Intelligent Fusion Server

User Manual

User Manual

About this Manual

This Manual is applicable to Intelligent Fusion Server.

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 in the company website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

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

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS 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 OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

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 when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

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

1. This device may not cause harmful interference.
2. 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, the 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: 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: www.recyclethis.info

Industry Canada ICES-003 Compliance

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

Applicable Models

This manual is applicable to the models listed in the following table.

Series	Model
Intelligent Fusion Server	DS-IX2002-A1U/X
	DS-IX2004-A1U/X

Symbol Conventions

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

Symbol	Description
NOTE	Provides additional information to emphasize or supplement important points of the main text.
WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or 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 VAC to 240 VAC or 12 VDC 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 rises from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

Preventive and Cautionary Tips

Before connecting and operating your device, please pay attention to the following tips:

- Ensure device is installed in a well-ventilated, dust-free environment.
- Device is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure device is properly secured to a rack or shelf. Major shocks or jolts to the device as a result of dropping it may cause damage to the sensitive electronics within the device.
- Use the device in conjunction with a UPS if possible.
- Power off the device before connecting and disconnecting accessories and peripherals.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

TABLE OF CONTENTS

Chapter 1 Introduction

1.1 Introduction

Intelligent fusion server, hereinafter referred to as the server, can alarm, compare, search and analyze captured human face pictures. The server provides efficient, convenient and professional solution for different application scenes like entrance and exit, checkpoints and ect, and it is widely applied for public security, transportation, judicature, finance, telecommunication and other areas.

1.2 Key Features

- Supports human face list management.
- Supports human face list library arming.
- Supports human face detection for different cameras.
- Supports rapid search for human face information in capture library.
- Supports real-time comparison, list alarm, stranger alarm and high frequency alarm.
- Supports 1V1 comparison.
- Supports settings for alarm popup and sound.
- Supports searching picture by picture.
- Supports user authorization management of admin, operator and consumer.
- Supports recording, searching and exporting operation log, running log and alarm log.
- Supports NTP time synchronization and manual time synchronization.
- Supports software updating.

1.3 PC Requirements

The requirements for your PC are shown below.

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

Chapter 2 Startup

2.1 Activate Device

2.1.1 Activate via SADP Software

Purpose:

SADP is a tool to search, activate, and modify the online devices within your subnet.

Before you start:

- Get the SADP software from the official website *http://overseas.hikvision.com/en/*, and install the SADP according to the prompts.
- The server and the PC that runs the SADP should be in the same subnet.

The following steps show how to activate the server and modify its IP address.

Step 1 Run the SADP software.

Step 2 Find and select your server.

Step 3 Input the same password in **New Password** and **Confirm Password** text fields.

NOTE

- We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including 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.

Step 4 Click **Activate** to start activation.

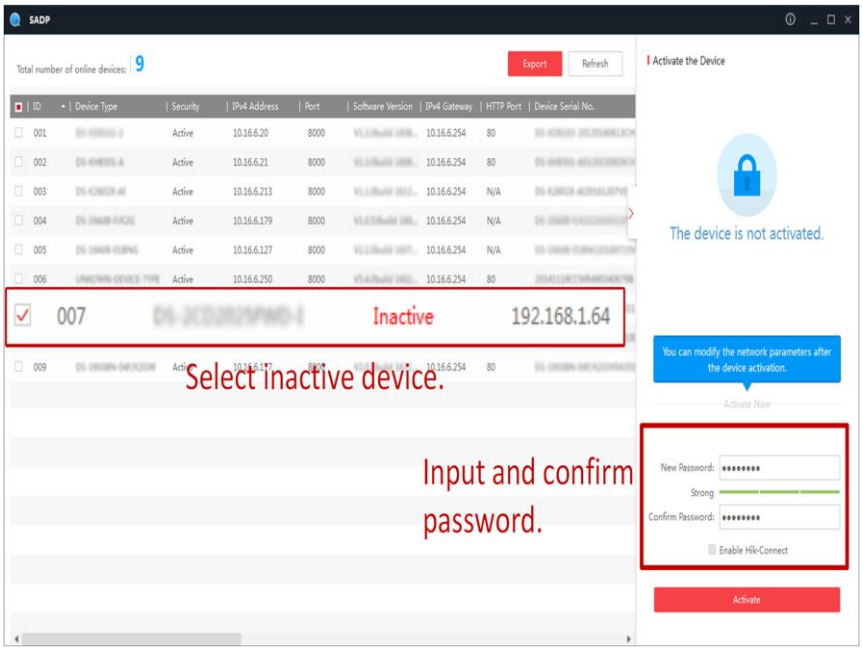

Figure 2-1 Activate via SADP Software

Step 5 Modify the IP address.

1) Select the activated server.
2) Input relevant parameters.
3) Input the admin password and click **Modify**.

2.1.2 Activate via Web Browser

The following steps show how to activate the server via web browser.

Step 1 Double-click the IE browser

Step 2 Input the default IP address (192.168.1.64) of the server into the address bar.

Step 3 Press **Enter** to enter the activation interface.

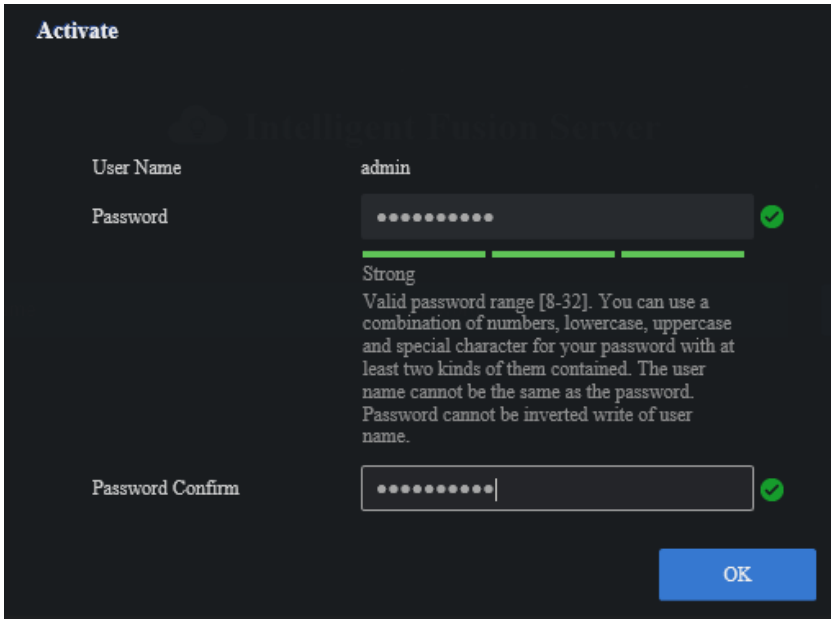

Figure 2-2 Activation Interface

Step 4 Input the same password in **Password** and **Password Confirm**.

Step 5 Click **OK** to complete the activation.

NOTE

After activation, the password of root user will be changed, and the password of admin is the same with that of root user.

2.2 Login

Purpose:

You can get access to the server with 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.

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

Figure 2-3 Login Interface

Step 2 Input the **User Name** and **Password**.

Step 3 Click **Login**.

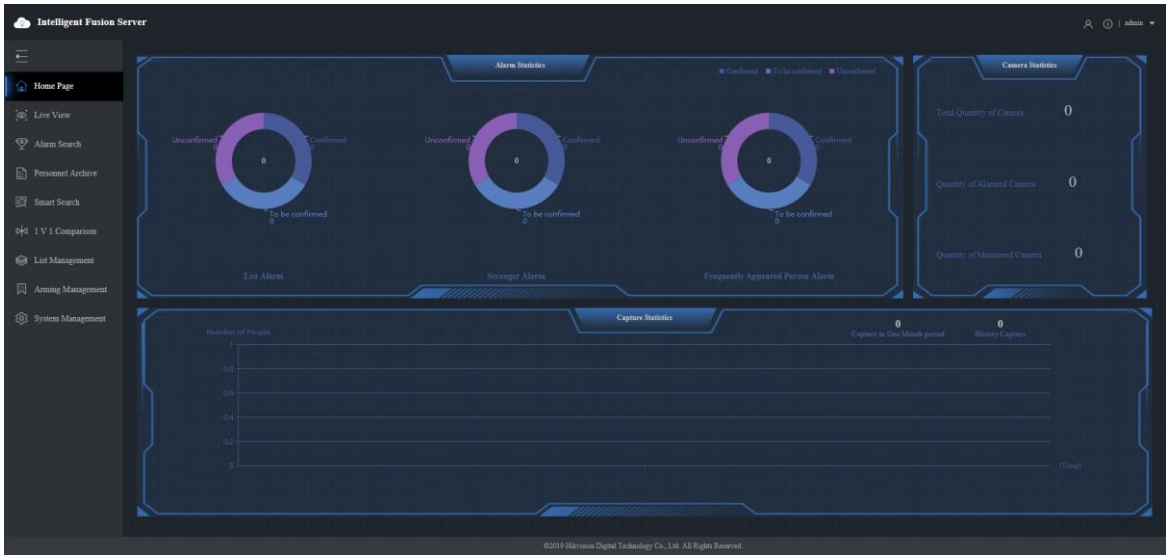

Figure 2-4 Home Page

NOTE

- After logging in via admin account, you enter the home page interface by default. You can check alarm statistics, camera statistics, and capture statistics information
- For the specific server interface, please refer to the actual one you run.

Chapter 3 Main Configuration

3.1 Modify Node IP

You can modify IP via SADP software or logging in the node operating system. Here we take logging in operating system as an example.

Step 1 Log in the node operating system via ssh tool or other way. The user name is root, and the password is the one that you set when activating the server.

Step 2 Input **ifconfig** and press **Enter** to check the network interface card.

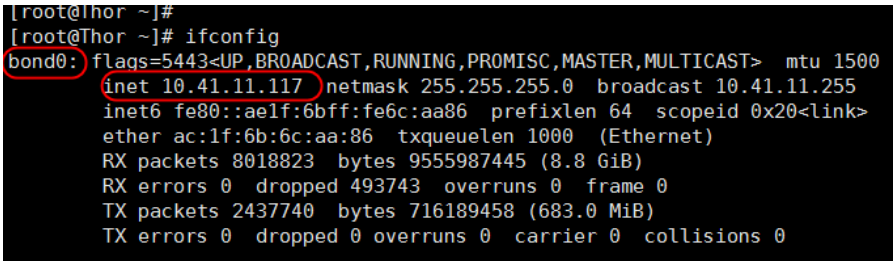

Figure 3-1 Check Network Interface Card

Step 3 Input **cd /etc/sysconfig/network-scripts** and press **Enter** to enter the configuration file catalog of network interface card.

Step 4 Input **ls** and press **Enter** to check the configuration file of network interface card.

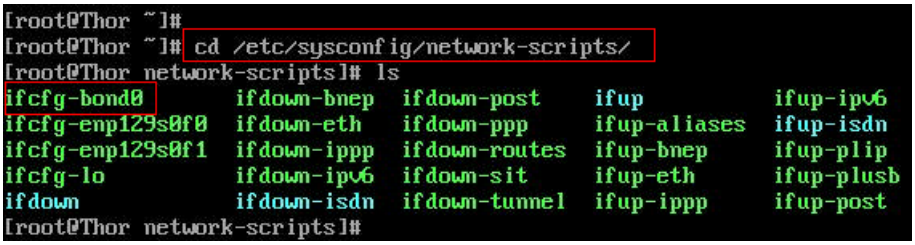

Figure 3-2 Check Configuration File

NOTE

For the name of network interface card configuration file, please refer to the actual one you run.

Step 5 Input **vi ifcfg-bond0**, press **Enter**, and then press **I** to enter editing mode. You need to set network parameters according to actual demands.

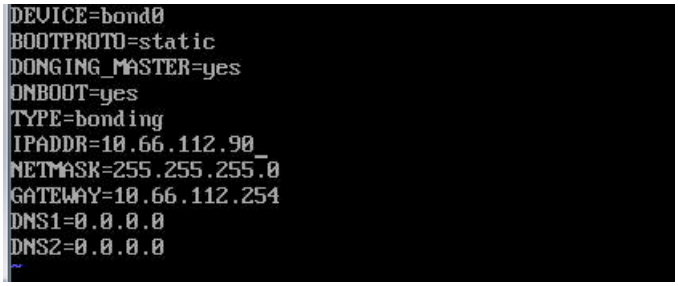

Figure 3-3 Edit Network Parameters

Step 6 Press **ESC** to exit editing mode. Input **:wq** and press **Enter** to save and exit configuration file.

Step 7 Input **service network restart** press **Enter** to restart network service.

Figure 3-4 Restart Network Service

Step 8 (Optional) Input **ifconfig** and press **Enter** to check the edited network parameters.

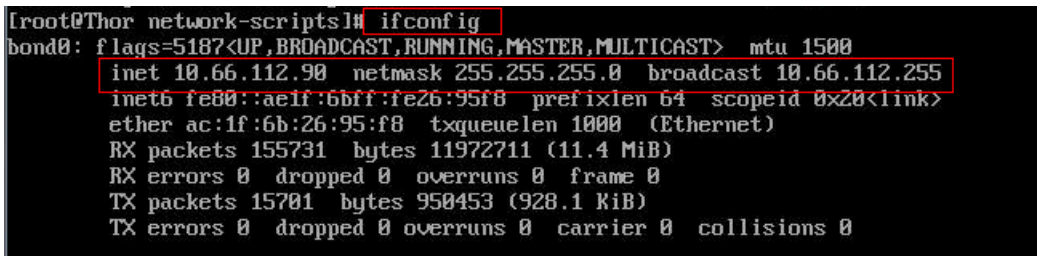

Figure 3-5 Check Network Parameters

3.2 Deploy Micro Video Cloud

Micro video cloud is used to store human face picture and video.

3.2.1 Install Micro Video Cloud

You need to login operating system to install micro video cloud.

Before you start:

Install ssh tool, such as Xshell.

NOTE

Here we take Xshell tool as an example to login node.

Step 1 Open Xshell tool, input **ssh 10.41.11.117 2343** and press **Enter**.

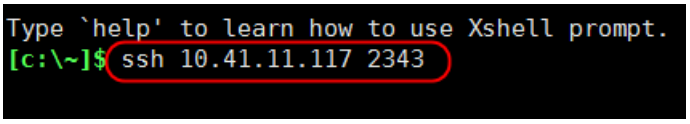

Figure 3-6 Set up ssh Connection

Step 2 Input **root** as user name and password.

Step 3 Input **cd /yunstorage** and press **Enter** to enter installation script catalog.

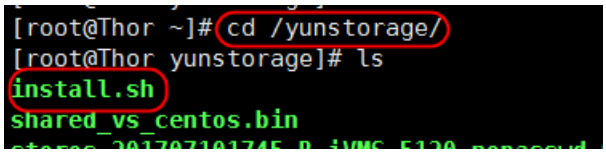

Figure 3-7 Basic Settings Interface

Step 4 Input **./install.sh** and press **Enter** to install script.

Figure 3-8 Install Script

3.2.2 Import License

- Apply License

Step 1 Input ***https://10.41.11.117:5120*** in IE browser and press **Enter** to enter HikCStor Management System.

Step 2 When logging in for the first time, set the same password in **Login Password** and **Confirm Password**, and click **Create**.

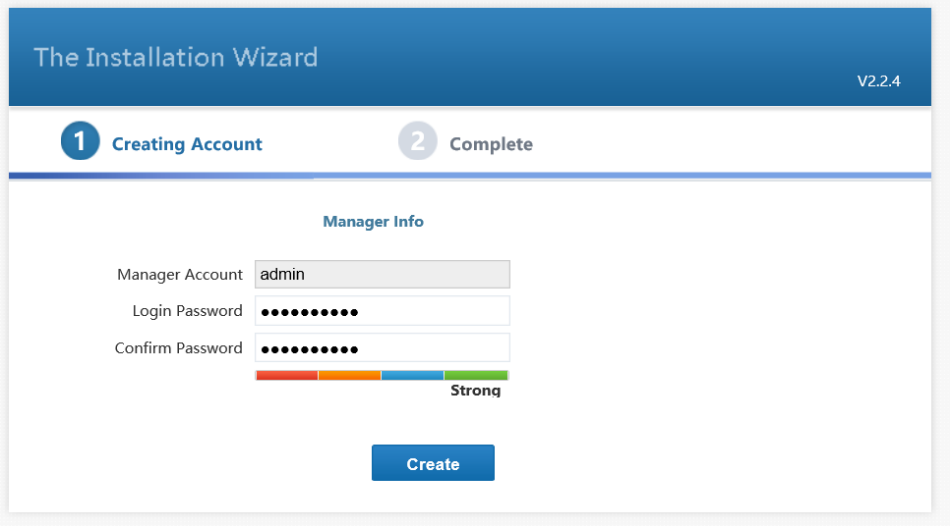

Figure 3-9 Create Account

Step 3 Input the **User Name** and **Password**, and click **Login**.

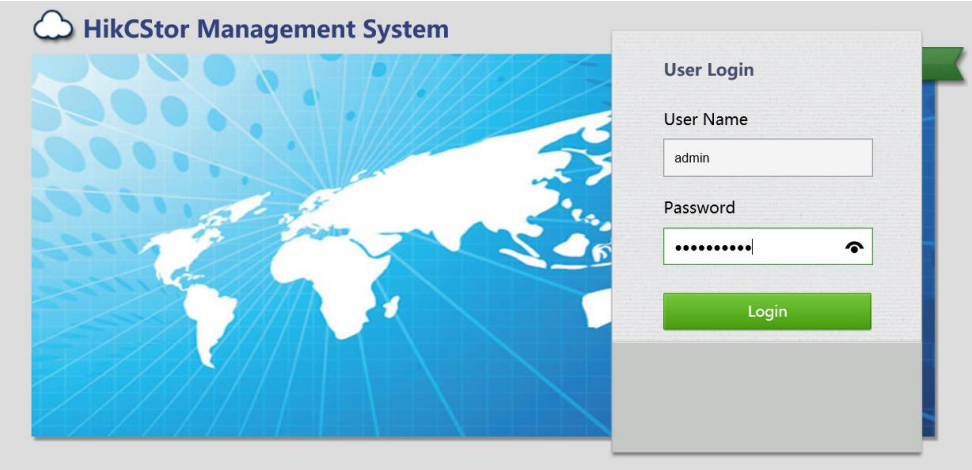

Figure 3-10 Login Interface

Step 4 Click **Apply License**.

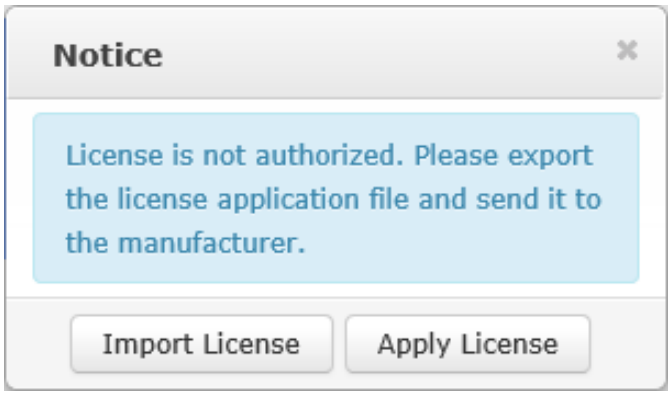

Figure 3-11 Click Apply License

Step 5 Input relevant application information, and click **Export Application**.

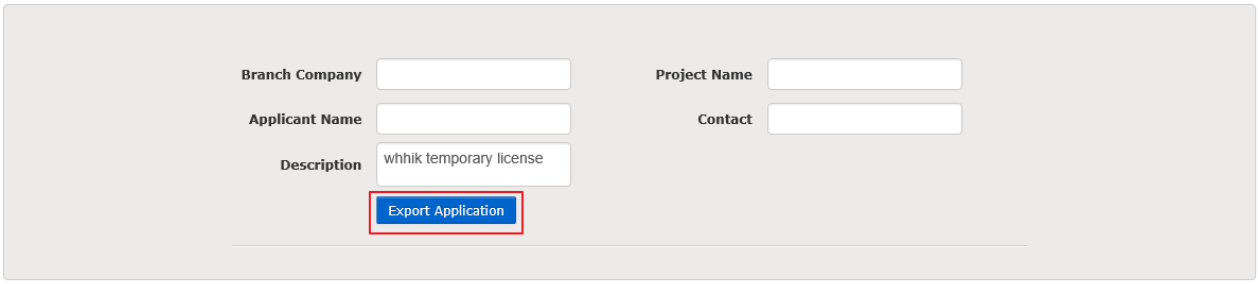

Figure 3-12 Click Export Application

NOTE

Project name refers to project number or JKN number.

Step 6 You need to send exported license, storage node number, hard disk number and total capacity of hard disk and micro video cloud version information to chenshengli@hikvision.com.cn or zhangle1@hikvision.com.cn via email for applying license file.

- Import License

Step 1 Go to the home page of HikCStor Management System.

Step 2 Click **Import License**.

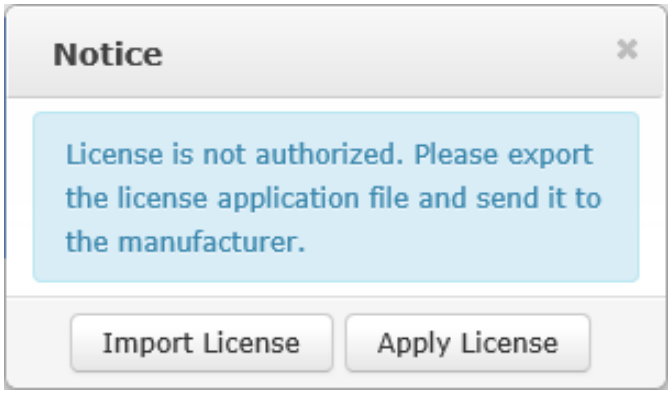

Figure 3-13 Click Import License

Step 3 Click **Import License File**, click **Choose File** in the popup dialogue box to select license file, and click **OK** to complete.

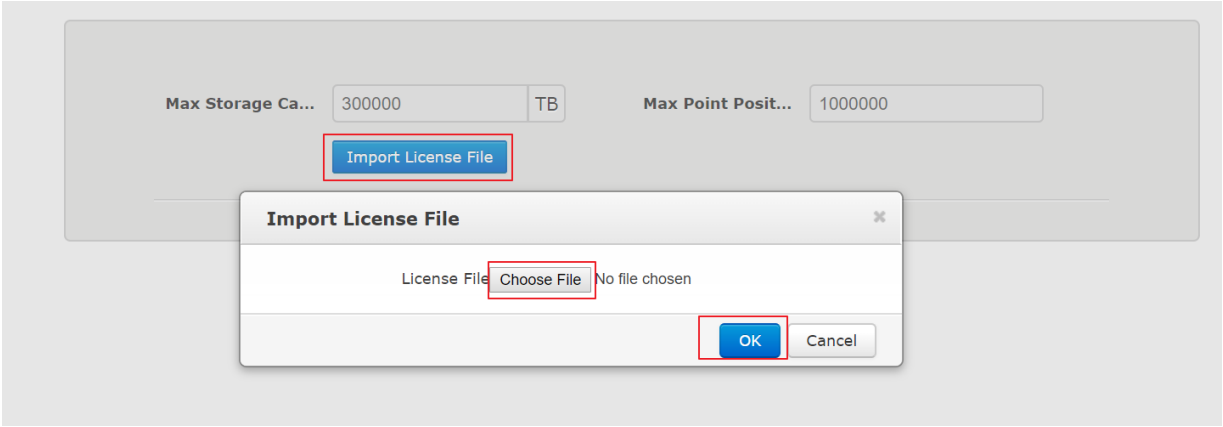

Figure 3-14 Choose File

3.2.3 Format Storage Volume

Step 1 Input ***https://10.41.11.117:5119*** in IE browser and press **Enter** to enter Storage Node Management System.

Step 2 When logging in for the first time, set the same password in **Login Password** and **Confirm Password**, and click **Create**.

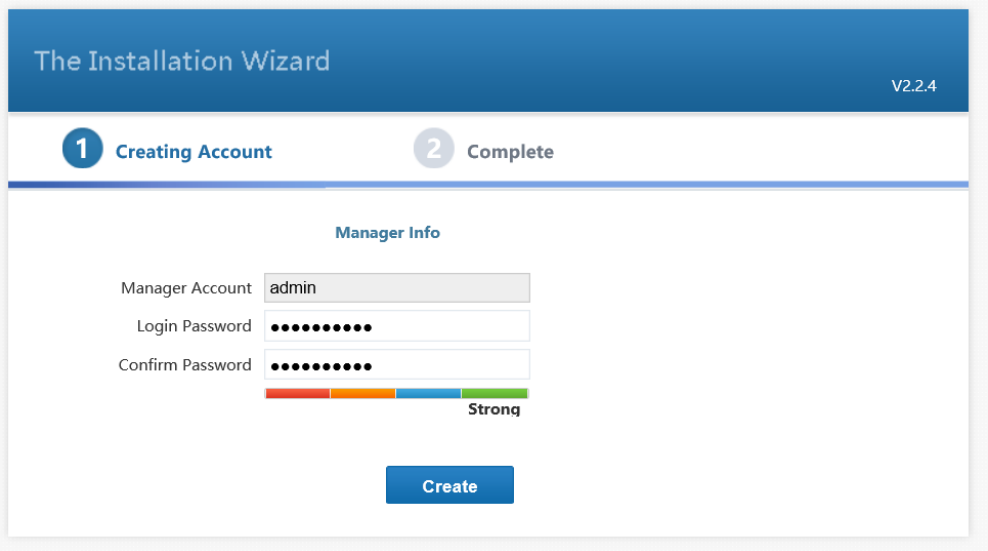

Figure 3-15 Create Account

Step 3 Input the **User Name** and **Password**, and click **Login**.

