



Comparison 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.

Symbol Conventions

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

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

TABLE OF CONTENTS

Chapter 1 Log in	1
1.1 Agreement	1
1.2 PC Configuration Requirements.....	1
1.3 Log in	2
Chapter 2 Smart Analysis Unit Management.....	3
2.1 Add Smart Analysis Unit.....	3
2.2 Delete Smart Analysis Unit.....	4
2.3 Restart Smart Analysis Unit.....	5
2.4 Turn off Smart Analysis Unit	5
2.5 Configure Network Parameters	5
2.6 View Hardware Usage Rate.....	6
2.7 Export Device List	7
Chapter 3 System Management	8
3.1 Configure Time	8
3.2 Modify Admin Password	9
3.3 Search for Log.....	10
3.4 Enable Alarm Sound	10
3.5 Maintain Device	10
3.5.1 Upgrade Software	10
3.5.2 Restore Default	11
3.5.3 Download Maintenance Log	11
3.6 Authorize Operation	11
3.6.1 Import License.....	11
3.6.2 View Authorization Information	12
3.7 Authorize Operation	13
3.8 View Information	13
3.8.1 View HelpDoc	13
3.8.2 View Version Info.	13
3.8.3 View Open Source Software Licenses	13
3.9 Log out.....	13

Chapter 1 Log in

1.1 Agreement

Comparison server interface (<https://IP:10443>), hereinafter referred to as the 10443 interface, is mainly used to view the analysis node status and authorization.

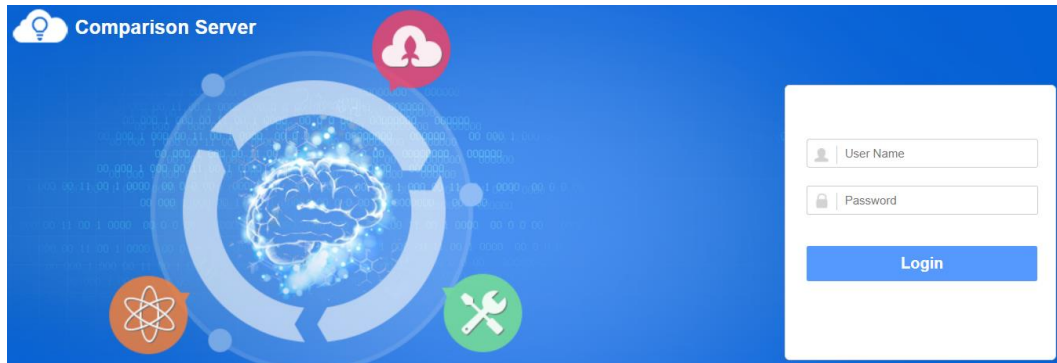


Figure 1-1 10443 Interface

Comparison service management Interface (<http://IP:8912/xveccompare-web>), hereinafter referred to as the 8912 interface, is mainly used to configure the model comparison service.

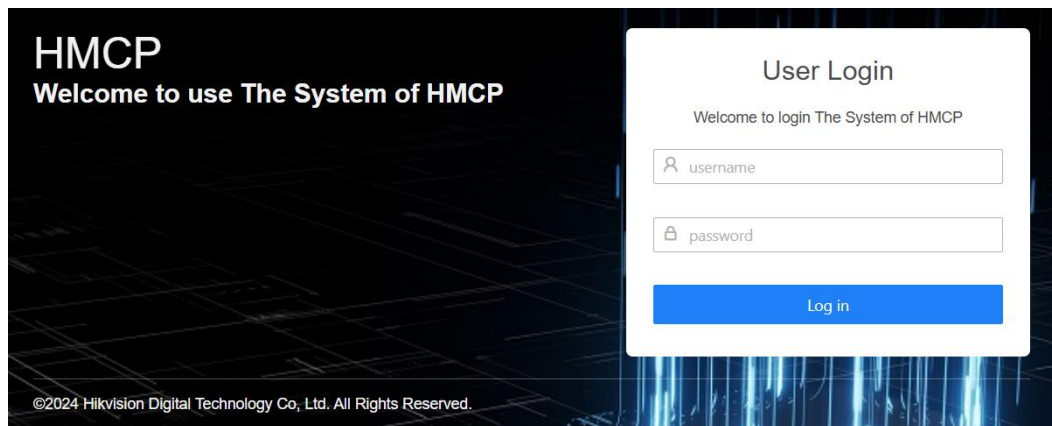


Figure 1-2 8912 Interface

1.2 PC Configuration Requirements

You can access the device through the IE browser. The PC configuration requirements for accessing the device are as follows.

