

## H5S Video Platform

# User manual

Document version 18

Release date 2024/10/23

## Disclaimers

The products, services, or features you purchase are subject to the commercial contracts and terms of linkingvision. All or part of the products, services, or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Zero Vision makes no express or implied representations or warranties regarding the content of this document.

Due to product version upgrades or other reasons, the content of this document may be updated from time to time. Unless otherwise agreed, this document is only intended as a guide for use. All statements, information, and recommendations in this document do not constitute any express or implied warranty.

## Trademark Declaration

h5stream and other linkingvision trademarks are trademarks of linkingvision (shanghai) Co.,Ltd.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

**Copyright ©linkingvision (shanghai) Co.,Ltd. All rights reserved.**

Without the written permission of the company, no unit or individual may extract or copy part or all of the contents of this document without authorization, and shall not transmit it in any form Broadcast.

linkingvision (shanghai) Co.,Ltd.

Website: [www.linkingvision.cn](http://www.linkingvision.cn)

Telephone: 021-52216167

Mailbox: [info@linkingvision.com](mailto:info@linkingvision.com)

# Index

<b>1 Preface</b>	<b>7</b>
<b>2 Version update</b>	<b>9</b>
1 Version update description .....	10
<b>3 Content Overview</b>	<b>11</b>
1 Live playback on the intranet .....	13
Video source support .....	13
Operating platform support .....	13
Support for Domestic CPU .....	14
Live streaming protocol support .....	14
Video encryption support .....	14
2 Cloud live playback .....	14
<b>4 Software installation</b>	<b>17</b>
1 Windows installation .....	18
2 Linux Install .....	20
3 Linux performance improvement configuration .....	21
4 Open the management interface .....	23
5 Install License .....	25
6 Port .....	26
7 Menu .....	27
<b>5 Device configuration</b>	<b>29</b>
1 Video source configuration .....	31
RTSP/RTMP video source configuration .....	31
ONVIF video source configuration .....	32
File video source configuration .....	34
2 Device SDK configuration .....	34
Hikvision SDK configuration .....	36
Dahua SDK configuration .....	38
Huawei IVS configuration .....	40
ONVIFSTG configuration .....	42
Tiandy SDK configuration .....	43
UNVSDK configuration .....	44
Hikvision CVR configuration .....	46
3 Platform access configuration .....	47
Hikvision ISC configuration .....	47
Dahua ICC configuration .....	51
Dahua DSS configuration .....	53
4 Device Search .....	54

---

5	RTMP Streaming Configuration .....	54
6	Video single protocol access .....	55
7	Embedded page mode .....	56
8	Customize the window pane .....	58
9	Device import .....	59
10	Configuration of monitoring points .....	59
<b>6</b>	<b>Real-time video</b>	<b>63</b>
1	Real-time video operation .....	64
2	RTC WS playback mode .....	65
3	View operations .....	68
4	View Layout .....	69
5	Pan tilt control .....	70
6	Video patrol .....	71
7	Voice intercom .....	72
8	Scan and play .....	73
<b>7</b>	<b>Playback video</b>	<b>75</b>
1	Advanced replay .....	77
2	File .....	78
3	Playback .....	80
4	Screenshot .....	81
5	Thumbnail .....	81
6	Task .....	82
<b>8</b>	<b>Emap</b>	<b>85</b>
1	Map configuration .....	86
2	Map operation .....	86
<b>9</b>	<b>Region management</b>	<b>89</b>
1	Add and delete regions .....	90
2	Regional resource allocation .....	90
<b>10</b>	<b>User management</b>	<b>93</b>
1	Role management .....	94
2	User management .....	95
3	Security management .....	96
4	Play Code .....	97
<b>11</b>	<b>Cloud cascading</b>	<b>99</b>
1	Cascade configuration .....	100



<b>12 Video AI management</b>	<b>103</b>
1 Video quality detection .....	104
2 Object detection .....	105
3 Advanced target detection .....	106
<b>13 WEBRTC</b>	<b>109</b>
1 Cloud mode .....	110
2 Forwarding mode .....	111
<b>14 Standard protocol</b>	<b>115</b>
1 RTSP/RTMP/FLV real-time forwarding .....	116
2 HLS real-time forwarding .....	118
3 RTMP push stream forwarding .....	119
<b>15 System configuration</b>	<b>121</b>
1 Network configuration .....	122
RTSP protocol .....	122
HTTP protocol .....	122
HTTPS certificate configuration .....	124
MQTT Server .....	125
2 Video recording management .....	128
3 Transcoding management .....	130
Default transcoding configuration .....	132
Customize transcoding configuration .....	134
GPU mode selection .....	136
NVIDIA GPU Mode .....	138
System GPU mode .....	142
TAV1 GPU mode .....	143
4 Video configuration .....	143
5 System restart .....	144
6 Automatic maintenance .....	144
7 Restore default configuration .....	144
8 Log configuration .....	144
9 Configure snapshots .....	144
10 License import .....	145
11 Production environment configuration .....	146
12 Product customization .....	146
<b>16 Reverse proxy</b>	<b>149</b>
1 Basic proxy .....	152
2 load balancing .....	154
3 Specify proxy .....	156

---

<b>17 Reinforcement Guidelines</b>	<b>161</b>
1 User management .....	162
<b>18 Appendix A FAQ</b>	<b>165</b>
	<b>0</b>

# 1.Preface

---

---

# 1 Preface

## Preface

Thank you very much for using our company's products. We will be happy to provide you with the best and highest quality service.

This manual may contain technical inaccuracies or text errors.

The content of this manual will be updated regularly without notice; the updated content will be added to the new version of this manual.

The interface images extracted from this manual are only used as examples. The interface may vary between versions, so please refer to the actual interface for accuracy.

We have a professional support team to answer your questions. Thank you for your support.

## 2.Version update

---

---

## 2 Version update

### 2.1 Version update description

#### Version update description

Version	Date	Describe
r13	2020/01/15	Update the main interface
r14	2022/03/07	r14Version update
r16	2023/03/06	r16Version update

## 3.Content Overview

---

### 3 Content Overview

#### Content Overview

In recent years, the Internet has developed rapidly, especially the mobile Internet. Various mobile APPs are developed based on HTML5 and FLASH technology. Due to various problems, browsers have begun to stop supporting it. However, traditional security manufacturers still use ActiveX to play videos. ActiveX currently only supports IE, so how to support non-FLASH video playback without plug-ins on various browsers and APPs has become very important.

The methods for playing videos natively in browsers vary. A basic requirement for security live streaming is low latency, which requires delay control within 1 second or 500 milliseconds. This poses a great challenge to HTML5 video live streaming technology.

With the popularity of cloud technology, remote video playback and sharing are also very important.

The H5S video platform solves the problems of HTML5 native video and cloud video live streaming. The H5S video platform supports WEBRTC, WEBSOCKET, and RTMP playback technologies. The following table lists the technologies supported by various browsers.

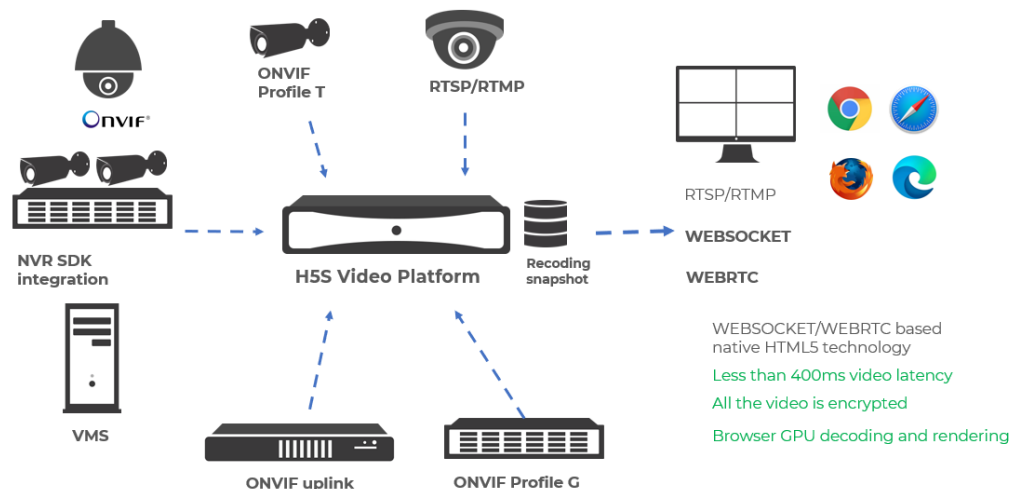
*Default support H264	Chrome	Firefox	IE11	Edge	Safari
WIN7	RTC WS(H265)	RTC WS	RTMP	RTC WS(H265)	-
WIN 8/10/11	RTC WS(H265)	RTC WS	RTMP WS	RTC WS(H265)	-
macOS	RTC WS	RTC WS	-	RTC WS	RTC WS RTC(H.265) WS(H.265)
iOS 13+ (Phone)	RTC RTC(H.265)	RTC RTC(H.265)	-	RTC RTC(H.265)	RTC RTC(H.265)
iOS 13+ (Pad)	RTC WS RTC(H.265) WS(H.265)	RTC WS RTC(H.265) WS(H.265)	-	RTC WS RTC(H.265) WS(H.265)	RTC WS RTC(H.265) WS(H.265)
Android	RTC WS	RTC WS	-	RTC WS	-



### 3.1 Live playback on the intranet

#### Live broadcast playback on the intranet

H5S video platform is a video management platform that supports Windows Linux (CentOS ubuntu). It integrates multiple brands and formats of videos, and converts multiple formats of video data into unified video data through a video application engine. It does not require installing multiple video plugins on the platform, and can smoothly play multiple brands and formats of videos on the platform interface, improving the convenience, ease of use, and scalability of integrated videos, as well as the simplicity of the platform. At the same time, it can set up streaming media information for a certain period of time for storage, and can also import videos for a certain period of time for playback.



#### 3.1.1 Video source support

##### Video source support

H5S video platform supports MP4/AVI files as video sources, which brings great convenience to user testing. Currently, video surveillance cameras support RTSP, and RTMP still has a certain market share. H5STREAM supports RTSP/RTMP very well. As the standard ONVIF for video surveillance, H5S video platform also supports it and allows users to control ONVIF PTZ through RESTFUL interface. It supports Hikvision NVR SDK/Dahua NVR SDK/Tiandi Weiye SDK/Huawei IVS access, supports GB downlink and uplink, and supports Hikvision ISC and Dahua DSS platform video access.

#### 3.1.2 Operating platform support

##### Operating platform support

H5S video platform is a cross-platform video platform. It supports multiple operating systems, including Windows 7/8/10, Windows Server, CentOS,

---

Ubuntu, and can run on cloud platforms such as Alibaba Cloud and Huawei Cloud.

### 3.1.3 **Support for Domestic CPU**

#### **Support for Domestic CPU**

In addition to supporting x64 series CPUs, the H5S video platform also supports ARM v8 architecture CPUs including Kunpeng 920 and Feiteng, and is compatible with Loongson 3 series CPUs.

### 3.1.4 **Live streaming protocol support**

#### **Live streaming protocol support**

RTMP/RTSP is a relatively traditional streaming media protocol, which is well supported in the H5S video platform. The emerging WEBSOCKET and WEBRTC are also well supported in the H5S video platform, allowing for high-performance decoding and ultra-low latency. At the same time, the H5S video platform supports playback support for protocols such as RTMP/RTSP/WEBRTC.

### 3.1.5 **Video encryption support**

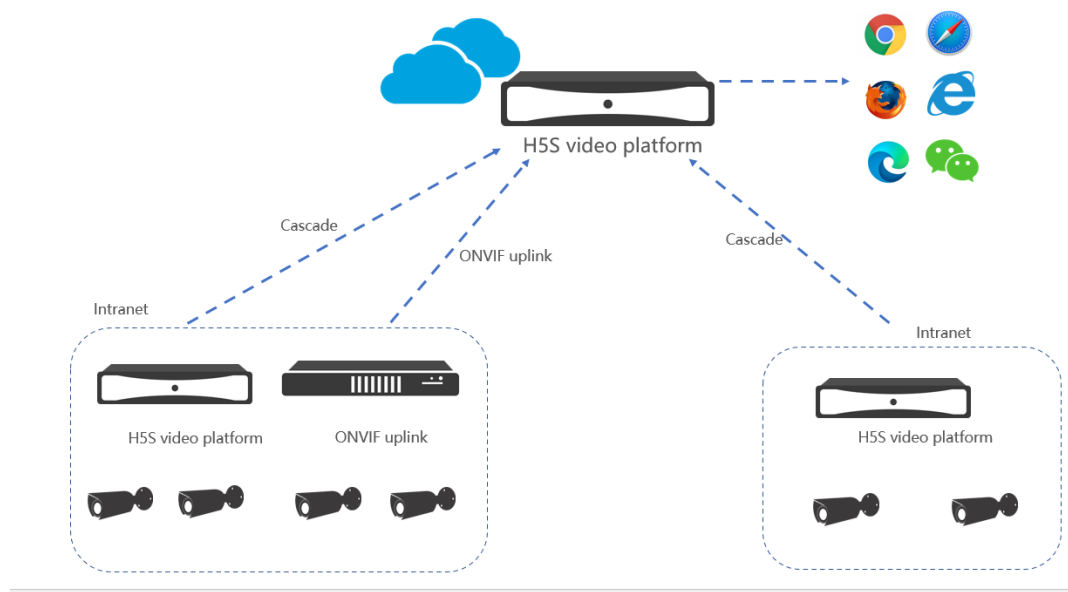
#### **Video encryption support**

The H5S video platform supports playing videos without plug-ins on the browser, and all video data can be encrypted using asymmetric encryption, fully ensuring the security of video data.

## 3.2 **Cloud live playback**

### **Cloud live playback**

If users need to remotely access live video, using traditional NAT port mapping or DDNS is both cumbersome and insecure. The video platform supports cloud streaming mode and all streams are encrypted, ensuring communication security.





## 4. Software installation

---

---

## 4 Software installation

### Software installation preparation

Windows 7/8/10, Windows Server 2008/2012/2016, Centos 7, RockyLinux 8, Ubuntu16.04/18.04 and other 64-bit operating systems, 4G memory, 1 core CPU and above. It can also run on the Linux system of Kunpeng 920 Feiteng Loongson. The version corresponds to the following.

CPU	operating system	Version name
x64	Windows 7/8/10, Windows Server 2008/2012/2016/2019	h5s-*-win64-release.zip h5s-*-win64-release.exe (Installation package)
x64	CentOS 7/RockyLinux 8/Ubuntu16.04/18.04/20.04 Debian 9/10/11 (Centos 8 Not recommended)	h5s-*-linux-x86_64-64bit.tar.gz
Kunpeng 920 Flying RK3399(ARMv8)	Linux	h5s-*-linux-armv8-64bit.tar.gz
Longxin No.3	Linux	h5s-*-linux-loongson-64bit.tar.gz

### Download the installation package

Download the corresponding installation package from the following link  
<https://linkingvision.com/download/h5stream/>

## 4.1 Windows installation

### Install Windows Run Support Package

Please download all the runtime support libraries from the following link:

<https://linkingvision.com/download/h5stream/win/VisualC%2B%2BRedistributable/>

Please install in order, 2008, 2010, 2013, 2015-2019. If there is an installation failure, please update the operating system in the System and Security check update in the Control Panel.

If Windows 2012 still cannot solve the problem, please refer to the following link or update the operating system at the operating system update section.

[https://answers.microsoft.com/en-us/windows/forum/windows8\\_1-windows\\_install/api-ms-win-crt-string-1-1-0dll-and-others-missing/85a91890-ed8a-4e6e-8f94-b53639c39970?auth=1](https://answers.microsoft.com/en-us/windows/forum/windows8_1-windows_install/api-ms-win-crt-string-1-1-0dll-and-others-missing/85a91890-ed8a-4e6e-8f94-b53639c39970?auth=1)

## Run manually

Unzip the product package and run h5ss.bat. If you install it using a Windows installation package, the service will automatically start. If you manually run it again, you need to stop the service. It is recommended to stop the service before manually running it.

certificate	3/14/2018 8:03 PM	File folder	
conf	3/23/2018 11:32 P...	File folder	
logs	3/23/2018 11:32 P...	File folder	
ssl	3/14/2018 8:03 PM	File folder	
www	3/17/2018 9:08 PM	File folder	
avcodec-57.dll	2/5/2018 8:39 PM	Application extens...	7,255 KB
avdevice-57.dll	2/5/2018 8:35 PM	Application extens...	152 KB
avfilter-6.dll	2/5/2018 8:35 PM	Application extens...	2,819 KB
avformat-57.dll	2/5/2018 8:39 PM	Application extens...	2,578 KB
avresample-3.dll	2/5/2018 8:35 PM	Application extens...	217 KB
avutil-55.dll	2/5/2018 8:39 PM	Application extens...	561 KB
cmnlib.dll	3/14/2018 7:35 PM	Application extens...	1,587 KB
gencertificate.bat	2/5/2018 7:07 PM	Windows Batch File	1 KB
h5ss.bat	2/5/2018 7:07 PM	Windows Batch File	1 KB
h5ss.exe	3/14/2018 7:35 PM	Application	1,334 KB
libeay32.dll	2/5/2018 8:29 PM	Application extens...	2,044 KB
libprotobuf.dll	2/5/2018 10:40 PM	Application extens...	2,364 KB
live555.dll	2/5/2018 8:27 PM	Application extens...	237 KB
nssm.exe	2/5/2018 8:03 PM	Application	324 KB
openssl.cnf	2/5/2018 7:07 PM	CNF File	11 KB
PocoFoundation64.dll	2/5/2018 10:37 PM	Application extens...	1,524 KB
PocoJSON64.dll	2/5/2018 10:37 PM	Application extens...	241 KB
PocoNet64.dll	2/5/2018 10:37 PM	Application extens...	979 KB
PocoUtil64.dll	2/5/2018 10:37 PM	Application extens...	417 KB
PocoXML64.dll	2/5/2018 10:18 PM	Application extens...	574 KB
regservice.bat	2/5/2018 8:03 PM	Windows Batch File	1 KB
ssleay32.dll	2/5/2018 8:27 PM	Application extens...	345 KB
swresample-2.dll	2/5/2018 8:39 PM	Application extens...	181 KB
swscale-4.dll	2/5/2018 8:35 PM	Application extens...	698 KB
unregservice.bat	2/5/2018 8:03 PM	Windows Batch File	1 KB

## Install as a service to run

You can directly run regservice.bat to install the service or run unregservice.bat to cancel the installation of the service. You need to use an administrator to open the cmd command line to run the script.

\*You can start and stop services in the service management tool.

---

## Control Panel\All Control Panel Items\Administrative Tools

The service name of the H5S video platform is H5Stream

## 4.2 Linux Install

### Decompress install package

Linux release package has soft link, user only can decompress on Linux, don't support decompress on Windows and then copy to Linux.

### Manual running

cd to root directory of h5s, and then start below command to start h5s process:

```
#./h5ss.sh
```

If you want to stop h5s, you can use kill command. First use ps command to find the PID:

```
#ps -ef | grep h5ss
```

Then kill the PID, The PID is ps command's output PID:

```
#kill -9 PID
```

### Run as system service

Copy release package to /opt/h5ss, this path can't be changed, because the service scripts use absolute path, reference as below:

```
/opt/h5ss/  
|-- certificate  
|-- conf  
|-- gencertificate.sh  
|-- h5ss  
|-- h5ss.service  
|-- h5ss.service.sh  
|-- h5ss.sh  
|-- lib  
|-- logs  
|-- openssl  
|-- openssl.cnf  
|-- www
```

### Centos 7/8

```
#cp h5ss.service /usr/lib/systemd/system/
```

```
#systemctl enable h5ss.service
```

```
#systemctl start h5ss.service
```

If you want to upgrade h5ss, you need stop service and use "systemctl disable h5ss.service" to disable service, and then repeat about 3 command.

### Ubuntu 18.04/20.04/22.04

```
#sudo mkdir -p /usr/lib/systemd/system/
```



```
#sudo apt install systemd
#sudo cp h5ss.service /usr/lib/systemd/system/
#sudo systemctl enable h5ss.service
#sudo systemctl start h5ss.service
```

Stop service command: `systemctl stop h5ss.service`

## 4.3 Linux performance improvement configuration

### Linux performance improvement configuration

The default parameter configuration of Linux distributions is not very good for supporting high-capacity systems, so it is necessary to modify the parameters to improve performance.

```
#sudo vi /etc/security/limits.conf
```

Add the following lines at the end of the file

```
root soft nofile 655350
root hard nofile 655350
* soft nofile 655350
* hard nofile 655350
* soft nproc 655350
* hard nproc 655350

##
##
#@student      soft  core           0
#@student      hard  rss            10000
#@faculty      soft  nproc          20
#@faculty      hard  nproc          20
#@faculty      hard  nproc          50
#ftp           hard  nproc          0
#@student      -     maxlogins       4
# End of file
root soft nofile 655350
root hard nofile 655350
* soft nofile 655350
* hard nofile 655350
* soft nproc 655350
* hard nproc 655350
~
```

```
#sudo vi /etc/sysctl.conf
```

---

Add the following lines at the end of the file

```
fs.file-max = 655350
kernel.pid_max = 655350
net.core.rmem_max = 128000000
net.core.somaxconn = 10000
kernel.core_pattern = core.%e
```

```
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
fs.file-max = 655350
kernel.pid_max = 655350
net.core.rmem_max = 128000000
net.core.somaxconn = 10000
kernel.core_pattern = core.%e
~
~
~
```

#sudo sysctl -p

## Linux performance view

#ulimit -a

open files 和 max user processes 为655350

```
core file size          (blocks, -c) unlimited
data seg size           (kbytes, -d) unlimited
scheduling priority     (-e) 0
file size               (blocks, -f) unlimited
pending signals         (-i) 14950
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files              (-n) 655350
pipe size               (512 bytes, -p) 8
POSIX message queues    (bytes, -q) 819200
real-time priority      (-r) 0
stack size              (kbytes, -s) 8192
cpu time                (seconds, -t) unlimited
max user processes      (-u) 655350
virtual memory          (kbytes, -v) unlimited
file locks              (-x) unlimited
```

#cat /proc/sys/kernel/pid\_max

pid\_max 为655350

```
[root@localhost user]# cat /proc/sys/kernel/pid_max
655350
```

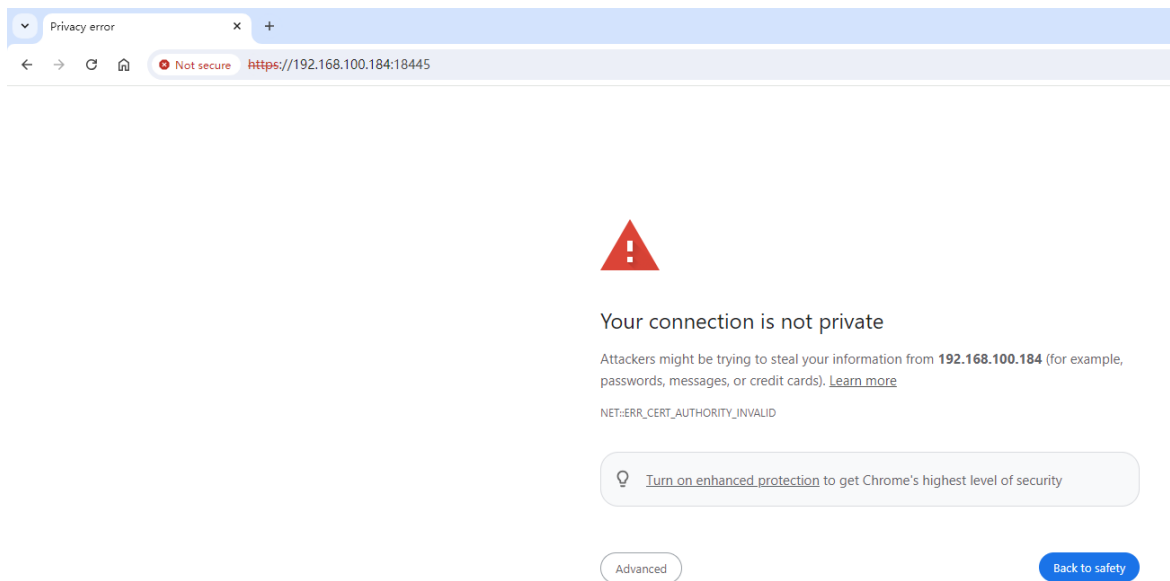
You can check whether the following variables are the same as those in the configuration file.

#cat /proc/sys/net/core/rmem\_max

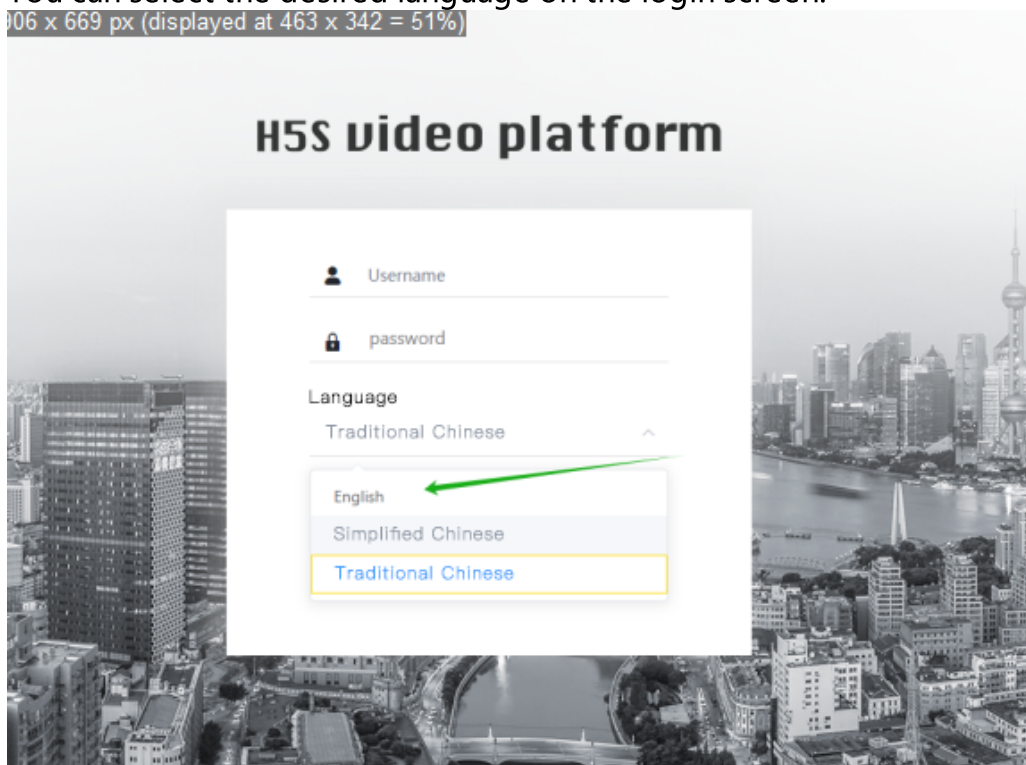
#cat /proc/sys/net/core/somaxconn



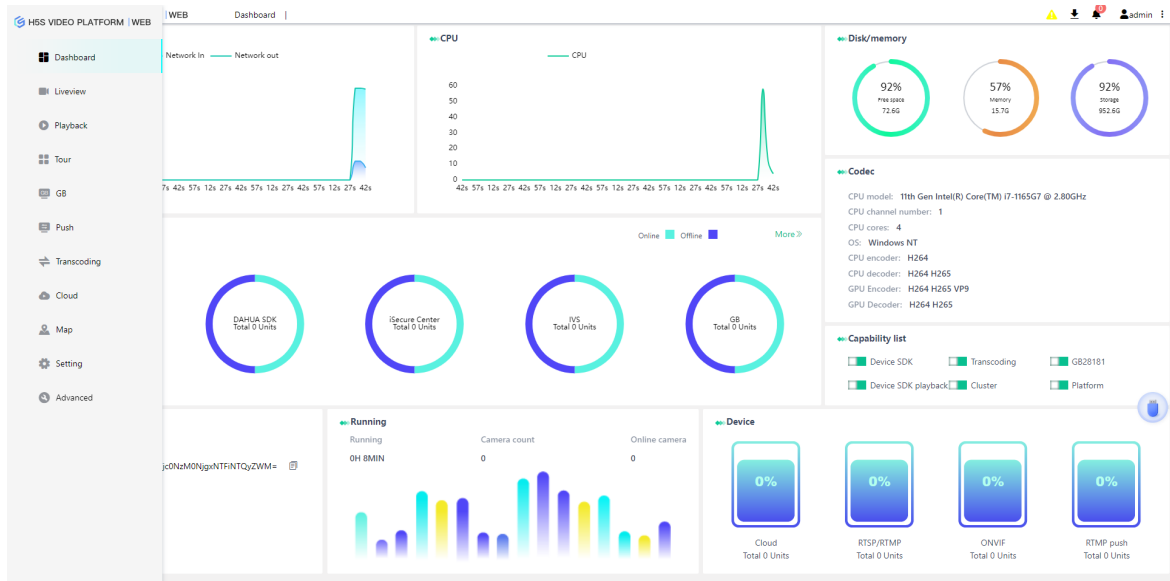
use HTTPS, you need to click the advanced button below. The main reason is that the default certificate for H5S is self-signed.



You can select the desired language on the login screen:



The following is the English login interface:



## 4.5 Install License

### Install License

In logs/h5sslog\_2021-03-23\_11-06.log (the specific file name is determined at runtime), it is shown as follows:

```
[2021-03-23 11:06:10.120] [h5ss] [info] [t31684] h5ss started Hostid
NTI4Mzg1NjY3NDZmNTVhN2MyYzVlNDZhN2UxZDEwOWU=
```

Or copy and obtain the HostidID in the management interface of H5SWeb. Then send the Hostid to [info@linkingvision.com](mailto:info@linkingvision.com). After receiving the h5ss.lic license file, place the h5ss.lic file in the conf directory, and then restart h5ss. Please turn off all virtual network cards and remove all USB network cards when generating the Hostid.

If you want to replace the lic file, you need to move or delete the original lic file. Renaming is not supported because H5S only recognizes the .lic suffix and supports different authorization file names.

If you use the license import function of the management interface, if the original license file name is inconsistent with the new license file name, please manually remove the original license file first, so that only the new license file takes effect.



## 4.6 Port

### Port

The ports used by H5S are shown in the following table. All ports can be modified in conf/h5ss.conf:

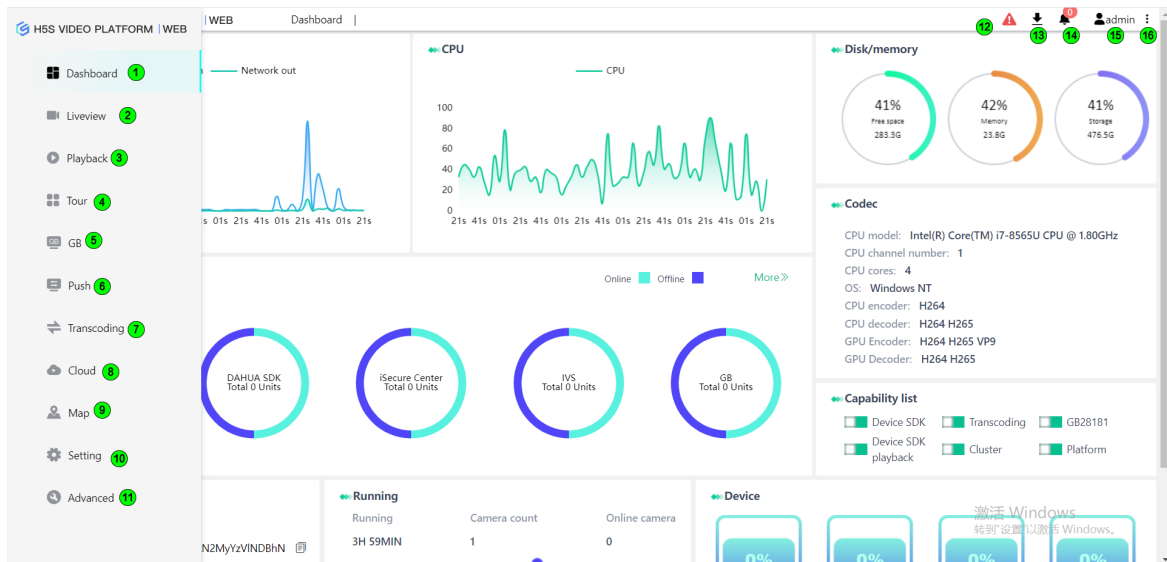
Name	Port	Protocol	Describe
HTTP	18085(r16 and later versions) 8080 (r15 and previous versions)	TCP	Management Port
HTTPS	18445(r16 and later versions) 8443 (r15 and previous versions)	TCP	Encrypted management port
RTSP	8554	TCP	RTSP forwarding
RTSP(TLS)	8555	TCP	RTSP Forwarding Reserved
RTMP	8935	TCP	RTMP forwarding
RTMP(TLS)	8936	TCP	RTMP Forwarding Reserved
FLV	8890	TCP	FLV forwarding
FLV(TLS)	8891	TCP	FLV Forwarding Reserved

WBERTC	50000-54999	TCP	For the port range, the number can be adjusted
TURN	9478	TCP	WEBRTC forwarding mode takes effect
GB SIP	5060	TCP/UDP	TCP/UDP can be configured
GB RTP	55000-59999	UDP	For the port range, the number can be adjusted

## 4.7 Menu

### Menu

The system menu is shown in the following figure. The system supports Dark mode and Light mode, which can be switched in the settings in the upper right corner.



Number	Name	Function
1	Dashboard	
2	Liveview	
3	Playback	
4	Tour	
5	GB	
6	Pash	

---

7	Transcoding	
8	Cloud	
9	Map	
10	Setting	
11	Advanced	
12	Alarm	
13	Download task	
14	Event	
15	User	
16	More	



## 5.Device configuration

---

## 5 Device configuration

### Introduction to device configuration

In the H5S system, each video channel is assigned a token, and video access and API calls are based on tokens. There are two types of token generation: static configuration and dynamic generation. RTSP/RTMP/RTMP streaming/ONVIF/file sources are all static configurations, and device SDKs (including platform access) are all dynamically generated tokens. The reason for dynamically generating tokens is that the device contains multiple channels. Once a token is generated, it will not change and will correspond one-to-one with the device's channels.

You can view the corresponding token in **Setting-» Device-» All**.

ID	Name	IP	Port	User name	Online status	Token	Keywords filter
1	Device1 (0)	invalid	invalid	invalid	false	1d54--0	H5_CH_DEV
2	114	invalid	invalid	invalid	true	1d54--1	H5_CH_DEV
3	104(4G)	invalid	invalid	invalid	true	1d54--2	H5_CH_DEV
4	Device1 (3)	invalid	invalid	invalid	false	1d54--3	H5_CH_DEV
5	Device1 (4)	invalid	invalid	invalid	false	1d54--4	H5_CH_DEV
6	Device1 (5)	invalid	invalid	invalid	false	1d54--5	H5_CH_DEV
7	Device1 (6)	invalid	invalid	invalid	false	1d54--6	H5_CH_DEV
8	Device1 (7)	invalid	invalid	invalid	false	1d54--7	H5_CH_DEV

The token entered by the user is composed of letters and numbers. The token cannot be repeated and supports a single hyphen and underscore. Special characters (such as @#\$ etc.) are not supported. Correct examples include token1\_1 and token1-1. Double hyphens are not supported, and examples of unsupported tokens include token1--1.

### Delete default configuration

In the H5S system, four default configurations are provided for debugging purposes and are for reference only. You can delete the relevant configurations before actual use.

ID	Name	IP	Port	User name	Online status	Type	Token	Keywords filter
1	Cam1	192.168.1.1	554	admin	false	H5_STREAM	5255	Edit Delete

The top screenshot shows the 'H5S VIDEO PLATFORM | WEB' interface with the 'Setting' tab selected. The left sidebar shows 'Region' and 'Device' options. The 'Device' section is expanded, showing 'RTSP/RTMP', 'ONVIF', 'Device SDK', 'RTMP push', and 'File'. The main table has columns: ID, Name, IP, Port, User name, Online status, Type, and Token. It contains one row: ID 1, Name Cam1, IP invalid, Port invalid, User name admin, Online status false, Type H5\_FILE, and Token 54a0. There are 'Add' and 'Delete' buttons at the top left of the table.

The bottom screenshot shows the same interface, but the 'ONVIF' option is selected in the sidebar. The table now contains one row: ID 1, Name Device1, IP 192.168.100.209, Port 37777, User name admin, Online status true, Type H5\_DEV\_DH, and Token 1d54. There are 'Add', 'Delete', and 'Setting' buttons at the top left of the table.

## 5.1 Video source configuration

### 5.1.1 RTSP/RTMP video source configuration

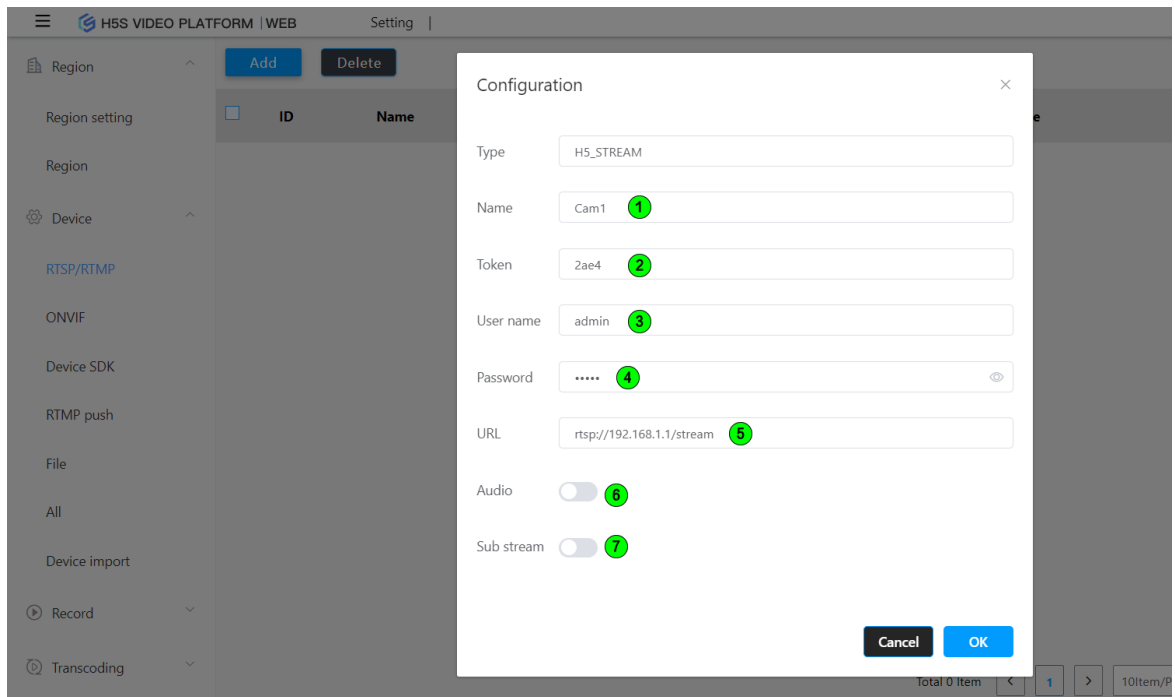
#### Introduction to RTSP/RTMP video sources

RTSP/RTMP uses pull streaming to obtain video. This protocol does not support PTZ control. If PTZ control is required, ONVIF or device SDK can be used instead.

Due to the fact that most of the current systems adopt the on-demand streaming mode, the online status is obtained through IP address and port detection. The default detection function is enabled. If you want to disable it, you can go to **Setting-» Protocol-» RTSP** and turn off the RTSP service detection, or you can configure the detection interval.

#### Add Delete

Add and delete in **Setting-» Device -» RTSP/RTMP**. The following figure shows the corresponding fields. You should remove the user and password from the URL, and set the username & password separately. If you need to delete or modify, you can directly select the device to edit and delete.



