HCP V2.3 Body Camera and Dock Station Delivery Manual

Contents

1 Scheme Overview

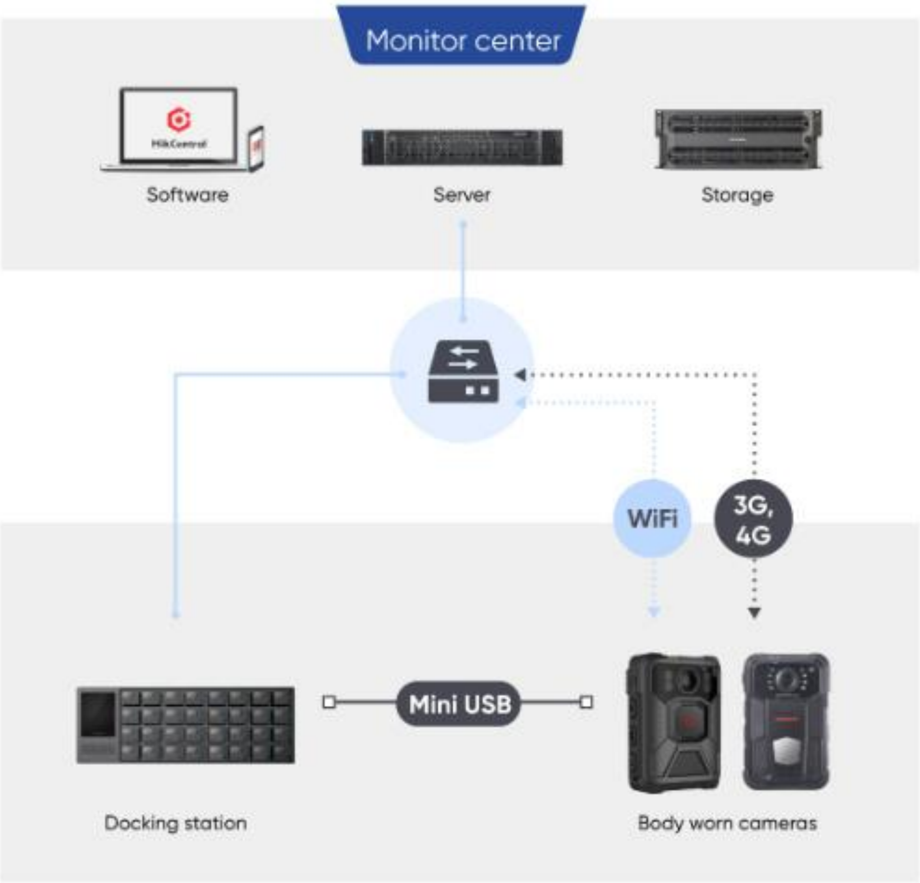
Fixed monitoring usually covers important urban scenarios, but the scope is limited. For the city as a whole, that means there are still some blind spots. Composed of wearable cameras and acquisition stations, the system enables flexible and agile responses, enabling rapid deployment in emergency situations and when fixed surveillance is unavailable or not feasible.

The Hikvision Portable Law Enforcement System features body cameras, portable PTZ dome cameras, integrated video recording, 3G and 4G wireless transmission, GPS positioning and centralized management.

Dock stations provide a simplified way to access and back up law enforcement data while also charging cameras, and portable PTZ cameras provide vital views of streets and around the city for field safety.

2 System Structure

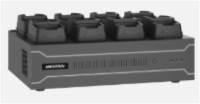
HCP + Dock Station + Body Camera



- ✓ The device is connected to the platform through 4G to realize business functions.
- ✓ The user wears the Body Camera for law enforcement, and can use the device to record, record, take photos, and alarm with one button.
- ✓ The headquarters can view Live View/Play Back in real time on the client side, and can initiate two-way intercom and other functions.
- ✓ After the user's law enforcement is completed, plug the Body Camera into the Dock Station to charge, and the content stored in the Body Camera will be automatically uploaded.
- ✓ The content in the Dock Station can be searched in the client and added to the evidence management module.

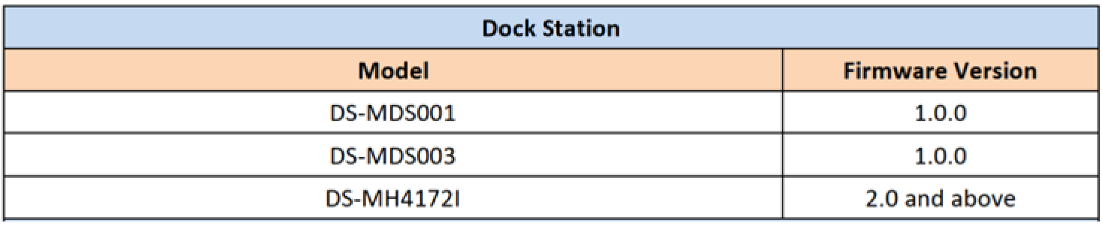
[Note]: In this scenario, in addition to the firewall entry and exit rules, port mapping is also involved. Because real-time recording will generate large 4G traffic, if it exceeds the customer's traffic package, there may be business risks, and it is recommended to use it with caution.

3 Product List

Product Name	Product Image	Product Number
Dockstation		DS-MDS003/2T/8
Dockstation		DS-MH4172I
Dockstation		DS-MDS001

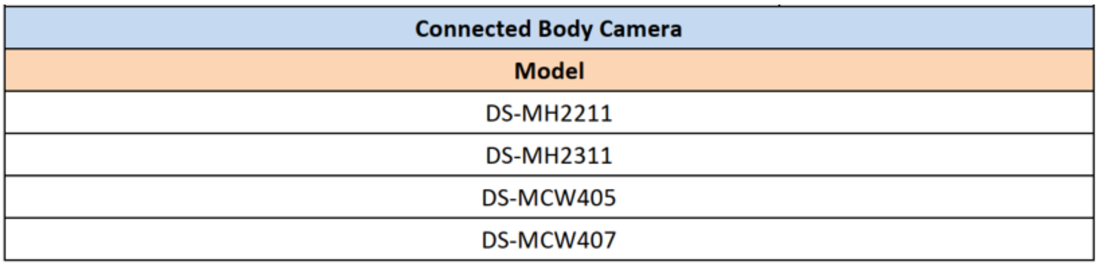
Body camera		DS-MH2311(C)

The models of the Dock Station are as follows:



Dock Station	
Model	**Firmware Version**
DS-MDS001	1.0.0
DS-MDS003	1.0.0
DS-MH4172I	2.0 and above

The models of the Body Camera are as follows:



Connected Body Camera
Model
DS-MH2211
DS-MH2311
DS-MCW405
DS-MCW407

4 Confirm Network Environment

Regardless of the network situation, the following information needs to be confirmed in advance before the project is implemented and deployed:

- ✓ Confirm the network deployment between the monitoring center and all clients, whether the HCP server and the client are in the same LAN, and whether they include security protection media, such as firewalls, route mapping, etc.;
- ✓ Confirm that the network between the device and the platform server can be connected (for example, tools such as Socket Tool can be used to check key ports) to ensure that the device can be added to the platform normally;
- ✓ Confirm the network interconnection between the servers in the monitoring center. It is recommended that the network port of the central switch be gigabit or above;
- ✓ Confirm the egress bandwidth of the customer accessing the Internet (if WEB and APP need to be accessed on the external network)

4.1 Port Mapping

- ✓ Map the ports in the port list. The handheld device initiates registration with the platform through TCP port 7660, and relies on port 16001 for two-way intercom, so this port needs special attention.

- ✓ In addition, if the firewall function of the server operating system needs to be enabled, you need to configure the inbound and outbound rules according to the port dependency table.
- ✓ The following module ports need to be mapped to the external network. Only minimal mapped ports required for SYS and ISUP.

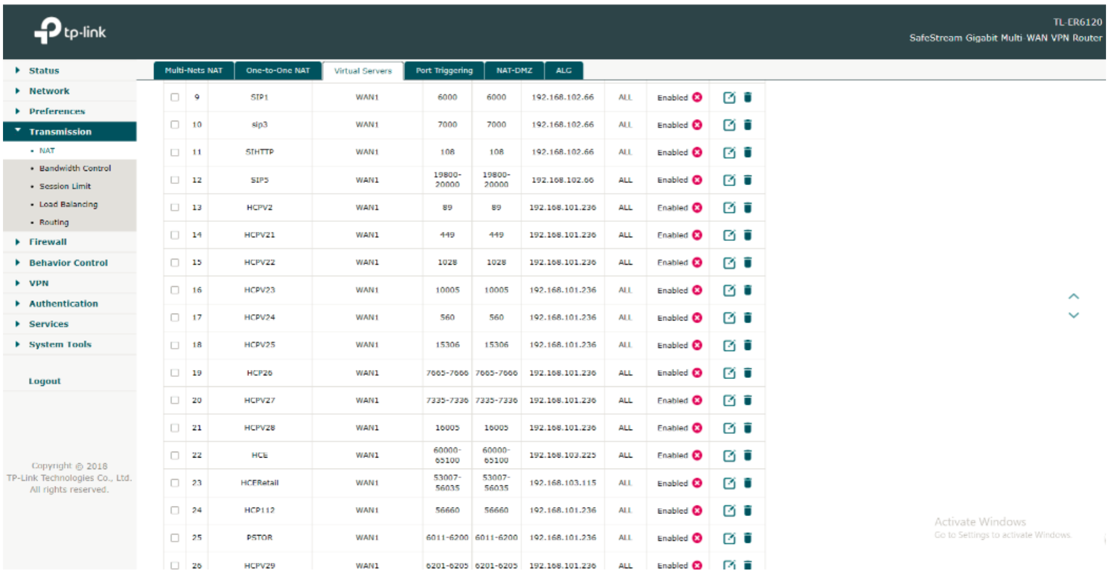
Source Device	**Destination Device**	**Destination Port Number（Listening）**	**Protocol**	**Port Description**
Web Client, Control Client	SYS	80	TCP	Used for Web Client & Control Client access in HTTP protocol
Web Client, Control Client	SYS	443	TCP	Used for Web Client & Control Client access in HTTP protocol
ISUP Device	SYS	7660	TCP	Used for receiving registration from ISUP devices
ISUP Device	SYS	7332	TCP	Used for receiving alarm from ISUP devices
ISUP Device	SYS	7334	UDP	Used for receiving alarm from ISUP devices
Streaming Server	SYS	7661	TCP	Used for getting stream from ISUP device via Streaming Server
ISUP Device	SG/SMS	16001	TCP	ISUP Port for Two-Way Audio
ISUP Device	SG/SMS	16003	TCP	ISUP port for Broadcasting
ISUP Device	SYS	6123	TCP	Used for the picture storage of ISUP devices
Web Client, Control Client	SG/SMS	554	TCP	Used for getting stream for live view (real-time streaming port)
Web Client, Control Client	SG/SMS	559	TCP	Used for getting stream for Google Chrome, Firefox, or Safari
Web Client, Control Client	SG/SMS	10000	TCP	Used for getting stream for playback (video file streaming port)
ISUP Device	SG/SMS	16000	TCP	Used for getting stream from

				ISUP device via plugin
SYS	SG/SMS	6001	TCP	Used for getting the status of the Streaming Serve
SYS	SG/SMS	6678	TCP	Used for editing configuration for Streaming Server
SYS	SMS	8208	TCP	Listen port for Service Manager after encrypted transmission enabled

For more details, please refer to "HikCentral Professional V2.3 Communication Matrix"

4.2 Router Mapping

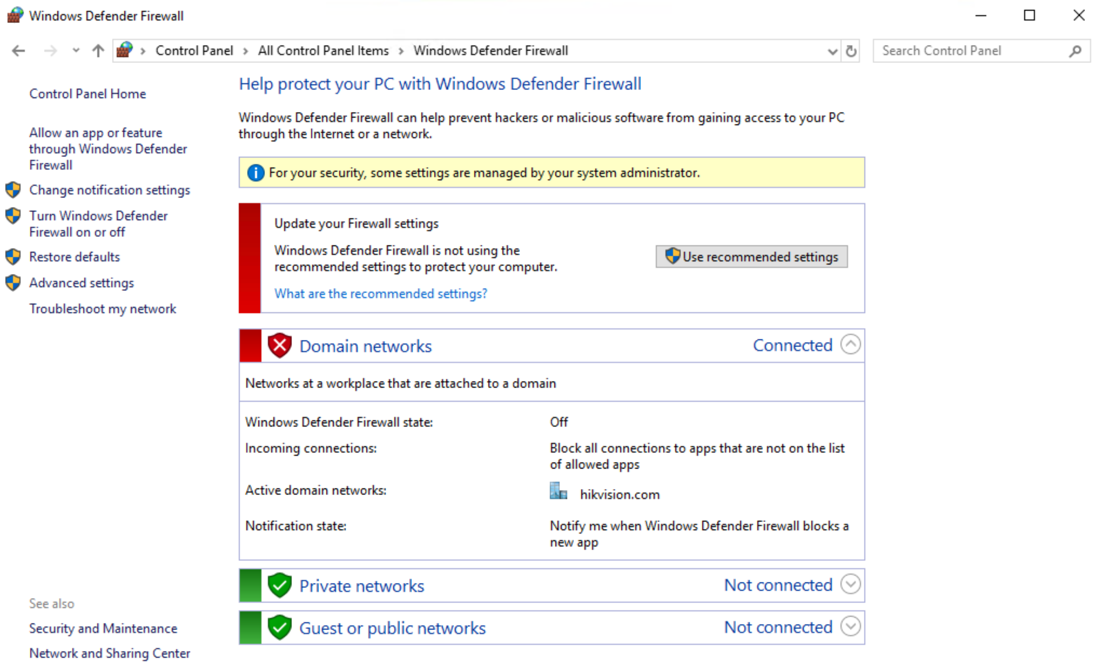
Log in to the router and configure the routing for the corresponding port. As shown below. Since the configuration interface and options of each router manufacturer are different, it is for reference only.



□	9	SIP1	WAN1	6000	6000	192.168.102.66	ALL	Enabled	
□	10	sip3	WAN1	7000	7000	192.168.102.66	ALL	Enabled	
□	11	SIHTTP	WAN1	108	108	192.168.102.66	ALL	Enabled	
□	12	SIP5	WAN1	19800-20000	19800-20000	192.168.102.66	ALL	Enabled	
□	13	HCPV2	WAN1	89	89	192.168.101.236	ALL	Enabled	
□	14	HCPV21	WAN1	449	449	192.168.101.236	ALL	Enabled	
□	15	HCPV22	WAN1	1028	1028	192.168.101.236	ALL	Enabled	
□	16	HCPV23	WAN1	10005	10005	192.168.101.236	ALL	Enabled	
□	17	HCPV24	WAN1	560	560	192.168.101.236	ALL	Enabled	
□	18	HCPV25	WAN1	15306	15306	192.168.101.236	ALL	Enabled	
□	19	HCP26	WAN1	7665-7666	7665-7666	192.168.101.236	ALL	Enabled	
□	20	HCPV27	WAN1	7335-7336	7335-7336	192.168.101.236	ALL	Enabled	
□	21	HCPV28	WAN1	16005	16005	192.168.101.236	ALL	Enabled	
□	22	HCE	WAN1	60000-65100	60000-65100	192.168.103.225	ALL	Enabled	
□	23	HCERetail	WAN1	53007-56035	53007-56035	192.168.103.115	ALL	Enabled	
□	24	HCP112	WAN1	56660	56660	192.168.101.236	ALL	Enabled	
□	25	PSTOR	WAN1	6011-6200	6011-6200	192.168.101.236	ALL	Enabled	
□	26	HCPV29	WAN1	6201-6205	6201-6205	192.168.101.236	ALL	Enabled	

4.3 Windows built-in firewall inbound and outbound rule configuration (optional)

Select Firewall in Control Panel - select Advanced Settings.


Windows Defender Firewall
Control Panel › All Control Panel Items › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center
Use recommended settings

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

For your security, some settings are managed by your system administrator.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

What are the recommended settings?

Domain networks — Connected

Networks at a workplace that are attached to a domain

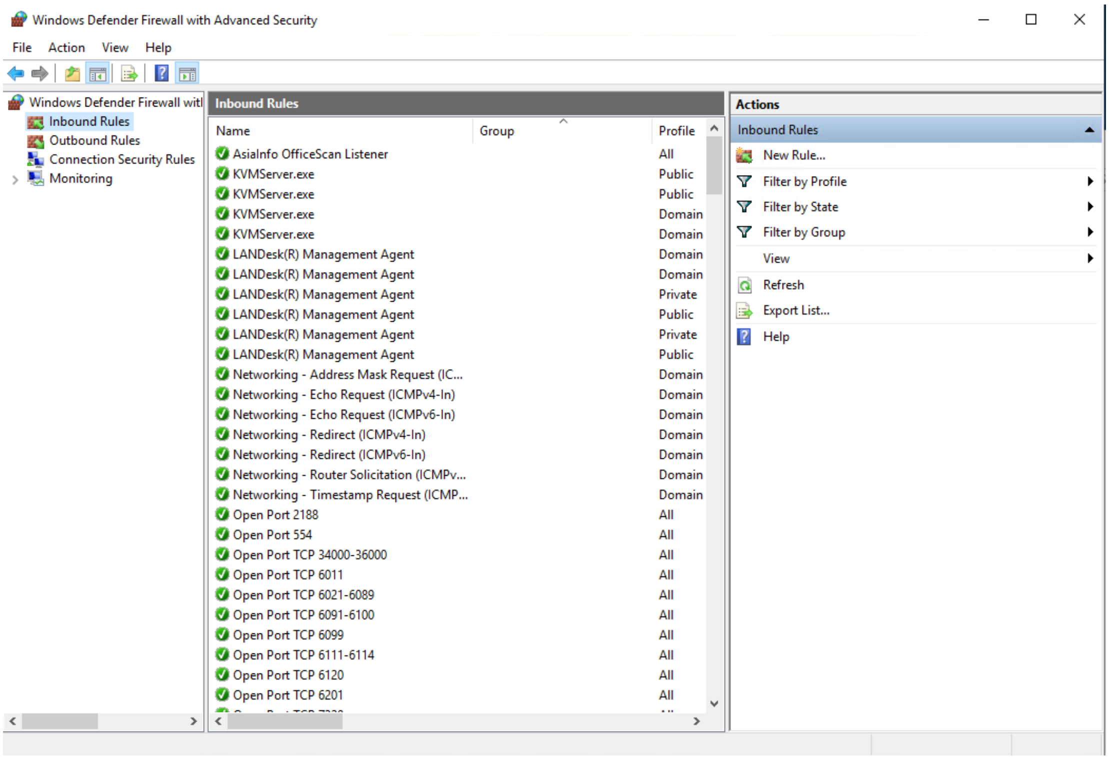
Windows Defender Firewall state:	Off
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active domain networks:	hikvision.com
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Private networks — Not connected

Guest or public networks — Not connected

Select Inbound Rules and Outboard Rules for inbound and outbound rule settings.

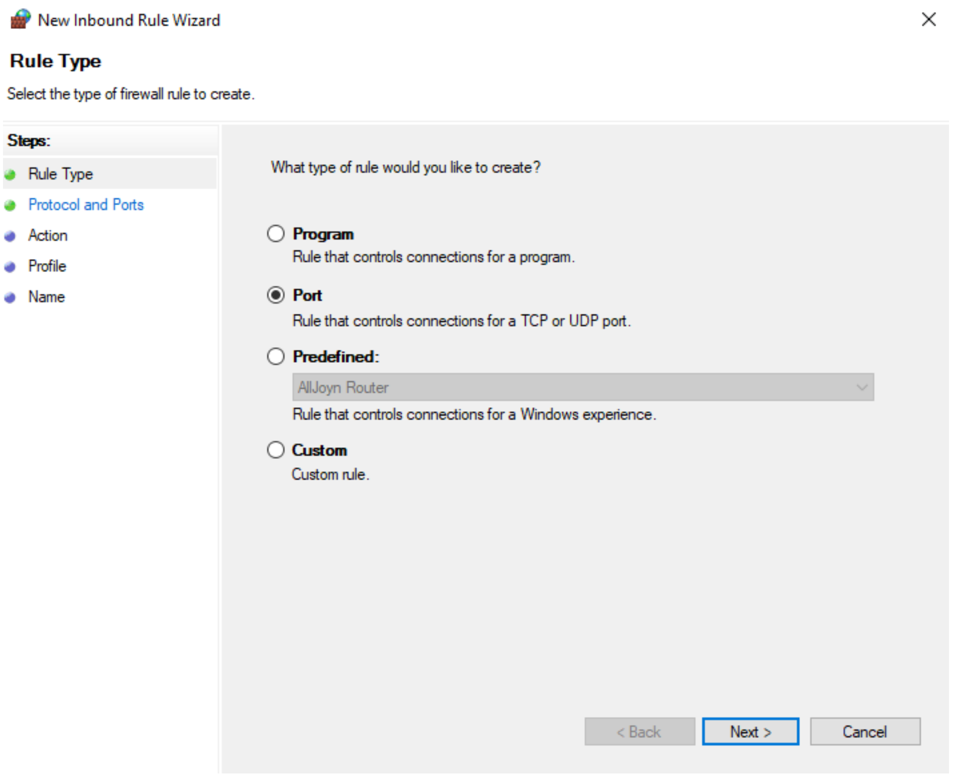
The following takes inbound rule configuration as an example. Click New Rules to get started.