Table 1-1 Configuration Requirements

Component Name	Configuration Requirements
Operating System	Microsoft Windows 7, 10
CPU	Intel Pentium IV 3.0 GHz or above
Memory	1 GB or higher
Resolution	1024 × 768 or higher resolution
Browser	10443 Interface: IE8 to IE11 8912 Interface: Chrome

 Note

The screenshots are for illustration purposes only. For details, refer to the actual display of the interface.

1.3 Log in

Steps

Step 1 Enter *https://IP:10443* in the IE browser address bar, and press Enter. The IP is the your device's IP address.

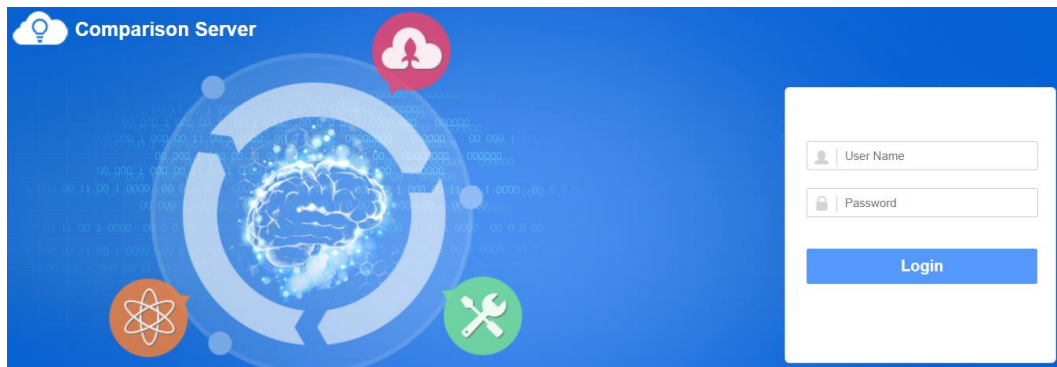


Figure 1-3 Login Interface

Step 2 Enter the user name and password when activating the device, and then click **Login**.

Chapter 2 Smart Analysis Unit Management



Note

To ensure business consistency between the 10443 interface and the 8912 interface, add or delete smart analysis units under **Device Management** → **Device Details** on the 8912 interface.

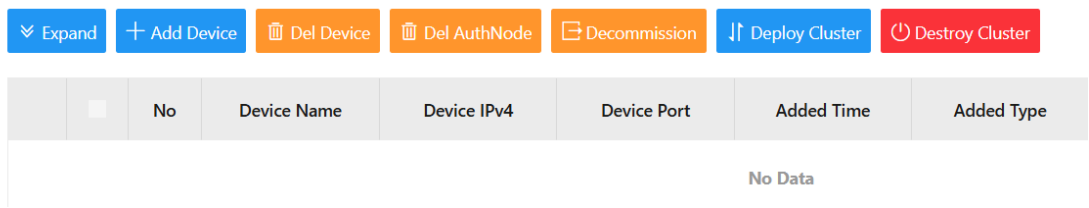


Figure 2-1 Device List Interface

2.1 Add Smart Analysis Unit

You can add smart analysis units on your local device or similar other devices. The added smart analysis units cannot be added again.

Before you start

- The IP address of the intelligent analysis unit has been obtained.
- The to-be-added smart analysis unit has not added other smart analysis units.

Steps

Step 1 Click Service → Smart Unit → Add.

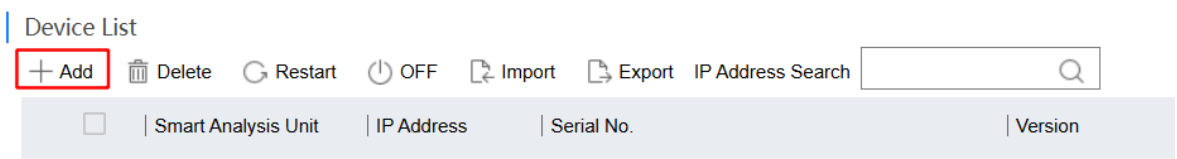


Figure 2-2 Smart Analysis Unit Adding Interface

Step 2 Enter the name, the IP address of the smart analysis unit, the user name, and the password, keep the port number as the default, and click **OK**.