Number	Name	Function
1	Name	
2	Token	
3	User name	
4	Password	
5	URL	
6	Audio	
7	Sub stream	

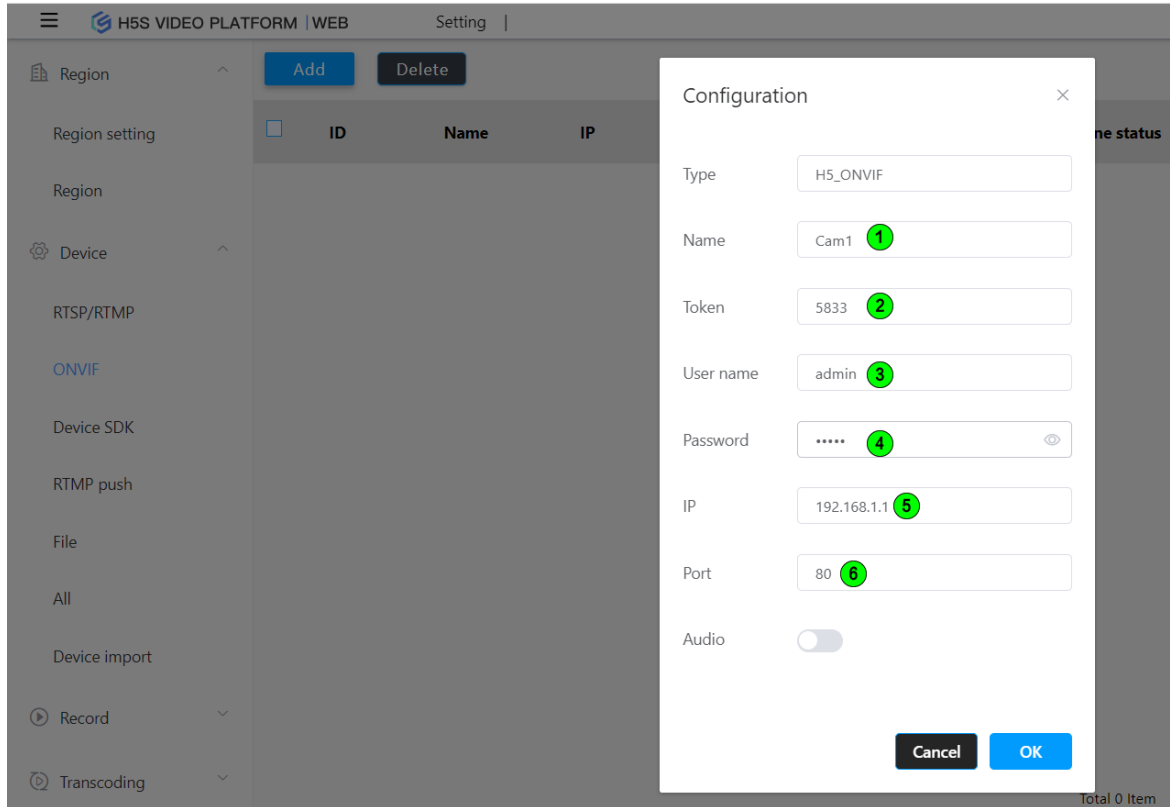
## 5.1.2 ONVIF video source configuration

### Introduction to ONVIF Camera

ONVIF is a popular international standard for camera interfaces. Currently, both domestic and international cameras support this standard, and H5S supports the ONVIF ProfileS feature set. Devices that use ONVIF integration support pan-tilt control and primary and secondary streams.

### Add Delete

Add and delete ONVIF in **Setting-» Device-» ONVIF**. The following figure shows the corresponding fields. The port is an ONVIF protocol port, and ports from different manufacturers may be different. If you need to delete or modify it, you can directly select the device to edit and delete. ONVIF type does not support NAT mapping.



\*Some cameras (such as the new version of Hikvision cameras) have ONVIF disabled by default. You can go to the corresponding interface to enable it and add an ONVIF username and password to enable the ONVIF function.

Number	Name	Function
1	name	
2	Token	
3	User name	
4	Password	
5	IP	
6	Port	

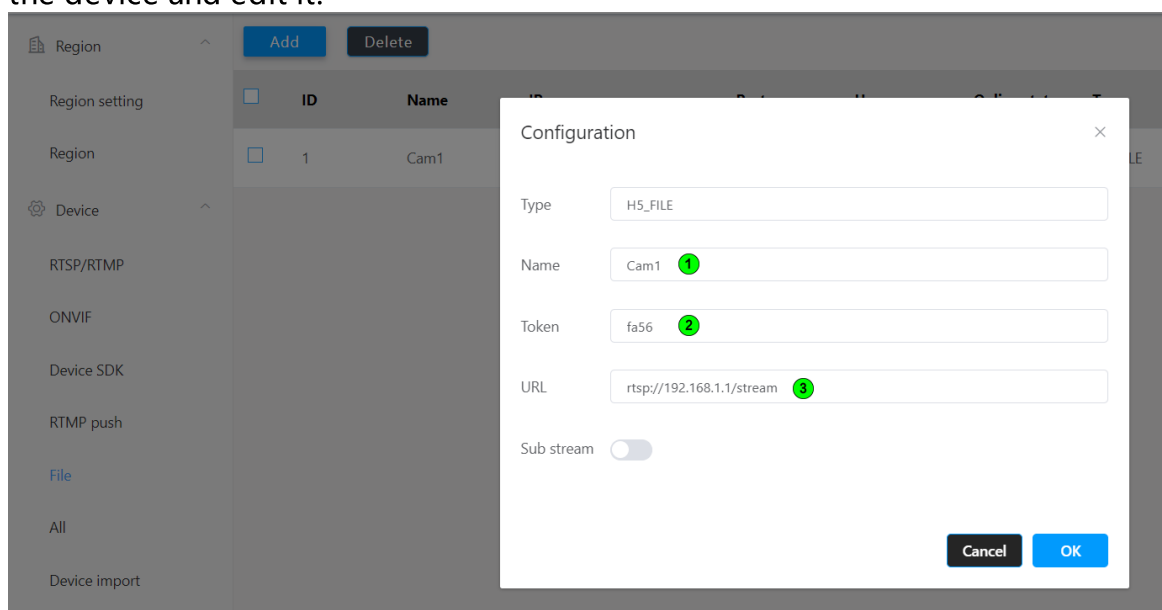
### 5.1.3 File video source configuration

#### Introduction to file video source

File source is a method that can use video files as the test video source. Currently, only MP4 files of H5S videos are supported. The official website of Linkingvision provides the test video sources h5ssample.mp4 and h5ssamplesub.mp4 in <https://linkingvision.com/download/h5stream/video/>. You can download them to your local computer. The two files correspond to the main stream and the auxiliary stream respectively. If you copy the path name from Windows Explorer, you need to replace \ with \\.

#### Add Delete

Add and delete in **Setting-» Device-» File**. The following figure shows the corresponding fields. If you need to delete or modify, you can directly select the device and edit it.



Number	Name	Function
1	name	
2	Token	
3	URT	

## 5.2 Device SDK configuration

#### Introduction to Device SDK

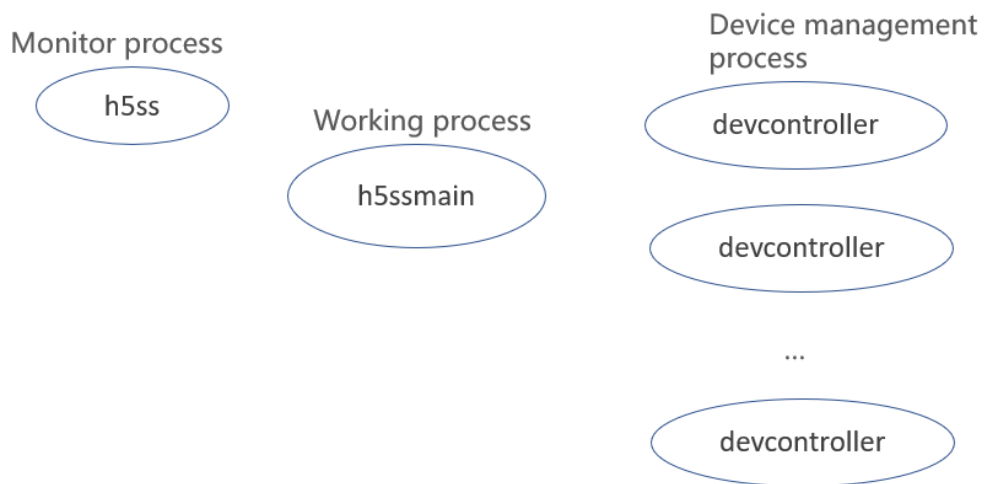
H5S integrates the device SDKs of mainstream video surveillance manufacturers in China, thus supporting richer functions. Since the device SDKs include software libraries from other manufacturers, from the perspective of

software product stability, H5S provides two modes of operation, one is centralized and the other is sandbox.

Centralized mode means that all devices run in one process space. The advantage is high efficiency and no cross-process communication costs, and the disadvantage is that all devices are interrelated, which can lead to abnormality in all devices if an exception occurs.

**In Sandbox mode, it supports the offline channel of the NVR connected to the playback device SDK.**

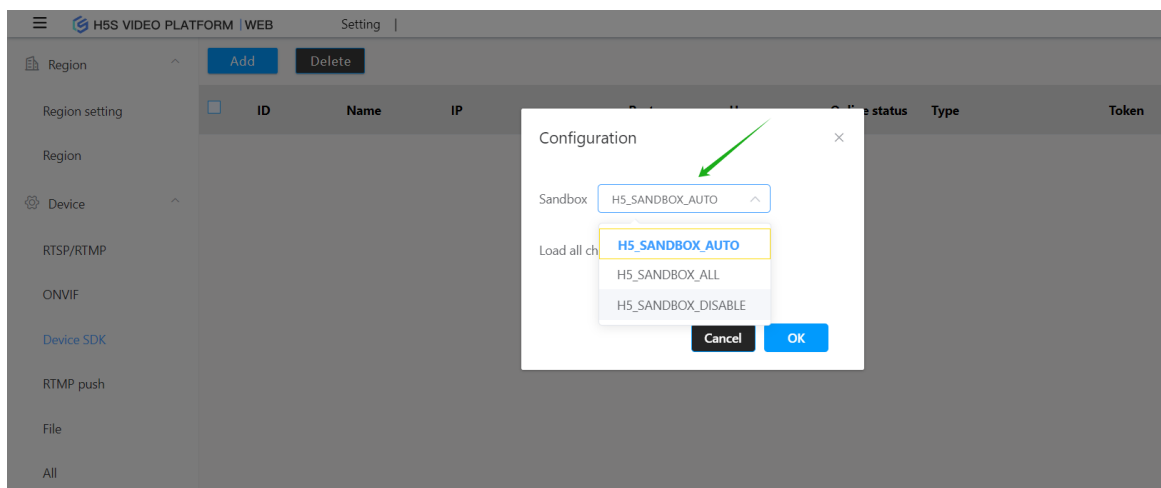
The Sandbox mode creates a separate process for each device. The advantage is isolation and high stability; the disadvantage is increased cross-process communication costs. The Sandbox mode can be referenced in the following diagram:



H5S adopts the centralized mode by default, which can be modified in **Setting-» Device-» Device SDK**. H5\_SANDBOX\_AUTO indicates that each device is configured separately; H5\_SANDBOX\_ALL indicates that the Sandbox mode is enabled for all devices, regardless of individual device configuration. H5\_SANDBOX\_DISABLE indicates that all Sandbox modes are disabled, regardless of individual device configuration.

There is a configuration item in the configuration settings that loads all channels. This configuration is enabled by default, indicating that all channels provided by the SDK will be loaded, regardless of whether there is a camera configuration or whether the channel is online. If this configuration is disabled, only online channels will be loaded.

The above two configurations need to be restarted to take effect after modification.



## 5.2.1 Hikvision SDK configuration

### Introduction to Hikvision SDK

Hikvision SDK supports all video devices of Hikvision series (except for the ezviz), including cameras, NVRs, and some access control devices with video functions. It also supports CVR, which will be introduced later in the configuration.

### Add Delete

Add in **Setting-» Device-» Device SDK**, select H5\_DEV\_HIK as the type, where the sandbox configuration is effective when the total sandbox configuration is H5\_SANDBOX\_AUTO. The port is defaulted to 8000, but if modified or mapped, a new port can be used.

If you need to delete or modify it, you can directly select the device and edit it to delete.



The screenshot shows the 'Configuration' dialog box in the H5S VIDEO PLATFORM WEB interface. The dialog contains the following fields and controls, each marked with a numbered green circle:

- 1. Type: H5\_DEV\_HIK (dropdown)
- 2. Name: Device1 (text input)
- 3. Token: 93bd (text input)
- 4. User name: admin (text input)
- 5. Password: masked with dots (password input)
- 6. IP: 192.168.1.1 (text input)
- 7. Port: 8000 (text input)
- 8. API Port: 80 (text input)
- 9. API HTTPS: false (dropdown)
- 10. Audio: toggle switch (on)
- 11. Sandbox: toggle switch (on)
- 12. ISAPI: toggle switch (on)
- 13. Sub event: false (dropdown)
- 14. Max channels: 0 (text input, with note '(0 stand for all channels)')

Buttons at the bottom right: Cancel, OK.

Number	Name	Function
1	Type	Device type
2	Name	Device name
3	Token	Token same with naming rule for tokens
4	User name	Device user name
5	Password	Device password
6	IP	Device IP
7	Port	Device port
8	API port	Device API port, same with web interface
9	API HTTPS	Device API use HTTPS or not
10	Audio	Enable audio
11	Sandbox	Enable sandbox
12	ISAPI	Use ISAPI for live view
13	Sub event	Subscribe event
14	Max channel	Loading how many channels, default is 0, sand for all the channels

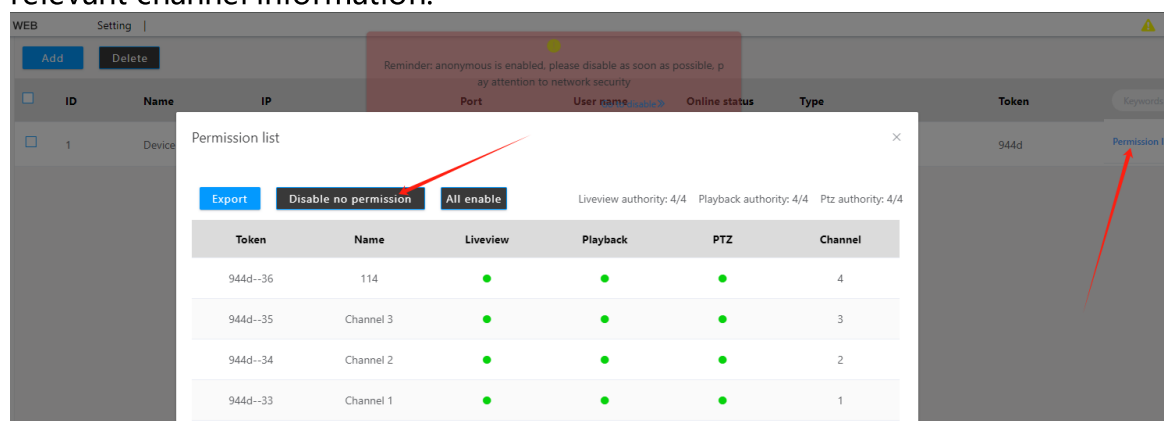
\*If you enter the wrong password and cannot log in online even after correcting it, you can check whether the device configuration interface has enabled illegal

login, or wait for 30 minutes to automatically unlock. You can refer to the following interface.



## Permission List

Hikvision SDK supports obtaining the current user's operation permissions, and can check whether there are corresponding operation permissions. The channel number corresponds to the device web page channel number. You can disable channels without permissions with one click. You can also export relevant channel information.



## 5.2.2 Dahua SDK configuration

### Introduction to Dahua SDK

The Dahua SDK supports all recent video devices from Dahua, including cameras and NVRs, and also supports EVS.

### Add Delete

Add in the **Setting-》Device-》Device SDK**, select the type H5\_DEV\_DH, where the sandbox configuration is effective when the total sandbox configuration is H5\_SANDBOX\_AUTO. The port is defaulted to 37777, but if you modify or map it, you can use the corresponding new port.

If you need to delete or modify it, you can directly select the device and edit it to delete.

The screenshot shows the 'Configuration' dialog box in the H5S VIDEO PLATFORM WEB interface. The dialog contains the following fields and their corresponding numbers:

- 1: Type (dropdown menu)
- 2: Name (text input)
- 3: Token (text input)
- 4: User name (text input)
- 5: Password (password input)
- 6: IP (text input)
- 7: Port (text input)
- 8: API Port (text input)
- 9: API Https (dropdown menu)
- 10: Audio (toggle switch)
- 11: Sandbox (toggle switch)
- 12: Sub event (dropdown menu)
- 13: Max channels (text input)

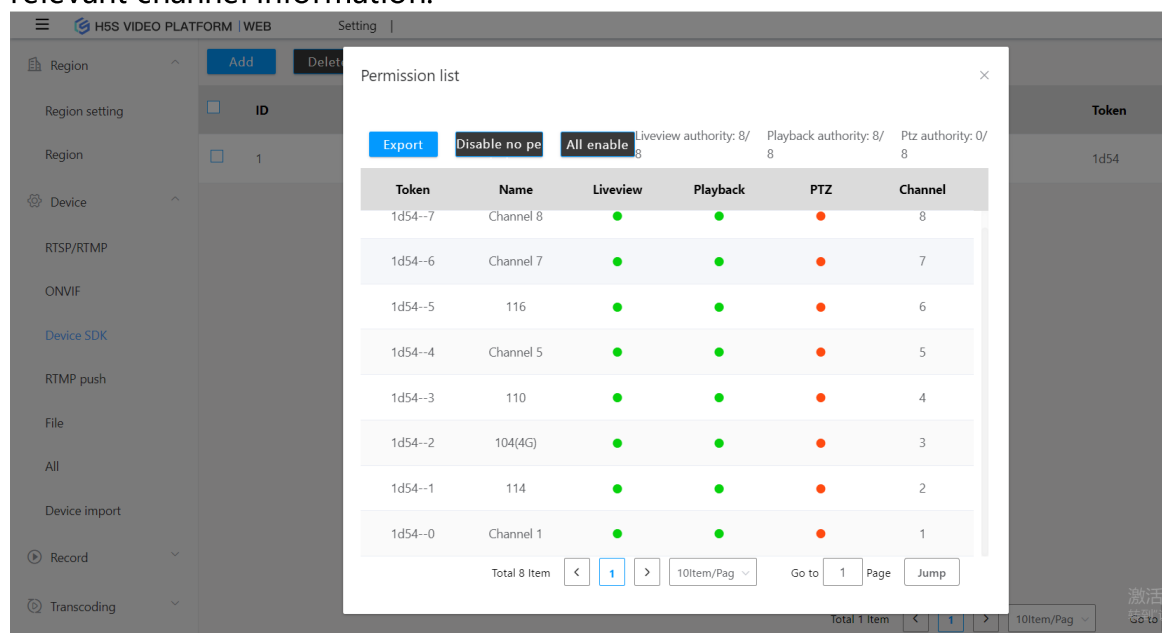
The background interface shows a sidebar with options like Region, Device, RTSP/RTMP, ONVIF, Device SDK, RTMP push, File, All, Device import, Device export, Record, and Transcoding. The main area displays a table with columns: ID, Name, IP, Port, User name, Online status, and Type.

Number	Name	Function
1	Type	Device type
2	Name	Device name
3	Token	Token same with naming rule for tokens
4	User name	Device user name
5	Password	Device password
6	IP	Device IP
7	Port	Device port
8	API port	Device API port, same with web interface
9	API HTTPS	Device API use HTTPS or not
10	Audio	Enable audio
11	Sandbox	Enable sandbox
12	Sub event	Subscribe event
13	Max channel	Loading how many channels, default is 0, stand for all the channels

## Permission List

The Dahua SDK supports obtaining the current user's operation permissions, which can be checked for corresponding operation permissions. The channel

number corresponds to the device web page channel number. It is possible to disable channels without permissions with one click. It is also possible to export relevant channel information.



## 5.2.3 Huawei IVS configuration

### Introduction to Huawei IVS

Huawei IVS SDK supports Huawei IVS1800 and IVS3800.

#### Add Delete

Add it in **Setting-» Device-» Device SDK**, and select H5\_DEV\_IVS as the type. The sandbox configuration takes effect when the total sandbox configuration is set to H5\_SANDBOX\_AUTO. The port is defaulted to 18531, but if you modify or map it, you can use the corresponding new port.

IVS: A user can only log in once at a time. It is recommended to create a new user for testing.

If you need to delete or modify it, you can directly select the device and edit it to delete.

The screenshot shows the 'Configuration' dialog for adding a device. The fields are numbered as follows:

- 1: Type (dropdown menu)
- 2: Name (text input)
- 3: Token (text input)
- 4: User name (text input)
- 5: Password (password input)
- 6: IP (text input)
- 7: Port (text input)
- 8: Audio (toggle switch)
- 9: Sandbox (toggle switch)
- 10: Buffertime (text input, unit: Millisecond)
- 11: Max channels (text input, note: (0 stand for all channels))

Buttons at the bottom right: Cancel, OK.

Number	Name	Function
1	Type	Device type
2	Name	Device name
3	Token	Token same with naming rule for tokens
4	User name	Device user name
5	Password	Device password
6	IP	Device IP
7	Port	Device port
8	Audio	Enable audio
9	Sandbox	Enable sandbox
10	Buffertime	Video cache time, default is not to cache, unit is milliseconds
11	Max channel	Loading how many channels, default is 0, sand for all the channels

## 5.2.4 ONVIFSTG configuration

### Introduction to ONVIF STG

ONVIF STG type supports ONVIF Profile S/Profile T/Profile G, and supports cameras and network hard disk video recorders. ONVIF STG supports r18.1 and later.

### Add Delete

Add it in **Setting-» Device-» Device SDK**, and select H5\_DEV\_ONVIFSTG as the type. The sandbox configuration takes effect when the total sandbox configuration is set to H5\_SANDBOX\_AUTO. The port is defaulted to 80, but if you modify, you can use the corresponding new port. ONVIF type does not support NAT mapping.

IVS: A user can only log in once at a time. It is recommended to create a new user for testing.

If you need to delete or modify it, you can directly select the device and edit it to delete.

The screenshot shows the 'Configuration' dialog for adding a new device. The fields are as follows:

- 1: Type (H5\_DEV\_ONVIFSTG)
- 2: Name (Device1)
- 3: Token (40b6)
- 4: User name (admin)
- 5: Password (masked)
- 6: IP (192.168.1.1)
- 7: Port (80)
- 8: Audio (toggle)
- 9: Sandbox (toggle)
- 10: Buffertime (0 Millisecond)
- 11: Max channels (0)

Number	Name	Function
1	Type	Device type
2	Name	Device name
3	Token	Token same with naming rule for tokens
4	User name	Device user name
5	Password	Device password
6	IP	Device IP

7	Port	Device port
8	Audio	Enable audio
9	Sandbox	Enable sandbox
10	Buffertime	Video cache time, default is not to cache, unit is milliseconds
11	Max channel	Loading how many channels, default is 0, stand for all the channels

## 5.2.5 Tiandy SDK configuration

### Introduction to Tiandy SDK

The Tiandy SDK supports all recent video devices from Tiandy, including cameras and NVRs.

### Add Delete

Add in the **Setting-> Device -> Device SDK**, select the type H5\_DEV\_TD, where the sandbox configuration is effective when the total sandbox configuration is H5\_SANDBOX\_AUTO. The port is defaulted to 3000, but if you modify or map it, you can use the corresponding new port.

If you need to delete or modify it, you can directly select the device and edit it to delete.

The screenshot shows the 'Configuration' dialog box for adding a device. The fields are numbered as follows:

- 1: Type (H5\_DEV\_TD)
- 2: Name (Device1)
- 3: Token (29fe)
- 4: User name (admin)
- 5: Password (masked)
- 6: IP (192.168.1.1)
- 7: Port (3000)
- 8: Audio toggle (checked)
- 9: Sandbox toggle (checked)
- 10: Max channels (0)

Number	Name	Function
1	Type	Device type

---

2	Name	Device name
3	Token	Token same with naming rule for tokens
4	User name	Device user name
5	Password	Device password
6	IP	Device IP
7	Port	Device port
8	Audio	Enable audio
9	Sandbox	Enable sandbox
10	Max channel	Loading how many channels, default is 0, sand for all the channels

### 5.2.6 UNVSDK configuration

#### Introduction to the UNVSDK

The UNV SDK supports all of UNV's recent video devices, including cameras and NVRs, but not including NVRs based on the IMOS platform.

#### Add Delete

Add it in **Setting-» Device-» Device SDK**, select H5\_DEV\_UNV as the type, and the sandbox configuration will take effect when the total sandbox configuration is set to H5\_SANDBOX\_AUTO. The port is defaulted to 80, but if you modify or map it, you can use the corresponding new port.

If you need to delete or modify it, you can directly select the device and edit it to delete.



The screenshot shows the 'Configuration' dialog box in the H5S VIDEO PLATFORM WEB interface. The dialog contains the following fields and their corresponding numbers:

- 1: Type (dropdown menu)
- 2: Name (text input)
- 3: Token (text input)
- 4: User name (text input)
- 5: Password (password input)
- 6: IP (text input)
- 7: Port (text input)
- 8: API Port (text input)
- 9: API Https (dropdown menu)
- 10: Audio (toggle switch)
- 11: Sandbox (toggle switch)
- 12: VMS (toggle switch)
- 13: Sub event (dropdown menu)
- 14: Max channels (text input)

The background interface shows a sidebar with options like Region, Device, RTSP/RTMP, ONVIF, Device SDK, RTMP push, File, All, Device import, Device export, Record, and Transcoding. The main area displays a table with columns: ID, Name, IP, Port, User name, Online status, and Type.

Number	Name	Function
1	Type	Device type
2	Name	Device name
3	Token	Token same with naming rule for tokens
4	User name	Device user name
5	Password	Device password
6	IP	Device IP
7	Port	Device port
8	API port	Device API port, same with web interface
9	API HTTPS	Device API use HTTPS or not
10	Audio	Enable audio
11	Sandbox	Enable sandbox
12	VMS	Device is VMS or not
13	Sub event	Subscribe event
14	Max channel	Loading how many channels, default is 0, sand for all the channels

## 5.2.7 Hikvision CVR configuration

### Introduction to Hikvision CVR configuration

Hikvision SDK supports Hikvision CVR series storage products (tested with DS-A72024R).

#### Add Delete

Add in **Setting-» Device-» Device SDK**, select H5\_DEV\_HIK as the type, where the sandbox configuration is effective when the total sandbox configuration is H5\_SANDBOX\_AUTO. The port is defaulted to 8000, but if modified or mapped, a new port can be used.

The CVR includes multiple subsystems, but the password for SDK access is 12345 by default, which is not the password for the CVR subsystem. If you need to view this password, please log in to the SMH terminal and use the following command to view the SDK password.

```
$/b_iscsi/nvr/bin/nvruser getuser admin
```

If you need to delete or modify it, you can directly select the device and edit it to delete.

The screenshot shows the 'Device SDK' configuration window in the H5S VIDEO PLATFORM WEB interface. The window has a sidebar on the left with various settings categories. The main area displays a table with columns: ID, Name, IP, Port, User name, Online status, and Type. A 'Configuration' dialog box is open, showing fields for Type (H5\_DEV\_HIK), Name (Device1), Token (93bd), User name (admin), Password (\*\*\*\*\*), IP (192.168.1.1), Port (8000), API Port (80), API Https (false), Audio (toggle), ISAPI (toggle), Sub event (false), and Max channels (0). The 'Sandbox' toggle is also visible. The dialog has 'Cancel' and 'OK' buttons at the bottom right.

Number	Name	Function
1	Type	Device type
2	Name	Device name
3	Token	Token same with naming rule for tokens
4	User name	Device user name
5	Password	Device password
6	IP	Device IP
7	Port	Device port
8	API port	Device API port, same with web interface
9	API HTTPS	Device API use HTTPS or not

10	Audio	Enable audio
11	Sandbox	Enable sandbox
12	ISAPI	Use ISAPI for live view
13	Sub event	Subscribe event
14	Max channel	Loading how many channels, default is 0, sand for all the channels

## 5.3 Platform access configuration

### 5.3.1 Hikvision ISC configuration

#### Preparation for Hikvision ISC configuration

Before configuration, you need to obtain the IP address and port of the ISC platform. The port is 443 by default, and you need to obtain the partner AppKey and partner AppSecret from the ISC administrator. You can also refer to the API documentation to add them through the API. The default integration uses the device storage of ISC. If you need to use the centralized storage of ISC, you need to modify bCentralRecord to true in the corresponding node of conf/h5ss.conf to switch to ISC centralized storage.

The partner AppKey and partner AppSecret can be configured from the Hikvision ISC operation center. The specific method is as follows

1. Enter the operation management center (<http://ip:8001/center>), enter the [Status Monitoring] module, select [API Gateway], select the [API Management] function, and enter the API management center.

**API网关 V3.2.0**

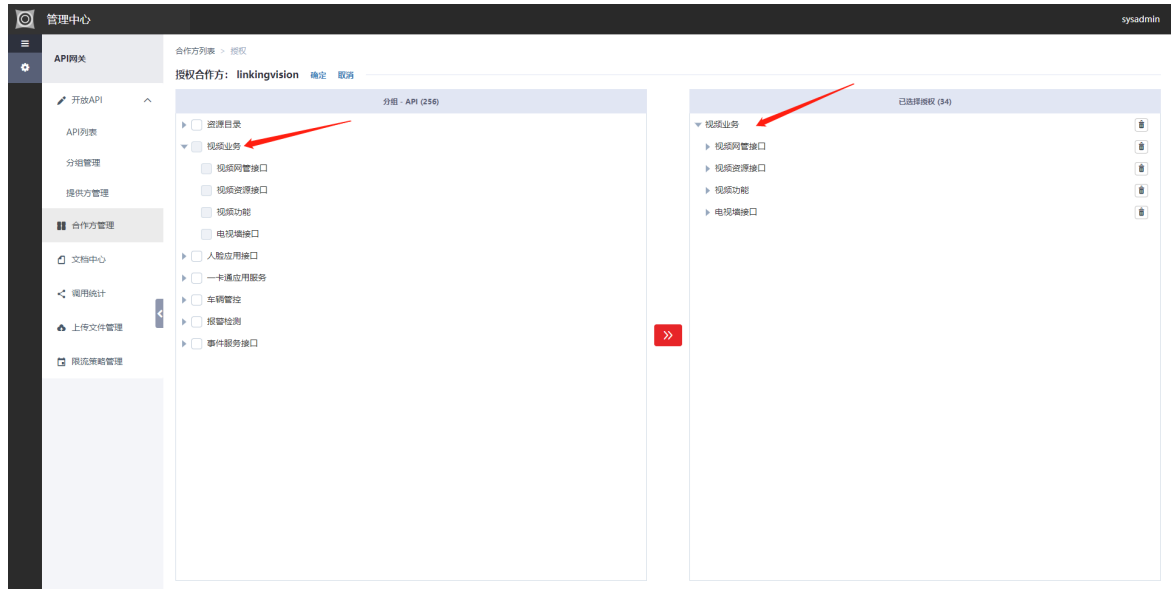
安装路径: C:\Program Files\hikvision\web (C盘: 可用201.4GB / 总310.0GB)

**服务列表**

实例名称	服务类型	所属中间件	端口号	服务名/地址
artemis-portal-192.168.100.132-#1	artemis-portal(artemi...	-	52730 (TCP)	hik.artem... hik.art
artemis-192.168.100.132-#1	artemis(artemis)	JRE	9016 (TCP)	hik.artem

2. Select [Partner Management]. After the platform is installed, an internal partner will be created by default. You can use this partner for interface call testing. The actual running environment requires the creation of new partners based on actual conditions.

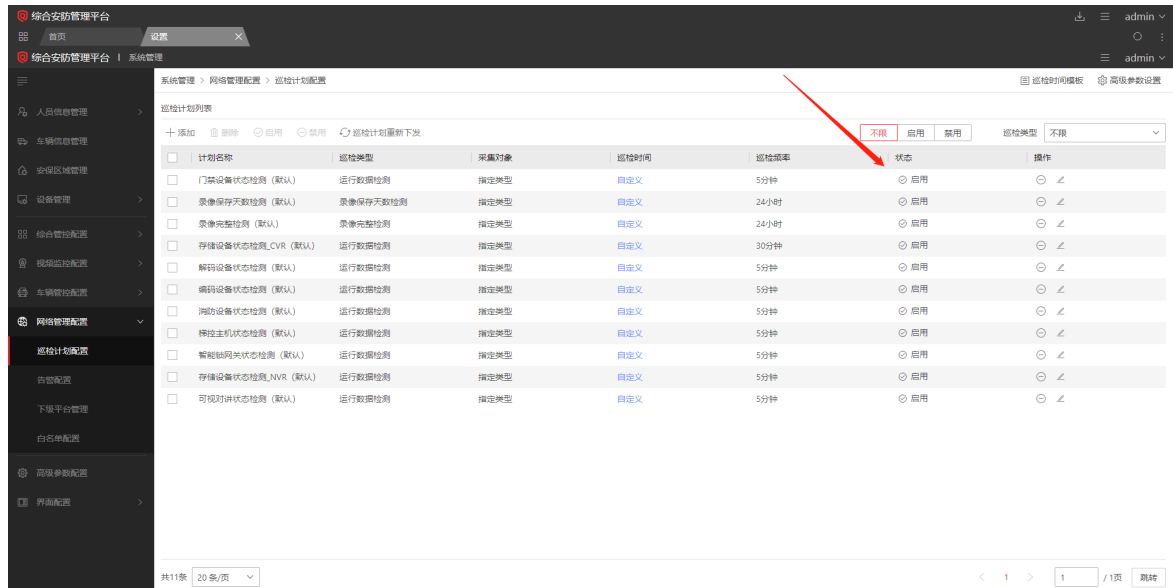
3. Click on the name of the partner to enter the partner details interface and obtain the partner key (AK) and partner secret (SK). Select the permission to check the video business.



The H5S video platform uses the following APIs to integrate with ISC, and it is necessary to ensure that the following APIs are properly authorized.

API	Describe
/api/resource/v1/cameras	Get monitoring point resources by paging
/api/nms/v1/online/camera/get	Obtain the online status of the monitoring point
/api/video/v1/ptzs/controlling	Carry out PTZ operation interface according to the monitoring point number
/api/video/v1/presets/searches	Query preset point information
/api/video/v1/presets/addition	Set preset point information
/api/video/v1/presets/deletion	Delete preset point information
/api/video/v1/cameras/playbackURLs	Obtain the URL for streaming playback at the monitoring point
/api/video/v1/cameras/previewURLs	Obtain the URL for previewing and streaming at the monitoring point

By default, the ISC does not have the function of obtaining device status. You can refer to the following figure to open the inspection plan. If you still have offline after opening the inspection plan, you need to contact Hikvision to check if there is a service that has not been enabled.

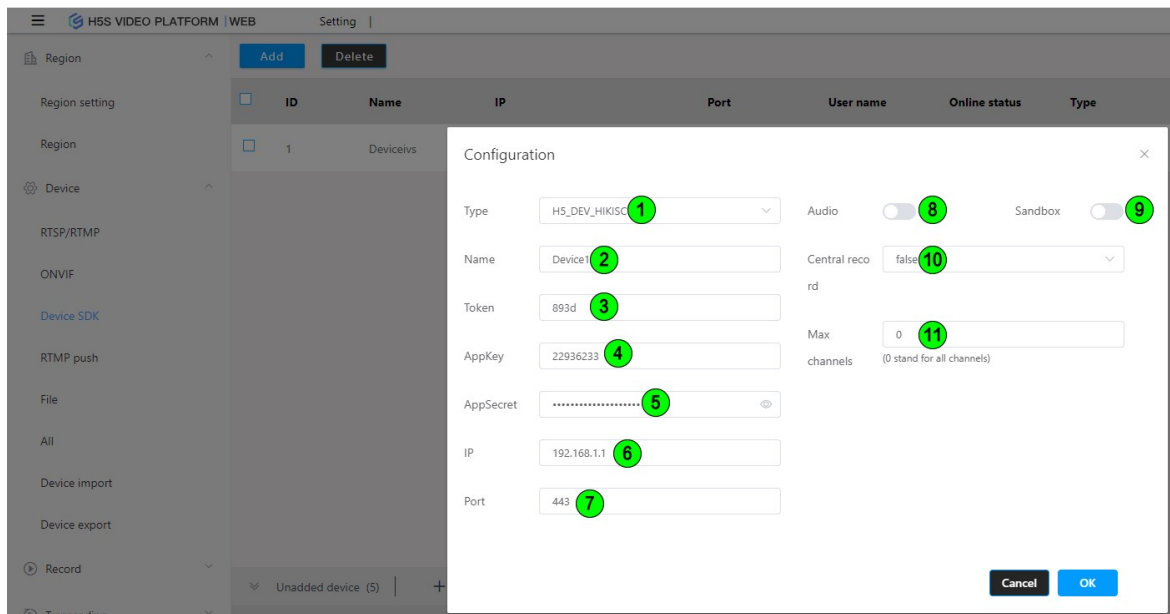


## Add Delete

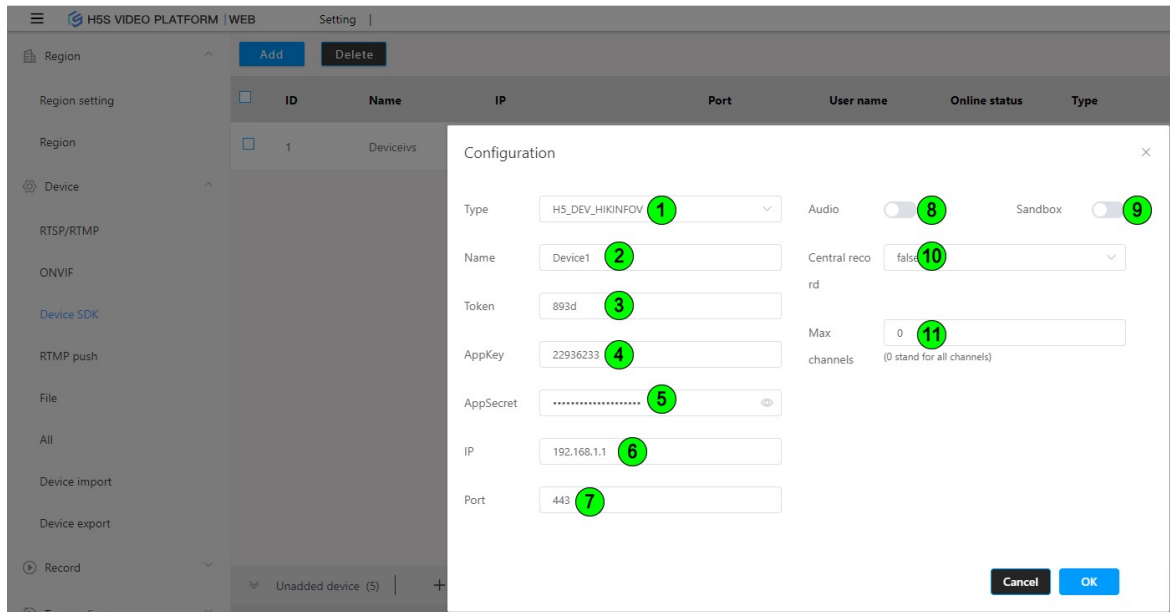
Add in the **Setting-》Device-》Device SDK**, select the type H5\_DEV\_HIKISC, where the sandbox configuration is effective when the total sandbox configuration is H5\_SANDBOX\_AUTO. The port is defaulted to 443, but if you modify or map it, you can use the corresponding new port.

If you need to delete or modify it, you can directly select the device and edit it to delete.

If it is a Hikvision InfoVision series platform, select the H5\_DEV\_HIKINFOV type when adding it.



Number	Name	Function
1	Type	Device type
2	Name	Device name
3	Token	Token same with naming rule for tokens
4	AppKey	Device AppKey
5	AppSecret	Device AppSecret
6	IP	Device IP
7	Port	Device port
8	Audio	Enable audio
9	Sandbox	Enable sandbox
10	Central record	Central record or device record
11	Max channel	Loading how many channels, default is 0, sand for all the channels



### 5.3.2 Dahua ICC configuration

#### Introduction to Dahua ICC

Dahua ICC supports Dahua ICC platform access.

#### Add Delete

Add in the **Setting-» Device-» Device SDK**, select the type H5\_DEV\_DHICC, where the sandbox configuration is effective when the total sandbox configuration is H5\_SANDBOX\_AUTO. The port is defaulted to 443, but if modified or mapped, a new port can be used.

If you need to delete or modify it, you can directly select the device and edit it to delete.

The screenshot shows the 'Configuration' dialog box in the H5S VIDEO PLATFORM WEB interface. The dialog is titled 'Configuration' and has a close button (X) in the top right corner. It contains the following fields and controls, each numbered in a green circle:

- 1: Type (dropdown menu, currently set to H5\_DEV\_DHICC)
- 2: Name (text input, currently set to Device1)
- 3: Token (text input, currently set to 893d)
- 4: User name (text input, currently set to admin)
- 5: Password (password input, currently set to \*\*\*\*\*)
- 6: Client ID (text input, currently set to CompanyName)
- 7: Client Secret (text input, currently set to 42bec152-8f04-476a-9aec-e7d616ff3cd)
- 8: IP (text input, currently set to 192.168.1.1)
- 9: Port (text input, currently set to 443)
- 10: Audio (toggle switch, currently turned off)
- 11: Sandbox (toggle switch, currently turned off)
- 12: Central record (dropdown menu, currently set to false)
- 13: Max channels (text input, currently set to 0)

At the bottom right of the dialog are 'Cancel' and 'OK' buttons. The background interface shows a sidebar with navigation options like 'Region', 'Device', 'RTSP/RTMP', 'ONVIF', 'Device SDK', 'RTMP push', 'File', 'All', 'Device import', 'Device export', and 'Record'. The main area displays a table with columns for ID, Name, IP, Port, User name, Online status, and Type, with one device listed.