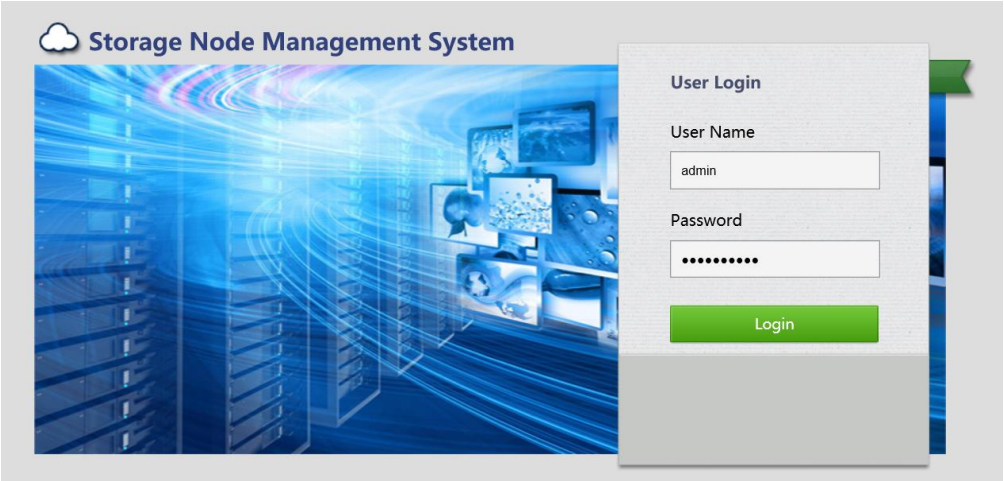

Figure 3-16 Login Interface

Step 4 Go to **Device > Storage Volume**, select storage volume, and click **Format Storage Volume**.

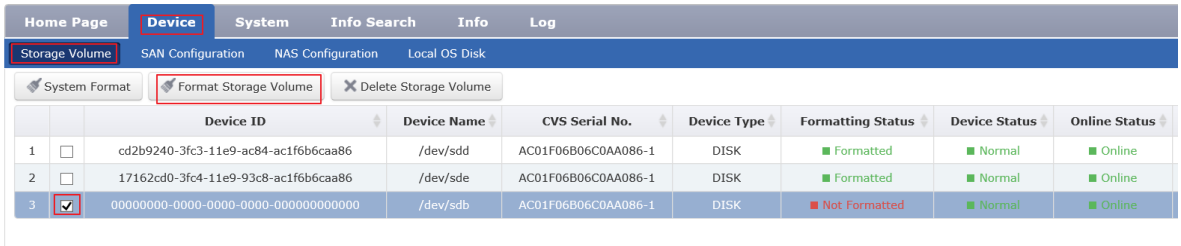

Figure 3-17 Select Storage Volume

Step 5 Select **Force** as **Format**, keep other parameters as default values, and click **OK**.

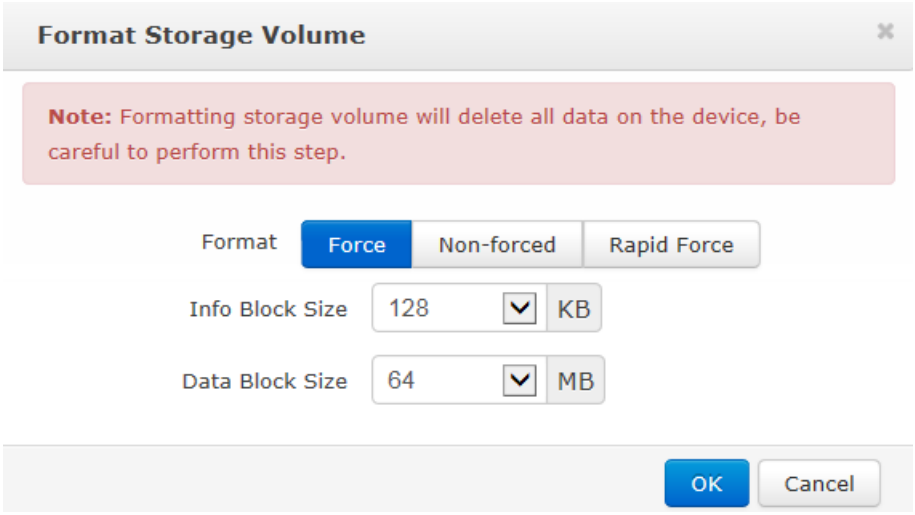

Figure 3-18 Format Storage Volume

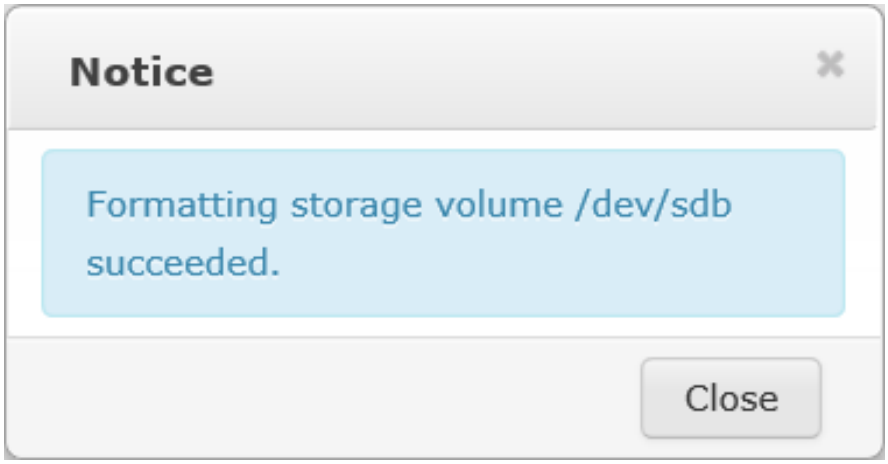

Figure 3-19 Formatting Completed

NOTE

If there are multi storage volumes to be formatted, please repeat the same steps as shown above.

3.2.4 Create Micro Video Cloud Cluster

1 to 2 nodes can be created as standalone micro video cloud and 3 to 8 nodes can be created as cluster micro video cloud.

NOTE

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

- **Create Standalone Micro Video Cloud**

Step 1 Click **Cluster Deployment**.

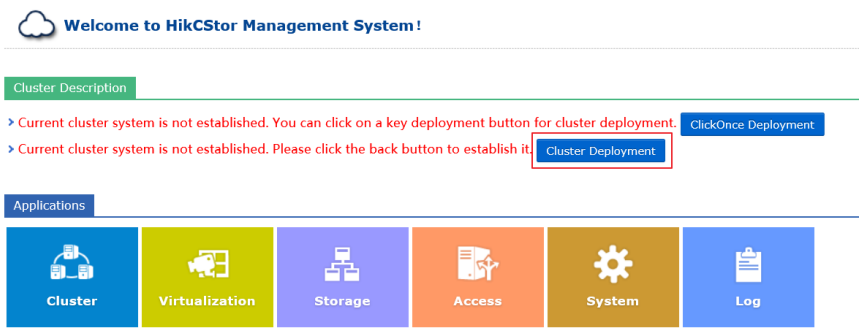

Figure 3-20 Click Cluster Deployment

Step 2 Select **Standalone**.

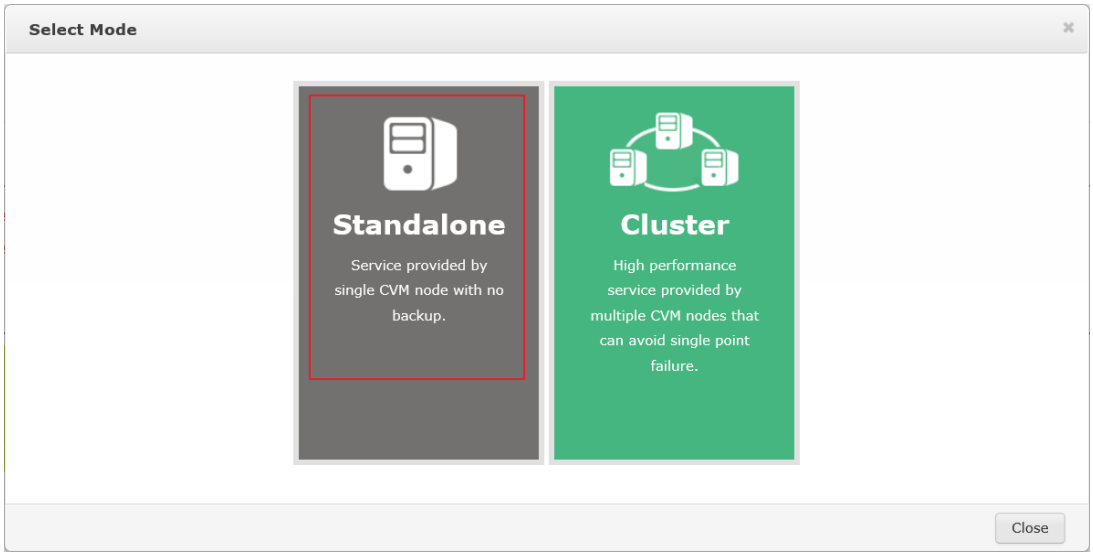

Figure 3-21 Select Standalone

Step 3 Input ID (here we take light-cloud as an example) in **Cloud ID**, click **Synchronization** to synchronize time, and click **Establish Cluster** to complete.

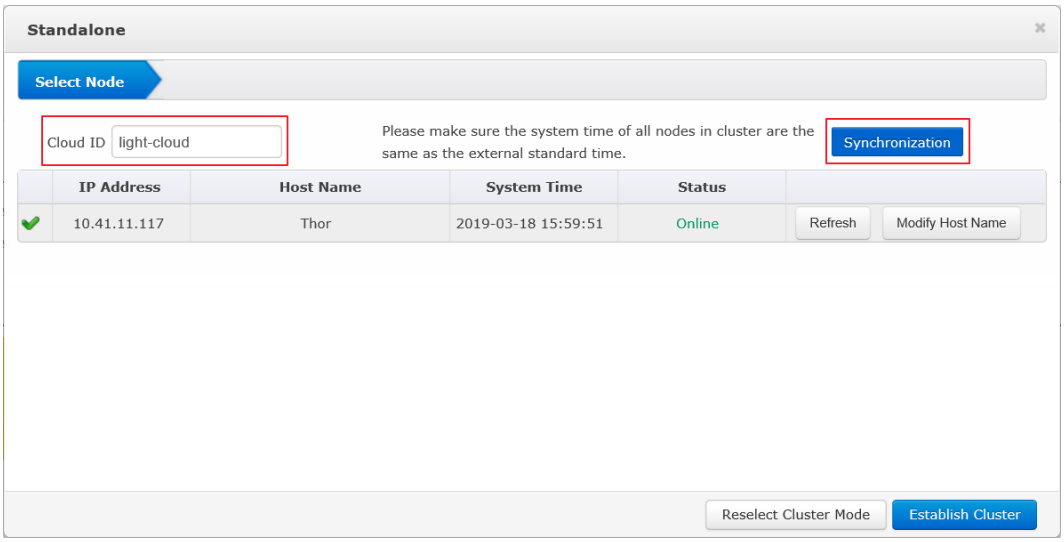

Figure 3-22 Click Establish Cluster

Step 4 After creating cluster, you can check created cluster in the list, as shown below.

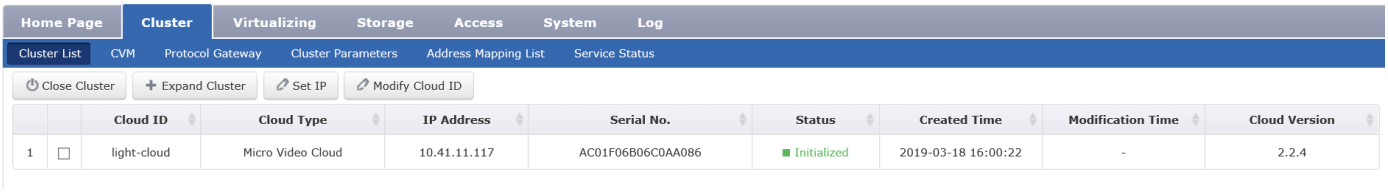

Figure 3-23 Cluster List

- **Create Cluster Micro Video Cloud**

Step 1 Input ***https://10.41.11.117:5120*** in IE browser and press **Enter** to enter HikCStor Management System.

Step 2 When logging in for the first time, set the same password in **Login Password** and **Confirm Password**, and click **Create**.

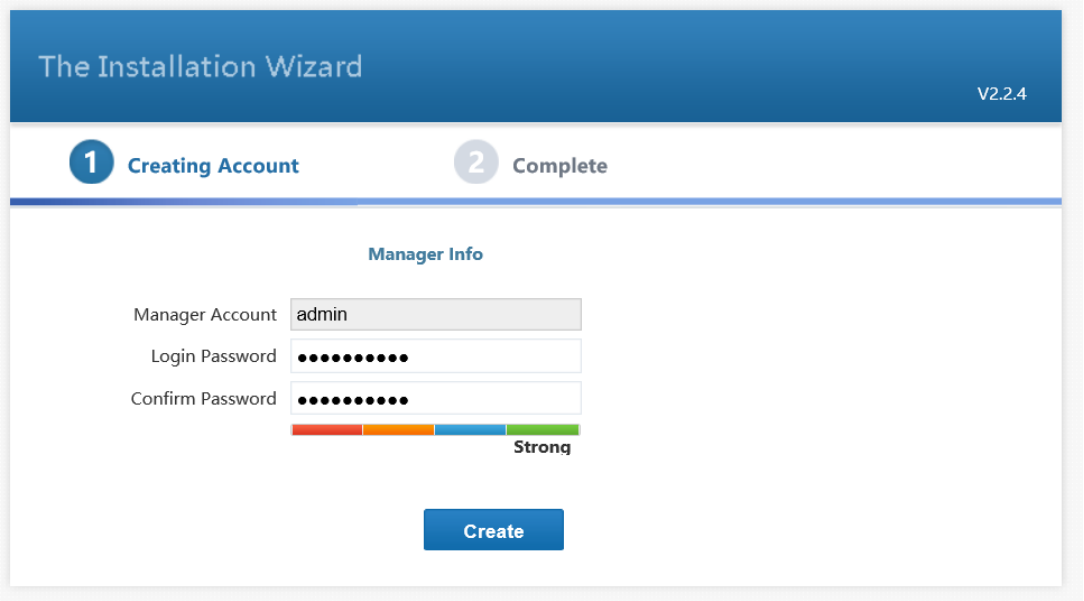

Figure 3-24 Create Account

Step 3 Input the **User Name** and **Password**, and click **Login**.

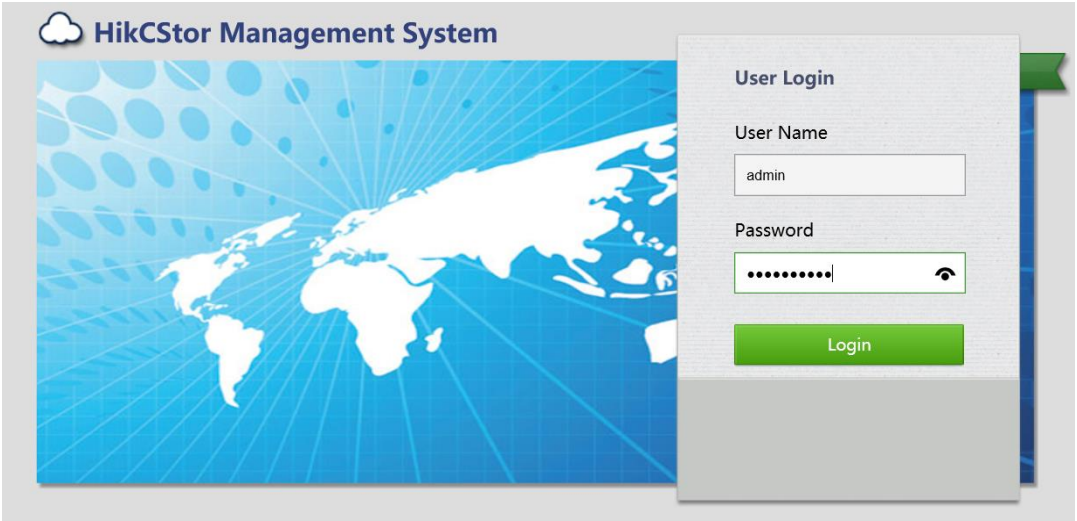

Figure 3-25 Login Interface

Step 4 Click **Cluster Deployment**.

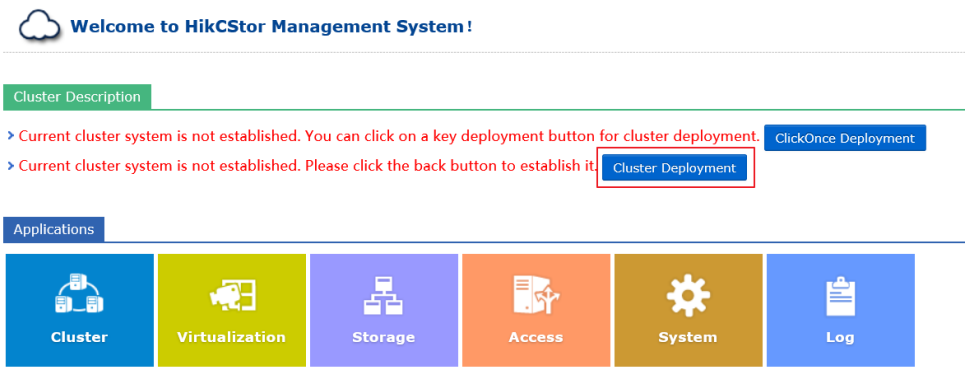

Figure 3-26 Click Cluster Deployment

Step 5 Select **Cluster**.

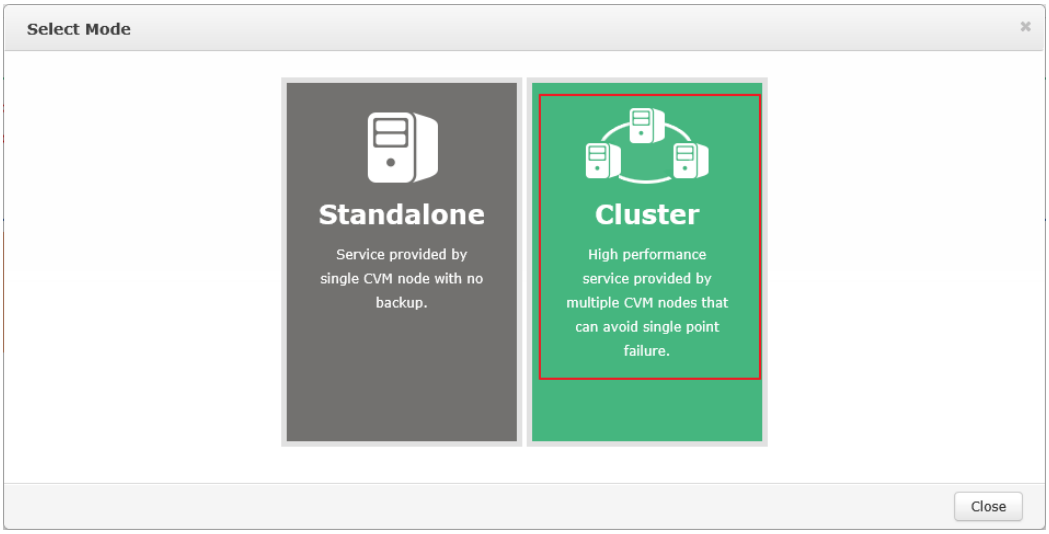

Figure 3-27 Select Cluster

Step 6 Input the IP address of storage nodes, and click **Add** to add storage nodes.

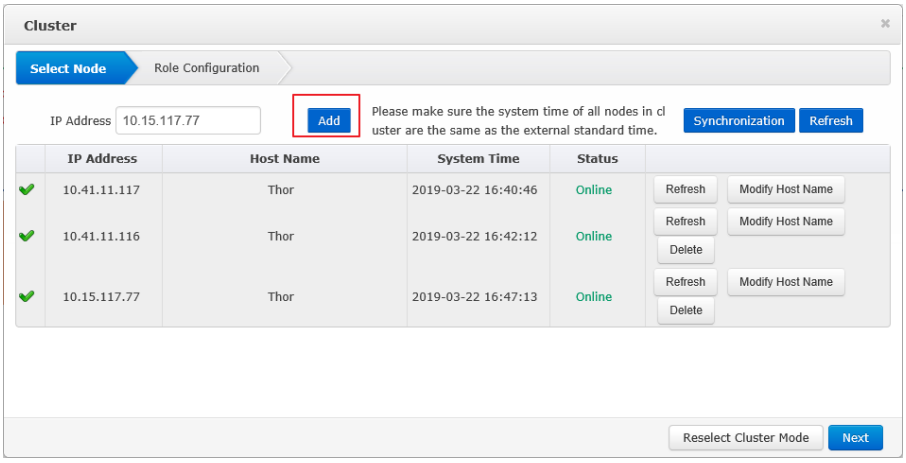

Figure 3-28 Add Storage Nodes

Step 7 Click **Modify Host Name** to modify the host name of different nodes.

Step 8 Click **Synchronization** to synchronize time, and then click **Next**.

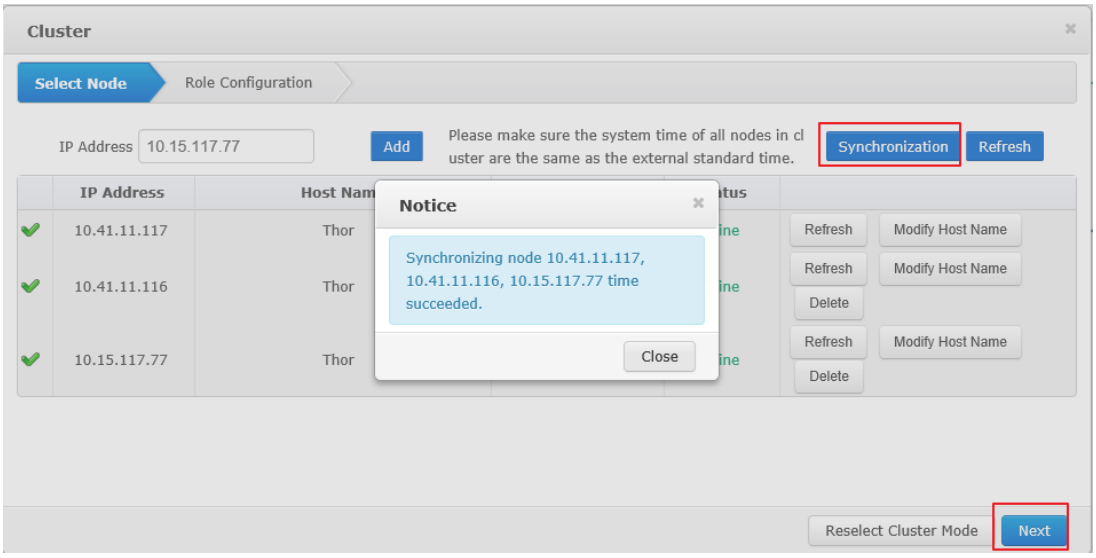

Figure 3-29 Synchronize Time

Step 9 Input an idle IP address of same subnet in **Virtual IP Address**, and click **Detect**.

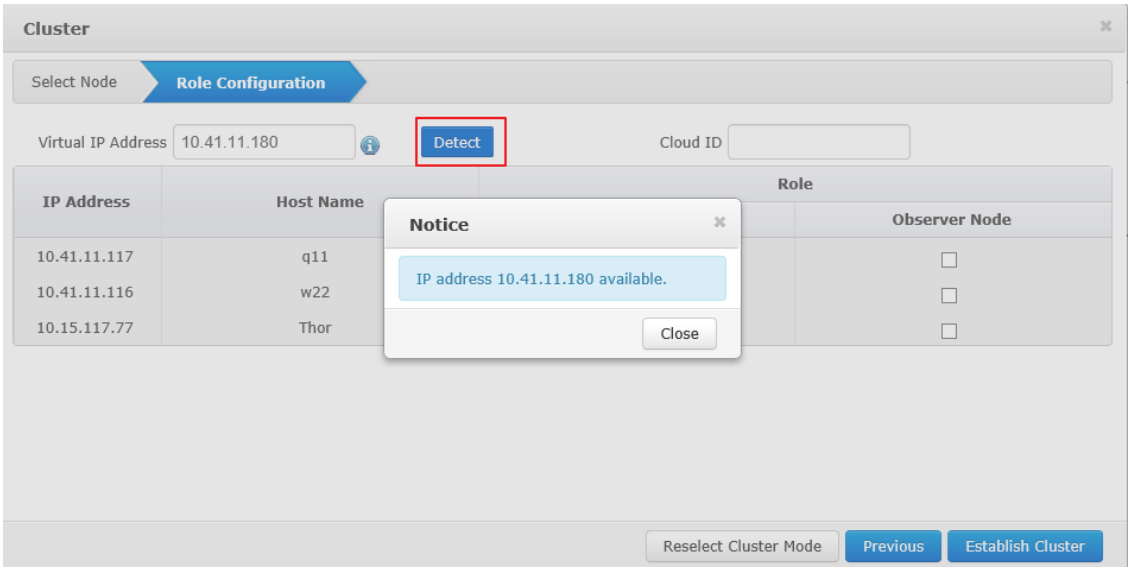

Figure 3-30 Detect Virtual IP

Step 10 Input ID (here we take light-cloud as an example) in **Cloud ID**, click **Establish Cluster**. After creating cluster, you can check created cluster in the list.