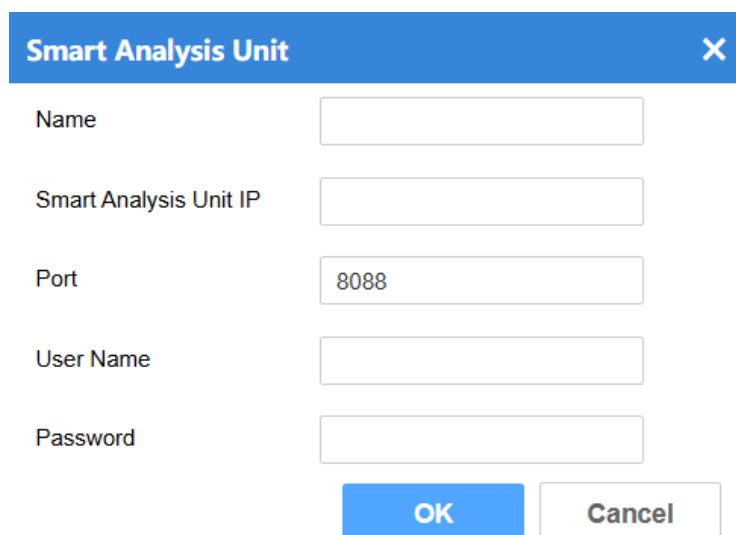
A dialog box titled "Smart Analysis Unit" with a close button (X) in the top right corner. It contains five input fields: "Name", "Smart Analysis Unit IP", "Port" (with the value "8088" entered), "User Name", and "Password". At the bottom, there are two buttons: "OK" (blue) and "Cancel" (white with a grey border).

Figure 2-3 Add Smart Analysis Unit

 Note

- The name of the smart analysis unit cannot be the same, with a value range of 1 to 32, supporting letters, numbers, Chinese characters, and special characters. Special characters do not include `[#~%!\$^="'"?<>():,;. •! @ ¥ ……&*—+ 【】 {} : ; “ ” ‘ ’ | , ° 、 《 》 ? \ .
- By importing a template file saved with smart analysis unit information, you can add units in batches. You can click  **Import** →  **Export Template** to obtain the template file.
- When you add some devices, the user name and password are required to verify permissions for enhancing security.

2.2 Delete Smart Analysis Unit

The added smart analysis unit needs to be deleted first before it can be added again.

 Caution

The offline smart analysis unit, after being deleted, only supports being added again by the node added most recently, and does not support being added by other nodes.

Steps

Step 1 Click **Service** → **Smart Unit**. Select the units you want to delete.

Step 2 Click **Delete**, and Click **OK** in the pop-up dialogue box.



Note

The cluster will be destroyed after you delete the primary/secondary node.

2.3 Restart Smart Analysis Unit

Before you start

The smart analysis node is in online status.

Steps

Step 1 Click **Service** → **Smart Unit**. Select the units you want to restart.

Step 2 Click **Restart**, and Click **OK** in the pop-up dialogue box.

2.4 Turn off Smart Analysis Unit

Before you start

The smart analysis node is in online status.



Caution

After the smart analysis unit is turned off, it can only be powered on by pressing the power button, and remote power-on is not supported. If the device is equipped with a BMC, remote power-on is supported through the BMC.

Steps

Step 1 Click **Service** → **Smart Unit**. Select the units you want to turn off.

Step 2 Click **OFF**, and Click **OK** in the pop-up dialogue box.

2.5 Configure Network Parameters

You can modify the network parameters of the smart analysis unit through the Web interface.

Before you start

The device has at least 1 network port connected with a network cable.

Steps

Step 1 Click **Service** → **Smart Unit**. Select the units you want to turn off.

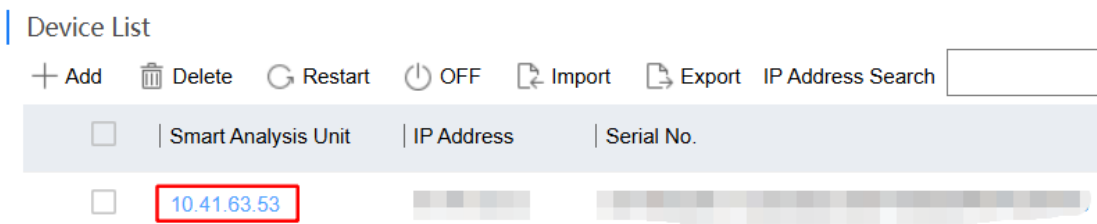


Figure 2-4 Click Name

 Note

- The primary and secondary nodes of that have already formed a cluster do not support modifying the LAN network parameters.
- After modifying the LAN network parameters, you need to re-add the smart analysis unit.