Number	Name	Function
1	Type	Device type
2	Name	Device name
3	Token	Token same with naming rule for tokens
4	User name	Device user name
5	Password	Device password
6	Client ID	Device Client ID
7	Client Secret	Device Client Secret
8	IP	Device IP
9	Port	Device port
10	Audio	Enable audio
11	Sandbox	Enable sandbox
12	Central record	Central record or device record
13	Max channel	Loading how many channels, default is 0, sand for all the channels



### 5.3.3 Dahua DSS configuration

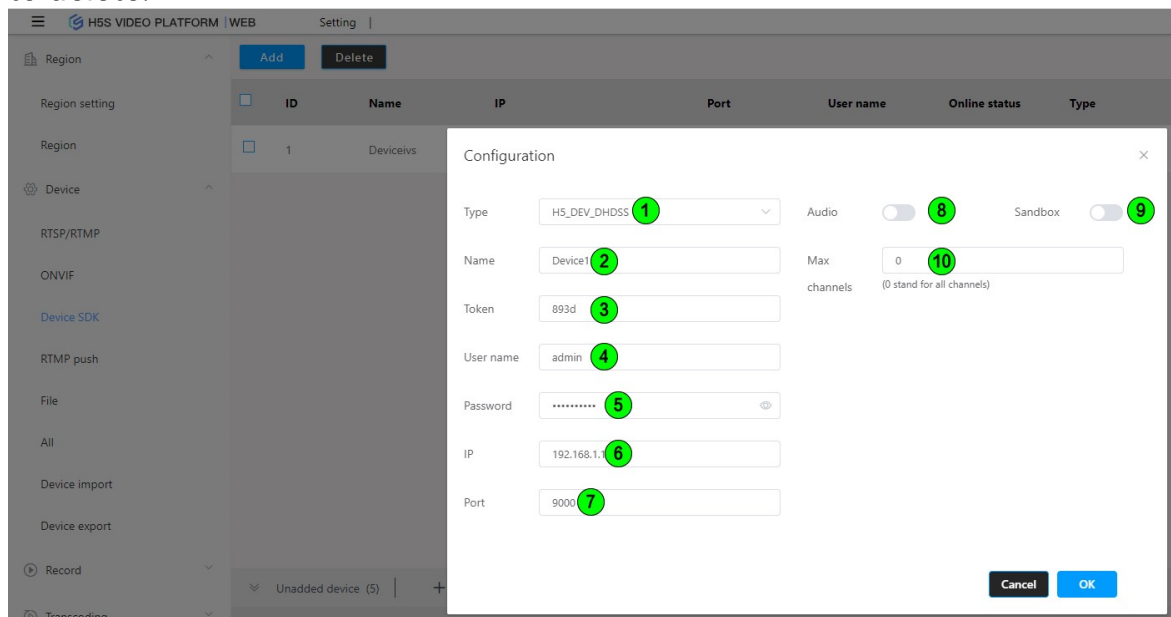
#### Introduction to Dahua DSS

Dahua DSS supports Dahua DSS platform access, only supports Windows deployment, supports real-time video and pan-tilt control, and does not support playback.

#### Add Delete

Add in the **Setting-» Device-» Device SDK**, select the type H5\_DEV\_DHDSS, where the sandbox configuration is effective when the total sandbox configuration is H5\_SANDBOX\_AUTO. The port is defaulted to 9000, but if modified or mapped, a new port can be used.

If you need to delete or modify it, you can directly select the device and edit it to delete.



Number	Name	Function
1	Type	Device type
2	Name	Device name
3	Token	Token same with naming rule for tokens
4	User name	Device user name
5	Password	Device password
6	IP	Device IP
7	Port	Device port
8	Audio	Enable audio

9	Sandbox	Enable sandbox
11	Max channel	Loading how many channels, default is 0, sand for all the channels

## 5.4 Device Search

### Introduction to Device Search

The system supports ONVIF-based device search. When adding ONVIF and ONVIF STG (Profile S/Profile T/Profile G) types, the system automatically searches for ONVIF devices on the current network segment, supporting cameras and NVRs.

<div> <div>Unadded device (5)</div> <div>+ Add</div> <div>Refresh</div> </div>					
	ID	IP	Port	ONVIF address	Model
<input type="checkbox"/>	1	10.168.1.196	80	/onvif/device_service	DS-7632N-I2
<input type="checkbox"/>	2	10.168.1.143	80	/onvif/device_service	CS-X5S-4W-C
<input type="checkbox"/>	3	10.168.1.116	80	/onvif/device_service	DS-2CD3T86FWDV2-I3S

## 5.5 RTMP Streaming Configuration

### Introduction to RTMP Streaming

RTMP streaming supports the standard RTMP streaming protocol, which is mainly used for streaming from devices such as drones. This protocol does not support pan-tilt control or on-demand streaming. If you need pan-tilt control or on-demand streaming, we recommend using GB28181.

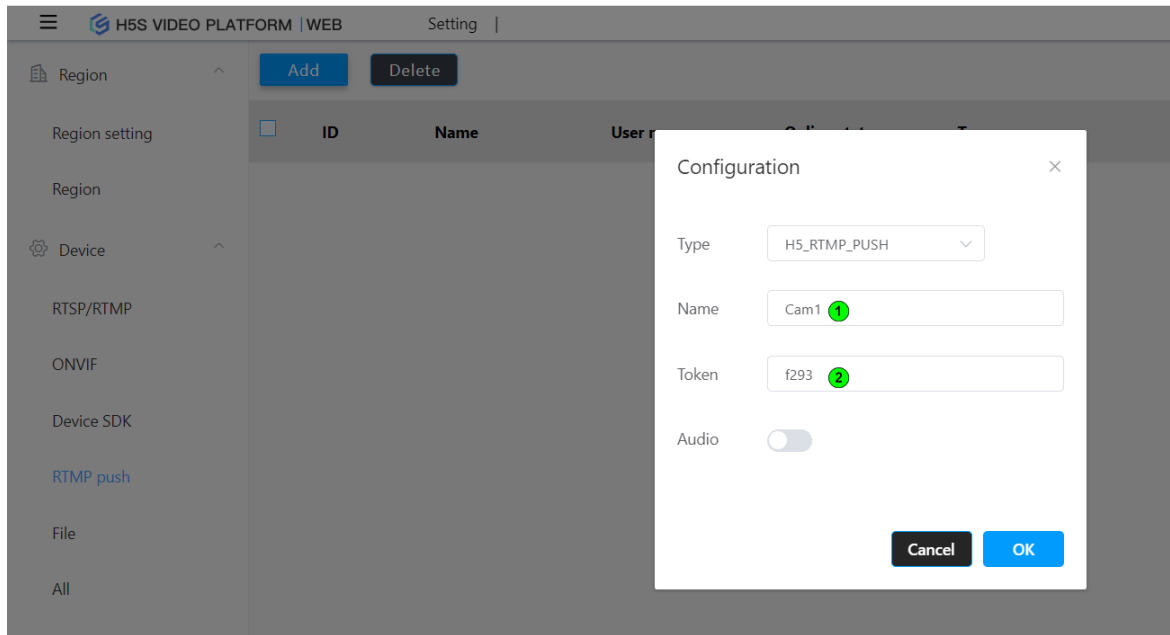
To stream RTMP, you first need to add a token to h5s and then compose an RTMP streaming address.

Adding a good address will generate a streaming address, which is /live/08b2. Combining the RTMP service port in the configuration, you can obtain the streaming address. rtmp://192.168.100.108:8935/live/08b2 where 8935 is the RTMP service port and 192.168.100.108 is the server IP address.

### Add Delete

Add it in **Setting-» Device-» RTMP Streaming**. After adding it, generate an address according to the rules, and then use the streaming device to stream to the address. Refresh the management interface, and when the online status changes to true, you can play the video.

If you need to delete or modify it, you can directly select the device and edit it to delete.



Number	Name	Function
1	Name	
2	Token	

## 5.6 Video single protocol access

### Video single protocol access

If you need to specify a specific protocol for access, use the following command format. The stream parameter controls the playback stream, with main being the main stream and sub being the sub stream.

<http://localhost:8080/ws.html?token=token2&session=4ec4>

<http://localhost:8080/rtc.html?token=token2&session=4ec4>

<http://localhost:8080/ws.html?token=token2&stream=main&session=4ec4>

<http://localhost:8080/rtc.html?token=token2&stream=sub&session=4ec4>

If you need to play automatically, starting from r11.3, ws.html and rtc.html support autoplay, and you can add autoplay=true.

<http://192.168.100.122:8080/rtc.html?token=token1&autoplay=true&session=4ec4>

<http://192.168.100.122:8080/ws.html?token=token1&autoplay=true&session=4ec4>

<http://localhost:8080/rtmp.html?token=token2&session=4ec47>

<http://localhost:8080/rtmp2.html?token=token2&session=4ec47>

---

The token needs to be replaced with the configured token or generated token. If it is an NVR or platform device, you can view the corresponding token in **Setting-» Device-» All**. Alternatively, you can use GetDeviceSrc/GetGbDeviceSrc/GetCloudDeviceSrc to obtain it separately. For specific usage methods, please refer to the API documentation.

If authentication is enabled for the service, you need to obtain a session from the Login API and keep it alive using the Keepalive API (the default timeout is 600 seconds). To add a session to the original address, use the following command format.

<http://192.168.100.145:8080/ws.html?token=1d4f&session=4ec47fb4-a74a-4e02-96a1-369151cfc09>

In the case of configuring a playback code, you can use the playback code instead of the session to play the video. For playback code settings, refer to **Setting-» System-» User-» Play Code**

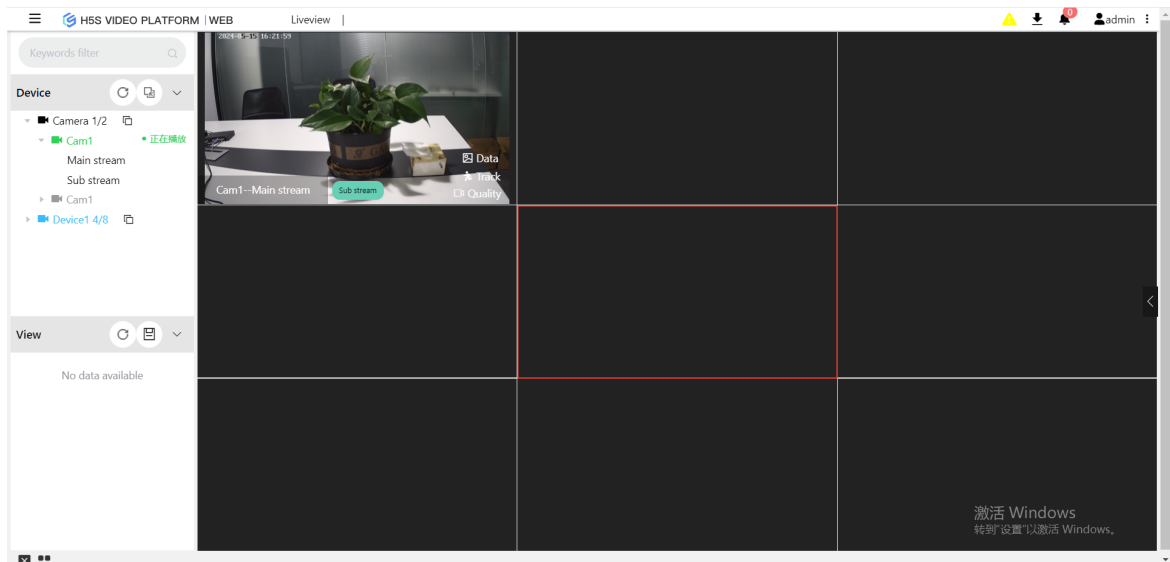
<http://192.168.100.145:8080/ws.html?token=1d4f&session=0031>

## 5.7 Embedded page mode

### Embedded page mode

H5S provides rich interface management functions, which can be easily integrated into third-party systems. You can add "embed=true" to the corresponding interface address to enter the embedded mode. If the server has authentication enabled, you need to add session to the address, such as

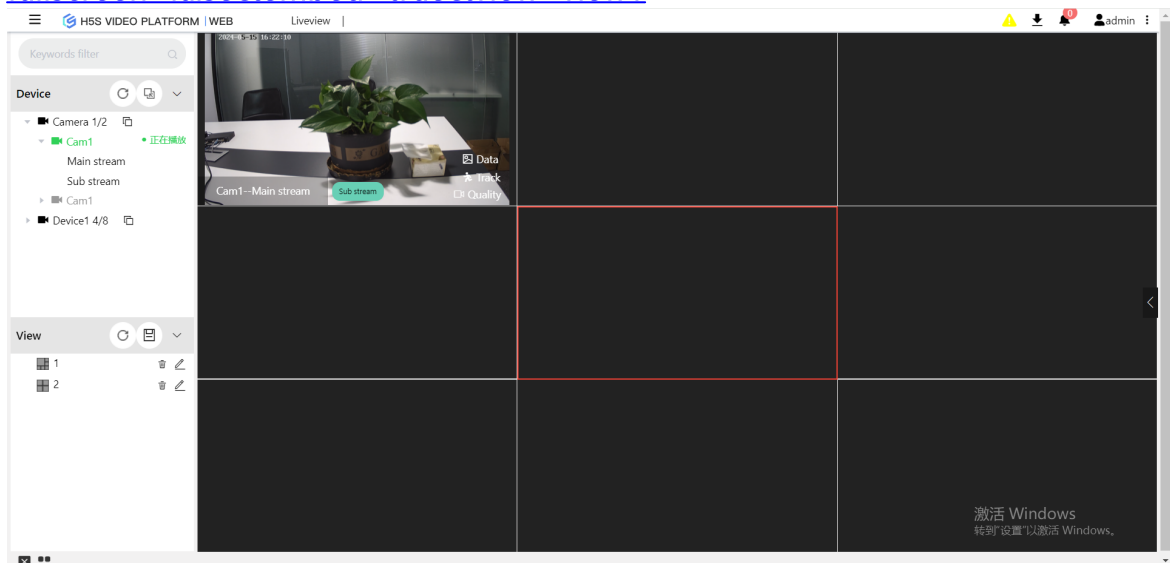
<http://192.168.100.145:8080/#/LiveView?embed=true&session=4ec47fb4-a74a-4e02-96a1-369151cfc09> and <http://192.168.100.158:8080/#/Map?embed=true>



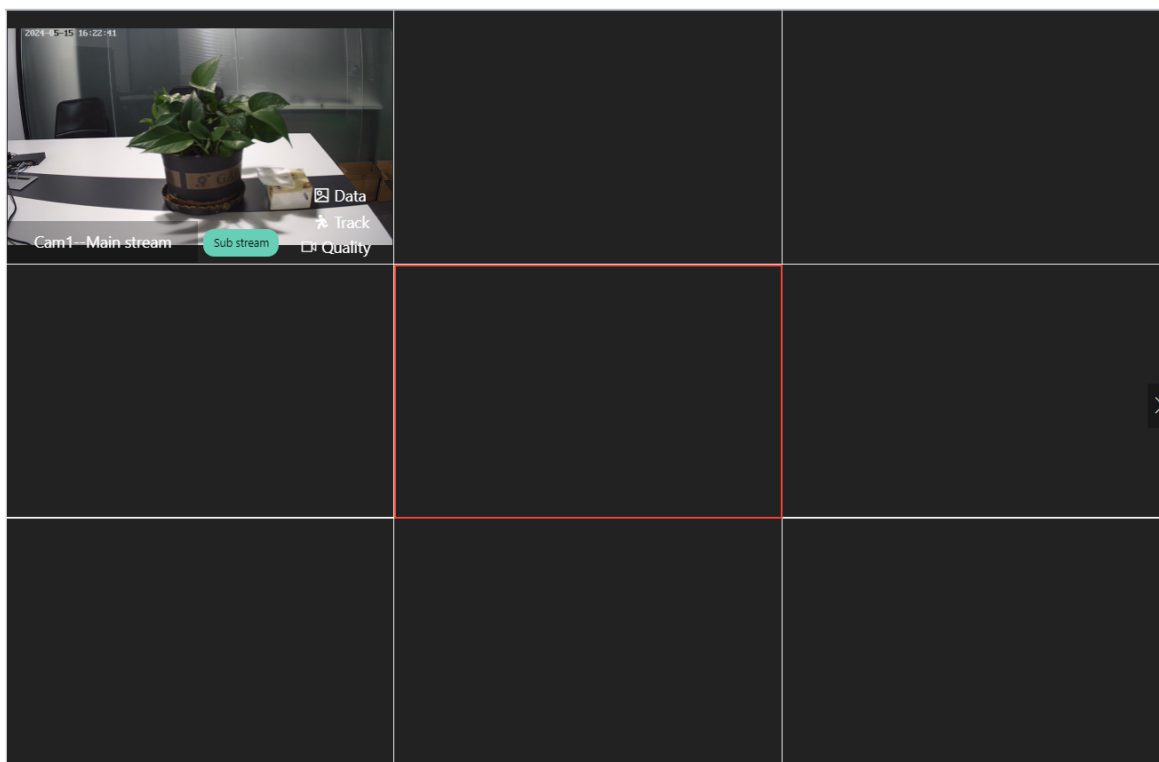
### View-based access

Enter the embedded mode in the real-time video interface, and specify the view to display in the address.

[http://192.168.100.145:8080/#/Liveview?  
fullscreen=false&embed=true&view=view1](http://192.168.100.145:8080/#/Liveview?fullscreen=false&embed=true&view=view1)



You can also set fullscreen to true to enter full screen mode.

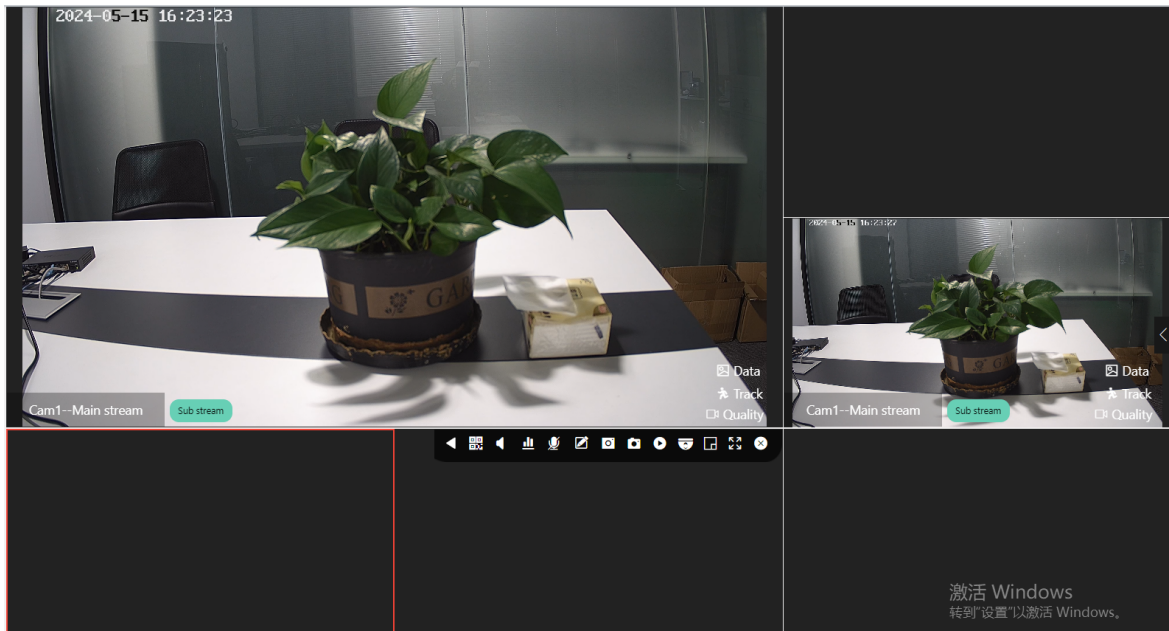


## 5.8 Customize the window pane

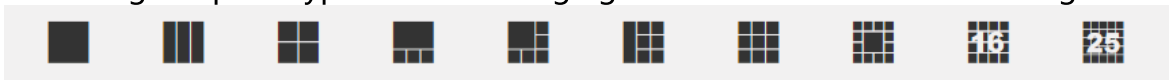
### Customize pane mode

In addition to the embedded mode, H5S also provides a custom pane mode, which can be referenced as follows:

<http://192.168.100.145:8080/#/layout?1=1d4f&3=31a5&type=5&stream=main&ctrl=true&session=4ec47fb4-a74a-4e02-96a1-369151cfcb09>



Where 1, 2, 3, 4, etc. are the corresponding pane numbers (numbered from left to right line by line), followed by the video source token for that pane, with type indicating the pane type. The following figure is numbered from left to right:



The example is the pane type with type=5. The first window plays 1d4f, the third window plays 31a5, and the other 2, 4, 5, and 6 do not play any video. stream=main(stream=sub indicates the auxiliary stream) means that all the videos played are the main stream. ctrl controls whether to display the video control menu.

## 5.9 Device import

### Device import

H5S supports importing device lists from a table. You can download the file template in **Setting-» Device-» Device Import**, modify the template, and then import it into the system.

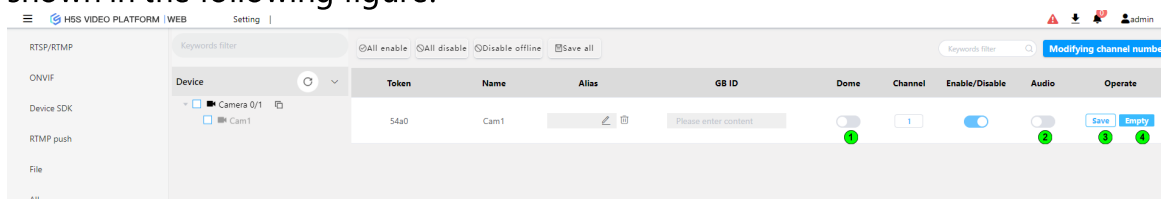
## 5.10 Configuration of monitoring points

### Introduction to configuration of monitoring points

The sources configured into H5S and the sources automatically generated by the device SDK are all monitoring points. All sources are enabled by default, but in some cases, some channels automatically generated by the SDK are not

actually needed. These sources can be disabled in the monitoring point configuration, and the disabled monitoring points do not occupy authorization.

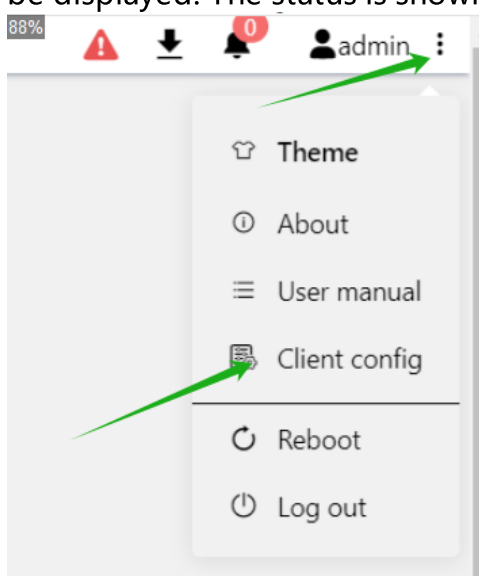
Enter the monitoring point configuration from **Setting-» Camera Points**, as shown in the following figure:



Number	Name	Function
1	Dome	
2	Audio	
3	Save	
4	Empty	

The monitoring point's national standard ID is used for the national standard uplink. The audio on/off setting is used to control the audio function of individual sources. The audio switch configuration is set to "Reserved" and has not yet taken effect. After deletion, the monitoring point configuration will revert to the default, but this configuration will still be present.

The disabled monitoring point will have a horizontal line on the device tree, indicating that the device cannot be operated. You can also turn off the display of disabled nodes by selecting **Client Config**. The disabled nodes will no longer be displayed. The status is shown in the following image:









## 6.Real-time video

---

## 6 Real-time video

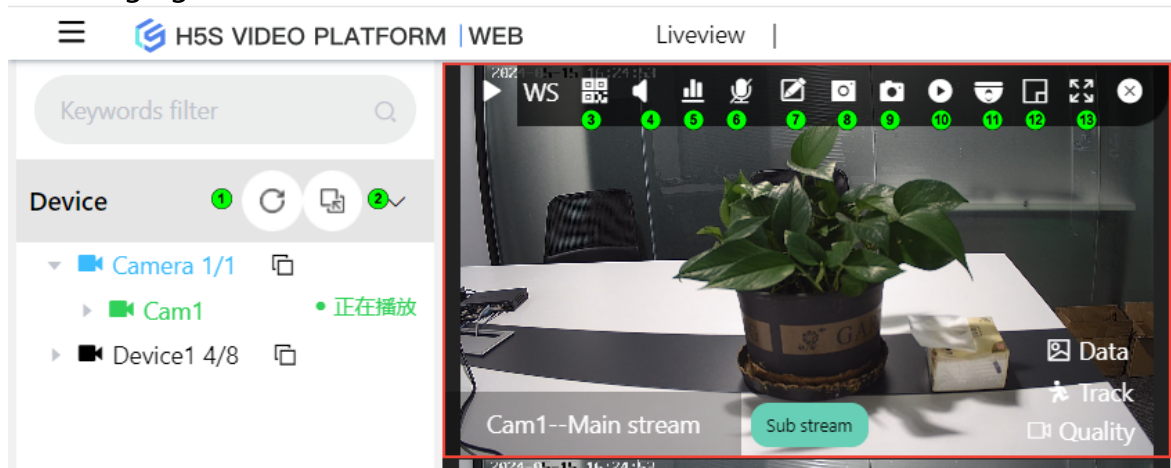
### Real-time video introduction

As introduced in the content overview section, in the H5S system, all clients are based on modern browser technology, so H5S recommends RTC and WS playback technology. H5S supports both RTC and WS technology, and clients can modify the playback method as needed. RTC is mainly used in low-latency intranet environments and has high network requirements; WS is mainly used in complex network environments where special network configurations are not required.

### 6.1 Real-time video operation

#### Real-time video operation

Enter the real-time video interface, and you can click the device to play the video. The menu of the real-time video interface can be referred to in the following figure:

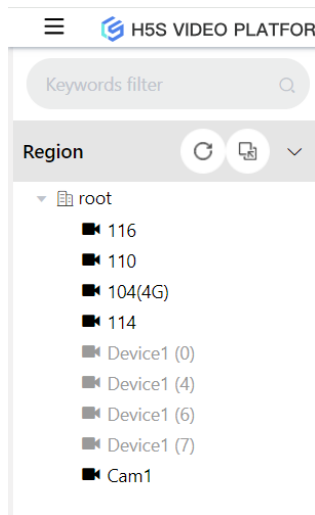


Number	Name	Function
1	Refresh	
2	Switching regions	
3	QR code	
4	Turn on sound	
5	Encoding information	
6	Turn on the microphone	
7	AI annotation	
8	Local capture	

9	Service screenshot	
10	Service video recording	
11	Ptz	
12	Electronic amplification	
13	Full screen	

There are two types of screenshots: one is server-side screenshot, and the other is client-side screenshot. Client-side screenshots are downloaded to the browser, while server-side screenshots are stored on the server.

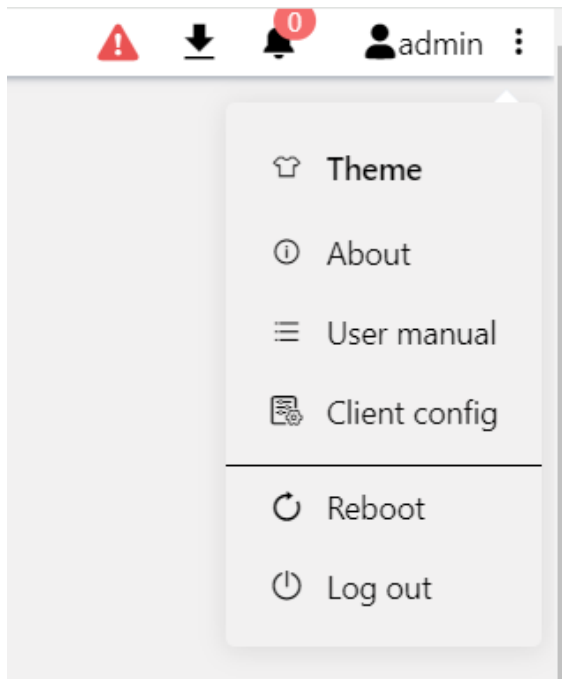
The default view is the device view. You can also click to switch to the area view. After switching, you can refer to the following figure for area device configuration.



## 6.2 RTC WS playback mode

### RTC WS/WS2 playback mode switching

The real-time video playback method can be configured on the client side. Enter the **Client Config** in the upper right corner of the interface.



You can switch between RTC and WS/WS2 playback. RTC and WS2 support playback control, while WS does not. RTC engine can be v1. The playback on the real-time interface after switching will be based on this method. This page can also set watermark.

H5S will automatically detect the decoding types supported by the browser and determine whether to start transcoding. This way, clients don't need to worry about whether a camera supports H264 or H265. It is recommended to use client devices with GPUs as much as possible. This eliminates the need for servers to perform an H265-to-H264 conversion process, significantly saving server CPU resources.

### Client config

Liveview protocol: RTC

RTC

WS2

WS

RTC

Playback protocol: WS2

WS2

H264 CPU decode:

Watermark

Watermark

Enable watermark

Disable watermark

RTC engine

v1

Display disable

Show

Hide

Image quality selection

Show

Hide

WS decoder: H264 H265

RTC decoder: H264 H265

Aspect ratio:

Video background color

Black

Cancel

Save

Chrome supports H265 GPU decoding in WS and WS2 modes starting from version 105, and Chrome supports RTC H265 decoding starting from version 127. This eliminates the need for servers to transcode H265. If Chrome supports it, the WS decoder will appear as H265 in client configuration. If the browser is configured with NVIDIA, it generally supports H265. Intel integrated graphics requires a CPU from the Intel Core series of generation 12 or later. If H265 decoding is supported, it will be displayed in the WS decoder.

The Chrome RTC H265 decoding function is disabled by default. You need to add the `--enable-features=WebRtcAllowH265Receive --force-fieldtrials=WebRTC-Video-H26xPacketBuffer/Enabled` startup parameters.

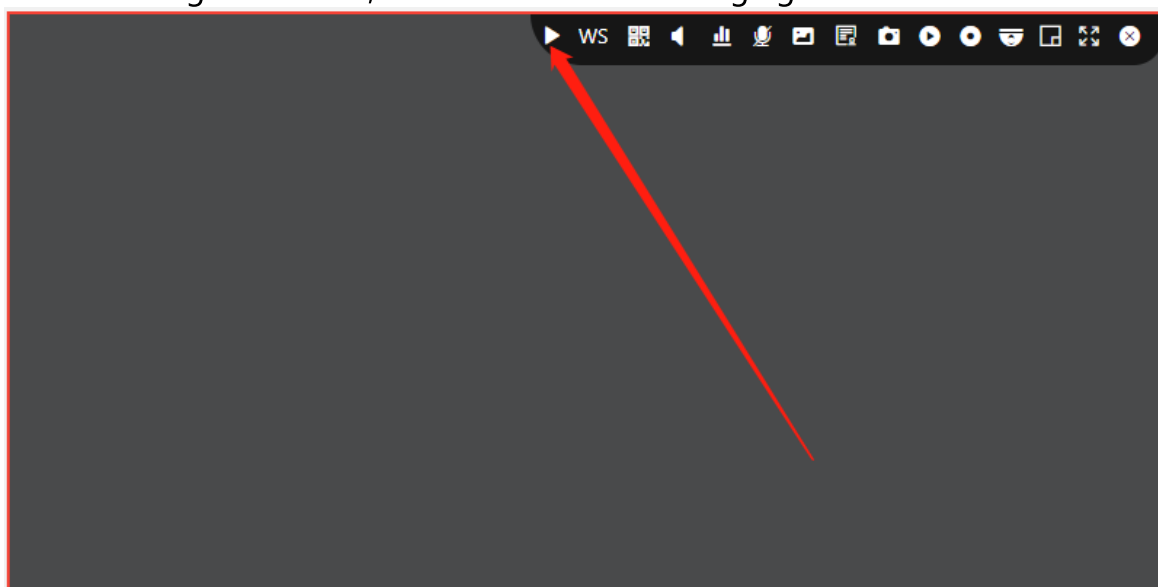
---

Take Windows as an example, open cmd.exe  
cd C:\Program Files\Google\Chrome\Application  
chrome.exe --enable-features=WebRtcAllowH265Receive --force-fieldtrials=WebRTC-Video-H26xPacketBuffer/Enabled

After starting in this way, the RTC decoder will contain H265.

The "Display Disabled" option indicates whether the device tree displays disabled devices, the "Image Quality Selection" option indicates whether the real-time image displays buttons for image quality selection, and the "AI Display" option indicates whether the AI analysis results are displayed on the real-time image.

Click the leftmost button in the playback interface to view whether the current mode is using WS or RTC, as shown in the following figure:

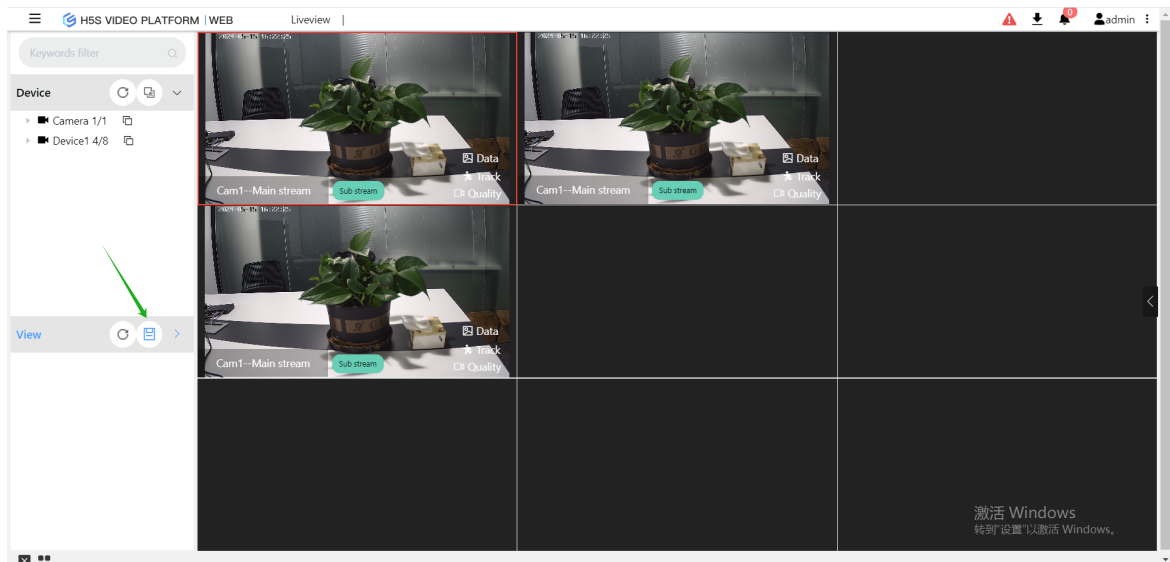


## 6.3 View operations

### View operations

During the live video playback, you can save the current playback view, add, delete, and modify views. The following interface can be used for reference:



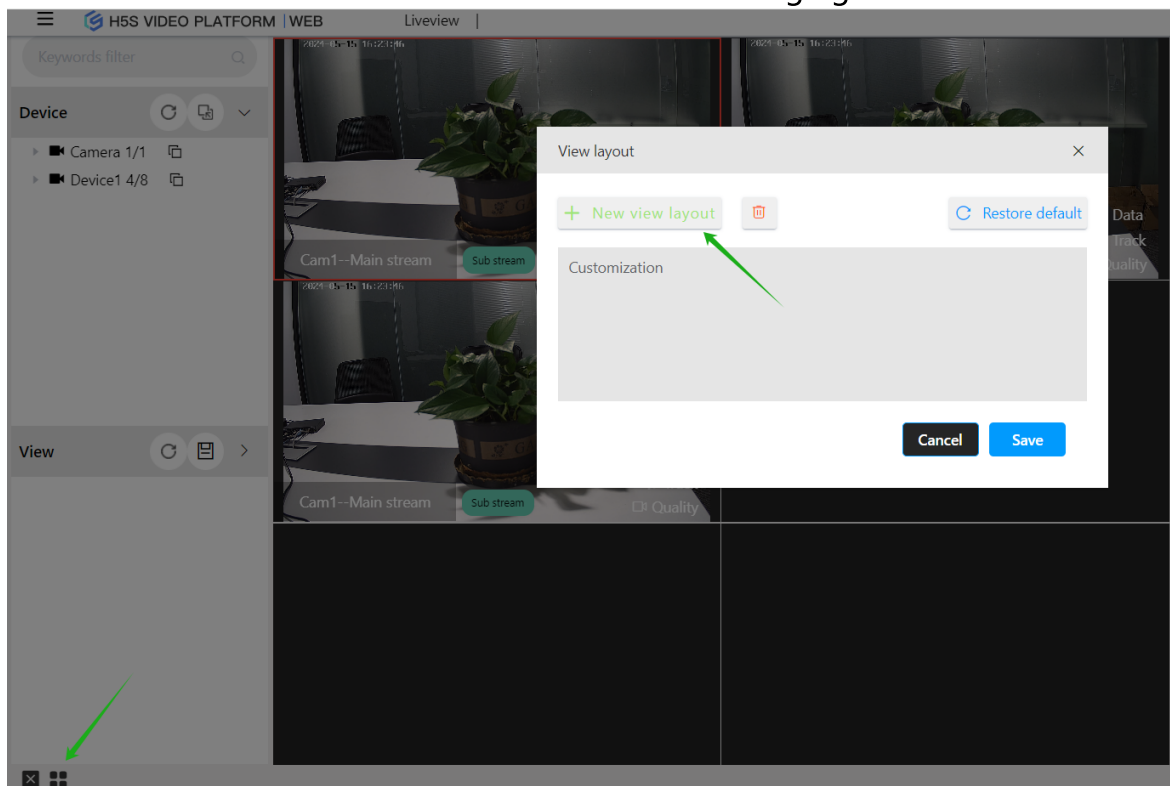


You can click the view to switch. The configured view is also patrolled by view in the video patrol.

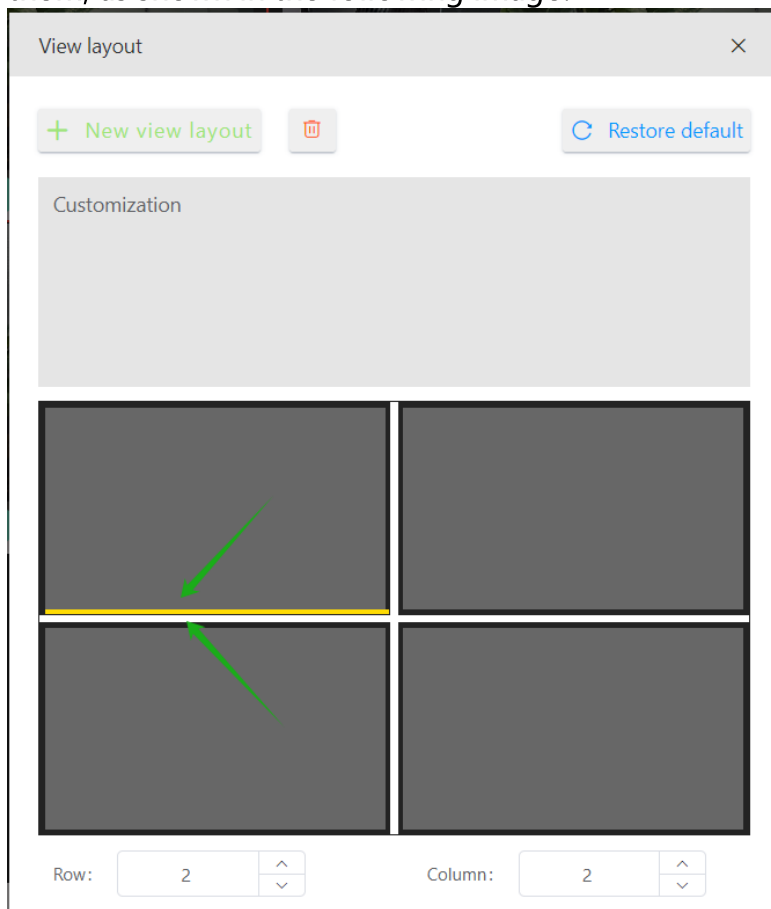
## 6.4 View Layout

### View Layout

Starting from r17, the Web interface supports custom view layouts, which can be customized as needed. Please refer to the following figure for reference:



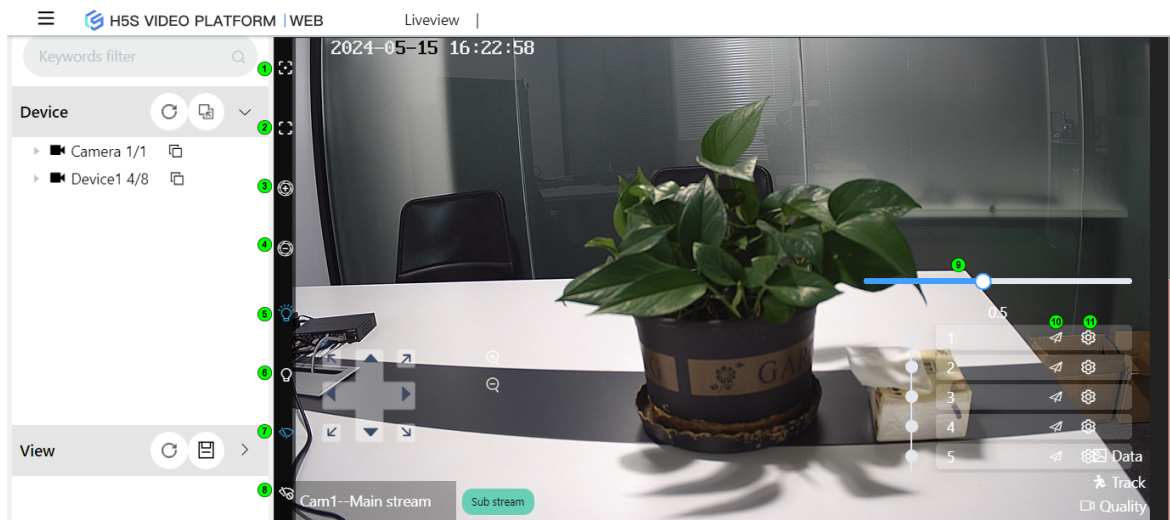
When merging the grids, you can click on the adjacent yellow lines to merge them, as shown in the following image:



## 6.5 Pan tilt control

### Pan tilt control

The pan-tilt control supports most of the pan-tilt operations, but the light wiper only supports Hikvision SDK access. Please refer to the following figure:



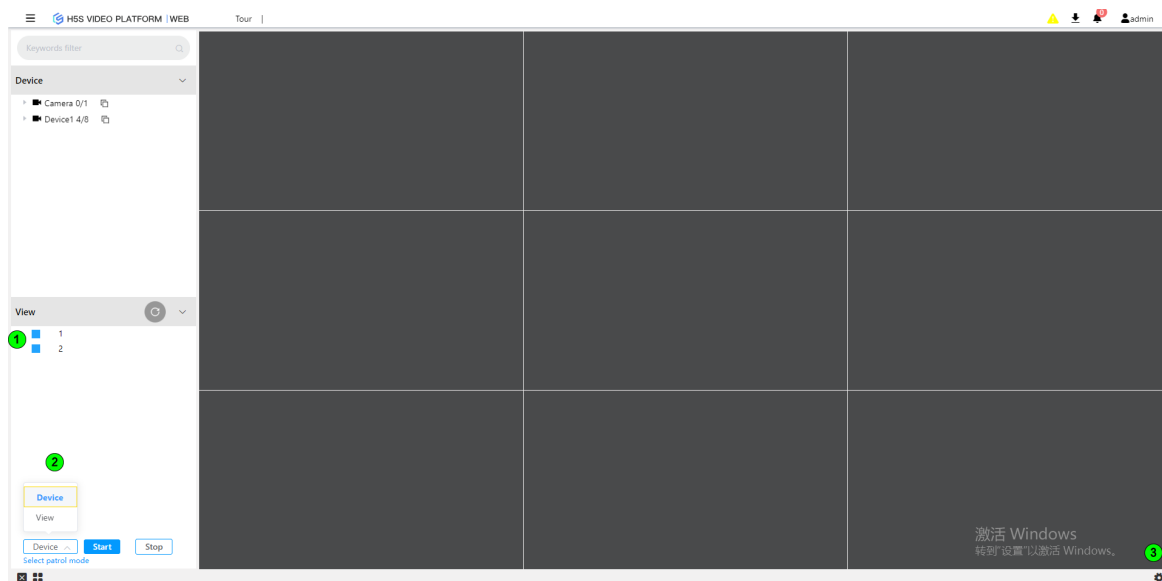
\*By default, only 5 preset positions are displayed. You can modify the interface code to increase the number of preset positions according to your needs.

