Media Live

User Guide

Issue 01

Date 2024-05-13

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Media Live is a broadcast-grade livestreaming service that supports features such as channel management and content encryption, making it an ideal option for media assets and broadcasting.

NOTE

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

2 Scenarios

Media Live is applicable to PGC platforms that provides online livestreaming, such as carriers and radio stations. Typical customers include CCTV and Mango TV in China and CH7 and MNC outside China.

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	Dashboard	• You can view the downstream traffic and peak downstream bandwidth on the current day. • You can change the CDN billing option.
	Domain name management	You can add, delete, disable, and enable ingest domain names and streaming domain names for Media Live.
	Channel Management	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 downstream concurrent requests.
	Tools	You can obtain the replay URL to watch the replay 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.

Resources

Table 5-1 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 5-2 Function constraints

Item	Description
Channel	Except for channels whose input type is **FLV_PULL**, all other channels allow only one input stream and can output streams of multiple bitrates only after transcoding.

Clients

Table 5-3 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.

Item	Description
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.

6 Getting Started

6.1 Quick Start

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

Figure 6-1 Getting started with Media Live

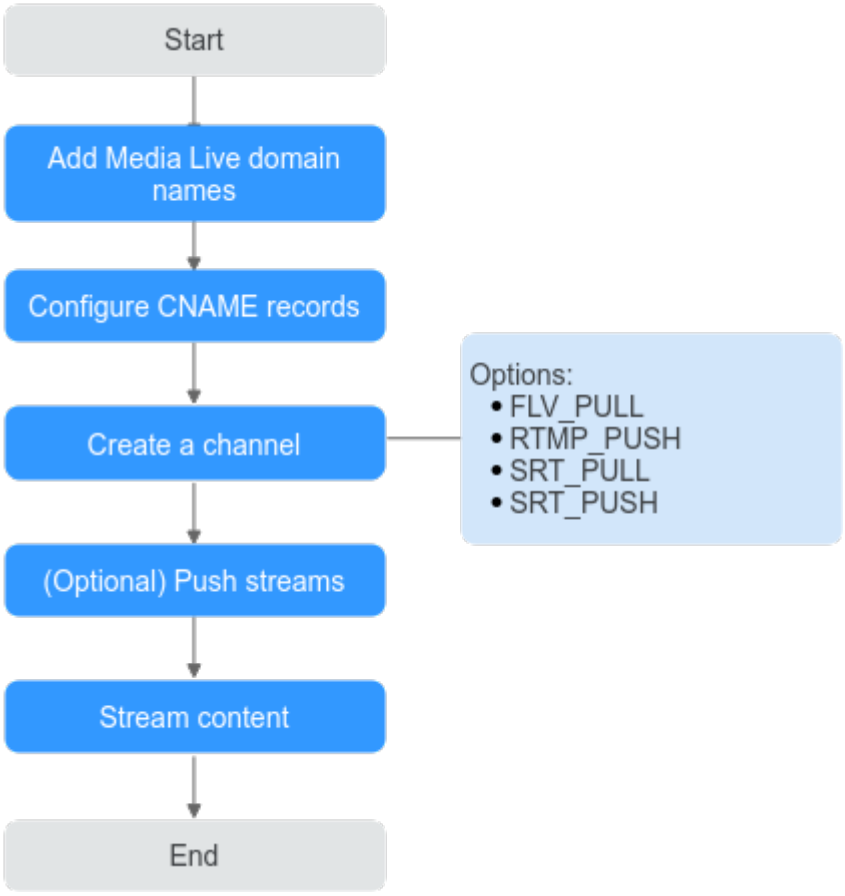


Table 6-1 describes how to get started with Live.

Table 6-1 Getting started with 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 ingest domain name needs to be configured for stream push.
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)** 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. Media Live requires an ingest domain name and a streaming domain name, and the two domain names must be different.

  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 an ingest domain name.

Table 6-2 Domain name parameters

Parameter	Description
Domain Name	Enter a second-level ingest domain name or streaming domain name. A domain name contains up to 42 characters and is case-insensitive. An ingest domain name must be different from a streaming domain name. Wildcard domains are not allowed. Example: test-push.example.com **NOTE** 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.
Enterprise Project	Add domain names to enterprise projects for unified management. Create an enterprise project by referring to **Creating an Enterprise Project**. The default enterprise project is named **default**. On the **Enterprise Project Management** page, **create an enterprise project** and **add a 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.

Parameter	Description
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 and ME-Riyadh of Huawei Cloud (International) By default, this function is unavailable in ME-Riyadh. If you have additional requirements, **submit a service ticket** for technical support.
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: • **Chinese mainland** Select this option when the audience is in the Chinese mainland. The domain name must be licensed by the Ministry of Industry and Information Technology (MIIT). • **Outside Chinese mainland** Select this option when the audience is outside the Chinese mainland (including in Hong Kong, Macao, and Taiwan). • **Global** Select this option when there is audience in and outside the Chinese mainland (including in Hong Kong, Macao, and Taiwan). The domain name must be licensed by the Ministry of Industry and Information Technology (MIIT).

Parameter	Description
Supported Protocols	Media stream protocols supported by streaming domain names. The value cannot be changed once configured, and defaults to **FLV+RTMP**. Options: • **FLV+RTMP** • **HLS**

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.

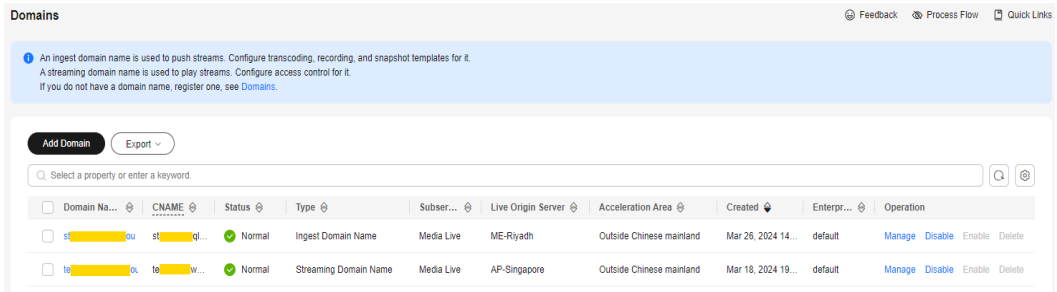
----End

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 6-2**.

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 CDN nodes of Huawei Cloud Live for faster livestreaming.

Figure 6-2 CNAME record



6.3 Pushing Streams and Streaming Content on a PC

This section describes how to push streams and stream content on a PC using the 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.

Pushing Streams

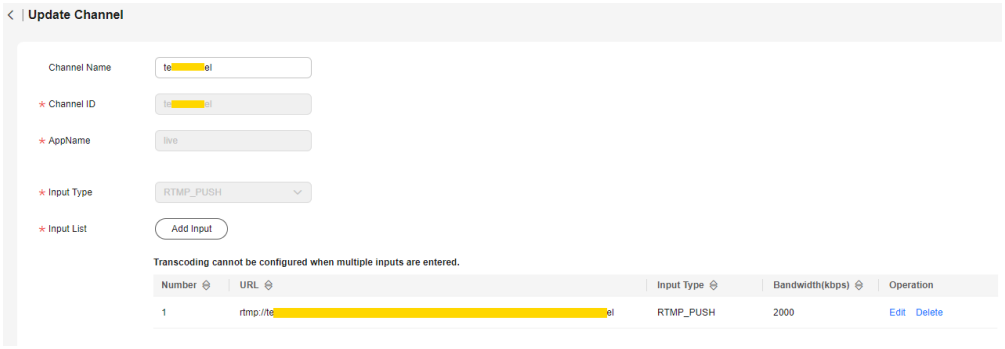
Step 1 Obtain the ingest URL.

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

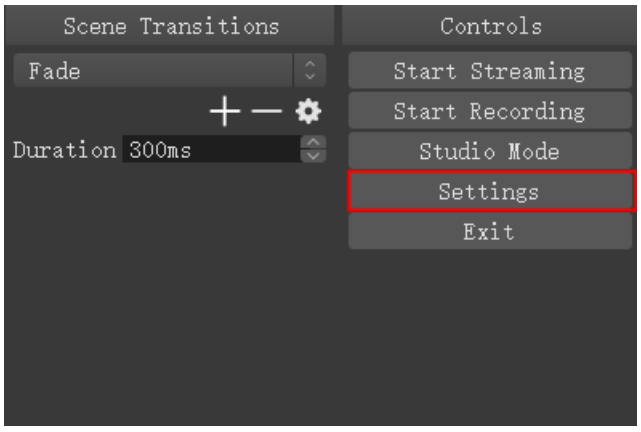
   The ingest URL is required only when **Input Type** is set to **RTMP_PUSH**. If **FLV_PULL** is selected, stream push is not required. The streaming URL provided by the user is directly obtained and used by Media Live to push streams to the origin server.

   The ingest URL is the value of URL in **Input List** shown in **Figure 6-3**, for example, rtmp://live-push.example.com/live/huaweitest?request_source=ott&channel_id=huaweitest.