Inbound Rules

Name	Group	Profile
AsiaInfo OfficeScan Listener		All
KVMServer.exe		Public
KVMServer.exe		Public
KVMServer.exe		Domain
KVMServer.exe		Domain
LANDesk(R) Management Agent		Domain
LANDesk(R) Management Agent		Domain
LANDesk(R) Management Agent		Private
LANDesk(R) Management Agent		Public
LANDesk(R) Management Agent		Private
LANDesk(R) Management Agent		Public
Networking - Address Mask Request (IC...		Domain
Networking - Echo Request (ICMPv4-In)		Domain
Networking - Echo Request (ICMPv6-In)		Domain
Networking - Redirect (ICMPv4-In)		Domain
Networking - Redirect (ICMPv6-In)		Domain
Networking - Router Solicitation (ICMPv...		Domain
Networking - Timestamp Request (ICMP...		Domain
Open Port 2188		All
Open Port 554		All
Open Port TCP 34000-36000		All
Open Port TCP 6011		All
Open Port TCP 6021-6089		All
Open Port TCP 6091-6100		All
Open Port TCP 6099		All
Open Port TCP 6111-6114		All
Open Port TCP 6120		All
Open Port TCP 6201		All

Select Port and set the ports that need to be opened.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

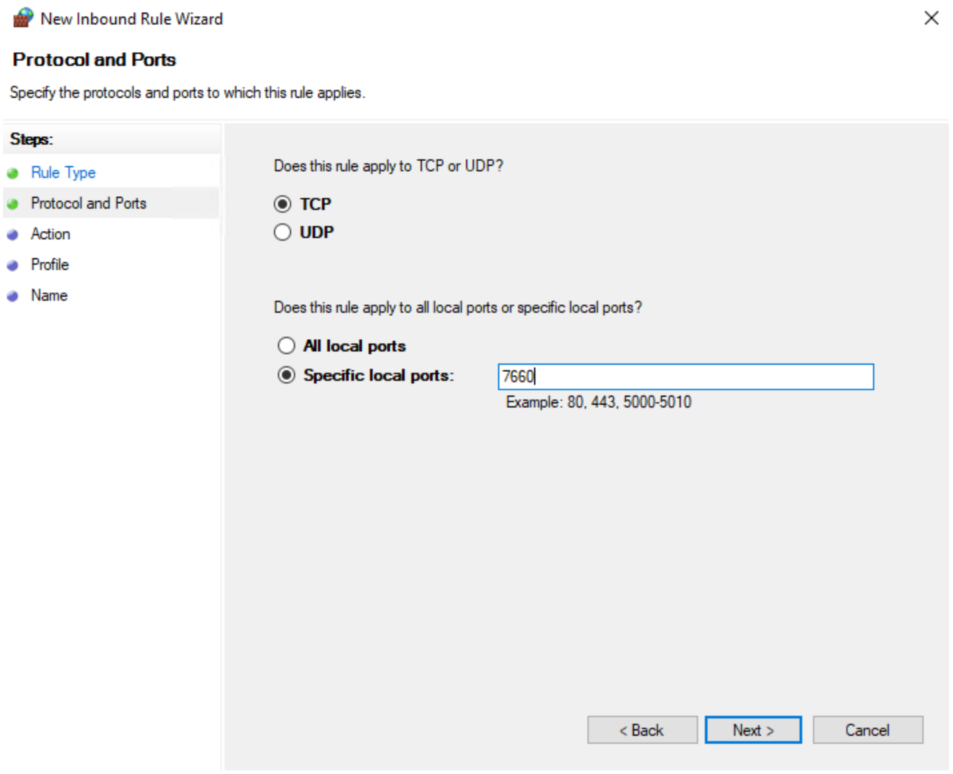
What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.



New Inbound Rule Wizard

Protocol and Ports

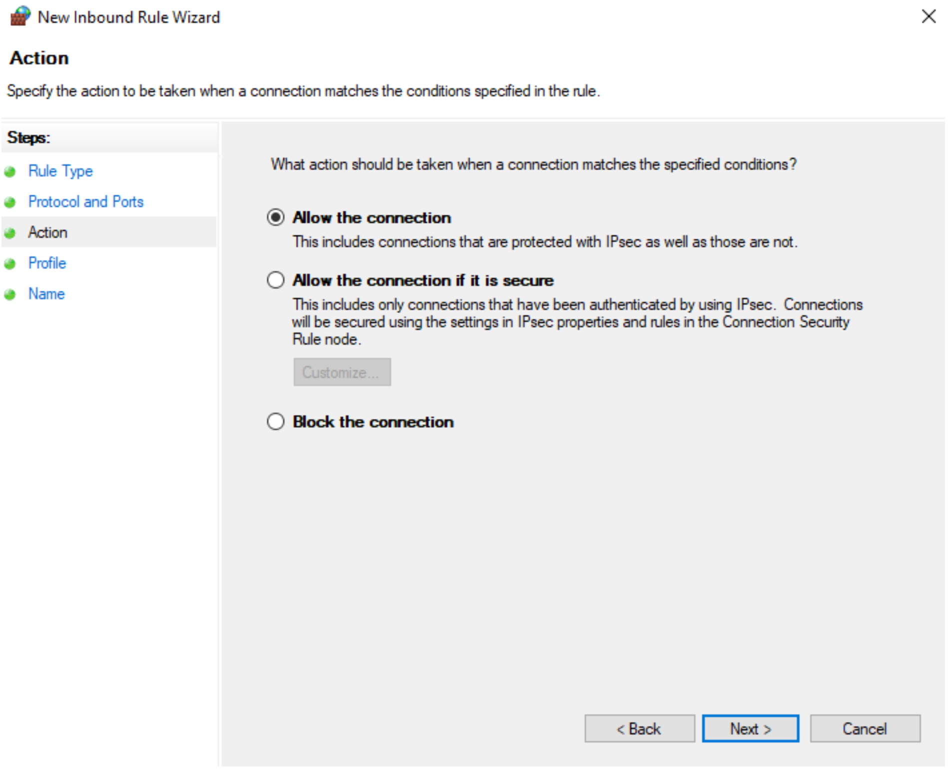
Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all local ports or specific local ports?

○ **All local ports**
● **Specific local ports:** 7660
Example: 80, 443, 5000-5010



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

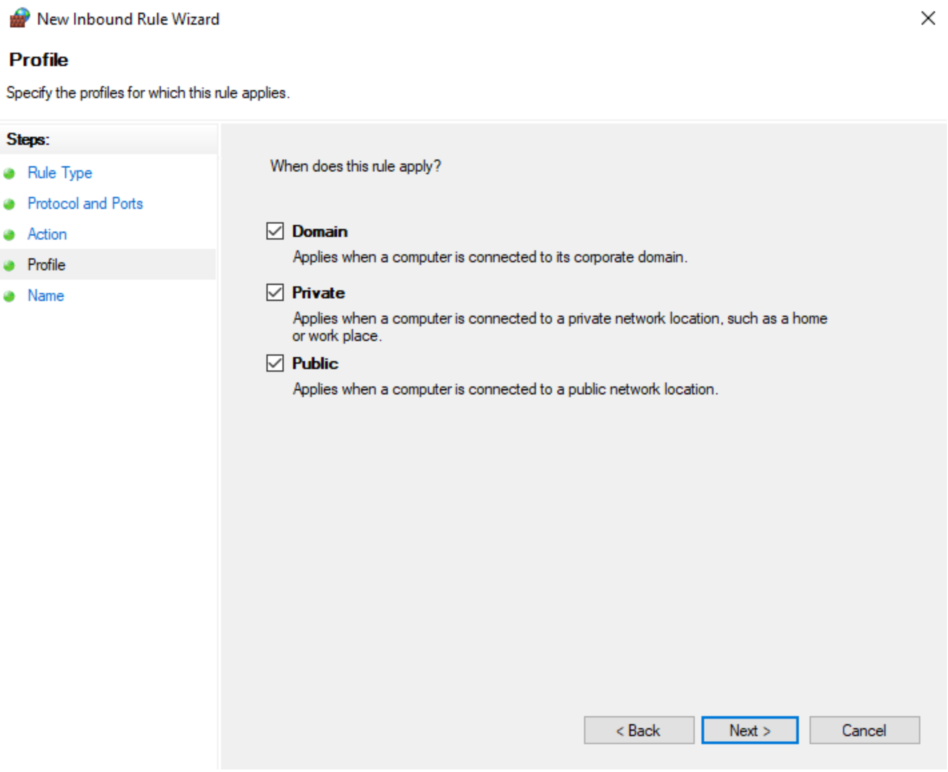
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

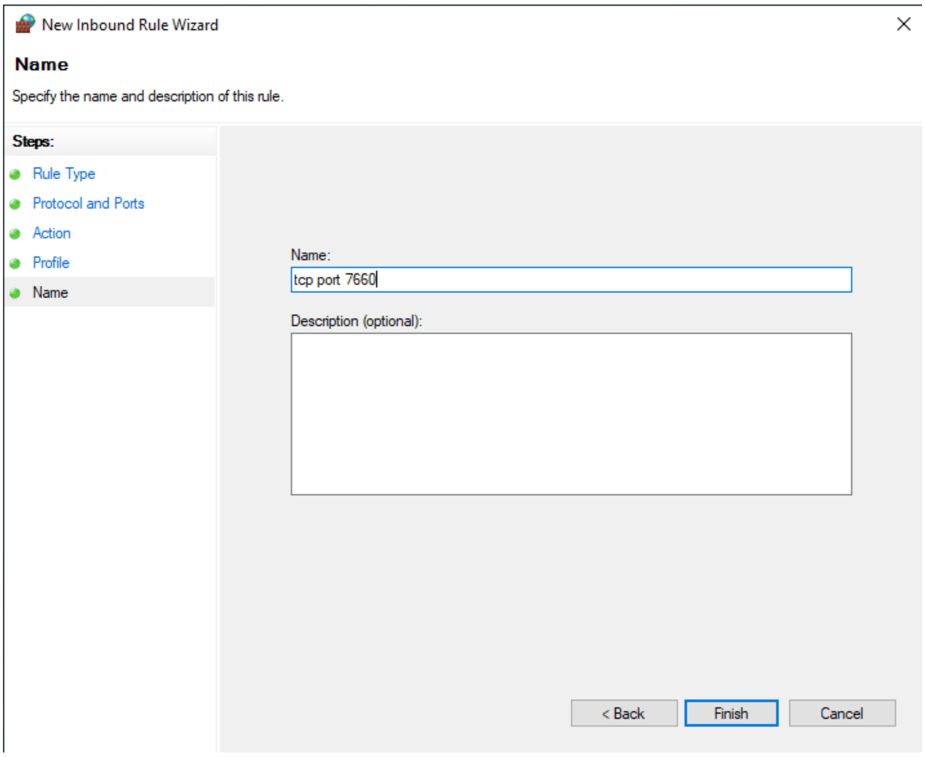
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.



Name

Specify the name and description of this rule.

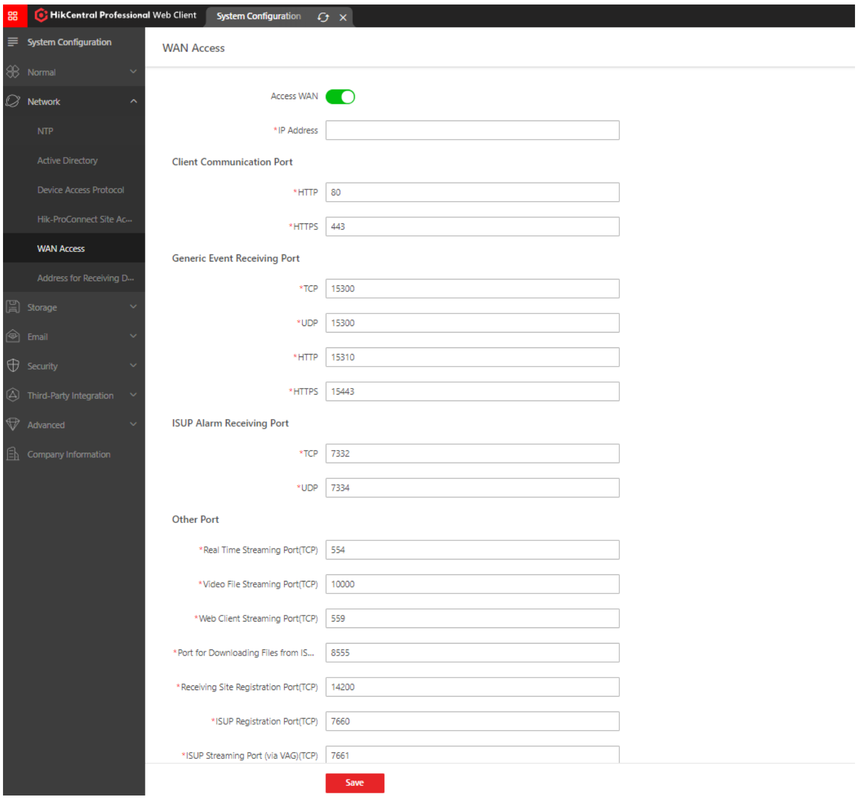
Name: tcp port 7660

Description (optional):

Click Finish, and in the same way, you can configure outbound rules.

4.4 Server WAN Access Configuration

It is necessary to enable HCP and configure WAN IP. The path is as follows: **System Configuration-Network-WAN Access.**



WAN Access

Access WAN: ●

*IP Address:

Client Communication Port

*HTTP: 80

*HTTPS: 443

Generic Event Receiving Port

*TCP: 15300

*UDP: 15300

*HTTP: 15310

*HTTPS: 15443

ISUP Alarm Receiving Port

*TCP: 7332

*UDP: 7334

Other Port

*Real Time Streaming Port(TCP): 554

*Video File Streaming Port(TCP): 10000

*Web Client Streaming Port(TCP): 559

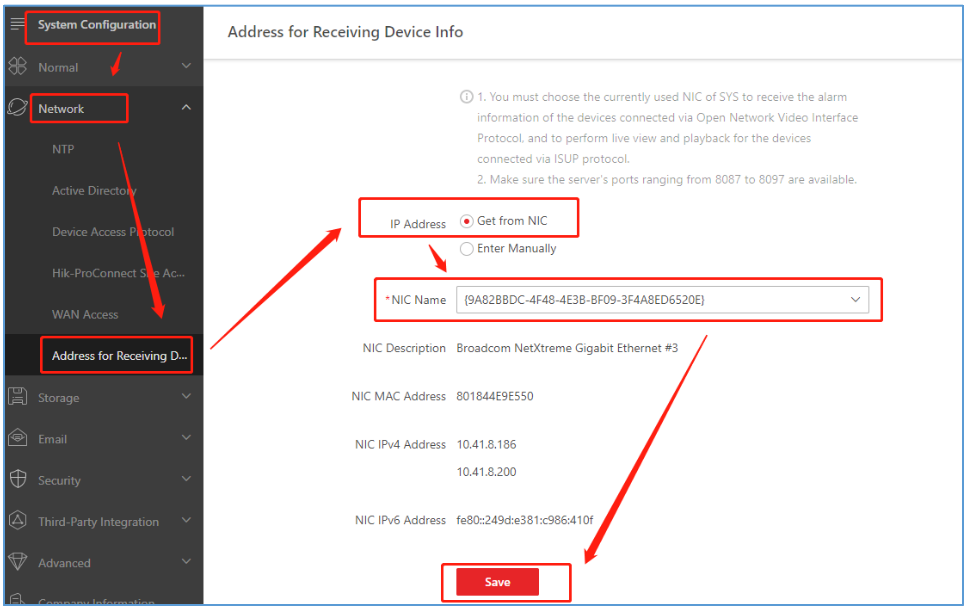
*Port for Downloading Files from IS...: 8555

*Receiving Site Registration Port(TCP): 14200

*ISUP Registration Port(TCP): 7660

*ISUP Streaming Port (via VAG)(TCP): 7661

Enter the address of the receiving device information page and select the correct network card (the IP address of the network card is used to access the HCP)



Address for Receiving Device Info

1. You must choose the currently used NIC of SYS to receive the alarm information of the devices connected via Open Network Video Interface Protocol, and to perform live view and playback for the devices connected via ISUP protocol.

2. Make sure the server's ports ranging from 8087 to 8097 are available.

IP Address ● Get from NIC
○ Enter Manually

*NIC Name {9A82BBDC-4F48-4E3B-BF09-3F4A8ED6520E}

NIC Description Broadcom NetXtreme Gigabit Ethernet #3

NIC MAC Address 801844E9E550

NIC IPv4 Address 10.41.8.186
10.41.8.200

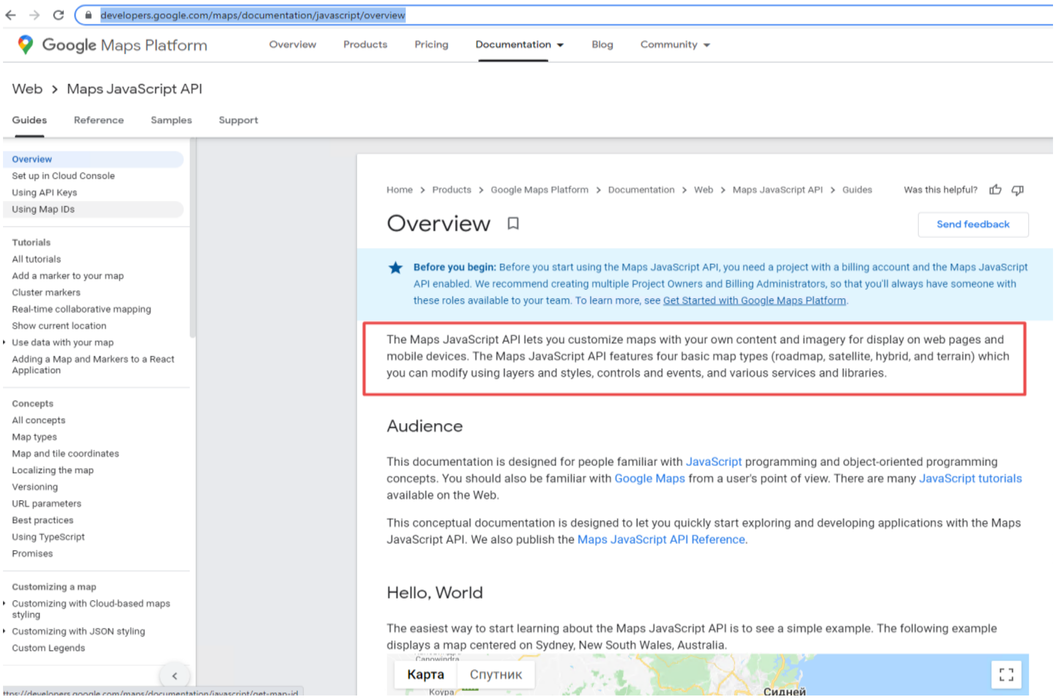
NIC IPv6 Address fe80::249d:e381:c986:410f

4.5 Google Maps Key Application

Customers need to apply for Google Map Key by themselves. For details, please refer to the document "How to Apply API key on GIS Map"

The article link is as follows:

https://hiknow.hikvision.com.cn/kms/sys/attachment/sys_att_main/sysAttMain.do?method=view&fdId=17d1e520bb7ca8d25bffc674c3a9db37



Overview

Before you begin: Before you start using the Maps JavaScript API, you need a project with a billing account and the Maps JavaScript API enabled. We recommend creating multiple Project Owners and Billing Administrators, so that you'll always have someone with these roles available to your team. To learn more, see Get Started with Google Maps Platform.

The Maps JavaScript API lets you customize maps with your own content and imagery for display on web pages and mobile devices. The Maps JavaScript API features four basic map types (roadmap, satellite, hybrid, and terrain) which you can modify using layers and styles, controls and events, and various services and libraries.

Audience

This documentation is designed for people familiar with JavaScript programming and object-oriented programming concepts. You should also be familiar with Google Maps from a user's point of view. There are many JavaScript tutorials available on the Web.

This conceptual documentation is designed to let you quickly start exploring and developing applications with the Maps JavaScript API. We also publish the Maps JavaScript API Reference.

Hello, World

The easiest way to start learning about the Maps JavaScript API is to see a simple example. The following example displays a map centered on Sydney, New South Wales, Australia.

