Media Live

User Guide

Issue	01
Date	2025-01-24

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Overview

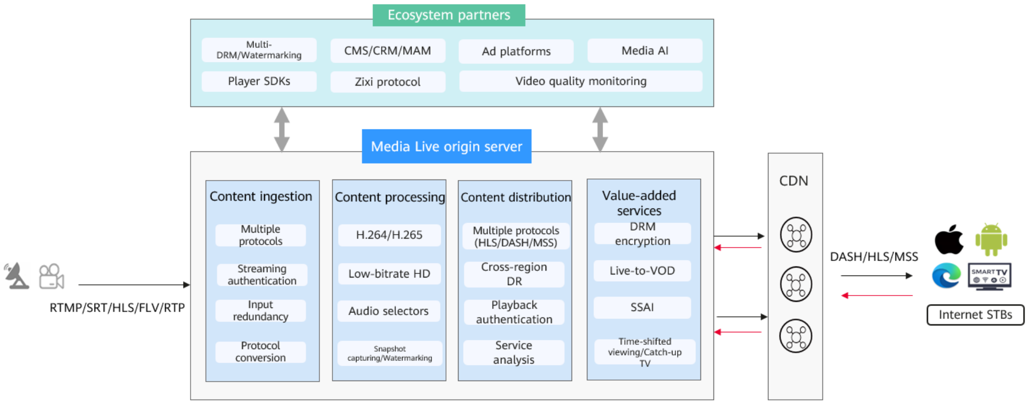
Huawei Cloud Media Live ensures stable broadcast-grade streaming for the industry's leading PGC players, around the clock with zero interruptions. Powered by the abundant compute resources of Huawei Cloud AZs worldwide and Huawei's years of audio/video expertise, Media Live helps TV stations and OTT platforms confidently deliver media content to their global audiences with unparalleled clarity and performance.

NOTE

Enabling the Live console means enabling Media Live. For details, see **Quick Start**.

Service Architecture

Figure 1-1 Service architecture



Features

Multi-protocol primary/standby stream input

RTMP, SRT, HLS, and FLV are supported for stream input. Primary/Standby input URLs are provided for each stream to ensure stable and reliable transmission.

High-quality transcoding

H.264/H.265 transcoding with versatile levels of resolution, bitrate, and frame rate is available. Standard transcoding and low-bitrate HD transcoding are supported.

Lower bitrate needed for the same image quality improves user experience and reduces content distribution costs.

Real-time packaging of multi-protocol livestreams

Livestreaming, catch-up TV, and time-shifted viewing are supported for HLS, DASH, and MSS output streams. Transcoding templates can be applied in real time to distribute content with adaptive bitrate.

With VOD origin servers, live-to-VOD captures and preserves event highlights for permanent access and multi-channel distribution.

Digital rights management (DRM)

FairPlay, Widevine, PlayReady, and Multi-DRM safeguard your high-value media assets.

Stream quality monitoring

Input stream quality monitoring (per minute and by channel) and downstream statistics (traffic, bandwidth, status codes, and concurrency) keep you well-informed of stream quality in real time.

2 Scenarios

Broadcast and TV

Huawei Cloud Media Live ensures 24/7 broadcast-grade streaming for broadcasters, TV stations, and carriers. With the worldwide CDN points of presence (PoPs), a higher compression rate for the same image quality improves user experience and inexpensively distributes live content.

Livestreaming of major sports events

Local and global CDN PoPs facilitate international livestreaming of major sports events, and offer premium live video experience in areas where these programs have a high viewership. SRT streams can be smoothly transmitted even in poor network conditions. Real-time packaging enables streams to play at different bitrate levels to ensure good video experience on multiple devices.

Live entertainment

Powerful real-time transcoding allows streaming movies at a high level of bitrate and frame rate. DRM encryption and digital watermarking protect the copyright of high-value media content.

3 Functions

Huawei Cloud Media Live enables PGC platforms to create media live transcoding templates and channels to livestream premium content. For details, see **Table 3-1**.

Table 3-1 Functions

Type	Function	Description
Live console	Overview	● You can view the downstream traffic and peak downstream bandwidth on the current day. ● You can change the CDN billing option.
	Domains	You can add, delete, disable, and enable ingest domain names and streaming domain names for Media Live.
	Channels	You can create, enable, modify, disable, and delete a channel.
	Live Transcoding	You can create, modify, and delete a Media Live transcoding template.
	Service Monitoring	You can view the monitoring information about a streaming domain name, including the downstream bandwidth/traffic, all status codes returned in request response, and number of concurrent downstream requests.
	Cloud Resource Authorization	If DRM encryption needs to be enabled for a channel and **Interconnection Mode** is set to **FunctionGraph proxy access**, you need to enable **FunctionGraph agency** in advance. After the authorization is successful, Media Live can query functions, workflows, and triggers, and call functions.

Type	Function	Description
	Catch-Up TV/ Time-Shifted Viewing URL Generation	You can obtain a catch-up TV/time-shifted viewing URL to watch catch-up TV of a channel.

4 Product Advantages

Global Acceleration and Nearby Access

- 800+ nodes outside the Chinese mainland, covering 130+ countries and regions
- 180 Tbit/s+ bandwidth reserve for elastic scaling upon traffic bursts
- Faster, stable access for users across regions and networks

Industry-leading Proprietary Technology

- Intelligent routing helps identify the optimal route based on factors such as access location and network quality, delivering content 20%+ faster.
- Proprietary software-hardware synergy improves service performance.

Secure Transmission

- Full-link HTTPS transmission and advanced security control ensure stable service running and data security.
- Automatic node failover offers high service availability.
- The 24/7 local expert service responds to your needs in a timely manner.

Lower Costs and Higher Efficiency

- Lower operations costs and latency and less retrieval bandwidth usage
- Easy configuration in just a few steps and more efficient deployment

5 Constraints

Before using Media Live, understand the following constraints.

Channel Inputs

Table 5-1 Channel input constraints

Item	Description
Transcoded stream frame rate	The transcoded stream frame rate cannot be higher than the input frame rate.
Transcoded stream resolution	The transcoded stream resolution cannot be higher than the input resolution.
Audio/Video encoder	● Video: H.264 and H.265 ● Audio: AAC, MP1, MP2, and MP3 Note: MP1, MP2, and MP3 are only available for TS inputs. By default, the inputs are transcoded into AAC outputs. ● Subtitling is not supported.

Item	Description
Input specifications	Details: ● RTMP stream push is supported. ● HTTP-FLV stream pull is supported. The sequence header must be carried when playback starts. ● HLS-PULL stream pull is supported, as well as the HLS V3, HTTP, or HTTPS. ● SRT-Listener stream push is supported. Only TS streams are supported and **streamid** is optional. ● SRT-Caller stream pull is supported. Only TS streams are supported. ● Encrypted streams are not supported. ● Audio-only inputs are not supported, with at least one video stream required. Video-only outputs are not supported. For video-only outputs, one mute stream will be automatically added. ● The encoder parameters of the primary and standby inputs must be the same. Otherwise, the playback may be interrupted during input redundancy. ● Inputs: bitrate ≤ 50 Mbit/s, frame rate ≤ 60 FPS, resolution ≤ 4K
Input GOP duration	Recommendations: ● Set the value to 1 second or an integer multiple of 1 second. ● Set the segment duration configured for a channel to an integer multiple of the GOP duration.

Channel Outputs

Table 5-2 Channel output constraints

Item	Description
Audio/Video encoder	● Video: H.264 and H.265 ● Audio: AAC ● Subtitling is not supported.
MSS	Neither encrypted nor unencrypted MSS streams (H.265) can be output.
DRM encryption	DRM encryption algorithms supported: ● HLS: sample-aes ● DASH: CENC ● MSS: CENC

Resources

Table 5-3 Resource constraints

Item	Description
Number of channels	A tenant can create a maximum of 500 channels. To create more channels, **submit a service ticket**.

Functions

Table 5-4 Function constraints

Item	Description
Channel function	All channels support only single-bitrate inputs, and multi-bitrate outputs are available only after transcoding. **SRT_PUSH** channels and **RTMP_PUSH** channels cannot be created at the same time for one domain name.

Clients

Table 5-5 Client constraints

Item	Description
Encoding format	In iOS 16.0 or later, the maximum HE-AAC audio bitrate is 64 Kbit/s. This constraint does not apply to AAC-LC.
Client	If the displayed segment duration of the source stream is different from the actual segment duration, the audio and video may be out of sync. To solve this potential issue, the client should support audio-to-video synchronization.

APIs

Media Live sets a limit on the number of API calls to prevent service interruption caused by repeated API calls in a short period of time.

Table 5-6 API request throttling

API Category	API Name	Max. User Requests	Max. API Requests
OTT Channel Management	● Creating an OTT Channel ● Querying Channel Information ● Deleting Channel Information ● Modifying Channel Packaging Information ● Modifying Channel Input Stream Information ● Modifying Channel Recording Information ● Modifying General Channel Information ● Changing the Channel Status ● Modifying Channel Transcoding Template Information	80 times/minute	80 times/minute

6 Getting Started

6.1 Quick Start

If you want to use Media Live with your own domain names, see **Figure 6-1**.

Figure 6-1 Getting started with Media Live

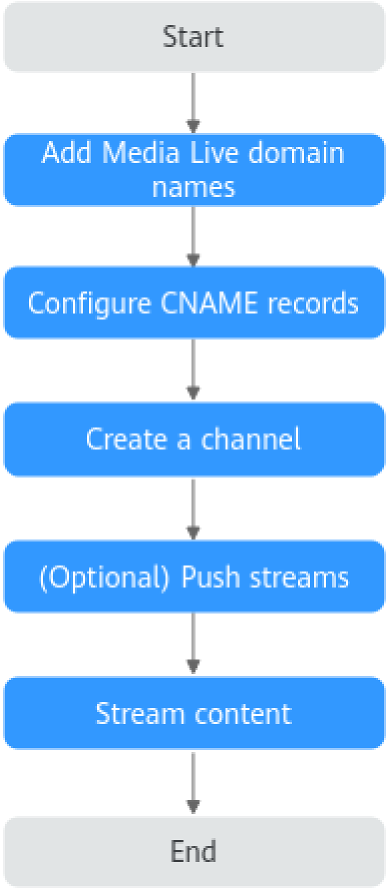


Table 6-1 describes how to get started with Media Live.

Table 6-1 Getting started with Media Live

No.	Operation	Description
1	**Adding domain names**	Add an ingest domain name and a streaming domain name to Media Live. You can register a level-1 domain name (for example, example.com) and use two level-2 domain names (for example, live-play.example.com and live-push.example.com) as the ingest domain name and streaming domain name.
2	**Configuring CNAME records**	Live assigns a CNAME record to the ingest domain name and streaming domain name. Add the CNAME records to your domains' DNS records to enable live streaming acceleration.
3	**Creating a channel**	You can create a channel before the media livestreaming starts. The media file input type can be: ● **FLV_PULL**: Stream push is not required. The streaming URL provided by the user is directly obtained and used by Media Live to push streams to the origin server. The streaming URL supports only HTTP. ● **RTMP_PUSH**: An RTMP ingest domain name needs to be configured for stream push. ● **HLS_PULL**: Stream push is not required. The streaming URL provided by the user is directly obtained and used by Media Live to push streams to the origin server. If **Input Type** is set to **HLS_PULL**, the media URLs provided users have the following constraints: – A streaming URL supports only HTTP and HTTPS. – Encrypted streams are not supported. – Audio-only streams are not supported. – Subtitling is not supported. ● **SRT_PULL**: Stream push is not required. The streaming URL provided by the user is directly obtained and used by Media Live to push streams to the origin server. ● **SRT_PUSH**: An SRT ingest domain name needs to be configured for stream push. To ensure reliability, channels of the **SRT_PUSH** input type must be able to: – Support primary and standby URLs. The encoder needs to push streams to both the primary and standby URLs. – Resume stream push when the stream push by the encoder is interrupted. The recommended interval for resuming stream push is shorter than the duration of a segment.

No.	Operation	Description
4	**Pushing streams**	You can use a third-party streaming tool such as Open Broadcaster Software (OBS) to push streams.
5	**Streaming content**	You can use a third-party player such as VLC media player to stream content.

6.2 Adding Domain Names

This section describes how to add an ingest domain name and a streaming domain name.

Prerequisites

- You have registered with Huawei Cloud and completed real-name authentication.

  NOTE

  If you are a **Huawei Cloud (International/Europe)** user, you need to complete real-name authentication when you:

  - Purchase and use cloud services on Huawei Cloud nodes in the Chinese mainland. In this case, real-name authentication is required by the laws and regulations of the Chinese mainland.
  - Plan to use Live in regions in the Chinese mainland.
- Domain names for Media Live are available. A **PUSH** channel requires an ingest domain name and a streaming domain name, and the two domain names must be different. A **PULL** channel does not require an ingest domain name.

  NOTE

  If you want to perform livestreaming acceleration in Huawei Cloud regions in or outside the Chinese mainland, the domain names must complete ICP filing in advance as required by the Ministry of Industry and Information Technology (MIIT).
- When a new IAM user uses Media Live for the first time, they need to configure the permission to create a domain name.

Adding Domain Names of Media Live

Add the ingest and streaming domain names to Live. The following describes how to add an ingest domain name. The procedure for adding a streaming domain name is the same.

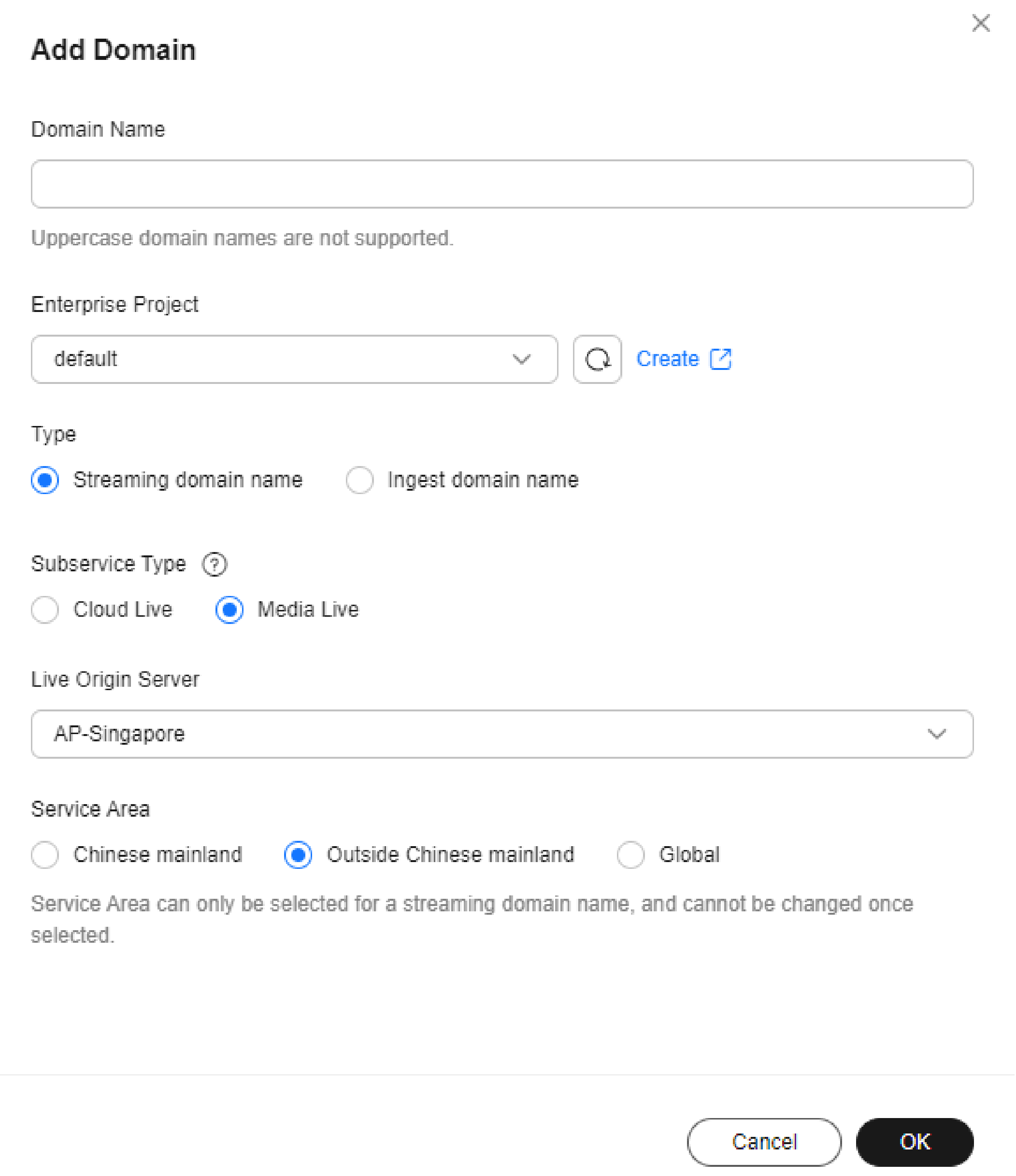
Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Add Domain**. On the displayed page, enter a streaming domain name or an ingest domain name.

A **PUSH** channel requires an ingest domain name and a streaming domain name, while a **PULL** channel requires only a streaming domain name.

Figure 6-2 Adding a domain name



Add Domain

Domain Name

Uppercase domain names are not supported.

Enterprise Project

default

Create

Type

● Streaming domain name ○ Ingest domain name

Subservice Type

○ Cloud Live ● Media Live

Live Origin Server

AP-Singapore

Service Area

○ Chinese mainland ● Outside Chinese mainland ○ Global

Service Area can only be selected for a streaming domain name, and cannot be changed once selected.

Cancel OK

Table 6-2 Parameters

Parameter	Description
Domain Name	Enter a second-level ingest domain name or streaming domain name, for example, test-push.example.com. **NOTE** - The domain name can contain a maximum of 64 characters, which cannot contain uppercase letters. - An ingest domain name must be different from a streaming domain name. Wildcard domains are not allowed. - By default, you can add up to 64 domain names in your account. To add more domain names, **submit a service ticket**.
Enterprise Project	Add domain names to enterprise projects for unified management. On the **Create Enterprise Project** page, **create an enterprise project** (whose name is **default** by default) and **add the user group to the enterprise project**. By doing so, users in this user group obtain the permissions on the domain names in the enterprise project. **NOTE** Only an enterprise account can configure enterprise projects.
Type	If you enter an ingest domain name for **Domain Name**, then select **Ingest Domain Name** for **Type**. The domain name type cannot be changed once configured.
Subservice Type	Subservice type of the Live service. Options: - **Cloud Live**: This easy-to-use livestreaming service provides diverse live acceleration capabilities for entertainment, e-commerce, and education scenarios. - **Media Live**: This broadcast-grade livestreaming service supports features such as channel management and content encryption, making it an ideal option for media assets and broadcasting. Select **Media Live**.
Live Origin Server	Area where the Live origin server is located. For details, see How Do I Select a Live Origin Server and Acceleration Area? The Live origin server cannot be changed once configured. Select the nearest origin server. Currently, Live is supported in the following regions: - CN North-Beijing4 of Huawei Cloud (Chinese Mainland) - AP-Singapore, ME-Riyadh, CN-Hong Kong, and AF-Johannesburg of Huawei Cloud (Singapore) By default, ME-Riyadh, CN-Hong Kong, and AF-Johannesburg are unavailable. To select these regions, **submit a service ticket** to contact Huawei Cloud technical support. - Dublin of Huawei Cloud (Europe): EU-Dublin.

Parameter	Description
Service Area	Area where streaming domain names can be accelerated. For details, see How Do I Select a Live Origin Server and Acceleration Area? This parameter is valid only for streaming domain names, and cannot be changed once configured. If the video is not played in the selected acceleration area, the livestreaming quality may be compromised. Select an acceleration area that fits your needs. Options: ● **Europe** Select this option when the audience is in Europe. ● **Global** Select this option when the audience is not in Europe. **NOTICE** If the **Service Area** you select involves cross-border data transfer, you shall be responsible for such transfer. For details, see section 2.3 "Processing Your Content Data" of **Live Service Agreement**.
Stream Push Protocol	The parameter is displayed only when an ingest domain name is added. Stream push protocol of Media Live. Options: ● **RTMP**: **RTMP_PUSH** channels require RTMP ingest domain names. ● **SRT**: **SRT_PUSH** channels require SRT ingest domain names.

Step 4 Click **OK**.

A domain name whose **Status** is **Configuring** is displayed in the domain name list. About 3 to 5 minutes later, if the status becomes **Normal**, the domain name has been added.

Step 5 Repeat **step 1** to **step 4** to add a streaming domain name.

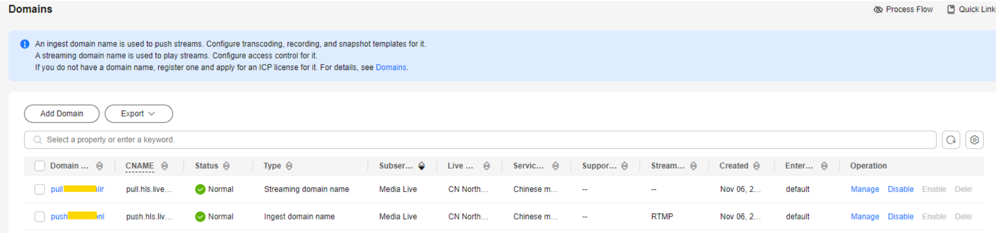
----End

Configuring CNAME Records

After domain names are added, a CNAME domain name is assigned to the ingest domain name and streaming domain name, respectively. You can log in to the **Live console** and view the domain names on the **Domains** page, as shown in **Figure 6-3**.

Add a CNAME record with your DNS provider. For details, see **Configuring CNAME Records**. After the CNAME record takes effect, all requests for your ingest domain name and streaming domain name are redirected to nodes of CDN and Live CDN for faster livestreaming.

Figure 6-3 Domains



Domains

Process Flow Quick Link

An ingest domain name is used to push streams. Configure transcoding, recording, and snapshot templates for it.
A streaming domain name is used to play streams. Configure access control for it.
If you do not have a domain name, register one and apply for an ICP license for it. For details, see Domains.

Add Domain Export

Select a property or enter a keyword.

□	Domain ...	CNAME	Status	Type	Subser...	Live ...	Servic...	Suppor...	Stream...	Created	Enter...	Operation
□	pull[redacted]lir	pull.hls.live...	✓ Normal	Streaming domain name	Media Live	CN North...	Chinese m...	--	--	Nov 06, 2...	default	Manage Disable Enable Delet
□	push[redacted]nl	push.hls.liv...	✓ Normal	Ingest domain name	Media Live	CN North...	Chinese m...	--	RTMP	Nov 06, 2...	default	Manage Disable Enable Delet

6.3 Pushing Streams and Streaming Content on a PC

This section describes how to push streams and stream content on a PC using third-party software.

Prerequisites

- You have configured an ingest domain name and a streaming domain name on the Live console by referring to **Adding Domain Names**.
- You have created a channel by referring to **Creating a Channel**.
- You have installed a streaming tool (recommended: **Open Broadcaster Software**). If you have not installed it yet, download and install it.
- You have installed a media player (recommended: **VLC media player**). If you have not installed it yet, download and install it.

Notes

- Check the output resolution of Open Broadcaster Software (OBS).

  Pay attention to the input and output resolution levels configured in OBS and the resolution level configured in the live transcoding template of the channel to guarantee the playback.

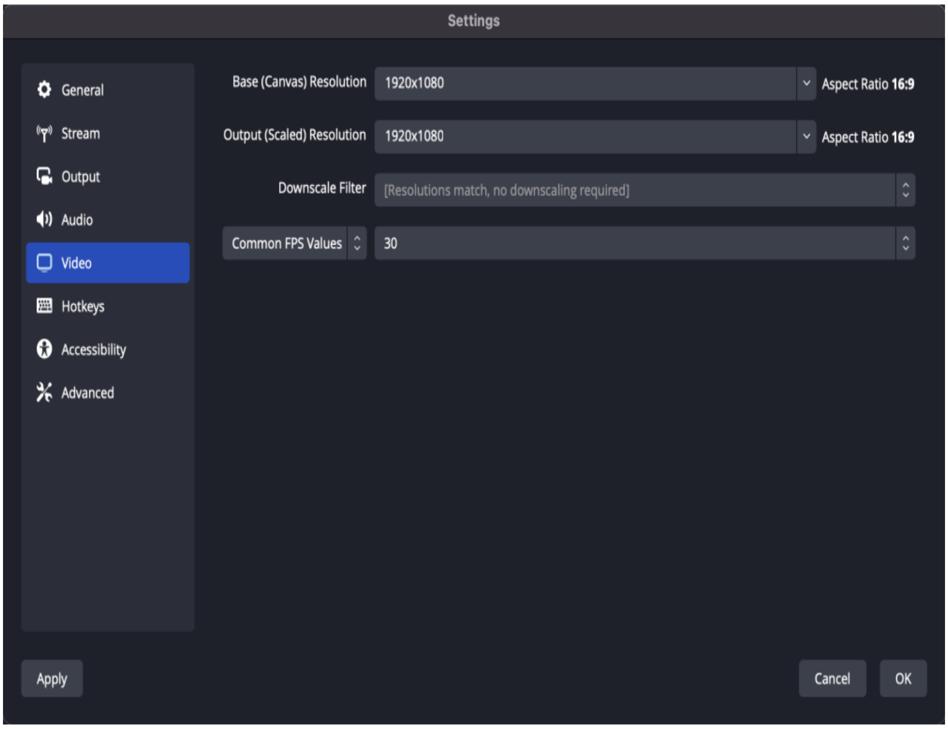
  To view the input and output resolution levels of OBS, perform the following steps:

  a. Open OBS on the local PC.

  b. On the top navigation bar, choose **File** > **Settings**.

  c. In the navigation pane on the left, choose **Video** to view **Base (Canvas) Resolution** and **Output (Scaled) Resolution**.

Figure 6-4 Video settings



Base (Canvas) Resolution 1920x1080 Aspect Ratio 16:9

Output (Scaled) Resolution 1920x1080 Aspect Ratio 16:9

Downscale Filter [Resolutions match, no downscaling required]

Common FPS Values 30

- Check the GOP duration of OBS following **Step 3**.

  You can set the GOP duration (recommended: 1–2 seconds) for OBS stream push. A GOP duration too long will compromise user experience when the I-frame interval of the source stream fluctuates greatly.

