



Video Cloud Smart Analysis Server

User Manual

About this Document

- This Document 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 Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL,

CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

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

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

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

FCC Conditions

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

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

EU Conformity Statement



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



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

<http://www.recyclethis.info>.



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

Industry Canada ICES-003 Compliance

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

Preface

Applicable Model

This manual is applicable to Video Cloud Smart Analysis Server.

Symbol Conventions

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

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

Safety Instruction

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

Contents

Chapter 1 Introduction	1
Chapter 2 Startup	2
2.1 PC Requirements	2
2.2 Activation	2
2.2.1 Activate via SADP Software	2
2.2.2 Activate via Web Browser	3
2.3 Login	4
Chapter 3 Configuration Wizard	5
3.1 Create Analysis Cluster	5
3.1.1 Add Smart Analysis Unit	5
3.1.2 Create Stand-alone Analysis Cluster	6
3.1.3 Create Master and Backup Cluster	6
3.2 Upload Algorithms	7
3.3 Pre-allocate Resource	8
3.4 Configure Big Data Service Address	9
3.5 Reset Standard	10
Chapter 4 Smart Analysis Unit Management	11
4.1 Add Smart Analysis Unit to Cluster	11
4.2 Disband Cluster	11
4.3 Delete Smart Analysis Unit	11
4.4 Restart Smart Analysis Unit	12
4.5 Power off Smart Analysis Unit	12
4.6 Configure Network Parameters	12
4.7 View Hardware Resource	13
4.9 Check Node Information	14
Chapter 5 GPU Resource Management	15
5.1 Pre-allocate Algorithm Resource	15
5.2 Check Available GPU Resource	15
5.3 Check GPU Resource Allocation	15

Chapter 6 Task Information	17
6.1 Check Task Information.....	17
6.2 Task Data Statistics.....	17
6.3 Check Output Statistics	18
Chapter 7 System Management.....	19
7.1 Basic Settings	19
7.1.1 Configure SDK Service	19
7.1.2 Configure Calculating Pool	19
7.1.3 Configure Management System	19
7.1.4 Configure Face Data Library Capacity	20
7.2 Time Configuration.....	21
7.3 User Management.....	21
7.3.1 Add User	21
7.3.2 Modify Password.....	22
7.3.3 Delete User	22
7.4 Log Management.....	23
7.4.1 Search Log.....	23
7.4.2 Download Maintenance Log	23
7.5 Configure Score Setting.....	23
7.6 Device Maintenance.....	24
7.6.1 Software Updating	24
7.6.2 Restore Defaults	25
7.7 Check Algorithm List.....	25
7.8 Authorization Information	25
7.8.1 Authorization Analysis Capability.....	25
7.8.2 Dongle Information	25
7.8.3 Configure Authorization Address	26
7.8.4 Cloud Storage Configuration.....	26
7.8.5 List Synchronization	26
7.9 Enable Alarm Sound	26
7.10 Help Center	27

7.11 Version Information	27
7.12 Open Source Software License	27
7.13 Logout	27

Chapter 1 Introduction

Video cloud smart analysis server can perform intelligent analysis and extract structured data towards faces, human bodies, vehicles and targeted behaviors in certain pictures and videos. Capable to provide efficient, convenient and professional solutions for such scenarios as entrance and exit, checkpoint and security monitoring point, the video cloud smart analysis server can be widely used in various fields like public security, transportation, judicature, finance, telecommunication, and so on and so forth.

Functions

- Analysis towards faces, human bodies and vehicles in certain pictures and videos.
- Targeted behaviors analysis.
- Pre-allocation of algorithm resource.
- Supports to create analysis cluster(s).
- Supports to check chip details.
- Allowed to configure network parameters of the server remotely.
- Three-tier authority management of administrators, operators and consumers.
- Allowed to record, search and export running, operation and alarm logs.
- Time synchronization by manual operation or through NTP server.
- Supports upgrading remotely.

Chapter 2 Startup

2.1 PC Requirements

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

Table 2-1 PC Requirements

Operating System	CPU	Memory	Resolution	Browser
Microsoft Windows 7, Microsoft Windows 10	Intel® Pentium IV 3.0 GHz or more advanced version	1 GB or larger	1024 × 768 or higher	IE8 to IE11

**Note**

The interface varies from version to version.

2.2 Activation

The server is available only after being activated.

2.2.1 Activate via SADP Software

Before You Start

- Obtain SADP Software from official website.
- The PC and server have been connected to each other on the same network segment.

Steps

1. Install and run the SADP software. The software searches all online devices within the local area network. Device type, IP address, activation status, device serial number and other information are shown in the list.

**Note**

Initial Server IP Address: 192.168.1.64.