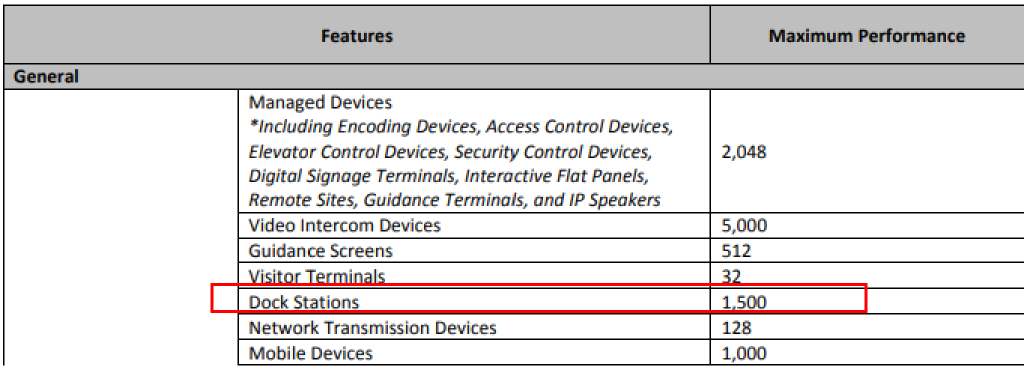
4.6 Platform License

To use HCP V2.3 Body Camera and Dock station services normally, you need to confirm whether to purchase the following license sales items:

✓ **HikCentral-P-DockStation-1Unit**

✓ **HikCentral-P-VSS-1Ch**

The above are the minimum items, HCP 2.3 can support access to up to 1500 Dock Stations



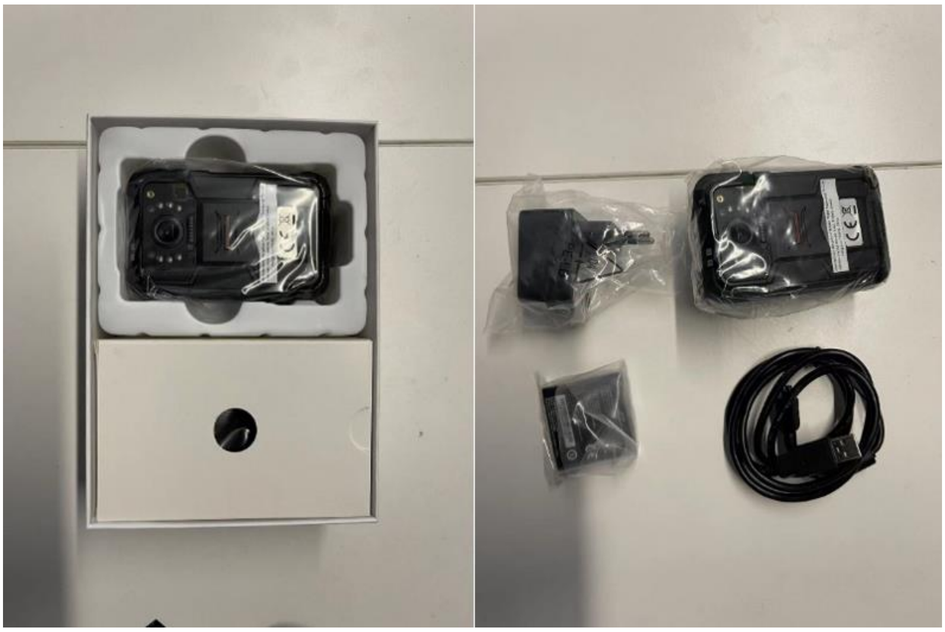
Features		Maximum Performance
General		
	Managed Devices **Including Encoding Devices, Access Control Devices, Elevator Control Devices, Security Control Devices, Digital Signage Terminals, Interactive Flat Panels, Remote Sites, Guidance Terminals, and IP Speakers*	2,048
	Video Intercom Devices	5,000
	Guidance Screens	512
	Visitor Terminals	32
	Dock Stations	1,500
	Network Transmission Devices	128
	Mobile Devices	1,000

5. Body Camera configuration

5.1 Image of Body Camera

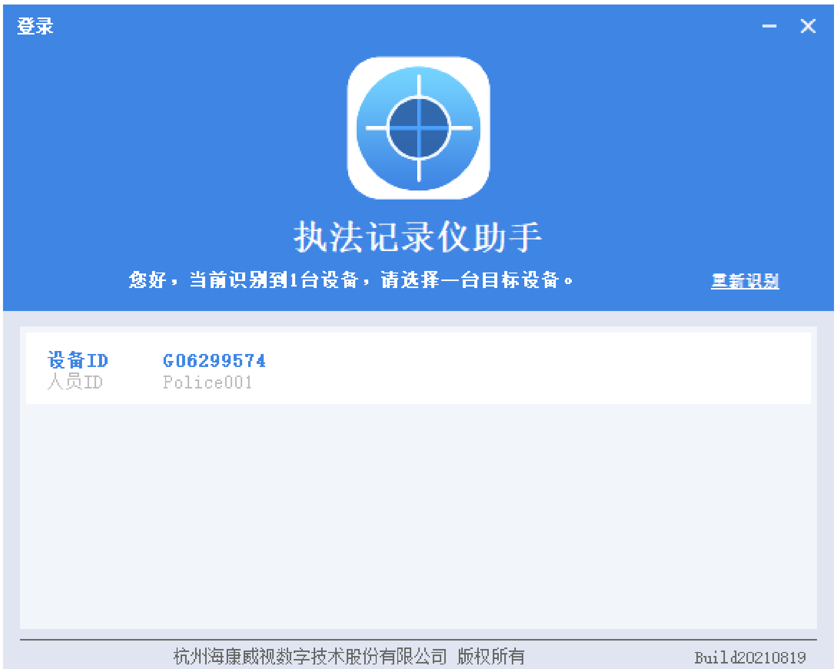
After unpacking, the Body Camera shipped overseas will generally have the following contents as shown in the figure:

Body Camera, serial cable, charger, battery



5.2 Configuration using the BodyCameraAssistant tool

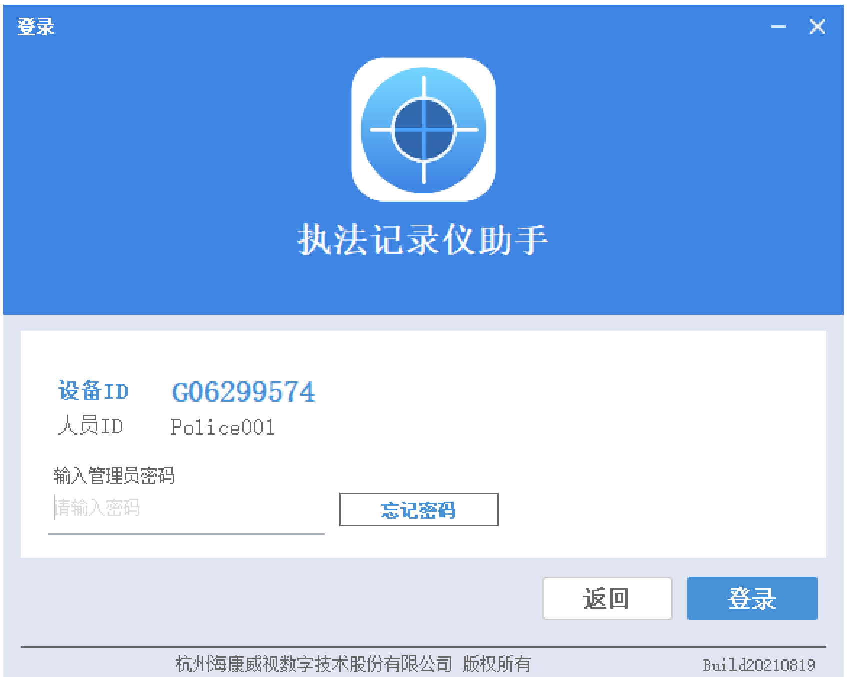
- ✓ Use the BodyCameraAssistant tool to edit the parameters of the device. After connecting the Body Camera to the PC using the serial cable, open the BodyCameraAssistant tool, select the corresponding device, and log in after entering the password. **The default password is 123456.**



您好，当前识别到1台设备，请选择一台目标设备。

设备ID G06299574
人员ID Police001

杭州海康威视数字技术股份有限公司 版权所有 Build20210819



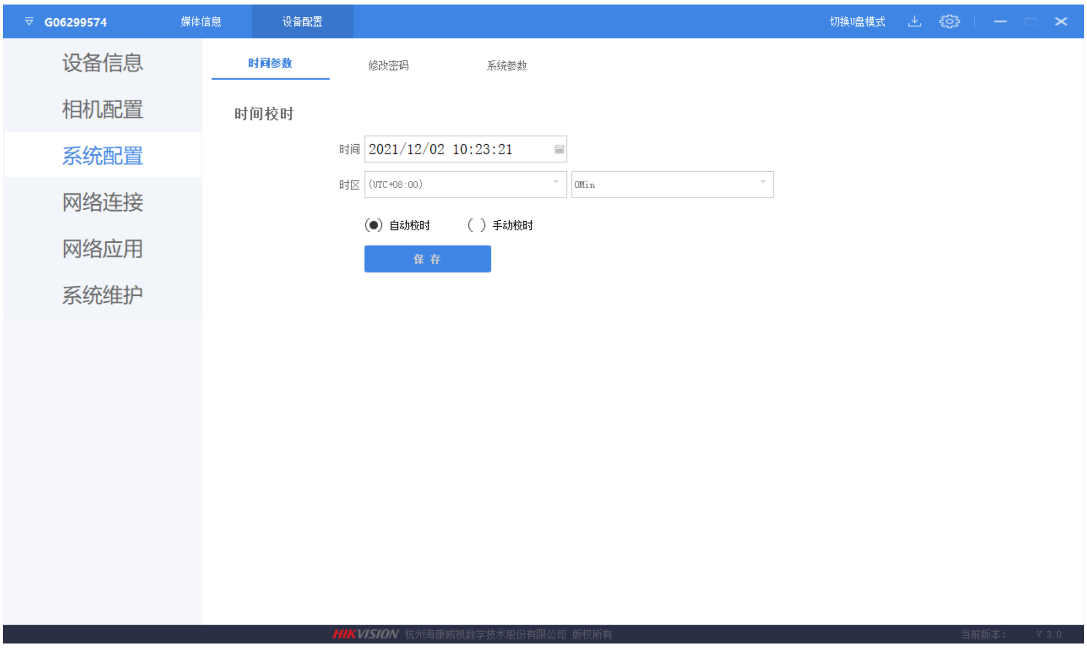
设备ID G06299574
人员ID Police001

输入管理员密码
请输入密码

杭州海康威视数字技术股份有限公司 版权所有 Build20210819

- ✓ BodyCameraAssistant has quite a lot of configuration contents. When you use it for the first time, you can configure other information such as time and Ehome for the device.

- ✓ At present, the BodyCameraAssistant tool can only set Ehome. If other protocols are required, they can be configured on the device "Setting-Network-video platform"

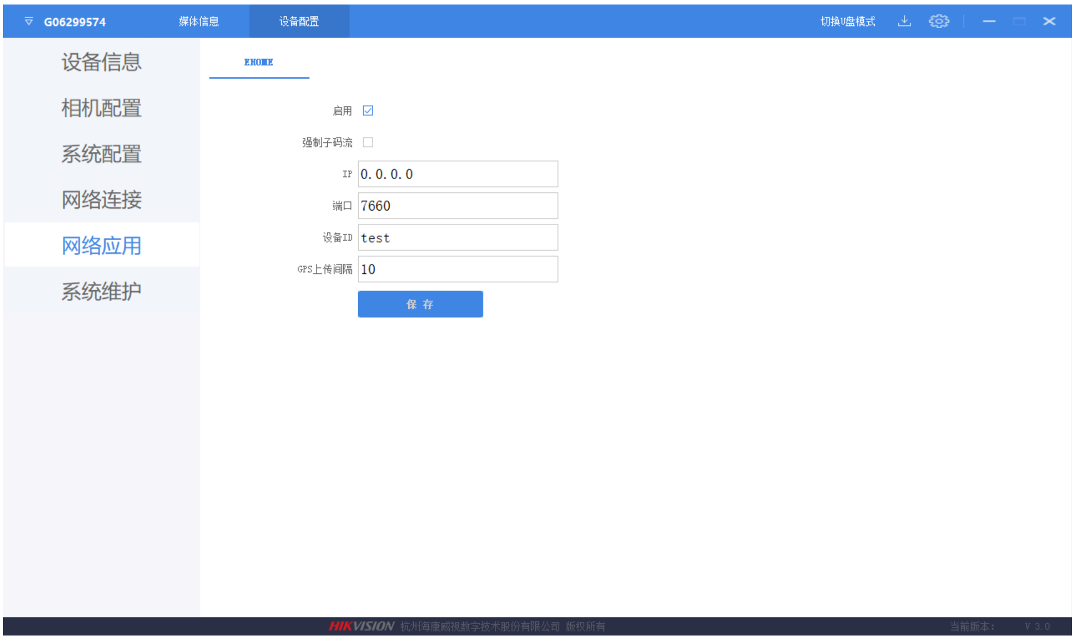


时间校时

时间 2021/12/02 10:23:21

时区 (UTC+08:00) 0Min

● 自动校时 ( ) 手动校时



启用 ☑

强制子码流 □

IP 0. 0. 0. 0

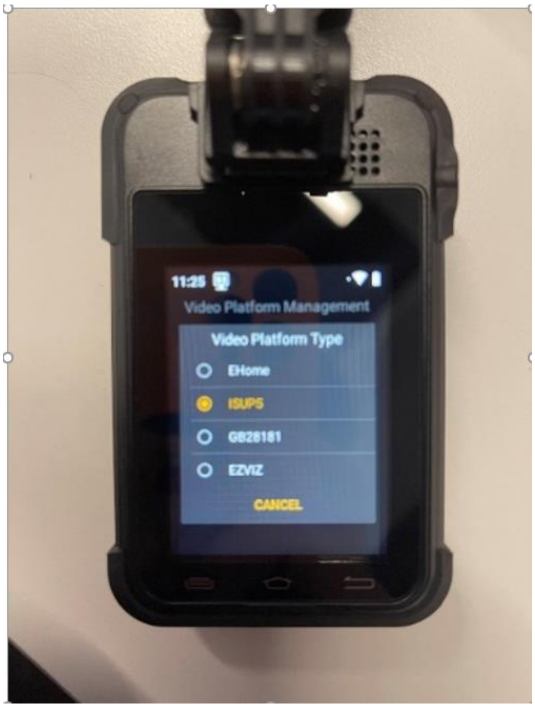
端口 7660

设备ID test

GPS上传间隔 10

5.3 Configure platform information on Body Camera

- ✓ On the Video Platform Type page of Body Camera, select ISUP5.



11:25

Video Platform Management

Video Platform Type

○ EHome

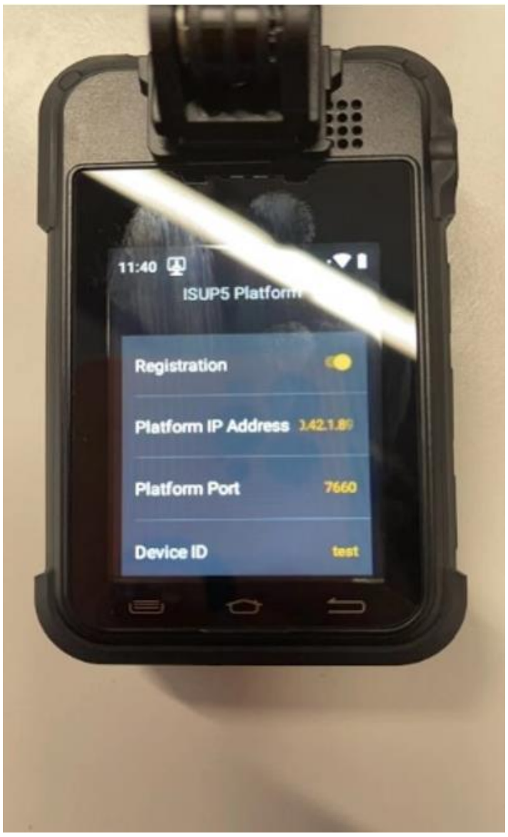
● ISUP5

○ GB28181

○ EZVIZ

CANCEL

✓ On the Platform page of the Body Camera, configure the Platform IP Address (the platform IP to be added), Platform (the ISUP port of HCP is 7660), Device ID, and ISUP Login Password.



11:40

ISUP5 Platform

Registration ●

Platform IP Address 3.42.1.89

Platform Port 7660

Device ID test

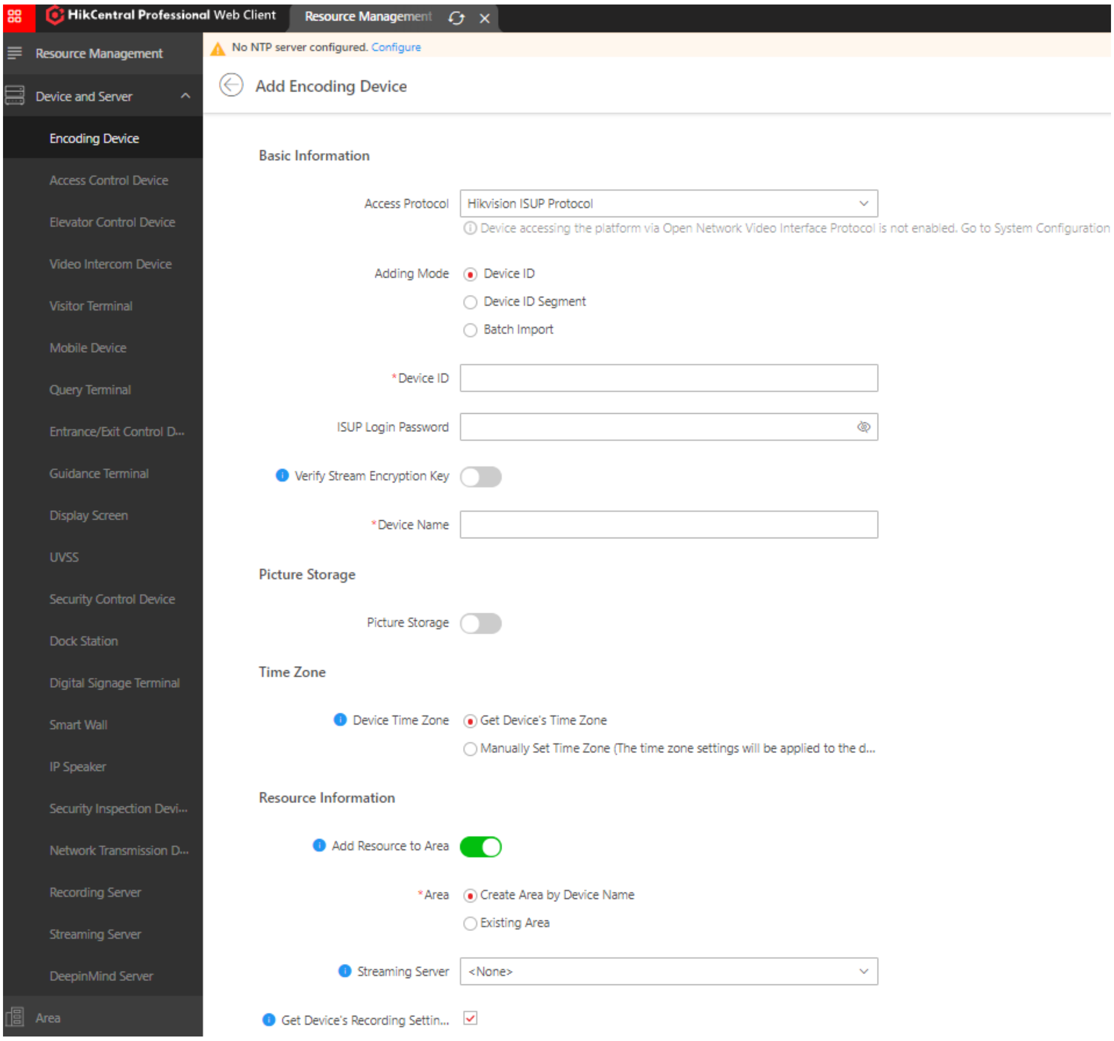
6. HCP configuration

6.1 Add Body Camera to HCP

Log in to HCP 2.3, go to **General-Resource Management->Encoding Device->Click** Add to add a handheld device.

- ✓ **Access Protocol:** Hikvision ISUP Protocol
- ✓ **Device ID:** consistent with the device configuration
- ✓ **ISUP Login Password:** consistent with the device configuration
- ✓ **Device Name:** The device will be added to the platform with this name.
- ✓ **Verify Stream Encryption Key:** Enable stream encryption (this is a new feature in HCP 2.3)

Click Add to finish adding



No NTP server configured. Configure

Add Encoding Device

Basic Information

Access Protocol: Hikvision ISUP Protocol

ⓘ Device accessing the platform via Open Network Video Interface Protocol is not enabled. Go to System Configuration

Adding Mode: ● Device ID ○ Device ID Segment ○ Batch Import

*Device ID:

ISUP Login Password:

Verify Stream Encryption Key: off

*Device Name:

Picture Storage

Picture Storage: off

Time Zone

Device Time Zone: ● Get Device's Time Zone ○ Manually Set Time Zone (The time zone settings will be applied to the d...