Pushing Streams

Step 1 Obtain the ingest URL.

1. Log in to the **Live console**.
2. In the navigation pane on the left, choose **Channels** under **Media Live**. The **Channels** page is displayed.
3. Find the desired channel and click **Manage** on the right. The **Update Channel** page is displayed.

   The ingest URL is required only when **Input Type** is set to **RTMP_PUSH** or **SRT_PUSH**. If **FLV_PULL**, **HLS_PULL**, or **SRT_PULL** is selected, stream push is not required. The streaming URL provided by the user is directly obtained and used by Media Live to push streams to the origin server.

   An example of the ingest URL is shown in **Figure 6-5**.

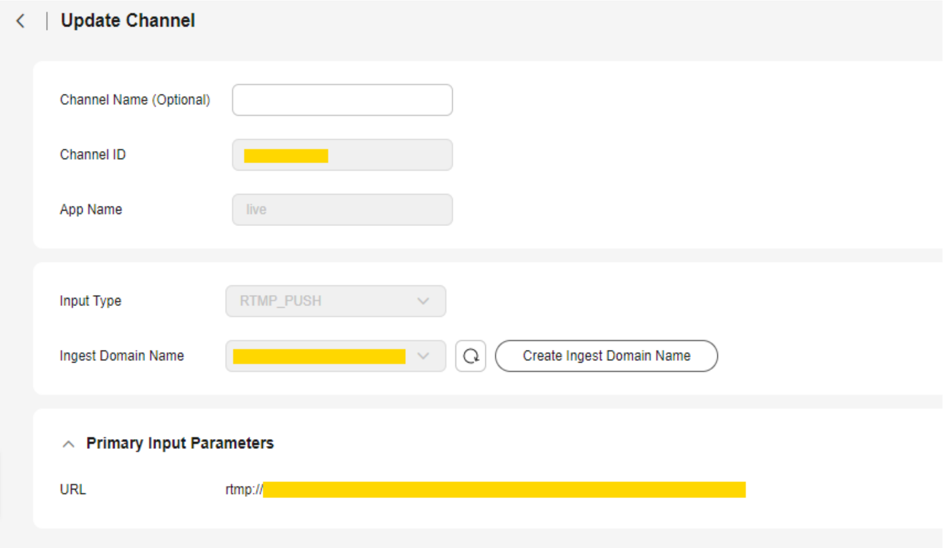
   NOTICE

   SRT_PUSH channels and **RTMP_PUSH** channels cannot be created at the same time for one domain name.

   – **RTMP_PUSH** URL example: rtmp://live-push.example.com/live/huaweitest?request_source=ott&channel_id=huaweitest

– **SRT_PUSH** URL example: srt://live-srt-push.example.com:5000?streamid=#!::h=push.bj4.srt.transcodeonline.com,r=live/srtpush,request_source=ott,channel_id=srtpush,m=publish

Figure 6-5 Viewing the ingest URL



Update Channel

Channel Name (Optional)

Channel ID [redacted]

App Name live

Input Type RTMP_PUSH

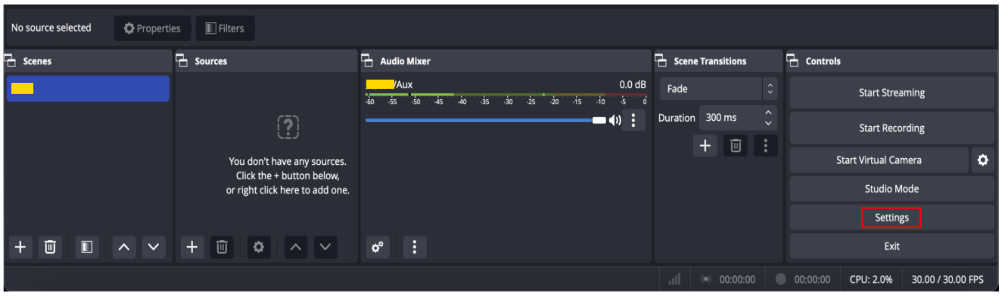
Ingest Domain Name [redacted]

Primary Input Parameters

URL rtmp://[redacted]

Step 2 Run OBS and click **Settings** in the lower right corner.

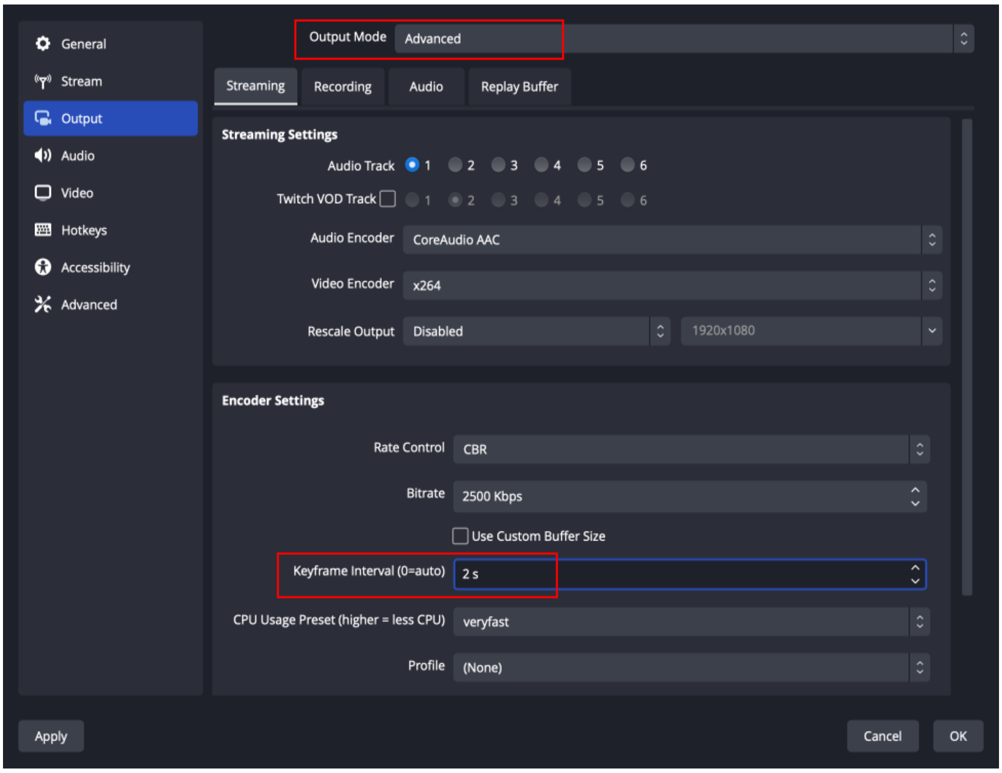
Figure 6-6 Settings



You don't have any sources.
Click the + button below,
or right click here to add one.

Step 3 In the navigation pane on the left, choose **Output**. Set **Output Mode** to **Advanced** and **Keyframe Interval** to **2**.

Figure 6-7 Output settings



Output Mode: Advanced

Streaming Settings

Audio Track ● 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

Twitch VOD Track □ ○ 1 ● 2 ○ 3 ○ 4 ○ 5 ○ 6

Audio Encoder: CoreAudio AAC

Video Encoder: x264

Rescale Output: Disabled 1920x1080

Encoder Settings

Rate Control: CBR

Bitrate: 2500 Kbps

□ Use Custom Buffer Size

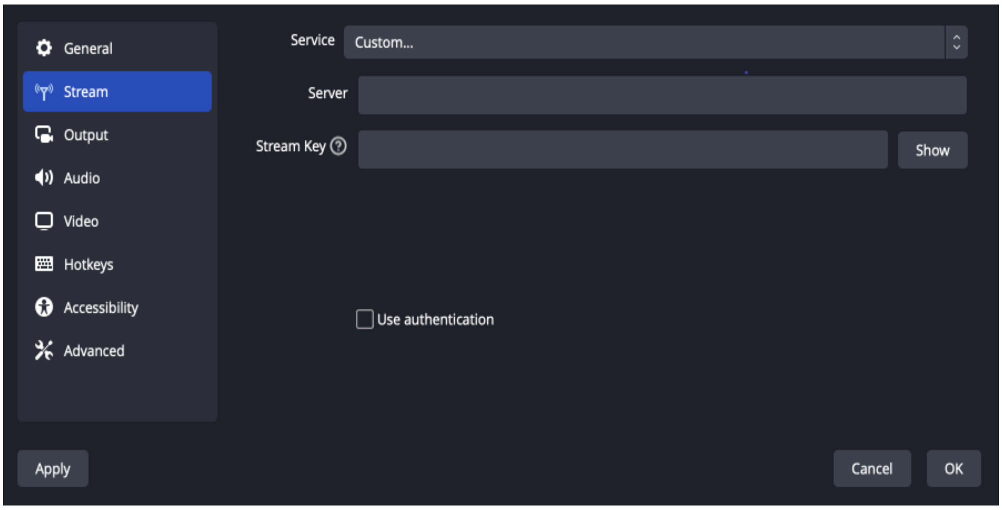
Keyframe Interval (0=auto): 2 s

CPU Usage Preset (higher = less CPU): veryfast

Profile: (None)

Step 4 In the navigation pane on the left, choose **Stream** and enter the ingest URL obtained in 1.

Figure 6-8 Livestream settings



Service: Custom...

Server:

Stream Key:

□ Use authentication

The ingest URL consists of two parts: **Server** and **Stream Key**.

NOTE

The parameter names on the GUI may vary depending on the OBS version, but the rules for configuring the parameters are the same.

Rules for setting an **RTMP_PUSH** ingest URL:

- **Server**: Enter the part from the beginning of the ingest URL to the ***AppName***, for example, rtmp://live-push.example.com/live/
- **Stream Key**: Enter the URL containing ***StreamName***, for example, huaweitest?request_source=ott&channel_id=huaweitest

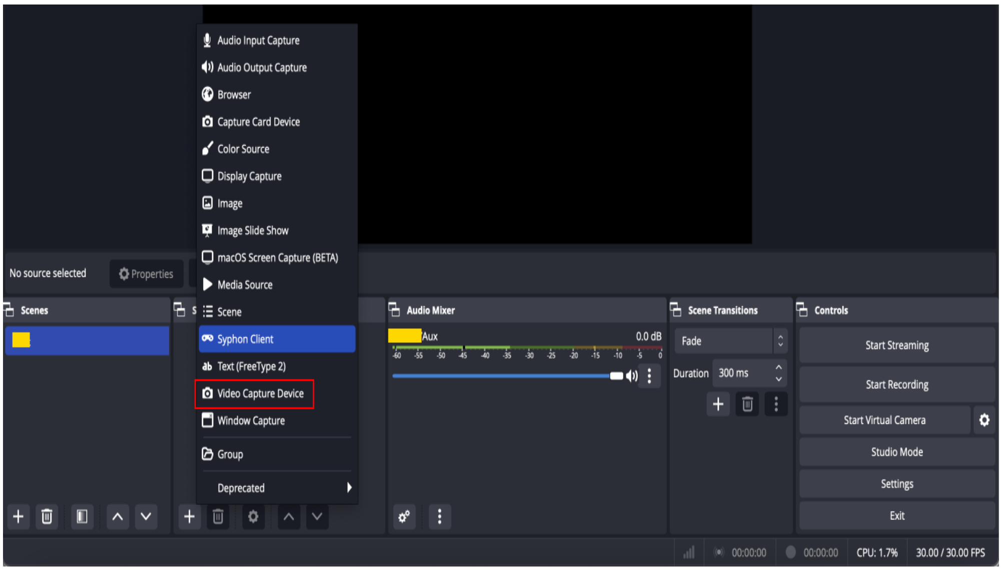
Rules for setting an **SRT_PUSH** ingest URL:

- Method 1:
  - **Server**: Enter a server URL, for example, srt://live-srt-push.example.com:5000
  - **Stream Key**: Enter the URL following **streamid=**, for example, #!::h=push.bj4.srt.transcodeonline.com,r=live/srtpush,request_source=ott,channel_id=srtpush,m=publish
- Method 2:
  - **Server**: Enter a complete URL, for example, srt://live-srt-push.example.com:5000?streamid=#!::h=push.bj4.srt.transcodeonline.com,r=live/srtpush,request_source=ott,channel_id=srtpush,m=publish
  - **Stream Key**: Leave it empty.

Step 5 Click **OK**.

Step 6 Click **+** in the lower left corner of the **Sources** area and add a stream source.

Figure 6-9 Source settings



- **Media Source** indicates local media files.
- **Video Capture Device** indicates a camera. If a camera is available on the PC, the camera is directly enabled.

Step 7 Click **Start Streaming** in the lower right corner.

----End

Streaming Content

Step 1 Obtain the streaming URL.

1. Log in to the **Live console**.
2. In the navigation pane on the left, choose **Channels** under **Media Live**. The **Channels** page is displayed.
3. Find the desired channel and click **Manage** on the right. The **Update Channel** page is displayed.

   View the streaming URL, as shown in **Figure 6-10**. Streaming URLs whose output protocol is HLS, DASH, or MSS can be assembled. Examples:

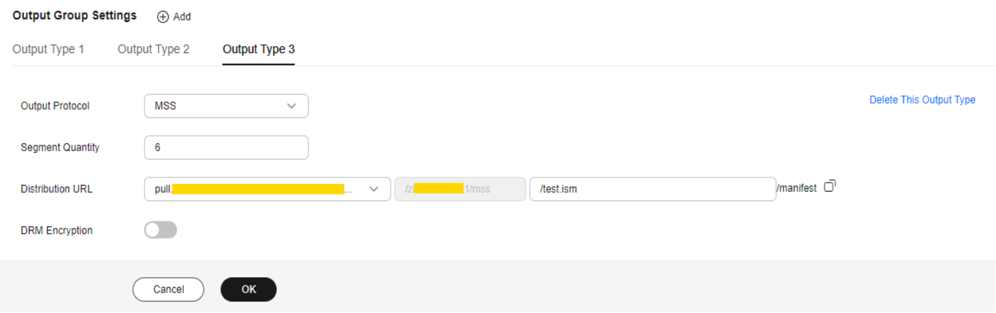
   – HLS: https://live-play.example.com/{*channelId*}/hls/{*unique_string*}/index.m3u8

   – DASH: https://live-play.example.com/{*channelId*}/dash/{*unique_string*}/index.mpd

   – MSS: https://live-play.example.com/{*channelId*}/mss/{*unique_string*}.ism/Manifest

   A streaming URL supports HTTPS. You can configure an HTTPS certificate by referring to **HTTPS Certificates**.

Figure 6-10 Viewing the streaming URL



Output Group Settings ⊕ Add

Output Type 1 | Output Type 2 | Output Type 3

Output Protocol: MSS

Segment Quantity: 6

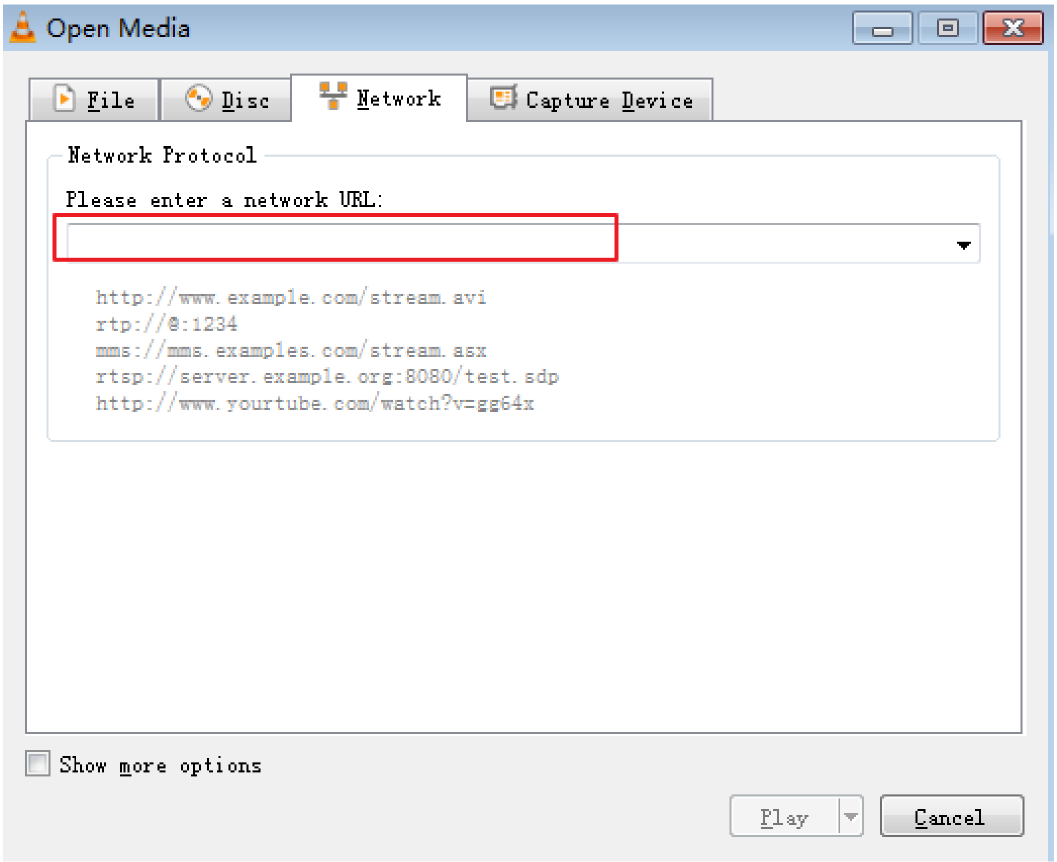
Distribution URL: pull.[redacted]... /z[redacted]1/mss /test.ism /manifest

DRM Encryption: ○

Step 2 Run VLC.

Step 3 On the menu bar, choose **Media** > **Open Multiple Files**.

Step 4 In the displayed dialog box, enter the streaming URL obtained in **1**. Click **Play**.



Open Media
File
Disc
Network
Capture Device
Network Protocol
Please enter a network URL:
http://www.example.com/stream.avi
rtp://@:1234
mms://mms.examples.com/stream.asx
rtsp://server.example.org:8080/test.sdp
http://www.yourtube.com/watch?v=gg64x
□ Show more options
Play
Cancel

----End

7 Console Operations

7.1 Prerequisites

Preparations

- You have registered with Huawei Cloud and completed real-name authentication.

  NOTE

  If you are a **Huawei Cloud (International/Europe)** user, you need to complete real-name authentication when you:

  - Purchase and use cloud services on Huawei Cloud nodes in the Chinese mainland. In this case, real-name authentication is required by the laws and regulations of the Chinese mainland.
  - Plan to use Live in regions in the Chinese mainland.
- Domain names for Media Live are available. A **PUSH** channel requires an ingest domain name and a streaming domain name, and the two domain names must be different. A **PULL** channel does not require an ingest domain name.

  NOTE

  If you want to perform livestreaming acceleration in Huawei Cloud regions in or outside the Chinese mainland, the domain names must complete ICP filing in advance as required by the Ministry of Industry and Information Technology (MIIT).
- When a new IAM user uses Media Live for the first time, they need to configure the permission to create a domain name.

Notes

Live may assign a default ingest domain name to you. Examples:

- Ingest domain name format in the Chinese mainland: *{projectid}***.hwcloudlive.com**

  Example: 0c283a271****************9459b6a.hwcloudlive.com
- Ingest domain name format outside the Chinese mainland: *{projectid}***.ott.huawei**

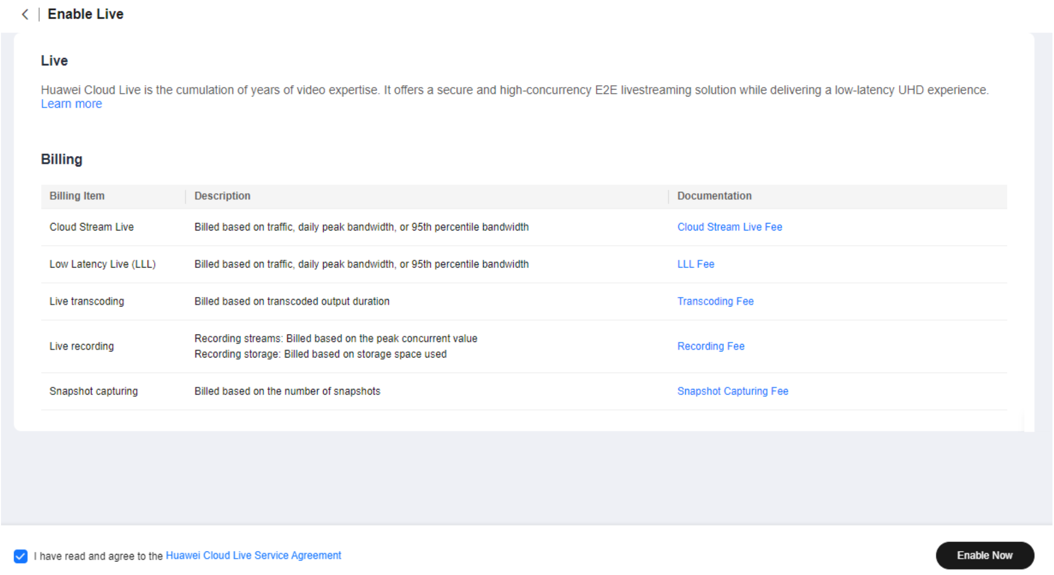
Example: 0c283a271****************9459b6a.ott.huawei

The preceding ingest domain names are for internal use of the service. If you are assigned these domain names, the domain names are visible but cannot be called or used. This does not affect your use of Live or cause extra fees.

Risk Warning on the First Service Enabling

If you purchase Live for the first time, the page shown in **Figure 7-1** will be displayed. You need to check the details of each billing item and read the *Huawei Cloud Live Service Agreement* carefully before enabling Live.

Figure 7-1 Enabling Live



< | Enable Live

Live

Huawei Cloud Live is the cumulation of years of video expertise. It offers a secure and high-concurrency E2E livestreaming solution while delivering a low-latency UHD experience.
Learn more

Billing

Billing Item	Description	Documentation
Cloud Stream Live	Billed based on traffic, daily peak bandwidth, or 95th percentile bandwidth	Cloud Stream Live Fee
Low Latency Live (LLL)	Billed based on traffic, daily peak bandwidth, or 95th percentile bandwidth	LLL Fee
Live transcoding	Billed based on transcoded output duration	Transcoding Fee
Live recording	Recording streams: Billed based on the peak concurrent value Recording storage: Billed based on storage space used	Recording Fee
Snapshot capturing	Billed based on the number of snapshots	Snapshot Capturing Fee

☑ I have read and agree to the Huawei Cloud Live Service Agreement

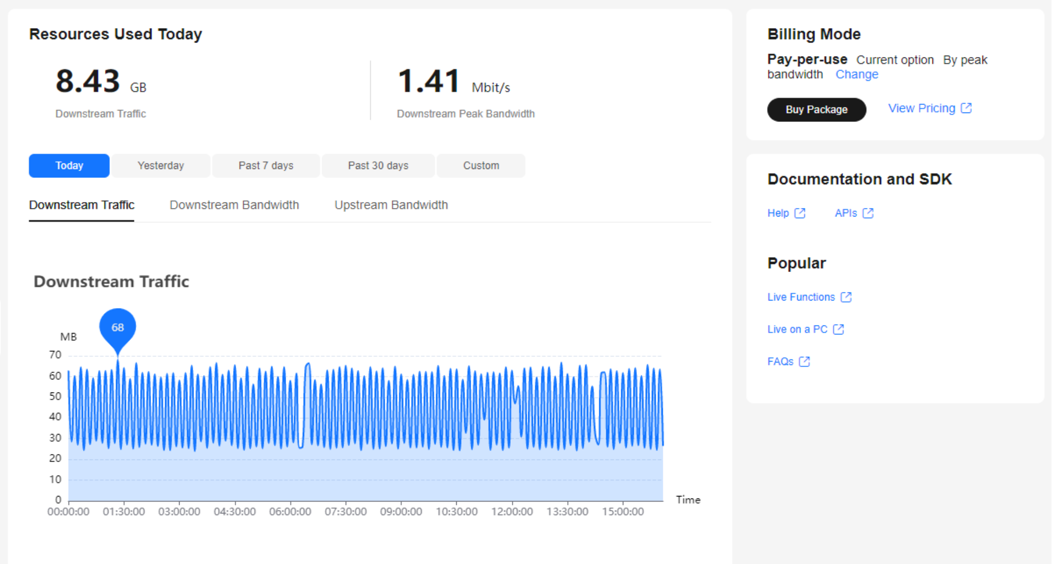
7.2 Functions

On the Live Console, you can manage Media Live domain names, transcoding templates, and channels. In addition, resource monitoring is provided to help you analyze data in real time.

Dashboard

Log in to the **Live console**. The **Dashboard** page is displayed.

Figure 7-2 Dashboard



Resources Used Today

8.43 GB Downstream Traffic

1.41 Mbit/s Downstream Peak Bandwidth

Billing Mode

Pay-per-use Current option By peak bandwidth Change

On this page, you can check the following information. You can also click **Quick Links** in the upper right corner to read the documentation.

- **Today**
  - **Downstream Traffic**: total downstream traffic used by all streaming domain names on the current day
  - **Downstream Peak Bandwidth**: peak value of the downstream bandwidth used by all streaming domain names on the current day
- You can check the recent livestreaming resource usage trend.
  - **Downstream Traffic**: total downstream traffic used by all streaming domain names in a specific period
  - **Downstream Bandwidth**: total downstream bandwidth used by all streaming domain names in a specific period
  - **Upstream Bandwidth**: total upstream bandwidth used by the streaming device of a selected streaming domain name in a specific period

  NOTE

  You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.
- **Billing Mode** displays the current CDN billing mode. You can click **Change** to change the CDN billing mode.

Functions

You can configure or use the functions in the navigation pane of the **Live console**.

Table 7-1 Functions of the console

Category	Function	Description
Domains	**Adding Domain Names**	You can add and manage your own acceleration domain names and view the CNAME records of the domain names.
	HTTPS Certificates	If the streaming URL of Media Live needs to start with **https://**, configure an HTTPS certificate by referring to **HTTPS Certificates**.