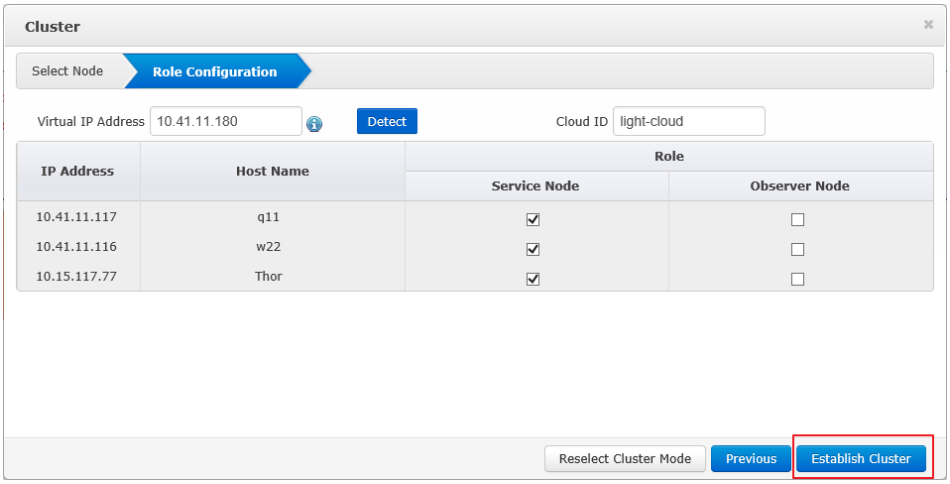

Figure 3-31 Create Cluster

3.2.5 Set Storage Parameters

NOTE

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

Step 1 Input ***https://10.41.11.117:5119*** in IE browser and press **Enter** to enter Storage Node Management System.

Step 2 Go to **System** > **Storage Configuration**.

Step 3 Input the virtual IP of cluster micro video cloud in **CVM IP** (for standalone micro video cloud, input node IP).

Step 4 Input the value that you have set when creating micro video cloud. Here we take light-cloud as an example.

Step 5 Select **Memory Accelerate** as **Accelerate Type** if the node memory is 128 GB, and select **SSD Accelerate** as **Accelerate Type** if the node memory is 256 GB.

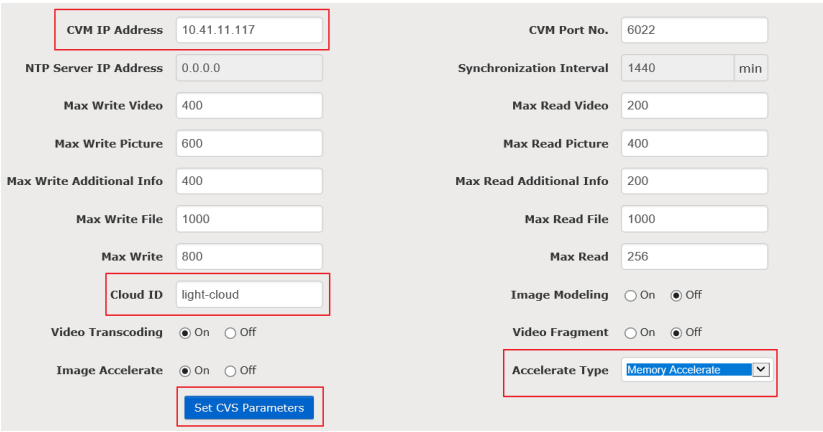

Figure 3-32 Set Storage Parameters

NOTE

You can check node memory by inputting **free –g** in node operating system.

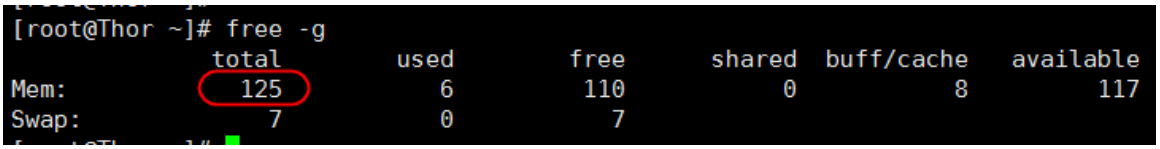

Figure 3-33 Node Memory

Step 6 After setting parameters, click **Set CVS Parameters** to complete.

3.2.6 Add Domain to Storage Node

Step 1 Log in the HikCStor Management System.

Step 2 Go to **Virtualizing** > **Domain Management**, and click **Create**.

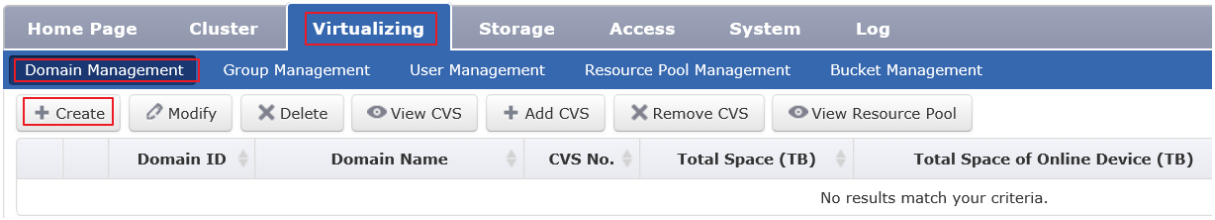

Figure 3-34 Create Domain

Step 3 Input **Domain Name** and click **OK**.

Step 4 Check created domain, and click **Add CVS**.

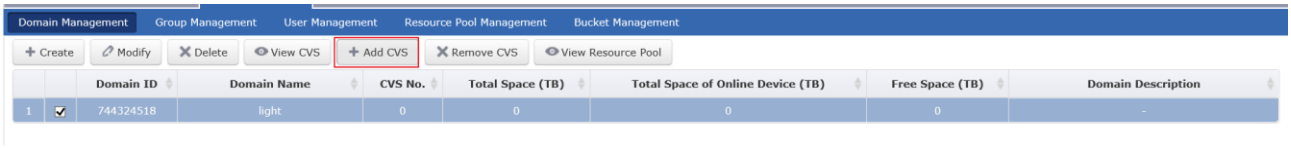

Figure 3-35 Check Created Domain

Step 5 Check storage node and click **OK**.

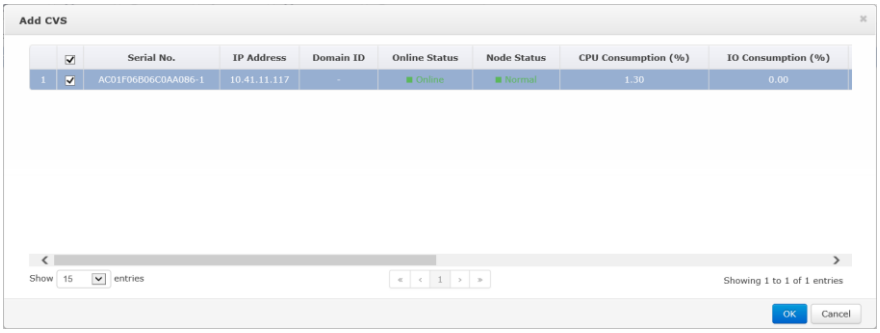

Figure 3-36 Add CVS

3.2.7 Create Static Pool

NOTE

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

Purpose:

Static pool is used to storage human face picture of list library.

Step 1 Go to **Virtualizing** > **Resource Pool Management**.

Step 2 Click **Create**, and set parameters in the popup dialog box, as shown below.

Table 3-1 Parameter Setting

Parameter Name	Description
Domain ID	Select the domain that you created.
User Name	Select admin.
User Permission	Select read/ write.
Resource Pool Name	Input staticpool.
Resource Pool Type	Select picture.
Accelerate Picture	Select accelerate.
Storage Mode	Select dispersed.
Overwrite Mode	Select not.
Resource Pool Capacity	Input 300.
Max. Locking up Attempts	Input 10.

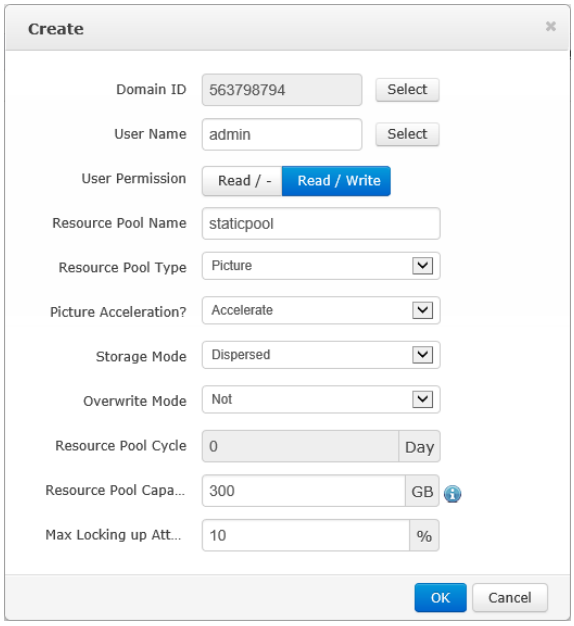

Figure 3-37 Create Static Pool

NOTE

When adding smart storage unit, you will need the ID of static resource pool.

3.2.8 Create Video Pool

Purpose:

Video pool is used to storage video files that are manually uploaded.

Step 1 Go to **Virtualizing** > **Resource Pool Management**.

Step 2 Click **Create**, and set parameters of video pool in the popup dialog box, as shown below.

Table 3-2 Parameter Setting

Parameter Name	Description
Domain ID	Select the domain that you created.
User Name	Select admin.
User Permission	Select read/ write.
Resource Pool Name	Input videopool.
Resource Pool Type	Select video.

Parameter Name	Description
Storage Mode	Select centralized.
Overwrite Mode	Select capacity.
Resource Pool Capacity	Input 100.
Max. Locking up Attempts	Input 10.

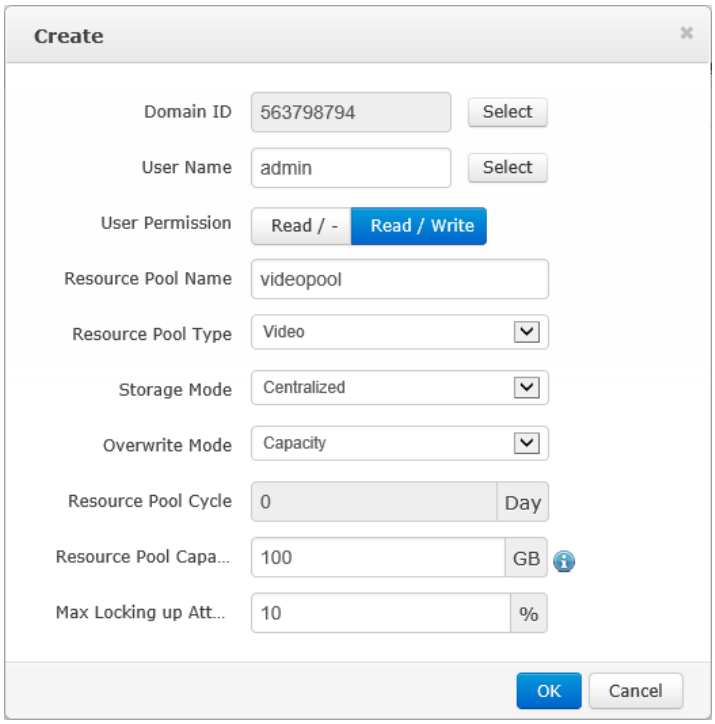

Figure 3-38 Create Video Pool

NOTE

When adding smart storage unit, you will need the ID of video resource pool.

3.2.9 Create Dynamic Pool

Purpose:

Dynamic pool is used to storage the human face pictures that are captured by the camera.

Step 1 Go to **Virtualizing** > **Resource Pool Management**.

Step 2 Click **Create**, and set parameters of dynamic pool in the popup dialog box, as shown below.

Table 3-3 Parameter Setting

Parameter Name	Description
Domain ID	Select the domain that you created.
User Name	Select admin.
User Permission	Select read/ write.
Resource Pool Name	Input dynamicpool.
Resource Pool Type	Select picture.
Accelerate Picture	Select accelerate.
Storage Mode	Select dispersed.
Overwrite Mode	Select capacity.
Resource Pool Capacity	Input remaining capacity.
Max. Locking up Attempts	Input 10.

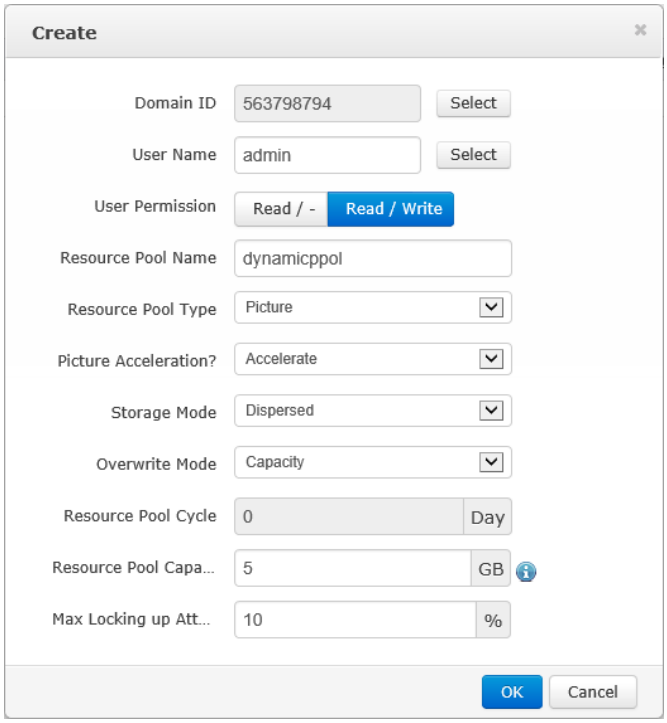

Figure 3-39 Create Dynamic Pool

NOTE

When adding smart storage unit, you will need the ID of dynamic resource pool.

3.2.10 Add Micro Video Cloud

Step 1 Log in the Intelligent Fusion Server.

Step 2 Go to **System Management** > **System Configuration** > **Cloud Storage Configuration**, and click **Add**.

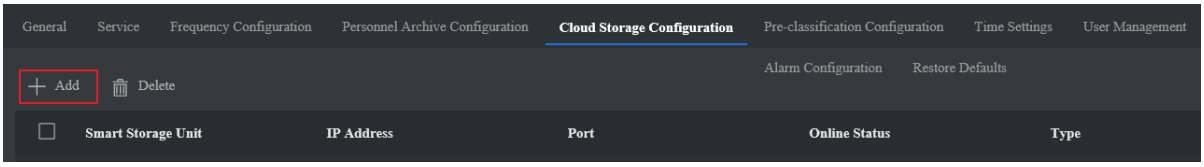

Figure 3-40 Set Cloud Storage

Step 3 Set parameters of **Smart Storage Unit**.

Table 3-4 Parameter Setting

Parameter Name	Description
Name	Input the name as you like. Here we take CVM as an example.
Smart Storage Unit IP	Input the virtual IP of cluster micro video cloud (for standalone micro video cloud, input node IP).
Dynamic Resource Pool ID	Input dynamic resource pool ID that you created.
Static Resource Pool ID	Input static resource pool ID that you created.
Video Resource Pool ID	Input video resource pool ID that you created.
User Name	Input admin.
Password	Input the password when you logging in the HikCStor Management System.
Visit Key and Encryption KEY	Go to **HikCStor Management System** > **Virtualizing** > **User Management**. You can obtain Visit Key and Encryption KEY by clicking Download Key, and access_key is Visit Key and secret_key is Encryption KEY.

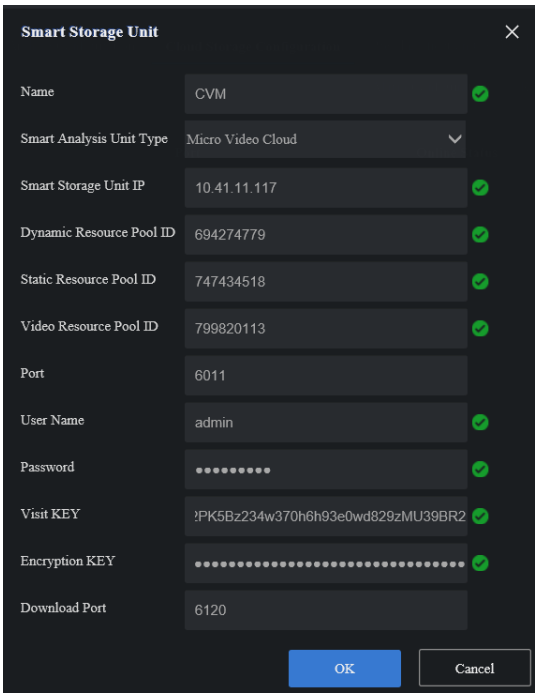

Figure 3-41 Add Smart Storage Unit

Step 4 After setting parameters, click **OK** to complete.

3.3 Create Cluster

3.3.1 Add Node

Before you start:

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

NOTE

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

Step 1 Go to **System Management** > **Cluster Management**, and click **Add**, as shown below.

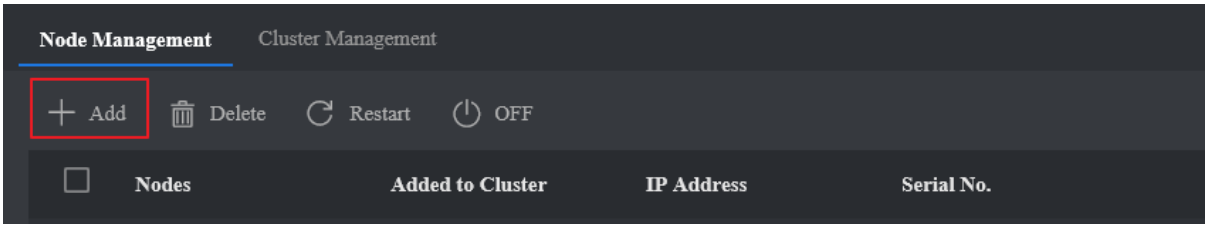

Figure 3-42 Add Node

Step 2 Input **Name**, **Nodes IP**, **User Name** and **Password**, and click **OK** to complete.

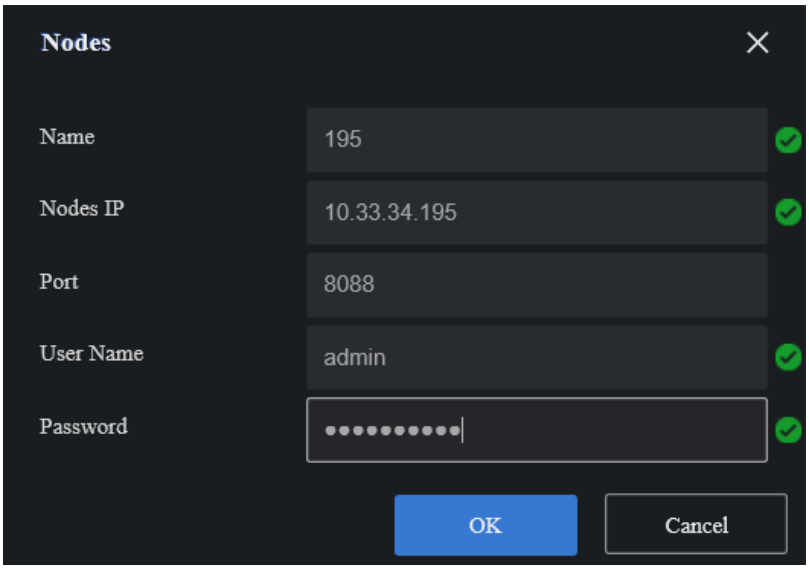

Figure 3-43 Input Nodes Information

NOTE

If there are multi nodes to be added, please repeat the same steps as shown above.

3.3.2 Create Standalone Cluster

Single node can create standalone cluster. After creating cluster, the server can analyze data.

Before you start:

The node is online.

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

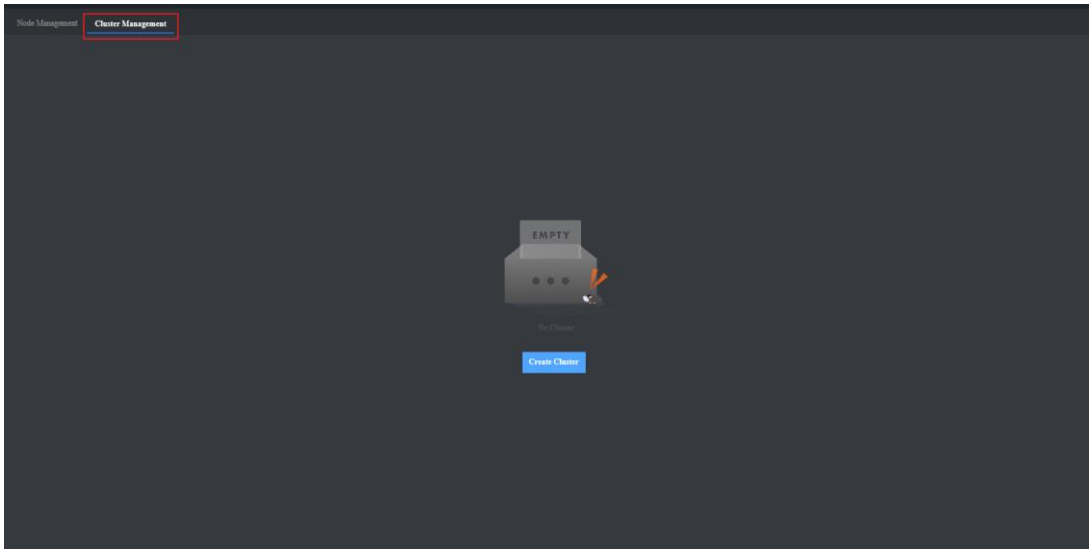

Figure 3-44 Click Create Cluster

Step 2 Select node, and click **Next**.

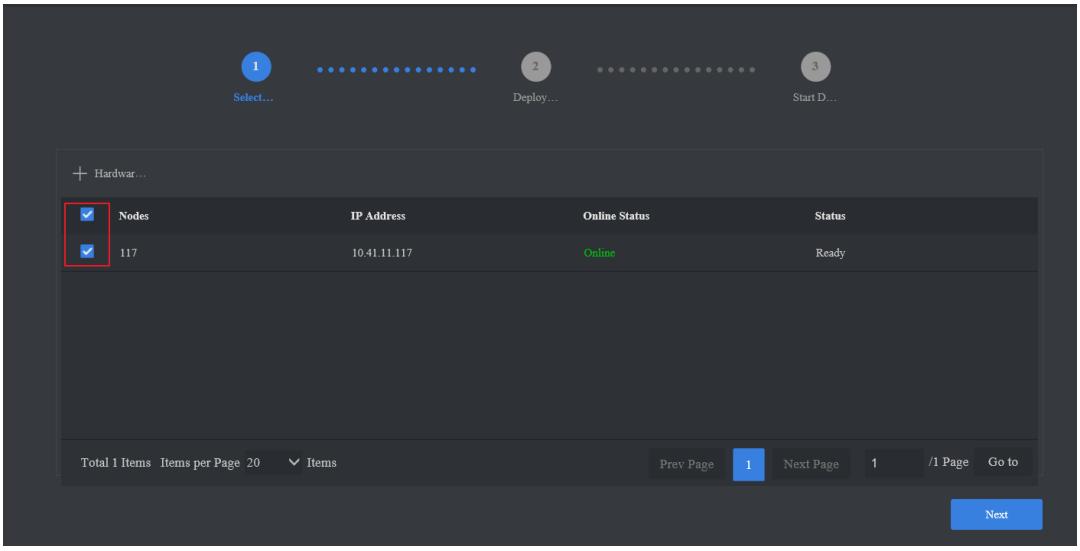

Figure 3-45 Select Nodes

Step 3 Click **Start Deploying** to deploy.

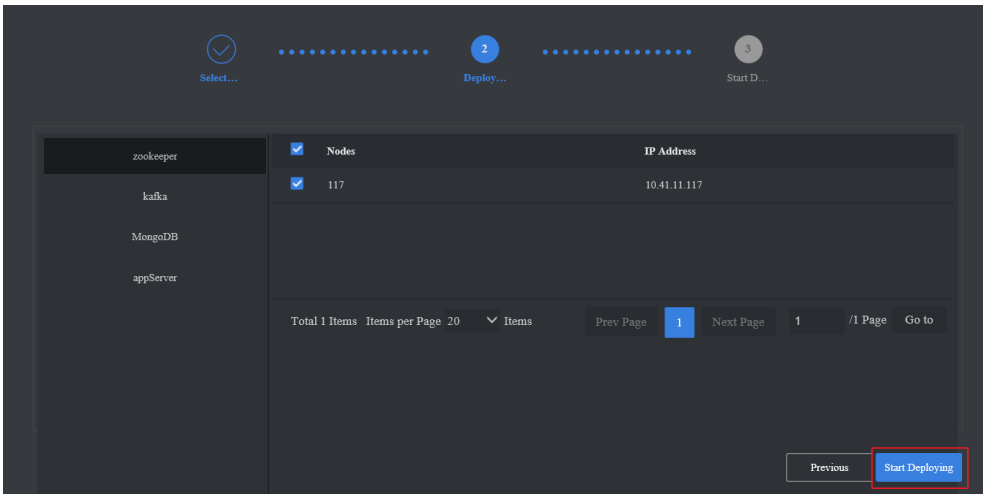

Figure 3-46 Click Start Deploying

Step 4 Click **OFF** after deploying.

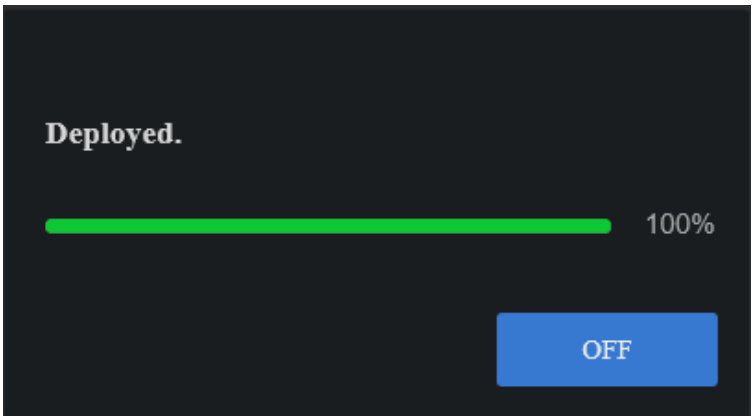

Figure 3-47 Click OFF

Step 5 Click **Resource Configuration** to allocate resources for face picture analysis and face video analysis.

