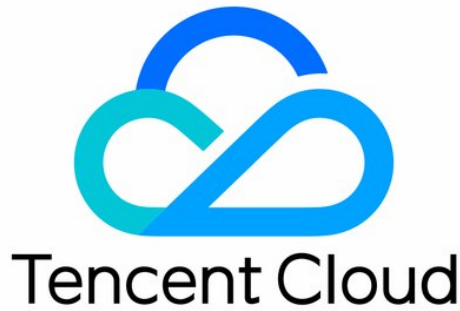


# Intelligent Viewdata Computing Practical Tutorial



## Copyright Notice

©2013–2024 Tencent Cloud. All rights reserved.

The complete copyright of this document, including all text, data, images, and other content, is solely and exclusively owned by Tencent Cloud Computing (Beijing) Co., Ltd. ("Tencent Cloud"); Without prior explicit written permission from Tencent Cloud, no entity shall reproduce, modify, use, plagiarize, or disseminate the entire or partial content of this document in any form. Such actions constitute an infringement of Tencent Cloud's copyright, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

## Trademark Notice

 Tencent Cloud

This trademark and its related service trademarks are owned by Tencent Cloud Computing (Beijing) Co., Ltd. and its affiliated companies ("Tencent Cloud"). The trademarks of third parties mentioned in this document are the property of their respective owners under the applicable laws. Without the written permission of Tencent Cloud and the relevant trademark rights owners, no entity shall use, reproduce, modify, disseminate, or copy the trademarks as mentioned above in any way. Any such actions will constitute an infringement of Tencent Cloud's and the relevant owners' trademark rights, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

## Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

## Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

# Contents

## Practical Tutorial

GB/T28181 Protocol Access Practice

RTMP Protocol Access Practical

Based on the existing network, add new NVR devices and connect to the platform

Grant different operational permissions to sub-accounts

Viewing Sub-account Operation Logs

# Practical Tutorial

## GB/T28181 Protocol Access Practice

Last updated: 2024-08-15 09:51:57

This document introduces how to access devices through the GB28181 protocol to IVC.

### Note:

You can also watch [GB/T28181 Protocol Access Demonstration Video](#) to understand the overall access process.

## Access Configuration Process

### Step 1: Create devices in the console

1. log in to [IVC Console](#).
2. In the left navigation bar, select the **Device Access** feature, and first navigate to Device Organization **Device Organization**. Select the corresponding device organization, click **Add Device** (you can choose **Manual Addition** or **Bulk Import**. This document explains manual addition as an example).



3. After the device is successfully created, its initial status is **Unregistered**.



### Step 2: Obtain device national standard configuration information

click the device name to enter the **Device Details** page, and view and record the configuration information generated for the device (as shown in the red box below).

← 国标设备1

基本信息			
设备名称	国标设备1	设备ID	9c02f538-88bc-40a2-8000-382bc661bca8后
设备状态	未注册	服务节点	上海1
设备类型	NVR	流传输协议	TCP
接入协议	GB28181	设备组织	示例组织
描述	-		

国标配置信息			
SIP 服务器编码	3101000002000000001	SIP 服务器域	3101000000
SIP 服务器地址	81.69.54.26	SIP 服务器端口	5871
设备密码	.....	设备组码	31011000001180001760

**Note:**

When there are many devices, it is recommended to use the **Export Device Information** feature to export device configuration information in bulk.

## Step 3: log in to the device Web interface for configuration

### Hikvision device configuration example (using IPC as an example)

HIKVISION® 预览 配置

系统 网络 基本配置 高级配置 视音频 图像 事件 存储

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: 5061  
 传输协议: UDP  
 白名单: 编辑

平台1

启用  
 协议版本: GB/T28181-2016

SIP服务器ID: 000000  
 SIP服务器域: [redacted]  
 SIP服务器地址: [redacted]  
 SIP服务器端口: [redacted]  
 SIP用户名: 000160  
 SIP用户认证ID: 000160  
 密码: [redacted]  
 密码确认: [redacted]

注册有效期: 3600 秒  
 注册状态: 在线  
 心跳周期: 60 秒  
 28181码流索引: 主码流 (定时)  
 注册间隔: 60 秒  
 最大心跳超时次数: 3