Resource Information

Add Resource to Area: on

*Area: ● Create Area by Device Name ○ Existing Area

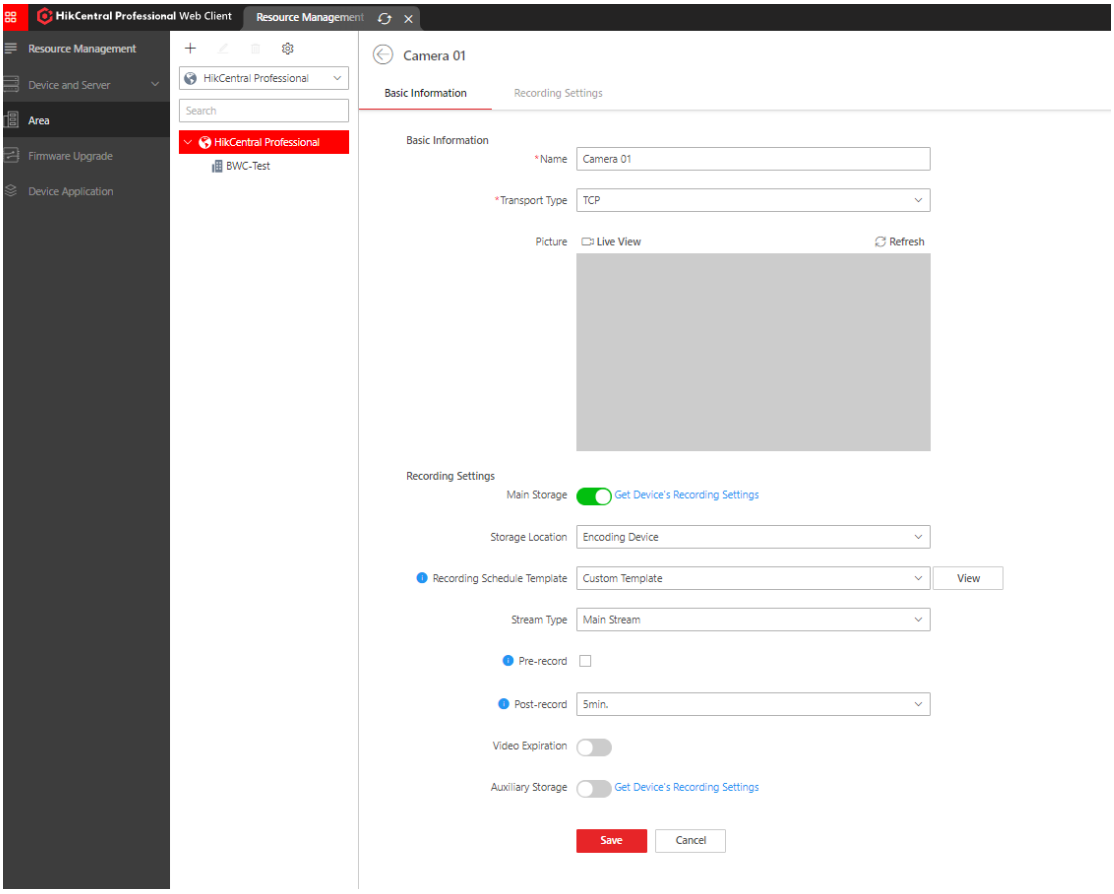
Streaming Server: <None>

Get Device's Recording Settin... ☑

6.2 Recording Schedule Settings

Select the Area page, you can see the successfully added channel, click the channel name to enter the editing related information. Body Camera can be configured with local main memory or pStor or CVR, and does not support video playback.

[Note] In order to avoid generating a large amount of mobile data, the recording of the Body Camera is generally selected to be stored locally on the device. At this time, the platform will issue an empty recording plan to the device. Whether to record or not depends on whether recording is enabled on the Body Camera.



Basic Information

*Name: Camera 01

*Transport Type: TCP

Picture

Recording Settings

Main Storage: on

Storage Location: Encoding Device

Recording Schedule Template: Custom Template

Stream Type: Main Stream

Pre-record: □

Post-record: 5min.

Video Expiration: off

Auxiliary Storage: off

6.3 Add Dock Station to HCP

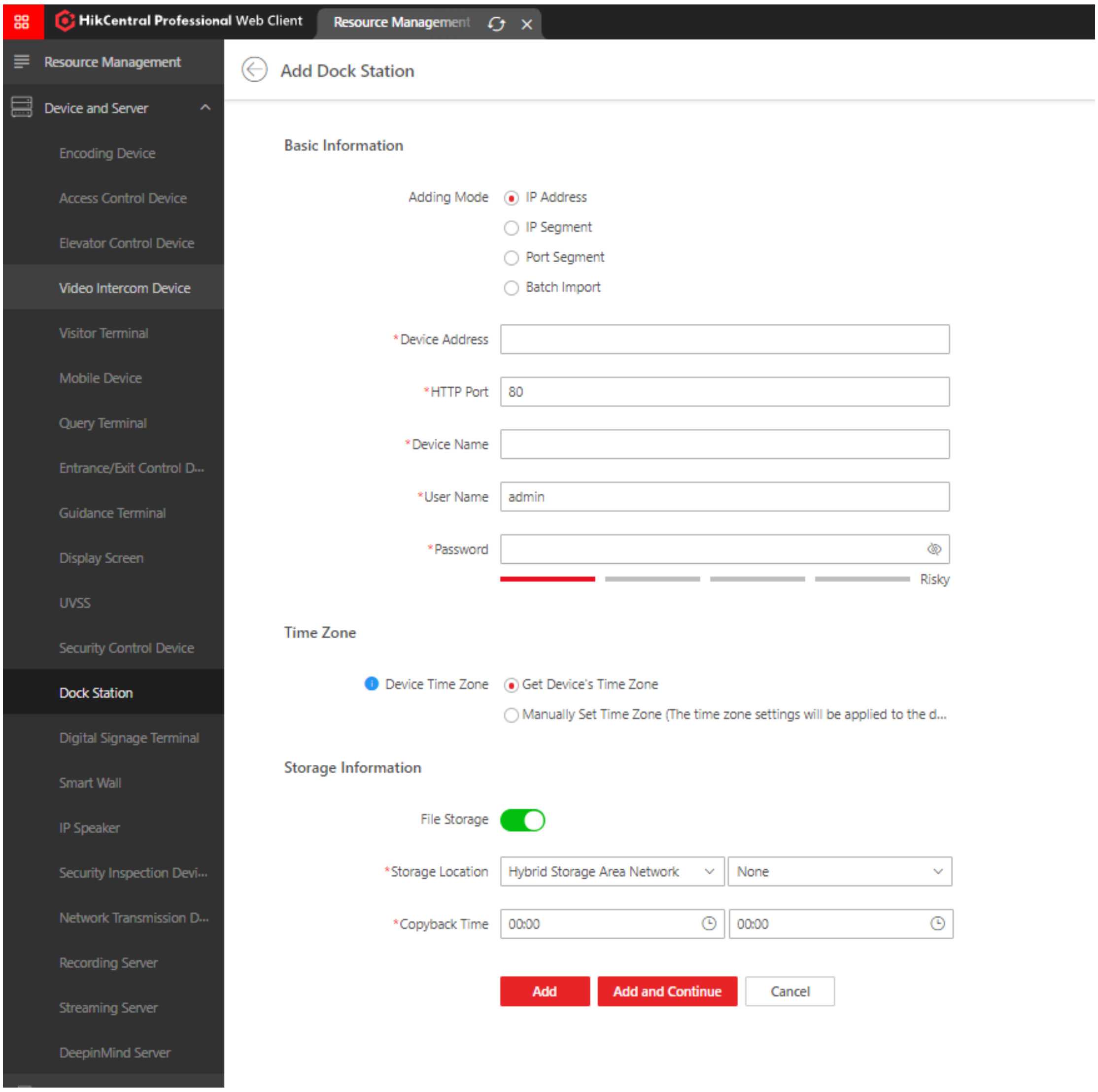
Go to **General-Resource Management->Dock Station ->Click Add to add a Dock Station**.

- ✓ **Adding Mode:** IP Address
- ✓ **Device Address:** Device IP
- ✓ **Device Port:** Determined according to the actual situation (the default port is 5651,

and devices such as MDS001 and MDS003 use port 80)

- ✓ **Device Name:** The device will be added to the platform with this name.
- ✓ **User Name:** Device login name
- ✓ **Password:** Device login password
- ✓ **File Storage:** Set the file storage location, optional pStor or CVR, and configure the return time

Click Add to complete the addition



Add Dock Station

Basic Information

Adding Mode: ● IP Address ○ IP Segment ○ Port Segment ○ Batch Import

*Device Address:

*HTTP Port: 80

*Device Name:

*User Name: admin

*Password: Risky

Time Zone

Device Time Zone: ● Get Device's Time Zone ○ Manually Set Time Zone (The time zone settings will be applied to the d...

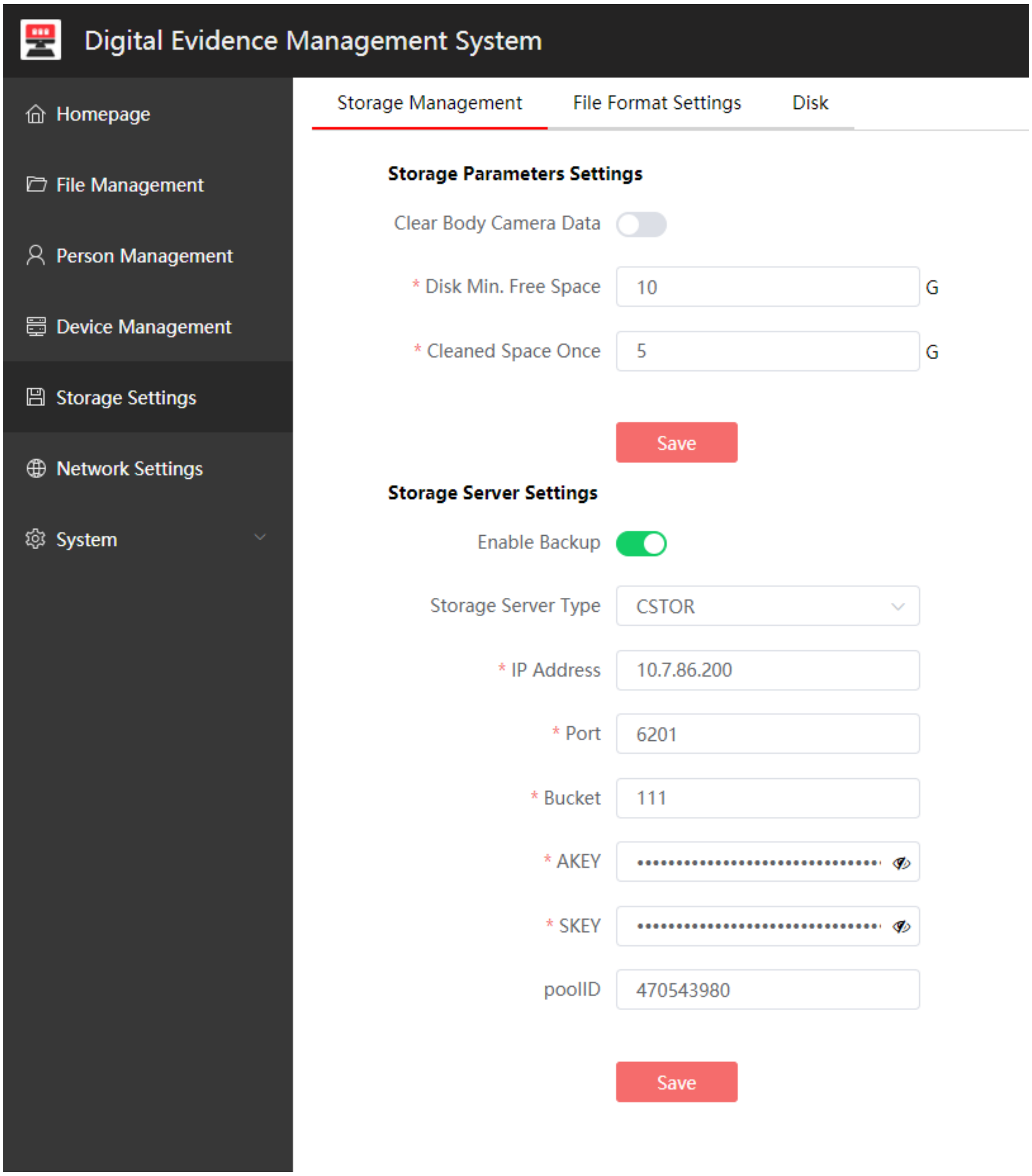
Storage Information

File Storage: on

*Storage Location: Hybrid Storage Area Network | None

*Copyback Time: 00:00 | 00:00

After the addition is complete, you can remotely jump to the WEB side of the Dock Station. On the Storage Settings page, you can see the storage server configuration issued by the platform.



Storage Parameters Settings

Clear Body Camera Data ○

* Disk Min. Free Space 10 G

* Cleaned Space Once 5 G

Storage Server Settings

Enable Backup ●

Storage Server Type CSTOR

* IP Address 10.7.86.200

* Port 6201

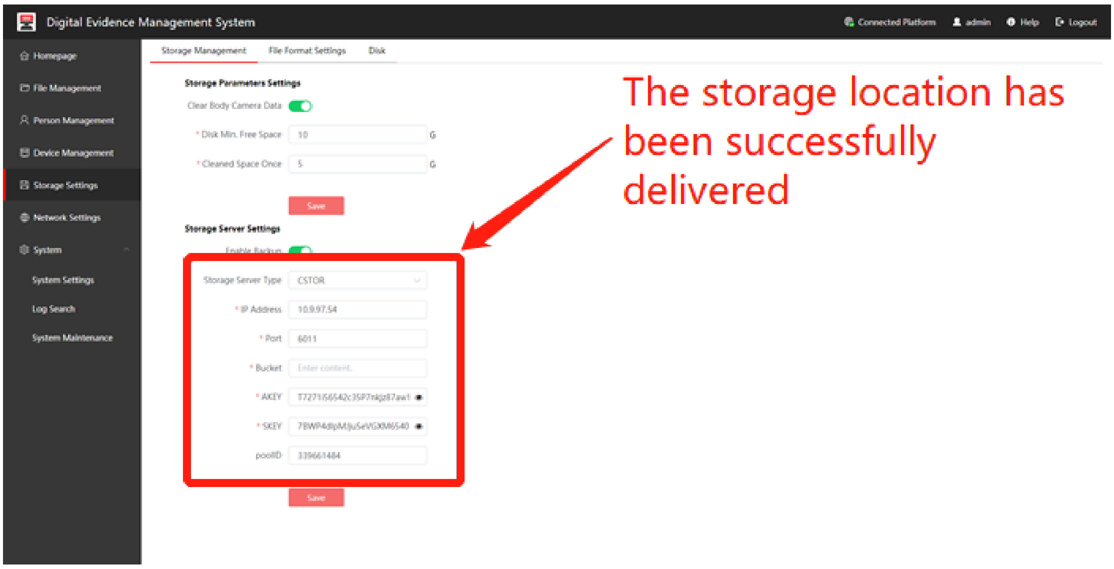
* Bucket 111

* AKEY ································

* SKEY ································

poolID 470543980

Configure whether to clear the Body Camera data and file format as needed



Storage Parameters Settings

Clear Body Camera Data: on

* Disk Min. Free Space: 10 G

* Cleaned Space Once: 5 G

Storage Server Settings

Enable Backup: on

Storage Server Type: CSTOR

* IP Address: 10.9.97.54

* Port: 6011

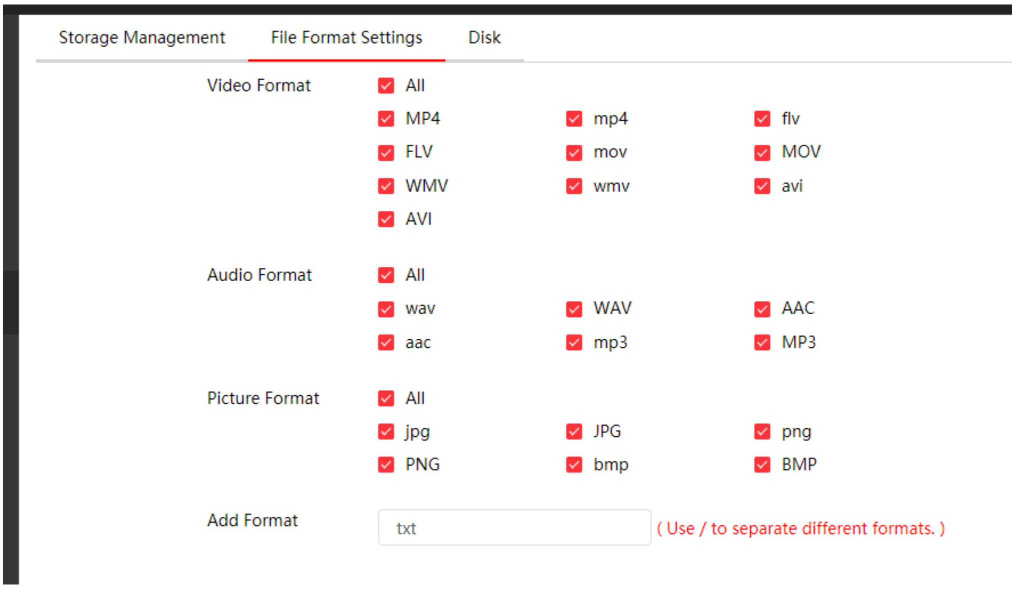
* Bucket: Enter content.

* AKEY: T7271I56542c3SP7nkjz87aw1

* SKEY: 7BWP4dlpMJjuSeVGXM6540

poolID: 339661484

The storage location has been successfully delivered



Video Format: ☑ All

☑ MP4 ☑ mp4 ☑ flv

☑ FLV ☑ mov ☑ MOV

☑ WMV ☑ wmv ☑ avi

☑ AVI

Audio Format: ☑ All

☑ wav ☑ WAV ☑ AAC

☑ aac ☑ mp3 ☑ MP3

Picture Format: ☑ All

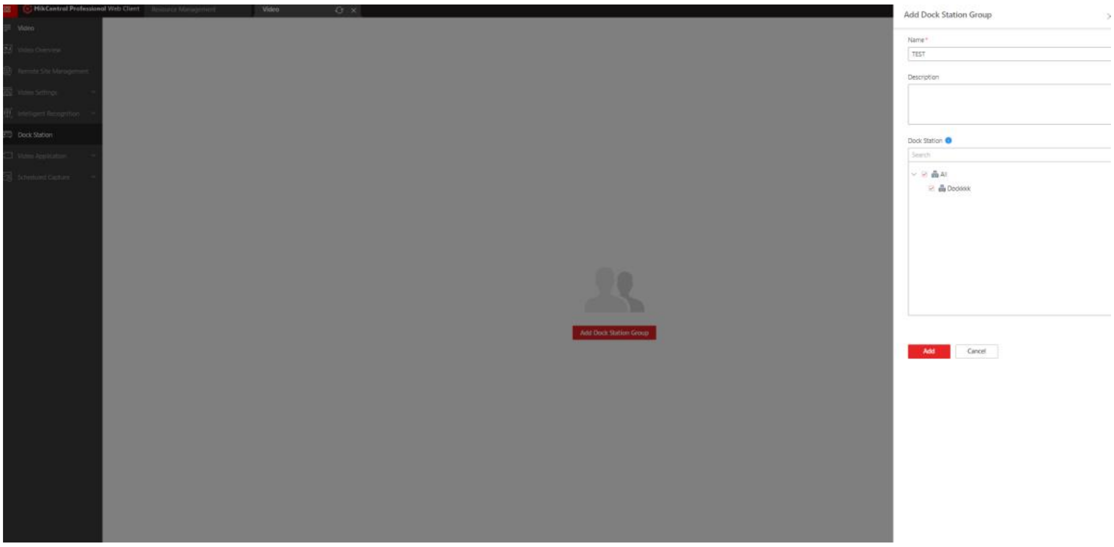
☑ jpg ☑ JPG ☑ png

☑ PNG ☑ bmp ☑ BMP

Add Format: txt (Use / to separate different formats.)

6.4 Dock Station Group Configuration

✓ Enter Video – Dock Station, then add a dock station group, fill in the name of the dock station group, and check the corresponding dock station, then click Add.