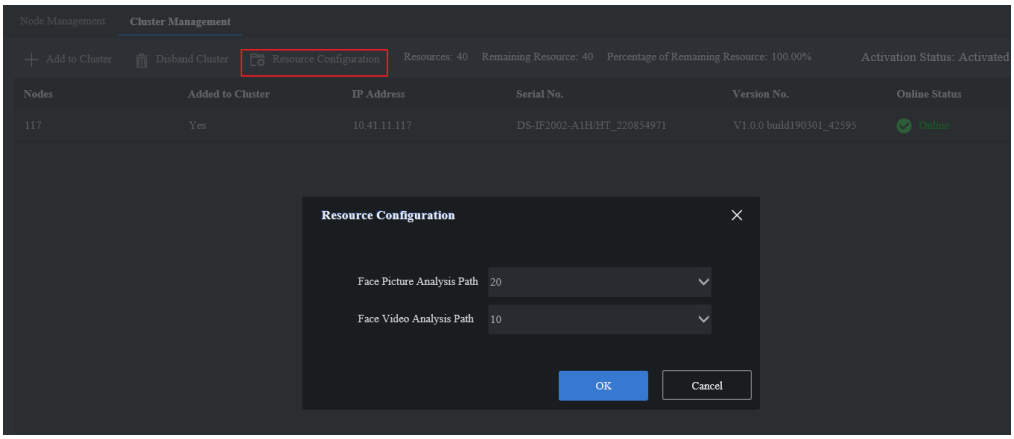

Figure 3-48 Allocate Resource

NOTE

If the allocated resource quantity is 0, the server cannot be able to handle respective analysis task.

3.3.3 Create Master and Backup Cluster

Two nodes or above can create master and backup cluster. After creating cluster, the server can analyze data.

Before you start:

The nodes are online.

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

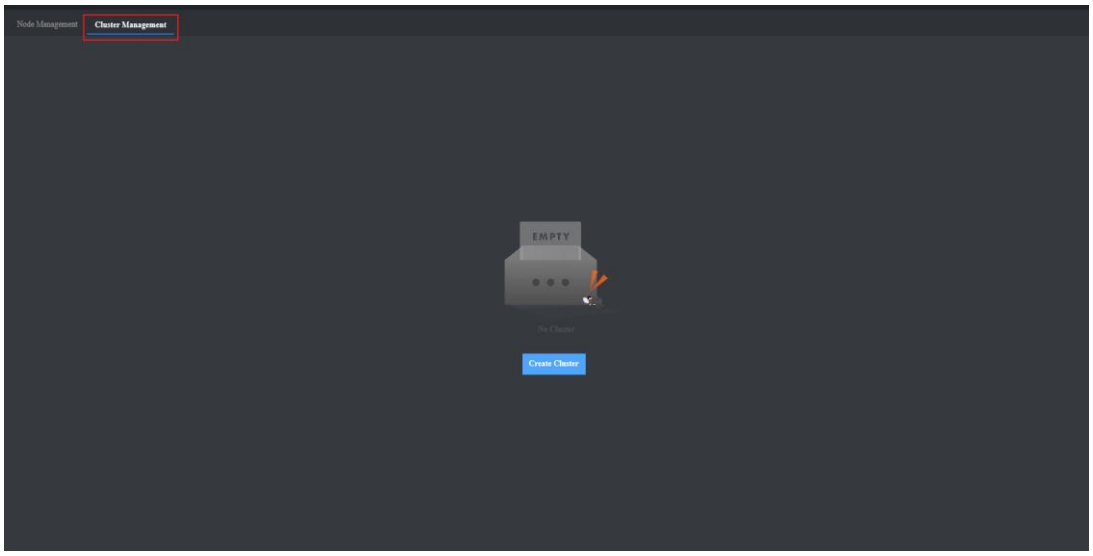

Figure 3-49 Click Create Cluster

Step 2 Select nodes, and click **Next**.

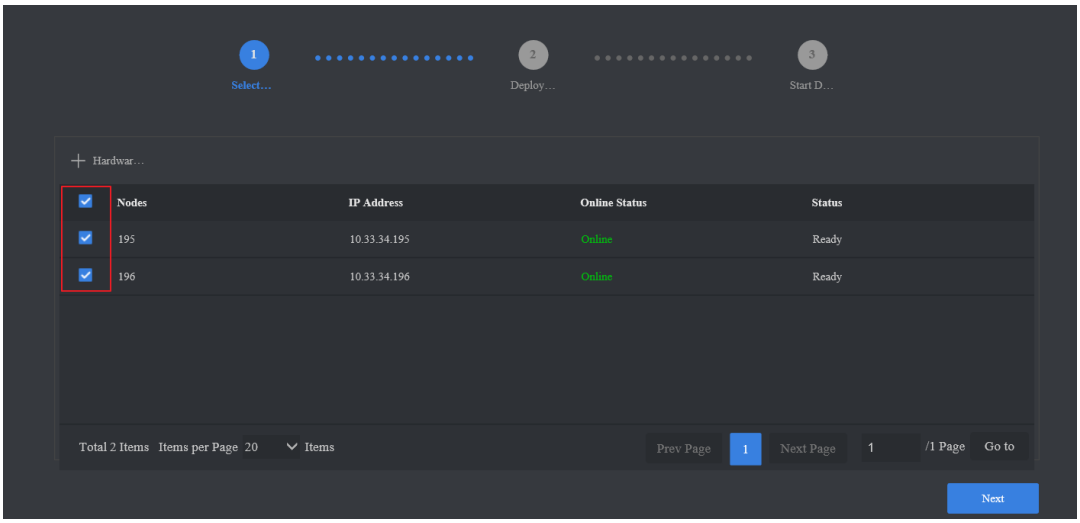

Figure 3-50 Select Nodes

Step 3 Click **appServer**, input an idle IP address of same subnet in **Virtual IP**, and click **Start Deploying** to deploy.

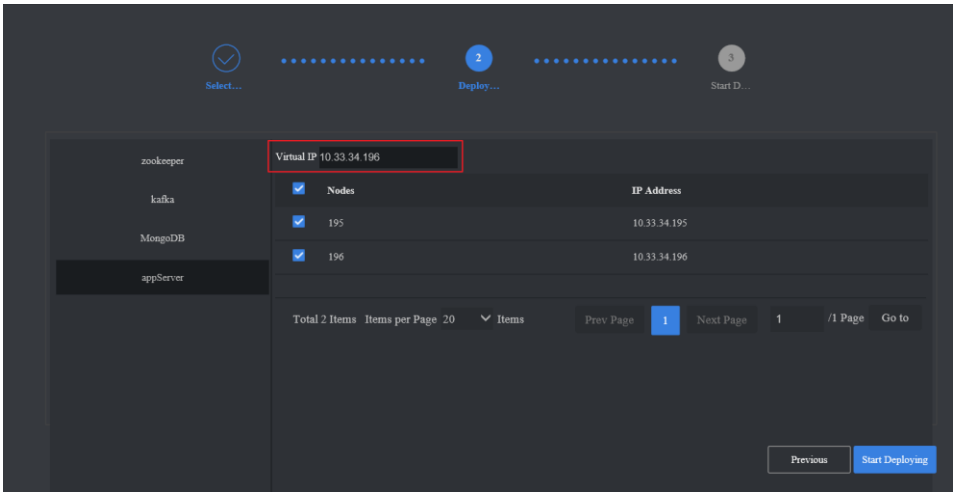

Figure 3-51 Input Virtual IP

Step 4 Click **OFF** after deploying.

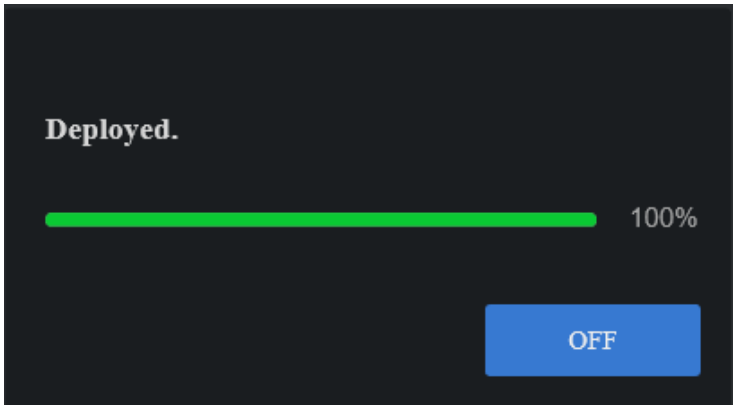

Figure 3-52 Click OFF

Step 5 Click **Resource Configuration** to allocate resources for face picture analysis and face video analysis.

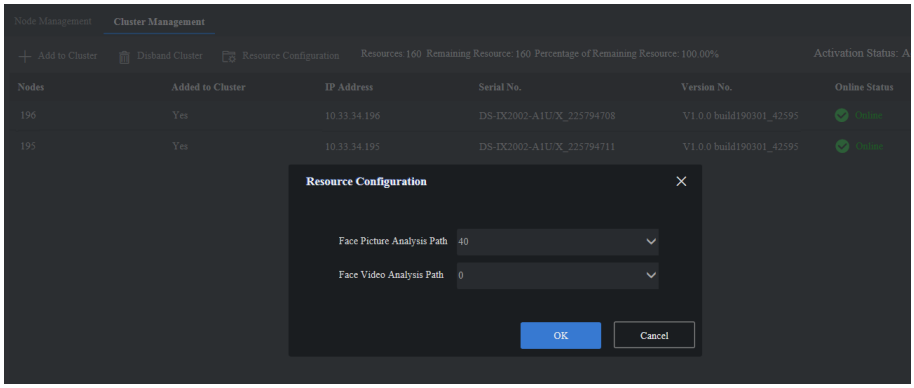

Figure 3-53 Allocate Resource

NOTE

If the allocated resource quantity is 0, the server cannot be able to handle respective analysis task.

3.4 Add Face List Library

Purpose:

Face list library is used to add different list libraries, including normal library, blacklist library and VIP library.

Step 1 Go to **List Management**, and click **Add**, as shown below.

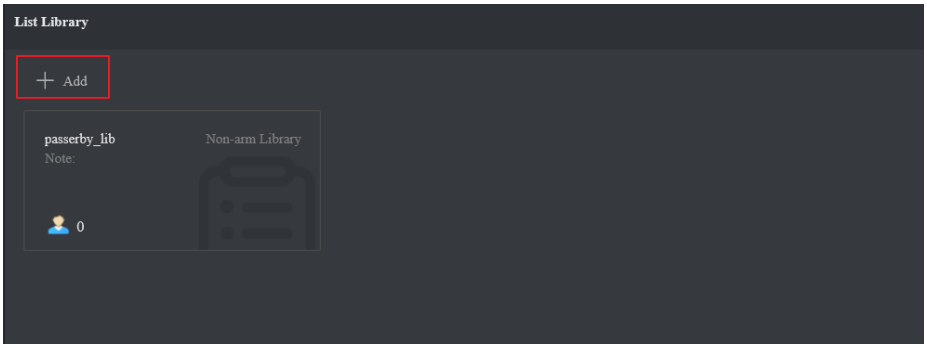

Figure 3-54 List Library Interface

Step 2 Input relevant parameters in the dialogue box according to actual demands. Here we take blacklist arm library as an example.

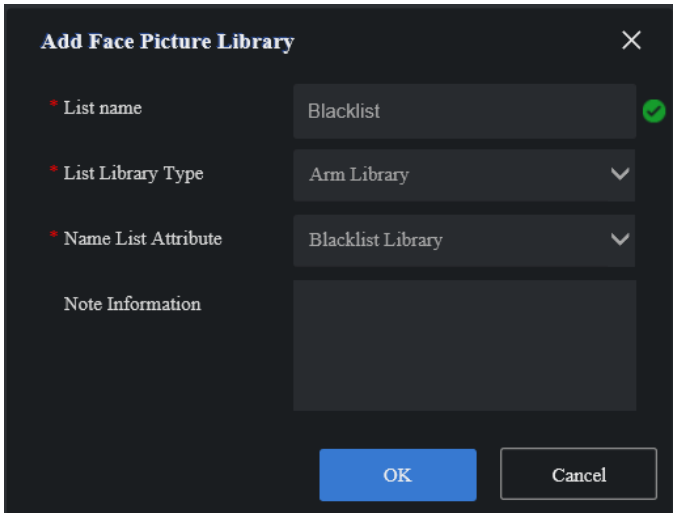

Figure 3-55 Add Face List Library

Step 3 After setting, click **OK** to complete.

Step 4 (Optional) After adding face list library, click to modify list library information and click to delete it.

NOTE

- The passerby library is created by default and cannot be deleted. It is used to add captured stranger face pictures.
- Deleting list library will delete all relevant personnel information.
- Only non-arm list library can be deleted.

3.5 Add Personnel Information

Before you start:

Face List library has been added.

Step 1 Click list library you want to add personnel in.

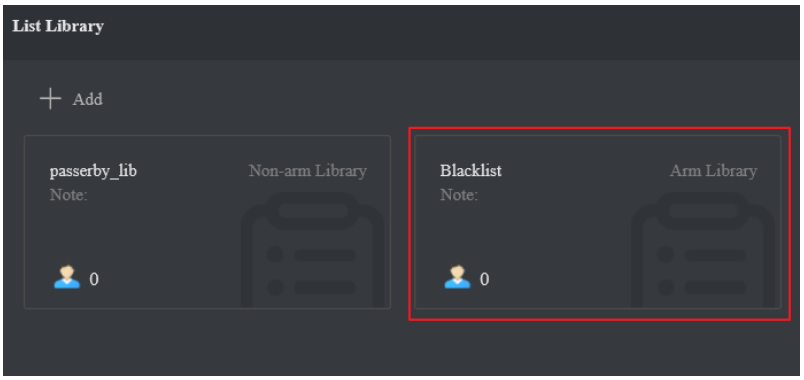

Figure 3-56 Click List Library

Step 2 Click **Add**, input relevant parameters in the dialogue box, and upload face picture.

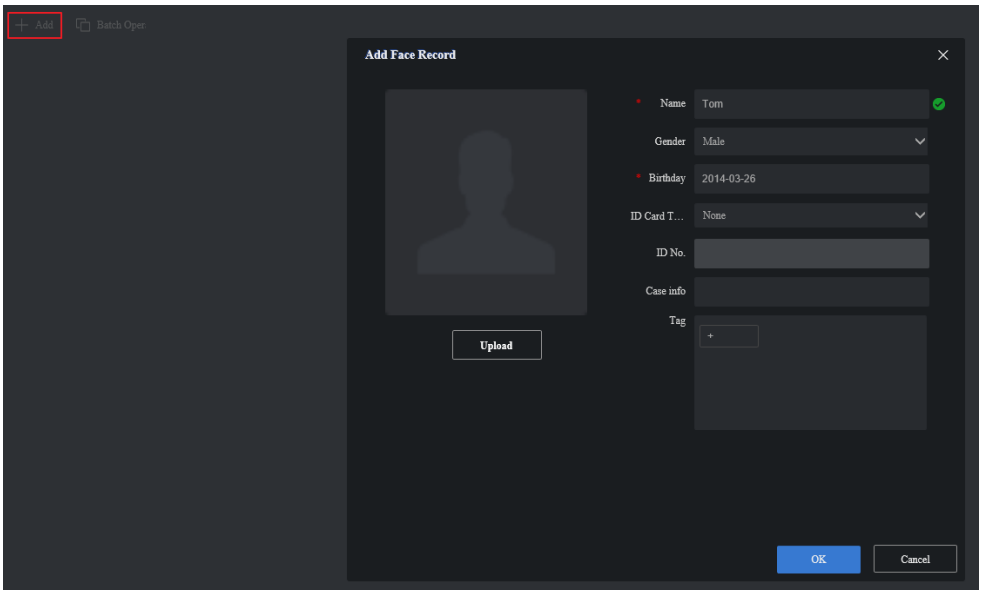

Figure 3-57 Add Personnel Information

NOTE

- It is required to input name and birthday, and you can input other parameters according to actual demands.
- The server supports uploading face picture in the format of jpg, jpeg, bmp, tif and png.

Step 3 Click **OK** to complete.

Step 4 (Optional) After adding personnel information, you can click to modify it, click to delete it, and to set search conditions and search.

3.6 Create Analysis Task

Analysis task includes real-time analysis task and local video record analysis task. Before creating analysis task, you should add respective resource like camera, video record and etc.

3.6.1 Add Camera

Before you start:

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

NOTE

- Add one camera only for each time.
- is control center and is area. The camera should be added to control center first and then it can be added to area. Here we take adding camera to control center and user as admin as an example.

Step 1 Go to **Arming Management > Device**, click **admin** and **Add** to input camera information, as shown below.

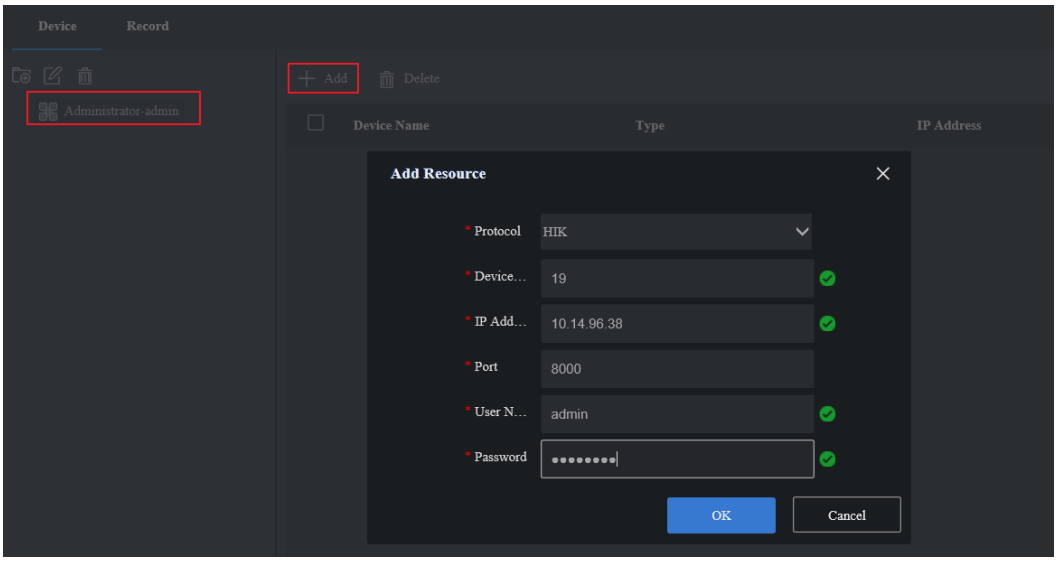

Figure 3-58 Add Camera

Step 2 Click **OK** to complete.

Step 3 Click , select **Type** as **Area**, input name, and click **OK**.

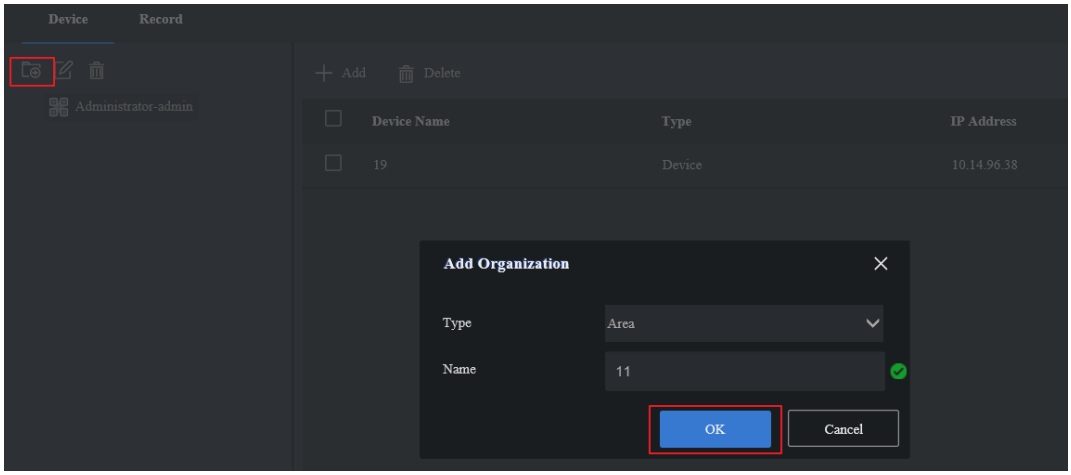

Figure 3-59 Add Area

NOTE

The area name supports Chinese, number, lowercase and uppercase, and special characters “-, _”, with 32 characters at most.

Step 4 Select added area, and click **Add**.

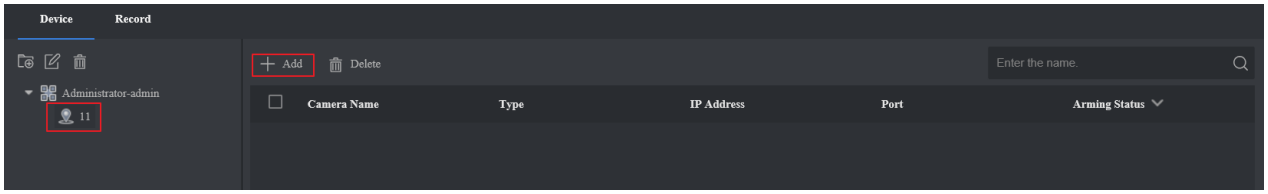

Figure 3-60 Click Add

NOTE

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

Step 5 Check the camera that is to be added to area, and click **OK**.

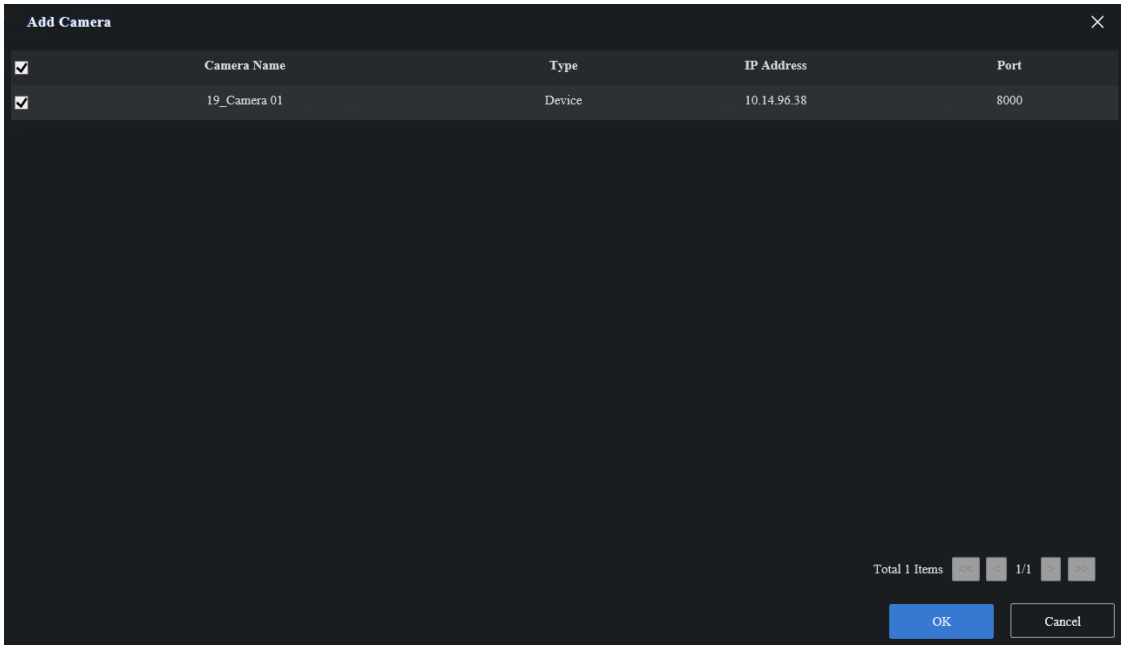

Figure 3-61 Add Camera to Area

NOTE

The control center can add other control centers and areas under its tree format.

3.6.2 Add Video Record

NOTE

Here we take adding import video record into default list and user as admin as an example.

Step 1 Go to **Arming Management** > **Record**, click ▶ of admin and click **Default List**.

Step 2 Click **Import**.

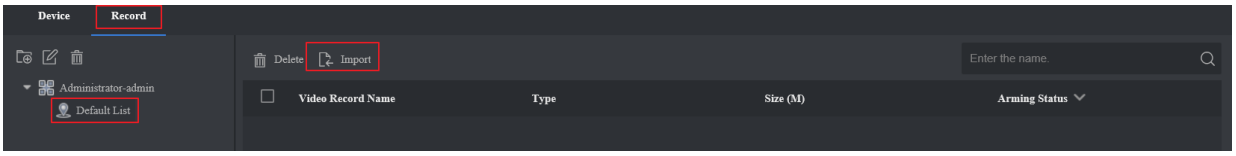

Figure 3-62 Click Import

Step 3 Click **Browse** to select video record files, set video starting time as actual recording time, and click **OK**, as shown below.

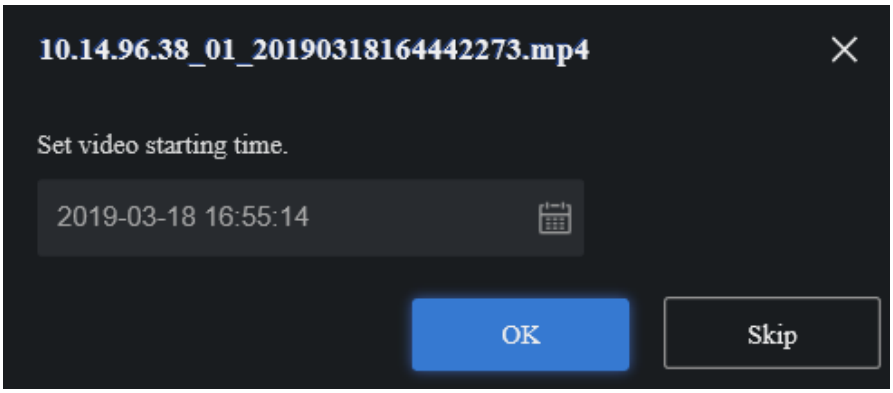

Figure 3-63 Set Video Starting Time

Step 4 Click **Import** to import.