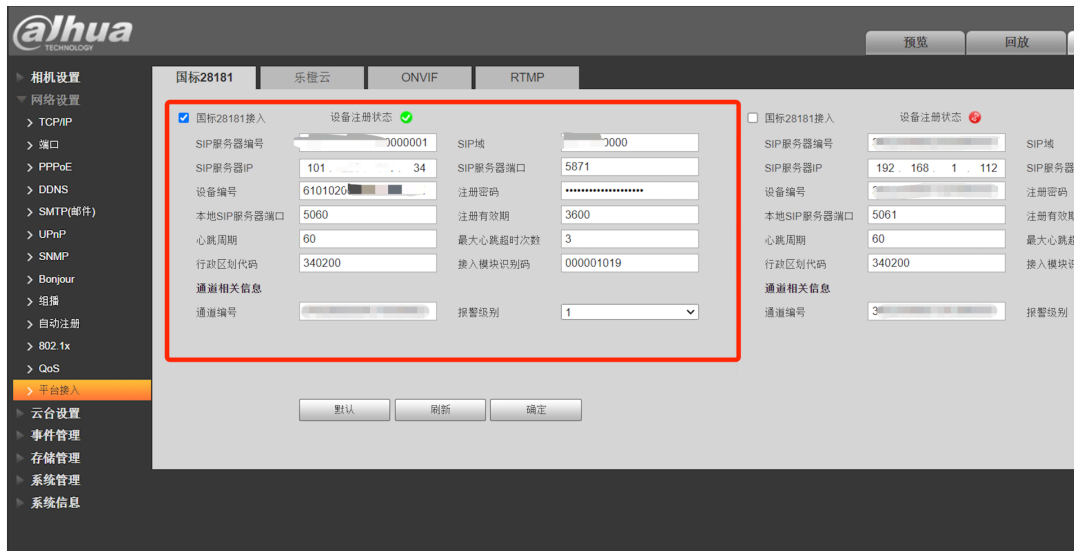
编码ID: 视频通道编码ID

通道号	视频通道编码ID
1	34020000001310000001

保存

Configuration Parameters	Configuration Instructions
Local SIP Port	<b>Must be changed to other port numbers like 5061, 5062, etc.</b> (Do not use the device's default port number 5060, as it may be blocked by the router).
Transfer protocol	This refers to the protocol used for signaling transmission, <b>prioritize choosing the TCP protocol.</b>
Protocol Version	Select GB/T28181-2016.
SIP Server ID	Enter the SIP Server ID generated by the platform in Step 2.
SIP Server Domain	Enter the SIP Server Domain generated by the platform in Step 2 ( <b>it's the first 10 digits of the SIP Server ID</b> ).
SIP Server Address	Enter the SIP Server IP generated by the platform in Step 2.
SIP Server Port	Enter the SIP Server Port number generated by the platform in Step 2.
SIP Username and SIP User Authentication ID	Enter the device code generated by the platform in Step 2, for example: 34020000001320000001
Password and Password Confirmation	Enter the device password in Step 2 ( <b>entered when creating the device in the console</b> ).
Registration Validity Period	The validity period for the device registration on the platform. <b>It is recommended to use the default value of 3600s.</b>
Heartbeat Interval	The time interval at which the device sends heartbeat information. <b>It is recommended to use the default value of 60s.</b>
Maximum Timeout Count	If the heartbeat continuously times out and reaches the "maximum number of timeouts," the device is considered unable to establish a connection with the platform. <b>It is recommended to use the default value of 3 times.</b>
Video Channel Encoding ID	The rule is consistent with the SIP username. Change the 11th–13th digits to 131, and it is recommended to write them in ascending order based on the channel number, ensuring no duplicates, for example: 34020000001310000001, 34020000001310000002, <b>Note:</b> <ul style="list-style-type: none"> <li>• <b>Just ensure that the channel coding ID here does not repeat with the above [SIP username], otherwise, it will prompt "parameter error". However, it doesn't matter if it's the same as the channel coding ID of other devices.</b></li> <li>• <b>The same rule applies when configuring NVR devices here.</b></li> </ul>

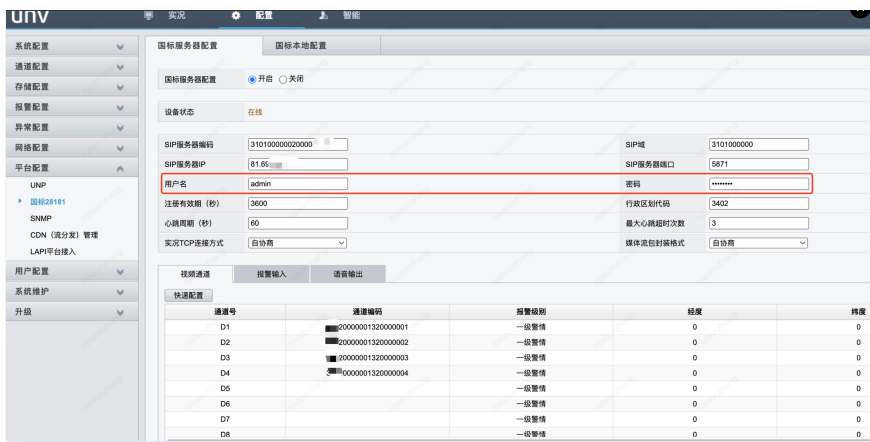
## Dahua Device Configuration Example (using IPC as an example)



Parameter Configuration	Configuration Instructions
SIP Server Number	Enter the SIP Server ID generated by the platform in Step 2.
SIP Server Domain	Enter the SIP Server Domain generated by the platform in Step 2 (the first 10 digits of the SIP Server ID).
SIP Server IP	Enter the SIP Server IP generated by the platform in Step 2.
SIP Server Port	Enter the SIP Server Port number generated by the platform in Step 2.
Device Number	Enter the device code generated by the platform in Step 2, for example: 34020000001320000001
Registration Password	Enter the device password in Step 2 (entered when creating the device in the console).
Local SIP Server Port	<b>Must be changed to other port numbers like 5061, 5062, etc.</b> (Do not use the device's default port number 5060, as it may be blocked by the router).
Registration Validity Period	The validity period for the device registration on the platform. It is recommended to use the default value of 3600s.
Heartbeat Interval	The time interval at which the device sends heartbeat information. It is recommended to use the default value of 60s.
Maximum Timeout Count	If the heartbeat continuously times out and reaches the "maximum number of timeouts," the device is considered unable to establish a connection with the platform. It is recommended to use the default value of 3 times.

<p>Channel Number</p>	<p>The rule is consistent with the SIP username. Change the 11th–13th digits to 131, and it is recommended to set them in ascending order based on the channel number, ensuring no duplicates, for example: 34020000001310000001, 34020000001310000002,</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>Just ensure that the channel encoding ID here does not repeat with the above [Device Number], otherwise, it will prompt "parameter error." However, it doesn't matter if it's the same as the channel encoding ID of other devices.</li> <li>The same rule applies when configuring NVR devices here.</li> </ul>
-----------------------	---

### Yushi Device Configuration Demonstration (using NVR as an example)



Parameter Configuration	Configuration Instructions
SIP Server Code	Enter the SIP Server ID generated by the platform in Step 2.
SIP Domain	Enter the SIP Server Domain generated by the platform in Step 2 (the first 10 digits of the SIP Server ID).
SIP Server IP	Enter the SIP Server IP generated by the platform in Step 2.

SIP Server Port	Enter the SIP Server Port number generated by the platform in Step 2.
Username	Log in to the device Web end with the username. <div style="border: 1px solid #00aaff; padding: 5px; margin-top: 10px;"><b>Note:</b> Do not enter the device code generated by the platform here.</div>
Password	Enter the device password in Step 2 (entered when creating the device in the console).
Registration Validity Period	The validity period for the device registration on the platform. It is recommended to use the default value of 3600s.
Heartbeat Interval	The time interval at which the device sends heartbeat information. It is recommended to use the default value of 60s.
Maximum Timeout Count	If the heartbeat continuously times out and reaches the "maximum number of timeouts," the device is considered unable to establish a connection with the platform. It is recommended to use the default value of 3 times.
Channel Number	The rule is consistent with the SIP username. Change the 11th–13th digits to 131, and it is recommended to set them in ascending order based on the channel number, ensuring no duplicates, for example: 34020000001310000001, 34020000001310000002,
Local GB Configuration	Enter the device code generated by the platform in Step 2, for example: 34020000001320000001

## Step 4: Complete the configuration

After completing the above configuration process, switch to the [IVC Console](#) and refresh the **Device Access** page. At this point, the device status will be shown as "online", indicating that the device has been successfully registered and is online.