Number	Name	Function
1	Zoom in and focus	
2	Reduce focus	
3	Enlarge aperture	
4	Reduce aperture	
5	Light on	
6	Light off	
7	Windshield wipers on	
8	Wiper off	
9	Pan tilt speed	
10	Call preset position	
11	Set the preset position	

## 6.6 Video patrol

### Video patrol

Patrol can be performed according to all devices or selected views. The configuration can be referred to the following figure:



Number	Name	Function
1	View	
2	Select patrol mode	
3	Set up	

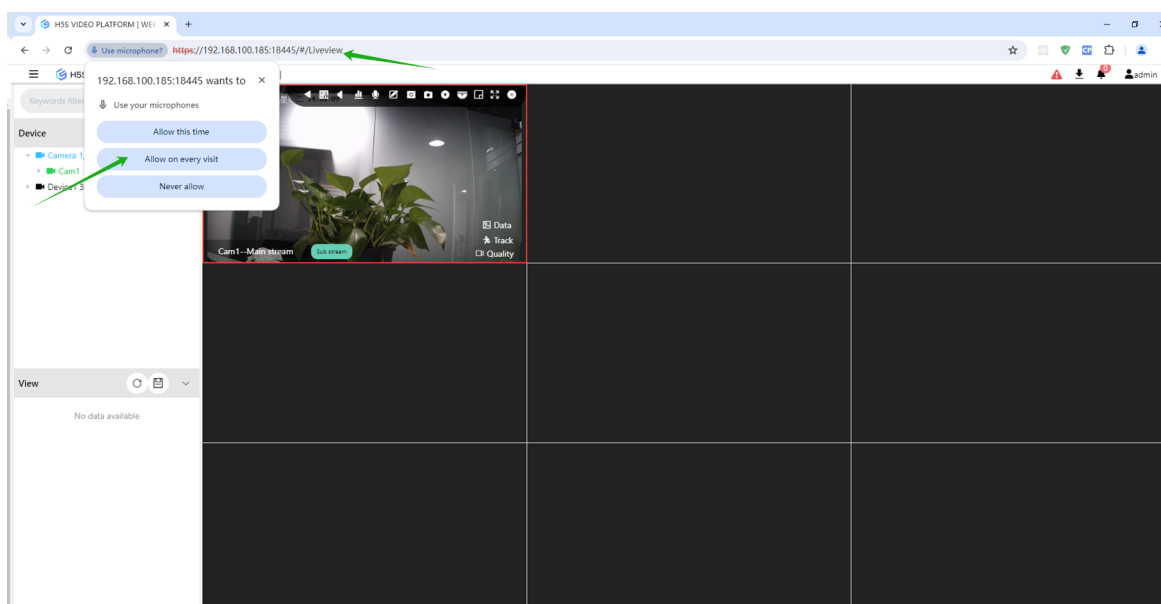
## 6.7 Voice intercom

### Voice intercom

H5S supports camera intercom and supports all cameras added by Hikvision SDK or access control devices with video functions.

Voice intercom requires HTTPS access to the server, with an address such as <https://192.168.100.158:8443/#/Liveview>.

You can refer to the following figure:

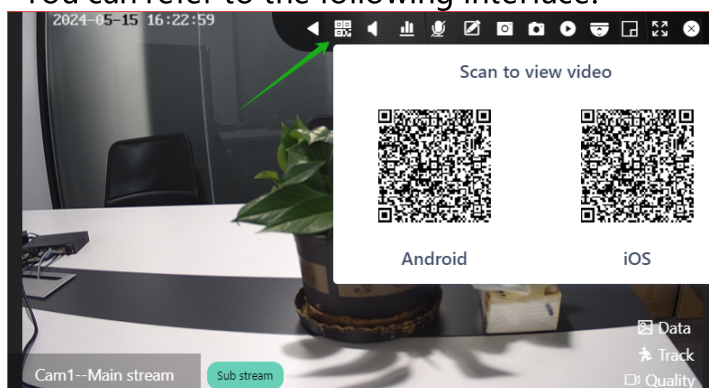


## 6.8 Scan and play

### Scan and play

H5S supports the mainstream HTML5 low-latency video playback technology, so it supports WeChat and Alipay. Click the QR code in the video playback interface to scan with WeChat and Alipay respectively (due to the older Android browser kernel of Alipay, Android Alipay is not supported for the time being).

You can refer to the following interface:



After scanning, the following interface will appear. Click the video playback button to play the video. You can also click the pan-tilt button to operate the pan-tilt function.

The screenshot is captured on the server side, and you can search and view the corresponding image on H5SWeb.

Start to start server video recording, stop to stop server video recording, and search and replay corresponding videos on H5SWeb.



## 7.Playback video

---

## 7 Playback video

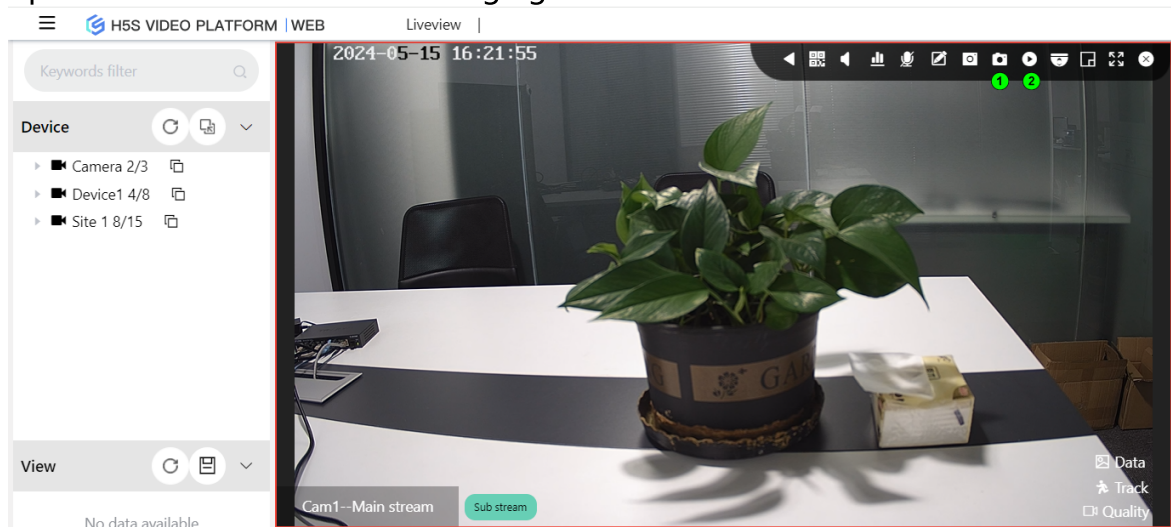
### Introduction to playback video

Due to the need for control support during playback, the playback video section uses RTC technology. If you cannot see the video during playback, please refer to the WEBRTC section configuration.

Video storage is divided into two cases: H5S storage and NVR or third-party platform storage. H5S playback and playback refer to video storage on H5S, while device playback and archiving refer to NVR or third-party platform storage.

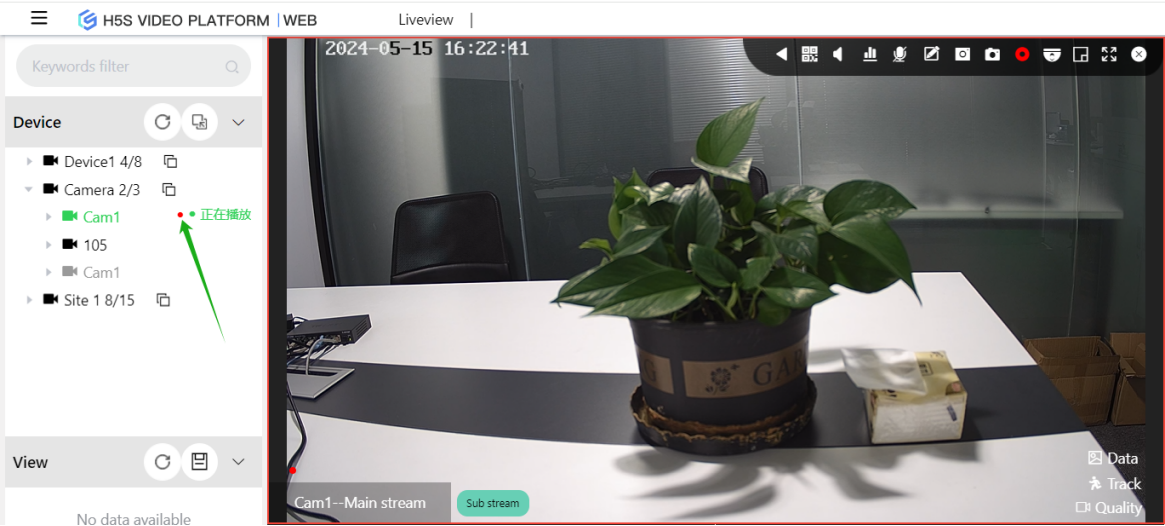
Capturing images refers to H5S capturing images.

If you need to store or capture images on H5S, you can refer to the control operations shown in the following figure:



After starting manual video recording, it will continue to cycle through the recording. If you do not need to record, you can manually stop it. After starting video recording, the device tree will display a prompt, as shown in the following image:





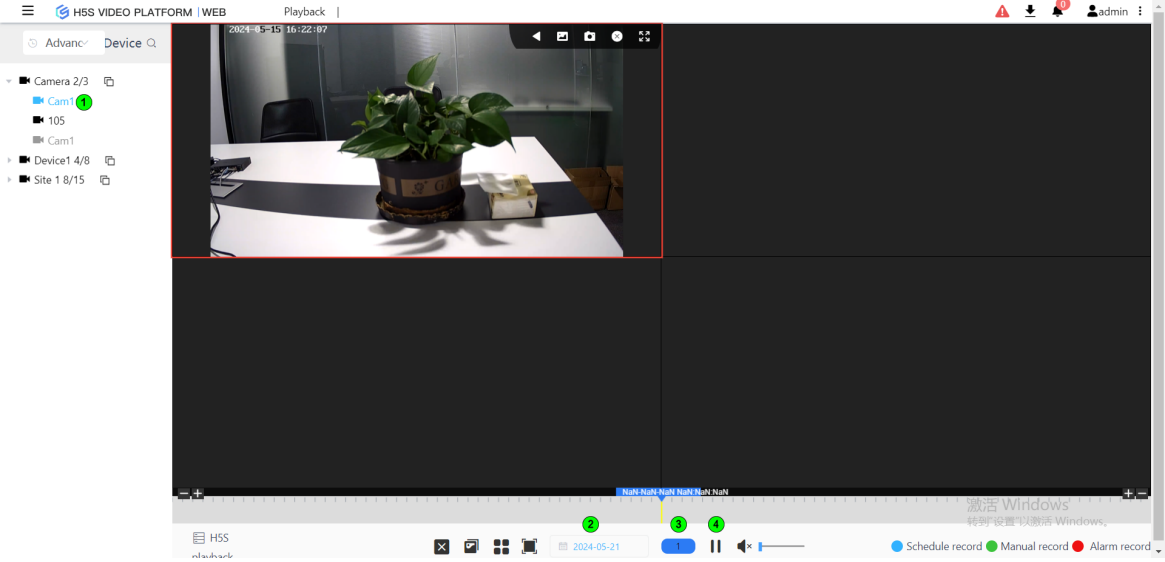
## 7.1 Advanced replay

### Introduction to advanced playback

Advanced playback supports remote storage and service storage. Remote storage is playback from the device, and service storage is playback from H5S.

### Advanced playback operation

Advanced playback is a timeline-based playback mode that allows you to drag the timeline to select, as well as select the date and speed of the video. You can pause and play during playback.



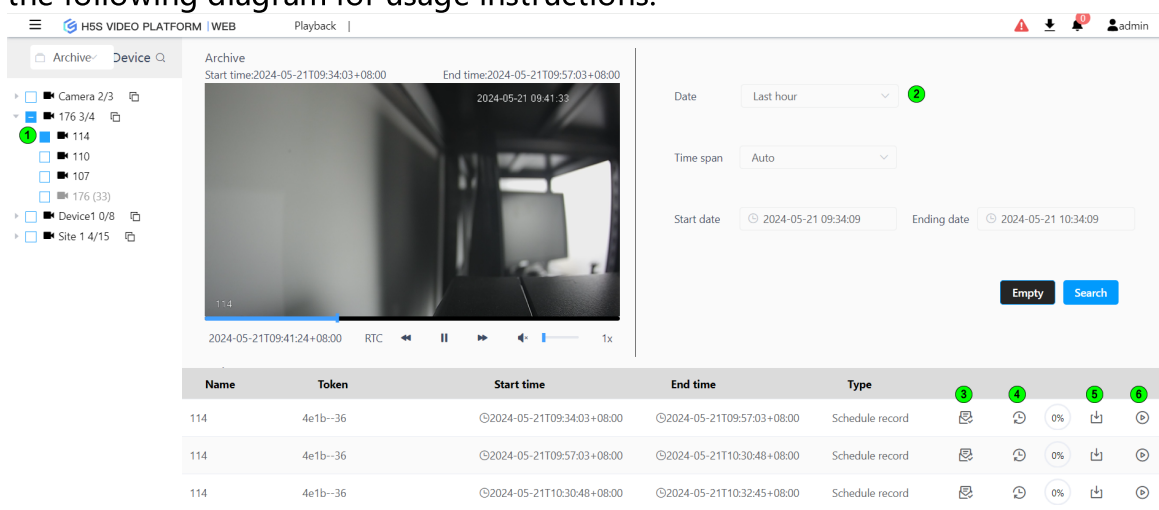
Number	Name	Function
--------	------	----------

1	Cam1	
2	Date	
3	Double speed	
4	Play pause	

## 7.2 File

### File

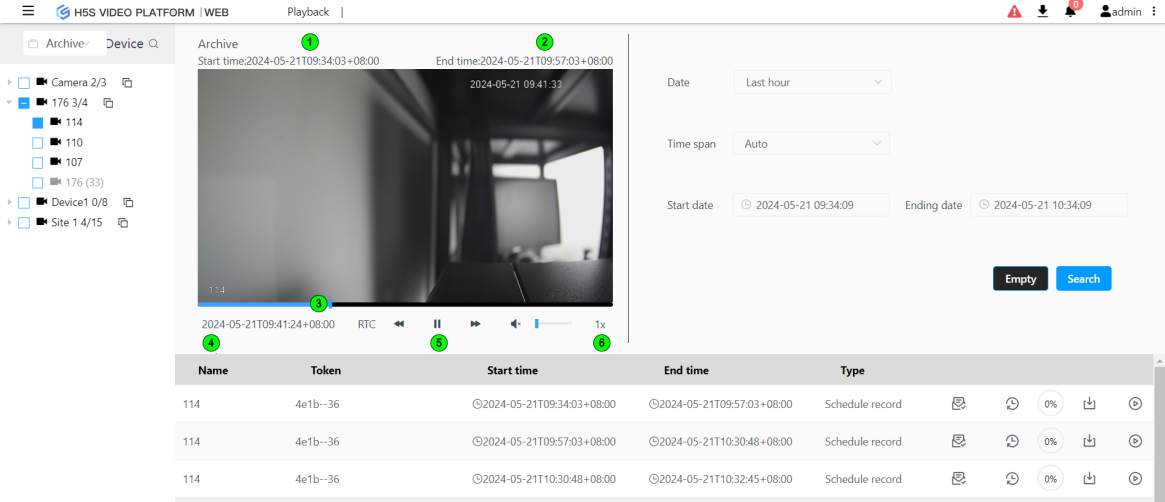
Archiving is the playback of video recordings from NVRs or platforms connected to H5S, and the objects of operation require device SDK access (including NVRs and third-party platforms) or national standard access. Refer to the following diagram for usage instructions:



Number	Name	Function
1	Camera	
2	Date	
3	File	
4	Refresh	
5	Download	
6	Online playback	

Since the video is stored on the device, you need to click Start Archiving, Start Refreshing, and then wait until the progress reaches 100% before downloading. The progress can be queried through the GetArchiveStatus API.

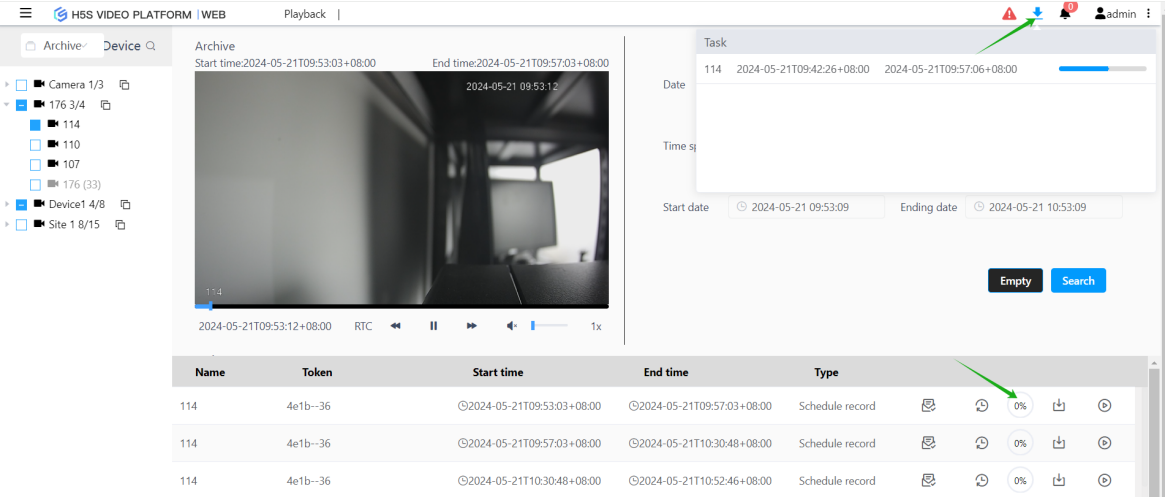
If you want to play back the video directly, you can click the playback button to play back the video. Note that video playback does not require archiving. The video playback operation can be referred to in the following figure:



Number	Name	Function
1	start time	
2	End time	
3	Time progress bar	
4	Current playback time	
5	Play pause	
6	Double speed	

Archiving Status

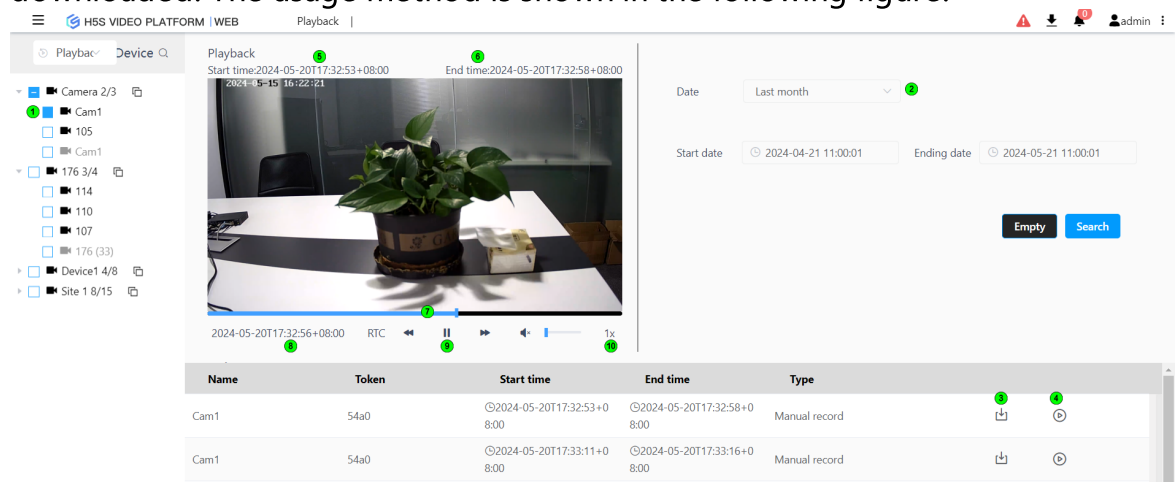
Starting from r17, the interface displays tasks that are being archived, as shown in the following figure:



## 7.3 Playback

### Playback

Playback is to play back the data of H5S video, which can be played directly or downloaded. The usage method is shown in the following figure:

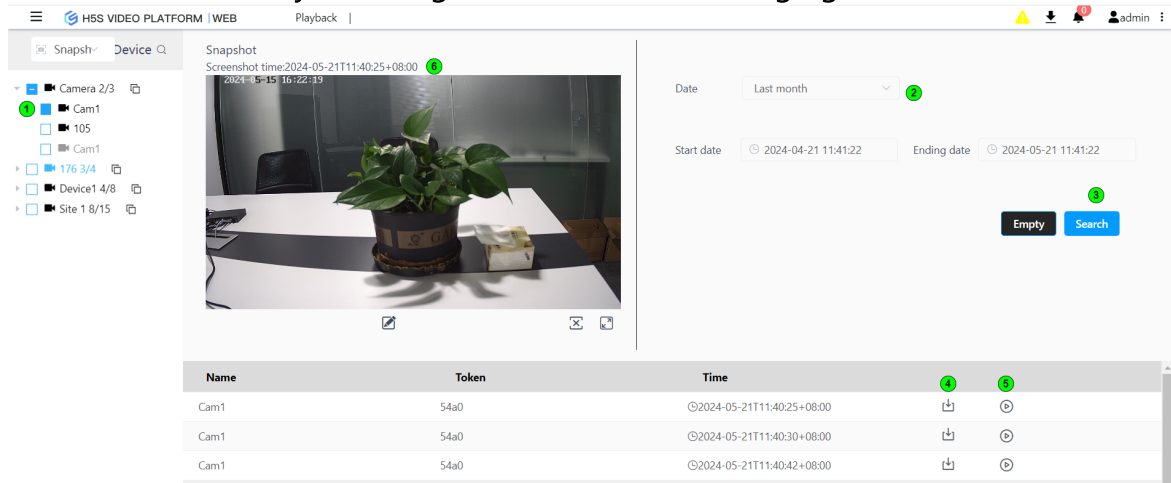


Number	Name	Function
1	Cam1	
2	Date	
3	Download	
4	Online playback	
5	Start time	
6	End time	
7	Time progress bar	
8	Rewind to the current time	
9	Play pause	
10	Double speed	

## 7.4 Screenshot

### Screenshot

The screenshot is a picture captured on H5S, which can be previewed or downloaded directly. For usage, refer to the following figure:

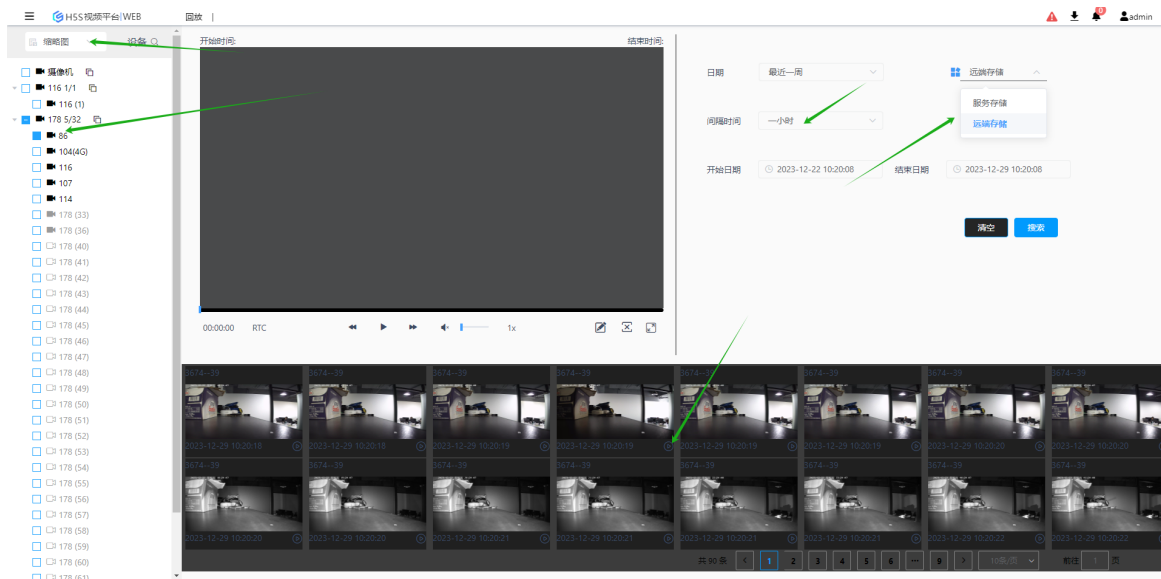


Number	Name	Function
1	Camera	
2	Date	
3	Search	
4	Download	
5	Online playback	
6	Capture time	

## 7.5 Thumbnail

### Thumbnail

Thumbnails are images captured at specific points in time within a video for preview purposes. Currently, the new Hikvision NVR or H5S server video recorded by the Hikvision SDK supports the thumbnail function, with a time interval corresponding to the screenshot time interval. Clicking on the image will play the corresponding video. For usage instructions, refer to the following image:

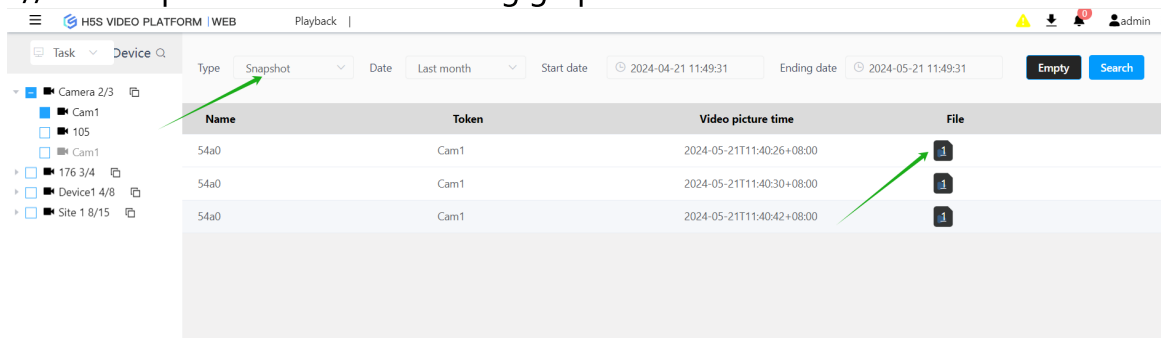


## 7.6 Task

### Search for screenshot tasks

The status of user screenshots can be searched in tasks. For usage, refer to the following figure:

//TODO update the status-bearing graph.



### Search for archiving tasks

The status of the user's archived videos can be searched in the task, and the tags 1, 2, and so on are the archived segmented files.

//TODO update the status map.

Task

Device

Camera 2/3

176 3/4

114

110

107

176 (33)

Device1 3/8

Site 1 5/15

Type

Archive

Date

Last month

Start date

2024-04-21 13:42:44

Ending date

2024-05-21 13:42:44

Empty

Search

Name	Token	Record start time	Record end time	File
4e1b--36	114	2024-05-21T09:42:26+08:00	2024-05-21T09:57:06+08:00	1
4e1b--36	114	2024-05-21T09:53:00+08:00	2024-05-21T09:57:06+08:00	1
4e1b--36	114	2024-04-29T03:14:28+08:00	2024-04-29T03:48:22+08:00	1





## 8.Emap

---

## 8 Emap

### 8.1 Map configuration

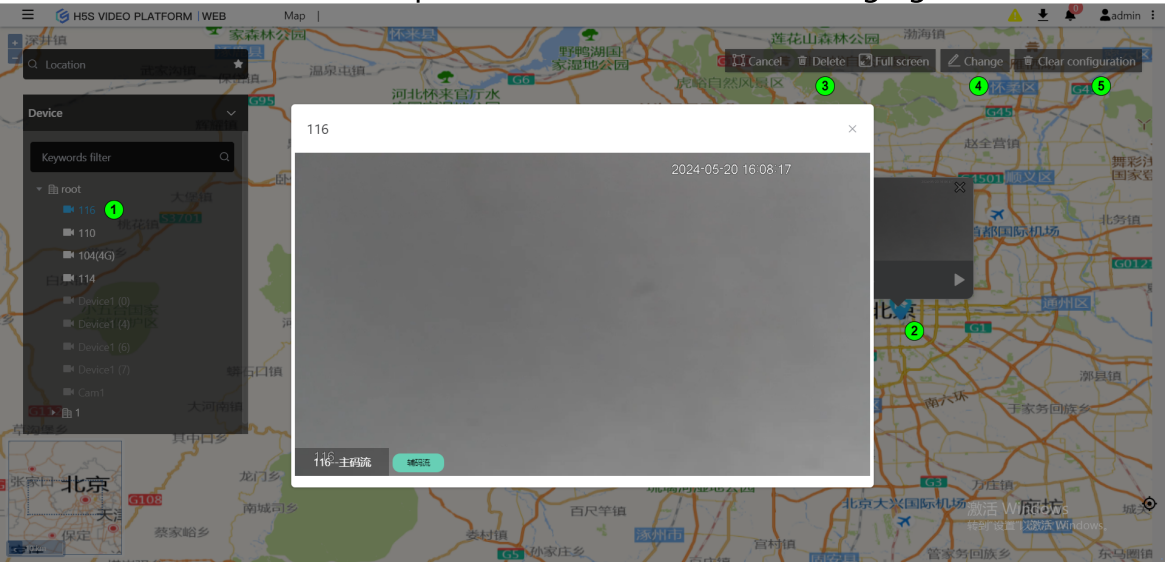
#### Map configuration

H5S supports Gaode Map and Google Map. You can select Gaode Map and Google Map in **Setting-》Map-》Map Setting**. The system default is Gaode Map.

### 8.2 Map operation

#### Map operation

Map operation is based on area view. You can first configure cameras in the area, click on the camera, and then click on the corresponding point on the map to add the camera to the map. You can refer to the following figure:



Number	Name	Function
1	Root	
2	Monitoring points	
3	Delete	
4	Change	
5	Clear configuration	

Modifying the view can modify the default map location loaded by the map, and clearing the configuration can clear the cameras added to the map.

To delete a camera, first select the corresponding camera by clicking on it, then click on the map and release the mouse after selecting the corresponding

camera. Finally, click on Delete. You can refer to the following image for operation:





## 9.Region management

---

## 9 Region management

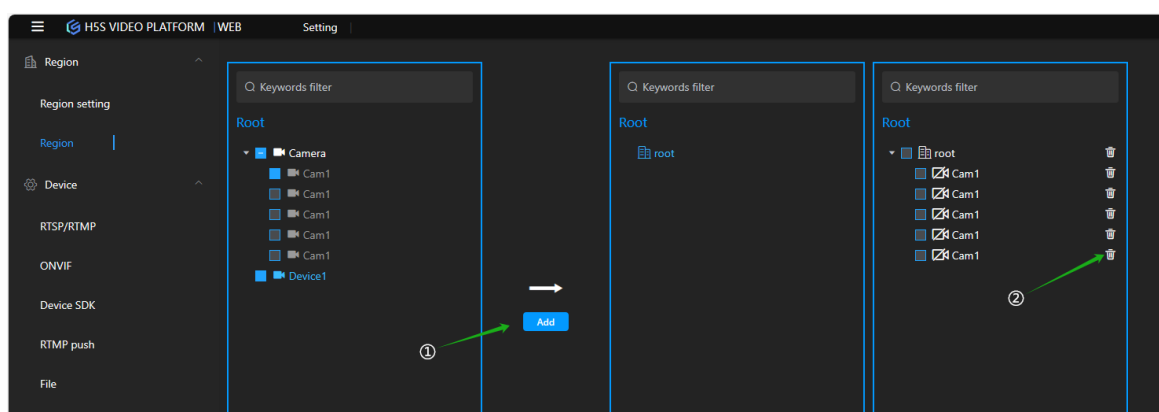
### Introduction to region management

Area management provides a method for reorganizing cameras, adding and deleting areas, and assigning cameras to areas.

### 9.1 Add and delete regions

#### Add and delete regions

You can perform the operation of **Setting-» Region-» Delete/Add Region**. For specific usage, please refer to the following figure:

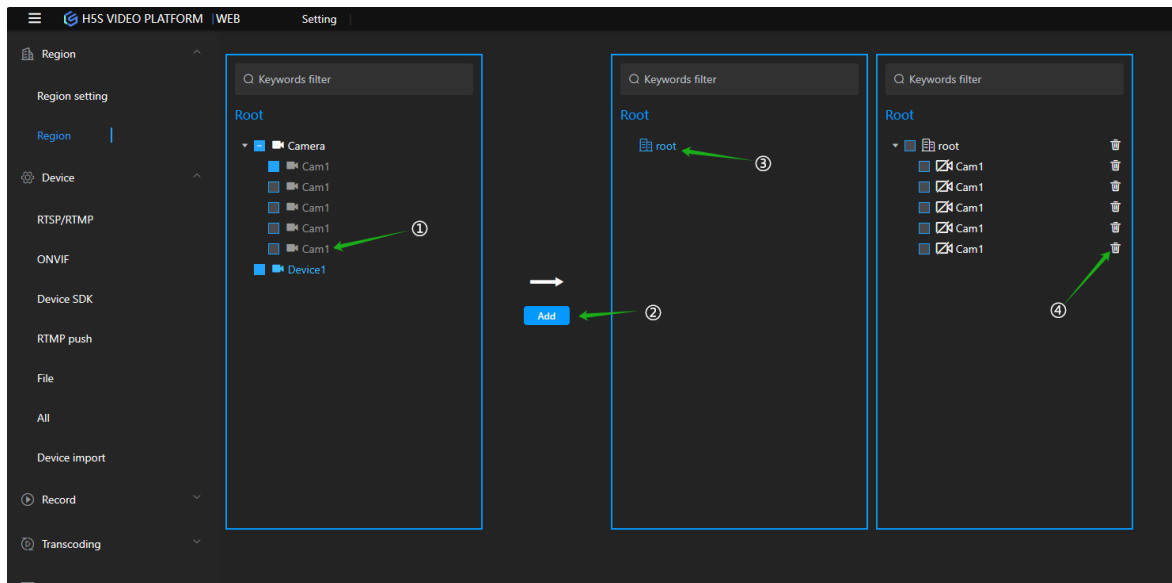


Number	Name	Function
1	Add	
2	Delete	

### 9.2 Regional resource allocation

#### Regional resource allocation

You can go to **Setting-» Region-» Region** and select the camera and area. Then you can add the selected camera to the selected area. For specific usage, refer to the following image:



Number	Name	Function
1	Cam1	
2	Add	
3	root	
4	Delete	





## 10. User management

---

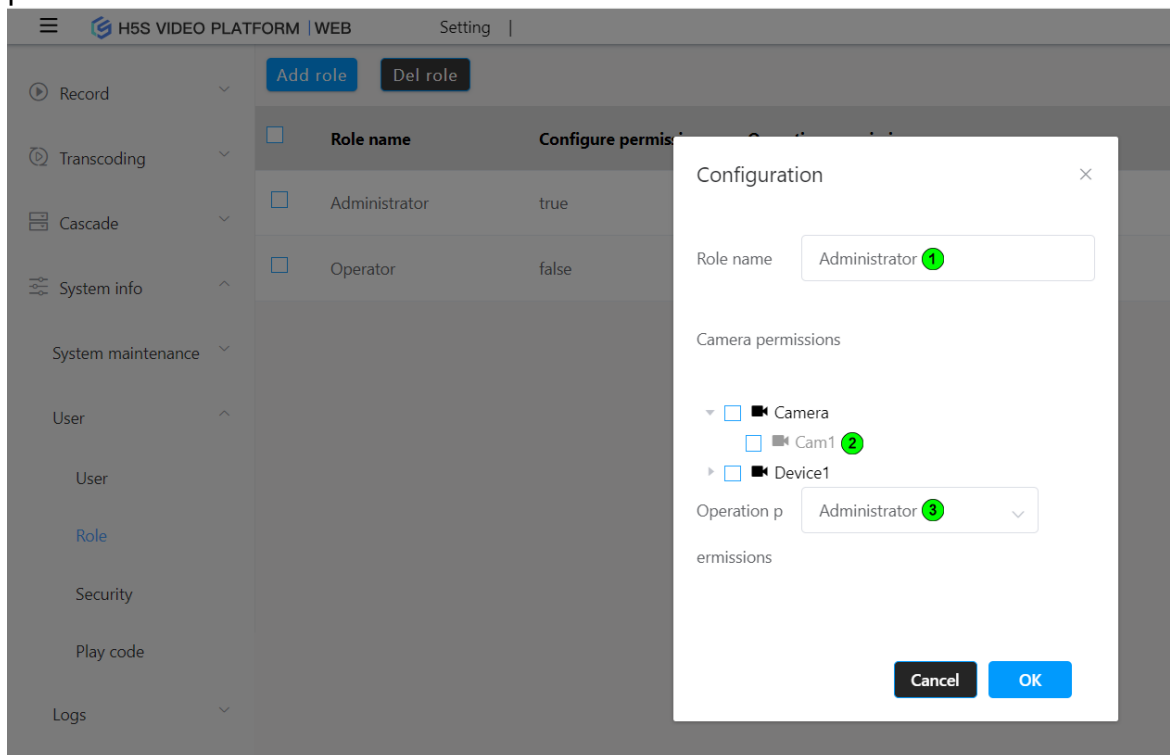
## 10 User management

### 10.1 Role management

#### Role management

In **Setting-» Systeminfo-» User-» Role** , add and delete roles. The system has two default roles: Administrator and Operator. The Administrator has the highest permissions (the administrator role cannot be deleted), while the Operator only has operational permissions. There are two types of roles: Administrator and Operator. The Administrator type is an administrator, while the Operator type is an operator.

If the type or operation permission is Administrator, it has the default permission to access all cameras.



Number	Name	Function
1	Role name	
2	Cam1	
3	Operation Permissions	

## 10.2 User management

### User management

In the **Setting-» Systeminfo-» User User**. From there, you can add or delete users. The default username is "admin" and the default password is "12345". Starting from version 14.15, the default password has been changed to "Vision@168".