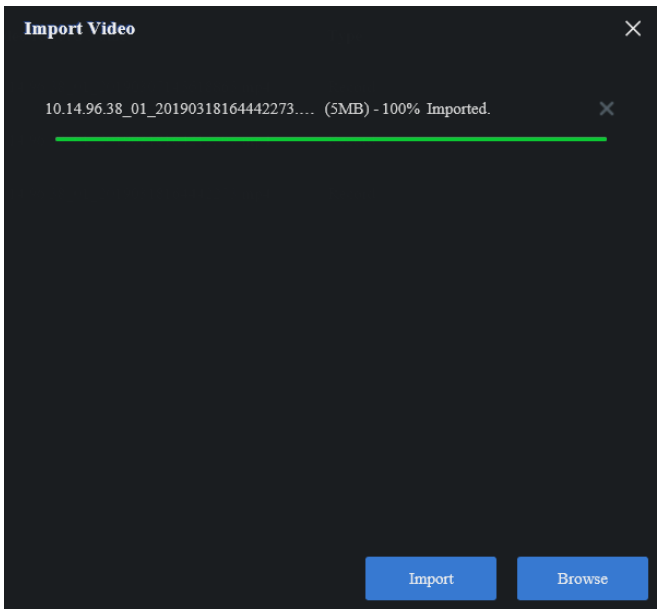

Figure 3-64 Click Import

3.6.3 Create Real-time Analysis Task

Purpose:

Real-time analysis task is used to analyze faces in monitoring scene in real time.

Before you start:

- Add respective camera.
- Allocate respective resources.

Step 1 Go to **Arming Management > Task Management**, click **New**.

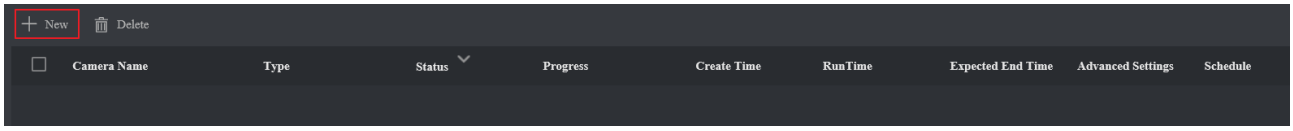

Figure 3-65 Task Management Interface

Step 2 Check camera or multi cameras, click **Create**.

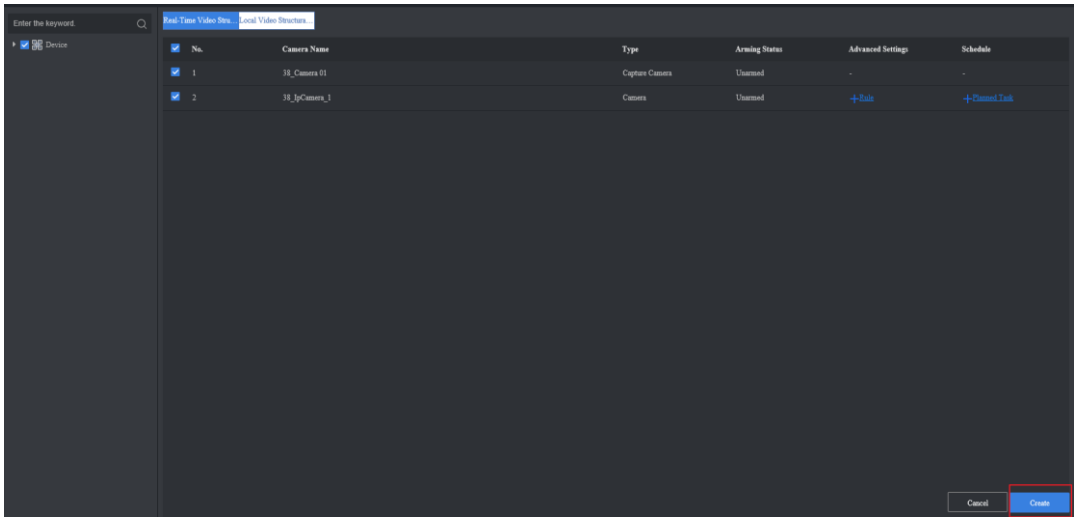

Figure 3-66 Click Create

Step 3 Click **OK** in the popup dialogue box.

Step 4 (Optional) Click **Rule** in **Advanced Settings** list, set detailed rule in the popup interface, and click **OK** to complete.

- Click ☐ to draw detection area, and the server executes full screen detection by default.
- Click to draw min. pupil distance, and you can set max. pupil distance as well. After setting, the server detects the face between min. and max. pupil distance only.
- For other parameters, you can use the default ones.

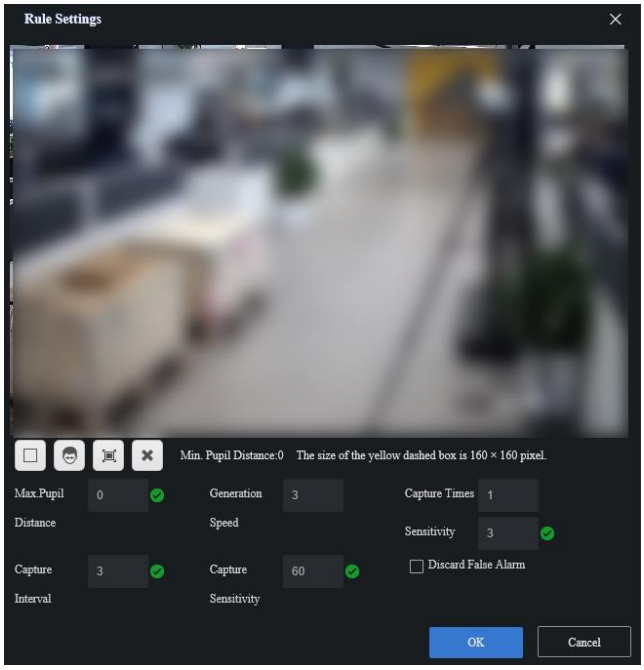

Figure 3-67 Set Rule

NOTE

- If a prompt informing you of installing a plug-in pops up, please install it accordingly. Before installing the plug-in, close IE browser.
- For drawing detection area, rectangle is supported only.

Step 5 (Optional) Click **Planned Task** in **Schedule** list, set detailed schedule in the popup interface, and click **OK** to complete.

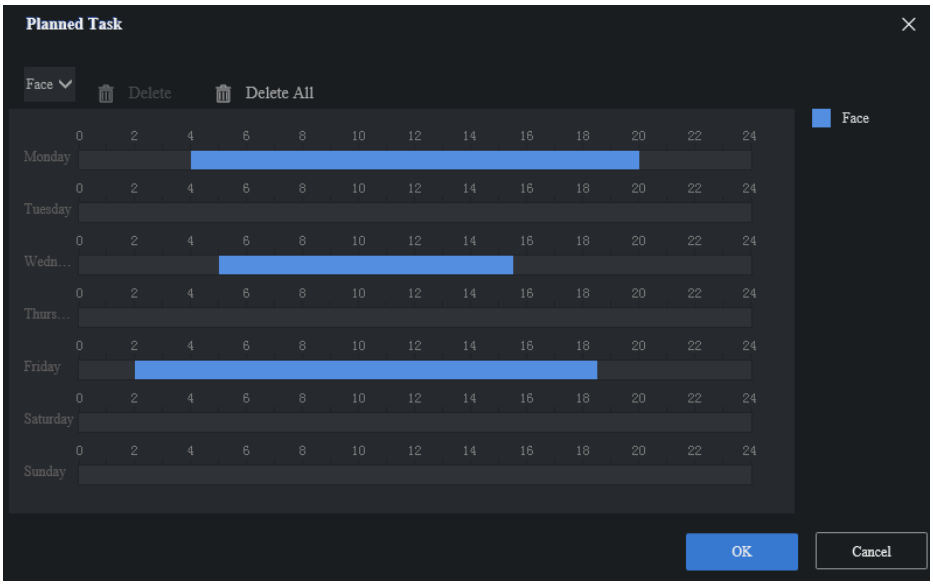

Figure 3-68 Set Planned Task

3.6.4 Create Video Record Analysis Task

Purpose:

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

Before you start:

- Import video record files.
- Allocate respective resources.

Step 1 Go to **Arming Management > Task Management**, click **New**.

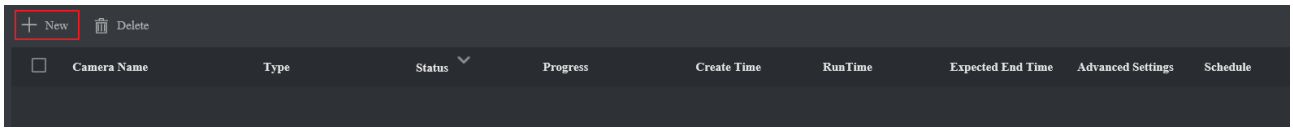

Figure 3-69 Click New

Step 2 Select **Local Video Structural Task**, check video record file or multi files, click **Create**.

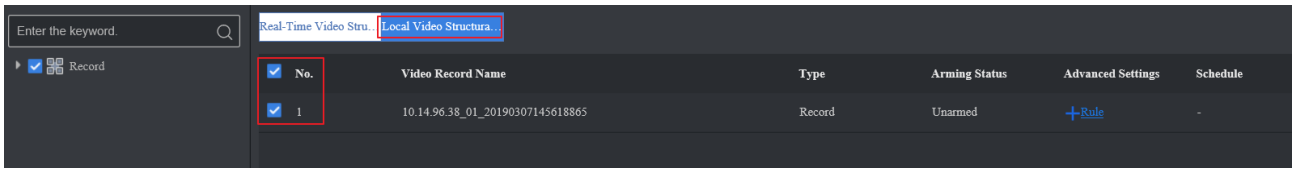

Figure 3-70 Check Video Record File

Step 3 Click **OK** in the popup dialogue box.

Step 4 (Optional) Click **Rule** in **Advanced Settings** list, set detailed rule in the popup interface, and click **OK** to complete.

- Click ☐ to draw detection area, and the server executes full screen detection by default.
- Click to draw min. pupil distance, and you can set max. pupil distance as well. After setting, the server detects the face between min. and max. pupil distance only.
- For other parameters, you can use the default ones.

NOTE

- If a prompt informing you of installing a plug-in pops up, please install it accordingly. Before installing the plug-in, close IE browser.
- For drawing detection area, rectangle is supported only.

3.7 Add List Arming

Purpose:

Listing arming is used to link face in face list library with camera. After adding list arming, when the similarity between face captured by camera and that of face list library reaches configured threshold, the server will send out alarm.

Before you start:

- Camera has been added and armed.
- Face list library and personnel information have been added.
- Selecting **Arm Library** as **List Library Type** for list library you want to arm.

Step 1 Go to **Arming Management** > **List Arming**, and click **New**.

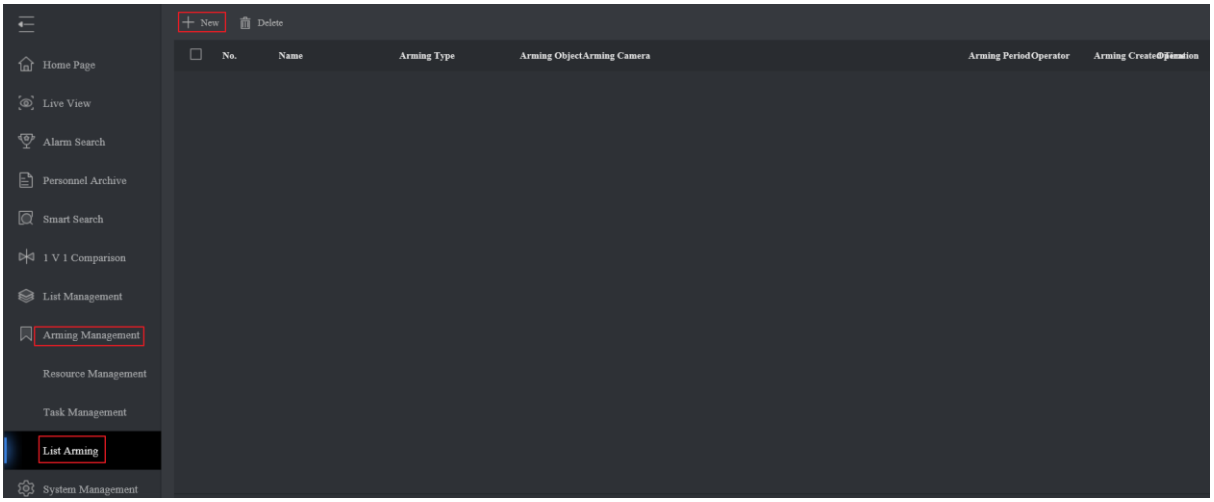

Figure 3-71 Add List Arming

NOTE

- Here we take arming blacklist library as an example.
- The specific parameter values filled in the relevant interfaces below are for reference only. You need to input relevant parameter values according to actual condition.

Step 2 Set relevant parameters.

Table 3-5 Parameter Setting

Parameter Name	Description
Name and Note	Input relevant information according to actual condition.
Arming Type	Select list arm.

Parameter Name	Description
Arming Object	Select blacklist library.
Arming Camera	Select camera that is to be armed.
Arming Time	Set arming time.
Threshold	The larger the threshold, and the higher requirement for face similarity will be.

NOTE

If **Stranger Arm** is selected as **Arming Type**, you should select arming object accordingly.

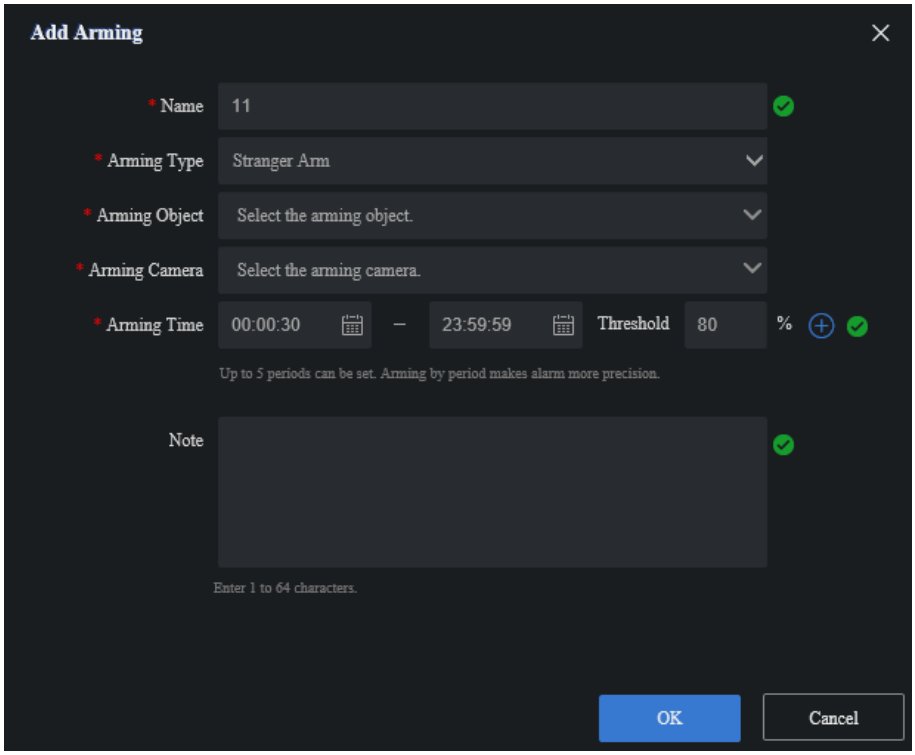

Figure 3-72 Set List Arming Parameters

NOTE

You can click ⊕ to arm at different time period.

Step 3 Click **OK** to complete.

Step 4 (Optional) After adding list arming, you can click ✎ to modify parameters, and click **Delete** to delete after checking respective arming.

3.8 Enable Frequency Alarm

Purpose:

Frequency alarm is used to count the frequency that personnel appears in monitoring scene. When the frequency reaching configured threshold, the server will generate alarm information.

Before you start:

Camera has been added and armed.

Step 1 Go to System **Management** > **System Configuration** > **Frequency Configuration**.

Step 2 Set relevant parameters.

Table 3-6 Parameter Setting

Parameter Name	Description
Enable	Check Enable.
Camera	Select the camera which you need to count the personnel appearance frequency.
List to Filter	It filters the personnel in list library, and the server will not count the personnel appearance frequency.
Filtering Threshold	It compares the similarity between face captured by camera and that of face list library. The server will not count personnel appearance times when the similarity is larger than or equal to this value you configured.
Appeared Times	Frequency alarm will generate only when the appeared times is larger than the configured times.
Capture Internal (min)	It is the internal of capturing face pictures, and the unit is minute.
Similarity	It compares the similarity between newly captured face pictures and all captured face pictures. The server will count appearance times for the same personnel when the similarity is larger than or equal to this value you configured.
Day Range	It is the statistics period of personnel appearance frequency.

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

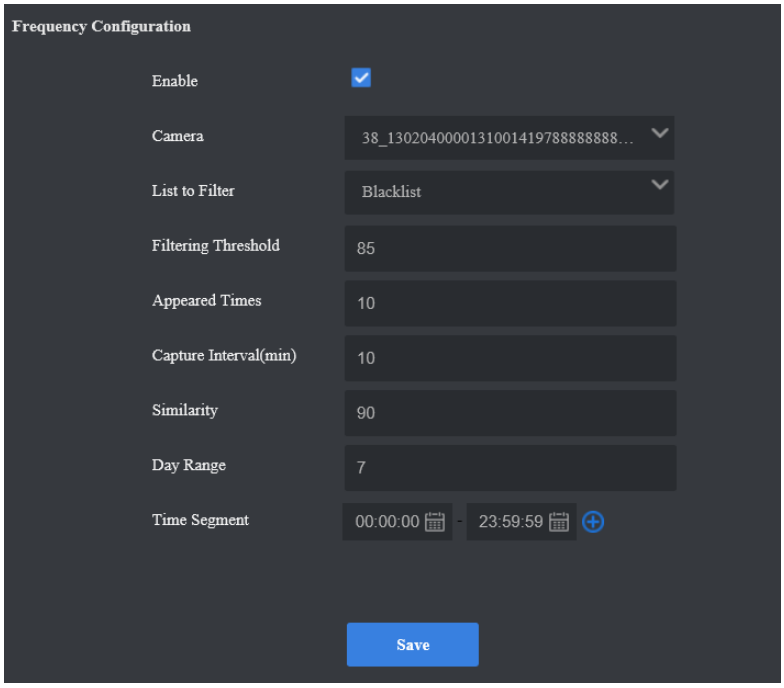

Figure 3-73 Enable Frequency Alarm

Step 3 Click **Save** to complete.

3.9 Enable Personnel Archive Configuration

Purpose:

Personnel archive is used to compare the similarity between face captured by camera and that of face list library. When the similarity reaches the configured threshold, the server classifies the face picture into real name archive, otherwise, into the pedestrian archive.

One archive for one personnel, and the archive records total times that one personnel appears, appeared time and captured picture.

Before you start:

- Camera has been added and armed.
- Selecting **Arm Library** as **List Library Type** for passerby library.

Step 1 Go to System **Management** > **System Configuration** > **Personnel Archive Configuration**.

Step 2 Set relevant parameters.

Table 3-7 Parameter Setting

Parameter Name	Description
Enable	Check Enable.
Arming Object	Selecting passerby library is required, and select other arming object according to actual demands.
Arming Camera	Select camera.
Threshold	It compares the similarity between face captured by camera and that of face list library (except passerby library). When the similarity reaches the configured this threshold, the server classifies the face picture into real name archive, otherwise, into the pedestrian archive.

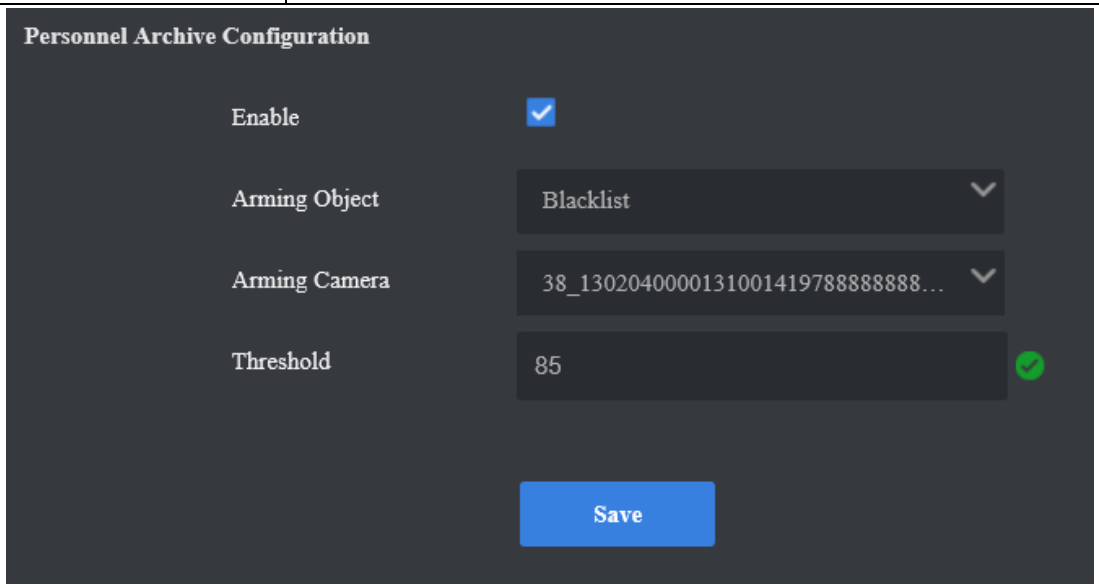

Figure 3-74 Enable Personnel Archive

Step 3 Click **Save** to complete.

Chapter 4 Smart Application

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

4.1 Live View

It displays face pictures captured by the camera, list alarm information, stranger alarm information, and frequently appeared person alarm information in real time.

Before you start:

- Add list arming.
- Enable frequency alarm.

Step 1 Click **Live View**.

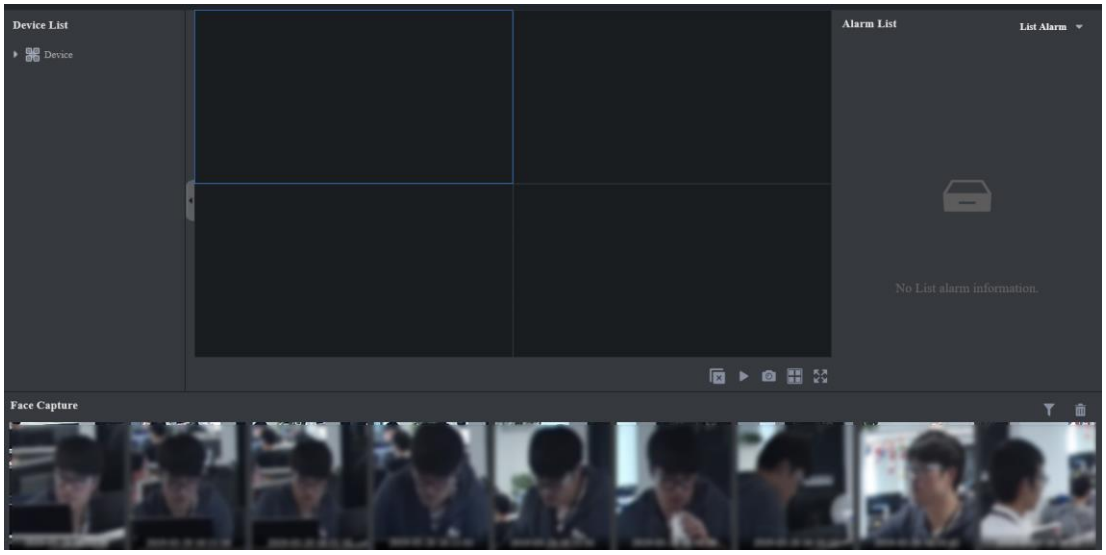

Figure 4-1 Live View Interface

NOTE

- If a prompt informing you of installing a plug-in pops up, please install it accordingly. Before installing the plug-in, close IE browser.
- In the live view interface, the bottom area displays face pictures captured by the camera in real time, and the right area displays list alarm information, stranger alarm information, and frequently appeared person alarm information in real time.

Step 2 Double-click camera to start live view.