2. Check the desired server and set server password in the **Activate Device** window. Click **Activate**.

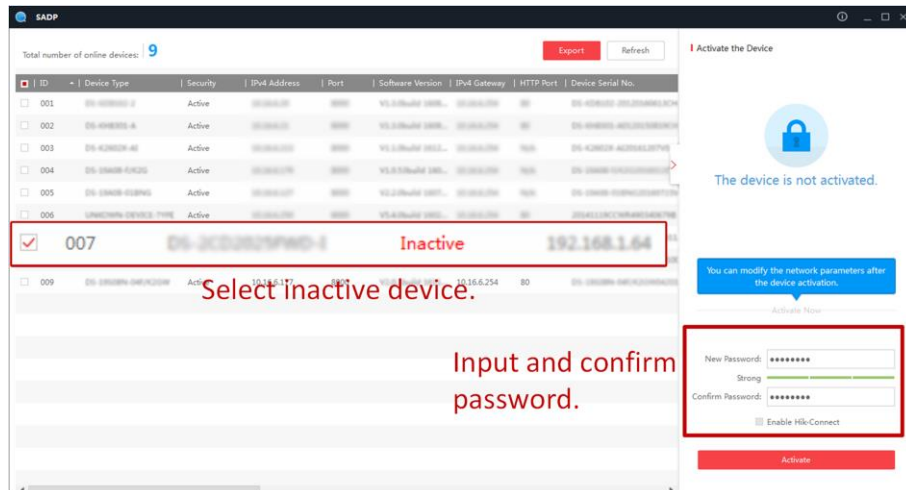


Figure 2-1 Activate Big Data Server

Note

- After server is activated, the **Activation Status** will change to **Active**.
- 8 to 32 characters allowed, including at least 2 of the following types: upper-case letters, lower-case letters, digits, and special characters.
- To protect your privacy and enterprise data, avoid device network security problem, we highly recommend you create a strong password in accordance with security rules.

3. Modify server IP address.

- 1) Select the activated server. Enter IP address, subnet mask and gateway, etc. in the **Modify Network Parameters** window.
- 2) Enter the password and click **Modify**. The popped up **Network Parameters Edited** indicates that network parameters settings take effect.

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, strengthen your own protection. We highly recommend you to assess the network security regularly. If the device is under network security risks, contact with your dealer or the nearest service center.
- In order to increase the security of your product, it is necessary to configure all passwords and other security settings properly. Please be mindful of your user name and password.

2.2.2 Activate via Web Browser

You can activate the server through web browser.

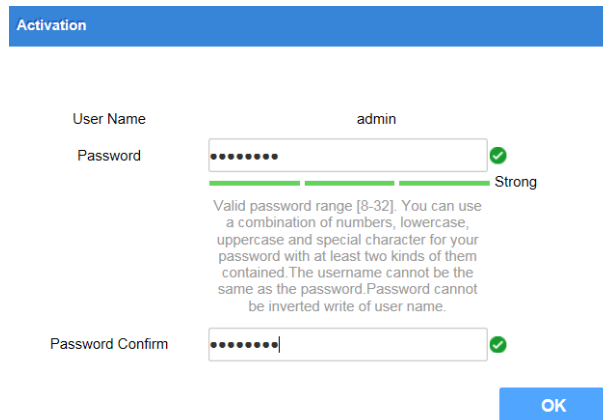
Before You Start

- Ensure that your PC and the server are directly connected.

- Ensure that IP address of the PC changed so it can connect to the server properly.

Steps

1. Open IE browser. Enter IP address of the server in the address bar and press **Enter**.



The image shows the 'Activation' interface of the Video Cloud Smart Analysis Software. It features a blue header with the word 'Activation'. Below the header, there are three input fields: 'User Name' with the value 'admin', 'Password' with masked characters and a green checkmark, and 'Password Confirm' with masked characters and a green checkmark. A green progress bar is visible below the password field, with the word 'Strong' at the end. A text box provides instructions: '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 username cannot be the same as the password. Password cannot be inverted write of user name.' At the bottom right, there is a blue 'OK' button.

Figure 2-2 Activation Interface

2. Enter **Password** and confirm, then Click **OK**.

2.3 Login

You can log in to the video cloud smart analysis server through IE browser.

Before You Start

Obtain IP address of video cloud smart analysis server.

Steps

1. Open IE browser. Enter server IP address in the address bar and press **Enter**.



The image shows the 'Login' interface of the Video Cloud Smart Analysis Software. It features a blue background with a central graphic of a brain surrounded by the words 'Efficient', 'Intelligent', and 'Professional'. On the right side, there is a white login box with two input fields: 'User Name' and 'Password', and a blue 'Login' button. The top left corner of the interface has the text 'Video Cloud Smart Analysis Software' and a cloud icon.

Figure 2-3 Login Interface

2. Enter user name and password.
3. Click **Login**.

Chapter 3 Configuration Wizard

Create an analysis cluster and upload algorithm library for smart analysis of targets in pictures and videos, including faces, human bodies and vehicles.

3.1 Create Analysis Cluster

3.1.1 Add Smart Analysis Unit

Add smart analysis unit(s) to create an analysis cluster.

Before You Start

Ensure that the smart analysis unit is online.

Steps

1. Go to **Service** → **Smart Unit**.
2. Click **Add**.

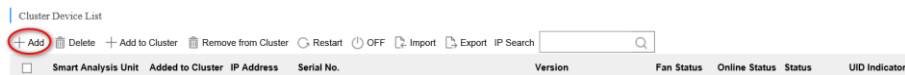


Figure 3-1 Add Smart Analysis Unit

3. Enter **Name** and **Smart Analysis Unit IP**, and keep **Port** as default value.

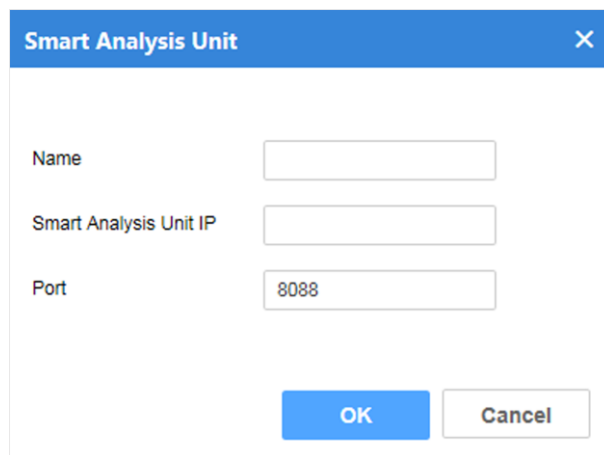


Figure 3-2 Configure Parameters

4. Click **OK**.

Note

The name of each unit cannot be duplicated. Letters, digits and special characters are allowed, excluding `][#~%!\$^&@:;""'"/\+\_`.