The screenshot displays the 'H5S VIDEO PLATFORM | WEB' interface with the 'Setting' menu open. The 'User' section is selected, showing a list of users with 'admin' highlighted. An 'Add user' dialog box is open, featuring the following fields and options:

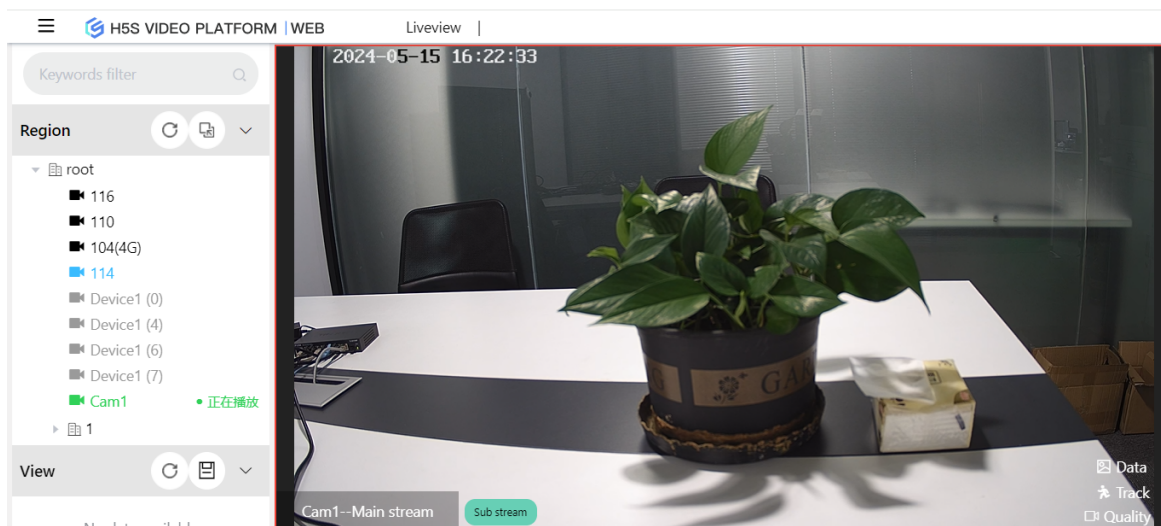
- User name:** A text input field containing 'Operator'.
- New password:** A password input field with masked characters '.....' and a visibility toggle icon.
- Confirm password:** A password input field with masked characters '.....' and a visibility toggle icon.
- Role:** A dropdown menu currently set to 'Administrator'.

Below the password fields, a security notice states: 'To improve your password security, it is recommended to use the following:' followed by a list of requirements:

- Password length should be at least 8 characters
- The password must contain at least one uppercase letter.
- The password must contain at least one lowercase letter.
- The password must contain at least one number.
- The password must contain at least one special character. for example, @ # &, etc.
- The password cannot have two consecutive increasing or decreasing numbers. For example, 12 321 5678, etc.
- The password cannot contain the username.

At the bottom right of the dialog box are 'Cancel' and 'OK' buttons.

If the user is not an administrator role, they can only see the assigned cameras in the area after logging in.

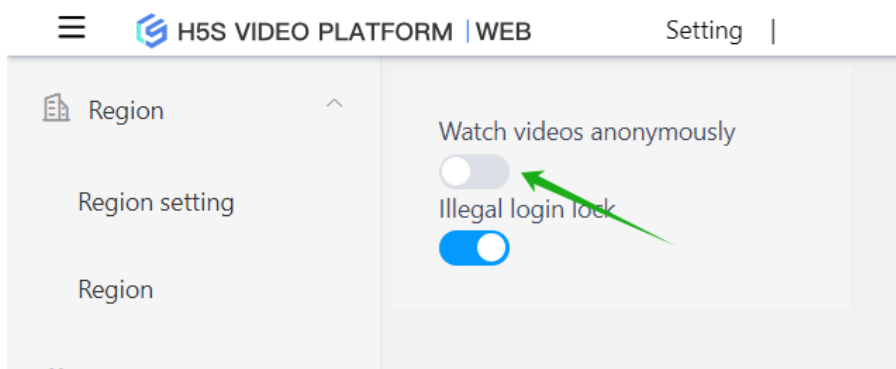


The password in the configuration file is MD5-hashed. The default password is 12345. If you need to change the password, you also need to regenerate the MD5 digest. You can use [www/tool.html](http://www/tool.html) to generate the MD5 digest.

## 10.3 Security management

### Security management

If you are using an older version, H5S allows anonymous browsing of videos by default. Since 14.15, H5S has disabled anonymous browsing by default. To enable or disable anonymous browsing by default, go to **Setting-» Systeminfo-» User-» Security**. Please disable anonymous browsing in production environments.



You can also enable the illegal login lockout in the above interface.

## 10.4 Play Code

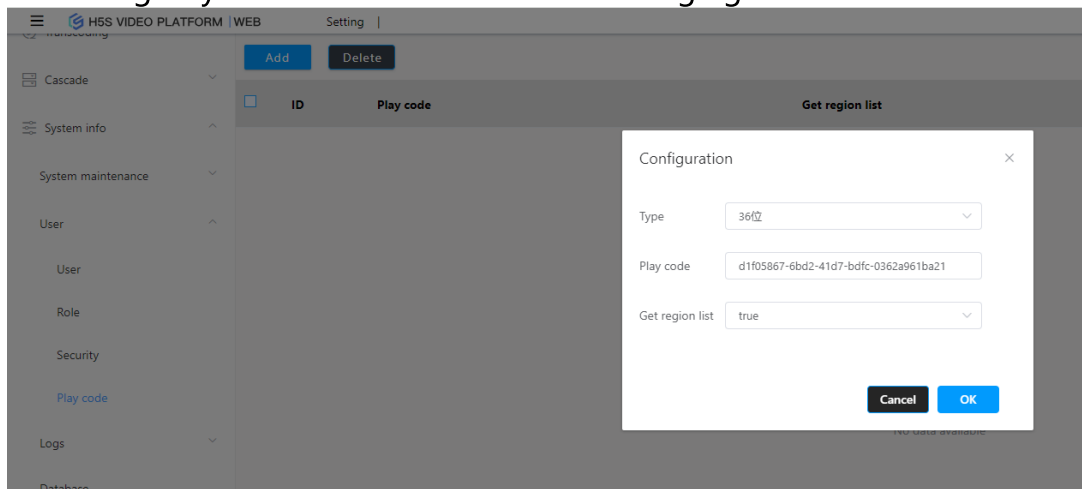
### Play Code

Starting from version 14.19, H5S supports playback codes. You can add or delete playback codes on the H5S video platform. Playback codes can be used to play videos instead of sessions. Playback codes can be considered as fixed sessions, but their permissions are limited. Playback codes can only access the following APIs.

Name	Path	Describe
RTSP/RTMP video forwarding		Forwarding part of reference standard protocol
WS/RTC video real-time and playback	/api/v1/h5swsapi /api/v1/h5srtcapi	
Screenshot	/api/v1/Snapshot	
Playback screenshot	/api/v1/PbSnapshot	
Start manual video recording	/api/v1/ManualRecordStart	
Stop manual video recording	/api/v1/ManualRecordStop	
File	/api/v1/Archive	
Archive screenshots	/api/v1/ArchiveSnapshot	
Get archive status	/api/v1/GetArchiveStatus	
Search for service videos	/api/v1/Search	
Search remote video	/api/v1/SearchDeviceRecordByTime	
Pan tilt control	/api/v1/Ptz	
Set the preset position	/api/v1/SetPreset	
Delete preset position	/api/v1/DelPreset	
Obtain the preset position list	/api/v1/GetPresets	
Acquire the video source cache data frame	/api/v1/GetImage	

Get the loaded image	/api/v1/GetLoadingImage	
Get the list of regions	/api/v1/GetRegion	You need to specify whether you have permission to obtain the region list when adding the playback code; the default region is empty and you need to manually add devices

Enter **Setting-» Systeminfo-» User-» Play Code** to add and delete play codes. You can specify whether the play code has permission to obtain a region list. There are 4-digit and 36-digit modes for play codes, which can be selected according to your needs. Refer to the following figure:



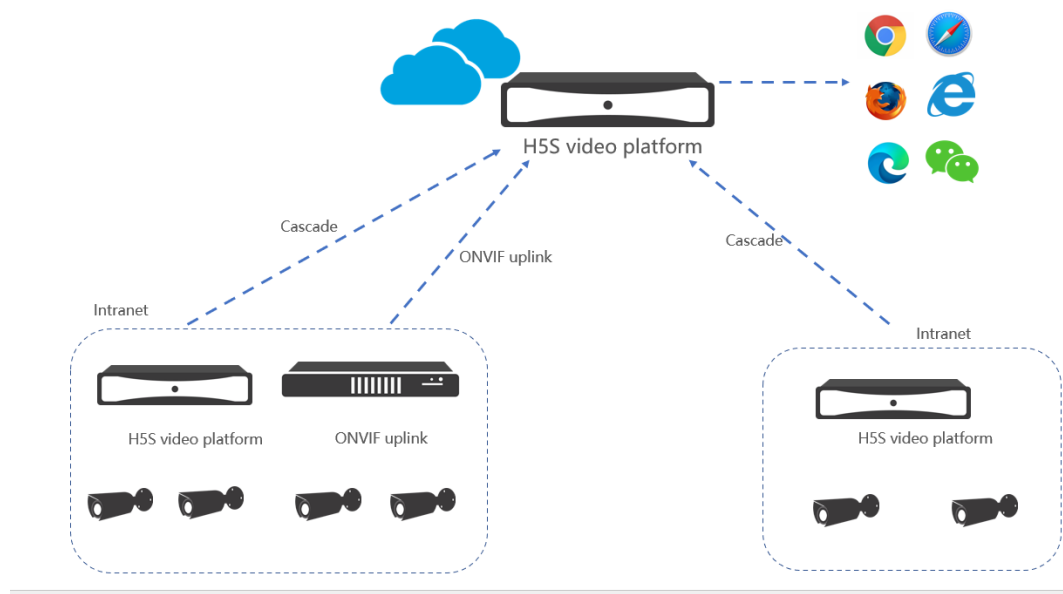
# 11.Cloud cascading

---

## 11 Cloud cascading

### Introduction to Cloud Cascading

Cascading is a mode in which the intranet H5S is connected to the cloud H5S through a private protocol. It is divided into intranet configuration and cloud configuration, as shown in the following figure:

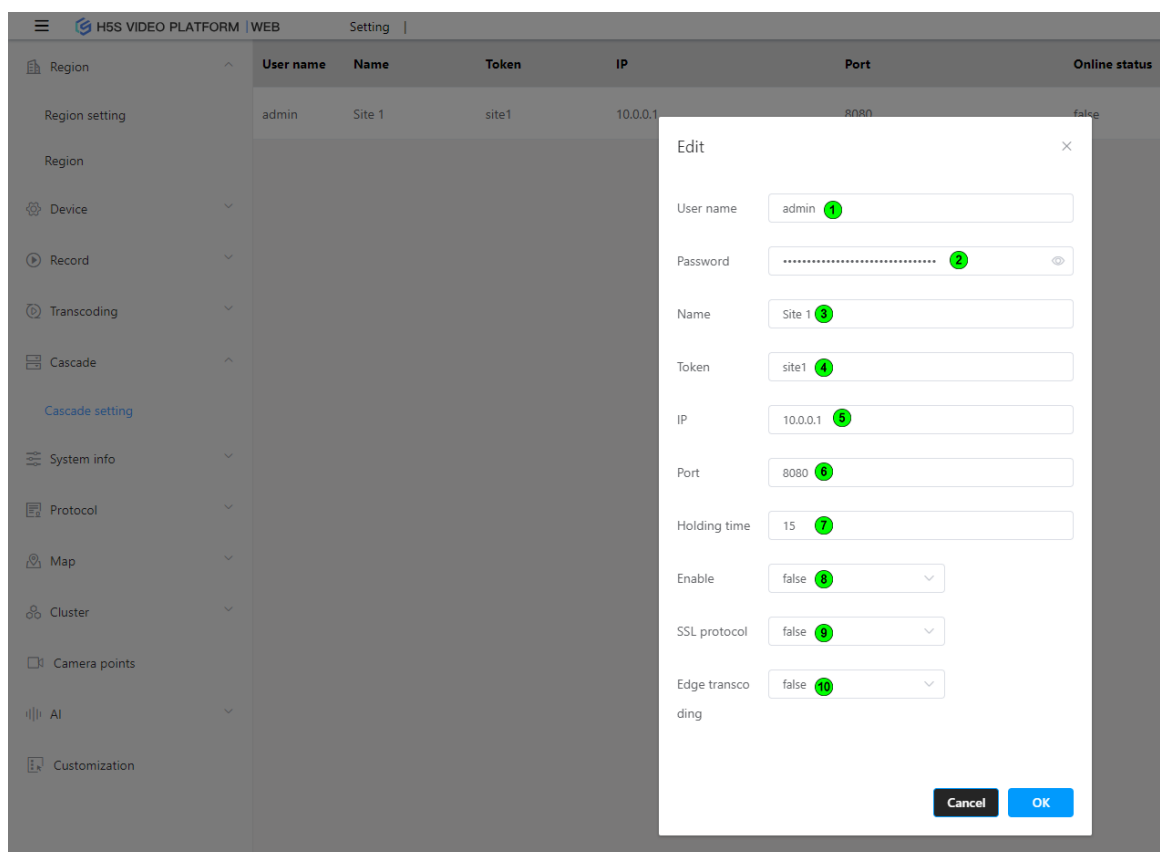


### 11.1 Cascade configuration

#### Cascade intranet service configuration

Enter **Setting-» Cascade-» Cascade Setting**, and configure cloud parameters as shown in the following figure:





Number	Name	Function
1	User name	
2	Password	
3	Name	
4	Token	
5	IP	
6	Port	
7	Holding time	
8	Enable	
9	SSL protocol	
10	Edge transco	


The user name and password are the user name and password of the cloud. The cloud supports multiple intranet service registrations, and the numbers of different intranet services cannot be the same. If the SSL protocol is enabled, the corresponding port should be the HTTPS port;

Edge transcoding is used to reduce the transcoding load on the server by uploading the transcoded content from the intranet service. If edge transcoding is not enabled, the original video data is sent to the cloud and transcoded by the cloud before being sent to the client.

### Cascading cloud service configuration

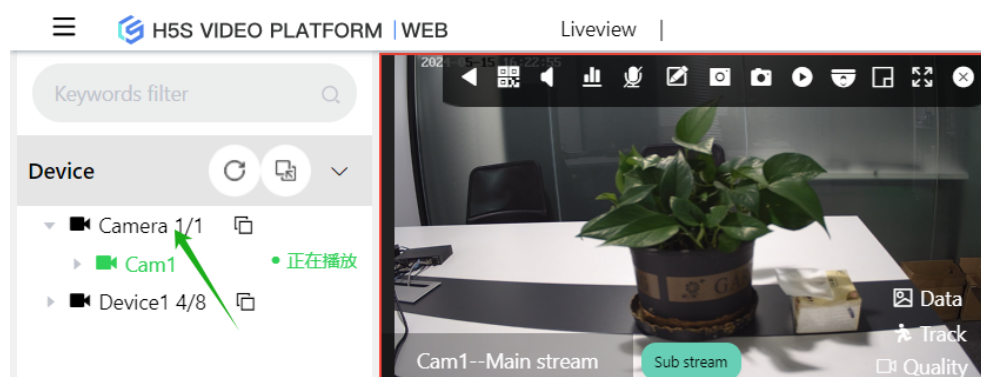
The default cloud server can accept connections from local servers without configuration. If you use WebRTC in Cloud mode, since the cloud server typically does not have a public IP address locally, the public IP address is mapped out. You need to set bCloudMode and the corresponding public IP address. Refer to the WebRTC configuration for the public network environment.

If there is an intranet service registration, you can enter the **Cloud Video** menu to see the registered H5S, and you can also see the corresponding node in the real-time video interface.



Name	Token	IP
Site 1	site1	192.168.100.165

The following figure shows Site 1 is a device registered in the cloud cascade:



**\*r17 and later versions cannot be cascaded with r16 and earlier versions.**

## 12.Video AI management

---

## 12 Video AI management

### Introduction to Video AI Management

H5S supports regular detection of camera video image quality, and can detect blurry and dark images. In addition, H5S also supports deep learning-based object detection and classification, which is divided into basic object detection and advanced object detection.

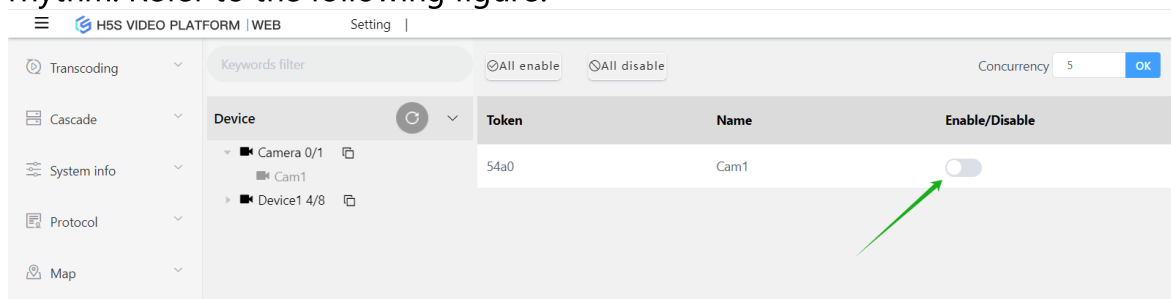
AI configuration requires AI software license. You can check whether there is relevant AI license in **Setting-» AI-» AI License**. Video quality detection requires a basic AI channel greater than 0.

H5S needs to be deployed to Windows 10/Windows Server 2016/Windows Server 2019 or Ubuntu 20.04 based on x86-64 CPUs.

### 12.1 Video quality detection

#### Video quality detection

H5S supports regular detection of camera video image quality, which can detect blurry and too dark images. You can turn it on or off in **Setting-» AI-» VQD**, or select the device and turn it on or off all at once. The default detection interval is 5 minutes, and a camera will be detected every 5 minutes. For example, if there are 10 cameras that need to be detected, it will take 50 minutes to complete the entire process. After that, it will continue to cycle from the first camera, or you can modify the interval to speed up the detection rhythm. Refer to the following figure:



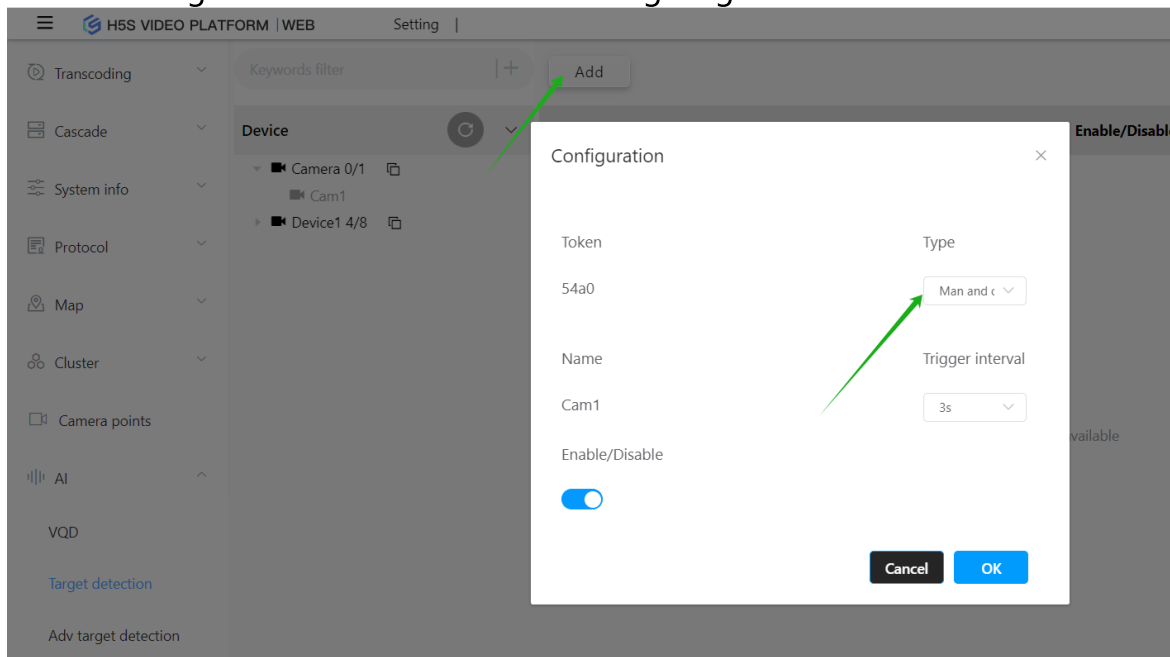
After configuration, the results can be viewed in the alarm panel after a detection interval. Refer to the following figure (the camera was covered during the test, resulting in a blurred image):

Token	Name	Device token	Type	Time	Online/Offline
1	116	1d54--5	The image is blur and black	2024-05-20T16:39:06.167831+08:00	<input checked="" type="checkbox"/>
2	116	1d54--5	The image is blur and black	2024-05-20T16:39:01.383319+08:00	<input checked="" type="checkbox"/>
3	116	1d54--5	The image is blur and black	2024-05-20T16:38:56.178953+08:00	<input checked="" type="checkbox"/>
4	116	1d54--5	The image is blur and black	2024-05-20T16:38:51.289713+08:00	<input checked="" type="checkbox"/>
5	116	1d54--5	The image is blur and black	2024-05-20T16:38:46.705024+08:00	<input checked="" type="checkbox"/>
6	116	1d54--5	The image is blur and black	2024-05-20T16:38:41.083319+08:00	<input checked="" type="checkbox"/>
7	116	1d54--5	The image is blur and black	2024-05-20T16:38:36.286295+08:00	<input checked="" type="checkbox"/>
8	116	1d54--5	The image is blur and black	2024-05-20T16:38:31.063764+08:00	<input checked="" type="checkbox"/>

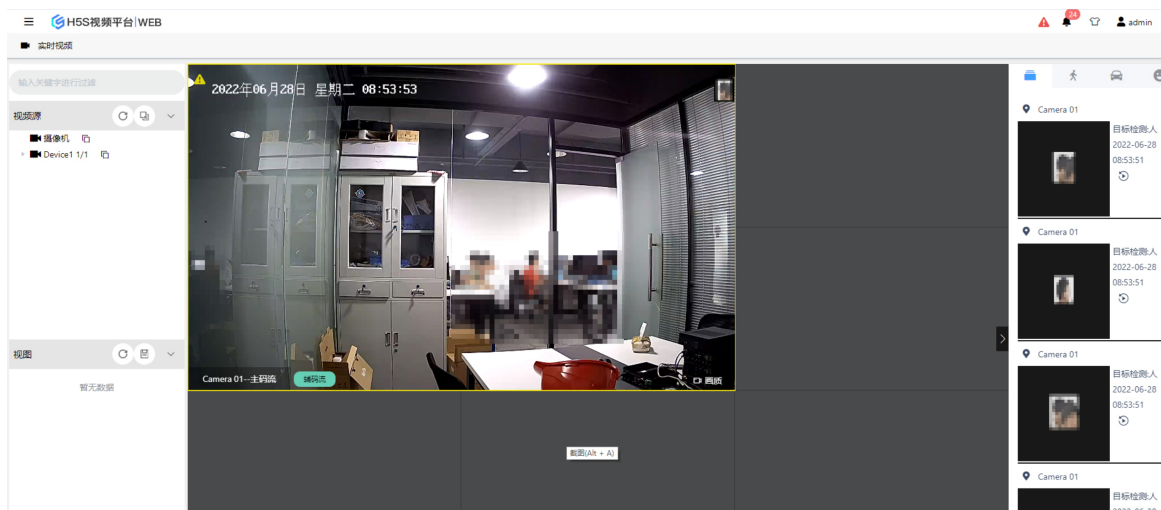
## 12.2 Object detection

### Object detection

H5S supports deep learning-based target detection and classification. Basic target detection relies on basic AI channel permissions. **Setting-» AI-» Target Detection** is turned on or off. It supports types of detection such as people and cars/cars/faces. The trigger interval is the interval between alarms triggered for the same target. Please refer to the following diagram:



After configuration, you can view the real-time detection results on the real-time video interface. Please refer to the following figure:

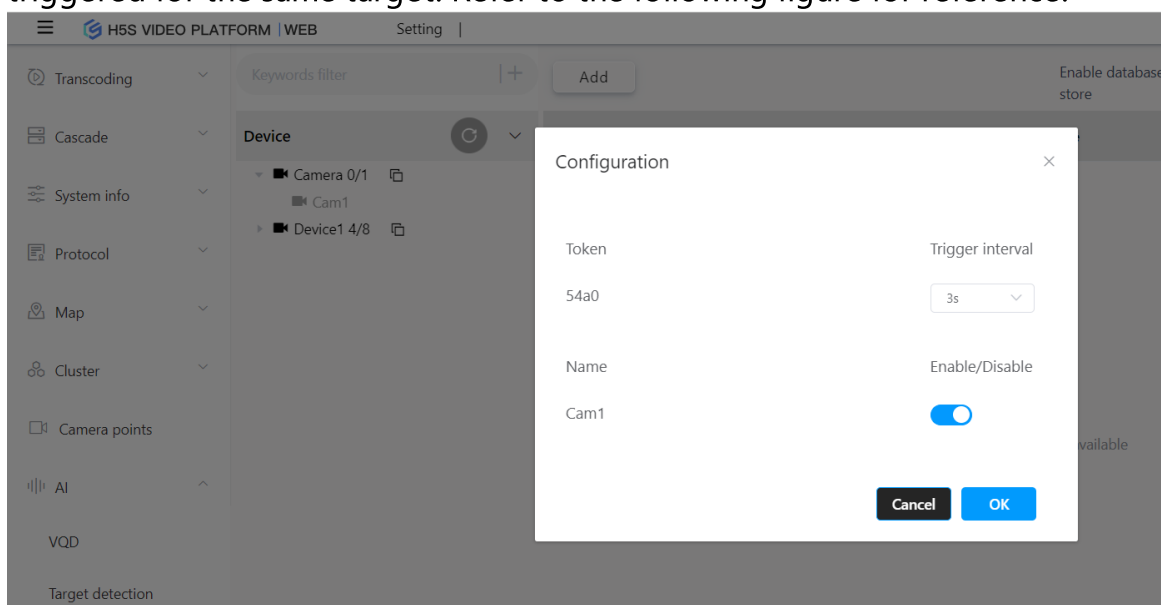


## 12.3 Advanced target detection

### Object detection

H5S supports deep learning-based target detection and classification. Advanced target detection relies on advanced AI channel permissions.

**Setting-» AI-» Adv Target Detection** to enable or disable. Supports safety helmet type detection, where the trigger interval is the interval between alarms triggered for the same target. Refer to the following figure for reference:



After configuration, you can search for detection results in the event panel, as shown in the following figure:

H5S视频平台 | WEB

事件

实时事件

事件搜索

事件调试

视频质量检测

高级目标检测

输入关键词进行过滤

设备

摄像头

Device1

Camera 01

时间

2022-07-25 08:20:02022-07-25 09:20:00

最近

一小时

100

查询

编号	名称	设备编号	类型	时间	图片
81	Camera 01	f5fd--1	人	2022-07-25T09:18:27+08:00	
82	Camera 01	f5fd--1	人	2022-07-25T09:18:27+08:00	
83	Camera 01	f5fd--1	人	2022-07-25T09:18:27+08:00	
84	Camera 01	f5fd--1	人	2022-07-25T09:18:27+08:00	
85	Camera 01	f5fd--1	人	2022-07-25T09:18:26+08:00	
86	Camera 01	f5fd--1	人	2022-07-25T09:18:26+08:00	
87	Camera 01	f5fd--1	人	2022-07-25T09:18:23+08:00	
88	Camera 01	f5fd--1	人	2022-07-25T09:18:21+08:00	
89	Camera 01	f5fd--1	人	2022-07-25T09:18:19+08:00	
90	Camera 01	f5fd--1	人	2022-07-25T09:18:18+08:00	

< 1 ... 5 6 7 8 9 10 > 共 100 条

前往 9 页





## 13.WEBRTC

---

## 13 WEBRTC

### Introduction to WebRTC

WebRTC itself has relatively high requirements for the network, and there are generally three types of scenarios.

The H5S server and browser clients are all on the intranet: no additional configuration is required, using the default configuration

The H5S server is in the cloud, and there is a mapped public IP address in the cloud (such as Alibaba Cloud and Huawei Cloud): use the Cloud mode

The H5S server is on the intranet, and the public IP and port are obtained through intranet mapping (private server with a telecommunications public IP): using forwarding mode

After modifying the cloud mode and forwarding mode configurations, it is necessary to restart the h5s service.

### 13.1 Cloud mode

#### Cloud mode

If you use WEBRTC in Cloud mode, since cloud servers generally do not have public IP addresses locally, public IP addresses are mapped out. You need to set the cloud mode and corresponding public IP address. Go to **Setting-»**

**Protocol-» WEBRTC-» Cloud model** and refer to the following figure.

The screenshot shows the 'Setting' page for the 'Cloud model' in the H5S VIDEO PLATFORM. The left sidebar lists various settings categories, with 'WEBRTC' expanded to show 'Cloud model'. The main content area displays four configuration items, each with a green circle number indicating a step:

- Enable:** A checkbox labeled '1' with the value 'false'.
- Internet address:** A text input field labeled '2' containing the value '47.75.117.15'.
- Minimum port:** A text input field labeled '3' containing the value '50000'.
- Maximum port:** A text input field labeled '4' containing the value '54999'.

At the bottom right of the configuration area, there are two buttons: 'Cancel' and 'Save'.

Number	Name	Function
--------	------	----------

1	Turn on cloud mode	
2	Public IP address in the cloud	
3	Minimum value of port range	
4	Maximum port range	

Cloud service WEBRTC needs to open the TCP port range of the configuration file; if it is Alibaba Cloud, it needs to open the security group configuration and open all the configured nPortRangeMin to nPortRangeMax TCP ports, as shown in the following figure.

☐ 允许      自定义 TCP      50000/54999      IPv4地址段访问      0.0.0.0/0

After configuration, please restart the H5S service.

## 13.2 Forwarding mode

### Forwarding mode

The forwarding mode is based on TURN technology. You can refer to the following figure to open the TURN service. The IP address is the server address where H5S is located, and the port is the port used by the TURN service. The IP address and port will be mapped by the router to the external network's IP and port. If there is no mapping, the two sets of IP addresses and ports are the same. **Setting-》Protocol-》WEBRTC TURN Service** refers to the following figure.

H5S VIDEO PLATFORM | WEB

Setting |

Record

Transcoding

Cascade

System info

Protocol

RTSP

WEBRTC

Cloud model

Forwarding mode

TURN service

Enable

false

IP

192.168.100.103

Port

9478

Cancel

Save

Number	Name	Function
1	IP	
2	Port	

After configuring the TURN service, you can configure the forwarding mode. Refer to the following figure, where the IP address and port are the mapped addresses and ports. If there is no mapping, use the address and port of the TURN service. The username and password can remain default.

If the client accesses the RTC service using an intranet Web service address, the server will detect that it is an intranet client based on the intranet Web address. In this case, the TURN traffic will go directly to the TURN service pointed to by the intranet IP address and intranet port, rather than through the mapped IP address and port.

H5S VIDEO PLATFORM | WEB Setting

Record

Transcoding

Cascade

System info

Protocol

RTSP

WEBRTC

Cloud model

Forwarding mode

TURN service

HTTP

Enable

false

IP

47.75.117.15

Port

9478

User

h5stream

Password

.....

Intranet address

192.168.100.103

Intranet port

9478

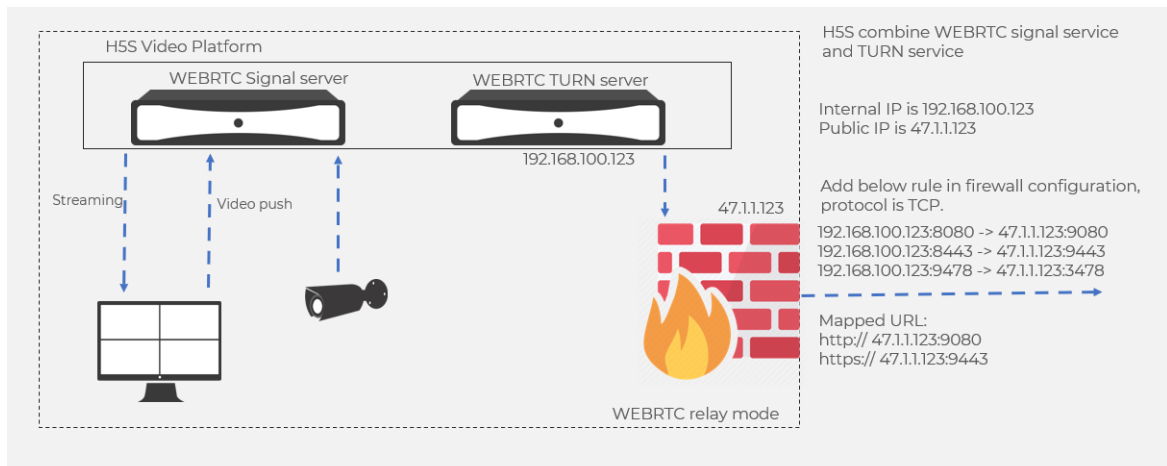
Internal web service address

192.168.100.103

Cancel Save

Number	Name	Function
1	Port	
2	Intranet port	
3	IP	
4	Intranet address	
5	Internal web service address	

The following figure shows an example of configuring forwarding mode.



The intranet IP address of the H5S service is 192.168.100.123, and the corresponding public IP address is 47.1.1.123. First, add the following three mappings (assuming that the h5s port is default and has not been modified) in the firewall or router, with the protocol set to TCP:

192.168.100.123:8080 -> 47.1.1.123:9080

192.168.100.123:8443 -> 47.1.1.123:9443

192.168.100.123:9478 -> 47.1.1.123:3478

The browser access address after mapping is

http:// 47.1.1.123:9080

https:// 47.1.1.123:9443

For the configuration of the corresponding forwarding mode and TURN service, please refer to the figure above.

## 14. Standard protocol

---

---

## 14 Standard protocol

### Introduction to standard protocol

The configuration interface and API have been added to the src of H5S. In addition to supporting js video playback libraries, they can also be accessed directly using RTSP RTMP clients. Starting from r15.14, H5S supports pushing the accessed video to a third-party streaming media server through the RTMP streaming protocol.

### 14.1 RTSP/RTMP/FLV real-time forwarding

#### RTSP/RTMP/FLV real-time forwarding

The following is the default port configuration, and there is a corresponding url for src of token1. main corresponds to the main stream, and sub corresponds to the sub stream. If there is no \$\$, the main stream is used by default. If it is FLV, you need to add the .flv suffix after the token.

RTSP: `rtsp://ip:8554/live/token1?session=ea99904d-8355-4590-8c03-9ddd205835a7`

RTSP: `rtsp://ip:8554/live/token1$$main?session=ea99904d-8355-4590-8c03-9ddd205835a7`

RTSP: `rtsp://ip:8554/live/token1$$sub?session=ea99904d-8355-4590-8c03-9ddd205835a7`

RTMP: `rtmp://ip:8935/live/token1$$main?session=ea99904d-8355-4590-8c03-9ddd205835a7`

RTMP: `rtmp://ip:8935/live/token1$$sub?session=ea99904d-8355-4590-8c03-9ddd205835a7`

FLV: `http://ip:8890/live/token1.flv?session=ea99904d-8355-4590-8c03-9ddd205835a7`

FLV: `http://ip:8890/live/token1$$main.flv?session=ea99904d-8355-4590-8c03-9ddd205835a7`

FLV: [http://ip:8890/live/token1\\$\\$sub.flv?session=ea99904d-8355-4590-8c03-9ddd205835a7](http://ip:8890/live/token1$$sub.flv?session=ea99904d-8355-4590-8c03-9ddd205835a7)

The following figure shows an example of VLC playing RTSP video forwarding. VLC also supports FLV and RTMP playback.





### RTSP/RTMP/FLV real-time forwarding authentication

Starting from r15.1, all RTSP and RTMP forwarding require session authentication. The session can be obtained from the Login API in the following format. Please ensure that a valid session is used when making requests.

RTSP: `rtsp://ip:8554/live/token1?session=ea99904d-8355-4590-8c03-9ddd205835a7`

RTSP: `rtsp://ip:8554/live/token1$$main?session=ea99904d-8355-4590-8c03-9ddd205835a7`

RTSP: `rtsp://ip:8554/live/token1$$sub?session=ea99904d-8355-4590-8c03-9ddd205835a7`

RTMP: `rtmp://ip:8935/live/token1$$main?session=ea99904d-8355-4590-8c03-9ddd205835a7`

RTMP: `rtmp://ip:8935/live/token1$$sub?session=ea99904d-8355-4590-8c03-9ddd205835a7`

### RTSP/RTMP/FLV real-time forwarding playback code

In the case of configuring a playback code, you can use the playback code instead of the session to play the video. For playback code settings, refer to **Setting-» Systeminfo-» User-» Play Code**.

RTSP: `rtsp://ip:8554/live/token1?session=0031`

RTSP: `rtsp://ip:8554/live/token1$$main?session=0031`

RTSP: `rtsp://ip:8554/live/token1$$sub?session=0031`

RTMP: `rtmp://ip:8935/live/token1$$main?session=0031`

RTMP: `rtmp://ip:8935/live/token1$$sub?session=0031`

---

FLV: <http://ip:8890/live/token1.flv?session=0031>

### FLV HTML Real-time Playback

There is an example of flv.html in the www directory, which is based on mpegts.js and can be played by clicking the following link in h5s web.

<http://ip:18085/flv.html?token=dff9&session=1234>

Note: The actual port for the flv protocol is 8890.

## 14.2 HLS real-time forwarding

### HLS real-time forwarding

Starting from r17, HLS supports two modes: on-demand streaming and continuous streaming. By default, all channels are on-demand streaming. Due to limitations in the protocol itself, HLS has a delay of more than 3 seconds. The following is a default port configuration with a corresponding url for src of token1. main corresponds to the main stream, and sub corresponds to the sub stream. The session parameter also supports playback codes.

HLS protocol address: <http://ip:18085/api/v3/token1/main/stream.m3u8?session=ea99904d-8355-4590-8c03-9ddd205835a7>

The service provides a player based on hls.js (<https://github.com/video-dev/hls.js>) internally, which can be used to verify the HLS protocol on Windows using Chrome/Firefox. Other browsers that support the HLS protocol can directly access the HLS protocol address.

hlsjs address: <http://ip:18085/hlsjs.html?token=token1&stream=main&session=ea99904d-8355-4590-8c03-9ddd205835a7>

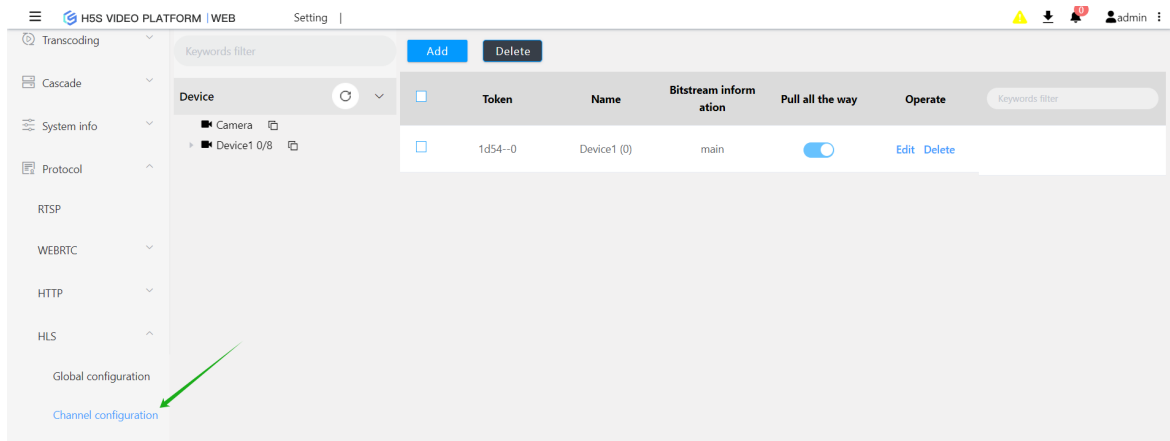
### HLS fmp4/mpegts mode

HLS supports fmp4 and mpegts packaging, with the default being fmp4 format. Some older Android HLS players do not support fmp4, and you can modify it to mpegts in **Setting-» Protocol-» HLS-» Global Configuration**. After modification, you need to restart.

### HLS channel configuration

HLS adopts a segmented mode. If you pull streaming from the camera on demand, the first frame time of HLS is very slow. You can configure the channel

to be in a continuous streaming mode, which will generate segmented files in advance and load faster.

