Intelligent Fusion Server

User Manual

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED “AS IS” AND “WITH ALL FAULTS AND ERRORS”. HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR

PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: ***http://www.recyclethis.info***.

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: ***http://www.recyclethis.info***.

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Preface

Applicable Model

This manual is applicable to Intelligent Fusion Server.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Note	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

Contents

Chapter 1 Introduction

Intelligent fusion server (hereafter referred as the sever), equipped with professional GPU card, integrates deep learning-based algorithms of picture structuration and video structuration. It combines analysis, storage and application as one. By recognizing, analyzing, modelling and comparing pictures of vehicles, the server can perform functions as list alarm, vehicle arming.

1.1 Key Features

- Supports list alarm, stranger alarm, and license plate alarm.
- Settings of alarm popup and sound.
- Establish archives for each personnel.
- Supports management of AI algorithm packages.
- Rapid 1V1 face similarity comparison.
- Display search results in order of similarity from high to low.
- Supports to view the usage of device resource.
- User permission management of admin, operator and consumer.
- NTP time synchronization and manual time synchronization.
- Supports software updating.

1.2 PC Requirements

You can get access to the server with web browser.
The requirements for your PC are shown as below.

- Operating system: Microsoft Windows 7, Microsoft Windows 10.
- CPU: Intel Pentium IV 3.0 GHz or more advanced version.
- Memory: 1G or larger.
- Resolution: 1024 × 768 or higher.
- Web browser: Internet Explorer 8 to 11.

Chapter 2 Configuration Wizard

2.1 Login

You can get access to the server by web browser.

Note

You shall acknowledge that the use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, please strengthen your own protection. If the product does not work properly, please contact with your dealer or the nearest service center.

Steps

1. Open web browser, enter the IP address of the server and then press **Enter**.

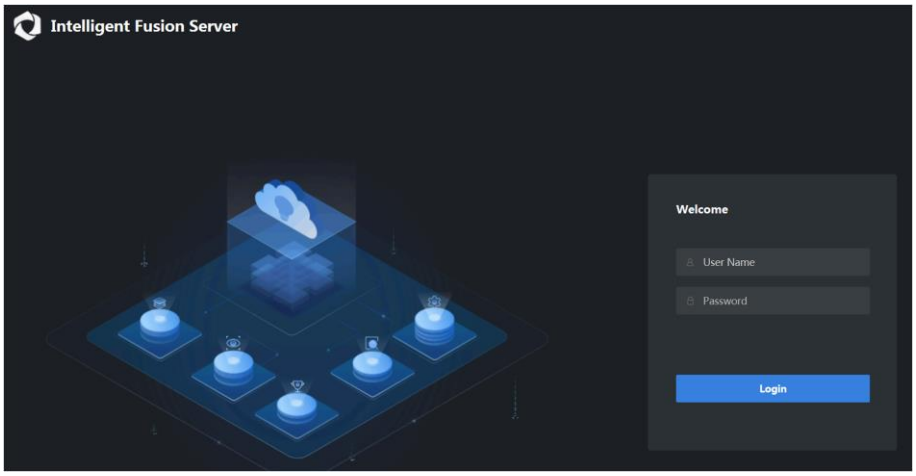

Figure 2-1 Login Interface

2. Enter **User Name** (admin) and **Password**(set for activation).
3. Click **Login**.

Note

- If the server is inaccessible, go to **Internet Options** → **Advancement**, check **Enable TLS1.1** and **Enable TLS1.2**.
- The specific interface varies from product to product.

2.2 Create Cluster

Note

The nodes that create micro video cloud cluster should be the same with that of creating analysis cluster. Otherwise, exception may occur.

2.2.1 Add Node

Before You Start

The node is online and on the same subnet with the server.

Note

The specific parameter values filled in the relevant interfaces below are for reference only. You need to configure relevant parameter values according to actual needs.

Steps

1. Go to **System Management** → **Cluster Management** → **Node Management**
2. Click **Add**.

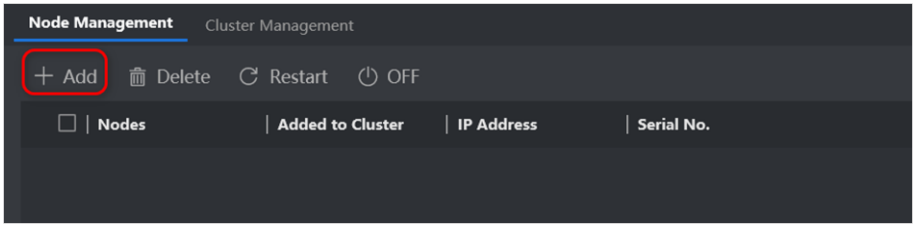

Figure 2-2 Add Notes

3. Enter **Name**, **Nodes IP**, **User Name** and **Password**.
4. Click **OK**.

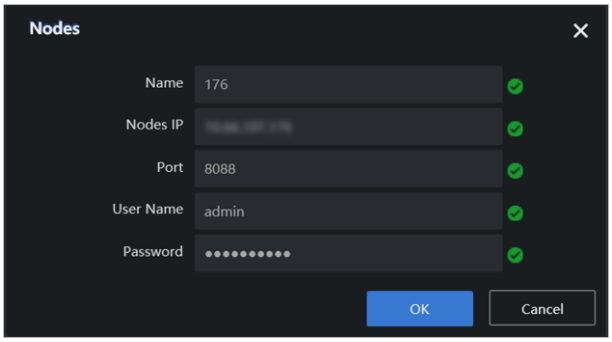

Figure 2-3 Configure Nodes Information

Note

If there are multiple nodes to be added, please follow the steps above to finish.

2.2.2 Create Stand-Alone Cluster

A single node can create a stand-alone cluster. Data can only be analyzed after the cluster is created.

Before You Start

Ensure the node is online.

Steps

1. Go to **System Management** → **Cluster Management**, and click **Create Cluster**.

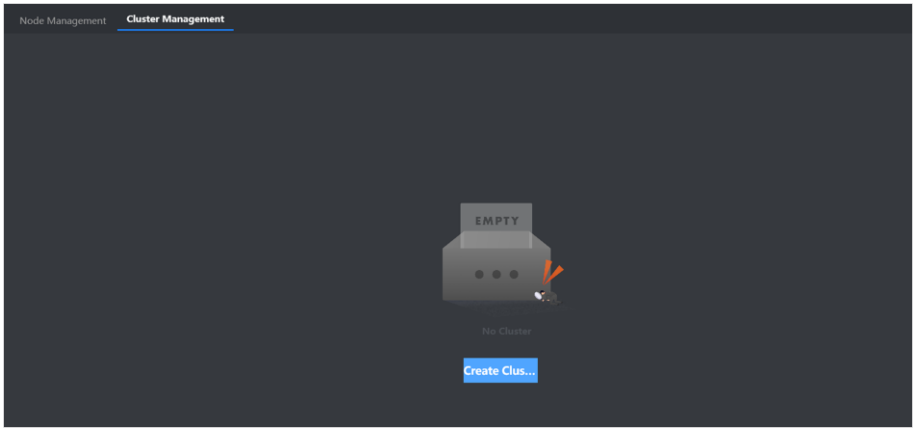

Figure 2-4 Click Create Cluster

2. Select the desired node, and click **Next**.

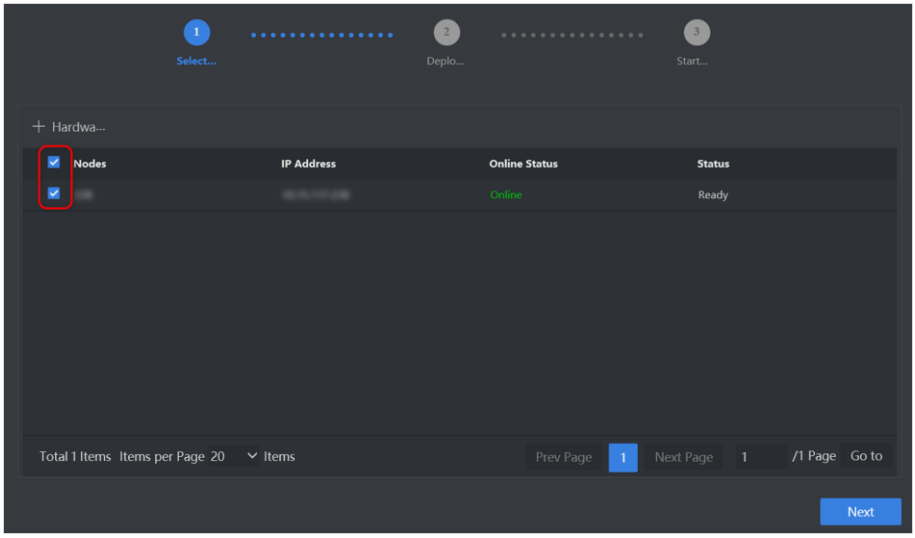

Figure 2-5 Select Node

3. Click **zookeeper**, **kafka**, **MongoDB**, **appServer** respectively, and check the desired nodes.

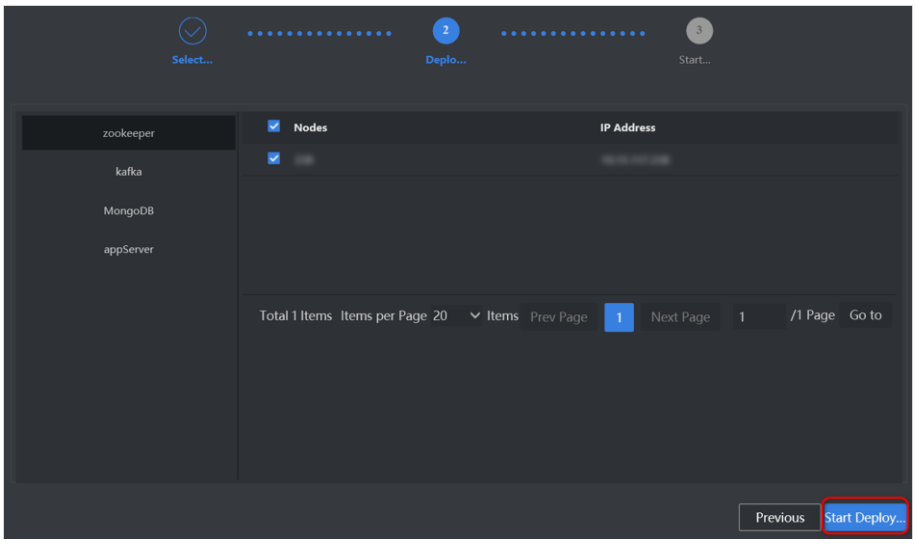

Figure 2-6 Deploying Service

4. Click **Start Deploying**.
5. Click **OFF** after deploying is completed.

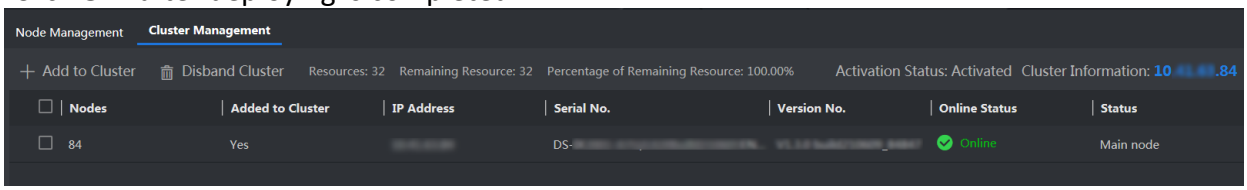

Figure 2-7 Deployed

6. Go to **Resource** → **Algorithm Resource** → **General Algorithm**, click  to allocate resources according to your actual needs.

Face Picture Analysis Path

Intelligent analysis and comparison of faces in pictures.

Face Video Analysis Path

Intelligent analysis and comparison of faces in videos.

Structured Picture Analysis Channel

Intelligent analysis of target (vehicle) attributes in pictures.

Structured Video Analysis Channel

Intelligent analysis of target (vehicle) attributes in videos.

Note

If the value of available resource is zero, the corresponding analysis task cannot be performed.

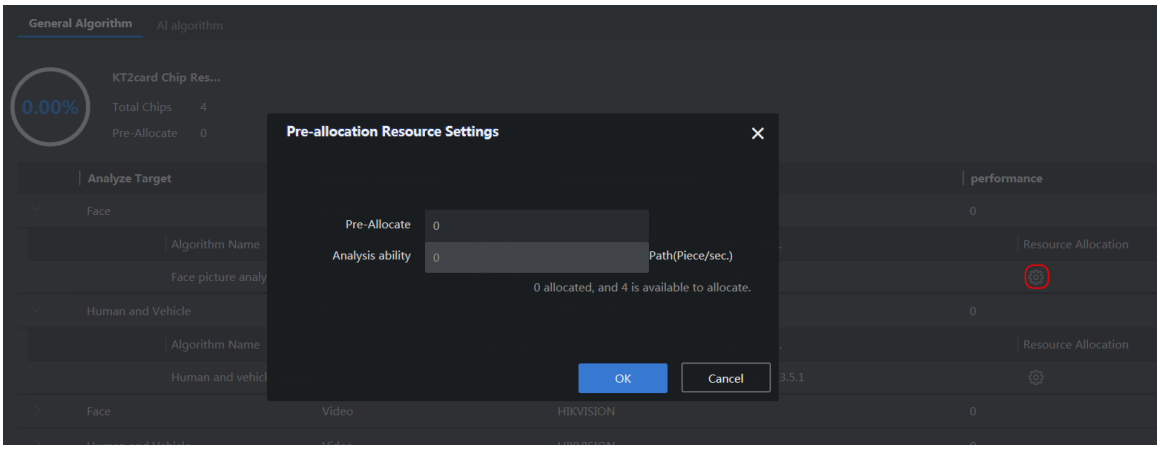

Figure 2-8 Allocate Resource

Note

The interfaces vary according to different types of GPU. If the figure above is different with the actual one, the later prevails.

2.2.3 Create Working and Backup Cluster

Two or more nodes can create a working and backup cluster. Data can only be analyzed after the cluster is created.

Before You Start

- Ensure that at least 2 nodes are added.
- All the nodes should be on the same subnet.
- The master node and backup node must share the same type of GPU.

Steps

1. Go to **System Management** → **Cluster Management**, and click **Create Cluster**.
2. Select the desired nodes, and click **Next**.
3. Click **zookeeper**, **kafka**, **MongoDB**, **appServer** respectively, and check the desired nodes.
4. Click **appServer**, and enter an unused IP address in **Virtual IP**.
5. Click **Start Deploying**.
6. Click **OFF** after deploying is completed.
7. Go to **Resource** → **Algorithm Resource** → **General Algorithm**, click  to allocate resources according to your actual needs.

Face Picture Analysis Path

Intelligent analysis and comparison of faces in pictures.

Face Video Analysis Path

Intelligent analysis and comparison of faces in videos.

Structured Picture Analysis Channel

Intelligent analysis of target (vehicle) attributes in pictures.

Structured Video Analysis Channel

Intelligent analysis of target (vehicle) attributes in videos.

Note

If the value of available resource is zero, the corresponding analysis task cannot be performed.

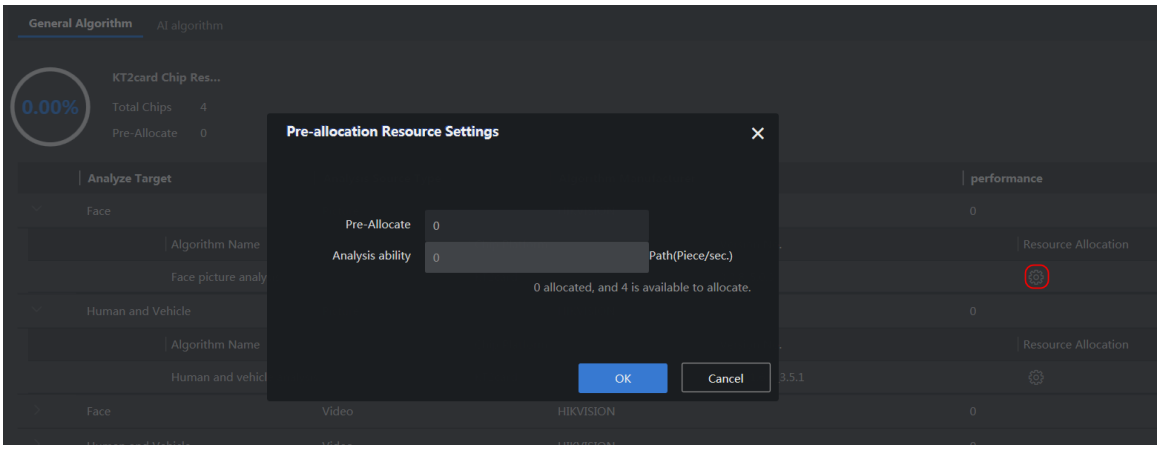

Figure 2-9 Allocate Resource

2.3 Add Face List Library

Add different list libraries, including normal library, blocklist library, and VIP library.

