



Security Inspection Analyzer

User Manual

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

HDMI[™] : The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect

data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

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.

Safety Instructions



Security inspection analyzer is a professional equipment. The equipment is not suitable for use in locations where children are likely to be present.

Professional
Equipment

- 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.
- 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.

TABLE OF CONTENTS

1	Overview.....	7
	1.1 Introduction	7
	1.2 Key Feature	7
	1.3 Indicator Description.....	7
	1.4 Buzzer Description	7
	1.5 Interface Description	7
	1.6 Wiring Diagram	8
2	Local Operation	8
	Chapter 2.....	8
	2.1 Startup, Shutdown and Activation.....	8
	2.1.1 Startup	8
	2.1.2 Activation.....	8
	2.1.3 Export GUID File	9
	2.1.4 Quick Unlock.....	9
	2.1.5 Shutdown.....	10
	2.2 Boot Wizard.....	11
	2.3 Live View	12
	2.3.1 Live View Menu	12
	2.3.2 Live View Convenient Operation.....	13
	2.4 Playback	14
	2.5 Picture Query	17
	2.6 Security.....	18
	2.6.1 Intelligent Configuration	18
	2.6.2 Contraband Configuration.....	20
	2.7 Camera	20
	2.7.1 Online Device.....	21
	2.7.2 Coding Parameters	22
	2.7.3 Display Settings.....	27
	2.7.4 Packages Passed Statistics	28
	2.7.5 Prohibited Items Statistics.....	28
	2.8 Storage	29
	2.9 System	30
	2.9.1 General	30
	2.9.2 User Settings.....	30
	2.9.3 Network Settings	34

2.9.4 Event Settings	37
2.9.5 Live View Settings	40
2.10 System Maintenance	42
2.10.1 Security Check Info	42
2.10.2 System Info	42
2.10.3 Log Information	45
2.10.4 Configuration Settings	46
2.10.5 Upgrade	47
2.10.6 Default Settings	47
2.10.7 Network Resource Statistics	48
2.10.8 Advanced Settings	48
2.11 Platform	49
2.12 Others	50
2.12.1 View Alarms & Exceptions	50
2.12.2 View Backups	50
3 Remote Operation	50
Chapter 3	51
3.1 Login and Activate the Device	51
3.1.1 Login	51
3.1.2 Activation	51
3.2 Live View	52
3.3 Playback	53
3.4 Search Pictures	54
3.5 Configuration	55
3.5.1 Local Configuration	55
3.5.2 System	56
3.5.3 Network	64
3.5.4 Video & Audio	67
3.5.5 Image	69
3.5.6 Event	70
3.5.7 Storage	73
3.5.8 Smart Security Check	74
3.5.9 AI Open Platform	76
3.6 Data Statistics	76

1 Overview

1.1 Introduction

Intelligent security check analyzer adopts embedded design, friendly interactive interface and embedded deep learning algorithm to achieve docking with third-party security check machine. It can complete the intelligent transformation of traditional security check machine, achieve networking of security check machine and X-ray picture structure, and intelligently classify the prohibited items. It can dock with video monitoring system, and personnel channel system for security control.

1.2 Key Feature

- Low delay: The screen delay is within 50 ms with smooth use sense but without stuck sense.
- Intelligent recognition of the prohibited goods: the device structures the security pictures and intelligently identify the prohibited items in the pictures, such as knives, guns, liquids, umbrellas, batteries, mobile phones, laptops, spray cans, etc. And linkage output can be carried out to prompt suspicious items.
- Breaks the traditional information island and achieves the network of security check. The platform can be combined with video monitoring to achieve information fusion.
- Achieves 4 IPC accesses, and information fusion of security check and safety protection.
- LOOP VOUT

As a disaster recovery solution, LOOP VOUT function can be enabled automatically or by pressing a peripheral button, and is designed to pick up the original video input signal if the device should be going through malfunction or breakdown, ensuring on-site security inspection processes properly.

Note: Models of ISD-ST102D-DHV and ISD-ST102D-DHV4G only support 2 IPC accesses.

1.3 Indicator Description

Refer to the device's Quick Start Guide for detailed indicator description.

1.4 Buzzer Description

3 long durations and 2 short durations: The equipment appears full hard disk, hard disk error, network disconnection, IP conflict, illegal access, picture capture exceptions, alarm input and other anomalies.

Note:

The device needs to set linkage in the local or web site to enable the above alarm sounds.

3 long durations: Incorrect password.

1.5 Interface Description

Refer to the device's Quick Start Guide for detailed interface description.

1.6 Wiring Diagram

Refer to the device's Quick Start Guide for detailed wiring description.

2 Local Operation

2.1 Startup, Shutdown and Activation

2.1.1 Startup

Caution:

- Please confirm that access voltage meets the requirements of intelligent security check analyzer and ensure the analyzer properly grounded.
- Abnormal power supply will result in abnormal operation for intelligent security check analyzer, even damaging it. It is recommended to use the regulated power supply.

Note:

- Please ensure that the display or monitor is connected with VGA 1/HDMI 1 output of the device before startup.

The detailed steps for startup are as follows:

Step 1 Plug in the power. (100V AC to 240 V AC)

Step 2 Set the power switch to I for starting up.

Note:

- The power indicator is blue after starting up.
- If you need to restart the device after soft shutdown through the main menu (please refer to 2.1.5 Shutdown), you can directly press the power button on the front panel for starting up.
- It can be configured simply through the boot wizard to make the device work normally after starting up.

2.1.2 Activation

Caution:

Please understand that you are responsible for the reasonable configuration of all passwords and security settings of other related products, and take care of your username and password.

The device must be activated and set a login password at the first use to login and use it normally later.

The steps of activation are as follows:

Step 1: The activation interface will pop up after the device is started up.

Step 2: Creates the login password and enter again the password for confirmation.

Note:

- The default username is admin.
- The password consists of 8-16 characters, including at least 2 of the following types: digits, lowercase letter, uppercase letter or special characters.
- The strength of the password is divided into 3 levels: weak, medium and strong. In order to protect personal privacy and enterprise data, and prevent the device from the network security problems, it is recommended that you set a strong password strength that meets the security specifications.

Step 3: (Optional) Check the “Export GUID File” to exporting it for resetting the password.

Step 4: Enter “IPC Activation Password”. If it is the same as that of the webcam, it is unnecessary to enter the webcam activation password again at the time of adding the webcam.

Step 5: Click “OK”.

2.1.3 Export GUID File

GUID File can be exported after device activation and password modification. And the password can be reset via importing the GUID file when forgetting the password.

Note:

Please confirm that the USB has been plugged into the USB interface correctly before exporting the GUID file.

Step 1: Enter the interface of exporting GUID file.

Step 2: Select the device name and folder exported.

Step 3: Click “Export” to export GUID file into the specific folder category of USB.

Step 4: Click “OK” in the pop-up prompt box.

2.1.4 Quick Unlock

Set Unlock Pattern

Enter the interface of setting unlock pattern for quick unlock after device activation. The detailed steps are as follows:

Step 1: Hold and press the mouse to draw the lines among the 9 points until the pattern is finished and then release the mouse.

Note:

- Each point can only be drawn once when drawing the pattern.
- The unlock pattern should consist of 4-9 points.

Step 2: Press the mouse again and repeat to draw lines as Step 1 pattern drawn. When the two unlock patterns are consistent, the setting is successful, and the system will automatically exit the interface of set unlock pattern.

Note:

If the two patterns are not consistent, user should repeat Step 1 and Step 2.

Unlock

Note:

The unlock pattern need to be configured before unlock.

When unlock with the pattern, you will be logged on as an administrator.

The details are as follows:

Step 1: Right-click to enter the unlock interface in case of logout.

Step 2: Enter the main menu after drawing the unlock pattern set.

Note:

- If click “Forget Unlock Pattern” or “Switch User”, normal login interface can be entered.
- If the unlock pattern drawn is inconsistent with the setting one, it will prompt “Unlock pattern error, please try again.”
- If 5 times of unlock pattern drawn are wrong, automatically switch to the normal login interface.

2.1.5 Shutdown

Caution:

When the system prompts “System shutdown is in progress...” please do not press the button “Power Switch”.

When the device is operating (especially recording), do not force shutdown. (That is disconnect the power supply directly.)

Main Menu Shutdown



Step 1: Click the picture in the top right corner to enter the interface of “Device Shutdown”.

Step 2: Click “Shutdown” and pop up the prompt box.

Step 3: Click “Yes” and shut down the device.

Right-click to exit interface of “Device Shutdown”.

Press Shutdown Button on Panel

Step 1: Press the “Power Button” on the front panel for more than 3 seconds and pop up the prompt box “Shut down the system?”

Step 2: Click “Yes” and shutdown.

2.2 Boot Wizard

After the device is started, the system time configuration, network configuration, hard disk initialization and other simple operations can be carried out through the boot wizard to make the device work normally.

Note:

If you need to skip the wizard, click “Exit” directly or right click on a random area, and click “Yes” in the dialog box “Exit the Boot Wizard?” popping up.

The detailed steps are as follows:

Step 1: Set system time

Set local “Time Zone”, “Date Display Format”, “System Date” and “System Time”.

Step 2: Security check Info

Set the manufacturer, type, visual angle and start time of the security check machine.

Step 3: Intelligent analysis

1. Select video input channel in the “Enable Algorithm Detection”.

The settings of the intelligent analysis interface will only take effect for the currently selected channel after saving.

2. Set “Security Check Configuration Info”

Set “Calibration Type”, “Transmission Direction”, “Font Size”, “Channel Size” and “Text Following Mode”.

Note:

The direction of convey belt is configured incorrectly, which results in failure of intelligent recognition. And the wrong channel size configuration of security check machine may cause an exception for intelligent recognition.

3. Draw the picture recognition area of package passed

Select “Default Recognition Area” and the red box of default recognition area will appear automatically in the screen.

Select “Re-draw Recognition Area” and press the left button of mouse to draw the rectangular area in the screen.

Note:

Non-security screen in the recognition area will affect the effect of intelligent recognition.

4. In the “Prohibited Items Detection Configuration” list on the right, check different types prohibited items, recognize the type and click “Edit” to set the color for different prohibited items. The color of prohibited items not checked is dark red by default.

Step 4: Configure network

1. Select “Work Mode”, “Network Card” and its type.
2. Check “Auto Obtain IPv4 Address” or set network parameters manually.

Set “IPv4 Address”, “IPv4 Subnet Mask”, “IPv4 Default Gateway” manually, or check “Auto Obtain IPv4 Address”.

3. You can obtain DNS server automatically or fill in by yourself.

Step 5: Click “OK” and finish boot wizard.

2.3 Live View

The pictures of each channel can be seen in the Live View interface.

Note:

Right-click to enter the unlock interface when the device is in the standby mode.

2.3.1 Live View Menu

The menu at the bottom side of Live View interface is as follows:

Fig 2-4 Menu of Live View Interface

Table 2-1 Icon Description of Live View Menu

Icon	Name	Description
	Following Mode	The following modes can be selected as follows: close following, line following, point line following and separation following.
	All Day Time Lapse Video	Turn on/off the all day time lapse video. Please refer to the details in “2.9.1 VideoPlan Configuration”.
	Full Screen	Full screen Live View
	Unpacking Platform Access	Click the button to send related info. to the platform for fine inspection.

	Alarm	Click the button to view detailed alarm information.
---	-------	--

2.3.2 Live View Convenient Operation

Enter the Live View screen, select the channel to be operated with the left mouse button, and the convenient operation menu will pop up.



Fig 2-4 Live View Convenient Menu Diagram

Table 2-2 Live View Convenient Menu Description

Button	Description
	Hide smart information
	Screenshot
	Silence
	Switch Main Stream /Sub Stream

Status Bar

The number of package passed, prohibited items, device running time and bound AI model can be checked through the top status bar.

When the analyzer adds the security gate, the status bar will also display the number of metal detection and the total number of people.

Screenshot

Live View the channel firstly, then click the “Screenshot” to capture the current picture, and save it to the hard disk.

Users can view and back up in file management.

Manual Record

Click “Manual Record” to turn on/off it.

Intelligent Info.

Click “Intelligent Info.” to display it or not. After turning on, the system will automatically label the dangerous goods.

2.4 Playback

Playback Interface Description

Select "Playback" in the upper menu bar to enter the playback interface.

Table 2-3 Description of Playback Control Bar

Button	Description	Button	Description	Button	Description
	Clip		Clip Time		Cut and Export
	Back		Forward		Play
	Pause		Slow Down		Speed up
	Split Screen 1		Split Screen 2		Full screen / Exit full screen
	Add tag		Lock		

Single Channel Playback

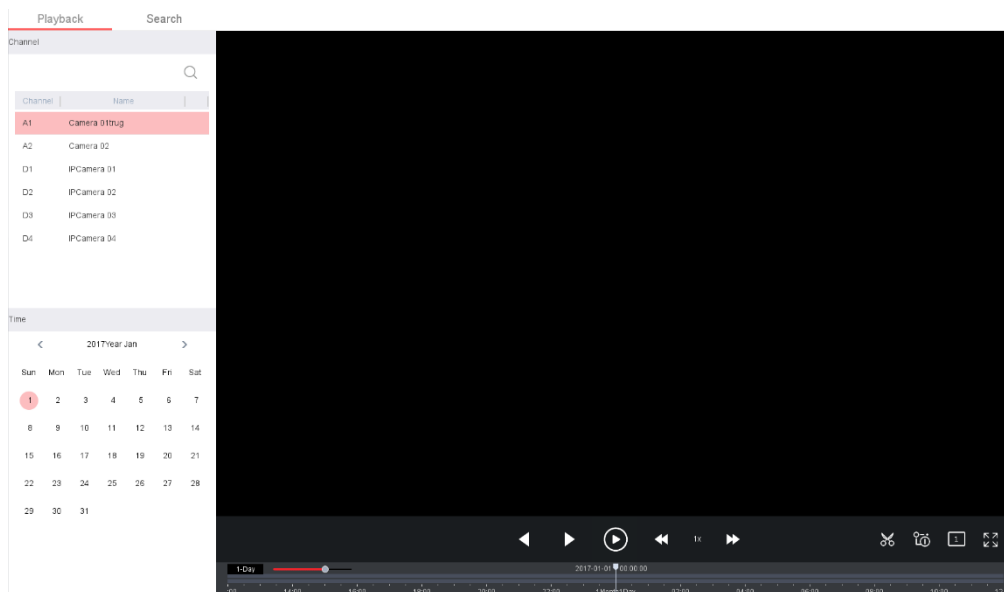
Single channel video playback means that only one channel video is played back at a time.

Step 1: Select "Playback" and enter playback interface.

Step 2: Check a video playback channel in the channel list.

Step 3: View the video of the current month in the calendar area. If there is video on that day, the background color of the date is green.

Step 4: Double click the date to be played back to start playing back the video of the channel.



Note:

After selecting the channel, the calendar area will automatically display the current month's videos. If there are videos on that day, the background color of the date will be green.

Multi-channel Playback

Multi-channel video playback means that the video of multiple channels is played back each time.

Step 1: Select "Playback" and enter playback interface.

Step 2: Check multiple channels to playback in the channel list.

Step 3: View the video of the current month in the calendar area. If there is video on that day, the background color of the date is green.

Step 4: Double click the date to be played back to enter multi-channel synchronous playback interface.

Note:

- The maximum number of ways to support simultaneous playback varies with different product models. Please refer to our official websites for details.
- If the selected channel exceeds the maximum number of simultaneous playback channels supported by the device, it will prompt "Exceed the Max. number of playback channels supported".
- When the channel is checked for multi-channel simultaneous playback, and the maximum number of simultaneous playback channels is not exceeded, the picture will automatically adapt to the number of playback channels. For example, if four channels are checked, the picture will automatically switch to four pictures
- The first progress bar displays the video information of the selected channel, and the second progress bar displays the video information of all channels.

- The intelligent search mode of full screen area intrusion is adopted by default. If no relevant information is found, the intelligent search method of full screen motion detection will be adopted.

Custom Playback

Custom playback function supports the retrieval according to the recording time, event type, goal characteristics, etc. and plays the video.

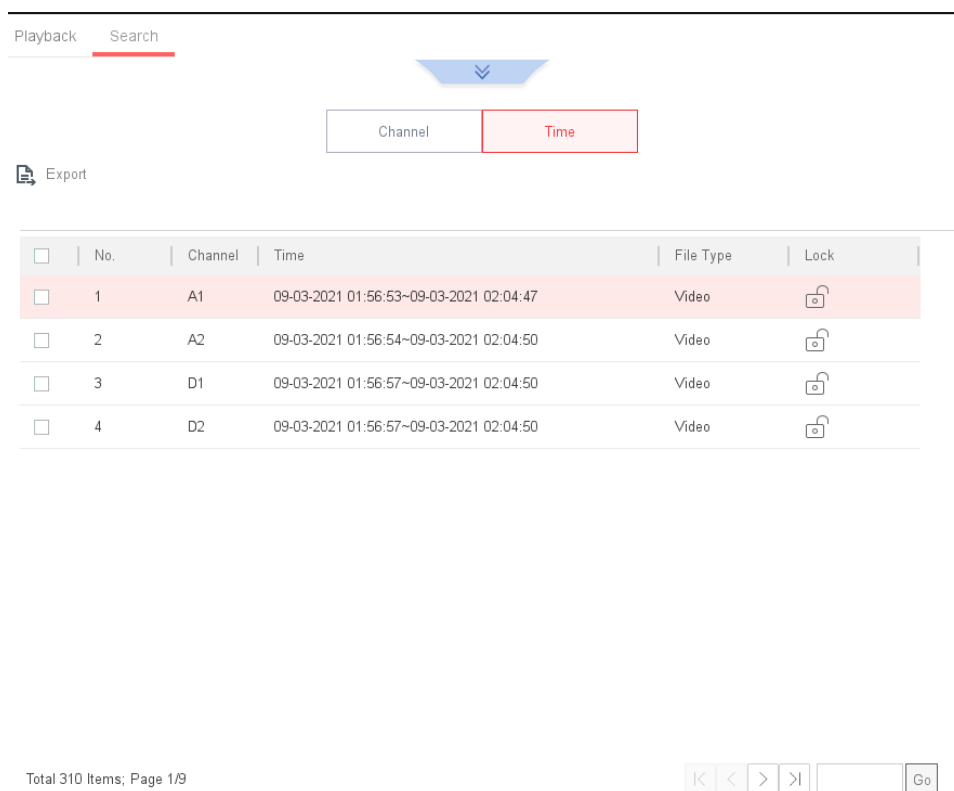
Step 1: Select “Playback” and enter playback interface.