Category	Function	Description
Channels	**Creating a Channel**	You can create a channel before the media livestreaming starts. The media file input type can be: ● **FLV_PULL**: Stream push is not required. The streaming URL provided by the user is directly obtained and used by Media Live to push streams to the origin server. The streaming URL supports only HTTP. ● **RTMP_PUSH**: An RTMP ingest domain name needs to be configured for stream push. ● **HLS_PULL**: Stream push is not required. The streaming URL provided by the user is directly obtained and used by Media Live to push streams to the origin server. If **Input Type** is set to **HLS_PULL**, the media URLs provided users have the following constraints: – A streaming URL supports only HTTP and HTTPS. – Encrypted streams are not supported. – Audio-only streams are not supported. – Subtitling is not supported. ● **SRT_PULL**: Stream push is not required. The streaming URL provided by the user is directly obtained and used by Media Live to push streams to the origin server. ● **SRT_PUSH**: An SRT ingest domain name needs to be configured for stream push. To ensure reliability, channels of the **SRT_PUSH** input type must be able to: – Support primary and standby URLs. The encoder needs to push streams to both the primary and standby URLs. – Resume stream push when the stream push by the encoder is interrupted. The recommended interval for resuming stream push is shorter than the duration of a segment.
Live Transcoding	**Creating a Transcoding Template**	You can configure a transcoding template for live videos to transcode live streams into video streams with different resolutions and bitrates to meet a broad range of requirements.

Category	Function	Description
Service Monitoring	**Service Monitoring**	You can view the monitoring information about a streaming domain name, including the downstream bandwidth/traffic, all status codes returned in request responses, number of concurrent downstream requests, and input quality.
Cloud Resource Authorization	**Cloud Resource Authorization**	If DRM encryption needs to be enabled for a channel and **Interconnection Mode** is set to **FunctionGraph proxy access**, you need to enable **FunctionGraph agency** in advance. After the authorization is successful, Media Live can query functions, workflows, and triggers, and call functions.
Tools	**Obtaining a Catch-Up TV/ Time-Shifted Viewing URL**	You can obtain the catch-up TV/time-shifted viewing URL of a channel.

7.3 Permissions Management

7.3.1 Creating a User and Assigning Live Permissions

This section describes how to use **IAM** to implement refined permissions management for your Live resources. With IAM, you can:

- Create IAM users for employees from different departments of your enterprise. In this way, each IAM user has a unique security credential to use Live resources.
- Assign only the permissions required for users to perform a specific task.
- Entrust a Huawei Cloud account or cloud service to perform efficient O&M on your Live resources.

If your Huawei Cloud account does not require individual IAM users, skip this section.

This section describes the procedure for assigning permissions. For details, see **Figure 7-3**.

Notes

Submit a service ticket to apply for permissions management on the following two types of Live users:

- Users who had created domain names in the AP-Singapore region before March 1, 2022.
- Users who had created domain names in the CN North-Beijing4 region before March 16, 2022.

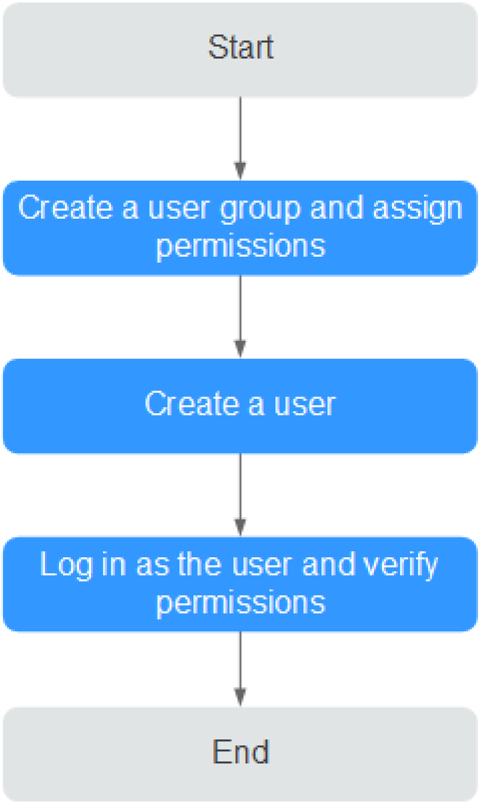
After **permissions management** is enabled, unauthorized **IAM users** cannot call the Live APIs. Ensure that IAM users have been assigned the Live permissions.

Prerequisites

Learn about the Live permissions that can be assigned to the user group and assign the permissions as required. For details, see the **system-defined permissions on Live**.

Process Flow

Figure 7-3 Process for assigning read-only permissions on Live


Start
Create a user group and assign permissions
Create a user
Log in as the user and verify permissions
End

1. **Create a user group and assign permissions**

   Create a user group on the IAM console, and attach the **Live ReadOnlyAccess** policy to the group.

2. **Create a user and add them to the user group**

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the Live console as the created user, and verify that the user only has read permissions on Live.

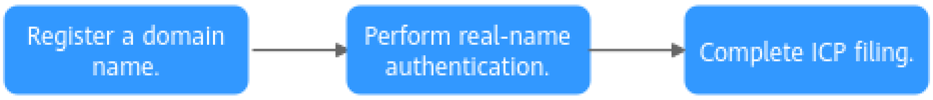
   Choose **Live** in **Service List**. Then click **Domains** to add a domain name. If a message is displayed indicating insufficient permissions for performing the operation, the **Live ReadOnlyAccess** policy has taken effect.

7.4 Domain Name Management

7.4.1 Domain Name Admission Standards

Before connecting your domain name to Huawei Cloud Media Live, you can read this section to understand the access conditions and restrictions of acceleration domain names to avoid losses caused by rule violations

Admission Process



1. Register a domain name: If you do not have a domain name, you can purchase one from Huawei Cloud or a DNS provider.

   NOTE

   A top-level domain name cannot be used as an ingest domain or streaming domain. If your domain name is **example.com**, you can use second-level domain names, for example, **test-push.example.com** and **test-play.example.com**, as the ingest domain and streaming domain.

2. Perform real-name authentication: You can log in to the **Huawei Cloud official website** and complete real-name authentication for individuals or enterprises.

   NOTE

   If you are a **Huawei Cloud (International/Europe)** user, you need to complete real-name authentication when you:

   - purchase and use cloud services on Huawei Cloud nodes in the Chinese mainland. In this case, real-name authentication is required by the laws and regulations of the Chinese mainland.
   - plan to use Live in regions in the Chinese mainland.

3. Complete ICP filing: If you want to perform livestreaming acceleration in Huawei Cloud regions in or outside the Chinese mainland, the domain names of Media Live must complete ICP filing in advance as required by the Ministry of Industry and Information Technology (MIIT).

Quantity Limit

By default, you can add up to 64 domain names in your account. If you have additional requirements, **submit a service ticket** for technical support.

Content Moderation

Media Live does not support the access of websites that violate related laws and regulations, including but not limited to:

- Websites that contain pornographic content or content related to gambling, illegal drugs, frauds, or infringement

- Gaming websites that run on illegal private servers
- Websites that provide pirated games/software/videos
- P2P lending websites
- Unofficial lottery websites
- Unlicensed hospital and pharmaceutical websites
- Inaccessible websites or websites that do not contain any substantial information

NOTE

- If your acceleration domain name content violates related laws and regulations, you shall bear the related risks.
- If any pornographic content or content related to gambling, illegal drugs, or frauds is found on your domain name, the domain name and other domain names that use the same origin server will be deleted from Media Live and can no longer access Media Live. Acceleration domain name quota of the account will be reduced to 0.

Domain Name Rules

Table 7-2 describes the domain name rules.

Table 7-2 Domain name rules

Domain Name Status	Rule
A domain name that has no access traffic for more than 90 days (the domain name is either working or malfunctioning)	The domain name will be automatically disabled and the records related to the domain name will be saved. If you want to continue using the domain name, **re-enable it**.
A domain name that has been disabled for more than 90 days (the domain name may not have been approved)	The records related to the domain name will be automatically deleted. If you want to continue using the domain name, **add it again**.

7.4.2 Adding Domain Names

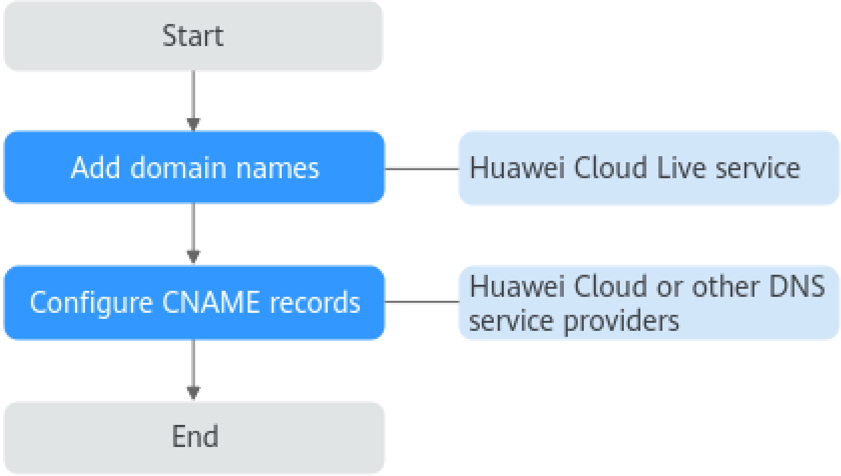
Before using Media Live, you must add ingest domain names and streaming domain names to Media Live.

Before connecting your domain name to Huawei Cloud Media Live, you need to understand the access conditions and restrictions of acceleration domain names to avoid losses caused by rule violations. For details, see **Domain Name Admission Standards**.

Domain Name Admission Process

Figure 7-4 shows the process of using your own domain name for livestreaming acceleration.

Figure 7-4 Admission process


Start
Add domain names
Huawei Cloud Live service
Configure CNAME records
Huawei Cloud or other DNS service providers
End

1. **Add an ingest domain name and a streaming domain name** (both licensed) to Media Live.
2. **Configure CNAME records** at your domain names' DNS providers so that the CNAME records allocated to Live point to the domain names.

Prerequisites

- You have registered with Huawei Cloud and completed real-name authentication.

  NOTE

  If you are a **Huawei Cloud (International/Europe)** user, you need to complete real-name authentication when you:

  - Purchase and use cloud services on Huawei Cloud nodes in the Chinese mainland. In this case, real-name authentication is required by the laws and regulations of the Chinese mainland.
  - Plan to use Live in regions in the Chinese mainland.
- Domain names for Media Live are available. A **PUSH** channel requires an ingest domain name and a streaming domain name, and the two domain names must be different. A **PULL** channel does not require an ingest domain name.

  NOTE

  If you want to perform livestreaming acceleration in Huawei Cloud regions in or outside the Chinese mainland, the domain names must complete ICP filing in advance as required by the Ministry of Industry and Information Technology (MIIT).
- When a new IAM user uses Media Live for the first time, they need to configure the permission to create a domain name.

Notes

- An area needs to be specified for stream push, and the streaming domain name needs to be associated with an ingest domain name. In this way, a streaming domain name can be used to watch livestreaming in the area where the ingest domain name is located. That is, a streaming domain name cannot be used to watch livestreaming in and outside China at the same time.
- The price of livestreaming outside China is different from that in China. For details, see **Pricing Details**.
- If the streaming URL is not used in the selected **Service Area**, the playback quality may be compromised.
- If the **Service Area** of the streaming domain name is **Chinese mainland** or **Global**, and the origin server of the ingest domain name is in the Chinese mainland, the domain names must be licensed in the Chinese mainland.
- Live may assign a default ingest domain name to you. Examples:
  - Ingest domain name format in the Chinese mainland: *{projectid}***.hwcloudlive.com**

    Example: 0c283a271****************9459b6a.hwcloudlive.com
  - Ingest domain name format outside the Chinese mainland: *{projectid}***.ott.huawei**

    Example: 0c283a271****************9459b6a.ott.huawei

  The preceding ingest domain names are for internal use of the service. If you are assigned these domain names, the domain names are visible but cannot be called or used. This does not affect your use of Live or cause extra fees.

Procedure

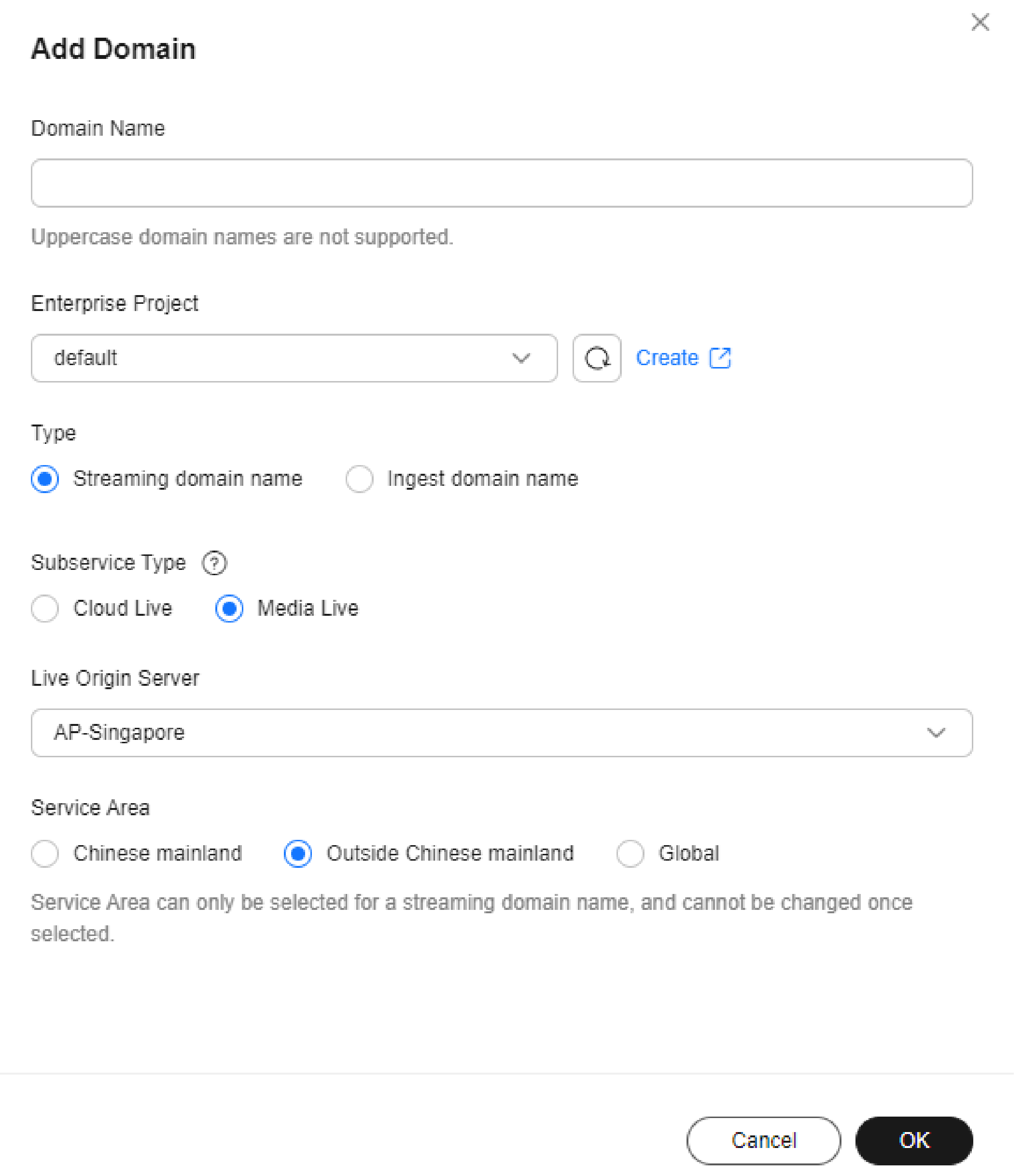
Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Add Domain**. On the displayed page, enter a streaming domain name or an ingest domain name.

A **PUSH** channel requires an ingest domain name and a streaming domain name, while a **PULL** channel requires only a streaming domain name.

Figure 7-5 Adding a domain name



Add Domain

Domain Name

Uppercase domain names are not supported.

Enterprise Project

default

Type

● Streaming domain name ○ Ingest domain name

Subservice Type

○ Cloud Live ● Media Live

Live Origin Server

AP-Singapore

Service Area

○ Chinese mainland ● Outside Chinese mainland ○ Global

Service Area can only be selected for a streaming domain name, and cannot be changed once selected.

Table 7-3 Parameters

Parameter	Description
Domain Name	Enter a second-level ingest domain name or streaming domain name, for example, test-push.example.com. **NOTE** ● The domain name can contain a maximum of 64 characters, which cannot contain uppercase letters. ● An ingest domain name must be different from a streaming domain name. Wildcard domains are not allowed. ● By default, you can add up to 64 domain names in your account. To add more domain names, **submit a service ticket**.

Parameter	Description
Enterprise Project	Add domain names to enterprise projects for unified management. On the **Create Enterprise Project** page, **create an enterprise project** (whose name is **default** by default) and **add the user group to the enterprise project**. By doing so, users in this user group obtain the permissions on the domain names in the enterprise project. **NOTE** Only an enterprise account can configure enterprise projects.
Type	If you enter an ingest domain name for **Domain Name**, then select **Ingest Domain Name** for **Type**. The domain name type cannot be changed once configured.
Subservice Type	Subservice type of the Live service. Options: ● **Cloud Live**: This easy-to-use livestreaming service provides diverse live acceleration capabilities for entertainment, e-commerce, and education scenarios. ● **Media Live**: This broadcast-grade livestreaming service supports features such as channel management and content encryption, making it an ideal option for media assets and broadcasting. Select **Media Live**.
Live Origin Server	Area where the Live origin server is located. For details, see How Do I Select a Live Origin Server and Acceleration Area? The Live origin server cannot be changed once configured. Select the nearest origin server. Currently, Live is supported in the following regions: ● CN North-Beijing4 of Huawei Cloud (Chinese Mainland) ● AP-Singapore, ME-Riyadh, CN-Hong Kong, and AF-Johannesburg of Huawei Cloud (Singapore) By default, ME-Riyadh, CN-Hong Kong, and AF-Johannesburg are unavailable. To select these regions, **submit a service ticket** to contact Huawei Cloud technical support. ● Dublin of Huawei Cloud (Europe): EU-Dublin.

Parameter	Description
Service Area	Area where streaming domain names can be accelerated. For details, see How Do I Select a Live Origin Server and Acceleration Area? This parameter is valid only for streaming domain names, and cannot be changed once configured. If the video is not played in the selected acceleration area, the livestreaming quality may be compromised. Select an acceleration area that fits your needs. Options: ● **Europe** Select this option when the audience is in Europe. ● **Global** Select this option when the audience is not in Europe. **NOTICE** If the **Service Area** you select involves cross-border data transfer, you shall be responsible for such transfer. For details, see section 2.3 "Processing Your Content Data" of **Live Service Agreement**.
Stream Push Protocol	The parameter is displayed only when an ingest domain name is added. Stream push protocol of Media Live. Options: ● **RTMP**: **RTMP_PUSH** channels require RTMP ingest domain names. ● **SRT**: **SRT_PUSH** channels require SRT ingest domain names.

Step 4 Click **OK**.

A domain name whose **Status** is **Configuring** is displayed in the domain name list. About 3 to 5 minutes later, if the status becomes **Normal**, the domain name has been added.

Step 5 Add a CNAME record to your domain's DNS records.

For details, see **Configuring CNAME Records**. Once the configuration takes effect, livestreaming acceleration is automatically enabled for the domain name.

----End

7.4.3 Configuring CNAME Records

After a domain name is added, the system automatically assigns a CNAME record to the domain name. You need to add the CNAME record to your domain's DNS records. Acceleration is enabled once the configuration takes effect.

Notes

- Configure CNAME records for the ingest domain name and streaming domain name separately.

Prerequisites

You have added an ingest domain name and a streaming domain name.

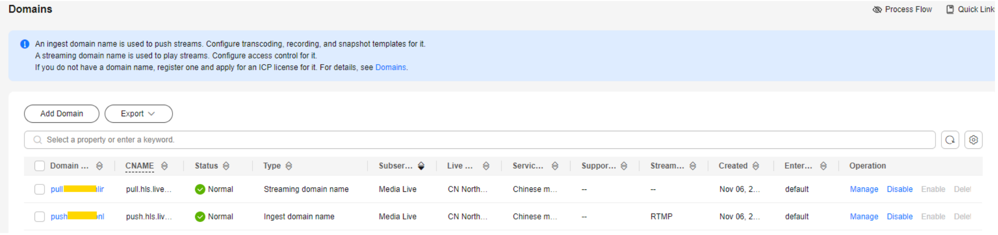
Procedure

The following uses a streaming domain name as an example. The procedure for configuring the CNAME record for an ingest domain name is the same.

Step 1 Obtain the CNAME record.

1. Log in to the Live console. In the navigation pane, choose **Domains**.
2. Obtain the corresponding CNAME in the **CNAME** column.

Figure 7-6 Domains



Domains

An ingest domain name is used to push streams. Configure transcoding, recording, and snapshot templates for it.
A streaming domain name is used to play streams. Configure access control for it.
If you do not have a domain name, register one and apply for an ICP license for it. For details, see Domains.

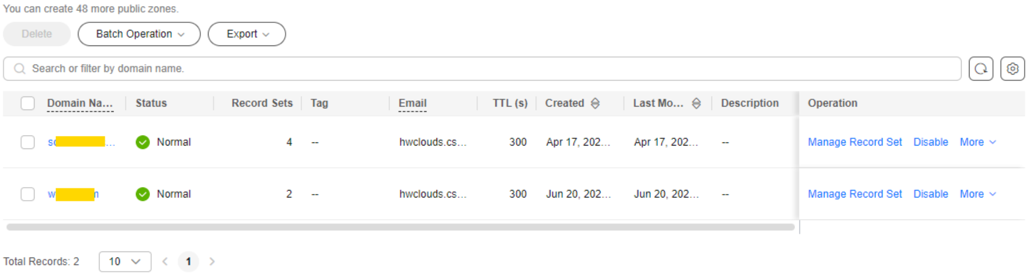
Domain ...	CNAME	Status	Type	Subser...	Live ...	Servic...	Suppor...	Stream...	Created	Enter...	Operation
pull[redacted]lir	pull.hls.live...	Normal	Streaming domain name	Media Live	CN North...	Chinese m...	--	--	Nov 06, 2...	default	Manage Disable Enable Delet
push[redacted]nl	push.hls.liv...	Normal	Ingest domain name	Media Live	CN North...	Chinese m...	--	RTMP	Nov 06, 2...	default	Manage Disable Enable Delet

Step 2 Log in to the **Domain Name Service (DNS)** console.

Step 3 In the navigation pane on the left, choose **Public Zones**.

Step 4 Click the target domain name in the **Domain Name** column, as shown in **Figure 7-7**.

Figure 7-7 Domain name list



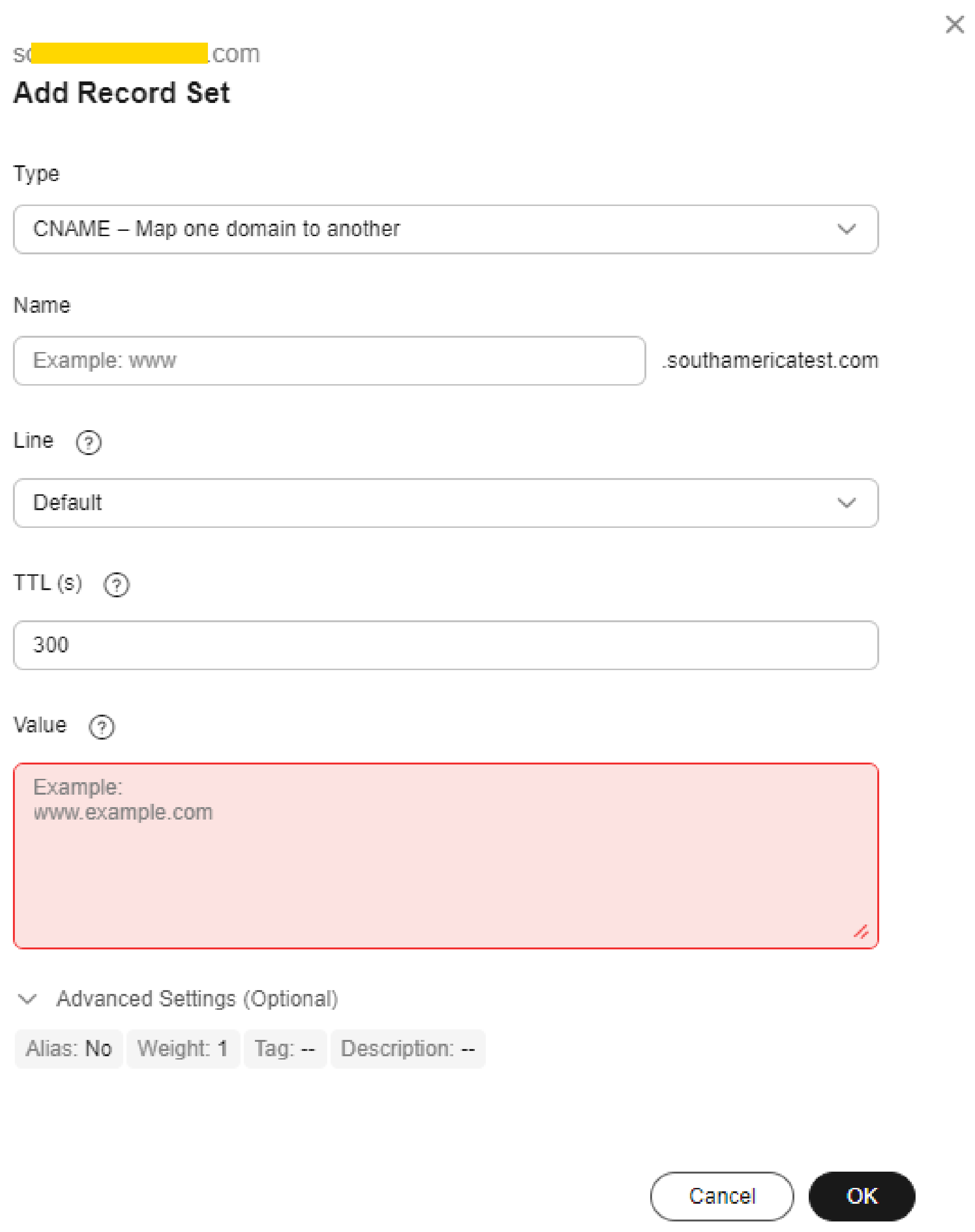
You can create 48 more public zones.