国标接入 1个设备

包含子组织

<input type="checkbox"/>	设备名称/ID	协议类型	设备类型	状态	服务节点	通道数	描述	操作
<input type="checkbox"/>	国标设备1	GB28181	IPC	在线	上海三区	1	-	禁用 更多操作

共 1 条 20 条 / 页

## Audio and Video Configuration Precautions

On the same network, issues such as video stuttering or live broadcast failure often occur due to insufficient or fluctuating network resources. Refer to the following configurations for audio and video parameters.

#### **Note:**

- Do not enable any private encodings from the vendor such as smart264, smart265, SVC, etc., otherwise, registration will fail!
- For some vendor devices, modifying the camera configuration under NVR configuration pages may not take effect. It is strongly recommended to log in to the IPC device end for configuration!

## IPC Audio and Video Configuration Specifications

The following diagram uses Hikvision IPC as an example, other vendor devices are similar.

The screenshot displays the Hikvision IPC configuration interface for video settings. The interface includes a sidebar with navigation options like '本地', '系统', '网络', '视音频', '图像', '事件', and '存储'. The main area is titled '配置' and has sub-tabs for '视频', '音频', and 'ROI'. The '视频' tab is active, showing various settings:

- 码流类型: 主码流 (定时)
- 视频类型: 复合流
- 分辨率: 1920\*1080P
- 码率类型: 变码率
- 图像质量: 中
- 视频帧率: 25 fps
- 码率上限: 1024 Kbps
- 视频编码: H.264
- Smart264: 关闭
- 编码复杂度: 中
- I帧间隔: 50
- SVC: 关闭
- 码流平滑: 50 [清晰<->平滑]

Red annotations provide additional guidance:

1. 选择复合流时, 需注意音频配置
2. 上云选择变码率
3. 帧率建议选择25
4. 码率上限需根据自身网络条件进行配置
5. 视频编码可选择H.264或H.265
6. I帧间隔建议选择50

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

**配置**

视频 **音频** ROI

音频编码: AAC

采样率: 16kHz

音频码率: 32kbps

音频输入: MicIn

输入音量: 64

环境噪声过滤: 关闭

保存

1.音频编码建议选择 AAC 或 G.711

2.采样率优先选择 8000

## NVR Audio and Video Configuration Specifications

The following diagram uses Hikvision NVR as an example, other vendor devices are similar.

**配置**

预览 回放 图片 **配置** 插件下载 admin 帮助 注销

视频 码流信息叠加 零通道

通道: [D1] 海康PTZ球机07

码流类型: 主码流 (定时)

视频类型: 视频流

分辨率: 1280\*720(720P)

码率类型: 变码率

图像质量: 中

视频帧率: 25 fps

码率上限: 1024 Kbps

视频编码: H.264

Smart264: 关闭

复制到... 保存

1.选择相应的视频通道, 即NVR下挂载的摄像头

2.若需上传音频, 选择复合流 (前提是摄像头支持音频功能)

3.降低分辨率, 有利于减少视频码率

4.选择变码率

5.建议帧率 25 或以下, 不要选择全帧率

6.建议码率上限不要超过 2048kbps, 请依据自己网络条件调整

# RTMP Protocol Access Practical

Last updated: 2024-08-15 09:54:32

This document will introduce how to access IVC through the RTMP protocol. We will discuss two methods: **Device Streaming** and **Software Streaming**.

## ! Note:

You can also watch the [RTMP Protocol Access Practical Demonstration Video](#) to understand the overall access process.

## 1. Camera Streaming Example

### 1. Create a Device

1. log in to [the IVC Console](#), and select **Device Management** from the left sidebar.
2. First, select the Device Organization, click **Add Device**, and choose the RTMP Protocol.



3. You can choose custom {appname} and {streamname} parameters to generate a custom RTMP streaming address.

## ! Note:

The platform-generated RTMP streaming address format is `rtmp://{domain name}/{appname}/{streamname}`, all three parameters can be customized.

- Domain name refers to the domain. You can upload an ICP-registered push domain name as per the page instructions, otherwise, the default will be the platform service's Public IP Address.
- The app name only supports English, numbers, and must not exceed 32 characters. Otherwise, it defaults to live.
- The stream name only supports English, numbers, and must not exceed 32 characters. Otherwise, it defaults to a 10-digit device ID generated by the platform.