Steps

1. Go to **List Management**, and click **Add**.

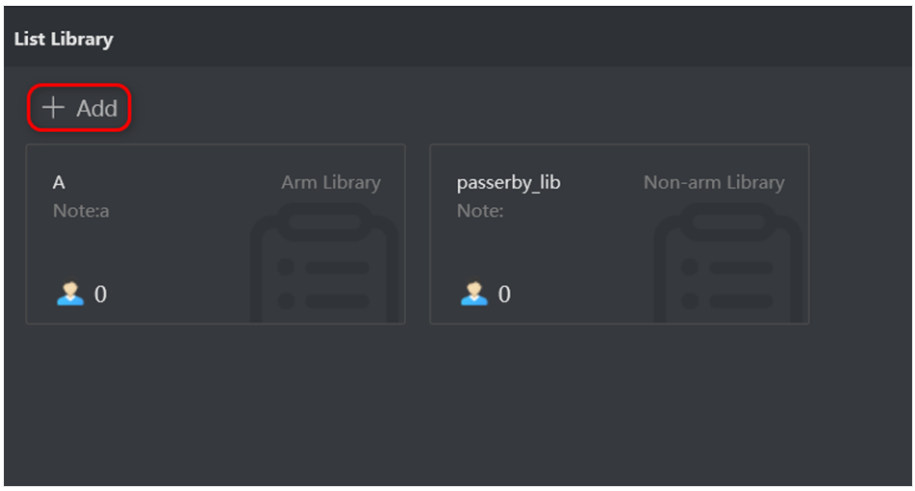

Figure 2-10 List Library Interface

2. Configure relevant parameters according to actual demands.

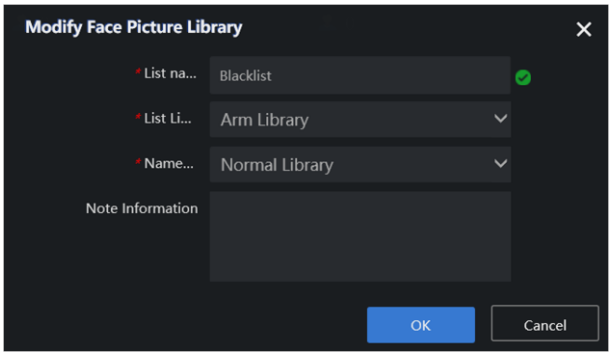

Figure 2-11 Add Face List Library

Note

Only when **List Library Type** is set as **Arm Library** can the alarming and personnel archive function be performed.

3. Click **OK**.
4. Optional: Other operations.
   - Click to modify list library information.
   - Click to delete the list library.

Note

- The passerby library is created by default and cannot be deleted. It is used to add captured stranger face pictures.
- Deleting a list library will delete all relevant personnel information.
- Only when no arming list is added, can the arm library be deleted.

2.4 Add Personnel Information

Before You Start

Ensure a face list library is added.

Steps

1. Click the desired list library to add personnel information.

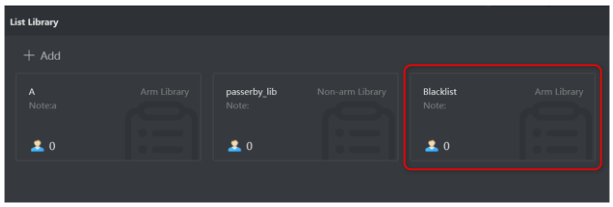

Figure 2-12 Click List Library

2. Click **Add**, enter relevant parameters, and upload face pictures.

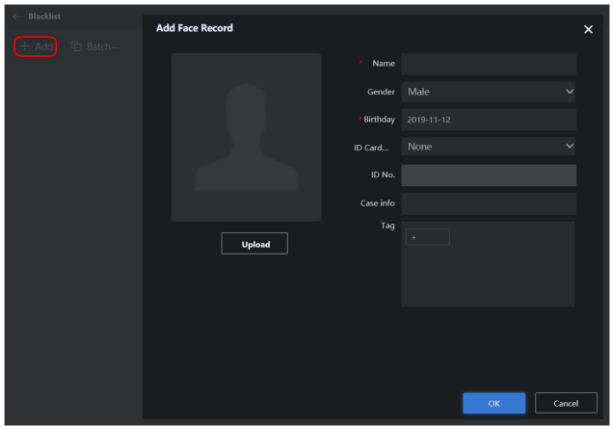

Figure 2-13 Add Personnel Information

Note

- **Name** and **Birthday** are required, enter other contents according to actual demands.
- Face pictures in the format of JPEG, BMP, TIF, PNG, and static GIF are supported.

3. Click **OK**.
4. Move your mouse to the desired item, and click different icons for further operations.
   - Click to edit personnel information.
   - Click to delete personnel information.
   - Click to search personnel information.

2.5 Create Analysis Task

Analysis task includes real-time analysis task and local video record analysis task. Before creating

analysis task, you should add respective resource like camera, video record and etc.

2.5.1 Add Camera

Add the desired camera for arming.

Before You Start

Obtain the IP address, user name and login password of the camera.

Steps

Note

- Add one camera only for each time.
- indicates control center and indicates area. The camera should be added to control center first before added to area. Here we take adding camera to control center "test" as an example.

1. Go to **Resource** → **Camera Management**.
2. Go to **admin** → .

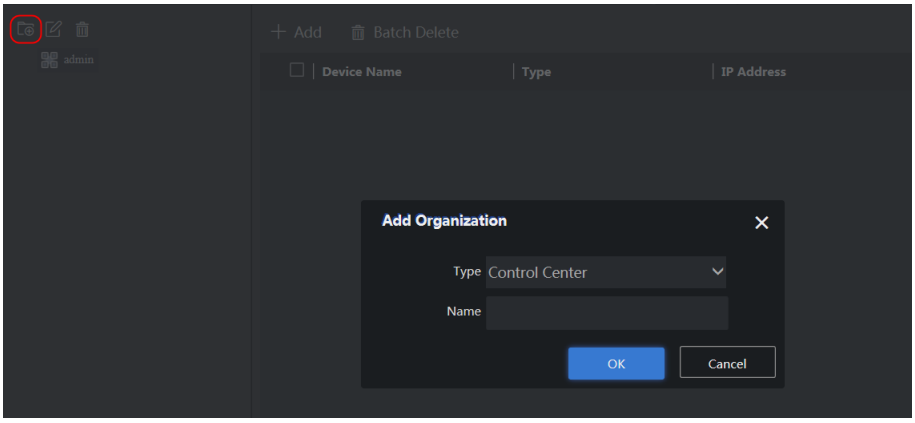

Figure 2-14 Add Control Center

3. Select **Control Center** as **Type** and enter the name of control center.
4. Click **OK**.
5. Click the newly-added control center and enter information in the popup window.

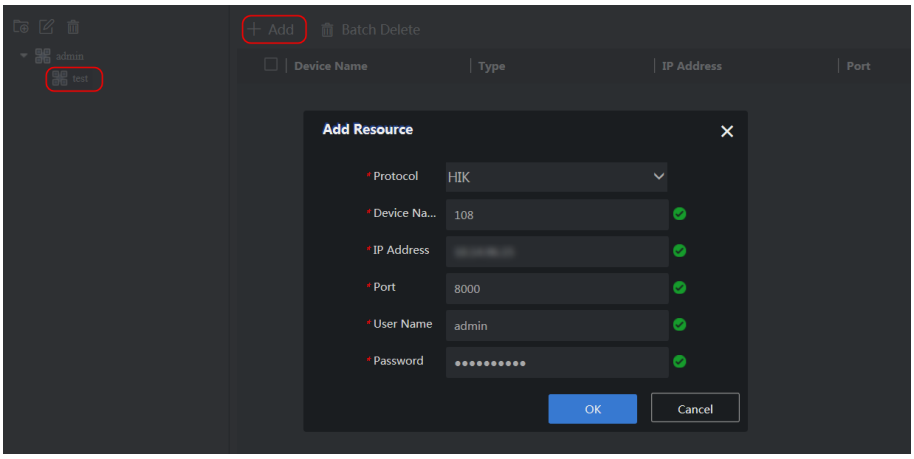

Figure 2-15 Add Camera

6. Click **OK**.
7. Click .
8. Select **Area** as **Type** and enter the name of area.

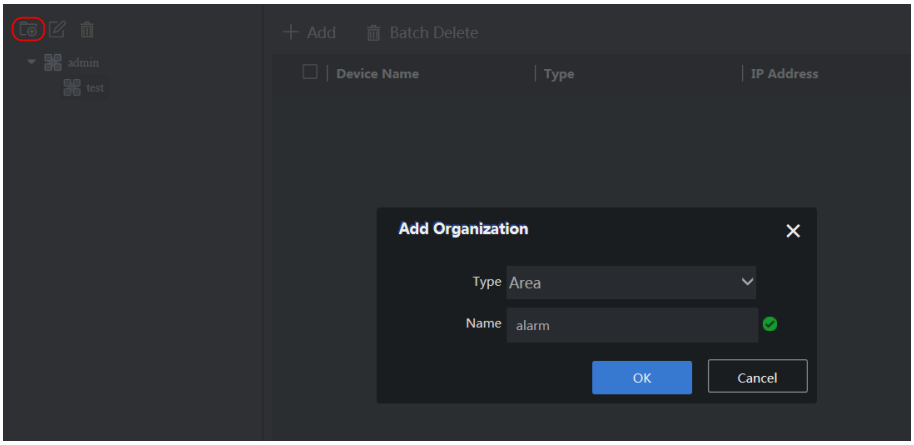

Figure 2-16 Add Area

9. Click **OK**.

Note

The area name supports digits, lower-case letters, upper-case letters, and special characters like "-" and " _". Up to 32 characters are allowed.

10. Click the newly-added area, and then click **Add**.

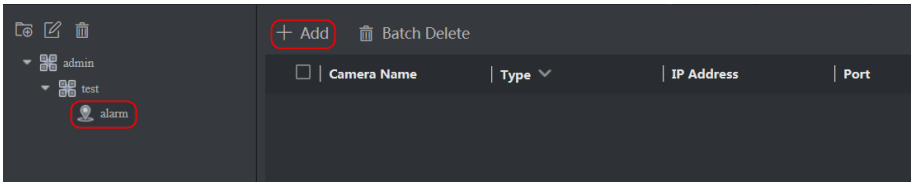

Figure 2-17 Add Camera to Area

Note

The camera can be armed only after it is added to area.

11. Select the desired camera.
12. Click **OK**.

Note

Both control center and area can be added to control center, but only camera can be added to area.

2.5.2 Create Real-time Analysis Task

Real-time analysis task is used to conduct real-time analysis of targets in monitoring scene.

Before You Start

The camera has been added.

Steps

1. Go to **Target Arming** → **Task Management** → **Real-Time Task List**, click **New**.

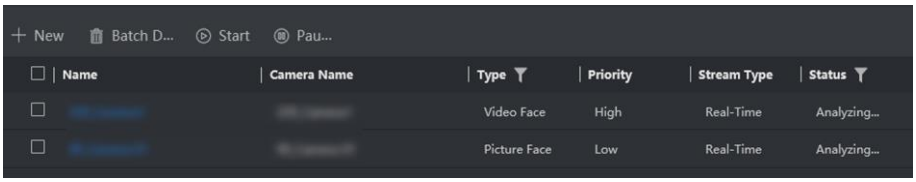

Figure 2-18 Task Management Interface

2. Check a desired camera or multiple cameras, click **Create**.

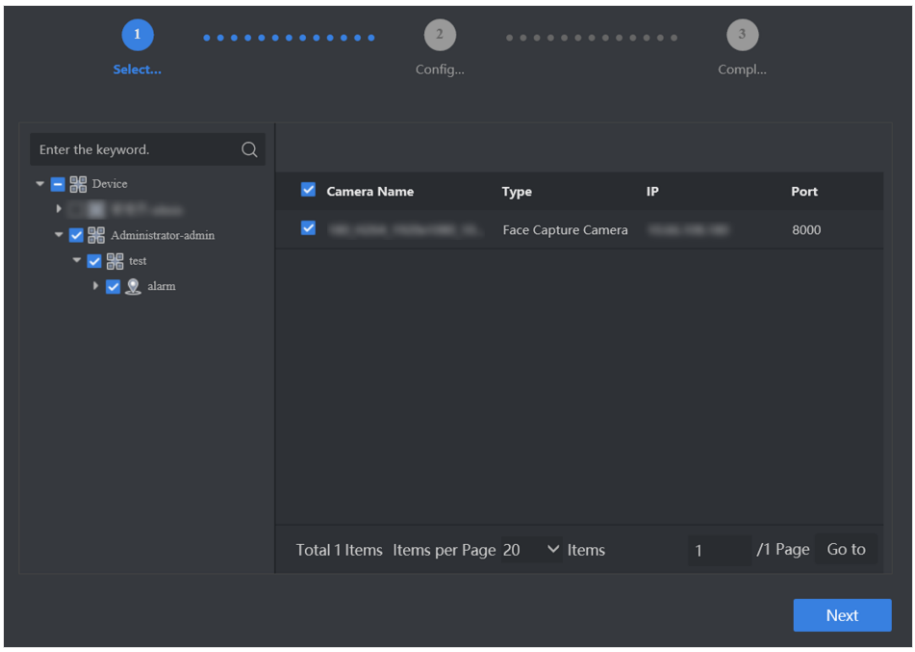

Figure 2-19 Check Cameras

3. Optional: Click in **Rule Settings** list to set detailed rules.
   - Click to draw the detection area. Full screen detection is set by default.
   - Click to draw min. pupil distance, and you can set max. pupil distance as well. After the minimum and maximum value are set, only face whose pupil distance is within the range will be detected.
   - Keep other parameters as default value.

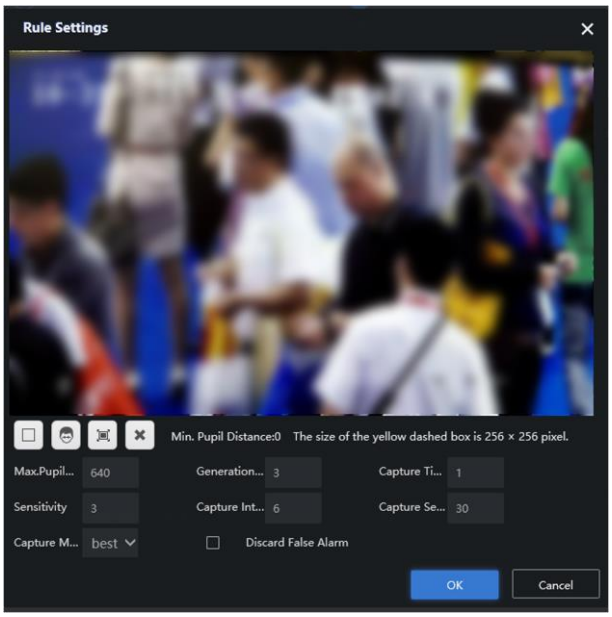

Figure 2-20 Set Rule

Caution

This step is only applicable for face capture of video streams from normal network cameras.

4. Click **OK**.
5. Click to set detailed schedule. The server performs all-hours analysis by default.
6. Click **Create**.

Video Structure

Analysis of target attributes in videos. This type of analysis task should be created before you set license plate arming.

Video Face

Analysis and comparison of faces in videos.

Picture Structure

Analysis of target attributes in pictures. This type of analysis task should be created before you set license plate arming.

Picture Face

Analysis and comparison of faces in pictures.

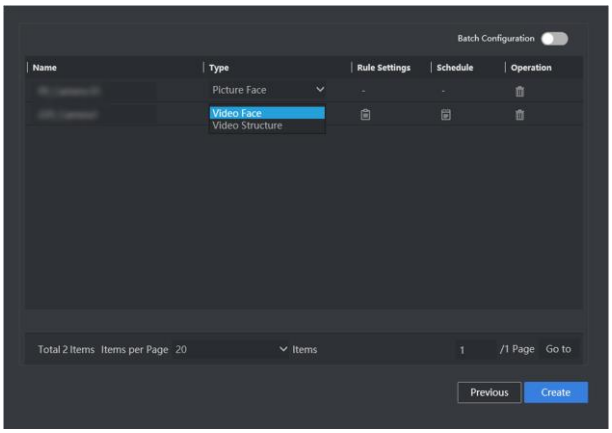

Figure 2-21 Create Real-time Analysis Task

Note

By clicking **Configure** on the upper-right corner, you can configure the task application intervals.

