



Edge Facial Recognition Server

User Manual

Legal Information

©2021 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

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 edge facial recognition 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

Danger

- This is a class A product and may cause radio interference in which case the user may be required to take adequate measures.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- The equipment must be connected to an earthed mains socket-outlet.
- Shock hazard! Disconnect all power sources before maintenance.
- This equipment is not suitable for use in locations where children are likely to be present.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or

the leakage of flammable liquid or gas.

- Dispose of used batteries according to the instructions.
- This equipment is not suitable for use in locations where children are likely to be present.
- Keep body parts away from fan blades. Disconnect the power source during servicing.

Caution

- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains, etc. The openings shall never be blocked by placing the equipment on a bed, sofa, rug or other similar surface.
- Keep a minimum 5 cm distance around the equipment for sufficient ventilation.
- The USB port of the equipment is used for connecting to a mouse, a keyboard, or a USB flash drive only.
- Burned fingers when handling the heat dissipation parts. Wait one-half hour after switching off before handling the parts.
- This equipment is suitable for use in server room only.
- Install the equipment according to the instructions in this manual.
- To prevent injury, this equipment must be securely attached to the rack in accordance with the installation instructions.

Contents

Chapter 1 Introduction	1
1.1 Key Features	1
1.2 PC Requirements	1
Chapter 2 Configuration Wizard	2
2.1 Activate	2
2.2 Login	3
2.3 Create Analysis Cluster	4
2.4 Add Face List Library	5
2.5 Add Personnel Information	5
2.6 Create Analysis Task	6
2.6.1 Add Camera	7
2.6.2 Create Real-time Analysis Task	9
2.6.3 Create Video Record Analysis Task	11
2.7 Add Arming	13
2.7.1 Add List Arming	13
2.7.2 Add Stranger Arming	15
2.8 Enable Frequency Alarm	16
2.9 Enable Low Frequency Alarm	17
2.10 Enable Personnel Archive	18
Chapter 3 Smart Application	21
3.1 Live View	21
3.2 Alarm Search	22
3.2.1 List Alarm	22
3.2.2 Stranger Alarm	23
3.2.3 Frequently Appeared Person Alarm	25
3.2.4 Low Frequency Alarm	26
3.3 Personnel Archive	28
3.4 1 V 1 Comparison	30

Chapter 4 Smart Search	32
4.1 Search by Facial Attribute	32
4.2 Search by Face Picture	33
4.3 Confirm Identification	34
Chapter 5 System Management.....	36
5.1 Cluster Management.....	36
5.1.1 Restart Node.....	36
5.1.2 Power off Node	36
5.1.3 Disband Cluster	36
5.2 System Configuration	37
5.2.1 Configure General Information.....	37
5.2.2 Configure Service.....	37
5.2.3 Configure Cloud Storage	38
5.2.4 Configure Time	38
5.2.5 User Management.....	38
5.2.6 Configure Display Parameters	40
5.2.7 Configuration Live View	40
5.2.8 Restore Default	41
5.2.9 Configure Data Upgrade.....	42
5.2.10 Configure Strategy Parameter	42
5.3 Operation and Maintenance.....	42
5.3.1 Check Hardware Status	42
5.3.2 Search Log.....	43
5.3.3 Check Online User	43
5.3.4 Check Version Information	43
5.3.5 Check Help Document	43
5.3.6 Upgrade Software	43
5.4 Log Out.....	44

Chapter 1 Introduction

Based on the intelligent analysis technology, the edge facial recognition server (hereafter referred as the sever) can achieve various intelligent applications, such as analyzing, comparing, searching, and giving alarms. The server can provide efficient, convenient, and professional solutions for scenarios such as entrances and exits, and checkpoints. It is widely applied for public security, transportation, judicature, financial, telecommunication, and other fields.

1.1 Key Features

- Human face list management.
- Human face list library arming.
- Human face detection in different monitoring scenarios.
- Rapid search for human face information in capture library.
- Supports list alarm, stranger alarm, high frequency alarm, low frequency alarm, and license plate alarm.
- Settings of alarm popup and sound.
- Establish archives for each personnel.
- Rapid 1V1 face similarity comparison.
- Searches picture by attribute or picture, and displays search results in order of similarity from high to low or in time order.
- Supports personnel identification and displaying search results in order of similarity from high to low.
- Views the usage of device resource.
- User permission management of admin, operator and consumer.
- NTP or manual time synchronization.
- Software updating available.

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 10 or 11.

Chapter 2 Configuration Wizard

2.1 Activate

The device can be activated via Web browser. The default IP address is 192.168.1.64.

Before You Start

- Make sure your PC connects to the Internet.
- Modify the IP address of your PC to make sure the PC and the server are on the same subnet.

Steps

1. Double click the IE browser, and enter the default IP address (192.168.1.64) of the server.
2. Press **Enter** to enter the activation interface.

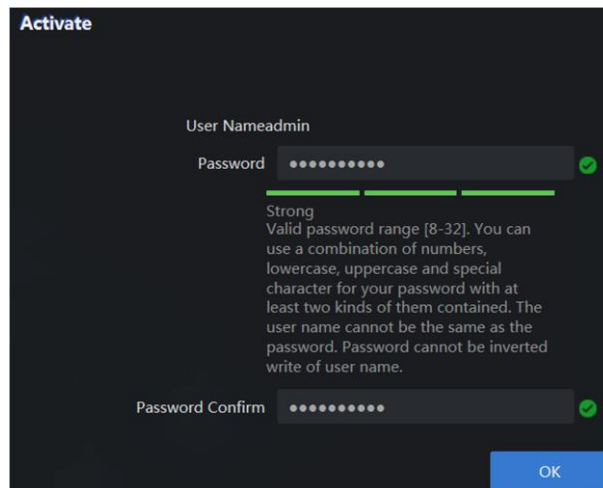


Figure 2-1 Activation Interface

Caution

Strong Password recommended-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. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Note

The password of root user will be changed when the activation password is set. As a result, the password of root user will be the same as that of admin user.

3. Enter password and confirm.
4. Click **OK**.

2.2 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 2-2 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.
-

2.3 Create Analysis Cluster

A node named 'Local' is established by default. Use the node to create an analysis cluster for data analyzing.

Before You Start

Ensure that the node is online.

Steps

1. Go to **System Management** → **Cluster Management**, and select the node.
2. Click **Create Cluster**, and click **OK**.

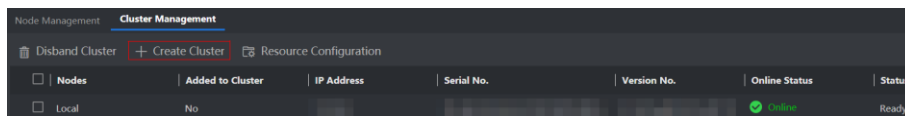


Figure 2-3 Create Cluster

Refresh the page, if the status shows **Activated**, the cluster is created.

3. Click **Resource Configuration** to allocate resources for different analysis tasks.

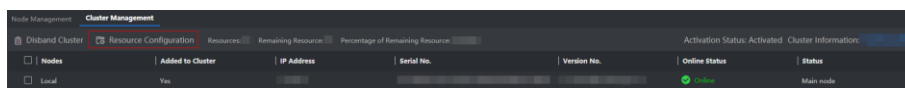


Figure 2-4 Resource Configuration

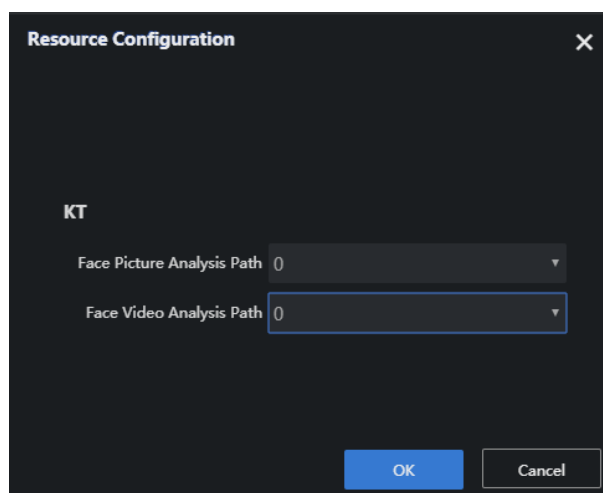


Figure 2-5 Allocate Resource

Note

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

2.4 Add Face List Library

Add different list libraries for list arming. The passerby library is created by default.

Steps

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

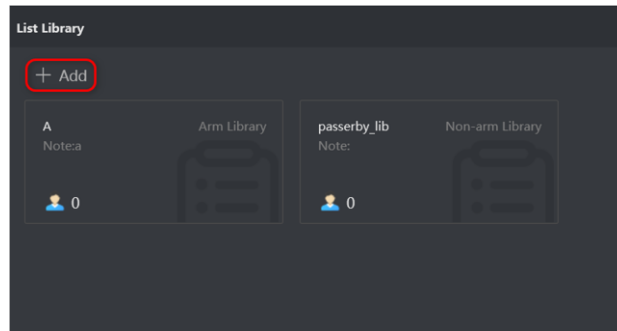


Figure 2-6 Add List Library

2. Enter the library name and related information.

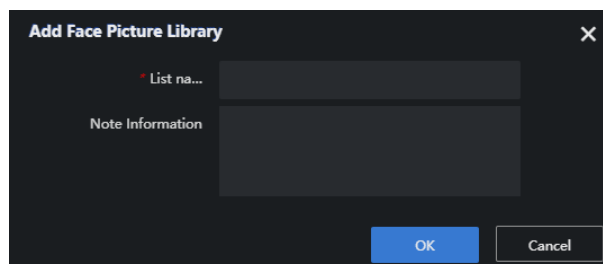




Figure 2-7 Configure Library Information

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.
-

2.5 Add Personnel Information

Before You Start

A face list library has been added.

