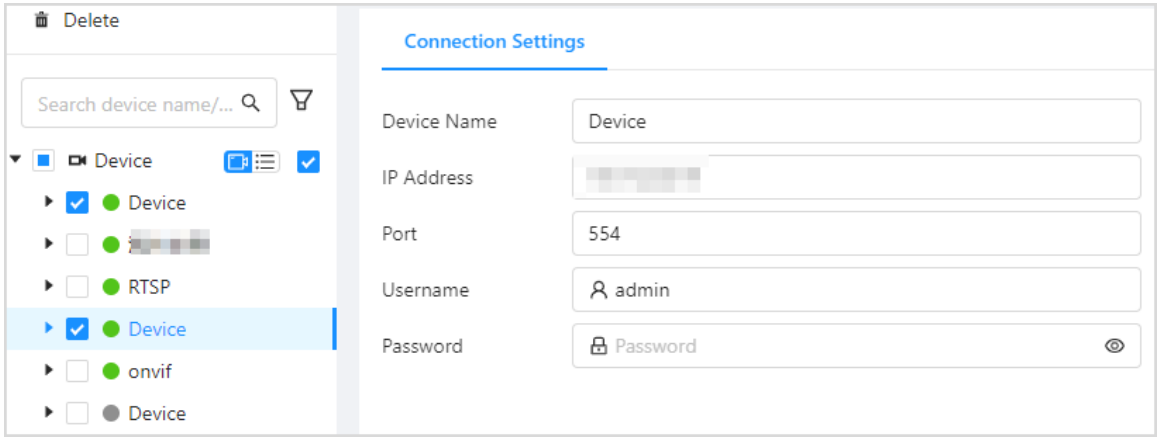
- Select device tree and device on the left, and then click **Delete** to delete the device of the type.

Figure 3-24 Delete device



- Click  to switch between device mode and channel mode.
- Click  to filter devices that are online or offline.
- Enter the device name for the IP address in the search bar to search for the device.
- Click device to modify the device name, IP addresses, ports, usernames and passwords in batches.

Figure 3-25 Modify connection



3.3.3 Arming Channels

Bind channels to face database to compare the face snapshots with the face images in the database. When the similarity meets the threshold, alarms will be triggered.

Prerequisites

- **Status**: Online.
- **Analysis status**: .

There are two methods for enabling analysis:

- Enable analysis one by one: Click .
- Enable analysis in batches: Select the channels and then click **Start Analysis**.

3.3.3.1 Arming Channels Manually

Arm the face database for a single channel.

Step 1 On the channel list page, click the corresponding on the channel list.

Step 2 Select the face database that you want to arm.

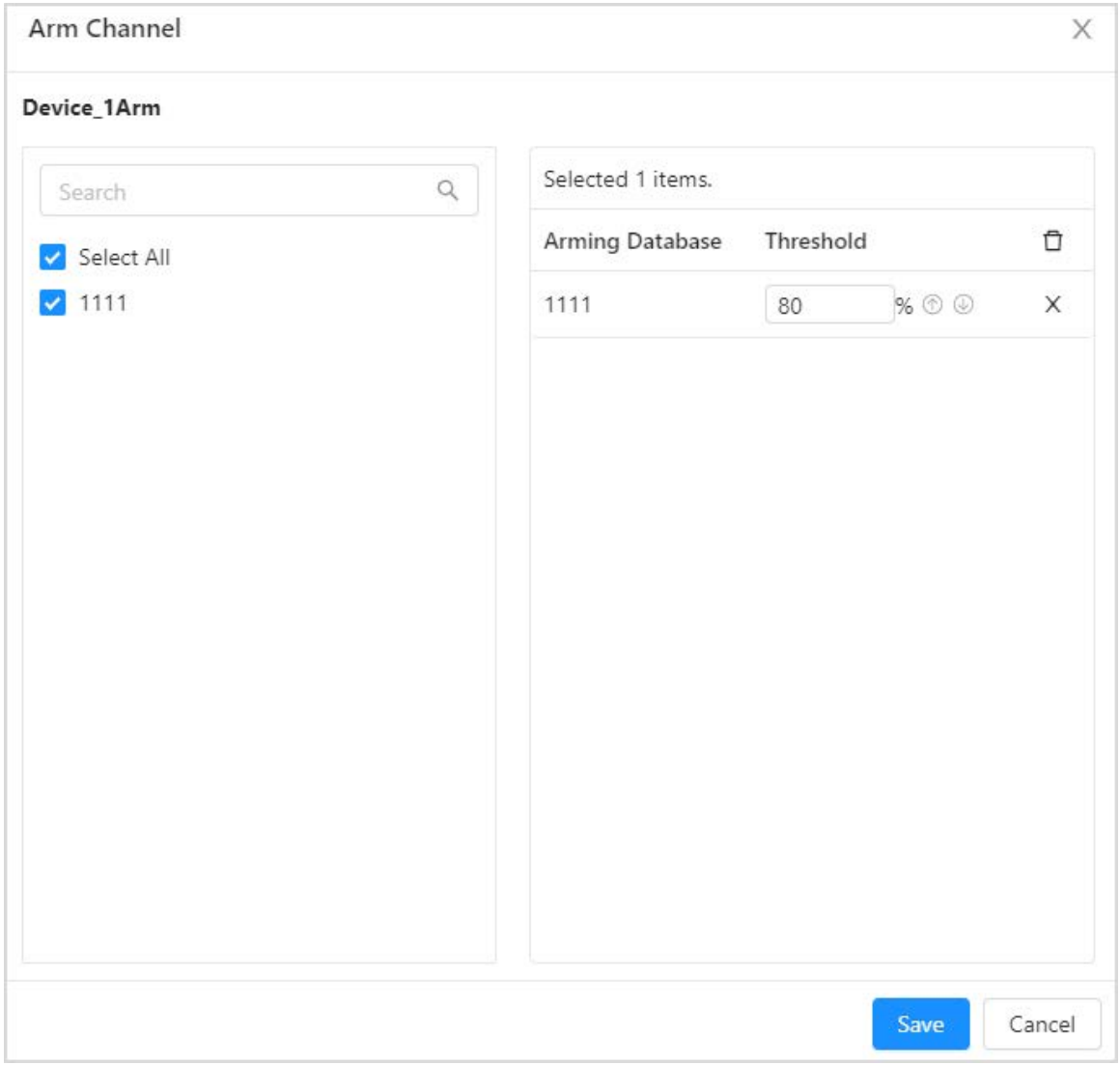
- Only armed face databases will be displayed. Static face database arm is also available.
- If the arming channel has arm tasks, the corresponding face database will be selected.

Step 3 Set the threshold.

When the server compares face image with the images in the face database, it will display the similarity of the two images. When the similarity reaches the threshold, the system will trigger an alarm.

Step 4 Click **Save**.

Figure 3-26 Arm channel



3.3.3.2 Arming Channels in Batches

Arm face database for channels in batches.。

Step 1 On **Channel List**, select the channels that you want to arm face database for.

Step 2 Click **Batch Arm** above the channel list.

Step 3 Select the face database that you want to arm.

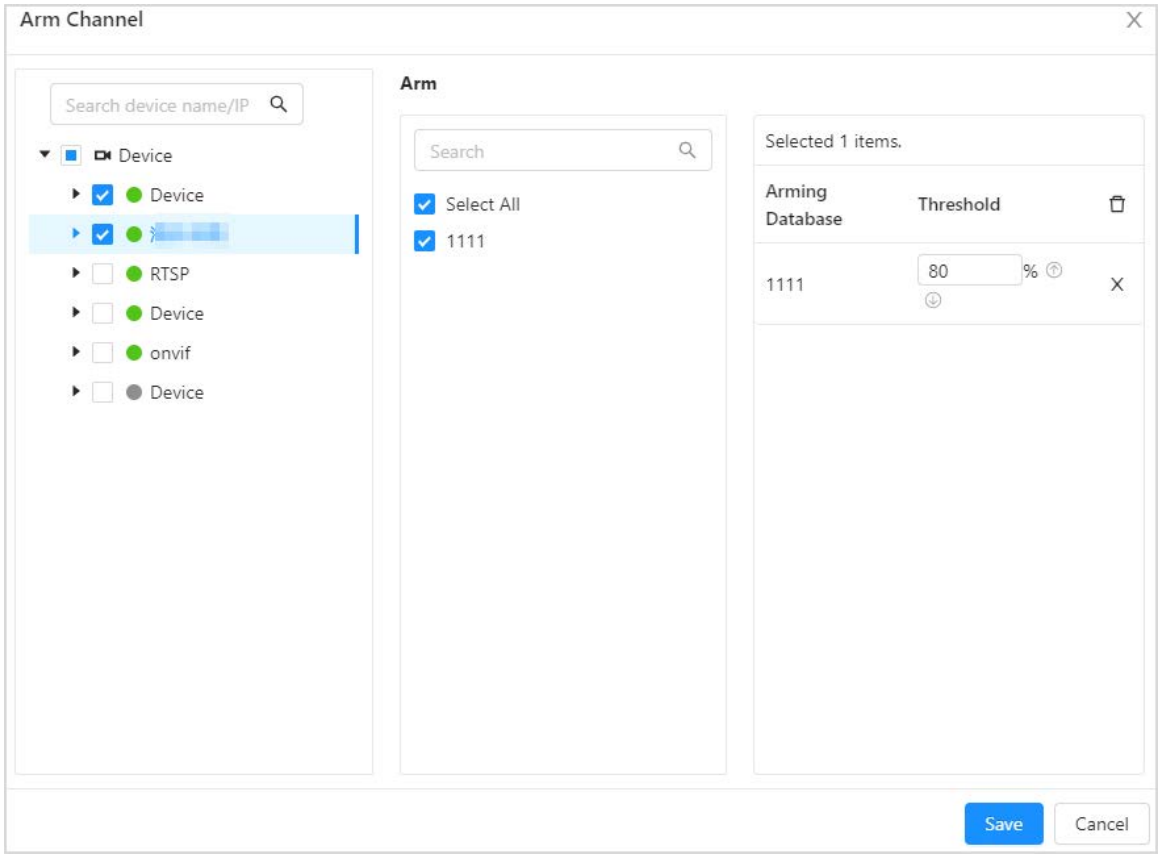
- Only armed face databases will be displayed in the list. Static face databases can be armed.
- If the selected channels already have arming tasks, then the corresponding armed face database will be selected.

Step 4 Set the threshold.

When the server compares face images and matches the images to those in the face database, the similarity will be displayed for the 2 images. When the similarity reaches or is higher than the threshold, the system will trigger an alarm.

After setting a threshold for a channel, you can click the corresponding to fill down and click to fill up to set thresholds in batch.

Figure 3-27 Batch arm



Step 45 Click **Save**.

3.4 Face Comparison

Compares two face images, and decides whether they are the same person based on similarity level.

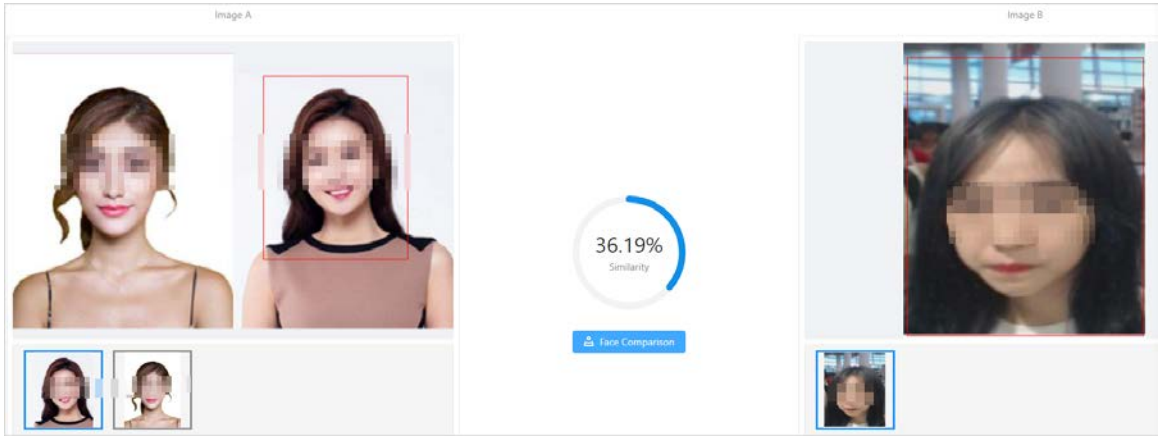
Step 1 Click **Face Comparison**.

Step 2 Click **Upload Picture** to upload picture A and picture B from the local computer.

Step 3 Click **Face Comparison**.

Step 4 Move the cursor to the image, and click **Delete** or **Reselect** to reupload the pictures.

Figure 3-28 Comparison result



- When there are multiple matches, you can select a face from the lower section for it to appear in the upper section.
- Supports image resolution: 100×100 to 4096×4096.

3.5 Face Database

There are 2 types of face database, static and armed. Face database are used to manage static face images. You can create a database and upload face images with the same attributes. The used capacity of the face database and armed face database is displayed in the upper area.

3.5.1 Face Database Management

You can add, modify and delete face databases.

3.5.1.1 Adding Face Databases

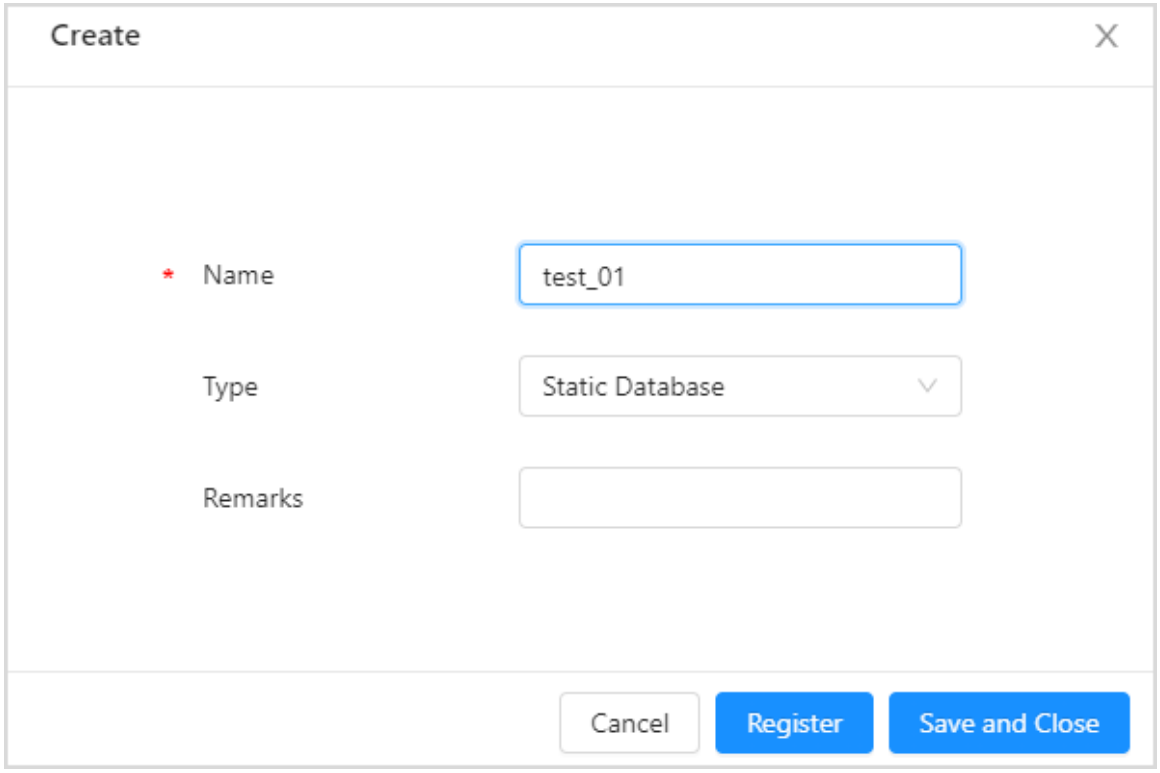
Step 1 Log in to the webpage.

Step 2 Click **Face Database** to enter the face database page.

Step 3 Click **Add**, and then enter the name, select the type and enter the remarks.

Type includes static database and arming database. Static databases cannot be armed and disarmed.

Figure 3-29 Create a face database



Step 4 Click **Save and Close**.

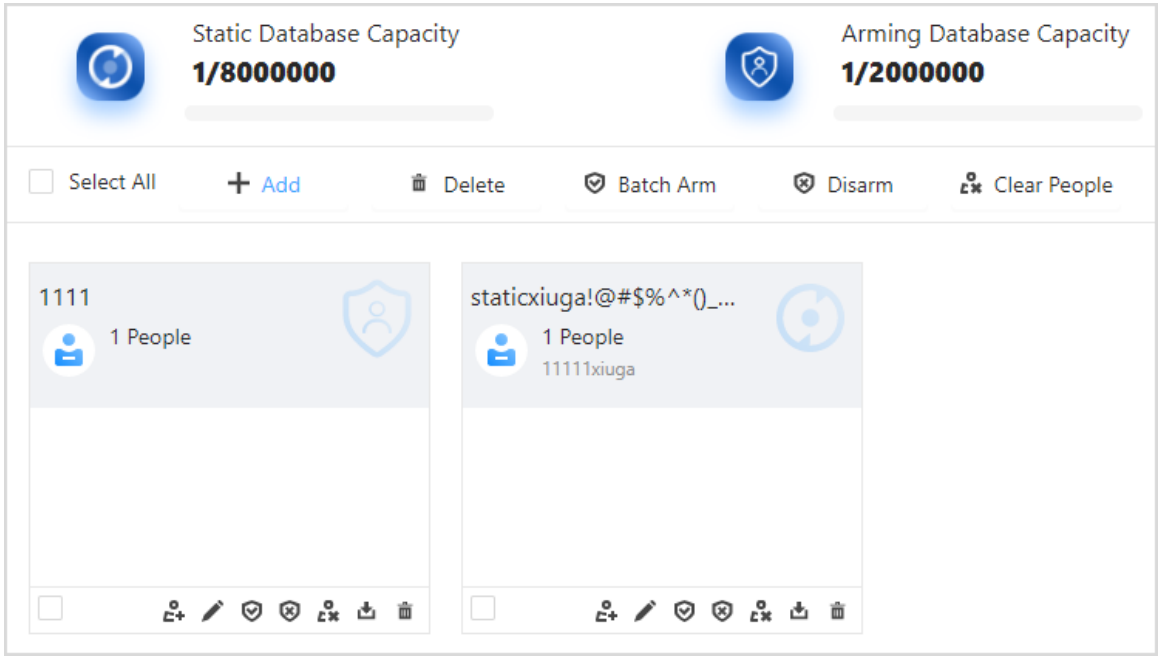
Click **Register** to enter the registration page.