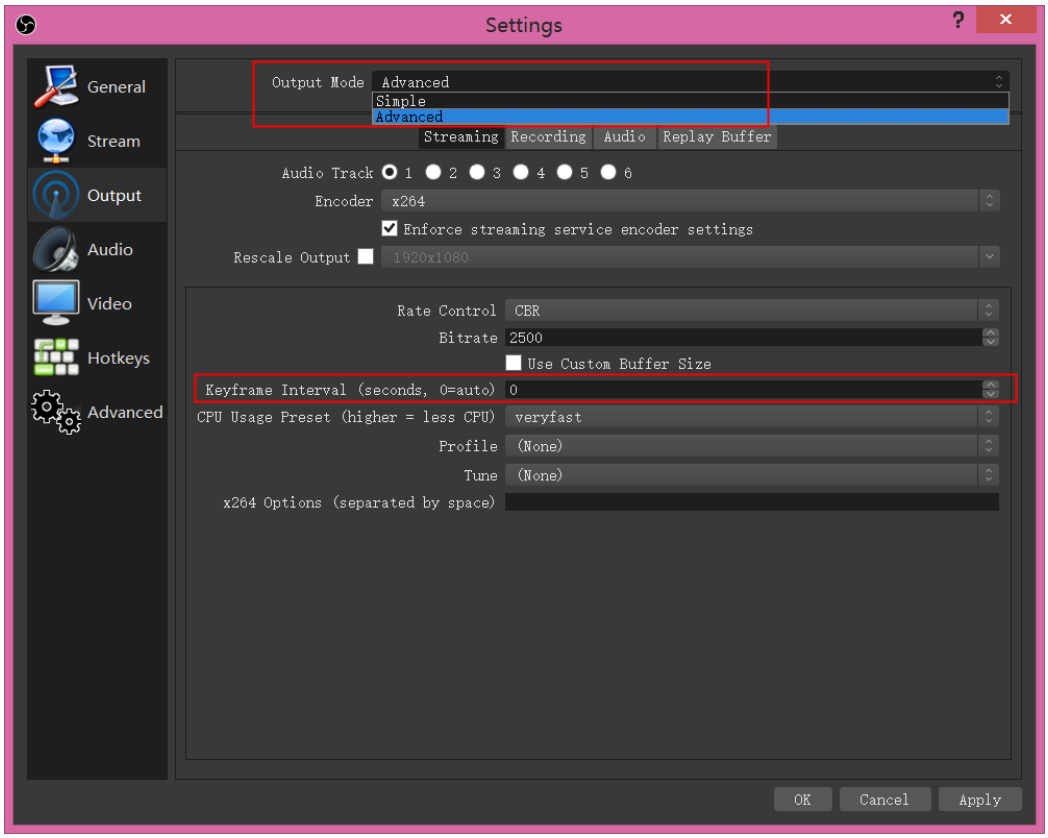
Figure 6-3 Viewing the ingest URL



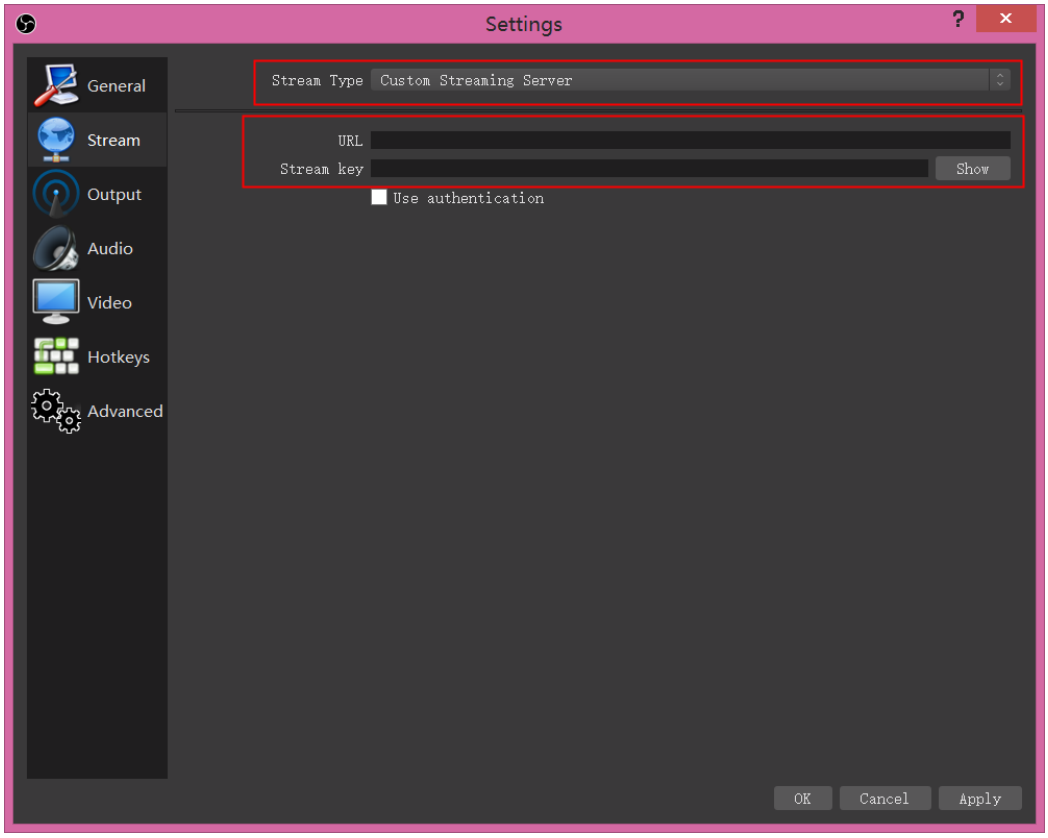
Step 2 Run OBS and click **Settings** in the lower right corner.



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



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



An ingest URL consists of the following two parts:

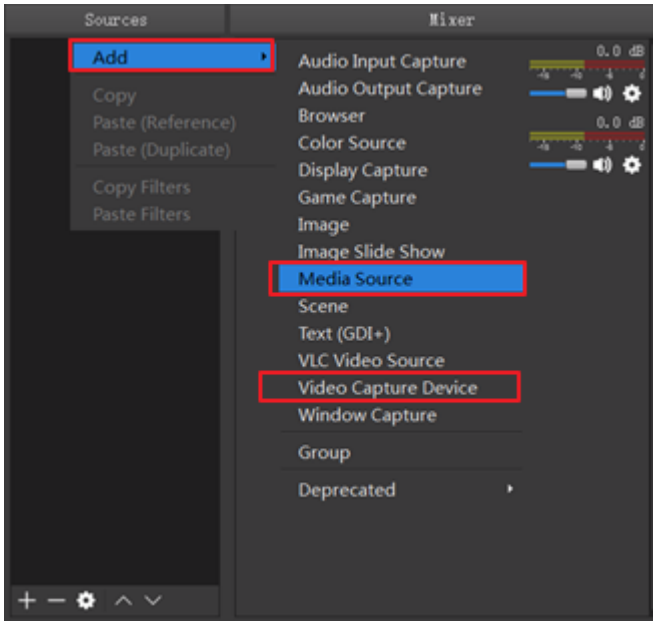
- **URL**: Enter the part from the beginning of the ingest URL to the ***AppName***, for example, **rtmp://live-push.example.com/live/**.
- **Stream Key**: Enter the URL containing ***StreamName***, for example, **huaweitest?request_source=ott&channel_id=huaweitest**.

NOTE

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

Step 5 Click **OK**.

Step 6 Right-click the **Sources** area, and add a stream source.



- **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.

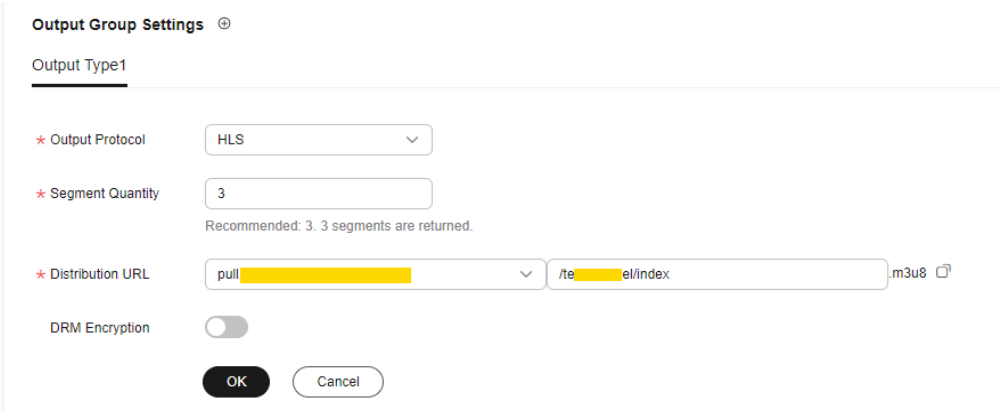
1. Log in to the Live console.
2. In the navigation pane on the left, choose **Media Live** > **Channel Management**. The **Channel Management** page is displayed.
3. Find the corresponding channel and click **Manage** on the right. The **Update Channel** page is displayed.

   View the streaming URL, as shown in **Figure 6-4**. Streaming URLs whose output protocol is HLS, DASH, or MSS can be assembled. Examples are as follows:

- HLS: http://live-play.example.com/live/huaweitest/index.m3u8
- DASH: http://live-play.example.com/live/huaweitest/index.mpd
- MSS: http://live-play.example.com/live/huaweitest.ism/manifest

The preceding example URLs use the HTTP protocol. Streaming URLs also support the HTTPS protocol. If you want to use a URL starting with **https://**, configure an HTTPS certificate by referring to **HTTPS Certificates**.

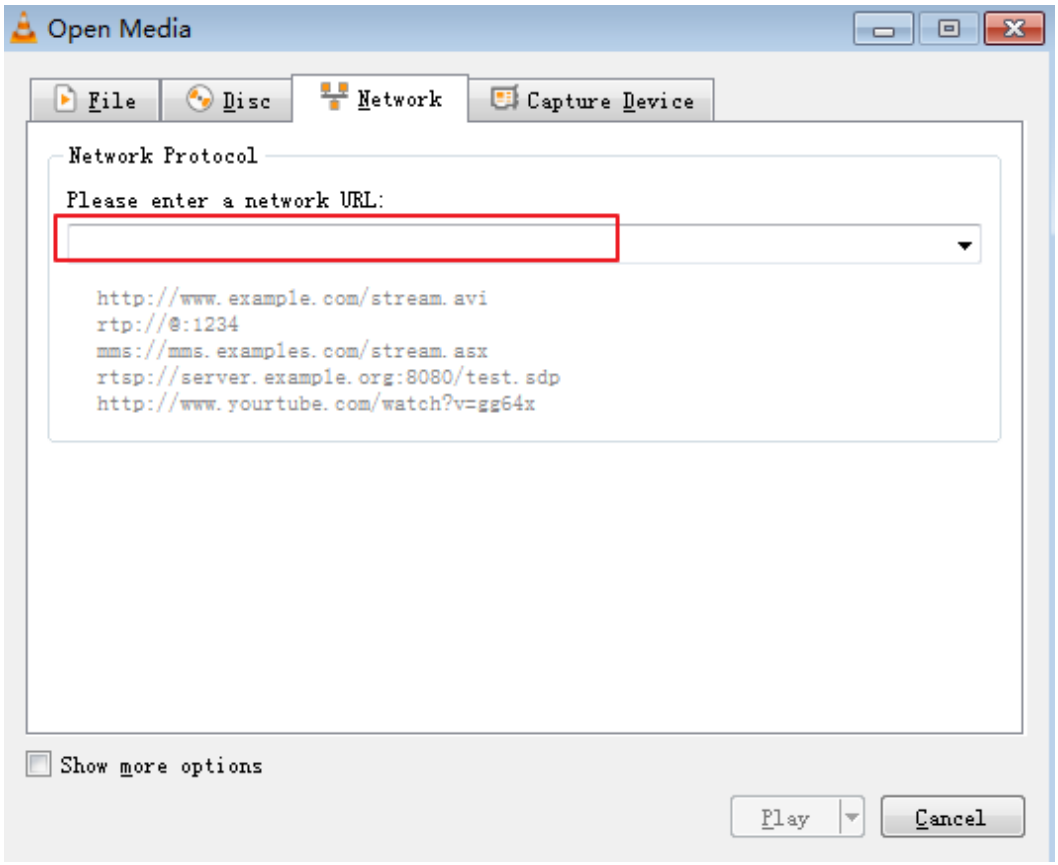
Figure 6-4 Viewing the streaming URL



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 **step 1**. Click **Play**.



----End

7 Console Operations

7.1 Prerequisites

Prerequisites

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

  NOTE

  If you are a **Huawei Cloud (International)** 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. Media Live requires an ingest domain name and a streaming domain name, and the two domain names must be different.

  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.