Step 2: Select video playback channel and the calendar will automatically display the video of the current month.

Step 3: Set custom search conditions.

1. Click “Custom Search Conditions”

2. Click  to unfold the retrieval condition setting and redefine the search conditions.



Playback Search

Channel Time

Export

☐	No.	Channel	Time	File Type	Lock
☐	1	A1	09-03-2021 01:56:53~09-03-2021 02:04:47	Video	
☐	2	A2	09-03-2021 01:56:54~09-03-2021 02:04:50	Video	
☐	3	D1	09-03-2021 01:56:57~09-03-2021 02:04:50	Video	
☐	4	D2	09-03-2021 01:56:57~09-03-2021 02:04:50	Video	

Total 310 Items; Page 1/9

< < > > | Go

3. Input the retrieval conditions and click "Retrieval".

Note:

- Click “Unfolded” to unfold more conditions.
- Click “Empty Conditions” to restore the default search conditions.
- Click "Store" to submit to save the current search as a historical search record for next use.

4. Double click the search result to jump back, or click “Exit”

Step 4: Select “Custom” in the playback interface.

Step 5: View the video in the playback interface and carry out the related operation.

If "Skip Normal Video" is selected in Live View strategy, only red progress bar will be played (multi-channel and single channel are supported); if speed adjustment mode is selected, both red and blue will be played according to the set speed (single channel is supported only).

2.5 Picture Query

The device supports capturing alarm pictures into "Picture Query" for unified management. You can view pictures and related videos in this interface, and download them.

Note:

Please confirm that USB has accessed to the interface before exporting pictures,

The device supports export JPG. Pictures. When the pilot function is enabled, JPG and BMP pictures will be exported at the same time.

Step 1: Click “Picture” to enter the interface.

The screenshot displays the 'Picture Query' interface. At the top, there are filters for 'Time' (2021-04-02 00:00:00 - 2021-04-02 23:59:59), 'Picture ...' (Hazardous Goods), and 'Channel' ([A1] Camera 01). Below these are checkboxes for 'High', 'Medium', and 'Low' severity levels, each with an 'All' option. A list of hazardous goods types is shown with checkboxes: bottles, knives, guns, and umbrellas. There are 'Search' and 'Reset' buttons. Below the filters, there are 'Export Selected' and 'Export All' buttons. At the bottom, there is a table with columns: 'No.', 'Time', 'Hazardous Article Type', and 'Operation'. The table is currently empty. At the very bottom, there is a status bar showing 'Total 0 Items; Page 1/1' and navigation controls.

No.	Time	Hazardous Article Type	Operation
-----	------	------------------------	-----------

Step 2: Set query terms, including “Time”, “Picture Classification”, “Types of Dangerous Goods” and “Channel”.

Picture Classification: The analyzer can query 4 picture types, including package passed picture, behavior picture, manual capture picture and face detection picture.

Types of Dangerous Goods: including liquid, knives, guns, umbrellas, batteries, scissors, spray cans, mobile phones, laptops, lighters, handcuffs, fireworks, flickers, defibrillator, etc.

Step 3: Click “Query”

Step 4: Check the picture to be exported in the list below.

Step 5: Click “Download Selected” or “Download All”, the download progress can be viewed via progress bar.

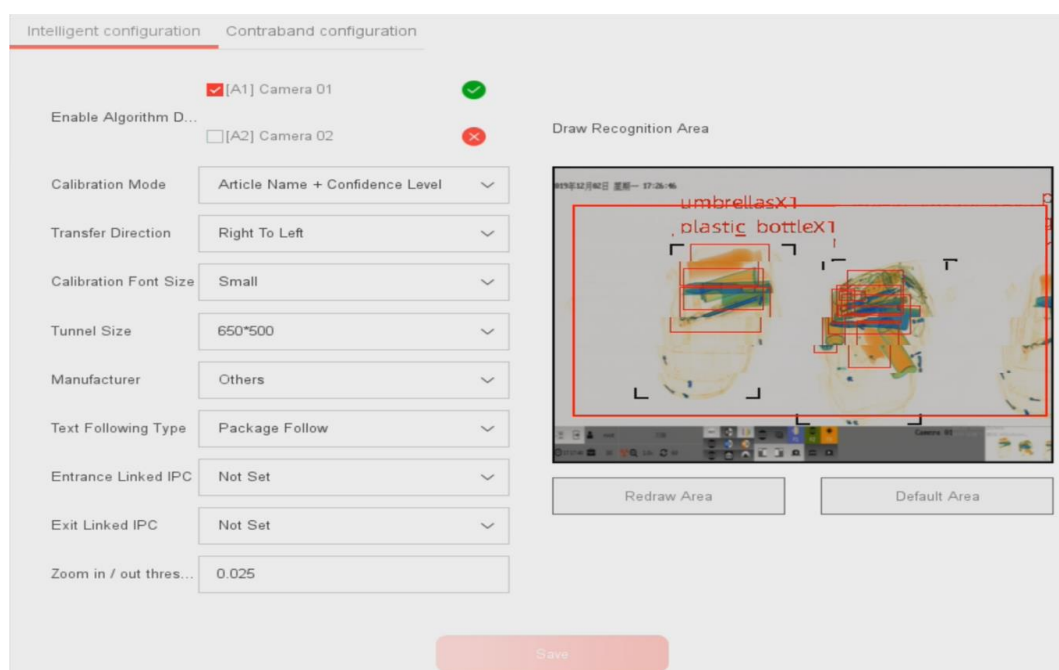
Note:

- You can click and view “Associated Video” in the picture details area on the right.
- You can click the "Download" icon corresponding to the picture in the picture list, or select the picture to download and click "Download Selected"; or click "Download All" to download the picture to the storage medium.
- You can also click "Play Associated Video" in "Associated Video Details" to view the video related to the package passed pictures. Click "Download Associated Video" to download the video to the storage medium.
- If the Live View interface has intelligent block diagram, the size and position of the block diagram captured will be consistent with the Live View interface.

2.6 Security

2.6.1 Intelligent Configuration

Step 1: Select “Security → Intelligent Configuration” and enter the interface.



Step 2: Select video input channel in the “Enable Algorithm Detection”

Note:

The icon  /  indicates the connection status of the channel a1 or a2.

The settings of the intelligent analysis interface will only take effect for the currently selected channel after saving.

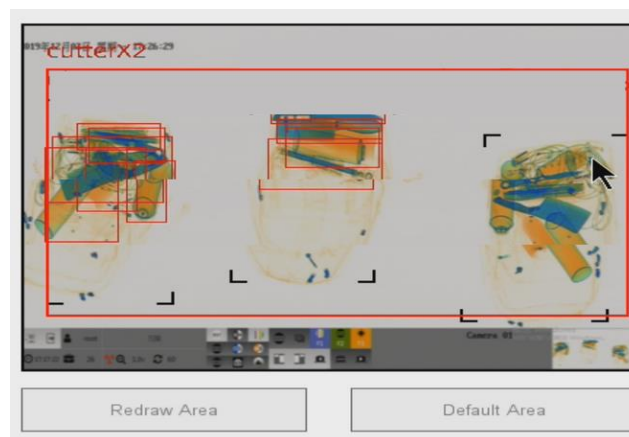
Step 3: Set "Security Check Configuration Info"

Set "Calibration Type", "Transfer Direction", "Calibration Font Size", "Tunnel Size", "Manufacturer" and "Text Following Mode", "Linked Enter/Exit IPC", "Zoom In/out threshold".

Note:

The direction of convey belt is configured incorrectly, which results in failure of intelligent recognition. And the wrong channel size configuration of security check machine may cause an exception for intelligent recognition.

Step 4: Draw the package passed pictures recognition area.



Select "Default Recognition Area" and the red box of default recognition area will appear automatically in the screen.

Select "Re-draw Recognition Area" and press the left button of mouse to draw the rectangular area in the screen.

Note:

The drawn recognition area cannot contain black objects or areas, or the smart recognizing function might not in proper service.

Stretch or drag to change the size or location of the drawn area.

Step 5: Click "Save".

2.6.2 Contraband Configuration

☒ Select All	Color	Grade	☐ Select All	☒ Select All	☒ Select ...	Linked C...	Filter Size	Edit
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	120*20	
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	100*20	
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	40*20	
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	100*20	
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	50*0	
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	100*0	
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	0*0	
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	0*0	
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	0*0	
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	0*0	
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	50*0	
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	0*0	
☒	Dark Red	High	☐ Buzzer	☒ Voice Pr...	☒ Alarm	Local->3	50*0	

Save

Step 1: Select “Security → Contraband Configuration”. In the list below, check different types of

prohibited items, recognize the type and click  “Edit” to set the color for different prohibited items. The color of the prohibited items not checked is dark red by default.

Step 2: In the “Prohibited Items Detection Configuration” list, click the alarm mode.

Audible warning: When alarm is happening, the device will beep for warning after checking.

Voice broadcast: When alarm is happening, the device will have a voice broadcast after checking.

Local ->1-4: Check the linkage alarm output channel when the event occurs.

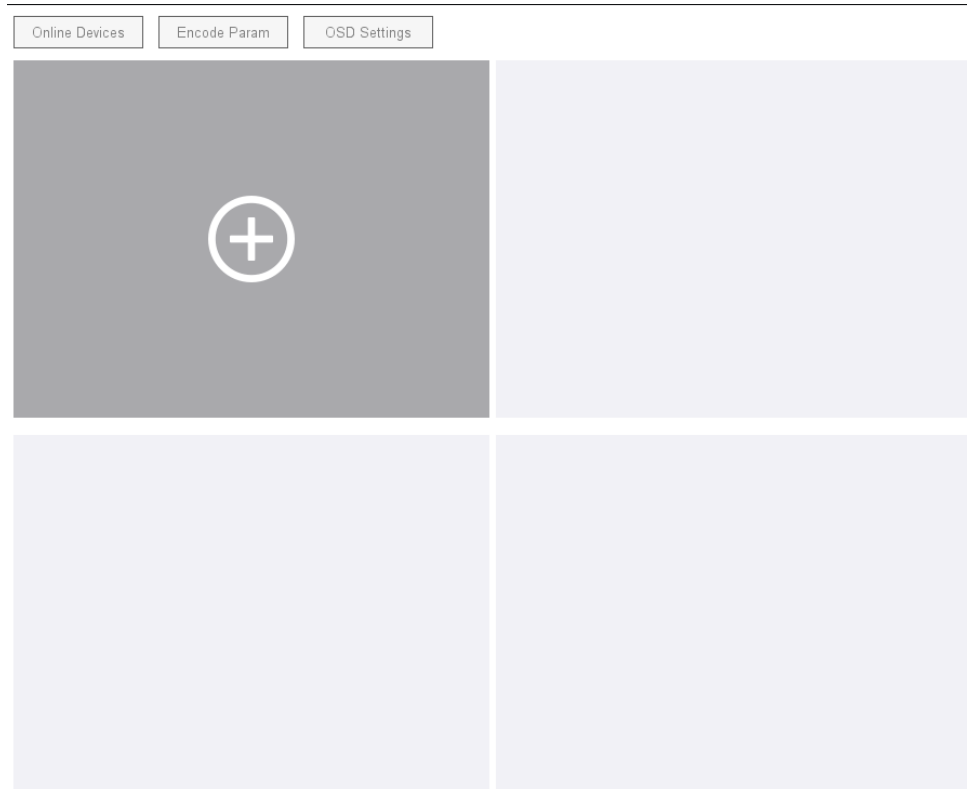
Step 3: Click “Save”.

Note:

- If the user do not draw the recognition area, the configuration parameters will not be saved.
- The intelligent analysis parameter configuration will take effect for both channels at the same time.

2.7 Camera

Click “Monitoring Configuration” to view current external monitoring equipment status.



Note:

The device supports access to 4 external devices. Only Channel 1 can add a security check gate. When the camera is connected, one of them supports behavior and the other supports face capture.

If there are no more than 4 devices added, you can move the mouse to the blank space and click "+" to add a webcam.

2.7.1 Online Device

Online webcam configuration

In the "Online Device", you can add a webcam and security check gate, view/delete the added cameras, upgrade the webcam, manage the protocol, and enable the automatic switching (H.265) function.

Note:

Only channel 1 can add a security check gate

Select the webcam in the list and click the "Edit" button to modify the network parameters of the webcam, such as IP channel address, protocol, port number, etc.

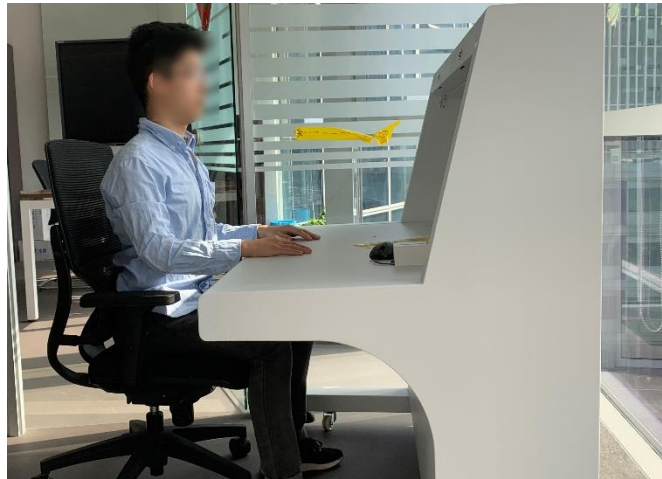
Note:

Installation instructions of webcam:

- Security check analyzer supports access to Hikvision brand webcam. Recommended type:

2mm length lens, wide angle lens (horizontal wide angle is also allowed). Please avoid using fixed focus camera.

- According to the requirements of personnel behavior algorithm, please ensure that the proportion of the head and shoulder of the operator in the image taken by the installation position of the webcam is less than 1/6 of the whole image.



- If there are many people in the monitoring range, you can draw the monitoring range in the local menu to select the operator position. If the monitoring range is not selected, the alarm linkage will only occur when no one is present by default.
- There is a certain probability to identify the object as the operator for the algorithm.

2.7.2 Coding Parameters

Recording parameters

Step 1 Select “Monitoring Settings → Coding Parameters → Recording Parameters”, and enter the interface of “Recording Parameters”.

Encode Param

Record Parameters

Sub-stream Parameters

Select Channel

[A1] Camera 01

Main Stream (Continuous)

Stream Type

Video

Resolution

1280*1024(SXGA)

Bitrate Type

Constant Bitrate

Video Quality

Medium

Frame Rate

30fps

Max. Bitrate Mode

General bit rate

Max. Bitrate (Kb...

2048

Recommended Max. Bitrate Range

2912~4853(Kbps)

Video Encoding

H.264

Main Stream (Event)

Stream Type

Video

Resolution

1280*1024(SXGA)

Bitrate Type

Constant Bitrate

Video Quality

Medium

Frame Rate

30fps

Max. Bitrate Mode

General bit rate

Max. Bitrate (Kb...

2048

Recommended Max. Bitrate Range

2912~4853(Kbps)

Video Encoding

H.264

Save

Step 2: Set recording parameters, and please refer to the following table for details.

Table 2-4 Recording Parameters Description

Parameter Name	Parameter Description	Parameter Settings
Channel Selection	Select the channel to set the recording parameters	Select via Dropdown List.
Types of Video Compression Parameters	Types of video compression parameters are divided into main stream (timing) and substream (event). ● Main stream (timing): Coding parameters of the normal video. ● Sub-stream (event): Coding parameters when the alarm input and other events occur.	Set respectively.
Bit Stream Type	The type is video stream.	Video Stream: Recording information only contains video information.
Resolution	Resolution is a measure of image fineness, which refers to the number of pixels per	Select via DrowDownList. Note: The resolution of recording is related to

23

Parameter Name	Parameter Description	Parameter Settings
	unit length.	IP device.
Bit Rate Type	Bit rate type is divided into variable bit rate and fixed bit rate. ● Variable bit rate: Bit rate will vary with scene, and video quality is adjustable in level 6. ● Fixed bit rate: The bit rate is encoded according to the upper limit of the bit rate, and the video quality is not adjustable.	Select via DrowDownList. Note: Bit rate type is related to the webcam channel.
Video Quality	It can only be set in the case of variable bit rate. The optional setting items are: highest, higher, medium, low, lower and lowest.	Select via DrowDownList.
Video Frame Rate	Video frame rate refers to the number of video frames per second, which is used to measure the number of display frames.	Select via DrowDownList. Unit: fps Value range: 1fps, 2fps, 4fps, 6fps, 8fps, 10fps, 12fps, 15fps, 16fps, 18fps, 20fps, 22fps, 25fps, 30fps and full frame rate can be selected. Note: Video frame rate is related to the IP device.
Bit Rate Limit Mode	Bit rate limit mode divided into general bit rate and custom bit rate (32-8192). ● General bit rate: The system offers fixed value parameters. ● Custom bit rate (32-8192): User inputs the value of bit rate.	Select via DrowDownList.
Bit Rate Limit (Kbps)	The bit rate limit (kbps) refers to the theoretical maximum bit rate and the reference value of recording coding.	● The bit rate limit mode is general bit rate Select via DrowDownList. The optional settings are 32Kbps~8192Kbps. ● The bit rate limit mode is custom bit rate Input manually via text box Setting range: 32Kbps~8192Kbps.
Recommended	According to the resolution and frame rate set by the user, an appropriate range	No need to set.