3.1.2 Create Stand-alone Analysis Cluster

The stand-alone analysis cluster contains at least one smart analysis unit. There is only one master node in the cluster, and the rest are computing nodes. If the master node is offline, the cluster will not be available.

Before You Start

Ensure that smart analysis units are online and on the same subnet.

Steps

1. Go to **Service** → **Smart Unit**.
2. Check the desired smart analysis unit, and click **Create Cluster**.

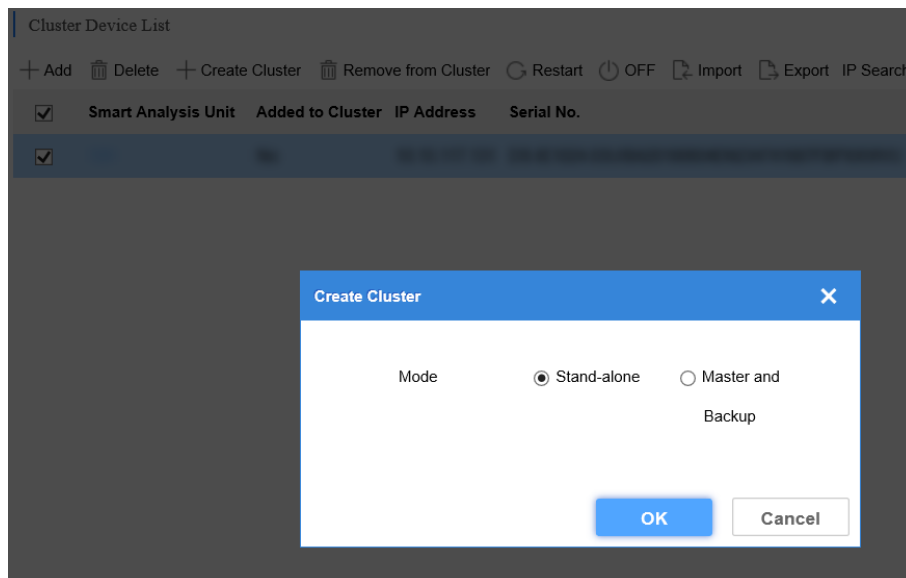


Figure 3-3 Create Stand-Alone Cluster

3. Select **Stand-alone** as **Mode**.
4. Click **OK**.

3.1.3 Create Master and Backup Cluster

The master and backup cluster contains at least two smart analysis units. There are one primary node and one backup node in the cluster, and the rest are computing nodes. If the master node is offline, the backup node will automatically replace the master node to continue the work.

Before You Start

- Ensure that smart analysis units are online.
- Ensure that the master and back-up nodes are on the same subnet, and can connect to computing nodes.

Steps

1. Go to **Service** → **Smart Unit**.

2. Check the desired smart analysis units, and click **Create Cluster**.

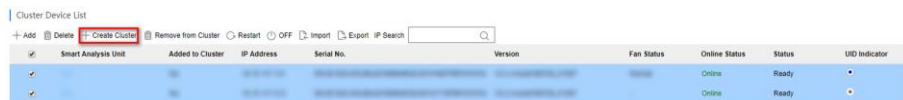


Figure 3-4 Select Smart Analysis Unit



A master and backup cluster cannot be created by a single smart analysis unit.

3. Select **Master and Backup** as **Mode**, and enter **Virtual IP**.

Virtual IP

A service address that the cluster provides, which can be used to send tasks.

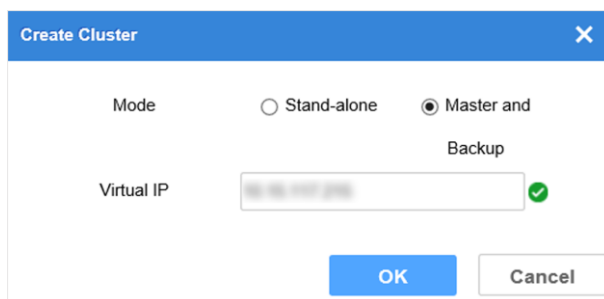


Figure 3-5 Create Master and Backup Cluster



Virtual IP is an external service IP address provided by the cluster, which can be used for assigning tasks.

4. Click **OK**.

3.2 Upload Algorithms

Upload algorithm packages to execute analysis tasks.

Before You Start

Obtain and save algorithm packages to local storage.

Steps

1. Go to **System** → **Algorithm Library** → **Analysis Algorithm List**.
2. Click **Add**.
3. Click **Browse** to select algorithm package(s).