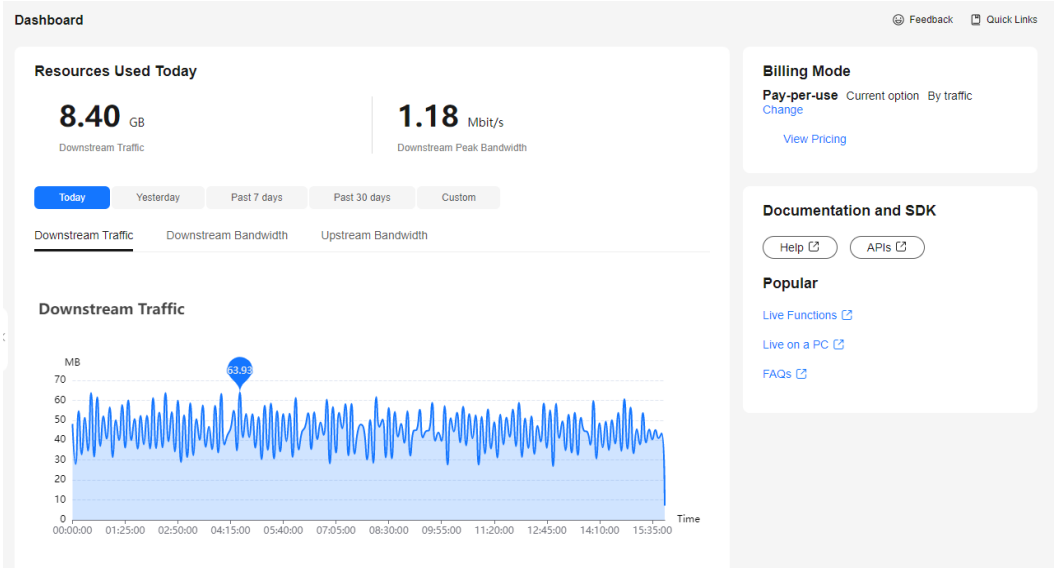
7.2 Functions of the Console

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 7-1 Dashboard



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

- **Today**
  - **Downstream Traffic**: Total downstream traffic used by all streaming domain names on the current day
  - Downstream peak bandwidth: Downstream peak bandwidth used by all streaming domain names on the current day
- The usage trend displays 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 peak 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 needs to start with **https://**, configure an HTTPS certificate by referring to **HTTPS Certificates**.
Channel Management	**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 ingest domain name needs to be configured for stream push.
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.
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 response, and number of downstream concurrent requests.
Tools	**Obtaining the Replay URL of a Channel**	You can obtain the replay 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 7-2**.

Notes

Permissions management is not performed on the following two types of Live users. To perform permissions management, **submit a service ticket**.

- 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.

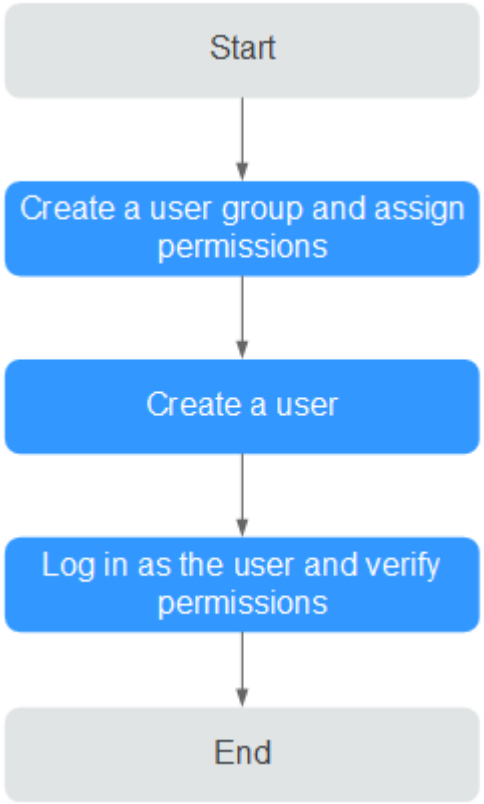
After **permissions management** is enabled, unauthorized **IAM users** cannot call the Live APIs. Ensure that IAM users have been assigned the Live permissions.

Prerequisites

Learn about the Live permissions that can be assigned to the user group and assign the permissions as required. For details, see the Live permissions listed in **Permissions Management**.

Process Flow

Figure 7-2 Process for assigning only read permissions on Live



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

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

2. **Create an IAM user and add it 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 using the created user, and verify that the user only has read permissions on Live.

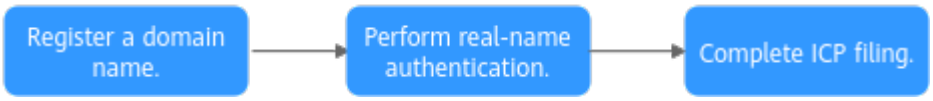
   Choose **Live** in **Service List**. Then click **Domains** to add a domain name. If a message is displayed indicating insufficient permissions for performing the operation, the **Live ReadOnlyAccess** policy has taken effect.

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 a domain name from 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. For details, see **Real-Name Authentication**.

   NOTE

   If you are a **Huawei Cloud (International)** 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 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

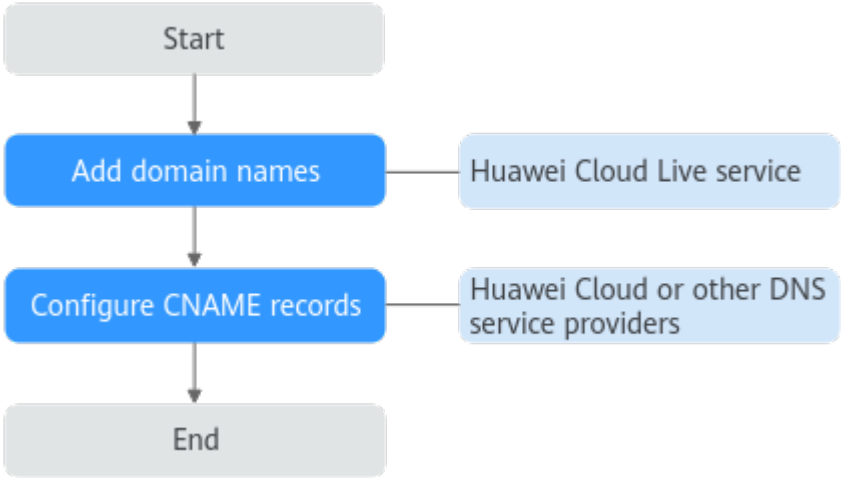
Before using Media Live, you must add ingest domain names and streaming domain names to Media Live.

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 7-3 shows the process of using your own domain name for livestreaming acceleration.

Figure 7-3 Admission process



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)** 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. Media Live requires an ingest domain name and a streaming domain name, and the two domain names must be different.

  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 acceleration 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.

Figure 7-4 Adding a domain name

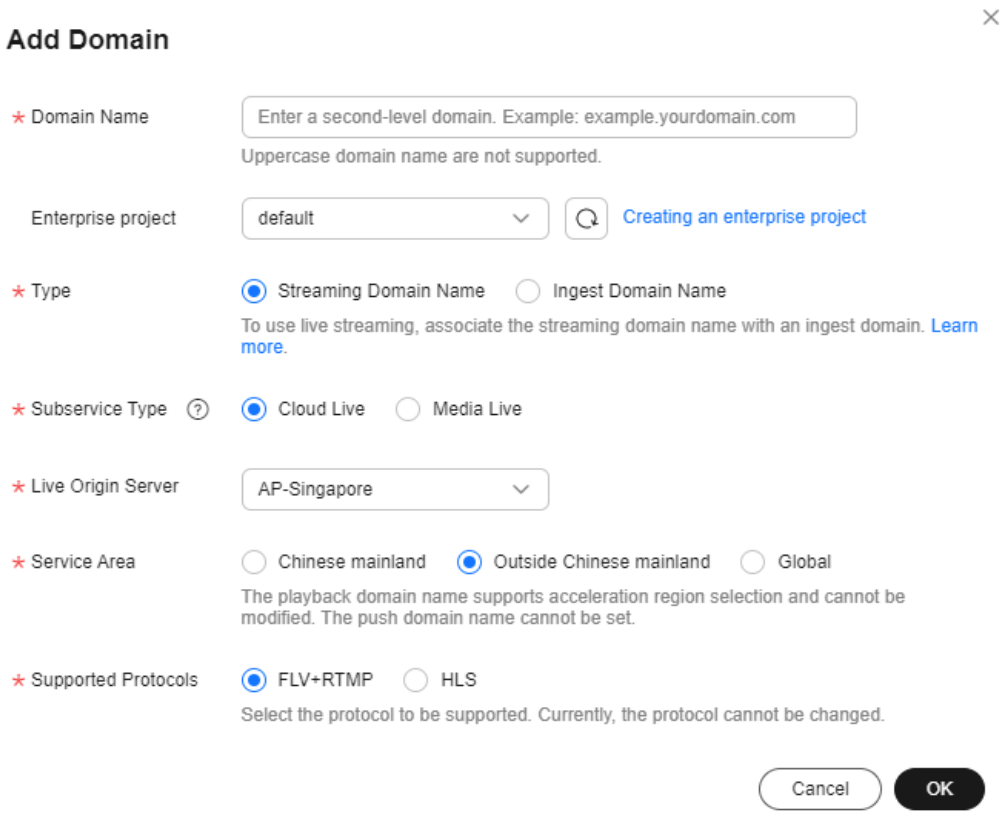


Table 7-3 Domain name parameters

Parameter	Description
Domain Name	Enter a second-level ingest domain name or streaming domain name. A domain name contains up to 42 characters and is case-insensitive. An ingest domain name must be different from a streaming domain name. Wildcard domains are not allowed. Example: test-push.example.com **NOTE** 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.
Enterprise Project	Add domain names to enterprise projects for unified management. Create an enterprise project by referring to **Creating an Enterprise Project**. The default enterprise project is named **default**. On the **Enterprise Project Management** page, **create an enterprise project** and **add a 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**.

Parameter	Description
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 and ME-Riyadh of Huawei Cloud (International) By default, this function is unavailable in ME-Riyadh. If you have additional requirements, **submit a service ticket** for technical support.
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: • **Chinese mainland** Select this option when the audience is in the Chinese mainland. The domain name must be licensed by the Ministry of Industry and Information Technology (MIIT). • **Outside Chinese mainland** Select this option when the audience is outside the Chinese mainland (including in Hong Kong, Macao, and Taiwan). • **Global** Select this option when there is audience in and outside the Chinese mainland (including in Hong Kong, Macao, and Taiwan). The domain name must be licensed by the Ministry of Industry and Information Technology (MIIT).
Supported Protocols	Media stream protocols supported by streaming domain names. The value cannot be changed once configured, and defaults to **FLV+RTMP**. Options: • **FLV+RTMP** • **HLS**

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 3** to **Step 4** to add an ingest domain name.

Step 6 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

- If your domain name is registered on the Huawei Cloud Domain Registration Service, configure the CNAME record by referring to the following **procedure**.
- If your domain name is not registered on the Huawei Cloud Domain Registration Service, configure the CNAME record following the guidance provided by your DNS service provider.
- 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.