Parameter Name	Parameter Description	Parameter Settings
Range of Bit Rate Limit	of reference bit rate limit is recommended.	
Video Coding	Used to set the video coding format.	Select via DrowDownList. Note: Video coding format options are related to IP device. If the access IP device supports H.265, the video coding options are H.264 and H.265; if the access IP device does not support h.265, the video coding only displays the current video coding format. (H.264 or Mpeg4)

Step 3: Click “Apply” and save the settings.

Sub-stream Parameters Configuration

Sub-stream (network transmission) parameters are used for network transmission. When the network environment is not ideal, users can use the sub stream to Live View the network and reduce the transmission bandwidth. The sub-stream is also suitable for mobile phone monitoring.

The specific steps are as follows:

Step 1: Select “Monitoring Settings → Coding Parameters → Sub-stream Parameters”, and enter the interface of “Sub-stream Parameters”.

Step 2: Set sub-stream parameters, and please refer to the table below for details.

Table 2-5 Sub-stream Parameter Description

Parameter Name	Parameter Description	Parameter Settings
Channel Selection	Select the channel to set the recording parameters	Select via Dropdown List.
Bit Stream Type	The type is video stream.	Video Stream: Recording information only contains video information.
Resolution	Resolution is a measure of image fineness, which refers to the number of pixels per unit length.	Select via DrowDownList. Note: The resolution of recording is related to IP device.

Parameter Name	Parameter Description	Parameter Settings
Bit Rate Type	Bit rate type is divided into variable bit rate and fixed bit rate. ● Variable bit rate: Bit rate will vary with scene, and video quality is adjustable in level 6. ● Fixed bit rate: The bit rate is encoded according to the upper limit of the bit rate, and the video quality is not adjustable.	Select via Dropdown List. Note: Bit rate type is related to webcam channel.
Video Quality	It can only be set in the case of variable bit rate. The optional setting items are: highest, higher, medium, low, lower and lowest.	Select via Dropdown List.
Video Frame Rate	Video frame rate refers to the number of video frames per second, which is used to measure the number of display frames.	Select via DropDownList. Unit: fps Value range: 1fps, 2fps, 4fps, 6fps, 8fps, 10fps, 12fps, 15fps, 16fps, 18fps, 20fps, 22fps, 25fps, 30fps and full frame rate can be selected. Note: Video frame rate is related to the IP device.
Bit Rate Limit Mode	Bit rate limit mode divided into general bit rate and custom bit rate (32-8192). ● General bit rate: The system offers fixed value parameters. ● Custom bit rate (32-8192): User inputs the value of bit rate.	Select via DropDownList.
Bit Rate Limit (Kbps)	The bit rate limit (kbps) refers to the theoretical maximum bit rate and the reference value of recording coding.	● The bit rate limit mode is general bit rate Select via DrowDownList. The optional settings are 32Kbps~8192Kbps. ● The bit rate limit mode is custom bit rate Input manually via text box Setting range: 32Kbps~8192Kbps.
Recommended Range of Bit	According to the resolution and frame rate set by the user, an appropriate range of reference bit rate limit is	No need to set.

Parameter Name	Parameter Description	Parameter Settings
Rate Limit	recommended.	
Video Coding	Used to set the video coding format.	Select via DrowDownList. Note: Video coding format options are related to IP device. If the access IP device supports H.265, the video coding options are H.264 and H.265; if the access IP device does not support h.265, the video coding only displays the current video coding format. (H.264 or Mpeg4)

Step 3: Click “Apply” and save the settings.

2.7.3 Display Settings

Step 1: Select “Camera→ OSD Settings” to enter the interface.

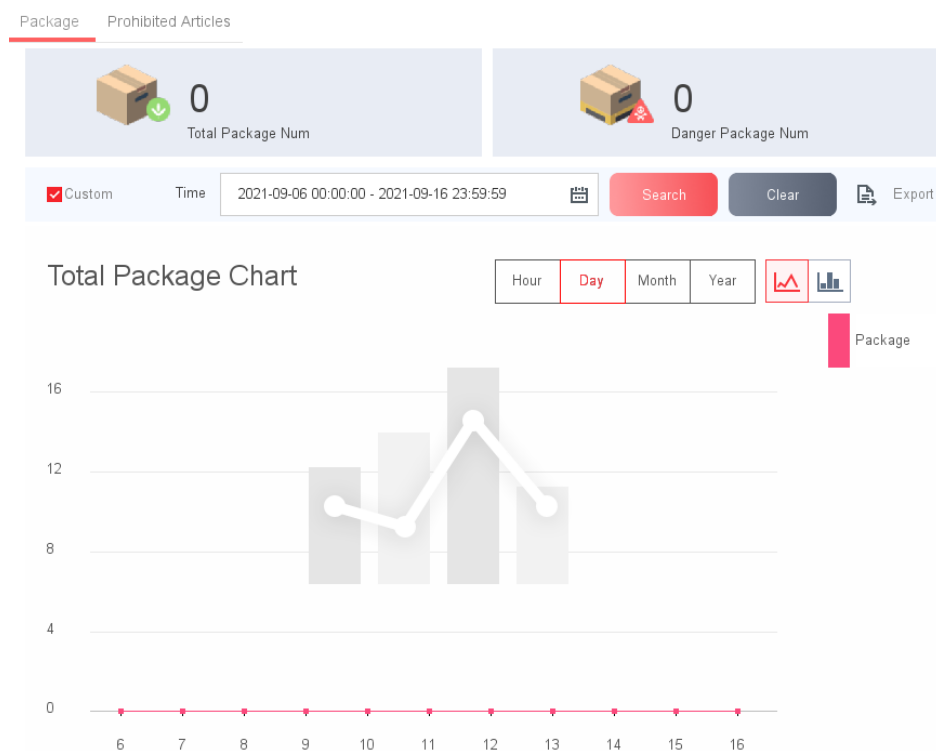
Step 2: Select a camera and enter the camera name.

Step 3: Set the OSD display scheme, date and time format, and image quality such as brightness, contrast, saturation, and hue.

In the data statistics interface, you can check the total number of packages passed and prohibited items, and check those quantity in the setting period.

2.7.4 Packages Passed Statistics

Step 1: Select “Data Statistics → Packages Passed Statistics” to enter the interface.

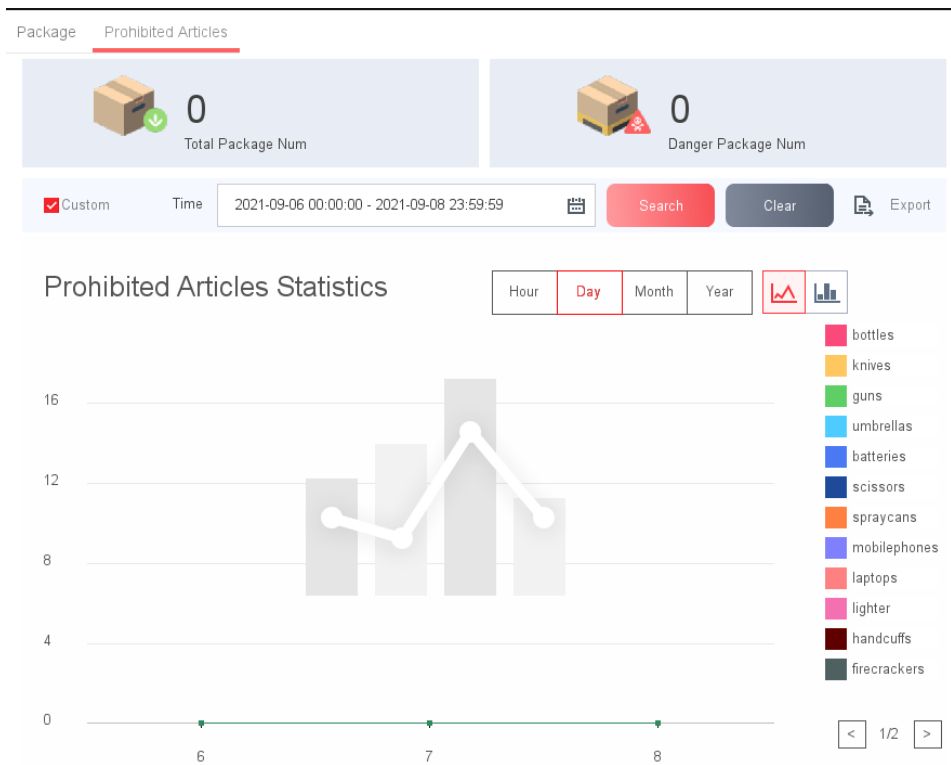


Step 2: Select statistical methods: Year (10 years), Day (30 days), Hour (24 hours).

Step 3: Select the time period need to view and click “Find”. The statistical data of the packages passed in the different periods of the set time can be obtained.

2.7.5 Prohibited Items Statistics

Step 1: Select “Data Statistics → Prohibited Items Statistics” to enter the interface.



Step 2: Select statistical methods: Year (5 years), Day (30 days), Hour (24 hours).

Step 3: Select the time period need to view and click “Find”. The statistical data of the prohibited items can be obtained in the different periods of the set time and the prohibited items will be unlabeled and displayed in different colors.

2.8 Storage

Select “Storage Management” and enter “Storage Device” interface.

Storage Device

Format Total Capacity 3726.02GB Remaining Capacity 3706.00GB

☐	Group ...	Capacity	Status	Property	Type	Free Space	Group	Load/Uninstall
☐	1	3726.02GB	Normal	Read/...	Local	3706.00GB	1	

Check the HD to be operated and click the “Format” in the top left corner. And click the “OK” in the pop-up window for initializing the HD.

Check the HD to be operated and click the “ ” at the end of the list. And click the “Yes” in the pop-up window to uninstall the HD.

2.9 System

2.9.1 General

Step 1: Select “System → General” to enter the interface of “General Configuration”.

General		User Settings	Network Settings	Event Settings	Live View Settings
Language	English				
Time Zone	(GMT+08:00) Beijing, Urumqi, Singapore				
Date Format	MM-DD-YYYY				
System Date	04-24-2024				
System Time	17:31:12				
Device Name	SecurityAnalyzer				
Device Code	255				
VGA/HDMI Resolution	1024*768/60HZ				
VGA2/HDMI2 Resolution	1024*768/60HZ				
Enable Wizard	☐				
Enable Password	☐				
Auto Reboot	☐				

Apply

Step 2: Set “VGA/HDMI Resolution”, “VGA/HDMI2 Resolution”, “Language”, “Time Zone”, “Date Display Format”, “System Date”, “System Time”, “Device Name”, “Device No.”, “Screen Saver Time”.

Step 3: Check whether to enable “Boot Wizard” and “Operation Password”, and “Auto Reboot” .

Step 4: Click “Apply”.

Pilot Function

The Live View interface will appear “False Alarm Capture” and “Missing Alarm Capture” icons after turning on the function.

User can click button for manual capture in the Live View interface.

The images can be seen according to the following steps after manual capture: “File Management → Manual Capture → False Alarm Capture / Missing Alarm Capture”.

2.9.2 User Settings

Note:

- The default administrator user name is admin.
- The administrator can add and delete the users and configure user parameters.

- The device can be added 32 users.

Caution:

- The administrator should configure the user rights properly, and it is recommended to use custom users for management in daily maintenance.
- It is recommended to update the password regularly and carry out an update maintenance every three months for improving the security of network usage. If the product needs high security requirements for the use environment, it is recommended to update it once a month or once a week.
- It is suggested that the administrator should effectively manage the device account and user rights, delete irrelevant users and rights, and close unnecessary network ports.
- When the user inputs the wrong password, the device will be prompted with locking information; when the admin user inputs the wrong password seven times in a row or the ordinary user inputs the wrong password five times in a row, the device will be in the locked state automatically.

Add Users

The specific steps are as below:

Step 1: Select “System → User Settings” to enter the interface of “User Configuration”.

General

User Settings

Network Settings

Event Settings

Live View Settings

+

Add

🗑

Delete

☐	No.	User Name	Security	Level	Operation
☐	1	admin	Weak	Administrator	✎ — —

Step 2: Click “Add” and the rights will be confirmed. Please input the admin password firstly, then user can be added after confirming.

Step 3: Edit the information of the new user and select the level.

Note:

- Supports English and digits naming.
- The password consists of 8-16 characters, including at least 2 of the following types: digits, lowercase letter, uppercase letter or special characters, and cannot contain username.

● The strength of the password is divided into 3 levels: weak, medium and strong. In order to protect personal privacy and enterprise data, and prevent the device from the network security problems, it is recommended that you set a strong password strength that meets the security specifications.

● There are two user levels: ordinary user and operator. The default rights of the two levels are different (the operator has all rights in the "Channel Configuration", while the ordinary user has only the rights of local playback and remote playback).

Step 4: Click "OK". Save and return the interface of "User Management".

Step 5: Select the user successfully added and click  to enter the interface of "Rights Configuration".

Step 6: Set the user rights.

Note:

● The user rights are divided into local configuration, remote configuration and channel configuration.

● After modifying any configuration rights, click "Apply" and save the modification.

Step 7: Click "OK", save and return to the interface of "User Management".

Rights Description

● Local configuration

- Local log search: view the system log and information.
- Local parameter settings: set parameter, restore default parameters, import / export parameters.
- Local advanced management: be able to carry out hard disk management (initialization, setting hard disk properties), upgrading system programs, and clearing IO alarm output.
- Local shutdown/restart: be able to carry out the operation of restart/shutdown.

● Remote configuration

- Remote log search: remote view logs recorded on the analyzer.
- Remote parameter settings: remote set parameter, restore default parameters, import / export parameters.
- Remote control serial port: built transparent channel and send/receive data of

RS232/RS485 port.

- Remote control local output: be able to send remote button.
- Remote alarm deployment, control alarm output: be able to carry out deployment remotely (it requires that send the alarm/abnormality status to the remote client.) and control alarm output.
- Remote advanced management: be able to remotely carry out hard disk management (initialization, setting hard disk properties), upgrading system programs, and clearing IO alarm output.
- Remote shutdown / restart: be able to remotely carry out the operation of restart/shutdown.

● Channel Configuration

- Remote Live View: Remote Live View scene of each channel.
- Local manual operation: local manual start / stop recording, local manual start / stop capturing, local manual start / stop alarming.
- Local playback: local playback of video files recorded on security check intelligent analyzer.
- Remote playback / download: remote playback and download of video files recorded on the security check intelligent analyzer.
- Local backup: local backup of video files recorded on the security check intelligent analyzer.
- Local Live View: local Live View scene of each channel.

Note:

- Only admin has the right of “Restore Default Parameter”.

- Channel configuration supports setting rights on a channel separately.

Delete User

The specific steps are as below:

Step 1: Select “System Management → User Configuration” to enter the interface of “User Configuration”, select the user and click “Delete”.

Step 2: Click “Yes”, and finish the operation.

Edit User

The specific steps are as below:

Step 1: Select “System Management → User Configuration” to enter the interface of “User

Configuration”, select the user to be modified and click “Modify”.

Step 2: Edit user information. Modify the username, password, user level and MAC address, etc.

Note:

- Only the super admin has the right to modify the password of admin account.
- The super admin can modify the password of ordinary user or operator.
- Ordinary user or administrator can modify their own password.

Step 3: Click “OK” and save the information.

Note:

- Supports English, digits and Chinese naming.
- Supports ordinary users to modify their own password.
- There are two levels of user level: ordinary user and operator. The default rights of the two levels are different (the operator has all rights in the "Channel Configuration", while the ordinary user has only the rights of local playback and remote playback).

2.9.3 Network Settings

Basic Configuration

TCP/IP Configuration

Step 1: Select “System → Network Settings” to enter the interface of “Basic Configuration”.

The screenshot displays the 'Network Settings' page of a device management interface. The left sidebar contains menu items: Picture, Statistics, Security, Camera, Storage, System (highlighted), Maintenance, Playback, and Platform. The main content area has tabs for General, User Settings, Network Settings (active), Event Settings, and Live View Settings. Under Network Settings, there are sub-tabs: TCP/IP (active), NTP, 4G, and Access Platform. The configuration fields include:

- Working Mode:** Multi-address Settings (dropdown)
- Network Card:** NIC1 (dropdown)
- Network Card Type:** 10M/100M/1000M Self-Adaptive (dropdown)
- DHCP:** Disabled (toggle)
- IPv4 Address:** 10 . 6 . 113 . 12
- IPv4 Subnet:** 255 . 255 . 255 . 0
- IPv4 Default Gateway:** 10 . 6 . 113 . 254
- MAC Address:** 98:df:82:e1:2b:8f
- MTU(Bytes):** 1500
- Default Route:** NIC1 (dropdown)
- Auto Get DNS Server:** Disabled (toggle)
- Preferred DNS Server:** 10 . 1 . 7 . 97
- Alternative DNS Server:** 10 . 1 . 7 . 98
- Destination Address:** (empty field)

Buttons for 'Test' and 'Apply' are located at the bottom right of the configuration area.

Step 2: Select “Work Mode”, “Network Card” and network card type.

Note:

NIC 1 connects to the network. You can connect IPC to NIC 2 interface with cables.

Step 3: Check “Auto Obtain IPv4 Address”, or set manually network parameters.

Step 4: Set MTU and select default route.

Step 5: Click “Apply” and save the settings.

Step 6: Select whether to open DNS server, fill in the preferred and alternative server address.

Note:

When selecting the network card, please pay attention to the specific location of LAN1 and LAN2 in the device as shown below.

NTP

Enable NTP, the device can be regularly timed via NTP server to ensure the accuracy of system time.

General User Settings **Network Settings** Event Settings Live View Settings

TCP/IP **NTP** 4G Access Platfo...

Enable ☒

Timing Interval (...) 60

NTP Server Add...

NTP Port 123

Apply

Step 1: Select “System Configuration → Net Configuration” to enter the “Basic Configuration” interface of “Net Configuration”.

Step 2: Select “NTP” property page and set NTP relevant parameters.