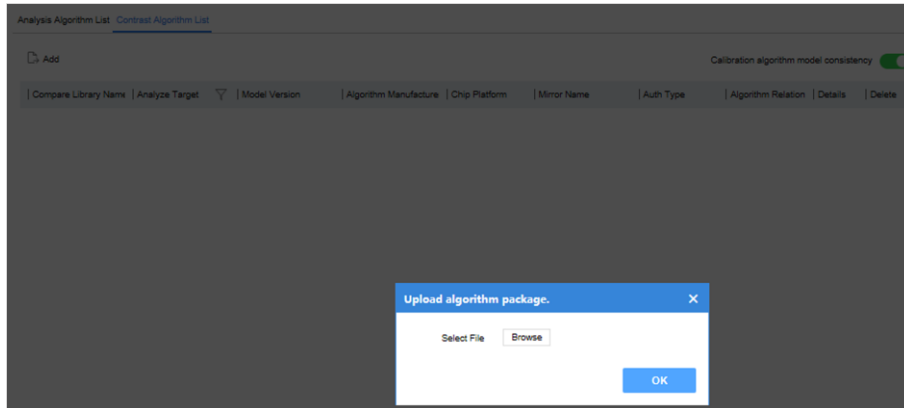


Figure 3-6 Upload Algorithm Package

4. Click **OK**.

5. Optional: Click  to view the detailed information of uploaded algorithm package.

3.3 Pre-allocate Resource

In case some of the analysis tasks occupy too many resources, which will lead to a long wait for other analysis tasks, you may allocate resource in advance. Please allocate algorithm resources according to your actual needs.

Steps

1. Go to **Algorithm** → **Pre-allocation Resource**.

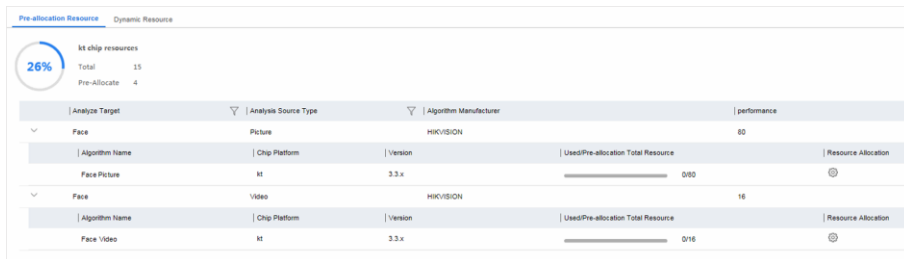


Figure 3-7 Pre-allocation Resource Interface

2. Click  below **Resource Allocation** to configure.

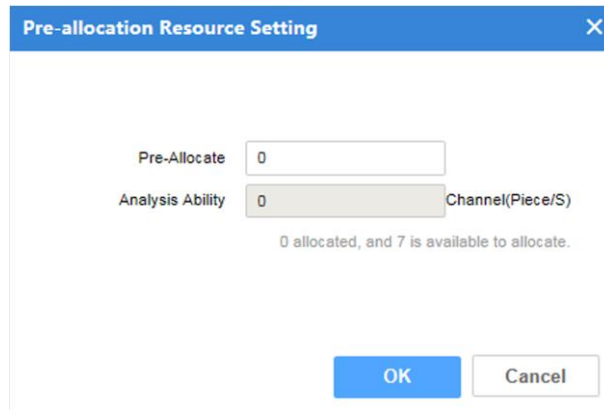


Figure 3-8 Pre-allocate Resource

3. Click **OK**.

3.4 Configure Big Data Service Address

Configure full-text search before executing face analysis task. You can skip this part when executing other tasks. Full-text search address refers to the IP address of face big data server.

Before You Start

Obtain the IP address of face big data server.

Steps

1. Go to **System** → **Basic Settings**.

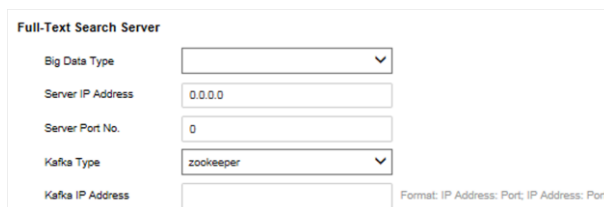


Figure 3-9 Configure Full-text Search Address

2. Configure full-text search parameters.

Big Data Type

Select **Face Big Data** or **Merger Big Data** according to actual conditions.

Server IP Address

Enter the IP address of big data server.

Server Port No.

Enter the port number of big data server.

Kafka Type

Select **kafka** or **zookeeper** according to actual conditions.

Kafka IP Address

- If **kafka** is selected, enter the IP address as following format: IP: 9092.
- If **zookeeper** is selected, enter the IP address as following format: IP: 2181.



"9092" and "2181" are the port number of kafka and zookeeper respectively.

Example

Kafka IP Address: 10.66.112.139:9092; Zookeeper IP Address: 10.66.112.138:2181.

3. Click **Save**.

3.5 Reset Standard

Reset standard before executing face analysis task. You can skip this part when executing other tasks. Resetting standard can divide the face list information in the big data server into multiple small files, which can help the device synchronize face list information more quickly.

Before You Start

Ensure that full-text search address is configured.

Steps

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

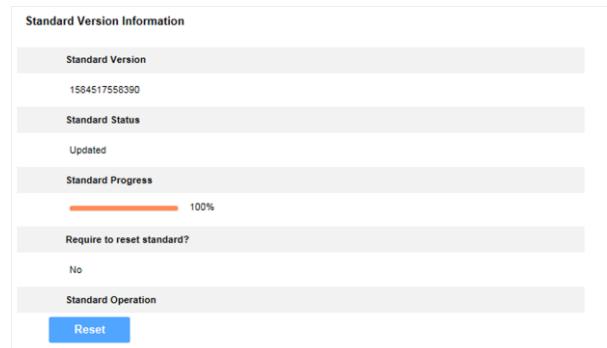


Figure 3-10 Reset Standard

2. Click **Reset**.

Chapter 4 Smart Analysis Unit Management

4.1 Add Smart Analysis Unit to Cluster

Add new smart analysis unit(s) into cluster to enhance analysis capacity.

Before You Start

Ensure that smart unit(s) has been added.

