

Media Live

User Guide

Issue 01
Date 2026-02-06



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Prerequisites	1
2 Permissions Management	3
2.1 Creating a User and Assigning Live Permissions	3
3 Domains	5
3.1 Domain Name Admission Standards	5
3.2 Domain Name Admission Process	7
3.3 Adding Domain Names	7
3.4 Configuring CNAME Records	12
3.5 Managing Domain Names	16
3.6 Configuring IPv6 Access	17
3.7 Configuring a Geo-blocking Whitelist	18
3.8 Verifying Domain Name Ownership	20
3.9 Stream Push and Playback Authentication	23
3.9.1 Overview	23
3.9.2 Referer Validation	24
3.9.3 URL Validation	26
3.9.4 IP Address ACL	37
3.10 HTTPS Certificates	39
3.10.1 Configuration Methods	39
3.10.2 HTTPS Certificate Requirements	43
4 Flows	48
4.1 Creating a Flow	48
4.2 Pushing Streams to a Third Party Through SRT	51
5 Channels	56
5.1 Creating a Channel	56
5.2 Managing Channels	79
6 Media Processing	82
6.1 Creating a Transcoding Template	82
6.2 Creating a Watermark Template	87
6.3 Creating a Watermark Rule	89
7 Service Monitoring	92

8 Cloud Resource Authorization	99
9 Tools	101
9.1 Obtaining a Catch-Up TV/Time-Shifted Viewing URL	101
9.2 Querying SCTE Signals	103
10 Third-Party CDN Interconnection (OBT)	106
10.1 Adding Domain Names	106
10.2 Creating a Channel	107
11 Video Bitrate Filtering	111
12 Appendix	116
12.1 Signed URL Generation Tool	116

1 Prerequisites

Registering with Huawei Cloud

- You have **registered** a HUAWEI ID, enabled Huawei Cloud services, and completed **real-name authentication**.

NOTE

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

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

NOTE

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

- When a new IAM user uses Media Live for the first time, they need to configure the permission to create a domain name.

Notes

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

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

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

2 Permissions Management

2.1 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 2-1](#).

Notes

You need to [submit a service ticket](#) to enable permissions management in either of the following cases:

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

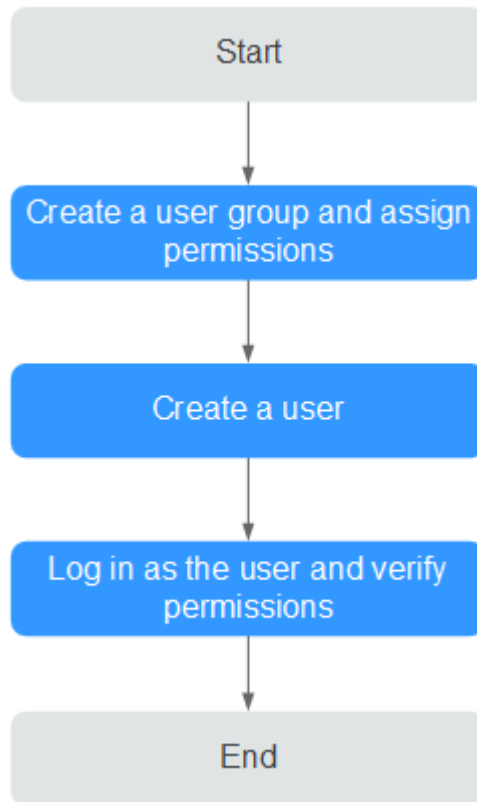
After [permissions management](#) is enabled, unauthorized [IAM users](#) cannot call the Live APIs. To gain access, they must be granted the corresponding Live permissions.

Prerequisites

Learn about the Live permissions that can be assigned to the user group and assign the permissions as required. For details, see the [system-defined permissions for Live](#).

Process Flow

Figure 2-1 Process for assigning read-only permissions on Live



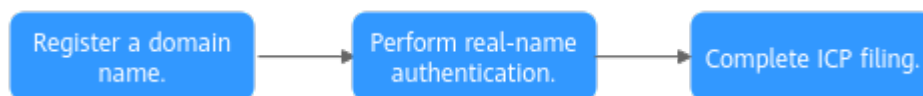
1. **Create a user group and assign permissions**
Create a user group on the IAM console, and attach the **Live ReadOnlyAccess** policy to the group.
2. **Create a user and add them to the user group**
Create a user on the IAM console and add the user to the group created in **1**.
3. **Log in** and verify permissions.
Log in to the Live console as the created user, and verify that the user only has read permissions on Live.
Choose **Live** in **Service List**. Then click **Domains** to add a domain name. If a message is displayed indicating insufficient permissions for performing the operation, the **Live ReadOnlyAccess** policy has taken effect.

3 Domains

3.1 Domain Name Admission Standards

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

Admission Process



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

NOTE

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

2. Perform real-name authentication: Log in to the [console](#) and complete real-name authentication for your account (individual or enterprise). For details, see [real-name authentication](#).

NOTE

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

- purchase and use cloud services on Huawei Cloud nodes in the Chinese mainland. In this case, real-name authentication is required by the laws and regulations of the Chinese mainland.
 - plan to use Live in regions in the Chinese mainland.
3. Complete ICP filing: If you want to perform livestreaming acceleration in Huawei Cloud regions in or outside the Chinese mainland, the domain names of Media Live must complete ICP filing in advance as required by the Ministry of Industry and Information Technology (MIIT).

Quantity Limit

By default, you can add up to 64 domain names in your account. If you have any special requirements, [submit a service ticket](#) to contact Huawei Cloud 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, fraud, 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 violates related laws and regulations, you shall bear the related risks.
- If any pornographic content or content related to gambling, illegal drugs, or fraud 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 3-1](#) describes the domain name rules.

Table 3-1 Domain name rules

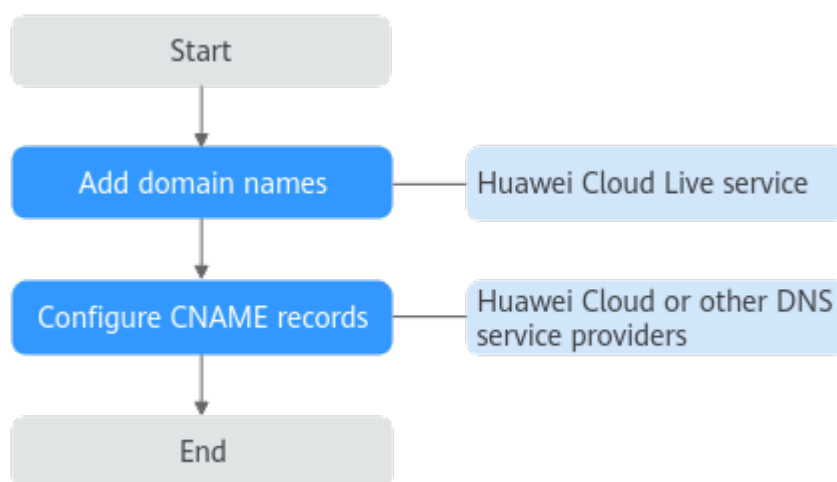
Domain Name Status	Rule
A domain name that has no access traffic for more than 90 days (the domain name is either working or malfunctioning)	The domain name will be automatically disabled, and the records related to the domain name will be saved. If you want to continue using the domain name, re-enable it .

Domain Name Status	Rule
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 .

3.2 Domain Name Admission Process

Figure 3-1 shows the process of using your own domain name for livestreaming acceleration.

Figure 3-1 Domain name 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 addresses allocated by Live point to your domain names.

3.3 Adding Domain Names

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

Prerequisites

- You have **registered** a HUAWEI ID, enabled Huawei Cloud services, and completed **real-name authentication**.

 NOTE

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

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

 NOTE

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

- When a new IAM user uses Media Live for the first time, they need to configure the permission to create a domain name.