3.5.1.2 Editing Face Databases

Step 1 Log in to the webpage.

Step 2 Click **Face Database** to enter the face database page.

Figure 3-30 Face database



Static face databases cannot be armed and disarmed.

Step 3 Select and edit the face database.

Table 3-6 Edit face database

Icon	Description
	Registration.
	Edit the name and remarks for the face database.
	Arm the face database.
	Disarm the face database.
	Clear people from the face database. This function clears data of the current database, but does not disarm databases that are bound to channels.
	Delete the face database.

3.5.1.3 Armed Face Database

You can bind face databases with remote device. When the device takes snapshots and compares the snapshot with images in the face database and the similarity reaches the threshold, the system triggers an alarm.

Step 1 Log in to the webpage.

Step 2 Click **Face Database** to enter the face database page.

Step 3 Add a face database.

Step 4 Click the corresponding to arm the face database.

- Static databases cannot be armed or disarmed.
- Multiple face databases can be bound to a channel.
- Click **Batch Arm** to select remote devices for each database in the batch.

Figure 3-31 Armed face database

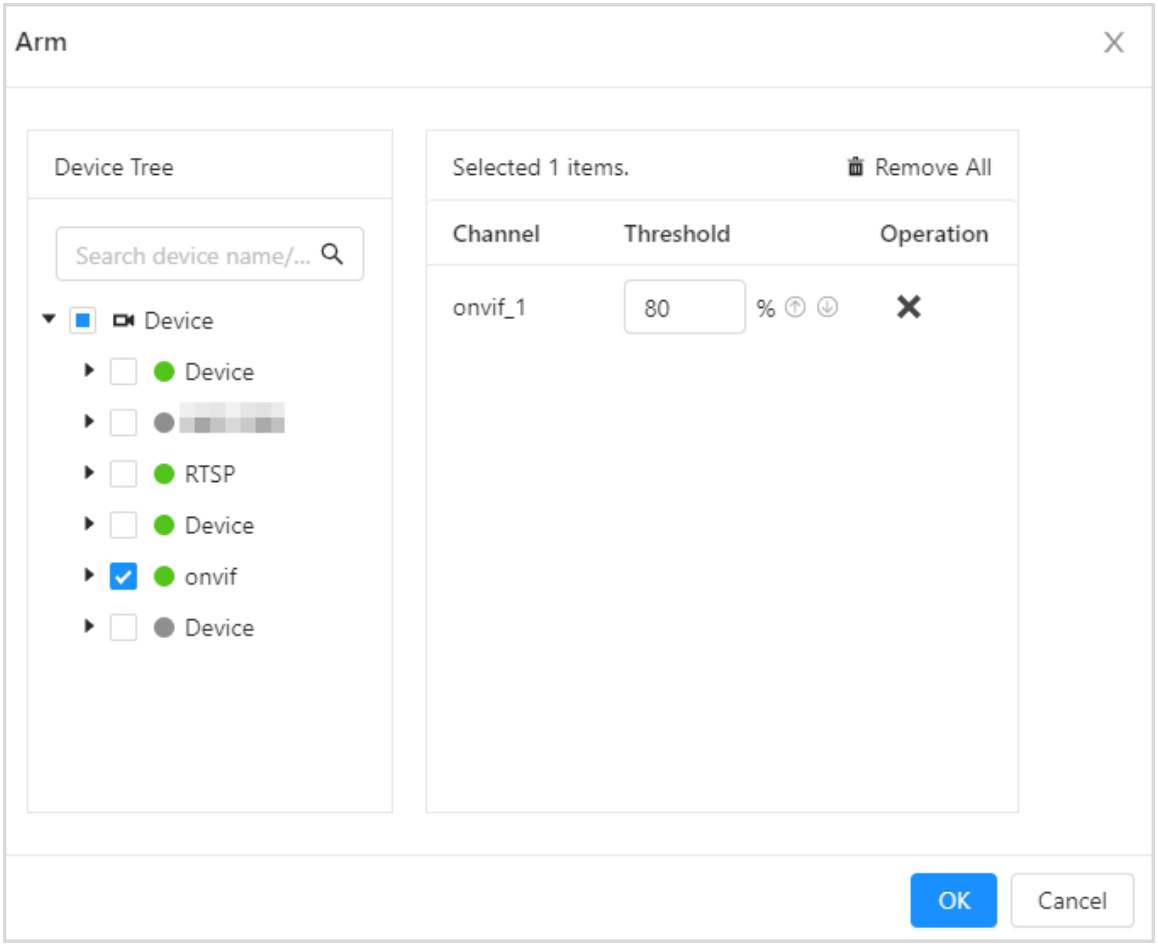
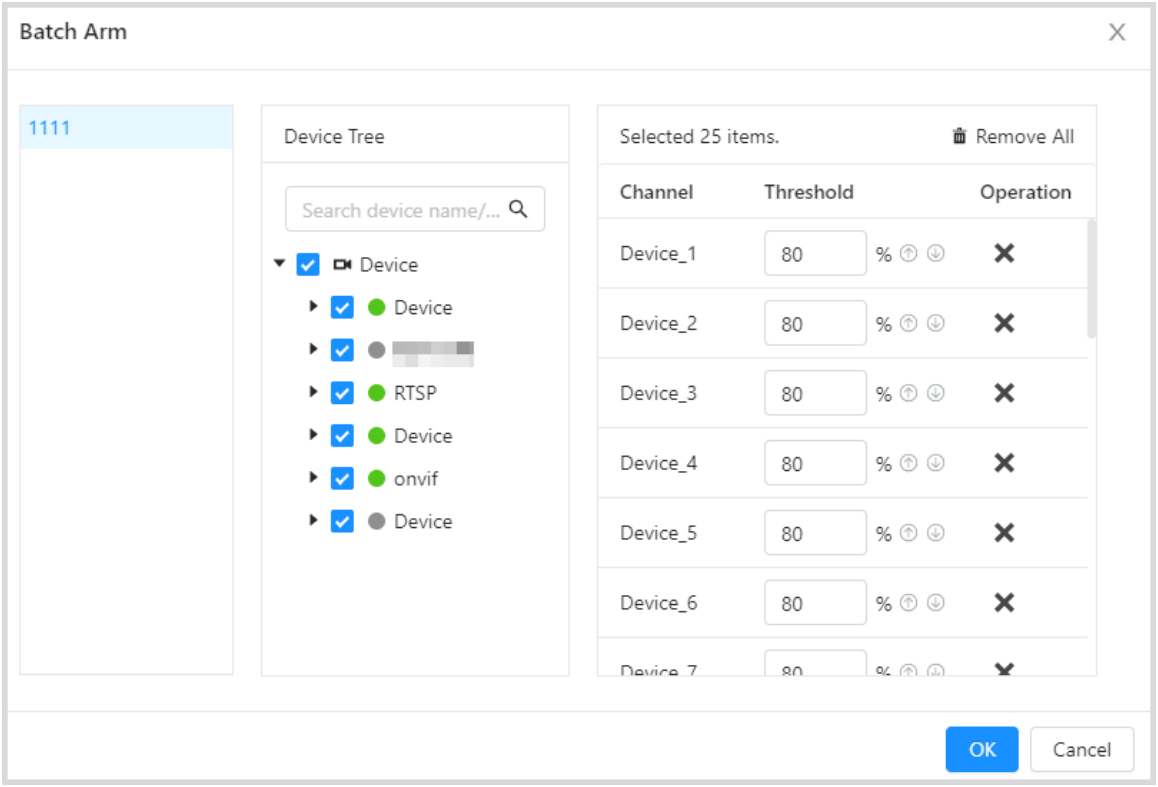


Figure 3-32 Batch arm



Step 5 On the device tree area, select the channels that need to be armed.

The selected channel is displayed in the list in the left area.

After setting a threshold for a channel, click to fill down, and then click to fill up to set threshold in batches.

Related Operations

Click to disarm face databases. Select the face databases, and then click **Disarm** to disarm the face database in batches.

3.5.2 Face Information Management

You can add face images to the face database to create a face, comparison and search basis.

3.5.2.1 Adding Face Information

You can add face information one by one or import face information in batches.

3.5.2.1.1 Adding Face Information Manually

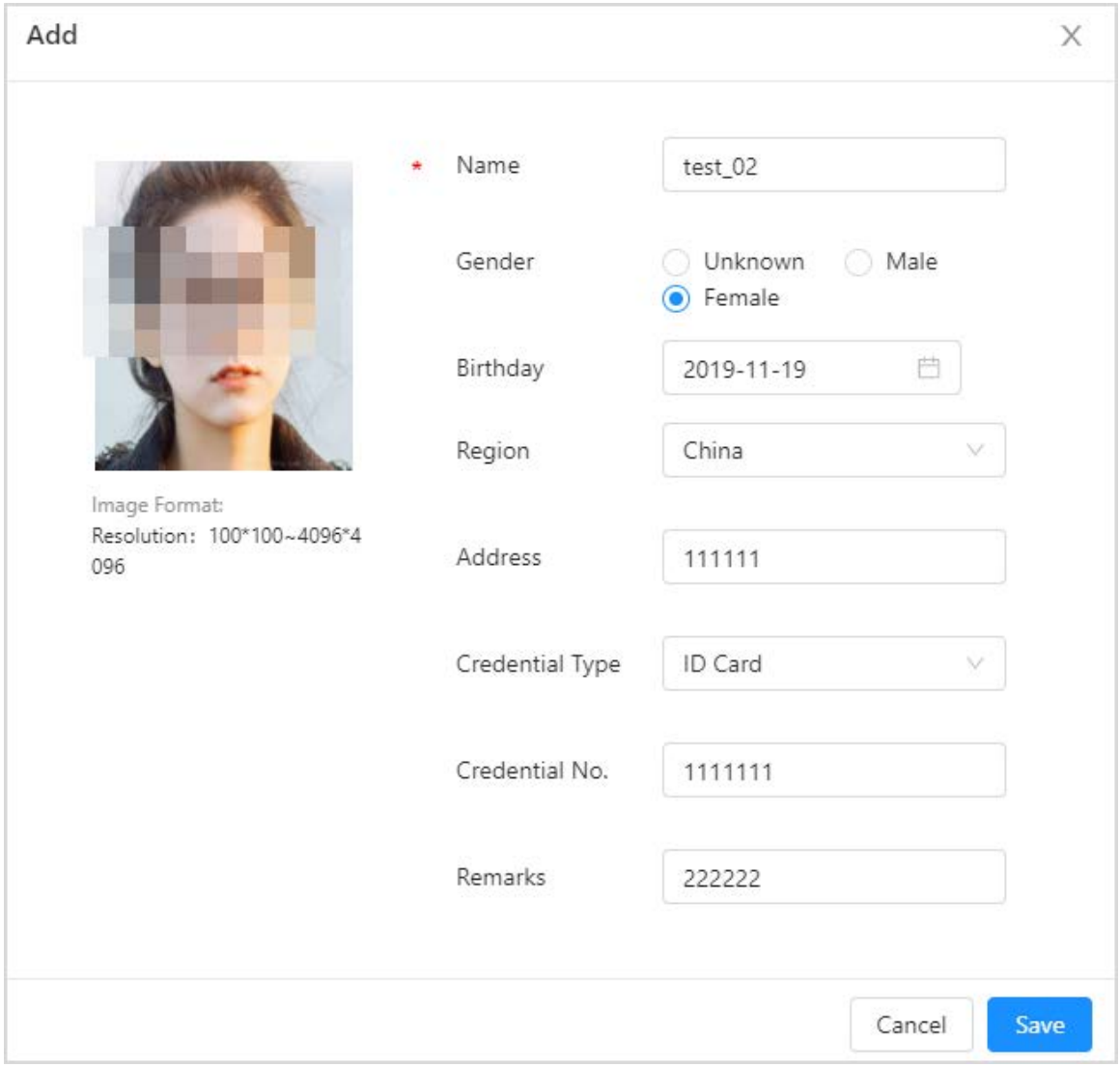
You can add face information one by one.

Step 1 Log in to the webpage.

Step 2 Click **Face Database** to enter the face database page.

Step 3 Click the corresponding of the face database or click the created face database, and then click **Add**.

Figure 3-33 Registration



Step 4 Click **Upload Picture** to select face images and enter information.

- Image resolution: 100×100～4096×4096.
- * means required options.

Step 5 Click **Save**.

3.5.2.1.2 Batch Registration

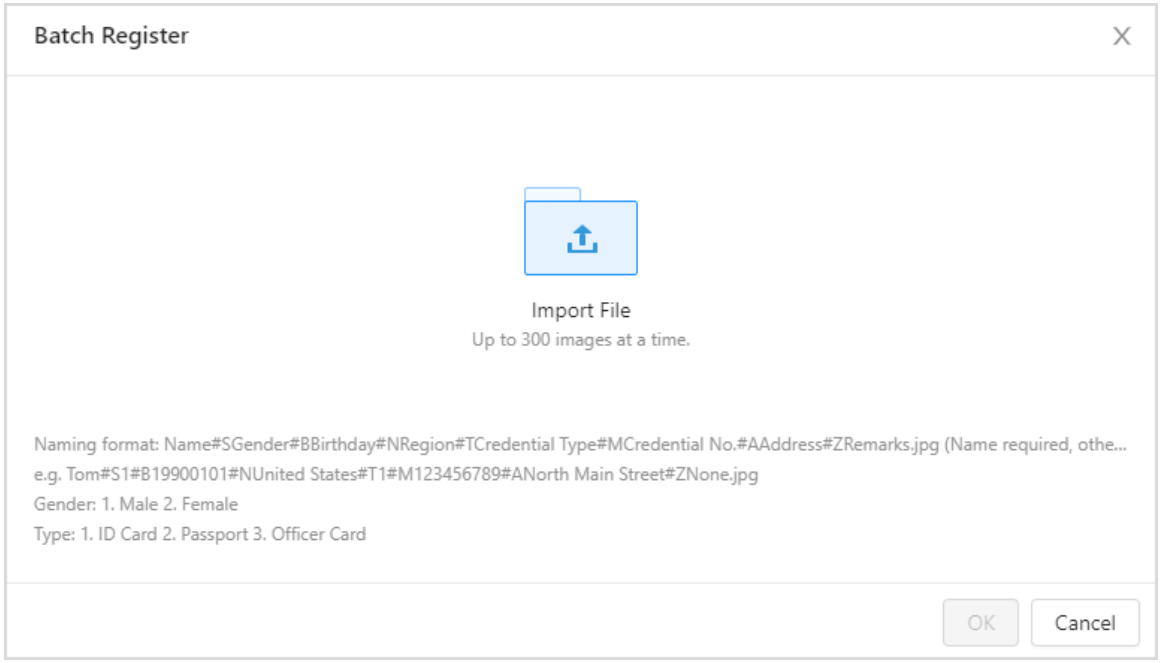
You can import face images in batches to face database.

Step 1 Log in to the webpage.

Step 2 Click **Face Database** to enter the face database page.

Step 3 Click the created face database to enter the page, and then click **Batch Register**.

Figure 3-34 Batch Register



Step 4 Click **Import File** to select files from the local computer according to the requirements of the page.

Step 5 Click **OK**.

Related Operations

If the files fail to be imported, you can export the failed image ZIP package to the local computer for details on the failure.

3.5.2.2 Modifying Face Information

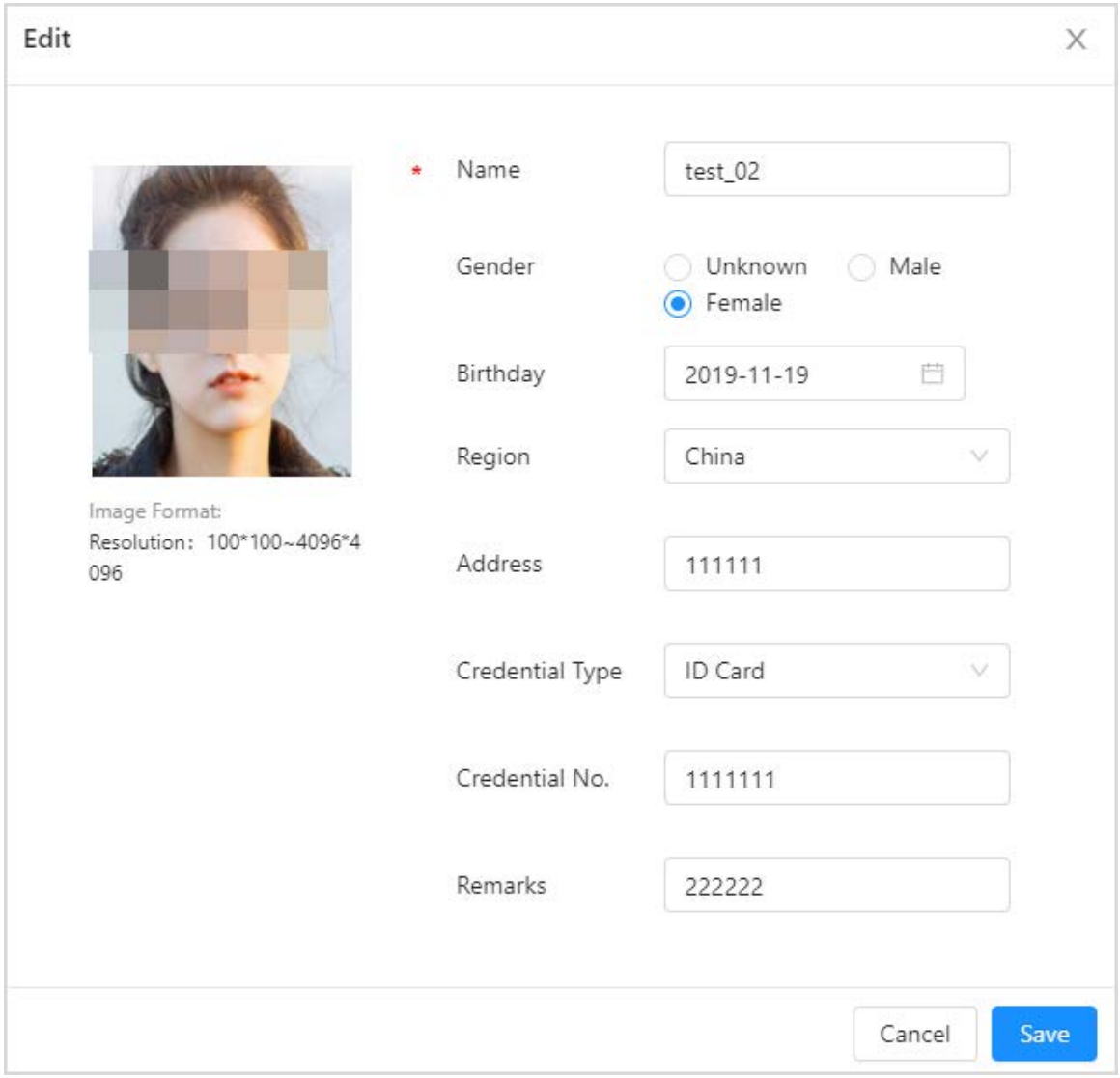
Step 1 Log in to the webpage.