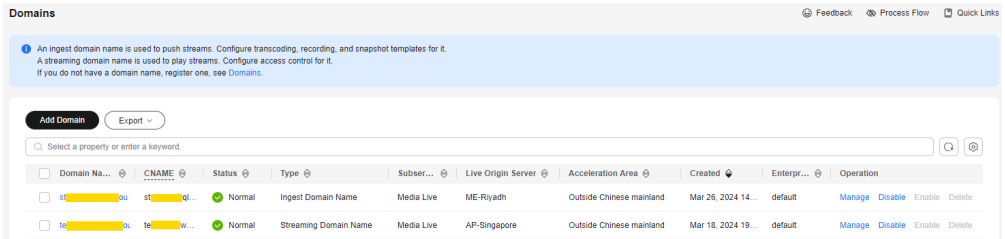
Procedure

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 7-5 Obtaining the CNAME record



Step 2 Log in to the **DNS console**.

Step 3 In the navigation pane on the left, select **Public Zone**. The domain name list page is displayed.

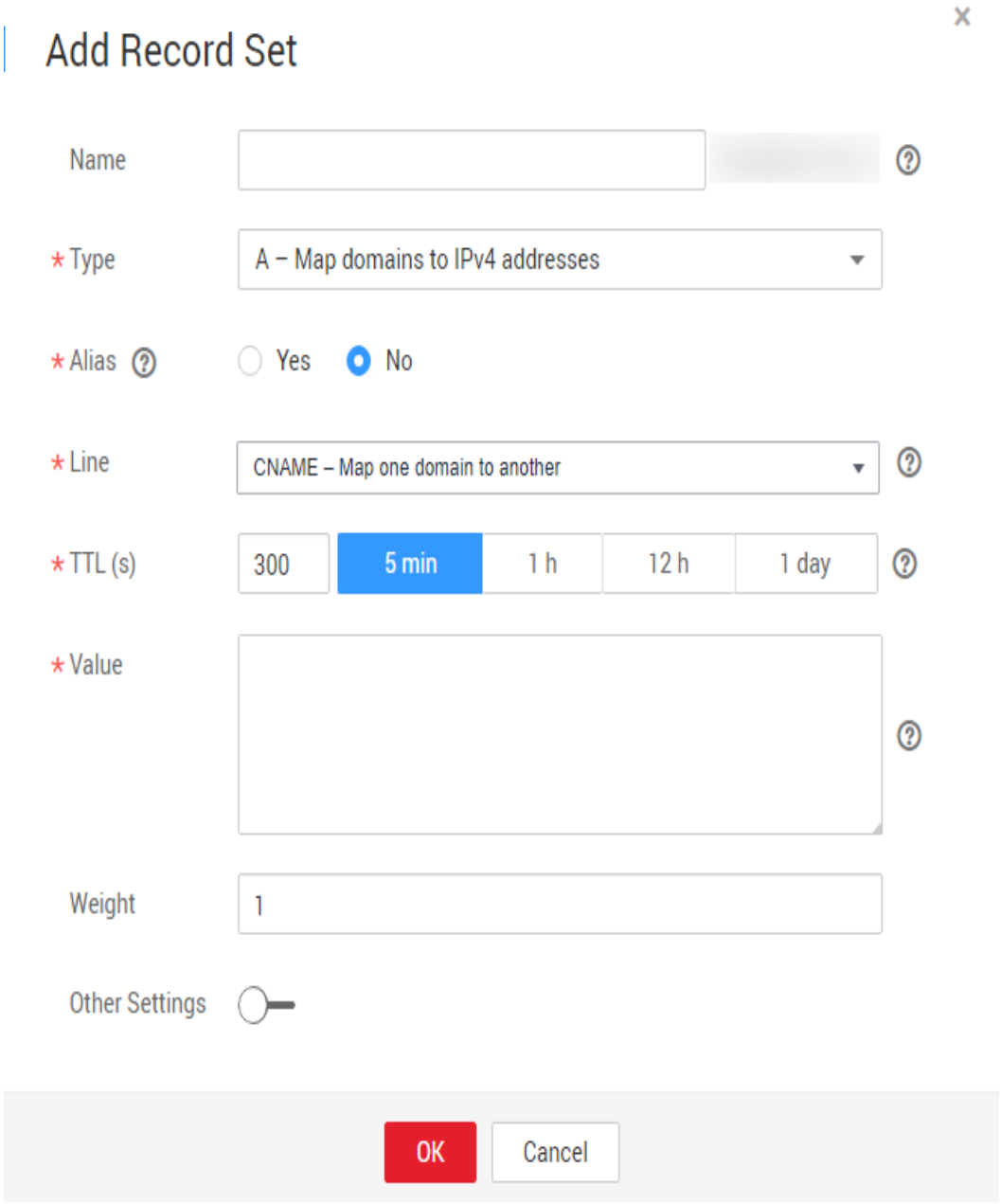
Step 4 Click the target domain name in the **Name** column.

Use the domain name **example.com** as an example. Locate the row containing **example.com**.

Figure 7-6 Domain name list

Step 5 In the upper right corner of the page, click **Add Record Set**.

Figure 7-7 Adding a record set



Configure the parameters as instructed by **Table 7-4**.

Table 7-4 Parameters

Parameter	Description	Example Value
Name	Enter the level-2 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**.

Parameter	Description	Example Value
Type	Type of the record set, which should be **CNAME-Canonical name** here	CNAME-Map one domain to another
Alias	Whether to associate the record set with a cloud resource name • **Yes**: Associate the record set with a cloud resource. For details, see **Record Set**. • **No**: Do not associate the record set with a cloud resource.	No
Line	Resolution line. The DNS server will return the IP address of the specified line based on the source of visitors. For details, see **Resolution Line**. The default value is **Default**. This parameter is supported only for public domain names.	Default
TTL (s)	Cache duration of the record set (unit: s) The smaller the value is, the quicker the record takes effective.	The default value is **5 min**. If there are no special requirements, retain the default value.
Value	Domain name to be pointed to, that is, the CNAME obtained in **1**	For example, if the streaming domain name is **play-test.example.com**, enter **play-test.example.com.c.cdnhwc3.com**.
Weight	(Optional) Weight of a record set. When multiple record sets of the same name and line are created in a zone, the one with a larger weight takes effect in priority. The default value is **1**. This parameter is supported only for public domain names. The value ranges from 0 to 100.	1
Tags	(Optional) Identifier of a record set. Each tag contains a key and a value. You can add 10 tags at most to a record set.	example_key1 example_value1

Parameter	Description	Example Value
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 7-8**.

Figure 7-8 Command output

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.

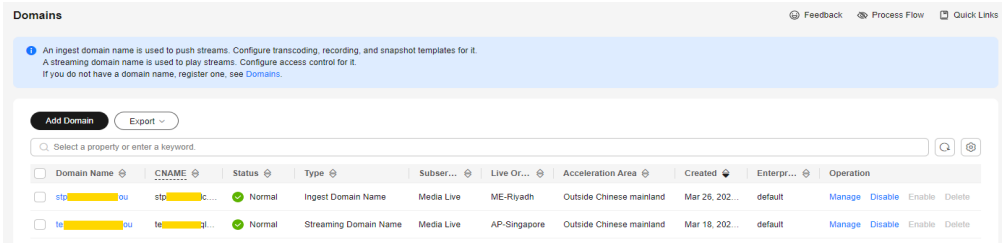
Step 2 In the navigation pane, choose **Domains**.

Step 3 Perform the following operations as required.

- View domain name details.

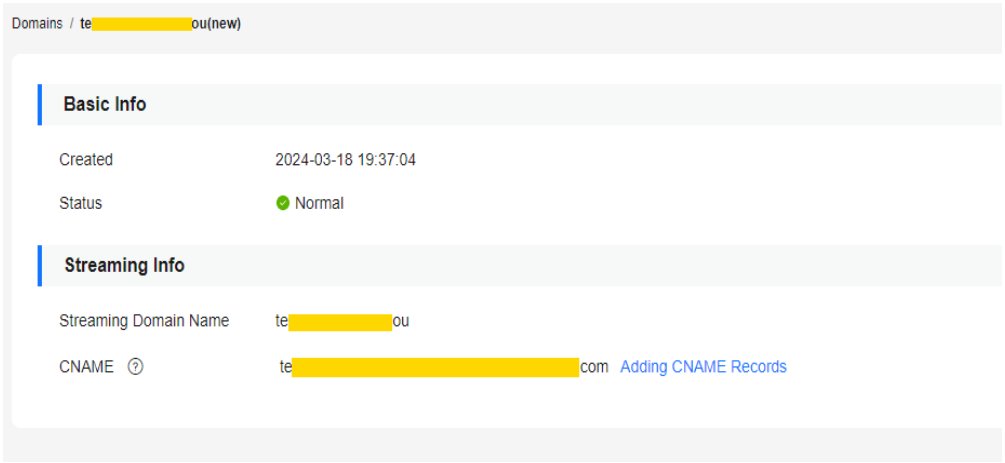
  In the domain list, you can view the CNAME record, type, status, and creation time of a domain name.

Figure 7-9 Domain status



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

Figure 7-10 Domain information



- 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 the Region Access Whitelist

By default, a user's IP address belongs to the acceleration region configured for the streaming domain name and can be used to access the Live service to pull

streams. To specify the regions that can be accessed by a streaming domain name, perform the operations described in this section.

Prerequisites

- The region access whitelist can only be configured for streaming domain names.
- Only one region access 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 region access needs to be specified and click **Manage** in the row of the domain name. The **Basic Info** page is displayed.

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

Step 5 Click **Add**. In the **Geo-blocking** dialog box that is displayed, select the regions that the current streaming domain name can access and add them to **Selected Area**.

Step 6 Click **OK**. The region access whitelist has been added.

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

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

----End

7.4.6 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**.

7.4.7 Playback Authentication

7.4.7.1 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 a denylist or allowlist to control who can use Live to play video.	For details, see **ACL**.