Steps

1. Go to **Service** → **Smart Unit**.
2. Check the desired smart unit(s).
3. Click **Add to Cluster**.
4. Click **OK** to add the new smart analysis unit into cluster.

4.2 Disband Cluster

A cluster will be disbanded if the master node under it is removed.

Steps

1. Go to **Service** → **Smart Unit**.
2. Check the master node.
3. Click **Remove From Cluster**
4. Click **OK**.



Note

In the cluster mode of master and back-up, removing either the master or backup node(s) will lead to the disbandment of the cluster. After that, the back-up node(s) needs to be re-activated.

4.3 Delete Smart Analysis Unit

A smart analysis unit can only be added to one node. You need to delete an analysis unit from a node before add it to another one.

Steps



Caution

If an offline smart analysis unit is deleted, it can only be added to the latest one node who just added it.

1. Go to **Service** → **Smart Unit**.

2. Check the desired smart unit(s).
3. Click **Delete**.
4. Click **OK**.

4.4 Restart Smart Analysis Unit

Before You Start

Ensure that smart analysis unit(s) is online.

Steps

1. Go to **Service** → **Smart Unit**.
2. Check smart analysis unit to be restarted.
3. Click **Restart**.
4. Click **OK**.

4.5 Power off Smart Analysis Unit

Before You Start

Ensure that smart analysis unit(s) is online.

Steps

1. Go to **Service** → **Smart Unit**.
2. Check the desired smart analysis unit(s).
3. Click **OFF**.
4. Click **OK**.



Note

Press the power button to turn the device on after the smart analysis unit is powered off.

4.6 Configure Network Parameters

Configure the network parameters of smart analysis unit(s) through IE browser.

Before You Start

Ensure that the device connects to network cable.

Steps

1. Go to **Service** → **Smart Unit**.
2. Click on the name of smart analysis unit.

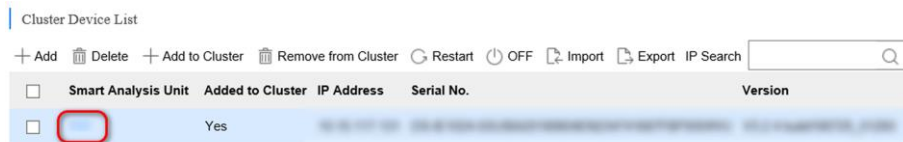


Figure 4-1 Cluster Device List

Note

- Master or back-up node(s), which is added to cluster, is not allowed to be configured.
- Re-add the smart analysis unit(s) after its parameters changed.

3. Click **Network Setting**. Edit network parameters as needed.

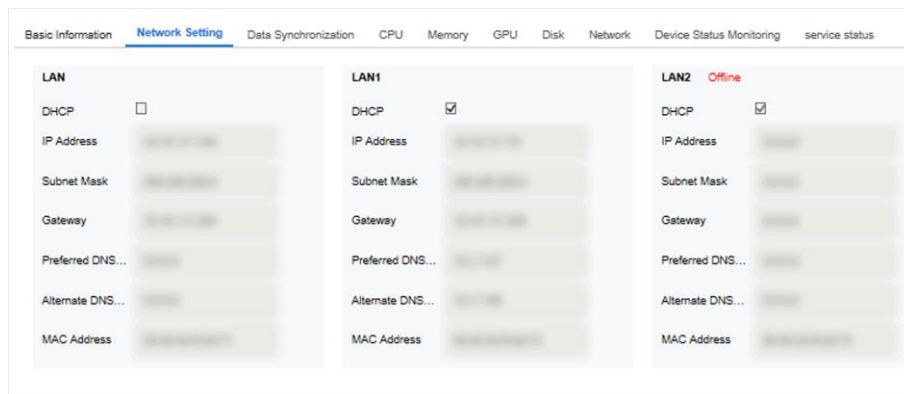


Figure 4-2 Edit Network Parameters

Note

Device with P4 or T4 chip(s) only have the LAN interface.

4. Click **OK**.

4.7 View Hardware Resource

View detailed information such as CPU, memory, GPU and Disk Usage, etc.

Steps

1. Go to **Service** → **Smart Unit**.
2. Click on the name of smart analysis unit.
3. Click different tabs to view the usage of hardware.

4.9 Check Node Information

View the detailed information of each node.

Steps

1. Go to **Service** → **Node Info**.
2. Click on the node name to check details.

Node Info

ID:00-40-3d-f3-b0-71

IP Address:10.15.117.104

Online Status:Online

Total Resource:700

Allocated Resource:0

Remaining Resource:700

Chip Info

No.	Chip ID	Chip Platform	Total Resource	Use Resource	Algorithm Name	Pre-allocation Resource	Dynamic Resource	Load Status	Full Analysis
1	00-40-3d-f3-b0-71_10-254-254-18_8501	kt	100	0		0	0	unknown	Yes
2	00-40-3d-f3-b0-71_10-254-254-18_8501	kt	100	0		0	0	unknown	Yes
3	00-40-3d-f3-b0-71_10-254-254-14_8501	kt	100	0		0	0	unknown	Yes
4	00-40-3d-f3-b0-71_10-254-254-17_8501	kt	100	0		0	0	unknown	Yes
5	00-40-3d-f3-b0-71_10-254-254-16_8501	kt	100	0		0	0	unknown	Yes
6	00-40-3d-f3-b0-71_10-254-254-18_8501	kt	100	0		0	0	unknown	Yes
7	00-40-3d-f3-b0-71_10-254-254-20_8501	kt	100	0		0	0	unknown	Yes

Figure 4-3 Check Node Information

3. Optional: Click  to set filter conditions.

Chapter 5 GPU Resource Management

Check the allocation and usage of algorithm resource.