- The time interval of timing is 1-10080 minutes. The default is 60 minutes.
- If the device is connected to the public network, please fill in the NTP server address that provides timing function, such as 210.72.145.44 (IP address of national time service center server).
- If the device is connected to the private network, NTP server can be set up via NTP software for timing.

Step 4: Click “Apply” and save the settings.

4G

Enable 4G function to connect to 4G network and view signal strength.

Note:

Only devices with 4G module function support 4G related network configuration.

Step 1: Select “System Configuration → Net Configuration” to enter the “Basic Configuration” interface of “Net Configuration”.

Step 2: Select “4G” property page and enter “4G” interface.

Step 3: Check enable 4G.

Step 4: View 4G “Signal Strength”.

Platform Access

The device supports access to the intelligent security check management platform.

Step 1: Select “System Configuration → Net Configuration” to enter the “Advanced Configuration” interface of “Net Configuration”.

The screenshot shows a settings application with a top navigation bar containing 'General', 'User Settings', 'Network Settings' (highlighted with a red underline), 'Event Settings', and 'Live View Settings'. Below the navigation bar is a sub-menu with four tabs: 'TCP/IP', 'NTP', '4G', and 'Access Platform' (highlighted with a red border). The 'Access Platform' page contains the following configuration options:

- Enable:** A green toggle switch is turned on.
- Access Type:** A dropdown menu showing 'isup5.0'.
- Access service IP:** An empty text input field.
- Access service Port:** A text input field containing '7031'.
- Enrollment Status:** A label showing 'Offline'.
- Device ID:** A text input field containing 'G64279165'.
- Secret Key:** An empty text input field.

At the bottom of the page is a red 'Apply' button.

Step 2: Check “Enable”.

Step 3: Configure “Access Type”, “Access Server IP”, “Access Server Port”.

Step 4: Click “Apply” and save settings.

2.9.4 Event Settings

Alarm Input

Step 1: Select “System → Event Settings → Alarm Input” and enter the alarm input interface.

Edit

Alarm Input No.

Local<-1

Alarm Type

N.O

Alarm Name

Enable

Arming Schedule

Linkage Action

☐ Normal Linkage	☐ Trigger Alarm Output	☐ Recording Lin...
☐ Audio Warning	☐ Local->1 ☐ Local->2	☐ A1 ☐ A2

Copy to

Apply

Edit

Step 2: Click “Edit”  .

Step 3: Set the alarm type of this alarm input and check “Alarm Input”.

Step 4: Select alarm type and fill in the alarm name.

Step 5: Select “Deployment Time” property page, and enter this interface.

Step 6: Set the deployment period for this channel and select “Week” as some day of the week to configure this day.

Note: Each time period cannot be crossed and included.

Step 7: Click “Linkage”, enter motion detection linkage interface, and select normal linkage, linkage alarm output and record linkage.

Step 8: Set linkage option parameters.

Note:

Alarm input can trigger the call of preset points, cruises and tracks of multiple channels, but only one of them can be called (mutual exclusion setting of linkage state).

Step 9: Click “Apply” and finish the settings.

Note:

If the settings of other channels are the same as that of this channel, click “Copy to...” and enter the interface. Select the alarm input to be copied and copy the alarm input processing mode to other channels.

Alarm Output

Linkage alarm output can be set when alarming.

Step 1: Select “System→ Event Settings→ Alarm Output” and enter the alarm output interface.

Step 2: Click the alarm output to be set and “Edit”  to enter the interface of alarm output deployment time.

Step 3: Set the alarm output delay, name and deployment time. Select “Week” as some day of the week to configure this day.

Note:

- If "manual clear" is selected for time delay, when an alarm occurs, the "Trigger" in the alarm output interface will change to "Clear", and the alarm can be eliminated only by clicking the "Clear" button.

- Each time period cannot be crossed and included.

- 8 periods can be set in a day at most.

Step 5: Repeat the above steps and set the deployment plan of the whole week.

Note: If the plan of other date is the same as it, click “Copy” and copy to other time.

Step 6: Click “OK” and finish the settings.

Note:

Click “Copy to...” to copy the settings to other channels if their settings are the same as it.

Exception Settings

Exception Settings is the warning of abnormal events. Exception events include hard disk full (when hard disk space is recorded fully), hard disk error (when writing hard disk or hard disk is not initialized), network disconnection (without connecting to network cable), IP conflict, illegal access (user password error), exception record / capture (such as no video hard disk), and all types.

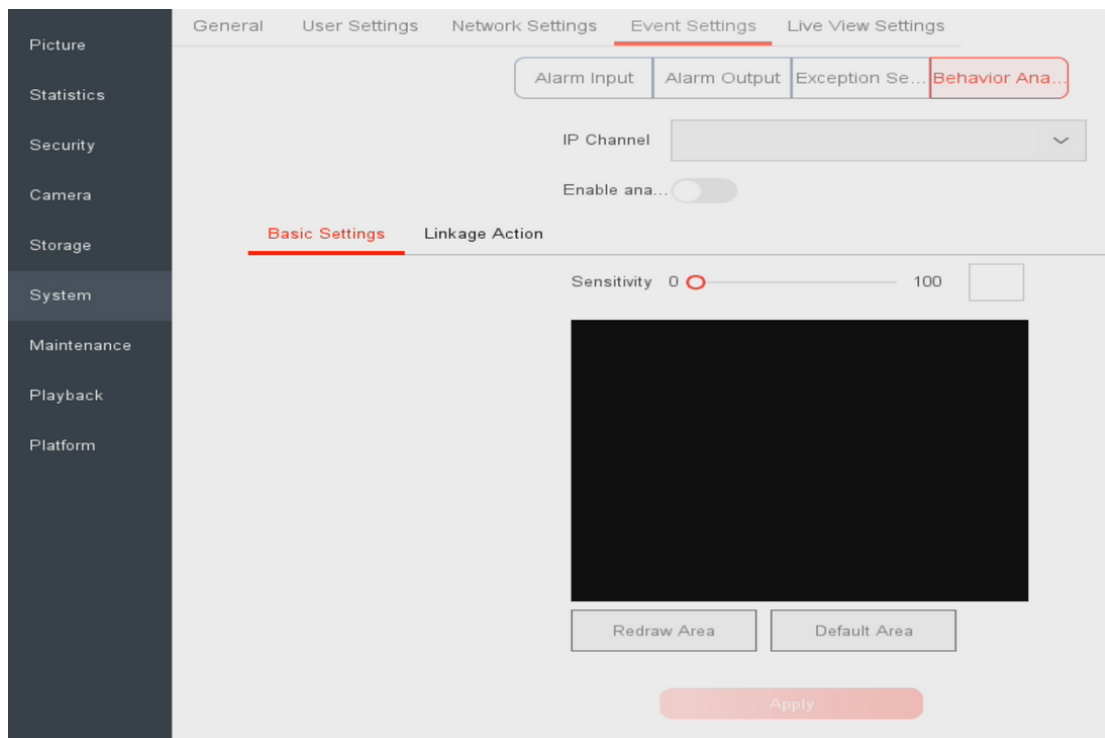
Step 1: Select “System → Event Settings → Exception Settings” and enter the exception settings interface.

Step 2: Set the exception parameters, including exception type, audio warning and trigger alarm output, etc.

Step 3: Click “Apply” and save settings.

Behavior

Step 1: Select “System→ Event Settings → Behavior” and enter the operator behavior interface.



Step 2: Select the channel to alarm and check “Enable Analysis”.

Note:

The operator behavior device only supports one webcam channel for behavior. If one webcam channel has enabled behavior, other channels will not be able to enable it.

Step 3: Draw the area of operator behavior detection.

Step 4: Set operator behavior sensitivity (0~100).

Step 5: Set the deployment period for this channel and select “Week” as some day of the week to configure this day.

Note: Each time period cannot be crossed and included.

Step 6: Click “Linkage Method”, enter motion detection linkage interface, and select normal linkage and linkage alarm output.

Step 7: Click “Apply” and finish settings.

2.9.5 Live View Settings

Users can set Live View display mode, channel display order and polling switch time in “Live View Configuration”.

Step 1: Select “System→ Live View Settings→ Basic Configuration” and enter the basic configuration interface.

Step 2: Select output port and set panel array mode of Live View.

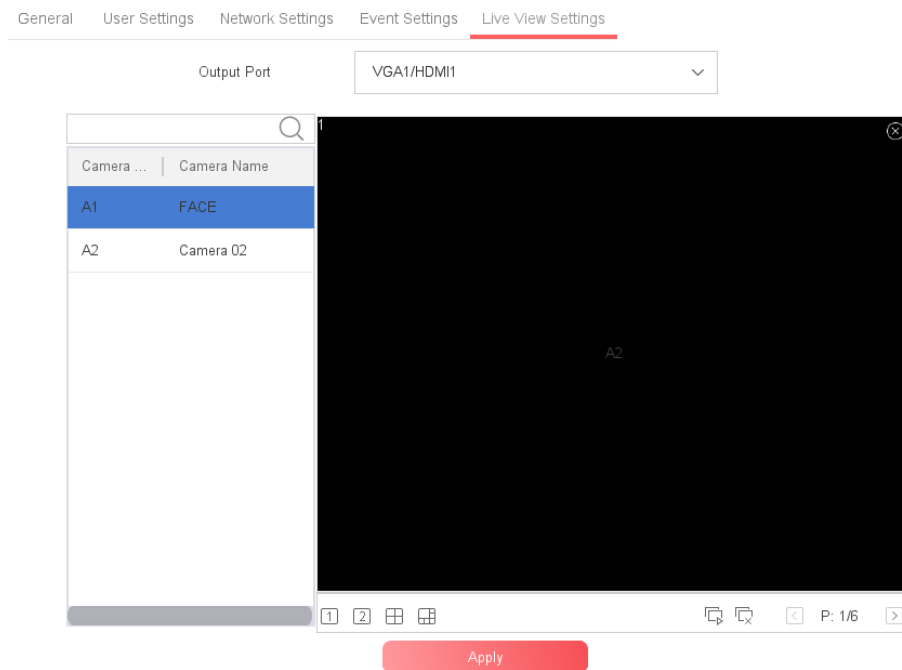
Note:

- If VGA2 / HDMI2 is selected as the output port, only A1 or A2 channel can be selected, and only 1 image Live View is supported.
- The auxiliary screen can only display the image of analog channel.

Step 3: Set channel Live View display order.

The details are as below (Take channel A1 and A2 Live View display position exchange as an example.):

1. Select “View Configuration” property page.
2. Click the area on the right and select A2 to make it selected, as shown in the figure.



3. Move the mouse to select A1 on the left, and double-click A1. At this point, the first window automatically becomes A1, and the second window becomes “+ Channel Number”.
4. Click the second window in the right area to make it selected.
5. Move the mouse to select left A2 and double-click it. At this point, the second window automatically becomes A2.

Note:

User can click “Open All Live View” at the bottom right or “Close All Live View” to carry out quick operation.

Step 4: Click “Apply” and save the settings.

Note:

If the user needs to turn on the function of Live View automatic polling, the polling time interval need to be selected on the “Switching Time”. The optional settings are: no switching, 5 seconds, 10 seconds, 20 seconds, 30 seconds, 60 seconds, 120 seconds and 300 seconds.

2.10 System Maintenance

2.10.1 Security Check Info

Enter the page and input security check machine information.

[Security Check Info](#) [System Info](#) [Log Info](#) [Config](#) [Upgrade](#) [Default](#) [Network Resource Statistics](#) [Advanced](#)

Manufacturer

Others

Model

Angle of View

Single View

Year of Starting

0

Year

Save

2.10.2 System Info

Device Information

View device information including device name, model, and serial number.

Channel Status: View channel status.

Recording Status: View recording status and encoding parameters of each channel.

Alarm Status: View status of each alarm input and output and event linkage.

Network Status: View network connections and configuration properties of the device.

Hard Drive Status: View the status and property information of the connected hard disk.

Picture

Statistics

Security

Camera

Storage

System

Maintenance

Playback

Platform

Security Check Info

System Info

Log Info

Config

Upgrade

Default

Network Resource Statistics

Advanced config

Device Info

Version Info

Network Status

Device Name	SecurityAnalyzer
Model	ISD-ST9204D-DHV4G
Serial No.	ISD-ST9204D-DHV4G162022022AARRJ51869396WVU
Input Channel No.	2
Output Channel No.	2
Network Camera No.	0
HDD No.	1
HDD Capacity	3726.02GB
Alarm Inputs	2
Alarm Outputs	3

Version Info

Select “Maintenance → System Info → Version Info” to view the version information of the device.

Picture

Statistics

Security

Camera

Storage

System

Maintenance

Playback

Platform

Security Check Info

System Info

Log Info

Config

Upgrade

Default

Network Resource Statistics

Advanced config

Device Info

Version Info

Network Status

Firmware Version

V1.8.1, Build 220217

Algorithm Version

V2.0.0, Build 211206

Engine Version

V2.0.3, Build 220210

Extended Board Version

V1.8.1, Build 220217

Model Version

V2.0.0, Build 211110

MCU Version

Build 211008

FPGA Version

Build 210913

MSTAR Version

Build 220111

Network Status

View network connections and configuration properties of the device.

Picture

Statistics

Security

Camera

Storage

System

Maintenance

Playback

Platform

Security Check Info

System Info

Log Info

Config

Upgrade

Default

Network Resource Statistics

Advanced config

Device Info

Version Info

Network Status

NIC	LAN1	LAN2
IPv4 Address	10.6.113.12	169.254.72.231
IPv4 Subnet Mask	255.255.255.0	255.255.0.0
IPv4 Default Gateway	10.6.113.254	0.0.0.0
IPv6 Address 1	fe80::9adf:82ff:fee1:2b8f/64	fe80::9adf:82ff:fee1:2b90/64
IPv6 Address 2	fe80::9adf:82ff:fee1:2b90/64	
IPv6 Default Gateway		
MAC Address	98:df:82:e1:2b:8f	
Preferred DNS Server	10.1.7.97	
Alternative DNS Server	10.1.7.98	
Enable DHCP	Enable	
Enable PPPoE	Disable	
PPPoE Address		
PPPoE Subnet Mask		

2.10.3 Log Information

Search and Export Logs

Step 1 Click **Maintenance** → **Log Information** to enter the Search Logs page.

Security Check Info System Info **Log Info** Config Upgrade Default Network Resource Statistics Advanced config

Time 2021-09-13 00:00:00 - 2021-09-13 23:59:59

Major Type All Type Sub Type ☒ Select All

Search Export Log

- ☒ Alarm Input
- ☒ Alarm Output
- ☒ Face Detection Alarm Started
- ☒ Face Detection Alarm Stopped
- ☒ Illegal Access
- ☒ HDD Full
- ☒ HDD Exception
- ☒ IP Address Conflict
- ☒ Network Cable Disconnected
- ☒ Record/Capture Exception
- ☒ IP Camera Disconnected
- ☒ Dial Exception

Step 2 Set the search conditions and click **Search** to display the log list.

Note

If more than 2000 logs are found, the system will display the first 2000 logs.

Step 3 Search and Export Logs.

- For detailed log information, click  or left double-click the log information to enter the log details page.

- Click **Previous** or **Next** to display the previous log details or the next log details.
- Click **OK** to return to the log list page.

- Export log information in the search list.

1. Select the log information you want to export.
2. Click **Export** to enter Export Logs page.
3. Click **Export** and the prompt “Logs are exported.” will pop up.
4. Click **OK** to view the exported log information.

Note: Make sure that the backup device is connected before you export logs. The log file is a txt text file named after the log export time, such as 20160617145846logBack.txt.

Export All Logs

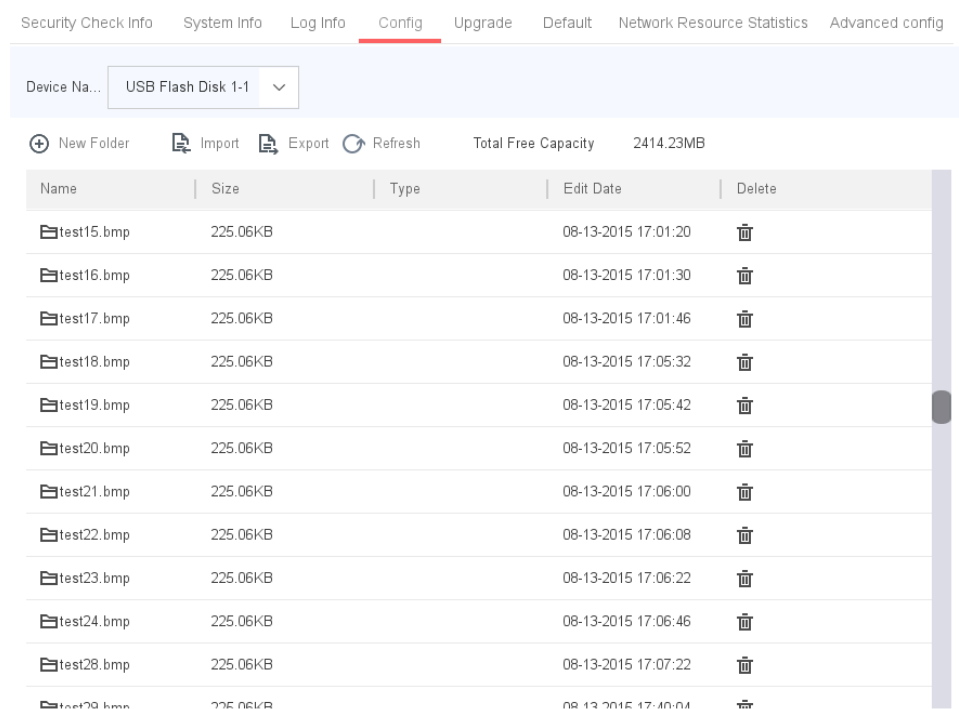
To export all logs, click **Export All** to export all log information of the hard disk to the U disk.

2.10.4 Configuration Settings

Export configuration file of the device to facilitate timely backup of the configuration file. If multiple devices use the same settings, importing configuration file of the device is more time-efficient.