Notes

- An area needs to be specified for stream push, and the streaming domain name needs to be associated with an ingest domain name. In this way, a streaming domain name can be used to watch livestreaming in the area where the ingest domain name is located. That is, a streaming domain name cannot be used to watch livestreaming in and outside China at the same time.
- The pricing for Live differs inside and outside the Chinese mainland. For details, see [Live Pricing Details](#).
- If the streaming URL is not used in the selected **Service Area**, the playback quality may be compromised.
- If the **Service Area** of the streaming domain name is **Chinese mainland** or **Global**, and the origin server of the ingest domain name is in the Chinese mainland, the domain names must be licensed in the Chinese mainland.
- Live may assign a default ingest domain name to you. Examples:
 - Ingest domain name format in the Chinese mainland:
{projectid}.hwcloudlive.com
Example: 0c283a271*****9459b6a.hwcloudlive.com
 - Ingest domain name format outside the Chinese mainland:
{projectid}.ott.huawei
Example: 0c283a271*****9459b6a.ott.huawei

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

Procedure

Step 1 Log in to the [Live console](#).

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

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

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

Figure 3-2 Adding a domain name

Add Domain ✕

Domain Name

Enter a value.

Uppercase domain names are not supported.

Enterprise Project

default ▼ 🔄 [Create](#)

Subservice Type ?

Cloud Live Media Live

Type

Streaming domain name Ingest domain name

Live Origin Server

CN North-Beijing4 ▼

Service Area

Chinese mainland Outside Chinese mainland Global

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

Cancel OK

Table 3-2 Parameters

Parameter	Description
Domain Name	<p>Enter a second-level ingest domain name or streaming domain name, for example, test-push.example.com.</p> <p>If the system displays a message indicating that you need to verify the domain name ownership after you enter the domain name, click View Verification Methods on the right and perform operations by referring to Verifying Domain Name Ownership.</p> <p>NOTE</p> <ul style="list-style-type: none">• A domain name can contain a maximum of 64 characters and cannot contain uppercase letters.• An ingest domain name must be different from a streaming domain name. Wildcard domains are not allowed.• By default, you can add up to 64 domain names in your account. If you need to add more domain names, submit a service ticket.• Domain names must be unique across all regions.
Enterprise Project	<p>Add domain names to enterprise projects for unified management.</p> <p>You can create an enterprise project or use the default one whose name is default. If you are using an IAM user, the user group that you are in must be authorized to manage the enterprise project. For details, see Authorizing a User Group to Manage an Enterprise Project. By doing so, users in this user group obtain the permissions on the domain names in the enterprise project.</p> <p>NOTE</p> <p>Only an enterprise account can configure enterprise projects.</p>
Subservice Type	<p>Subservice type of the Live service.</p> <p>Options:</p> <ul style="list-style-type: none">• 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. <p>Select Media Live.</p>
Type	<p>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.</p>

Parameter	Description
Live Origin Server	<p>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.</p> <p>Currently, Live is supported in the following regions:</p> <ul style="list-style-type: none">• CN North-Beijing4 of Huawei Cloud (Chinese Mainland)• AP-Singapore, ME-Riyadh, CN-Hong Kong, and AF-Johannesburg of Huawei Cloud (Singapore) Not available in ME-Riyadh and AF-Johannesburg by default. To use Live in these two regions, submit a service ticket for Huawei Cloud technical support.• Dublin of Huawei Cloud (Europe): EU-Dublin.
Service Area	<p>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.</p> <p>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.</p> <p>Options:</p> <ul style="list-style-type: none">• 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 the audience is 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). <p>NOTICE If the Service Area you select involves cross-border data transfer, you shall be responsible for such transfer. For details, see section 2.3 "Processing Your Content Data" of Live Service Agreement.</p>
Stream Push Protocol	<p>The parameter is displayed only when an ingest domain name is added.</p> <p>Stream push protocol of Media Live.</p> <p>Options:</p> <ul style="list-style-type: none">• RTMP: RTMP_PUSH channels require RTMP ingest domain names.• SRT: SRT_PUSH channels require SRT ingest domain names.

Step 4 Click **OK**.

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

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

For details, see [Configuring CNAME Records](#). Once the configuration takes effect, livestreaming acceleration is automatically enabled for the domain name.

----End

3.4 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 the domain name you added is on Huawei Cloud, configure the CNAME record following the [Procedure](#). If the domain name you added is not on Huawei Cloud, configure the CNAME record following the guidance provided by your domain name's DNS 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.

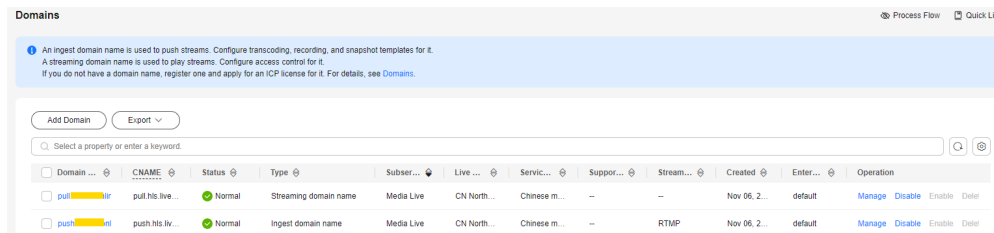
Procedure

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 3-3 Domains



The screenshot shows the 'Domains' management interface. At the top, there is a blue header with a warning icon and text: 'An ingest domain name is used to push streams. Configure transcoding, recording, and snapshot templates for it. A streaming domain name is used to play streams. Configure access control for it. If you do not have a domain name, register one and apply for an ICP license for it. For details, see Domains.' Below the header are 'Add Domain' and 'Export' buttons. A search bar contains the text 'Select a property or enter a keyword.' The main content is a table with the following columns: Domain, CNAME, Status, Type, Subser..., Live..., Servic..., Suppor..., Stream..., Created, Enter..., and Operation. Two rows are visible in the table:

Domain	CNAME	Status	Type	Subser...	Live...	Servic...	Suppor...	Stream...	Created	Enter...	Operation
pullhislive.com	pullhislive.com	Normal	Streaming domain name	Media Live	CN North...	Chinese m...	--	--	Nov 06, 2...	default	Manage Disable Enable Deler
pushhislive.com	pushhislive.com	Normal	Ingest domain name	Media Live	CN North...	Chinese m...	--	RTMP	Nov 06, 2...	default	Manage Disable Enable Deler

Step 2 Log in to the [DNS console](#).

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

Step 4 Click the target domain name in the **Domain Name** column, as shown in **Figure 3-4**.

Figure 3-4 Domain name list

You can create 48 more public zones.

Delete Batch Operation Export

Search or filter by domain name.

<input type="checkbox"/>	Domain Name	Status	Record Sets	Tag	Email	TTL (s)	Created	Last Mo...	Description	Operation
<input type="checkbox"/>	sc...	✔ Normal	4	--	hwclouds.cs...	300	Apr 17, 202...	Apr 17, 202...	--	Manage Record Set Disable More
<input type="checkbox"/>	w...	✔ Normal	2	--	hwclouds.cs...	300	Jun 20, 202...	Jun 20, 202...	--	Manage Record Set Disable More

Total Records: 2 10 < 1 >

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

Figure 3-5 Adding a record set

sc[redacted]com ×

Add Record Set

Type
CNAME – Map one domain to another

Name
Example: www .southamericatest.com

Line ?
Default

TTL (s) ?
300

Value ?
Example:
www.example.com

Advanced Settings (Optional)

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

Cancel OK

Configure the parameters by referring to [Table 3-3](#).