Step 2 Click **Face Database** to enter the face database page.

Step 3 Click the created face database to enter a single face database page.

Step 4 Click the ✎ of the face information to edit personal information.

Figure 3-35 Edit personal information



Step 5 Click **Save**.

3.6 AI Search

You can configure the features of people, motor vehicles and non-motor vehicles to search for images based on their features. You can also upload images of faces, human bodies, motor vehicles or non-motor vehicles to search by image.

Some of the snapshots display **not extracted**. This means there are no results for the recognized targets because the image is not complete or its resolution is too low.

3.6.1 Alarm Search

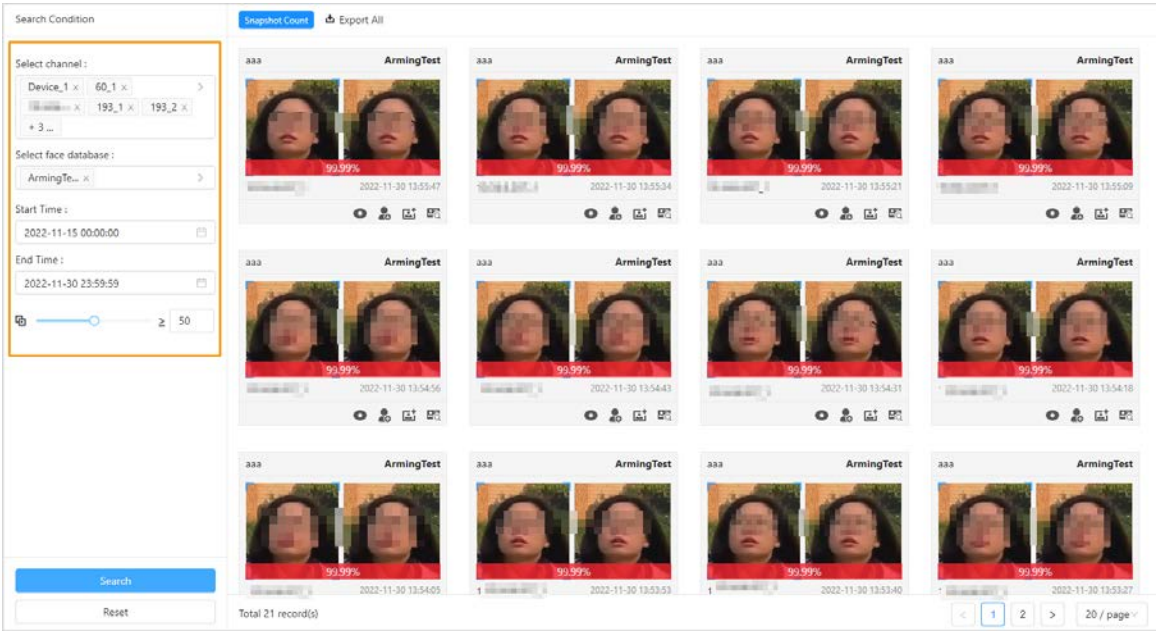
Search for alarm information for the channel and face databases within a defined period.

Step 1 Log in to the webpage. and then click **AI Search** and **Alarm Query**.

Step 2 Configure search conditions and similarity.

Step 3 Click **Search** and then the system displays the results.

Figure 3-36 Alarm query



Step 4 (Optional) Click **Snapshot Count**, the system displays the total number of results, but only the top 1,000 images are displayed.

Related Operations

Alarm operations.

- Click of the search results to view details on the alarm.
- Click of the search results to add the snapshot to the face database.
- Click of the search results to search the snapshot face database, and then enter the face search page. For details, see "3.6.2.1 Snapshot Database Search".
- Click of the search results to enter the **Face Search** page. For details, see "3.6.2.2 Face Database Search".

3.6.2 Face Search

You can search for faces in the snapshot database.

3.6.2.1 Snapshot Database Search

Face search supports searching for snapshots under the search conditions. It also matches pictures or snapshots from a device and channel. You can find the snapshot that the similarity above the threshold.

Step 1 Log in to the webpage, and then select **AI Search** > **Face Search**.

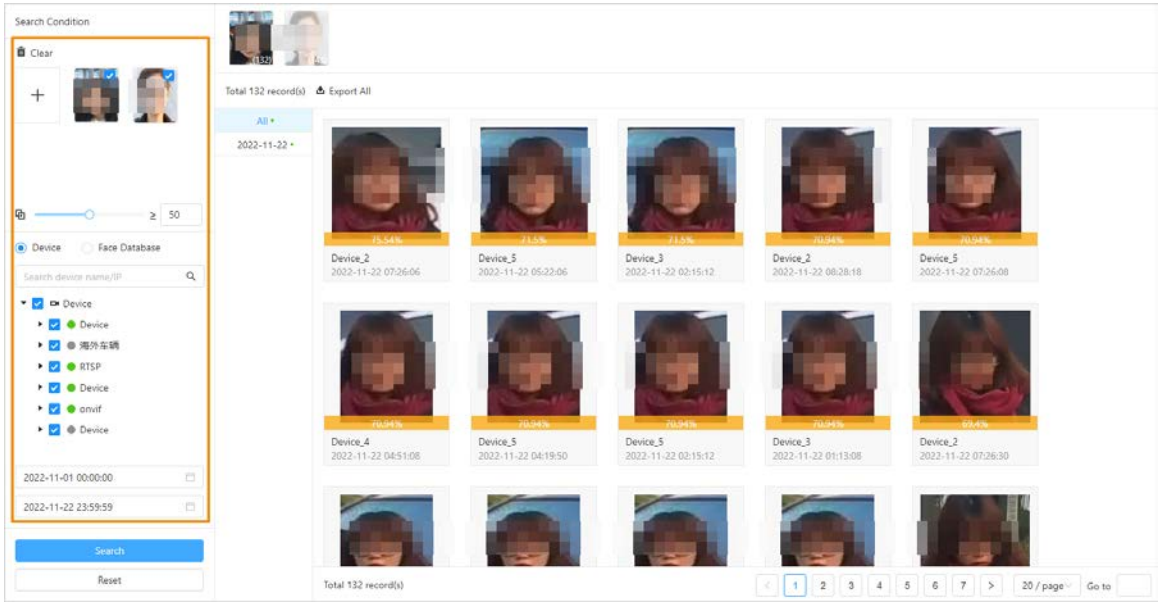
Step 2 Configure the search condition, and then select **Device.**

Search by channels and device is available.

Step 3 Click **Search** and the results are displayed.

- You can search by uploading images, and the system will display the search results.

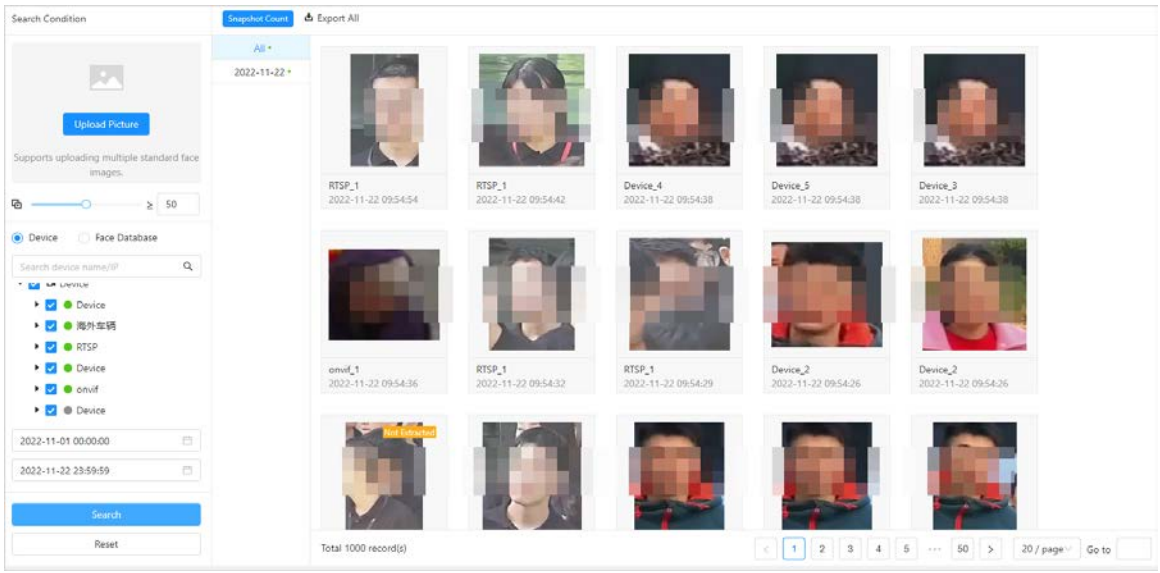
Figure 3-37 Upload images



- You can upload up to100 from local computers at the same time.
- If there are many targets in the images, the system will recognize targets automatically. You can upload up to 32 images at a time, but the image's file size is limited to 20 MB.
- Click **Clear** to clear the uploaded images.
- Click **Reset** to reset the search conditions. But uploaded images will not be cleared.

- If you do not upload images, the system displays all the snapshots from the selected channels.

Figure 3-38 Snapshot search



Snapshot operations:

- View details on the image. Click the corresponding of the snapshot, and the system displays the image details.

Figure 3-39 Image details

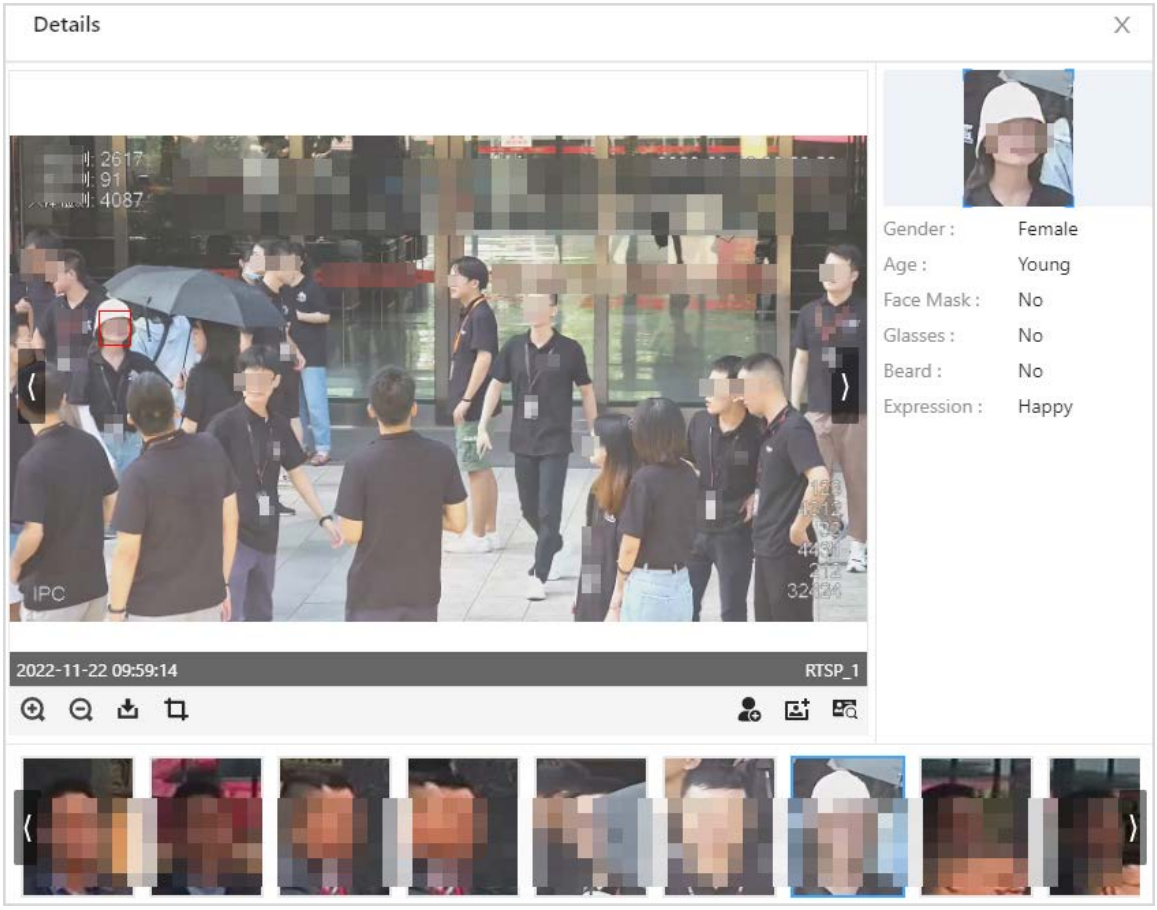
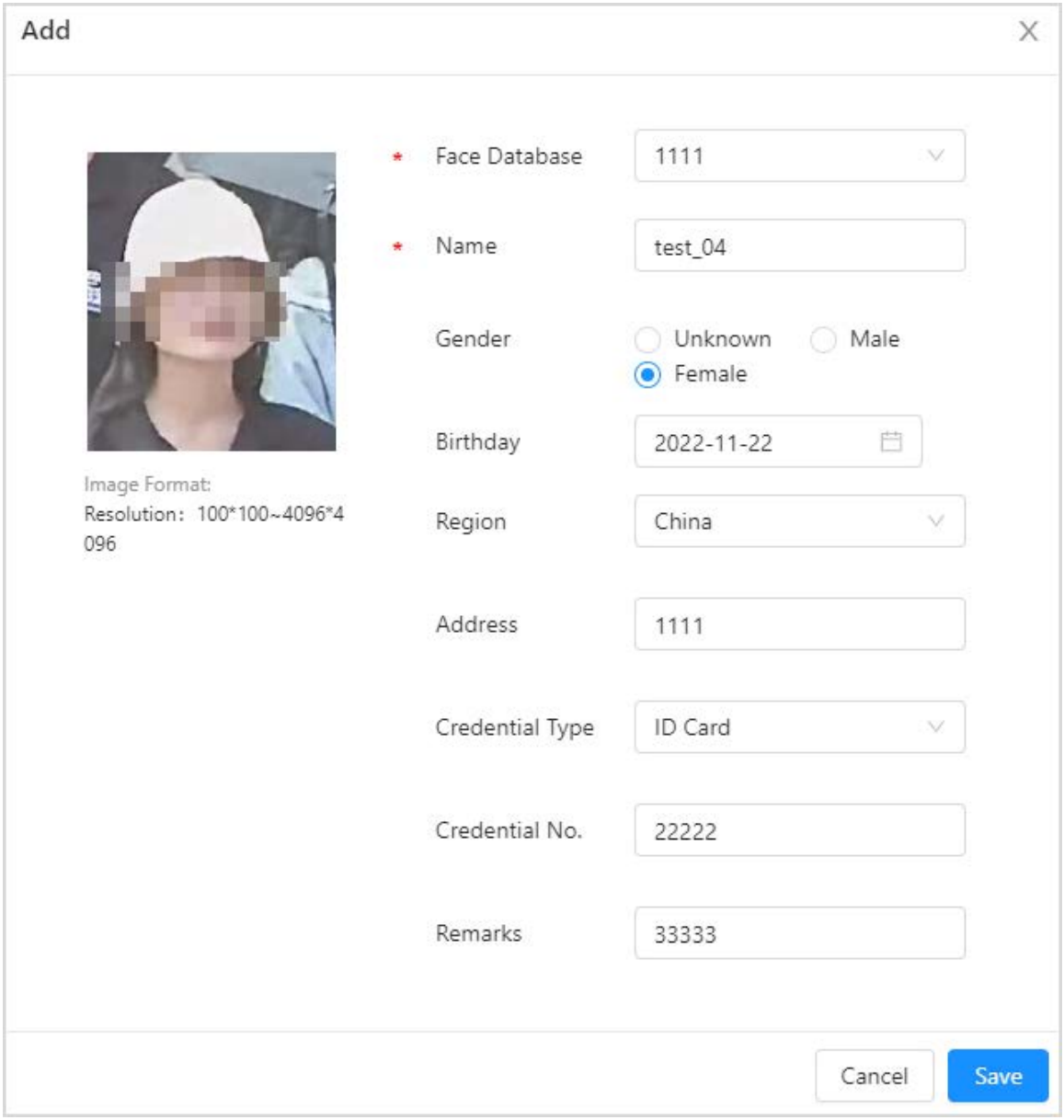


Table3-7 Icon description

Icon	Description
	Zoom in.
	Zoom out.
	Download images to local computer.
	Crop image. You can search for faces with cropped images or download the cropped face images.
	For details, see the following introduction.