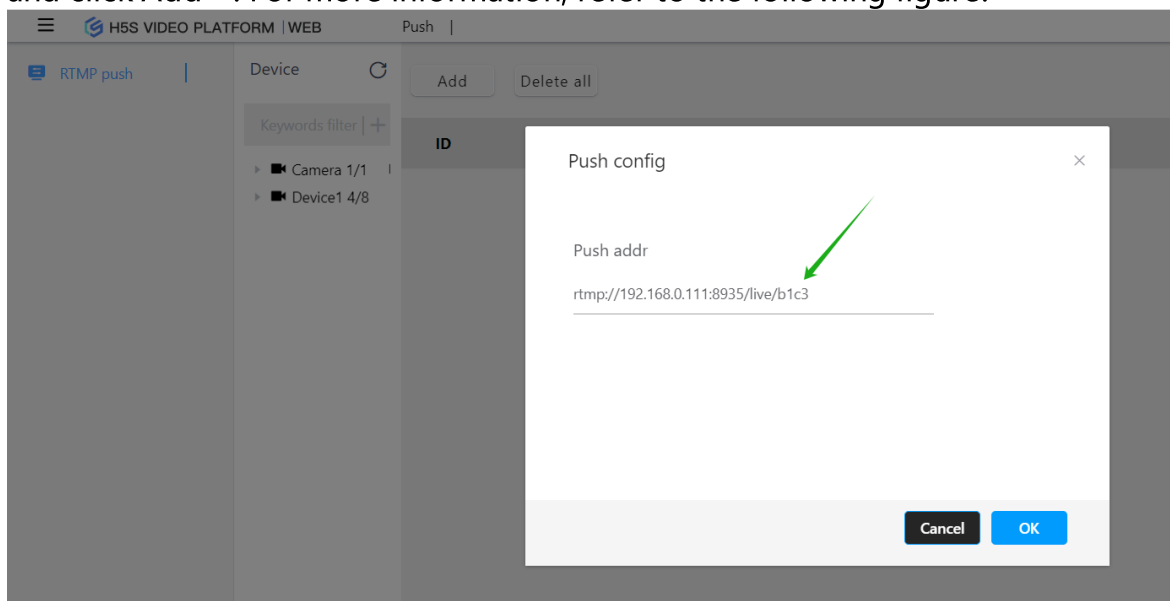


## 14.3 RTMP push stream forwarding

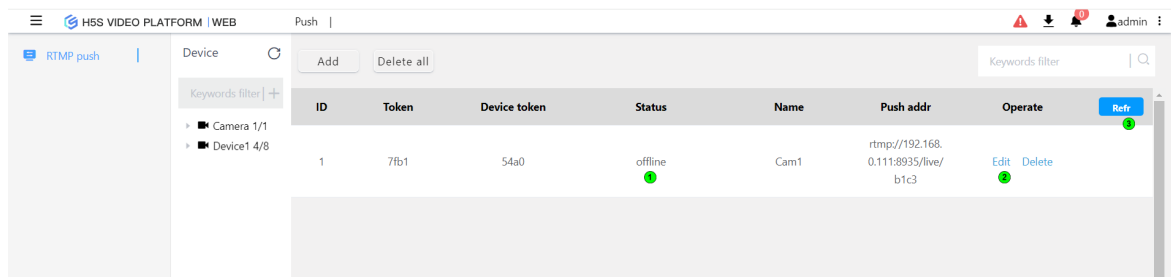
### RTMP push stream forwarding

Before configuring RTMP push streaming forwarding, find the address of the third-party RTMP push streaming service. Since RTMP does not support H265 transmission, all streaming data will be transcoded into H264 before being pushed; if the stream is H264, the service will not perform transcoding.

In the **Push**, select the video stream that needs to be streamed and forwarded, and click Add +. For more information, refer to the following figure:



After adding, you can refresh the corresponding interface to check whether the streaming is successful. For details, refer to the following figure:



Number	Name	Function
1	Offline	
2	Edit	
3	Refr	

## 15.System configuration

---

## 15 System configuration

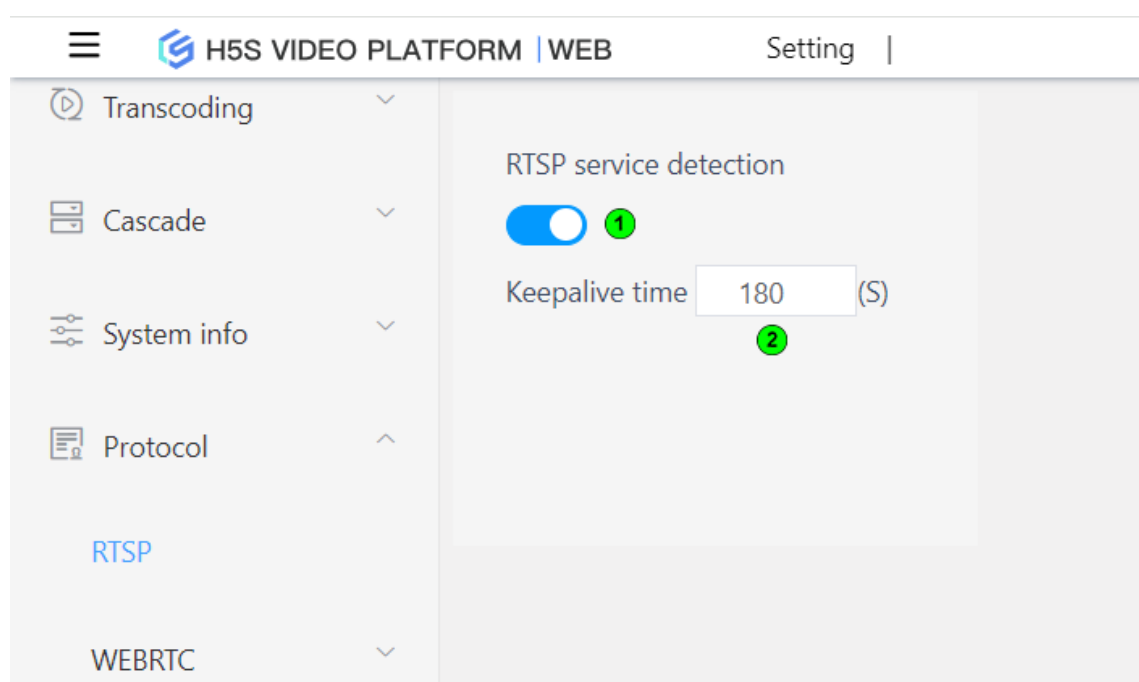
### 15.1 Network configuration

#### 15.1.1 RTSP protocol

##### RTSP protocol

The RTSP protocol is a streaming media protocol. If you use the on-demand streaming mode, there is no way to obtain the online status of the video source corresponding to RTSP/RTMP. H5S uses an IP address and port detection method to obtain the online status, which is enabled by default. It can also be turned off.

Enter **Setting-» Protocol-» RTSP** Configuration to check whether it is enabled, and you can configure the detection interval. Refer to the following figure:



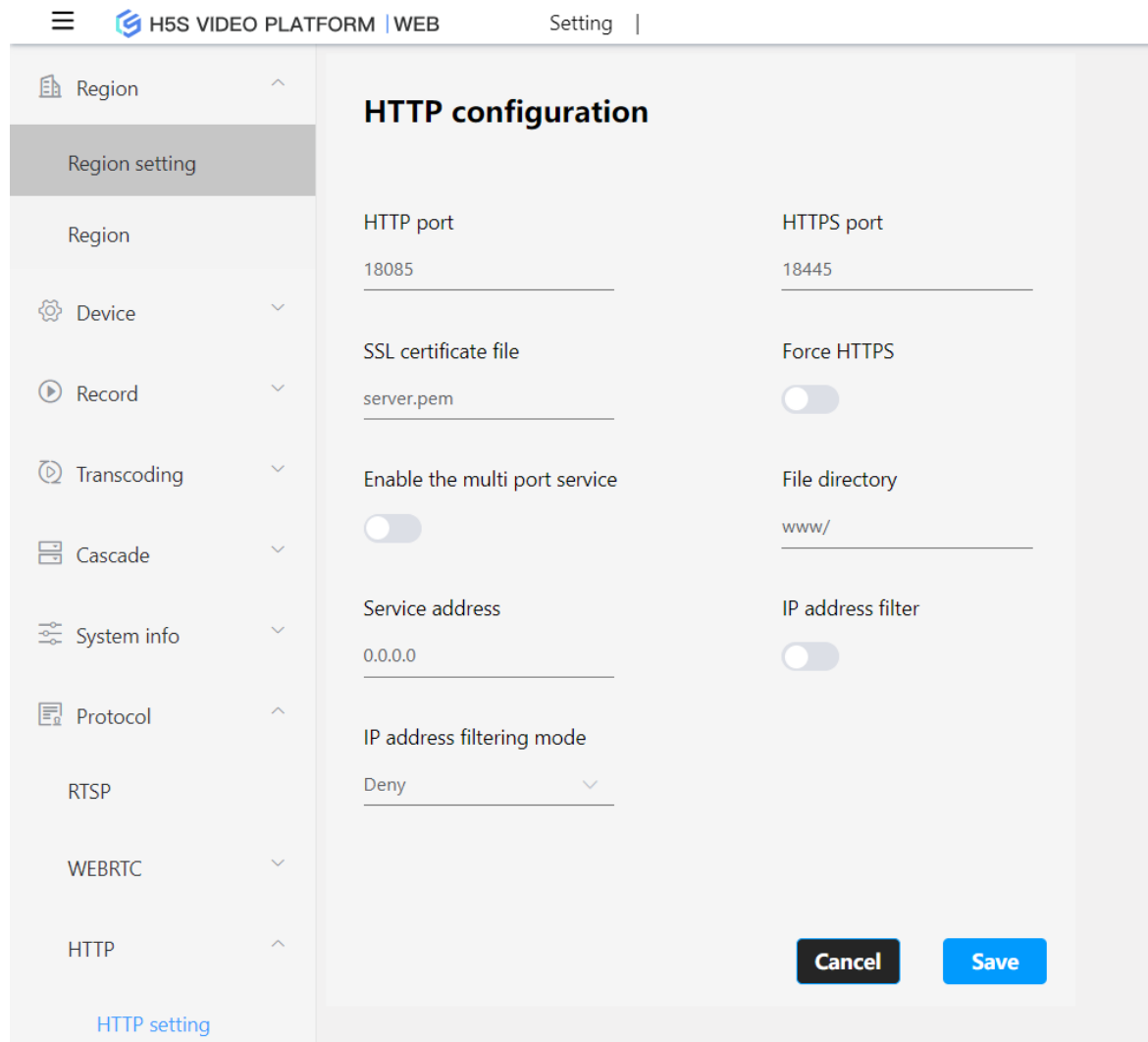
Number	Name	Function
1	RTSP service detection	
2	Keepalive time	

#### 15.1.2 HTTP protocol

##### HTTP protocol configuration

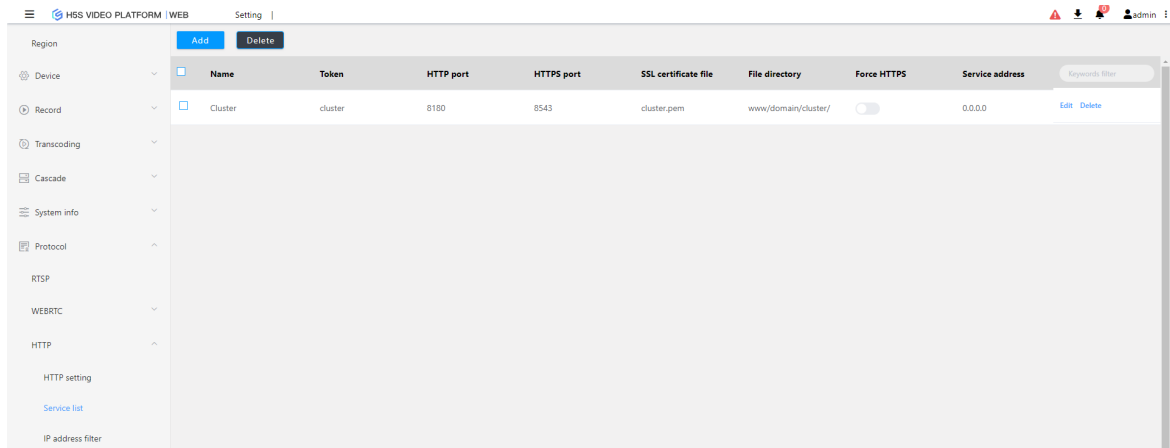
Enter **Setting-» Protocol-» HTTP-» HTTP setting** Configuration HTTP Parameters, support HTTP port, HTTPS port, certificate name (certificate in certificate/ directory), whether to enforce HTTPS, whether to support multiple

domains, HTML storage location. After modification, you need to restart it. Refer to the following figure:



### HTTP domain configuration

Enter **Settings-» Protocol-» HTTP-» Service list** to add or delete domains. The system defaults to the cluster interface. If you enable multiple domains, you can access it through the localhost domain name. Refer to the following figure:



### 15.1.3 HTTPS certificate configuration

#### HTTPS certificate configuration

H5S supports issuing certificate configuration. Modify the run directory certificate/server.pem. If the corresponding file name is modified in the HTTP protocol configuration, the corresponding file can be modified. This is applicable to multi-domain configurations. The following content is introduced with the file name server.pem.

It is recommended to download the nginx type certificate configuration in the following format.

```
-rw-r--r-- 1 root root 1675 May 28 2019 2275836_linkingvision.cn.key
-rw-r--r-- 1 root root 4073 May 28 2019 2275836_linkingvision.cn_nginx.zip
-rw-r--r-- 1 root root 3683 May 28 2019 2275836_linkingvision.cn.pem
```

Use a text editor (notepad++ is recommended) to clear the contents of server.pem. Then, copy the contents of the nginx pem file and the nginx key file into server.pem. The final file structure can be seen in the following image.

After modifying the server.pem file, restart the H5S service.



```

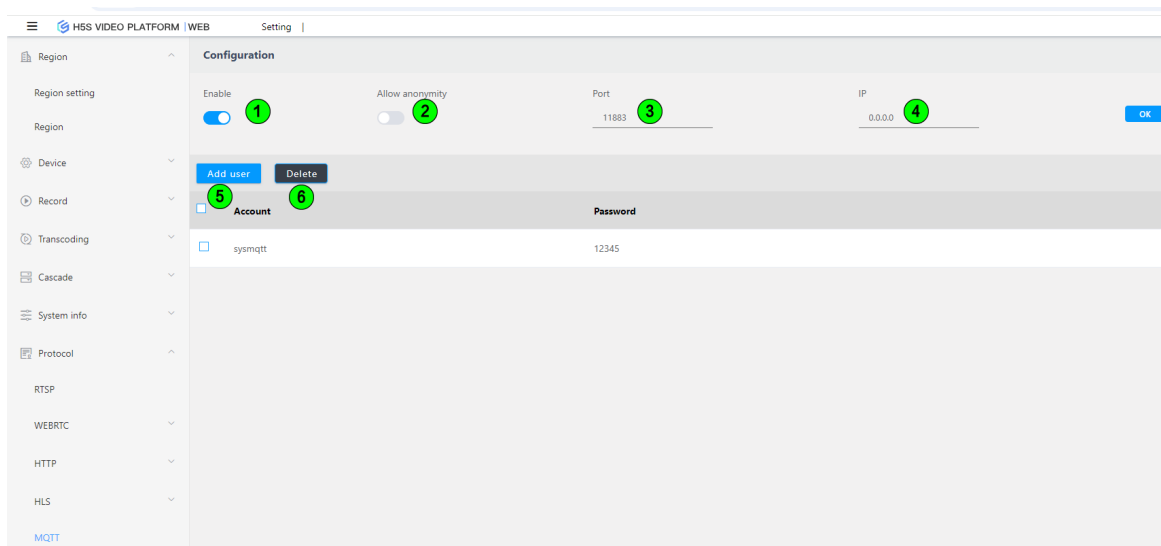
1 -----BEGIN CERTIFICATE-----
2 MIIFmJCCBIKGAwIBAgIQAxUnQ0MmWu5Wvp2tJGP97DANBgkqhkiG9w0BAQsFADBu
3 MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLEXB3
4 d3cuZGlnaWNlcnQuY29tMS0wKwYDVQQDEYRFBmNyeXB0aW9uIEV2ZXJ5d2hlcmUg
5 RfYgVExTIEBIC0gRzEwHhcNMjkwNTI4MDAwMDAwWhcNMjAwNTI3MTIwMDAwWjAb
6 7Mc3lqu89bgElDANBgkqhkiG9w0BAQsFAAOCAQEASocB2iatuVqWiSaWYFSJD5tg
7 HMBd0VYOfP5+PuMMGjA5O6bhPNLA2x3l5sz6006TvyWoLMzBo2vhRYpow8NxPuw/
8 EWog5KsH7cd1DquXnRa0X5ATcAxusvrS2egG5i9dOANYdpyzUulB3+Xzjsn5RMqa
9 ra6G0F6GuCG2FvEJTjCriXz/RJcwIWXoY7etXoBQaHuNGqKXS5caz1JhZSQ2ZCuG
10 wH8AdYZV46Gj6/gRklG+r6nH3nv6jMUUfL046Geh5NPGMk1QLZinzsaImYKUjWDa
11 2RgexB7MASSEduCCSRqfptQQ3Or7cPxOcRgnDrMmqm2Reim2Ng8kpCZJgNRlpg==
12 -----END CERTIFICATE-----
13 -----BEGIN CERTIFICATE-----
14 MIIEqjCCA5KGAwIBAgIQAnmsRYvBskWr+YBTzSybstANBgkqhkiG9w0BAQsFADBh
15 MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLEXB3
16 d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDEXdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
17 QTAEfW0xNzExMjc2MTBaFw0yNzExMjc2MTBaMG4xCzAJBgNVBAYTAlVT
18 SwW3AU4ETK+GQf2kFzYZkby5SFrHdPomunx2HBzViUchGoofGgg7gHW0W3MlQAXW
19 M0r5LUvStcr82QDWYNPaUy4taCQmyaJ+VB+6wxHstSigOlSNF2a6vg4rgexixeiV
20 4YSB03Yqp2t3TeZHM9ESfkus74nQyW7pRGezj+TC44xCagCQQOzzNmzEAP2SnCrJ
21 sNE2DpRVMnL8J6xBRdjmOsC3N6cQuKuRXbzByVBjCqAA8t1L0I+9wXJerLPyErjy
22 rMKWaBFLmfK/AHNF4ZihwPGOc7w6UHczBZXH5RFzJNnw+WNKuTPIOHfnVH8lg==
23 -----END CERTIFICATE-----
24 -----BEGIN RSA PRIVATE KEY-----
25 MIIEowIBAAKCAQEahaIiLhCi4Z0tsX9CZ+tIlxXtTCsLTIUnuYFuIwDPls0aUUTB
26 IlX26XjfyjMwkQUeanGuGUC+CKw4akouTod8E04vcrAqXoLBwqnx0XMV2LiV4Cax
27 5b8GdLlf62xajR/M6G07LqSIqi08PTyJPTXVIRYbDqvX08hUIhMnUUA5iIMP0N8
28 Pm+JhDiJAqiDmpimsGSskqGbvuytRCBVEmIRVloFjkFYwLtBrqiA8cMo+alkRGquJ
29 Dha+eP5yhtT13QuaFgcs/QNU5WpvF+4KX9XrhrYvvXW2jkrNO2fCrspbn4hQx8p5
30 2P4zrwKBgDuFkBgU5HyO5C6qyFbNuA62lIe9p/kE/PeN2BriIQaT0ShQt3ZWAL/n
31 xqWnU8JlJM4jhW7ngopGCPXn3FZk2hHoPtYF4sRlOGHXASGAE6BAv+POxsbu8WNk
32 i2AIw1Q/6BOza0WoPr/rqz0XCos2A0+FTqoxpeM4wPuzOnlxtKAp
33 -----END RSA PRIVATE KEY-----

```

#### 15.1.4 MQTT Server

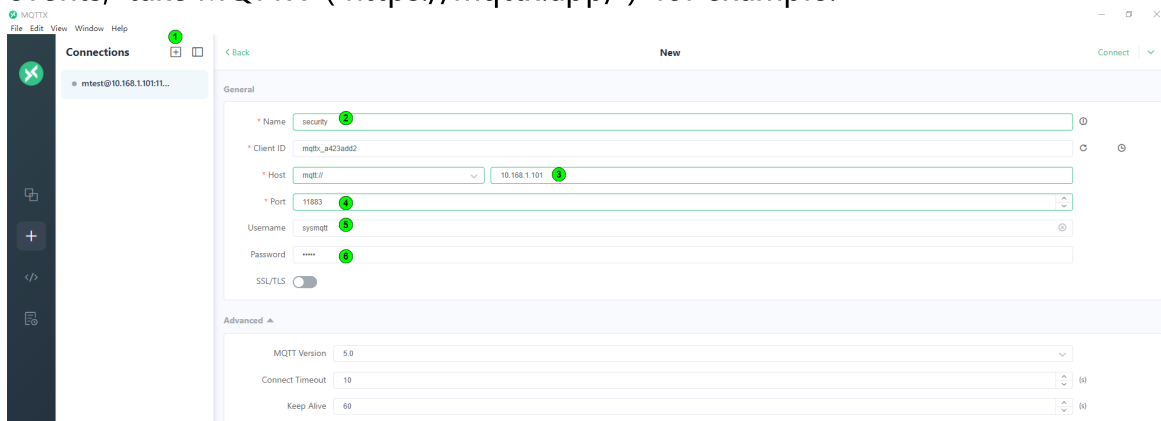
##### MQTT server configuration

Starting from R18, H5S has built-in MQTT service and pushes device alarms to the MQTT server by default. Go to **Settings ->Protocol ->MQTT** to configure MQTT service parameters. After configuration, it needs to be restarted to take effect.



Number	Name	Function
1	Enable	Start or stop MQTT service, restart takes effect
2	Allow anonymity	Enable or disable MQTT authentication
3	Port	MQTT server port
4	IP	MQTT server IP
5	Add user	Add MQTT user
6	Delete	Delete MQTT user

After MQTT is enabled, third-party MQTT clients can be used to subscribe to events, take MQTTX ( <https://mqttx.app/> ) for example.



Number	Name	Function
1	Connect	Connect to MQTT server

2	Name	Connection name
3	Host	MQTT server IP
4	Port	MQTT server port
5	Username	MQTT user name
6	Pasword	MQTT user password

After opening the link, you can subscribe to the alarm. The topic format is secureEvent/device/token/type, where the token is the camera channel and the type is the alarm type as follows

H5S\_EVENT\_MOTION motion

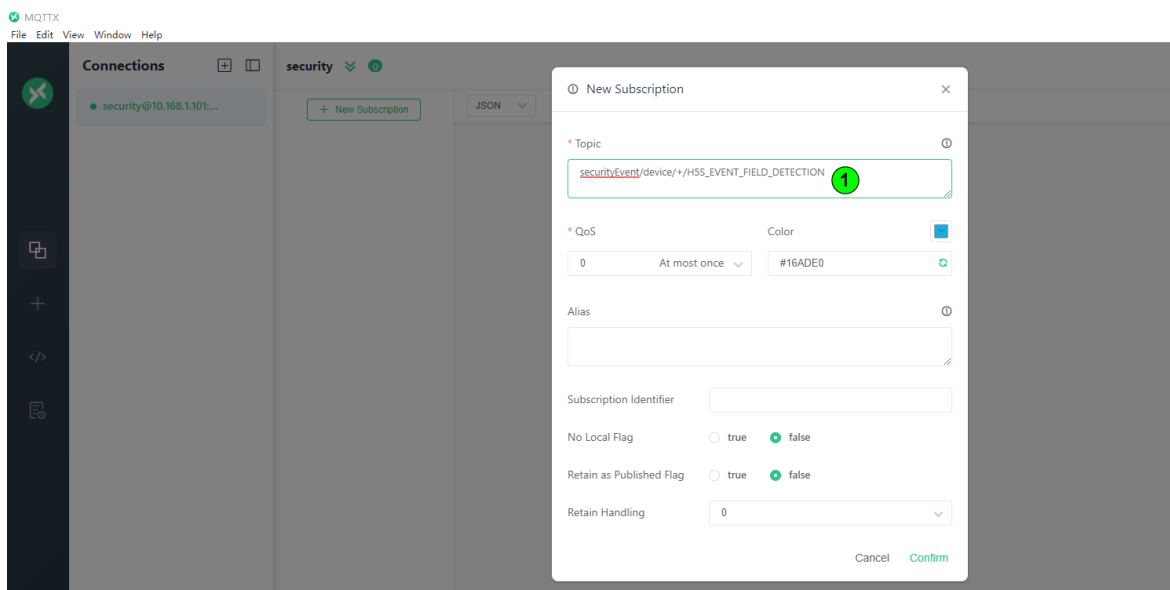
H5S\_EVENT\_CROSS\_LINE cross line

H5S\_EVENT\_FIELD\_DETECTION field detection

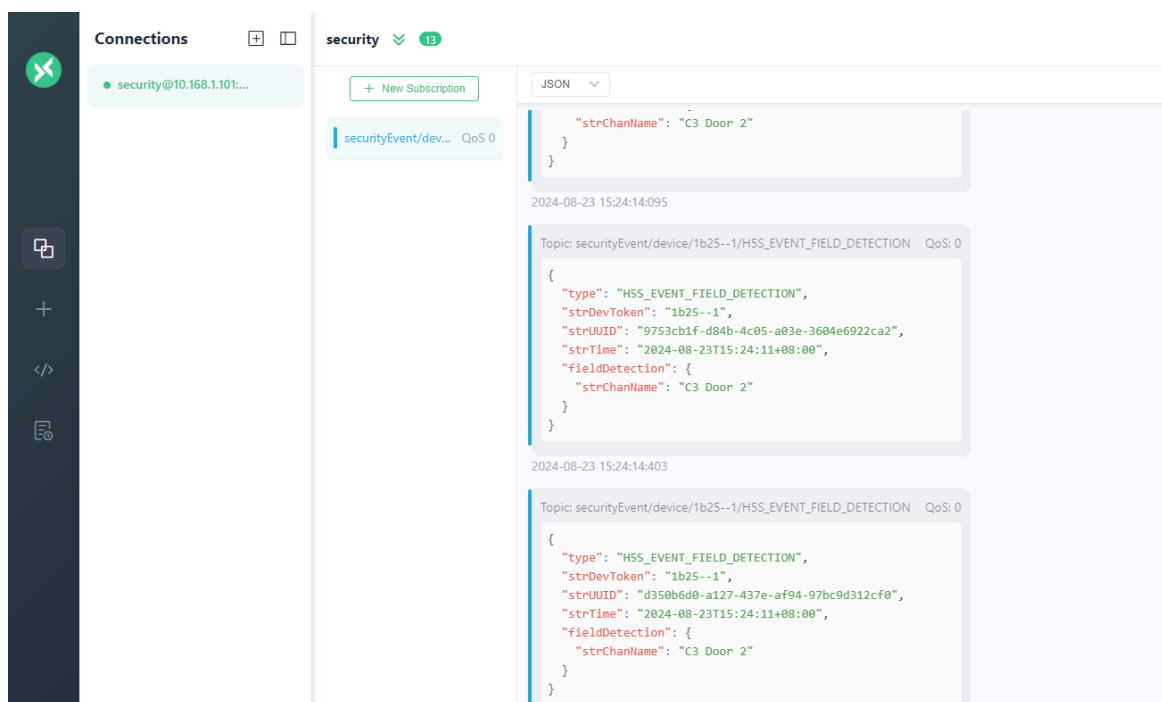
H5S\_EVENT\_SMOKE\_DETECTION smoke detection

H5S\_EVENT\_CONS\_VEHI\_DETECTION construction vehicles

securityEvent/device/+ /H5S\_EVENT\_FIELD\_DETECTION can subscribe all the channel field detection event. securityEvent/device/# subscribe all the event. single-level wildcard is +, multi-level wildcard#



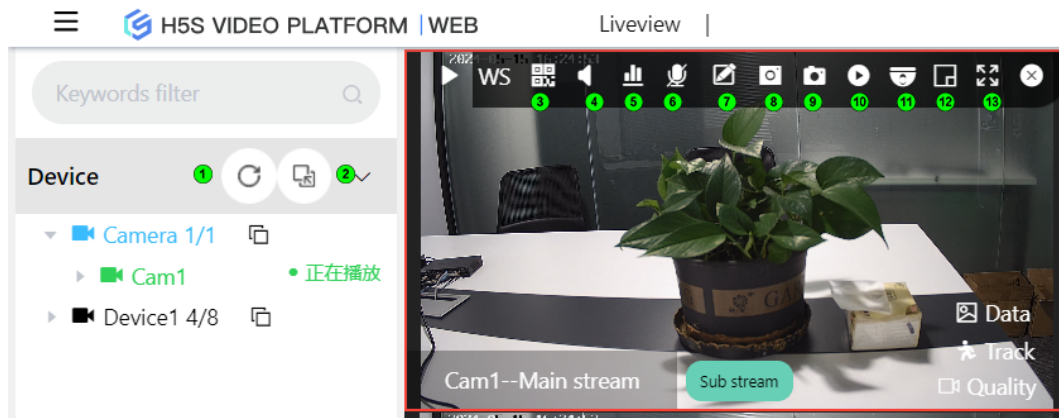
Receive real-time device alarms after successful subscription



## 15.2 Video recording management

### Video recording control

You can start and stop recording on the real-time video interface. For specific instructions, refer to the real-time video section of the manual:



Number	Name	Function
1	Refresh	
2	Switching regions	
3	QR code	
4	Turn on sound	

5	Encoding information	
6	Turn on the microphone	
7	AI annotation	
8	Screenshot	
9	Capture	
10	Start recording, stop recording	
11	Pan tilt control	
12	Electronic amplification	
13	Full screen enlargement	

### Loop Recording Configuration

The system video recording is set to cycle coverage by default. You can modify `bAutoFullDel` in `conf/h5ss.conf` to turn on or off cycle coverage, or modify `nDiskAutoDelPercent` to change the percentage of starting cycle coverage. By default, cycle coverage starts when it exceeds 92% of the disk. After modification, you need to restart.

```

96  "system": {
97    "nLogTypeComment": "log type H5_LOG_DEBUG/H5_LOG_INFO/H5_LOG_WARNING/H5_LOG_ERROR",
98    "nLogType": "H5_LOG_INFO",
99    "bConsoleLogComment": "Console log enable true/false ",
100   "bConsoleLog": true,
101   "bRotatingLogComment": "Enable rotating log",
102   "bRotatingLog": false,
103   "nRotatedFilesComment": "Rotated files default 5, each 2M",
104   "nRotatedFiles": 5,
105   "nLoginTimeoutComment": "Login session timeout",
106   "nLoginTimeout": 600,
107   "bEnableLinkagentComment": "Enable Linkagent (true or false)",
108   "bEnableLinkagent": false,
109   "nServerThreadNumComment": "Server thread number",
110   "nServerThreadNum": 200,
111   "nRecordInDayComment": "Record recycle time in day",
112   "nRecordInDay": 90,
113   "nSnapshotInDayComment": "Snapshot recycle time in day",
114   "nSnapshotInDay": 90,
115   "bAutoFullDelComment": "Delete Old record/snapshot when disk is full",
116   "bAutoFullDel": true,
117   "bReIndexComment": "Sync the record/snapshot from disk when restart",
118   "bReIndex": false,
119   "nDiskAutoDelPercentComment": "Disk start auto delete percent(10 to 92)",
120   "nDiskAutoDelPercent": 92,
121   "bDynSrcSaveComment": "Save the RESTful API added src to conf file",
122   "bDynSrcSave": true,
123   "bUserRTPTSComment": "Use RTSP source TS or use receive time",
124   "bUserRTPTS": true,
125   "bUseLive555Comment": "Use RTSP source TS or use receive time",
126   "bUseLive555": true,
127   "nNetCheckTimeoutComment": "Network check timeout, unit is ms",
128   "nNetCheckTimeout": 500
129 }
```

### Video path configuration

Starting from 9.1, the mediastore supports absolute path configuration for video recording locations. In `conf/h5ss.conf`, modify `bEnableStorPath` to true and modify the corresponding `strRoot`. Currently, only one path configuration is supported and multiple paths are not supported. After modification, you need to restart.

```

289 },
290 "storage": {
291   "bEnableStorPathComment": "enable storage path, default path is www/mediastore",
292   "bEnableStorPath": false,
293   "nRecordDurationComment": "record duration time (min)",
294   "nRecordDuration": 20,
295   "vol": [
296     {
297       "strLocationComment": "virtual path in http",
298       "strLocation": "/mediastore",
299       "strRootComment": "root path of this volume, absolute path",
300       "strRoot": "d:/"
301     }
302   ],
303   "rec": []
304 },

```

### Video recording configuration is prohibited

After configuring the video recording path, if strRoot does not exist, all video recordings will be prohibited. For example, if the following p:/ does not exist, the system will prohibit all types of video recordings.

```

290 "storage": {
291   "bEnableStorPathComment": "enable storage path, default path is www/mediastore",
292   "bEnableStorPath": true,
293   "nRecordDurationComment": "record duration time (min)",
294   "nRecordDuration": 20,
295   "vol": [
296     {
297       "strLocationComment": "virtual path in http",
298       "strLocation": "/mediastore",
299       "strRootComment": "root path of this volume, absolute path",
300       "strRoot": "p:/"
301     }
302   ],
303   "rec": []
304 },

```

## 15.3 Transcoding management

### Introduction to Transcoding Management

Find the transcoding section in the configuration file. The configuration file has different transcoding profiles: default

H5S supports hardware and software codecs based on Intel GPU/NVIDIA GPU, and can obtain the currently supported codecs in the dashboard.



If it is a software codec, h5s supports most operating systems. For detailed configuration, please refer to NVIDIA GPU mode and system GPU mode.

On Windows, you can update the driver at the following link:

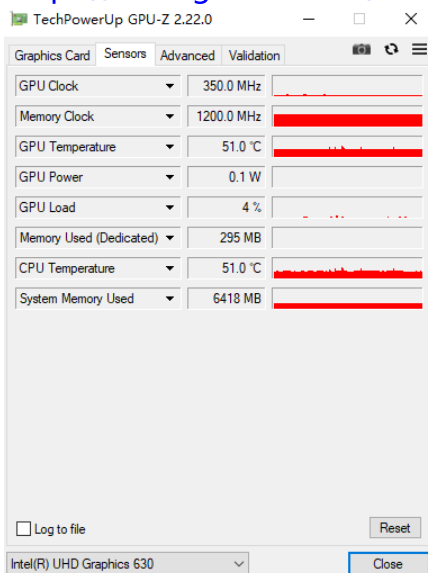
<https://downloadcenter.intel.com/>

The Linux H5S release package includes Intel-related drivers. Run `installgpudriver.sh` in the release directory as root. Additionally, Linux recommends running H5S as root.

The default version requires a transcoding license to have transcoding functionality. Please send an email to [info@linkingvision.com](mailto:info@linkingvision.com) to obtain a transcoding license.

You can use GPU-Z on Windows to view the usage of the GPU. You can download it from the following link:

<https://linkingvision.com/download/tools/GPU-Z.2.22.0.exe>

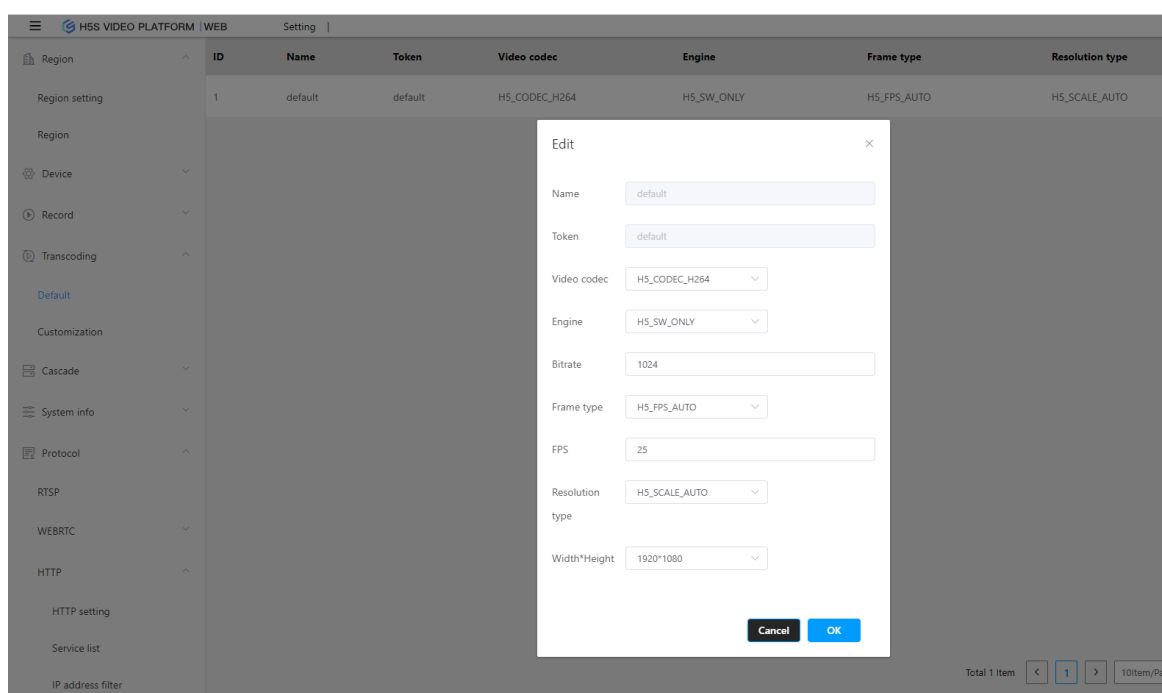
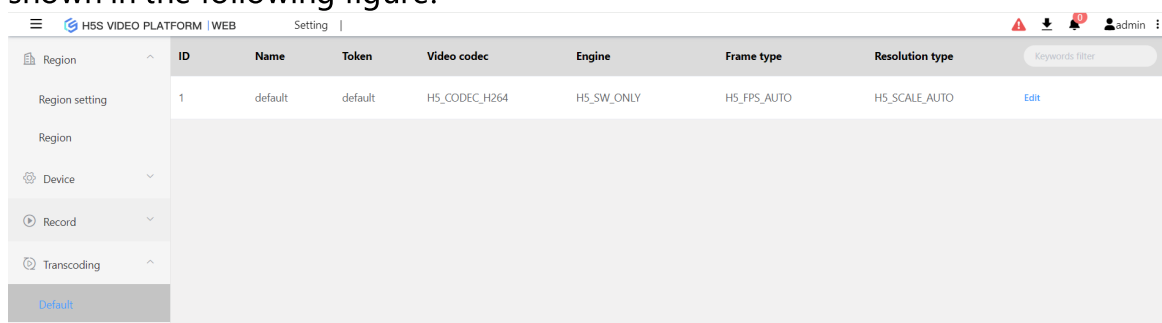


### 15.3.1 Default transcoding configuration

#### Default H265 to H264 conversion configuration default

Since browsers currently do not support H.265, h5s will automatically detect the H.265 stream and find a suitable transcoding method to convert H.265 to H.264. Of course, if it is already H.264, nothing will be done.