2.5.3 Create Video Record Analysis Task

Video record analysis task is used to analyze targets in video files.

Before You Start

- Import video record files.
- Allocate resources.

Steps

1. Go to **Resource** → **Video Management**.
2. Click **Default List**, and then click **Import**.

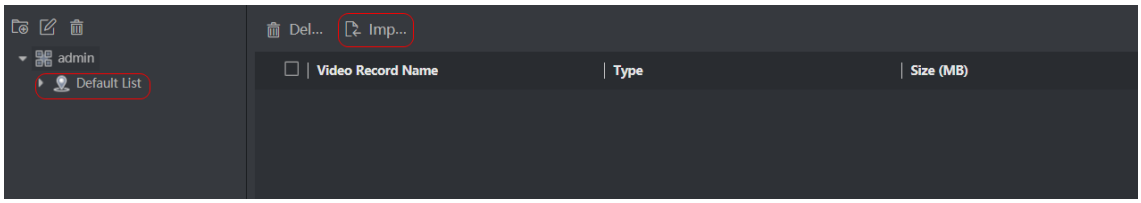

Figure 2-22 Import Video

3. Click **Browse** to select desired video recording files.
4. Set the actual time of recording as video starting time.

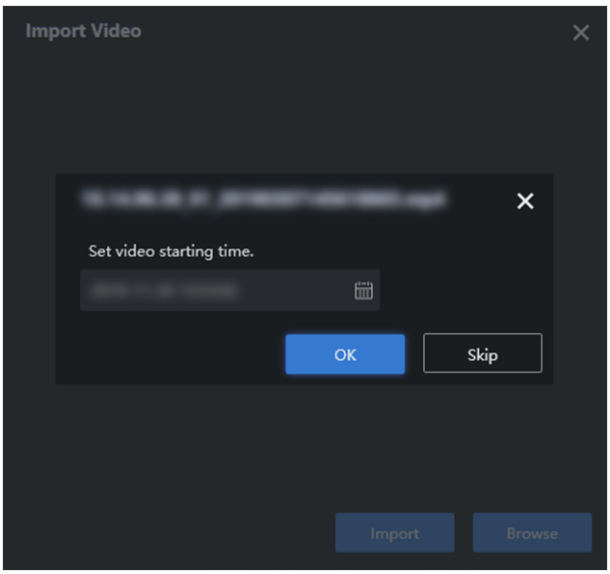

Figure 2-23 Set Video Starting Time

Note

If the video starting time is not set, the time of analysis results will be inconsistent with that of actual recording.

5. Click **OK**.
6. Click **Import**, and select the desired videos in the list.
7. Click **Next**.

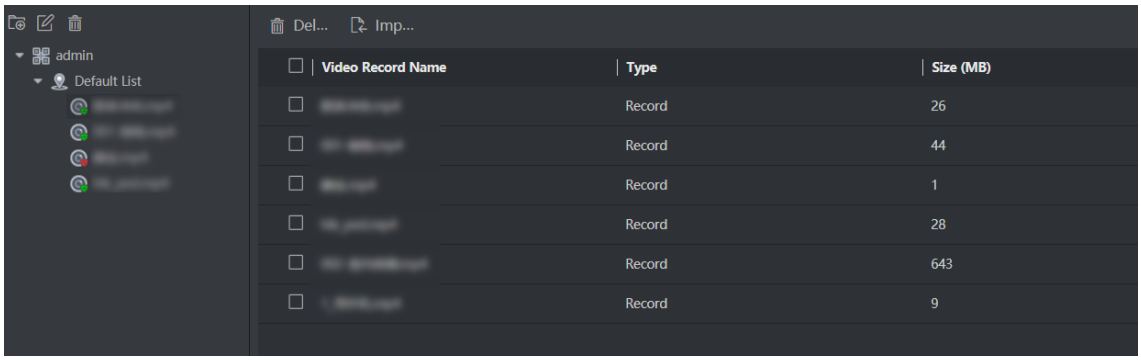

Figure 2-24 Select Recordings

Note

If the live view function is disabled, you may have to install a plug-in in accordance with the prompt. Close web browser before installing the plug-in.

8. Click in **Rule Settings** list to set detailed rules in the popup interface.
   - Click to draw the detection area. Full screen detection is set by default.
   - Click to draw min. pupil distance, and you can set max. pupil distance as well. After pupil distance is set, only faces whose pupil distance is between min. and max. pupil distance value will be detected.
   - Keep other parameters as default value.

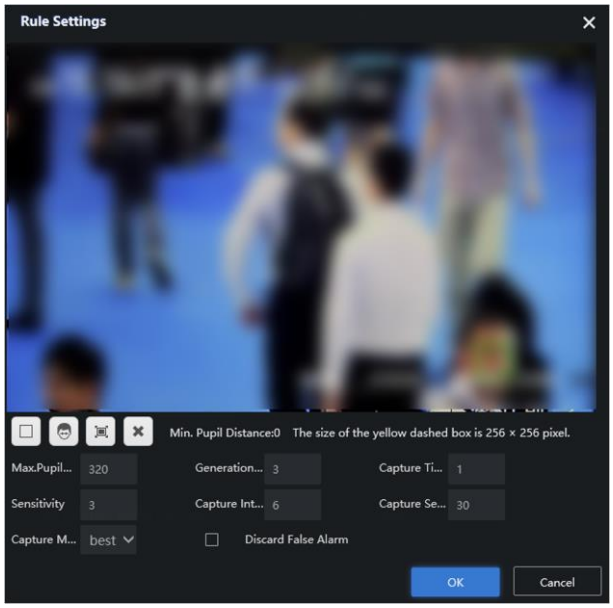

Figure 2-25 Set Rule

9. Click **Create**.

Video Structure

Analysis of target attributes in videos. This type of analysis task should be created before you set license plate arming.

Arming Analysis

If enabled, arming analysis will be performed.

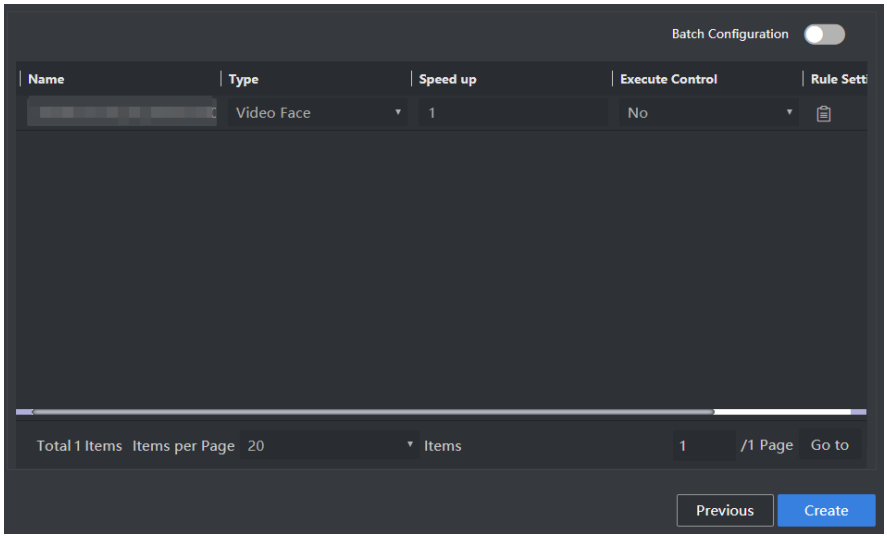

Figure 2-26 Create Video Record Analysis Task

2.6 Create AI Algorithm Task

Creating AI algorithm task is only available when there is one or more T4 device in the cluster.

2.6.1 Import AI Algorithm Package

Importing AI algorithm package(s) is required for creating analysis task(s).

Before You Start

Get an AI algorithm package.

Steps

1. Go to **System Management** → **System Config** → **Algorithm Library**, and click **Add**.

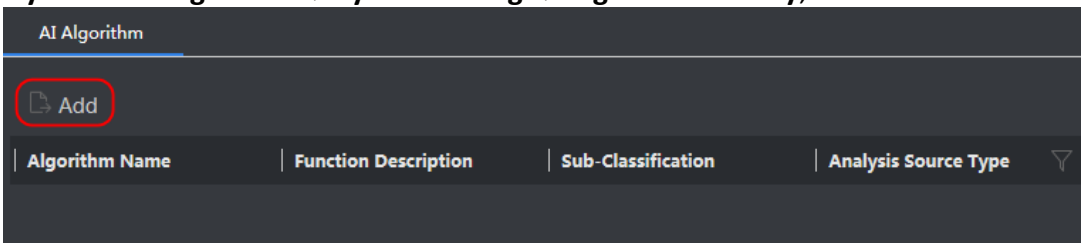

Figure 2-27 Add AI Algorithm Package

2. Click **Browse**, and select the desired algorithm package and description file (.json file).

Note

AI algorithm packages include encrypted algorithm packages and non-encrypted packages, and the former is only applicable to the device it is imported to.

3. Configure the parameters.

Algorithm Name

Enter a name as desired.

Sub-Classification

Enter the sub-classification of analysis type. Click **Edit** → **Add** to add sub-classification as desired.

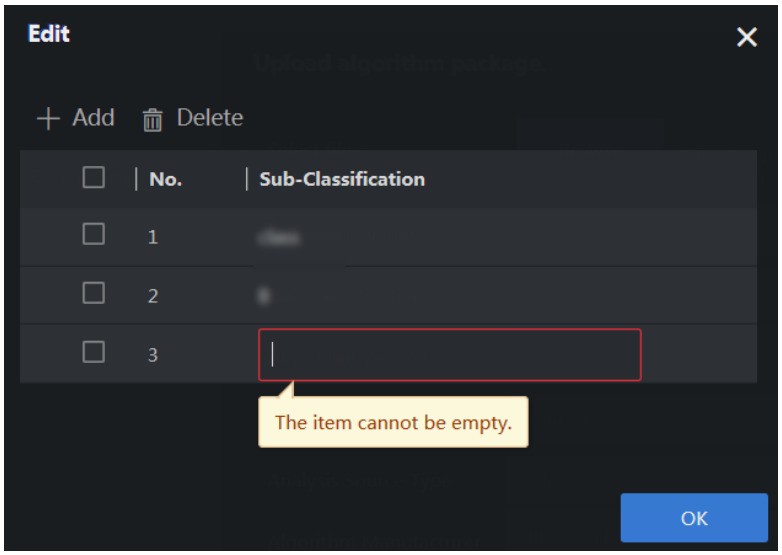

Figure 2-28 Add Sub-Classification

Algorithm Version

Keep the version as default value.

Analysis Source Type

Video: Analyze the recordings or videos of cameras.
Picture: Analyze the pictures submitted by the client. Captured pictures cannot be analyzed directly.

Note

Select **Analysis Source Type** as **Video** for video analysis task, and **Picture** for picture analysis task.

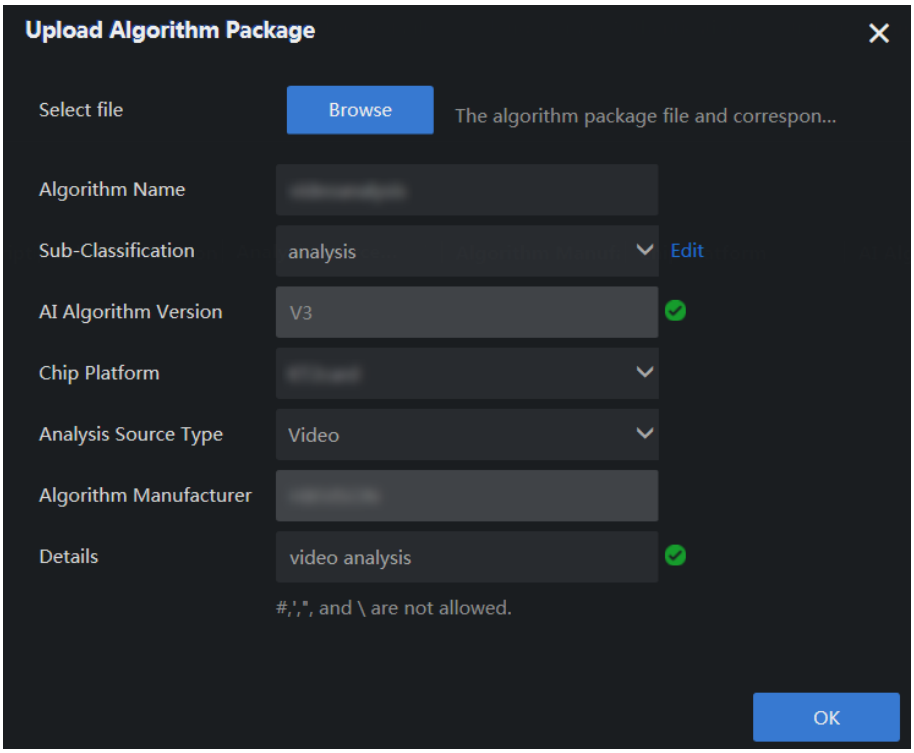

Figure 2-29 Algorithm Package Parameter

4. Click **OK**.
5. Optional: Click or to check details or delete the corresponding algorithm.

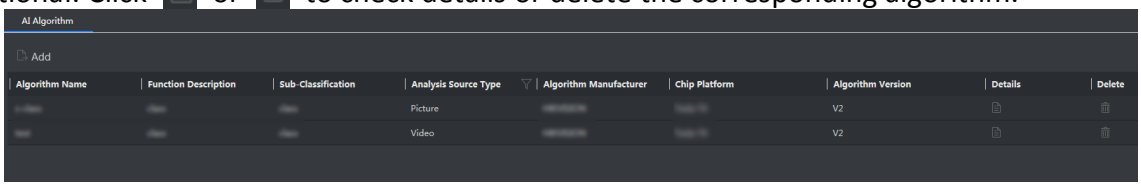

Figure 2-30 Algorithm List

2.6.2 Allocate Analysis Resource

Before You Start

Import AI algorithm package(s).

Steps

1. Go to **Resource** → **Algorithm Resource** → **AI Algorithm**, and click to allocate resources for AI algorithm package.

Note

Allocate resource of **Video Analysis Channel(s)** for video analysis task, and **Picture Analysis Channel(s)** for picture analysis task.

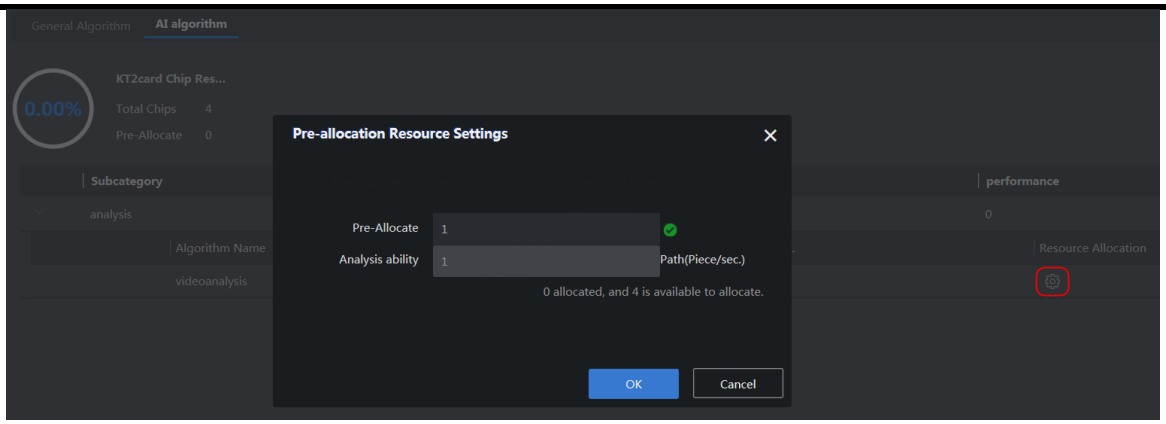

Figure 2-31 Allocate Resource for AI Algorithm Package

Note

If the value of available resource is zero, the corresponding analysis task cannot be performed.

2.6.3 Create Video Analysis Task

You can create video analysis task(s) of AI algorithms, and arm cameras (except capture cameras) through the web interface. Detection, classification, behavior, OCR model, and mixed analysis tasks are allowed to be created.

Before You Start

- Import video analysis algorithm(s).
- Allocate video analysis resource.

Steps

1. Go to **Target Arming** → **AI Task Management**, and click **New**.
2. Configure related parameters.

   Name

   Enter a name as desired.