Export Configuration Files

Step 1 Click **Maintenance** → **Config Settings**.



Step 2 Select the device name.

Step 3 Click **Export**, and the export encryption window will pop up.

Step 4 Set the password and click **OK**.

The device prompts "The configuration files are exported." message and the configuration file is displayed in the list column.

Import Configuration Files

Step 1 Click **System Maintenance** → **Configuration Settings**.

Step 2 Select the device name and the configuration file to be imported in the list column.

Step 3 Click **Import** and the import decryption window will pop up.

Step 4 Enter the decryption password when you export the configuration file, click **OK** and the confirmation window will pop up.

2.10.5 Upgrade

Step 1 Click **Maintenance** → **Upgrade** to enter the Upgrade page.

Security Check Info System Info Log Info Config Upgrade Default Network Resource Statistics Advanced config

Device Na... USB Flash Disk 1-1 ▾

Upgrade Refresh

File Name	File Size	File Format	Edited On	Delete
test15.bmp	225.06KB		08-13-2015 17:01:20	
test16.bmp	225.06KB		08-13-2015 17:01:30	
test17.bmp	225.06KB		08-13-2015 17:01:46	
test18.bmp	225.06KB		08-13-2015 17:05:32	
test19.bmp	225.06KB		08-13-2015 17:05:42	
test20.bmp	225.06KB		08-13-2015 17:05:52	
test21.bmp	225.06KB		08-13-2015 17:06:00	
test22.bmp	225.06KB		08-13-2015 17:06:08	
test23.bmp	225.06KB		08-13-2015 17:06:22	
test24.bmp	225.06KB		08-13-2015 17:06:46	
test28.bmp	225.06KB		08-13-2015 17:07:22	
test29.bmp	225.06KB		08-13-2015 17:40:04	

Step 2 Select the upgrade file and click Upgrade. The system starts to upgrade.

Note

- Restart the device to update after upgrading.
- If the upgrade fails and the device fails to work normally after startup, contact the supplier.

2.10.6 Default Settings

Step 1 Click **Maintenance** → **Default** to enter the Default Settings page.

Security Check Info System Info Log Info Config Upgrade Default Network Resource Statistics Advanced config

Restore Default Settings Partly Restore

Restore Factory Settings Restore All to Factory Settings

Restore Inactive Status Restore to Inactive Status

Step 2 Select the default settings type.

- If you select **Restore Default Parameters**, all parameters except time, user account, IP address, subnet mask, default gateway, MTU, and server port number will be restored to factory settings.
- If you select **Restore to Factory Settings**, all parameters will be restored to factory settings.
- If you select **Restore to Inactivated State**, the admin password will be blank, all user accounts

will be deleted, and other parameters will not be restored.

Step 3 A prompt will pop up. Click **Yes** to restart the device.

Note

After the default configuration, some or all parameters will be restored to default settings.

2.10.7 Network Resource Statistics

You can view the network access status in the network resource statistics page. Viewing via remote access will occupy the device's network output bandwidth. You can view the device's network access bandwidth in real time in the network resource statistics page.

Click **Maintenance** → **Network Resource Statistics** to enter the page.

Security Check InfoSystem InfoLog InfoConfigUpgradeDefaultNetwork Resource StatisticsAdvanced

Refresh

Type	Bandwidth
IP Camera	0bps
Remote Live View	0bps
Remote Playback	0bps
Net Total Idle	
Net Receive Idle	256Mbps
Net Send Idle	200Mbps

You can view resource statistics including network transmission surplus, remote Live View bandwidth, remote playback and downloaded files and grasp the system network status in real time.

2.10.8 Advanced Settings

The advanced settings interface is for technical supporter to maintain the system. You can export pilots, edit the parameters of EDID, package detection and export maintenance information.

Security Check Info	System Info	Log Info	Config	Upgrade	Default	Network Resource Statistics	Advanced config
Pilot export	EDID config	Package Det...	Confidence ...	Maintenance ...	pos set	pkg assoc set	
Time	2024-04-24 00:00:00 - 2024-04-24 23:59:59		Channel	[A1] Camera 01		Search	Reset
Type	All		Export All				
No.	Time	Hazardous Article Type					

Pilot Export

Select “Maintenance → Advanced Config → Pilot Export”, choose time and channel, click “Search”, you can export related content.

EDID Config

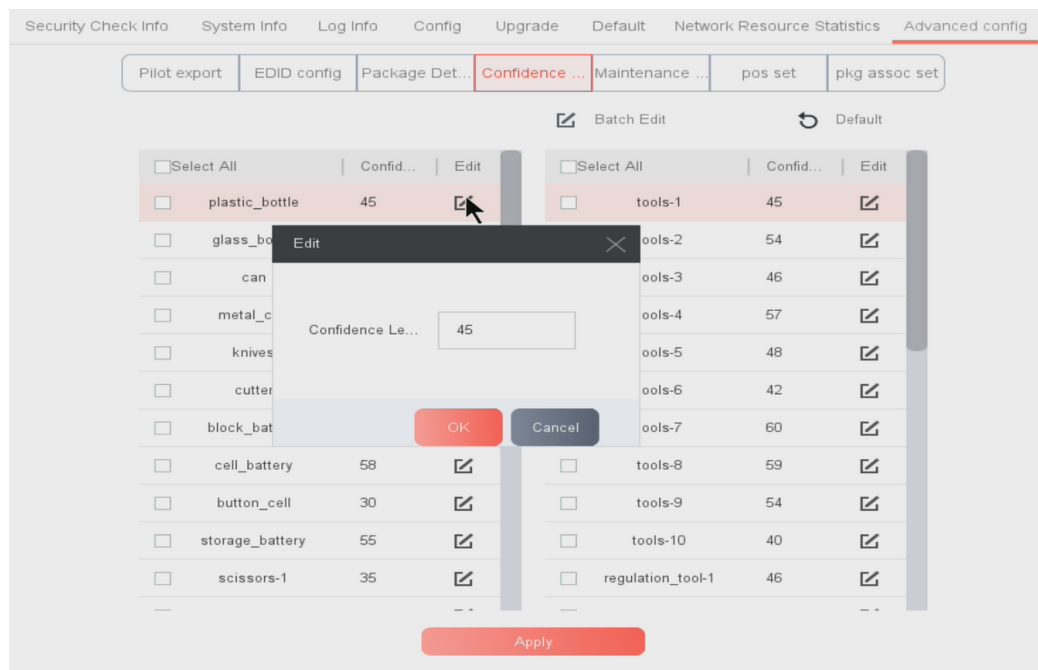
Select “Maintenance → Advanced Config → EDID Config”, you can configure EDID parameters.

Package Delete Config

Technicians can set the parameters of package delete config and enable Pk mode.

Confidence Level

“Maintenance → Advanced Config → Confidence”, Click Edit and you can set the confidence level of the check goods.

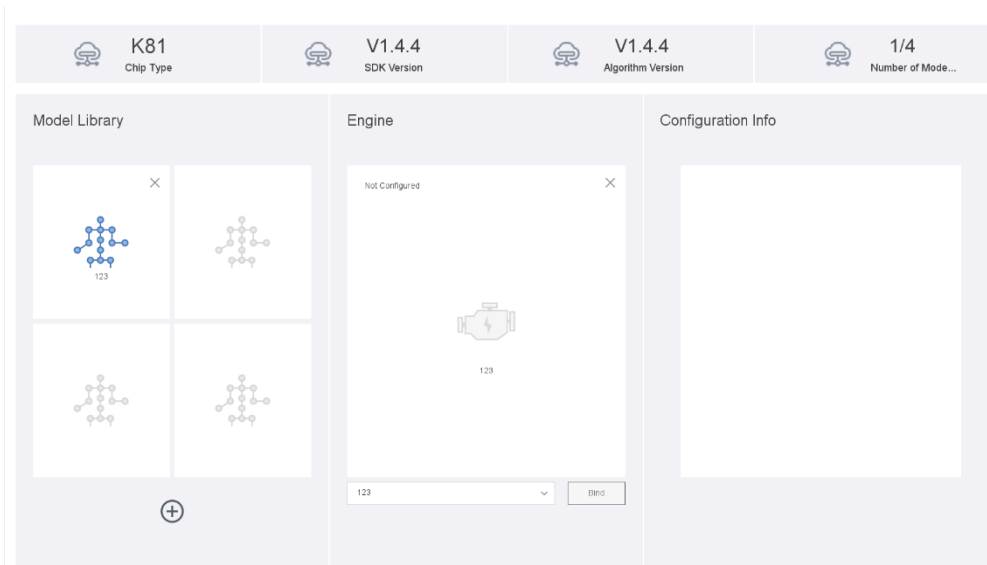


Maintenance Information Export

In “Maintenance → Advanced Config → Maintenance Information Export” interface, you can export the maintenance information.

2.11 Platform

You can view the SDK version, algorithm version and other information of the device, and import the model library file input from the AI open platform for application in the actual security check environment.



Step 1 Select **Open Platform** to enter the page.

Step 2 Click **+**, select the model file and Label file, create the model name, and click **OK**.

Step 3 Select a model in Engine Section and click **Binding**.

Then you can view related information in the Configuration Information Section.

Step 4 Start the task in Configuration Information Section.

Step 5 Save the settings.

2.12 Others

2.12.1 View Alarms & Exceptions



Step 1 Click  in the upper right corner of the page to enter the Alarm Information page. You can view abnormal alarm, regular alarm, or intelligent alarm information in this page.



Step 2 Click  to set the event notification type, including full hard disk, hard disk error, network disconnection, IP conflict, illegal access, video signal loss, abnormal recording/capture, etc.

2.12.2 View Backups



Step 1 Click  in the upper right corner of the page to enter the View Backup page. You can view the backup progress in this page.



Step 2 Click  to check the remaining space of the backup media and perform related configurations, such as New Folder, Format, etc.

3 Remote Operation

After the device is connected to the network, the device can be operated remotely via the web

page.

3.1 Login and Activate the Device

3.1.1 Login

Step 1 Use a network cable to connect the device to the network.

Step 2 Modify the network configuration according to the local network IP.

Step 3 Enter the IP address of the device in the browser address bar.

Step 4 Enter the user name and password to log in to the device web terminal.



- When you log in to the device for the first time, the page will prompt 'lease click here to download and install the plug-in. Close the browser when installing the plugin.'. Follow the prompts to download and install the plug-in.
- If the HTTP port is not set to 80, please enter "http://IP address: port number" in the address bar of the browser, such as http://192.168.1.64:81.
- When the password is wrong, the browser will prompt a lock message reminder. When the admin user enters a wrong password 7 times or the ordinary user enters a wrong password 5 times, the device will lock the user account for 30 minutes.

3.1.2 Activation

The first time you use the device, you will need to activate the device and create a login password.

The activation steps are as follows:

Step 1 In a web browser on your PC, enter the IP address. The activation page opens.

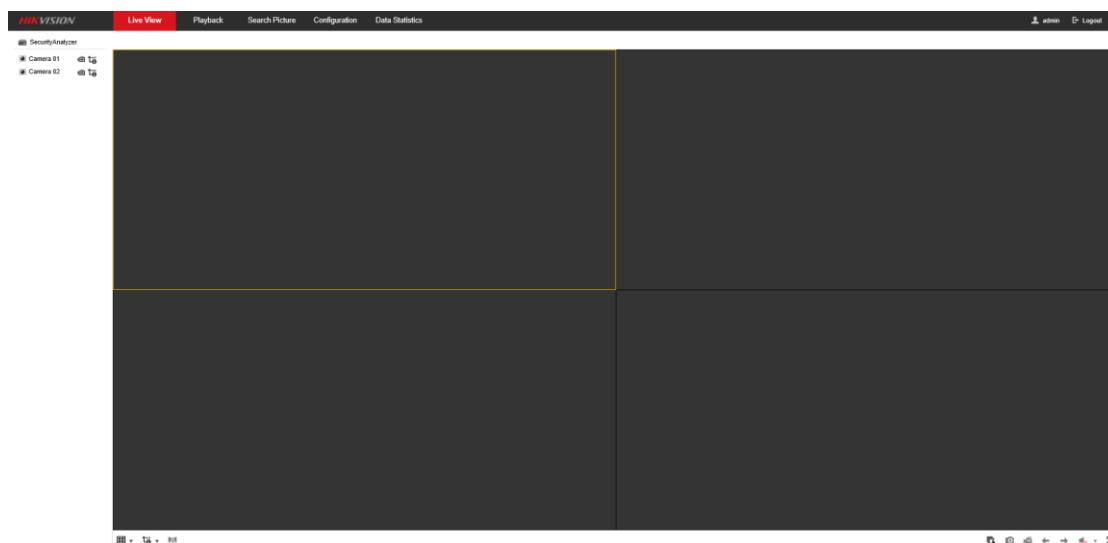
Step 2 Enter a password and confirm it.

Note:

- Default User Name: admin.
- The password should be 8 to 16 characters in length and contain two or more of the following categories: numbers, lowercase letters, uppercase letters, and special character.
- We provide the following levels of password security: low, medium, and high. To protect your personal privacy, corporate data, and network security of your device, we

recommended that you set a high-security level password that complies with security regulations.

3.2 Live View



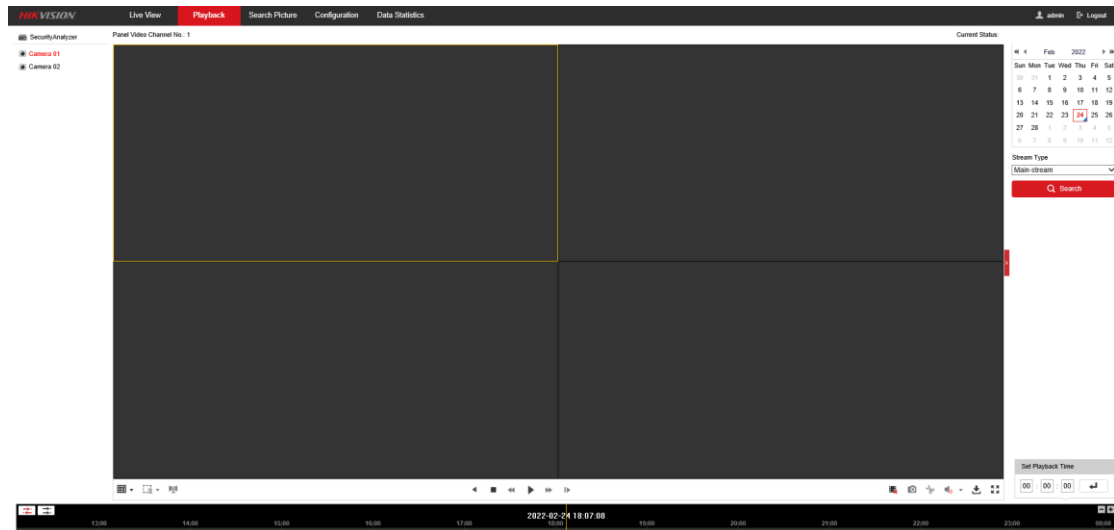
- Click  on the left side of the page to open/close the corresponding Live View image.
- There are shortcut control icons at the bottom of the page, including start/stop Live Viewing, screenshot, start/stop recording, turn on sound, full-screen playback, etc. Refer to Table 3-2 for detailed Live View control bar icon description.

Table 3-2 Live View Control Bar Icon Description

Icon	Description	Icon	Description
	Disable Live View/Enable Live View		Enable Manual Recording /Disable Manual Recording
	Split View		Full Screen
	Start Live Viewing All /Stop Live Viewing All		Live View Manual Capture
	Start Recordings/Stop All Recordings		Enable Main Stream/Sub Stream -Main Stream: HD Stream; -Sub Stream: Standard Definition Stream;
	Previous Frame/Next Frame	-	-
(Reserved Functions)			
	Audio Intercom		Panoramic View

3.3 Playback

Click **Playback** to enter the search video playback page. You can search, playback and download videos stored in the device.



Note

Refer to 3.5.1 Local Configuration for the path settings of videos and pictures saved in the playback page.

- Search Video: Select a day on the calendar page on the right, click **Search** to display the qualified video files on the timeline. Drag the timeline to the position where you want to play, and click **Play** to playback the video. If you want to seek to a specific time in a video file, you can manually set the Playback Time Parameter at the bottom right side of the window to seek to a specific time in a video file and start playing.
- Capture: Click  at the bottom of the playback page to capture a picture and save it on the local computer.
- Video Clipping: Click  at the bottom right side of the window to clip the searched playback video, and click the icon again to stop editing. At this time, it will prompt "editing Completed" under the calendar, and the edited video will be stored on the local computer.
- Stop Playback of All Videos: Click  to halt playback of all videos.
- Asynchronous/Synchronous Playing Mode: Click  to switch between synchronous playing mode and asynchronous playing mode. You can watch two channels at the same time.
- Split View: Click  to enter split view mode. There are total 3 video playing modes: single screen, four screen & nine screen.
- Clear (Reserved)
- Panoramic View (Reserved)

- Search and Download Videos: Click  at the bottom right side of the window, and the video download page will pop up, as shown in
 - Select the video type and time, and click **Search** to display the qualified videos in the right list.
 - Check the video that you want to download to the local computer, and click **Download** to download the video.
 Click **Configuration→Local→Replay** to view videos.

Note

In single-frame playback mode, each time you click the button, the video will skip to next frame. After playback is enabled, click **Edit** to edit the video file, click **Edit** again to stop editing, and the edited video will be saved in the corresponding file path.

3.4 Search Pictures

Click **Search Pictures** to enter the page to search and download pictures stored in the device.

Search Conditions

Channel

[A1] Camera 01

Major Type

Picture Of Hazardous Go

Sub Type

All

Start Time

2021-04-02 00:00:00

End Time

2021-04-02 23:59:59

Search

Export

- Search Pictures: select the channel and type, set time conditions, and click **Search** to display the qualified picture in the right list.
- Export: Click **Export** to select the export path.
- Select the pictures you want to view and click **Download Picture** to save the pictures to your local computer. You can download multiple pictures at a time.
- Select the file you want to view and click **Details** to view pictures and videos.