### 手动添加设备 ×

设备名称 \*

接入协议 \* GB28181 RTMP 网关接入 IVCP

设备类型 \* IPC

服务节点 上海测试1 ▼

为了节省网络宽带，请务必按照设备实际所在地选择最近的服务节点  
请确保选定的服务节点已**添加推流域名**，否则无法自定义下述参数

AppName   
用于生成推流地址，若不填写则该参数默认为live

StreamName   
用于生成推流地址，若不填写则该参数默认为平台生成的设备编码

描述   
0 / 128

确定
取消

4. Complete the device addition.

## 2. Obtain the RTMP Streaming Address

1. Go to the details page of the newly created device to get the streaming address as follows.

← RTMP1
文档指引

#### 基本信息

设备名称	RTMP1	设备 ID	0d8...
设备状态	未注册	服务节点	上海三区
设备类型	IPC	接入协议	RTMP
设备组织	RTMP接入	描述	-

#### 推播流地址

复制播流地址进行实况播放时会产生上行和下行网络消耗费用

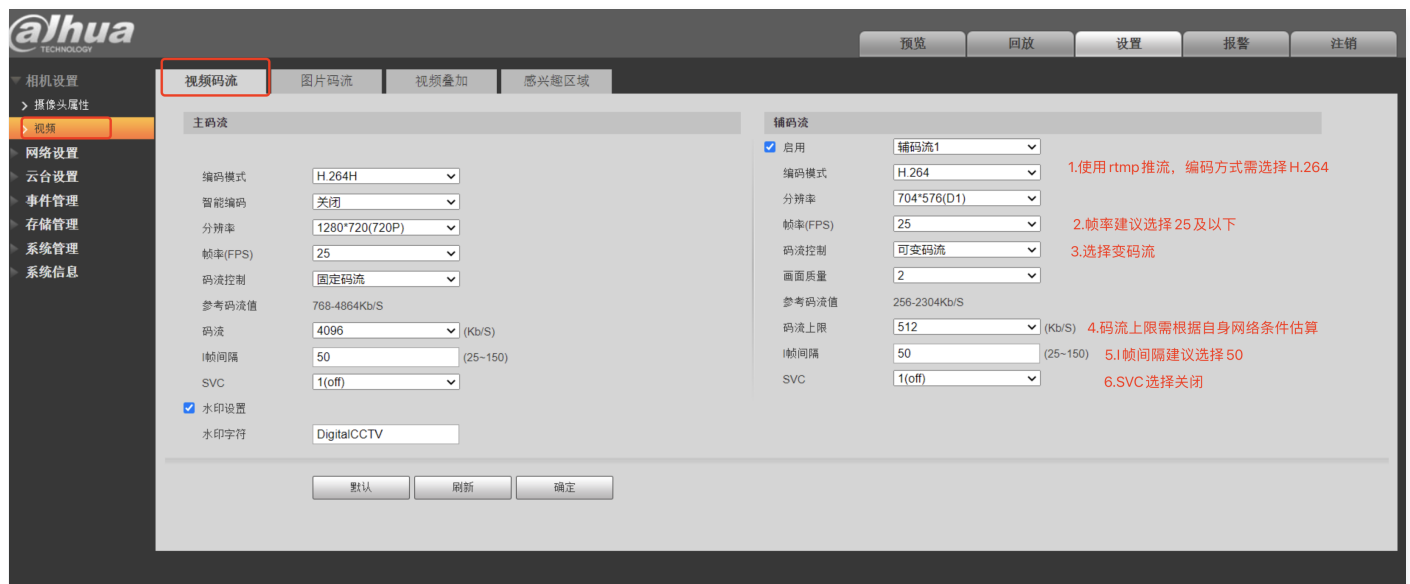
推流地址

rtmp://61...152/live/0d9L.../2S?token=cms\_131C...37A

播放地址

## 3. Device Configuration

1. Log in to the device Web Configuration Page, first configure the audio and video parameters (take Dahua Camera – Auxiliary Stream as an example).



2. Choose Custom Address Type, configure the streaming address generated by our platform, and enable streaming.



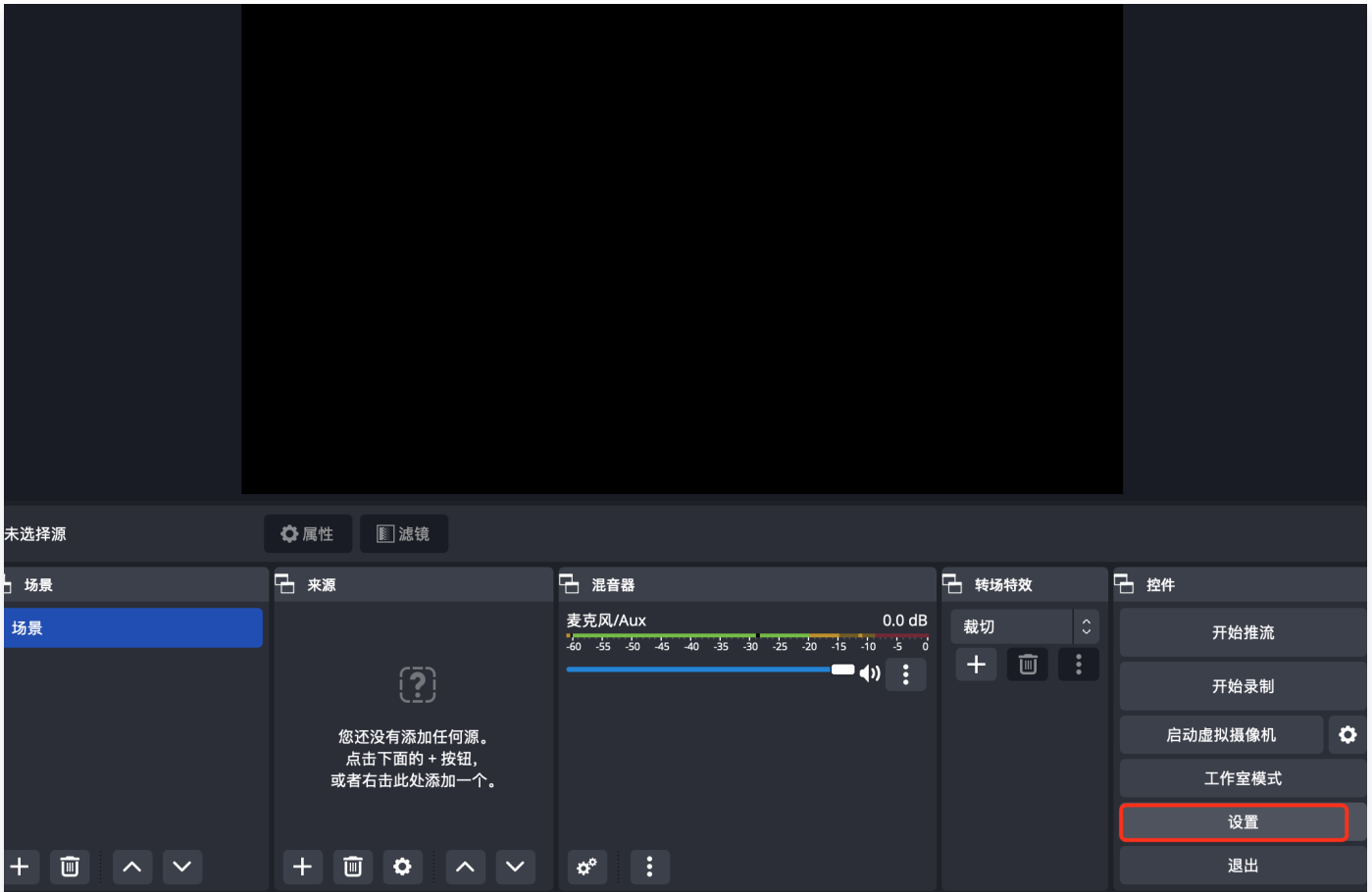
## 2. Software streaming example (using OBS Software as an example)

1. Go to [OBS official website](#) to download and install.

### ! Note:

OBS is a free open-source video recording and real-time communication software with multiple features. It is widely used in video capturing and live streaming.