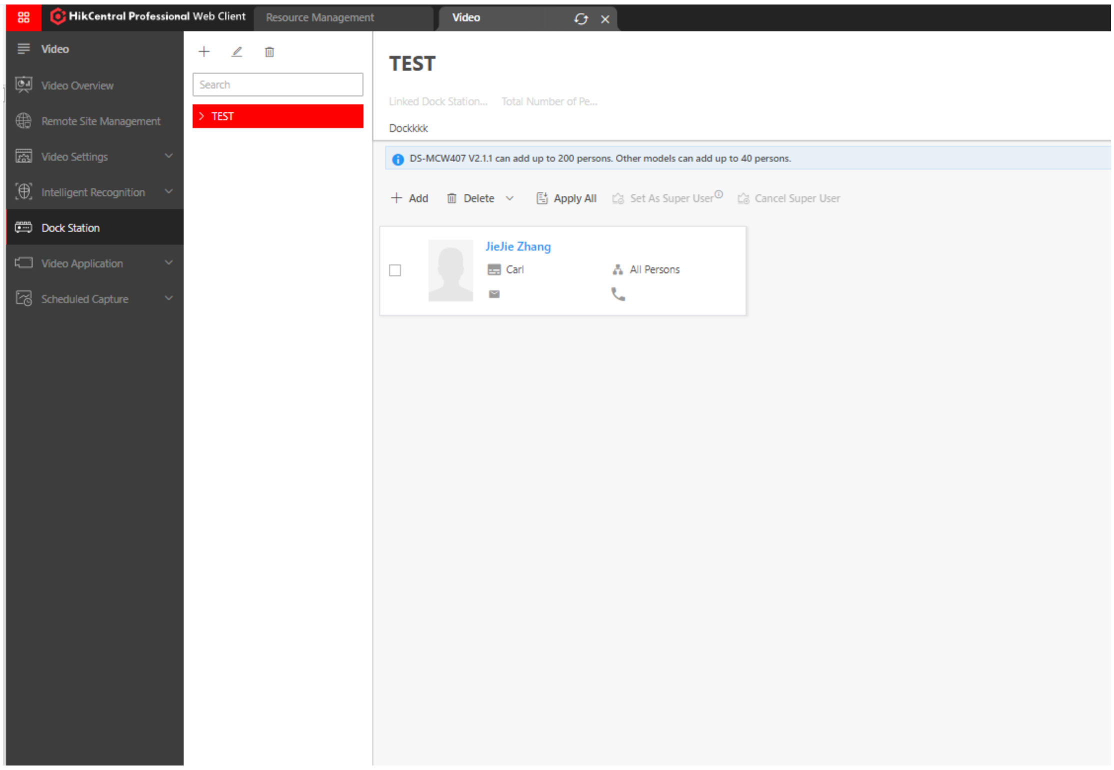
Add Dock Station Group

Name*: TEST

Description:

- ✓ You can associate a person in an established dock station group, click ADD to add, you can directly import the person added in the Person module, you can assign a person, or set/cancel the person's collection station super user authority.

[Note]: Version 2.1.1 of DS-MCW407 can support 200 people, other models can support up to 40 people. Apply all: Send personnel to the dock stations included in the dock station group (it will cover the personnel uploaded on the web side of the dock station).

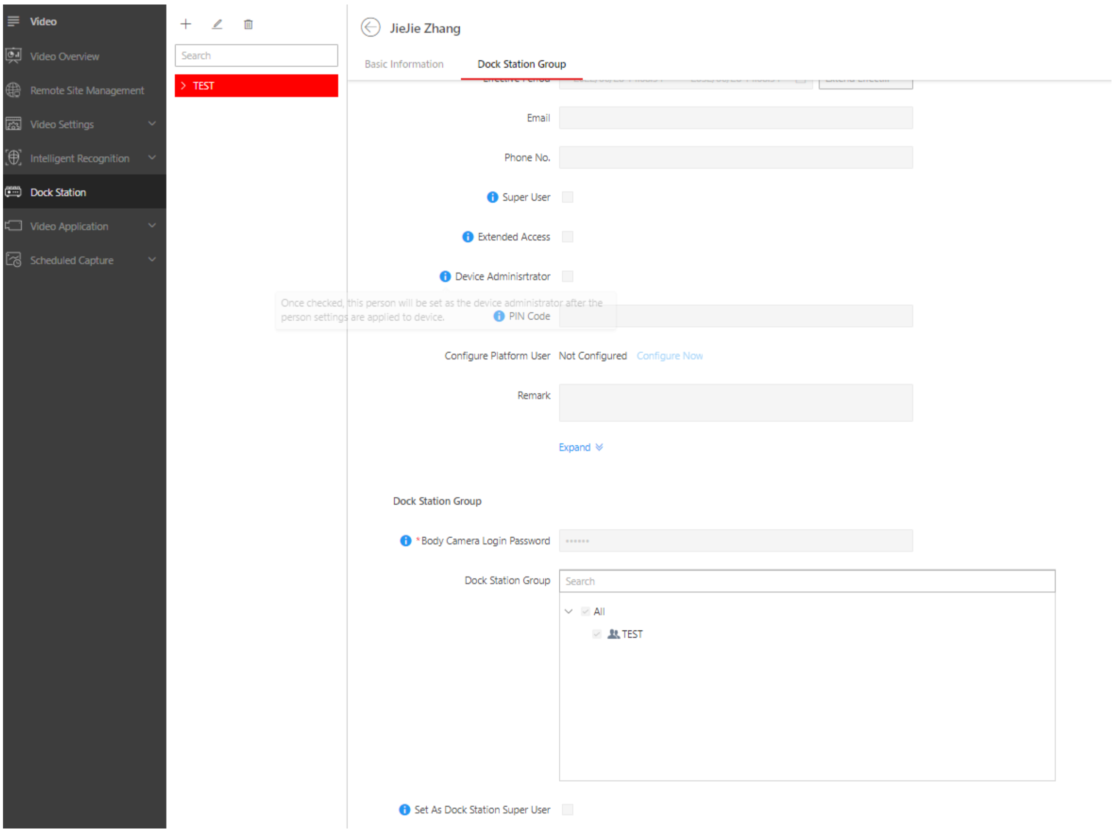


TEST

Linked Dock Station...: Dockkkk

DS-MCW407 V2.1.1 can add up to 200 persons. Other models can add up to 40 persons.

- ✓ Click the person's name to enter the editing interface. In the Dock Station Group directory, a login password can be configured for the person. After the distribution is completed, the login password can be used to log in to Body Camera.



JieJie Zhang

Email

Phone No.

Super User □

Extended Access □

Device Adminisrtrator □

Once checked, this person will be set as the device administrator after the person settings are applied to device.

PIN Code

Configure Platform User: Not Configured Configure Now

Remark

Dock Station Group

*Body Camera Login Password: ······

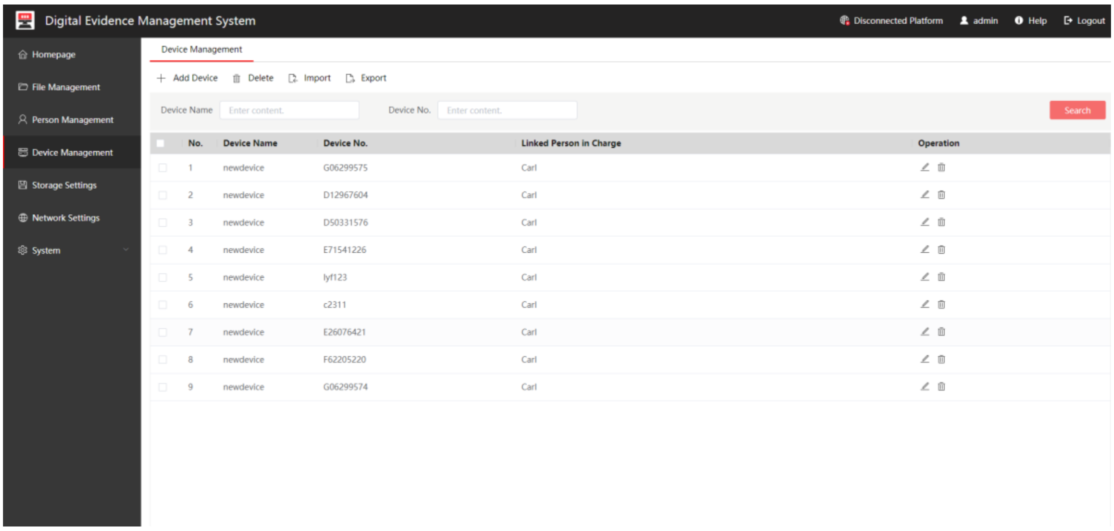
Dock Station Group: Search

All

TEST

Set As Dock Station Super User □

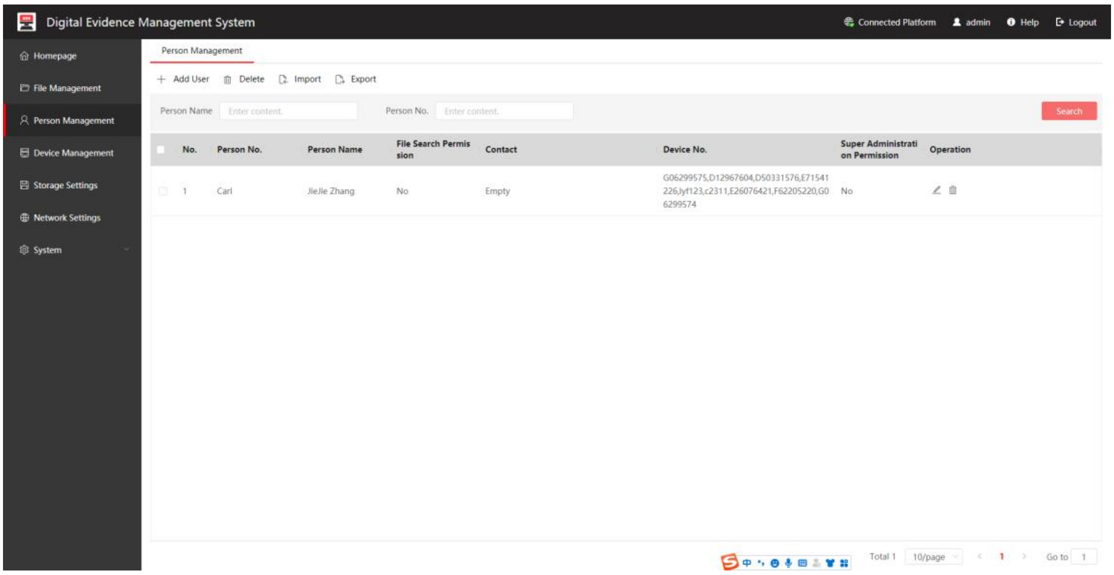
✓ The Device Management interface can automatically identify the BWC inserted into the Dock Station. Click Edit to bind the device to the person.



Device Name: Enter content. Device No.: Enter content.

No.	Device Name	Device No.	Linked Person in Charge	Operation
1	newdevice	G06299575	Carl	
2	newdevice	D12967604	Carl	
3	newdevice	D50331576	Carl	
4	newdevice	E71541226	Carl	
5	newdevice	lyf123	Carl	
6	newdevice	c2311	Carl	
7	newdevice	E26076421	Carl	
8	newdevice	F62205220	Carl	
9	newdevice	G06299574	Carl	

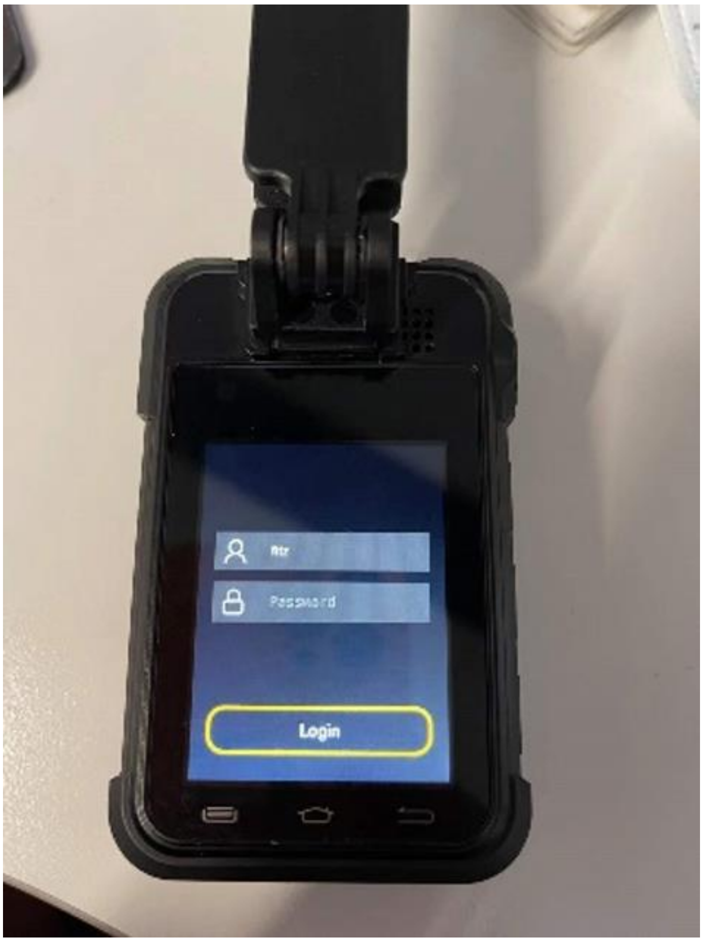
✓ After clicking Send, the personnel will be sent to each Dock Station in the Dock Station Group, and then the Dock Station will send the personnel to the Body Camera, and the user can log in to the Body Camera through the set password.



Person Name: Enter content.

Person No.: Enter content.

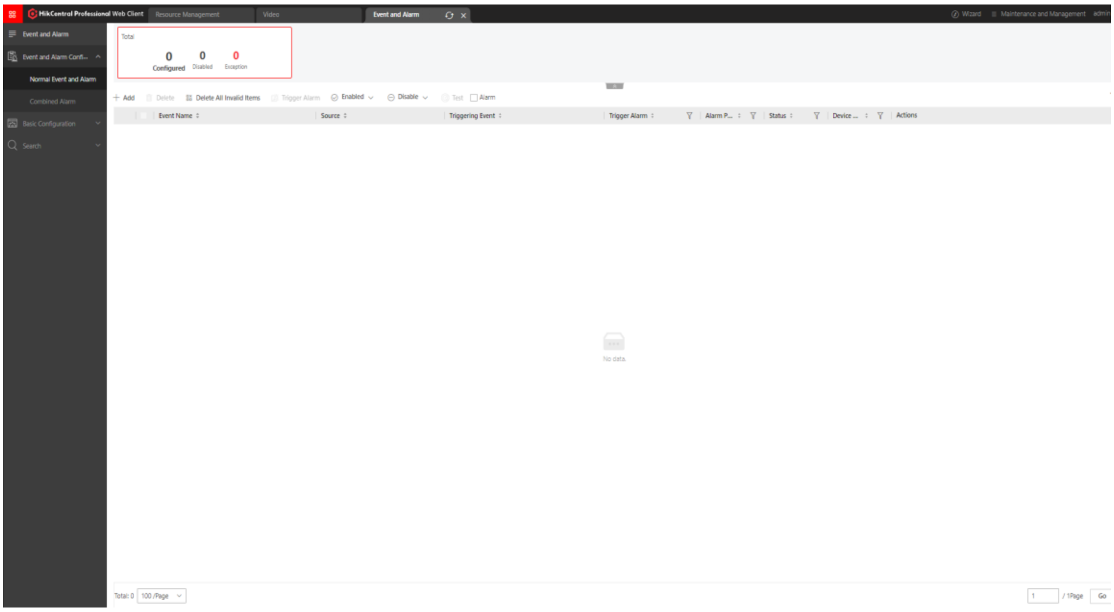
□	No.	Person No.	Person Name	File Search Permission	Contact	Device No.	Super Administration Permission	Operation
□	1	Carl	JieJie Zhang	No	Empty	G06299575,D12967604,D50331576,E71541226,lyf123,c2311,E26076421,F62205220,G06299574	No	



- ✓ As shown above, the personnel has been successfully sent to the Dock Station, and the Dock Station has sent the personnel to the Body Camera.

6.5 Body Camera one-key alarm configuration

- ✓ Go to **General - Event and Alarm**, click Add to add a new alarm.

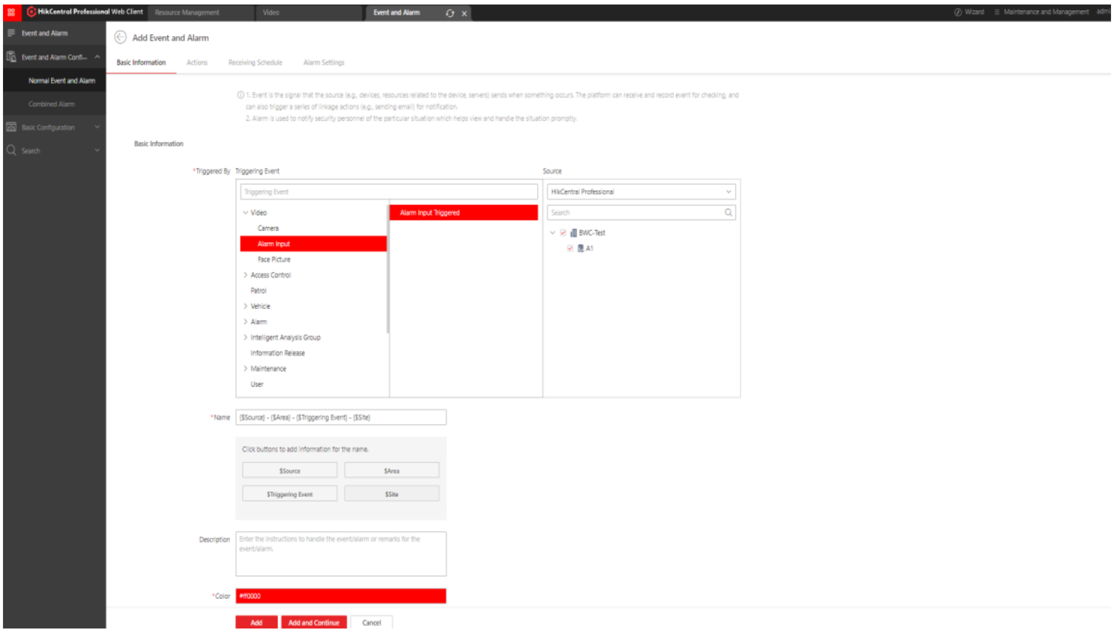


Total

0 Configured 0 Disabled 0 Exception

Total: 0 100 /Page

- ✓ Select Video – Alarm input – Alarm Input Triggered in order in the trigger event, and select the trigger under Body Camera as shown in the figure.



Add Event and Alarm

1. Event is the signal that the source (e.g., devices, resources related to the device, servers) sends when something occurs. The platform can receive and record event for checking, and can also trigger a series of linkage actions (e.g., sending email) for notification.
2. Alarm is used to notify security personnel of the particular situation which helps view and handle the situation promptly.

Basic Information

*Triggered By Triggering Event

Source: HikCentral Professional

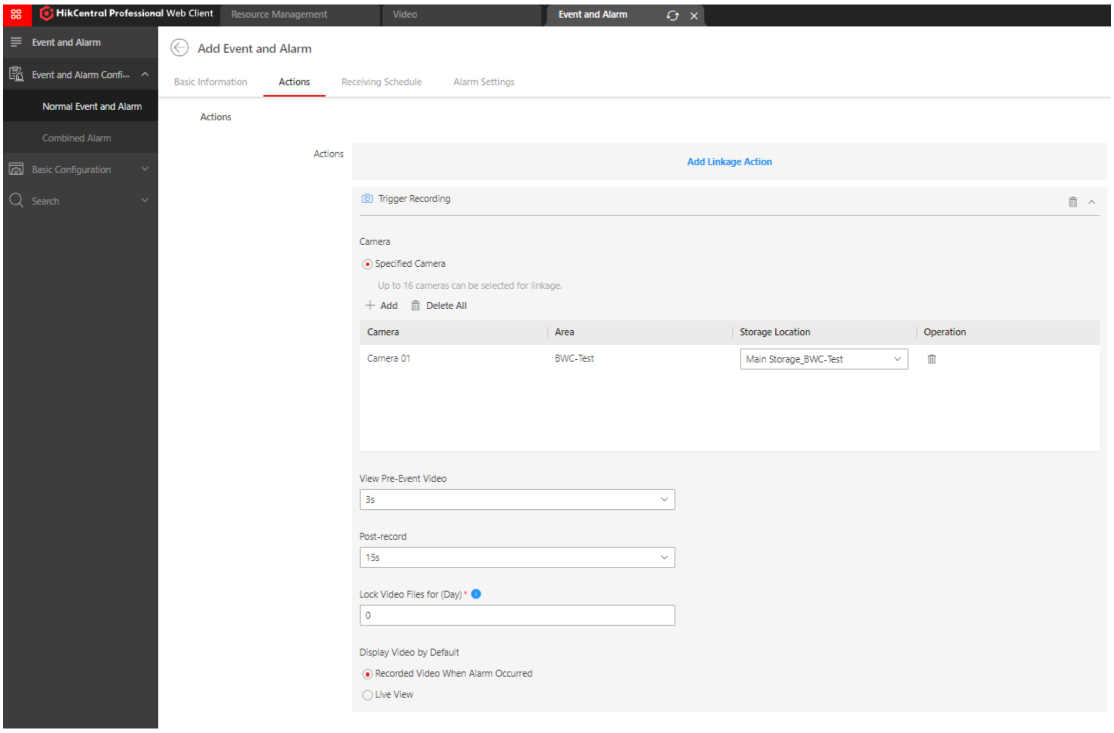
*Name: {$Source} - {$Area} - {$Triggering Event} - {$Site}

Click buttons to add information for the name.