Steps

1. Click the desired list library to add personnel.

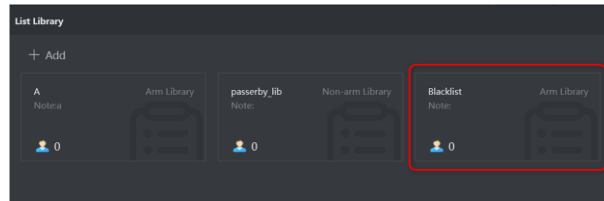


Figure 2-8 Click List Library

2. Click **Add**, enter relevant parameters in the dialogue box, and upload face pictures.

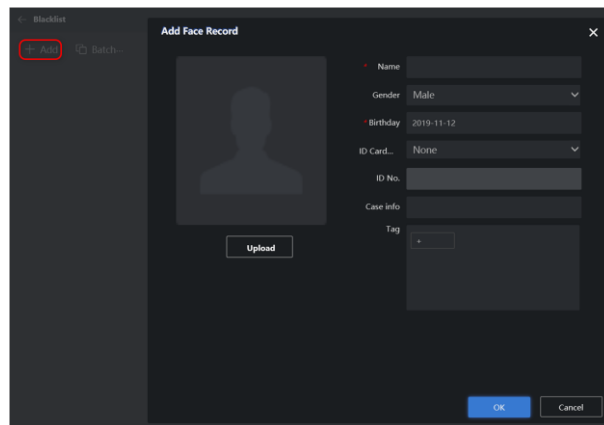





Figure 2-9 Add Personnel Information

Note

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

2.6 Create Analysis Task

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

analysis task, you should add respective resources like cameras, video records, etc.

2.6.1 Add Camera



Before creating analysis tasks, you need to add camera channels for real-time analysis.

Before You Start

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

Steps

Note

- Add one camera at a 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 **Target Arming** → **Task Management** → **Camera Management**.
2. Go to **Administration-admin** → .

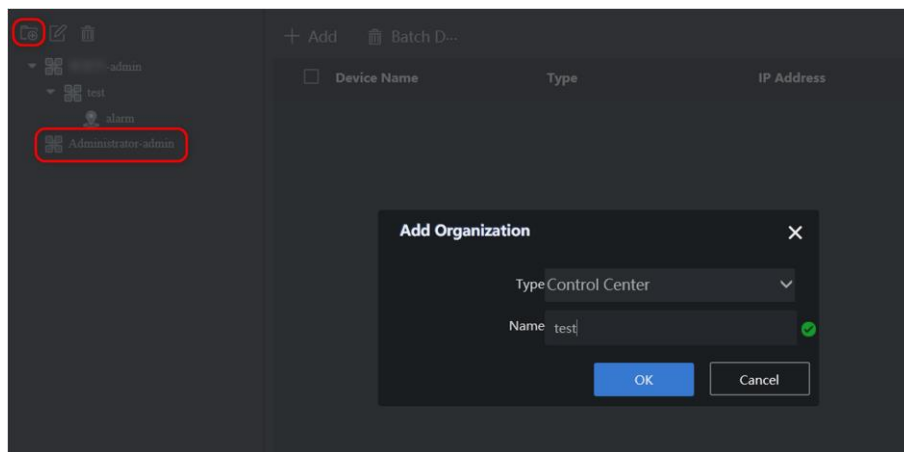


Figure 2-10 Add Control Center

3. Select **Type** as **Control Center**, and enter a name, then click **OK**.
4. Click the newly-added control center, and click **Add**.
5. Enter information in the popup window, and click **OK**.

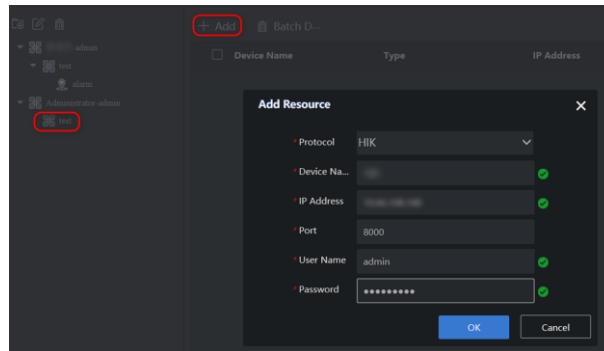



Figure 2-11 Add Camera

6. Click , and select **Type** as **Area**.
7. Enter a name, and click **OK**.

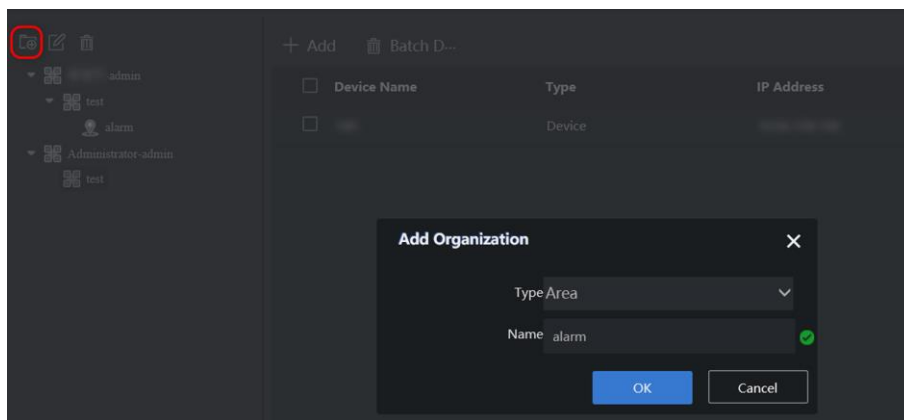


Figure 2-12 Add Area

Note

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

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

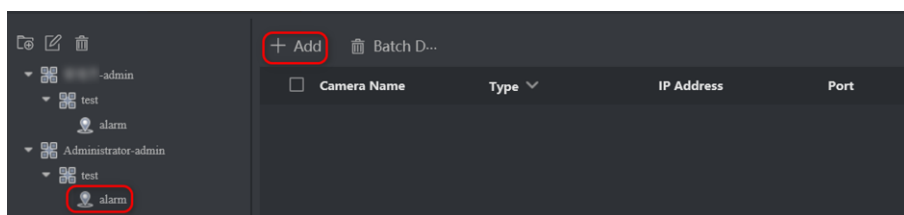


Figure 2-13 Add Camera to Area

Note

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

9. Select the desired camera(s), and click **OK**.

Note

Both control centers and areas can be added to control centers, but only cameras can be added to areas.

2.6.2 Create Real-time Analysis Task

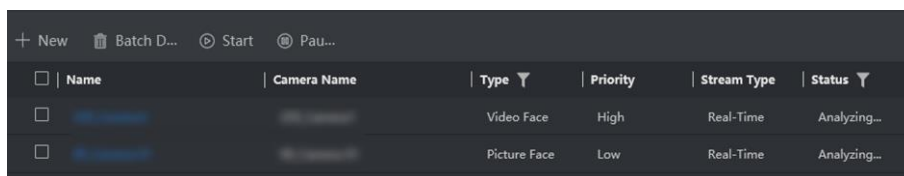
Real-time analysis task is used to perform real-time analysis of targets in monitoring scene.

Before You Start

The camera has been added.

Steps

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



<input type="checkbox"/>	Name	Camera Name	Type	Priority	Stream Type	Status
<input type="checkbox"/>	Video Face	Video Face	Video Face	High	Real-Time	Analyzing...
<input type="checkbox"/>	Picture Face	Picture Face	Picture Face	Low	Real-Time	Analyzing...

Figure 2-14 Task Management

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

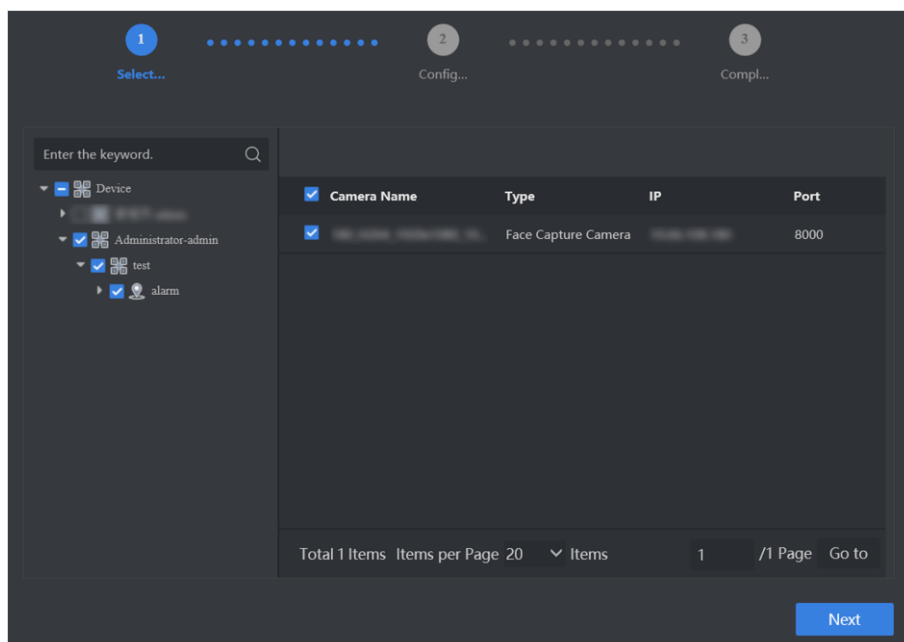



Figure 2-15 Check Cameras

3. Optional: Click  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 pupil distance is set, only faces whose pupil distance is between the minimum and maximum values will be detected.
- Keep other parameters as default value.

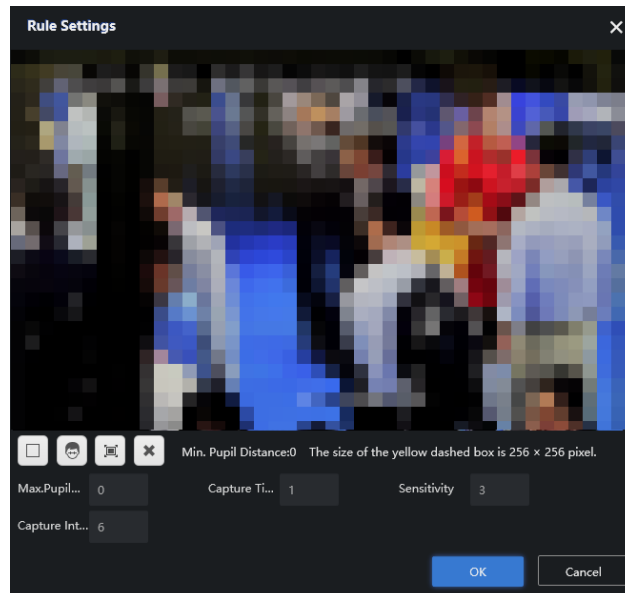



Figure 2-16 Set Rule

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 Face

Analysis and comparison of faces in videos.