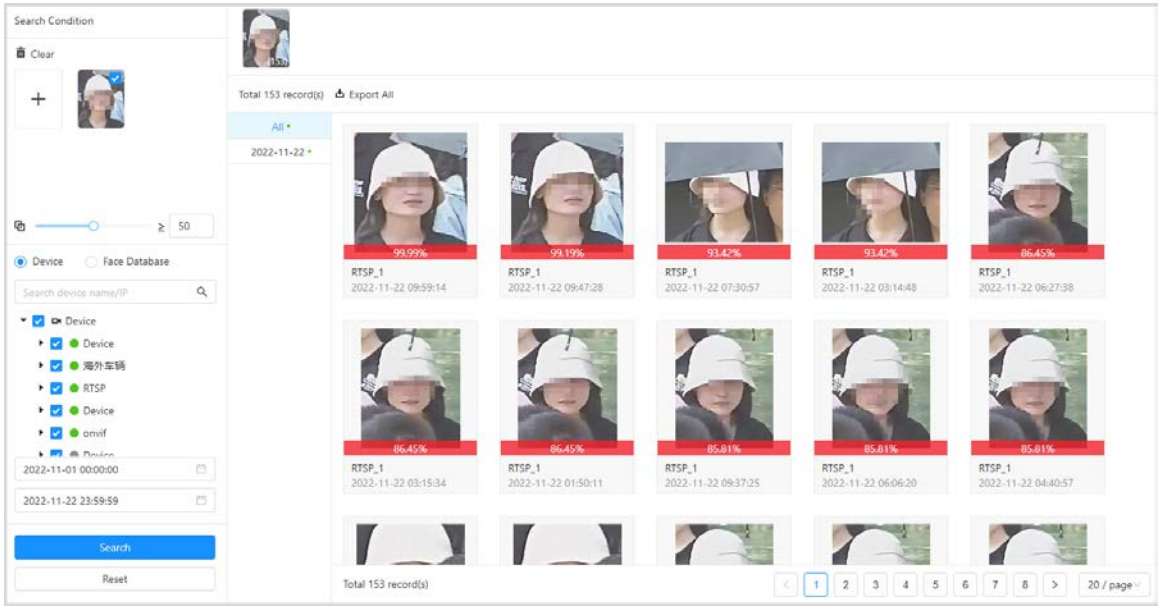
- Adding face databases. Click the corresponding of the image. and then configure the information. Click **Save** to add the snapshot face information to face database.

Figure 3-40 Add to face database



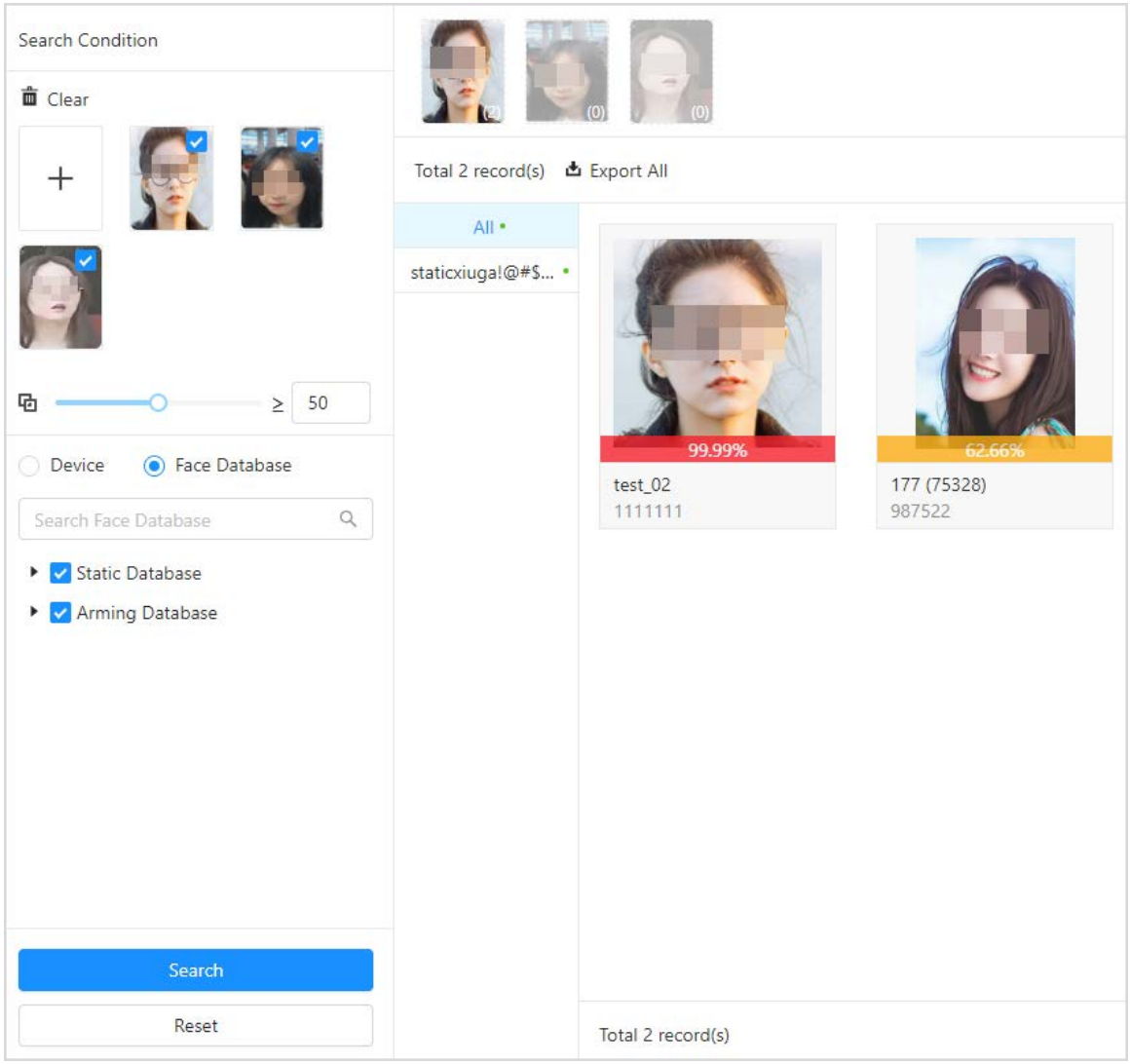
- Search for faces in snapshot database. Click the corresponding of the snapshot, the system uploads the snapshot to search conditions page. Select the channel, configure the similarity and time, and then click **Search**. The system displays the results.

Figure 3-41 Snapshot search



- Search for face in face database. Click the corresponding of the images, the system uploads the face database images to the search condition page. Select the channel, configure similarity and time, and then click **Search**, the system displays results.

Figure 3-42 Face database search



You can upload multiple face images at a time and the results will be displayed by classification.

3.6.2.2 Face Database Search

Face database search supports searching for face images under set conditions in face database. It compares the face images through face search and displays feedback and information on the similarity level.

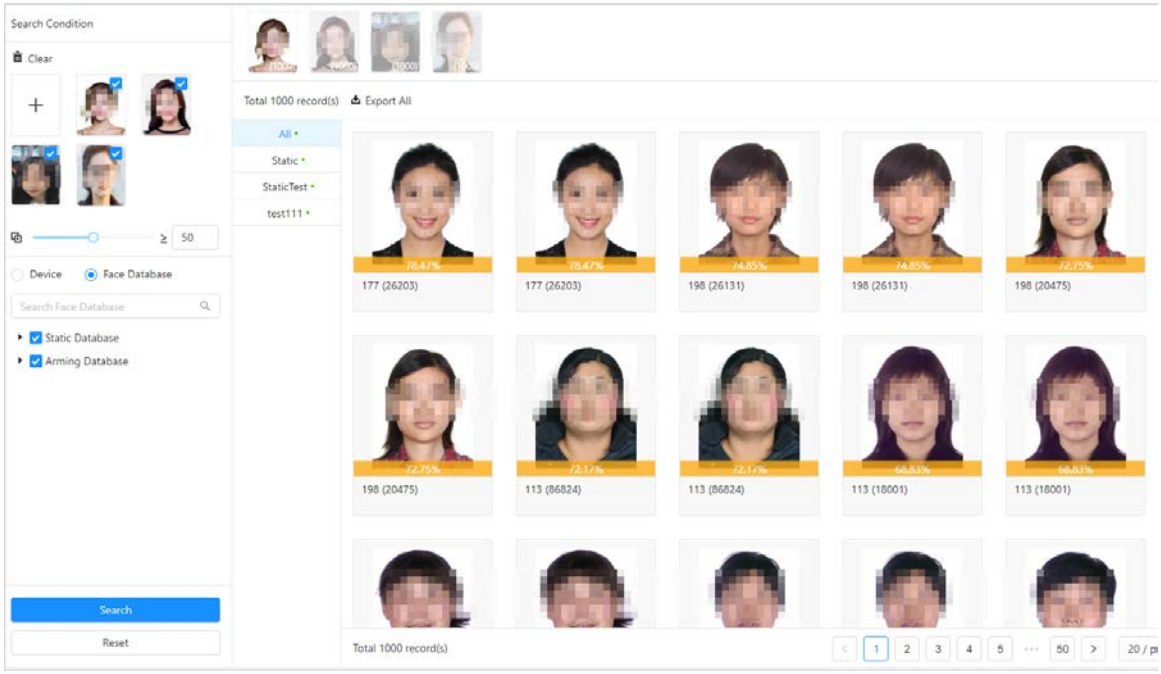
Step 1 Log in to the webpage, and then select **AI Search** > **Face Search**.

Step 2 Configure search conditions, and then select **Face Database**.

Step 3 Click **Search**, and the system displays results.

- You can search by the uploaded images, and the system will display the results.

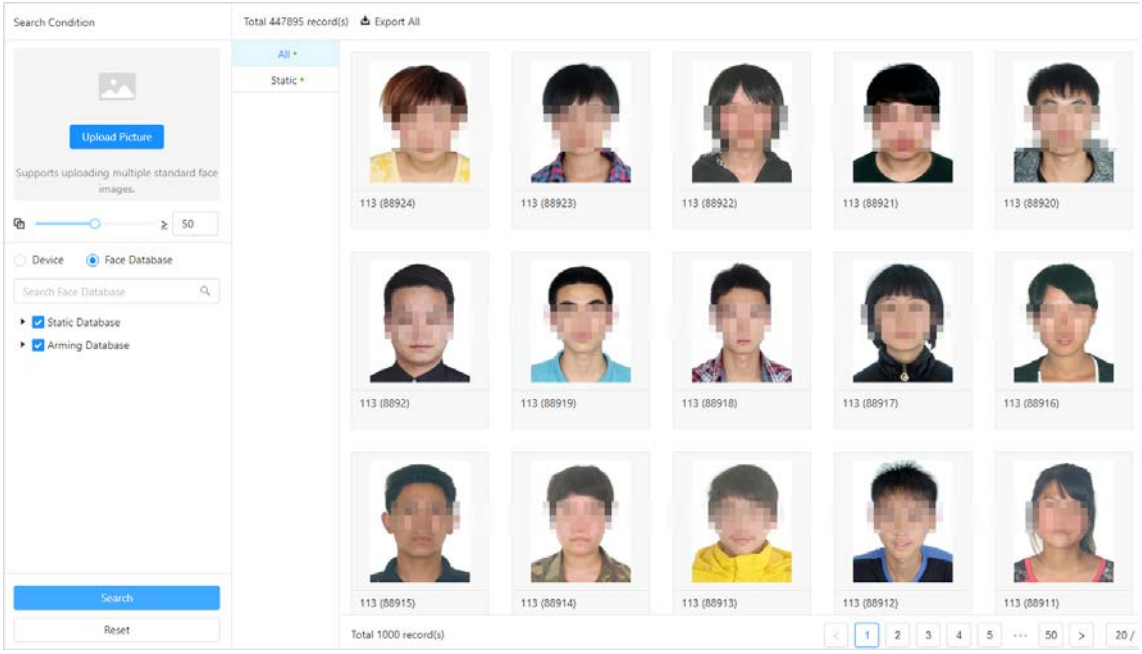
Figure 3-43 Upload images



- You can upload up to 100 images from local computers at the same time.
- If there are many target in the images, the system recognizes targets automatically. You can upload up to 32 images at a time to search for, but the image's file size is limited to20 MB.
- Click **Clear** to clear the uploaded images.
- Click **Reset** to reset search conditions but not clear uploaded images.

- You can search without uploading images, and the system will display the search results.

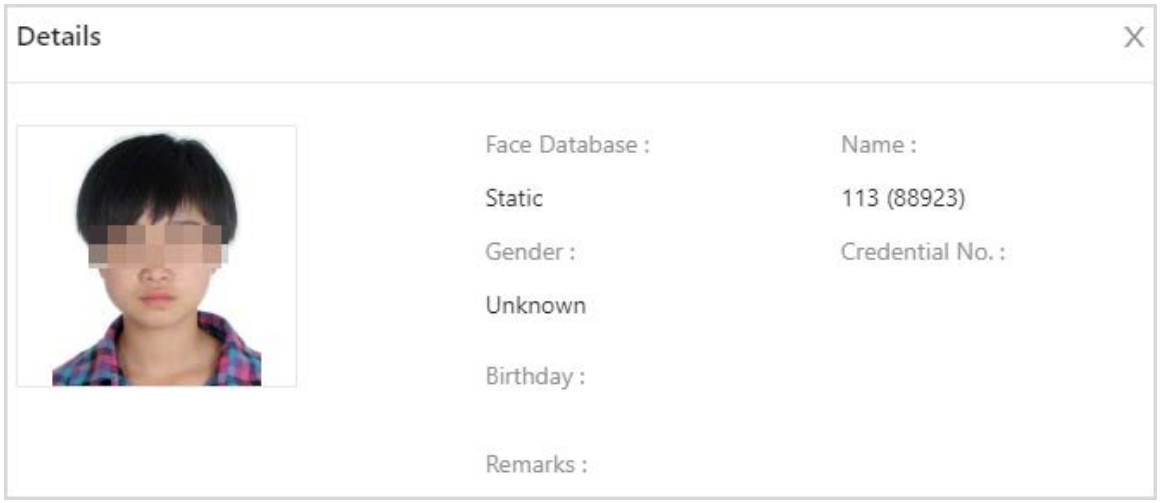
Figure 3-44 Snapshot search



Face database search operations:

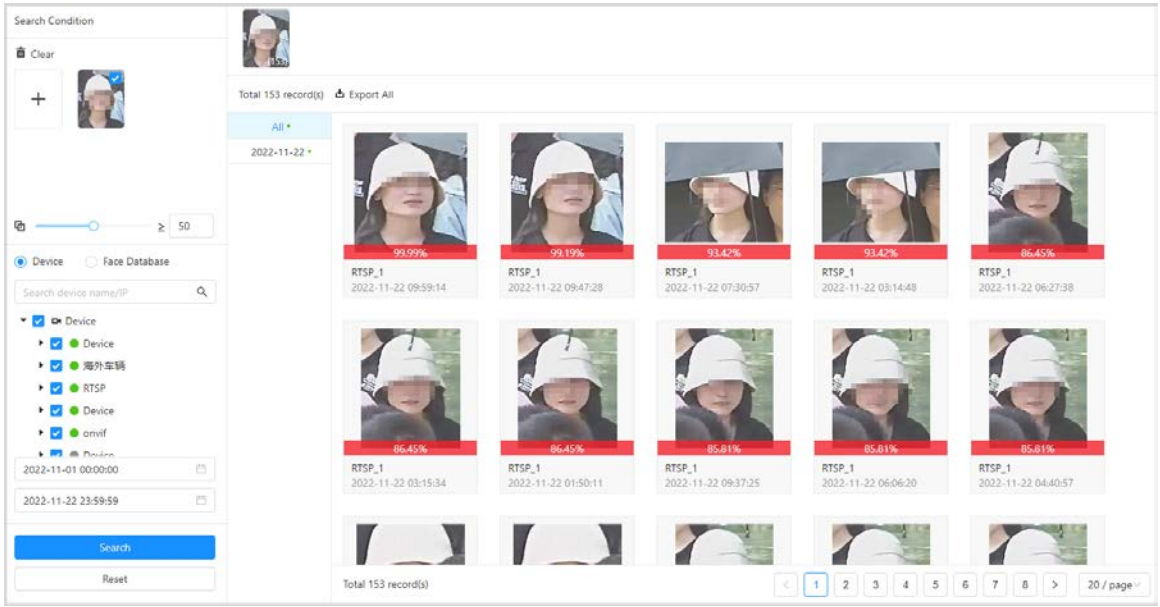
- View details. Click the corresponding of the image, the system displays the face details.

Figure 3-45 Detailed information



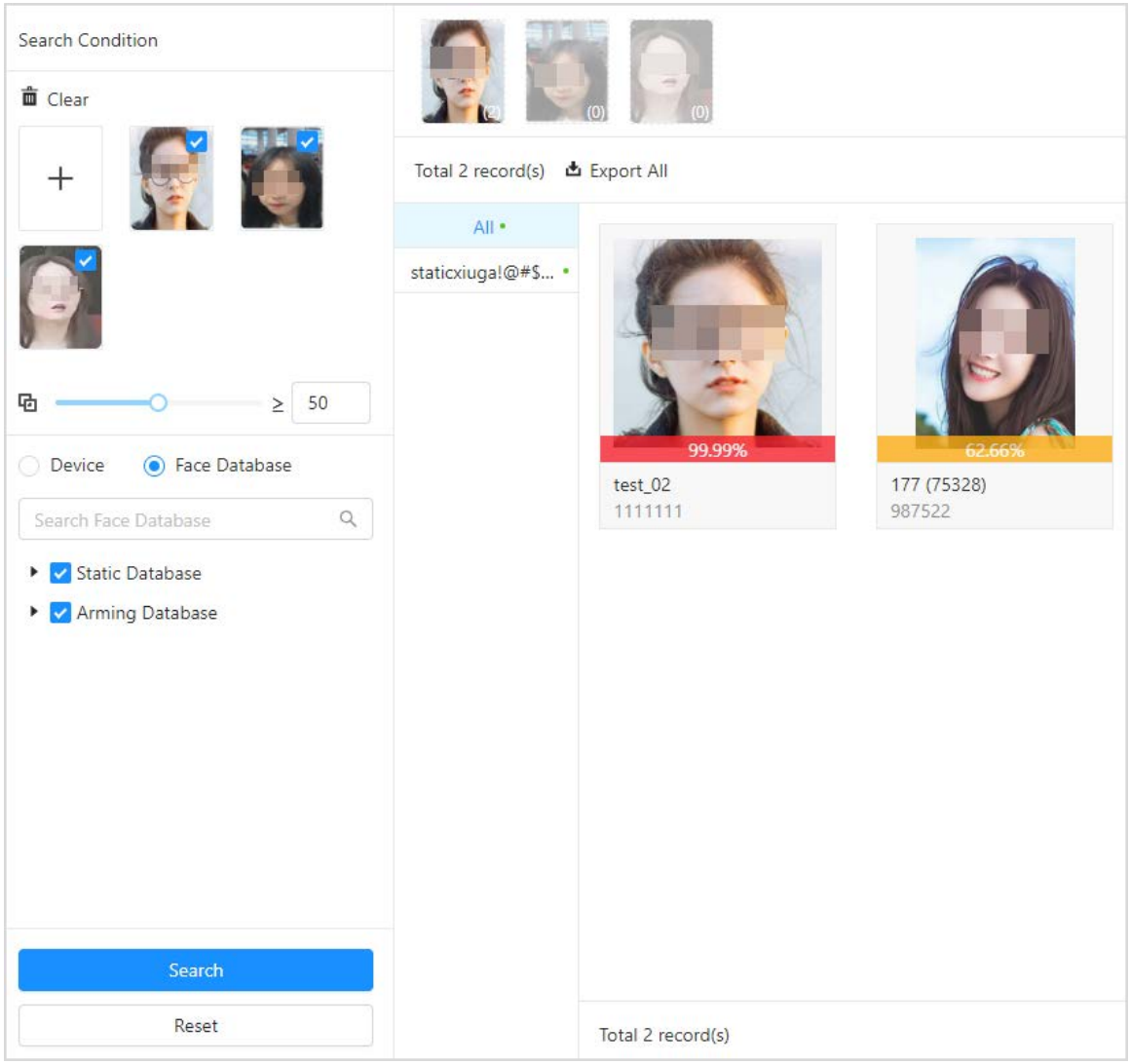
- You can search for faces in snapshot database. Click the corresponding of the snapshot, the system uploads the snapshot to the search conditions page. Select the channel, configure the similarity and time and then click **Search**. the system displays the results.