Description: Enter the instructions to handle the event/alarm or remarks for the event/alarm.

*Color: #ff0000

- ✓ Generally, the one-key alarm function of the Body Camera is realized with the linkage recording. You can configure the linkage recording as shown in the figure below. Here you can choose the linkage rules.



Add Event and Alarm

Actions

Actions

Trigger Recording

Camera

● Specified Camera

Up to 16 cameras can be selected for linkage.

Camera	Area	Storage Location	Operation
Camera 01	BWC-Test	Main Storage_BWC-Test	

View Pre-Event Video: 3s

Post-record: 15s

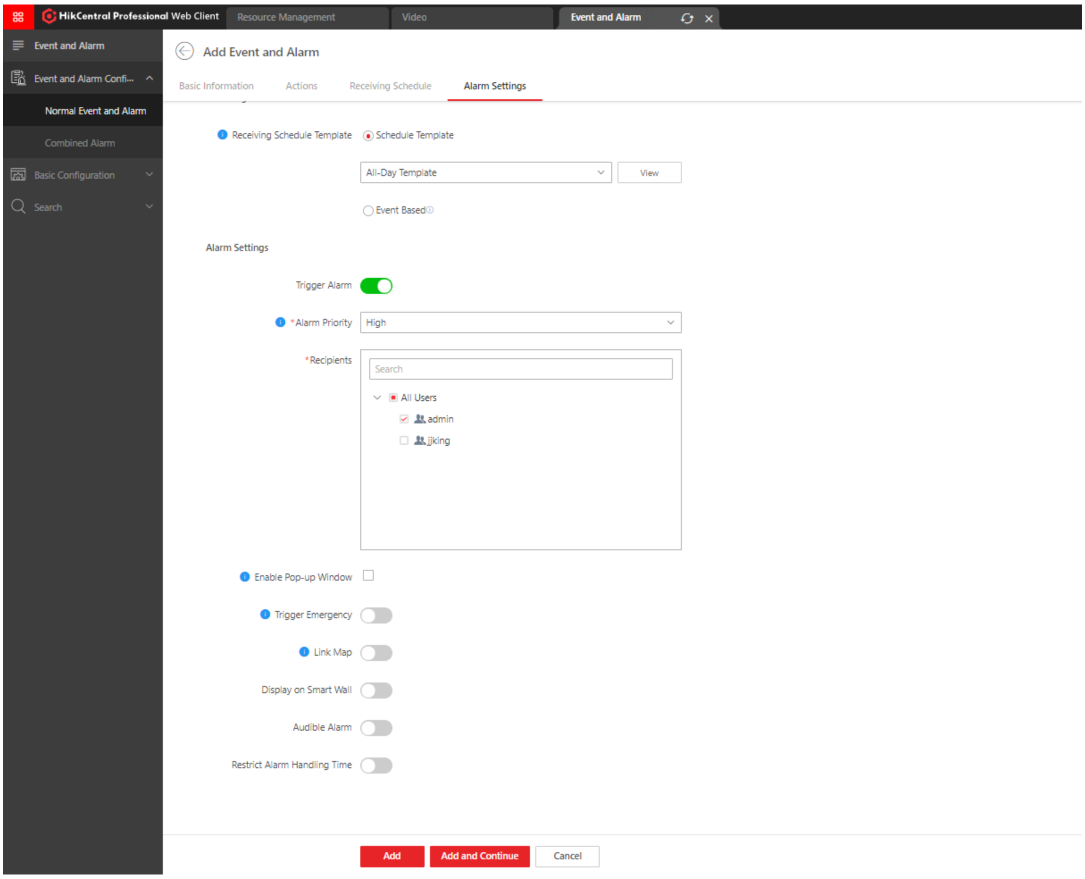
Lock Video Files for (Day)*: 0

Display Video by Default

● Recorded Video When Alarm Occurred

○ Live View

✓ And choose whether to trigger the alarm according to the actual situation. If you need to trigger, select the user who accepts the alarm, the alarm level, whether to open the pop-up window, etc.



Add Event and Alarm

Receiving Schedule Template: ● Schedule Template — All-Day Template; ○ Event Based

Alarm Settings

Trigger Alarm: On

*Alarm Priority: High

*Recipients: Search

- All Users
  - ☑ admin
  - □ jjking

Enable Pop-up Window: □

Trigger Emergency: Off

Link Map: Off

Display on Smart Wall: Off

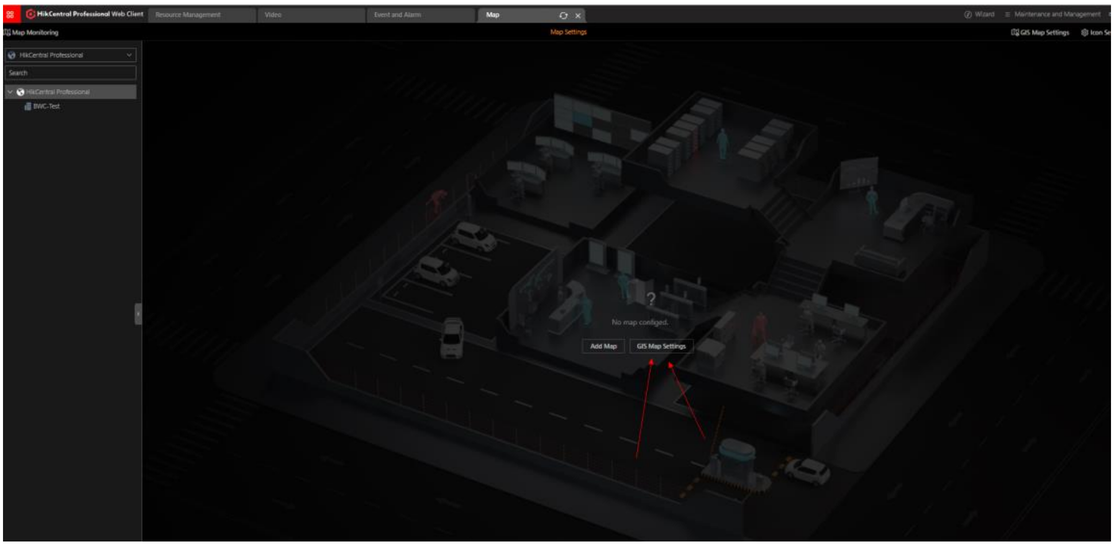
Audible Alarm: Off

Restrict Alarm Handling Time: Off

✓ After completing the above configuration, press the red button on the Body Camera to complete a one-key alarm.

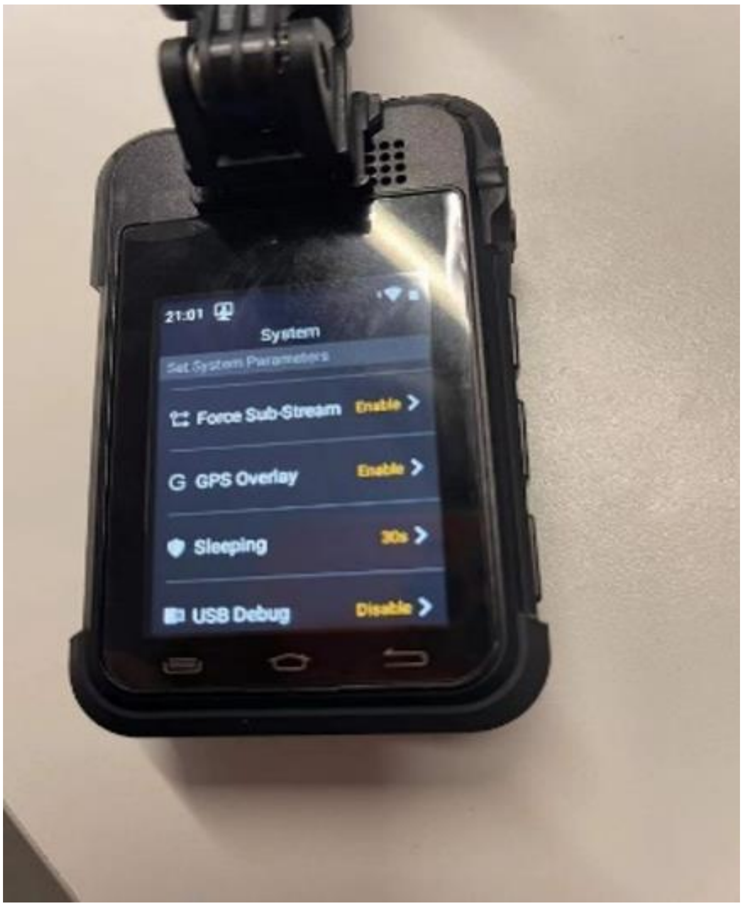
6.6 Body Camera Map Configuration

- ✓ Enter HCP 2.3, click **Map - Map Settings - GIS Map Settings** to configure the GIS map, and add the Body Camera to the specified location.



No map configed.

- ✓ On the Body Camera, go to **System - Turn on GPS Overlay.**

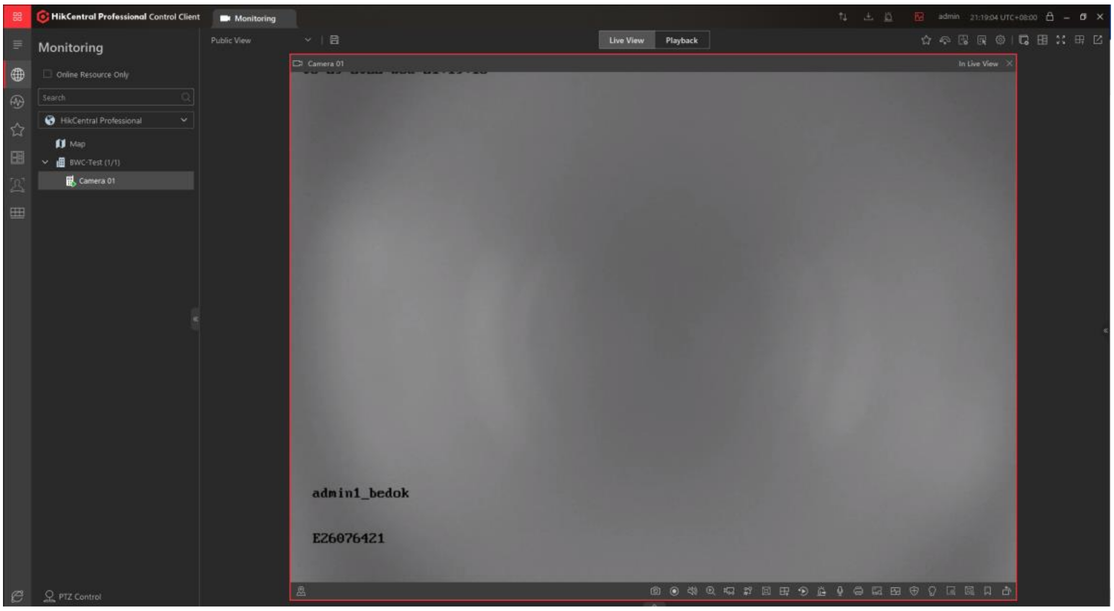


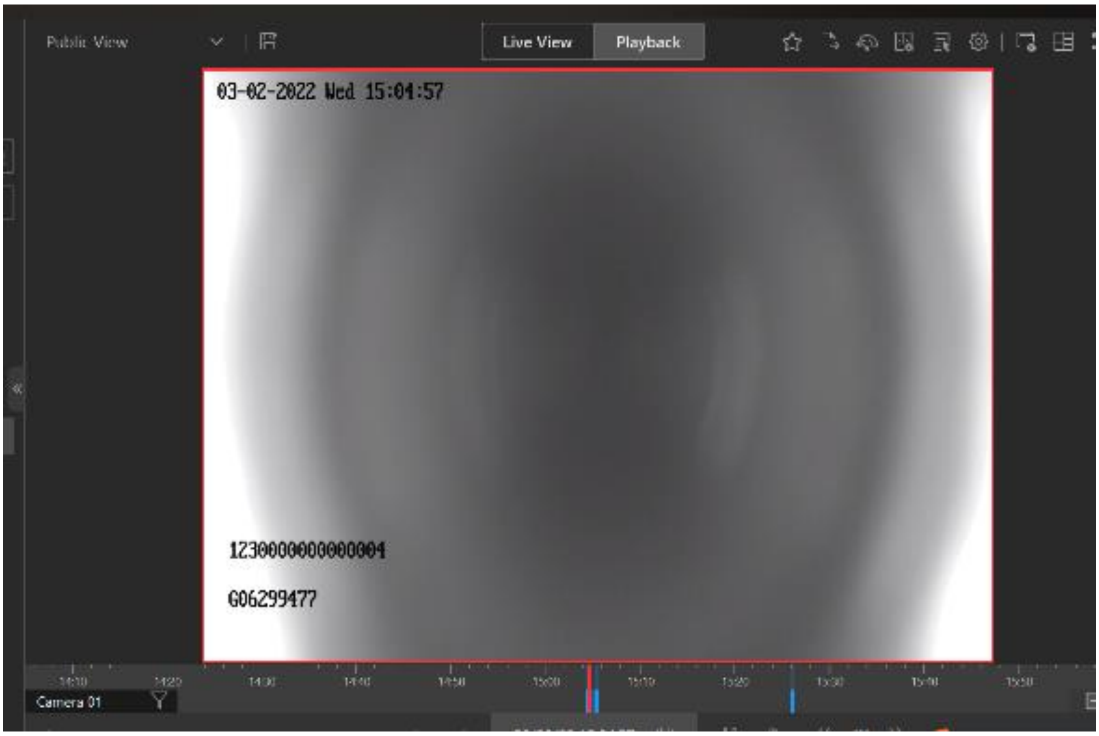
Force Sub-Stream Enable
GPS Overlay Enable
Sleeping 30s
USB Debug Disable

7 Functional Verification

7.1 Body Camera Preview And Playback

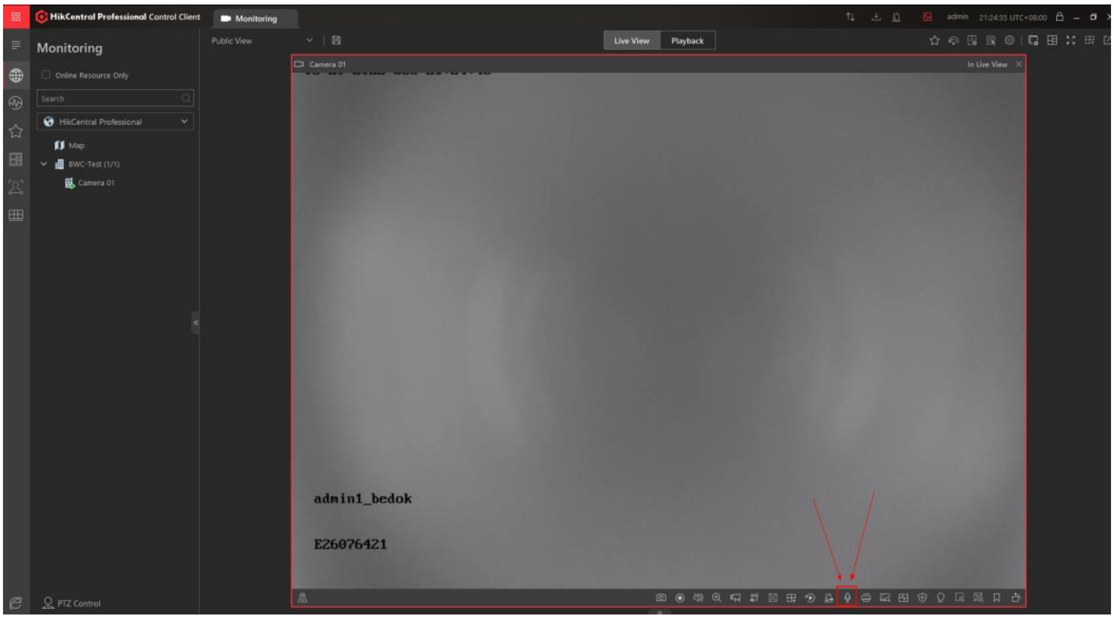
The body camera recording schedule does not support configuration. When configuring on the WEB side of the platform, a recording schedule with an empty plan template will be generated on the platform, and it will not be actually delivered to the device, so the actual recording of the device can be used as the standard.

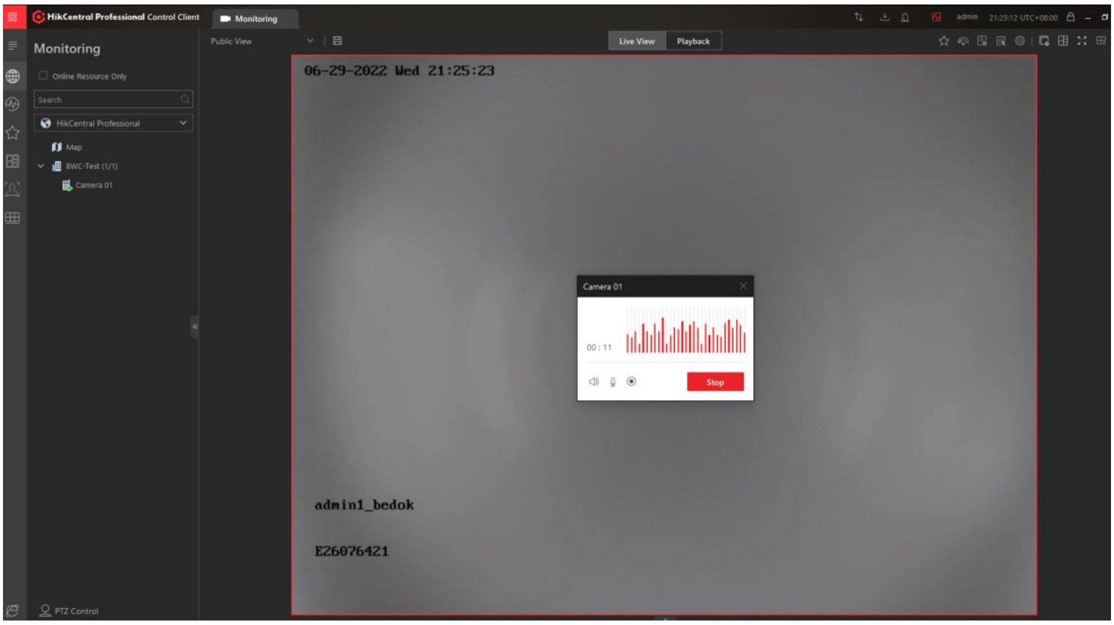




7.2 Body Camera two-way intercom

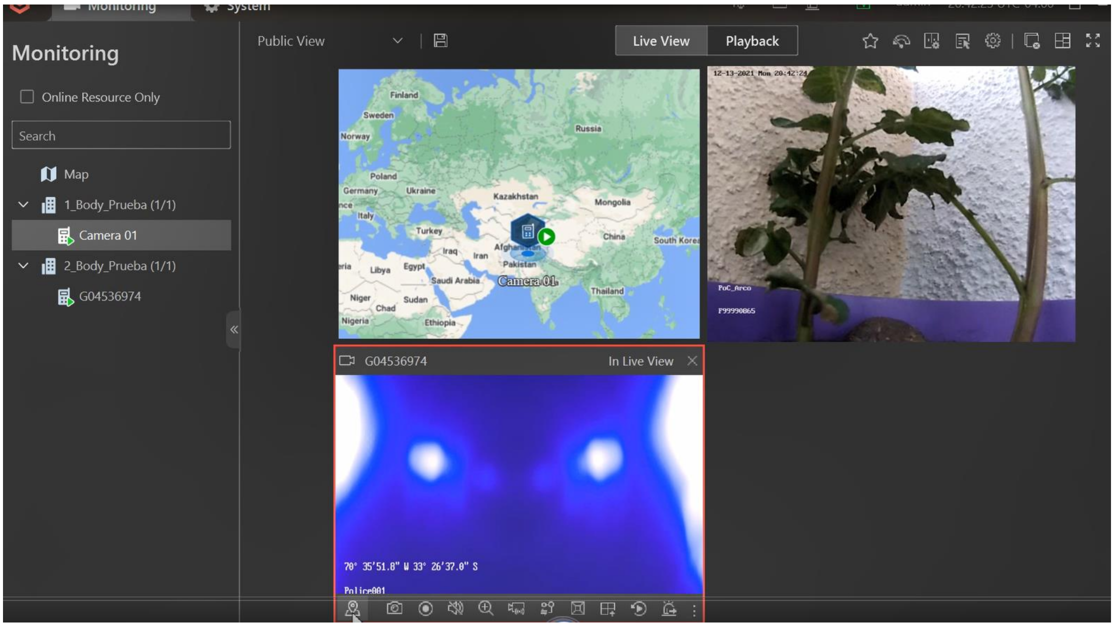
In the preview/playback/alarm interface, click the button below to initiate a two-way intercom to the device, but the device cannot initiate intercom to the platform actively.



