

# Intelligent Fusion Server User Manual

#### **User Manual**

COPYRIGHT ©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

#### All Rights Reserved

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the 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 ( f 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			
	Provides additional information to emphasize or supplement important points of the main text.			
	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.			
	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
1.1 Introduction	1
1.2 Key Features	1
1.3 PC Requirements	1
Chapter 2 Startup	2
2.1 Activate Device	2
2.1.1 Activate via SADP Software	2
2.1.2 Activate via Web Browser	3
2.2 Login	4
Chapter 3 Main Configuration	6
3.1 Modify Node IP	6
3.2 Deploy Micro Video Cloud	7
3.2.1 Install Micro Video Cloud	7
3.2.2 Import License	8
3.2.3 Format Storage Volume	. 10
3.2.4 Create Micro Video Cloud Cluster	. 12
3.2.5 Set Storage Parameters	. 18
3.2.6 Add Domain to Storage Node	. 19
3.2.7 Create Static Pool	. 20
3.2.8 Create Video Pool	. 21
3.2.9 Create Dynamic Pool	. 22
3.2.10 Add Micro Video Cloud	. 24
3.3 Create Cluster	. 25
3.3.1 Add Node	. 25
3.3.2 Create Standalone Cluster	. 26
3.3.3 Create Master and Backup Cluster	. 28
3.4 Add Face List Library	. 30
3.5 Add Personnel Information	. 31
3.6 Create Analysis Task	. 33
3.6.1 Add Camera	. 33
3.6.2 Add Video Record	. 35
3.6.3 Create Real-time Analysis Task	. 36
3.6.4 Create Video Record Analysis Task	. 39
3.7 Add List Arming	. 39
3.8 Enable Frequency Alarm	. 42
3.9 Enable Personnel Archive Configuration	. 43
Chapter 4 Smart Application	. 45
4.1 Live View	. 45

4.2 Alarm Search	
4.2.1 List Alarm	
4.2.2 Stranger Alarm	
4.2.3 Frequently Appeared Person Alarm	
4.3 Personnel Archive	
4.4 Smart Search	53
4.4.1 Normal Search	53
4.4.2 Search by Picture	
4.4.3 Confirm Identification	
4.5 1 V 1 Comparison	
Chapter 5 System Management	59
5.1 Cluster Management	59
5.1.1 Delete Node	59
5.1.2 Restart Node	59
5.1.3 Close Node	59
5.1.4 Add to Cluster	59
5.1.5 Disband Cluster	61
5.2 Operation and Maintenance	61
5.2.1 Check Hardware Status	61
5.2.2 Check Service Status	61
5.3 System Configuration	
5.3.1 General Configuration	
5.3.2 Service Configuration	
5.3.3 Pre-Classification Configuration	
5.3.4 Time Configuration	63
5.3.5 User Management	64
5.3.6 Display Configuration	65
5.3.7 Live View Configuration	
5.3.8 Alarm Configuration	67
5.3.9 Restore Defaults	
5.4 Log	
5.5 Software Updating	
5.6 Online Users	
5.7 Help	
5.8 Version	

# 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 <u>http://overseas.hikvision.com/en/</u>, 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.

## 

- 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.

SADP	¥-									0 _ D ×
Total num	ber of online devices: 9							Export	Refresh	Activate the Device
• 1 ID	•   Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Pa	ort   Device Serial	No.	
001	25-409032-2	Active	10.16.6.20	8000	VL1064/108.	10.16.6.254	80	25.408307.2	IL21MHUDH	
002	25-698225-A	Active	10.16.6.21	8000	VLLIbuly 1886.	10.16.6.254	80	D5-008203, 4	1.0.0000	4
003	DS-KINEDS-AL	Active	10.16.6.213	8000	V5.1.0640/1012-	10.16.6.254	N/A	D5-628028-4	0111374	
004	05-15409-6425	Active	10.16.6.179	8000	VL1556-04100.	10.16.6.254	N/A	24 2008 10	>	The device is not activated
005	05-15406-718NG	Active	10.16.6.127	8000	1220644387	10.16.6.254	N/A	11.1008-01	PACTOARTYPA	The device is not activated.
006	UNIONN OF/ICE-TITE	Active	10.16.6.250	8000	V5435uile 1812.	10.16.6.254	80	20411803	A40340276	
~	007			4	Inacti	ve		192.168.1	L.64	
009	05-1950P4-045420W	<sup>Acti</sup> Se	lectina	activ	ve devid	e.10.16.6.254	80	05-202094-8	6,0000400	You can modify the network parameters after the device activation.
						Inpu pass	t ar wo	nd con rd.	firm	New Passmord:
									,	Activate

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.