7.4.7.2 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 7-11 Configuring referer validation

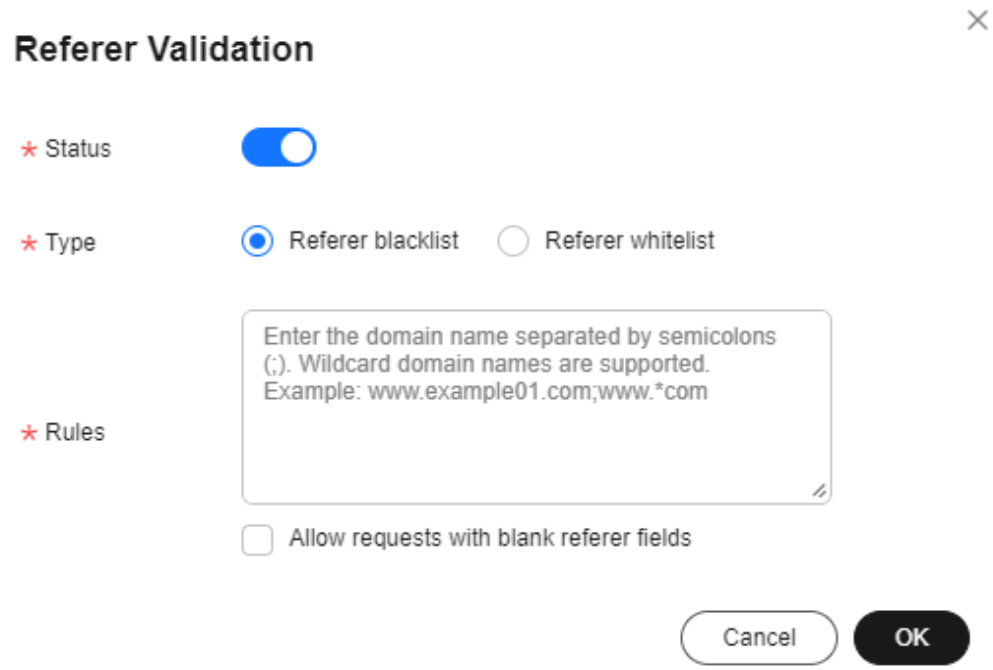


Table 7-6 describes the parameters.

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

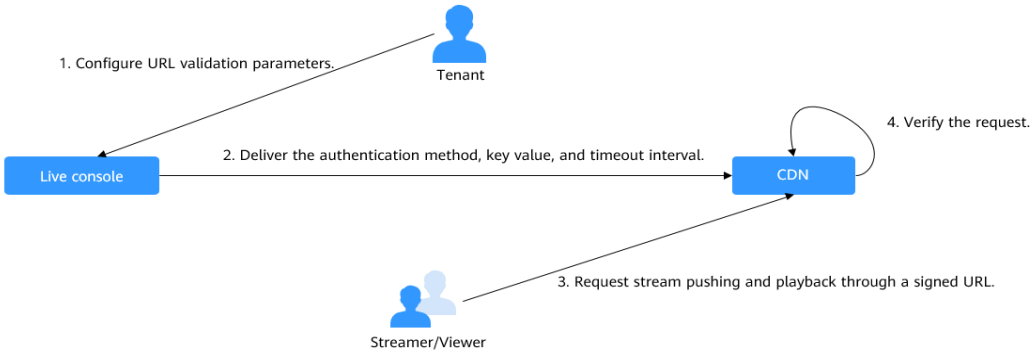
7.4.7.3 URL Validation

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 customer service.

Working Principle

Figure 7-12 URL validation working principles



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 7-13 Configuring URL validation

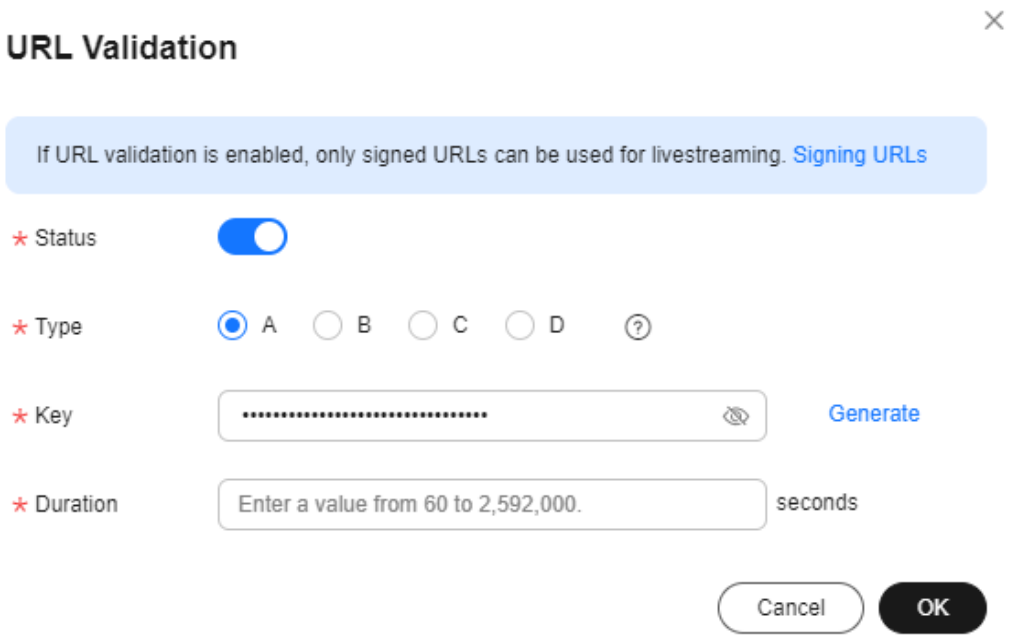


Table 7-7 URL validation parameters

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 in either of the following ways.

- Manually generate a signed URL based on the configured authentication type. For details, see **Signing Method A**, **Signing Method B**, **Signing Method C**, and **Signing Method D**.
- Use the tool to automatically generate a signed URL. For details, see **Signed URL Generation Tool**.

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 1800s, users can access the streaming URL within 1800s 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: 1800s
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 1249s, the streaming URL expiration time is the current time plus 1249s.

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: 1249s
```

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 1249s, the streaming URL expiration time is the current time plus 1249s.

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: 1249s
```

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();
    }

}
```

7.4.7.4 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 row containing the target streaming domain name.

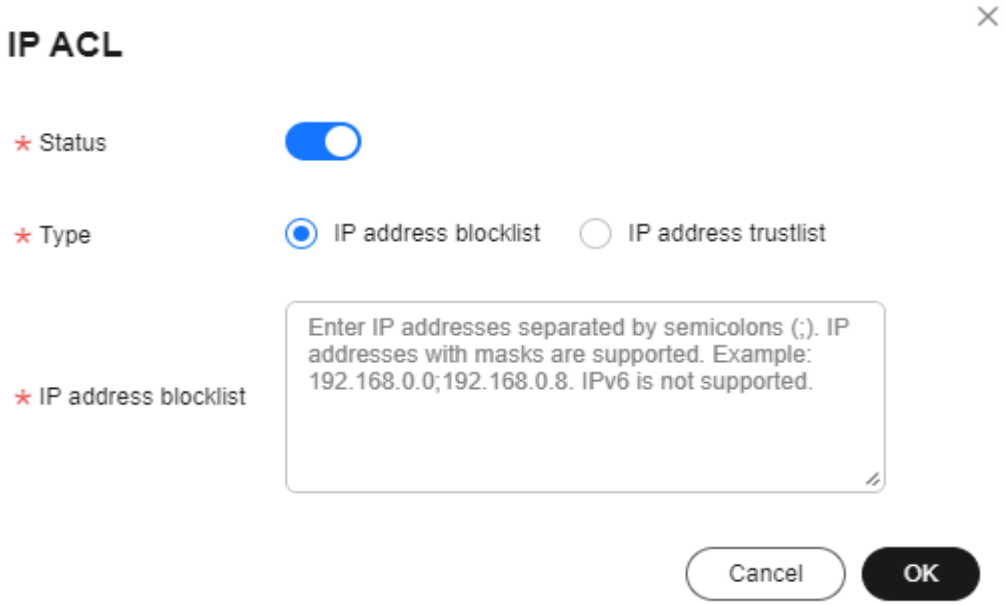
Set **Subservice Type** of the domain name to **Cloud Live**.

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 7-14 Configuring an ACL



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

7.4.8 HTTPS Certificates

7.4.8.1 Configuration Method

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

Context

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, go to the **SSL Certificate Manager** to buy an HTTPS certificate.
- 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.

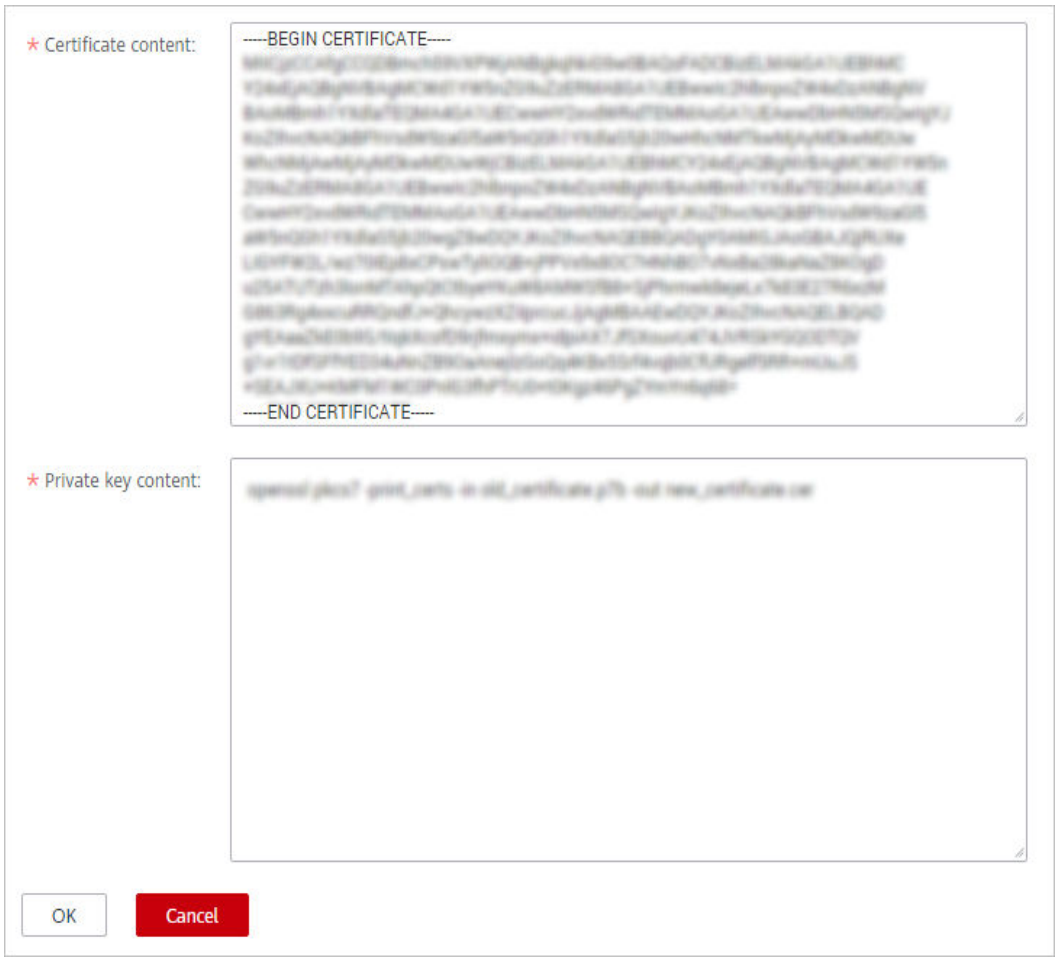
Step 2 In the navigation pane, choose **Domains**.

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 **Template Settings** > **HTTPS Certificate**.

Step 5 Click **Add**. On the page displayed, configure HTTPS parameters, as shown in **Figure 7-15**.

Figure 7-15 Configuring the HTTPS 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 7-16 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**.

Step 6 Click **OK**.

Step 7 Verify whether HTTPS secure acceleration has taken effect.

Use an HTTPS streaming URL to play a 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**.

7.4.8.2 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 7-17**.

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 7-17 A certificate in **PEM** format