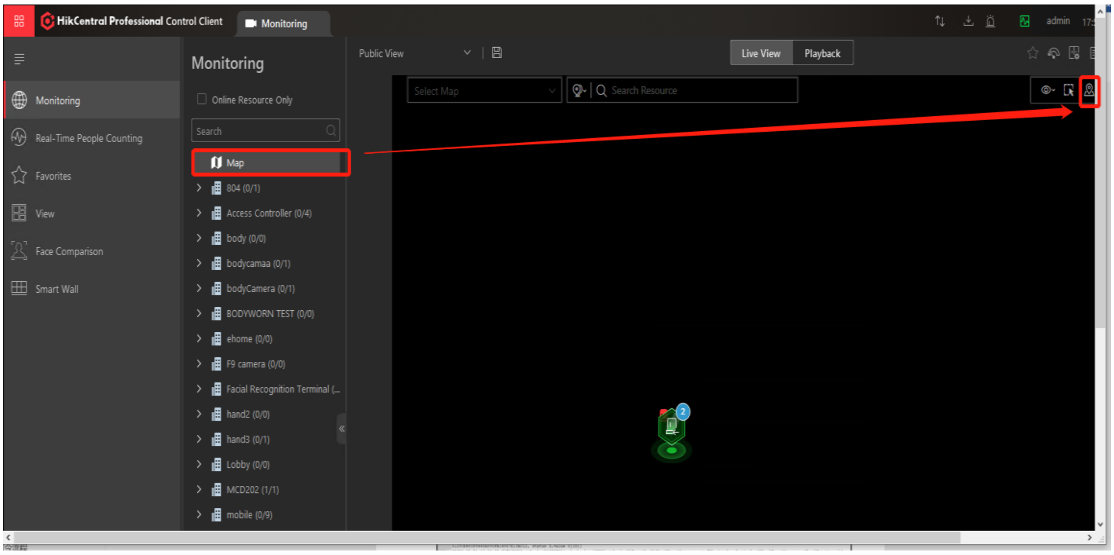


7.3 Body Camera real-time positioning

During the preview process, you can click the map button on the preview interface to locate, the Body Camera will automatically report GPS information, and the location will be automatically updated.

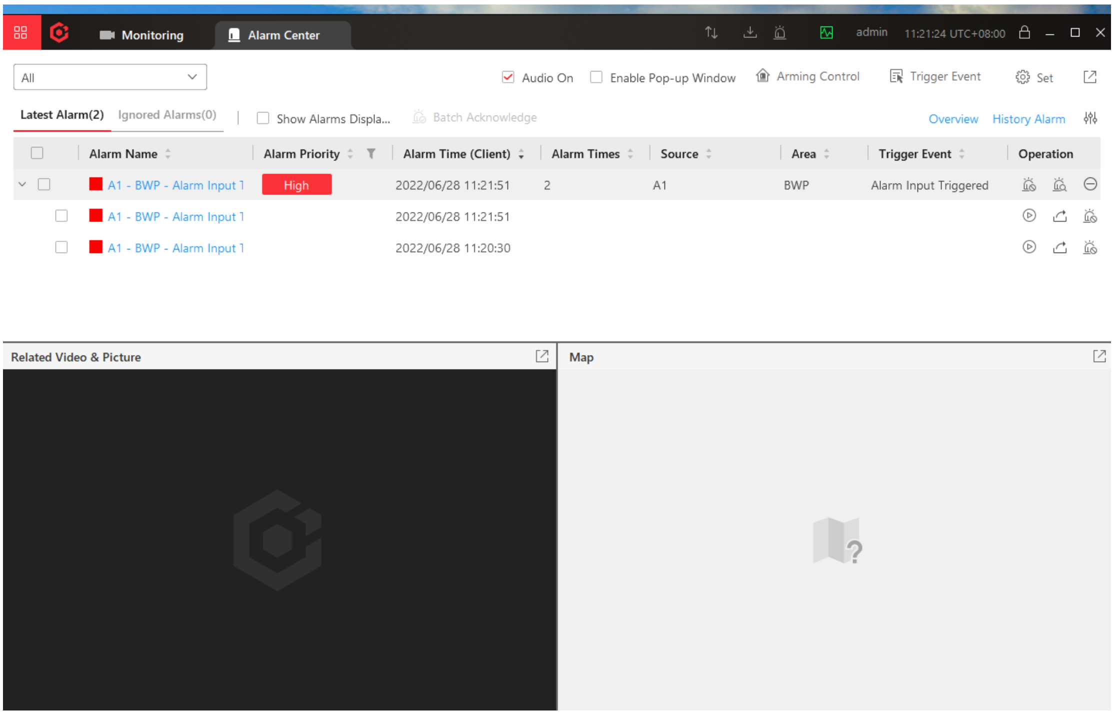


The client can support one-key positioning of multiple Body Cameras, but the WEB side does not support it. The one-key positioning method is shown in the figure.

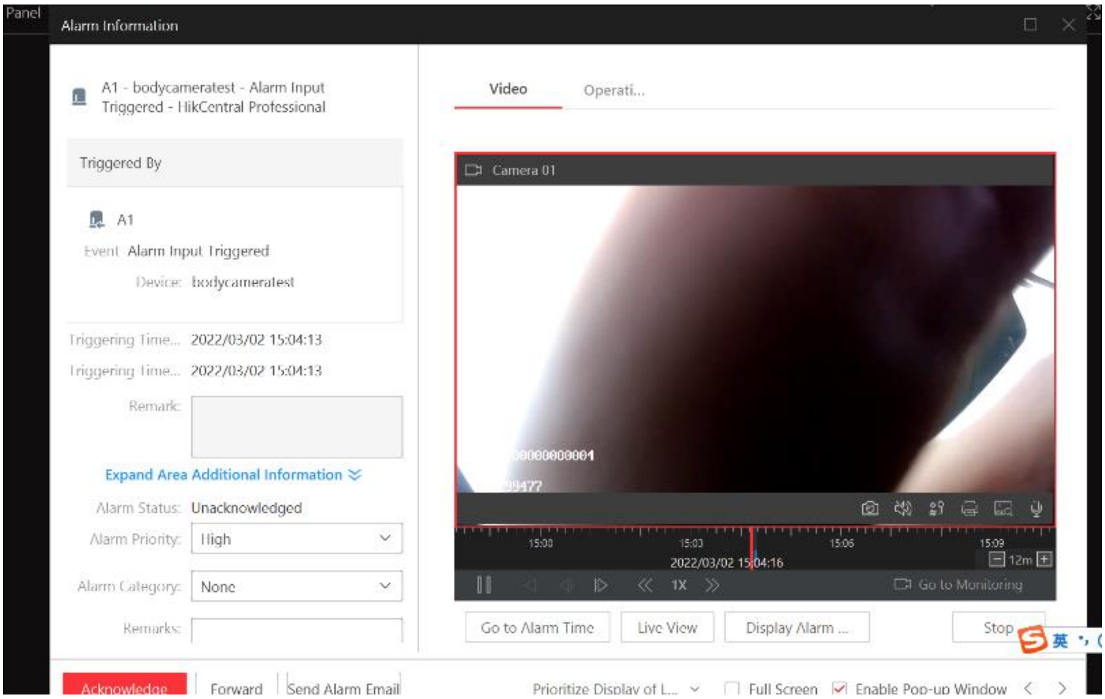


7.4 Body Camera one-key alarm

Press the emergency alarm button of the Body Camera, you can receive the alarm on the client, and view the video of the alarm.



□	Alarm Name	Alarm Priority	Alarm Time (Client)	Alarm Times	Source	Area	Trigger Event	Operation
□	🟥 A1 - BWP - Alarm Input 1	High	2022/06/28 11:21:51	2	A1	BWP	Alarm Input Triggered	
□	🟥 A1 - BWP - Alarm Input 1		2022/06/28 11:21:51					
□	🟥 A1 - BWP - Alarm Input 1		2022/06/28 11:20:30					



A1 - bodycameratest - Alarm Input Triggered - HikCentral Professional

Triggered By

A1

Event: Alarm Input Triggered

Device: bodycameratest

Triggering Time... 2022/03/02 15:04:13

Triggering Time... 2022/03/02 15:04:13

Remark:

Expand Area Additional Information

Alarm Status: Unacknowledged

Alarm Priority: High

Alarm Category: None

Remarks:

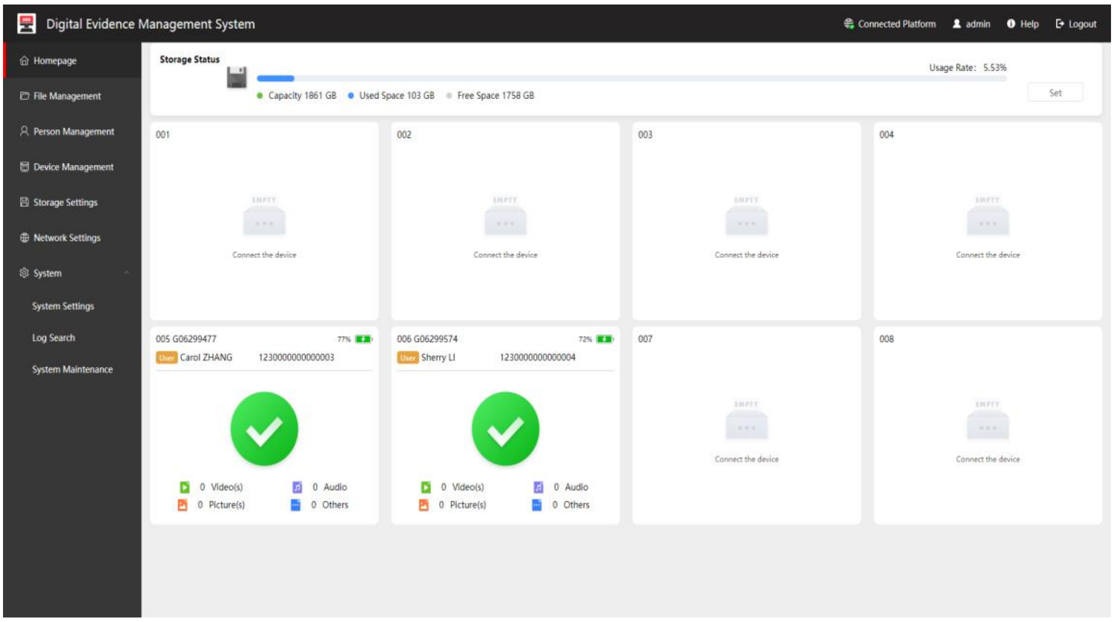
2022/03/02 15:04:16

[Note]: DS-2311C only supports automatic start of recording, but does not support automatic stop, DS-MCW407 can support automatic start and stop of recording.

7.5 Upload the recorded content of the Body Camera to the Dock Station

After the Body Camera is plugged into the Dock Station, you can see the contents of the files recorded by the device in File Management. Click upload to upload the Body

Camera files to the Dock Station.



Storage Status

Usage Rate: 5.53%

Capacity 1861 GB · Used Space 103 GB · Free Space 1758 GB

001 Connect the device

002 Connect the device

003 Connect the device

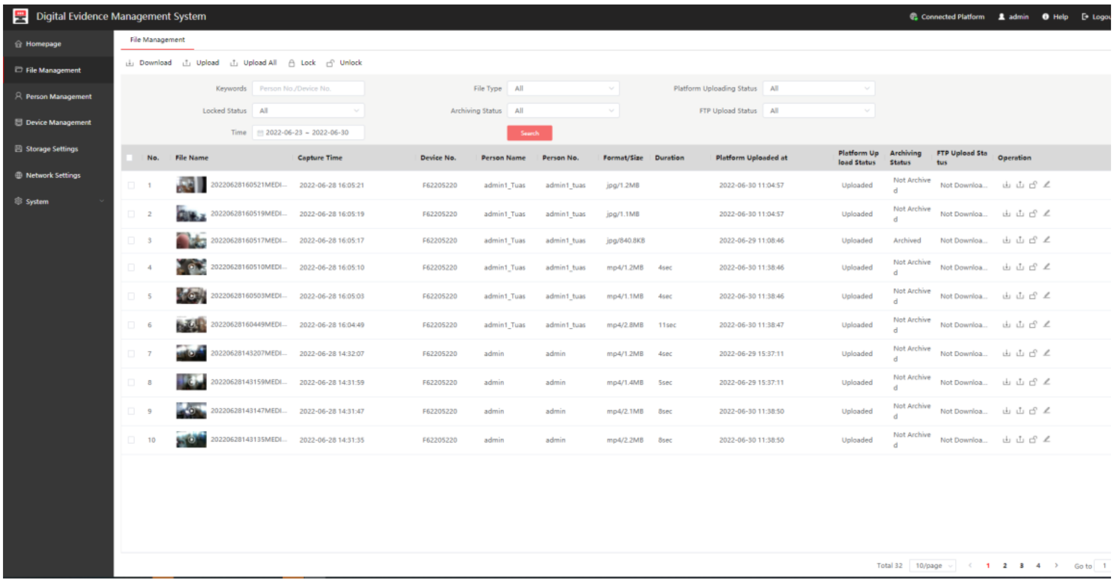
004 Connect the device

005 G06299477 77%
User Carol ZHANG 1230000000000003
0 Video(s) 0 Audio
0 Picture(s) 0 Others

006 G06299574 72%
User Sherry LI 1230000000000004
0 Video(s) 0 Audio
0 Picture(s) 0 Others

007 Connect the device

008 Connect the device



Keywords: Person No./Device No.
File Type: All
Platform Uploading Status: All
Locked Status: All
Archiving Status: All
FTP Upload Status: All
Time: 2022-06-23 ~ 2022-06-30

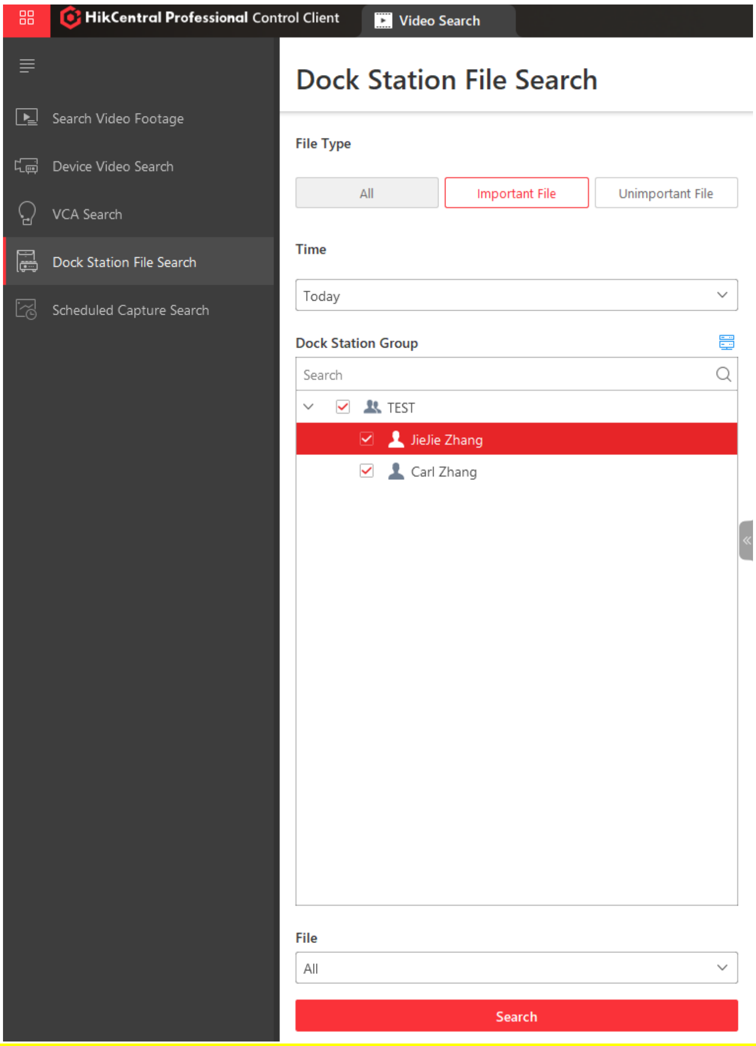
No.	File Name	Capture Time	Device No.	Person Name	Person No.	Format/Size	Duration	Platform Uploaded at	Platform Upload Status	Archiving Status	FTP Upload Status	Operation
1	20220628160521MEDI...	2022-06-28 16:05:21	F62205220	admin1_Tuas	admin1_tuas	jpg/1.2MB		2022-06-30 11:04:57	Uploaded	Not Archived	Not Downloa...	
2	20220628160519MEDI...	2022-06-28 16:05:19	F62205220	admin1_Tuas	admin1_tuas	jpg/1.1MB		2022-06-30 11:04:57	Uploaded	Not Archived	Not Downloa...	
3	20220628160517MEDI...	2022-06-28 16:05:17	F62205220	admin1_Tuas	admin1_tuas	jpg/840.8KB		2022-06-29 11:08:46	Uploaded	Archived	Not Downloa...	
4	20220628160510MEDI...	2022-06-28 16:05:10	F62205220	admin1_Tuas	admin1_tuas	mp4/1.2MB	4sec	2022-06-30 11:38:46	Uploaded	Not Archived	Not Downloa...	
5	20220628160503MEDI...	2022-06-28 16:05:03	F62205220	admin1_Tuas	admin1_tuas	mp4/1.1MB	4sec	2022-06-30 11:38:46	Uploaded	Not Archived	Not Downloa...	
6	20220628160449MEDI...	2022-06-28 16:04:49	F62205220	admin1_Tuas	admin1_tuas	mp4/2.8MB	11sec	2022-06-30 11:38:47	Uploaded	Not Archived	Not Downloa...	
7	20220628143207MEDI...	2022-06-28 14:32:07	F62205220	admin	admin	mp4/1.2MB	4sec	2022-06-29 15:37:11	Uploaded	Not Archived	Not Downloa...	
8	20220628143159MEDI...	2022-06-28 14:31:59	F62205220	admin	admin	mp4/1.4MB	5sec	2022-06-29 15:37:11	Uploaded	Not Archived	Not Downloa...	
9	20220628143147MEDI...	2022-06-28 14:31:47	F62205220	admin	admin	mp4/2.1MB	8sec	2022-06-30 11:38:50	Uploaded	Not Archived	Not Downloa...	
10	20220628143135MEDI...	2022-06-28 14:31:35	F62205220	admin	admin	mp4/2.2MB	8sec	2022-06-30 11:38:50	Uploaded	Not Archived	Not Downloa...	

Total 32 10/page < 1 2 3 4 > Go to 1

7.6 HCP CS Client Viewing Dock Station Storage Content

Enter the client and select **Investigation-Video Search-Dock Station File** Search in turn.

[Note]: When searching here, you need to select the personnel in the corresponding collection station group, and select the time to start the search.



Dock Station File Search

File Type

All | Important File | Unimportant File

Time

Today

Dock Station Group

Search

☑ TEST

☑ JieJie Zhang

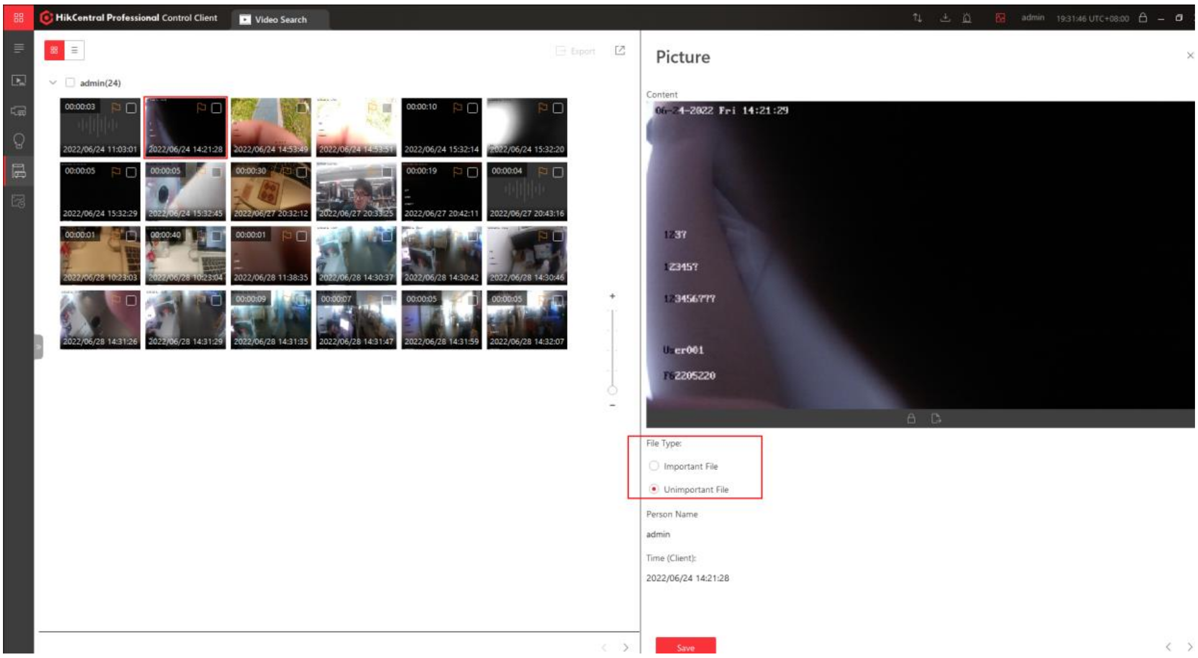
☑ Carl Zhang

File

All

Search

[Note]: HCP 2.3 newly added video can be added as an important file or an unimportant file after the video is retrieved.