Activate		
User Name	admin	
Password	•••••	0
	Strong	
	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	•••••••	0
	O	ζ

Figure 2-2 Activation Interface

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

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

### 

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.



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.





## 

- 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.

[root@lhor ~]#
[root@Thor ~]# ifconfig
<pre>bond0: flags=5443<up,broadcast,running,promisc,master,multicast> mtu 1500</up,broadcast,running,promisc,master,multicast></pre>
inet 10.41.11.117 )netmask 255.255.255.0 broadcast 10.41.11.255
inet6 fe80::aelf:6bff:fe6c:aa86
ether ac:1f:6b:6c:aa:86
RX packets 8018823 bytes 9555987445 (8.8 GiB)
RX errors 0 dropped 493743 overruns 0 frame 0
TX packets 2437740 bytes 716189458 (683.0 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 Is and press Enter to check the configuration file of network interface card.

[root@Thor ~]# [root@Thor ~]# cd	∕etc∕sysconf	ig/network-scri	pts∕	
<u>[root@Thor networ</u>	k-scripts]# 1	S		
ifcfg-bond0	if down-bnep	ifdown-post	ifup	ifup-ipv6
ifcfg-enp129s0f0	ifdown-eth	ifdown-ppp	ifup-aliases	ifup-isdn
ifcfg-enp129s0f1	ifdown-ippp	ifdown-routes	ifup-bnep	ifup-plip
ifcfg-lo	ifdown-ipv6	ifdown-sit	ifup-eth	ifup-plusb
ifdown	ifdown-isdn	ifdown-tunnel	ifup-ippp	ifup-post
[root@Thor networ	k-scripts]#			

Figure 3-2 Check Configuration File

## 

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.

DEVICE=bond0	
BOOTPROTO=static	
DONGING_MASTER=yes	
ONBOOT=yes	
TYPE=bond ing	
IPADDR=10.66.112.90_	
NETMASK=255.255.255.0	
GATEWAY=10.66.112.254	
DNS1=0.0.0.0	
DNS2=0.0.0.0	
<i></i>	

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.



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.

[root@Thor ~]#(cd /yunstorage/)
<pre>[root@Thor yunstorage]# ls</pre>
install.sh
<pre>shared_vs_centos.bin</pre>

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.

The Installation W	/izard v2.2.4
1 Creating Accour	t Complete
	Manager Info
Manager Account	admin
Login Password	•••••
Confirm Password	•••••
	Strong
	Create

Figure 3-9 Create Account

HikCStor Management System	
	User Login
6000.	User Name
10000	admin
Source at 240	Password
	Login

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

Figure 3-10 Login Interface

### Step 4 Click Apply License.

Notice	×
License is not authorized. Please export the license application file and send it to the manufacturer.	
Import License Apply License	

Figure 3-11 Click Apply License

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

Branch Company		Project Name	
Applicant Name		Contact	
Description	whhik temporary license		
	Export Application		

Figure 3-12 Click Export Application



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 <a href="mailto:chenshengli@hikvision.com.cn">chenshengli@hikvision.com.cn</a> or <a href="mailto:zhangle1@hikvision.com.cn">zhangle1@hikvision.com.cn</a> via email for applying license file.
- Import License
- Step 1 Go to the home page of HikCStor Management System.

#### Step 2 Click Import License.

Notice	×
License is not authorized. Please export the license application file and send it to the manufacturer.	
Import License Apply 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.

Max Storage Ca	300000 TB	Max Point Posit	1000000	
	Import License File			
Impor	t License File		×	
	License File Choose File	No file chosen		
		ОК	Cancel	

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.