```
-----BEGIN CERTIFICATE-----
MIIDxDCCAqygAwIBAgIEAJgGCTANBgkqhkiG9w0BAQUFADBuMQswCQYDVQQGEwJj
bjELMAkGA1UECAwCZ2QxCzAJBgNVBAcMAnN6MQswCQYDVQQKDAJodzELMAkGA1UE
CwwCaHcxGDAWBgNVBAMMD21OT0MgUm9vdCBDQSBWMjERMA8GCSqGSIb3DQEJARYC
aHcwHhcNMTYwNTE3MDEyODQ2WhcNMjEwNTE2MDEyODQ2WjBdMQswCQYDVQQGEwJj
bjELMAkGA1UECBMCZ2QxCzAJBgNVBAoTAmh3MQswCQYDVQQLEwJodzEUMBIGA1UE
AxQLKi5vd3Nnby5jb20xETAPBgkqhkiG9w0BCQEWAmh3MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909e
[redacted]
HRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZp
Y2F0ZTAdBgNVHQ4EFgQUmNstyLA+uGec0xx8f+XPLs3AiEUwHwYDVR0jBBgwFoAU
PRaAjcivt51G+7642KLZ+GbJTIQwDQYJKoZIhvcNAQEFBQADggEBABkMXMrUMhEH
ZNhbl9blt90NKQJpi7ugy7rj+vft4fUYeTvapsRwNutjWGVmnWB3HV85tnbIgVsa
0pP6yKbJ+mJhL5AB/crDMDMqGhywUEoG80kzEQJSeUHJ/R/iTaksmkqSPyDrbvaN
1DpIf5Sa7YA9VbWYpIZDuOhyk07HSZc8kcSmD+0K9gOke7QS1L3FKAvdgqJepeL6
A137VUmYTdh2mqS78LcpSs+SofipppOGgi5AuimZqp5xrn8Od6GjQqEc7nGH5foQ
1Jq8ekhn07Aqd7chFbDfW4qLSY7nEHT3uLzGME8Y9QQ4zs5H7lCaJVGXtoTQfpXR
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 7-18**.