Table 3-3 Parameters

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

Parameter	Description
Name	Enter the second-level domain name. You do not need to enter the suffix. For example, if the streaming domain name is play-test.example.com , enter play-test .
Line	Used when the DNS server is resolving a domain name. It returns the IP address of the server according to the visitor source. For details, see Resolution Lines . This parameter is available only for public domain names. Select Default .
TTL (s)	How long a local DNS server caches the DNS record. It is measured in seconds. The smaller the value is, the quicker the record takes effective. The default value is 300 seconds. You can retain the default value.
Value	Domain name to be pointed to, that is, the CNAME address obtained in step 1 of this section. For example, if the streaming domain name is play-test.example.com , enter play-test.example.com.cdnhwc3.com .
Alias	Whether to associate the record set with a cloud resource. <ul style="list-style-type: none">• Enabled: The record set will be associated with a cloud resource.• Disabled: The record set will not be associated with a cloud resource. Toggle off the switch, that is, disable this function.
Weight	(Optional) Weight of a record set. The value ranges from 0 to 1000 and defaults to 1 . This parameter is available only for public domain names. If a resolution line in a zone contains multiple record sets of the same type, you can implement weighted routing by setting different weights for them. For details, see Configuring Weighted Routing . Set this parameter to 1 .
Tag	(Optional) Identifier of a record set. Each tag contains a key and a value. You can add up to 10 tags to a record set. For details about how to name a key and a value, see Adding a CNAME Record Set . Examples: <ul style="list-style-type: none">• example_key1• example_value1
Description	(Optional) Supplementary information about the domain name. You can enter up to 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 3-6**.

Figure 3-6 Command output

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

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

3.5 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.

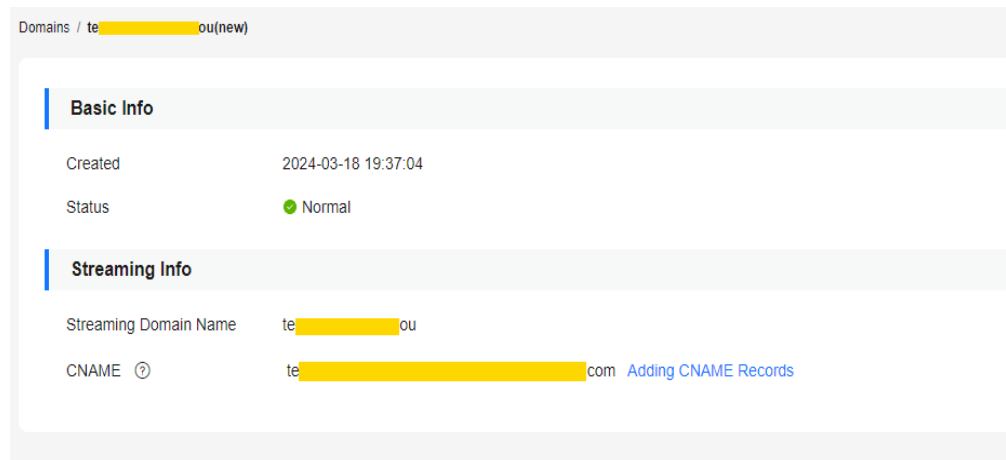
In the domain list, you can view the CNAME record, type, status, and creation time of a domain name.

Figure 3-7 Domains

Domain	CNAME	Status	Type	Subser...	Live...	Servic...	Suppor...	Stream...	Created	Enter...	Operation
pull.his.live	pull.his.live	Normal	Streaming domain name	Media Live	CN North...	Chinese m...	--	--	Nov 06, 2...	default	Manage Disable Enable Deler
push.his.lv	push.his.lv	Normal	Ingest domain name	Media Live	CN North...	Chinese m...	--	RTMP	Nov 06, 2...	default	Manage Disable Enable Deler

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

Figure 3-8 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

3.6 Configuring IPv6 Access

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

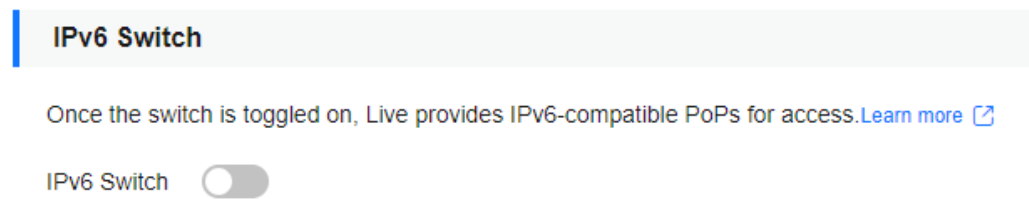
Notes

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

Procedure

- Step 1** Log in to the [Live console](#).
- Step 2** In the navigation pane, choose **Domains**.
- Step 3** Click **Manage** in the **Operation** column of the desired domain name. The **Basic Info** page is displayed.
- Step 4** Toggle on the IPv6 switch.

Figure 3-9 IPv6 switch



----End

3.7 Configuring a Geo-blocking Whitelist

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

Notes

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

Prerequisites

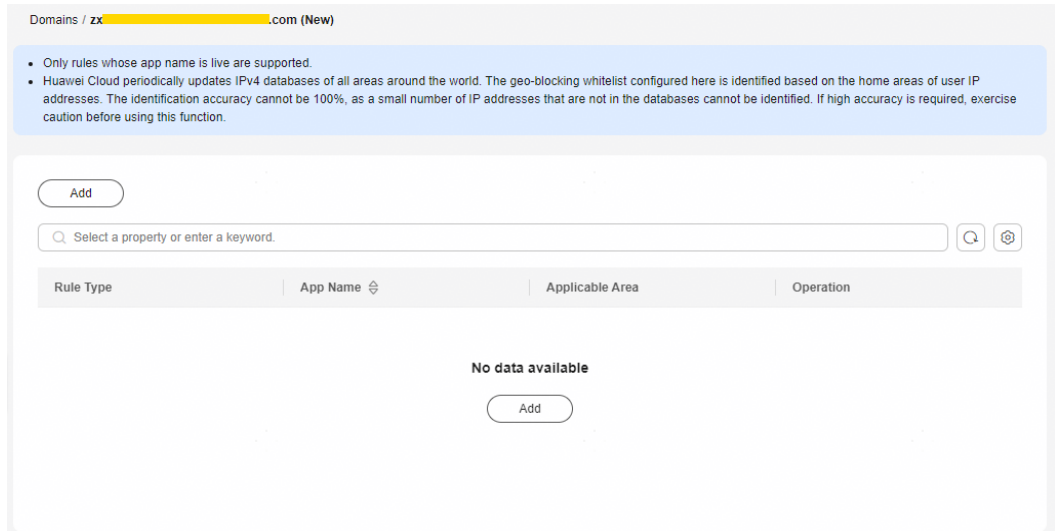
- A geo-blocking whitelist can only be configured for streaming domain names.
- Only one geo-blocking whitelist can be configured for each streaming domain name. The whitelist can be modified or deleted.