The Installation Wizard V2.2.4								
1 Creating Account	nt 2 Complete							
	Manager Info							
Manager Account	admin							
Login Password	•••••							
Confirm Password	•••••							
	Strong							
	Create							

Figure 3-15 Create Account

Step 3	Input the	User Name	and Password.	and click <b>Login</b> .
eccp e	inpactice.	••••		

Storage Node Management System	
	User Login
	User Name
	admin
	Password
	Login

Figure 3-16 Login Interface

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

н	ome	Page	Device	System	Info Sea	arch Info	Log				
St	Storage Volume SAN Configuration NAS Configuration Local OS Disk										
System Format 🛛 🚿 Format Storage Volume 🛛 🗙 Delete Storage			te Storage Volume								
			D	evice ID	÷	Device Name 🕴	CVS Serial No. 🔶	Device Type 🛊	Formatting Status 🕴	Device Status 🕴	Online Status 🕴
1		]	2b9240-3fc3-1	1e9-ac84-ac1f6b6c	aa86	/dev/sdd	AC01F06B06C0AA086-1	DISK	Formatted	Normal	Online
2		17162cd0-3fc4-11e9-93c8-ac1f6b6caa86 /dev/sde		/dev/sde	AC01F06B06C0AA086-1	DISK	Formatted	Normal	Online		
3		000	00000-0000-0	000-0000-0000000	00000	/dev/sdb	AC01F06B06C0AA086-1	DISK	Not Formatted	Normal	Online

Figure 3-17 Select Storage Volume

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

Format Storage Volume	ж
<b>Note:</b> Formatting storage volume will delete all data on the device, be careful to perform this step.	
Format Force Non-forced Rapid Force	
Info Block Size 128 KB	
Data Block Size 64 MB	
OK Canc	el

Figure 3-18 Format Storage Volume

Notice					
Formatting storage volume /dev/sdb succeeded.					
Close					

Figure 3-19 Formatting Completed

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.

## 

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.

Select Node         Cloud ID light-cloud       Please make sure the system time of all nodes in cluster are the same as the external standard time.         IP Address       Host Name       System Time       Status
IP Address     Host Name     System Time     Status
IP Address Host Name System Time Status
2 10.41.11.117 Thor 2019-03-18 15:59:51 Online Refresh Modify Host Nar

Figure 3-22 Click Establish Cluster

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

Home Page	Cluster	Virtualizing Sto	rage Access S	ystem Log					
Cluster List C	Cluster List CVM Protocol Gateway Cluster Parameters Address Mapping List Service Status								
🖒 Close Cluster	O Close Cluster + Expand Cluster Set IP Modify Cloud ID								
(	Cloud ID  🔶	Cloud Type	IP Address	Serial No.	Status 🕴	Created Time	Modification Time	Cloud Version 🕴	
1 🗆 li	ght-cloud	Micro Video Cloud	10.41.11.117	AC01F06B06C0AA086	Initialized	2019-03-18 16:00:22	-	2.2.4	

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.

The Installation W	/izard	V2.2.4
1 Creating Accour	t 2 Complete	
	Manager Info	
Manager Account	admin	
Login Password	•••••	
Confirm Password	•••••	
	Strong	
	Create	

Figure 3-24 Create Account

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

HikCStor Management System	
	User Login
	User Name
10000	admin
the state of the state	Password
	··········
	Login

Figure 3-25 Login Interface

Step 4 Click Cluster Deployment.

Welcome	e to HikCStor Man	agement System	n!			
Cluster Description						
<ul> <li>Current cluster sys</li> <li>Current cluster sys</li> </ul>	tem is not established. <sup>1</sup> tem is not established. I	You can click on a key Please click the back b	deployment button fo outton to establish it	or cluster deployment. Cluster Deployment	ClickOnce Deployment	
Applications	<b>~</b>	品		*	Ê	
Cluster	Virtualization	Storage	Access	System	Log	

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.

Clu	ister					
Se	elect Node Ro	ole Configuration				
	IP Address 10.15.1	I17.77 Pl	ease make sure the system tir ster are the same as the extern	ne of all nodes nal standard tir	in cl ne. Sync	hronization Refresh
	IP Address	Host Name	System Time	Status		
V	10.41.11.117	Thor	2019-03-22 16:40:46	Online	Refresh	Modify Host Name
~	10 41 11 116	There	2010 02 22 16:42:12	0-11	Refresh	Modify Host Name
•	10.41.11.110	THOP	2019-03-22 16:42:12	Online	Delete	
~	10 15 117 77	Ther	2010 02 22 16:47:12	Opline	Refresh	Modify Host Name
•	10.13.117.77	THO	2019-03-22 10:47:15	Onine	Delete	
					Resele	ct Cluster Mode Next

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.