Figure 3-46 Snapshot search



- Search for faces in face database. Click the corresponding of the images, the system uploads the face database images to the search condition page. Select the face database, configure similarity and time, and then click **Search**, the system displays the results.

Figure 3-47 Face database search



You can upload multiple face images at a time and the results display by classification.

3.6.3 Human Search

Configure conditions of human features to search for humans or search by images through uploading images.

3.6.3.1 Search by Feature

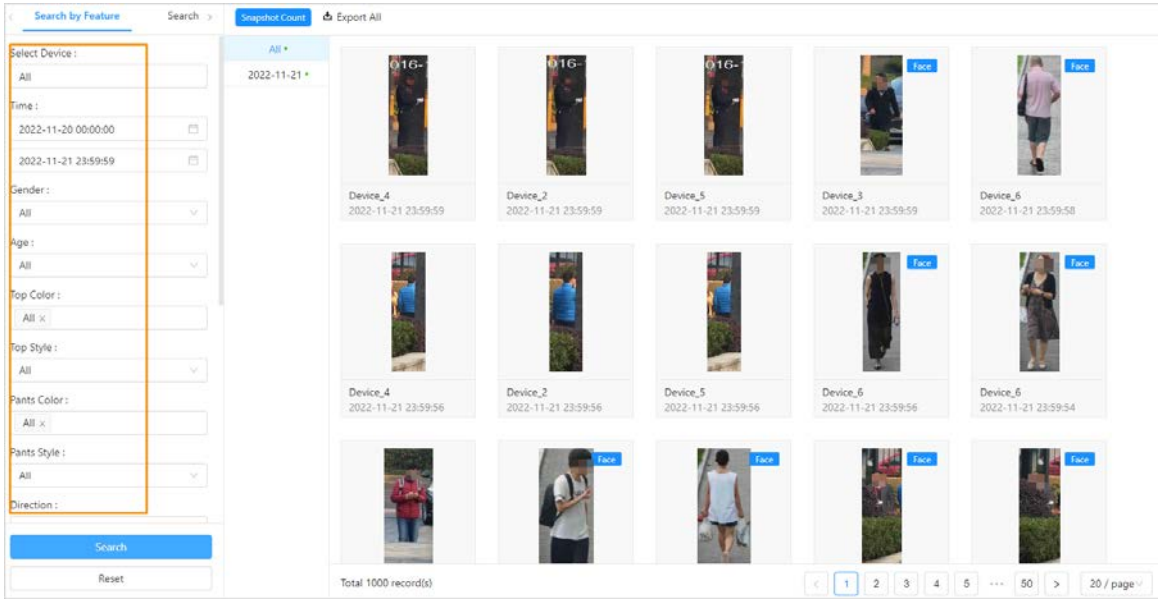
Configure search conditions of human to search for images to meet the requirements.

Step 1 Log in to the webpage, and then select **AI Search** > **Human Search** > **Feature Search**.

Step 2 Configure search conditions, and then click **Search**.

- Search results support view details and search by images.
- The "Face" on the upper right area on the image means the human image is related to the face. Click to search in snapshot face database. For details, see"3.6.2.1 Snapshot Database Search".

Figure 3-48 Searching by face



3.6.3.2 Search by Image

You can upload human images from local computer and configure the similarity of local images and snapshots captured by selected channels, and then search for human images that reach or above the threshold.

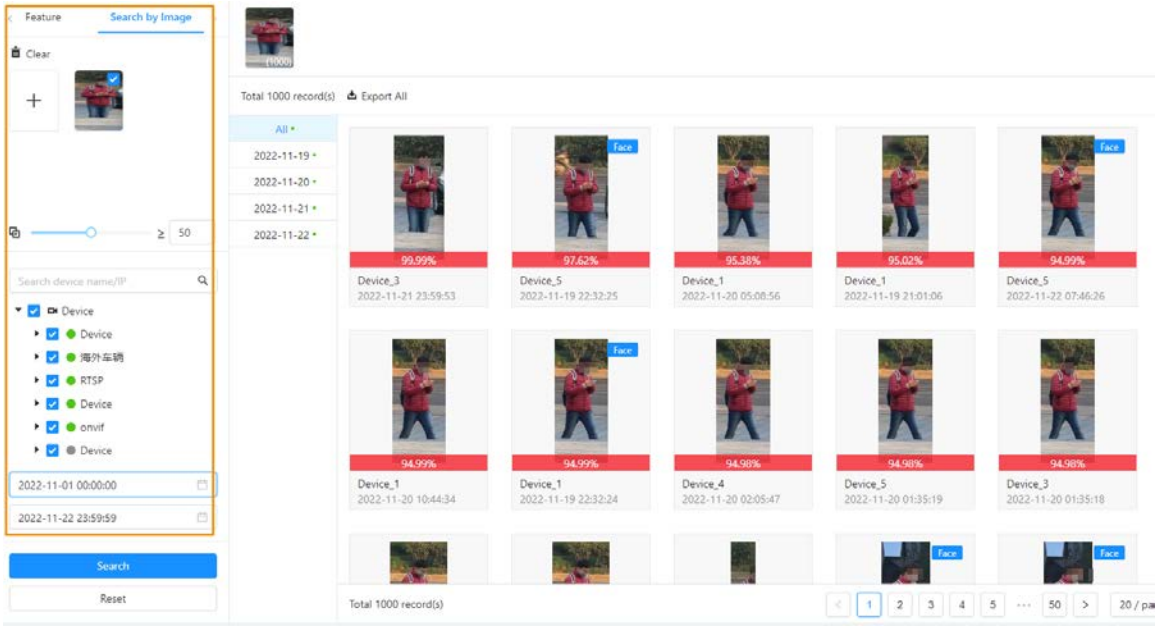
Step 1 Log in to the webpage. Select **AI Search** > **Human Search** > **Search by Image**.

Step 2 Upload human images from local computers, and then enter search conditions such as time, similarity, and channels.

Step 3 Click **Search**.

- You can upload up to 100 images from local computers at the same time.
- If there are many target in the images, the system recognizes targets automatically. You can upload up to 32 images at a time to search, but the image's file size is limited to 20 MB.
- Click **Clear** to clear the uploaded images.
- Click **Reset** to reset the search conditions. The uploaded images will not be cleared.

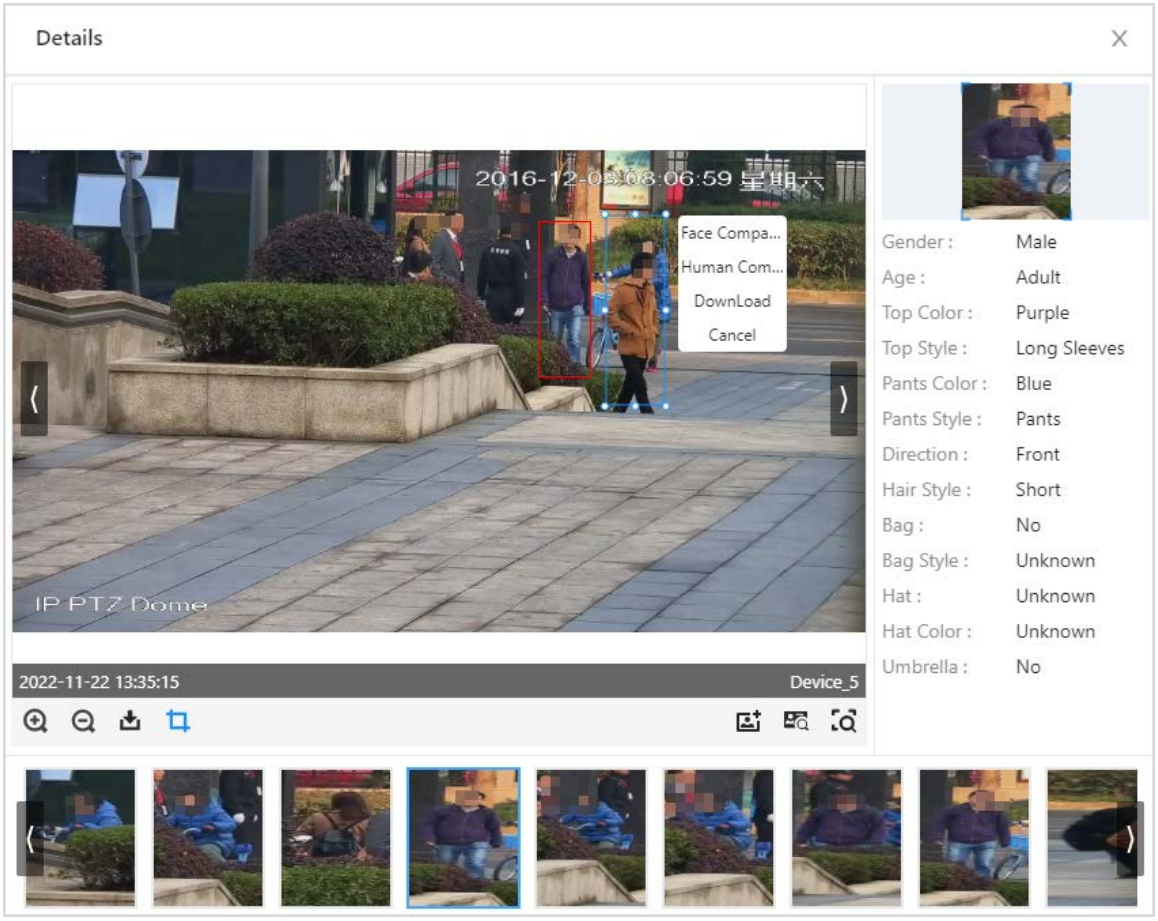
Figure 3-49 Searching by Image



Related operations:

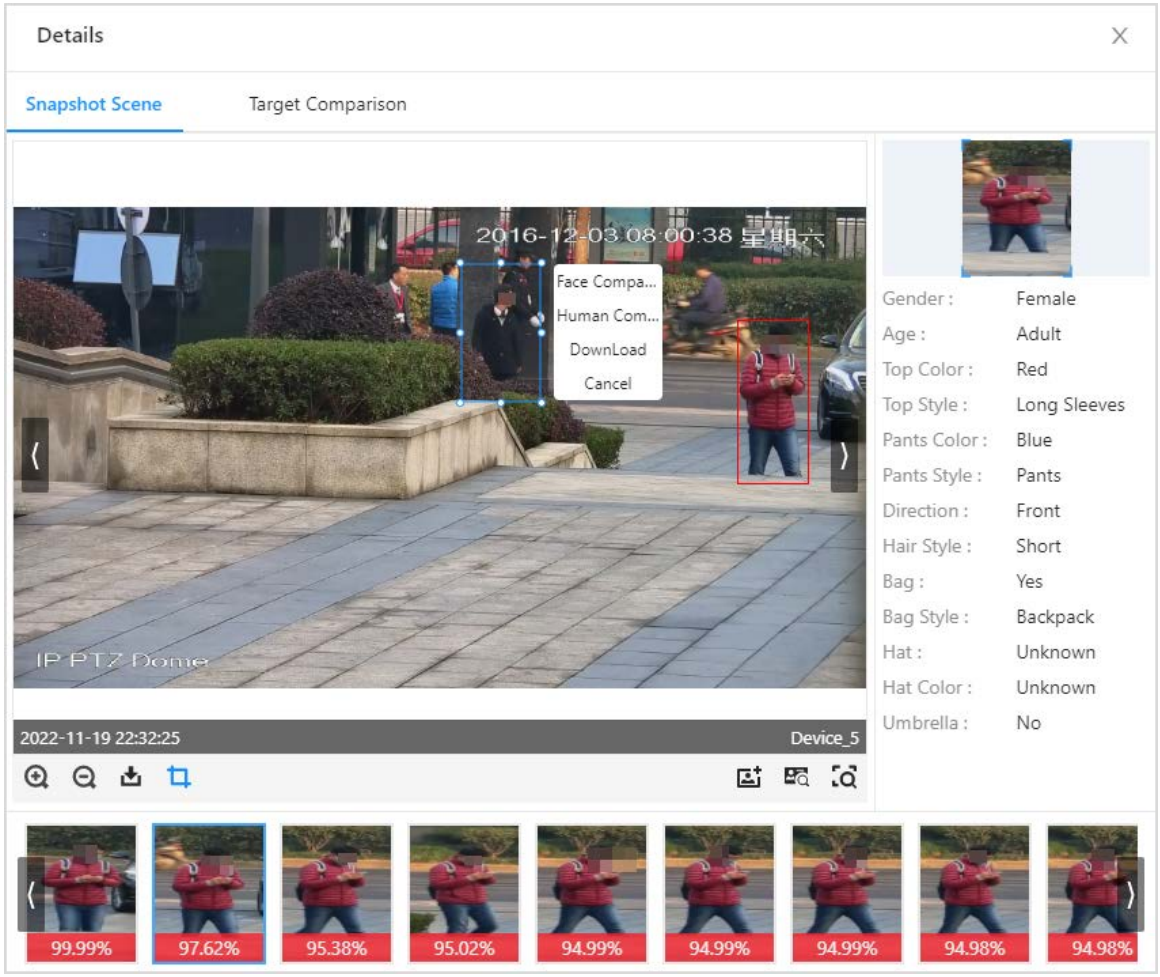
- Click to view details.
  - View detailed snapshot information.
    - Includes images of the scene, details on the features, and more.
    - Click to capture targets and search for faces, humans, and more. In addition, you can download snapshots.

Figure 3-50 Capturing targets



- Click to search for targets by image.
- For details, see Table3-7.

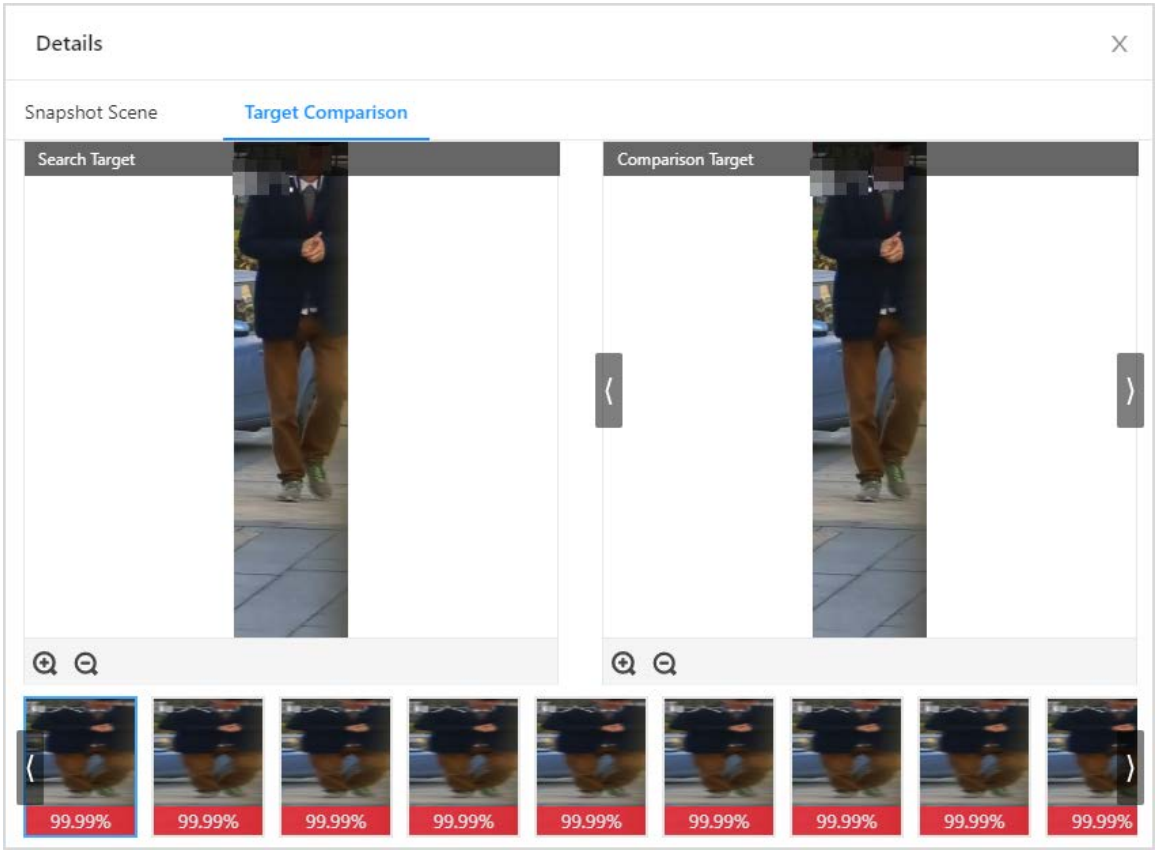
Figure 3-51 Snapshot scene



- Target comparison.

  Compare the snapshots with the images in the snapshot database.

Figure 3-52 Target comparison



- Click to search by images.

3.6.4 Vehicle Search

You can search for snapshots by uploading vehicle images or configuring vehicle features to search by image.