   Camera Name

   Select the desired camera(s) for arming. Creating video analysis task(s) of AI algorithms and arming cameras except capture cameras are allowed.

   Sub-Classification/Version No.

   Select a value as desired.
3. Click **Add Rule**, and configure related parameters as needed.

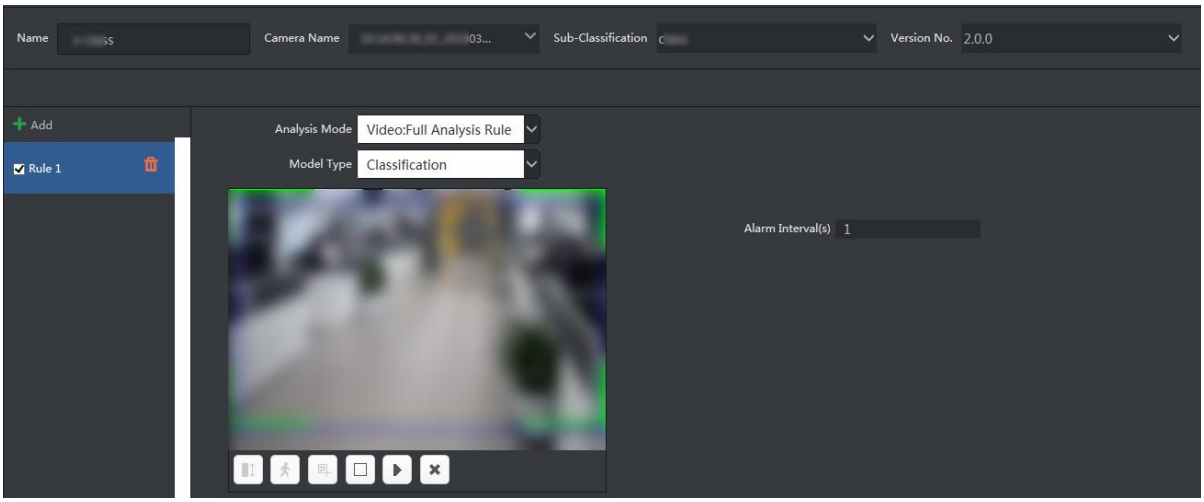

Figure 2-32 Create Task

Note

The parameters to be configured vary from different rules. The figure above is for illustration purpose only.

4. Click **Save**.
5. Optional: Check the results through the client.

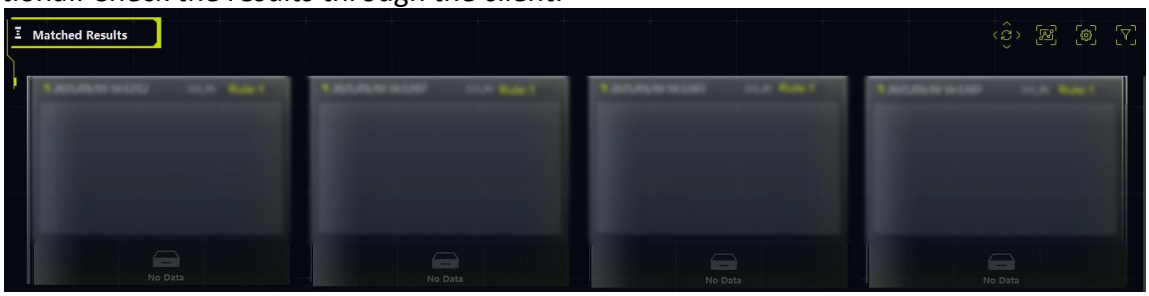

Figure 2-33 Check Analysis Result

2.6.4 Create Picture Analysis Task

Picture analysis task(s) should be created through the client. Detection, classification, OCR model, and mixed analysis tasks are allowed to be created.

Before You Start

- Allocate video analysis resource.
- Install the corresponding client and check AI dashboard.

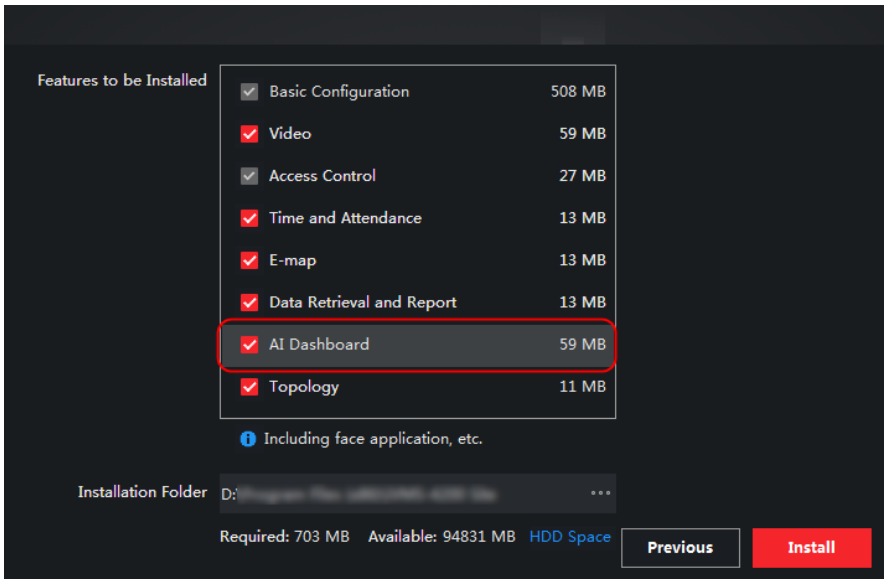

Figure 2-34 Check AI Dashboard

Steps

1. Log in to the client, and go to **Device Management** → **Add** to add the server.
2. Configure related parameters.

Name

Enter a name as desired.

Address

Enter the IP address of the server. For stand-alone cluster, enter the actual IP address of cluster. For working and backup cluster, enter the virtual IP address.

Port

Keep it as the default value.

User Name/Password

Enter the user name and password for login.

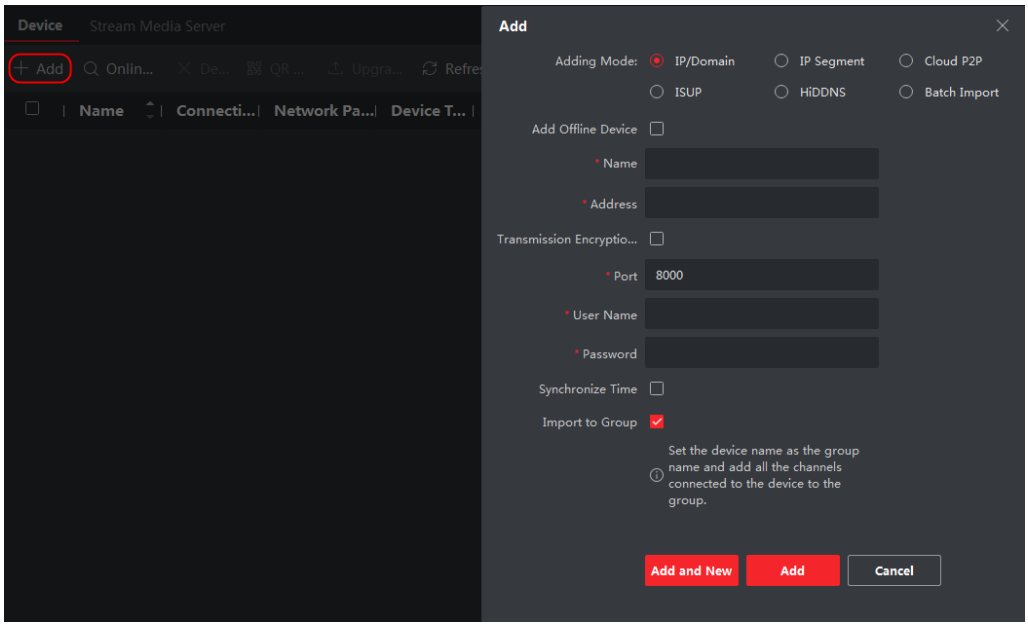

Figure 2-35 Add Server

2. Go back to the homepage, and click **AI Dashboard**.

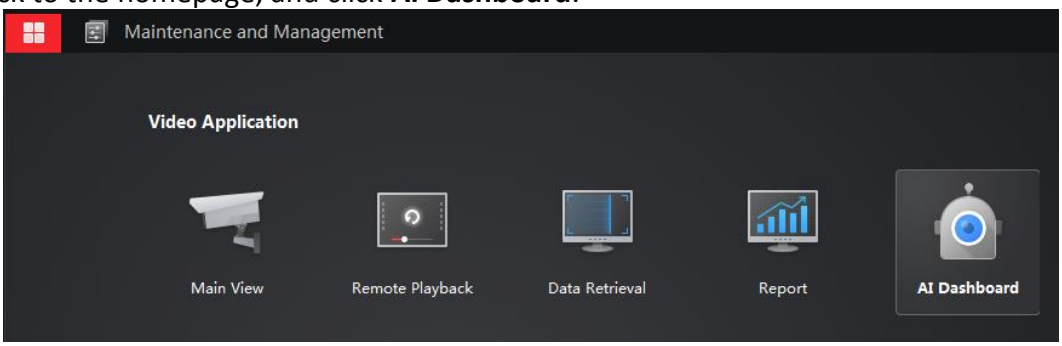

Figure 2-36 AI Dashboard

3. Go to **AI Open Platform** →  .
4. Check the desired devices, and click **OK** to get imported AI algorithm package.

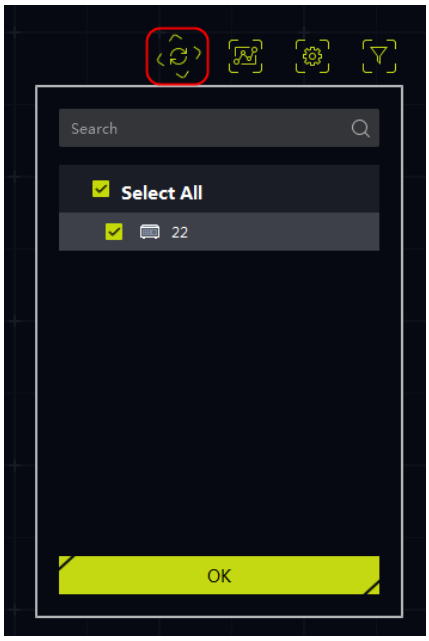

Figure 2-37 Model Package

5. Click **Picture Importing & Analysis**, and select a folder path.
6. Configure other parameters as required.

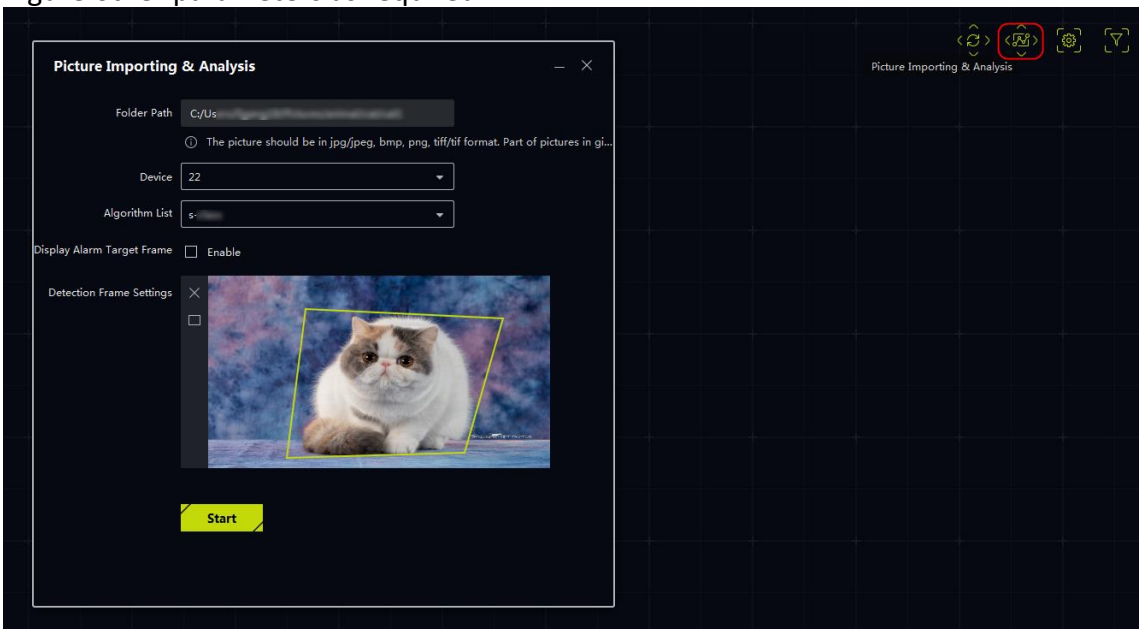

Figure 2-38 Import Picture

7. Click **Start**, and check analysis results after finished.

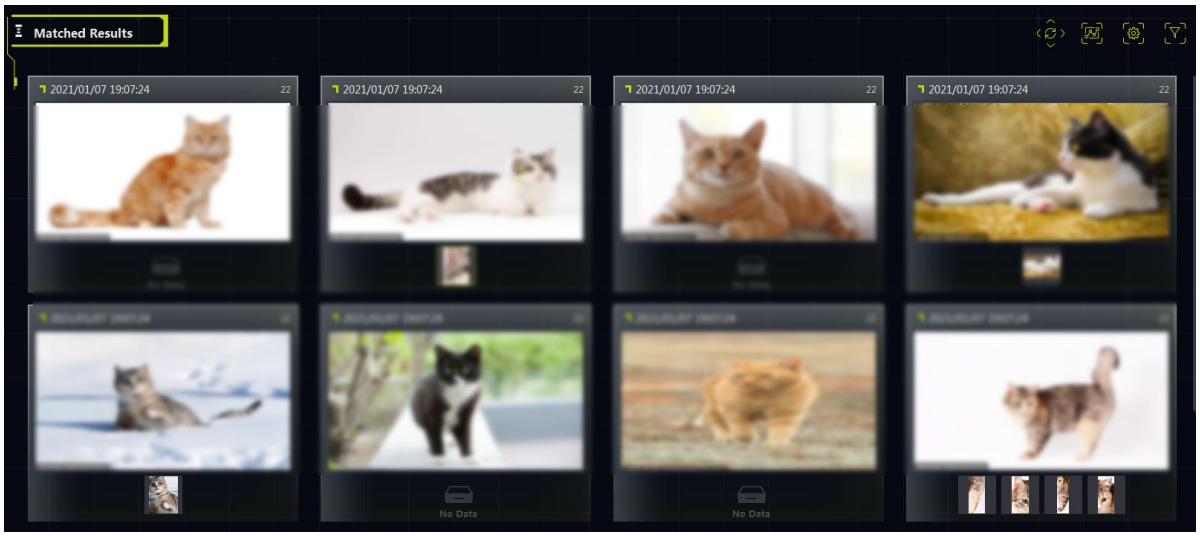

Figure 2-39 Check Analysis Result

2.6.5 AI Alarm Search

The AI alarm events can be searched through the client.

Before You Start

Install the client.

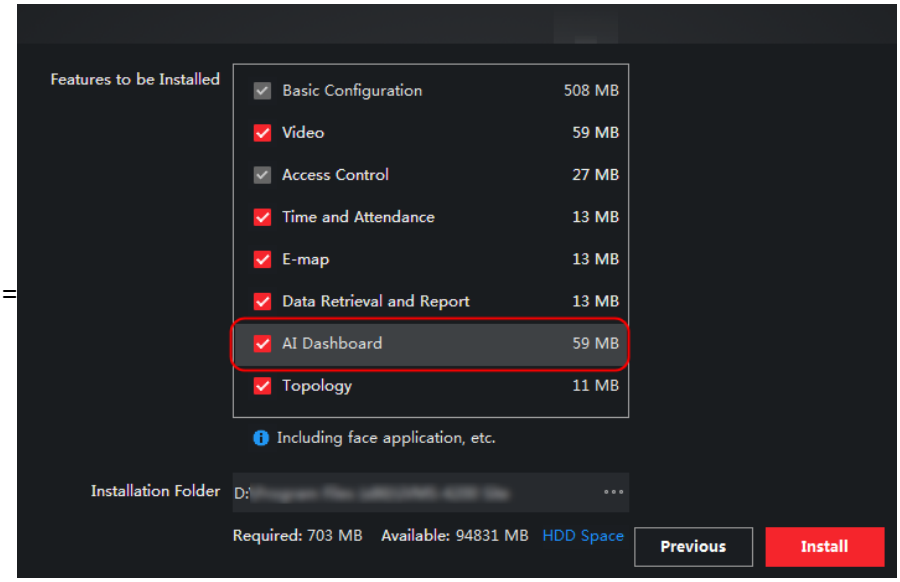

Figure 2-40 Check AI Dashboard

Steps

1. Log in to the client, and go to **Device Management** → **Add** to add the server.
2. Configure related parameters.

Name

Enter a name as desired.