Enter **Setting-» Transcoding-» Default** to modify relevant parameters, as shown in the following figure:



#### Parameter meanings

Field	Meaning	Describe
Name	Configuration Name	Default configuration, cannot be deleted. If it is customized, it can be modified and deleted



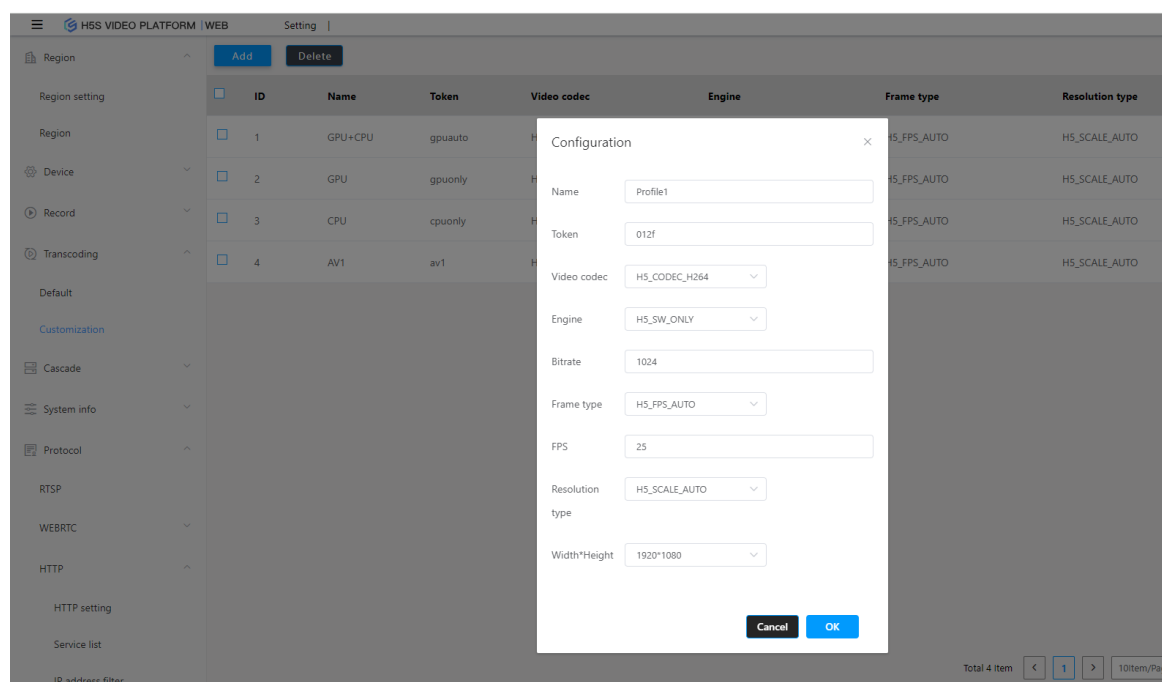
Number	Configuration number	Default configuration, cannot be deleted. If it is customized, it can be modified and deleted
Video coding	H5_CODEC_H264 H5_CODEC_AV1	The default is H5_CODEC_H264, which is mainly used for HTML5 video support. H5_CODEC_AV1 requires more computing power. If you need H5_CODEC_AV1 support, please contact product technical support. You need to use a TAV1 transcoding card
Engine	H5_SW_ONLY H5_GPU_AUTO H5_GPU_ONLY	H5_SW_ONLY indicates that only CPU transcoding is used and no GPU is loaded H5_GPU_AUTO indicates the use of both CPU and GPU in a load balancing mode H5_GPU_ONLY indicates using only GPU It is necessary to check whether the NVIDIA GPU mode and system GPU mode have loaded the GPU. If not, the system will automatically select the CPU
Code rate	The bit rate after transcoding, in bps	The range is 64 to 10240, with a default of 1024. It can also be modified to 2048 or 3072 to improve image quality
Frame rate type	H5_FPS_AUTO H5_FPS_FIXED H5_FPS_DYNAMIC	H5_FPS_AUTO indicates that the same frame rate is used as the video source H5_FPS_FIXED indicates a fixed frame rate, with a specific value of <b>frame rate</b> H5_FPS_DYNAMIC is an experimental type and is not open to the public for the time being
Frame rate	Frame rate 5-25	It takes effect when the frame rate type is H5_SCALE_FIXED
Resolution type	H5_SCALE_AUTO H5_SCALE_FIXED H5_SCALE_DYNAMIC	H5_SCALE_AUTO indicates that the same resolution as the video source is used H5_SCALE_FIXED indicates a fixed resolution, with a specific value of <b>width and height</b> H5_SCALE_DYNAMIC is an experimental type and is not available to the public for the time being
Width and height	Resolution width and height	It takes effect when the resolution type is H5_SCALE_FIXED

## 15.3.2 Customize transcoding configuration

### Customize transcoding configuration

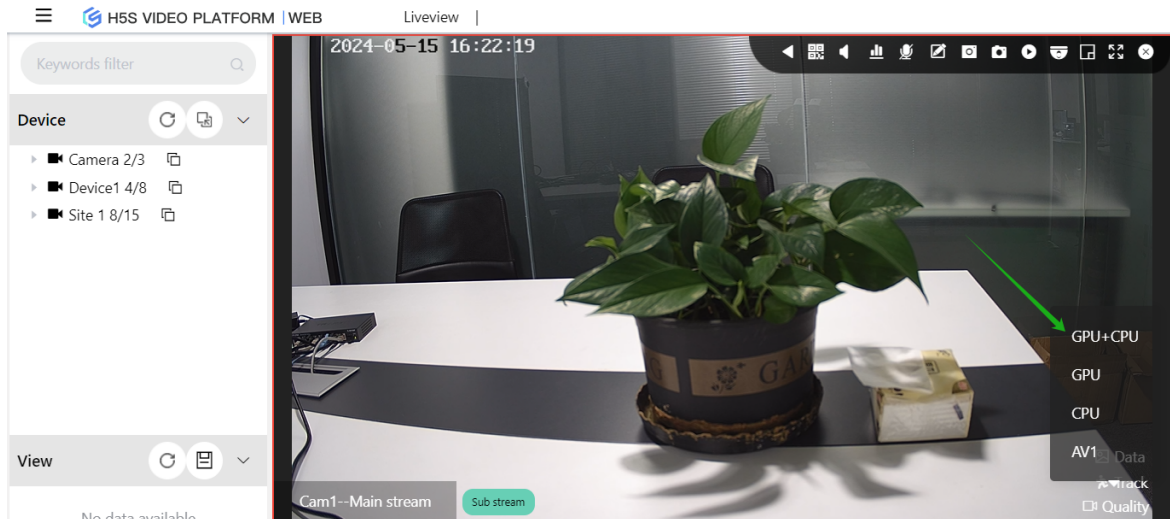
H5S supports user-defined transcoding, and users can add custom transcoding configurations in the settings.

Enter **Setting-» Transcoding-» Customization** to modify relevant parameters. For the meaning of relevant parameters, refer to the default transcoding configuration. For specific parameters, refer to the following figure:



The above figure has three profiles configured

This is a transcoding configuration that can be selected in the real-time video playback window. Profile1, Profile2, and Profile3 can be used for high-quality, medium-quality, and low-quality playback in actual use. Refer to the following image:



In the cloud streaming mode, you can enable edge device transcoding, which can reduce the load on the central server. In the cascading configuration, simply modify `bEdgeTranscoding` to `true`.

```

100 "cloud": {
101   "strServerNameComment": "Site/Server name",
102   "strServerName": "Site 1",
103   "strServerTokenComment": "Site/Server token",
104   "strServerToken": "site1",
105   "bEnableComment": "Enable connect",
106   "bEnable": true,
107   "strCloudIpComment": "Cloud ip address or domain name",
108   "strCloudIp": "127.0.0.1",
109   "strCloudPortComment": "Cloud port",
110   "strCloudPort": "8080",
111   "bSSLComment": "Enable SSL for cloud connect",
112   "bSSL": false,
113   "strUserComment": "User for cloud connect",
114   "strUser": "admin",
115   "strPasswdComment": "Password MD5 hashed, default 12345",
116   "strPasswd": "827ccb0eea8a706c4c34a16891f84e78",
117   "nKeepaliveTimeComment": "Keepalive time interval, default is 3s",
118   "nKeepaliveTime": 15,
119   "bEdgeTranscodingComment": "Enable edge transcoding, default is disable",
120   "bEdgeTranscoding": true

```

All nodes and servers in the cloud streaming mode need to have the same custom transcoding configuration. The cloud streaming intranet server and cloud streaming public network server need to have the same name and number (token) Profile, but other parameters except for the name and number (token) can be configured according to actual requirements.

### 15.3.3 GPU mode selection

#### GPU mode selection

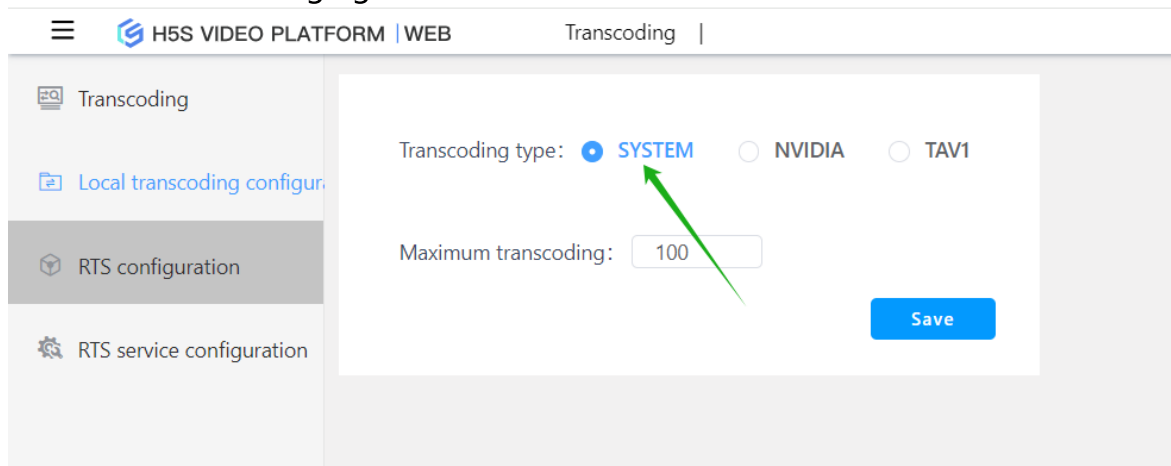
The H5S mode disables GPU transcoding, and you can modify the default configuration of the transcoding engine options to enable GPU transcoding support:

H5\_SW\_ONLY indicates that only CPU transcoding is used without loading GPU

H5\_GPU\_AUTO indicates that both CPU and GPU are used simultaneously, using a load balancing mode

H5\_GPU\_ONLY indicates that only the GPU is used

It is necessary to check whether the NVIDIA GPU mode and system GPU mode have loaded the GPU. If there is no GPU loaded, the system will automatically choose the CPU. The system mode will automatically select the GPU. The NVIDIA mode uses only the NVIDIA GPU card, and the TAV1 mode uses the TAV1 transcoding card. The TAV1 mode supports transcoding in AV1 format. Refer to the following figure:



If the system has a GPU, you can choose according to the actual situation. The selection method is shown in the following table:

Operating system	GPU	Type	Describe
Windows 10/2016/2019	Intel	System GPU mode	Does not support multi-graphics card mode
Windows 10/2016/2019	AMD	System GPU mode	Does not support multi-graphics card mode
Windows 10/2016/2019	NVIDIA single graphics card	System GPU mode	Does not support multi-graphics card mode
Linux	Intel	System GPU mode	Does not support multi-graphics card mode

Windows 10/2016/2019	NVIDIA multi-graphics card (including single card)	NVIDIA GPU mode	Support multiple GPU graphics cards, and it is recommended to use the same model RTX A2000 supports 10-channel 1080P H265 to H264 transcoding
Linux	NVIDIA multi-graphics card (including single card)	NVIDIA GPU mode	Support multiple GPU graphics cards, and it is recommended to use the same model
Linux	RK3568/RK3566/RK3588	System GPU mode	RK3588 has the best performance and can support 15-channel 1080P H265 to H264 transcoding

After determining the mode, you need to configure the mode. You can configure the mode in **Transcoding-» Local transcoding configuration** Settings. After modifying the mode, you need to restart H5S. The maximum transcoding is the maximum number of transcodings supported by the GPU. The specific number can be adjusted based on hardware measurements.

### H5S Operation Requirements

Linux running H5S requires root access. Using a regular account can lead to slow video start-up or green screen issues.

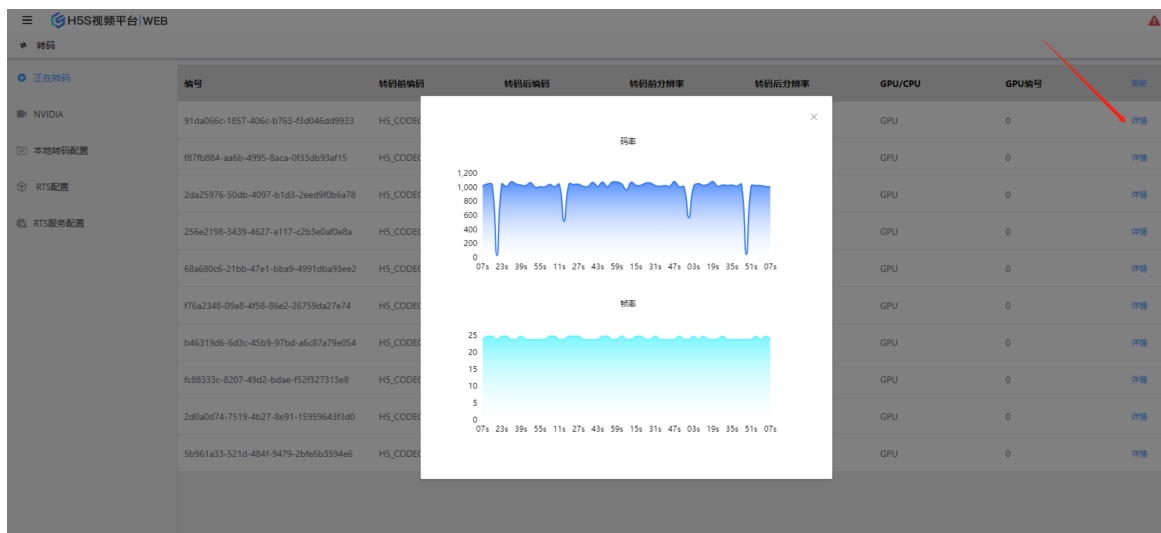
### Transcoding status

Enter the **transcoding-» transcoding status** to view the detailed information of the transcoding process.

Transcoding indicates the ongoing transcoding process. GPU/CPU indicates the type of resources used for the transcoding process. GPU number indicates the number of GPUs used. If there are multiple GPUs, the system will load balance across multiple GPUs,

Click on the details to view the real-time frame rate and bit rate, as shown in the following figure:

正在转码	编号	转码前编码	转码后编码	转码前分辨率	转码后分辨率	GPU/CPU	GPU编号	详情
NVIDIA	91da066c-1857-406c-b763-f3d046dd9933	H5_CODEC_H265	H5_CODEC_H264	1920x1080	1920x1080	GPU	0	详情
本地转码配置	8f7b884-aa6b-4995-8aca-0f33db93af15	H5_CODEC_H265	H5_CODEC_H264	1920x1080	1920x1080	GPU	0	详情
RTS配置	2da25976-50db-4097-b1d3-2eed9f0b6a78	H5_CODEC_H265	H5_CODEC_H264	1920x1080	1920x1080	GPU	0	详情
RTS服务器配置	256e2198-3439-4627-a117-c2b3e0af0e8a	H5_CODEC_H265	H5_CODEC_H264	1920x1080	1920x1080	GPU	0	详情
	68a680c6-21bb-47e1-bba9-4991db93ee2	H5_CODEC_H265	H5_CODEC_H264	1920x1080	1920x1080	GPU	0	详情
	f76a2348-09a8-4f58-86e2-26759da27e74	H5_CODEC_H265	H5_CODEC_H264	1920x1080	1920x1080	GPU	0	详情
	b46319d6-6d3c-45b9-97bd-a6c87a79e054	H5_CODEC_H265	H5_CODEC_H264	1920x1080	1920x1080	GPU	0	详情
	fc88333c-8207-4942-bdae-f52f27313a8	H5_CODEC_H265	H5_CODEC_H264	1920x1080	1920x1080	GPU	0	详情
	2d0a0d74-7519-4b27-8e91-15959643f3d0	H5_CODEC_H265	H5_CODEC_H264	1920x1080	1920x1080	GPU	0	详情
	5b961a33-521d-484f-9479-2bf6b3594e6	H5_CODEC_H265	H5_CODEC_H264	1920x1080	1920x1080	GPU	0	详情




### 15.3.4 NVIDIA GPU Mode

#### GPU supports the number of codes

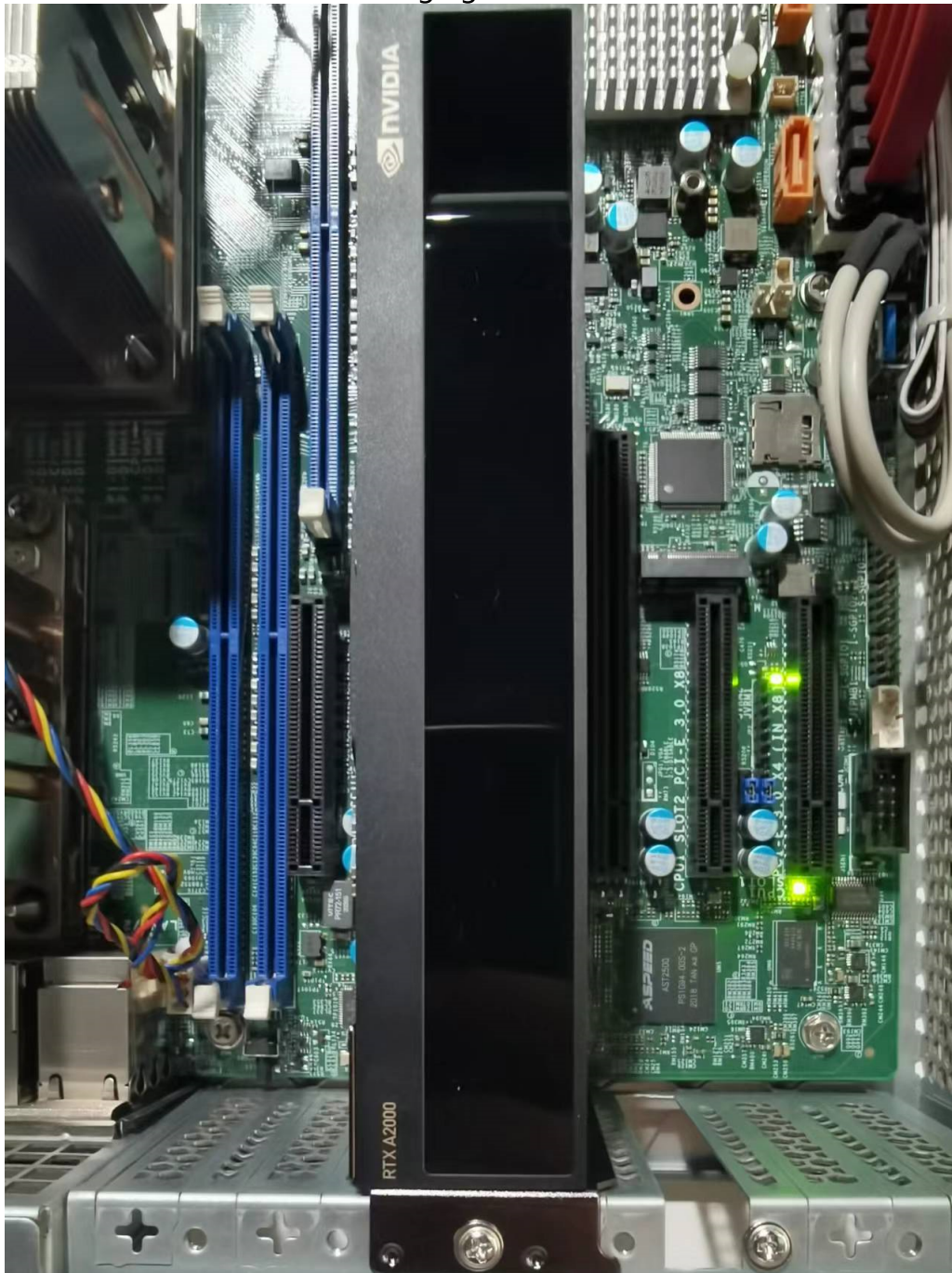
NVIDIA has limited the number of encodings for GPUs. You can visit the following link to confirm the number of encodings for specific models. Some graphics cards have only 3 transcoding sessions, and it is recommended to choose the Unrestricted type.

<https://developer.nvidia.com/video-encode-and-decode-gpu-support-matrix-new>

Consumer (GeForce)				Professional (NVIDIA RTX / Quadro)				Server (Data Center)				DGX	
<div> <input type="text" value="Search for names.."/></div>													
BOARD	FAMILY	CHIP	NVENC Generation	Desktop/ Mobile	# OF CHIPS	# OF NVENC /CHIP	Total # of NVENC	Max # of concurrent sessions	H.264 (AVCHD) YUV 4:2:0	H.264 (AVCHD) YUV 4:4:4	H.264 (AVCHD) Lossless	H.265 (HEVC) 4K YUV 4:2:0	
Quadro K620 / K1200	Maxwell (1st Gen)	GM107	4th Gen	D	1	1	1	3	YES	YES	YES	NO	
Quadro K2200	Maxwell (1st Gen)	GM107	4th Gen	D	1	1	1	Unrestricted	YES	YES	YES	NO	
Quadro M500M / M520M	Maxwell (1st Gen)	GM108	N/A	M	1	0	0	n/a	NO	NO	NO	NO	
Quadro M600M / M620M	Maxwell (1st Gen)	GM107	4th Gen	M	1	1	1	Unrestricted	YES	YES	YES	NO	
Quadro M1000M / M1200M / M2000M	Maxwell (1st Gen)	GM107	4th Gen	M	1	1	1	Unrestricted	YES	YES	YES	NO	
Quadro M2000	Maxwell (GM206)	GM206	5th Gen	D	1	1	1	Unrestricted	YES	YES	YES	YES	
Quadro M2200M	Maxwell (GM206)	GM206	5th Gen	M	1	1	1	Unrestricted	YES	YES	YES	YES	
Quadro M3000 / M4000 / M5500	Maxwell (2nd Gen)	GM204	5th Gen	M	1	2	2	Unrestricted	YES	YES	YES	YES	
Quadro M4000 / M5000	Maxwell (2nd Gen)	GM204	5th Gen	D	1	2	2	Unrestricted	YES	YES	YES	YES	
Quadro M6000	Maxwell (2nd Gen)	GM200	5th Gen	D	1	2	2	Unrestricted	YES	YES	YES	YES	
Quadro P500 / P520	Pascal	GP108	N/A	M	1	0	0	0	NO	NO	NO	NO	
Quadro P400	Pascal	GP107	6th Gen	D	1	1	1	3	YES	YES	YES	YES	



NVIDIA graphics cards are mostly PCIE interfaces, and the installation method can be referred to the following figure:

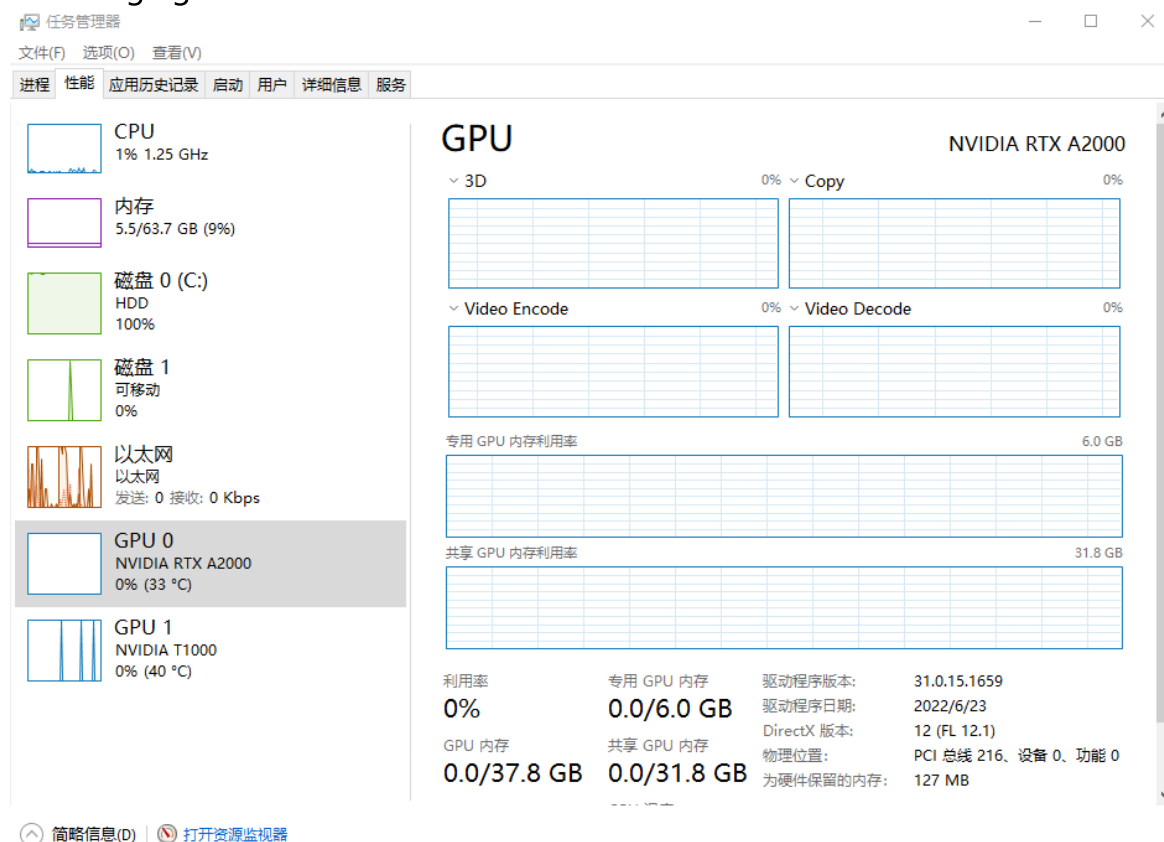


### Installation of GPU driver

NVIDIA graphics driver needs to be installed separately. You can download the corresponding driver from the following link.

<https://www.nvidia.com/download/index.aspx>

After the Windows driver is installed, the corresponding driver information can be displayed on the **Performance** page of the Task Manager. Refer to the following figure:



The installation of the NVIDIA driver for Linux is a bit troublesome. It is recommended to use Ubuntu 20.04, which comes with the NVIDIA GPU driver. Refer to the following figure for applying the driver, starting the software and updating it. Then select the driver, and it is recommended to choose tested, and then select Apply Changes.





Linux can check the working status of the GPU using nvidia-smi:

```
user@user-Super-Server:~$ nvidia-smi
Wed Sep  7 08:56:52 2022
+-----+
| NVIDIA-SMI 515.65.01    Driver Version: 515.65.01    CUDA Version: 11.7    |
+-----+
| GPU   Name               Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf    Pwr:Usage/Cap|      Memory-Usage | GPU-Util  Compute M. |
|=====-=~=~=~=~=~=~=~=|=|
| 0   NVIDIA RTX A2000     Off          | 00000000:3B:00.0 Off |          5%      Default |
| 33%   63C    P2      36W /  70W | 2104MiB / 6138MiB |              N/A |
+-----+
+-----+
| Processes:                                                       GPU Memory |
|  GPU   GI    CI          PID    Type   Process name                  Usage       |
|=====-=~=~=~=~=~=~=~=|=|
|  0   N/A   N/A       1379      G   /usr/lib/xorg/Xorg              4MiB       |
|  0   N/A   N/A       6953      C   ...nux-x86_64-64bit/h5ssmain 2093MiB    |
+-----+
```

### NVIDIA status display

If the GPU configuration is normal, the NVIDIA submenu option will appear during **transcoding**, where the ENC utilization rate will be relatively high. If the ENC reaches around 80%, it indicates that the resources have reached their limit. Refer to the following figure:



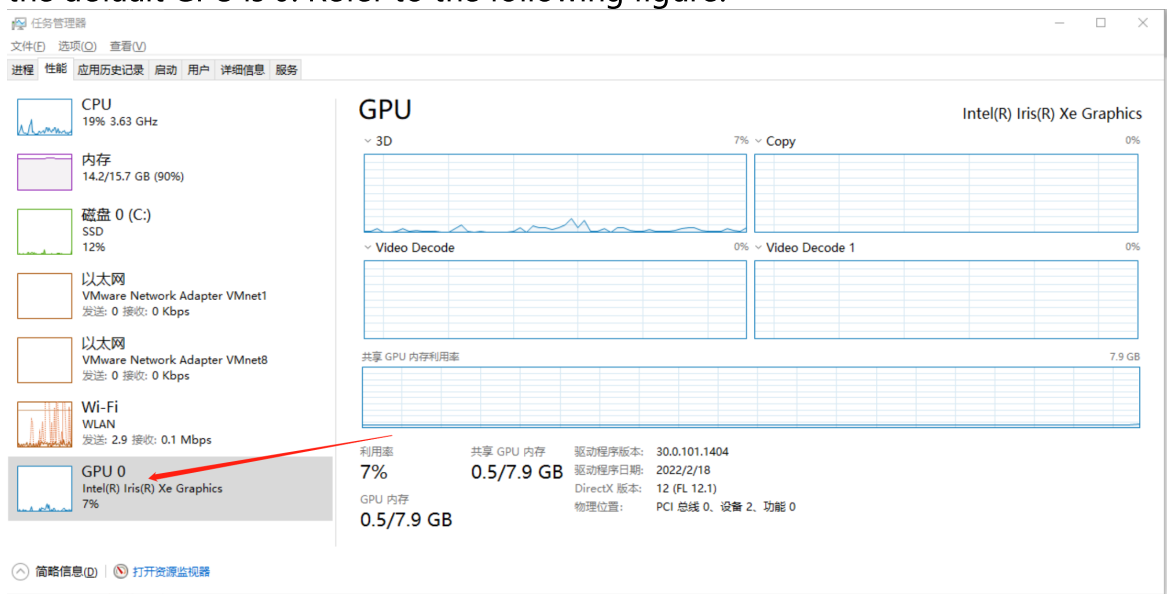
### 15.3.5 System GPU mode

#### System GPU mode

The system GPU mode uses the GPU acceleration transcoding that comes with the operating system, and can only support one graphics card.

#### Windows system GPU mode

As long as the GPU can be loaded by the Windows Task Manager, it can be used to accelerate transcoding. Only one graphics card can be supported, and the default GPU is 0. Refer to the following figure:



## Linux Rockchip system GPU mode

The H5S armv8 release includes the RK3568/RK3566/RK3588 transcoding-related driver components by default. After enabling GPU transcoding, you will see the transcoding resources as GPU in the transcoding status. Rockchip does not provide a resource utilization display.

### 15.3.6 TAV1 GPU mode

#### TAV1 GPU mode

TAV1 GPU mode refers to the use of TAV1 GPU transcoding cards, which only supports Linux platforms based on Intel CPUs.

The TAV1 GPU mode supports H265/H264/AV1 transcoding, and can be modified to the corresponding type in the default transcoding configuration or custom transcoding configuration. The AV1 type only takes effect in the RTC playback mode.

## 15.4 Video configuration

### Video loading image configuration

Find the video section in the configuration file (conf/h5ss.conf), as shown in the following figure:

```
282  "video": {  
283    "nLangComment": "language H5_LANG_CN/H5_LANG_EN",  
284    "nLang": "H5_LANG_CN",  
285    "bEnableShowLatestImageComment": "enable show latest video",  
286    "bEnableShowLatestImage": true,  
287    "strLoadingImageFileComment": "loading image filename",  
288    "strLoadingImageFile": "connecting.gif"  
289  },
```

By default, h5s stores the last I frame of the video in memory, so that the latest frame image will be loaded when the video is loaded. In some cases, this feature may not be needed. You can set `bEnableShowLatestImage` to false to prevent the display of the latest image and instead display the default image.

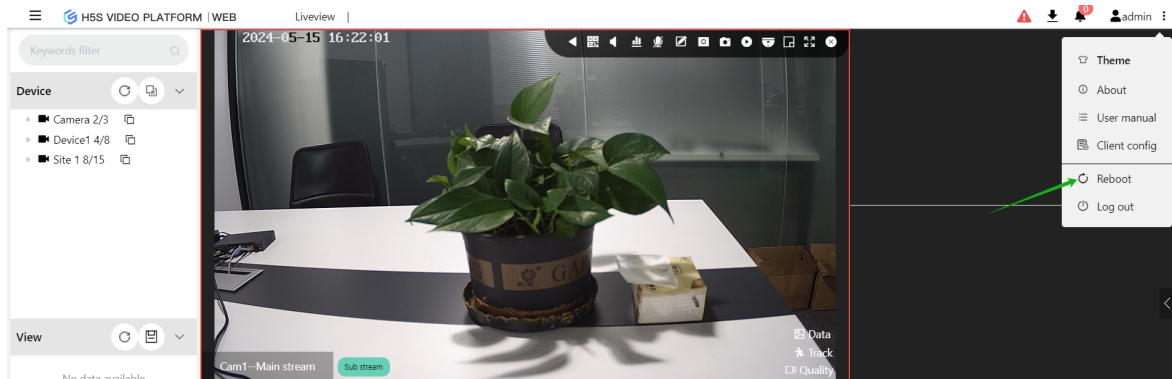
If the version is a group version, you can modify the default image. The publishing package includes a `connecting.gif`, or you can place a custom image in the `conf` directory and modify `strLoadingImageFile` to the corresponding file name to load the image before playback. If you do not need this feature, simply delete the corresponding image.

---

## 15.5 System restart

### System restart

If the H5S service is running, you can refer to the manual's installation section to restart it. H5S supports restarting from the interface, as shown in the following figure:



## 15.6 Automatic maintenance

### Automatic restart

Enter **Setting-» Systeminfo-» System maintenance-» Automatic Maintenance** to set the system to restart periodically. By default, the system does not restart periodically, but you can choose the frequency and time of the scheduled restart.

## 15.7 Restore default configuration

### Restore default configuration

First, backup the conf/h5ss.conf file, then delete it and restart the system. The system will restore the default configuration.

## 15.8 Log configuration

### Log configuration

Go to **Setting-» System-» Logs** to configure the log level and log cycle coverage. Restart is required after modification.

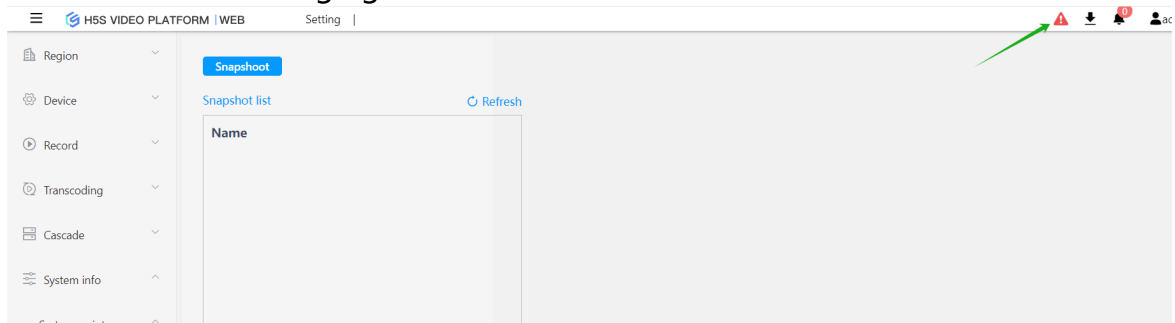
## 15.9 Configure snapshots

### Configure snapshots

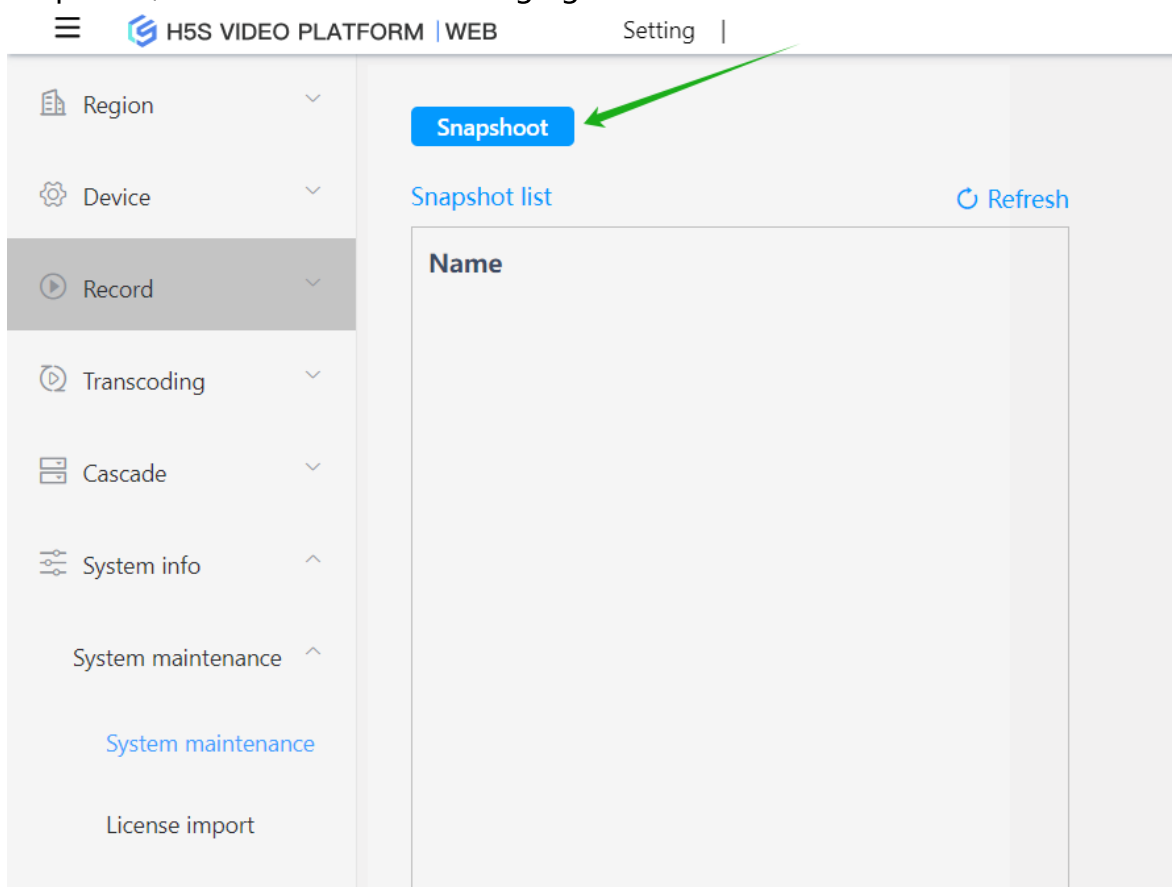
The H5S configuration is based on the configuration file, which is conf/h5ss.conf. To prevent accidental damage to the configuration file, it is recommended to take a snapshot of the configuration before entering the

production environment. If the configuration is accidentally damaged, the system will start from the most recent snapshot configuration.

If the system has not taken a snapshot, the system will give an alarm prompt, as shown in the following figure:



Enter **Setting-» System Maintenance-» System Maintenance** to configure snapshots, as shown in the following figure:



## 15.10 License import

### License import

If you are using a test license and the current system is already running normally, go to **Setting-» Systeminfo-» System Maintenance-» License**

---

**import** to import a new license. If the system is not running with a license, you can refer to the manual installation section to import it. After modification, you need to restart.

## 15.11 Production environment configuration

### Production environment configuration

Before the development is completed and entered into the production environment, it is recommended to add a configuration snapshot to the management page configuration section and modify the log to a circular overwrite mode. If it is Linux, please refer to the installation section for system optimization. You can refer to the manual **Linux Performance Improvement Configuration Log Configuration Configuration Snapshot**.

## 15.12 Product customization

### Product customization

Starting from r17, you can modify the interface icons or names based on the actual project. To do so, go to **Setting-» Customization** and modify the relevant content. You can download existing images and modify new images based on their dimensions.

☰

H5S VIDEO PLATFORM | WEB

Setting |

Region

Device

Record

Transcoding

Cascade

System info

Protocol

Map

Cluster

Camera points


AI

Customization


Customization

Custom ico

Icon download.ico



Please select file



Default

Save

Custom logo


Logo download

Simplifier

▼

H5S VIDEO PLATFORM | WEB

Please select file



Support svg format

Default

Save

Customize login logo

Logo download

Simplif

▼

H5S video platform, version 18

All rights reserved©linkingvision





## 16.Reverse proxy

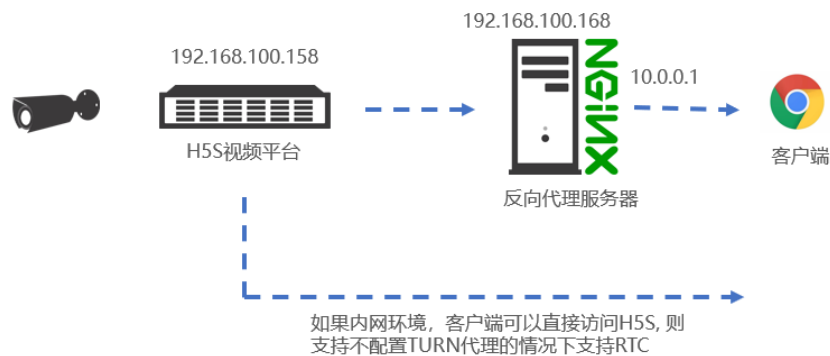
---

## 16 Reverse proxy

### Introduction to Reverse Proxy

Due to the complexity of business, enterprise applications will use NGINX proxy for many services during actual use, and then expose a public domain name or IP address for use. This chapter uses Centos 7 (applicable to RockyLinux 8) as an example for configuration. The following figure shows two IP addresses for the reverse proxy server, one is 192.168.100.168, and the other is 10.0.0.1.

After configuring the proxy, all environments support WS; however, if the client can directly access H5S, it can also be accessed after configuring the reverse proxy with RTC. If the client cannot access H5S, TURN needs to be configured.