3.6.4.1 Search by Feature

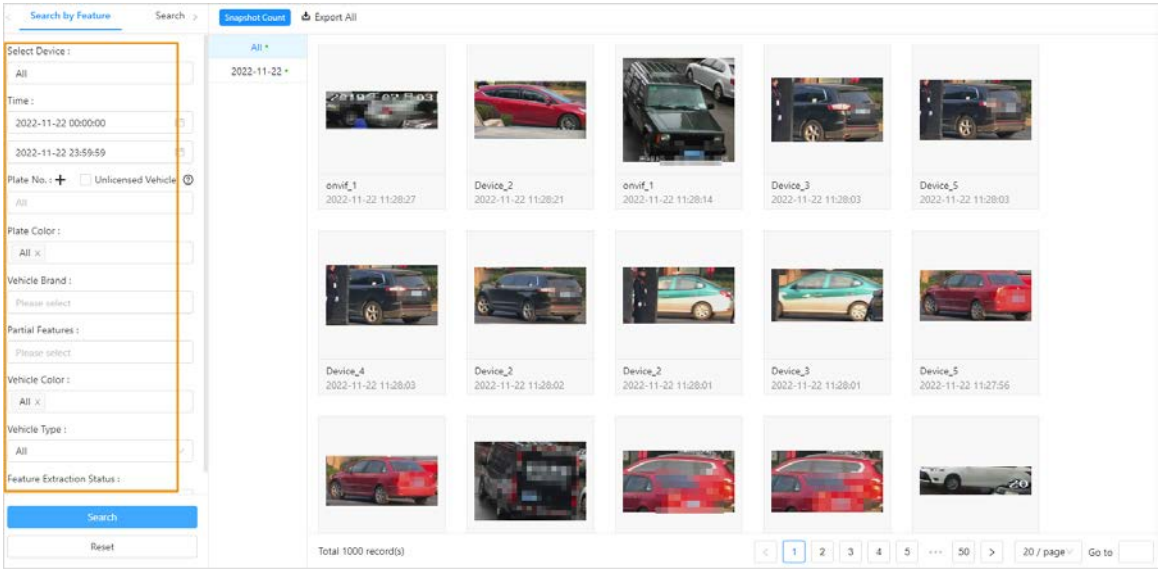
Specify search conditions to search for vehicles.

Step 1 Log in to webpage, and then select **AI Search** > **Vehicle Search** > **Search by Feature**.

Step 2 Specify search conditions, including device, time, plate number, vehicle brand, vehicle color, and more.

Step 3 Click **Search**, and the search results are displayed on the right.

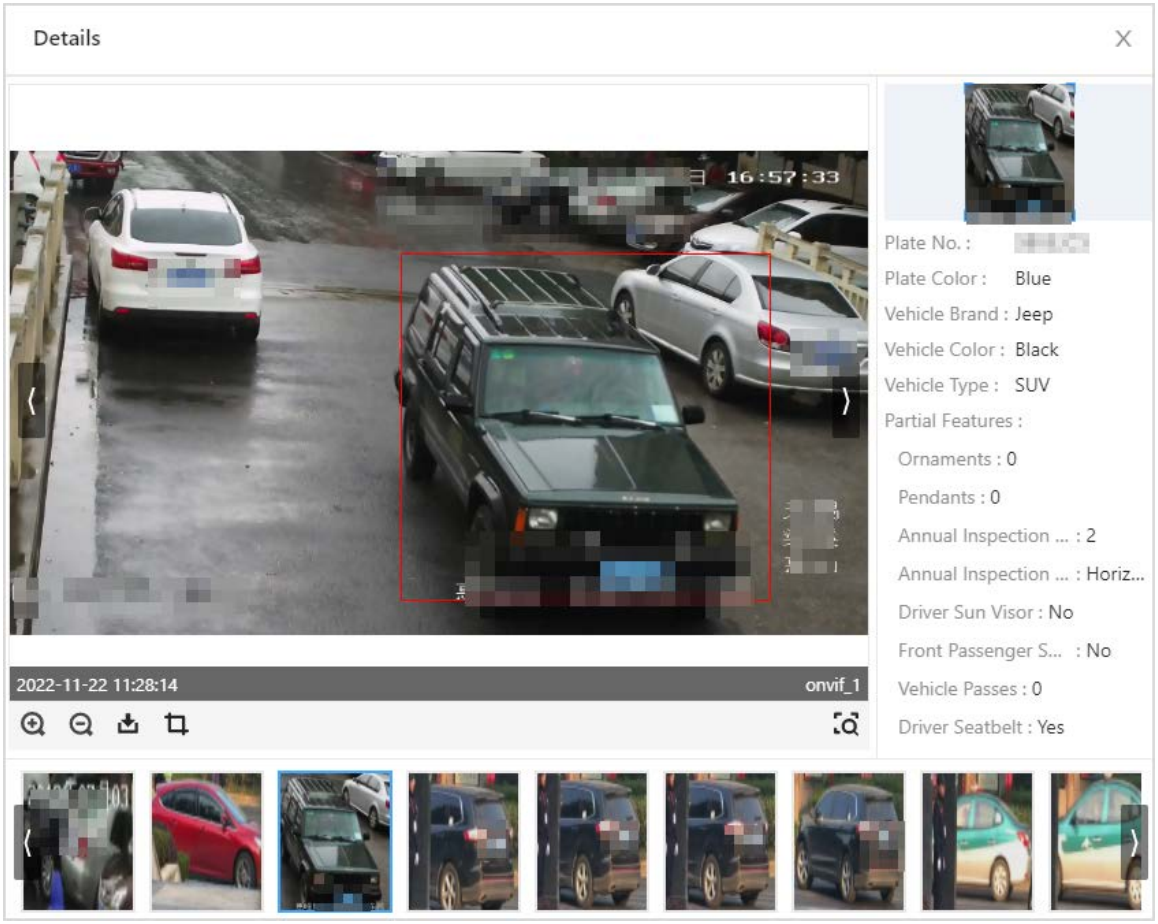
Figure3-53 Search by feature



Related operations：

- Click to view details. Click to capture a vehicle image in scene to search by image or download the captured vehicles.

Figure 3-54 Capturing vehicle



- Click to upload images in scene to search by image.

3.6.4.2 Search by Image

You can upload vehicle images from local computers and set the similarity. The system searches for the vehicle images that meet the similarity from the snapshot database.

Step 1 Log in to the webpage, and then select **AI Search** > **Vehicle Search** > **Search by Image**.

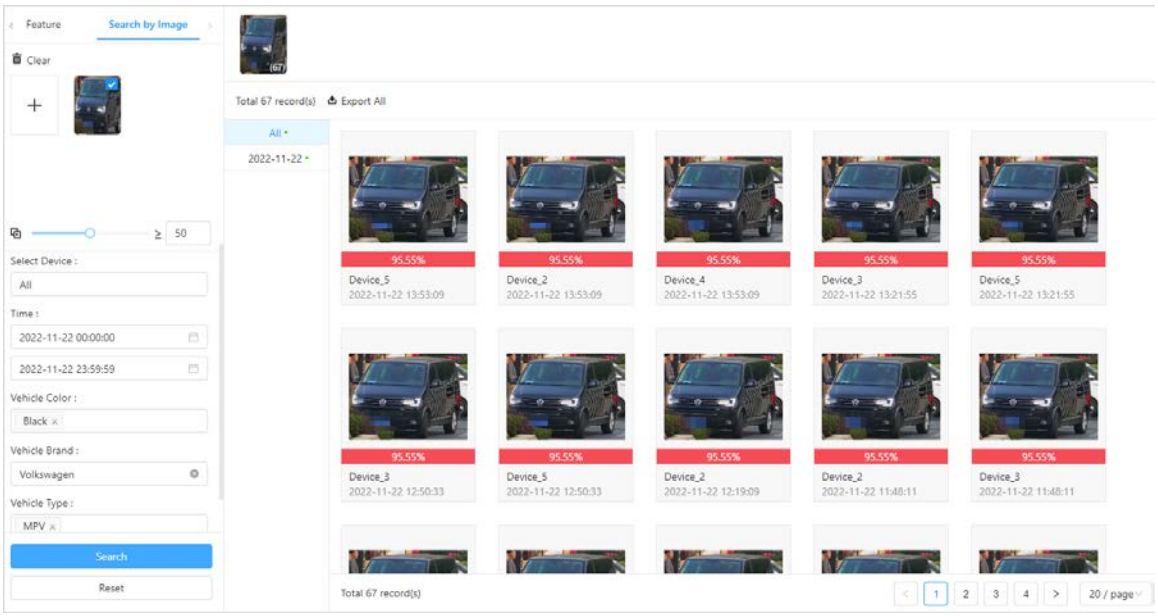
Step 2 Upload vehicle images from local computers, and then set search conditions, including similarity, channels and time.

- If there is more than one vehicle on the image, the system will recognize them all, and you need to select the target you want to search. The selected one will be displayed on the right.
- You can select only one vehicle image at a time to search for. After you select the image, the system will automatically recognize the vehicle color, brand and type.

Step 3 Click **Search**.

- Click **Clear** to clear the upload images.
- Click **Reset** to reset the search conditions. The uploaded images will not be cleared.

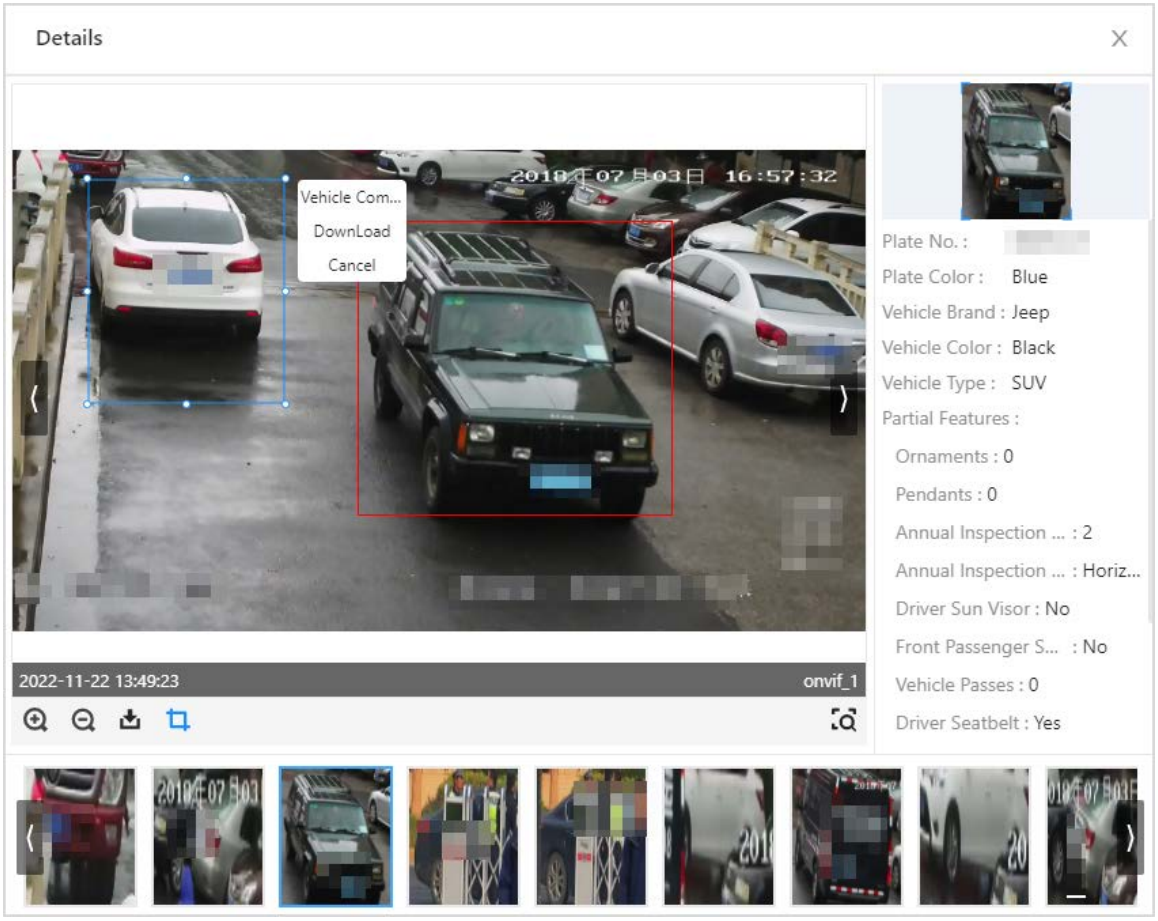
Figure 3-55 Searching by image



Related operations:

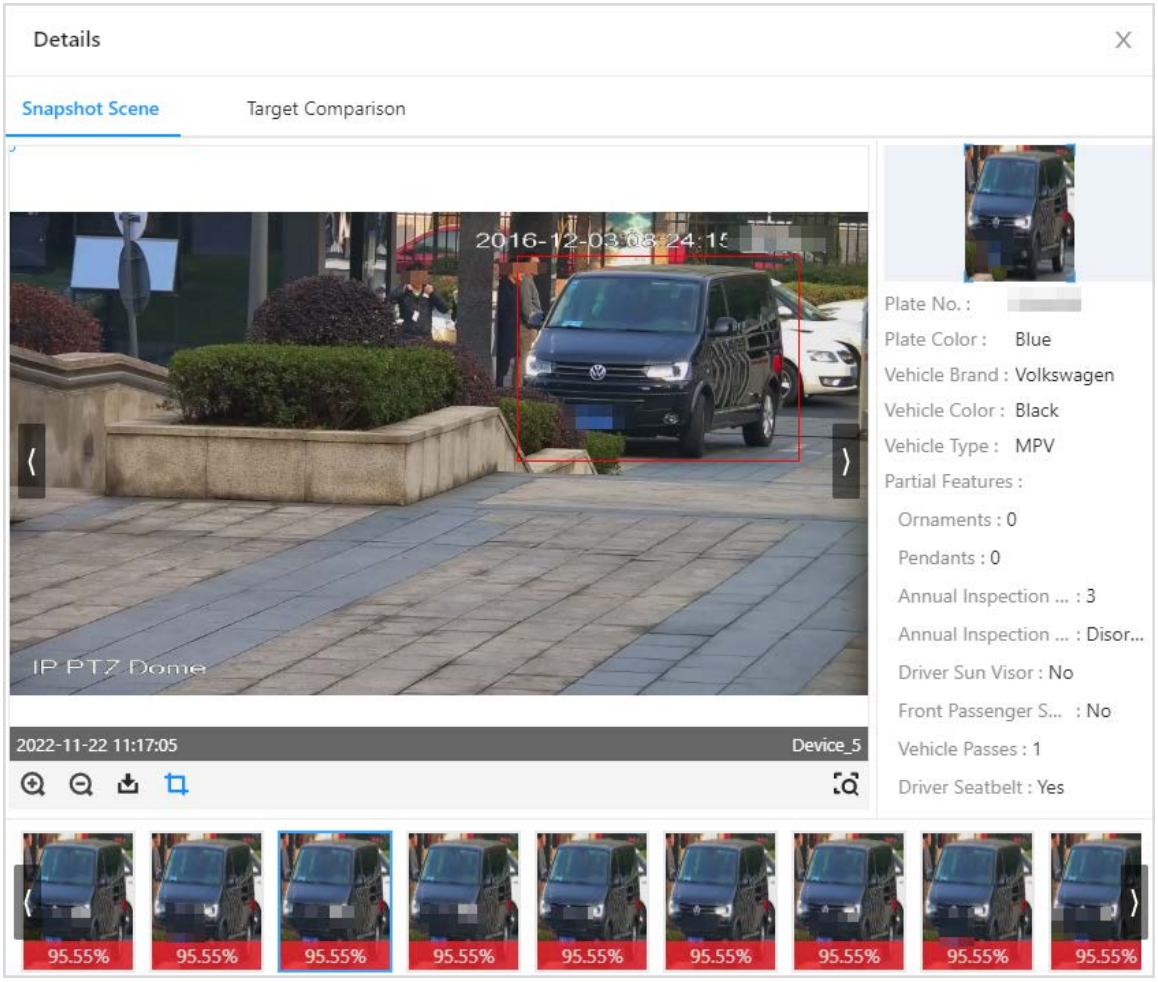
- Click to view details.
  - View detailed snapshot information.
    - Including scene images, features, and more.
    - Click to capture vehicles to search by image and download the captured vehicle images.

Figure 3-56 Capturing vehicle



- Click to search for targets in scene by image.
- For icon descriptions, seeTable3-7.

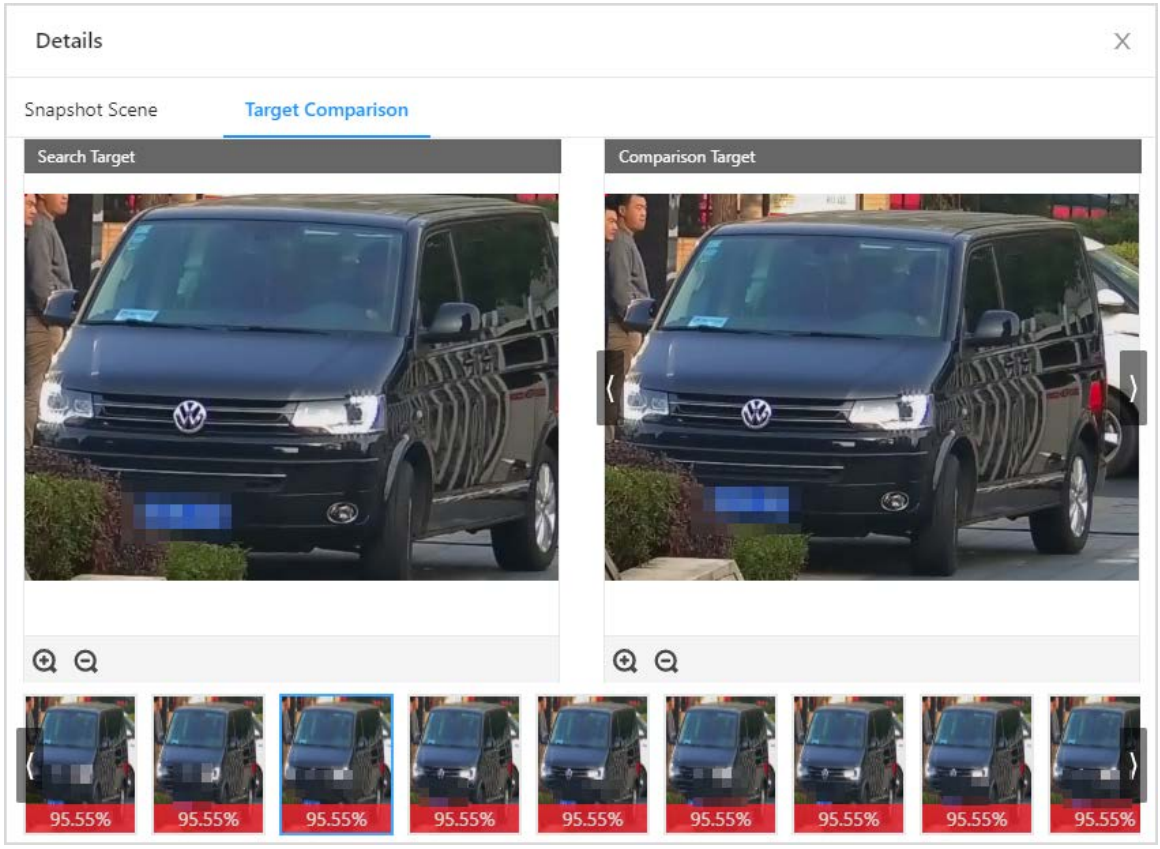
Figure 3-57 Snapshot scene



- Target comparison.