Address

Enter the IP address of the server. For stand-alone cluster, enter the actual IP address of cluster. For working and backup cluster, enter the virtual IP address.

Port

Keep it as the default value.

User Name/Password

Enter the user name and password for login.

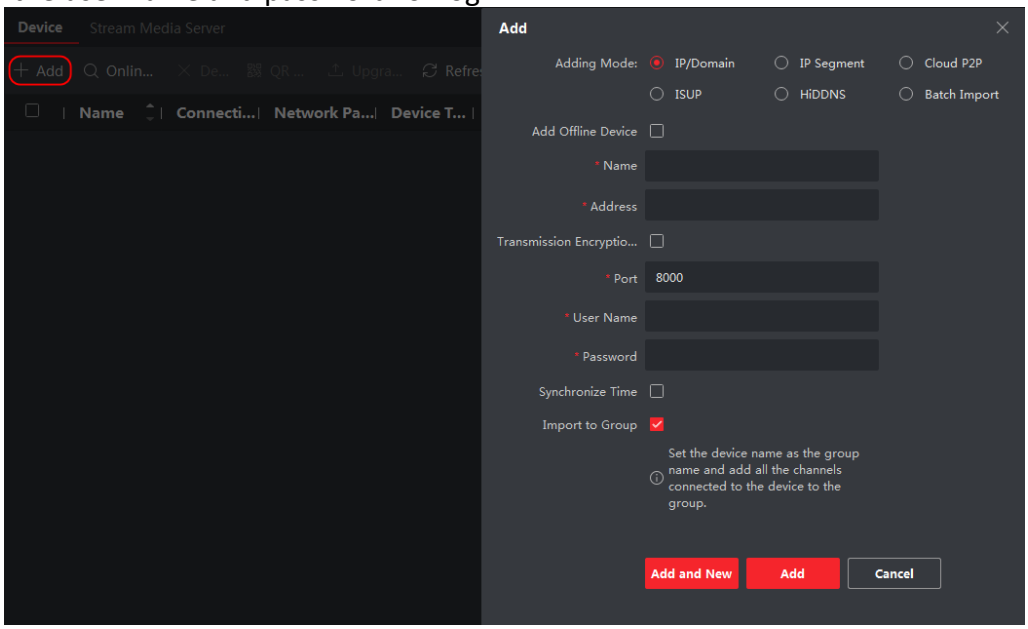

Figure 2-41 Add Server

3. Go back to the homepage, and click **Data Retrieval**.

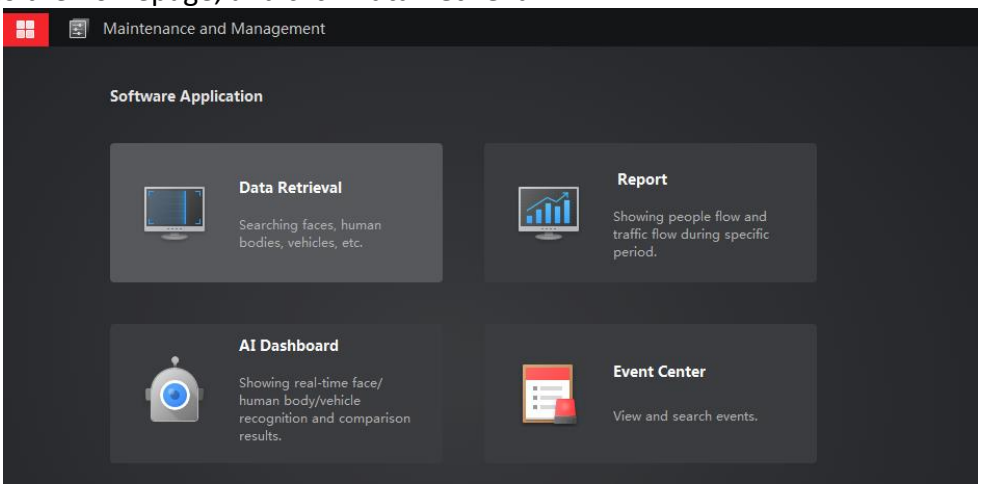

Figure 2-42 Data Retrieval

4. Click **AI Dashboard Retrieval** and set search conditions, then click **Search**.

Video & Capture Analysis Task

Alarm events triggered by video analysis tasks.

Picture Importing & Analysis Task

Alarm events triggered by picture analysis tasks.

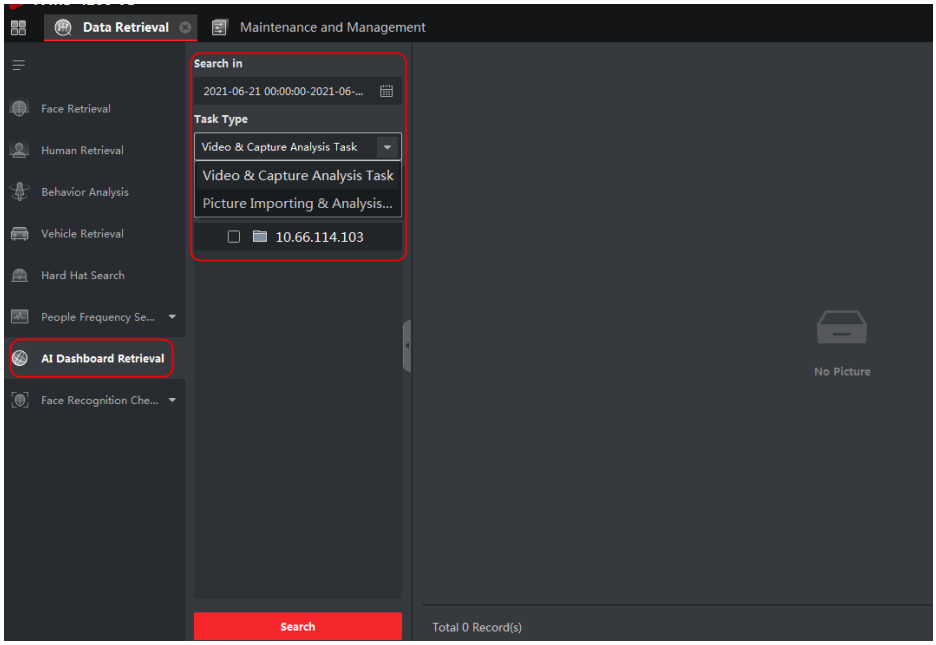

Figure 2-43 Search AI Alarm Event

2.7 Add Arming

2.7.1 Add List Arming

Listing arming is used to compare the target captured by cameras with that of list library. If the similarity between this two pictures reaches the configured threshold value, a list alarm will be triggered.

Before You Start

- Cameras have been added and armed.
- A face list library has been created and personnel information added.
- Select **Arm Library** as **List Library Type** for the desired list library.

Steps

1. Go to **Target Arming** → **List Arming**, and click **New**.
2. Configure the parameters as below.

Table 2-1 Parameter Setting

Parameter Name	Description
Name/Note	Enter relevant information according to actual condition.

Parameter Name	Description
Arming Type	Select **List Arm**.
Arming Object	Select the desired list library.
Arming Camera	Select the desired camera.
Arming Time	Set arming time. You can click  to customize arming period.
Threshold	A high threshold value requires a high similarity.

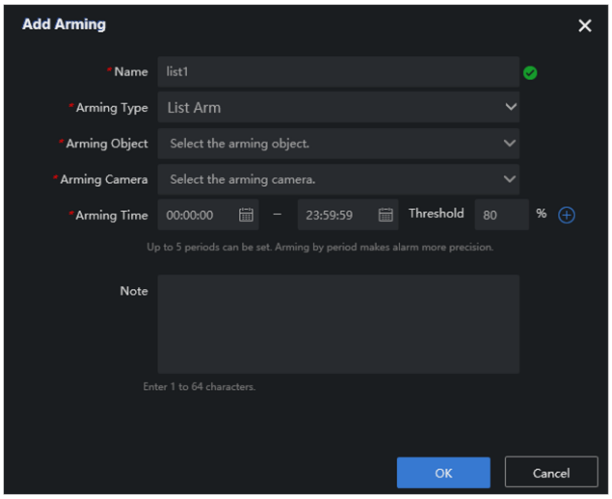

Figure 2-44 Set List Arming Parameters

3. Click **OK**.

Table 2-2 Parameter Setting

Operation	Description
Modify Arming Parameters	Click  to modify the arming parameters.
Delete Arming	Select the desired arming, and click  .

2.7.2 Add Stranger Arming

Stranger arming is used to compare the target captured by cameras with that of list library. If the similarity between this two pictures does not reach the configured threshold value, a stranger alarm will be triggered.

Before You Start

- Cameras have been added and armed.
- A face list library has been created and personnel information added.
- Select **Arm Library** as **List Library Type** for the desired list library.

Steps

1. Go to **Target Arming** → **List Arming**, and click **New**.
2. Configure the parameters as below.

Table 2-3 Parameter Setting

Parameter Name	Description
Name and Note	Enter relevant information according to actual condition.
Arming Type	Select **Stranger Arm**.
Arming Object	Select the desired list library.
Arming Camera	Select the desired camera.
Arming Time	Set arming time. You can click  to customize arming period.
Threshold	A high threshold value requires a high similarity.

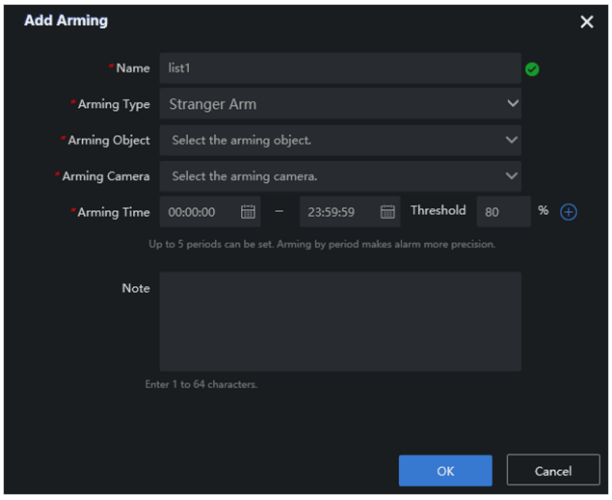

Figure 2-45 Set Stranger Arming Parameters

3. Click **OK**.

Table 2-4 Parameter Setting

Operation	Description
Modify Arming Parameters	Click  to modify the arming parameters.
Delete Arming	Select the desired arming, and click  .

2.7.3 Add License Plate Arming

License plate arming is used to compare the license plates recognized by cameras with those armed license plates. If this two plates match with each other, a license plate alarm will be triggered.

Before You Start

A real-time or video record analysis task has been created, and its type is set as **Video Structure** or **Picture Structure**.

Steps

1. Go to **Target Arming** → **License Plate Arming**, and check **Enable**.

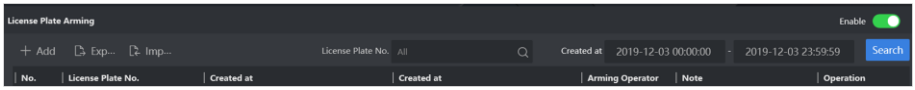

Figure 2-46 License Plate Arming Interface

Note

Import the template of license plate arming information to enable batch license plate arming. Go to **Export Arming List** → **Export Template** to get templates.

2. Click **Add**, and enter **License Plate No.**, **Start Time**, **End Time** and **Note**.

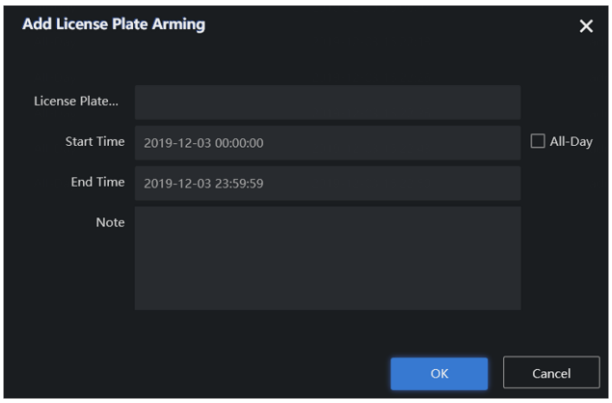

Figure 2-47 Add License Plate Arming

3. Click **OK**.

2.8 Reset Standard

Generally, the data of arming library will be synchronized to the server automatically. If any exception occurs during the process of data synchronization, you can reset standard to manually synchronize the data of arming library and server.

Before You Start

Full text retrieval has been set.

Steps

1. Go to **System Management** → **System Config** → **System Maintenance**.

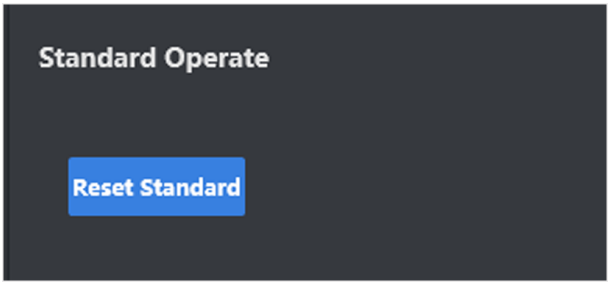

Figure 2-48 Reset Standard

2. Click **Reset Standard**.

2.9 Enable Personnel Archive

Personnel archive is used to compare the similarity between face pictures captured by camera and that of face list libraries(except the passerby library). If the similarity value is greater than or equal to threshold value, the captured picture will be classified and saved into the real name archive. Otherwise, it will be saved into the passerby archive. The archive records the appearance duration and captured pictures. Every personnel will be recorded with a separated archive.

Before You Start

- At least one camera has been added and armed.
- Select **Arm Library** as **List Library Type** for the desired passerby library.

Steps

1. Go to **System Management** → **System Config** → **Personnel Archive**.
2. Configure the parameters as below.

Table 2-7 Parameter Setting

Parameter Name	Description
Enable	Check **Enable**.
Arming Object	Select **Passerby Library** and other desired lists.
Arming Camera	Select desired cameras.

Parameter Name	Description
Threshold	Compare the similarity between face pictures captured by camera and that of face list library (except passerby library). If the similarity value is greater than or equal to the threshold value, the captured picture will be classified and saved into the real name archive. Otherwise, it will be saved into the passerby archive.

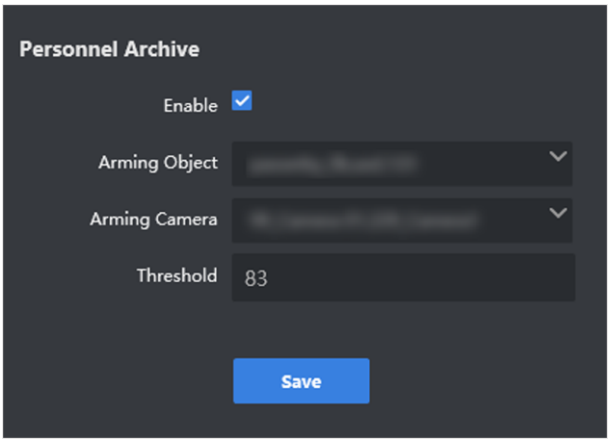

Figure 2-49 Enable Personnel Archive

3. Click **Save**.

Chapter 3 Smart Application

The smart application includes live view, alarm search, personnel archive and 1 V 1 comparison.

3.1 Live View

View captured face pictures, list alarm information, stranger alarm information.

Before You Start

Add list arming.

Steps

1. Click **Live View**.

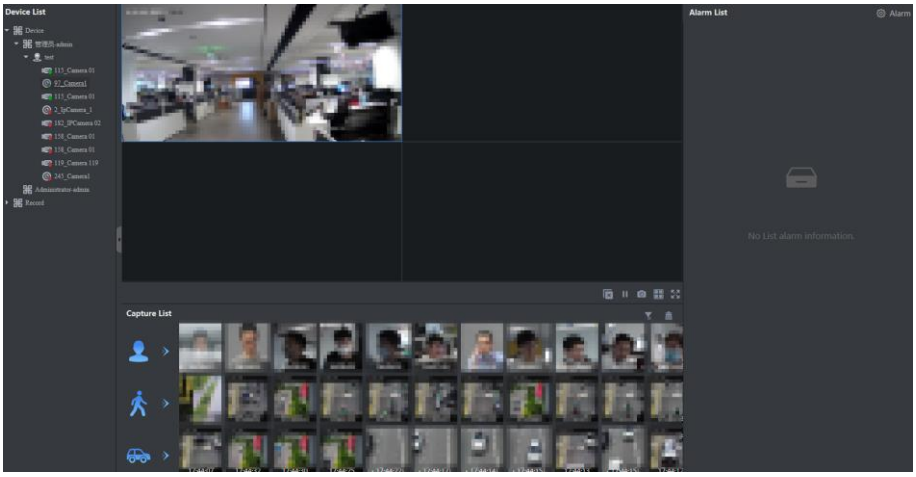

Figure 3-1 Live View

Note

In the live view interface, the bottom area displays real-time captured vehicle pictures, and the right area displays real-time list alarm information.