Domain Na...	Status	Record Sets	Tag	Email	TTL (s)	Created	Last Mo...	Description	Operation
s[redacted]...	Normal	4	--	hwclouds.cs...	300	Apr 17, 202...	Apr 17, 202...	--	Manage Record Set Disable More
w[redacted]n	Normal	2	--	hwclouds.cs...	300	Jun 20, 202...	Jun 20, 202...	--	Manage Record Set Disable More

Total Records: 2

Step 5 Click **Add Record Set** in the upper right corner.

Figure 7-8 Adding a record set



s[redacted].com

Add Record Set

Type

CNAME – Map one domain to another

Name

Example: www .southamericatest.com

Line

Default

TTL (s)

300

Value

Example:
www.example.com

Advanced Settings (Optional)

Alias: No Weight: 1 Tag: -- Description: --

Configure the parameters by referring to **Table 7-4**.

Table 7-4 Parameters

Parameter	Description
Type	Type of the record set. Select **CNAME – Map one domain to another** here.

Parameter	Description
Name	Enter the second-level domain name. You do not need to enter the suffix. For example, if the streaming domain name is **play-test.example.com**, enter **play-test**.
Line	Used when the DNS server is resolving a domain name. It returns the IP address of the server according to the visitor source. For details, see **Resolution Lines**. This parameter is available only for public domain names. Select **Default**.
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The smaller the value is, the quicker the record takes effective. The default value is 300 seconds. You can retain the default value.
Value	Domain name to be pointed to, that is, the CNAME record obtained in step 1 of this section. For example, if the streaming domain name is **play-test.example.com**, enter **play-test.example.com.c.cdnhwc3.com**.
Alias	Whether to associate the record set with a cloud resource. ● Enabled: The record set will be associated with a cloud resource. ● Disabled: The record set will not be associated with a cloud resource. Toggle off the switch, that is, disable this function.
Weight	(Optional) Weight of a record set. The value ranges from **0** to **1000** and defaults to **1**. This parameter is available only for public domain names. If a resolution line in a zone contains multiple record sets of the same type, you can **configure weighted routing** for each record set. Set this parameter to **1**.
Tag	(Optional) Identifier of a record set. Each tag contains a key and a value. You can add up to 10 tags to a record set. For details about how to name a key and a value, see **Adding a CNAME Record Set**. Examples: ● example_key1 ● example_value1
Description	(Optional) Describes a domain name. The description can contain a maximum of 255 characters.

Step 6 Click **OK**.

The record set you added is displayed in the list. If the status of the record set is **Normal**, the record set has been added.

Step 7 Perform 1 to 6 to configure the CNAME for the ingest domain name.

----End

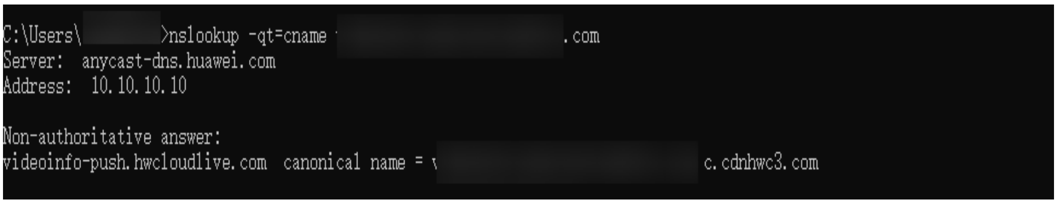
Verifying that the CNAME Has Taken Effect

Open the command line interface that comes with Windows and run the following command:

```
nslookup -qt=cname Acceleration domain name
```

If the CNAME is displayed, the CNAME has taken effect. A typical command output is shown in Figure 7-9.

Figure 7-9 Command output



```
C:\Users\[redacted]>nslookup -qt=cname [redacted].com
Server:  anycast-dns.huawei.com
Address:  10.10.10.10

Non-authoritative answer:
videoinfo-push.hwcloudlive.com  canonical name = [redacted]c.cdnhwc3.com
```

7.4.4 Managing Domain Names

After an ingest domain name or streaming domain name is added, you can view basic information about the added domain names on the **Domains** page. You can also disable, enable, or delete an added domain name as required.

Procedure

Step 1 Log in to the Live console.

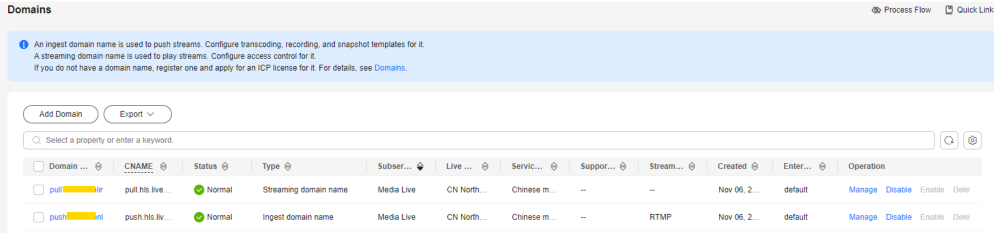
Step 2 In the navigation pane, choose **Domains**.

Step 3 Perform the following operations as required.

- View domain name details.

  In the domain list, you can view the CNAME record, type, status, and creation time of a domain name.

  Figure 7-10 Domains

  Domains

  An ingest domain name is used to push streams. Configure transcoding, recording, and snapshot templates for it.
  A streaming domain name is used to play streams. Configure access control for it.
  If you do not have a domain name, register one and apply for an ICP license for it. For details, see Domains.

  Select a property or enter a keyword.

Domain ...	CNAME	Status	Type	Subser...	Live ...	Servic...	Suppor...	Stream...	Created	Enter...	Operation
pull[redacted]lir	pull.hls.live...	Normal	Streaming domain name	Media Live	CN North...	Chinese m...	--	--	Nov 06, 2...	default	Manage Disable Enable Delet
push[redacted]nl	push.hls.liv...	Normal	Ingest domain name	Media Live	CN North...	Chinese m...	--	RTMP	Nov 06, 2...	default	Manage Disable Enable Delet

  Click **Manage** in the **Operation** column to view details.

- Disable a domain name.

  NOTICE

  After a domain name is disabled, the Media Live channels that are started properly under the domain name will be unavailable. When a domain name is disabled, affected channels cannot be restarted.

  To disable a domain name, click **Disable** in the row that contains the target domain name. If the status changes to **Disabled**, the domain name has been disabled.

- Enable a domain name.

  To enable a disabled domain name, click **Enable** in the **Operation** column. If the status changes to **Normal**, the domain name has been enabled.

- Delete a domain name.

  Only a domain name in the **Disabled** status can be deleted. After disabling a domain name, click **Delete** in the row containing the domain name to delete it.

----End

7.4.5 Configuring IPv6 Access

Once the IPv6 switch is toggled on, Live provides IPv6-compatible PoPs for access.

Notes

Most PoPs in the Chinese mainland support IPv6. After IPv6 access is enabled, if IPv6 is used to access Live but the optimal PoP does not support IPv6, IPv4 can still be used to access the PoP.

Procedure

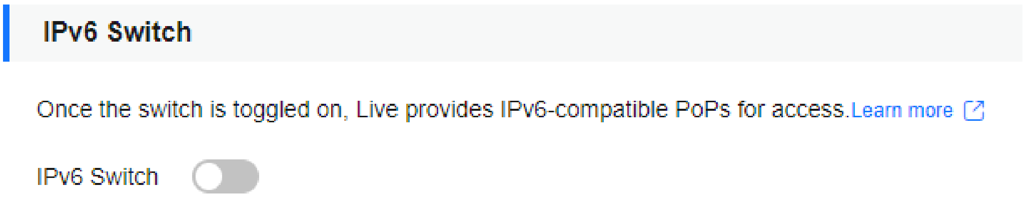
Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the **Operation** column of the desired domain name. The **Basic Info** page is displayed.

Step 4 Toggle on the IPv6 switch.

Figure 7-11 IPv6 switch



IPv6 Switch

Once the switch is toggled on, Live provides IPv6-compatible PoPs for access.Learn more

IPv6 Switch

----End

7.4.6 Configuring a Geo-blocking Whitelist

By default, a user's IP address belongs to the acceleration area configured for the streaming domain name and can be used to pull streams from Live. To specify the areas that can be accessed by a streaming domain name, perform the operations described in this section.

Notes

- Huawei Cloud periodically updates IPv4 databases in all areas around the world. The geo-blocking whitelist configured here may not be able to identify all IP addresses. Terminals cannot identify a small number of IP addresses that are not in the databases. If high accuracy is required, exercise caution when using this function.
- If IP addresses in the databases cannot be accurately identified, the request may be scheduled to an unexpected billing area and billed in that area. For details, see **Product Pricing Details**.

Prerequisites

- A geo-blocking whitelist can only be configured for streaming domain names.
- Only one geo-blocking whitelist can be configured for each streaming domain name. The whitelist can be modified or deleted.

Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 In the domain name list, find the streaming domain name whose geo-blocking needs to be specified and click **Manage** in the **Operation** column. The **Basic Info** page is displayed.

Step 4 In the navigation pane, choose **Templates** > **Geo-blocking**.

Step 5 Click **Add**. In the **Geo-blocking** dialog box that is displayed, select the areas where the streaming domain name can work and add them to **Selected Areas**.

Step 6 Click **OK**. The geo-blocking whitelist has been added.

After the whitelist is added, you can perform the following operations:

- Click **Edit** to change the areas that can be accessed by the streaming domain name.
- Click **Delete** to delete the whitelist.

----End

7.4.7 Stream Authentication

Live provides multiple authentication mechanisms, including URL validation and access control list (ACL) validation, to prevent livestreaming resources from being stolen. If multiple authentication mechanisms are configured, livestreaming resources can be accessed only after the access request passes all the authentication mechanisms.

The method of configuring streaming authentication is the same as that of configuring playback authentication. For details, see **URL Validation** and **ACL**.

7.4.8 Playback Authentication

7.4.8.1 Overview

Live provides referer validation, URL validation, and ACL to identify and filter out malicious visitors. Only visitors that meet the rules can use Live.

URL validation protects live resources from unauthorized download and theft. Referer validation uses referer blacklists/whitelists to prevent hotlinking. However, because the referer content can be forged, referer validation cannot well protect live resources. Therefore, you are advised to use URL validation. **Table 7-5** shows the authentication mechanism of the Live service.

Table 7-5 Authentication mechanism

Function	Description	Configuration
Referer validation	You can configure the referer blacklist and whitelist to identify and filter out malicious visitors.	For details, see **Referer Validation**
URL validation	You can configure a key and validate the URL to protect live resources.	For details, see **URL Validation**.
ACL	You can configure an IP address blacklist and whitelist to identify and filter out malicious visitors.	For details, see **ACL**.

7.4.8.2 Referer Validation

Referer validation allows you to control access sources based on the referer field carried in an HTTP request. CDN allows or rejects playback requests based on the configured blacklist or whitelist.

Notes

- This function is optional and is disabled by default.
- Whitelisting and blacklisting cannot be used simultaneously.
- A maximum of 100 domain names can be added to a blacklist or whitelist.
- Domain names added to a blacklist or whitelist are matched using regular expressions. For example, if you add **^http://test.*com$** to a blacklist or whitelist, **http://test.example.com** and **http://test.example01.com** are also matched.

Prerequisites

- **You have added an ingest domain name and a streaming domain name**.
- **CNAME records have been added** to your domains' DNS records.

Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

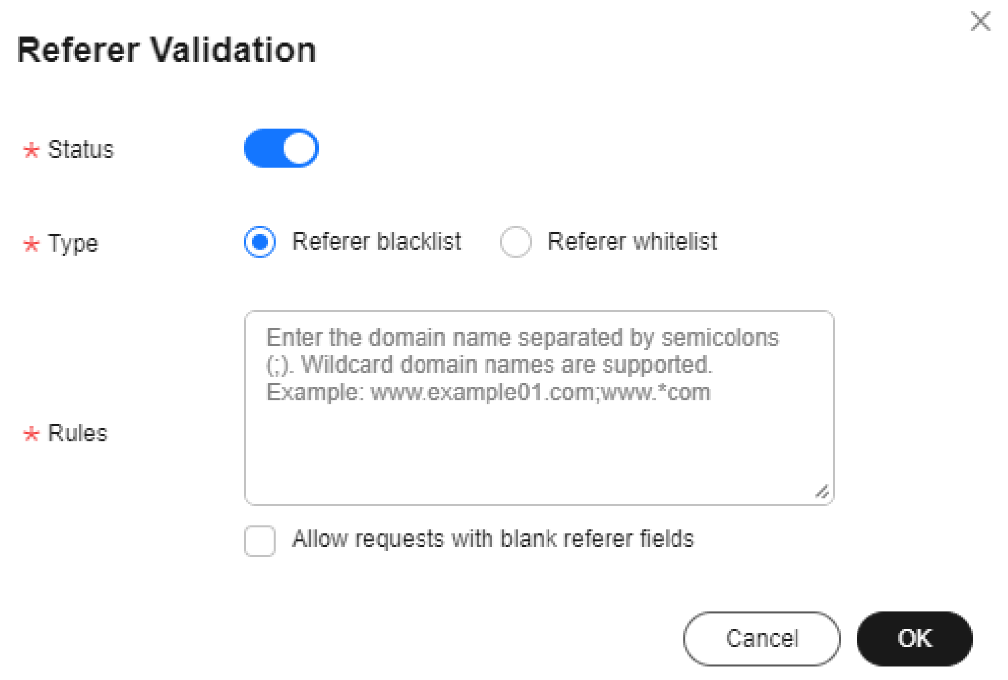
Step 3 Click **Manage** in the **Operation** column of the desired streaming domain name.

Step 4 In the navigation pane, choose **Basic Settings** > **Access Control**.

Step 5 Choose **Referer Validation**. The **Referer Validation** dialog box is displayed.

Step 6 Toggle on the **Status** switch to configure related parameters.

Figure 7-12 Configuring referer validation



Referer Validation

* Status

* Type ● Referer blacklist ○ Referer whitelist

* Rules

Enter the domain name separated by semicolons (;). Wildcard domain names are supported. Example: www.example01.com;www.*com

□ Allow requests with blank referer fields

Table 7-6 describes the parameters.

Table 7-6 Parameter description

Parameter	Description
Type	The blacklist and whitelist are supported. ● **Referer blacklist** allows all domains access to CDN except for the domains added to the blacklist. ● **Referer whitelist** denies all domains access to CDN except for the domains added to the whitelist. You can set whether to allow requests with empty referer fields, that is, whether to allow access through the browser address bar.
Rule	Domain name in the blacklist or whitelist. ● You can input 1 to 100 domain names. Use semicolons (;) to separate domain names. ● Domain names are matched using regular expressions. If **^http://test.*com$** is entered, **http://test.example.com** and **http://test.example01.com** are also matched.

Step 7 Click **OK**.

----End

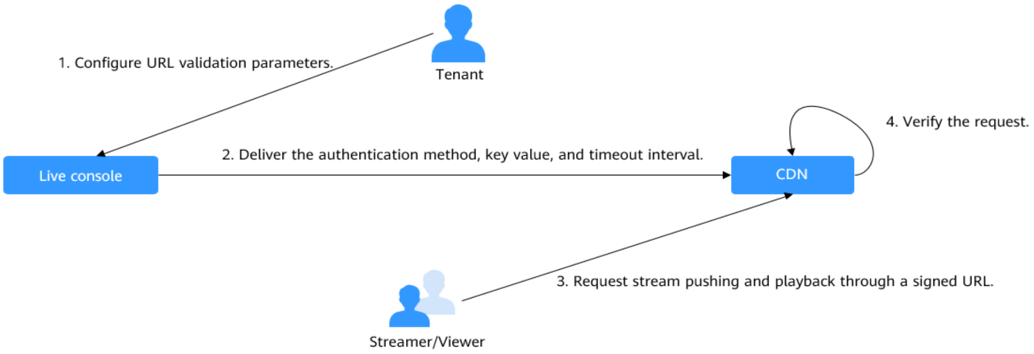
7.4.8.3 URL Validation

To prevent live resources from being stolen, you can configure URL validation to add authentication information to the end of the original ingest or streaming URL. When a streamer starts live streaming or a viewer requests playback, CDN verifies encrypted information in a URL. Only the requests that pass the verification are responded, and other illegitimate requests are rejected.

If you need to customize other validation rules, **submit a service ticket** to contact Huawei Cloud technical support.

Working Principle

Figure 7-13 URL validation working principles


Tenant
1. Configure URL validation parameters.
Live console
2. Deliver the authentication method, key value, and timeout interval.
CDN
4. Verify the request.
3. Request stream pushing and playback through a signed URL.
Streamer/Viewer

The process is as follows:

1. A tenant enables URL validation on the Live console and configures the authentication method, the key, and timeout interval.
2. The Live service delivers the configured authentication method, key value, and timeout interval to a CDN node.
3. The streamer or viewer requests CDN to push streams or play video through a signed ingest/streaming URL.
4. CDN verifies the request based on authentication information carried in the URL. Only requests that pass the verification are allowed.

Notes

- This function is optional and is disabled by default. After this function is enabled, the original URLs cannot be used. New signed URLs must be generated based on rules.
- Use different keys for streaming authentication and playback authentication to enhance security. If a signed URL expires or the signature fails the authentication, the livestream playback will fail and the message **403 Forbidden** will be returned.
- For persistent connection services such as RTMP and FLV, the server verifies the validation parameters only when receiving a user request. Once verified, the content can be played continuously.
- For HLS services, users keep sending requests that contain the same validation parameters after content is played. Once the validation parameters

expire, the server rejects the access request because the verification fails, which will interrupt the playback.

For such services, you need to set a proper authentication expiration time to prevent playback failures. For example, if the estimated HLS playback lasts less than 1 hour each time, you can set the expiration time to 3600 seconds.

Prerequisites

- **You have added an ingest domain name and a streaming domain name**.
- **CNAME records have been added** to your domains' DNS records.

Enabling URL Validation

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the **Operation** column of the desired domain name.

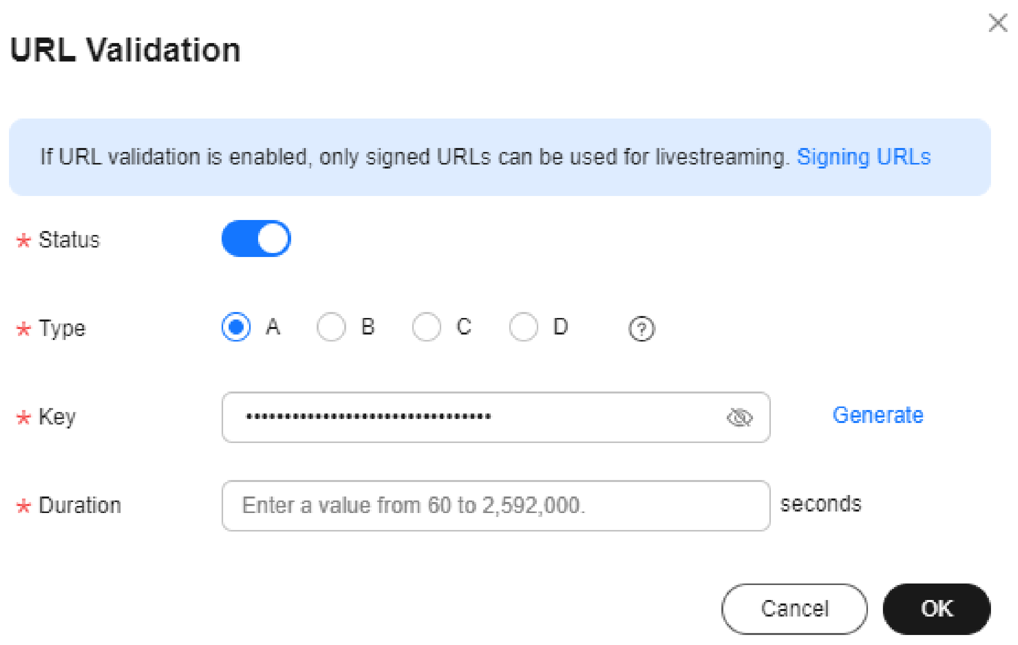
Step 4 In the navigation pane, choose **Basic Settings** > **Access Control**.

Step 5 Choose **URL Validation**.

The **URL Validation** dialog box is displayed.

Step 6 Toggle on the **Status** switch to configure related parameters.

Figure 7-14 Configuring URL validation



URL Validation

If URL validation is enabled, only signed URLs can be used for livestreaming. Signing URLs

* Status: on

* Type: ● A ○ B ○ C ○ D

* Key: •••••••••••••••••••••••••••••••• Generate

* Duration: Enter a value from 60 to 2,592,000. seconds

Table 7-7 URL validation parameters

Parameter	Description
Method	You can use signing method A, B, C, or D to calculate a signed string. Signing methods A and B: The Message Digest algorithm 5 (MD5) is used. For details, see **Signing Method A** and **Signing Method B**. Signing method C: A symmetric encryption algorithm is used. For details, see **Signing Method C**. Signing method D: The HMAC-SHA256 algorithm is used. For details, see **Signing Method D**. **NOTE** Signing methods A, B, and C have security risks. Signing method D is more secure and recommended.
Key	Authentication key. ● You can customize a key. A key consists of 32 characters. Only letters and digits are allowed. ● A key can also be automatically generated.
Duration	Timeout interval of URL authentication information, that is, the maximum difference between the request time carried in authentication information and the time when Live receives the request. This parameter is used to check whether an ingest URL or streaming URL expires. The unit is second. The value ranges from 1 minute to 30 days. **NOTE** ● For persistent connection services such as RTMP and FLV, the server verifies the validation parameters only when receiving a user request. Once verified, the content can be played continuously. ● For HLS services, users keep sending requests that contain the same validation parameters after content is played. Once the validation parameters expire, the server rejects the access request because the verification fails, which will interrupt the playback. For such services, you need to set a proper authentication expiration time to prevent playback failures. For example, if the estimated HLS playback lasts less than 1 hour each time, you can set the expiration time to 3600 seconds.

Step 7 Click **OK**.

Step 8 Obtain a signed URL by:

manually assembling it based on the configured authentication type. For details, see **Signing Method A**, **Signing Method B**, **Signing Method C**, and **Signing Method D**.

Step 9 Verify whether URL validation has taken effect.

Use a third-party livestreaming tool to verify the signed ingest URL and streaming URL. If the original ingest URL and streaming URL cannot be used but the signed ingest URL and stream URL can, URL validation has taken effect.

----End

Signing Method A

A signed string is calculated based on the **Key**, **timestamp**, **rand** (random), **uid** (set to **0**), and URL.

Signed URL format:

```
Original URL?auth_key={timestamp}-{rand}-{uid}-{md5hash}
```

Formula for calculating **md5hash** is:

```
sstring = "{URI}-{Timestamp}-{rand}-{uid}-{Key}"
HashValue = md5sum(sstring)
```

Table 7-8 Authentication fields

Field	Description
timestamp	Start time of a valid request. The value is the total number of seconds that have elapsed since 00:00:00 January 1, 1970. It is a decimal or hexadecimal integer. Example: **1592639100** (June 20, 2020 15:45)
Duration	How long a signed URL remains effective. If the validity period is set to 1,800s, users can access the streaming URL within 1,800s since the time indicated by **timestamp**. Authentication fails and the URL is inaccessible if users access the streaming URL 1800s later. For example, if the access time is 00:00:00 (GMT +08:00) on June 30, 2020, the URL expires at 00:30:00 (GMT+08:00) on June 30, 2020.
rand	Random number. The recommended value is a UUID, which cannot contain hyphens (-). Example: 477b3bbc253f467b8def6711128c7bec
uid	User ID. This parameter is not used now. Set it to **0**.

md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of digits (0 to 9) and lowercase letters.
	`sstring = "{URI}-{Timestamp}-{rand}-{uid}-{Key}"`
	`HashValue = md5sum(sstring)`

URI	Path from the domain name to the end in the original URL Example: /livetest/huawei1.flv
Key	Key value set on the console. For details, see **Enabling URL Validation**.

Signed URL example:

Generating a signed streaming URL is used as an example.

```
Original URL: http://test-play.example.com/livetest/huawei1.flv
timestamp: 1592639100
Validity Period: 1,800s
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
rand: 477b3bbc253f467b8def6711128c7bec
uid: 0
URI: /livetest/huawei1.flv
```

Obtain **md5hash** using the calculation formula.

```
HashValue = md5sum("/livetest/huawei1.flv-1592639100-477b3bbc253f467b8def6711128c7bec-0-
GCTbw44s6MPLh4GqgDpnfuFHgy25Enly") = dd1b5ffa00cf26acec0c169ae1cfabea
```

The signed streaming URL is:

```
http://test-play.example.com/livetest/huawei1.flv?
auth_key=1592639100-477b3bbc253f467b8def6711128c7bec-0-dd1b5ffa00cf26acec0c169ae1cfabea
```

Signing Method B

A signed string is calculated based on the **Key**, **timestamp**, and **StreamName**.

Signed URL format:

```
Original URL?txSecret=md5(Key + StreamName + txTime)&txTime=hex(timestamp)
```

Table 7-9 Authentication fields

Field	Description
txTime	Effective time of a streaming URL. The value is a hexadecimal Unix timestamp. If the value of **txTime** is greater than the requested time, the playback is normal. Otherwise, the playback is rejected. Example: 5eed5888 (that is, 2020.06.20 08:30:00)
Key	Key value set on the console. For details, see **Enabling URL Validation**.
txSecret	Encryption parameter in the URL. The value is obtained by using the MD5 encryption algorithm to encrypt the string consisting of **key**, **StreamName**, and **txTime**. `txSecret = md5 (Key + StreamName + txTime)`
Duration	How long a signed URL remains effective. If **txTime** is set to the current time and the validity period is set to 1,249s, the streaming URL expiration time is the current time plus 1,249s.

Signed URL example:

Generating a signed streaming URL is used as an example.

```
Original URL: http://test-play.example.com/livetest/huawei1.flv
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
```

```
StreamName: huawei1
txTime: 5eed5888
Duration: 1,249s
```

Obtain **txSecret** based on the calculation formula.

```
txSecret = md5(GCTbw44s6MPLh4GqgDpnfuFHgy25Enlyhuawei15eed5888) =
5cdc845362c332a4ec3e09ac5d5571d6
```

The signed streaming URL is:

```
http://test-play.example.com/livetest/huawei1.flv?
txSecret=5cdc845362c332a4ec3e09ac5d5571d6&txTime=5eed5888
```

Signing Method C

A signed string is calculated based on the **Key**, **Timestamp**, **AppName**, **StreamName**, and **CheckLevel**.