### Preparing the NGINX Environment

First install nginx. If it has already been installed, you can ignore it.

```
#yum install nginx
```

You can use the following command to reload the configuration of nginx:

```
#nginx -s reload
```

Copy the www directory from the H5S release package to /usr/share/nginx. For specific results, refer to the following figure:

```

[root@localhost www]# pwd
/usr/share/nginx/www
[root@localhost www]# ll
total 148
-rw-r--r--. 1 root root 2926 May 17 22:25 cluster.html
-rw-r--r--. 1 root root 6489 May 17 22:25 conference.html
drwxr-xr-x. 2 root root 271 May 17 22:25 css
-rw-r--r--. 1 root root 5066 May 17 22:25 demo.html
drwxr-xr-x. 2 root root 88 May 17 22:25 doc
drwxr-xr-x. 3 root root 21 May 17 22:24 domain
-rw-r--r--. 1 root root 1596 May 17 22:25 event.html
-rw-r--r--. 1 root root 2050 May 17 22:25 experiment.html
-rw-r--r--. 1 root root 4286 May 17 22:25 favicon.ico
-rw-r--r--. 1 root root 937 May 17 22:25 flv.html
drwxr-xr-x. 2 root root 209 May 17 22:25 fonts
-rw-r--r--. 1 root root 1996 May 17 22:25 hls.html
drwxr-xr-x. 2 root root 75 May 17 22:25 img
-rw-r--r--. 1 root root 7841 May 17 22:25 index.html
drwxr-xr-x. 2 root root 4096 May 17 22:25 js
-rw-r--r--. 1 root root 4201 May 17 22:25 linkweb.html
-rw-r--r--. 1 root root 4031 May 17 22:25 pbcontrol.html
-rw-r--r--. 1 root root 2070 May 17 22:25 playback.html
-rw-r--r--. 1 root root 4141 May 17 22:25 playback2.html
-rw-r--r--. 1 root root 3088 May 17 22:25 rtc.html
-rw-r--r--. 1 root root 3193 May 17 22:25 rtc2.html
-rw-r--r--. 1 root root 6118 May 17 22:25 rtcpush.html
-rw-r--r--. 1 root root 1074 May 17 22:25 rtmp.html
-rw-r--r--. 1 root root 1157 May 17 22:25 rtmp2.html
-rw-r--r--. 1 root root 4207 May 17 22:25 serverfilepb.html
-rw-r--r--. 1 root root 4158 May 17 22:25 serverpb.html
drwxr-xr-x. 4 root root 28 May 17 22:24 single
-rw-r--r--. 1 root root 11340 May 17 22:25 single.html
drwxr-xr-x. 6 root root 51 May 17 22:24 static
drwxr-xr-x. 2 root root 127 May 17 22:25 swf
-rw-r--r--. 1 root root 1513 May 17 22:25 tool.html
-rw-r--r--. 1 root root 4677 May 17 22:25 tour.html
-rw-r--r--. 1 root root 3214 May 17 22:25 ws.html
[root@localhost www]# █

```

Disable SeLinux and firewall. If you need to enable the firewall, you can configure rules as needed.

```
#setenforce 0
```

```
#systemctl stop firewalld
```

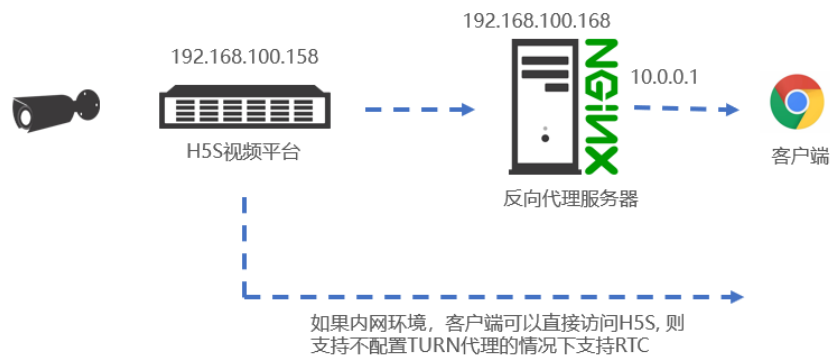
## H5S environment preparation

For testing convenience, it is necessary to add a video source with a token of token1 in H5S. ws.html rtc.html will default to the video source with token1.

## 16.1 Basic proxy

### Basic proxy

The basic proxy is an NGNIX proxy for one H5S. Refer to the following figure:



Modify the `/etc/nginx/nginx.conf` to the following configuration, and reload the configuration after modification:

```
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;

include /usr/share/nginx/modules/*.conf;

events {
    worker_connections 1024;
}

http {
    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
        '$status $body_bytes_sent "$http_referer" '
        '"$http_user_agent" "$http_x_forwarded_for"';

    access_log /var/log/nginx/access.log main;

    sendfile        on;
    tcp_nopush      on;
    tcp_nodelay      on;
    keepalive_timeout 65;
```

```
types_hash_max_size 2048;

include      /etc/nginx/mime.types;
default_type application/octet-stream;

include /etc/nginx/conf.d/*.conf;

server {
    listen      80 default_server;
    listen     [::]:80 default_server;
    server_name _;
    root        /usr/share/nginx/www;

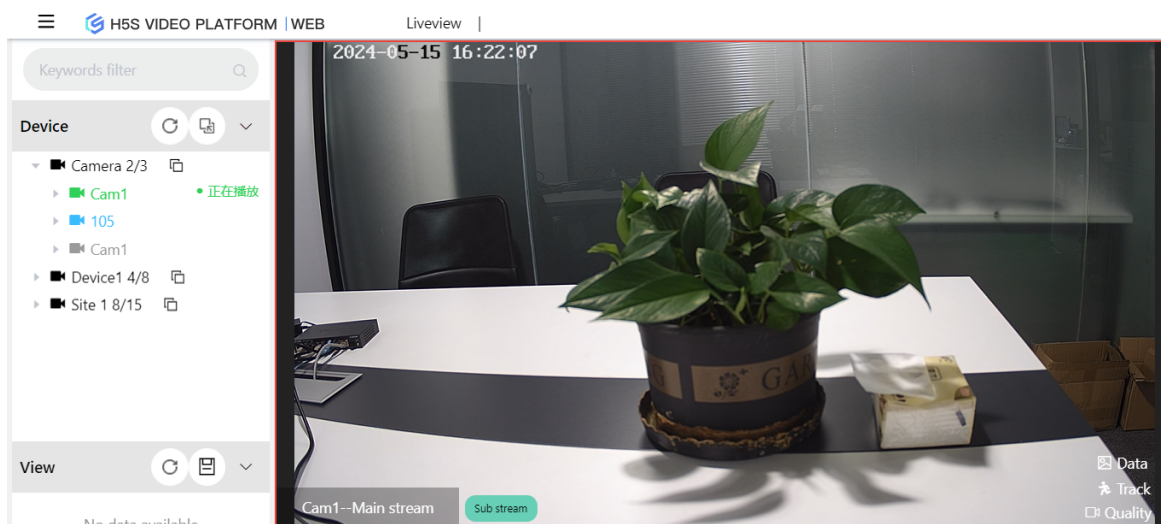
    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    location / {
    }
    location /api/v1/ {
        proxy_pass http://192.168.100.158:8080;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
    }

    error_page 404 /404.html;
        location = /40x.html {
        }

    error_page 500 502 503 504 /50x.html;
        location = /50x.html {
        }
    }
}
```

Then enter `http://10.0.0.1/` in the browser to log in to H5S and view the video

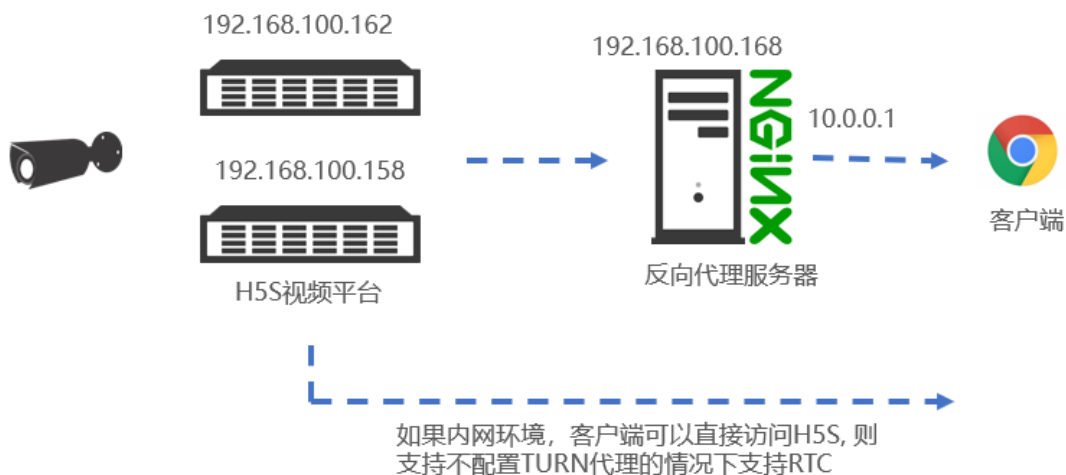


You can also use the single-page access tool to access the video:  
<http://10.0.0.1/ws.html?token=token1>

## 16.2 load balancing

### Load balancing proxy

The load balancing proxy is an NGINX proxy that multiplexes multiple H5S, each of which is configured with the same video source and token. This allows NGINX to select backend servers for streaming based on policy. Refer to the following diagram:



Modify the `/etc/nginx/nginx.conf` to the following configuration, and reload the configuration after modification:

```
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;

include /usr/share/nginx/modules/*.conf;

events {
    worker_connections 1024;
}

http {
    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
        '$status $body_bytes_sent "$http_referer" '
        '"$http_user_agent" "$http_x_forwarded_for"';

    access_log /var/log/nginx/access.log main;

    sendfile        on;
    tcp_nopush      on;
    tcp_nodelay      on;
    keepalive_timeout 65;
    types_hash_max_size 2048;

    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    include /etc/nginx/conf.d/*.conf;

    upstream h5sbackend {
        #least_conn;
        #random;
        #ip_hash;
        server 192.168.100.158:8080;
        server 192.168.100.162:8080;
    }

    server {
        listen 80 default_server;
        listen [::]:80 default_server;
        server_name _;
```

---

```
root    /usr/share/nginx/www;

# Load configuration files for the default server block.
include /etc/nginx/default.d/*.conf;

location / {
}

location /api/v1/ {
    proxy_pass http://h5sbackend/api/v1/;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
}

error_page 404 /404.html;
    location = /40x.html {
}

error_page 500 502 503 504 /50x.html;
    location = /50x.html {
}
}
```

You can use the single-page access tool to access the video, which will be forwarded from different H5S according to the policy:

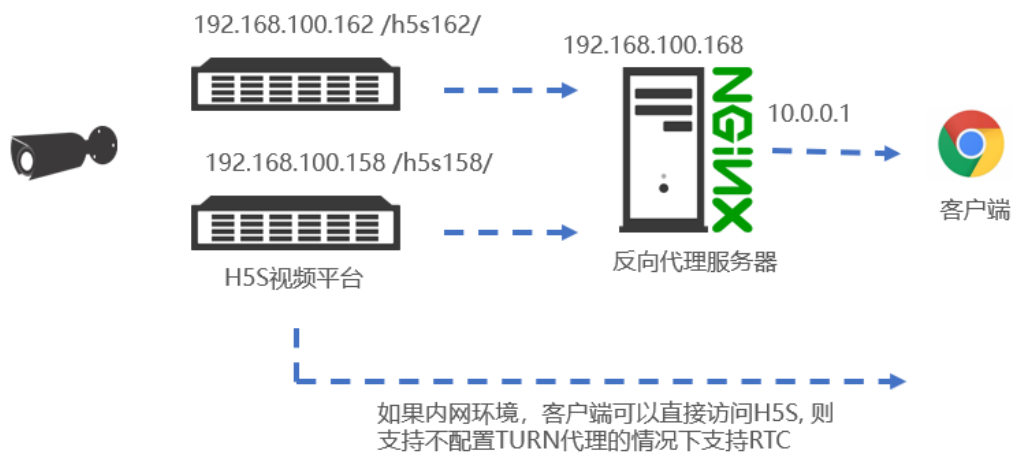
<http://10.0.0.1/ws.html?token=token1>

## 16.3 Specify proxy

### Specify proxy

The basic proxy is an NGINX proxy that handles multiple H5S, each with a different video source configuration. The business program knows which H5S service the token is on, so it can use a specified proxy mode. This allows NGINX to find the correct H5S based on the API path. Refer to the following diagram:





Modify the `/etc/nginx/nginx.conf` to the following configuration, and reload the configuration after modification:

```
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;

include /usr/share/nginx/modules/*.conf;

events {
    worker_connections 1024;
}

http {
    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
        '$status $body_bytes_sent "$http_referer" '
        '"$http_user_agent" "$http_x_forwarded_for"';

    access_log /var/log/nginx/access.log main;

    sendfile        on;
    tcp_nopush      on;
    tcp_nodelay      on;
    keepalive_timeout 65;
    types_hash_max_size 2048;

    include          /etc/nginx/mime.types;
```

---

```
default_type    application/octet-stream;

include /etc/nginx/conf.d/*.conf;

server {
    listen      80 default_server;
    listen      [::]:80 default_server;
    server_name _;
    root        /usr/share/nginx/www;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    location / {

location /h5s158/api/v1/ {
    proxy_pass http://192.168.100.158:8080/api/v1/;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
}

location /h5s162/api/v1/ {
    proxy_pass http://192.168.100.162:8080/api/v1/;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
}

error_page 404 /404.html;
    location = /40x.html {
    }

error_page 500 502 503 504 /50x.html;
    location = /50x.html {
    }
}
}
```

Modify ws.html under /usr/share/nginx/www, and change rootpath (default is '/') to '/h5s158/' corresponding to the path in the configuration. If it is /h5s158/,

request from the 158 H5S service, and if it is /h5s162/, request from the 162 H5S service.

```
70
71     var conf1 = {
72         videoId: 'h5sVideo1',
73         protocol: window.location.protocol, //'http:' or 'https:'
74         host: window.location.host, //'localhost:8080'
75         rootpath: '/h5s158/' // '/'
76         token: strToken,
77         streamprofile: strStream, // {string} - stream profile, main/sub or other predefined transc
78         hlsver: 'v1', //v1 is for ts, v2 is for fmp4
79         session: strSession, //session got from login
80         consolelog: 'true' // 'true' or 'false' enable/disable console.log
81     };
82
83     var v1 = new H5sPlayerWS(conf1);
84     if (GetURLParameter("autoplay") != undefined)
85     {
86         $('#h5sVideo1').prop("muted", true);
87         function autoplayFunction()
88         {
89             timer=setTimeout(function(){
90                 $('#h5sVideo1').parent().click()
91                 $('#playpause1').fadeOut();
92             },0);
93             return timer;
94         }
95         autoplayFunction();
```



## 17.Reinforcement Guidelines

---

---

## 17 Reinforcement Guidelines

### Reinforcement Guidelines

Hardening is a method of enhancing software network security to improve network defense capabilities. The following provides specific methods for hardening.

### 17.1 User management

If the version is 14.15 or later, in addition to retaining the user manual, the following reinforcement methods are enabled by default in the version.

#### Change password to strong password

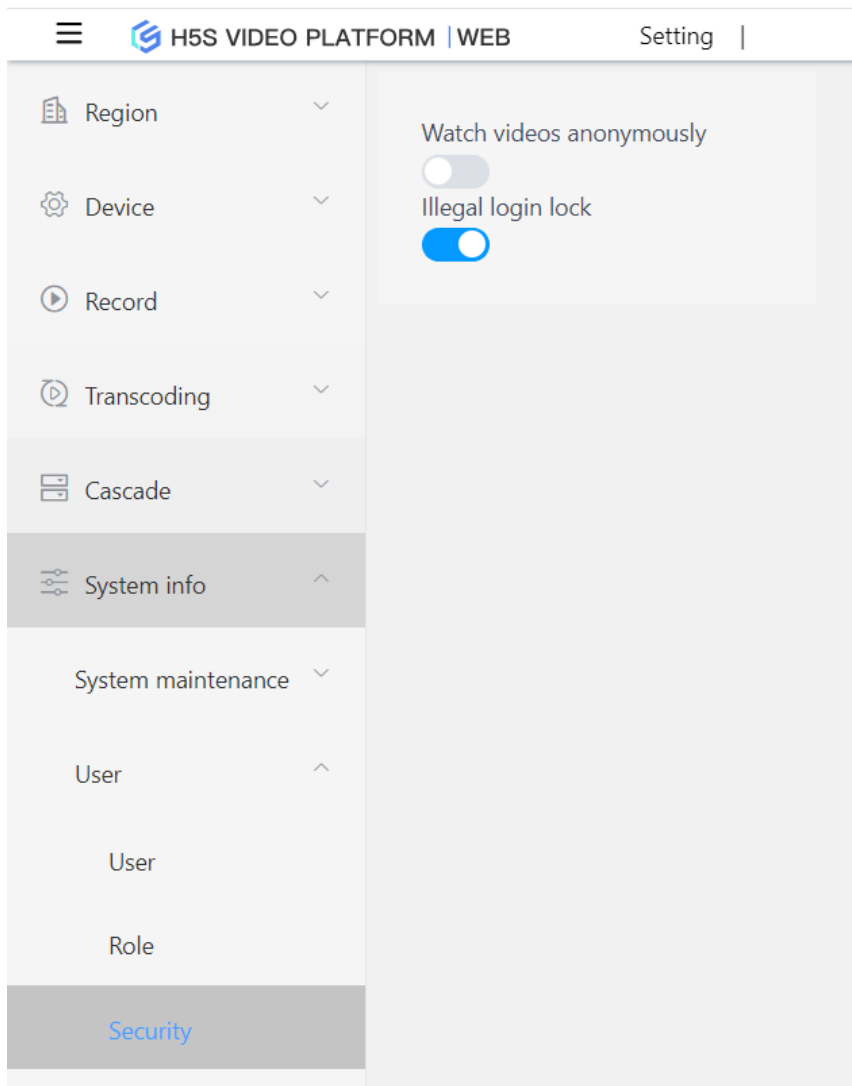
Go to **Setting-» Systeminfo-» User-» User** to change the passwords of all accounts. It is recommended that the passwords meet the following requirements:

1. The password length should be at least 8 characters.
2. The password must contain at least one uppercase letter.
3. The password must contain at least one lowercase letter.
4. The password must contain at least one number.
5. The password should contain at least one special character, such as @, #, &, etc.
6. The password cannot contain two consecutive numbers that increase or decrease. For example, 12, 321, 5678, etc.
7. The password cannot contain the user name.

#### Turn off anonymous browsing and turn on illegal login lock

Anonymous browsing allows users to view videos without logging in. It is recommended to completely disable anonymous browsing in production environments, especially on uncontrolled networks.

Enter **Settings-» System-» Users-» Security Management**. Turn off anonymous browsing and turn on illegal login lockout. Red indicates off and green indicates on. After modification, you need to restart, as shown in the following figure:



### Delete the relevant online documents

After deploying to the production environment, delete the online API documentation and operation documentation to prevent them from being stolen. The documentation is located in `www/doc` under the installation directory, with file names of **api.html** and **H5S Video Platform User Manual-zh.chm**.





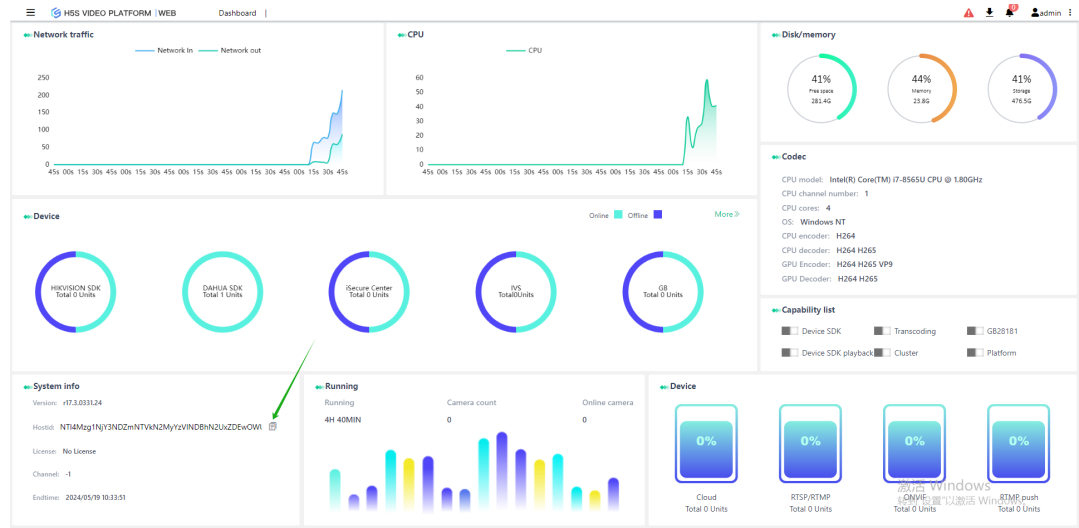
## 18.Appendix A FAQ

---

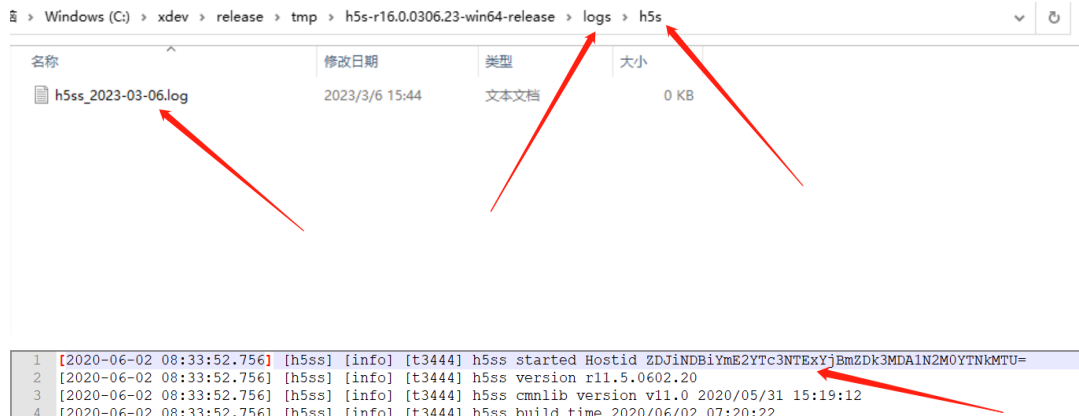
## 18 Appendix A FAQ

### 1. How to obtain a test license?

You can log in to the H5SWeb dashboard and click the copy button next to the HostID.



You can also open the directory logs/h5s/ and copy the hostid (r15 and earlier versions are in the logs directory, while r16 and later versions are in the logs/h5s directory). To prevent copying hostids generated on other machines, it is recommended to delete all log files in the h5s directory before starting h5s. The path can be referred to in the following figure:



Send the HostID and company name and address to [info@linkingvision.com](mailto:info@linkingvision.com) to obtain a test license

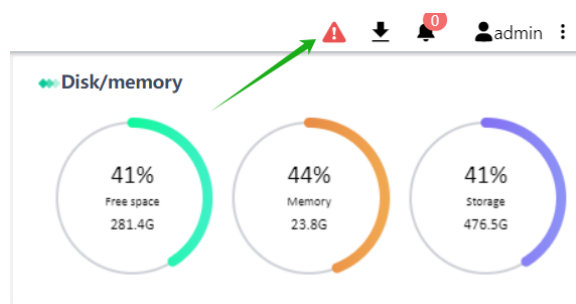
If you replace the new license, please delete or move the old license file from the conf directory. Do not back up to the conf directory. H5S reads the license file based on the file extension.

## 2. h5s service failed to start?

h5s uses multiple network ports to provide different services. The default ports are 18085 (r16 and later versions), 8080 (r15 and earlier versions), 18445 (r16 and later versions), 8443 (r15 and earlier versions), 8554, 8555, 8935, 8936, 8890, 8891, 18000 (r15.5 and later versions are defaulted to 18005), and 18005. These ports belong to the http rtsp rtmp flv services, and you can check for port conflicts. Sometimes you accidentally click gencertificate.bat, which resets the certificate. In this case, you need to restore the files under the certificate directory from the release package.

## 3. What is the function of the warning sign in the upper right corner of the configuration interface?

If you do not take a snapshot of the configuration, the system will prompt you in the upper right corner of the interface. It is recommended to take a snapshot after configuring the system and adding cameras or hard disk video recorders to prevent accidental configuration loss. If the accidental configuration is destroyed, the system will start from the latest snapshot.



## 4. How to configure the production environment?

Before the development is completed and enters the production environment, it is recommended to add a configuration snapshot to the management page configuration section and modify the log to a circular overwrite mode. If it is Linux, please refer to the installation section for system optimization.

## 5. Is there any naming rule for tokens in h5s?

The token of h5s is composed of letters and numbers, supports a single hyphen and underscore, and does not support special characters (such as @#\$ etc.). Correct examples include token1\_1 token1-1. Double

---

hyphens are not supported, and examples of unsupported tokens include token1--1.

**6. Can the installation path of h5s contain Chinese characters?**

h5s Windows version Linux installation path does not support Chinese.

**7. The h5s configuration file has been restored to its default state?**

H5S uses a JSON-formatted configuration file, which is prone to formatting errors when manually edited. It is recommended to use Notepad++ to modify the configuration file.

**8. How to configure the on-demand stream retrieval from the camera?**

The old version of H5S always obtains the code stream from the camera by default. You can modify the nConnectType in the source section of the configuration file h5ss.conf to H5\_ONDEMAND. Here, you modify the top-level configuration, rather than modifying each channel.

The old version of H5S always obtains the code stream from the Device SDK by default. You can modify the nConnectType in the device section of the configuration file h5ss.conf to H5\_ONDEMAND. This is the top-level configuration that needs to be modified.

**9. How to configure the camera to always obtain the code stream?**

The system fetches the code stream from the camera as needed by default. You can modify the nConnectType in the source section of the configuration file h5ss.conf to H5\_ALWAYS. This changes the top-level configuration, not each channel.

The system fetches the code stream from the Device SDK as needed by default. You can modify the nConnectType in the device section of the configuration file h5ss.conf to H5\_ALWAYS, which is the top-level configuration.

**10. Does the cloud streaming mode require configuration on the cloud?**

No, only the configuration of the local cloud part needs to be configured. Note that bEnable should be changed to true.

### 11. How to turn on the pre-recording function (obsolete)?

The pre-record function is disabled by default. Modify `bEnablePreRecord` to true to enable pre-record. Note that all channels will remain in streaming state after enabling pre-record.

### 12. What causes API login failure?

The password in the system needs to be encrypted using md5. If it is js, you can refer to [www/tool.html](http://www/tool.html).

### 13. What is the default password for h5s?

12345, the 827ccb0eea8a706c4c34a16891f84e7b in the configuration file is md5. Starting from version 14.15, the default password is Vision@168. If the user logs in for the first time, they are forced to change the default password. For password rules, please refer to the interface prompt. If the password is forgotten, you can modify the `strPasswd` field of admin in the `conf/h5ss.conf` configuration file to `ddc2f0ff1aab61a5a34a83514e47ed83`, which will change the default password to Vision@168. Please use Notepad++ to modify the configuration file. Before modifying, please stop H5S and backup the configuration file.

```
{
  "user": {
    "bTokenAuthComment": "token auth in the http header cookie for all api",
    "bTokenAuth": true,
    "bAnonymousViewComment": "allow anonymous user view video",
    "bAnonymousView": false,
    "bLoginLockComment": "The illegal log in lock",
    "bLoginLock": true,
    "users": [
      {
        "strUserComment": "Username",
        "strUser": "admin",
        "strPasswdComment": "Password MD5 hashed, default Vision@168",
        "strPasswd": "ddc2f0ff1aab61a5a34a83514e47ed83",
        "strUserTypeComment": "User type Administrator/Operator",
        "strUserType": "Administrator",
        "strRole": "Administrator"
      }
    ]
  }
},
```

### 14. Why can't I play the video from WebRTC?

The port for playing video over WebRTC is dynamic and requires opening the firewall to allow TCP. If you are using an AliCloud public IP address and cannot see it on your local machine, you need to set `bCloudMode` to true and fill in the corresponding public IP address in `strRelatedPublicIp`.

---

**15. How can I play a video in WeChat for less than 1 second?**

iOS 11 and above versions support WebRTC, which can achieve a latency of less than 1 second. On Android, if ws.html cannot be played, it is recommended to restore the webview kernel. The specific method is to visit debugtbs.qq.com in WeChat, click Clear TBS Kernel, and display the successful removal of the x5 kernel. After that, it will be restored to the Chrome kernel.

**16. The system Log contains too much content, and the disk is full. Is there a way to delete it regularly?**

Yes, refer to the manual **system configuration-》 log configuration**.

**17. All logs appear normal, but videos cannot be played on the webpage. What is the general reason?**

Some new ONIVF cameras may have h.265 as the default main stream, which can be changed to a secondary stream or the encoding format can be changed to h.264.

**18. How to use WebRTC to play video?**

Reference Manual Real-time **Video-》 RTC WS Playback Mode**.

**19. If it cannot run after installation on Windows Server 2008, 2012, 2016 or other Windows versions?**

If the software cannot be run after Windows installation, please download the following 5 packages or download them from the following link:

<https://linkingvision.com/download/h5stream/win/VisualC%2B%2BRedistributable/>

Please install in order, 2008, 2010, 2013, 2015-2019. If there is an installation failure, please update the operating system in the System and Security check update in the Control Panel

If Windows 2012 still cannot solve the problem, please refer to the following link:

[https://answers.microsoft.com/en-us/windows/forum/windows8\\_1-windows\\_install/api-ms-win-crt-string-1-1-0dll-and-others-missing/85a91890-ed8a-4e6e-8f94-b53639c39970?auth=1](https://answers.microsoft.com/en-us/windows/forum/windows8_1-windows_install/api-ms-win-crt-string-1-1-0dll-and-others-missing/85a91890-ed8a-4e6e-8f94-b53639c39970?auth=1)

## 20. How to optimize the slow display of the first frame image of the video?

The speed of the first frame image depends on the I-frame interval. Generally, the default configuration of the network camera is 25 or 50. You can change it to 20 and observe again. This value cannot be changed too small, otherwise it will affect the image quality.

## 21. How to open HLS?

The H5S HLS Server is disabled by default. If you need the HLS function, you need to modify the configuration file as follows.

```
"hls": {  
  "nHLSSinkTypeComment": "HLS Sink type H5_HLS_NONE/H5_HLS_V1(ts)/H5_HLS_V2(mp4)",  
  "nHLSSinkType": "H5_HLS_V1",  
  "nHLSSegmentNumComment": "HLS Segment number",  
  "nHLSSegmentNum": 4,  
  "nHLSDurationComment": "HLS Segment duration",  
  "nHLSDuration": 2  
},  
"hlsSinkType": "
```

## 22. How to enable Chrome autoplay video mode?

Starting from r11.3, ws.html and rtc.html have added support for autoplay,

You can add autoplay=true.

<http://192.168.100.122:8080/rtc.html?token=token1&autoplay=true>

<http://192.168.100.122:8080/ws.html?token=token1&autoplay=true>

## 23. Chrome and Firefox video is not working on Windows Server version?

Most browsers use the GPU for HTML5 decoding and rendering. If you cannot see the video on the server version, we recommend switching to a desktop or laptop computer, and we suggest using Windows 10 for testing.

## 24. How can I quickly upgrade h5s?

The configuration and lic files of the old version of h5s are applicable to the new version. When upgrading, first back up the conf directory, and then copy the files under the conf directory to the new version's conf directory.

If you need to keep old versions of videos, you can cut or copy the db and www/mediastore directories to the new version.

---

## 25. Can the mediastore directory under www be modified?

Starting from 9.1, the mediastore supports absolute path configuration for video recording locations. Modify bEnableStorPath to true and modify the corresponding strRoot. Currently, only one path configuration is supported, and multiple paths are not supported.

```
"storage": {
  "bEnableStorPathComment": "enable storage path, default path is www/mediastore",
  "bEnableStorPath": false,
  "vol": [
    {
      "strLocationComment": "virtual path in http",
      "strLocation": "/mediastore",
      "strRootComment": "root path of this volume, absolute path",
      "strRoot": "d:/"
    }
  ]
},
```

## 26. How to make the GB28181 device register with h5s again?

Sometimes after adding or deleting channels on the GB28181 device, the h5s does not receive the change information in a timely manner. You can use the following method of forced deregistration and re-registration.

This method is used to modify the port of the SIP service. For example, if the correct port is 5060, first modify it to an incorrect port such as 5080, save the configuration, and then change it back to 5060 and save the configuration. In this way, the device will be deregistered and re-registered with h5s.

SIP服务器地址	<input type="text" value="192.168.100.131"/>	✓
SIP服务器端口	<input type="text" value="5060"/>	✓

## 27. The Linux version device SDK driver cannot be loaded?

Sometimes users are unable to add SDK devices on Linux. After upgrading to a new version, they still cannot add SDK devices. They can refer to the Chinese manual and re-register the service.

## 28. Why can only one of the multiple national standard devices on the same local area network play video?

If H5S is deployed on the cloud, the SIP ports of multiple intranet devices may be the same, which can cause SIP message mapping errors for multiple devices. You can modify the SIP local port to a different port by referring to the following figure.



SNMP FTP Email **平台接入** HTTPS QoS 802.1x 集成协议 网络服务

平台接入方式: 28181

本地SIP端口: 5002 ✓

传输协议: UDP

白名单: 编辑

平台1 平台2

☒ 启用

协议版本: GB/T28181-2016

SIP服务器ID: 34020000002000000001 ✓

SIP服务器域: 3402000000 ✓

SIP服务器地址: 192.168.100.137 ✓

SIP服务器端口: 5060 ✓

SIP用户名: 34020000001180010701 ✓

SIP用户认证ID: 34020000001180010701 ✓

密码: .....

密码确认: .....

注册有效期: 3600 ✓ 秒

注册状态: 在线

心跳周期: 30 ✓ 秒

28181码流索引: 子码流

注册间隔: 60 ✓ 秒

最大心跳超时次数: 3 ✓

编码ID: 视频通道编码ID

通道号	视频通道编码ID
1	34020000001320010701

## 29. AXIS camera ONVIF access can not see the video?

AXIS ONVIF has replay attack protection enabled by default. One method is to synchronize the time and time zone of the h5s server and the AXIS camera.

Another way is to turn off the function on the camera.



Enter the general configuration, or manually enter it by replacing the following link with the actual IP address 10.0.0.148.

<http://10.0.0.148/admin/config.shtml?aca=yes>

Make sure Enable replay attack protection: is turned off.

The plain config page allows direct access to all the configurable parameters supported by the AXIS P1365 Mk II Network Camera. This page uses no extra scripts (Javascript or otherwise) and should function correctly in any browser or PDA. Select the parameter group to modify and configure the settings directly.

For help on parameters, please refer to the relevant help page available from the standard setup tools.  
Select a group of parameters to modify:

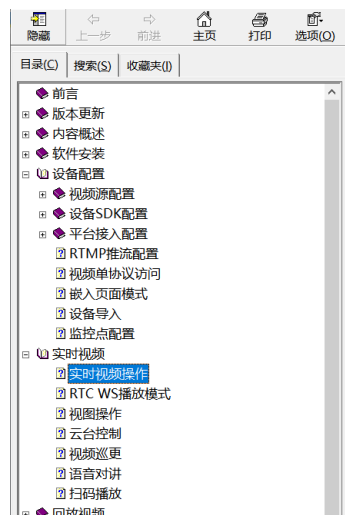
WebService

#### WebService

WebService UsernameToken:  
Enable replay attack protection: ☐  
Save page changes:

### 30. The right margin of the chm format document cannot be displayed?

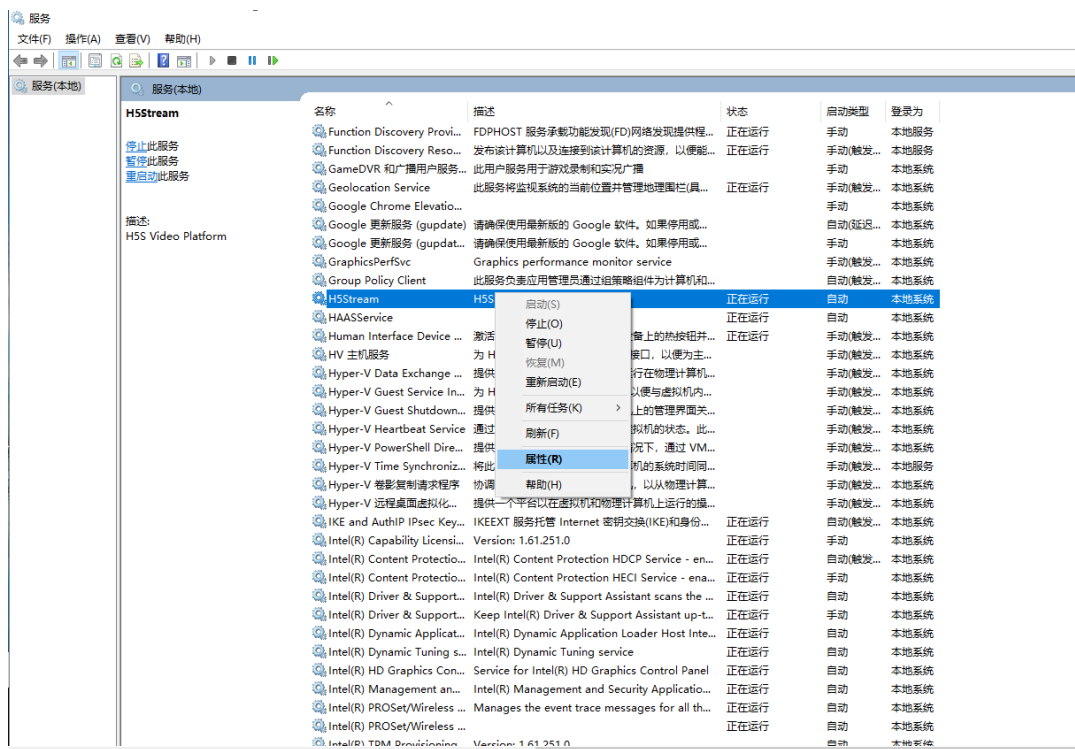
As shown in the figure below, the right side of the chm document is blank. You can cancel the prompt that **always asks before opening the file** when opening it.



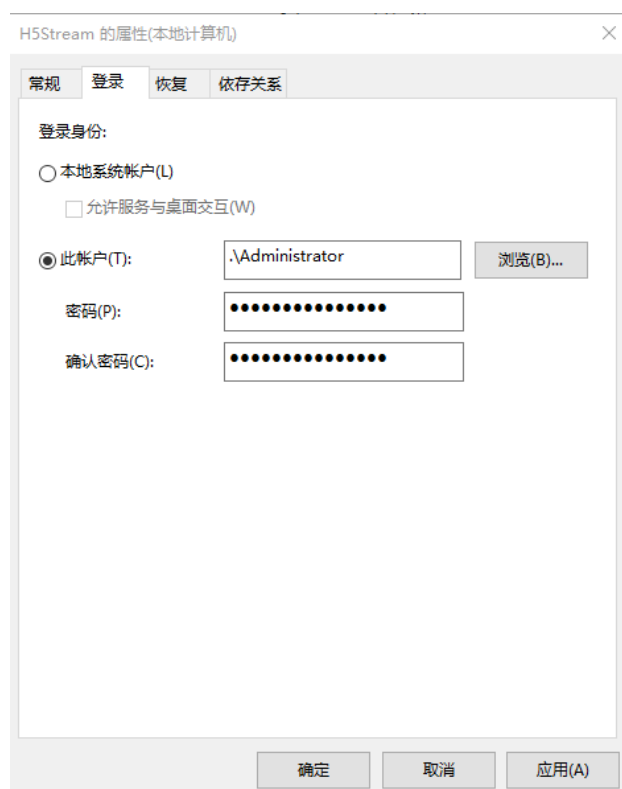


### 31. The Windows platform runs normally manually, but the service fails to start?

If the service runs normally manually on the Windows platform but fails to run, you can specify the account for the service to run to solve the problem. Refer to the following figure to open the service management tool:



Refer to the figure below and enter the system administrator account name and password in this account:



### 32. Can the RTSP/RTMP standard protocol be forwarded without the session parameter to play?

Starting from r15.1, the RTSP/RTMP standard protocol forwarding session parameter is required, and it is not required in versions prior to r15. However, in some cases, the RTSP/RTMP client cannot obtain the session. In this case, you can disable the session authentication for the RTSP/RTMP standard protocol forwarding (**it is recommended not to disable it in cases where the network is not controllable, as this poses a risk to information security**). However, the session parameter must be provided, and you can provide a fake value. Disabling session authentication requires modifying the conf/h5ss.conf configuration file. It is recommended to stop the service and back up the configuration before modifying it, and use notepad++ to modify it. After modifying the three parameters in the figure below to false, the RTSP/RTMP standard protocol forwarding session authentication is disabled. Refer to the following figure:

```

28  "rtsp": {
29    "bRTSPSinkComment": "Enable RTSP Server",
30    "bRTSPSink": true,
31    "nRTSPPortComment": "RTSP server port",
32    "nRTSPPort": 8554,
33    "nSSLPortComment": "RTSP over SSL server port",
34    "nSSLPort": 8555,
35    "bAuthComment": "Enable authentication for RTSP/RTSP over SSL",
36    "bAuth": true
37  },
38  "rtmp": {
39    "bRTMPSinkComment": "Enable RTMP Server",
40    "bRTMPSink": true,
41    "nRTMPPortComment": "RTMP server port",
42    "nRTMPPort": 8935,
43    "nSSLPortComment": "RTMP over SSL server port",
44    "nSSLPort": 8936,
45    "bAuthComment": "Enable authentication for RTMP/RTMP over SSL",
46    "bAuth": true
47  },
48  "flv": {
49    "bFLVSinkComment": "Enable FLV Server",
50    "bFLVSink": true,
51    "nFLVPortComment": "FLV server port",
52    "nFLVPort": 8890,
53    "nSSLPortComment": "FLV over SSL server port",
54    "nSSLPort": 8891,
55    "bAuthComment": "Enable authentication for FLV/FLV over SSL",
56    "bAuth": true
57  },

```

**33. When cascading, the lower level pushes the disabled channel to the upper level. Can we prevent the upper level from seeing it?**

Yes, after the subordinate has disabled all channels, it can be restarted, so that the superior will not see the disabled channels of the subordinate.

**34. Some versions of the SUSE operating system can be manually started by running h5ss.sh, but the service fails to run h5ss?**

<https://www.suse.com/support/kb/doc/?id=000015901> SUSE provides official advice that you can confirm the existing value by using the following command. If it is 512, you need to modify the h5ss.service file as follows.

```

linux-bzca:/opt/h5ss # systemctl show --property DefaultTasksMax
DefaultTasksMax=512
linux-bzca:/opt/h5ss #

```

这个问题的原因是旧一点的systemd

<https://github.com/systemd/systemd/issues/3211> 新版本的systemd已经修复该问题。原来的版本可以通过修改h5ss.service解决，在h5ss.service中加入TasksMax=infinity.