Table 3-1 Live View Interface Introduction

Interface Area	Description
Live View Interface	Live view with multi-channels is supported. ● Click to stop live view of current channel. ● Click to stop live view for all channels. ● Click to capture pictures manually. The captured picture will be saved automatically. Go to ***Configuration Live View*** to configure the saving path.

Interface Area	Description
	● Click to view in split window ● Click to view in full screen.
Capture List	Display the real-time captured vehicle pictures. ● Click to filter cameras or videos, only face pictures from selected cameras or videos will be displayed. ● Click to delete current displayed face pictures. ● Click to add the selected picture to list library. ● Click to take the selected picture as a target to search picture by picture. ● Click to take the selected picture as a target to confirm identification.

2. Optional: Click **Alarm** in the upper right corner of the interface to configure parameters according to actual needs.

Table 3-2 Parameter Setting

Parameter Name	Description
Real-time Alarm Display	Check the desired alarm types to display corresponding alarm information.
Type of Alarm Popups	Enable alarm pop-up window and check the desired alarm types.
Customized Alarm Sound	Enable alarm sound to broadcast alarm information through specific sound. Alarm sound is customizable by uploading MP3 files.
Alarm Prompt	Enable alarm prompt to broadcast alarm information through message.

3.2 Alarm Search

Search detailed information of list alarm, stranger alarm, and license plate alarm.

3.2.1 List Alarm

Compare the similarity between captured face pictures and those in list library like blocklist library. A list alarm will be triggered if the similarity reaches the configured value.

Before You Start

Add list arming.

Steps

1. Go to **Alarm Search** → **List Alarm**. By default, the server displays all current alarm information.

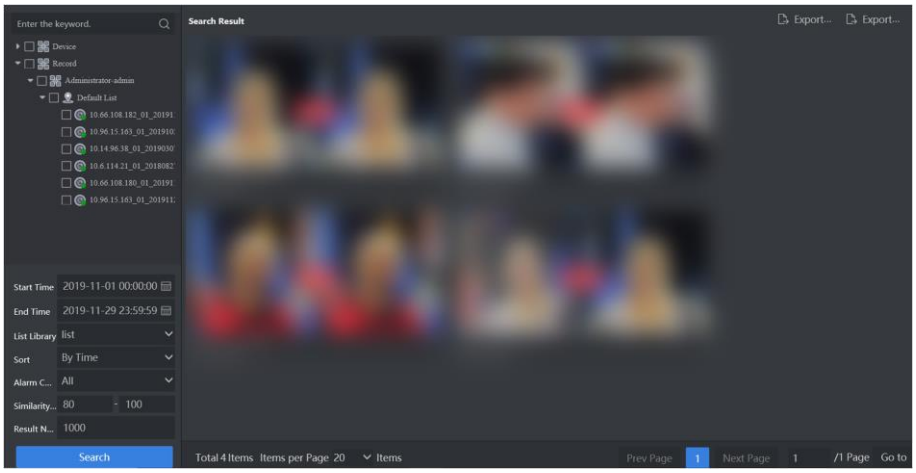

Figure 3-2 List Alarm Interface

2. Optional: Select the desired cameras or videos. If no camera or record is selected, all the alarm information will be searched.
3. Set search conditions according to actual needs.
4. Click **Search**.
5. Click alarm picture to view detailed information.

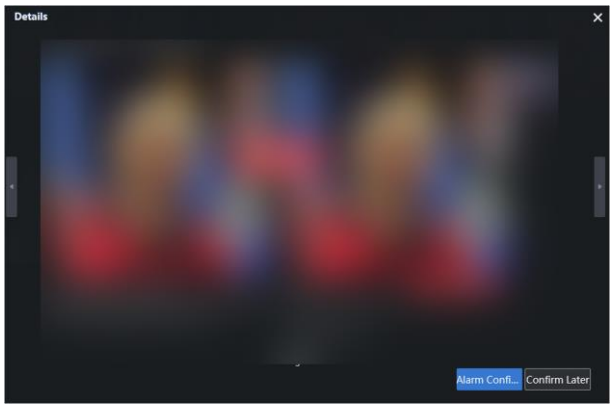

Figure 3-3 View Detailed Information

6. Optional: Click **Alarm Confirmation** to confirm.
7. Optional: Click **Export Current Page** or **Export All** to export alarm information.

3.2.2 Stranger Alarm

Compare the similarity between captured face pictures and those in list library. A stranger alarm will be triggered if the similarity value does not reach the configured value.

Before You Start

Add stranger arming.

Steps

1. Go to **Alarm Search** → **Stranger Alarm**. By default, the server displays all current alarm information.

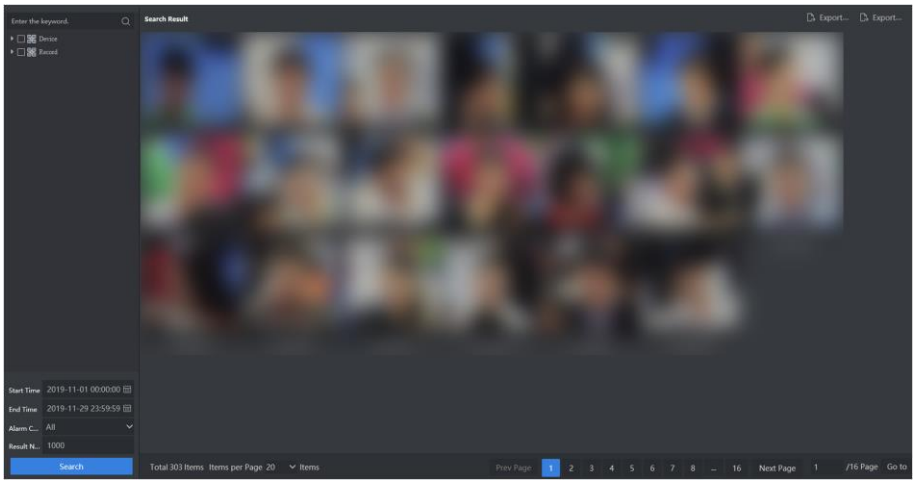

Figure 3-4 Stranger Alarm Interface

2. Optional: Select the desired cameras or records. If no camera or record is selected, all the alarm information will be searched.
3. Set search conditions according to actual needs.
4. Click **Search**.

5. Click stranger alarm picture to view detailed information.

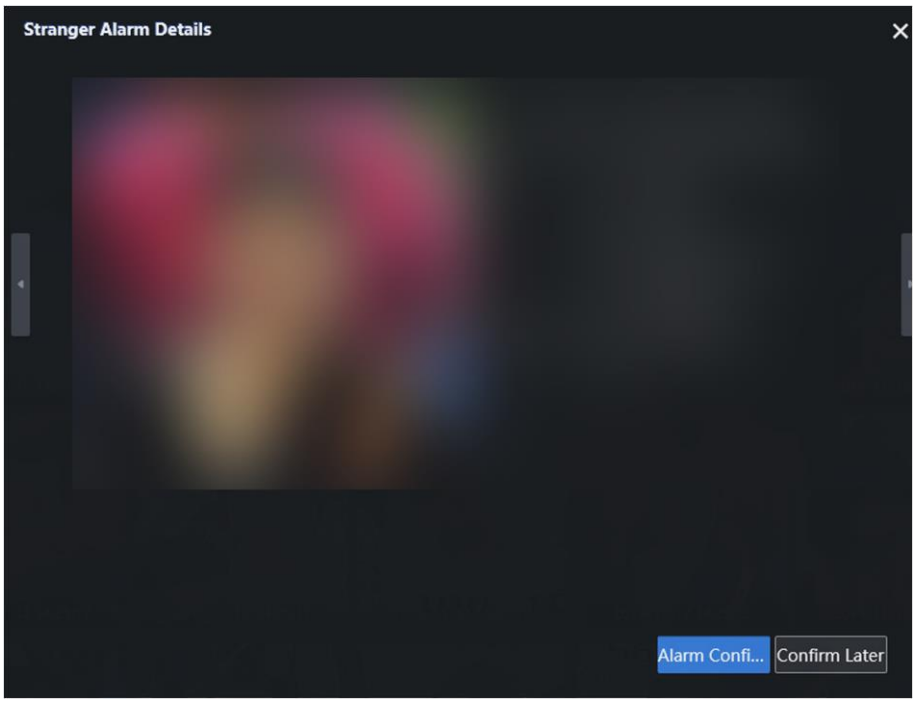

Figure 3-5 View Detailed Information of Stranger Alarm

6. Optional: Click **Alarm Confirmation** to confirm the alarm.
7. Optional: Click **Export Current Page** or **Export All** to export alarm information.

3.2.3 License Plate Alarm

Compare the license plate recognized by cameras with armed license plates. If the license plate captured by camera matches with one of the armed, a license plate alarm will be triggered.

Before You Start

Add license plate arming.

Steps

1. Go to **Alarm Search** → **Plate Alarm**. By default, the server displays all current alarm information.

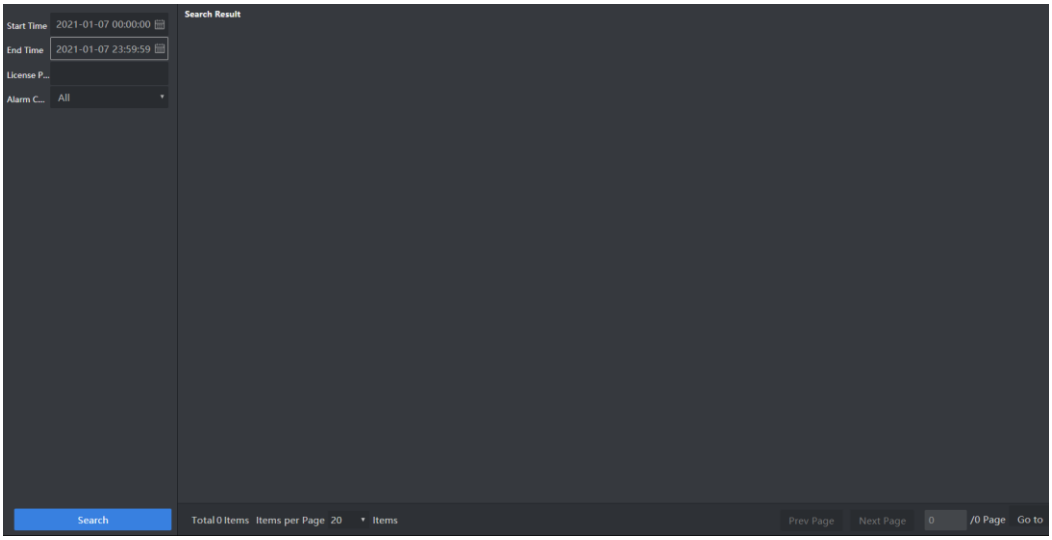

Figure 3-6 License Plate Alarm Interface

2. Optional: Select the desired cameras or records. If no camera or record is selected, all the alarm information will be searched.
3. Set search conditions according to actual needs.
4. Click **Search**.
5. Click alarm picture to view detailed information.

Figure 3-7 View Detailed Information-Plate Alarm

6. Optional: Click **Alarm Confirmation** to confirm the alarm.
7. Optional: Click **Export Current Page** or **Export All** to export alarm information.

3.3 Personnel Archive

Personnel archive records personnel appearance time period and respective captured pictures in monitoring scenes.

Before You Start

Enable personnel archive.

Steps

1. Go to **Smart Application** → **Personnel Archive**.

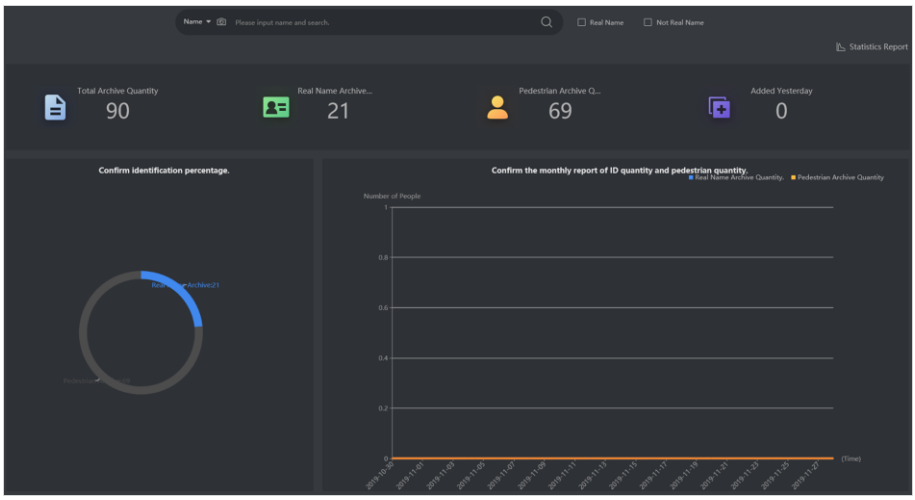

Figure 3-8 Personnel Archive Interface

Real Name

It refers to the personnel whose face picture is in list libraries, except the passerby library.

Not Real Name

It refers to the personnel whose face picture is in passerby library.

Statistic Report

You can also export the statistic report to generate an Excel or HTML file.

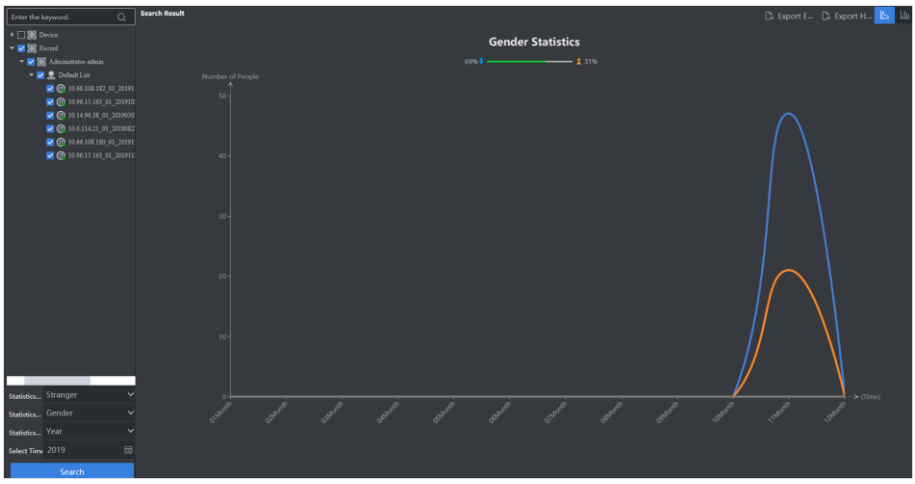

Figure 3-9 Statistic Report

2. Set search conditions according to actual needs and search personnel archive by clicking .

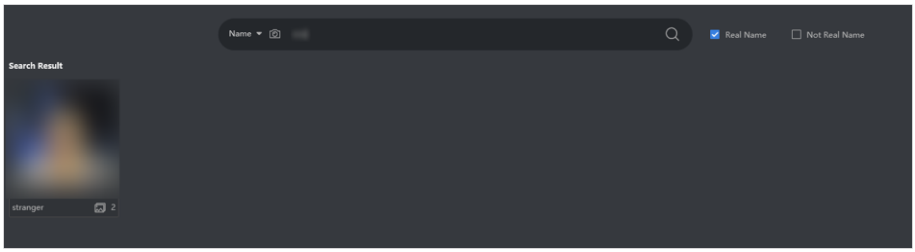

Figure 3-10 Personnel Archive Search Result

3. Click to view details.

3.4 1 V 1 Comparison

Upload two face pictures to compare their similarity degree.