Note

- Click **Configuration→Local→Playback Download** to view saved pictures.
- You can search pictures within the past seven days.

3.5 Configuration

3.5.1 Local Configuration

Go to **Configuration → Local**, and enter Local interface.

Playing Parameters

- **Protocol Type:** Select the protocol type used by the network Live View video image, TCP or UDP are selectable.
- **Stream Type:** The stream type used by the network Live View image, main stream and sub stream are selectable. It is recommended to select the main stream when the bandwidth is large, and select the sub-stream when the bandwidth is small.
- **Live View Performance:** Set the live view performance mode. Least Delay, Balanced, and Best Fluency are selectable.
- **Rule Information:** You can enable or disable the Rule Information. When enabled, a dynamic analysis box of smart security inspection will show on the Live View interface.

- **POS Information Overlay:** You can enable or disable the POS Information Overlay. When enabled, the items that trigger the alarm in the rule area will display text information on the screen.
- **Image Size:** The size of the Live View image. Full, 4:3 and 16:9 are selectable.
- **Auto Live View:** Open the Live View automatically. After logging in Web, all channels will automatically open the video Live View.
- **Capture File Format:** Select the file format of Web manual capture. JPEG and BMP are supported.

Video File

- **Record File Size:** The packed size of the manually recorded video files. 256 M, 512 M and 1G are selectable.
- **Video Saving Path:** Set the saving path of the manually recorded video files.
- **Save download playback files to:** Set the saving path of the download playback files.

Capture and Clip Settings

- **Save snapshots in live view to:** Set the saving path of the manually captured pictures in live view.
- **Save download pictures to:** Set the saving path of the download pictures.
- **Save clips when playback to:** Set the saving path of the clips when playback.

3.5.2 System

System Configuration

Basic Information

Go to **Configuration → System → System Settings → Basic Information** and enter Device Information page. You can view device No., model, serial No., firmware version, etc.

System

System Settings

Maintenance

Security

Camera Management

User Management

Network

Video/Audio

Image

Event

Storage

AI Open Platform

Basic Information

Time Settings

About

Device Name

SecurityAnalyzer

Device No.

255

Model

ISD-ST204D-DHV4G-R001

Serial No.

ISD-ST204D-DHV4G-R0011620240424AARRD90876

Firmware Version

V2.2.4 build 240415

Encoding Version

V5.0 build 000000

Version

V2.10.0 build 240328

V2.8.0 build 240409

Model Version

V2.9.0 build 231225

Web Version

V4.0.1 build 240415.2

Plugin Version

V3.0.7.38

build 240201

build 220824

build 240320

R001

Number of Channels

2

Number of HDDs

1

Number of Alarm Input

2

Number of Alarm Output

3

Save

Time Settings

Steps:

1. Go to **Configuration → System → System Settings → Time Settings**, and enter Time Settings interface.

2. Select the device located time zone from the drop-down list.

3. Set NTP and manual time sync.

NTP Synchronization can ensure that the system time of the device remains accurate. If you connect the device to a time server with Dynamic Host Configuration Protocol (DHCP) and configure the network parameters of the device, the device will automatically synchronize time with the time server.

Check and enable **NTP synchronization**, and configure the following parameters:

Server Address: IP address of NTP server.

NTP Port: Port of NTP server.

Interval: The time interval between the two synchronizing actions with NTP server, and it can be set from 1 to 10080 minutes.

NOTE

If the device is connected to a public network, you should use a public NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the device is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.

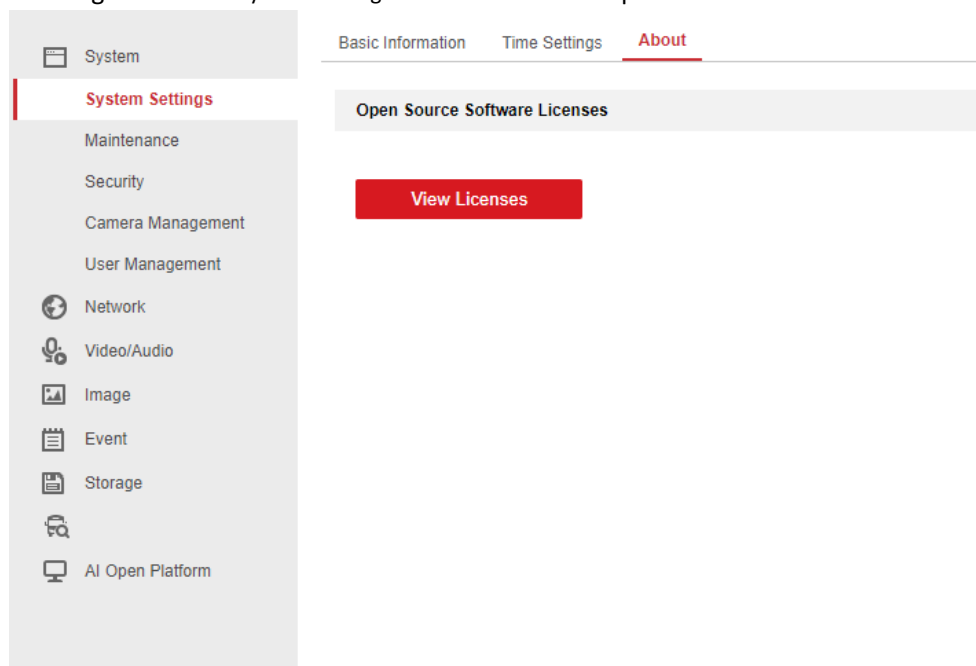
Manual Time Sync

Check **Manual Synchronization**, and you can view the current device time. Click “”, and you can set the specific date and time in the pop-up calendar and time box. You can also check **Sync. with Computer Time**, and the device time will be synchronized with the time of your computer.

4. Click **Save**.

About

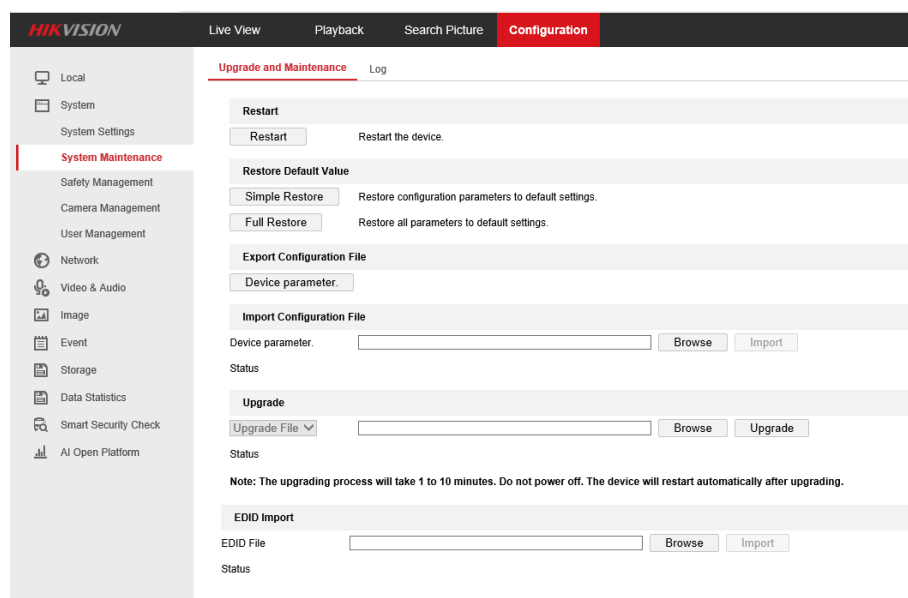
Select “Configuration → System Settings → About” to view open source software licenses.



System Maintenance

Upgrade and Maintenance

Go to **Configuration → System → System Settings → Time Settings**, and enter Time Settings page, and you can reboot the device, restore default parameters, import and export device parameters, and upgrade the device.



Reboot Device

Click **Reboot**, and click **OK** in the prompt.

● Restore Default Parameters

Click **Partly Restore** or **Restore All** to restore the device parameters. Click **OK** in the prompt to restore the device parameters and reboot the device.

Partly Restore: Reset all the parameters, except IP parameters, to the default settings.

Restore All: Restore all parameters to factory default settings.

- Import/Export Parameters

The configuration file can be exported to the local computer for backup. If multiple devices use the same configuration parameters, the configuration file of one device can be imported to multiple other devices of the same model.

Go to **Export Parameters → Device Parameters**, set the encryption password, and select the path to save the parameters to the local computer. Click **Save** to save the configuration parameters to the local computer.

Go to **Import Parameters → Browse**, select the device parameter file of the local computer, and click **Import** to import the device parameters. The device needs to be rebooted after importing.

- Upgrade

Click **Import Parameters → Browse**, select the local upgrade file, and click **Upgrade** to start upgrading... The device needs to be rebooted after upgrading.

Log

Go to **Configuration → System → System Maintenance → Log**, and you can view the device logs. Click **Export**, and select the path to export the device logs.

Advanced Configuration

Technicians can import EDID files and set EDID parameters.

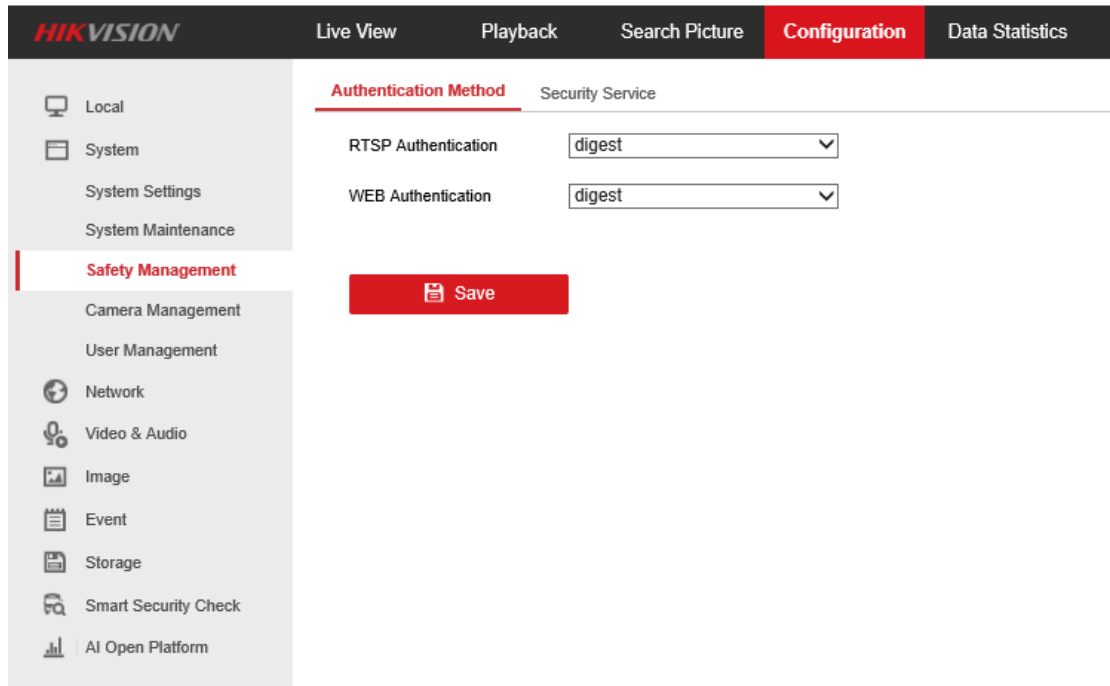
The screenshot shows the Hikvision web interface. The top navigation bar includes 'Live View', 'Playback', 'Search Picture', 'Configuration' (highlighted in red), and 'Data Statistics'. The left sidebar lists various system settings, with 'System Maintenance' highlighted in red. The main content area is titled 'Advanced Configuration' and contains two sections: 'EDID Import' and 'EDID Self-Adaptive'. The 'EDID Import' section has a text input for 'EDID File', a 'Browse' button, and an 'Import' button. The 'EDID Self-Adaptive' section has four rows of settings: 'EDID VGA Info' with a text input 'HIK HIK_VGA_IN 1280*1024/60HZ', 'EDID HDMI Info' with a text input 'HIK HIK_HDMI_IN 1280*1024/60HZ', 'EDID DVI Info' with a text input 'HIK HIK_DVI_IN 1280*1024/60HZ', and 'EDID Obtaining Port' with a dropdown menu set to 'NONE' and an 'Apply' button. A note at the bottom right states 'The device will reboot after the application takes effect.'

Safety Management

Authentication Mode

Steps:

1. Go to **Configuration → System → Safety Management → Authentication Method**, and enter Authentication Method page.



2. Select **digest** as the authentication method.

3. Click **Save**.

Security Service

The device supports SSH, SAPI, HTTP, RTSP and SADP security services.

1. Go to **Configuration → System → Security Management → Security Service**, and enter Security Service page.

2. Check the security services that need to be enabled.



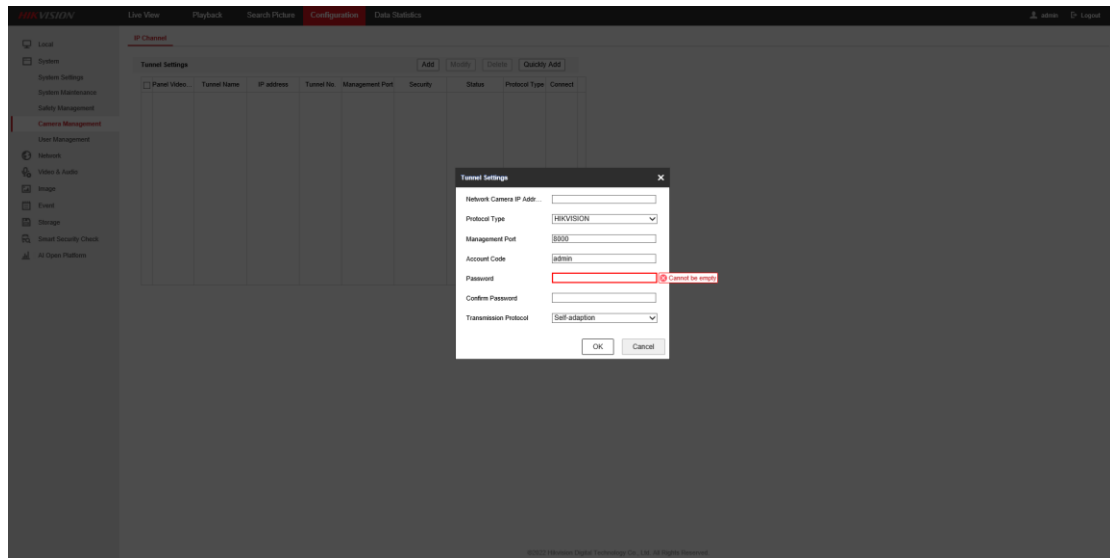
NOTE

If RTSP is disabled, RTSP Live View and playback will not be available, but the device security will be enhanced.

5. Click **Save**.

Camera Management

Go to **Configuration → System → Camera Management**, and enter Camera Management page.



NOTE

Only channel 1 supports access to a security gate.

NOTE

Click **Quick Add**, and you can add all network Channels in the same network segment to the device in batches.

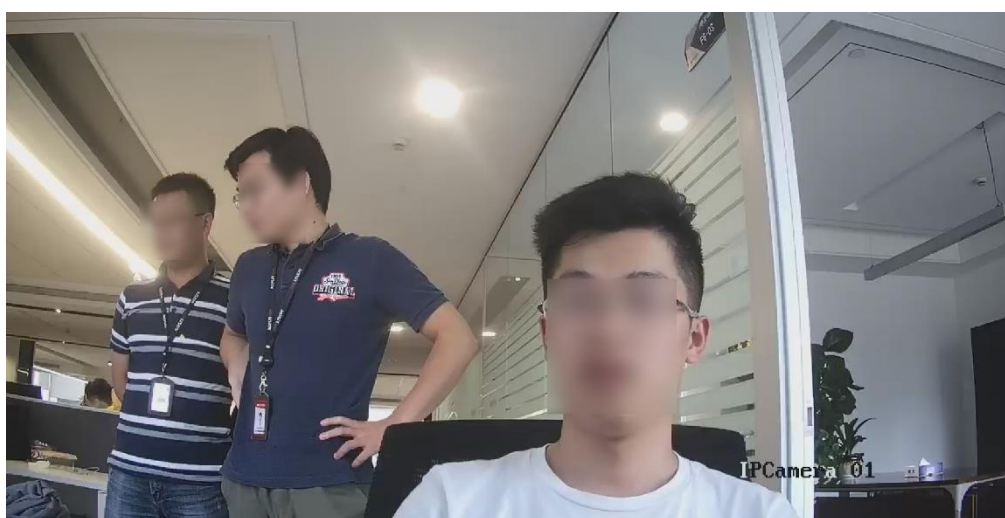
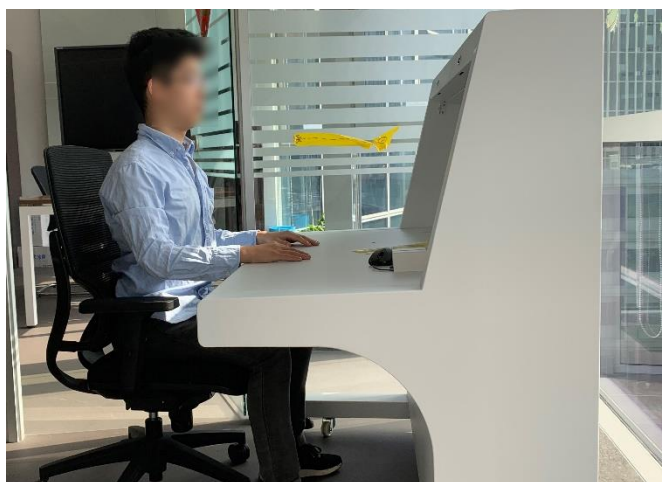
NOTE

The password used for the quick add operation is the password of the admin user.