Procedure

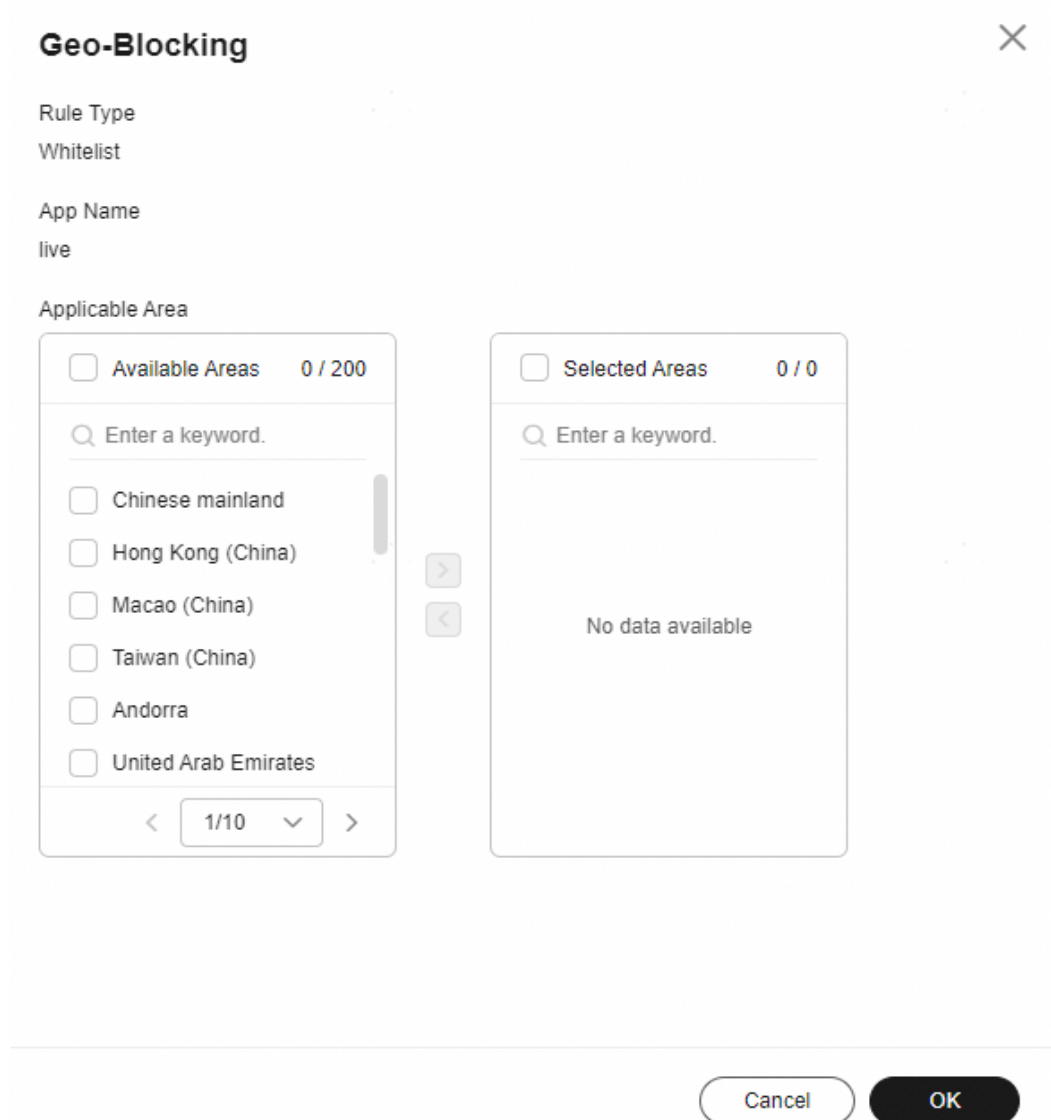
- Step 1** Log in to the [Live console](#).
- Step 2** In the navigation pane, choose **Domains**.

- Step 3** In the domain name list, find the streaming domain name whose geo-blocking needs to be specified and click **Manage** in the **Operation** column. The **Basic Info** page is displayed.
- Step 4** In the navigation pane, choose **Templates > Geo-blocking**, as shown in [Figure 3-10](#).

Figure 3-10 Geo-blocking



- Step 5** Click **Add**. In the **Geo-blocking** dialog box displayed on the right, select the areas where the streaming domain name can work and add them to **Selected Areas**, as shown in [Figure 3-11](#).

Figure 3-11 Geo-blocking

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

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

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

----End

3.8 Verifying Domain Name Ownership

When you add a domain name (for example, test.testlive.com) to Live for the first time, you must first verify the ownership of the root domain name (testlive.com). You can do this using either DNS- or file-based verification. The domain name can be added only after the verification is successful. Once the root domain is verified,

you can add other subdomain names (for example, testlive.com) of the same level without additional ownership verification.

Notes

Even if a domain name has been verified in an account, you must complete the verification process again when adding it to a different account.

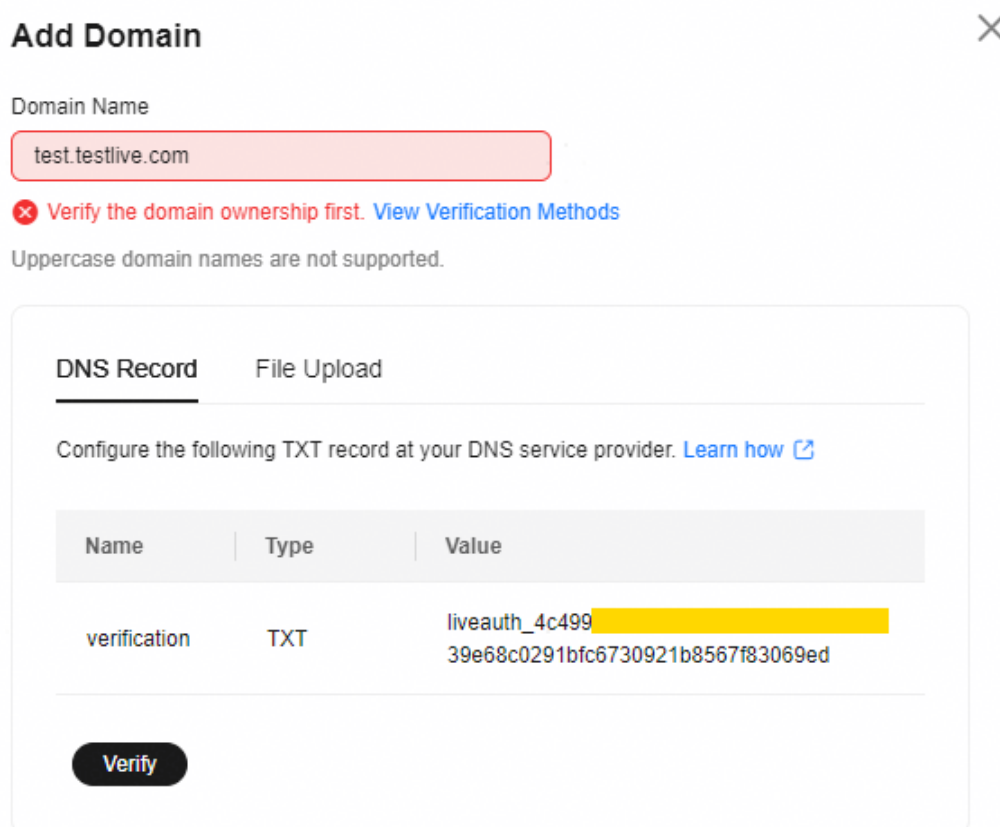
DNS Record-based Verification

The following uses test.testlive.com to illustrate the verification process.

Step 1 When you add a domain name to Live, if the system displays a message, asking you to verify the domain name ownership, click **View Verification Methods** and select **DNS Record**.

Do not close the verification page before the verification is complete.

Figure 3-12 Verifying the domain name ownership



Step 2 Configure a TXT record at your DNS provider.

The following uses Huawei Cloud as an example. The steps are the same for domains managed by other DNS providers, such as Wanwang, DNSPod, Xinnnet, and GoDaddy.

1. In the service list, choose **Networking > Domain Name Service**.
2. In the navigation pane, choose **Public Zones**.

3. Click **test.testlive.com**. In the upper right corner of the domain name details page, click **Add Record Set**.
 - **Name: verification**
 - **Type: TXT – Specify text records**
 - **Value:** Enter the value shown in **Figure 3-12**. The value is a 32-character string.
4. Click **OK** to add the record. It takes about 5 minutes for the TXT record to take effect.

Step 3 After the TXT record takes effect, return to the page for adding the domain name on the Live console and click **Verify** to validate the domain ownership.