Signed URL format:

```
Original URL?auth_info={Encrypted string}.{EncodedIV}
```

The algorithm for generating the authentication fields is as follows. For details about the code example, see **Sample Code**.

- LiveID = <AppName>+"/"+<StreamName>
- Encrypted string = UrlEncode(Base64(AES128(<Key>,"$"+<Timestamp>+"$"+<LiveID>+"$"+<CheckLevel>)))
- EncodedIV = Hex (IV used for encryption)

Table 7-10 describes encryption parameters in the algorithm.

Table 7-10 Encryption parameters

Field	Description
AppName	Application name, which is the same as the value of **AppName** in an ingest or streaming URL
StreamName	Stream name, which is the same as the value of **StreamName** in an ingest or streaming URL
Key	Key value set on the console. For details, see **Enabling URL Validation**.
LiveID	Live stream ID, which uniquely identifies a live stream. The value consists of **AppName** and **StreamName**. `LiveID = <AppName>+"/"+<StreamName>`
Timestamp	UTC time when an authentication parameter is generated, in **yyyyMMddHHmmss** format. This parameter is used to check whether the authentication parameter has expired, that is, whether the absolute value of the difference between **Timestamp** and the current time is greater than the configured timeout interval.

Field	Description
CheckLevel	Check level. The value is **3** or **5**. ● If **CheckLevel** is **3**, the system only checks whether the value of **LiveID** is matched. ● If **CheckLevel** is **5**, the system checks whether the value of **LiveID** is matched and whether **Timestamp** times out.
IV	Cipher block chaining (CBC) depends on the initialization vector (IV). IV consists of 16 random digits and letters and must be 128 bits. In CBC mode, PKCS7 padding is used.

Signed URL example:

Generating a signed streaming URL is used as an example.

```
Original URL: http://test-play.example.com/livetest/huawei1.flv
AppName: livetest
StreamName: huawei1
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
LiveID: livetest/huawei1
Timestamp: 20190428110000
CheckLevel: 3
IV: yCmE666N3YAq30SN
```

The encrypted string and EncodedIV are obtained according to the calculation formula.

```
Encrypted string = I90KW7GhxOMwoy5yaeKMStZsOC %2B6WIyqU2kLBYAvcso %3D
EncodIV = 79436d453636364e335941713330534e
```

The signed streaming URL is:

```
http://test-play.example.com/livetest/huawei1.flv?auth_info=I90KW7GhxOMwoy5yaeKMStZsOC
%2B6WIyqU2kLBYAvcso%3D.79436d453636364e335941713330534e
```

Signing Method D

A signed string is calculated based on the **Key**, **timestamp**, and **StreamName**.

Signed URL format:

```
Original URL?hwSecret=hmac_sha256(Key, StreamName + hwTime)&hwTime=hex(timestamp)
```

Table 7-11 Authentication fields

Field	Description
hwTime	Effective time of a streaming URL. The value is a hexadecimal Unix timestamp. If the value of **hwTime** + ***duration*** is greater than the requested time, the playback is normal. Otherwise, the playback is rejected. Example: 5eed5888 (that is, 2020.06.20 08:30:00)
Key	Key value set on the console. For details, see **Enabling URL Validation**.

Field	Description
hwSecret	Encryption parameter in the URL. The value is obtained using the HMAC-SHA256 algorithm, with *Key* and *StreamName* + *hwTime* as parameters. `hwSecret = hmac_sha256 (Key, StreamName + hwTime)`
Duration	How long a signed URL remains effective. If **hwTime** is set to the current time and the validity period is set to 1,249s, the streaming URL expiration time is the current time plus 1,249s.

Signed URL example:

Generating a signed streaming URL is used as an example.

```
Original URL: http://test-play.example.com/livetest/huawei1.flv
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
StreamName: huawei1
hwTime: 5eed5888
Duration: 1,249s
```

Obtain **hwSecret** based on the calculation formula.

```
hwSecret = hmac_sha256(GCTbw44s6MPLh4GqgDpnfuFHgy25Enly, huawei15eed5888) =
ce201856a0957413319e883c8ccae13602f01d3d91e21daf5161964cf708a6a8
```

The signed streaming URL is:

```
http://test-play.example.com/livetest/huawei1.flv?
hwSecret=ce201856a0957413319e883c8ccae13602f01d3d91e21daf5161964cf708a6a8&hwTime=5eed5888
```

Sample Code

The following is the code example for generating a signed string in method C:

```
import javax.crypto.Cipher;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;

import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;

public class Main {

    public static void main(String[] args) {

    // data="$"+<Timestamp>+"$"+<LiveID>+"$"+<CheckLevel>. For details, see "Signing Method C."
        String data = "$20190428110000$live/stream01$3";

        // A random 16-digit string consisting of digits and letters
    byte[] ivBytes = "yCmE666N3YAq30SN".getBytes();

        // Key value configured on the Live console
    byte[] key = "GCTbw44s6MPLh4GqgDpnfuFHgy25Enly".getBytes();

        String msg = aesCbcEncrypt(data, ivBytes, key);
    try {
      System.out.println(URLEncoder.encode(msg, "UTF-8") + "." + bytesToHexString(ivBytes));
    } catch (UnsupportedEncodingException e) {
      e.printStackTrace();
    }
    }

        private static String aesCbcEncrypt(String data, byte[] ivBytes, byte[] key) {
        try {
            SecretKeySpec sk = new SecretKeySpec(key, "AES");
            Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");

                        if (ivBytes != null) {
                cipher.init(Cipher.ENCRYPT_MODE, sk, new IvParameterSpec(ivBytes));
            } else {
                cipher.init(Cipher.ENCRYPT_MODE, sk);
            }

                        return Base64.encode(cipher.doFinal(data.getBytes("UTF-8")));
        } catch (Exception e) {
            return null;
        }
    }

        public static String bytesToHexString(byte[] src) {
        StringBuilder stringBuilder = new StringBuilder("");
        if ((src == null) || (src.length <= 0)) {
            return null;
        }

                for (int i = 0; i < src.length; i++) {
            int v = src[i] & 0xFF;
            String hv = Integer.toHexString(v);
            if (hv.length() < 2) {
                stringBuilder.append(0);
            }
            stringBuilder.append(hv);
        }
        return stringBuilder.toString();
    }
}
```

Base64 is used to encode encrypted strings.

```
public class Base64
{

    / ** Base64 encoding table */
    private static char base64Code[] =
    {
        'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R',
        'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j',
        'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1',
        '2', '3', '4', '5', '6', '7', '8', '9', '+', '/',};

    /**
     * The construction method is privatized to prevent instantiation.
     */
    private Base64()
    {
        super();
    }

    /**
     * Encode three bytes in a byte array into four visible characters.
     * @param bytes Byte data to be encoded
     * @return Base64 character string after encoding
     */
    public static String encode(byte[] bytes)
    {
        int a = 0;

        // Allocate memory based on the actual length after encoding for acceleration.
        StringBuffer buffer = new StringBuffer(((bytes.length - 1) / 3) << 2 + 4);
        // Encoding
        for (int i = 0; i < bytes.length; i++)
        {
            a |= (bytes[i] << (16 - i % 3 * 8)) & (0xff << (16 - i % 3 * 8));
            if (i % 3 == 2 || i == bytes.length - 1)
            {
                buffer.append(Base64.base64Code[(a & 0xfc0000) >>> 18]);
                buffer.append(Base64.base64Code[(a & 0x3f000) >>> 12]);
                buffer.append(Base64.base64Code[(a & 0xfc0) >>> 6]);
                buffer.append(Base64.base64Code[a & 0x3f]);
                a = 0;
            }
        }

        // For a byte array whose length is not an integral multiple of 3, add 0 before encoding and replace it with = after encoding.
        // The number of equal signs (=) is the same as the length of the missing data to identify the actual data length.
        if (bytes.length % 3 > 0)
        {
            buffer.setCharAt(buffer.length() - 1, '=');
        }
        if (bytes.length % 3 == 1)
        {
            buffer.setCharAt(buffer.length() - 2, '=');
        }
        return buffer.toString();
    }

}
```

7.4.8.4 ACL

You can add the IP addresses that are allowed or not allowed to play content to the whitelist or blacklist. CDN allows or rejects the playback requests based on the whitelist or blacklist.

Notes

- This function is optional and is disabled by default.
- Whitelists and blacklists cannot be used simultaneously.
- A maximum of 100 IP addresses can be added to a whitelist or blacklist.

Prerequisites

- **You have added an ingest domain name and a streaming domain name**.
- **CNAME records have been added** to your domains' DNS records.

Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the **Operation** column of the desired streaming domain name.

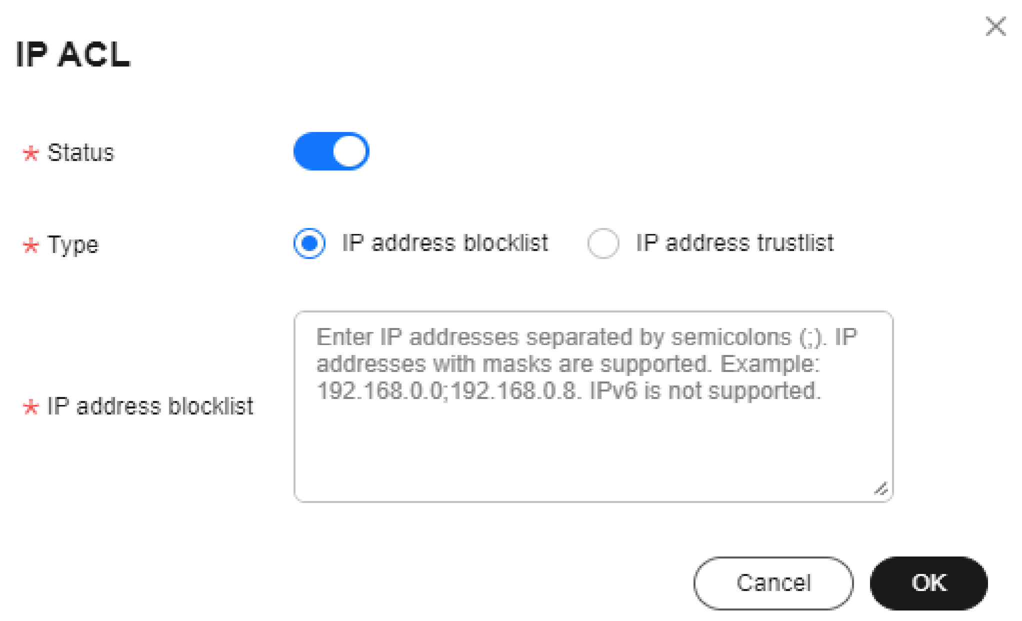
Set **Subservice Type** of the domain name to **Media Live**.

Step 4 In the navigation pane, choose **Basic Settings** > **Access Control**.

Step 5 Click **IP ACL**. The **IP ACL** dialog box is displayed.

Step 6 Toggle on the **Status** switch to configure related parameters.

Figure 7-15 Configuring an ACL



IP ACL

* Status

* Type ● IP address blocklist ○ IP address trustlist

* IP address blocklist Enter IP addresses separated by semicolons (;). IP addresses with masks are supported. Example: 192.168.0.0;192.168.0.8. IPv6 is not supported.

Step 7 Select **IP address blacklist** or **IP address whitelist**, and enter an IP address or IP address range. IPv6 is not supported.

Step 8 Click **OK**.

----End

7.4.9 HTTPS Certificates

7.4.9.1 Configuration Methods

You can configure HTTPS secure acceleration to protect your Media Live resources.

Context

Force HTTPS: If a user initiates an HTTP request, the server returns a 302 status code, and the user is redirected to HTTPS.

HTTPS has the following advantages over HTTP:

- HTTPS is a network protocol constructed based on SSL and HTTP for encrypted transmission and identity authentication. It is more secure than HTTP and prevents data from being stolen or changed during transmission, ensuring data integrity.
- Key user information is encrypted to prevent session IDs or cookies from being captured by attackers.

Prerequisites

- You have created a channel, as shown in **Creating a Channel**.
- **CNAME records have been added** to your domains' DNS records.
- The HTTPS certificate has been prepared. If no HTTPS certificate is available, buy one in **Cloud Certificate Manager (CCM)**.
- The HTTPS certificate format must meet the **requirements**. If your certificate is not in PEM format, **convert the certificate** to the PEM format.

Enabling HTTPS

Step 1 Log in to the **Live console**.

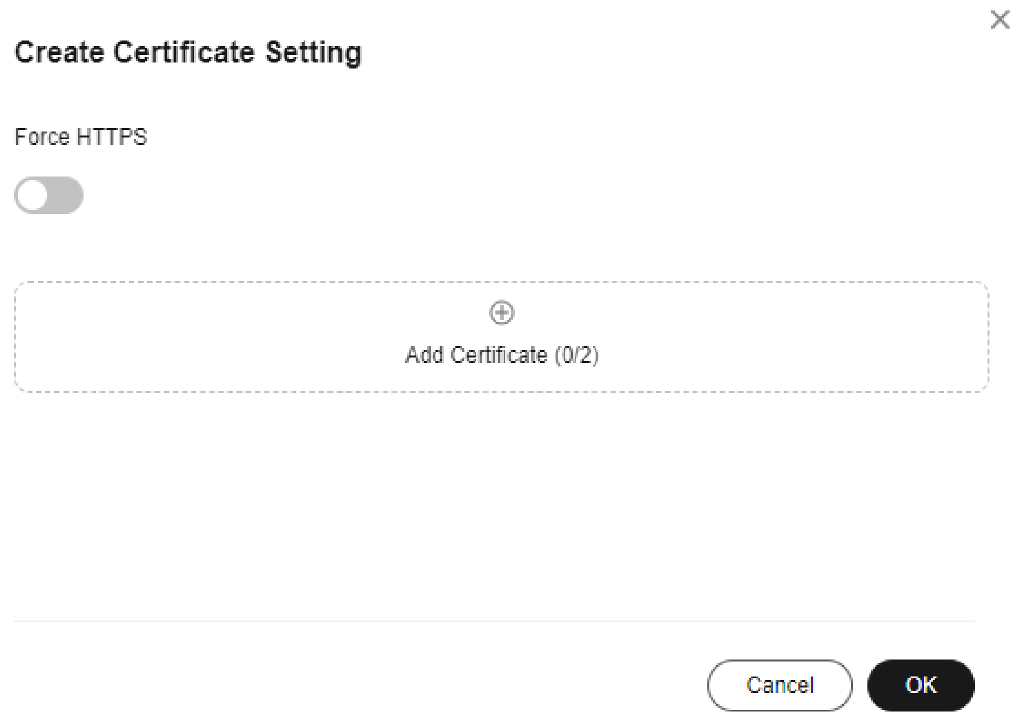
Step 2 In the navigation pane, choose **Domains**.

Step 3 Find the streaming domain name whose **Subservice Type** is **Media Live** and for which HTTPS secure acceleration needs to be configured. Then click **Manage**.

Step 4 In the navigation pane, choose **Templates** > **HTTPS Certificates**.

Step 5 Click **Create**. The **Create Certificate Setting** page is displayed, as shown in **Figure 7-16**.

Figure 7-16 Creating a certificate setting



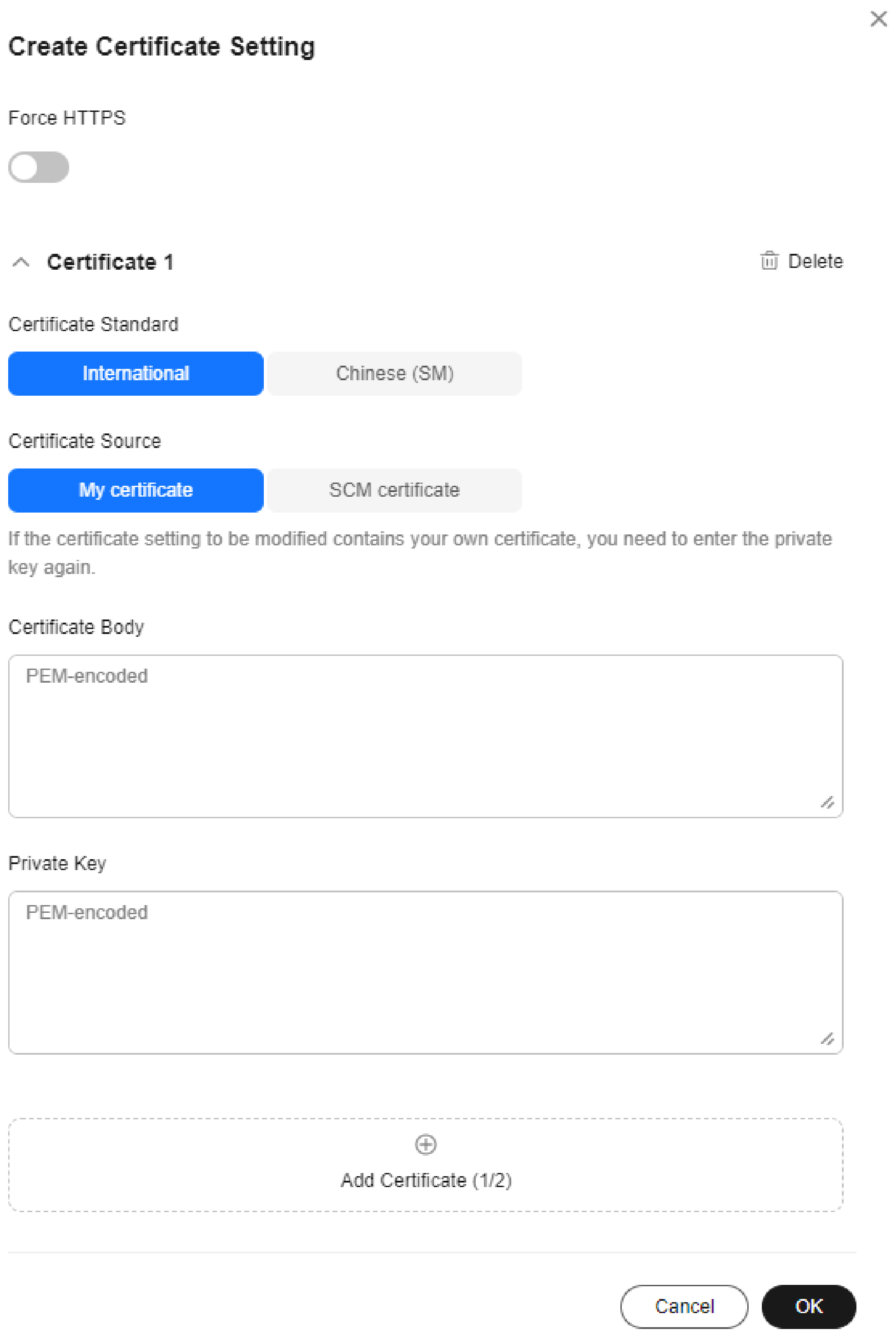
Step 6 Click **Add Certificate**. The settings of certificate 1 are displayed, as shown in **Figure 7-17**.

See **Table 7-12**. You can add a certificate only when:

- there is only one international standard certificate

- there is only one Chinese (SM) certificate
- there is one international standard certificate and one Chinese (SM) certificate.

Figure 7-17 Configuring a certificate



Create Certificate Setting

Force HTTPS

Certificate 1

Certificate Standard: International (selected) / Chinese (SM)

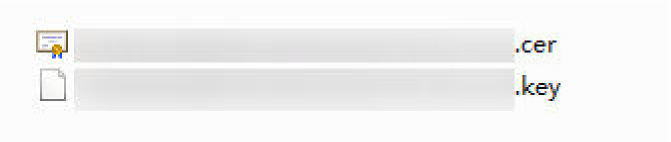
Certificate Source: My certificate (selected) / SCM certificate

If the certificate setting to be modified contains your own certificate, you need to enter the private key again.

Certificate Body: PEM-encoded

Private Key: PEM-encoded

Table 7-12 Parameters

Parameter	Description
Certificate Standard	Standard of the HTTPS certificate. Options: – **International** – **Chinese (SM)**
Certificate Source	Source of the HTTPS certificate. Options: – **My certificate**: a certificate obtained from a compliant channel – **SCM certificate**: a certificate purchased from Huawei Cloud SCM
International > **My certificate**	Open the obtained certificate file and private key file using a text tool, and copy certificate body and private key content to the corresponding text boxes. Certificates issued by different organizations have the following differences: – If your certificate is issued by the root CA, the certificate is a complete certificate. Copy the certificate content. **Figure 7-18** HTTPS certificate  – If your certificate is issued by an intermediate CA, the certificate file contains multiple certificates. You need to combine all the certificates into a single certificate. For details, see **Certificates Issued by Intermediate CAs**.
Chinese (SM) > **My certificate**	
International > **SCM certificate**	Click **Create SCM Certificate** on the right of **Certificate Name** to go to the SCM console and purchase a certificate as prompted. After the certificate is issued, it will be automatically displayed in the **Certificate Name** drop-down list box.
Chinese (SM) > **SCM certificate**	

Step 7 Select whether to enable **Force HTTPS**.

Enabling this function will convert all requests for your website to HTTPS requests.

Step 8 Click **OK**.

Step 9 Verify whether HTTPS secure acceleration has taken effect.

Use an HTTPS streaming URL to play a Media Live video. If the playback is successful, HTTPS secure acceleration has taken effect.

----End

Updating a Certificate

If your certificate is changed, you need to synchronize new certificate content to the HTTPS settings. The procedure to update a certificate is the same as that to **enable HTTPS**.

For **My certificate**, the **Private Key** text box is empty by default to ensure the security and confidentiality of the private key content. You need to enter the content again and submit it.

7.4.9.2 HTTPS Certificate Requirements

The HTTPS configuration only supports certificates or private keys in PEM format. The certificate/private key upload requirements vary depending on certificate issuing agencies.

Certificates Issued by Root CA

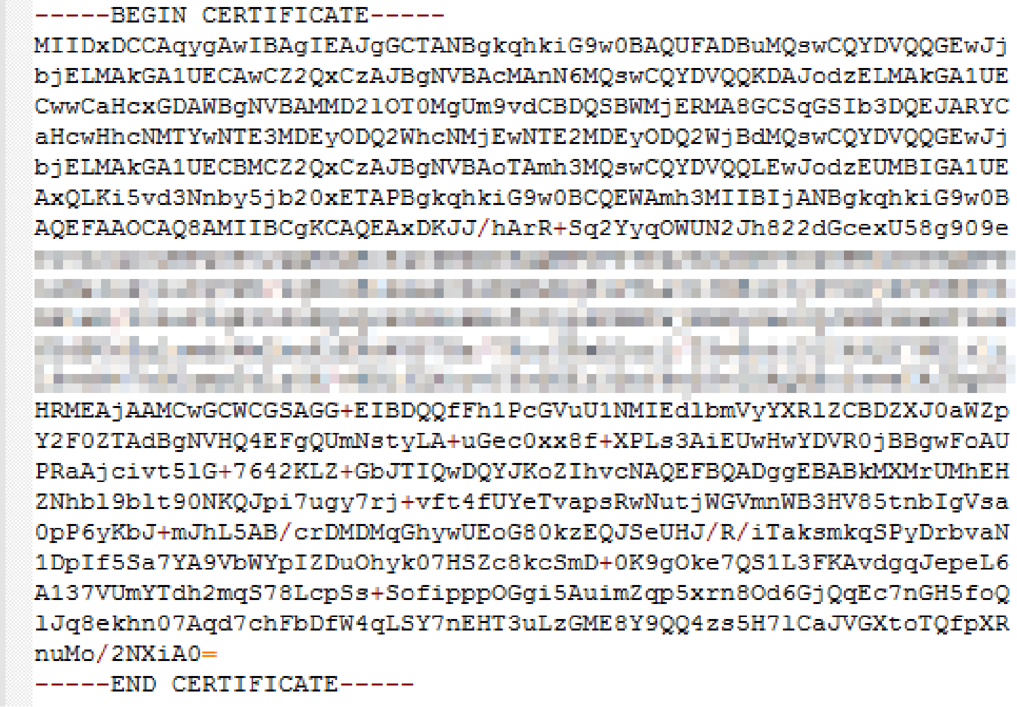
A Certificate issued by Root CA is a complete certificate. You only need to upload the certificate when configuring HTTPS.

Use the text program to open the certificate in the **PEM** format, then you can view the certificate content, as shown in **Figure 7-19**.

A certificate in **PEM** format

- The certificate starts with the **-----BEGIN CERTIFICATE-----** chain and ends with the **-----END CERTIFICATE-----** chain.
- Each line of the certificate content contains 64 characters, but the number of characters in the last line can be smaller than 64.
- No space is allowed in the certificate content.

Figure 7-19 A certificate in **PEM** format



```
-----BEGIN CERTIFICATE-----
MIIDxDCCAqygAwIBAgIEAJgGCTANBgkqhkiG9w0BAQUFADBuMQswCQYDVQQGEwJj
bjELMAkGA1UECAwCZ2QxCzAJBgNVBAcMAnN6MQswCQYDVQQKDAJodzELMAkGA1UE
CwwCaHcxGDAWBgNVBAMMD2lOT0MgUm9vdCBDQSBWMjERMA8GCSqGSIb3DQEJARYC
aHcwHhcNMTYwNTE3MDEyODQ2WhcNMjEwNTE2MDEyODQ2WjBdMQswCQYDVQQGEwJj
bjELMAkGA1UECBMCZ2QxCzAJBgNVBAoTAmh3MQswCQYDVQQLEwJodzEUMBIGA1UE
AxQLKi5vd3Nnby5jb20xETAPBgkqhkiG9w0BCQEWAmh3MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909e
[redacted]
HRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZp
Y2F0ZTAdBgNVHQ4EFgQUmNstyLA+uGec0xx8f+XPLs3AiEUwHwYDVR0jBBgwFoAU
PRaAjcivt5lG+7642KLZ+GbJTIQwDQYJKoZIhvcNAQEFBQADggEBABkMXMrUMhEH
ZNhbl9blt90NKQJpi7ugy7rj+vft4fUYeTvapsRwNutjWGVmnWB3HV85tnbIgVsa
0pP6yKbJ+mJhL5AB/crDMDMqGhywUEoG80kzEQJSeUHJ/R/iTaksmkqSPyDrbvaN
1DpIf5Sa7YA9VbWYpIZDuOhyk07HSZc8kcSmD+0K9gOke7QS1L3FKAvdgqJepeL6
A137VUmYTdh2mqS78LcpSs+SofipppOGgi5AuimZqp5xrn8Od6GjQqEc7nGH5foQ
lJq8ekhn07Aqd7chFbDfW4qLSY7nEHT3uLzGME8Y9QQ4zs5H7lCaJVGXtoTQfpXR
nuMo/2NXiA0=
-----END CERTIFICATE-----
```

Certificates Issued by Intermediate CAs

The certificate file issued by an intermediate agency contains several certificates. You need to combine the certificates into an integral one, and upload it when configuring HTTPS security acceleration. A combined certificate is shown as **Figure 7-20**.