2. Open OBS, click the **widget** in the bottom toolbar > **settings** button to enter the settings interface.

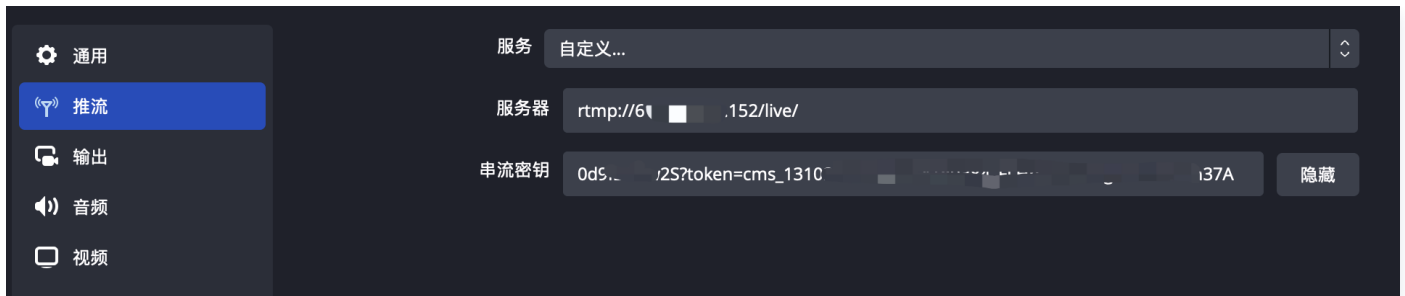


3. click **streaming** to enter the streaming settings page and make the following adjustments.

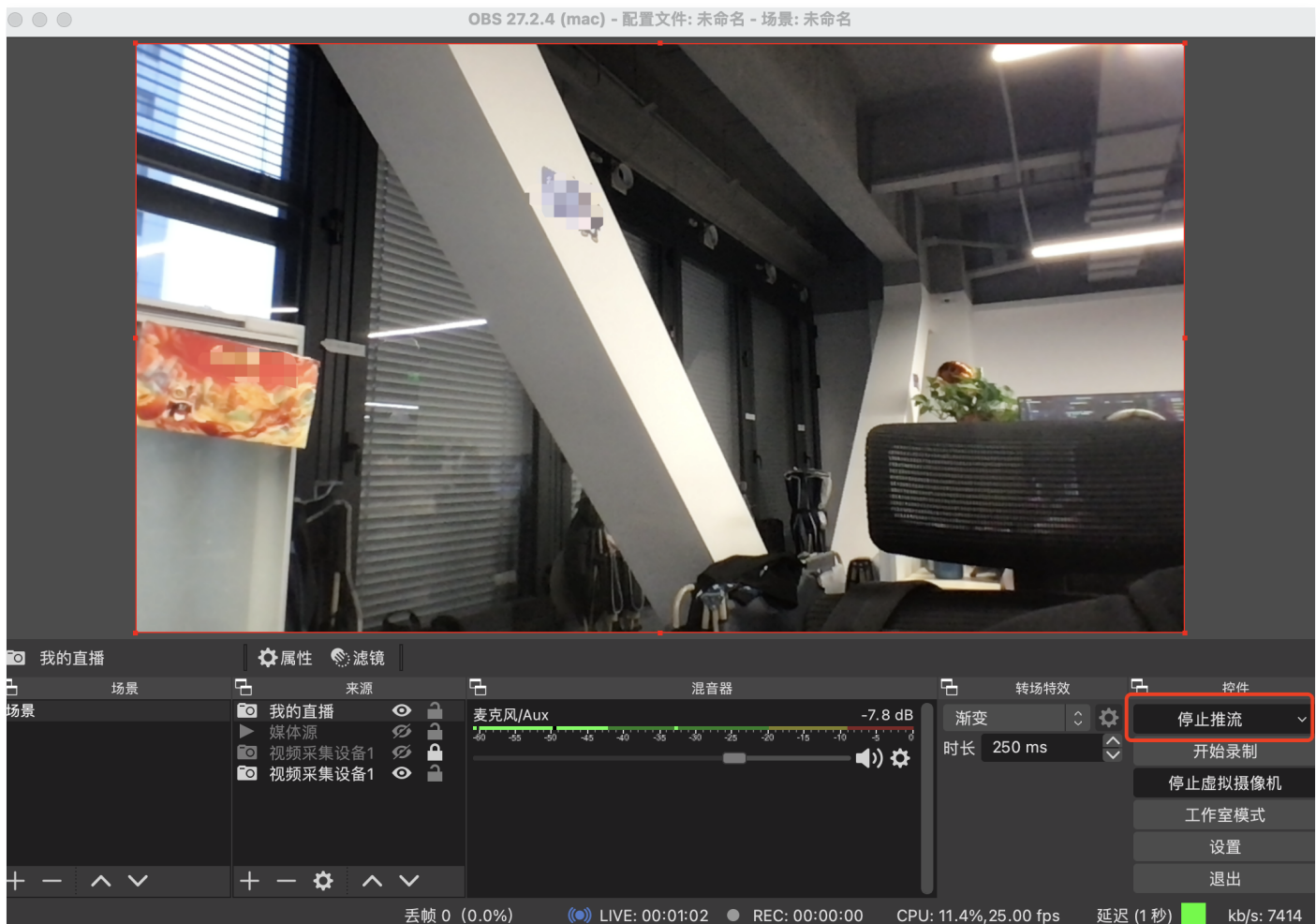
**Note:**

- Refer to steps 1 and 2 above for the steps to obtain the streaming address.
- For security, we enable Token Hotlink protection authentication configuration by default for customers. If you do not need it, you can disable it in the **Console – Service Configuration > Authentication Configuration**.