Steps

1. Go to **Smart Application** → **1 V 1 Comparison**.

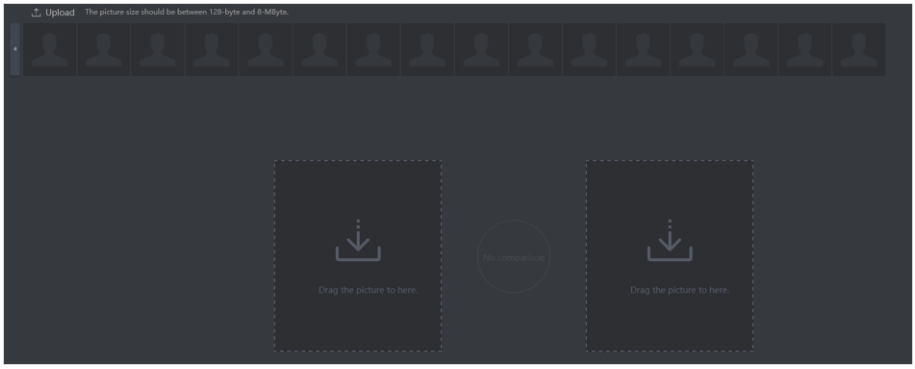

Figure 3-11 1 V 1 Comparison Interface

2. Click **Upload** to upload desired face pictures. If the selected picture contains multiple faces, these faces will all be uploaded.

Note

- Face pictures in the format of JPEG, BMP, TIF and PNG are supported. The resolution should be greater than 48 × 48 pixels and smaller than 64 MP, and the picture size should be greater than 128 KB and smaller than 8 MB.
- It is recommended to upload pictures with clear faces to improve the comparison accuracy.

3. Drag desired face pictures to comparison area for similarity comparison.

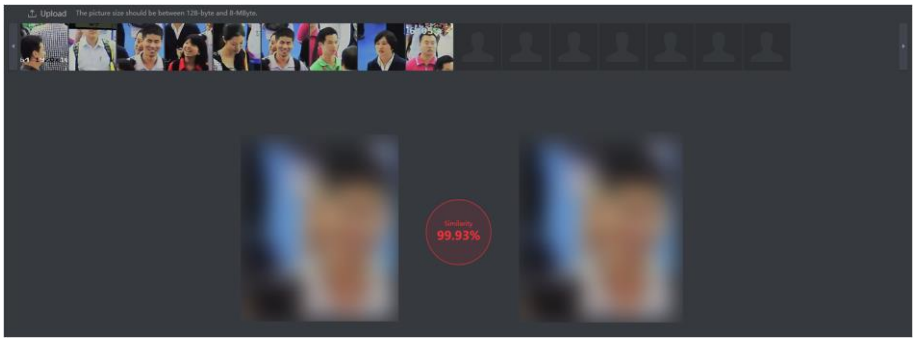

Figure 3-12 1 V 1 Comparison Result

Chapter 4 Smart Search

4.1 Search by Vehicle Attribute

Search captured vehicle pictures by vehicle attributes.

Before You Start

Alarm the camera.

Steps

1. Go to **Smart Search** → **Vehicle Search** → **Search by Attribute**. By default, the server displays all vehicle pictures captured by cameras.
2. Set detailed search conditions as needed. Fuzzy search for license plate is available.

Note

- If no camera or recording is selected, all captured vehicle pictures will be searched.
- You can set different search condition parameters by referring to ***Configure Display Parameters***

3. Click **Search**.

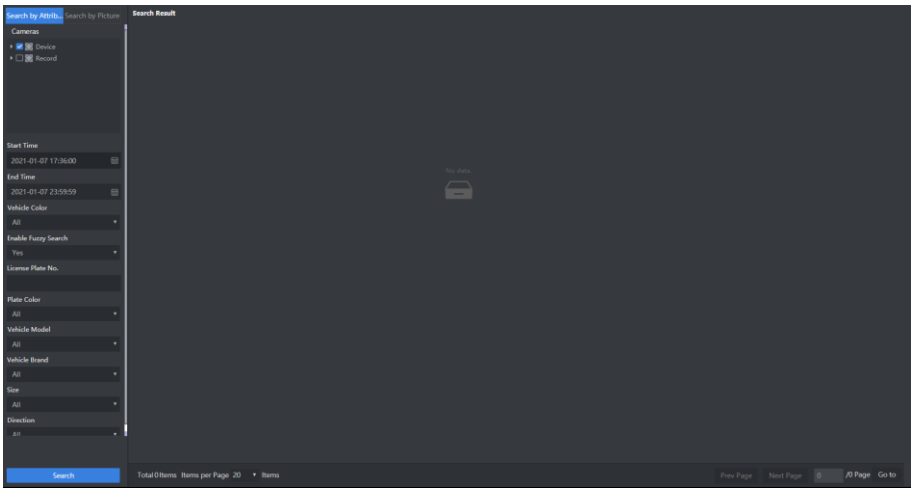

Figure 4-1 Vehicle Attribute Search Results

4. Click the face picture displayed to view detailed information.

Figure 4-2 Vehicle Capture Results

Note

Click to set this vehicle picture as target picture to search vehicle by vehicle.

5. Optional: Click **Export Current Page** or **Export All** to export captured information.

4.2 Search by Vehicle Picture

Upload a Vehicle picture to search related vehicle pictures in capture library.

Before You Start

Alarm the camera.

Steps

1. Go to **Smart Search** → **Vehicle Search** → **Search by Picture**. By default, the server displays all vehicle pictures captured by cameras.

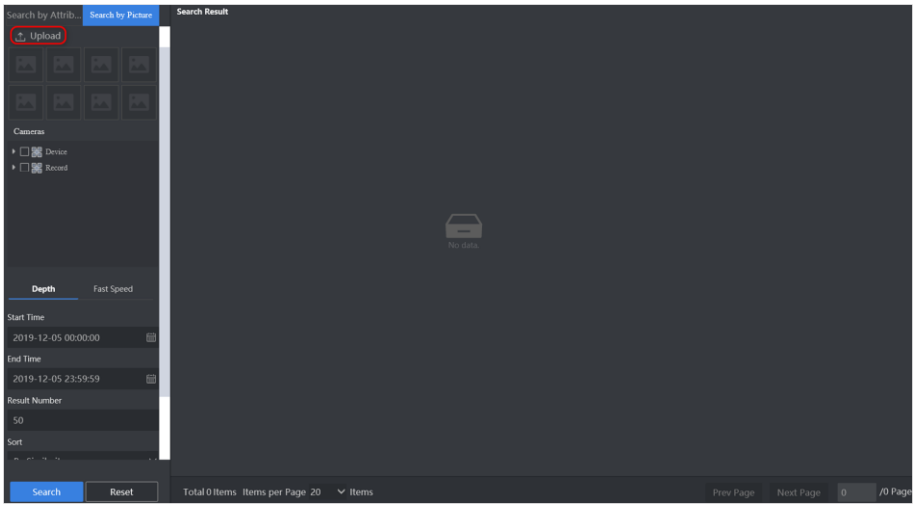

Figure 4-3 Search by Vehicle Picture Interface

2. Click **Upload** to upload desired vehicle pictures. The system will detect vehicles automatically.

Note

- Vehicle pictures in the format of JPEG, BMP, TIF and PNG are supported. The resolution should be greater than 48 × 48 pixels and smaller than 64 MP, and the picture size should be smaller than 8 MB.
- It is recommended to upload clear pictures of vehicles to improve the comparison accuracy.

3. Click the square frame above the vehicle and then click **OK**.
4. Select the desired vehicle picture and set detailed search conditions as needed.

Depth

Search by vehicle body similarities.

Fast Speed

Search by plate number, shape, brand and color.

Note

If no camera or recording is selected, all captured vehicle pictures will be searched.

5. Click **Search**.
6. Click the vehicle picture displayed to view detailed information.

Note

Click  to set this vehicle picture as target picture to search vehicle by vehicle.

7. Optional: Click **Export Current Page** or **Export All** to export searching results.

Chapter 5 System Management

5.1 Cluster Management

5.1.1 Delete Node

Before You Start

The node is online and not included in any cluster.

Steps

1. Go to **System Management** → **Cluster Management** → **Node Management**.
2. Check the desired node.
3. Click **Delete**, and click **OK** in the popup dialogue box.

5.1.2 Restart Node

Before You Start

The node is online.

Steps

1. Go to **System Management** → **Cluster Management** → **Node Management**.
2. Check the desired node.
3. Click **Restart**, and click **OK** in the popup dialogue box.

5.1.3 Power off Node

Before You Start

The node is online.

Steps

Note

After the node is powered off, the device can only be started by pressing power button, and remote start-up is not supported.

1. Go to **System Management** → **Cluster Management** → **Node Management**.
2. Check the desired node.
3. Click **OFF**, and click **OK** in the popup dialogue box.

5.1.4 Add More Nodes to Cluster

Add more nodes to cluster to enhance its capacity.

Before You Start

- Ensure the new node(s) is added to the list.
- The new nodes are on the same subnet of the cluster.

Steps

1. Go to **System Management** → **Cluster Management** → **Cluster Management**.
2. Click **Add to Cluster**.

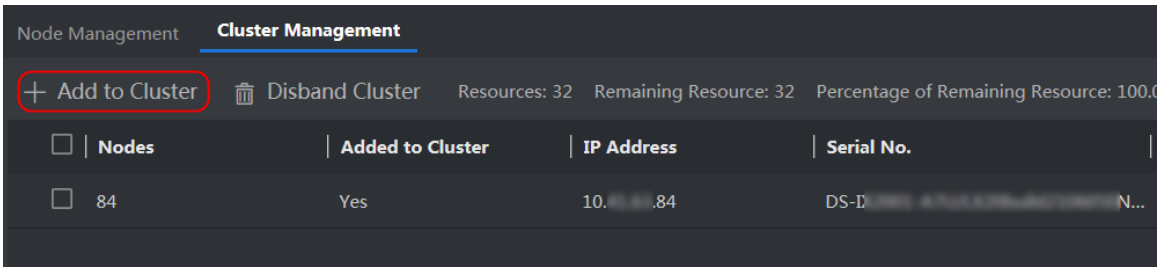

Figure 5-1 Add Nodes to Cluster

3. Check desired nodes, and click **Next**.

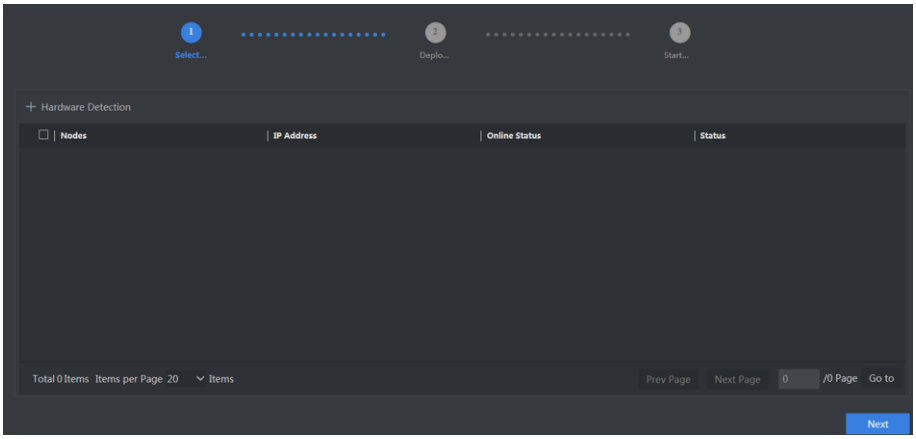

Figure 5-2 Check Desired Nodes

4. Click **Start Deploying**.
5. Click **OFF** after the cluster is deployed.

5.1.5 Disband Cluster

Steps

1. Go to **System Management** → **Cluster Management** → **Cluster Management**.
2. Click **Disband Cluster**.

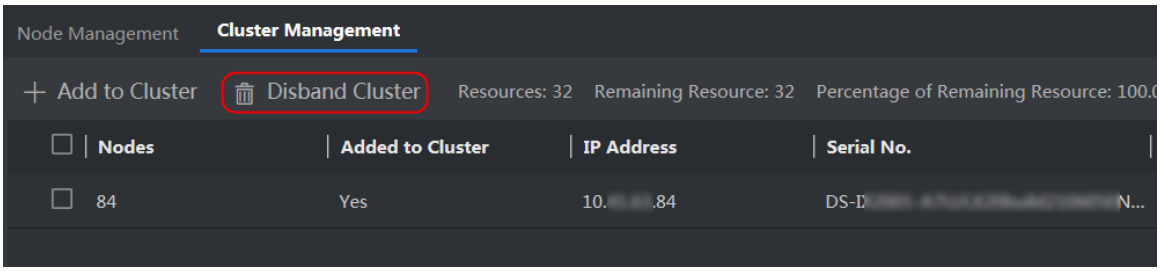

Figure 5-3 Disband Cluster

3. Click **OK**.

5.2 System Configuration

5.2.1 Configure General Information

You can keep the parameters in **General** as default value.

Note

- **Device Filter** is enabled by default, in which case the server is only accessible by its IP address. If you have configured port mapping, please disable the device filter function in order to access to the server normally.
- You can select a desired region in **Regional Configuration**. Delete structured task(s) before and reallocate resource for task(s) after switching regions.

5.2.2 Configure Service

It supports sending task analysis results to the configured IP address.

Before You Start

Obtain IP address, port or URL.

Steps

1. Go to **System Management** → **System Config** → **Service**.

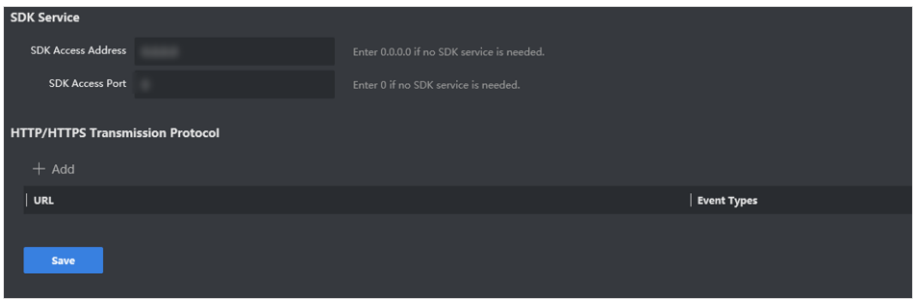

Figure 5-4 SDK Service

2. Set SDK service or HTTP transmission protocol according to actual needs.

SDK Service

Send task analysis results to the configured IP address via SDK protocol.

HTTP/HTTPS Transmission Protocol

Send task analysis results to the configured IP address via HTTP protocol.

3. Click **Save**.

5.2.3 Configure Score Setting

Score captured face pictures or pictures in the list library by attributes such as pupil distance, clarity, and pitch angle. This function can pass over those pictures with poor quality. The score setting is disabled by default.

Steps

1. Go to **System Management** → **System Config** → **Score Setting**.

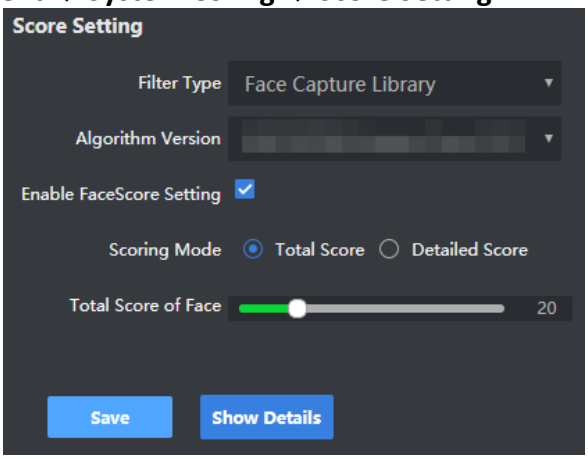

Figure 5-5 Score Setting

2. Select **Filter Type** as **Face Capture Library**.
3. Select an algorithm version, and enable score setting.
4. Set scoring mode as needed.
5. Click **Save**.
6. Optional: Click **Show Details** to check more information**.**
7. Optional: Click **Restore Default** to restore the default score value of each parameter under the detailed score mode**.**

5.2.4 Configure Pre-Classification

Steps

1. Go to **System Management** → **System Config** → **Pre-classification**.

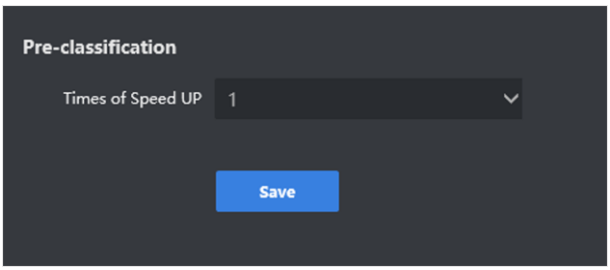

Figure 5-6 Pre-Classification Configuration

2. Set **Time of Speed Up** according to actual demands.
3. Click **Save**.

5.2.5 Configure Time

Synchronize the server time promptly. NTP and manual time synchronization are allowed .

Before You Start

Obtain the IP address and port of NTP server before synchronizing with NTP server time.