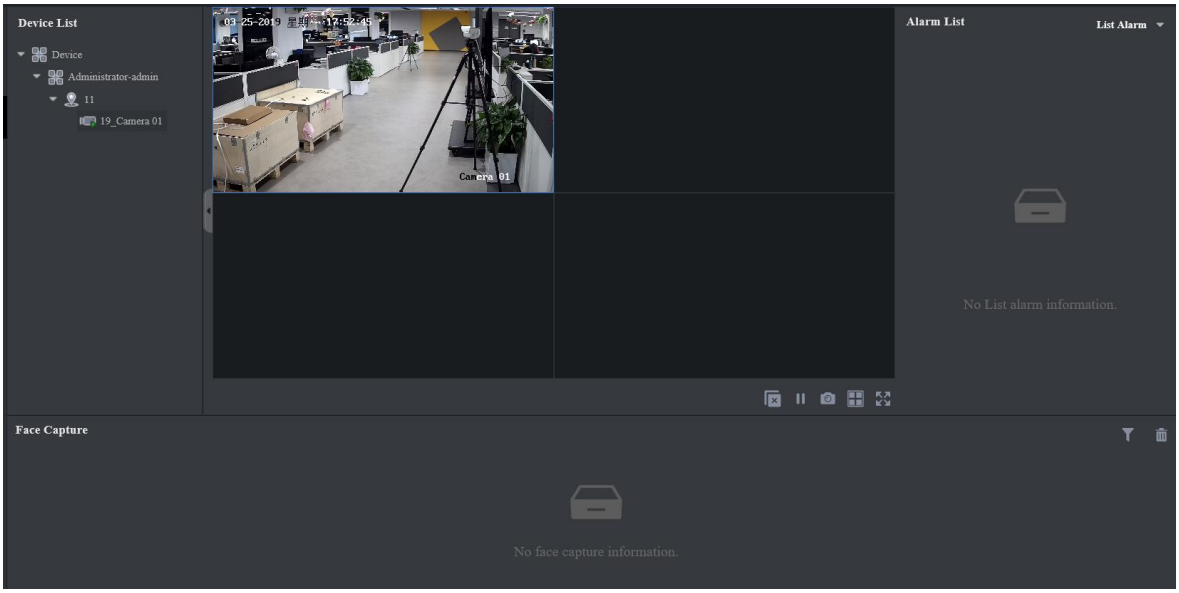

Figure 4-2 Double-click Camera

Table 4-1 Live View Interface Introduction

No.	Name	Description
1	Live view	It supports live view in multiple channels. : Click it to stop live view in current channel. : Click it to stop all live views. : Click it to capture picture manually and the picture will automatically be saved in your computer. If you want to modify save path, please refer to ***Section 5.3.7***.
2	Face capture	It captures faces in real time. : Click it to filter cameras, and the server will display face picture captured by the checked camera. : Click it to clear all current displayed face picture. : Click it to add face picture to list library. : Set this face picture as target picture to search picture by picture. : Set this face picture as target picture to confirm identification.

No.	Name	Description
3	List alarm	It displays latest list alarm information. Click … to view detailed information.
4	Stranger alarm	It displays latest stranger alarm information. Click … to view detailed information.
5	Frequently appeared person alarm	It displays all frequency alarm information. Click … to view detailed information.

4.2 Alarm Search

4.2.1 List Alarm

The server compares the similarity between captured face pictures and those in list library like blacklist library. When the similarity reaches configured value, the server will generate list alarm information.

Before you start:

Add list arming.

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

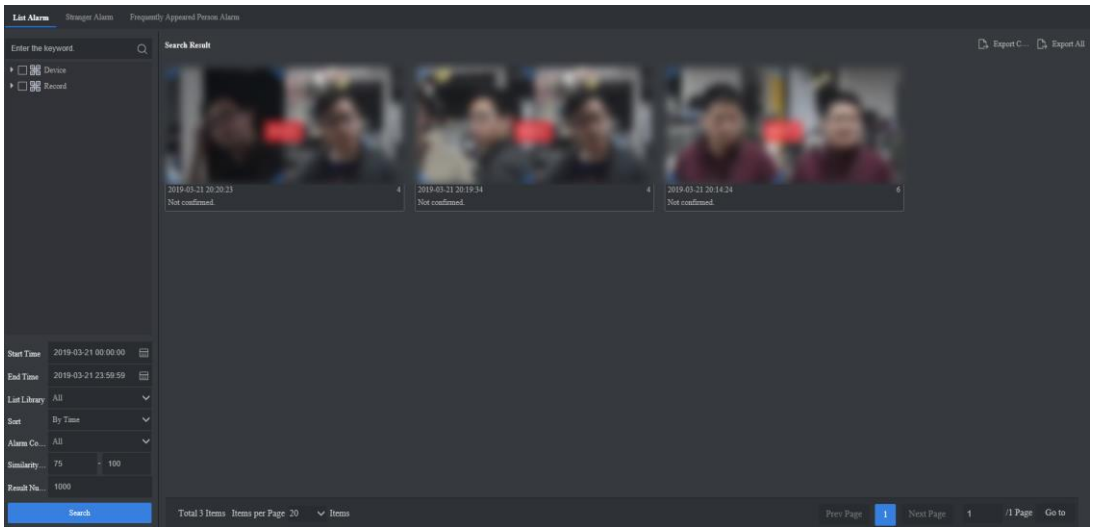

Figure 4-3 List Alarm Interface

Step 2 Select camera. If you do not select any camera, the server will search alarm information created by all cameras.

Step 3 Set search conditions like start time, end time, list library and etc.

Step 4 Click **Search** to search alarm information.

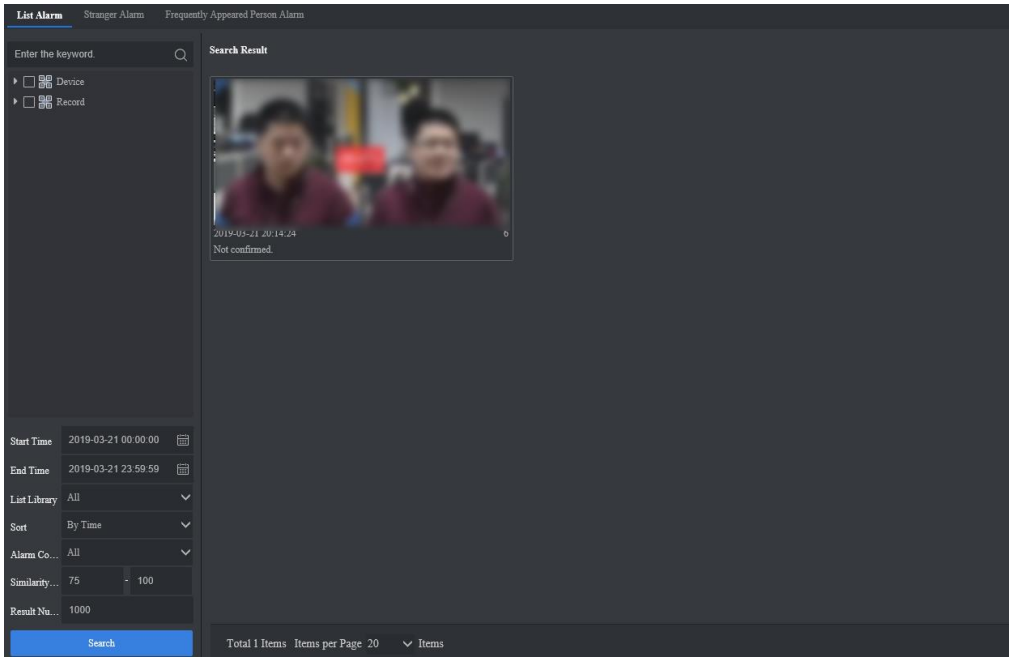

Figure 4-4 Click Search

Step 5 Click alarm picture to view detailed information.

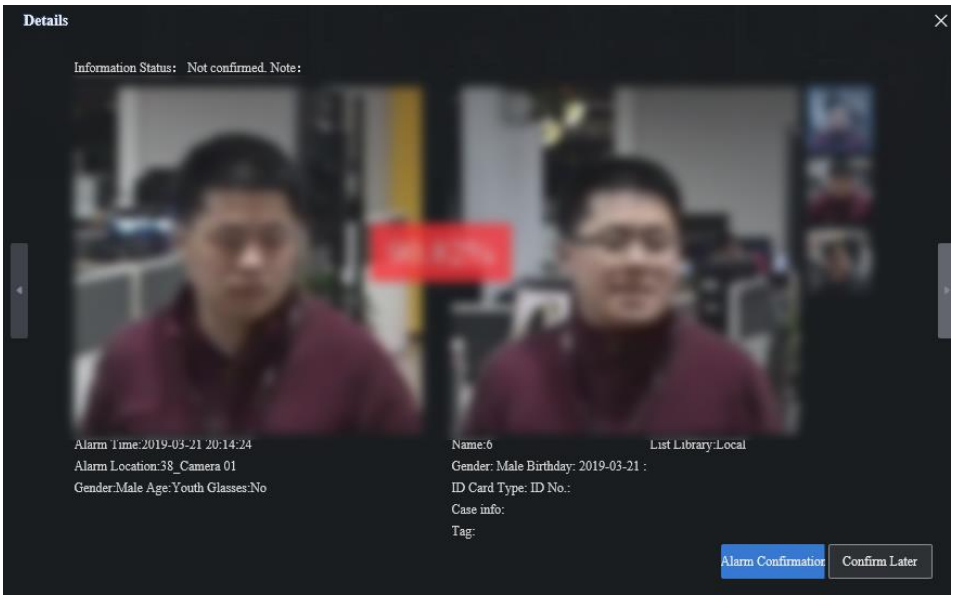

Figure 4-5 View Detailed Information

Step 6 Click **Alarm Confirmation** to confirm this alarm.

Step 7 Click **Export Current Page** or **Export All** to export alarm information.

4.2.2 Stranger Alarm

The server compares the similarity between captured face pictures and those in list library. When the similarity does not reach configured value, the server will generate stranger alarm information.

Before you start:

Add stranger arming.

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

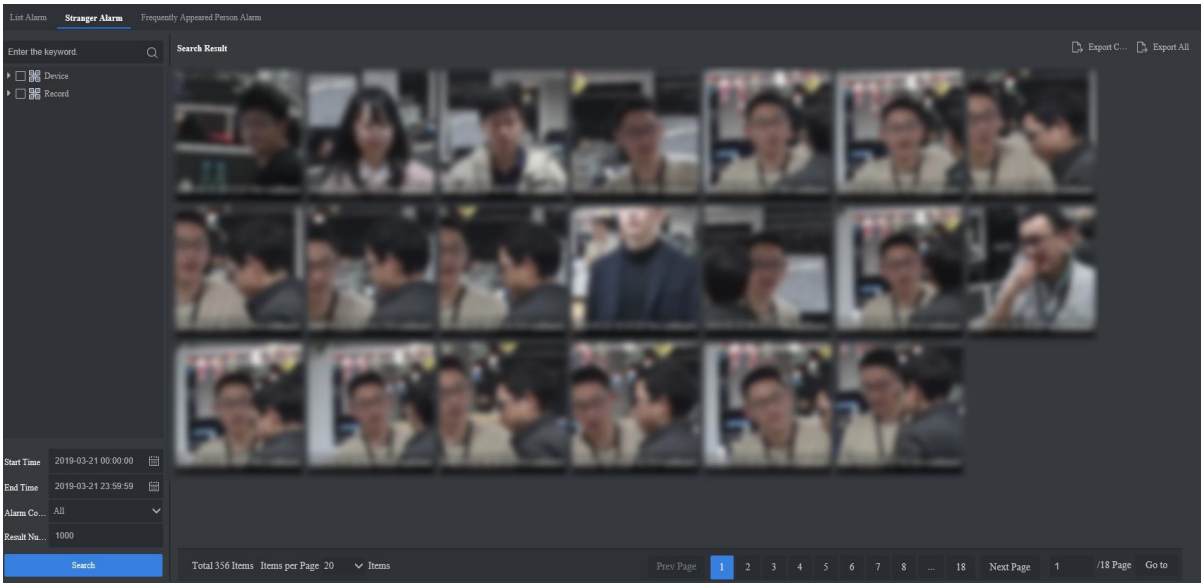

Figure 4-6 Stranger Alarm Interface

Step 2 Select camera. If you do not select any camera, the server will search alarm information created by all cameras.

Step 3 Set search conditions like start time, end time, list library and etc.

Step 4 Click **Search** to search stranger alarm information.

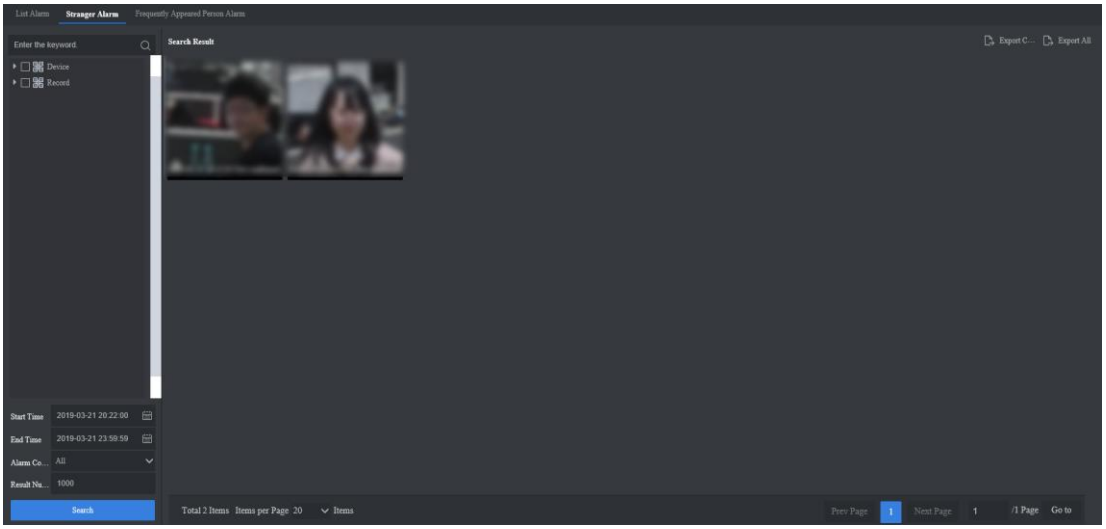

Figure 4-7 Click Search

Step 5 Click stranger alarm picture to view detailed information.

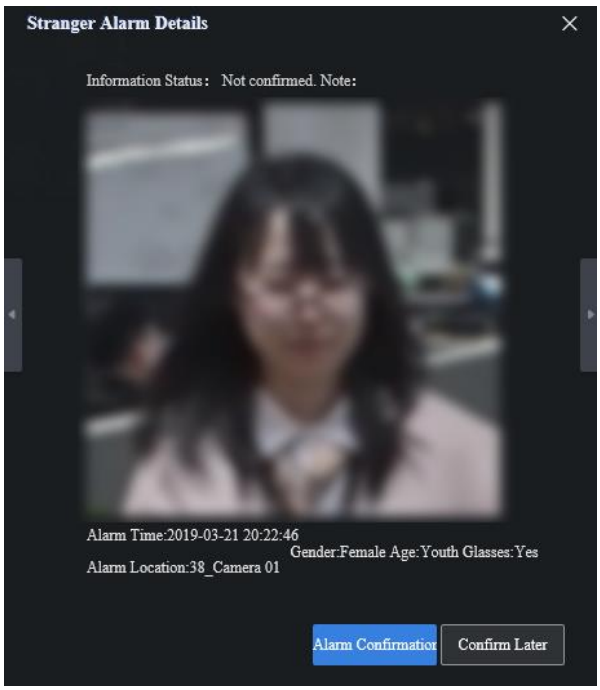

Figure 4-8 View Detailed Information

Step 6 Click **Alarm Confirmation** to confirm this alarm.

Step 7 Click **Export Current Page** or **Export All** to export stranger alarm information.

4.2.3 Frequently Appeared Person Alarm

The server counts person appearance times in monitoring scene. When times reach configured value, the server will generate alarm information.

Before you start:

Enable frequency alarm.

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

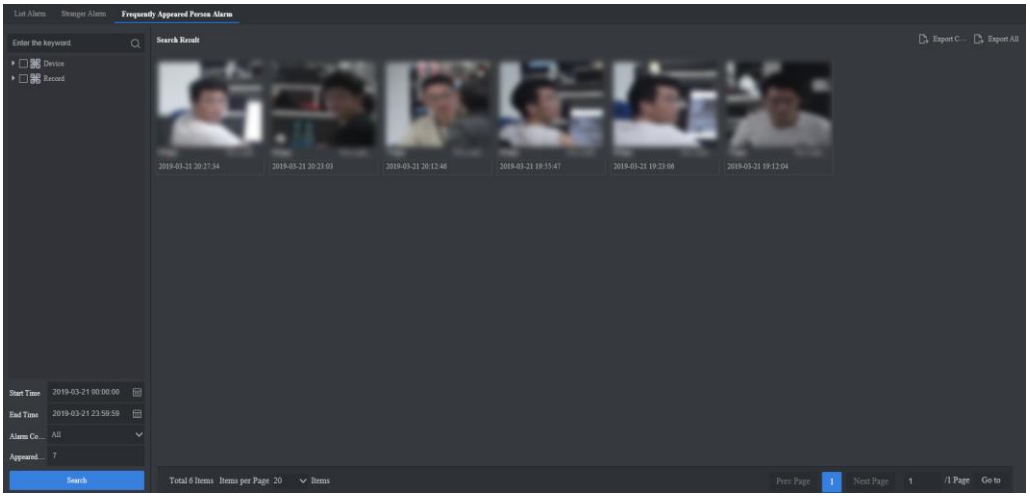

Figure 4-9 Frequently Appeared Person Alarm Interface

Step 2 Select camera. If you do not select any camera, the server will search alarm information created by all cameras.

Step 3 Set search conditions like start time, end time, list library and etc.

Step 4 Click **Search** to search alarm information.

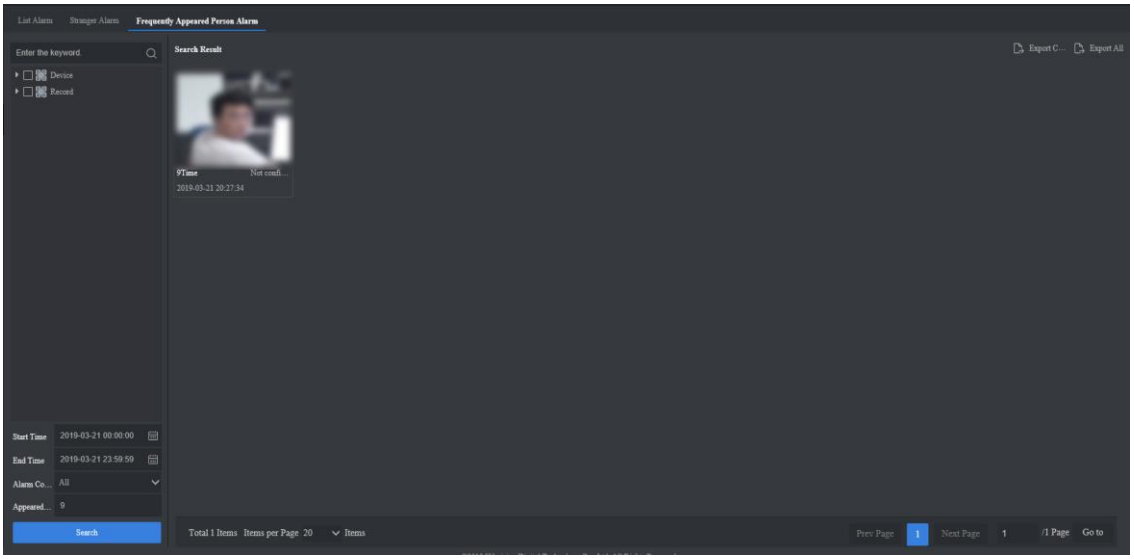

Figure 4-10 Click Search

Step 5 Click alarm picture to view detailed information.

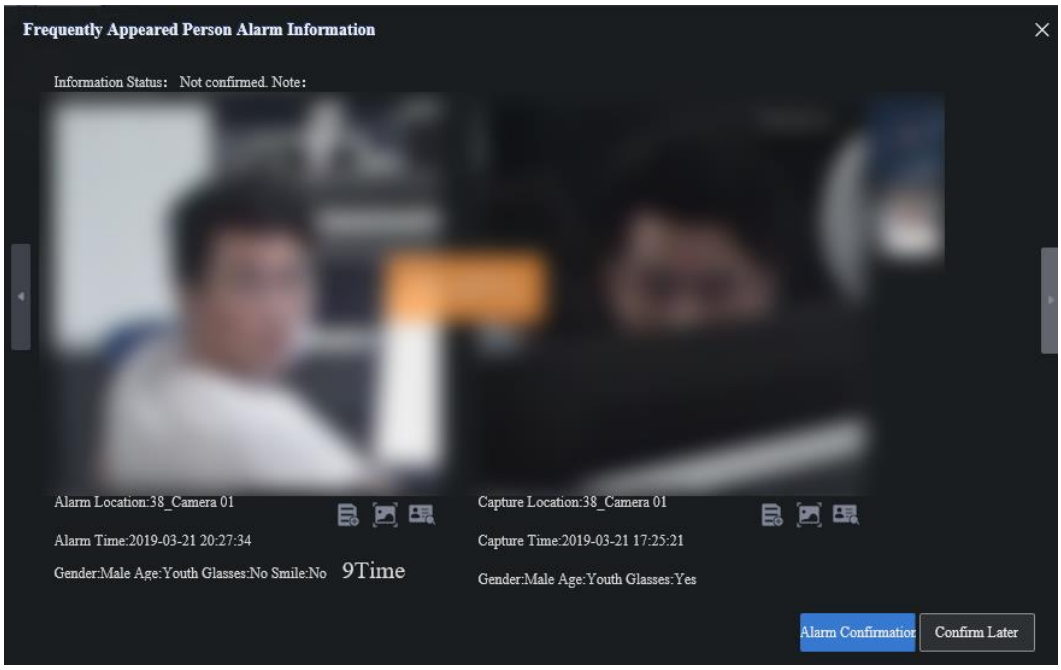

Figure 4-11 View Detailed Information

Step 6 Click **Alarm Confirmation** to confirm this alarm.

Step 7 Click **Export Current Page** or **Export All** to export alarm information.

4.3 Personnel Archive

Personnel archive records personnel appearance times, appearance time period in monitoring scene and respective captured picture.

Step 1 Go to **Personnel Archive**. By default, the server displays all personnel archive information.

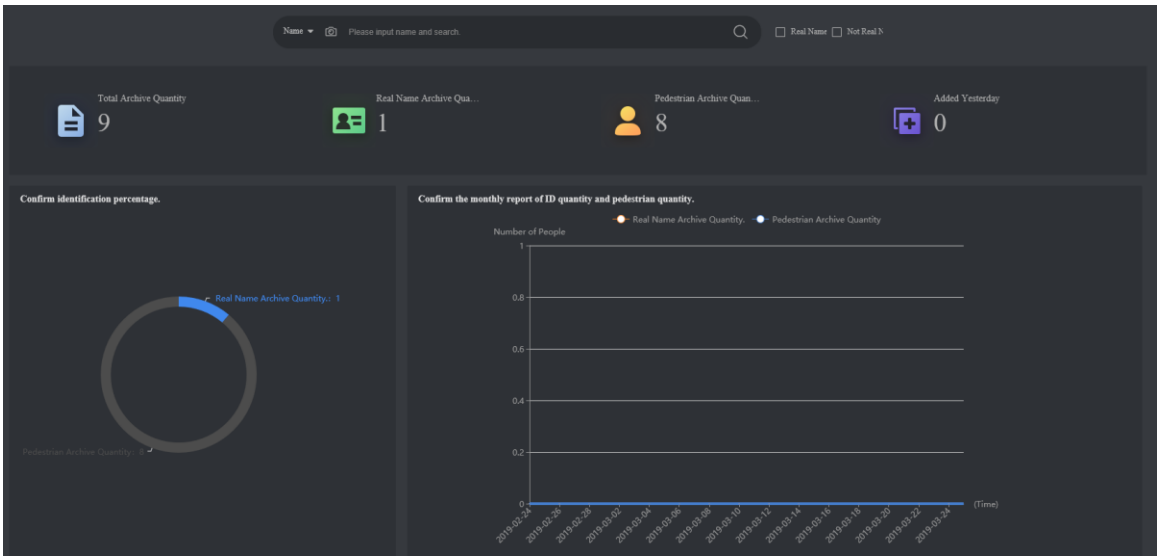

Figure 4-12 Personnel Archive Interface

NOTE

- Real Name: it refers to the personnel who is in arming list.
- Not Real Name: it refers to personnel in passerby library.

Step 2 (Optional) Click Real Name Archive Quantity: or Pedestrian Archive Quantity to view respective archive quantity.

Step 3 Set search conditions according to actual demands, and click to search personnel archive.

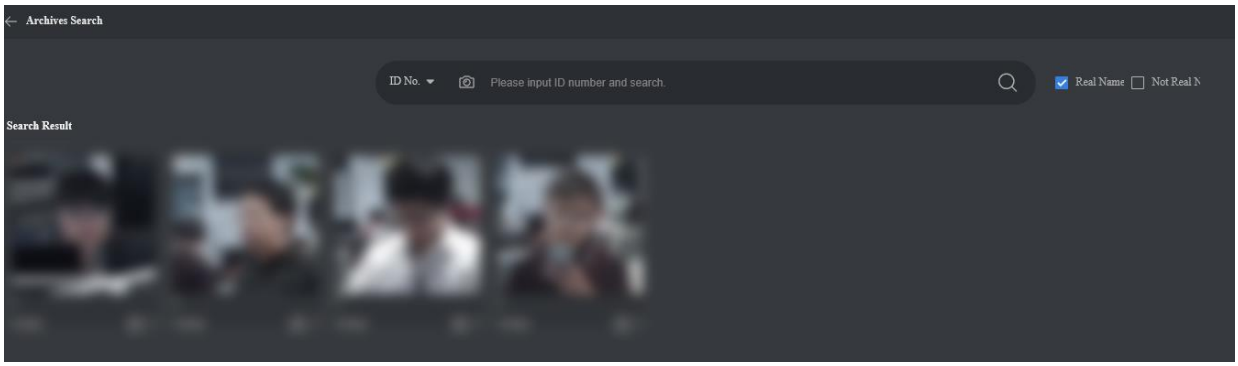

Figure 4-13 Personnel Archive Search Result

Step 4 Click to view the detailed information about personnel archive.

4.4 Smart Search

4.4.1 Normal Search

This function searches face pictures captured by cameras.

Before you start:

Alarm the camera.

Step 1 Go to **Smart Search** > **Normal Search**. By default, the server displays all face pictures captured by cameras.