Parameter Configuration	Description
Service Type	Default Self Definition
Server Address	Fill in the server address part of the streaming URL from step 2, for example <code>rtmp://{domain name}/{appname}/</code>
Stream Key	Fill in the stream name and all the contents after it in the streaming URL from step 2, for example <code>{streamname}?token=cms_131...37A</code>



4. Click **Controls > Start Streaming** on the toolbar to start streaming.



# Based on the existing network, add new NVR devices and connect to the platform

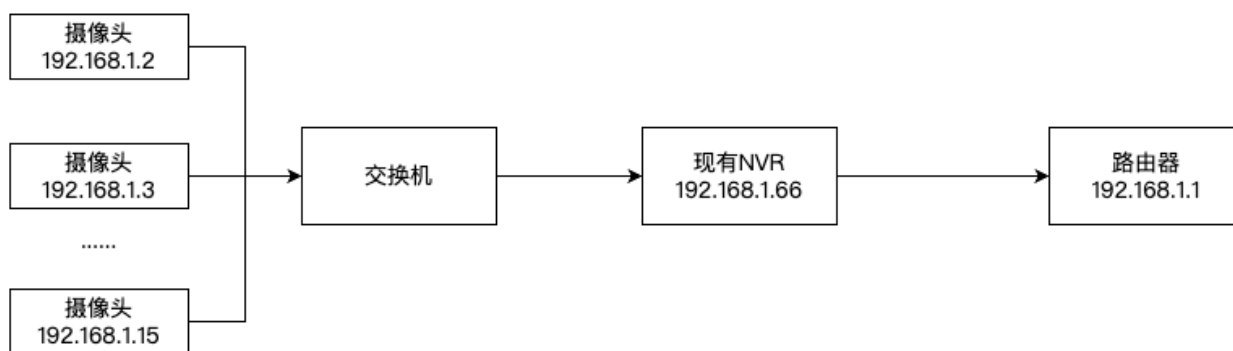
Last updated: 2024-08-15 09:59:55

## Background

The store already has a video surveillance system (as shown in the network diagram below), with data stored in the NVR Network Video Recorder. With business growth, the customer has proposed the following requirements:

- Storefronts are dispersed nationwide, and the headquarters needs to centralized control to access each storefront's device video at any time.
- The local Digital Video Recorder's storage capacity is insufficient, requiring immediate scale-out to meet the employees' need for retrospective analysis.
- Incidents of equipment theft and data tampering occur frequently, so data needs to be backed up to the cloud, ensuring data integrity and storage reliability in the cloud.
- The current networking setup cannot be changed to avoid impacting existing business operations.

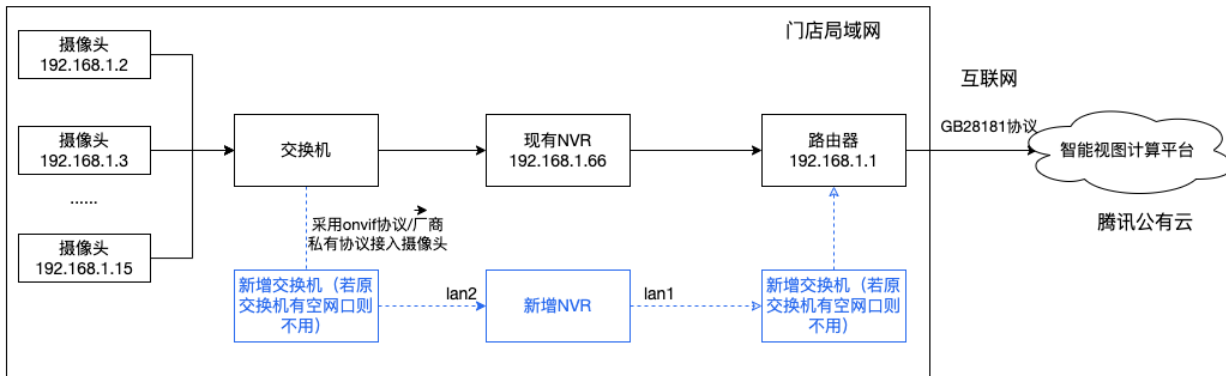
假设存量设备的内网ip地址及组网如下图



## Solution

Based on this context, each storefront needs to add one NVR device to extend the local storage cycle through a bypass grid connection. Simultaneously, this device will achieve nationwide device cloud aggregation via the Internet Access Platform. manage and back up data to the cloud.

说明：黑色线条表示现有组网，蓝色线条表示新增设备组网  
nvr一般有两张网卡，假设lan1口接路由器，lan2口接交换机（用于局域网内接摄像头）



## Operation Procedure

### Step 1: Install the new device and connect it to the existing cameras

1. Follow the solution by first installing the new NVR (Hikvision in this example) and setting up the network.
2. Determine the new NVR's private IP address and log in to its configuration page.