	IP Address	Host Nam	Notice	×	itus		
~	10.41.11.117	Thor	notice		ine	Refresh	Modify Host Name
~	10.41.11.116	Thor	Synchronizing node 10. 10.41.11.116, 10.15.1 succeeded.	.41.11.117, 17.77 time	ine	Refresh Delete	Modify Host Name
~	10.15.117.77	Thor		Close	ine	Refresh Delete	Modify Host Name

Figure 3-29 Synchronize Time

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

Cluster				
Select Node	Role Configuration			
Virtual IP Address	10.41.11.180	Detect	Cloud ID	
TD Addrocc	Host Name			Role
IF Address	nost nume	Notice	×	Observer Node
10.41.11.117	q11			
10.41.11.116	w22	IP address 10.4	1.11.180 available.	
10.15.117.77	Thor		Close	
			Reselect Cluste	r Mode Previous Establish Cluster

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.

Cluster			30
Select Node	Role Configuration		
Virtual IP Address	10.41.11.180 👔 Dete	ct Cloud ID light-clo	ud
TD Address	Host Name	R	ble
IP Address	HOST Name	Service Node	Observer Node
10.41.11.117	q11	$\checkmark$	
10.41.11.116	w22	$\checkmark$	
10.15.117.77	Thor		
		Reselect Cluster M	lode Previous Establish Cluster

Figure 3-31 Create Cluster

### 3.2.5 Set Storage Parameters

### 

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.

CVM IP Address	10.41.11.117	CVM Port No.	6022
NTP Server IP Address	0.0.0.0	Synchronization Interval	1440 min
Max Write Video	400	Max Read Video	200
Max Write Picture	600	Max Read Picture	400
Max Write Additional Info	400	Max Read Additional Info	200
Max Write File	1000	Max Read File	1000
Max Write	800	Max Read	256
Cloud ID	light-cloud	Image Modeling	⊖ On ● Off
Video Transcoding	● On ○ Off	Video Fragment	⊖ On  ● Off
Image Accelerate	● On ○ Off	Accelerate Type	Memory Accelerate
	Set CVS Parameters		

Figure 3-32 Set Storage Parameters

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

[root@Thor ~]	# free -g					
	total	used	free	shared	buff/cache	available
Mem:	125	6	110	Θ	8	117
Swap:	7	Θ	7			
I LOTI I						

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.

Home Pag	je Cluster	Virtualizing	Storage	Access	System	Log	
Domain Mana	agement Group	o Management User	Management R	esource Pool M	anagement E	Bucket Manageme	nt
+ Create	Modify	K Delete 💿 View CV	Add CVS	× Remove	e CVS	w Resource Pool	
	Domain ID 🍦	Domain Name	¢ CVS N	lo. 🕴 👘 Tota	al Space (TB)	Total S	pace of Online Device (TB)
					No	results match yo	our criteria.

Figure 3-34 Create Domain

Step 3 Input Domain Name and click OK.

Step 4 Check created domain, and click Add CVS.

Do	main Mar	nagement Gr	oup Managem	ent User Mana	agement	Resou	rce Pool Managemen	it Bu	cket Management				
4	Create	C Modify	🗙 Delete	• View CVS	+ Ad	d CVS	X Remove CVS	👁 View	Resource Pool				
		Domain ID	¢ De	omain Name	¢	CVS No.	Total Space (	(тв) 🔅	Total Space of Onlin	e Device (TB)	¢	Free Space (TB)	Domain Description
1		744324518		light		0	0		0			0	-

Figure 3-35 Check Created Domain

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

ld CVS							
V	Serial No.	IP Address	Domain ID	Online Status	Node Status	CPU Consumption (%)	IO Consumption (%)
1	AC01F06B06C0AA086-1			Online	Normal		0.00
<							>

Figure 3-36 Add CVS

## 3.2.7 Create Static Pool

### 

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.

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.

#### Table 3-1 Parameter Setting

Create				ж
Domain ID	563798794		Select	
User Name	admin		Select	
User Permission	Read / -	Read / Write		
Resource Pool Name	staticpool			
Resource Pool Type	Picture		~	
Picture Acceleration?	Accelerate		~	
Storage Mode	Dispersed		~	
Overwrite Mode	Not		~	
Resource Pool Cycle	0		Day	
Resource Pool Capa	300		GB	0
Max Locking up Att	10		%	
			C	Cancel

Figure 3-37 Create Static Pool

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.