Step 2 Click **Network Settings** to configure network parameters.

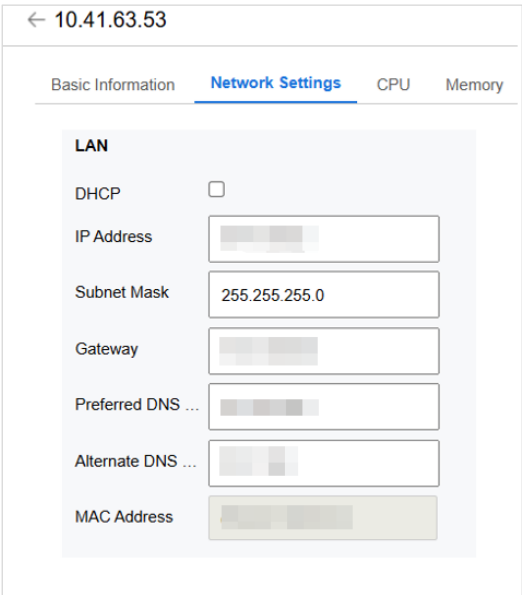


Figure 2-5 Configure Network Parameters

Step 3 Click **Save** after configuration.

2.6 View Hardware Usage Rate

You can view the usage rates of CPU, memory, GPU, and disk.

Steps

Step 1 Click **Service** → **Smart Unit**. Click the unit name.

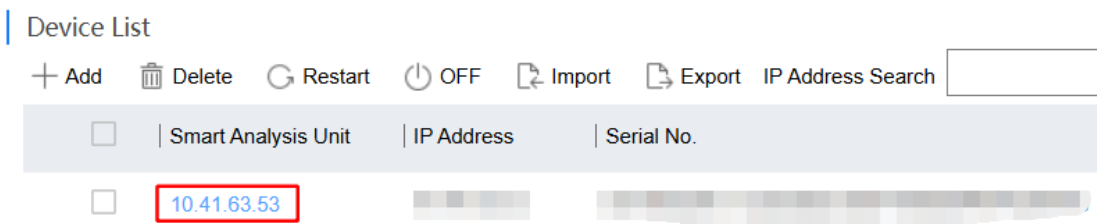


Figure 2-6 Click Name

Step 2 Click the tabs of **CPU**, **Memory**, **GPU**, or **Disk** to view the information of hardware usage rates.

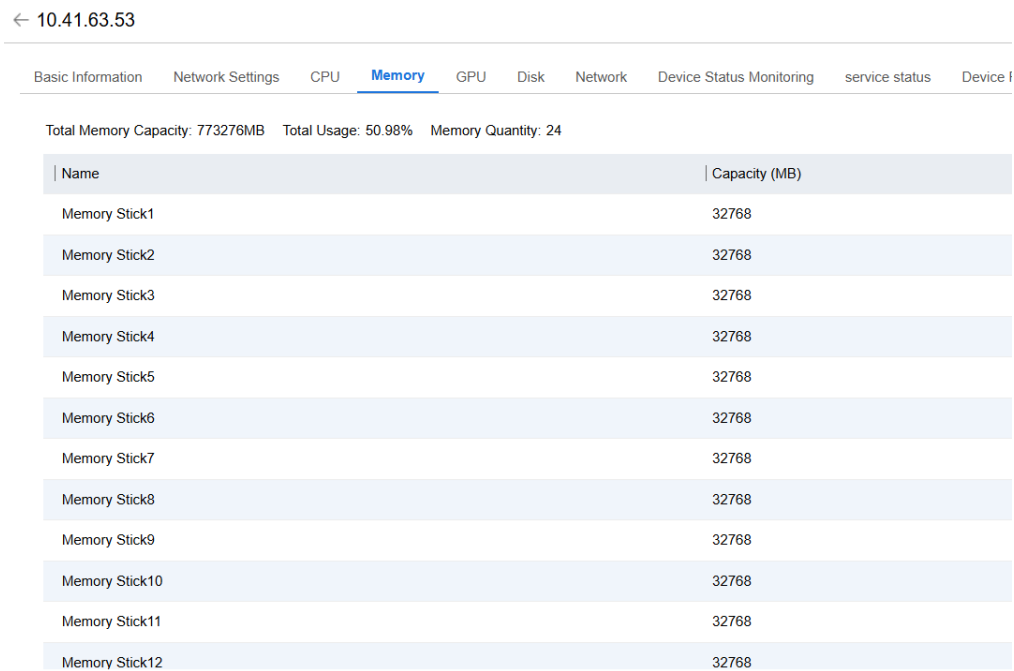


Figure 2-7 View Hardware Information

2.7 Export Device List

You can export the added smart analysis unit.