Picture Face

Analysis and comparison of faces in pictures.

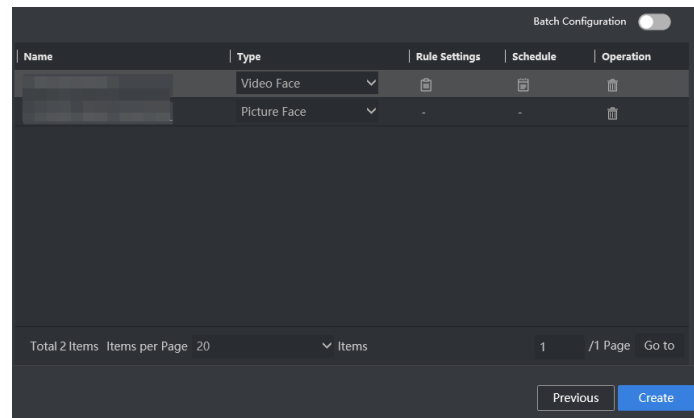


Figure 2-17 Create Real-time Analysis Task

2.6.3 Create Video Record Analysis Task

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

Before You Start

- Import video record files.
- Allocate resources.

Steps

1. Go to **Smart Application** → **Video Analysis**, and click **New**.
2. Click **Default List**, and then click **Import**.

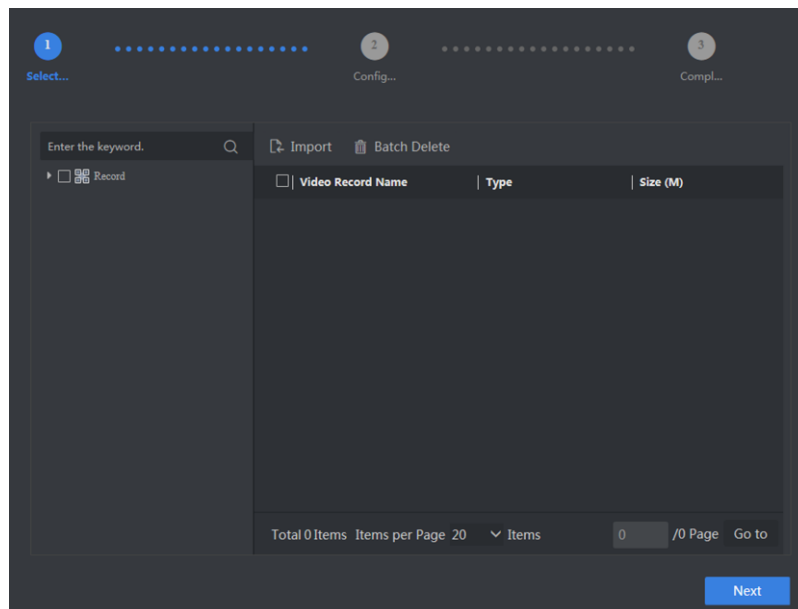


Figure 2-18 Import Video

Caution

Set the video starting time, otherwise the time of analysis results will be inconsistent with that of actual recording.

3. Click **Browse** to select desired video recording files.
4. Set the actual time of recording as starting time, and click **OK**.
5. Click **Import** and select the desired video(s), and click **Next**.

Video Face

Analysis and comparison of faces in videos.

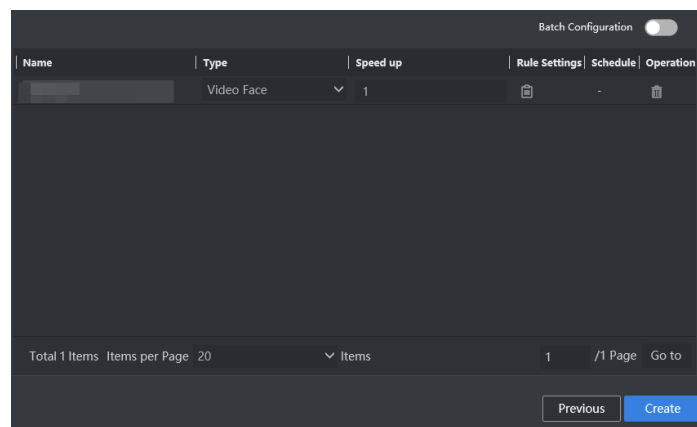





Figure 2-19 Select Recordings

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.

6. Optional: Click  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 pupil distance is set, only faces whose pupil distance is between the minimum and maximum values will be detected.
 - Keep other parameters as default value.

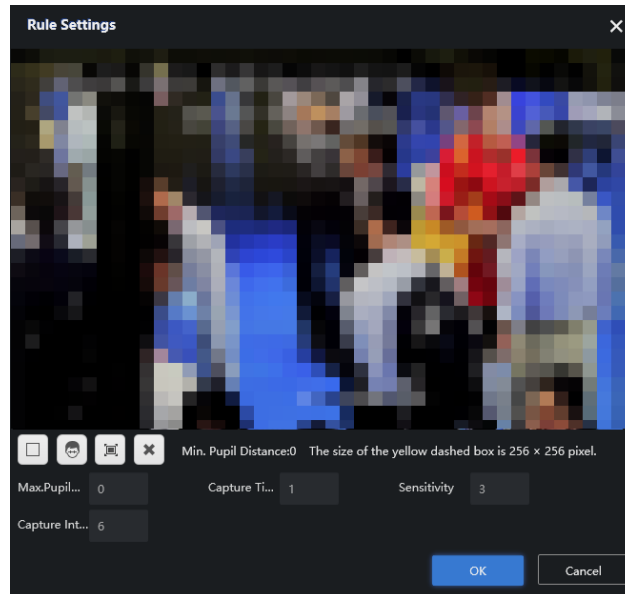


Figure 2-20 Set Rule

7. Click **OK** and **Create**.

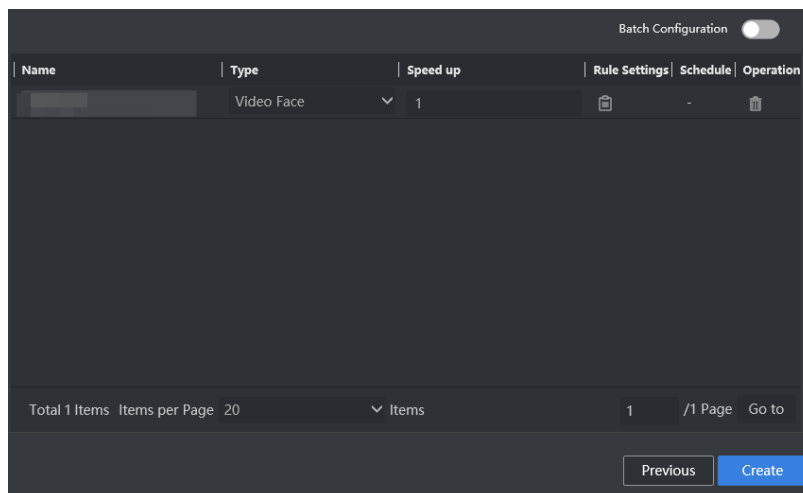


Figure 2-21 Create Video Record Analysis Task

2.7 Add Arming

2.7.1 Add List Arming

Listing arming is used to compare the faces 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.

Steps

1. Go to **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.
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.

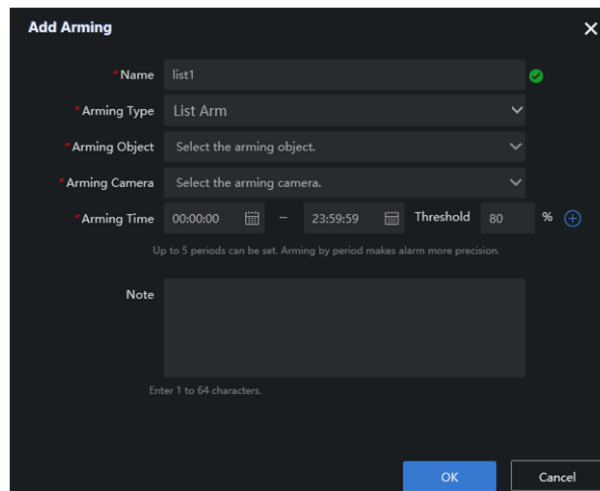




Figure 2-22 Set List Arming Parameters

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 faces 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.

Steps

1. Go to **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.

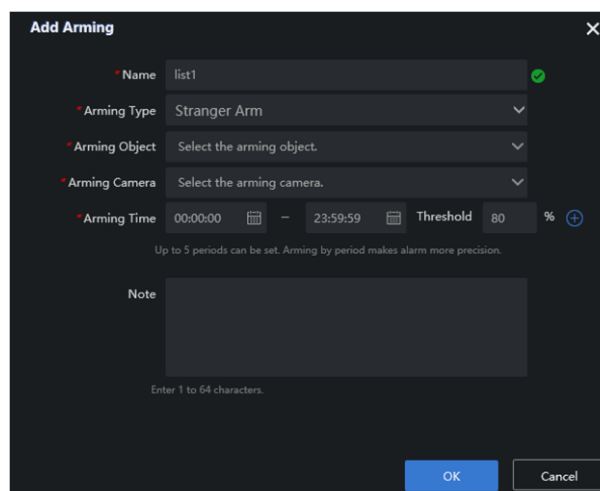




Figure 2-23 Set Stranger Arming Parameters

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  .

2.8 Enable Frequency Alarm

Frequency alarm is used to count the frequency of personnel's appearance in monitoring scenes. An alarm will be triggered if the frequency reaches the configured threshold during specific period.

Before You Start

One or multiple cameras are added and armed.

Steps

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

Table 2-5 Parameter Setting

Parameter Name	Description
Arming Camera	Select the desired camera to count the personnel appearance frequency.
Arming Object	Select the desired list library for arming and counting.
Filtering Threshold	Compare the similarity between face captured by camera and that of face list library. If the similarity is greater than or equal to the set value, the personnel captured will not be counted.
Times	Frequency alarm will be generated only when the appeared times is greater than the configured times.
Capture Interval (min)	The internal of capturing face picture for the same personnel. (Unit: minute)
Similarity	Compare the similarity between newly captured face pictures and all captured face pictures. If the similarity is greater than or equal to the configured value, the appearance frequency for the same personnel will be counted.
Day Range	The statistics period of personnel appearance frequency. The data of the earliest day will be covered by the newly-added data if the actual number of days is greater than this value.