Create			X
Domain ID	563798794	Select	
User Name	admin	Select	
User Permission	Read / - Read / Wri	te	
Resource Pool Name	videopool		
Resource Pool Type	Video	¥	
Storage Mode	Centralized	•	
Overwrite Mode	Capacity	•	
Resource Pool Cycle	0	Day	
Resource Pool Capa	100	GB 🚯	
Max Locking up Att	10	%	
		ОК	Cancel

Figure 3-38 Create Video Pool

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.

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.

Table 3-3 Parameter Setting

Create					ж
Domain ID	563798794		Select		
User Name	admin		Select		
User Permission	Read / - R	ead / Write			
Resource Pool Name	dynamicppol				
Resource Pool Type	Picture		~		
Picture Acceleration?	Accelerate		~		
Storage Mode	Dispersed		~		
Overwrite Mode	Capacity		~		
Resource Pool Cycle	0		Day		
Resource Pool Capa	5		GB		
Max Locking up Att	10		%		
			ОК	Can	cel

Figure 3-39 Create Dynamic Pool

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.

General	Service	Frequency Configuration	Personnel Archive Configuration	Cloud Storage Configuration	Pre-classification Configuration	Time Settings	User Management
+ Add	n Dele					Defaults	
	Smart Storag	ge Unit	IP Address	Port	Online Status	Туре	

Figure 3-40 Set Cloud Storage

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

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.

Smart Storage Unit	nel Storage Costiguistica.	×
Name	CVM	
Smart Analysis Unit Type	Micro Video Cloud 🗸	
Smart Storage Unit IP	10.41.11.117	
Dynamic Resource Pool ID	694274779	
Static Resource Pool ID	747434518	
Video Resource Pool ID	799820113	
Port		
User Name	admin	
Password	•••••	
Visit KEY	PK5Bz234w370h6h93e0wd829zMU39BR2	
Encryption KEY	••••••	
Download Port	6120	
	ОК Са	ancel

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.

### 

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.

Node Management Clust	er Management			
+ Add 🗂 Delete	C Restart ( <sup>1</sup> ) OFF			
Nodes	Added to Cluster	IP Address	Serial No.	



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

Nodes		×
Name	195	0
Nodes IP	10.33.34.195	0
Port	8088	
User Name	admin	0
Password	••••••	ø
	OK Ca	ncel

Figure 3-43 Input Nodes Information

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.

( Se	lect	2 Deploy	start D	
Nodes	IP Address	Online Status	Status	
117	10.41.11.117		Ready	
Total 1 Items Items per Page	20 V Items		1 Next Page 1	/1 Page Go to
				Next

Figure 3-45 Select Nodes

Step 3 Click Start Deploying to deploy.

Søleet	2 Deploy.	. Start D	
zookeeper	Nodes	IP Address	
kafka	<b>1</b> 17		
MongoDB			
appServer			
	Total 1 Items Items per Page 20 🗸 🗸	Items Prev Page 1 Next Page	1 /l Page Go to
			Previous Start Deploying

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.

Node Management	Cluster Management				
					tivation Status: Activated
					Online Status
					📀 Online
		Resource Configuration		×	
		Face Picture Analysis Path 2			
		Face Video Analysis Path 1			
			OK	Cancel	

Figure 3-48 Allocate Resource

### 

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.

		1.		2			3		
🗹 No	odes		IP Address		Online Status		Status		
<b>2</b> 19			10.33.34.195				Ready		
<b>2</b> 19	96		10.33.34.196				Ready		
Total 2 It	ems Items per Paş	ge 20 🗸 Iten				Page 1		/1 Page	Go to
									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.

	Select	•••••	Deploy	3 Start D
zookeep		Virtual IP 10.33.34.196		
kafka		Nodes	IP Address	
MongoD	в	✓ 195		
appServe		2 196	10.33.34.190	
		Total 2 Items Items per Page 20	) 🗸 Items Prev Page 📘	Next Page 1 /1 Page Go to Previous Start Deploying

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.