Use the text program to open all the certificates in the **PEM** format. Put the server certificate on the top and then the intermediate certificate. Generally, an instruction will be issued together with the certificate. Be aware of the rules in the instruction. The general rules are as follows:

- There are no lines between certificates.
- The formats of certificate chains are as follows:

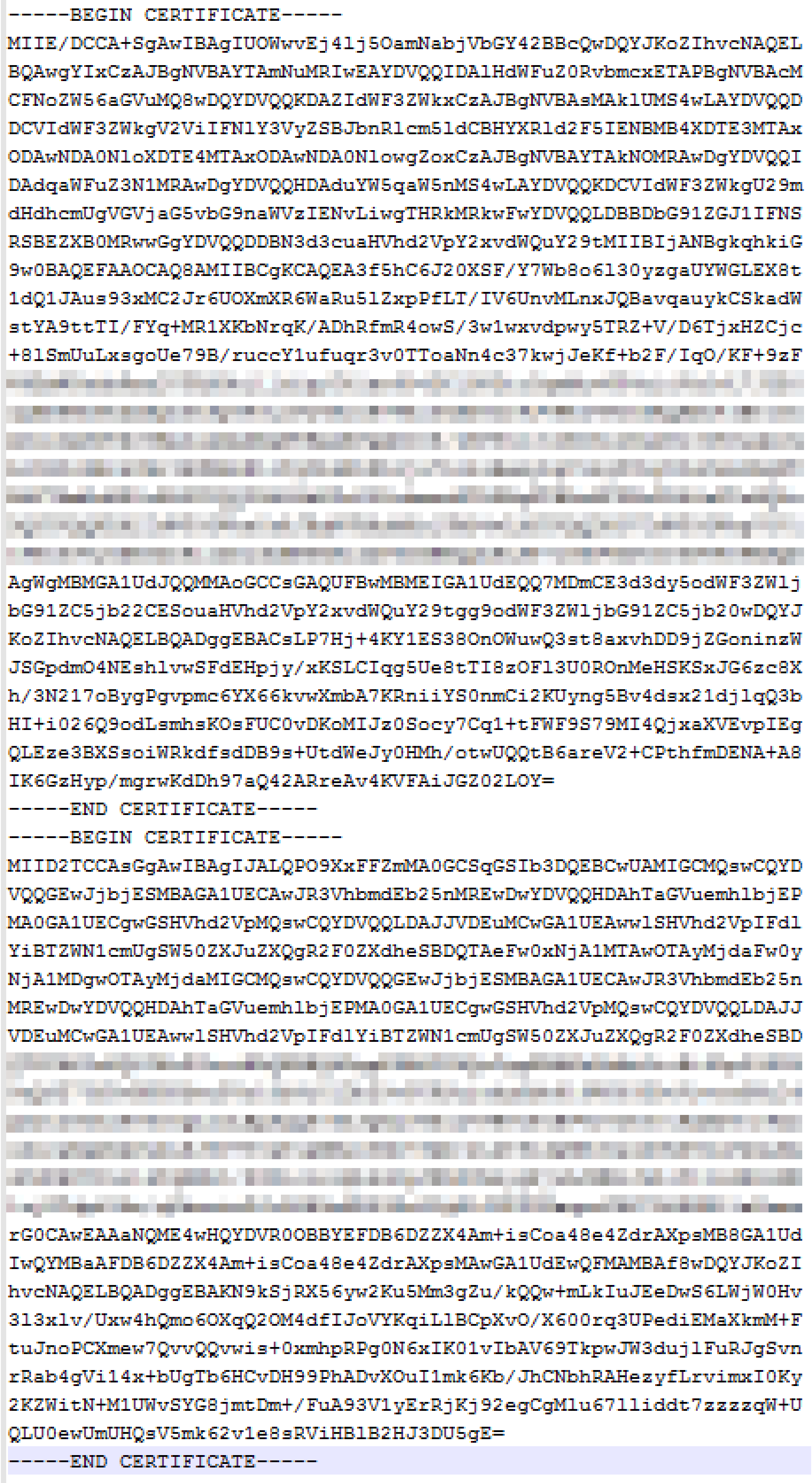
  -----BEGIN CERTIFICATE-----

  -----END CERTIFICATE-----

  -----BEGIN CERTIFICATE-----

  -----END CERTIFICATE-----

Figure 7-20 A combined certificate



```
-----BEGIN CERTIFICATE-----
MIIE/DCCA+SgAwIBAgIUOWwvEj41j5OamNabjVbGY42BBcQwDQYJKoZIhvcNAQEL
BQAwgYIxCzAJBgNVBAYTAmNuMRIwEAYDVQQIDAlHdWFuZ0RvbmcxETAPBgNVBAcM
CFNoZW56aGVuMQ8wDQYDVQQKDAZIdWF3ZWkxCzAJBgNVBAsMAklUMS4wLAYDVQQD
DCVIdWF3ZWkgV2ViIFNlY3VyZSBJbnRlcm5ldCBHYXRld2F5IENBMB4XDTE3MTAx
ODAwNDA0NloXDTE4MTAxODAwNDA0NlowgZoxCzAJBgNVBAYTAkNOMRAwDgYDVQQI
DAdqaWFuZ3N1MRAwDgYDVQQHDAduYW5qaW5nMS4wLAYDVQQKDCVIdWF3ZWkgU29m
dHdhcmUgVGVjaG5vbG9naWVzIENvLiwgTHRkMRkwFwYDVQQLDBBDbG91ZGJ1IFNS
RSBEZXB0MRwwGgYDVQQDDBN3d3cuaHVhd2VpY2xvdWQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3f5hC6J20XSF/Y7Wb8o6l30yzgaUYWGLEX8t
1dQ1JAus93xMC2Jr6UOXmXR6WaRu5lZxpPfLT/IV6UnvMLnxJQBavqauykCSkadW
stYA9ttTI/FYq+MR1XKbNrqK/ADhRfmR4owS/3w1wxvdpwy5TRZ+V/D6TjxHZCjc
+8lSmUuLxsgoUe79B/ruccY1ufuqr3v0TToaNn4c37kwjJeKf+b2F/IqO/KF+9zF
[redacted]
AgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMEIGA1UdEQQ7MDmCE3d3dy5odWF3ZW1j
bG91ZC5jb22CESouaHVhd2VpY2xvdWQuY29tgg9odWF3ZW1jbG91ZC5jb20wDQYJ
KoZIhvcNAQELBQADggEBACsLP7Hj+4KY1ES38OnOWuwQ3st8axvhDD9jZGoninzW
JSGpdmO4NEshlvwSFdEHpjy/xKSLCIqg5Ue8tTI8zOFl3U0ROnMeHSKSxJG6zc8X
h/3N217oBygPgvpmc6YX66kvwXmbA7KRniiYS0nmCi2KUyng5Bv4dsx21djlqQ3b
HI+i026Q9odLsmhsKOsFUC0vDKoMIJz0Socy7Cq1+tFWF9S79MI4QjxaXVEvpIEg
QLEze3BXSsoiWRkdfsdDB9s+UtdWeJy0HMh/otwUQQtB6areV2+CPthfmDENA+A8
IK6GzHyp/mgrwKdDh97aQ42ARreAv4KVFAiJGZ02LOY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID2TCCAsGgAwIBAgIJALQPO9XxFFZmMA0GCSqGSIb3DQEBCwUAMIGCMQswCQYD
VQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25nMREwDwYDVQQHDAhTaGVuemhlbjEP
MA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAJJVDEuMCwGA1UEAwwlSHVhd2VpIFdl
YiBTZWN1cmUgSW50ZXJuZXQgR2F0ZXdheSBDQTAeFw0xNjA1MTAwOTAyMjdaFw0y
NjA1MDgwOTAyMjdaMIGCMQswCQYDVQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25n
MREwDwYDVQQHDAhTaGVuemhlbjEPMA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAJJ
VDEuMCwGA1UEAwwlSHVhd2VpIFdlYiBTZWN1cmUgSW50ZXJuZXQgR2F0ZXdheSBD
[redacted]
rG0CAwEAAaNQME4wHQYDVR0OBBYEFDB6DZZX4Am+isCoa48e4ZdrAXpsMB8GA1Ud
IwQYMBaAFDB6DZZX4Am+isCoa48e4ZdrAXpsMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAKN9kSjRX56yw2Ku5Mm3gZu/kQQw+mLkIuJEeDwS6LWjW0Hv
3l3xlv/Uxw4hQmo6OXqQ2OM4dfIJoVYKqiLlBCpXvO/X600rq3UPediEMaXkmM+F
tuJnoPCXmew7QvvQQvwis+0xmhpRPg0N6xIK01vIbAV69TkpwJW3dujlFuRJgSvn
rRab4gVil4x+bUgTb6HCvDH99PhADvXOuI1mk6Kb/JhCNbhRAHezyfLrvimxI0Ky
2KZWitN+M1UWvSYG8jmtDm+/FuA93V1yErRjKj92egCgMlu67lliddt7zzzzqW+U
QLU0ewUmUHQsV5mk62v1e8sRViHBlB2HJ3DU5gE=
-----END CERTIFICATE-----
```

RSA Private Key

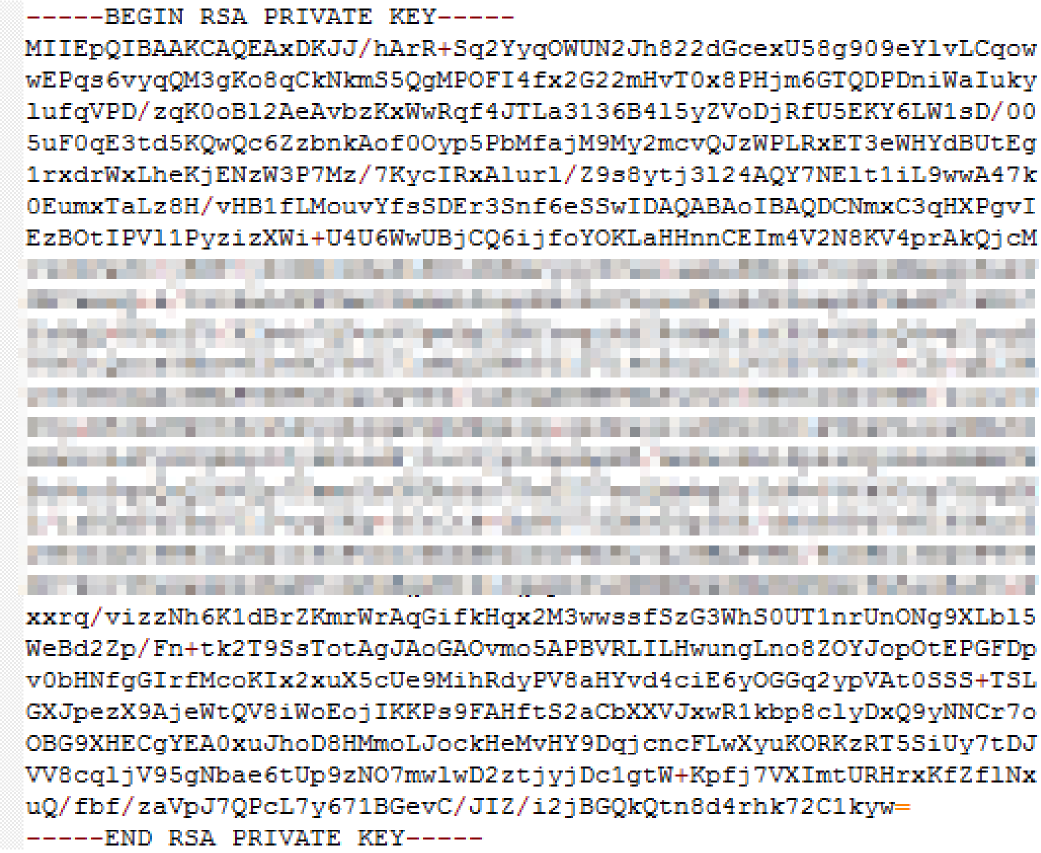
PEM files can contain certificates or private keys. If a PEM file contains only private keys, the file suffix may be replaced by KEY.

Use the text program to open the private key file in the PEM or KEY format, then you can view the private key content, as shown in Figure 7-21.

Content of an RSA private key:

- The private key starts with the **-----BEGIN RSA PRIVATE KEY-----** chain and ends with the **-----END RSA PRIVATE KEY-----** chain.
- Each line of the private key content contains 64 characters, but the number of characters in the last line can be smaller than 64.
- No space is allowed in the private key content.

Figure 7-21 An RSA private key



```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909eYlvLCqow
wEPqs6vyqQM3gKo8qCkNkmS5QgMPOFI4fx2G22mHvT0x8PHjm6GTQDPDniWaIuky
lufqVPD/zqK0oBl2AeAvbzKxWwRqf4JTLa3136B415yZVoDjRfU5EKY6LW1sD/00
5uF0qE3td5KQwQc6ZzbnkAof0Oyp5PbMfajM9My2mcvQJzWPLRxET3eWHYdBUtEg
1rxdrWxLheKjENzW3P7Mz/7KycIRxAlurl/Z9s8ytj3124AQY7NElt1iL9wwA47k
0EumxTaLz8H/vHB1fLMouvYfsSDEr3Snf6eSSwIDAQABAoIBAQDCNmxC3qHXPgvI
EzBOtIPVl1PyzizXWi+U4U6WwUBjCQ6ijfoYOKLaHHnnCEIm4V2N8KV4prAkQjcM
[redacted]
xxrq/vizzNh6K1dBrZKmrWrAqGifkHqx2M3wwssfSzG3WhS0UT1nrUnONg9XLbl5
WeBd2Zp/Fn+tk2T9SsTotAgJAoGAOvmo5APBVRLILHwungLno8ZOYJopOtEPGFDp
v0bHNfgGIrfMcoKIx2xuX5cUe9MihRdyPV8aHYvd4ciE6yOGGq2ypVAt0SSS+TSL
GXJpezX9AjeWtQV8iWoEojIKKPs9FAHftS2aCbXXVJxwR1kbp8clyDxQ9yNNCr7o
OBG9XHECgYEA0xuJhoD8HMmoLJockHeMvHY9DqjcncFLwXyuKORKzRT5SiUy7tDJ
VV8cqljV95gNbae6tUp9zNO7mwlwD2ztjyjDc1gtW+Kpfj7VXImtURHrxKfZflNx
uQ/fbf/zaVpJ7QPcL7y671BGevC/JIZ/i2jBGQkQtn8d4rhk72C1kyw=
-----END RSA PRIVATE KEY-----
```

If the certificate chain of a private key file contains the following information: **-----BEGIN PRIVATE KEY-----** and **-----END PRIVATE KEY-----**, or **-----BEGIN ENCRYPTED PRIVATE KEY-----** and **-----END ENCRYPTED PRIVATE KEY-----**, you need to use the OpenSSL tool to run the following command to convert the format.

```
openssl rsa -in old_key.pem -out new_key.pem
```

Format Conversion

The HTTPS configuration only supports certificates or private keys in **PEM** format. It is recommended that **OpenSSL** be used to convert certificates in other formats into the **PEM** format. The following examples illustrate some popular converting methods.

In the following examples, the name of certificates before conversion is **old_certificate** by default, and that of private keys before transformation is **old_key** by default. The new certificate and private key names are **new_certificate** and **new_key** respectively.

- **Converting DER to PEM**
  ```
  openssl x509 -inform der -in old_certificate.cer -out new_certificate.pem
  openssl rsa -inform DER -outform pem -in old_key.der -out new_key.pem
  ```
- **Converting P7B to PEM**
  ```
  openssl pkcs7 -print_certs -in old_certificate.p7b -out new_certificate.cer
  ```
- **Converting PFX to PEM**
  ```
  openssl pkcs12 -in old_certificat.pfx -nokeys -out new_certificate.pem
  openssl pkcs12 -in old_certificat.pfx -nocerts -out new_key.pem
  ```

To convert a PKCS8 private key to a PKCS1 one, run the following command:

```
openssl rsa -in old_certificat.pem -out pkcs1.pem
```

7.5 Channels

7.5.1 Creating a Channel

Video can be played on Media Live only after a channel is created.

Prerequisites

- **An ingest domain name has been added**.
- A live transcoding template has been created, as shown in **Creating a Transcoding Template**.
- If DRM encryption needs to be enabled for a channel and **Interconnection Mode** is set to **FunctionGraph proxy access** to provide the key for interconnecting with DRM, you need to:
  - enable **FunctionGraph agency** in advance by referring to **Cloud Resource Authorization**
  - **build a function** in FunctionGraph.

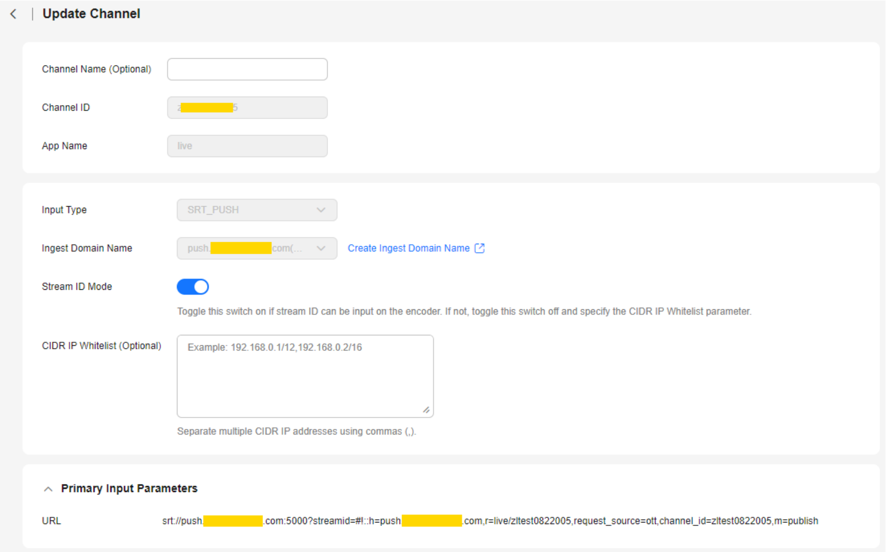
Notes

- A tenant can create a maximum of 500 channels. To create more channels, **submit a service ticket**.
- All channels support only single-bitrate inputs, and multi-bitrate outputs are available only after transcoding.
- **RTMP_PUSH** channels require RTMP ingest domain names. **SRT_PUSH** channels require SRT ingest domain names.

  SRT_PUSH channels and **RTMP_PUSH** channels cannot be created at the same time for one domain name.

- To ensure reliability, channels of the **SRT_PUSH** input type must be able to:
  - Support primary and standby URLs. The encoder needs to push streams to both the primary and standby URLs.
    - If the encoder supports *streamid*, only one input URL is returned by default, as shown in **Figure 7-22**.

Figure 7-22 Channel details



Update Channel

Channel Name (Optional)

Channel ID: z[redacted]5

App Name: live

Input Type: SRT_PUSH

Ingest Domain Name: push[redacted]com(...

Stream ID Mode: ●

Toggle this switch on if stream ID can be input on the encoder. If not, toggle this switch off and specify the CIDR IP Whitelist parameter.

CIDR IP Whitelist (Optional): Example: 192.168.0.1/12,192.168.0.2/16

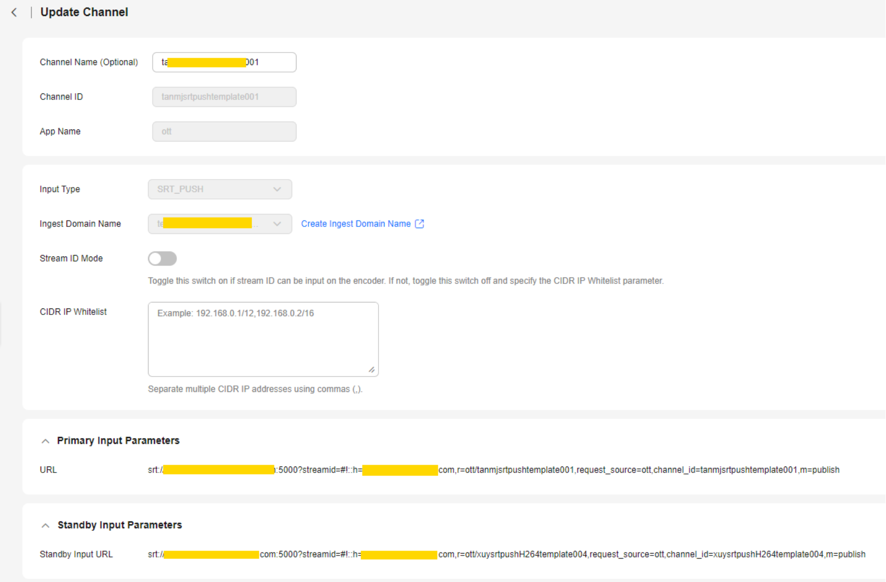
Separate multiple CIDR IP addresses using commas (,).

Primary Input Parameters

URL: srt://push[redacted].com:5000?streamid=#!::h=push[redacted].com,r=live/zltest0822005,request_source=ott,channel_id=zltest0822005,m=publish

    - If the encoder does not support *streamid*, both the primary and standby input URLs are returned, as shown in **Figure 7-23**.

Figure 7-23 Channel details



Update Channel

Channel Name (Optional): ta[redacted]001

Channel ID: tanmjsrtpushtemplate001

App Name: ott

Input Type: SRT_PUSH

Ingest Domain Name: te[redacted]...

Stream ID Mode: ○

Toggle this switch on if stream ID can be input on the encoder. If not, toggle this switch off and specify the CIDR IP Whitelist parameter.

CIDR IP Whitelist: Example: 192.168.0.1/12,192.168.0.2/16

Separate multiple CIDR IP addresses using commas (,).

Primary Input Parameters

URL: srt:/[redacted]:5000?streamid=#!::h=[redacted]com,r=ott/tanmjsrtpushtemplate001,request_source=ott,channel_id=tanmjsrtpushtemplate001,m=publish

Standby Input Parameters

Standby Input URL: srt:/[redacted]com:5000?streamid=#!::h=[redacted]com,r=ott/xuysrtpushH264template004,request_source=ott,channel_id=xuysrtpushH264template004,m=publish

  - Resume stream push when the stream push by the encoder is interrupted. The recommended interval for resuming stream push is shorter than the duration of one segment.
- When FunctionGraph is used for channel DRM encryption, the FunctionGraph version information is not contained. By default, the latest version is used.

- If the DRM system is faulty, 404 is returned.

Creating a Channel

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane on the left, choose **Channels** under **Media Live**.

Step 3 Click **Create Channel**. The **Create Channel** page is displayed.

Configure **Basic Info** as follows:

- **Channel Name**: Enter a channel name.
- **Channel ID**: Enter a channel ID.
- **App Name**: Application name, which defaults to **live** and cannot be changed.

Step 4 Click **Next**.

Configure parameters for adding inputs following **Table 7-13**.

Table 7-13 Parameters

Parameter	Description
Input Type	Input type of a channel media asset. Options: ● **FLV_PULL**: Stream push is not required. The streaming URL provided by the user is directly obtained and used by Media Live to push streams to the origin server. The streaming URL supports only HTTP. ● **RTMP_PUSH**: An RTMP ingest domain name needs to be configured for stream push. ● **HLS_PULL**: Stream push is not required. The streaming URL provided by the user is directly obtained and used by Media Live to push streams to the origin server. If **Input Type** is set to **HLS_PULL**, the media URLs provided users have the following constraints: – A streaming URL supports only HTTP and HTTPS. – Encrypted streams are not supported. – Audio-only streams are not supported. – Subtitling is not supported. ● **SRT_PULL**: Stream push is not required. The streaming URL provided by the user is directly obtained and used by Media Live to push streams to the origin server. ● **SRT_PUSH**: An SRT ingest domain name needs to be configured for stream push. To ensure reliability, channels of the **SRT_PUSH** input type must be able to: – Support primary and standby URLs. The encoder needs to push streams to both the primary and standby URLs. – Resume stream push when the stream push by the encoder is interrupted. The recommended interval for resuming stream push is shorter than the duration of a segment.

Parameter	Description
Input Type set to FLV_PULL	Configure the following parameters: ● **Primary Input Parameters**: **URL**, indicating the media stream URL obtained from the channel provider. Media Live directly uses the URL to push streams to the origin server. ● **Standby Input Parameters**: – **Primary/standby Input**: You can enable this function to set the standby media stream URL. – **Standby Input URL**: Obtain the standby media stream URL from the channel provider. – **Switchover Duration Threshold**: When the duration of abnormal channel playback reaches the threshold, the system automatically switches to another URL for stream pull and playback. – **Priority Settings**: Select **PRIMARY** (mainly the primary input URL) or **EQUAL** (switchover between primary and standby input URLs) as needed.
Input Type set to RTMP_PUSH	Configure the following parameters: **Ingest Domain Name**: Select an RTMP ingest domain name from the drop-down list box. If no ingest domain name is available, click **Create Ingest Domain Name** on the right and add an RTMP ingest domain name on the **Add Domain** page.