Parameter Name	Description
Time Segment	Set time period to count personnel appearance frequency.

The screenshot shows a dark-themed configuration window titled "Frequency". At the top, there is an "Enable" checkbox which is currently unchecked. Below it are several configuration fields: "Arming Camera" is a dropdown menu showing "185_IpCamera_1"; "Arming Object" is a dropdown menu showing "Select a list library"; "Filtering Threshold" is a text input field containing the number "85"; "Times" is a text input field containing "1"; "Capture Interval(min)" is a text input field containing "1"; "Similarity" is a text input field containing "1"; "Day Range" is a text input field containing "7"; and "Time Segment" is a time range selector showing "00:00:00" to "23:59:59" with calendar icons. At the bottom center of the window is a blue "Save" button.

Figure 2-24 Enable Frequency Alarm

3. Click **Save**.

2.9 Enable Low Frequency Alarm

Low frequency alarm is used to count the frequency of personnel's appearance in monitoring scenes. An alarm will be triggered if the frequency does not reach the configured threshold during specific period.

Before You Start

One or multiple cameras have been added and armed.

Steps

1. Go to **System Management** → **System Config** → **Low Frequency**.
2. Configure the parameters as below.

Table 2-6 Parameter Setting

Parameter Name	Description
Arming Camera	Select the desired camera to count the personnel appearance frequency.
Arming Object	Select the desired list library for arming and counting.

Parameter Name	Description
Times	Frequency alarm will be generated only when the appeared times is smaller than the configured times.
Capture Interval (min)	The internal of capturing face picture for the same personnel. (Unit: minute)
Day Range	The statistics period of personnel appearance frequency. The data of the earliest day will be covered by the newly-added data if the actual number of days is greater than this value.
Daily Alarm Time	Set time to alarm.

Figure 2-25 Enable Low Frequency Alarm

3. Click **Save**.

2.10 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 frequency, appearance duration and captured pictures. Every personnel will be recorded with a separated archive.

Before You Start

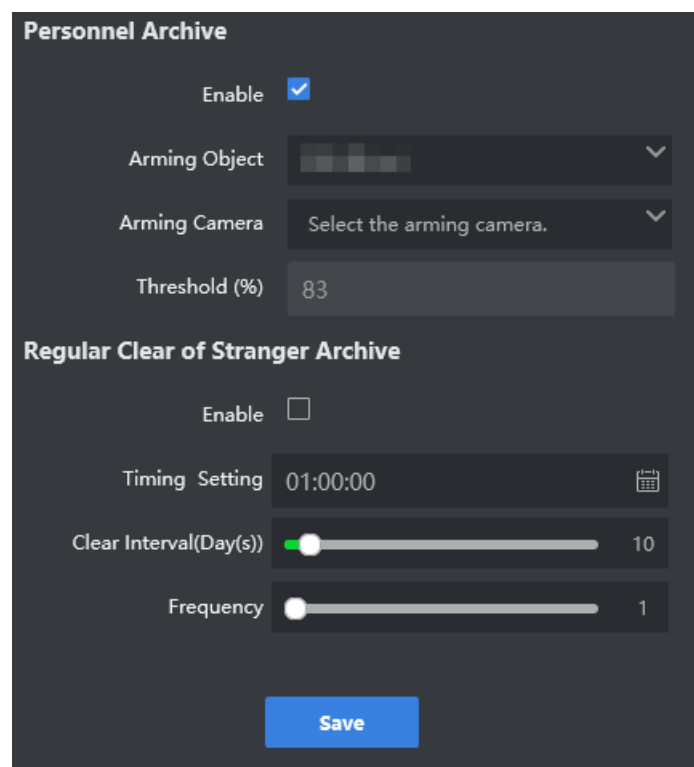
At least one camera has been added and armed.

Steps

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

Table 2-7 Parameter Setting

Parameter Name	Description
Arming Object	Select Passerby Library and other desired lists.
Arming Camera	Select the desired cameras.
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.
Timing Setting	Set the time for daily clear of stranger archive. For better performance, it is recommended to set between 00:00 am to 6:00 am.
Clear Interval (Day)	Set the day range of clear. For example, if this value is set as 10, then the information of strangers whose frequency is lower than the threshold in recent 10 days will be cleared.
Frequency	Set the threshold value for appearance frequency.



The screenshot shows a configuration window titled "Personnel Archive". It contains two main sections: "Personnel Archive" and "Regular Clear of Stranger Archive".

Personnel Archive

- Enable:** A checkbox that is checked (blue checkmark).
- Arming Object:** A dropdown menu showing a blurred image of a person.
- Arming Camera:** A dropdown menu with the text "Select the arming camera."
- Threshold (%):** A text input field containing the value "83".

Regular Clear of Stranger Archive

- Enable:** A checkbox that is unchecked.
- Timing Setting:** A text input field containing "01:00:00" with a calendar icon to its right.
- Clear Interval(Day(s)):** A slider control with a green indicator, ranging from 0 to 10, with "10" displayed on the right.
- Frequency:** A slider control with a white indicator, ranging from 0 to 1, with "1" displayed on the right.

At the bottom of the window is a blue button labeled "Save".

Figure 2-26 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, frequently appeared personnel alarm information, and low frequency alarm information.

Before You Start

Add list arming.

Steps

1. Click **Live View**.

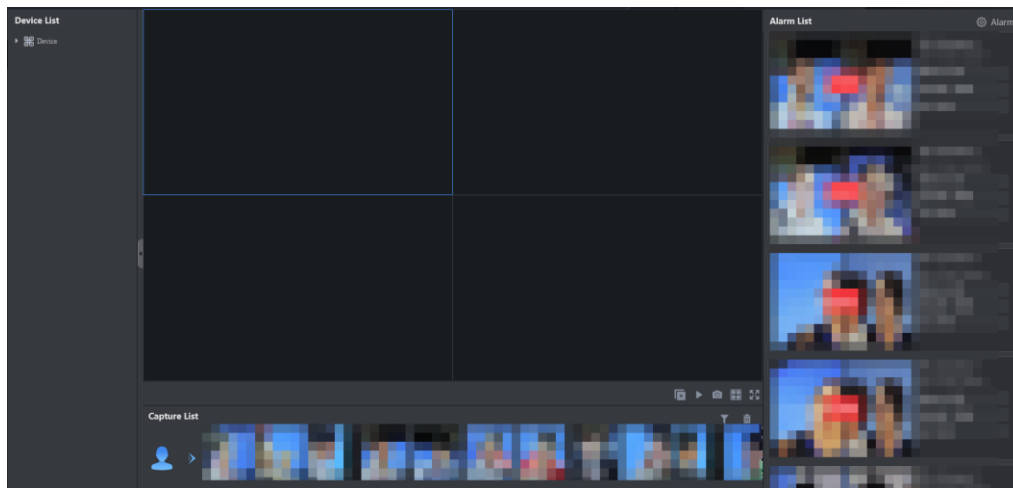












Figure 3-1 Live View

Note

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

Table 3-1 Live View Interface Introduction

Interface Area	Description
Live View Window	<p>Live view with multi-channels is supported.</p> <ul style="list-style-type: none">• 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 System Management → System

Interface Area	Description
	Config → Live View to configure the saving path. <ul style="list-style-type: none">Click  to view in split windowClick  to view in full screen.
Capture List	Display the real-time captured face pictures. <ul style="list-style-type: none">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, frequently appeared person alarm and license plate alarm.

3.2.1 List Alarm

Compare the similarity between captured face pictures and those in list library like blacklist 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.

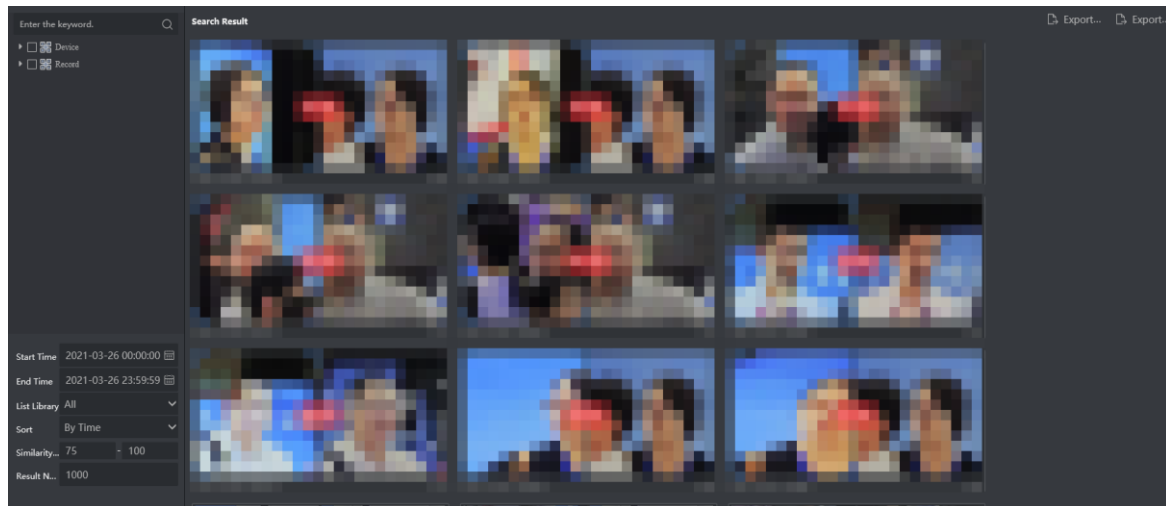


Figure 3-2 List Alarm

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. Optional: Click alarm picture to view detailed information.

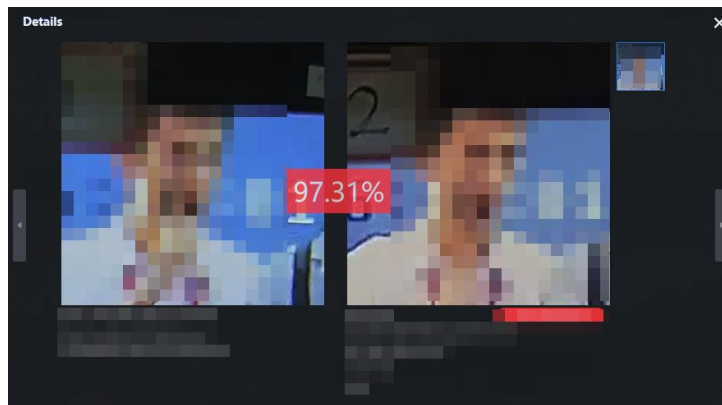


Figure 3-3 View Detailed Information-List Alarm

6. 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.