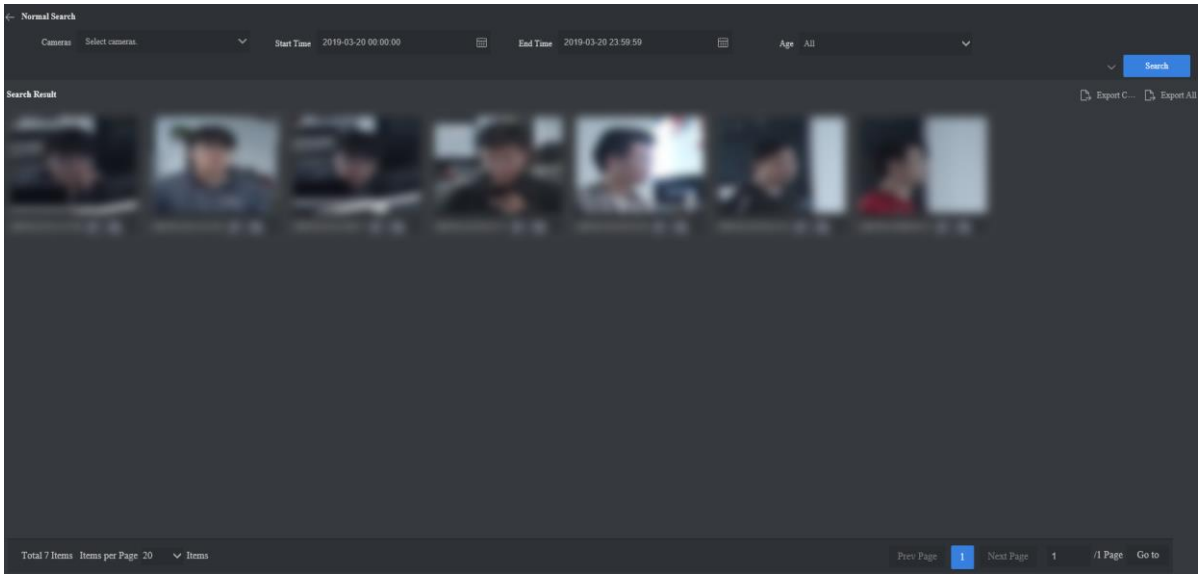

Figure 4-14 Normal Search Interface

Step 2 Select camera. If you do not select any camera, the server will search all face pictures captured by cameras.

Step 3 (Optional) Select record of camera to display the analysis result of record.

Step 4 Click ⌄ to unfold and set detailed search conditions.

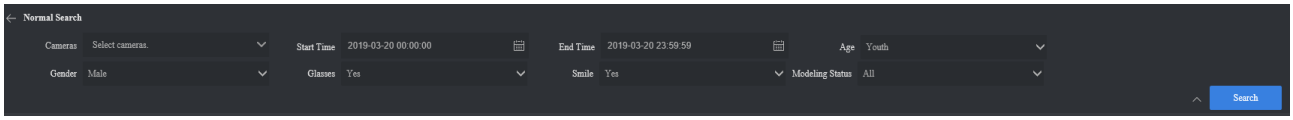

Figure 4-15 Set Search Conditions

NOTE

You can set different search condition parameters by referring to ***Section 5.3.6***.

Step 5 Click **Search**.

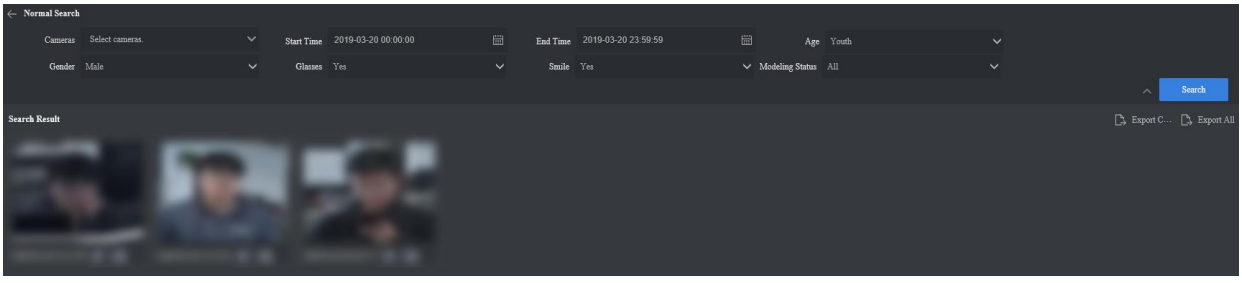

Figure 4-16 Search Result

Step 6 Click searched face picture to view detailed information.

Step 7 (Optional) 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.

Step 8 (Optional) Click **Export Current Page** or **Export All** to export captured information.

4.4.2 Search by Picture

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

Before you start:

Alarm the camera.

Step 1 Go to **Smart Search** > **Search by Picture**.

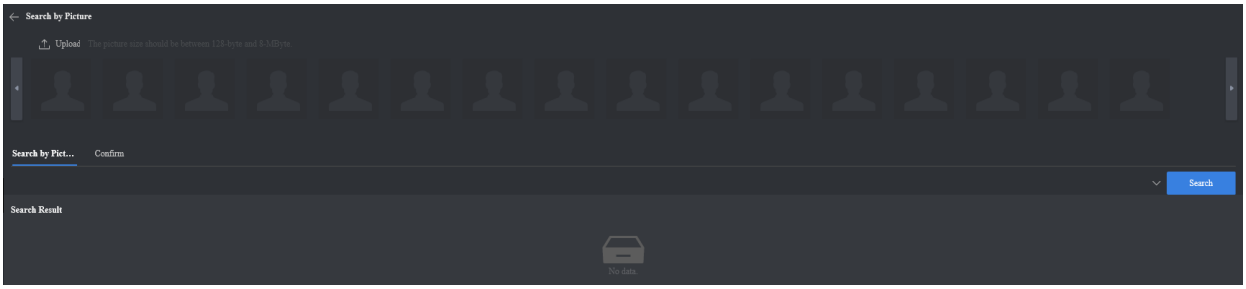

Figure 4-17 Search by Picture Interface

Step 2 Click **Upload** to upload to be searched face picture. If the uploaded picture contains multiple faces, and these faces will be uploaded.

NOTE

- The server supports uploading face picture in the format of jpg, jpeg, bmp, tif and png.
- In order to improve comparison accuracy, it is recommended to upload picture with clear face.

Step 3 Check the face picture that is to be searched, click  to unfold and set detailed search conditions.

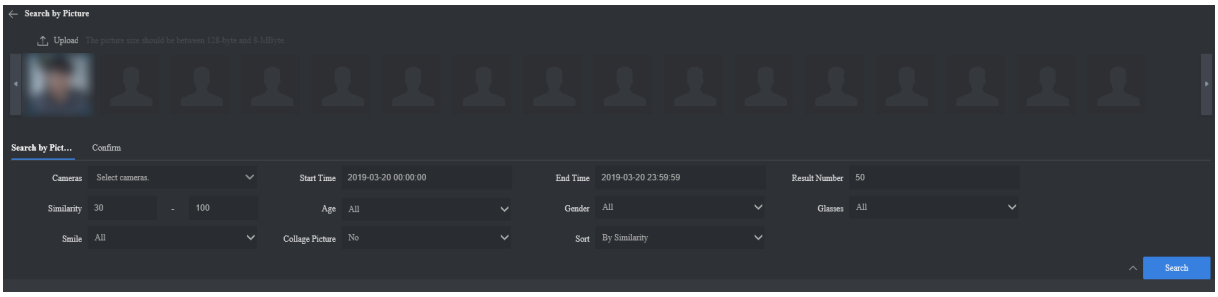

Figure 4-18 Set Search Conditions

NOTE

If you do not select any camera, the server will search all face pictures captured by cameras.

Step 4 Click **Search**, and the server displays all results by similarity degree or time order.

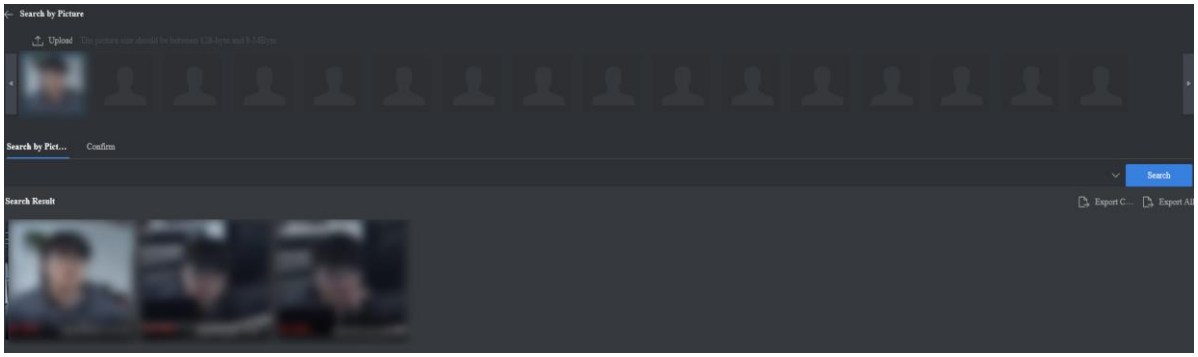

Figure 4-19 Search Result

Step 5 Click searched face picture to view detailed information.

Step 6 (Optional) 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.

Step 7 (Optional) Click **Export Current Page** or **Export All** to export alarm information.

4.4.3 Confirm Identification

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

Before you start:

Add face list library.

Step 1 Go to **Smart Search** > **Search by Picture** > **Confirm**.

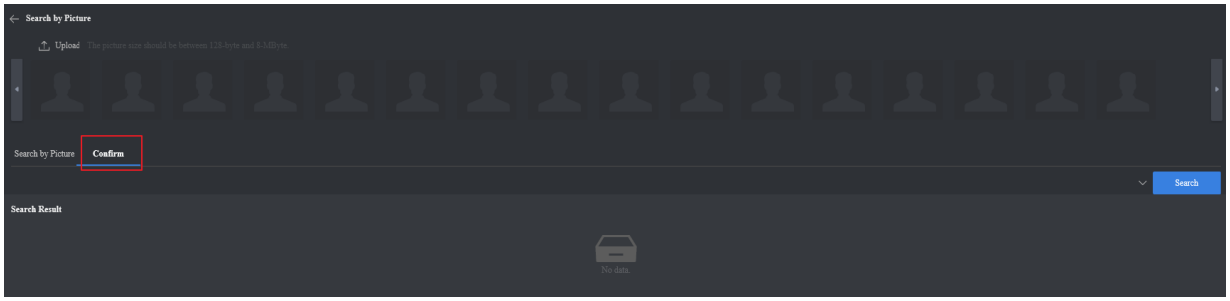

Figure 4-20 Confirm Identification Interface

Step 2 Click **Upload** to upload to be confirmed face picture.

NOTE

The server supports uploading face picture in the format of jpg, jpeg, bmp, tif and png.

Step 3 Click to unfold and set detailed search conditions.

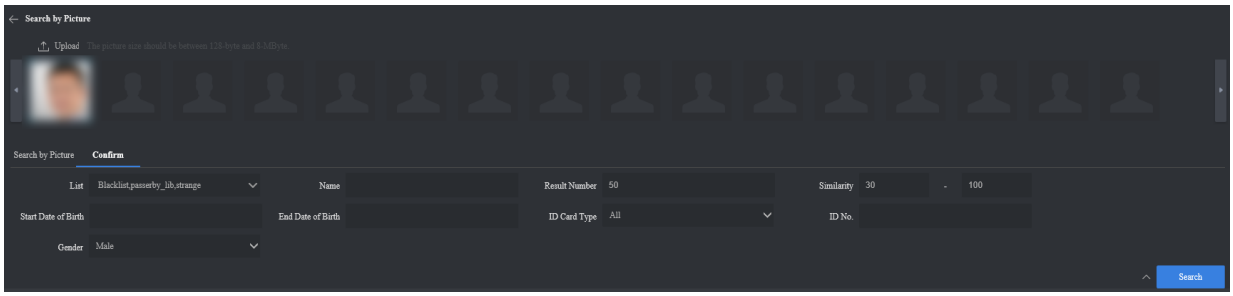

Figure 4-21 Set Search Conditions

NOTE

If you do not select any list, the server will search all lists.

Step 4 Click **Search**, and the server displays all results by similarity degree.

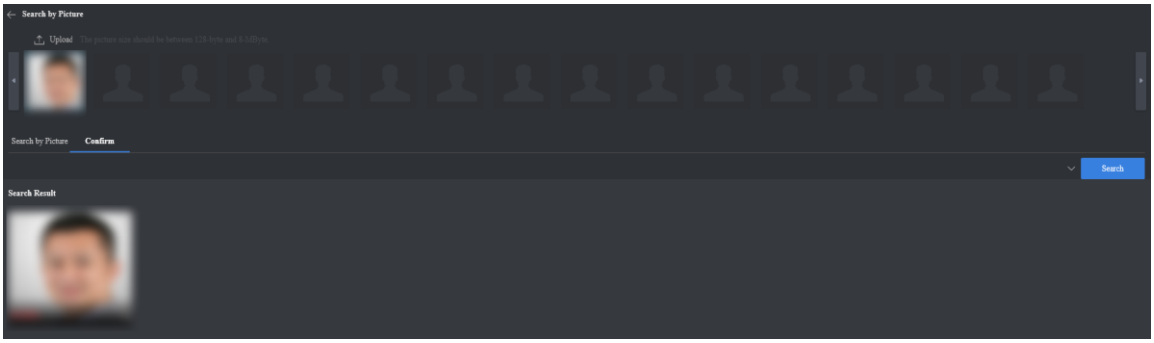

Figure 4-22 Search Result

Step 5 Click searched face picture to view detailed information.

Step 6 (Optional) 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.

4.5 1 V 1 Comparison

Upload two face pictures that are to be compared and compare their similarity degree.

Step 1 Go to **1 V 1 Comparison**.

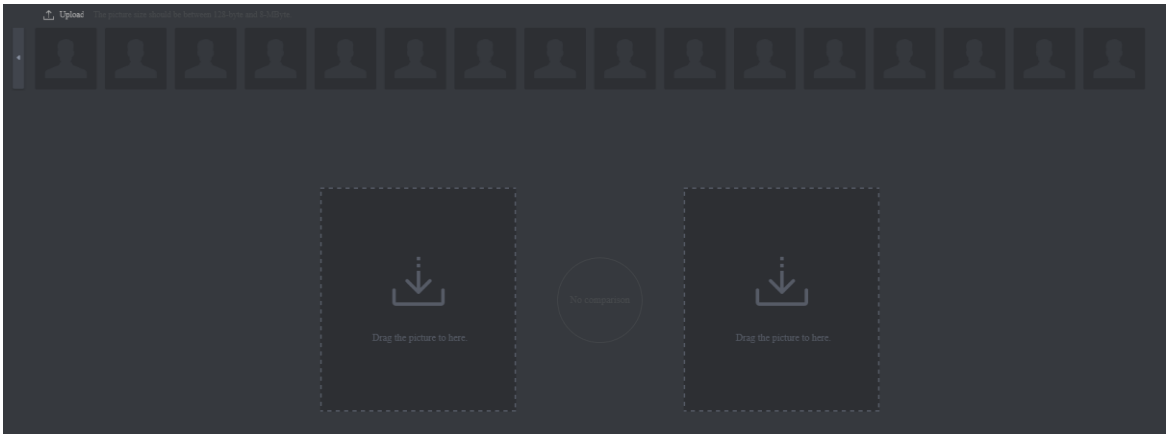

Figure 4-23 1 V 1 Comparison Interface

Step 2 Click **Upload** to upload to be compared face pictures. If the uploaded picture contains multiple faces, and these faces will be uploaded.

NOTE

- The server supports uploading face picture in the format of jpg, jpeg, bmp, tif and png.
- In order to improve comparison accuracy, it is recommended to upload picture with clear face.

Step 3 Drag to be compared face pictures to comparison area, and the server will complete similarity comparison.

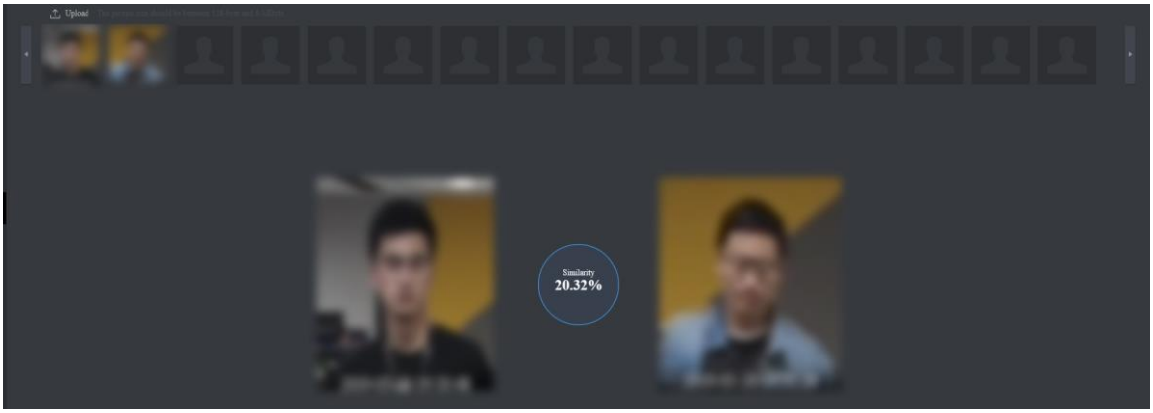

Figure 4-24 1 V 1 Comparison Result

Chapter 5 System Management

5.1 Cluster Management

5.1.1 Delete Node

Before you start:

Node is online and not in cluster.

Step 1 Go to **System Management** > **Cluster Management** > **Node Management**.

Step 2 Check node that needs to be deleted.

Step 3 Click **Delete**, and click **OK** in the popup dialogue box to complete.

5.1.2 Restart Node

Before you start:

Node is online.

Step 1 Go to **System Management** > **Cluster Management** > **Node Management**.

Step 2 Check node that needs to be restarted.

Step 3 Click **Restart**, and click **OK** in the popup dialogue box to complete.

5.1.3 Close Node

NOTE

After closing node, the server can be switched on by pressing power button only, and it does not support switching on in long distance.

Before you start:

Node is online.

Step 1 Go to **System Management** > **Cluster Management** > **Node Management**.

Step 2 Check node that needs to be closed.

Step 3 Click **OFF**, and click **OK** in the popup dialogue box to complete.

5.1.4 Add to Cluster

Add new node to cluster and this will enhance cluster’s capacity.

Before you start:

New node has been added.

Step 1 Go to **System Management** > **Cluster Management** > **Cluster Management**.

Step 2 Click **Add to Cluster**.

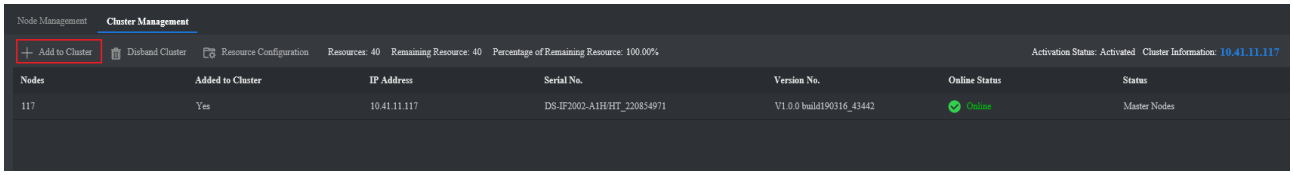

Figure 5-1 Click Add to Cluster

Step 3 Check node that needs to be added to cluster, and click **Next**.

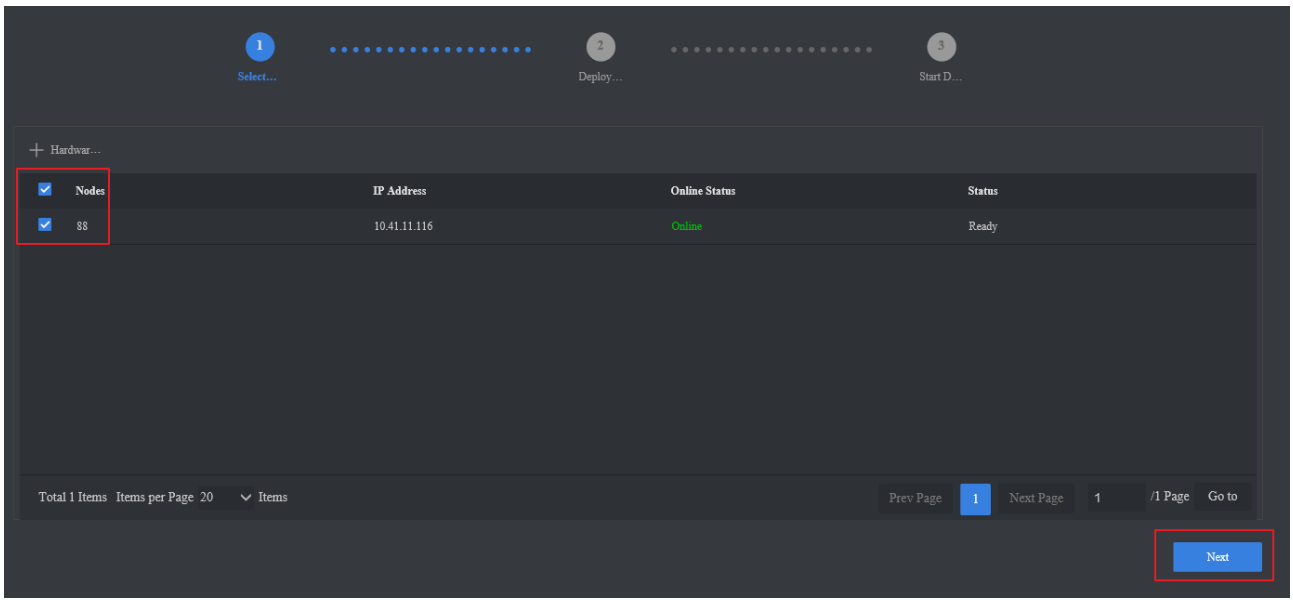

Figure 5-2 Check Node

Step 4 Click **Start Deploying**, and click **OFF** to close after deployed.

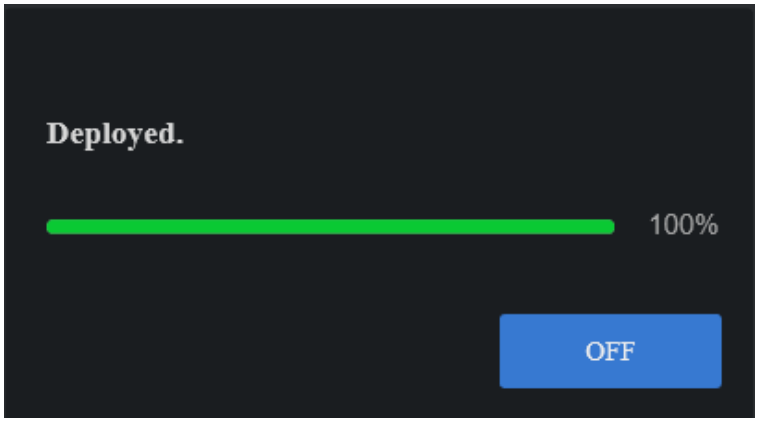

Figure 5-3 Deployed Interface

5.1.5 Disband Cluster

Step 1 Go to **System Management** > **Cluster Management** > **Cluster Management**.

Step 2 Click **Disband Cluster**.

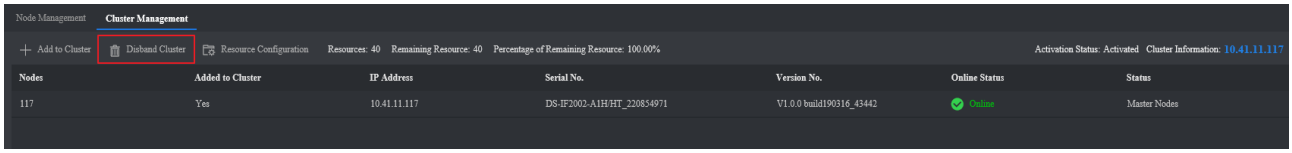

Figure 5-4 Disband Cluster

Step 3 Click **OK** to disband.

5.2 Operation and Maintenance

5.2.1 Check Hardware Status

It allows you to check information about CPU, memory, disk, GPU and etc.

Step 1 Go to **System Management** > **Operation and Maintenance** > **Hardware Status**.

Step 2 Click  in **Details** list.

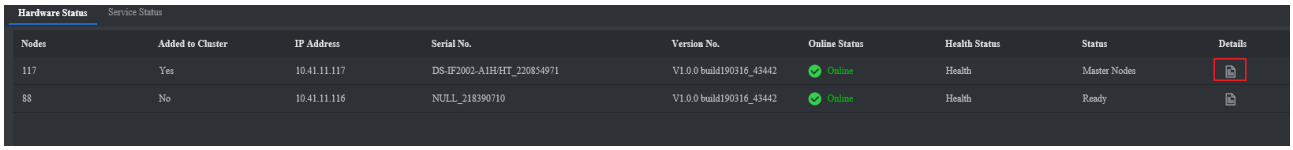

Figure 5-5 Hardware Status Interface

Step 3 Click tabs to check different hardware status.

5.2.2 Check Service Status

It allows you to check MongoDB, zookeeper, kafka and other service status.

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

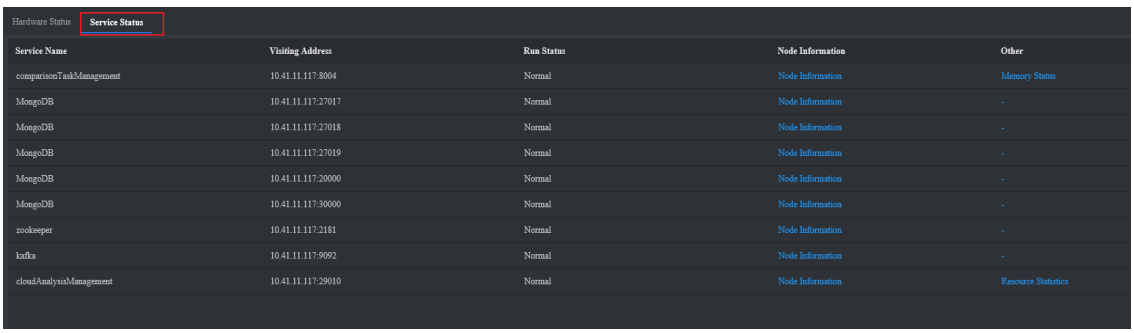

Figure 5-6 Service Status Interface

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

NOTE

- Node Information: it refers to the node of current service.
- Memory Status: it refers to the overall scale of memory, loaded data quantity, total number of dynamic library and captured duration.
- Resource Statistics: It refer to the total resource quantity and remaining resource.