				Activation Status: A
				Online Status
				_42595 😒 Online
				_42595 🤡 Online
	Resource Configuration		×	
	Face Picture Analysis Path 4			
	Face Video Analysis Path 0			
		OK	Cancel	

Figure 3-53 Allocate Resource

## 

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.

+ Add passerby_lib Non-arm Library Note:	+ Add passerby_lib Non-arm Library Note: 0	List Library		
passerby_lib Non-arm Library Note:	passerby_lib Non-arm Library Note:	+ Add		
<b>⊥</b> 0	<b>≗</b> 0	passerby_lib Note:		
		2 0		

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.

Add Face Picture Library		×
* List name	Blacklist	0
* List Library Type	Arm Library	~
* Name List Attribute	Blacklist Library	~
Note Information		
	OK	Cancel

Figure 3-55 Add Face List Library

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

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

### 

- 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.

+ Add C Batch Oper.				
	Add Face Record			
		• Name		
		Gender		
		<ul> <li>Birthday</li> </ul>		
		ID Card T		
		ID No.		
		Case info		
	Upload	Tag		
			OK	Cancel

Figure 3-57 Add Personnel Information

### 

- 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 M to modify it, click M to delete it, and M 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.

### 

- 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.

Device Record			
	Add Resource		×
	* Protocol	нк 🗸	
	Device		0
	• IP Add	10.14.96.38	0
	* Port		
	* User N	admin	0
	* Password	••••••	]ø
		ОК	Cancel

Figure 3-58 Add Camera

Step 2 Click **OK** to complete.

Step 3 Click **I**, select **Type** as **Area**, input name, and click **O**K.

Device Record				
to L to				
Administrator-admin				
	Add Organization		×	
	Туре		~	
	Name		ø	
		ОК	Cancel	

Figure 3-59 Add Area

### 

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.

Device Record						
	+ Add 🗂 Delete					Q
Administrator-admin	Camera Name	Туре	IP Address	Port	Arming Status 🗸	

Figure 3-60 Click Add

### 

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**.

Add Camera				×
⊻	Camera Name	Туре	IP Address	Port
	19_Camera 01	Device	10.14.96.38	8000
			Total 1 Items	< 1/1 > >>
			ОК	Cancel

Figure 3-61 Add Camera to Area

### 

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

### 3.6.2 Add Video Record

### 

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 **I** 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.

+ New	🛱 Delete								
	Camera Name	Туре	Status	Progress	Create Time	RunTime	Expected End Time	Advanced Settings	Schedule

Figure 3-65 Task Management Interface

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

▶ 🖬 第 Diviter 🔽 No. Camera Name Type Arming Startus Advanced Settlegs	Schedule
-	
✓ 1 38_Camora 01 Capture Camera Usaraned -	
🖬 2 31,1jCanuer, J Canuers Unernoid +2.04	
	Cancel 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 <a>[e]</a> 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

## 

- 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.

+ Ner	w 🗂 Delete								
	Camera Name	Туре	Status	Progress	Create Time	RunTime	Expected End Time	Advanced Settings	Schedule

Figure 3-69 Click New

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

Enter the keyword. Q	Real-	Time	Video Stru Lo	al Video Structura				
🕨 🔽 😝 Record		No.		Video Record Name	Туре	Arming Status	Advanced Settings	Schedule
				10.14.96.38_01_20190307145618865	Record	Unarmed		-

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 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.

### 

- 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

### 

- 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	5
-----------------------------	---

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.

### 

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

Add Arming							×
* Name	11					0	
* Arming Type	Stranger Arm				~		
* Arming Object	Select the an	ming object.			~		
* Arming Camera	Select the an	ming camera			~		
* Arming Time	00:00:30	-	23:59:59	Threshold	80	%	( <del>)</del>
	Up to 5 periods ca		g by period makes				
Note						0	
	Enter 1 to 64 charad						
				OK			Cancel

Figure 3-72 Set List Arming Parameters

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 **M** 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.

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.

Table 3-6 P	arameter Setting
-------------	------------------

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

Frequency Configuration			
Enable	•		
Camera	38_13020400001310014197888888888 🗸		
List to Filter	Blacklist		
Filtering Threshold	85		
Appeared Times			
Capture Interval(min)			
Similarity	90		
Day Range			
Time Segment	00:00:00 🛗 23:59:59 🛗 🔂		
	Save		

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.