----End

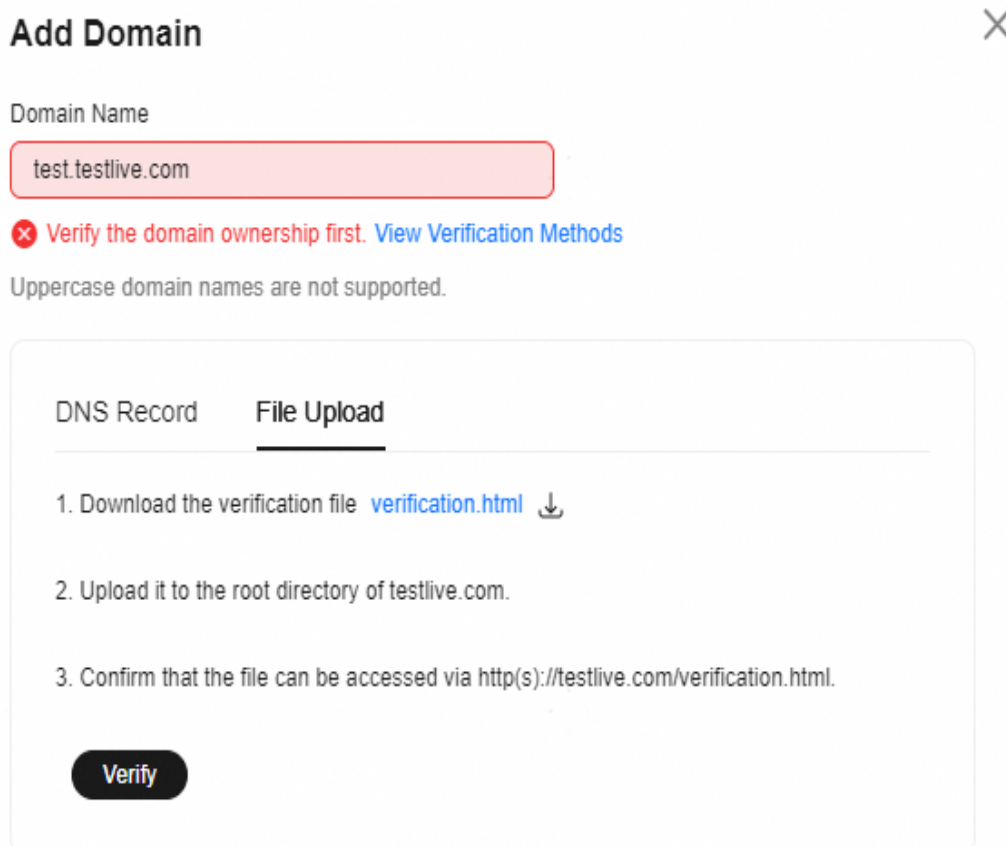
File-based Verification

The following uses test.testlive.com as an example to describe the verification process.

Step 1 When you add a domain name to Live, if the system displays a message, asking you to verify the domain name ownership, click **View Verification Methods** and select **File Upload**.

Do not close the verification page before the verification is complete.

Figure 3-13 Verifying the domain name ownership



Step 2 Download the **verification.html** file.

Step 3 Upload the file to the root directory of your domain server.

Ensure that the verification file can be accessed through <http://testlive.com/verification.html> or <https://testlive.com/verification.html>.

Step 4 Click **Verify**. Live will then access <http://testlive.com/verification.html> or <https://testlive.com/verification.html> to obtain the verification file.

If the system verifies that the obtained file is correct, the verification is successful.

----End

3.9 Stream Push and Playback Authentication

3.9.1 Overview

Stream Push Authentication

Media Live provides multiple authentication methods, including URL validation and IP address access control list (ACL), to prevent livestream resource theft. If multiple authentication methods are configured, livestream resources can be accessed only after the access request is approved by all the authentication methods.

The method of configuring stream push authentication is the same as that of configuring playback authentication. For details, see [URL Validation](#) and [IP Address ACL](#).

Note:

- By default, URL validation is not displayed. To use it, [submit a service ticket](#) to apply for the permission.
- If the stream push protocol of an ingest domain name is SRT, the configuration page of URL validation and ACL will be invisible. If you want to enable URL validation for an SRT ingest domain name, you can configure **CIDR IP Whitelist** and **Primary Input Decryption Parameters** (with **Decryption** enabled) when creating a channel. For details, see [Creating a Channel](#).

Playback Authentication

Media Live provides referer validation, URL validation, and IP address ACL to identify and filter out malicious visitors. Only authenticated visitors can use Media Live.

URL validation protects Live origin server resources from unauthorized download and theft. Referer validation uses referer blacklists/whitelists to prevent hotlinking. However, this method is not recommended as the referer content can be forged. You are advised to use URL validation. [Table 3-4](#) shows the authentication methods of Media Live.

Table 3-4 Authentication methods

Authen tication Method	Description
Referer Validation	You can configure a referer blacklist and whitelist to identify and filter out malicious visitors.
URL Validation	You can configure a key and validate the URL to protect your livestream resources.
IP Address ACL	You can configure an IP address blacklist and whitelist to identify and filter out malicious visitors.

3.9.2 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 1,000 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 enter `^http://test*.com$`, `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** Click **Edit** on the right of **Referer Validation**. The **Referer Validation** dialog box is displayed.
- Step 6** Toggle on the **Status** switch to configure related parameters, as shown in [Figure 3-14](#).

Figure 3-14 Configuring referer validation

Referer Validation

✕

⚠ Modifying the referer validation may cause livestream exceptions. Exercise caution when performing this operation.

Status

Type

Referer blacklist
 Referer whitelist

Rule

Enter domain names or regular expressions separated by semicolons (;). Example:
www.example01.com;www.*com

Allow requests with blank referer fields

Cancel

OK

See [Table 3-5](#).

Table 3-5 Referer validation parameters

Parameter	Description
Type	<p>The blacklist and whitelist are supported.</p> <ul style="list-style-type: none"> 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. <p>You can set whether to allow requests with a blank referer field, that is, whether to allow access through the browser address bar.</p>
Rule	<p>Domain names in the blacklist or whitelist.</p> <ul style="list-style-type: none"> You can input 1 to 100 domain names. Use semicolons (;) to separate domain names. Domain names are matched using regular expressions. If you enter <code>^http://test*.com\$</code>, <code>http://test.example.com</code> and <code>http://test.example01.com</code> are also matched.

Step 7 Click **OK**.

----End

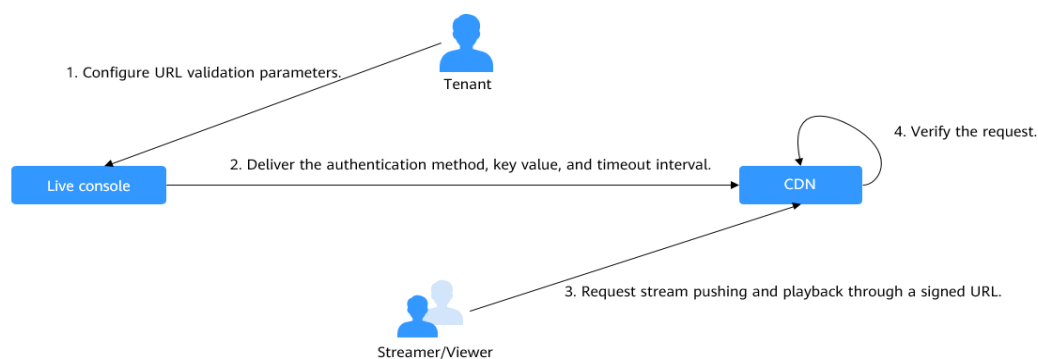
3.9.3 URL Validation

To prevent livestream 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 livestream is pushed or a viewer requests playback, CDN verifies the encrypted information in the URL. Only verified requests can be approved, and other illegitimate requests are rejected.

If you have other requirements on custom validation rules, [submit a service ticket](#) for Huawei Cloud technical support.

Working Principle

Figure 3-15 URL validation working principles



The process is as follows:

1. A tenant enables URL validation on the Live console and configures the signing method, key, and duration.
2. The configured signing method, key, and duration will be sent to a CDN PoP.
3. The streamer or viewer requests CDN to push streams or play video through the signed ingest or streaming URL.
4. CDN verifies the request based on authentication information in the URL. Only verified requests can be handled.

Notes

- By default, URL validation is not displayed. To use it, [submit a service ticket](#) to apply for the permission.
- 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 following rules.
- URL validation for streaming domain names supports only signing method D, which supports only HLS and does not support DASH or MSS.

- If the stream push protocol of an ingest domain name is SRT, the configuration page of URL validation and ACL will be invisible. If you want to enable URL validation for an SRT ingest domain name, you can configure **CIDR IP Whitelist** and **Primary Input Decryption Parameters** (with **Decryption** enabled) when creating a channel. For details, see [Creating a Channel](#).
- Use different keys for stream push 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 3,600 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 Click **Edit** on the right of **URL Validation**. The **URL Validation** dialog box is displayed.

Step 6 Toggle on the **Status** switch to configure related parameters, as shown in [Figure 3-16](#).