Picture

Content

File Type:

○ Important File

● Unimportant File

Person Name

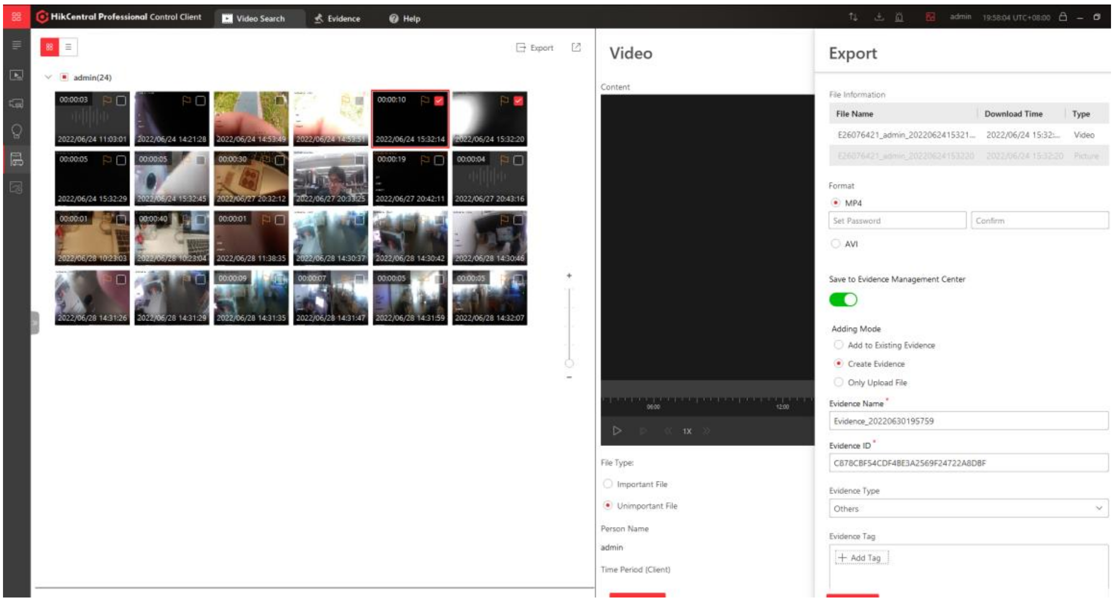
admin

Time (Client):

2022/06/24 14:21:28

Save

Select a file to export it and add it to the evidence center, as shown:



Export

File Information

File Name	Download Time	Type
E26076421_admin_2022062415321...	2022/06/24 15:32:...	Video
E26076421_admin_20220624153220	2022/06/24 15:32:20	Picture

Format
● MP4
Set Password | Confirm
○ AVI

Save to Evidence Management Center: On

Adding Mode
○ Add to Existing Evidence
● Create Evidence
○ Only Upload File

Evidence Name *: Evidence_20220630195759

Evidence ID *: C878CBF54CDF4BE3A2569F24722A8DBF

Evidence Type: Others

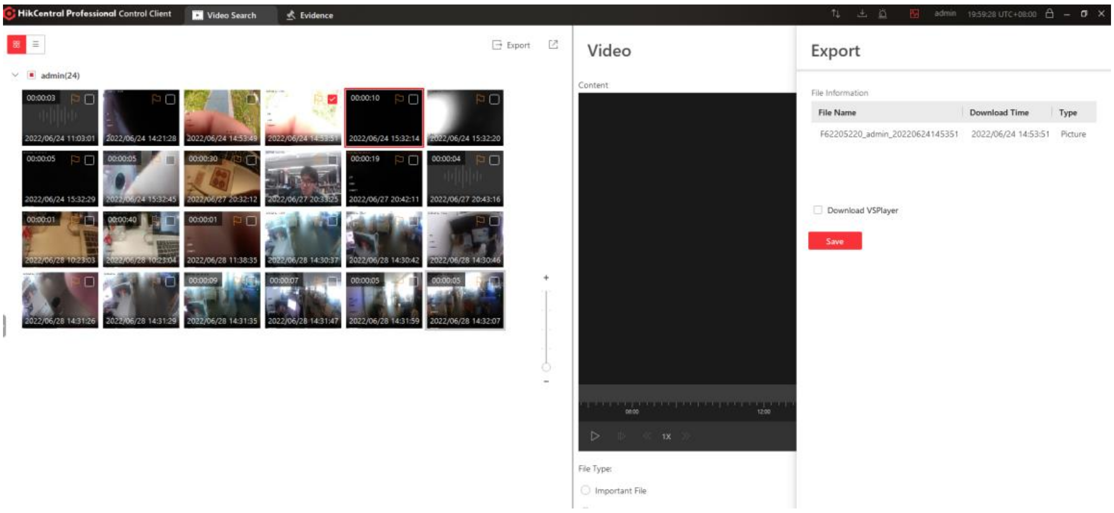
Evidence Tag: + Add Tag

File Type:
○ Important File
● Unimportant File

Person Name: admin

Time Period (Client)

[Note]: Pictures and audios do not support saving as evidence. If pictures and audios are selected, the option to add to the evidence center will not appear at this time.



Export

File Information

File Name	Download Time	Type
F62205220_admin_20220624145351	2022/06/24 14:53:51	Picture

□ Download VSPlayer

Save

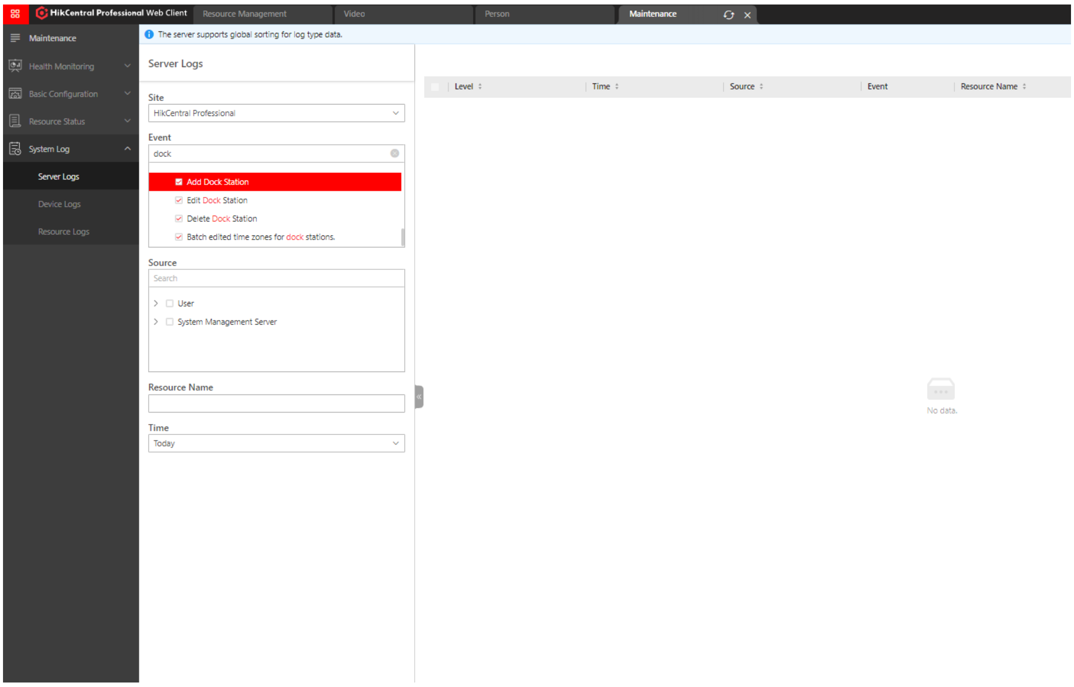
File Type:
○ Important File

8 Body Camera & Dock Station Service Maintenance

8.1 Check operation log

Operation log description: The operation log records a business operation performed by the platform user, and retains information such as the operator, operation target, and operation result.

Enter the WEB side of HCP 2.3, click **Maintenance-System Log-Search Dock Station** in the Event interface.



The server supports global sorting for log type data.

Server Logs

Site: HikCentral Professional

Event: dock

- ☑ Add Dock Station
- ☑ Edit Dock Station
- ☑ Delete Dock Station
- ☑ Batch edited time zones for dock stations.

Source: Search

- ☐ User
- ☐ System Management Server

Resource Name:

Time: Today

8.2 Log Location

Video Plugin Log

DAM Plugin Related

\HikCentral\VSM Servers\Log\SYS\DeviceCommunication\DockStation.log

\HikCentral\VSM Servers\Log\SYS\DeviceCommunication\EhomeSDKCommunication.log

\HikCentral\VSM Servers\Log\SYS\DeviceCommunication\DeviceCommunication.log

\HikCentral\VSM Servers\Log\SYS\deviceaccess.d\deviceevent.log

Video Related

\HikCentral\VSM Servers\Log\SYS\basevideo.s\dockstationgroup.log

\HikCentral\VSM Servers\Log\SYS\basevideo.s\gis.log

Log Configuration File

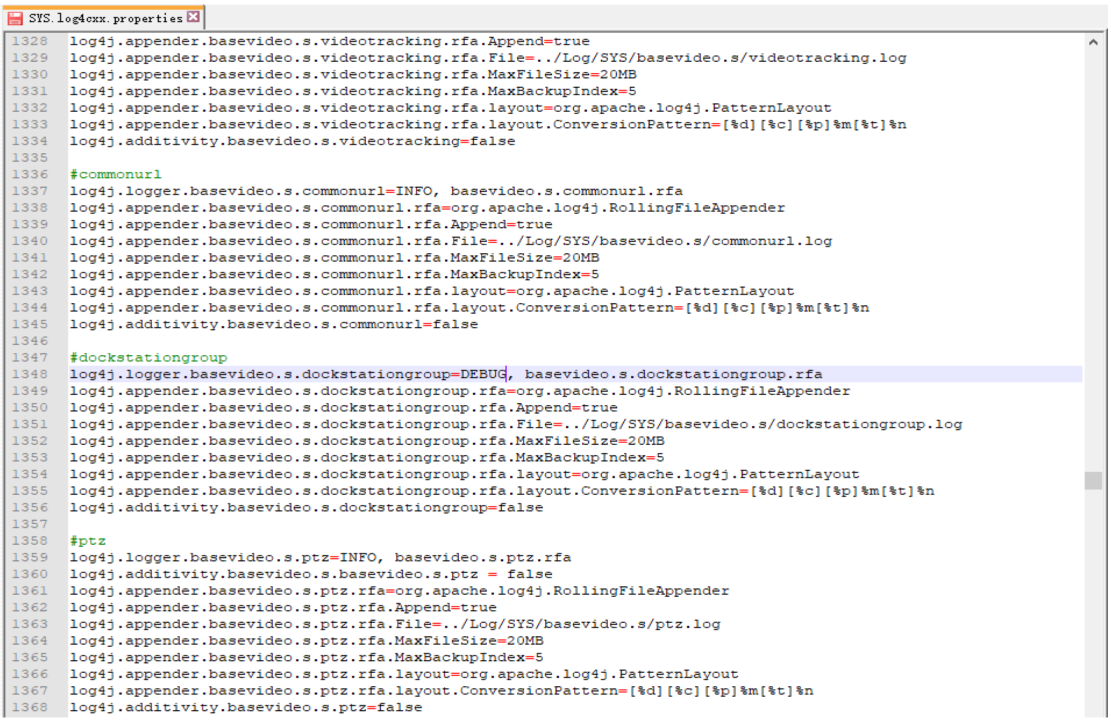
\HikCentral\VSM Servers\SYS\META_INFO\SYS\runtime_script\SYS.log4cxx.properties

Adjust log level

The default log level during product installation is INFO level. To facilitate analysis and locating problems, the log level can be lowered to DEBUG level.

Log configuration file location

HikCentral\VSM Servers\SYS\META_INFO\SYS\runtime_script\SYS.log4cxx.properties



SYS.log4cxx.properties

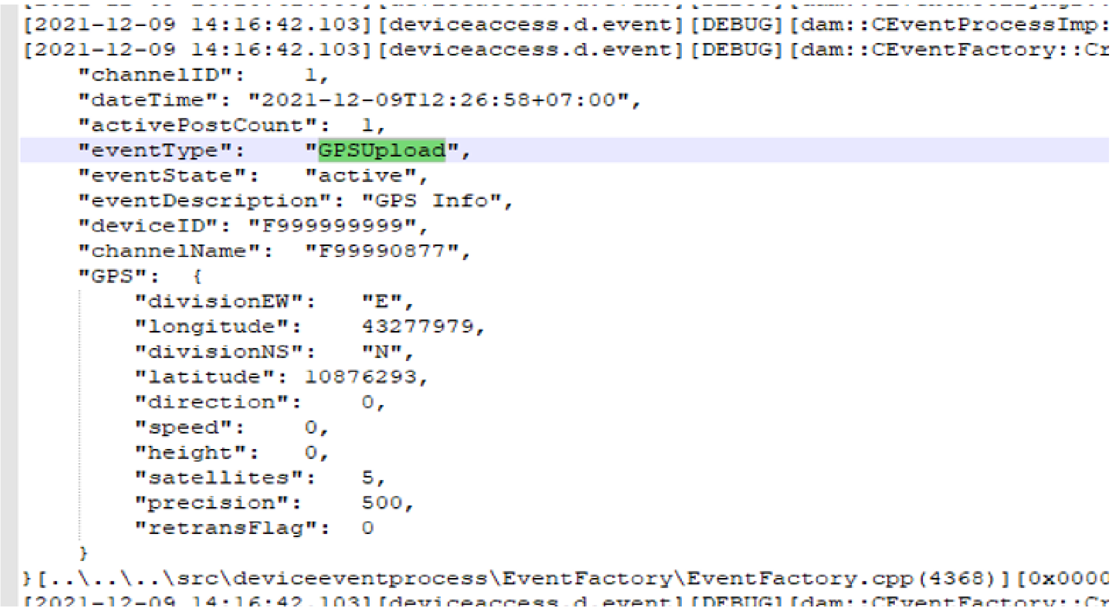
```
log4j.appender.basevideo.s.videotracking.rfa.Append=true
log4j.appender.basevideo.s.videotracking.rfa.File=../Log/SYS/basevideo.s/videotracking.log
log4j.appender.basevideo.s.videotracking.rfa.MaxFileSize=20MB
log4j.appender.basevideo.s.videotracking.rfa.MaxBackupIndex=5
log4j.appender.basevideo.s.videotracking.rfa.layout=org.apache.log4j.PatternLayout
log4j.appender.basevideo.s.videotracking.rfa.layout.ConversionPattern=[%d][%c][%p]%m[%t]%n
log4j.additivity.basevideo.s.videotracking=false

#commonurl
log4j.logger.basevideo.s.commonurl=INFO, basevideo.s.commonurl.rfa
log4j.appender.basevideo.s.commonurl.rfa=org.apache.log4j.RollingFileAppender
log4j.appender.basevideo.s.commonurl.rfa.Append=true
log4j.appender.basevideo.s.commonurl.rfa.File=../Log/SYS/basevideo.s/commonurl.log
log4j.appender.basevideo.s.commonurl.rfa.MaxFileSize=20MB
log4j.appender.basevideo.s.commonurl.rfa.MaxBackupIndex=5
log4j.appender.basevideo.s.commonurl.rfa.layout=org.apache.log4j.PatternLayout
log4j.appender.basevideo.s.commonurl.rfa.layout.ConversionPattern=[%d][%c][%p]%m[%t]%n
log4j.additivity.basevideo.s.commonurl=false

#dockstationgroup
log4j.logger.basevideo.s.dockstationgroup=DEBUG, basevideo.s.dockstationgroup.rfa
log4j.appender.basevideo.s.dockstationgroup.rfa=org.apache.log4j.RollingFileAppender
log4j.appender.basevideo.s.dockstationgroup.rfa.Append=true
log4j.appender.basevideo.s.dockstationgroup.rfa.File=../Log/SYS/basevideo.s/dockstationgroup.log
log4j.appender.basevideo.s.dockstationgroup.rfa.MaxFileSize=20MB
log4j.appender.basevideo.s.dockstationgroup.rfa.MaxBackupIndex=5
log4j.appender.basevideo.s.dockstationgroup.rfa.layout=org.apache.log4j.PatternLayout
log4j.appender.basevideo.s.dockstationgroup.rfa.layout.ConversionPattern=[%d][%c][%p]%m[%t]%n
log4j.additivity.basevideo.s.dockstationgroup=false

#ptz
log4j.logger.basevideo.s.ptz=INFO, basevideo.s.ptz.rfa
log4j.additivity.basevideo.s.basevideo.s.ptz = false
log4j.appender.basevideo.s.ptz.rfa=org.apache.log4j.RollingFileAppender
log4j.appender.basevideo.s.ptz.rfa.Append=true
log4j.appender.basevideo.s.ptz.rfa.File=../Log/SYS/basevideo.s/ptz.log
log4j.appender.basevideo.s.ptz.rfa.MaxFileSize=20MB
log4j.appender.basevideo.s.ptz.rfa.MaxBackupIndex=5
log4j.appender.basevideo.s.ptz.rfa.layout=org.apache.log4j.PatternLayout
log4j.appender.basevideo.s.ptz.rfa.layout.ConversionPattern=[%d][%c][%p]%m[%t]%n
log4j.additivity.basevideo.s.ptz=false
```

9 FAQ

9.1 The device reports GPS information, but the client cannot receive GPS push messages

Investigation ideas:

- ✓ Make sure the GPS on the Body Camera is turned on
- ✓ Modify the log level of deviceevent.log to DEBUG. After the event is triggered, search for GPSUpload in the log. If there are the following related messages, it means that the device has GPS reporting;



```
[2021-12-09 14:16:42.103][deviceaccess.d.event][DEBUG][dam::CEventProcessImp:
[2021-12-09 14:16:42.103][deviceaccess.d.event][DEBUG][dam::CEventFactory::Cr
    "channelID":    1,
    "dateTime": "2021-12-09T12:26:58+07:00",
    "activePostCount":  1,
    "eventType":    "GPSUpload",
    "eventState":   "active",
    "eventDescription": "GPS Info",
    "deviceID": "F999999999",
    "channelName":  "F99990877",
    "GPS":  {
        "divisionEW":   "E",
        "longitude":    43277979,
        "divisionNS":   "N",
        "latitude": 10876293,
        "direction":    0,
        "speed":    0,
        "height":   0,
        "satellites":   5,
        "precision":    500,
        "retransFlag":  0
    }
}[..\..\..\src\deviceeventprocess\EventFactory\EventFactory.cpp(4368)][0x0000
[2021-12-09 14:16:42.103][deviceaccess.d.event][DEBUG][dam::CEventFactory::Cr
```

9.2 Dock station return configuration related

✓ **Storage server types supported by the dock station:**

pStor: need to select picture and video pool.

CVR: file pool required.

✓ Add pStor storage, select the collection station to return the storage type to pStor, but cannot see pStor.

Check whether pStor has enabled image storage. You need to enable image storage to select.

✓ Add pStor storage, select the collection station to return the storage type to pStor, but cannot see pStor.

Check whether pStor has enabled image storage. You need to enable image storage to select

✓ Add pStor storage, select the collection station to return the storage type to pStor, but cannot see pStor.

Check whether the CVR has a file pool, only the file pool can be selected.

9.3 Issues related to dock station personnel

- If there is a group that fails to be delivered, an exception will be displayed in the dock station group list. Click the dock station group exception button to retry the delivery or view the error details. The error details include which dock stations have errors and the reasons for the errors.

Error Code:

1) The dock station is offline (**Error Code: 9905**)

Solution: Retry and deliver after the dock station goes online.

2) The dock station device does not exist (**Error Code: 903**)

Solution: The dock station device may have been deleted from the platform

3) There is a failure to deliver by personnel (**Error Code: 70005**)

Solution: If 70005 appears, you can check the detailed personnel-level delivery error to determine the cause.

- Click on the group with exception, and the Apply All option on the upper column of the personnel list indicates the exception. Click the exception button to retry the delivery or view the error details. The error details include which dock stations were delivered by the abnormal person and the cause of the error.

Person-level error code

1) Failed to model the avatars of the staff in the dock station group (**Error Code: 70003**)

Solution: replace clear avatar.

2) Failed to deliver the avatar of the dock station group (**Error Code: 70004**)

Solution: Failed to deliver the avatar, it is not the specific error reason, you need to contact the device to check the specific reason

3) Failed to deliver by the staff of the dock station group (**Error Code: 70008**)

Solution: Personnel failed to deliver, not specific error reasons, need to be researched and developed

4) The password of the dock station group is invalid (**Error Code: 70009**)

Solution: The personnel password is invalid, because the simple password device sends a complex password to the personnel or the complex password device sends a simple password to the personnel, and the personnel password needs to be modified to meet the requirements of the device