Parameter	Description
Input Type set to HLS_PULL	Configure the following parameters: ● **Max Bandwidth (Optional)**: A streaming URL provided by a user contains the parameter **BANDWIDTH** for media files of different bitrates. – If **Max Bandwidth** is specified and Media Live pulls a stream using the URL, the media file stream with the highest bitrate and bandwidth lower than the value of **Max Bandwidth** will be pushed to the origin server. – If **Max Bandwidth** is not specified and Media Live pulls a stream using the URL, the media file stream with the largest **BANDWIDTH** value will be pushed to the origin server. ● **Primary Input Parameters**: **URL**, indicating the media stream URL obtained from the channel provider. Media Live directly uses the URL to push streams to the origin server. ● **Standby Input Parameters**: – **Primary/standby Input**: You can enable this function to set the standby media stream URL. – **Standby Input URL**: Obtain the standby media stream URL from the channel provider. – **Switchover Duration Threshold**: When the duration of abnormal channel playback reaches the threshold, the system automatically switches to another URL for stream pull and playback. – **Priority Settings**: Select **PRIMARY** (mainly the primary input URL) or **EQUAL** (switchover between primary and standby input URLs) as needed. ● **Audio Selectors**: Up to eight audio selectors can be added. Click **Add Audio Selector** to add **Audio Selector 1**. Configure the following parameters: – **Selector Name**: Enter an audio selector name using only letters, digits, hyphens (-), and underscores (_). The name of each selector in the same channel must be unique. – **Selector Settings**: **PID selection**: This mode requires specifying **PID**. **PID**: ID of the audio stream in the input source. **Language selection**: This mode requires specifying **Language Code** and **Language Selection Policy**. **Language Code**: Confirm the language of each audio stream in the source input, select an audio stream, and enter the language code (2–3 lowercase letters) of that audio stream. For example, **eng** indicates English. **Language Selection Policy**: The value **LOOSE** indicates that the audio stream language is loosely matched with the

Parameter	Description
	selected language code. In the example of **eng**, the audio stream whose language is English in the source input will be preferentially selected. If audio streams in the language represented by the selected language code cannot be found, the audio stream with the lowest PID will be selected. The value **STRICT** indicates that the audio stream language is strictly matched with the selected language code. In the example of **eng**, only audio streams in English in the source input will be selected. If audio streams in the language represented by the selected language code cannot be found, a muted segment will be automatically added. When a device uses this audio selector to play a video, the playback is muted. **HLS audio selection**: This mode requires specifying **Group ID** and **Name**. **Group ID**: See the **GROUP-ID** attribute of the M3U8 audio stream. **Name**: See the "Name" attribute of the M3U8 audio stream.

Parameter	Description
Input Type set to SRT_PUSH	Configure the following parameters: ● **Ingest Domain Name**: Select an SRT ingest domain name from the drop-down list box. If no ingest domain name is available, click **Create Ingest Domain Name** on the right and add an SRT ingest domain name on the **Add Domain** page. ● **Stream ID Mode**: indicates whether the encoder allows inputting a stream ID. If not, you must specify **CIDR IP Whitelist**. ● **CIDR IP Whitelist (Optional)**: Enter whitelisted CIDR IP addresses in a maximum of 256 characters. Separate IP addresses using commas (,). ● **Audio Selectors**: Up to eight audio selectors can be added. Click **Add Audio Selector** to add **Audio Selector 1**. Configure the following parameters: – **Selector Name**: Enter an audio selector name using only letters, digits, hyphens (-), and underscores (_). The name of each selector in the same channel must be unique. – **Selector Settings**: **PID selection**: This mode requires specifying **PID**. **PID**: ID of the audio stream in the input source. **Language selection**: This mode requires specifying **Language Code** and **Language Selection Policy**. **Language Code**: Confirm the language of each audio stream in the source input, select an audio stream, and enter the language code (2–3 lowercase letters) of that audio stream. For example, **eng** indicates English. **Language Selection Policy**: The value **LOOSE** indicates that the audio stream language is loosely matched with the selected language code. In the example of **eng**, the audio stream whose language is English in the source input will be preferentially selected. If audio streams in the language represented by the selected language code cannot be found, the audio stream with the lowest PID will be selected. The value **STRICT** indicates that the audio stream language is strictly matched with the selected language code. In the example of **eng**, only audio streams in English in the source input will be selected. If audio streams in the language represented by the selected language code cannot be found, a muted segment will be automatically added. When a device uses this audio selector to play a video, the playback is muted.

Parameter	Description
Input Type set to SRT_PULL	Configure the following parameters: ● **Primary Input Parameters**: **URL**, indicating the media stream URL obtained from the channel provider. Media Live directly uses the URL to push streams to the origin server. ● **SRT Minimum Latency (Optional)**: stream pull latency when the channel type is **SRT_PULL** ● **Stream ID (Optional)**: stream ID of the streaming URL when the channel type is **SRT_PULL** ● **Standby Input Parameters**: – **Primary/standby Input**: You can enable this function to set the standby media stream URL. – **Standby Input URL**: Obtain the standby media stream URL from the channel provider. – **Switchover Duration Threshold**: When the duration of abnormal channel playback reaches the threshold, the system automatically switches to another URL for stream pull and playback. – **Priority Settings**: Select **PRIMARY** (mainly the primary input URL) or **EQUAL** (switchover between primary and standby input URLs) as needed. ● **Audio Selectors**: Up to eight audio selectors can be added. Click **Add Audio Selector** to add **Audio Selector 1**. Configure the following parameters: – **Selector Name**: Enter an audio selector name using only letters, digits, hyphens (-), and underscores (_). The name of each selector in the same channel must be unique. – **Selector Settings**: **PID selection**: This mode requires specifying **PID**. **PID**: ID of the audio stream in the input source. **Language selection**: This mode requires specifying **Language Code** and **Language Selection Policy**. **Language Code**: Confirm the language of each audio stream in the source input, select an audio stream, and enter the language code (2–3 lowercase letters) of that audio stream. For example, **eng** indicates English. **Language Selection Policy**: The value **LOOSE** indicates that the audio stream language is loosely matched with the selected language code. In the example of **eng**, the audio stream whose language is English in the source input will be preferentially selected. If audio streams in the language represented by the selected language code cannot be found, the audio stream with the lowest PID will be selected. The value **STRICT** indicates that the audio stream language is strictly matched with the selected language

Parameter	Description
	code. In the example of **eng**, only audio streams in English in the source input will be selected. If audio streams in the language represented by the selected language code cannot be found, a muted segment will be automatically added. When a device uses this audio selector to play a video, the playback is muted.

Step 5 Click **Next**.

Table 7-14 shows **Output Settings**.

Table 7-14 Parameters

Item	Parameter	Description
Audio Output	Add Audio Output	This parameter (optional) is displayed when the input type is **HLS_PULL**, **SRT_PULL**, or **SRT_PUSH**. You can bind an audio selector in **Audio Output** and set the language and stream name to be displayed in either of the following cases: ● The actual audio language and stream name are not displayed during channel output playback. ● You need to change the language and stream name of the audio. Note: Each **Audio Output** allows binding only one audio selector, and the audio selector of each **Audio Output** must be unique. Therefore, **Audio Output** configurations cannot outnumber audio selectors. Specifically, click **Add Audio Output** and add **Audio Output 1** by configuring the following parameters: ● **Audio Output Name**: Enter a name consisting of letters, digits, hyphens (-), and underscores (_). Each audio output name of the same channel must be unique. ● **Selector Name**: Select a configured audio selector from the drop-down list box. The audio selector of each audio output must be unique. ● **Language Code Control**: This setting changes only the displayed audio language, not the actual one. Options: – **Follow input**: If the output audio of the selected audio selector has a language, the language code and stream name of the output audio will be used. Otherwise, the language code and stream name configured here will be used. The default value is recommended. – **User-defined**: You can customize the language code and stream name of the output audio. ● **Language Code**: Enter a language code consisting of two or three lowercase letters. For example, eng indicates English. ● **Stream Name**: (optional) stream name displayed on the GUI

Item	Parameter	Description
Transcoding Settings	Transcoding Template	Select one or more created Media Live transcoding templates (see **Creating a Transcoding Template**) from the drop-down list box.
Other	Catch-Up TV and Time-Shifted Viewing	Enabling this function requires setting **Startover Window**, that is, the duration of the catch-up TV content that can be viewed of a channel. Unit: second. For details, see **Obtaining a Catch-Up TV/Time-Shifted Viewing URL**. **NOTE** ● The OBS path for storing live recordings is *OBS address*/*push_domain*/*AppName*/*Channelid*. ● After deleting channel A, use the ingest domain name, App Name, and channel ID of channel A to create channel B. If the recordings of channel A are not completely aged, the catch-up TV URL created by channel B can be used to view the recordings of channel A. The recordings of channel A cannot be viewed when they are completely aged.
Output Segment Parameters	Segment Duration	Duration of a single segment. The value defaults to **4s** and must be an integer multiple of the GOP duration. The value ranges from 1 to 10, in second. **CAUTION** Exercise caution when changing the segment duration, as this operation will affect the time-shifted viewing of catch-up TV content.
Output Group Settings **NOTE** You can click ⊞ on the right to add multiple output types.	Output Protocol	Protocol for output transcoded video. Options: ● **HLS** ● **DASH** ● **MSS**

Item	Parameter	Description
	HLS	Configure the following parameters: ● **Live Playlist Window Duration**: duration (in second) returned by the live playlist ● **Distribution URL**: Select a streaming domain name from the first drop-down list box and enter a playback address in the second drop-down list box. After both are assembled, a streaming URL is generated. Example for HLS: https://live-play.example.com/{*channelId*}/hls/{*unique_string*}/index.m3u8 Streaming URLs support HTTPS. You need to configure an HTTPS certificate by referring to **HTTPS Certificates**. NOTICE – If **Input Type** is set to **RTMP_PUSH** or **SRT_PUSH** in **Step 4**, the streaming domain name configured here and the ingest domain name configured in **Input Type** must be in the same region. – If **Input Type** is set to **FLV_PULL**, **HLS_PULL**, or **SRT_PULL** in **Step 4** and multiple output types have been set, the streaming domain names of all output types must be in the same region. – Neither encrypted nor unencrypted MSS streams (H.265) can be output. ● **DRM Encryption**: To enable DRM encryption, configure the parameters in **Table 7-15**. NOTICE – If DRM encryption needs to be enabled for a channel and **Interconnection Mode** is set to **FunctionGraph proxy access** to provide the key for interconnecting with DRM, you need to: enable **FunctionGraph agency** in advance by referring to **Cloud Resource Authorization** **build a function** in FunctionGraph. – If the DRM system is faulty, 404 is returned.

Item	Parameter	Description
	DASH	Configure the following parameters: ● **Manifest Window Duration**: duration (in second) returned by the live playlist ● **Streaming Delay**: timelapse before live content can be played. The value (in second) ranges from 1 to 120 and defaults to **20**. ● **Minimum Update Period**: minimum waiting time before the player requests to update the list. The value (in second) ranges from 1 to 120 and defaults to **2**. ● **Minimum Buffer Time**: smallest amount of available content that the player must reserve in the buffer. The value (in second) ranges from 1 to 120 and defaults to **10**. ● **Distribution URL**: Select a streaming domain name from the first drop-down list box and enter a playback address in the second drop-down list box. After both are assembled, a streaming URL is generated. Example for DASH: https://live-play.example.com/{*channelId*}/dash/{*unique_string*}/index.mpd Streaming URLs support HTTPS. You need to configure an HTTPS certificate by referring to **HTTPS Certificates**. NOTICE – If **Input Type** is set to **RTMP_PUSH** or **SRT_PUSH** in **Step 4**, the streaming domain name configured here and the ingest domain name configured in **Input Type** must be in the same region. – If **Input Type** is set to **FLV_PULL**, **HLS_PULL**, or **SRT_PULL** in **Step 4** and multiple output types have been set, the streaming domain names of all output types must be in the same region. – Neither encrypted nor unencrypted MSS streams (H.265) can be output. ● **DRM Encryption**: To enable DRM encryption, configure the parameters in **Table 7-15**. NOTICE – If DRM encryption needs to be enabled for a channel and **Interconnection Mode** is set to **FunctionGraph proxy access** to provide the key for interconnecting with DRM, you need to: enable **FunctionGraph agency** in advance by referring to **Cloud Resource Authorization** **build a function** in FunctionGraph. – If the DRM system is faulty, 404 is returned.

Item	Parameter	Description
	MSS	Configure the following parameters: ● **Manifest Window Duration**: duration (in second) returned by the live playlist ● **Distribution URL**: Select a streaming domain name from the first drop-down list box and enter a playback address in the second drop-down list box. After both are assembled, a streaming URL is generated. Example for MSS: https://live-play.example.com/{*channelId*}/mss/{*unique_string*}.ism/Manifest Streaming URLs support HTTPS. You need to configure an HTTPS certificate by referring to **HTTPS Certificates**. NOTICE – If **Input Type** is set to **RTMP_PUSH** or **SRT_PUSH** in **Step 4**, the streaming domain name configured here and the ingest domain name configured in **Input Type** must be in the same region. – If **Input Type** is set to **FLV_PULL**, **HLS_PULL**, or **SRT_PULL** in **Step 4** and multiple output types have been set, the streaming domain names of all output types must be in the same region. – Neither encrypted nor unencrypted MSS streams (H.265) can be output. ● **DRM Encryption**: To enable DRM encryption, configure the parameters in **Table 7-15**. NOTICE – If DRM encryption needs to be enabled for a channel and **Interconnection Mode** is set to **FunctionGraph proxy access** to provide the key for interconnecting with DRM, you need to: enable **FunctionGraph agency** in advance by referring to **Cloud Resource Authorization** **build a function** in FunctionGraph. – If the DRM system is faulty, 404 is returned.

Table 7-15 DRM configuration

Parameter	Description
Resource ID	Content resource ID provided by the DRM system
SPEKE Version	AWS SPEKE version. Currently, only version 1.0 is supported. For details, see **SPEKE**. This protocol must comply with **license requirements**.

Parameter	Description
DRM System	DRM encryption type. Constraints: - The HLS output protocol supports FairPlay. - The DASH output protocol supports Widevine, PlayReady, and PlayReady + Widevine. - The MSS protocol supports only PlayReady.
Encryption Level	DRM encryption level. The encryption key needs to be obtained from the DRM vendor. Options: - **content**: Each channel has one specific DRM encryption key. - **profile**: Each stream of a channel has one specific DRM encryption key. Constraints: HLS and DASH streams support both preceding encryption modes, while MSS streams support only **content** encryption.
Interconnection Mode	Mode of interconnecting with a DRM system. Options: - **HTTPS direct access**: Enter an HTTPS URL to obtain the DRM system. HTTP URLs are not supported. **Key** and **Value** in the header are used to verify the accuracy and validity of the URL obtained by the DRM system. These two fields are optional. To add them, click **Adding a Header** and specify **Header Key** and **Header Value**. A maximum of five groups of **Key** and **Value** can be added, but each **Key** must be unique. - **FunctionGraph proxy access**: You can **build a function** using FunctionGraph to package the obtained **Key** and **Value**. **Key** and **Value** can be dynamically obtained using functions. Other token authentication methods are also supported. This mode requires enabling **FunctionGraph agency** (see **Cloud Resource Authorization**) to authorize Media Live to call FunctionGraph functions. This mode requires specifying the **Function** parameter and selecting a function name from the drop-down list box. **NOTICE** When FunctionGraph is used for channel DRM encryption, the FunctionGraph version information is not contained. By default, the latest version is used.
URL	- URL of the key for DRM encryption. – **HTTPS direct access** requires entering an HTTPS URL. – If **FunctionGraph proxy access** is selected, the URL is automatically filled in and cannot be changed.

Step 6 Click **Finish**. A new line of channel content is displayed on the **Channels** page.

Step 7 Click **Start** in the **Operation** column to start the channel.

----End

Managing Channels

After creating a channel, you can perform the following operations as required:

- Starting a channel

  After a channel is created, click **Start** in the **Operation** column to start the channel.

- Stopping a channel

  To stop a channel, click **Stop** in the **Operation** column.

- Modifying a channel

  To modify a channel, click **Manage** in the **Operation** column and modify the configuration items of the channel. If the channel to be modified has been started, the channel automatically restarts after the modification. The restart takes about 30 seconds. During the channel restart, media streams will be interrupted. After the channel is restarted, media streams automatically resume.

- Deleting a channel

  To delete a channel, stop the channel and click **Delete** in the **Operation** column.

7.6 Live Transcoding

7.6.1 Creating a Transcoding Template

You can transcode livestreams into video streams with different resolutions and bitrates to meet a broad range of requirements. You can customize a transcoding template. When a channel is created, a transcoding template is configured. When channel content is played, transcoding is performed based on the transcoding template.

Function Overview

The transcoding function allows you to:

- Transcode source audio and video into one or more formats for playback on a wide range of devices.
- Adapt the output bitrate to different network bandwidths.
- Reduce the costs of distributing livestreams. Low-bitrate HD can reduce the bitrate usage by about 20% at the same resolution.
- Customize transcoding templates, such as the transcoding type, video bitrate, resolution, frame rate, and GOP duration.

For details about the function implementation, see Multi-bitrate Adaptation of Media Live.

Notes

- To delete a transcoding template, you need to manually delete it from all channels. Otherwise, the transcoding template still takes effect on the channels.
- The transcoding template of a channel takes effect when the channel playback starts. If the transcoding configuration is modified, the modification takes effect only after the channel is restarted.
- If you enable low-bitrate HD, you will be charged based on the rates of low-bitrate HD. For details about the price, see **Live Pricing Details**.
- Upsampling transcoding is not supported. If the resolution set in the transcoding template is higher than the original resolution, the transcoded streaming URL can be used for playback, but the played video still uses the original resolution. Upsampling is not applicable to the frame rate of a transcoded output.
- In the EU-Dublin region, **submit a service ticket** for review after configuring a template. The configuration takes effect only after it is approved.
- The resolution and frame rate of a transcoded output cannot be higher than those of the input.

Prerequisites

- **An ingest domain name has been added**.
- **CNAME records have been added** to your domains' DNS records.

Adding a Media Live Transcoding Template

You can add a Media Live transcoding template on the Live console.

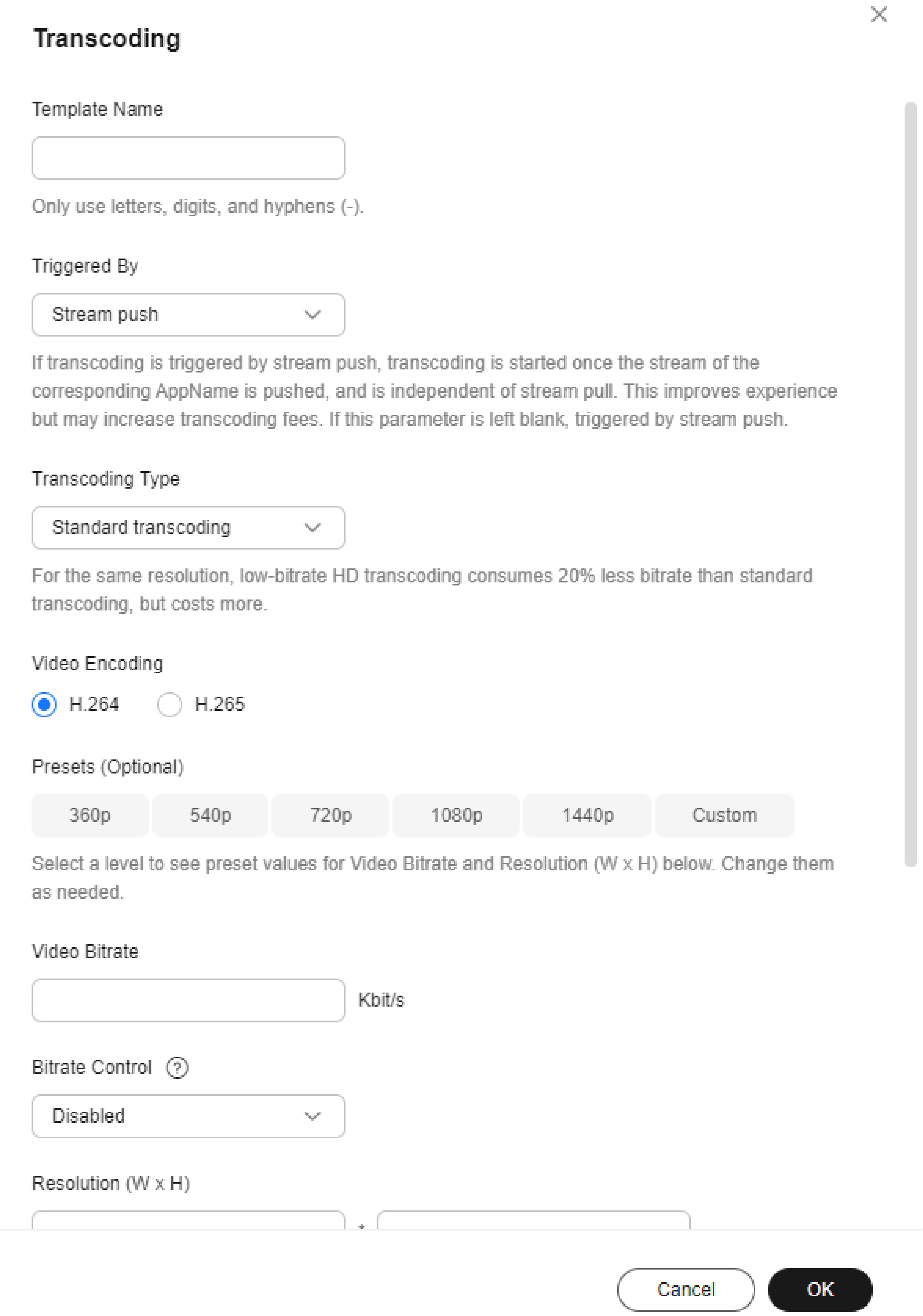
Step 1 Log in to the **Live console**.

Step 2 In the navigation pane on the left, choose **Live Transcoding** under **Media Live**.

Step 3 Click **Create Transcoding Template**. The **Transcoding** page is displayed on the right, as shown in **Figure 7-24**.

Configure transcoding parameters as instructed by **Table 7-16**.

Figure 7-24 Creating a transcoding template



Transcoding

Template Name

Only use letters, digits, and hyphens (-).

Triggered By

Stream push

If transcoding is triggered by stream push, transcoding is started once the stream of the corresponding AppName is pushed, and is independent of stream pull. This improves experience but may increase transcoding fees. If this parameter is left blank, triggered by stream push.

Transcoding Type

Standard transcoding

For the same resolution, low-bitrate HD transcoding consumes 20% less bitrate than standard transcoding, but costs more.

Video Encoding

● H.264 ○ H.265

Presets (Optional)

360p | 540p | 720p | 1080p | 1440p | Custom

Select a level to see preset values for Video Bitrate and Resolution (W x H) below. Change them as needed.

Video Bitrate

Kbit/s

Bitrate Control

Disabled

Resolution (W x H)

Table 7-16 Transcoding settings

Parameter	Description
Template Name	Name of a Media Live transcoding template. You can customize the name in letters, digits, and hyphens (-).
Triggered By	Transcoding is triggered by stream push. When a transcoding request is received, the transcoding template whose name is the same as the value of **AppName** in the request URL takes effect and transcoding starts.
Transcoding Type	Transcoding type of Media Live. Options: ● **Standard transcoding** ● **Low-bitrate HD** For the same resolution, low-bitrate HD transcoding consumes 20% less bitrate than standard transcoding but costs more. Low-bitrate HD means a lower output bitrate at a given image quality. If you enable this function, you will be billed based on the rates of low-bitrate HD. For details, see **Pricing Details**.
Video Encoding	Supported video encoding formats: ● **H.264** ● **H.265** **NOTICE** – Select only one encoding format for each channel. – **H.265** is displayed only when **Input Type** of a created channel is set to **SRT_PUSH**, **HLS_PULL**, or **SRT_PULL**.
Presets (Optional)	Resolution levels: ● **360p** ● **540p** ● **720p** ● **1080p** ● **1440p** ● **Custom** Select a level to see preset values for **Video Bitrate** and **Resolution (W x H)** below. Change them as needed.
Video Bitrate	Average bitrate of the transcoded video, in Kbit/s. Value range: 40 to 30,000

Parameter	Description
Bitrate Control	Bitrate control policy. Options: ● **Disabled**: Bitrate adaptation is disabled. The target bitrate is output as specified. ● **Not higher than source stream**: The target bitrate is the smaller value between the specified bitrate and the bitrate of the source file. ● **Adaptive to source stream**: The target bitrate is adaptive to the bitrate of the source file. Default value: **Disabled**
Resolution (W x H)	Width and height of the video, in pixel. If the input value of both sides is set to **0**, the video is output using the resolution of the source stream. If the value of one side is set to **0**, the value of that side will be converted proportionally according to the input value of the other side. Value range: ● Width: The value must be 0 or a multiple of 2 between 32 and 3,840. ● Height: The value must be 0 or a multiple of 2 between 32 and 2,160. **NOTICE** – The transcoded output resolution cannot be higher than the input resolution.
Video Frame Rate	Frame rate of the transcoded video. Options: ● **Retain the original** ● **Set a new one**: If you select this option, you need to enter the frame rate. The value ranges from 0 to 60. **0** means adaptive frame rate. The transcoded output frame rate cannot be higher than the input frame rate.
Use Source I-Frame	This function must be enabled for Media Live. After this function is enabled, the I-frame, position, and PTS of the transcoded stream are the same as those of the source stream. In this case, both the source and transcoded streams have the same GOP duration.
B-Frame Removal	After this function is enabled, the transcoded video does not contain B-frames.

Step 4 Click **OK**.

There is a new transcoding template on the **Live Transcoding** page.

----End

Managing Transcoding Templates

You can perform the following operations on your transcoding template:

- Editing a transcoding template

  Click **Edit** in the **Operation** column to modify parameters in the template. If the channel where the transcoding template is located has been started, you need to restart the channel for the modification to take effect. It takes about 30 seconds to restart the channel. During the channel restart, transcoding will be interrupted. After the channel is restarted, transcoding automatically resumes.
- Deleting a transcoding template

  Click **Delete** in the **Operation** column.

7.7 Service Monitoring

View the monitoring information about streaming domain names, including **CDN Downstream Bandwidth/Traffic**, **CDN Status Codes** returned in responses, **CDN Concurrent Downstream Requests**, **Transcoding Metrics**, and **Packaging Metrics**.

Notes

Bandwidth/Bitrate is counted by 1,000 (example: 1 Mbit/s = 1,000 Kbit/s) and traffic by 1,024 (example: 1 MB = 1,024 KB).

Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane on the left, choose **Service Monitoring** under **Media Live**.

Step 3 Select **CDN Downstream Bandwidth/Traffic**, **CDN Status Code**, **CDN Concurrent Downstream Requests**, **Transcoding Metrics**, or **Packaging Metrics** to view the statistics.

Move the cursor to the trend chart and scroll the mouse wheel to zoom in or zoom out the X axis (time).