An ingest domain name supports four signing methods (A, B, C, and D), while a streaming domain name supports only signing method D. The following figure uses an ingest domain name as an example.

Figure 3-16 Configuring URL validation

URL Validation

✕

⚠ Modifying the URL validation may cause livestream exceptions. Exercise caution when performing this operation.

i If URL validation is enabled, only signed URLs can be used for livestreaming.
[Signing URLs](#)

Status

Type

A B C D

Key

Generate

When selecting a new value of Type, you can also update the key value to reduce security risks.

Duration

seconds

Timeout interval of URL authentication information, which is the maximum difference between the request time in the authentication information and the time when Live receives the request. This parameter checks whether the ingest URL or streaming URL has expired.

CancelOK

Table 3-6 URL validation parameters

Parameter	Description
Type	<p>You can use signing method A, B, C, or D to calculate a signed string.</p> <p>Signing methods A and B: The Message Digest algorithm 5 (MD5) is used. For details, see Signing Method A and Signing Method B.</p> <p>Signing method C: A symmetric encryption algorithm is used. For details, see Signing Method C.</p> <p>Signing method D: The HMAC-SHA256 algorithm is used. For details, see Signing Method D.</p> <p>NOTE</p> <ul style="list-style-type: none">• Signing methods A, B, and C have security risks. Signing method D is more secure and recommended.• URL validation for streaming domain names supports only signing method D, which supports only HLS and does not support DASH or MSS.
Key	<p>Authentication key.</p> <ul style="list-style-type: none">• You can customize a key, which consists of 32 characters in letters and digits.• A key can also be automatically generated.
Duration	<p>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.</p> <p>NOTE</p> <ul style="list-style-type: none">• 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 3,600 seconds.

Step 7 Click **OK**.

Step 8 Obtain a signed URL in either of the following ways:

- Manually assemble it based on the selected signing method. For details, see [Signing Method A](#), [Signing Method B](#), [Signing Method C](#), and [Signing Method D](#).

- Use the validation address generation tool to quickly generate a signed URL for an RTMP ingest domain name. This method is recommended. 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 streaming URL can, URL validation has taken effect.

----End

Signing Method A

CAUTION

- Signing method A is supported only by RTMP ingest domain names, but not by streaming domain names.
- Use the validation address generation tool to quickly generate a signed URL for an RTMP ingest domain name. This method is recommended. For details, see [Signed URL Generation Tool](#).

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 3-7 Authentication fields

Field	Description
timestamp	Start time of a valid request. The value is the total number of seconds that have elapsed since 00:00:00 January 1, 1970. It is a decimal or hexadecimal integer. Example: 1592639100 (June 20, 2020 15:45)
Duration	How long a signed URL remains effective. If the validity period is set to 1,800s, users can access the streaming URL within 1,800s since the time indicated by timestamp . Authentication fails and the URL is inaccessible if users access the streaming URL 1800s later. For example, if the access time is 00:00:00 (GMT +08:00) on June 30, 2020, the URL expires at 00:30:00 (GMT+08:00) on June 30, 2020.

Field	Description
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	The original URL part that starts on the right of the domain name to the left of the question mark (?). For example, if the original URL is rtmp://live-push.example.com/live/huaweitest?request_source=ott&channel_id=huaweitest, the URI is /live/huaweitest.
Key	Key value set on the console. For details, see Enabling URL Validation .

Signed URL example:

The following shows how to generate a signed ingest URL:

```
Original URL: rtmp://live-push.example.com/live/huaweitest?request_source=ott&channel_id=huaweitest
timestamp: 1592639100
Duration: 1800s
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
rand: 477b3bbc253f467b8def6711128c7bec
uid: 0
URI: /live/huaweitest
```

Obtain **md5hash** using the calculation formula.

```
HashValue = md5sum("/live/huaweitest-1592639100-477b3bbc253f467b8def6711128c7bec-0-GCTbw44s6MPLh4GqgDpnfuFHgy25Enly") = 1832e24276a08e180152c9c8a98ff322
```

The signed ingest URL is:

```
rtmp://live-push.example.com/live/huaweitest?
request_source=ott&channel_id=huaweitest&auth_key=1592639100-477b3bbc253f467b8def6711128c7bec-0-
1832e24276a08e180152c9c8a98ff322
```

Signing Method B

CAUTION

- Signing method B is supported only by RTMP ingest domain names, but not by streaming domain names.
- Use the validation address generation tool to quickly generate a signed URL for an RTMP ingest domain name. This method is recommended. For details, see [Signed URL Generation Tool](#).

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 3-8 Authentication fields

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

Signed URL example:

The following shows how to generate a signed ingest URL:

```
Original URL: rtmp://live-push.example.com/live/huaweitest?request_source=ott&channel_id=huaweitest  
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly  
StreamName: huaweitest  
txTime: 5eed5888  
Duration: 1,249s
```

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

```
txSecret = md5(GCTbw44s6MPLh4GqgDpnfuFHgy25Enlyhuaweitest5eed5888) =  
1f5b30ca84581f14efd1f7aa39def2e3
```

The signed ingest URL is:

```
rtmp://live-push.example.com/live/huaweitest?  
request_source=ott&channel_id=huaweitest&txSecret=1f5b30ca84581f14efd1f7aa39def2e3&txTime=5eed5888
```

Signing Method C

CAUTION

- Signing method C is supported only by RTMP ingest domain names, but not by streaming domain names.
- Use the validation address generation tool to quickly generate a signed URL for an RTMP ingest domain name. This method is recommended. For details, see [Signed URL Generation Tool](#).

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 3-9](#) describes encryption parameters in the algorithm.

Table 3-9 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	Livestream ID, which uniquely identifies a livestream. 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. <ul style="list-style-type: none">• 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:

The following shows how to generate a signed ingest URL:

```
Original URL: rtmp://live-push.example.com/live/huaweitest?request_source=ott&channel_id=huaweitest
AppName: live
StreamName: huaweitest
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
LiveID: live/huaweitest
Timestamp: 20190428110000
CheckLevel: 3
IV: yCmE666N3YAq30SN
```

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

```
Encrypted string = I90KW7GhxOMwoy5yaeKMSk%2FsLt08T4Wlc6avfPBz9FQGIHRFOgkTOGHXWsXfl44x.
EncodedIV = 79436d453636364e335941713330534e
```

The signed ingest URL is:

```
rtmp://live-push.example.com/live/huaweitest?
request_source=ott&channel_id=huaweitest&auth_info=I90KW7GhxOMwoy5yaeKMSk
%2FsLt08T4Wlc6avfPBz9FQGIHRFOgkTOGHXWsXfl44x.79436d453636364e335941713330534e
```

Signing Method D

CAUTION

- Signing method D is supported only by RTMP ingest domain names and HLS streaming domain names.
- Use the validation address generation tool to quickly generate a signed URL for an RTMP ingest domain name. This method is recommended. For details, see [Signed URL Generation Tool](#).

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 3-10 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 .
hwSecret	Encryption parameter in the URL. The value is obtained using the HMAC-SHA256 algorithm, with <i>Key</i> and <i>StreamName</i> + <i>hwTime</i> as parameters. hwSecret = hmac_sha256 (<i>Key</i> , <i>StreamName</i> + <i>hwTime</i>)
Duration	How long a signed URL remains effective. If hwTime is set to the current time and the validity period is set to 1,249s, the streaming URL expiration time is the current time plus 1,249s.

Signed URL example:

Generating a signed streaming URL is used as an example.