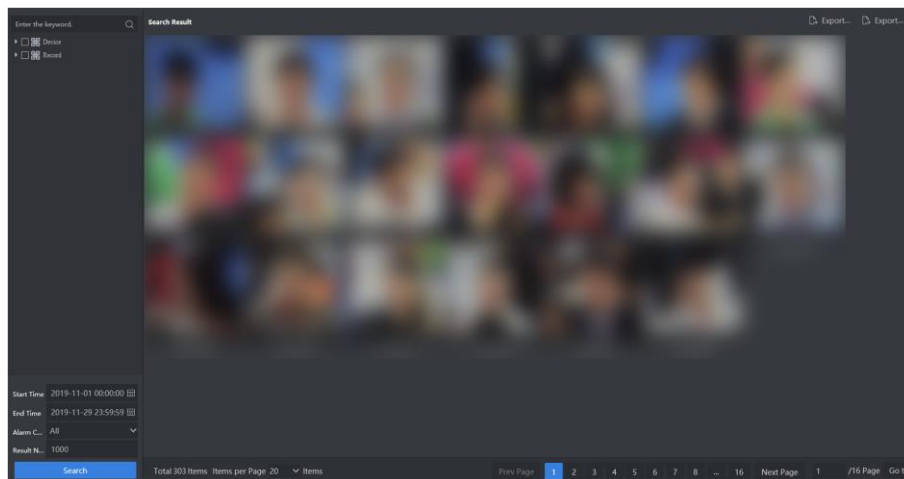


Figure 3-4 Stranger Alarm

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. Optional: Click stranger alarm picture to view detailed information.

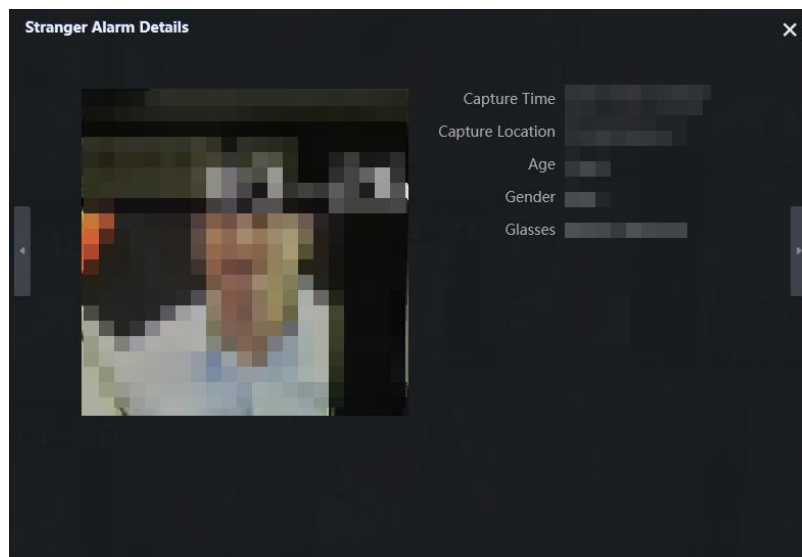


Figure 3-5 View Detailed Information-Stranger Alarm

6. Optional: Click **Export Current Page** or **Export All** to export alarm information.

3.2.3 Frequently Appeared Person Alarm

Count personnel appearance frequency in monitoring scenes. An alarm will be triggered if the frequency reaches the configured value.

Before You Start

Enable frequency alarm.

Steps

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

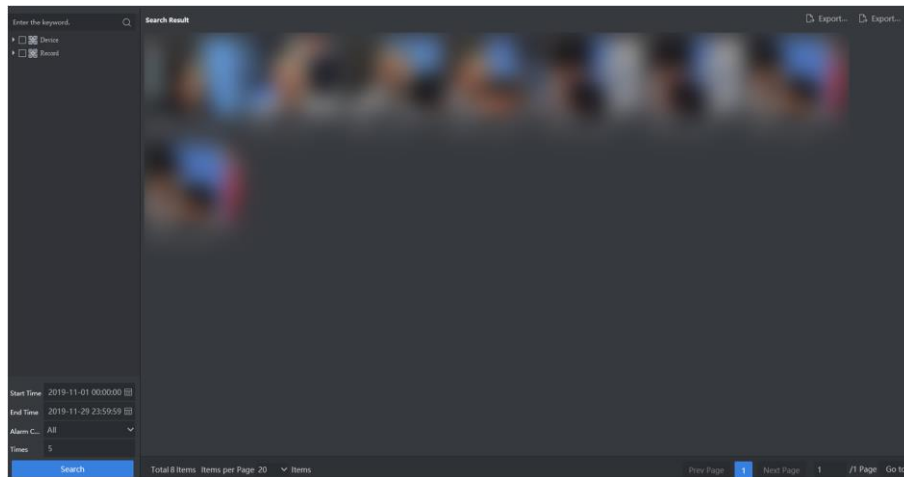


Figure 3-6 Frequently Appeared Person Alarm

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.

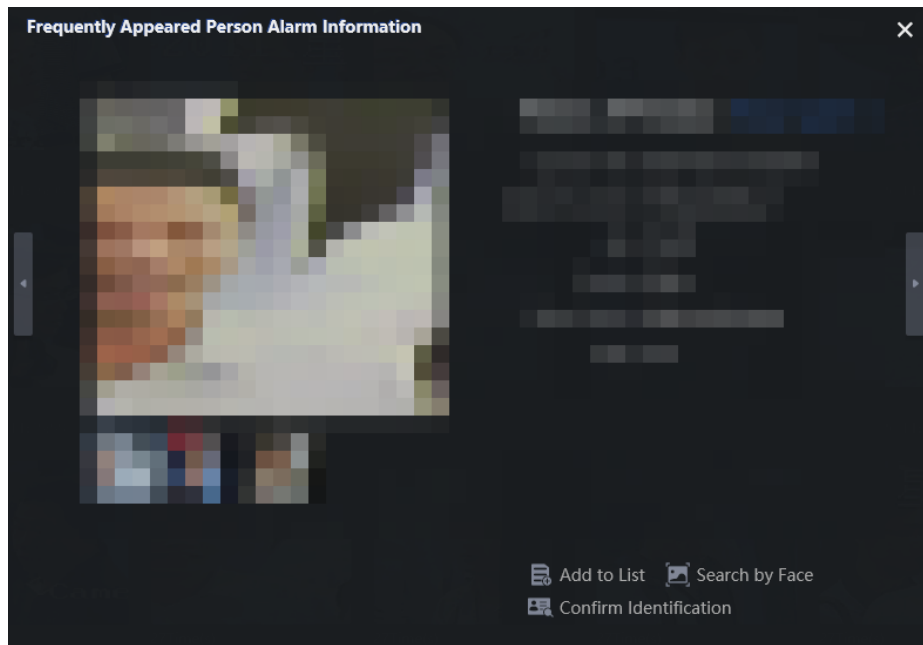


Figure 3-7 View Detailed Information-Frequently Appeared Person Alarm



Note

You can view all captured information of the target person by clicking **Capture History**.

6. Optional: Click **Export Current Page** or **Export All** to export alarm information.

3.2.4 Low Frequency Alarm

Count personnel appearance frequency in monitoring scenes. An alarm will be triggered if the frequency reaches the configured threshold during specific period.

Before You Start

Enable low frequency alarm.

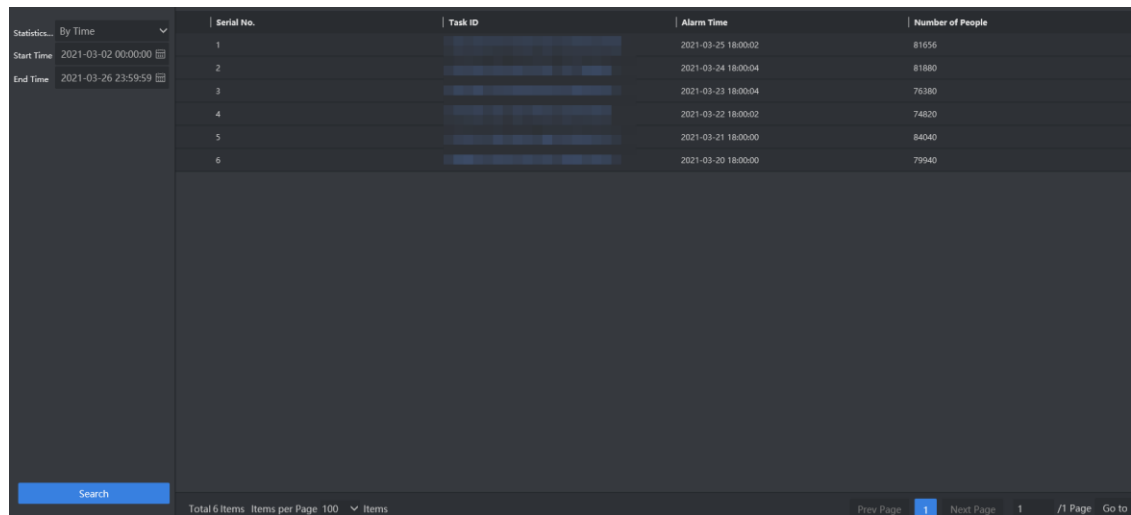
Steps

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



Note

Up to 100,000 items are supported.



The screenshot shows a web interface for the Edge Facial Recognition Server. On the left, there is a sidebar with a 'Statistics...' dropdown set to 'By Time'. Below it, 'Start Time' is set to '2021-03-02 00:00:00' and 'End Time' is set to '2021-03-26 23:59:59'. A 'Search' button is at the bottom of the sidebar. The main area displays a table with the following columns: 'Serial No.', 'Task ID', 'Alarm Time', and 'Number of People'. The table contains 6 rows of data. At the bottom of the main area, there is a pagination bar showing 'Total 6 Items', 'Items per Page: 100', and 'Page 1 / 1'.