#### ! Note:

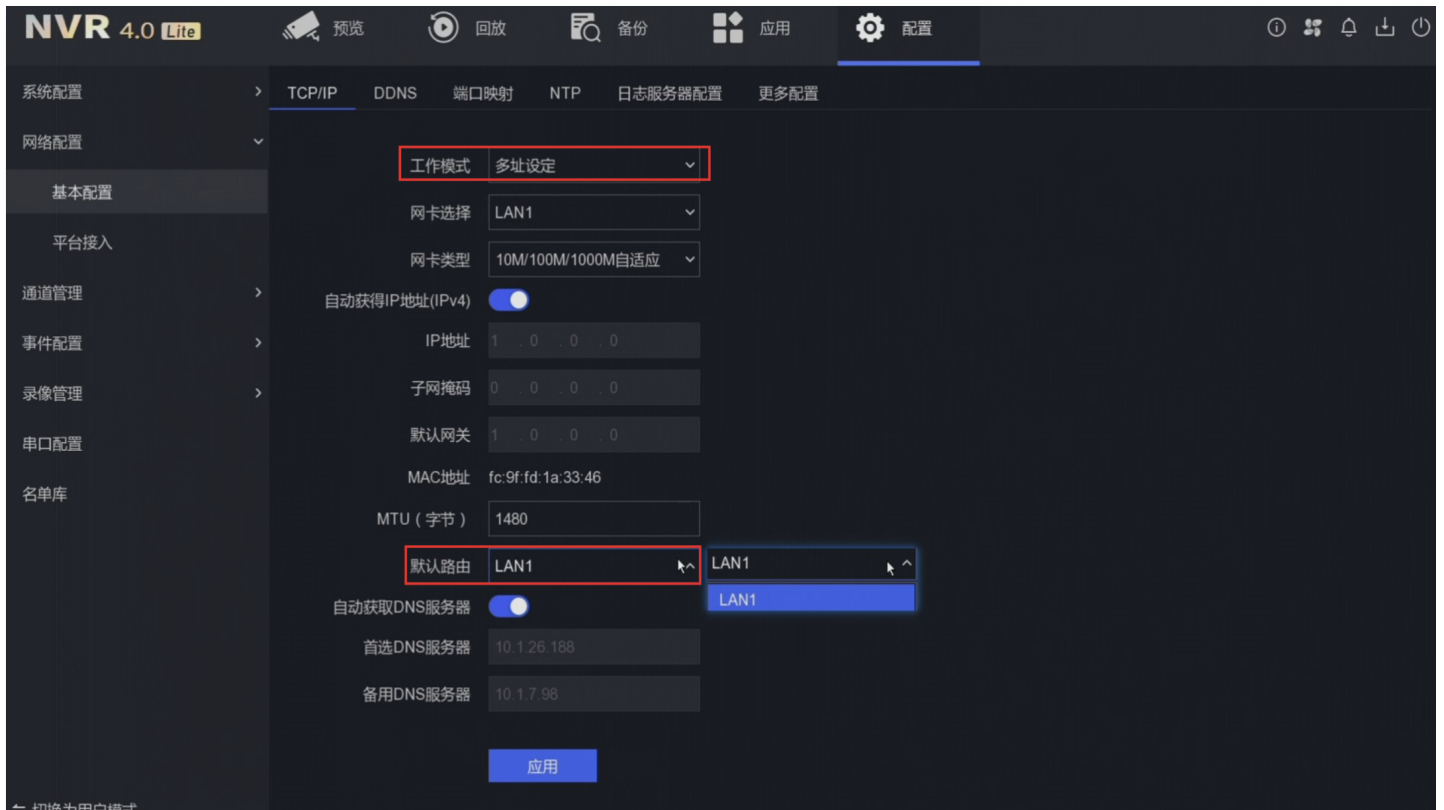
There are three ways to find the device's private IP: using the manufacturer's intranet device search tool, logging in to the router configuration page to find it, or directly connecting a monitor to the new NVR to log in and retrieve it.

3. Configure the device's network parameters

Enter the [Network Settings–Basic Configuration] page, change the Operation Mode to **"Multiple Address Setting"**, select LAN1 for the network card, set LAN1 to automatically obtain an IP address, enable automatic acquisition of DNS servers, select LAN1 for the default route, and click **"Apply"**.

#### ! Note:

- The multiple address setting mode means that the parameters of the two network cards are independent and do not affect each other.
- The default route means that when the system proactively connects to an external network, the data is forwarded by the default route. Since LAN1 will be used to access the public network, it is chosen as the default route.



Select LAN2 for the network card, assign an internal IP address to LAN2 (for example, 192.168.1.100), and click "Apply" after setting.

**Note:**

Since LAN2 will connect to cameras within the local area network, it needs to be on the same subnet as the cameras but without IP conflicts; otherwise, the cameras will not be accessible.

#### 4. Connecting Existing Cameras

Enter the [Device Access] page, and the NVR will automatically obtain information on all cameras within the local area network, allowing camera access.

You can choose a suitable protocol for access (generally supports multiple access protocols, for example, onvif); 'password' in the diagram refers to the camera's configuration end login password; the camera has multiple streams, accessing here does not affect its existing surveillance system's streaming.



系统配置 **GB28181** OTAP ISUP SDK ISAPI ONVIF 日志服务器

用户管理 启用

网络配置

网络参数

本地SIP端口 5069 注册有效期 3600

SIP服务器ID 3101000000200000000 心跳周期 60

SIP服务器域 3101000000 最大心跳超时次数 3

SIP服务器地址 81.69.54.26 速度类型 倍率

SIP服务器端口 5871 倍率 1

SIP用户认证ID 31011000001180006262 启用码流平滑

SIP用户认证密码 \*\*\*\*\* 启用私有信息

注册状态 ● 在线

模板配置

假日计划

布防计划

存储计划

异常配置

编码ID	编码ID类型	报警输入号	报警输入编码ID
报警输入编码ID		1	34020000001340000001
视频通道编码ID		2	34020000001340000002
		3	34020000001340000003
		4	34020000001340000004

# Grant different operational permissions to sub-accounts

Last updated: 2024-08-15 10:00:16

## Background

In reality, the root account needs to grant sub-accounts of employees at different levels with product feature operational permissions to meet security compliance requirements. This article will list the practice process of permission authorization under multiple scenarios.

## Prerequisites

- Tencent Cloud accounts are managed in Tencent Cloud Certificate Authority M CAM (Cloud Access Management). You need to understand the basic concepts of sub-accounts, permissions, policies, etc., in advance. Please refer to [CAM Operation Guide](#).

Among them, a policy is a collection of one or more operational permissions, categorized as follows:

	Creator	Application scenario	Predefined policies for this product	Description
Preset Policy	Various products of Tencent Cloud	A collection of frequently used product feature permissions	QcloudISSReadOnlyAccess	Users can only view, not modify
			IVC (ISS) Read-only Access Permission	
			QcloudISSFullAccess	Users can fully operate and view
			IVC (ISS) Full Read-Write Access Permission	
Custom Rules	User	Refined permission management, where users can create based on business scenarios themselves	No	No

- For the complete process of executing sub-account permission authorization, please refer to [User Permissions](#).