NOTE

Network Channel Installation Instructions

- The security analyzer supports access to Hikvision network Channels. Recommended types: lens length 2mm, and wide-angle lens (horizontal wide-angle is also possible). Please avoid using fixed focus Channels.
- According to the requirements of the human behavior algorithm, please ensure that the ratio of the operator's head and shoulders to the entire image is less than 1/6 in the image captured by the network Channel.



- If there are multiple people in the monitoring area, you can draw the monitoring area in the local menu to select the operator position. If the monitoring area is not selected, the alarm linkage will be triggered by default when no one is present.
- There is a certain chance for the algorithm to recognize the item as an operator.

User Management

Go to **Configuration → System → User Management**, and enter User Management page. Admin user can create user and operator. Up to 32 users can be created.



NOTE

After the admin user adds or changes the password of a user, if the user name is used to log in again, the system will pop up a prompt asking the user to change the password.

Add User

Steps:

1. Click **Add** in the User Management page, and enter Add User page.
2. Enter the user name and password, and select the user type. The basic permission and camera

permission of the new added user can be set.

- **Operator:** By default, the operator has the local permission of local viewing logs, and remote configuration permissions, including remote viewing logs and status, remote voice intercom, remote Live View, remote manual recording, remote PTZ control and remote playback.
 - **User:** By default, user has the local permissions of local viewing logs and local playback, and remote configuration permissions of remote viewing logs and status, and remote playback.
3. Click **OK**.

Edit User

Steps:

1. Enter User Management page, and select a user in the user list to be edited.
2. Click Edit, and enter Edit User page.
3. You can edit the user name, password, user type and permissions.
4. Click OK.



NOTE

You need to log in to the device with the admin user to edit related users of the device.

Delete User

Steps:

1. Enter User Management page, and select a user in the user list to be deleted.
2. Click **Delete**.
3. Click **OK** in the prompt to delete the user.

View Online User

Go to **Configuration → System → User Management**, and you can view the online user information and refresh the list to view the latest user information.



NOTE

Online users are SDK login users, not-web login users.

3.5.3 Network

Basic Settings



NOTE

If the device is used for network monitoring, you need to set network parameters.

TCP/IP Settings

Before connecting the device to the network, you need to set the network parameters first.

Steps:

1. Go to **Configuration → Network → Basic Settings → TCP/IP**, and enter TCP/IP page.

The screenshot shows the Hikvision Configuration interface. The top navigation bar includes Live View, Playback, Search Picture, Configuration (highlighted), and Data Statistics. The left sidebar shows Local, System, and Network options, with Basic Settings selected under Network. The main content area is titled TCP/IP and has tabs for Port and 4G. Under TCP/IP, the Working Mode is set to Multi-address Setting, Select NIC is NIC1, and NIC Type is Self-adaption. There is an unchecked checkbox for Auto-Obtain. Below these are input fields for IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway, MAC Address, and MTU. A section for DNS Server Settings includes an unchecked checkbox for Auto DNS, input fields for Preferred DNS Server and Alternative DNS Server, and a dropdown for Default Route set to Lan1. A red Save button is at the bottom.

2. Set the network parameters.

- You can set working mode, NIC, NIC type, IPv4 address, IPv4 subnet mask, IPv4 default gateway, Mac address, MTU, DNS server, etc.

NOTE

- If there is a DHCP server in the network, you can check **DHCP** to enable it.
- The effective value of MTU ranges from 500 to 1500.

3. Click **Save**.

Port Settings

You can set the device port No., including HTTP port, RTSP port, and service port.

RTSP refers to the port of real-time streaming protocol. It is an application layer protocol in the TCP/IP protocol system.

Steps:

1. Go to **Configuration → Network → Basic Settings → Port**, and enter Port page.
2. Set the HTTP port, RTSP port, and service port parameters.

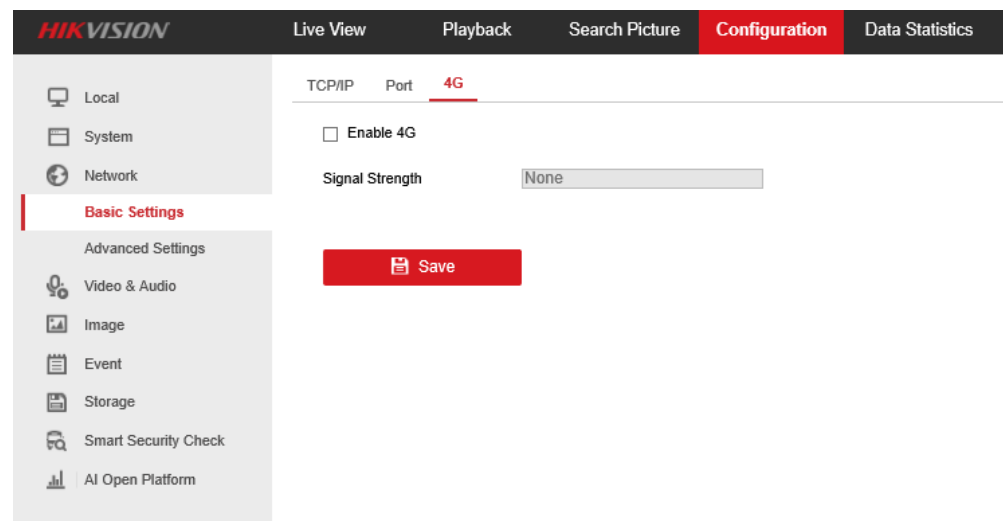
For network remote Live View, RTSP port is required. When network remote service is provided, HTTP port is required for web access. Service port is required in client.

- The effective values of RTSP port are 554, 1024 ~ 65535, and the default value is 554.
- The effective value range of service port is 2000 ~ 65535, and the default value is 8000.
- HTTP port is the web access port. The setting range is from 1 to 65535, and the default value is 80.

3. Click **Save**.

4G Settings

Select “Configuration → Network → Basic Settings → 4G”, check “Enable 4G” to connect to 4G network and view signal strength.



Advanced Settings

After the ISUP platform is accessed with the device, you can Live View, playback, and perform other operations on the ISUP platform.

Access Platform

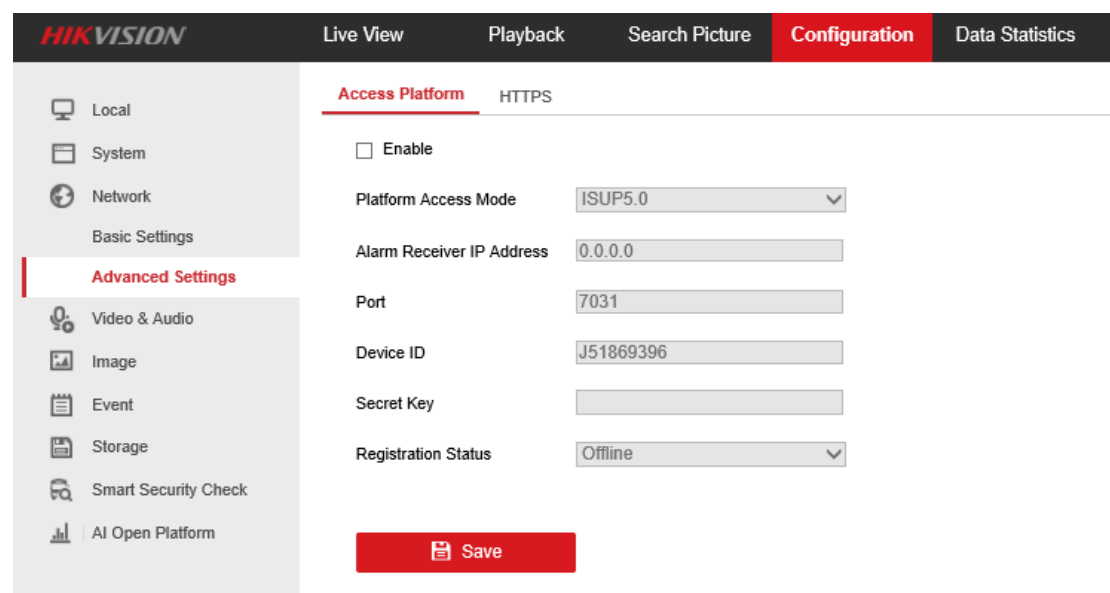


NOTE

Before the ISUP platform is accessed with the device, make ensure that the corresponding parameters have been configured.

Steps:

1. Go to **Configuration → Network → Advanced Settings → Access Platform**, and enter Platform Access interface.



2. Select the platform access mode, and check **Enable**.
3. Enter the Server IP address and port. You can refer to the following table.

Table 3-1 ISUP Access Setting Parameters Description

Parameter Name	Description
Server IP Address	The IP address of the platform server.
Port	The port No.of the platform server.It ranges from 1024 to 65535. Please refer to the actual data provided by the platform.
Device ID	Device fixed ID. It cannot be edited.

4. Click **Save**.



NOTE

To enable or disable ISUP access, you need to reboot the device to take it effect.

Https

Select “Configuration → Advanced Settings → Https” to install certificate.

The screenshot shows the Hikvision web interface. The top navigation bar includes 'Live View', 'Playback', 'Search Picture', 'Configuration' (highlighted), and 'Data Statistics'. The left sidebar has 'Local', 'System', and 'Network' categories. Under 'Network', 'Advanced Settings' is selected. The main content area is titled 'Access Platform' with 'HTTPS' selected. It contains an 'Enable' checkbox, an 'Install Certificate' section with three radio button options: 'Create Self-signed Certificate', 'Signed certificate is available, start the installation directly.', and 'Create the certificate request first and continue the installation.' (selected). Below these are buttons for 'Create Certificate Request' (with 'Create' and 'No file.'), 'Download Certificate Request' (with 'Certificate Download'), 'Delete Certificate Request' (with 'Delete'), and 'Install Generated Certificate' (with 'Browse' and 'Installation'). A red 'Save' button is at the bottom.

3.5.4 Video & Audio

Steps:

1. Go to **Configuration → Video and Audio → Video**, and enter Video page.

HIKVISION

Live View

Playback

Search Picture

Configuration

Data Statistics

Local

System

Network

Video & Audio

Image

Event

Storage

Smart Security Check

AI Open Platform

Recording

Channel

Stream Type

Video Type

Resolution

Bitrate Type

Image Quality

Video Frame Rate

Max. Bit Rate

Video Encoding

Copy To

Save

NOTE

Stream type support main stream (time), main stream (event) and sub-stream.

The main stream is used for recording and Live Viewing when the network bandwidth is large, and the sub-stream is used for recording and Live Viewing when the network bandwidth is small.

2. After the main stream and sub-stream are selected, you can set more details for the stream as follows.

- **Stream Type:** The stream is fixed as video stream, and there is no audio in the stream.
- **Resolution:** Select the resolution of the video stream.
- **Bitrate Type:** Select the video bitrate to constant or variable.
- **Video Quality:** When bitrate type is selected as Variable, 6 levels of video quality are selectable. When bitrate type is selected as constant, the video quality is fixed.
- **Frame Rate:** Set the frame rate. The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.
- **SVC:** Scalable Video Coding is an extension of the H.264/ MJPEG and H.265 standard. Select OFF/ON to disable/enable the SVC function. Select Auto and the device will automatically extract frames from the original video when the network bandwidth is insufficient.
- **Max. Bitrate:** Set the max. Bitrate.
- **Video Encoding:** Set the video encoding of the video.

3. (Optional) Click **Copy** to copy the same settings to other channels.

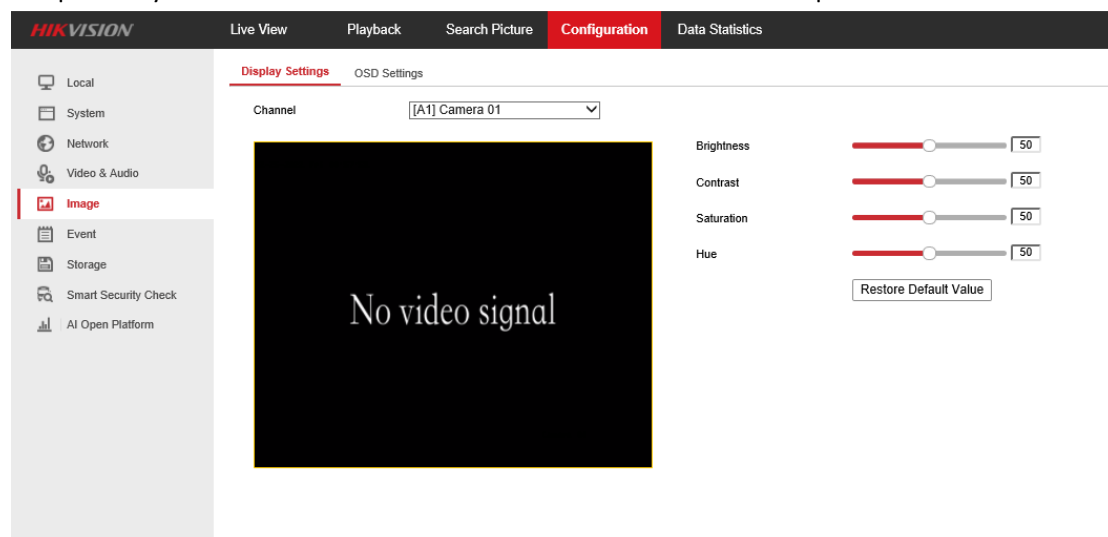
4. Click **Save**.

3.5.5 Image

Display Settings

Steps:

1. Select “Configuration → Image → Display Settings” to enter “Display Settings” interface, you can modify image display parameters.
2. Select a channel and move the slider to change parameters of brightness, contrast, saturation and hue.
3. Optional: you can click “Restore Default Value” to restore to default parameters.

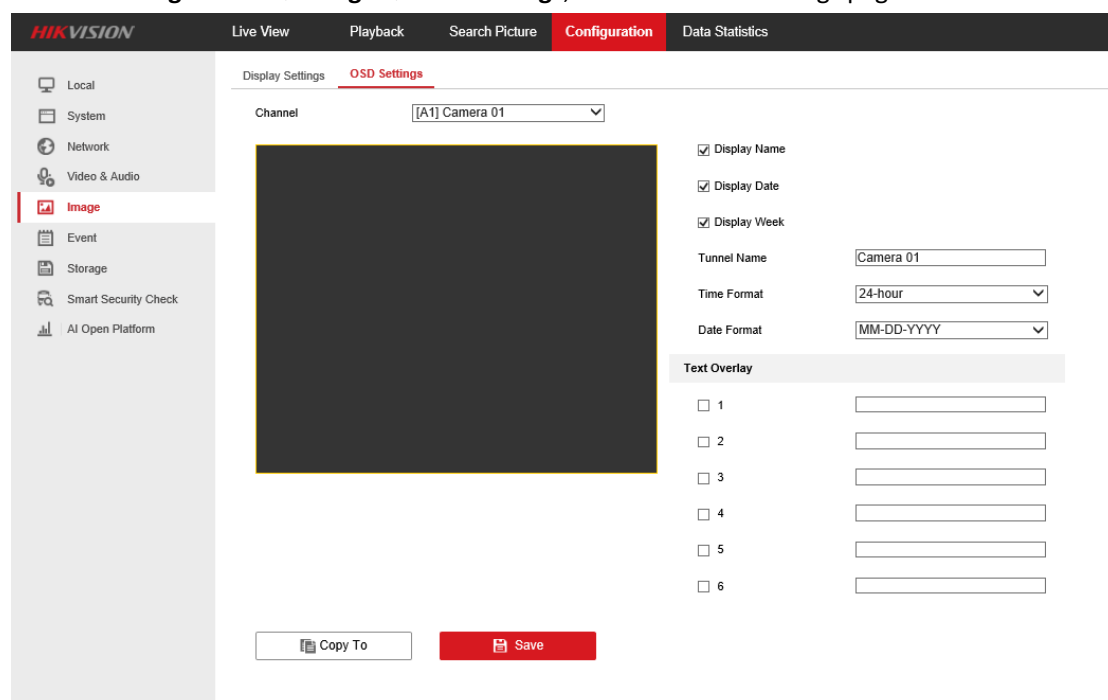


OSD Settings

OSD is the abbreviation of "On Screen Display". The Live Viewed OSD mainly includes the display of time and camera name.

Steps:

1. Go to **Configuration → Image → OSD Settings**, and enter OSD Settings page.



2. Select the channel.
3. Set the OSD parameters of this channel. If you need to change the OSD position, you can drag the OSD box to adjust it.

NOTE

- You can enter a custom channel name in Channel Name edit field.
 - You can select the appropriate time format and date format from the drop-down list.
 - You can customize to overlay text on the image in Text Overlay.
3. (Optional) Click **Copy** to copy the same settings to other channels.
 4. Click **Save**.