5.1 Pre-allocate Algorithm Resource

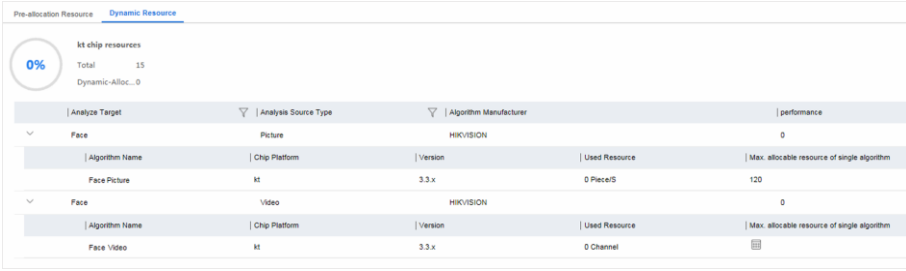
Please refer to *Pre-allocate Resource* for details.

5.2 Check Available GPU Resource

Check the occupied resource of different algorithm modules and the largest available resource of single algorithm.

Steps

1. Go to **Algorithm** → **Dynamic Resource**.
2. Click  to view details of each task.
3. Click  to view the number of available resource.



Pre-allocation Resource		Dynamic Resource		
1t chip resources				
Total		15		
Dynamic-Alloc...		0		
0%				
Analyze Target	Analysis Source Type	Algorithm Manufacturer	performance	
Face	Picture	HIKVISION	0	
Algorithm Name	Chip Platform	Version	Used Resource	Max. allocable resource of single algorithm
Face Picture	Ht	3.3.x	0 Piece/S	120
Face	Video	HIKVISION	0	
Algorithm Name	Chip Platform	Version	Used Resource	Max. allocable resource of single algorithm
Face Video	Ht	3.3.x	0 Channel	

Figure 5-1 Check Available Resource of Algorithm

5.3 Check GPU Resource Allocation

Steps

1. Click **Service** to view the algorithm resource allocation on the bottom-left corner of the interface.
2. Move mouse to the pie chart to view the resource usage.

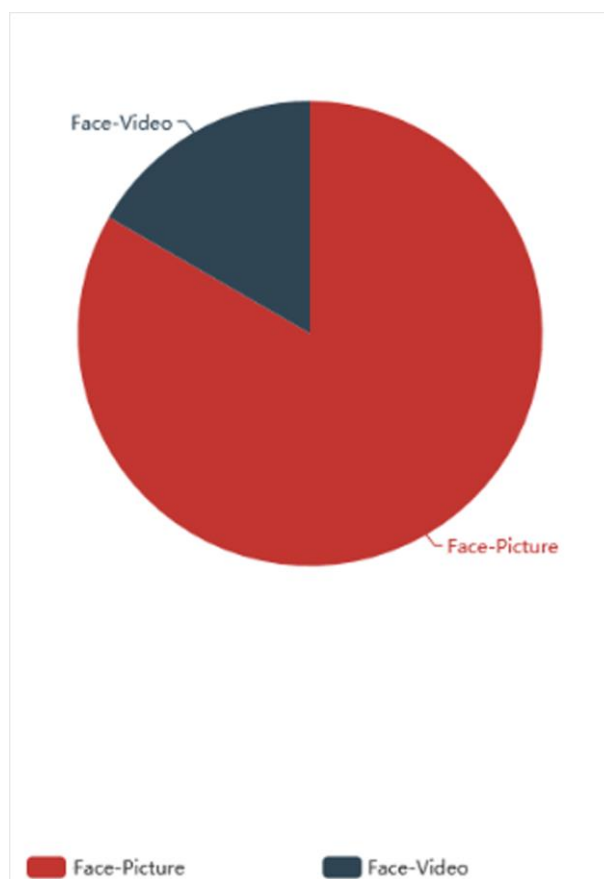


Figure 5-2 Check GPU Resource Allocation

Chapter 6 Task Information

6.1 Check Task Information

Check the details of video or picture analysis task.

Steps

1. Go to **Task Info** → **Task State**.

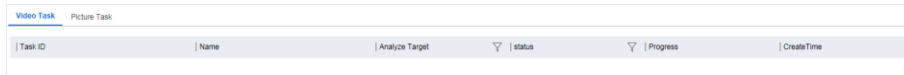


Figure 6-1 Task Information

2. Click on the task name to check details.
3. Optional: Click  to set display conditions.

6.2 Task Data Statistics

Check the data information of tasks processed by each algorithm.

Steps

1. Go to **Task Info** → **Data Statistics**.



Figure 6-2 Data Statistics Interface

2. Check the desired algorithm name.
3. Select a statistics period.

Table 6-1 Operation Description

Icon	Description
	Show the details in the format of line chart.
	Show the details in the format of line chart.

Icon	Description
	Return the chart form into the original one.
	Save the picture of current details.

6.3 Check Output Statistics

Check the analysis output information of tasks processed by each algorithm.