  Compare the upload target in the snapshot database.

Figure 3-58 Target comparison



- Click to search by image.

3.6.5 Non-Motor Vehicle Search

Configure the search conditions or upload non-motor vehicle images to search by image.

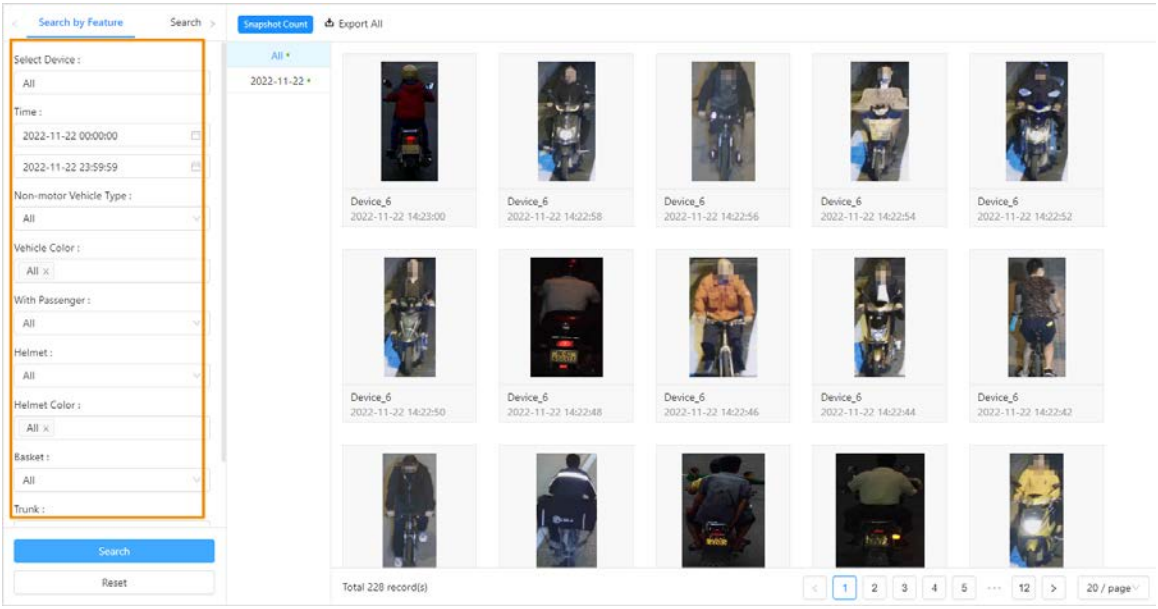
3.6.5.1 Search by Feature

Configure the non-motor vehicle search conditions to search for non-motor vehicles.

Step 1 Log in to the webpage, select **AI Search** > **Non-Motor Vehicle Search** > **Search by Feature**.

Step 2 Configure the search conditions, and then click **Search**.

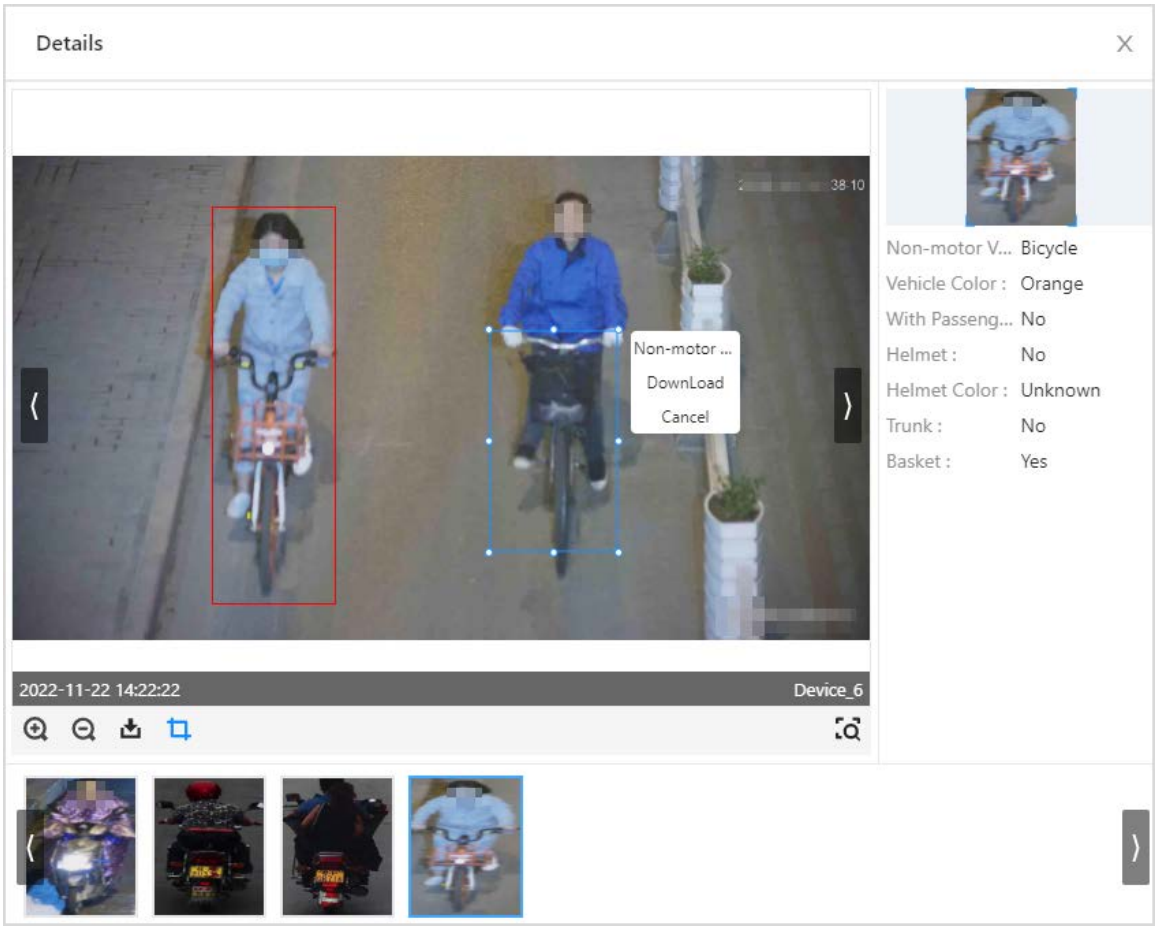
Figure3-59 Search by feature



Related operations:

- Click to view details. Click to capture targets in scene images to search by image or download the target image.

Figure 3-60 Capturing non-motor vehicle



- Click to search for the targets by image.

3.6.5.2 Search by Image

You can upload non-motor vehicle images from local computers, and then set search conditions to search for non-motor vehicle images from snapshot database.

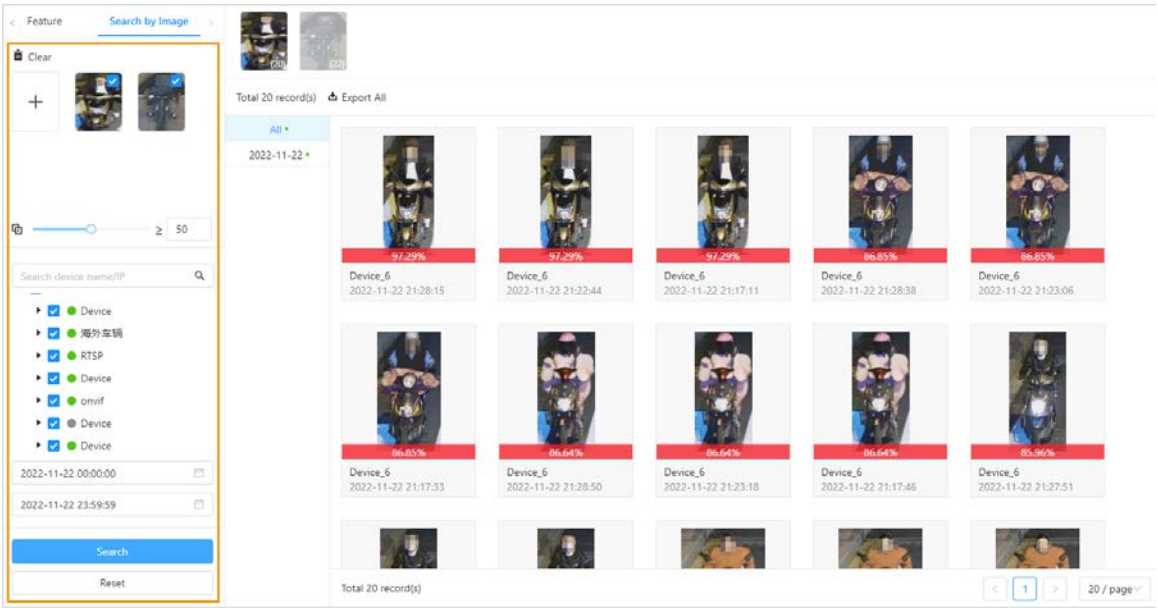
Step 1 Log in to webpage, and then select **AI Search** > **Non-motor Vehicle Search** > **Search by Image**.

Step 2 Upload images from local computers, and then set search conditions, including similarity, device, channel, time, and more.

Step 3 Click **Search**.

- You can upload up to 100 images from local computers at the same time.
- If there are many target in the images, the system recognizes targets automatically. You can upload up to 32 images at a time to search, but the image's file size is limited to 20 MB.
- Click **Clear** to clear the uploaded images.
- Click **Reset** to reset the search conditions. But the uploaded images will not be cleared.

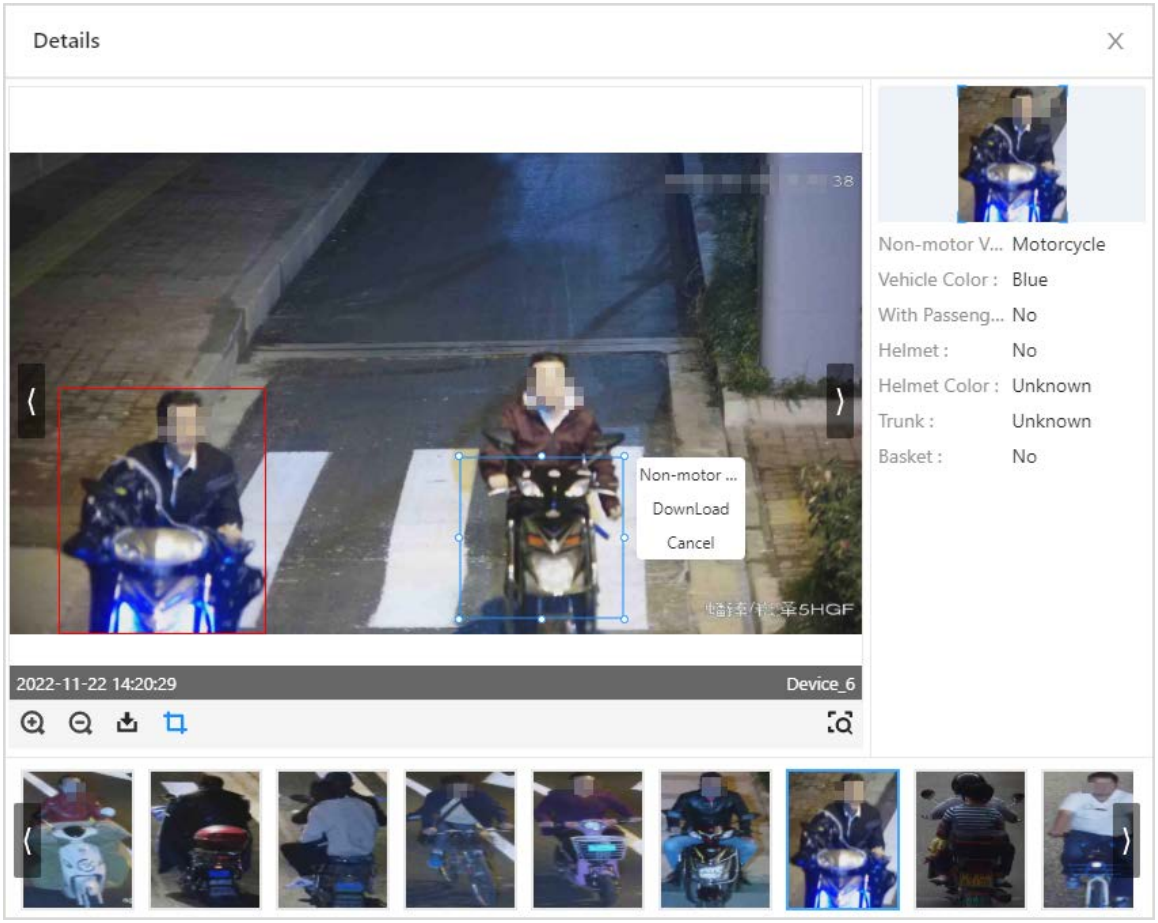
Figure 3-61 Searching by image



Related operations:

- Click to view details.
  - Includes scene images, features, and more.
  - Click to capture non-motor vehicle in scene images to search for non-motor vehicles or download the captured images.

Figure3-62 Capture targets



- ◇ Click to search for targets by image.
- ◇ For icon descriptions, seeTable3-7.

- Click to search by image.

3.7 Preview

You can view live videos, face snapshots and alarm information.

Video fluency is influenced by your computer. Normally, real time video of 1 or 2 channels is relatively smooth. When the real time video lags, click to download client for live view. For details, see "3.8 Client Operations".

Step 1 Log in to the webpage, and then click **Live**.

Step 2 Click to display the device list, and then double-click a device channel.

Figure 3-63 Live view

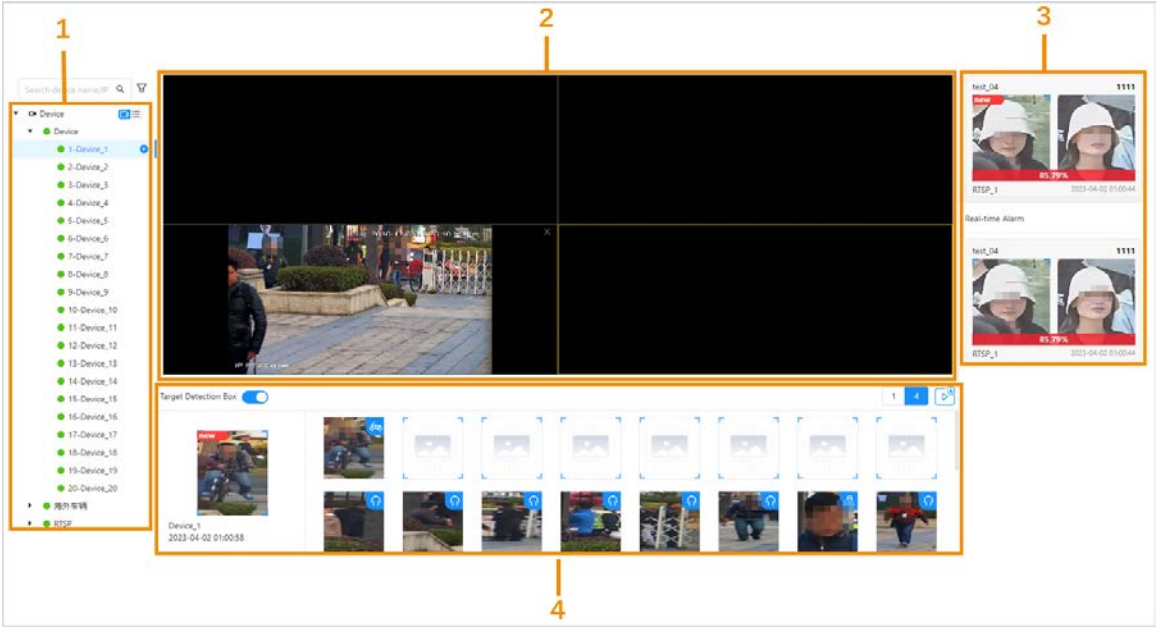


Table 3-8 Module description

No.	Module	Description
1	Device list	Displays device list and name. ● means the devices or channels are online, means the devices or channels are offline. ● means the live view channel. ● Supports fuzzy search for the device name or IP address. ● Click to filter the online or offline devices. ● Click to switch the device list or channel list.
2	Live view	Live view videos. ● You can select 1split or 4 splits. ● Click to download client for live view.
3	Alarm	Push real time alarm information, and display comparison results. ● Prerequisite: Add human images to armed face database and armed to channels. ● Top the latest alarm information on the alarm list, and displays **New** on the upper left corner. ● Hover your mouse over the alarm list to stop refresh real time alarm information (the topped latest alarm information still refreshes). After moving your mouse, the alarm information continues to refresh.