Serial No.	Task ID	Alarm Time	Number of People
1		2021-03-25 18:00:02	81656
2		2021-03-24 18:00:04	81880
3		2021-03-23 18:00:04	76380
4		2021-03-22 18:00:02	74820
5		2021-03-21 18:00:00	84040
6		2021-03-20 18:00:00	79940

Figure 3-8 Low Frequency Alarm

2. Set search conditions according to actual needs, and click **Search**.
3. Click the desired task ID to view alarm information.

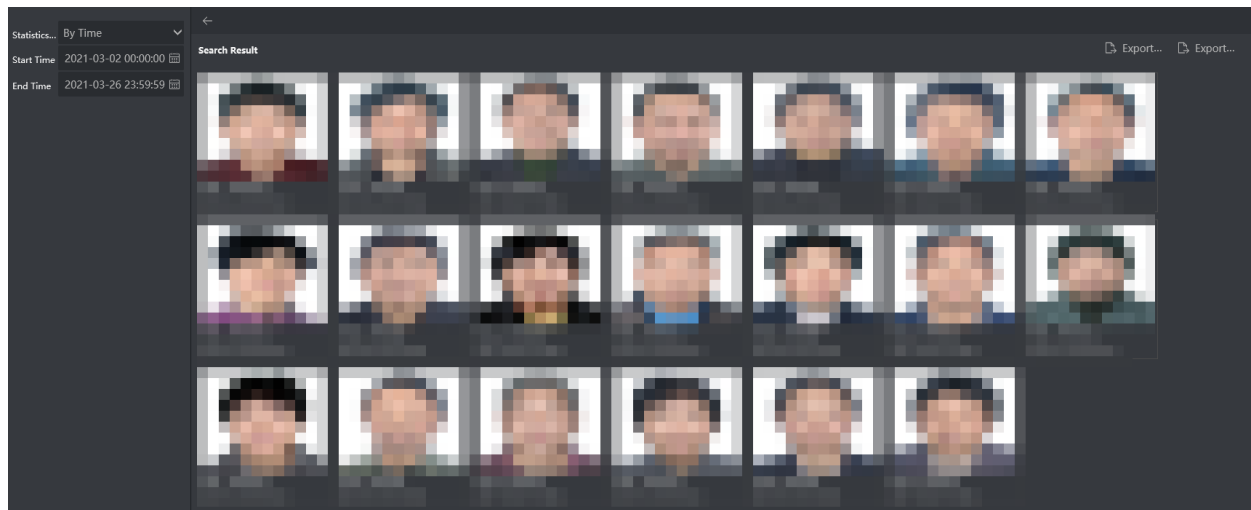


Figure 3-9 View Detailed Information-Frequently Appeared Person Alarm



Note

You can view all captured information of the target person by clicking **Capture History**.

6. Optional: Click alarm picture to view detailed information.

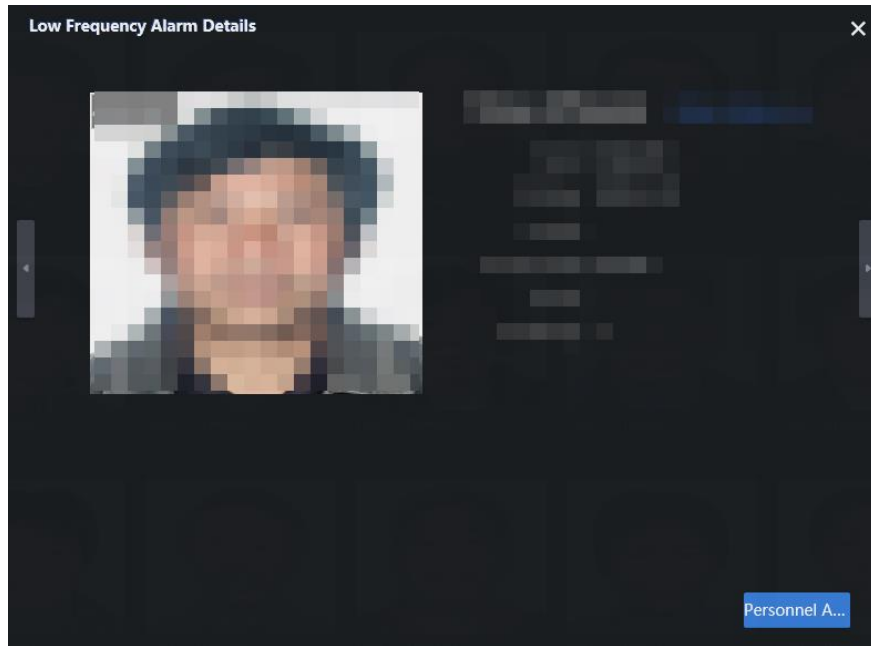


Figure 3-10 View Detailed Information-Low Frequency Alarm

7. Optional: Click **Personnel Archive** to check personnel information.
8. Optional: Click **Export Current Page** or **Export All** to export alarm information.

3.3 Personnel Archive

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

Before You Start

Enable personnel archive.

Steps

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

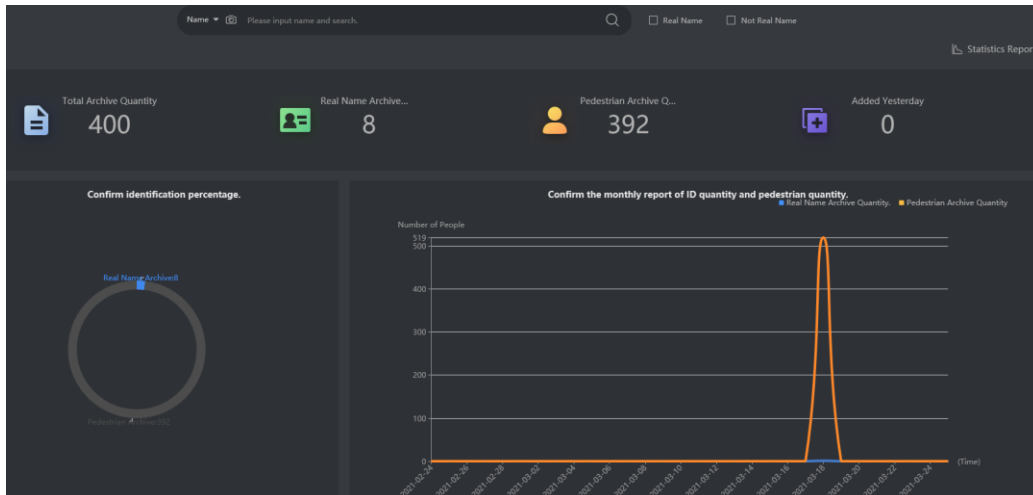


Figure 3-10 Personnel Archive

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

In accordance with gender, age or total personnel frequency in a period, the statistic report shows different figures of strangers and real name personnel recognized by cameras or in the videos. You can also export the statistic report to generate an Excel or HTML file.

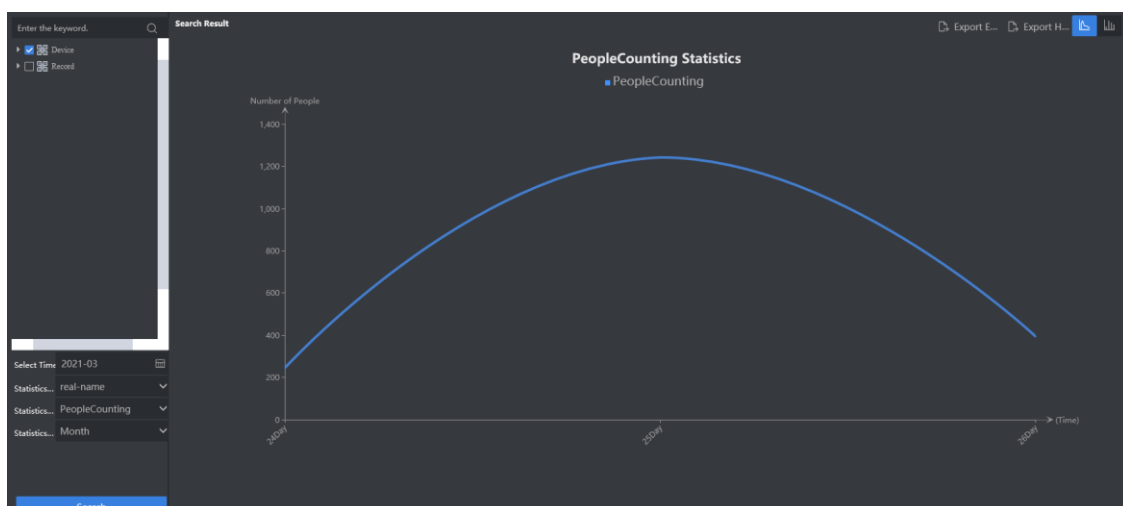


Figure 3-11 Statistic Report

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

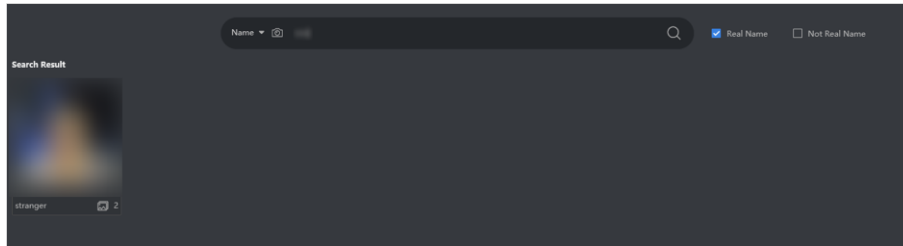



Figure 3-12 Personnel Archive Search Result

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**.

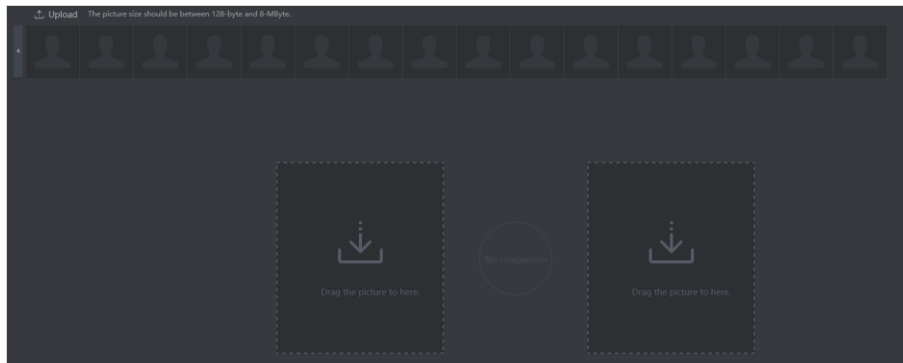


Figure 3-13 1 V 1 Comparison Interface

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.