Parameter Name	Description			
Enable	Check Enable.			
Arming Object	Selecting passerl object according	Selecting passerby library is required, and select other arming object according to actual demands.		
Arming Camera	Select camera.			
Threshold	It compares the s and that of face similarity reache classifies the face into the pedestri	similarity between face captured b list library (except passerby library s the configured this threshold, the e picture into real name archive, o an archive.	iy camera ). When the e server therwise,	
Personnel Archive Co	onfiguration			
E	nable	✓		
А	rming Object	Blacklist	~	
А	rming Camera	38_13020400001310014197888888888	~	
т	hreshold	85	0	
		Save		

Table 3-7 Parameter Setting

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

### 

- 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.

Device List * # Device * # Administrator-admin * 2 11 NOT 19_Camera 01		Alarm List	. <b>ict Alarm *</b>
		23	
Face Capture	e capture information.		

Figure 4-2 Double-click Camera

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.
		Since the second
2	Face capture	It captures faces in real time.
		Example: Click it to filter cameras, and the server will display face picture captured by the checked camera.
		interest in the clear all current displayed face picture.
		B: Click it to add face picture to list library.
		Set this face picture as target picture to search picture by picture.
		ERA: Set this face picture as target picture to confirm identification.

#### Table 4-1 Live View Interface Introduction

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

### 

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



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

$\leftarrow$ Normal Search									
Cameras		Start Time		End Time		Age			
Gender		Glasses		Smile		Modeling Status			
								~ *	Search

Figure 4-15 Set Search Conditions

### 

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 is to set this face picture as target picture to search picture by picture. Click is 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.

### 

- 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.

$\leftarrow$ Search by Picture										
1 Upload										
										ŀ
Search by Pict	Confirm									
Cameras			Start Time		End Time		Result Number			
Similarity					Gender		Glasses			
Smile			Collage Picture		Sort					
									~	Search

Figure 4-18 Set Search Conditions

### 

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.





Step 5 Click searched face picture to view detailed information.

Step 6 (Optional) Click is to set this face picture as target picture to search picture by picture. Click is 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.

### 

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.

$\leftarrow$ Search by Picture						
,↑ Upload						_
						ļ
Search by Picture	Confirm					
Search by Picture	Coafirm Blacklist.passerby_lib.strange	Name	Result Number	Similarity 30		
Search by Picture	CoafirmBlacklist, passerby_lib, strange	v Name End Date of Birth	Result Number ID Card Type	Similarity 30 ID No.		
Search by Picture	Coaffirm Blacklistpasserby_lib,strange	r Name End Date of Birth	Renth Number ID Gard Type	Similarity 30 ID No.		

Figure 4-21 Set Search Conditions

## 

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.

Search by Picture     Search by Pict				
▲ Uplead The picture size should be between 128-byte and 8-M.				
11 시시 /				
Search by Picture Confirm				
				∼ Search
Search Result				

Figure 4-22 Search Result

Step 5 Click searched face picture to view detailed information.

Step 6 (Optional) Click is to set this face picture as target picture to search picture by picture. Click is to set this face picture as target picture to confirm identification.

## 4.51 V1 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.

### 

- 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

### 

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.

Node Management Cluster Ma	anagement					
+ Add to Cluster 🏦 Disba	and Cluster 📑 Resource Configuration R	esources: 40 Remaining Resource: 40 Perc	entage of Remaining Resource: 100.00%		Acti	vation Status: Activated Cluster Information: 10,41,11,117
Nodes	Added to Cluster	IP Address	Serial No.	Version No.	Online Status	Status
117			DS-IF2002-A1H/HT_220854971	V1.0.0 build190316_43442	🥪 Online	Master Nodes

Figure 5-1 Click Add to Cluster

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

		Deploy	Start D	
+ Hardwar				
Nodes	IP Address	Online Status	Status	
88	10.41.11.116		Ready	
Total 1 Items Items per Page 20	✓ Items		Prev Page 1 Next Page	1 /1 Page Go to
				Next

Figure 5-2 Check Node

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

Deployed.	100%	
	OFF	



## 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.

Har	dware Status								
No	les	Added to Cluster	IP Address	Serial No.	Version No.	Online Status	Health Status	Status	Details
117				DS-IF2002-A1H/HT_220854971	V1.0.0 build190316_43442	🥪 Online	Health	Master Nodes	B
88					V1.0.0 build190316_43442	🥪 Online	Health	Ready	

#### 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.

Hardware Status Service Status				
Service Name	Visiting Address	Run Status	Node Information	Other
comparisonTaskManagement		Normal		
MongoDB		Normal		
zockeeper		Normal		
kafka				
cloudAnalysisManagement		Normal		

Figure 5-6 Service Status Interface

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

### 

- 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.