----End

CDN Downstream Bandwidth/Traffic

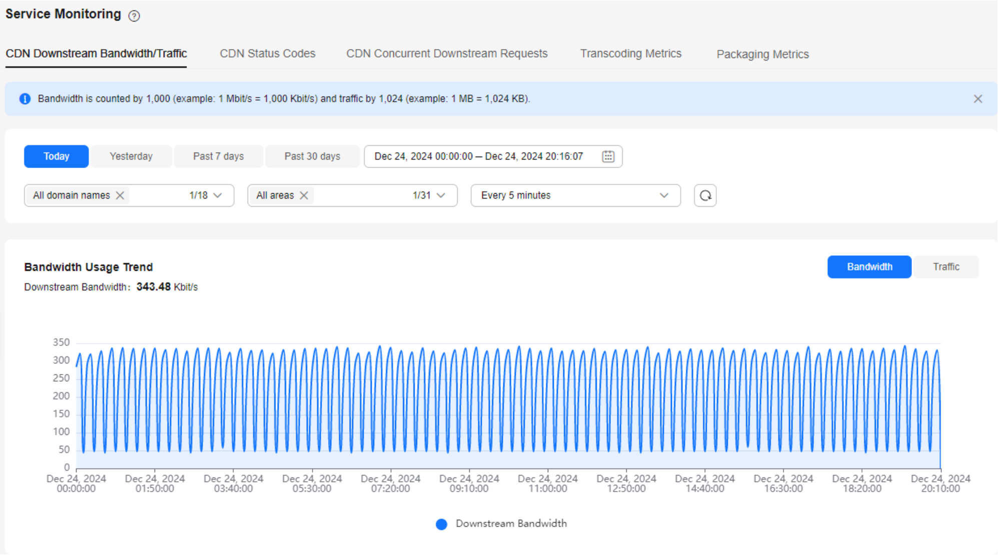
NOTE

- You can query data of the past 90 days.
- You can query data in a time span of up to 31 days.
- You can query data about up to 20 domain names at a time.
- The minimum statistical granularity is 5 minutes. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 08:04:59 (GMT+08:00) is displayed at the statistical point November 6, 2020 08:00:00 (GMT+08:00). The displayed data is the maximum value in the period of the selected granularity.
- Constraints on the statistical granularity: If the query time span is no longer than 2 days, the **Every 1 day** granularity is not supported. If the query time span is longer than 2 days and no longer than 7 days, the **Every 5 minutes** granularity is not supported. If the query time span is longer than 7 days, only the **Every 1 day** granularity is supported.

Select the desired time, streaming domain name, area, and statistical granularity. Click **Bandwidth** or **Traffic** on the right of the page to view the bandwidth or traffic usage trend.

- **Bandwidth Usage Trend** displays the bandwidth usage trend of the selected domain name, as shown in Figure 7-25. **Downstream Bandwidth: 2.00 Mbit/s** indicates the downstream peak bandwidth of the selected domain name in the query period.

Figure 7-25 CDN downstream bandwidth statistics



Bandwidth is counted by 1,000 (example: 1 Mbit/s = 1,000 Kbit/s) and traffic by 1,024 (example: 1 MB = 1,024 KB).

Dec 24, 2024 00:00:00 – Dec 24, 2024 20:16:07

All domain names 1/18

All areas 1/31

Every 5 minutes

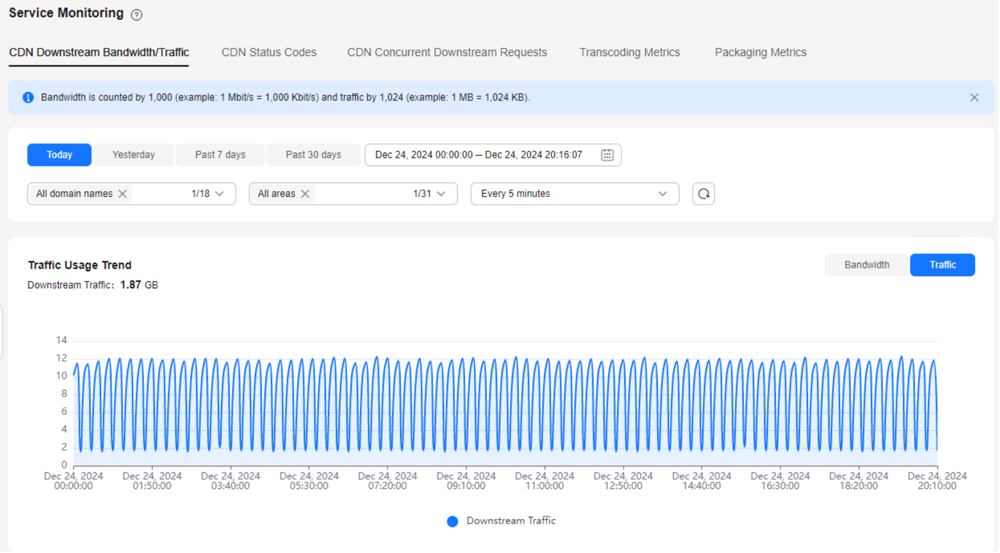
Bandwidth Usage Trend

Downstream Bandwidth: **343.48** Kbit/s

- **Traffic Usage Trend** displays the traffic usage trend of the selected domain name, as shown in Figure 7-26. **Downstream Traffic: 2.50 GB** indicates the traffic consumed by the selected domain name in the query period.

  The total traffic displayed in the trend chart is the sum of traffic measured every 5 minutes and converted from byte into MB, accurate to two decimal places.

Figure 7-26 CDN downstream traffic statistics



Bandwidth is counted by 1,000 (example: 1 Mbit/s = 1,000 Kbit/s) and traffic by 1,024 (example: 1 MB = 1,024 KB).

Dec 24, 2024 00:00:00 – Dec 24, 2024 20:16:07

All domain names 1/18

All areas 1/31

Every 5 minutes

Traffic Usage Trend

Downstream Traffic: **1.87** GB

CDN Status Code

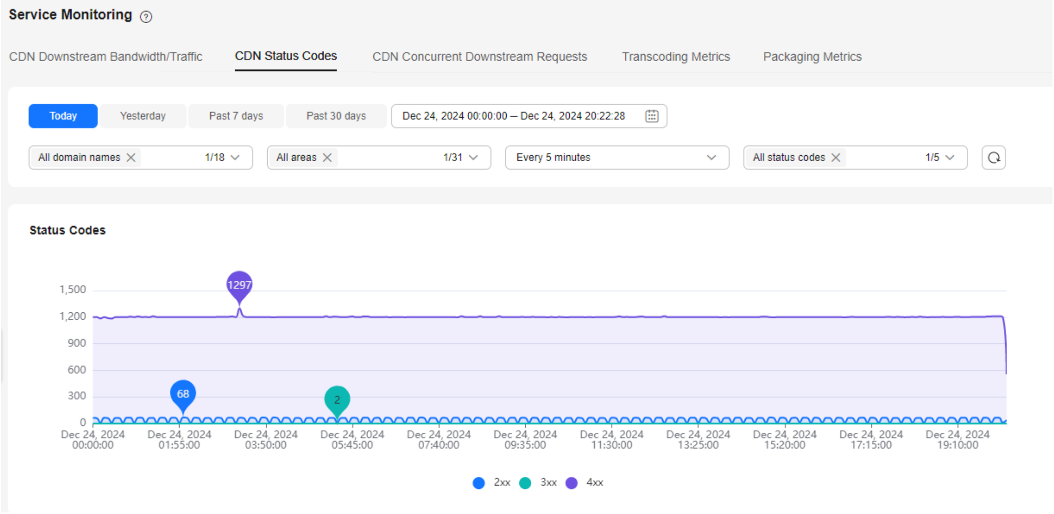
NOTE

- You can query data of the past 90 days.
- You can query data in a time span of up to 31 days.
- You can query data about up to 20 domain names at a time.
- The minimum statistical granularity is 5 minutes. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 08:04:59 (GMT+08:00) is displayed at the statistical point November 6, 2020 08:00:00 (GMT+08:00). The displayed data is the maximum value in the period of the selected granularity.
- Constraints on the statistical granularity: If the query time span is no longer than 2 days, the **Every 1 day** granularity is not supported. If the query time span is longer than 2 days and no longer than 7 days, the **Every 5 minutes** granularity is not supported. If the query time span is longer than 7 days, only the **Every 1 day** granularity is supported.

You can specify the time, streaming domain name, area, statistical granularity, and status code to view the trend chart of the corresponding status code, as shown in **Figure 7-27**.

The trend chart displays the number of status codes returned by the server.

Figure 7-27 CDN status code statistics



CDN Concurrent Downstream Requests

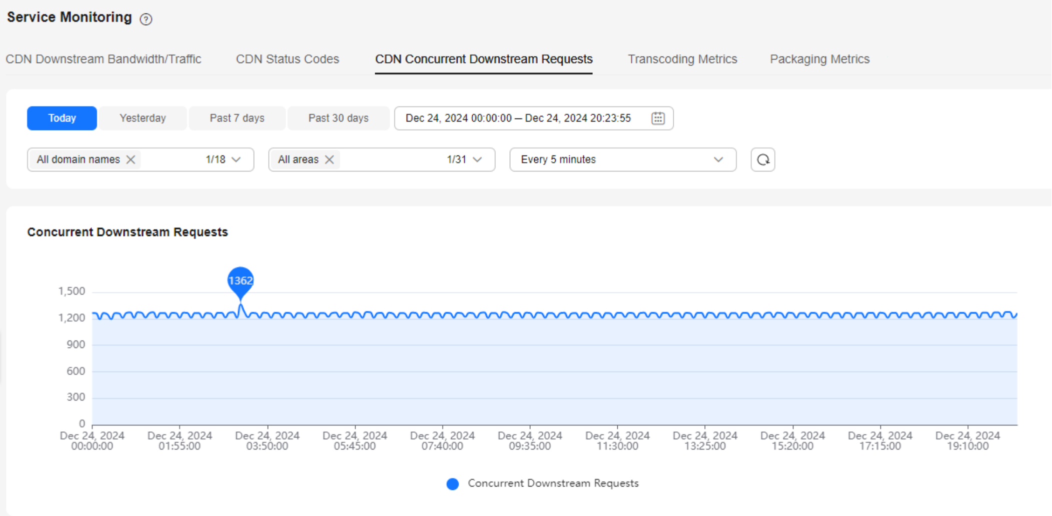
NOTE

- You can query data of the past 90 days.
- You can query data in a time span of up to 31 days.
- You can query data about up to 20 domain names at a time.
- The minimum statistical granularity is 5 minutes. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 08:04:59 (GMT+08:00) is displayed at the statistical point November 6, 2020 08:00:00 (GMT+08:00). The displayed data is the maximum value in the period of the selected granularity.
- Constraints on the statistical granularity: If the query time span is no longer than 2 days, the **Every 1 day** granularity is not supported. If the query time span is longer than 2 days and no longer than 7 days, the **Every 5 minutes** granularity is not supported. If the query time span is longer than 7 days, only the **Every 1 day** granularity is supported.

You can specify the time, streaming domain name, area, and statistical granularity to view the trend chart of the corresponding downstream concurrent requests.

The trend chart displays the number of streaming domain name requests received by the server.

Figure 7-28 Trend chart of CDN concurrent downstream requests



Dec 24, 2024 00:00:00 – Dec 24, 2024 20:23:55

All domain names 1/18

All areas 1/31

Every 5 minutes

Transcoding Metrics

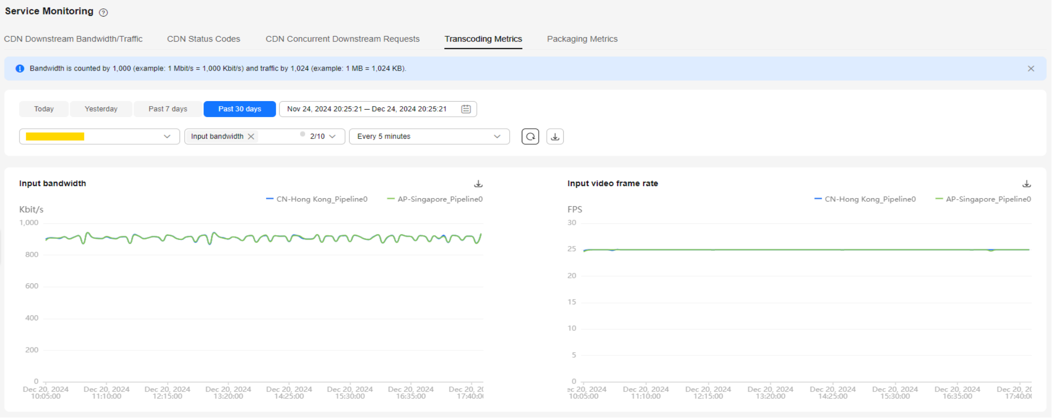
📖 NOTE

- You can query data of the past 90 days.
- You can query data in a time span of up to 30 days.
- The minimum statistical granularity of **Transcoding Metrics** is 1 minute. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 08:00:59 (GMT+08:00) is displayed at the statistical point November 6, 2020 08:00:00 (GMT+08:00). The displayed data is the maximum value in the period of the selected granularity.

Select the time, channel name, transcoding metric name (**Input bandwidth**, **Input video frame rate**, **Input disconnections**, **Dropped packets**, **Input switches for failover**, **Continuity errors**, **PID errors**, **Dropped frames**, **Duration of input without received packets**, and **Output bandwidth**), and statistical granularity to view the trend chart of the input quality.

See the following figure.

Figure 7-29 Trend chart of transcoding metrics



Bandwidth is counted by 1,000 (example: 1 Mbit/s = 1,000 Kbit/s) and traffic by 1,024 (example: 1 MB = 1,024 KB).

Nov 24, 2024 20:25:21 – Dec 24, 2024 20:25:21

Input bandwidth 2/10

Every 5 minutes

Packaging Metrics

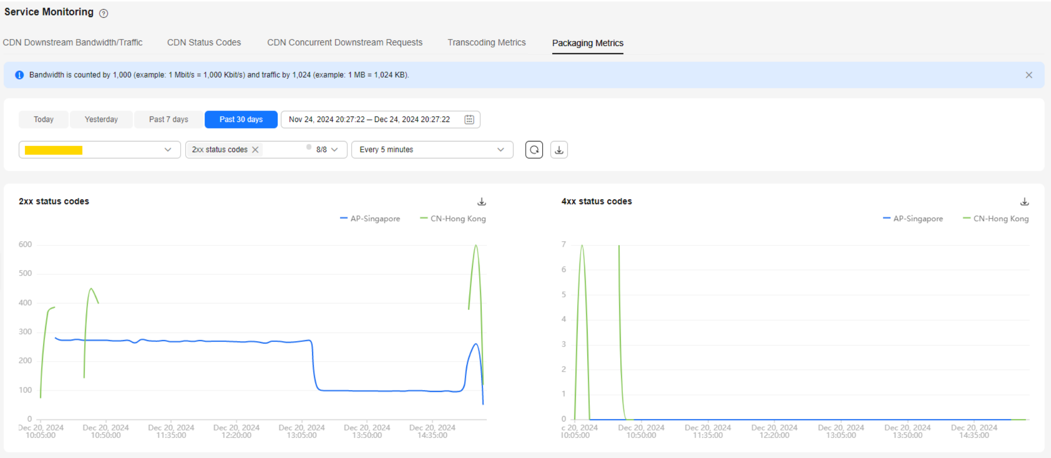
NOTE

- You can query data of the past 90 days.
- You can query data in a time span of up to 30 days.
- The minimum statistical granularity of **Packaging Metrics** is 1 minute. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 08:00:59 (GMT+08:00) is displayed at the statistical point November 6, 2020 08:00:00 (GMT+08:00). The displayed data is the maximum value in the period of the selected granularity.

Select the time, channel name, packaging metric name (**2xx status codes**, **4xx status codes**, **5xx status codes**, **HLS requests**, **DASH requests**, **MSS requests**, **Input traffic**, and **Output traffic**), and statistical granularity to view the trend chart of the input quality.

See the following figure.

Figure 7-30 Trend chart of packaging metrics



Service Monitoring

Bandwidth is counted by 1,000 (example: 1 Mbit/s = 1,000 Kbit/s) and traffic by 1,024 (example: 1 MB = 1,024 KB).

Past 30 days: Nov 24, 2024 20:27:22 – Dec 24, 2024 20:27:22

2xx status codes 8/8

Every 5 minutes

7.8 Cloud Resource Authorization

If DRM encryption needs to be enabled for a channel and **Interconnection Mode** is set to **FunctionGraph proxy access**, you need to enable **FunctionGraph agency** in advance by referring to this section.

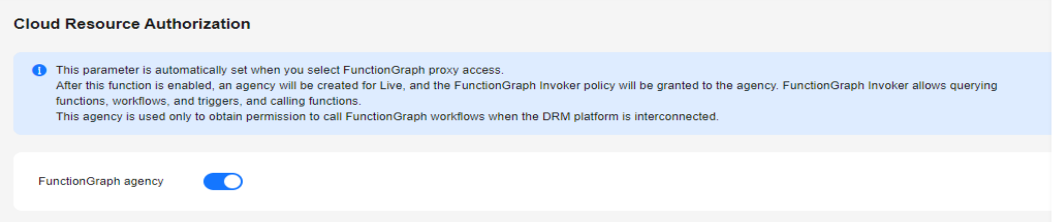
Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Cloud Resource Authorization** under **Media Live**.

You need to enable **FunctionGraph Resource Authorization** so that Media Live can call functions, workflows, and triggers of users. This agency is used only for DRM encryption. FunctionGraph functions are called to obtain the key for DRM encryption.

Figure 7-31 Cloud resource authorization



Cloud Resource Authorization

This parameter is automatically set when you select FunctionGraph proxy access.
After this function is enabled, an agency will be created for Live, and the FunctionGraph Invoker policy will be granted to the agency. FunctionGraph Invoker allows querying functions, workflows, and triggers, and calling functions.
This agency is used only to obtain permission to call FunctionGraph workflows when the DRM platform is interconnected.

FunctionGraph agency ●

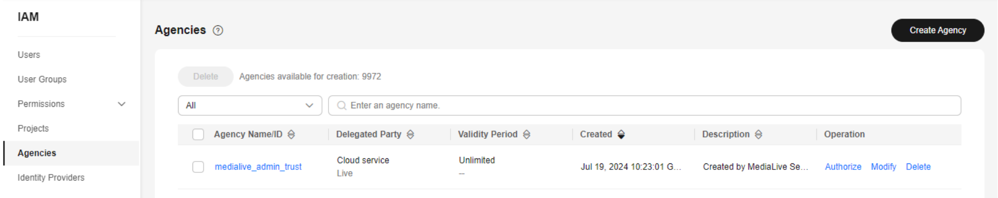
Step 3 Log in to the IAM console.

Step 4 In the navigation pane, choose **Agencies**, as shown in **Figure 7-32**.

After **FunctionGraph agency** is enabled for Media Live, the agency **medialive_admin_trust** is automatically added.

- This agency name can be used only for Live. If the agency name has been used by another service, the agency and permissions of **medialive_admin_trust** will be automatically reset when **FunctionGraph agency** is enabled. This affects the authorization by IAM on other services and their usage.
- The authorization permissions cannot be modified. If **FunctionGraph agency** is disabled for Media Live, the agency **medialive_admin_trust** will be automatically deleted. If **FunctionGraph agency** is enabled again, the agency **medialive_admin_trust** will be automatically re-created and its permissions will be reset to the default permissions.

Figure 7-32 IAM agencies



Agencies available for creation: 9972

Agency Name/ID	Delegated Party	Validity Period	Created	Description	Operation
medialive_admin_trust	Cloud service Live	Unlimited --	Jul 19, 2024 10:23:01 G...	Created by MediaLive Se...	Authorize Modify Delete

----End

7.9 Tools

7.9.1 Obtaining a Catch-Up TV/Time-Shifted Viewing URL

If you need to watch catch-up TV on Media Live, obtain a catch-up TV/time-shifted viewing URL of the channel by referring to this section.

Prerequisites

You have created a channel, as shown in **Creating a Channel**. The channel is running and **Catch-Up TV and Time-Shifted Viewing** has been enabled.

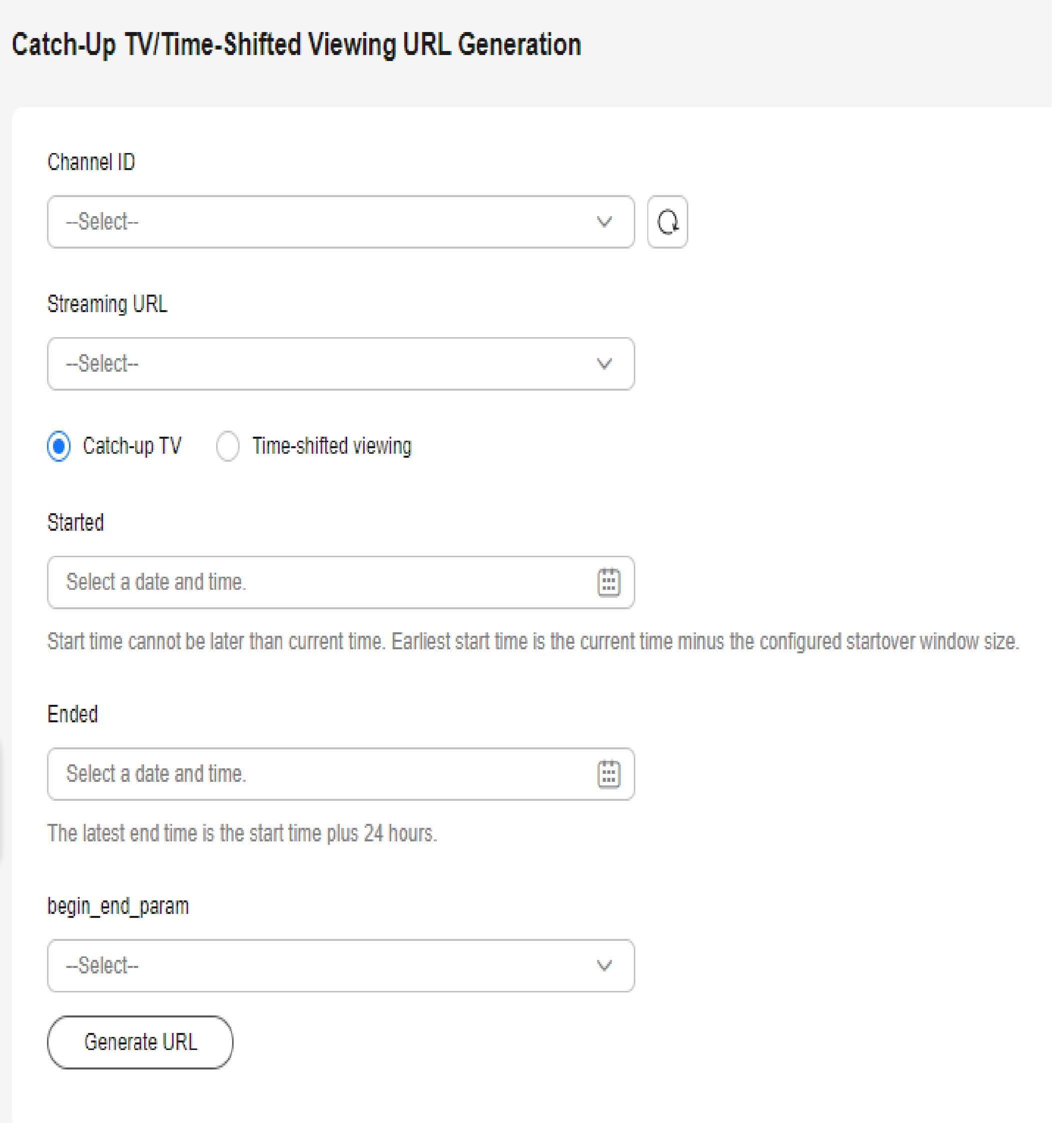
Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane on the left, choose **Tools** > **Catch-Up TV/Time-Shifted Viewing URL Generation** under **Media Live**.

See **Figure 7-33** and **Table 7-17**.

Figure 7-33 Catch-up TV/Time-shifted viewing URL generation



Catch-Up TV/Time-Shifted Viewing URL Generation

Channel ID

--Select--

Streaming URL

--Select--

● Catch-up TV ○ Time-shifted viewing

Started

Select a date and time.

Start time cannot be later than current time. Earliest start time is the current time minus the configured startover window size.

Ended

Select a date and time.

The latest end time is the start time plus 24 hours.

begin_end_param

--Select--

Generate URL

Table 7-17 Parameters

Parameter	Description
Channel ID	Select the ID of the desired channel from the drop-down list box. Before selecting a channel, click ⟳ on the right to hide deleted channels or channels with catch-up TV/time-shifted viewing disabled.
Streaming URL	Select the streaming URL of the channel from the drop-down list box.
Catch-up TV	Configure the following parameters: ● **Started**: When catch-up TV/time-shifted viewing is enabled for a channel, you need to set **Startover Window**. Users can view only the recorded content within the startover window. Click 📅. The calendar is displayed. The time segment of the historical video that can be viewed is highlighted. You can select the start time as required. **NOTICE** The start time must be earlier than the current time. For example, if the current time is 14:51 on August 16, the start time must be earlier than 14:51 on August 16. ● **Ended**: A catch-up TV URL can be used to watch catch-up TV content of up to 24 hours, so the end time can be at most one day later than the start time.
Time-shifted viewing	Configure the following parameters: **Time-Shifted Duration**: Enter a value for hour, minute, and second, respectively. The maximum value is 24 hours. When catch-up TV/time-shifted viewing is enabled for a channel, you need to set **Startover Window**. Users can view only the recorded content within the startover window.

Step 3 After configuring the preceding parameters, click **Generate URL**.

The catch-up TV/time-shifted viewing URL has been generated. You can click ⧉ on the right to copy the URL and start catch-up TV/time-shifted viewing.

- If the catch-up TV/time-shifted viewing URL is invalid, check whether the channel is still in the channel ID list. Click ⟳ on the right of the channel ID to refresh the page. The possible cause is that the channel has been deleted or catch-up TV has been disabled for the channel.
- If **Startover Window** of a catch-up TV/time-shifted viewing URL is set to 7 days, users will obtain the catch-up TV URL of the earliest day and need to watch immediately. Otherwise, data that had been recorded before **Startover Window** will be aged and cannot be played.

----End