## Scenario One: Authorize sub-accounts with full operational permissions

**Applicable to:**Headquarters operation and maintenance team, headquarters digital department (responsible for undertaking video business)

**Scenario:**This type of sub-account coordinates the overall business (acting as the role of a super administrator),

**Authorization policy:**The master account authorizes the sub-account with preset product policies: **QcloudISSFullAccess** IVC (ISS) full read/write access.

**Note:**

This type of sub-account can create multiple sub-accounts for regional personnel. It needs to be granted the **QcloudCamFullAccess** preset strategy. Then, the sub-account can be created.

## Scenario 2: Sub-accounts can only view device status and recordings, without any edit operations

**Applicable to:**Sub-accounts of regional personnel

**Scenario:**In coordination with headquarters personnel to troubleshoot equipment failures and routinely access videos of devices within their responsible region. Therefore, they can only live preview and playback recordings (local, cloud) of authorized devices, unable to edit device organization, add/delete devices, download cloud recordings, etc., nor can they view other features.

**Authorization policy:**Is required to be created by the master account with custom Definition policies (must include the following product interfaces). For details, please refer to [Custom Definition Policy Creation Guide](#). Finally granted to the sub-account.

API Name	Interface description
DescribeOrganization	Query Organization
DescribeDeviceChannel	Query Device Channel
DescribeDeviceRegion	Query All Device Service Nodes
DescribeDictionary	Get Dictionary
DescribeRecordPlaybackUrl	Get Cloud Recording Playback URL
DescribeUserDevice	Query Device
ListDevices	Get Device List
DescribeRecordFile	Recording File Retrieval
ControlDeviceStream	Get Streaming Address
ControlRecord	Recording Control
ControlRecordTimeline	Request Recording Timeline

---

PlayRecord	Recording Playback
RefreshDeviceChannel	Refresh Device Channel
ListTasks	Queries the list of tasks

# Viewing Sub-account Operation Logs

Last updated: 2024-08-15 10:01:12

## Background

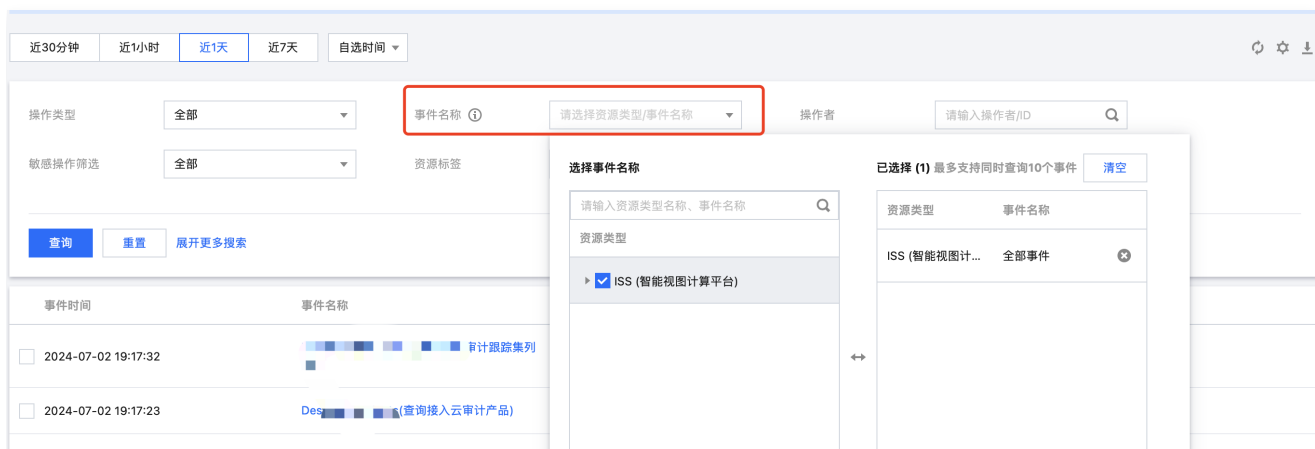
When employees use a Tencent Cloud sub-account to log in to the console or use the TencentCloud API to access resources under the main account, you may need the following information:

- What resources did the employees access?
- How do I check the modification records of resource configurations?
- Are employees accessing Tencent Cloud within the environment you specified?

At this time, you can view and track employees' operation logs through the [CloudAudit](#) product. CloudAudit supports the online viewing of operation records on the Tencent Cloud console and TencentCloud API within 90 days.

## Operation step

1. Log in to the [CloudAudit console](#), click on the Operation Records feature. Select the event name "IVC"



2. You can view the operation logs of sub-accounts by filtering through the "Operator".



3. Click the event details to view information such as the operator's source IP address and sub-account ID.

The screenshot displays the Tencent Cloud console interface for viewing event details. The main table lists several events, with the first one, 'DescribeAuditTracks(查询操作审计跟踪集列表)', highlighted with a red box. The right-hand panel provides detailed information for this event, also enclosed in a red box. The details include:

- 密钥 ID:** AKID[redacted]
- 事件名称:** DescribeAuditTracks
- 事件时间:** 2024-07-02 19:17:32
- 源 IP 地址:** 119.12[redacted]
- 资源地域:** -
- CAM 错误码:** -
- 事件区域:** ap-t[redacted]
- 事件源:** clou[redacted]
- 请求 ID:** e55c[redacted]
- 操作者:** 1000[redacted]

The '相关资源' (Related Resources) section shows no results. The '事件记录' (Event Log) section displays a JSON snippet of the event data:

```

1 {
2   "userIdentity": {
3     "principalId": "1000103002",
4     "accountId": "10002002",
5     "secretId": "AKIDLF[redacted]",
6     "sessionContext": {
7       "token":

```

## Shipping Log with Tracking Set

If you need to view employee operation records for a longer period, you can use CloudAudit's Tracking Set feature to deliver logs to a COS bucket or CLS.

When delivering to CLS, you can select specific operations of this product (such as sensitive operations) and configure alarm strategies in CLS. For detailed operations, please refer to [Using Log Delivery for Tracking Sets](#).