Steps

1. Go to **Task Info** → **Output Statistics**.

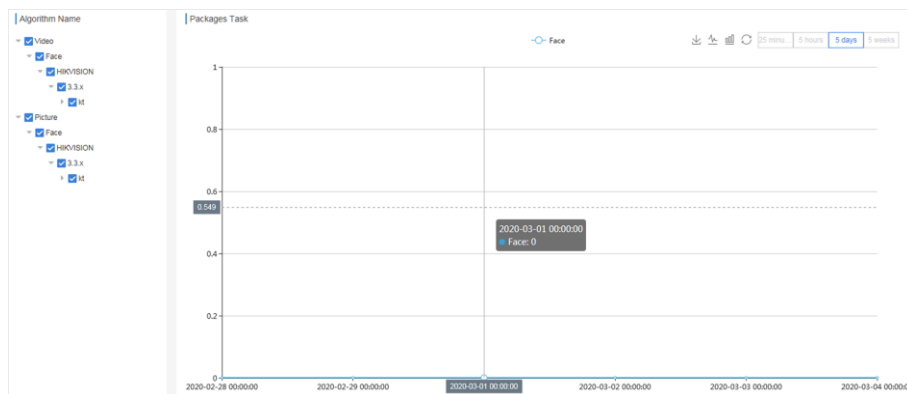


Figure 6-3 Output Statistics Interface

2. Check the desired algorithm name.
3. Select a statistics period.

Table 6-2 Operation Description

Icon	Description
	Show the details in the format of line chart.
	Show the details in the format of line chart.
	Return the chart form into the original one.
	Save the picture of current details.

Chapter 7 System Management

7.1 Basic Settings

7.1.1 Configure SDK Service

With SDK service configured, the device can send analysis results to the configured address by SDK protocol.

Steps

1. Go to **System** → **Basic Settings**.



The screenshot shows a configuration form titled "SDK Service". It contains two input fields: "SDK Access Address" with the value "0.0.0.0" and "SDK Access Port" with the value "0". To the right of each field is a small text instruction: "Enter 0.0.0.0 if no SDK service is needed." for the address and "Enter 0 if no SDK service is needed." for the port.

Figure 7-1 Configure SDK Service

2. Enter **SDK Access Address** and **SDK Access Port**.
3. Click **Save**.

7.1.2 Configure Calculating Pool

Loading to calculating pool is allowed.

Steps

1. Go to **System** → **Basic Settings**.



The screenshot shows a configuration form titled "Calculate Pool". It contains two input fields: "IP Address" with the value "0.0.0.0" and "Port" with the value "0". To the right of each field is a small text instruction: "Enter 0.0.0.0 if no SDK service is needed." for the IP address and "Enter 0 if no SDK service is needed." for the port.

Figure 7-2 Configure Calculating Pool

2. Enter **IP Address** and **Port**.
3. Click **Save**.

7.1.3 Configure Management System

Docking to management platform is allowed.

Steps

1. Go to **System** → **Basic Settings**.

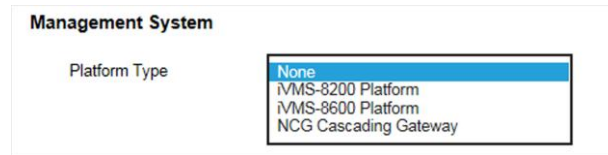


Figure 7-3 Configure Management System

2. Select a platform type as needed and configure related parameters.
3. Click **Save**.

7.1.4 Configure Face Data Library Capacity

The capacity of face data library is set as 100W by default. If the smart analysis unit is equipped with T4 chip(s), change the capacity into 300W.

Before You Start

Ensure that all the smart analysis units are equipped with T4 chips.

Steps

1. Go to **System** → **Basic Settings**.

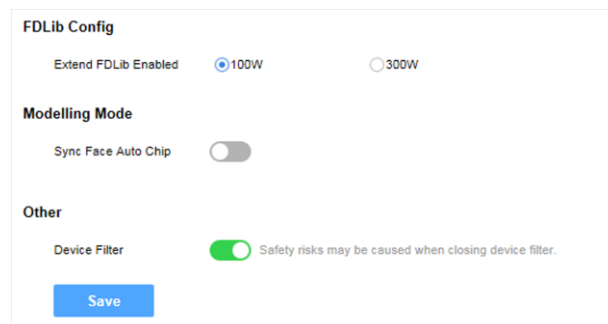


Figure 7-4 Configure Face Data Library Capacity



Sync Face Auto Chip

Disabled by default. If enabled, the type of chip assigned by face analysis task will be shown.

Device Filter

Enabled by default and the device can only be accessible by its IP address. If port mapping configured, disable this function for normal access.

-
2. Configure the parameters as needed.
 3. Click **Save**.

7.2 Time Configuration

Synchronize system time by manual operation or through NTP server.

Before You Start

Obtain the IP address and port number of the NTP server.

Steps

1. Go to **System** → **Time Settings**.

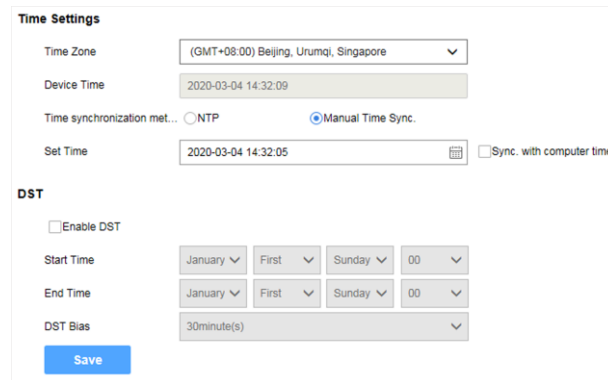


Figure 7-5 Configure Time Settings

2. Select **NTP** or **Manual Time Sync.** as needed.

Note

- The unit of interval is "minute".
 - If **Sync. with computer time** is checked, the device time will be synchronized with that of the computer.
-

3. Optional: Check **Enable DST** and configure related parameters as needed.

4. Click **Save**.

7.3 User Management

The system enabled an admin user by default. Only the admin user can add, delete users and modify user passwords. User types include administrators, operators, and consumers. Operators and consumers can only modify their own passwords.