Steps

Step 1 Click **Service** → **Smart Unit** → **Export**.

Step 2 Export the unit that has been added to the device list.

Chapter 3 System Management

3.1 Configure Time

If the time is incorrect, you can adjust it promptly. NTP time synchronization and manual time synchronization is available. When selecting NTP time synchronization, you need to obtain the IP address and port information of the NTP server.

Steps

Step 1 Click **System** → **Time Settings**.

Time Settings

Time Zone

(GMT+08:00) Beijing, Urumqi, Singapore

Device Time

2025-03-06 16:05:18

Time synchronization met...

☒ NTP

☐ Manual Time Sync.

Server Address

NTP Port

0

Interval

0

minute(s)

Save

Figure 3-1 NTP Time Synchronization Interface

Time Settings

Time Zone

(GMT+08:00) Beijing, Urumqi, Singapore

Device Time

2025-03-06 16:05:31

Time synchronization met...

☐ NTP

☒ Manual Time Sync.

Set Time

2025-03-06 16:05:28

☐ Sync. with computer time

Save

Figure 3-2 Manual Time Synchronization Interface

Step 2 Export the unit that has been added to the device list.

 Note

- The interval for time synchronization is in minutes.
- Check ***Sync. with computer time***, and the device's time will be the same as the PC's time.

Step 3 Click **Save**.

3.2 Modify Admin Password

Steps

Step 1 Click **User Management**. Click the row where the admin information is located, and click **Modify**.

 Caution

Set a high-strength password with sufficient complexity. Ensure to keep the password safe after the modification is completed.

Step 2 Enter the old password, new admin password, and confirmation password. Click **OK**.

Modify user

User Information

User Name

admin

Level

Administrator

Old Password

New Admin Password

1、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.

2、Do not use risky passwords(List of risky passwords:
1qaz2wsx,1qaz@WSX,1!@#\$QWER,p@ssword,passwd0rd,p@ssw0rd;)

3、Do not contain following characters in the password: the user name, 123, or admin (case insensitive).

4、The password cannot contain 4 consecutive repeated characters (such as 1111, 8888, and aaaa).

5、The password cannot contain 4 consecutive digits in ascending or descending order (such as 1234, 12345, and 4321).

6、Do not contain following characters (case insensitive) in the password: hik (whole word matched, with no letters before and after hik), hkws (whole word matched, with no letters before and after hkws), and hikvision.

Password Confirm

OK

Cancel

Figure 3-3 Modify Password

3.3 Search for Log

Logs include the running log, alarm log, and operation log. You can query or export logs.

- **Running Log**: It records the device running information.
- **Alarm Log**: It records the error alarm information.
- **Operation Log**: It records the Web interface operation information.

Steps

Step 1 Click **System** → **Log**.

Step 2 Select the log types, set searching conditions, and click . The system will automatically filter the log information that meets the conditions.

Step 3 (Optional) Click **Export**, and click **OK** in the pop-up dialogue box.

3.4 Enable Alarm Sound

When events such as disk full and list data synchronization exceptions occur, sound prompts are triggered. The default is not enabled.

Steps

Step 1 Click **Alarm** at the upper-right corner of the interface.

Step 2 Check **alarm sound** to enable the sound prompt.

3.5 Maintain Device

3.5.1 Upgrade Software

You can upgrade the device through the Web interface.

Before you start

- The device is online with no abnormalities.
- Upgrade file has been obtained.

Steps

Step 1 Click System → Device Maintenance.

Upgrade

Select device for updating.

VersionSearch Patch Package VersionSearch

☐	Device Name	IP Address	Serial No.	Version	▼ Patch Package Version ▼
--------------------------	-------------	------------	------------	---------	---------------------------

Upgrade file

Do not operate during file uploading. After the file upload is completed, please perform the upgrade operation within 10 minutes.