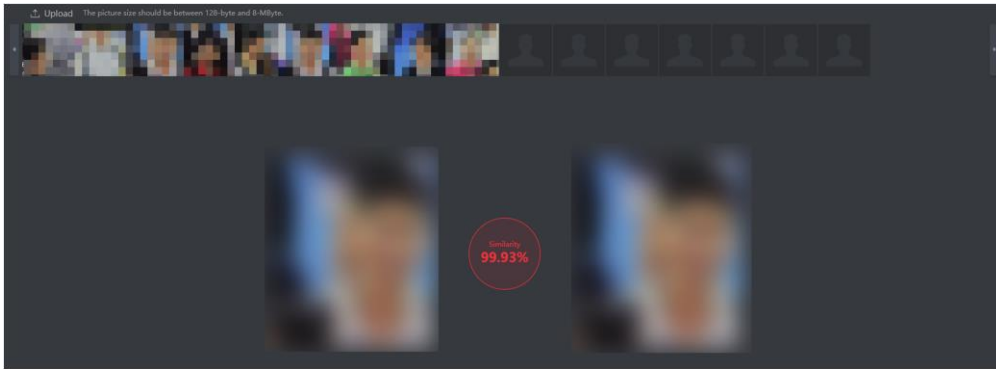


Figure 3-14 1 V 1 Comparison Result

Chapter 4 Smart Search

4.1 Search by Facial Attribute

Search captured face pictures by face attributes.

Before You Start

Alarm the camera.

Steps

1. Go to **Smart Search** → **Face Search** → **Search by Attribute**. By default, the server displays all captured face pictures.
2. Set detailed search conditions as needed.

Note

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

3. Click **Search**.

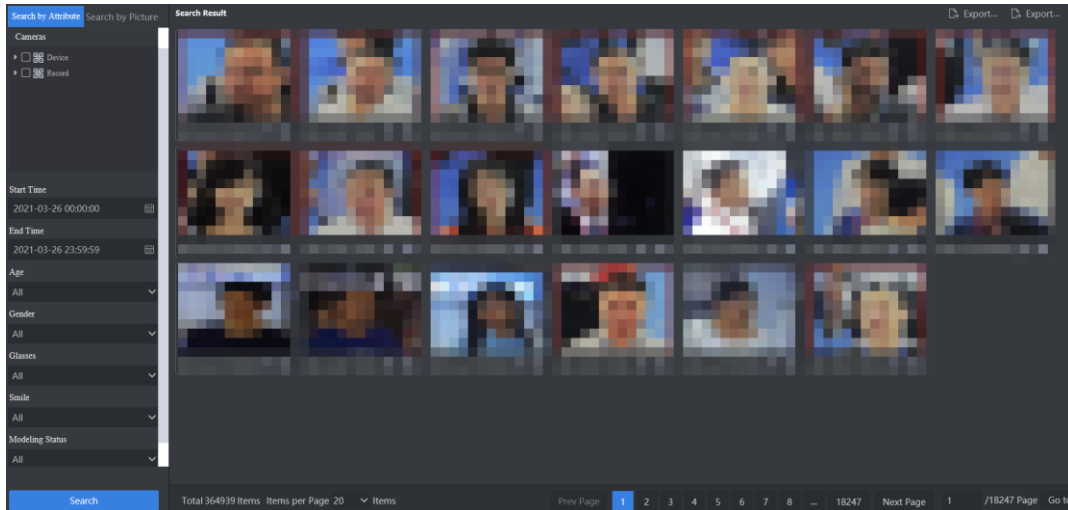





Figure 4-1 Search by Facial Feature Interface

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

Note

Click  to set this face picture as target picture to search picture by picture. Click  to set this face picture as target picture to confirm identification. Click  to add this face picture to list library.

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

4.2 Search by Face Picture

Upload a face picture to search similar pictures in capture library.

Before You Start

Alarm the camera.

Steps

1. Go to **Smart Search** → **Face Search** → **Search by Picture** → **Search by Face**.
 2. Click **Upload** to upload desired face pictures. The system will detect faces automatically.
-

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 smaller than 8 MB.
 - It is recommended to upload clear pictures of faces to improve the comparison accuracy.
-

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

Note

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

5. Click **Search**.

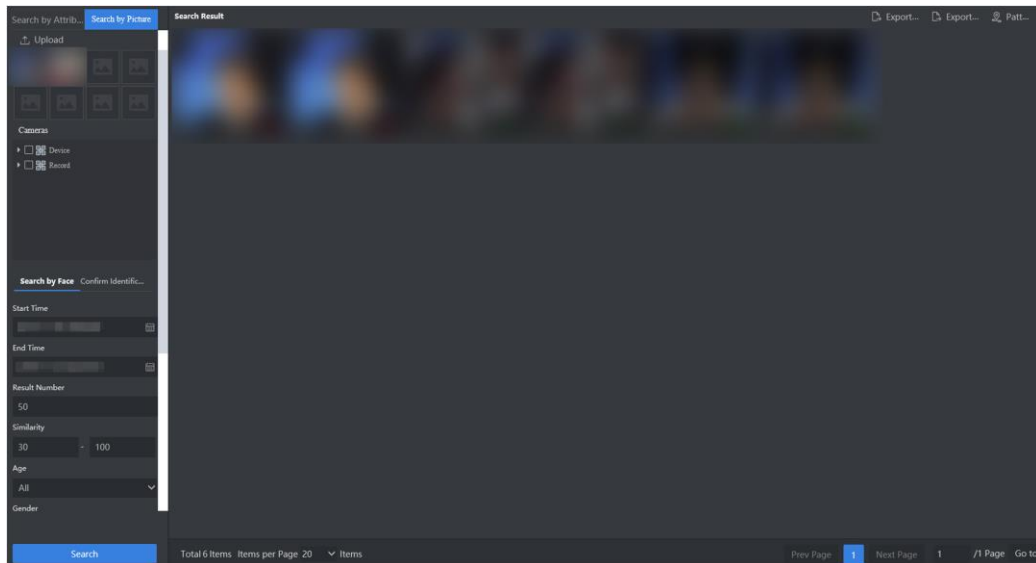





Figure 4-2 Search by Face Picture Results

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

Note

Click  to set this face picture as target picture to search picture by picture. Click  to set this face picture as target picture to confirm identification. Click  to add this face picture to list library.

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

4.3 Confirm Identification

Upload a face picture to search similar pictures in list library.

Before You Start

Add the list library.

Steps

1. Go to **Smart Search** → **Face Picture Search** → **Search by Picture** → **Confirm Identification**.
2. Click **Upload** to upload desired face pictures. The system will detect faces automatically.

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 16 MP, and the picture size should be smaller than 8 MB.
 - It is recommended to upload clear pictures of faces to improve the comparison accuracy.
-

3. Click the square frame above the face and then click **OK**.

4. Select the desired face picture and set detailed search conditions as needed.
-

Note

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

5. Click **Search**.

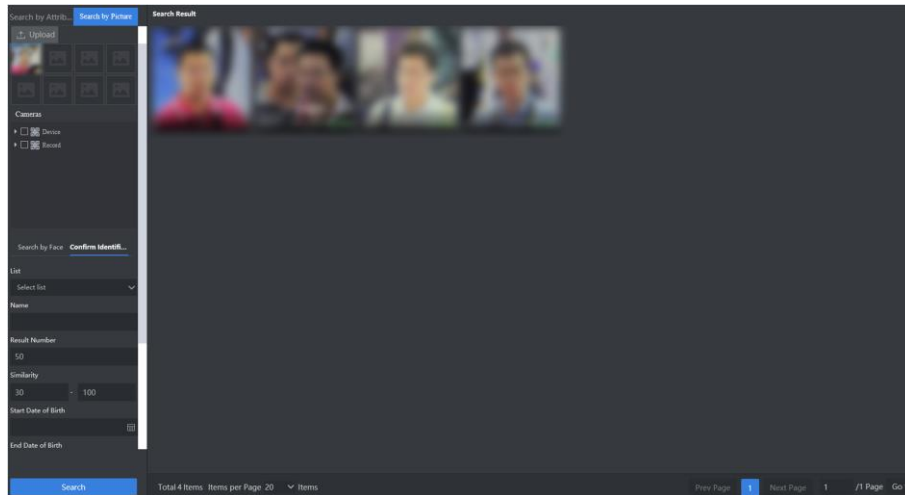




Figure 4-3 Confirm Identification Results

6. Click the face picture displayed to view detailed information.
-

Note

Click  to set this face picture as target picture to search picture by picture. Click  to set this face picture as target picture to confirm identification.

Chapter 5 System Management

5.1 Cluster Management

5.1.1 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.

5.1.2 Power off Node

Before You Start

The node is online.

Steps



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.

5.1.3 Disband Cluster

Steps

1. Go to **System Management** → **Cluster Management** → **Cluster Management**.
2. Select the node, and click **Disband Cluster**.

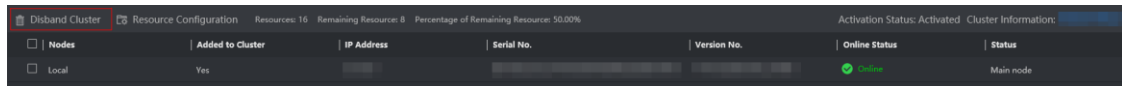


Figure 5-1 Disband Cluster

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.

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**.

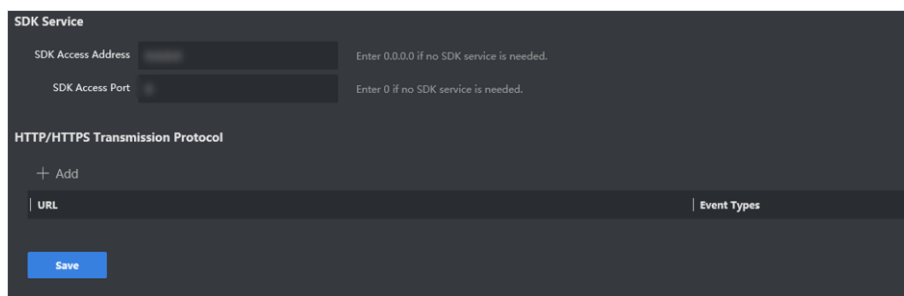


Figure 5-2 Service Configuration Interface

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 Cloud Storage

Keep the settings as the default value.