7.3.1 Add User

Up to 31 users can be added.

Steps

1. Go to **System** → **User Management**.
2. Click **Add** and enter user information.

Add user [X]

User Information

User Name

Level

Admin Password

Password

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

Password Confirm

OK **Cancel**

Figure 7-6 Add User

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.
 - It is recommended to reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
-

3. Click **OK** to complete the operation.

7.3.2 Modify Password

Steps

1. Go to **System** → **User Management**.
2. Click the user name, and then click **Modify**.
3. Enter the admin password and new password, and then confirm your new password.
4. Click **OK**.

7.3.3 Delete User

The default user admin cannot be deleted.

Steps

1. Go to **System** → **User Management**.
2. Click the user name line, and click **Delete**.
3. Click **OK** and enter admin password. Click **OK** again.

Note

Clearing user resource means deleting the device added by the user. If the user is deleted with the resource remained, the device added by the user will be moved to the administrator.

7.4 Log Management

7.4.1 Search Log

The system log includes running log, alarm log, and operation log. Searching and exporting logs are allowed.

- Running Log: Record the completion and failure information of detection event.
- Operation Log: Record the operation information of Web interface.
- Alarm Log: Record error and alarm information of device.

Steps

1. Go to **System** → **Log**.
2. Select the type of log.
3. Set the starting and ending time of search.
4. Click , and corresponding log information will be displayed.
5. Optional: Click **Export**, and click **OK** in the popped up box to export desired log(s).

7.4.2 Download Maintenance Log

Maintenance log is used by professional maintainer to maintain device.

Steps

1. Go to **System** → **Device Maintenance**.
2. Click **Download Maintenance Log**, and click **OK** in the popped up box.

Note

It may take a few minutes to export maintenance log(s). Please wait and select the save path as needed.

7.5 Configure Score Setting

Scoring captured face pictures or pictures in the list library by pupil distance, definition, tilt angle and other parameters, so as to filter those unqualified pictures. Score setting is off by default.

Steps

1. Go to **System** → **Score Setting**.
-

Figure 7-7 Configure Score Setting

2. Select **Face Capture Library** or **Face List Library** as **Filter Type**.
3. Select an algorithm type.
4. Configure parameters as needed and then click **Save**.
5. Optional: Click **Show Details** for more specific information.

7.6 Device Maintenance

7.6.1 Software Updating

Update the software via Web interface.

Before You Start

- Ensure that smart analysis unit(s) is online without any exception.
- Obtain upgrading files.

Steps

1. Go to **System** → **Device Maintenance**.

Figure 7-8 Software Upgrading

2. Check the desired smart analysis unit(s).
3. Click and select a desired file.
4. Click **Upgrade** after the file is uploaded.
5. Click **OK** to start upgrading.



Note

The device will restart automatically after upgrading completed.

7.6.2 Restore Defaults

Restore defaults includes Restore and Default. The device will reboot automatically after restoration, after which you need to activate the device again.

7.7 Check Algorithm List

Check the details of algorithms, such as analysis source type, analysis target, model version, algorithm manufacturer, algorithm version, and so on and so forth.

Steps

1. Go to **System** → **Algorithm Library** → **Analysis Algorithm List/Contrast Algorithm List/HEOP/Basic Component**.
2. Click  in the line of each algorithm to check more details.
3. Optional: Click  to set conditions for displaying.
4. Optional: Click  to delete the desired algorithm.

7.8 Authorization Information

7.8.1 Authorization Analysis Capability

Click **Authorization** at the top-right corner of the interface to view the largest analysis capability.



Caution

If the actual analysis capability is stronger than the authorized one, the latter shall prevail.

7.8.2 Dongle Information

Check information such as trial period and the maximum number of devices for creating cluster. The dongle document needs to be imported manually, contact with technical supporters for support.

Steps

1. Go to **Service** → **Smart Unit**.
2. Click on the name of a smart analysis unit.
3. Click **Basic Information** to view dongle details.

7.8.3 Configure Authorization Address

Configure the authorization address of cluster.

Steps

1. Go to **System** → **Auth Address**.
2. Click  and configure the authorization address.

7.8.4 Cloud Storage Configuration

Cloud storage is accessible for the device. This function is disabled by default. You can configure the related parameters as needed.

Before You Start

Get details of cloud storage parameters.

Steps

1. Go to **System** → **Cloud Storage Configuration**.
2. Enable **cloud storage**.
3. Click **Add**, and set the parameters.



Note

AK indicates access key, and SK indicates encryption key. You can get AK and SK on the cloud storage platform.

7.8.5 List Synchronization

Check the details of list synchronization on different nodes.

Steps

1. Go to **System** → **List Sync**.
2. Click the name of different nodes to check details.

7.9 Enable Alarm Sound

Enable alarm sound to trigger a sound prompt when exception occurs. The alarm sound is disabled by default.

Steps

1. Click **Alarm**.
2. Enable **Alarm Sound**.

7.10 Help Center

Refer to the help document by going to **Help** → **Help Document** on the upper-right corner of the interface to view or download the document.

7.11 Version Information

Check version information of different modules by going to **Help** → **Version** on the upper-right corner of the interface.

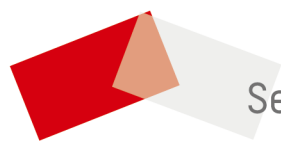
7.12 Open Source Software License

Check open source software license by going to **Help** → **Open Source Software License** on the upper-right corner of the interface.

7.13 Logout

Steps

1. Go to **admin** → **Logout** on the upper-right corner of the interface.
2. Click **OK**.



See Far, Go Further