Original URL: `https://live-play.example.com/{channelld}/hls/{unique_string}/index.m3u8`

Key: `GCTbw44s6MPLh4GqgDpnfuFHgy25Enly`

StreamName: `index`

hwTime: `5eed5888`

Duration: `1,249s`

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

`hwSecret = hmac_sha256(GCTbw44s6MPLh4GqgDpnfuFHgy25Enly, index5eed5888) = 63eb41e0c5c8d8f8058aa83488901ad279645217f7099a2bcdef4f0044aa5b4f`

The signed streaming URL is:

`https://live-play.example.com/{channelld}/hls/{unique_string}/index.m3u8?`

`hwSecret=63eb41e0c5c8d8f8058aa83488901ad279645217f7099a2bcdef4f0044aa5b4f&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();
}
}
```

3.9.4 IP Address 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.
- Whitelisting and blacklisting cannot be used simultaneously.
- A maximum of 1,000 IP addresses can be added to a whitelist or blacklist.
- If the stream push protocol of an ingest domain name is SRT, the configuration page of URL validation and ACL will be invisible. If you want to enable URL validation for an SRT ingest domain name, you can configure **CIDR IP Whitelist** and **Primary Input Decryption Parameters** (with **Decryption** enabled) when creating a channel. For details, see [Creating a Channel](#).

Prerequisites

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

Procedure

- Step 1** Log in to the [Live console](#).
- Step 2** In the navigation pane, choose **Domains**.
- Step 3** Click **Manage** in the **Operation** column of the desired streaming domain name.
Set **Subservice Type** of the domain name to **Media Live**.
- Step 4** In the navigation pane, choose **Basic Settings** > **Access Control**.
- Step 5** Click **Edit** on the right of **IP ACL**. The **IP ACL** dialog box is displayed.
- Step 6** Toggle on the **Status** switch to configure related parameters, as shown in [Figure 3-17](#).

Figure 3-17 Configuring an IP address ACL

IP ACL ✕

⚠ Modifying the IP ACL may cause livestream exceptions. Exercise caution when performing this operation.

Status

Type
 IP blacklist IP whitelist

Error code 403 will be returned for requests initiated by a blacklisted client IP address.

IP blacklist

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

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

Step 8 Click **OK**.

----End

3.10 HTTPS Certificates

3.10.1 Configuration Methods

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

Context

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

HTTPS has the following advantages over HTTP:

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

Prerequisites

- You have created a channel. For details, see [Creating a Channel](#).
- [CNAME records have been added](#) to your domains' DNS records.
- The HTTPS certificate has been prepared. If no HTTPS certificate is available, buy one in [SSL Certificate Manager \(SCM\)](#).
- The HTTPS certificate format must meet the [requirements](#). If your certificate is not in PEM format, [convert the certificate](#) to the PEM format.

Enabling HTTPS

Step 1 Log in to the [Live console](#).

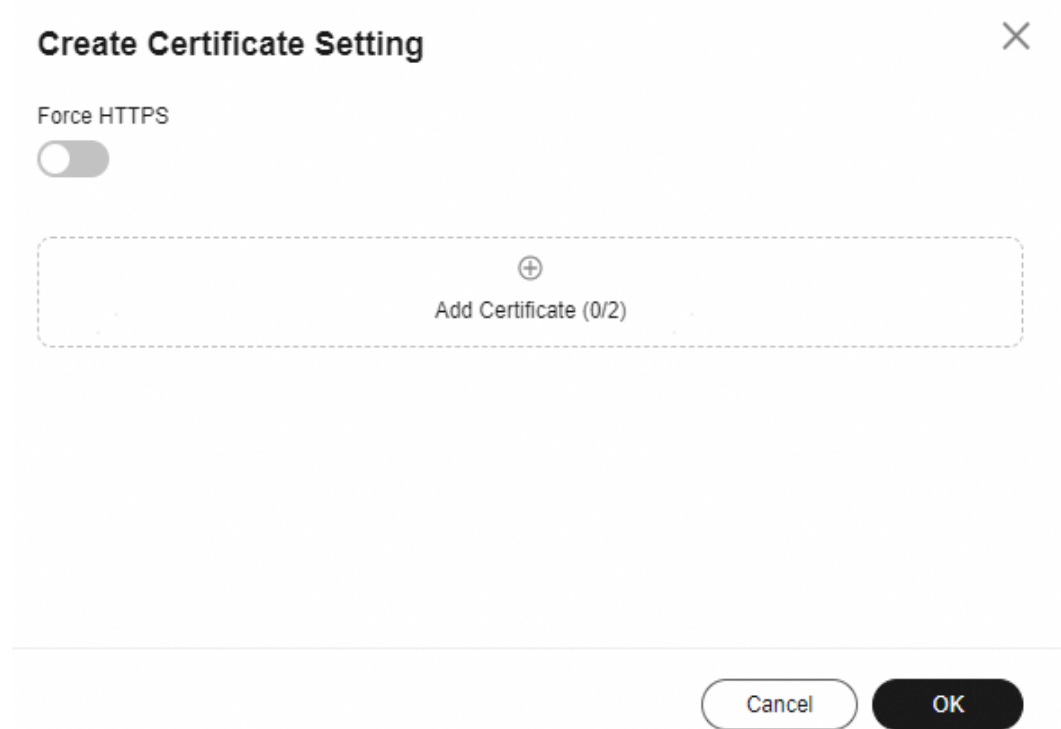
Step 2 In the navigation pane, choose **Domains**.

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

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

Step 5 Click **Create**. The **Create Certificate Setting** page is displayed, as shown in [Figure 3-18](#).

Figure 3-18 Creating a certificate setting



Step 6 Click **Add Certificate**. The settings of certificate 1 are displayed, as shown in [Figure 3-19](#).

For details about the parameter settings, see [Table 3-11](#). You can add a certificate only when:

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

Figure 3-19 Configuring a certificate

Create Certificate Setting ✕

Force HTTPS

^ **Certificate 1** 🗑 Delete

Certificate Standard

International Chinese (SM)

Certificate Source

My certificate SCM certificate

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

Certificate Body

PEM-encoded


Private Key

PEM-encoded

+
Add Certificate (1/2)

Cancel OK

Table 3-11 Parameters

Parameter	Description
Certificate Standard	Standard of the HTTPS certificate. Options: <ul style="list-style-type: none"> - International - Chinese (SM)
Certificate Source	Source of the HTTPS certificate. Options: <ul style="list-style-type: none"> - My certificate: a certificate obtained from a compliant channel - SCM certificate: a certificate purchased from Huawei Cloud SCM
International > My certificate	<p>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.</p> <p>Certificates issued by different organizations have the following differences:</p> <ul style="list-style-type: none"> - If your certificate is issued by the root CA, the certificate is a complete certificate. Copy the certificate content. <p>Figure 3-20 HTTPS certificate</p>  <p>- 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.</p>
Chinese (SM) > My certificate	
International > SCM certificate	Click Create SCM Certificate on the right of Certificate Name to go to the SCM console and purchase a certificate as prompted.
Chinese (SM) > SCM certificate	After the certificate is issued, it will be automatically displayed in the Certificate Name drop-down list.

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

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

Step 8 Click **OK**.

Step 9 Verify whether HTTPS secure acceleration has taken effect.

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

----End

Updating a Certificate

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

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

3.10.2 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 3-21](#).

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 3-22 A combined certificate