5.2.4 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**.

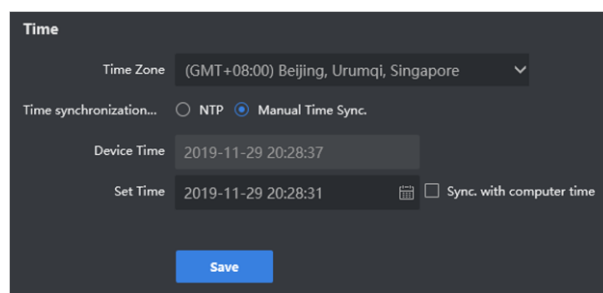


Figure 5-4 Time Configuration Interface

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. Click **Save**.

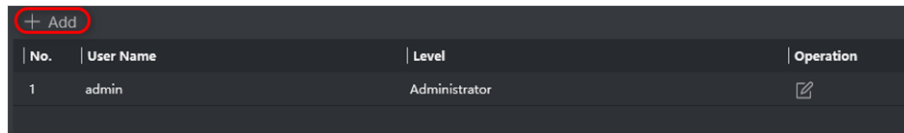
5.2.5 User Management

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

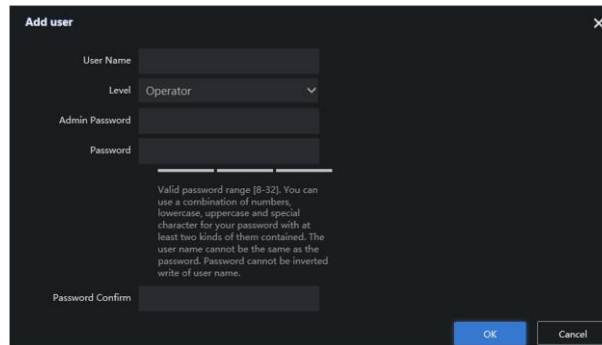
1. Go to **System Management** → **System Config** → **User**.



+ Add			
No.	User Name	Level	Operation
1	admin	Administrator	

Figure 5-5 User Management

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



Add user [X]

User Name

Level Operator [v]

Admin Password

Password

Valid password range [8-32]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained. The user name cannot be the same as the password. Password cannot be inverted write of user name.

Password Confirm

OK Cancel

Figure 5-6 Add User

Note

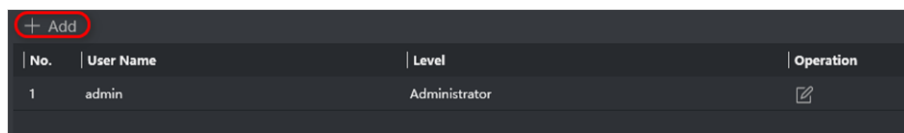
- We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product.
 - We recommend 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

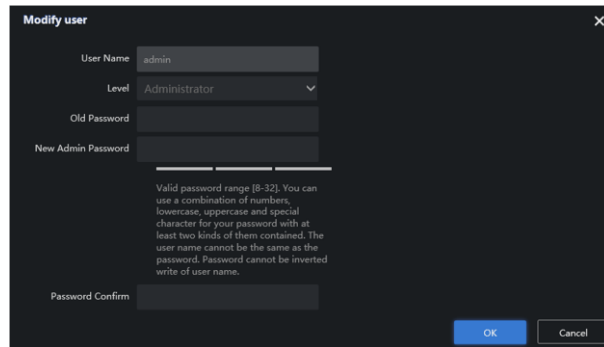
1. Go to **System Management** → **System Config** → **User**.



+ Add			
No.	User Name	Level	Operation
1	admin	Administrator	

Figure 5-7 User Management Interface

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



Modify user

User Name: admin

Level: Administrator

Old Password:

New Admin Password:

Valid password range [8-32]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained. The user name cannot be the same as the password. Password cannot be inverted write of user name.

Password Confirm:

OK Cancel

Figure 5-8 Modify User

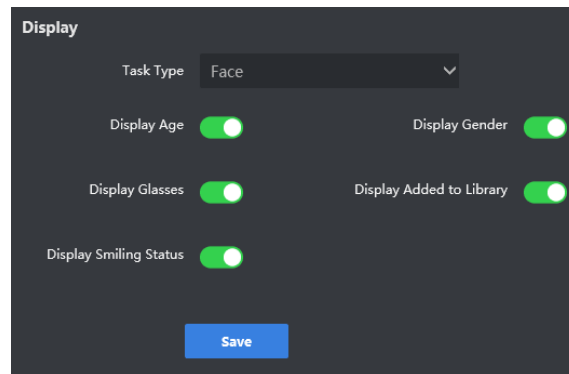
3. Click **OK**.

5.2.6 Configure Display Parameters

Configure the search conditions for smart search function. For example, if you do not enable **Display Gender**, there will be no gender option in search conditions.

Steps

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



Display

Task Type: Face

Display Age: ☒

Display Gender: ☒

Display Glasses: ☒

Display Added to Library: ☒

Display Smiling Status: ☒

Save

Figure 5-9 Display Configuration Interface

2. Set different search conditions according to actual needs.

3. Click **Save**.

5.2.7 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**.

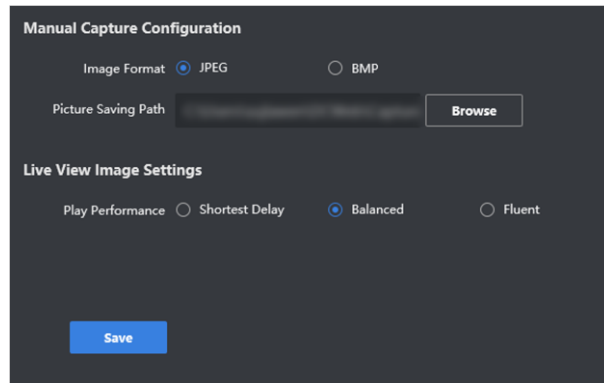


Figure 5-10 Live View Configuration Interface

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**.

5.2.8 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**.

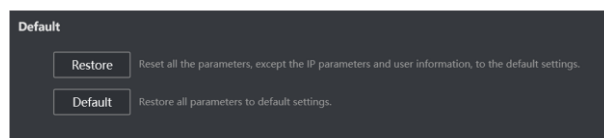


Figure 5-11 Restore Defaults Configuration Interface

2. Select restoration type according to actual demands.

5.2.9 Configure Data Upgrade

When your server is updated from the previous version V1.3 to V1.4, you need to upgrade the original data of the previous version.

Before You Start

Pause the ongoing analysis task(s).

Steps

1. Go to **System Management** → **System Config** → **Data Upgrade**.
2. Select a library type. If a capture library is selected, **Start Time** and **End Time** are required.
3. Click **Start**.

5.2.10 Configure Strategy Parameter

Configure parameters like similarity, captured picture score, and model fusion score, to promote the accuracy of personnel archive. Person strategy is enabled by default. It is recommended to keep the selection as the default status.

Steps


1. Go to **System Management** → **System Config** → **Strategy Parameter**.
2. Configure the desired parameters.
3. Click **Save**.

5.3 Operation and Maintenance

5.3.1 Check Hardware Status

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

Steps

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

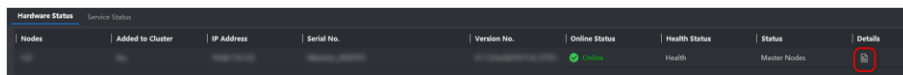


Figure 5-12 Hardware Status Interface

3. Click tabs to different hardware status.

5.3.2 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 Web 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.

5.3.3 Check Online User

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

5.3.4 Check Version Information

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

5.3.5 Check Help Document

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

5.3.6 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 Upgrade**.

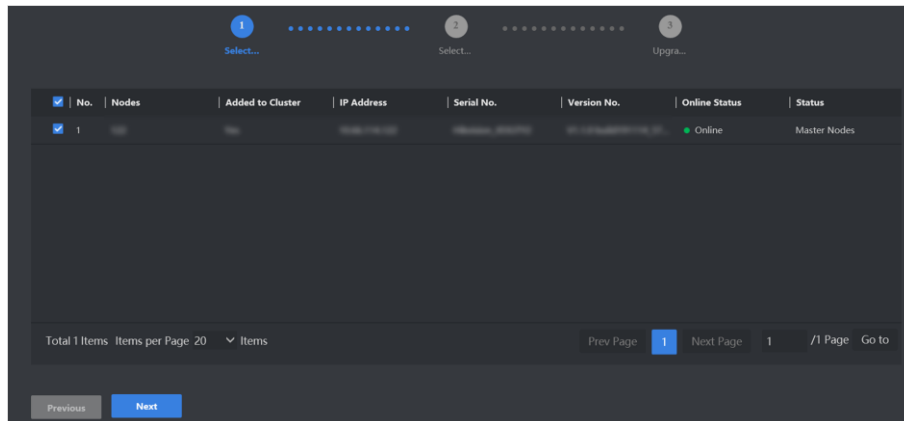


Figure 5-13 Software Updating Interface

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

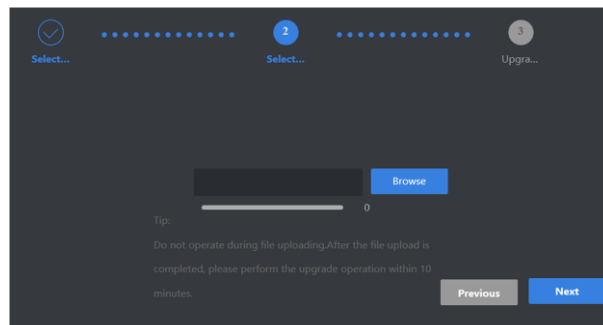


Figure 5-14 Select Uploading Files

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

4. Click **OK**.

Note

The device will reboot after updating completed.

5.4 Log Out

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



See Far, Go Further