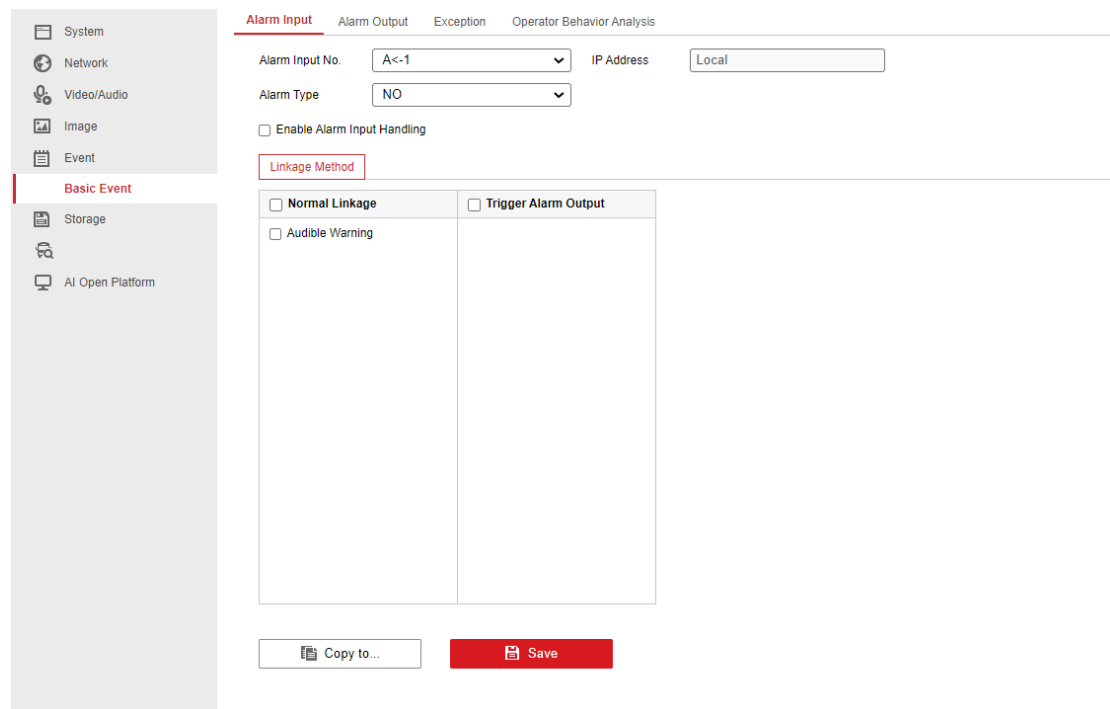
3.5.6 Event

Alarm Input

When there is a switch alarm, the alarm will be handled.

Steps:

1. Go to **Configuration → Event → Normal Event → Alarm Input**, and enter Alarm Input page.



The screenshot shows the 'Alarm Input' configuration page. On the left is a sidebar menu with categories: System, Network, Video/Audio, Image, Event, Basic Event, Storage, and AI Open Platform. The 'Event' category is selected, and 'Basic Event' is highlighted. The main content area has tabs for 'Alarm Input', 'Alarm Output', 'Exception', and 'Operator Behavior Analysis'. The 'Alarm Input' tab is active. It contains fields for 'Alarm Input No.' (set to 'A<-1'), 'Alarm Type' (set to 'NO'), and 'IP Address' (set to 'Local'). There is a checkbox for 'Enable Alarm Input Handling' which is unchecked. Below this is a 'Linkage Method' section with two columns: 'Normal Linkage' and 'Trigger Alarm Output'. The 'Normal Linkage' column has a checkbox for 'Audible Warning' which is unchecked. The 'Trigger Alarm Output' column is empty. At the bottom are 'Copy to...' and 'Save' buttons.

2. Select alarm input No. in the drop-down list, and set the alarm type. The alarm types includes normally open and normally closed.
3. Check **Handling Alarm Input**.
4. Set the alarm input linkage mode, including the settings of normal linkage, linkage alarm output, etc.
5. Click **Save**.



NOTE

If the settings of other channels are consistent with this channel, you can click **Copy to...** and enter the copy alarm input page, select the alarm input channel to be copied, and copy the alarm input handling methods to other channels.

Alarm Output

When an alarm occurs, you can set the linkage alarm output.

The screenshot shows the 'Alarm Output' configuration page. On the left is a sidebar menu with categories: System, Network, Video/Audio, Image, Event, Basic Event, Storage, and AI Open Platform. The main content area has four tabs: 'Alarm Input', 'Alarm Output' (which is selected and highlighted in red), 'Exception', and 'Operator Behavior Analysis'. Under the 'Alarm Output' tab, there are four configuration fields: 'Alarm Output No.' (a dropdown menu), 'IP Address' (a text input field), 'Delay' (a dropdown menu currently set to '5s'), and 'Alarm Status' (a dropdown menu currently set to 'ON' with a note '(cannot copy)' next to it). At the bottom of the configuration area, there are three buttons: 'Clear Alarm' (with a trash icon), 'Copy to...' (with a document icon), and 'Save' (a red button with a save icon).

Steps:

1. Go to **Configuration → Event → Normal Event → Alarm Output**, and enter Alarm Output page.
2. Select the alarm output No. to be set, set the alarm name and delay time.



NOTE

If you select Manual in delay, when an alarm occurs, you need to turn off the alarm output manually, and the alarm will end.

4. Click **Save**.



NOTE

If the settings of other channels are consistent with this channel, you can click **Copy to...** and enter the copy alarm output page, select the alarm output channel to be copied, and copy the settings of this channel to other channels.

Exception

The screenshot shows the 'Exception' configuration page. On the left is a sidebar with a menu: System, Network, Video/Audio, Image, Event, Basic Event (highlighted), Storage, and AI Open Platform. The main content area has tabs: Alarm Input, Alarm Output, Exception (active), and Operator Behavior Analysis. Below the tabs, 'Exception Type' is set to 'HDD Full'. There are two columns of settings: 'Normal Linkage' with a checkbox for 'Audible Warning', and 'Trigger Alarm Output' with a checkbox. A red 'Save' button is at the bottom.

Exception settings is the alarm handling for the exception events. Exception events include HDD full (when HDD space is full), HDD error (error while writing HDD or HDD is not initialized), network disconnection (no network cable connected), IP conflict, illegal Access (wrong user password), record/capture exception (such as no recording HDD, etc.) and all types.

Steps:

1. Go to **Configuration → Event → Normal Event → Exception**, and enter Exception page.
2. Set all exception parameters, including exception type, sound alarm and linkage alarm output.

Operator Behavior

The screenshot shows the 'Operator Behavior Analysis' configuration page. The sidebar is the same as the previous page. The main content area has tabs: Alarm Input, Alarm Output, Exception, and Operator Behavior Analysis (active). Below the tabs, 'Camera' is selected from a dropdown. There is a checkbox for 'Enable Behavior Analysis'. Below that are two sub-tabs: 'Basic Settings' (active) and 'Linkage Method'. Under 'Basic Settings', there is a 'Sensitivity' slider set to 0. A red 'Save' button is at the bottom.

Steps:

1. Go to **Configuration → Event → Normal Event → Operator Behavior**, and enter Operator Behavior page.
2. Select the channel to be alarmed, and check **Enable Behavior**.
3. Set the sensitivity of operator behavior (0 ~ 100).



The higher the sensitivity value, the easier it is to recognize the operator's absence behavior.



Periods cannot be overlapped or included.

4. Click Linkage Mode and enter Motion Detection Linkage page, and you can select regular linkage and linkage alarm output.

5. Click Apply.

3.5.7 Storage

HDD Management

Please initialize the HDD for the first use.

Steps:

1. Go to **Configuration → Storage → Storage Management → HDD Management**, and enter HDD Management page.
2. Check the HDD and click **Format**. After formatting, the device can start recording according to the recording schedule.

HDD Detection

● S.M.A.R.T Detection

S.M.A.R.T detection can monitor HDD head unit, HDD temperature, medium material on the disk surface, motor and its driving system, HDD internal circuit, etc. It can analyze and predict the potential problems of the HDD in time.

Steps:

1. Go to **Configuration → Storage → Storage Management → HDD Detection → S.M.A.R.T Detection**, and enter S.M.A.R.T Detection page.



- S.M.A.R.T detection function is enabled by default.
- If you select "Continue to use this disk when self-test is failed", the HDD will continue to be used when there is SMART exception.



WARNING

When the HDD S.M.A.R.T exception occurs, the HDD can continue to be used, but there will be a big risk. Please operate carefully.

2. Select the self-test type, and click Self-test.

- The self-test type includes short type, extended type, and transmission type.
- The evaluation status includes "Functional ", "Bad Sectors" and "HDD is going to fail ".
- The self-evaluation status includes "Passed" and "Failed".
- Users can use the S.M.A.R.T self-test function, self-test the HDD via S.M.A.R.T command, and check the overall status of the HDD.

● **Bad Sector Detection**

The system detects bad sectors in HDD through read-only method.

Steps:

1. Go to **Configuration → Storage → Storage Management → HDD Detection → Bad Sector Detection**, and enter Bad Sector Detection page.
2. Select HDD No. and detection area, and click **Start Detecting**.



NOTE

Detection area type includes Key Area Detection and Full Detection.

3. You can check the HDD bad sectors after the detection.

3.5.8 Smart Security Check

VCA Settings

Security Inspection Configuration

Steps:

1. Go to **Configuration → Smart Security Check → VCA Settings → Security Inspection Configuration**, and enter Security Inspection Configuration interface.
2. Select the video input camera.



NOTE

The smart analysis settings will only take effect for the currently selected camera after saving.

3. Check **Enable Algorithm Detection**.
4. Check **Enable Confidence**.



NOTE

Confidence is the suspicion degree of identified hazardous goods.

5. Set the conveyor belt direction, monitoring point information, security inspection machine channel size and the font size of calibration information.



NOTE

Wrong direction settings of the conveyor belt will result in intelligent recognition exception. Wrong size settings of the detection channel may cause intelligent recognition exception.

6. Draw the recognition area of the package screen.

Click **Default Recognition Area**, the default recognition area will automatically show on the screen.

Click **Redraw Recognition Area** and hold down the left mouse button to draw a rectangular area on the screen.



NOTE

The drawn recognition area cannot contain black objects or areas, or the smart recognizing function might not in proper service.

Stretch or drag to change the size or location of the drawn area.

If the recognition area is not drawn, the setting parameters cannot be saved.

7. Click **Save**.

Advanced Configuration

1. Select “Configuration → Smart Security Check → VCA Settings → Advanced Configuration”.

The screenshot shows the Hikvision web interface for VCA Settings. The top navigation bar includes Live View, Playback, Search Picture, Configuration (highlighted), and Data Statistics. The left sidebar lists various settings categories: Local, System, Network, Video & Audio, Image, Event, Storage, Smart Security Check (highlighted), and AI Open Platform. Under Smart Security Check, the 'VCA Settings' tab is active, and the 'Advanced Configuration' sub-tab is selected. The configuration fields are as follows:

Field	Value
Manufacturer	Hikvision
Model No.	test
Angle of View	Single View
Year of Starting	2000
Package Cutoff	4
Package Cutoff	50

A red 'Save' button is located at the bottom of the configuration area.

2. Select manufacturer and angle of view, fill in the model number, year of starting.

3. Maintenance and technical personnel can fill in the package cutting sensitivity and package cutting Pixel threshold.

4. Click **Save**.

Prohibited Item Settings

1. Select “Configuration → Smart Security Check → Prohibited Item Settings”. In the list below, check the prohibited items. Click **Edit** to edit prohibited items. You can set the color, confidence and linkage channel.

2. In the prohibited Item setting list, check linkage alarm mode.

Sound Alarm: After checking, when an alarm occurs, the device will beep to alarm.

Buzzer: The device buzzer will alarm when prohibited goods in the list is detected.

A->1-4: Alarm output channel linked when an event occurs.

3. Click **Save**.



NOTE

If the user does not draw an identification region, the configuration parameters cannot be saved.

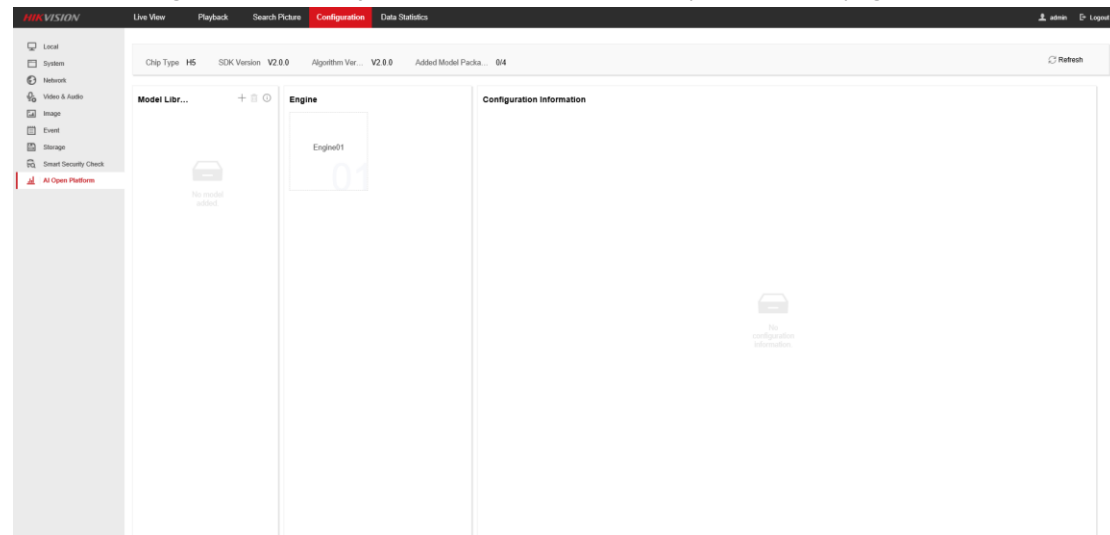
The intelligent analysis parameter configuration takes effect for both channels.

3.5.9 AI Open Platform

You can view the SDK version, algorithm version and other information, import the model library file input from the AI open platform, and apply it in the actual security inspection environment.

Steps:

1. Go to **Configuration → AI Open Platform**, and enter AI Open Platform page.



2. Click "+" in Model Library, select the model file and Label file, create the model name, and click **OK**.

3. Select an added model in Engine and click **Bind**.

You can view corresponding information in Configuration Information.

4. Enable **Task** in Configuration Information.

5. Click **Save**.

3.6 Data Statistics

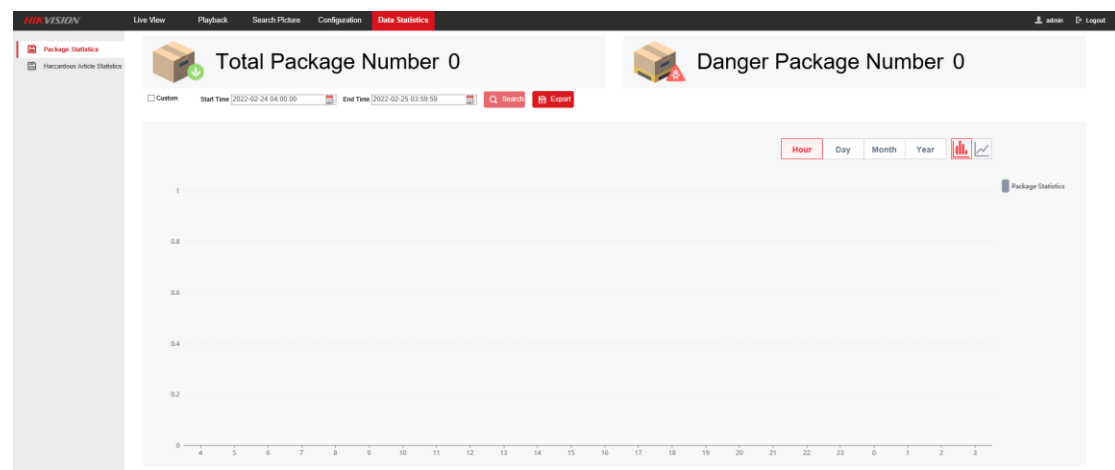
On the Data Statistics page, you can view the total number of packages passed by the security inspection machine and the total number of prohibited goods, and view the number of packages and prohibited goods within the set period.

Package Statistics

Steps:

1. Go to **Configuration → Data Statistics → Package Statistics**, and enter Package Data Statistics

page.

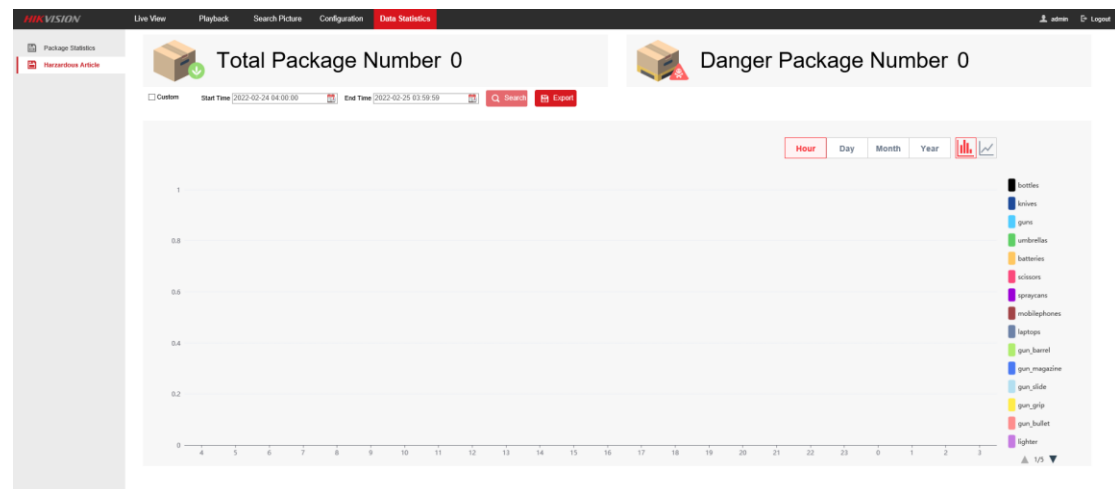


2. Select the statistics method, including year (5 years), month (12 months), day (30 days), or hour (24 hours).
3. If you need to view the statistics in an accurate time, select the exact period, and click **Search** to view the statistics.

Hazardous Article Statistics

Steps:

1. Go to **Configuration → Data Statistics → Hazardous Article Statistics**, and enter Prohibited Goods Data Statistics page.



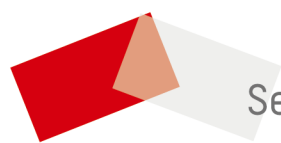
2. Select the statistics method, including year (5 years), month (12 months), day (30 days), or hour (24 hours).
3. If you need to view the statistics in an accurate time, select the exact period, and click **Search** to view the statistics.

Passing People and Metal Detection Statistics

Steps:

1. Go to **Configuration → Data Statistics → Passing People Statistics**, and enter Passing People Statistics page.
2. Select the statistics method, including year (5 years), month (12 months), day (30 days), or hour (24 hours).

3. If you need to view the statistics in an accurate time, select the exact period, and click **Search** to view the statistics.



See Far, Go Further