Figure 3-4 Software Upgrade Interface

Step 2 Select the to-be-upgraded device, click , and select the upgrade file. After uploading, click **Upgrade**.

Step 3 Click **OK** to start upgrade. The device will automatically restart after the upgrade is completed.

3.5.2 Restore Default

After reset, the device's IP address is retained, and the rest of the parameters are restored to the factory settings. The system will automatically restart after reset, and the device needs to be reactivated.

Steps

Step 1 Click **System** → **Device Maintenance**.

Step 4 Click Restore.

3.5.3 Download Maintenance Log

Maintenance logs are provided for professional maintenance personnel to maintain the device.

Steps

Step 1 Click **System** → **Device Maintenance**.

Step 5 Click Download Maintenance Log. Click **OK** in the pop-up dialogue box. Exporting the maintenance log may take a few minutes, please be patient and wait. Then, follow the prompts to select the save path.

3.6 Authorize Operation

3.6.1 Import License

Steps

Step 1 Click **System** → **License Operation**.

License Operation

Operation guide

License Type

Please select

Import/Export

Certificate File

Fingerprint

Import Cert...

Import

Figure 3-5 License Operation

Step 2 Set License Type to Comparison Server.

Step 3 Move the mouse cursor over Operation guide, and follow the prompt to finish license operation.

3.6.2 View Authorization Information

You can click **Service** → **Device** to view the information of authorized analysis ability and applied resource. Analysis tasks can only be processed when corresponding analysis abilities are available.



Caution

When the actual analysis ability of the device exceeds the authorized ability, take the maximum authorized analysis ability as the standard.

Authorization

Edits Remaining : 3

Save

No.	Algorithm group ID	Analyze Target	Analysis Source Type	Analysis Ability	Applied resource	Remaining Resource	Authorization Type
1	6900xc6d5	CompareAllAnalysis	modelData	180	180	0	false

Auth Info List

No.	Name	value	Operation
1	AuthAddrInfo	{ "AuthAddress": [{ "type": "HIK_CHIP", "url": "10.254.254.254:12345"}, { "type": "HIK_LICENSE", "url": "" }] }	Click To See
2	AbilityIdListInfo	{ "abilityId": "5baadca4206a43e8ac85173ac846863", "source": "model", "targetType": "73", "require": 180, "realityNum": 180, "left": 180, "used": 0, ... }	Click To See
3	MasterJson	{ "MasterNode": { "ip": "10.41.63.53", "port": 30080, "uuid": "afd126fef52c47168d7fa4715d2e572b"}, "NodeInfo": { "port": 30080, "name": "10.41.63.53", "uuid": "afd1..." } }	Click To See
4	ClientAuthInfo	{ "mac": "c4.cb.e1.e3.b9.d0", "nodeId": "afd126fef52c47168d7fa4715d2e572b", "nodeIp": "10.41.63.53", "nodeName": "10.41.63.53", "nodePort": 30080, "device..." }	Click To See
5	SafenetInfo	{ "safenetVersion": "aksusbd-9.15-1.x86_64", "safenetActive": "Active: active (running) since Thu 2025-03-06 20:15:53 CST; 13h ago", "safenetUID": "GtUm..." }	Click To See

Child Node Info

No.	Child Node Name	IP Address	status	Authorization
1	10.41.63.53	10.41.63.53	Online	Click To See

Figure 3-6 Authorization Information

3.7 Authorize Operation

SafeNet supports adding device IP addresses. Devices with IP addresses not on the list are not allowed to access safeNet.

Steps

Step 1 Click System → safeNet Configuration. Select Enable, and click Add.

Step 2 Enter the IP address of the allowed device, and click OK.

3.8 View Information

3.8.1 View HelpDoc

You can click **Help** → **Help document** at the upper-right corner of the interface to view or download the document.

3.8.2 View Version Info.

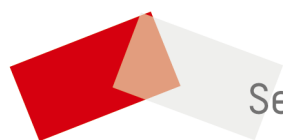
You can click **Help** → **Version** at the upper-right corner of the interface to view the version information of each module.

3.8.3 View Open Source Software Licenses

You can click **Help** → **Open Source Software Licenses** at the upper-right corner of the interface to view the open source declaration information.

3.9 Log out

You can click **admin** → **Logout** at the upper-right corner of the interface. Click **OK** in the pop-up dialogue box.



See Far, Go Further