5.3 System Configuration

5.3.1 General Configuration

You do not need to set any parameters, and just use the default ones.

NOTE

The server enables device filter function by default, and you can access to the server via its IP address only. If you have configured port mapping, please disable the device filter function in order to access to the server normally.

5.3.2 Service Configuration

It supports sending task analysis results to configured address.

Before you start:

Obtain IP address, port or URL.

Step 1 Go to **System Management** > **System Configuration** > **Service**.

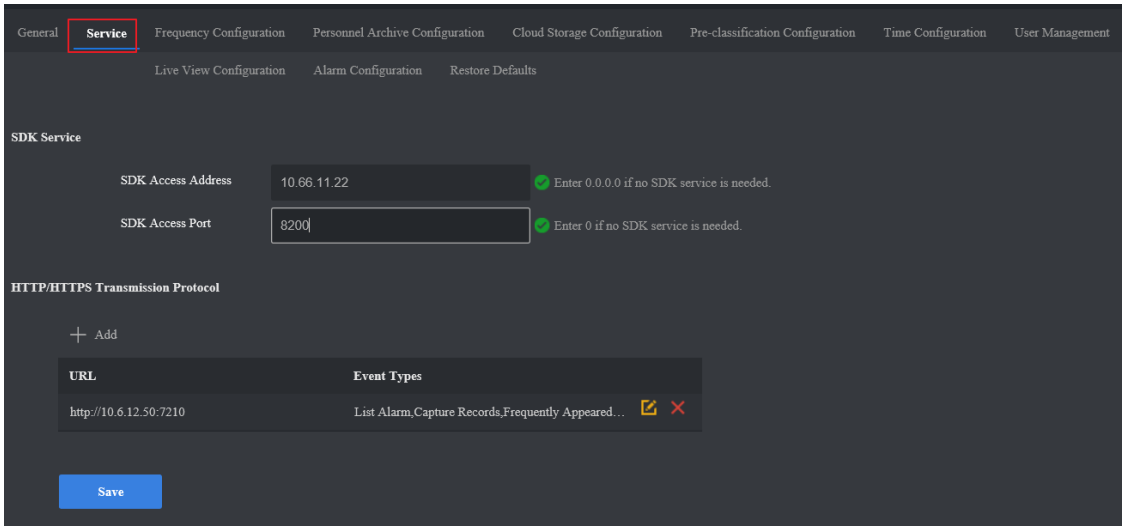

Figure 5-7 Service Configuration Interface

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

- SDK Service: it supports sending task analysis results to configured address via SDK protocol.
- HTTP Transmission Protocol: it supports sending task analysis results to configured address via HTTP protocol. Task analysis task includes list alarm information, capture information, and frequency alarm information.

Step 3 Click **Save** to save.

5.3.3 Pre-Classification Configuration

It pre-classifies personnel in list library to speed up the process of searching by picture and confirming identification.

Step 1 Go to **System Management** > **System Configuration** > **Pre-classification Configuration**.

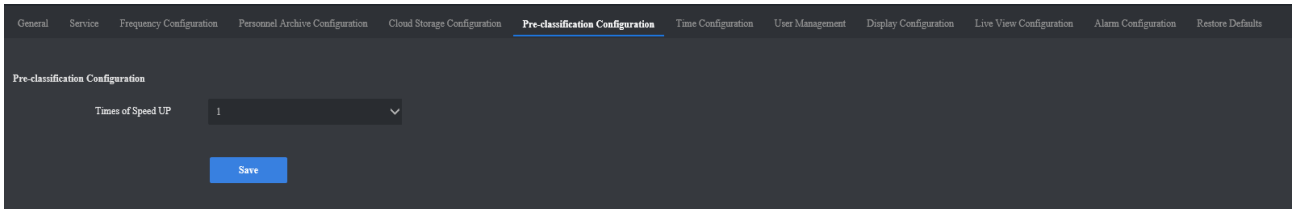

Figure 5-8 Pre-classification Configuration Interface

Step 2 Set **Times of Speed Up** according to actual demands, and click **Save**.

5.3.4 Time Configuration

It is used to synchronize the server time with NTP server time, or synchronize it manually.

Before you start:

If you select NTP, you should obtain NTP server IP address and its port first.

Step 1 Go to **System Management > System Configuration > Time Configuration**.

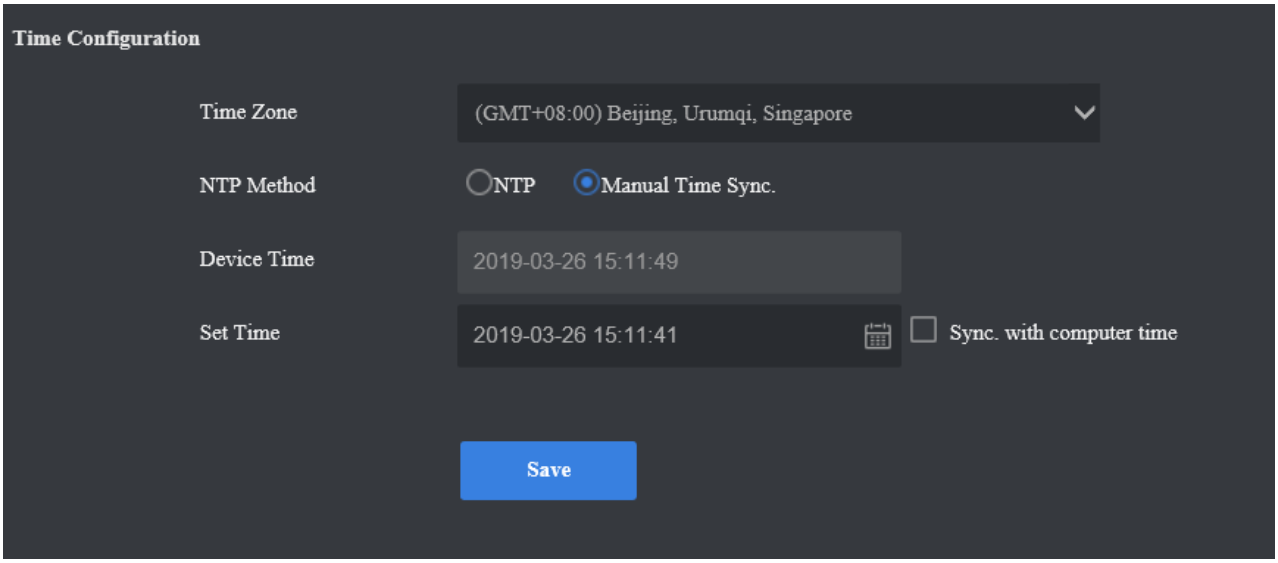

Figure 5-9 Time Configuration Interface

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

Step 3 Click **Save** to complete.

NOTE

Check **Sync. with computer time**, and the service time will be the same with that of the computer.

5.3.5 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. The server supports adding 32 users at most.

Step 1 Go to **System Management** > **System Configuration** > **User Management**.

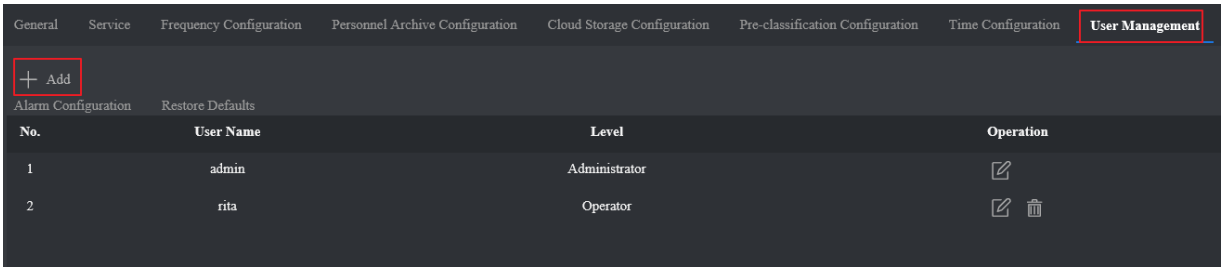

Figure 5-10 User Management Interface

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

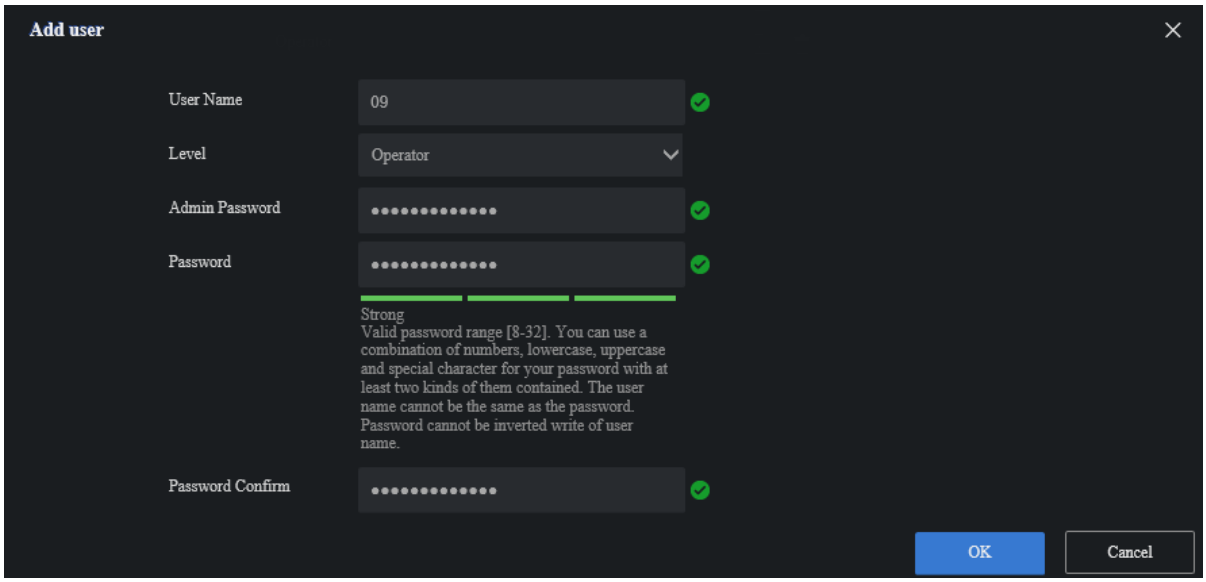

Figure 5-11 Add User

Step 3 Click **OK** to complete.

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.

5.3.6 Display Configuration

Purpose:

It is used to configure the search conditions for smart search function. For example, if you do not enable **Display Gender**, and there will be no gender option among search conditions in smart search interface.

Step 1 Go to **System Management** > **System Configuration** > **Display Configuration**.

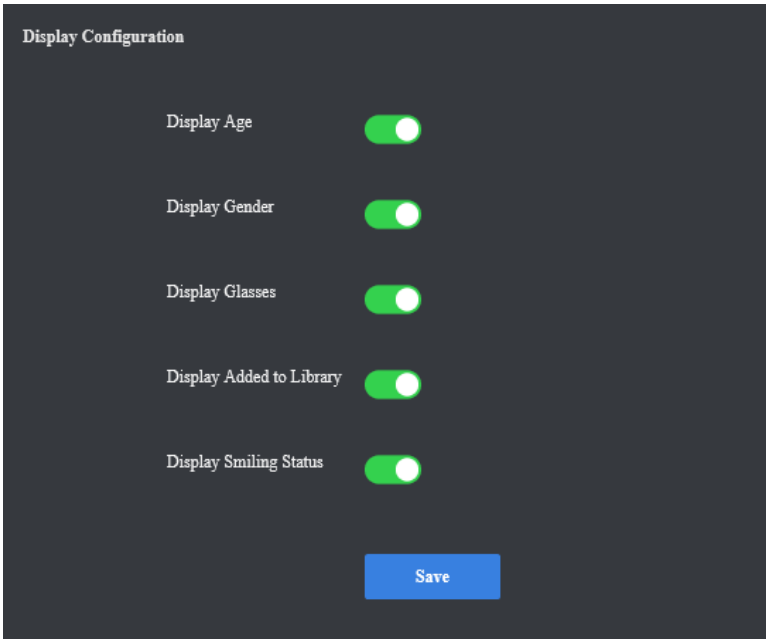

Figure 5-12 Display Configuration Interface

Step 2 Click , or to enable or disable displaying according to actual demands.

Step 3 Click **Save** to complete.

NOTE

stands for enabling displaying, and stands for disabling displaying.

5.3.7 Live View Configuration

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

Step 1 Go to **System Management** > **System Configuration** > **Live View Configuration**.

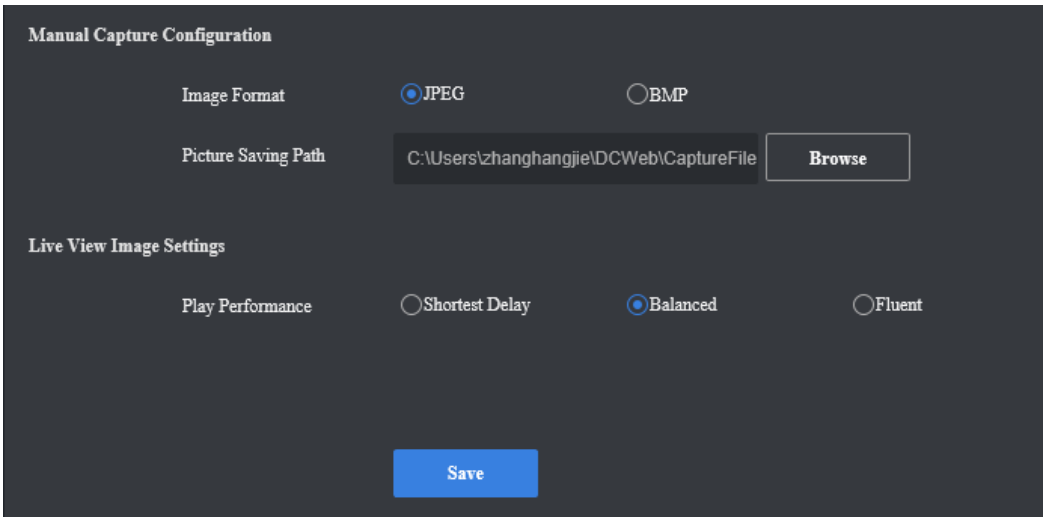

Figure 5-13 Live View Configuration Interface

Step 2 Set live view parameters.

- Manual Capture Configuration: it sets the image format JPEG or BMP, and picture saving path.
- Live View Image Settings: it sets the play performance of live view. It is recommended to use the default value.

Step 3 Click **Save** to complete.

5.3.8 Alarm Configuration

It enables alarm sound and popups, sets alarm popups type and alarm sound for live view interface when the server generating alarm information. Alarm configuration supports customized alarm sound.

Step 1 Go to **System Management** > **System Configuration** > **Alarm Configuration**.

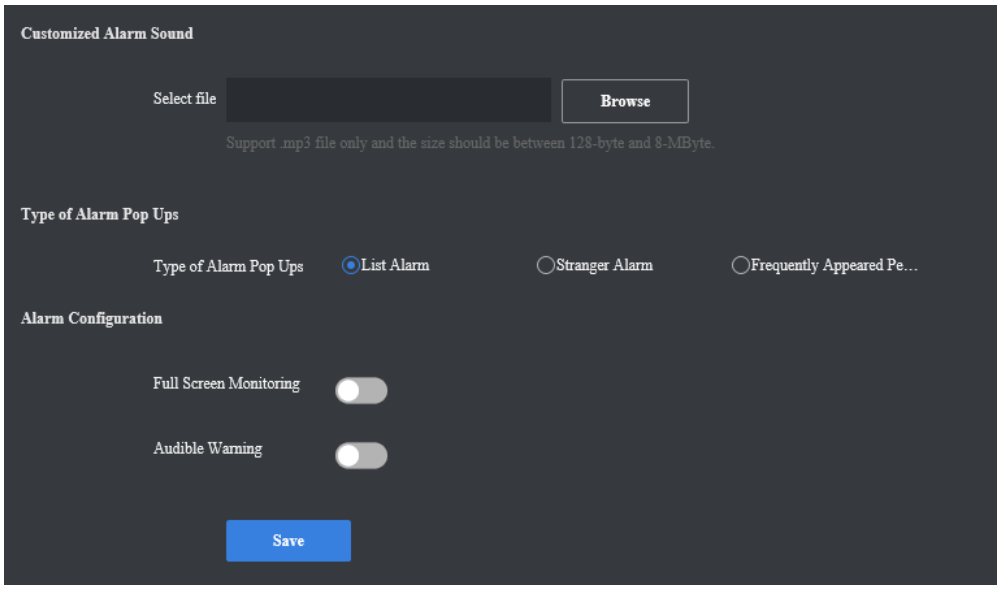

Figure 5-14 Alarm Configuration Interface

Step 2 (Optional) Click **Browse** to upload customized alarm sound.

Step 3 Enable alarm sound and popups, set alarm popups type and alarm sound according to actual demands.

NOTE

- stands for enabling displaying, and stands for disabling displaying.
- When generating alarm information, you can view alarm popup and audible warning in live view interface.

Step 4 Click **Save** to complete.

5.3.9 Restore Defaults

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.
- Default: restore all parameters to the default settings.

Step 1 Go to **System Management** > **System Configuration** > **Restore Defaults**.

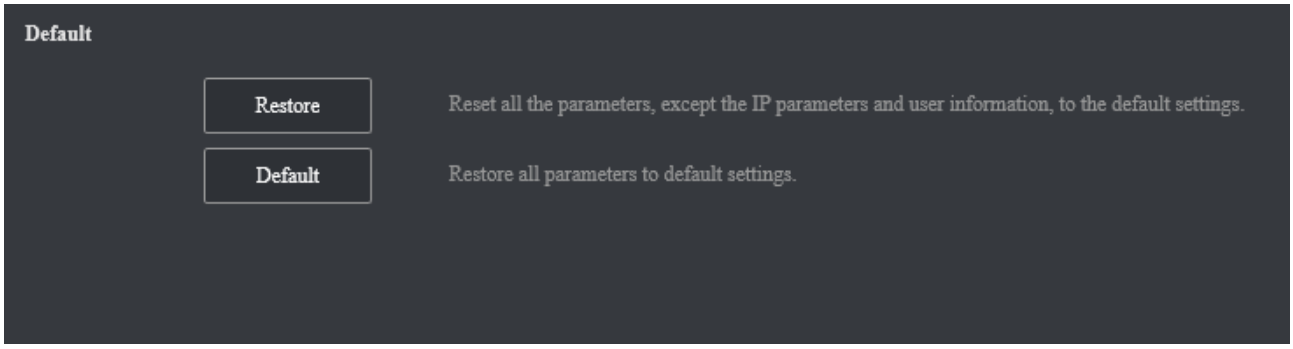

Figure 5-15 Restore Defaults Interface

Step 2 Select restoration type according to actual demands.

NOTE

In the cluster status, restoring defaults cannot be done.

5.4 Log

Log includes running log, alarm log and operation log. The server supports log searching and exporting.

- Running Log: it records server running information.
- Alarm Log: it records server alarm information
- Operation Log: it records server operation information in Web interface.

Step 1 Go to **System Management** > **Log**.

Step 2 Select log type, set search start time and end time, and click **Search** to search.

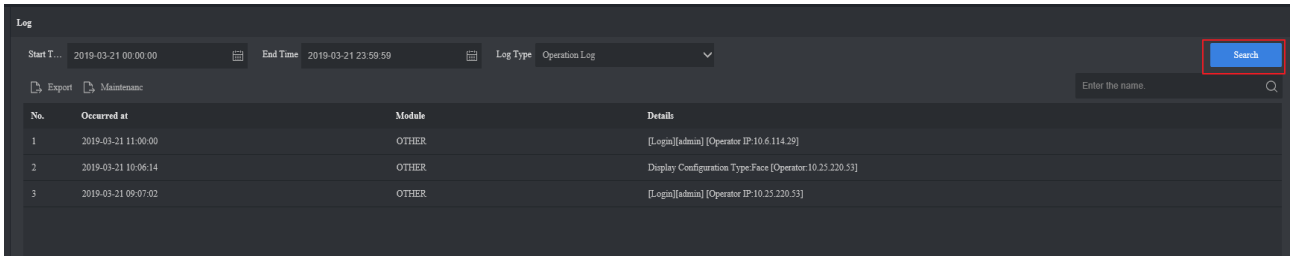

Figure 5-16 Log Interface

Step 3 Input search information in search bar, click to find log information.

Step 4 (Optional) Click **Export** to export searched log, and click **Maintenance** to export maintenance log, which is used by the maintenance staff when maintaining the server.

5.5 Software Updating

It allows to update the software via Web interface.

Before you start:

- The service is online and without any exception.
- Obtain updating files.

Step 1 Go to **System Management** > **Software Updating**.

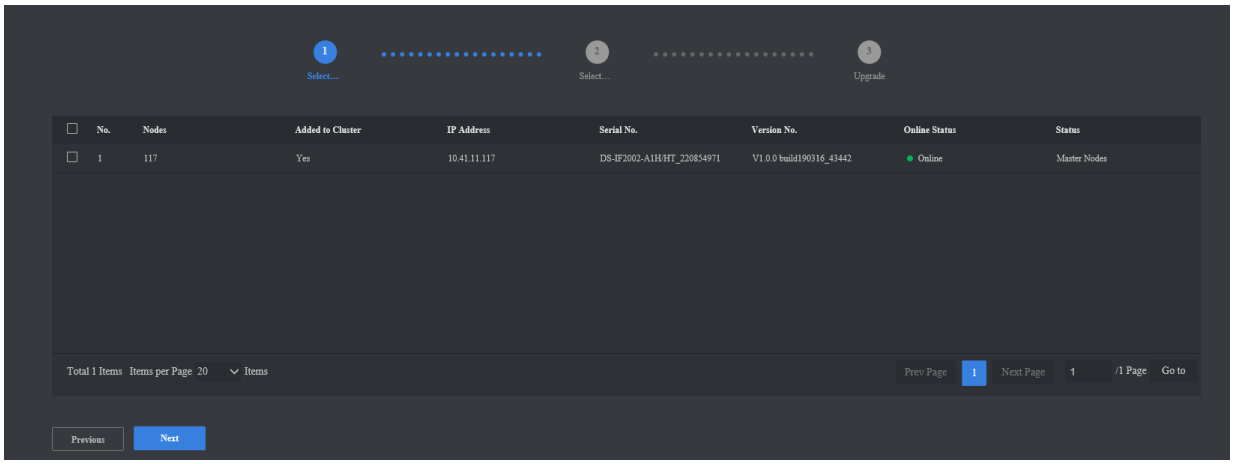

Figure 5-17 Software Updating Interface

Step 2 Check the server to update, and click **Next**.

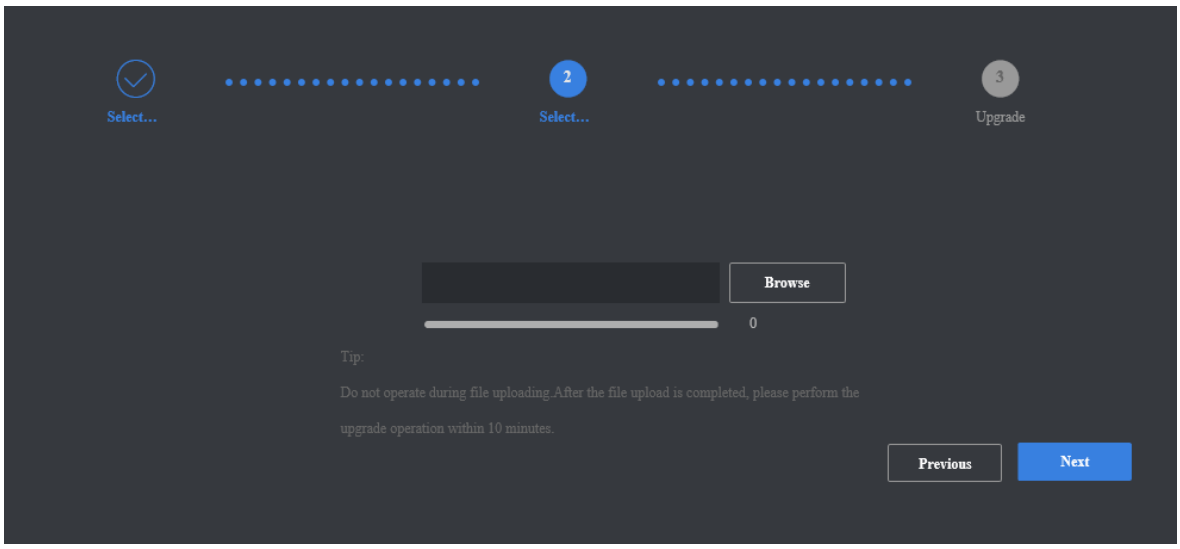

Figure 5-18 Select Updating Files

Step 3 Click **Browse** to upload updating files, and click **Next** after uploaded.

Step 4 Click **OK** to start updating.

NOTE

- Device will reboot after updating.
- After rebooting the device, logging in again is required.

5.6 Online Users

You can check total quantity of users and online users by going to on the top-right corner of the interface.

5.7 Help

You can refer to the help document by going to > **Help Document** on the top-right corner of the interface.

5.8 Version

You can check version information of different modules by going to > **Version Information** on the top-right corner of the interface.

UD14054B