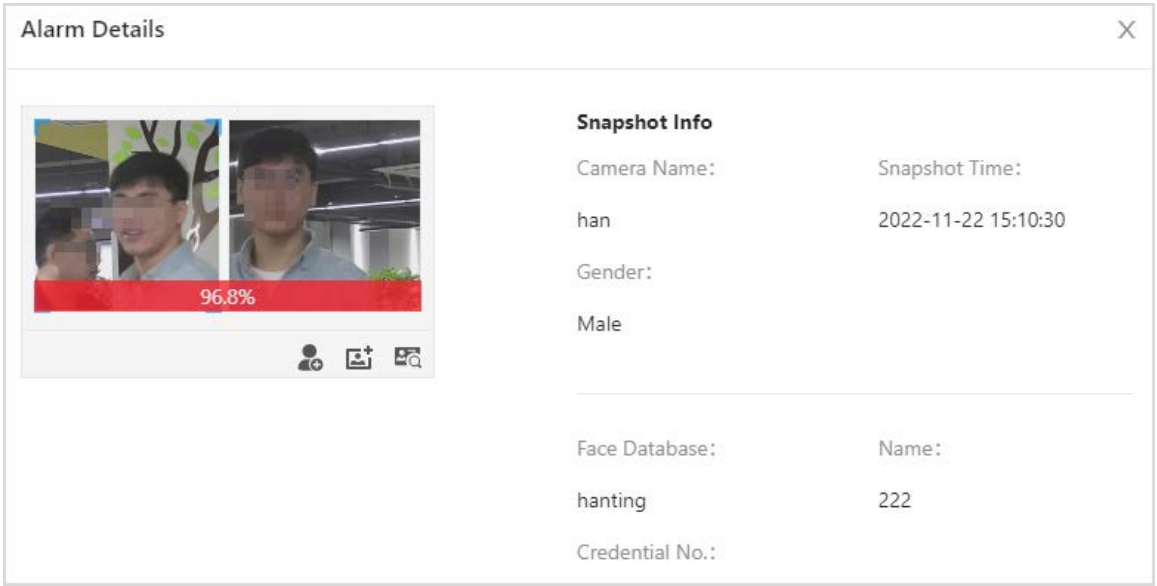
No.	Module	Description
4	Snapshot	Remote devices capture snapshots. ● Target Detection Box: ● After enable live view, the device displays captured targets on the live view. The latest snapshots display on the left, and displays **New** on the upper left corner. ◇ : Face. ◇ : Human. ◇ : Vehicle ◇ : Non-motor Vehicle. ● Hover your mouse over the real time snapshot list to stop refresh real time snapshot information (the left latest snapshot still refreshes). After moving your mouse, the information continues to refresh.

Related Operations

Click real alarm images to view the details. Snapshot database and face database search are available.

- Snapshot search, for details, see "3.6.2.1 Snapshot Database Search".
- Face database, for details, see "3.6.2.2 Face Database Search".

Figure 3-64 Alarm details



3.8 Client Operations

If the video lags or fails caused by the lacked web resources, you can download client to view real time videos.

3.8.1 Client Installation

Download and install intelligent micro center client (hereinafter as "client").

Step 1 You can download client by one of the 2 following ways:

- Download client from webpage.
  1. Enter http://*IP address* in Chrome, and then press Enter.
  2. Click **Client Download**.
     the installation package of the Client will be downloaded to the computer.
- On the **Preview** page, click  to download installation package.

Step 2 After the download is finished, open the installation package, double click the installation file, for example "General_IVS-MC8000-Client_Chn_Base_*Version*.exe", and then follow the on-screen instructions to complete installation.

Step 3 Double-click  on the desktop, and then enter the username, password and click **Login**.

Figure3-65 Live view

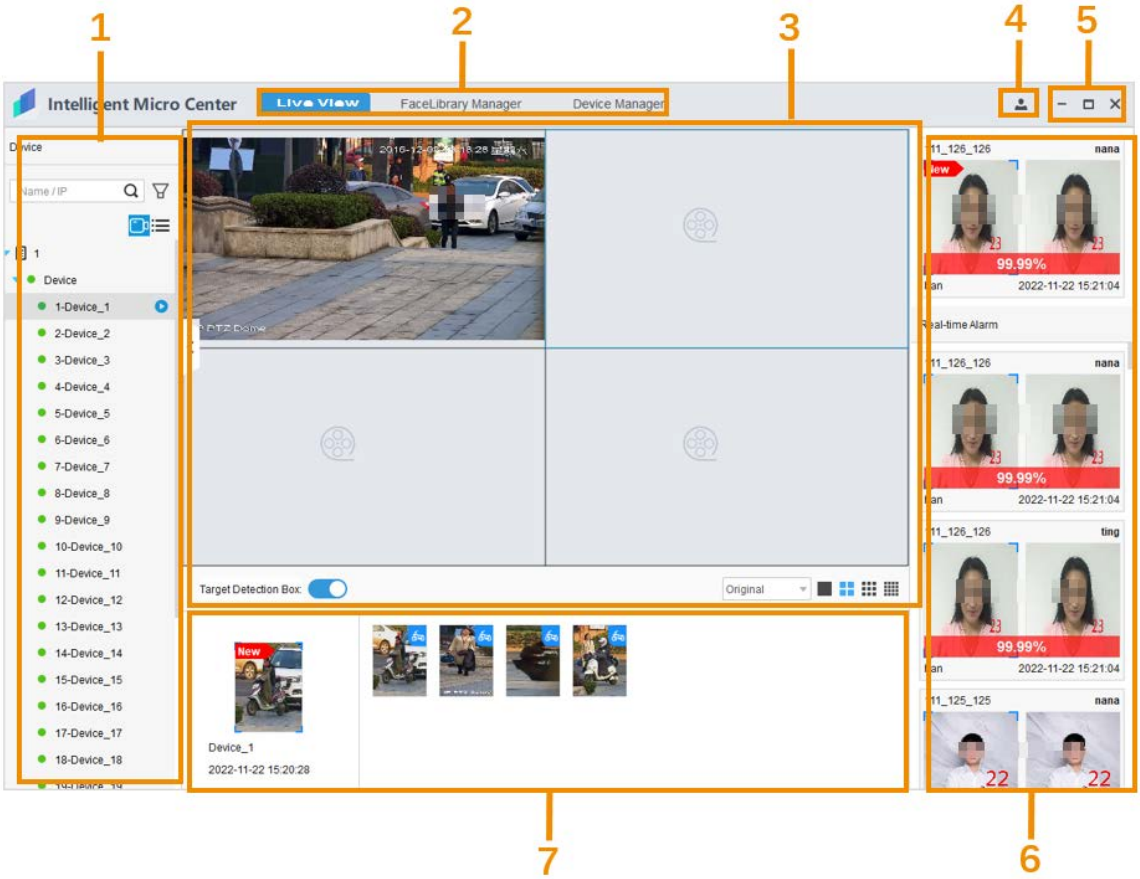


Table3-9 Client description

No.	Description
1	Function area.
2	Live view: displays real time videos.
3	• Change password, • View system information. • View open source statement. • View license agreement.
4	Maximize, minimize and exit. Double-click any area of the top to maximize or minimize the client.
5	Device list: displays the added servers, remote devices and channels.
6	Snapshot list.
7	Alarm information list. Double-click the alarm information to view details.

3.8.2 Adding the Servers

Before live view videos, you need to add servers to client.

Step 1 Log in to the webpage, and then click **Device Manager**.

Step 1 Click the + on the bottom left corner to add servers.

Figure3-66 Add servers

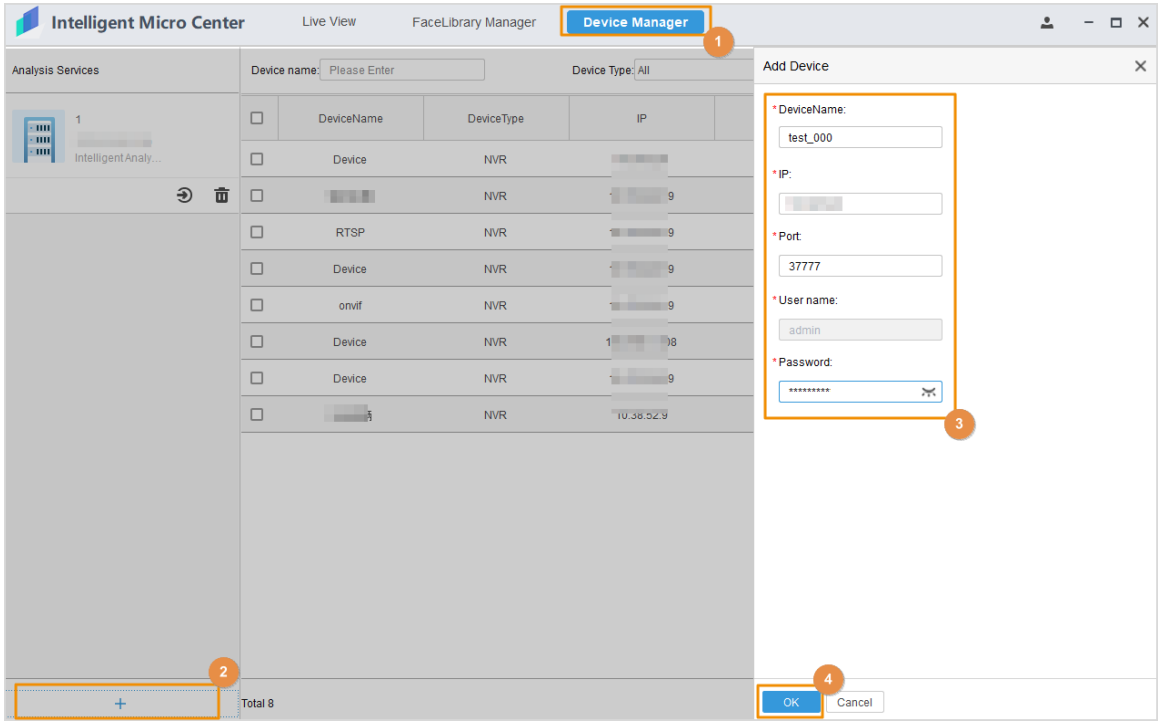


Table3-10 Parameter description

Parameter	Description
Device Name	You can customize the server name to distinguish from other servers on the client.
IP	The server's IP address.
Port	The server's port number (37777 by default).
Username	The username and password of the server (the username is admin by default and the password was set when initializing on the webpage.
Password	

Step 3 Click **OK**.

After you added the server, the server login and displays device information automatically.

- You can add, delete, edit and arm devices and channels on the webpage, for details, see"3.3 Device Management"
- You can log in to the client again to refresh device information.
- The login password will expire in seconds, and you need to log in again.

Related Operations

- Click to change the password of the server.
- Click to log out and click to log in.
- Click to delete servers.
- On the top area of the" Device Manager", you can set the search conditions includes device name, IP address, device type, and more.

3.8.3 Live View

After you logging in to the server on client, you can view real time videos and alarm information.

Step 1 Log in to the client, and then click **Live View**.

Step 2 Click on the left device list to select the server and the device.

Step 3 You can enable live view of channels by the following 3 ways:

- On the live view page, select a view window, and then double-click any channels to enable live view.
- On the channel list of the left side, select any channels and press the left mouse button to drag the channel to the live view window to enable live view.
- Select live view window, and then right-click **Live view** to enable live view.

Step 4 View real time alarm, and then double click alarm records to view details.

Figure 3-67 Live view

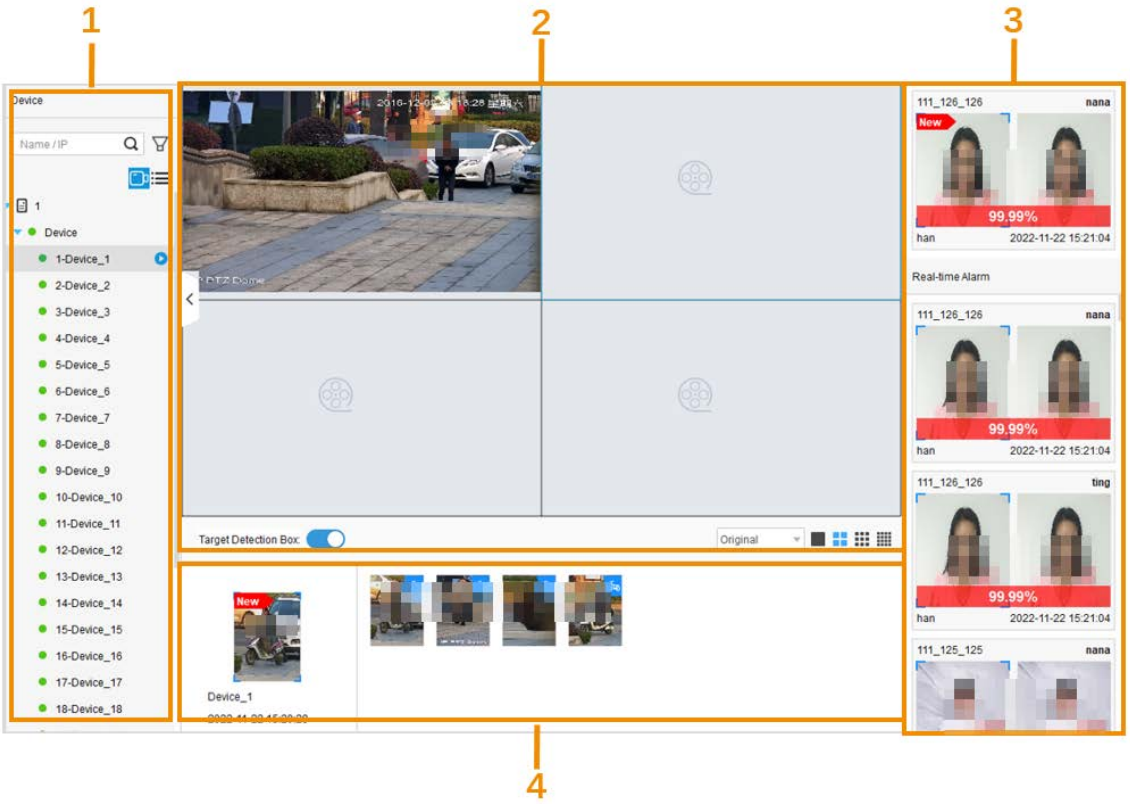


Table 3-11 Function module Description

No.	Module	Description
1	Resource list	Displays servers, device and channels. • : the server is offline. right-click **Login** to log in to the server. : the server is online, right-click **Logout** to log out. • : the device or channel is online. : the device or channel is offline. • the channel is live view, right-click"Stop view" to close video. channels without : the channel do not enable live view, and then right-click "Start View" to enable live view. • You can fuzzy search by device names or IP addresses. • Click to switch between online or offline devices. • Click to switch device channels or display by device channels.

No.	Module	Description
2	Live View	live view videos that supports selecting display scale and window splitting. ● Click Original on the bottom area to select display scale on the drop down list. ◇ Full Screen: Display full screen. ◇ Original: display the actual image, the image might appear letterbox. ● Split the window according to your needs. Select on the bottom area. window splitting supports 1, 4, 9, and 16 splits. the client can split up to 16 windows. ● Hover the mouse on the videos, and then click on the upper area to close live view.
3	Real time alarm	Push real time alarm information, and display comparison results. ● Prerequisite: Add human images to armed face database and armed to channels. ● Top the latest alarm information on the alarm list, and displays **New** on the upper left corner. ● Hover your mouse over the alarm list to stop refresh real time alarm information (the topped latest alarm information still refreshes). After moving your mouse, the alarm information continues to refresh.
4	Snapshot	Remote device captures snapshots. ● Target Detection Box: ● After enable live view, the device displays captured targets on the live view. The latest snapshots display on the left, and displays **New** on the upper left corner. ◇ : Face. ◇ : Human. ◇ : Vehicle ◇ : Non-motor Vehicle. ● Hover your mouse over the real time snapshot list to stop refresh real time snapshot information (the left latest snapshot still refreshes). After moving your mouse, the information continues to refresh.

3.8.4 Face Library Management

Step1 Log in to client, and then click **Face Library Manager**.

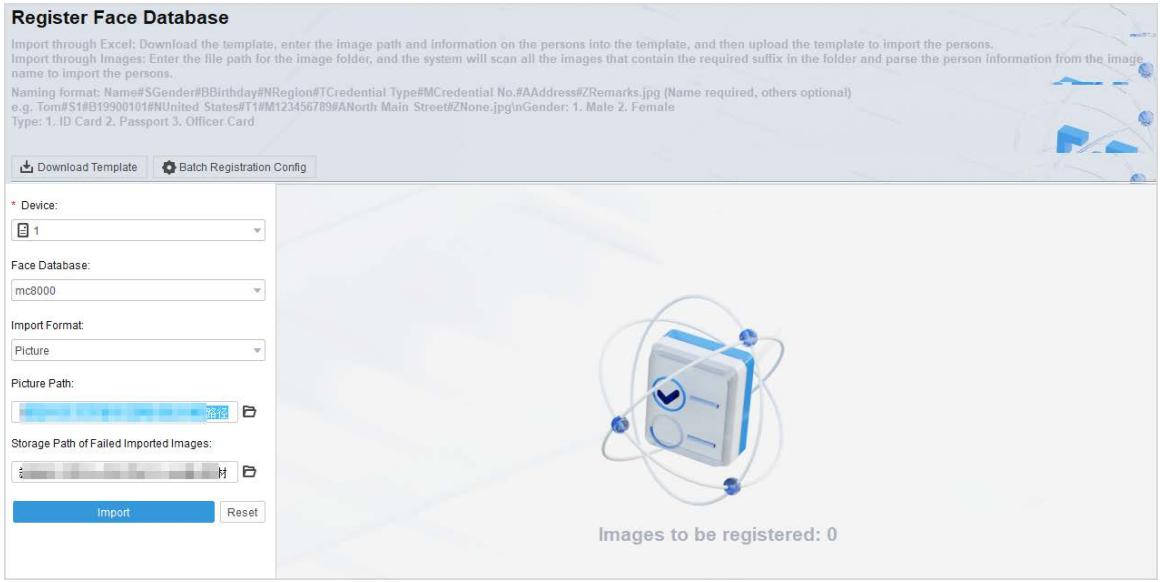
Step 2 Click **Download Template** to fill the template information.

Step 3 Configure **Batch Registration Config**, and then click **OK**.

Step 4 Select devices, face databases, import format, picture path and storage path of failed imported images.

Step 5 Click **Import.**

Figure 3-68 Face library manager



Importing face images to the face library occupies a large amount of memory. When importing more than 300,000 face images at a time, we recommend you do not perform any other operations to avoid an error occurring. If an error occurs, you can restart the client.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**
   Please refer to the following suggestions to set passwords.
   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.
2. **Update Firmware and Client Software in Time**
   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**
   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.
2. **Change Passwords Regularly**
   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
3. **Set and Update Passwords Reset Information Timely**
   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.
4. **Enable Account Lock**
   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.
5. **Change Default HTTP and Other Service Ports**
   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.
6. **Enable HTTPS**
   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.
7. **MAC Address Binding**
   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.
8. **Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**
   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.
   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:
   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.
10. **Audio and Video Encrypted Transmission**
    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.
    Reminder: encrypted transmission will cause some loss in transmission efficiency.
11. **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.
12. **Network Log**
    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.
13. **Construct a Safe Network Environment**
    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:
    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER 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