Steps

1. Go to **System Management** → **System Config** → **Time**.

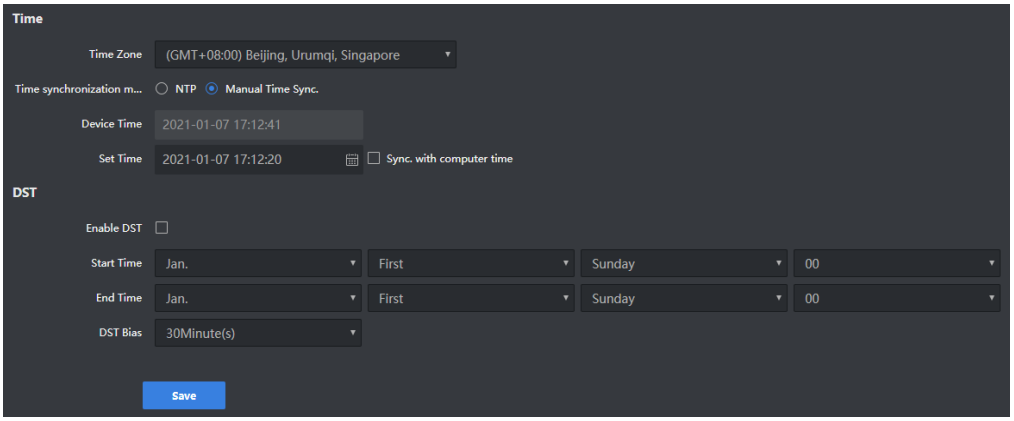

Figure 5-7 Time Configuration

2. Check **NTP** or **Manual Time Sync** according to actual demands.

Note

If **Sync. with computer time** is checked, the time of the server will be consistent with that of the computer.

3. Optional: Check **Enable DST** and set related parameters to synchronize the device time with that of the region where DST is applied.

Note

The device will restart if the time zone or DST settings change. You need to log in again.

4. Click **Save**.

5.2.6 User Management

There are three types of users, including admin, operator and consumer. Only admin has the permission to add and delete user, and edit user password. Operator and consumer have the permission to edit their own password only. Up to 32 users can be added.

Add User

Steps

1. Go to **System Management** → **System Configuration** → **User**

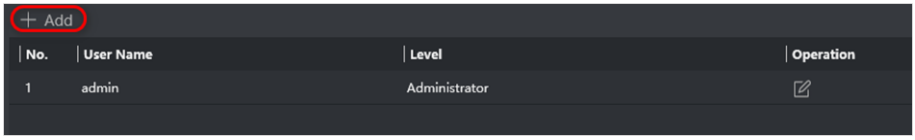

Figure 5-8 User Management Interface

2. Click **Add**, and input relevant information in the popup dialogue box.

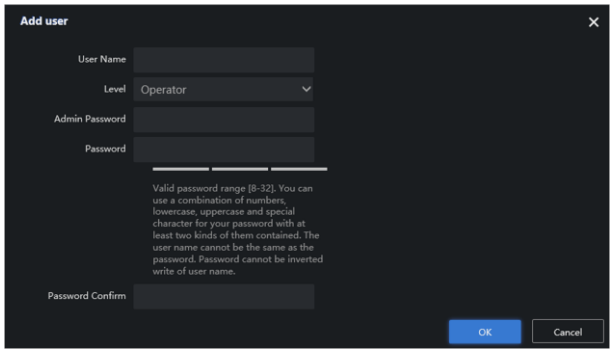

Figure 5-9 Add User

Note

- We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product.
- We recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

3. Click **OK**.

Modify Admin Password

Steps

1. Go to **System Management** → **System Config** → **User**.

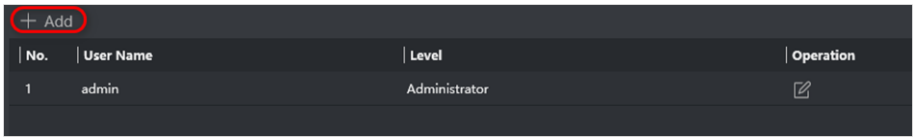

Figure 5-10 User Management

2. Click , and modify admin password in the popup dialogue box.

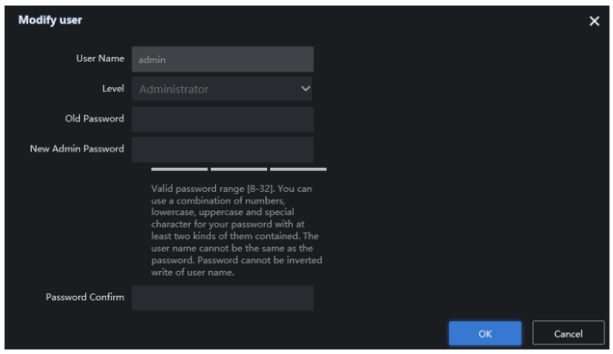

Figure 5-11 Modify User

3. Click **OK**.

5.2.7 Configure Display Parameters

Configure the search conditions for smart search function.

Steps

1. Go to **System Management** → **System Config** → **Display**.

Note

Enable **Display Time Zone** to display time zone in the search results, real-time alarms, and captured pictures. This function is disabled by default.

2. Set different search conditions according to actual needs.
3. Click **Save**.

5.2.8 Configuration Live View

Configure the play performance of live view, image format and saving path of manually captured pictures.

Steps

1. Go to **System Management** → **System Config** → **Live View**.

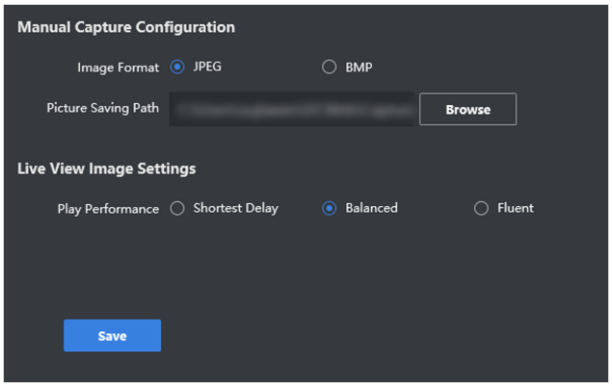

Figure 5-12 Live View Configuration

2. Set live view parameters.

   Manual Capture Configuration

   Select **JPEG** or **BMP** as **image format**, and configure **Picture Saving Path**.

   Live View Image Settings

   Set **Play Performance**. It is recommended to use default value.

3. Click **Save**.

5.2.9 Configure Person Pattern

Generate information of personnel movement path.

Steps

1. Go to **System Management** → **System Config** → **Person Pattern**.

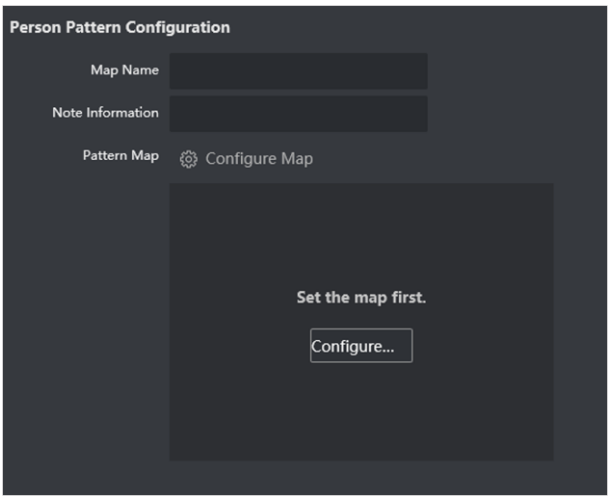

Figure 5-13 Person Pattern Configuration

2. Enter **Map Name** and **Note Information**.
3. Click **Configure Map** to upload a map.
4. Click **OK**.

5.2.10 Restore Default

Before You Start

The cluster has been disbanded.

Note

There are two types of restoration, including restore and default.

Restore

Restore all parameters, except the IP parameters and user information, to the default settings. As a result, the device will restart automatically and need to be activated again.

Default

Restore all parameters to the default settings. As a result, the device will restart automatically and need to be activated again.

Steps

1. Go to **System Management** → **System Config** → **Restore Defaults**.

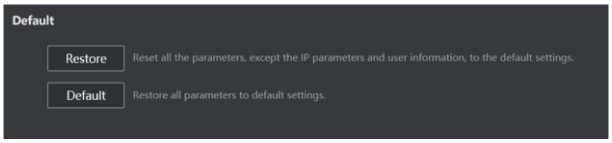

Figure 5-14 Restore Defaults Configuration

2. Select restoration type according to actual demands.

5.3 Enable Cloud Storage Authentication

If pictures submitted to the server attached with no authentication, or the authentication information expired, you need to enable cloud storage authentication.

Before You Start

Get the parameters of cloud storage.

Steps

1. Go to **System Management** → **System Config** → **Cloud Storage**.
2. Configure the related parameters.

IP Address

The IP address of micro video cloud.

Port

The port number of micro video cloud.

AK

Access key.

SK

Secret key.

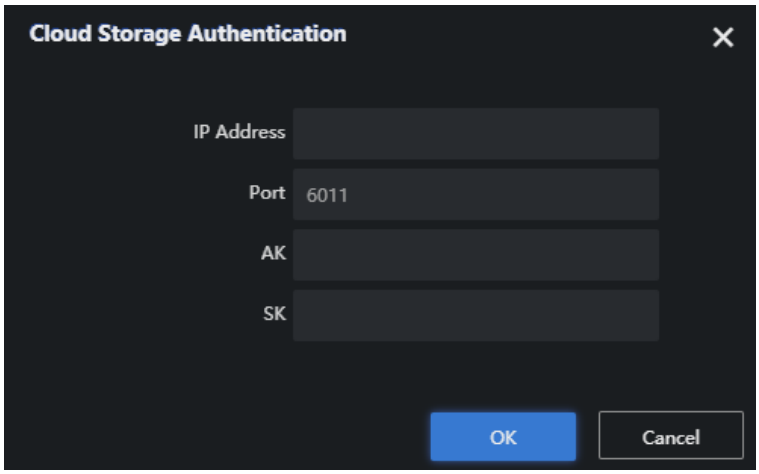

Figure 5-15 Cloud Storage Authentication

3. Click **OK**.

5.4 Strategy Parameters Configuration

To increase the precision of personnel archive, you can enable the scoring of similarity, captured picture, model fusion, etc. Personnel strategy is enabled by default.

Go to **System Management** → **System Config** → **Strategy Parameter** to check the parameters. It is recommended to keep the settings as default status.

5.5 Operation and Maintenance

5.5.1 Check Hardware Status

Check detailed information of CPU, memory, disk, GPU, etc.

Steps

1. Go to **System Management** → **Operation and Maintenance** → **Hardware Status**.
2. Click in **Details** list.

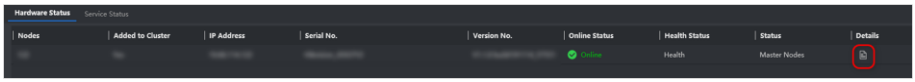

Figure 5-16 Hardware Status Interface

3. Click tabs to different hardware status.

5.5.2 Check Service Status

Check MongoDB, zookeeper, kafka and other service status.

Steps

1. Go to **System Management** → **Operation and Maintenance** → **Service Status**.

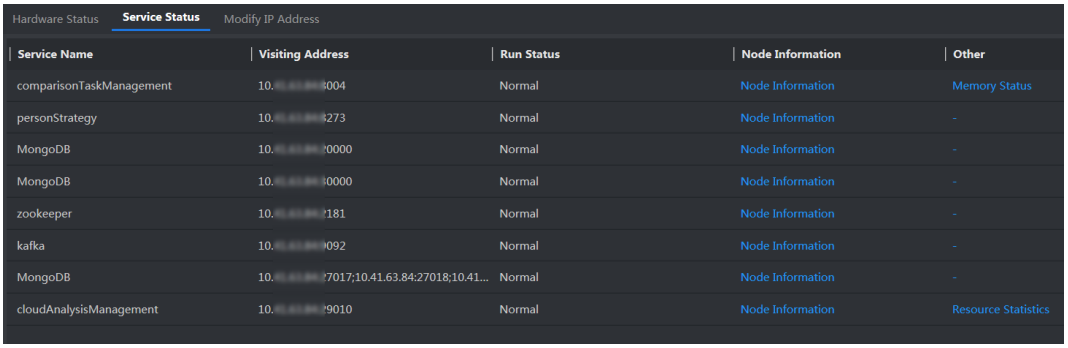

Figure 5-17 Service Status Interface

2. Click **Node Information**, **Memory Status** or **Resource Statistics** to check detailed information respectively.

   Node Information

   The node of current service.

   Memory Status

   The overall scale of memory, loaded data quantity, total number of dynamic library and capture duration.

   Resource Statistics

   The total and remaining resource quantity.

5.5.3 Modify IP Address

You can modify the IP address of cluster and micro video cloud through the web page of Intelligent Fusion Server.

1. Go to **System Management** → **Maintenance** → **Modify IP Address**.
2. Click **Modify IP Address**.

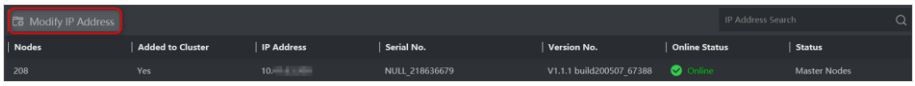

Figure 5-18 Modify IP Address

3. Modify the IP address as needed.
4. Click **Save**.

Figure 5-19 Save IP Address

5.5.4 Search Log

Log includes running log, alarm log and operation log. Searching and exporting logs are supported.

Running Log

Records running information.

Alarm Log

Records alarm information.

Operation Log

Records operation information in Wed interface.

Steps

1. Go to **System Management** → **Log**.
2. Select log type, set search start time and end time, and click **Search**.
3. Click **Export** to export searched log.
   - Enter search information in search bar, click to find log information.
   - Click **Maintenance** to export maintenance log for the maintenance staff's reference.

5.5.5 Check Online User

Check total quantity of users and real-time online users by click in the top-right corner of the interface.

5.5.6 Check Version Information

Go to → **Version** to check version information.

5.5.7 Check Help Document

Go to → **Help Document** to refer to help information.

5.5.8 Upgrade Software

It is allowed to upgrade software through web interface.

Before You Start

- The device is online and running normally.
- Obtain updating files.

Steps

1. Go to **System Management** → **Software Updating**.

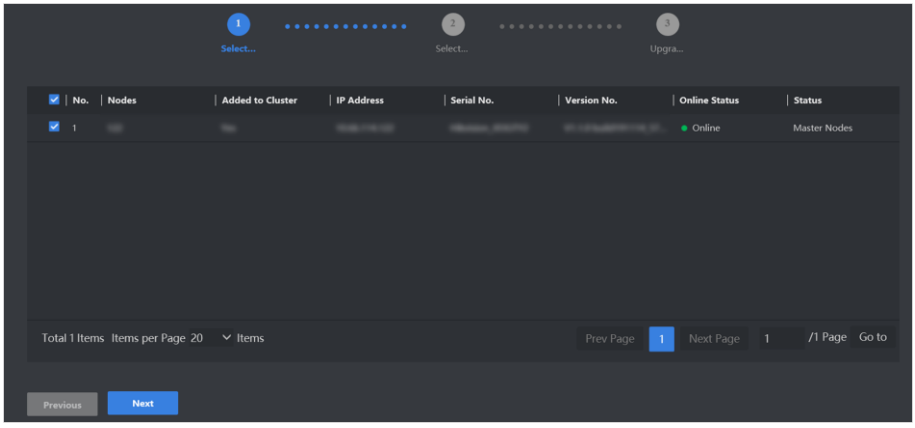

Figure 5-20 Software Updating Interface

2. Check the desired server, and click **Next**.

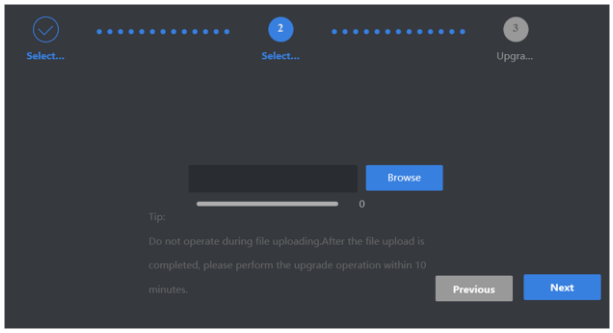

Figure 5-21 Select Uploading Files

3. Click **Browse** to upload updating files, and then click **Next**.

4. Click **OK**.

Note

The device will reboot after updating completed.

5.6 Log Out

Go to **admin** → **Logout** to log out.


See Far, Go Further