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 7-18 A combined certificate

```
-----BEGIN CERTIFICATE-----
MIIE/DCCA+SgAwIBAgIUOWwvEj4lj5OamNabjVbGY42BBcQwDQYJKoZIhvcNAQEL
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]
AgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMEIGA1UdEQQ7MDmCE3d3dy5odWF3ZWlj
bG91ZC5jb22CESouaHVhd2VpY2xvdWQuY29tgg9odWF3ZWljbG91ZC5jb20wDQYJ
KoZIhvcNAQELBQADggEBACsLP7Hj+4KY1ES38OnOWuwQ3st8axvhDD9jZGoninzW
JSGpdmO4NEshlvwSFdEHpjy/xKSLCIqg5Ue8tTI8zOF13U0ROnMeHSKSxJG6zc8X
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
rRab4gVi14x+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 7-19**.

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 7-19 An RSA private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909eYlvLCqow
wEPqs6vyqQM3gKo8qCkNkmS5QgMPOFI4fx2G22mHvT0x8PHjm6GTQDPDniWaIuky
lufqVPD/zqK0oBl2AeAvbzKxWwRqf4JTLa3136B4l5yZVoDjRfU5EKY6LW1sD/00
5uF0qE3td5KQwQc6ZzbnkAof0Oyp5PbMfajM9My2mcvQJzWPLRxET3eWHYdBUtEg
1rxdrWxLheKjENzW3P7Mz/7KycIRxAlurl/Z9s8ytj3124AQY7NE1t1iL9wwA47k
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 Channel Management

7.5.1 Creating a Channel

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

Prerequisites

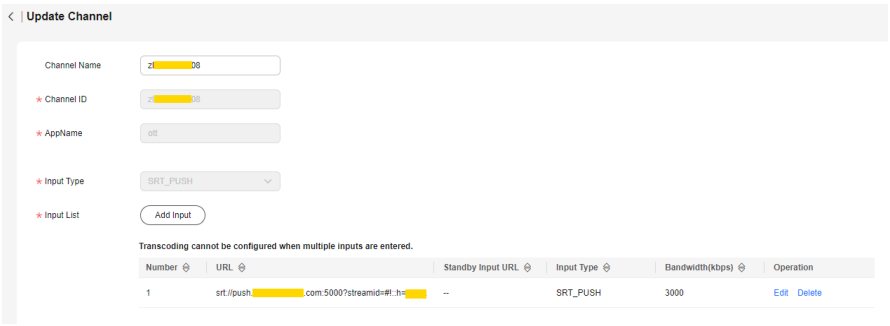
- **An ingest domain name has been added**.
- A live transcoding template has been created, as shown in **Creating a Transcoding Template**.

Constraints

- A tenant can create a maximum of 500 channels. To create more channels, **submit a service ticket**.
- Except for channels whose input type is **FLV_PULL**, all other channels allow only one input stream and can output streams of multiple bitrates only after transcoding.
- 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 7-20**.

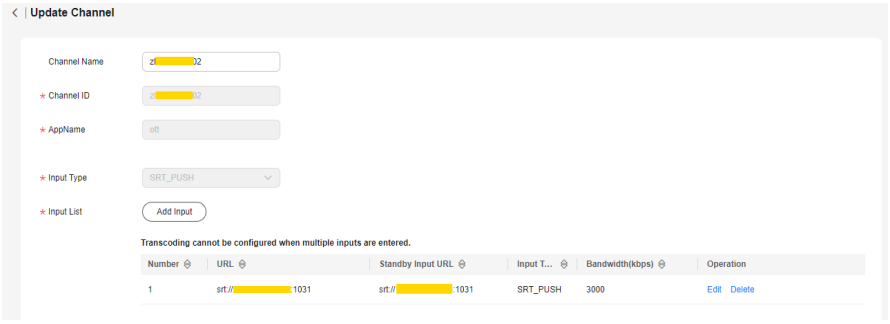
      To push streams to both the primary and standby regions, **submit a service ticket**.

Figure 7-20 Channel details



- If the encoder does not support *streamid*, both the primary and standby input URLs are returned, as shown in **Figure 7-21**.

Figure 7-21 Channel details



  - 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.

Creating a Channel

Step 1 Log in to the Live console.

Step 2 In the navigation pane on the left, choose **Media Live** > **Channel Management**.

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

Configure **Basic Info** as follows:

- **Channel Name**: Set the channel name.
- **Channel ID**: Set the channel ID.
- **AppName**: Application name, which defaults to **live** and cannot be changed.

Step 4 Click **Next**.

Configure parameters for adding inputs following **Table 7-12**.

Table 7-12 Parameters

Parameter	Description
Input Type	Input type of a channel media file. 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 ingest domain name needs to be configured for stream push.
Input List	Click **Add Input**. The **Add Input** dialog box is displayed. Configure the input list based on the selected input type: • If **Input Type** is set to **FLV_PULL**, configure the following parameters: – **URL**: Obtain the media stream URL from the channel provider. Media Live directly uses the URL to push streams to the origin server. – Then set **Bandwidth** (kbit/s). When **Input Type** is set to **HLS_PULL**, **Bandwidth** is unavailable. – **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 channel playback exception duration reaches the threshold, the system automatically switches to another URL for stream pull and playback. – You can set **Priority Settings** to **PRIMARY** (primary input URL) or **EQUAL** (switchover between primary and standby input URLs). • If **Input Type** is set to **RTMP_PUSH**, configure the following parameters: – Select the ingest domain name you added in **Adding Domain Names** from the drop-down list box. – Then set **Bandwidth** (kbit/s). After a channel is created, you can click **Manage** in the row where the channel is located to view the URLs in **Input List**. URL example: rtmp://live-push.example.com/live/huaweitest?request_source=ott&channel_id=huaweitest

Step 5 Click **OK**. The input list has been configured.

Step 6 Click **Next**.

Table 7-13 shows **Output Settings**.

Table 7-13 Parameters

Item	Parameter	Description
Transcoding	Transcoding Template	Select the Media Live transcoding template created in **Creating a Transcoding Template** from the drop-down list box. You can select multiple templates.
Other	Replay	If this function is enabled, you need to set **Max Replay Recording Time**, that is, the duration of the historical recorded content that users can view. Unit: second. For details about how to obtain a replay URL, see **Obtaining the Replay URL of a Channel**. **NOTE** • The OBS path for storing live recordings is *OBS address*/*push_domain*/*AppName*/*Channelid*. • After deleting channel A, use the ingest domain name, AppName, and channel ID of channel A to create channel B. If the recordings of channel A are not completely aged, the replay 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 default value is **4s**. The value must be an integer multiple of the GOP duration.
Output Group Settings **NOTE** You can click ⊞ on the right to add multiple output groups.	Output Protocol	Video transcoding output protocol. Options: • **HLS** • **DASH** • **MSS**: The MSS protocol is not displayed by default. To use it, **submit a service ticket**.
Output Group Settings	Segment Quantity	Recommended: • **HLS** or **DASH**: The recommended value is **3**, that is, three segments are returned. • **MSS**: The recommended value is **5**, that is, five segments are returned.

Item	Parameter	Description
	Distribution URL	Set **Distribution URL**, select a streaming domain name from the first drop-down list box, and enter the streaming URL in the second drop-down list box. After the assembling is complete, a new streaming URL is generated. Streaming URLs whose output protocol is HLS, DASH, or MSS can be assembled. Examples: • HLS: http://live-play.example.com/live/huaweitest/index.m3u8 • DASH: http://live-play.example.com/live/huaweitest/index.mpd • MSS: http://live-play.example.com/live/huaweitest.ism/manifest The preceding example URLs use HTTP. A streaming URL also supports HTTPS. If you want to use a URL starting with **https://**, configure an HTTPS certificate by referring to **HTTPS Certificates**. **NOTICE** • If **Input Type** is set to **RTMP_PUSH** in **Step 4**, the region of the configured streaming domain name must be the same as the region of the ingest domain name configured in **Input Type**. • If **Input Type** is set to **FLV_PULL** in **Step 4** and multiple output types are set, the regions of the streaming domain names of all output types must be the same.
	DRM Encryption	Used to enable DRM encryption. This parameter is not displayed by default. You need to **submit a service ticket** to obtain the parameter configuration permission. To enable it, configure the following parameters: • **DRM Type**: DRM encryption type • **DRM Vendor**: DRM encryption service vendor • **DRM Encryption Level**: The encryption key needs to be obtained from the DRM vendor. Options: – **content**: One channel has one specific DRM key. – **profile**: Each stream of a channel has one specific DRM key. • **DRM Content ID**: content ID of DRM • **KMS URL**: URL for obtaining the DRM key • **Token**: token used to obtain the DRM key URL

Step 7 Click **Finish**. A new line of channel content is displayed on the channel management page.

Step 8 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.
- Deleting a channel

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

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.
- In the **AP-Bangkok** region, **submit a service ticket** for review after configuring a template. The configuration takes effect only after it is approved.

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 **Media Live** > **Live Transcoding**.

Step 3 Click **Create Transcoding Template**. A page like **Figure 7-22** is displayed.

Configure transcoding parameters as instructed by **Table 7-14**.