### 

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.

General	Service Frequency Co		nel Archive Configuration			
SDK Ser	vice					
	SDK Access Addres	s 10.66.11.22				
	SDK Access Port	8200		Enter 0 if no SDK servio		
НТТР/Н	TTPS Transmission Protocol					
	+ Add					
	URL		Event Types			
	http://10.6.12.50:7210		List Alarm,Capture Record	s,Frequently Appeared 🗹 >		
	Save					

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.

Time Configuration		
Time Zone	(GMT+08:00) Beijing, Urumqi, Singapore	~
NTP Method	ONTP • Manual Time Sync.	
Device Time	2019-03-26 15:11:49	
Set Time	2019-03-26 15:11:41	Sync. with computer time
	Save	

Figure 5-9 Time Configuration Interface

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

Step 3 Click Save to complete.

### 

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.

General Service	Frequency Configuration	Personnel Archive Configuration	Cloud Storage Configuration	Pre-classification Configuration	Time Configuration	User Management
+ Add Alarm Configuration						
No.	User Name		Level		Operation	
1	admin		Administrator		Ľ	
2	rita		Operator		ピ 向	

Figure 5-10 User Management Interface

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

Add user				×
User Name	09	0		
Level	Operator 🗸	~		
Admin Password	•••••	0		
Password	•••••	0		
	Strong 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.	: t		
Password Confirm	•••••	Ø		
			OK	Cancel

Figure 5-11 Add User

Step 3 Click **OK** to complete.



- 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.
Display Configuration	
Display Age	<b>—</b>
Display Gender	•
Display Glasses	<b>—</b>
Display Added to Library	<b>—</b>
Display Smiling Status	<b>—</b>
	Sara
	Jarc

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.



### 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.

Manual Capture Configuration							
Image For	mat	⊙JPEG	OBMP				
Picture Sa	ving Path	C:\Users\zhanghangjie\D0	CWeb\CaptureFile	Browse			
Live View Image Settings							
Play Perfo	rmance	⊖Shortest Delay	<ul> <li>Balanced</li> </ul>	⊖Fluent			
		Save					

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.

Customized Alarn	n Sound			
	Select file		Browse	
Type of Alarm Po	p Ups			
	Type of Alarm Pop Ups	●List Alarm	⊖Stranger Alarm	OFrequently Appeared Pe
Alarm Configurat	ion			
	Full Screen Monitoring			
	Audible Warning			
	Save			

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.



- 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.

Default		
	Restore	Reset all the parameters, except the IP parameters and user information, to the default settings.
	Default	Restore all parameters to default settings.

Figure 5-15 Restore Defaults Interface

Step 2 Select restoration type according to actual demands.

### 

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.

Log					
Start T	2019-03-21 00:00.00	End Time 2019-03-21 23:59:59	Log Type Operation Log		Search
[]} Exp					Q
No.	Occurred at	Module		Details	
1				[Login][admin] [Operator IP:10.6.114.29]	
2				Display Configuration Type:Face [Operator:10.25.220.53]	
3		OTHER		[Login][admin] [Operator IP:10.25.220.53]	



Step 3 Input search information in search bar, click  $\square$  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.

		Select		Salect	Upgrade		
	o. Nodes	Added to Cluster	IP Address	Serial No.	Version No.	Online Status	Status
				DS-IF2002-A1H/HT_220854971	V1.0.0 build190316_43442	• Online	Master Nodes
Total 1 I	tems Items per Page 20 🗸 Items					Prev Page 1 Next Pag	ge 1 /1 Page Go to
Previous	n Next						

Figure 5-17 Software Updating Interface

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

Select	Select		Upgrade
		Browse	
	upgrade operation within 10 minutes.		Previous

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.

### 

- 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  $\bigcirc$  > **Help Document** on the top-right corner of the interface.

## 5.8 Version

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



UD14054B