Figure 7-22 Creating a transcoding template

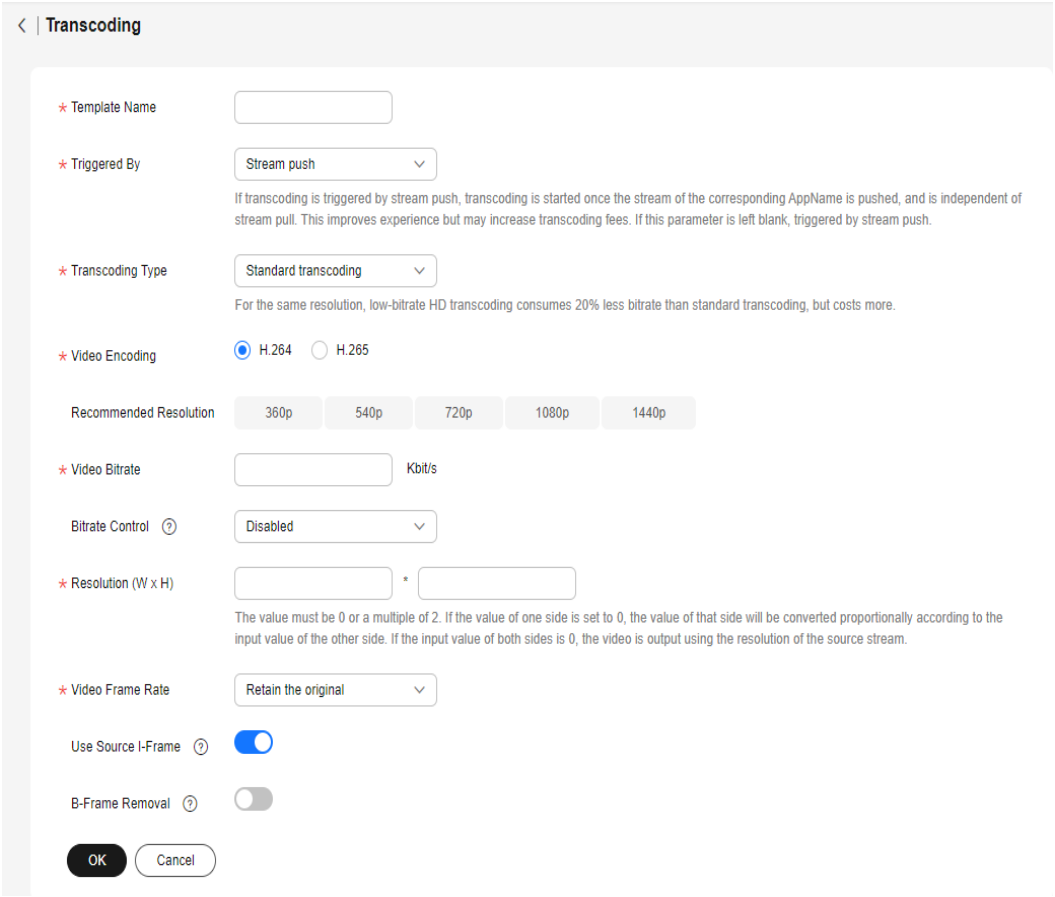


Table 7-14 Template parameters

Parameter	Description
Template Name	Name of a Media Live transcoding template. You can customize the name. Only letters, digits, underscores (_), and hyphens (-) are allowed.
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.

Parameter	Description
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 option, you will be billed based on the rates of low-bitrate HD. For details, see **Live Pricing Details**.
Video Encoding	Supported video encoding formats: • **H.264** • **H.265** **NOTICE** – Select only one encoding format for each channel.
Recommended Resolution	Display resolution. After the resolution level is selected, the **Video Bitrate** and **Resolution (W x H)** parameters are automatically set and the recommended values are provided. You can also change the values as needed.
Video Bitrate	Average bitrate of the transcoded video, in kbit/s. Value range: 40 to 30,000
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. That is, the bitrate does not increase. • **Adaptive to source stream**: The target bitrate is adaptive to the bitrate of the source file.

Parameter	Description
Resolution (W x H)	Width and height of the video, in pixel. If both the width and height are set to **0**, the output resolution is the same as the source resolution. If only the width or height is set to **0**, the output resolution will be scaled based on the value of the side that is not set to **0**. Value range: ● Width: 32 to 3,840. The value must be 0 or a multiple of 2. ● Height: 32 to 3,840. The value must be 0 or a multiple of 2.
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. If the value is set to **0**, the frame rate is adaptive.
Use Source I-Frame	Policy for outputting I-frames during encoding. Enable this function for Media Live. Options: ● If this function is disabled, I-frames are output based on the configured GOP duration. ● If this function is enabled, the output I-frames are the same as those of the source. That is, if the source contains I-frames, I-frames are output after encoding. If the source does not contain I-frames, non-I-frames are output after encoding. If this function is enabled, the GOP duration setting is invalid. For multi-bitrate transcoding, you are advised to enable **Use Source I-Frame** so that videos of different bitrates can have the same I-frame.
GOP Duration	I-frame interval by time, in seconds. The value ranges from 0 to 10 and defaults to **2**. If the value is not **0**, the I-frame interval is set based on the GOP duration. If the value is **0**, the default value is used. A larger GOP duration value indicates a longer livestreaming latency. A smaller GOP duration value indicates a higher probability of frame freezing.
B-Frame Removal	After this function is enabled, the transcoded video does not contain B-frames.

Step 4 Click **OK**.

A transcoding template is added 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

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 downstream concurrent requests.

Notes

The number system of bandwidth is 1024. For example, 1 Mbit/s is equal to 1024 Kbit/s.

Procedure

Step 1 Log in to the Live console.

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

Step 3 Select **Downstream Bandwidth/Traffic**, **Status Codes**, or **Downstream Concurrent Requests** 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).

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.
- Restrictions on the time granularity: If the query time span is no longer than 2 days, the 1-day granularity is not supported. If the query time span is longer than 2 days and no longer than 7 days, the 5-minute granularity is not supported. If the query time span is longer than 7 days, only the 1-day granularity is supported.

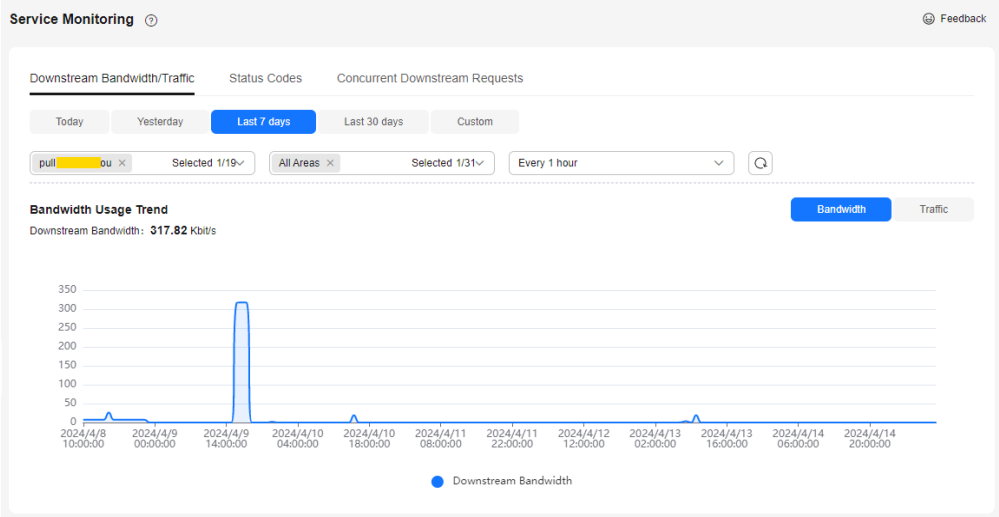
----End

Downstream Bandwidth/Traffic

Select the desired time, streaming domain name, area, and time 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 7-23**. **Downstream Bandwidth: 2.00 Mbps** indicates the downstream peak bandwidth of the selected domain name in the query period.

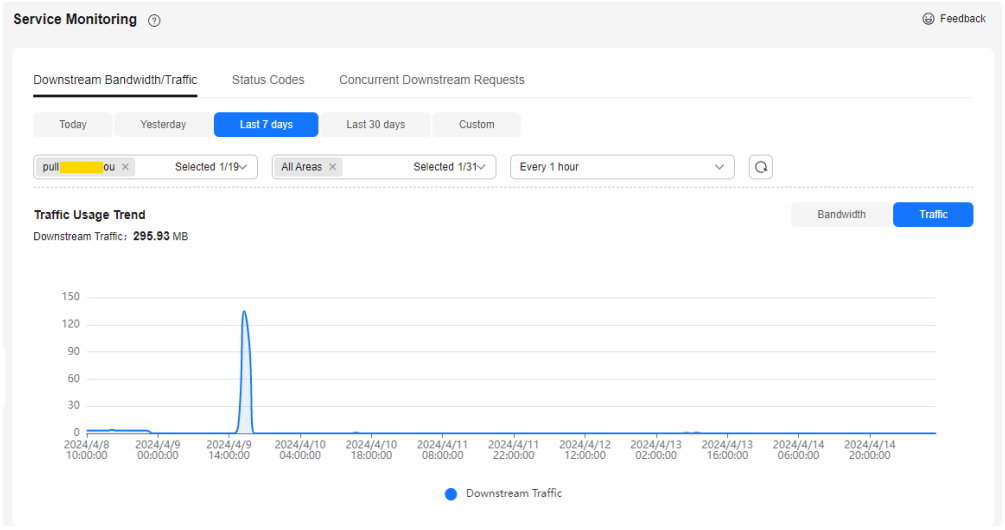
  Figure 7-23 Downstream bandwidth statistics



- **Traffic Usage Trend** displays the traffic usage trend of the selected domain name, as shown in **Figure 7-24**. **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 7-24 Downstream traffic statistics

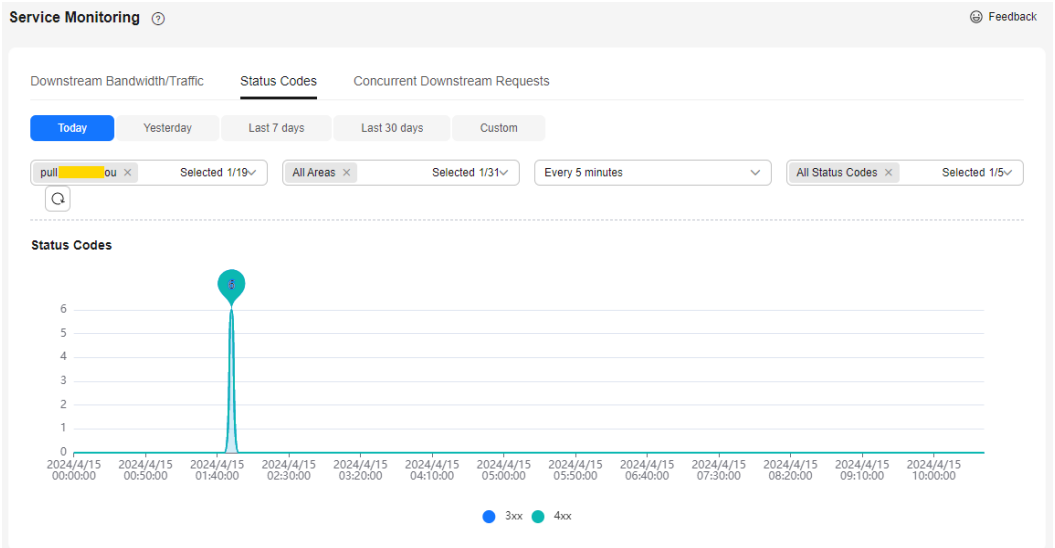


Status Codes

You can specify the time, streaming domain name, area, time granularity, and status code to view the trend chart of the corresponding status code, as shown in **Figure 7-25**.

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

Figure 7-25 Status code statistics

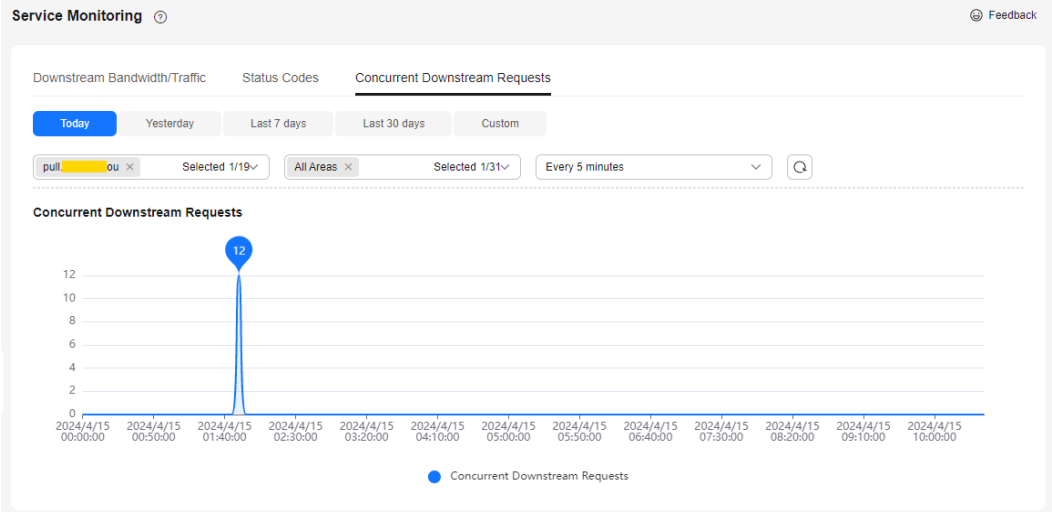


Downstream Concurrent Requests

You can specify the time, streaming domain name, area, and time 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 7-26 Downstream concurrent requests



7.8 Tools

7.8.1 Obtaining the Replay URL of a Channel

If you need to watch video replay on Media Live, obtain the replay URL of a channel by referring to this section.

Prerequisites

You have created a channel, as shown in **Creating a Channel**. The channel is running and the replay function has been enabled.

Procedure

Step 1 Log in to the Live console.

Step 2 In the navigation pane on the left, choose **Media Live** > **Tools** > **Replay URL Generation**.

The page shown in **Figure 7-27** is displayed. **Table 7-15** describes the required parameters.

Figure 7-27 Generating a replay URL

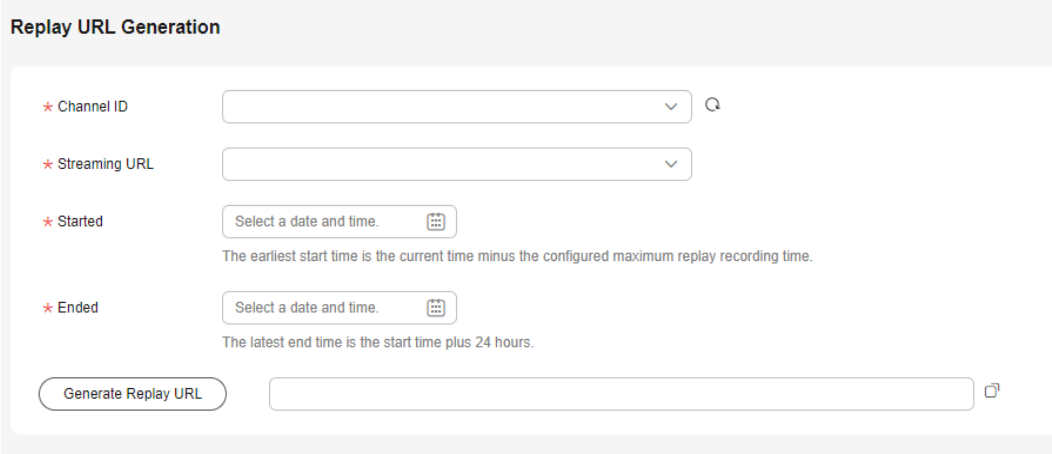


Table 7-15 Parameters

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 prevent deleted or modified channels from being displayed in the drop-down list box.
Streaming URL	Select the streaming URL of the channel from the drop-down list box.
Started	When the replay function is enabled for a channel, **Max Replay Recording Time** will be specified. You can watch replay only within the configured duration. 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.
Ended	A replay URL can be used to watch replay for a maximum of 24 hours. Therefore, the end time can be at most one day later than the start time.

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

The URL has been generated. You can click on the right to copy the URL and start the replay.

- If the 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 the replay function has been disabled for the channel.
- If **Max Replay Recording Time** is seven days, the replay URL you will obtain is the earliest day, and you need to watch the replay immediately. Otherwise,

the recordings generated before **Max Replay Recording Time** will be aged and cannot be played.

----End

7.9 Appendix

7.9.1 Signed URL Generation Tool

After configuring URL validation for an ingest domain name and a streaming domain name, you can use this tool to quickly generate signed URLs of the domain names.

Prerequisites

You have configured URL validation for your ingest and streaming domain names by referring to **Stream Authentication** and **URL Validation**.

Procedure

Step 1 Log in to the Live console.

Step 2 In the navigation pane, choose **Tools** > **URL Signing**.

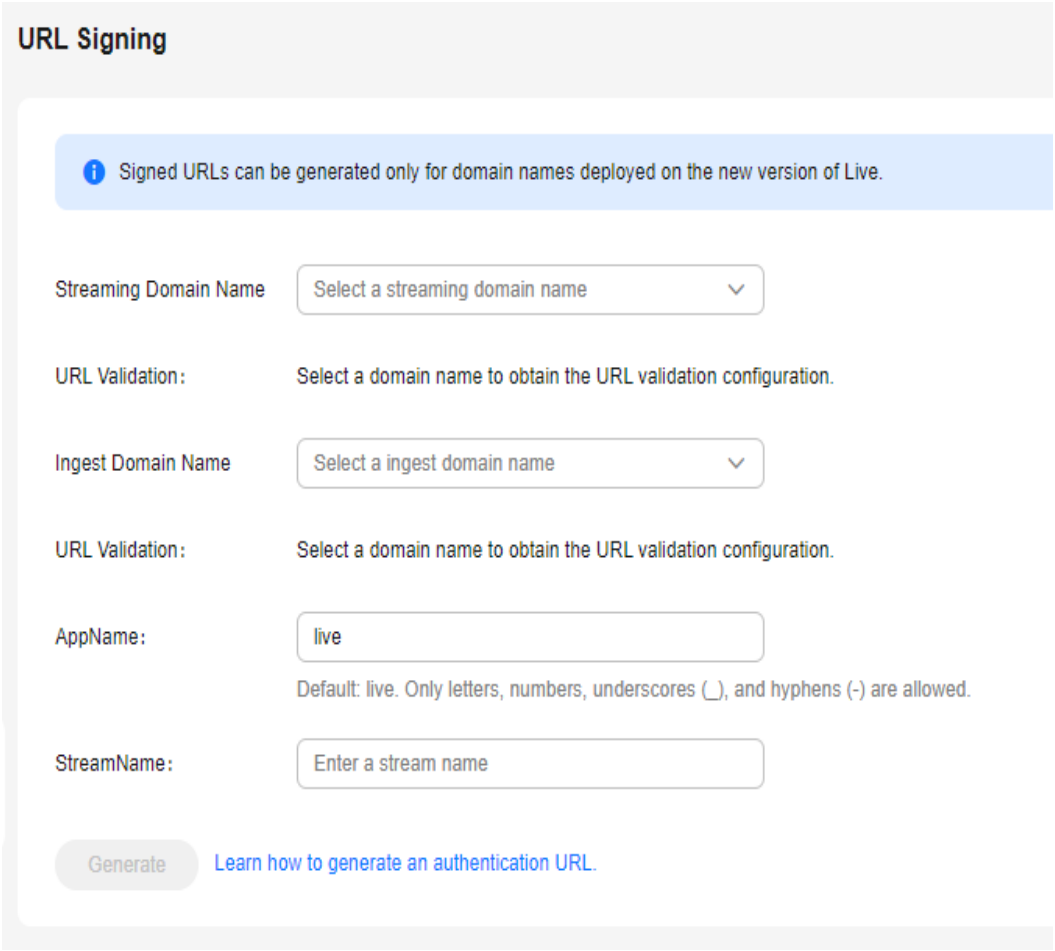
Step 3 Select the ingest domain name and streaming domain name for which a signed URL needs to be generated, and set **AppName** and **StreamName**.

You can generate a signed URL only for the streaming domain name or ingest domain name.

NOTE

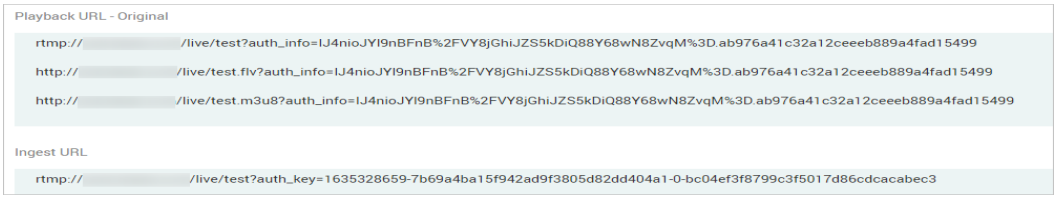
To generate a signed playback URL after transcoding, set **StreamName** to the value of *StreamName_Transcoding template ID*, for example, **huawei01_lld**. You can obtain the transcoding template ID on the **Transcoding** page of the Live console.

Figure 7-28 Generating a signed URL



Step 4 Click **Start generating** to generate the signed ingest and streaming URLs.

Figure 7-29 Signed URLs



----End