```
-----BEGIN CERTIFICATE-----
MIIE/DCCA+SgAwIBAgIUOWwvEj41j5OamNabjVbGY42BBcQwDQYJKoZIhvcNAQEL
BQAwYIxCzAJBgNVBAYTAmNuMRIwEAYDVQQIDAlHdWFuZ0RvbmNlcwETAPBgNVBACM
CFNoZW56aGVuMQ8wDQYDVQQKDAZidWF3ZWkxZWkxZWkxZWkxZWkxZWkxZWkxZWkx
DCVidWF3ZWkxZWkxZWkxZWkxZWkxZWkxZWkxZWkxZWkxZWkxZWkxZWkxZWkxZWkx
ODAwNDA0N1oXDTE4MTAxODAwNDA0N1owgZoxCzAJBgNVBAYTAKNOMRAwDgYDVQQI
DAdqawFuZ3N1MRawDgYDVQQHDAduYW5qaW5nMS4wLAYDVQQKDCVidWF3ZWkxZWkx
dHdhcmUgVGvjaG5vbG9naWVzIENvLiwgTHRkMRkwFwYDVQQLEDBBDBg91ZGJ1IFNS
RSBEZXB0MRwwGgYDVQQDDBN3d3cuaHVhd2VpY2xvdWQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA3f5hC6J20XSF/Y7Wb8o6130yzgaUYWGLEX8t
1dQ1JAus93xMC2Jr6UOXmXR6WaRu51ZxpPFLT/IV6UnvMLnxJQBavqauykCskadW
stYA9ttTI/FYq+MR1XKbNrqK/ADhrfmR4owS/3w1wxvdpwy5TRZ+V/D6TjxHZCjc
+81SmUuLxsgoUe79B/ruccY1ufuqr3v0TToaNN4c37kwjJeKf+b2F/IqO/KF+9zF
.....
AgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMEIGA1UdEQQ7MDmCE3d3dy5odWF3ZW1j
bG91ZC5jb22CESouaHVhd2VpY2xvdWQuY29tgg9odWF3ZW1jbG91ZC5jb20wDQYJ
KoZIhvcNAQELBQADggEBACsLP7Hj+4KY1ES38OnOWuwQ3st8axvhDD9jZGoninzW
JSGpdm04NEshlvSFdEHpjy/xKSLCIqg5Ue8tTI8zOF13U0ROnMeHKSXsJG6zc8X
h/3N217oBygPgvpmc6YX66kvwXmbA7KRniiYS0nmCi2KUyng5Bv4dsx21djlqQ3b
HI+i026Q9odLsmhsKOsfUC0vDKoMIJz0Socy7Cq1+tFWF9S79MI4QjxaXVEvpIEg
QLEze3BXSsoiWRkdfsDB9s+UtdWeJy0HMh/otwUQQtB6areV2+CPthfmDENA+A8
IK6GzHyp/mgrwKdDh97aQ42ARreAv4KVFAiJGZ02LOY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID2CCAsGgAwIBAgIJALQPO9XxFFZmMA0GCSqGSIb3DQEBCwUAMIGCMQswCQYD
VQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25nMREwDwYDVQQHDAhTaGVuemh1bjEP
MA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAAJVVDEuMCwGA1UEAw1SHVhd2VpIFd1
YiBTZWN1cmUgSW50ZXJuzXQgR2F0ZXdheSBDQTAeFw0xNjA1MTAwOTAyMjdaFw0y
NjA1MDgwOTAyMjdaMIGCMQswCQYDVQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25n
MREwDwYDVQQHDAhTaGVuemh1bjEPMA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAAJ
VDEuMCwGA1UEAw1SHVhd2VpIFd1YiBTZWN1cmUgSW50ZXJuzXQgR2F0ZXdheSBD
.....
rG0CAwEAAaNQME4wHQYDVR0OBBYEFDB6DZX4Am+isCoa48e4ZdrAXpsMB8GA1Ud
IwQYMBaAFDB6DZX4Am+isCoa48e4ZdrAXpsMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAKN9ksjRX56yw2Ku5Mm3gzU/kQQw+mLkIuJEeDwS6LWjW0Hv
313xlv/Uxw4hQmo6OXqQ2OM4dfIJoVYKqilLlBCpXvO/X600rq3UPediEMaXkmM+F
tuJnoPCXmew7QvvQQvwis+0xmhpRPg0N6xIK01vIbAV69TkpWJW3duj1FuRjGsvn
rRab4gVi14x+bUgTb6HCvDH99PhADvXOuI1mk6Kb/JhCNbhrAHezyfLrvimxIOKy
2KZWitN+M1UWvSYG8jmtDm+/FuA93V1yErRjKj92egCgMlu671liddt7zzzzqW+U
QLU0ewUmUHQsV5mk62v1e8sRViHB1B2HJ3DU5gE=
-----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 3-23](#).

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 3-23 An RSA private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909eY1vLCqow
wEPqs6vyqQM3gKo8qCkNkmS5QgMPOFI4fx2G22mHvT0x8PHjm6GTQDPDniWaIuky
luFqVpD/zqK0oBl2AeAvbzKxWwRqf4JTLA3136B415y2VoDjRfU5EKY6LW1sD/00
5uF0qE3td5KQwQc6ZzbnkAof0Oyp5PbMfajM9My2mcvQJzWPLRxET3eWHYdBUEg
1rxdrWxLheKjENzW3P7Mz/7KycIRxAlurl/Z9s8ytj3124AQY7NE1t1iL9wwA47k
0EumxTaLz8H/vHB1fLMouvYfsSDEr3Snf6eSSwIDAQABAoIBAQDCNmxC3qHXPgvI
EzBOtIPVl1PyzizXWi+U4U6WwUBjCQ6ijfoYOKLaHHnnCEIm4V2N8KV4prAkQjcm
-----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
```

4 Flows

4.1 Creating a Flow

Flows are centrally managed on the **Flows** page. Multiple channels can reference the same flow at a time, which improves channel O&M efficiency.

Notes

- By default, the **Flows** menu is not displayed. To use it, you need to [submit a service ticket](#).
- For SRT ingest scenarios, you are advised to enable encryption on the encoder for push streaming. For SRT streaming scenarios, when relaying to third parties, you are advised to enable encryption by default.

Procedure

- Step 1** Log in to the [Live console](#).
- Step 2** In the navigation pane on the left, choose **Flows**.
- Step 3** Click **Create Flow**. The **Create Flow** dialog box appears on the right, as shown in [Figure 4-1](#).

Figure 4-1 Creating a flow

Create Flow ✕

Flow Name

Start with a letter and use up to 64 characters of letters, digits, hyphens (-), and underscores (_).

Region

 ▼

Source Input Name

Start with a letter and use up to 64 characters of letters, digits, hyphens (-), and underscores (_).

Protocol

 ▼

Description (Optional)

CIDR IP Whitelist

 Delete

[+ Add](#) Whitelists you can still add: 19
Example: 10.0.0.0/16

Decryption

Enable this function if the source stream is encrypted. Otherwise, disable it.

Algorithm

 ▼

Passphrase

 👁

Cancel OK

See [Table 4-1](#).

Table 4-1 Parameters

Parameter	Description
Flow Name	Name of the flow. Start with a letter and use up to 64 characters of letters, digits, hyphens (-), and underscores (_).
Region	Select the region of the flow from the drop-down list. Details: <ul style="list-style-type: none">AP-Singapore, ME-Riyadh, CN-Hong Kong, and AF-Johannesburg are available on Huawei Cloud (International). ME-Riyadh and AF-Johannesburg are not displayed by default. To use Live in these two regions, submit a service ticket for Huawei Cloud technical support.
Source Input Name	Name of the source input. Start with a letter and use up to 64 characters of letters, digits, hyphens (-), and underscores (_).
Protocol	Protocol used by the flow. Options: <ul style="list-style-type: none">SRT listener: Stream push is required. After the flow is created, go to the Details page to view the Source IP and Source Port, and assemble them into an ingest URL, for example, <code>srt://{Source IP}:{Source Port}</code>.SRT caller: Stream push is not required. Media Live uses the SRT streaming URL that you provide to pull streams. NOTICE Streams can be pushed only after the flow is started.
SRT listener protocol parameters	<ul style="list-style-type: none">Description (Optional): Description of the flow.CIDR IP Whitelist: Enter the IP address of a stream push client. You can click Add to add up to 19 more IP addresses.
SRT caller protocol parameters	<ul style="list-style-type: none">Description (Optional): Description of the flow.Source IP: IP address of the source input. You can enter an IP address or a domain name.Source Port: Source input port. The value ranges from 1024 to 65535, excluding 2077 and 2088.Minimum Latency (Optional): Stream pull latency. The value ranges from 10 to 15,000, in milliseconds.Stream ID (Optional): Stream ID of the streaming URL.

Parameter	Description
Decryption	<p>Enable this function if the source stream is encrypted. Disable it if the source stream is not encrypted. If this function is enabled, provide the decryption algorithm and key.</p> <ul style="list-style-type: none">• Algorithm: Decryption algorithm.• Passphrase: Decryption key. <p>Decryption is enabled by default. You are advised to use encrypted input streams. Unencrypted streams have security risks.</p>

Step 4 Click **OK**. A line of flow-related content is added on the **Flows** page.

Step 5 Click **Start** in the **Operation** column to start the flow.

You can also perform the following operations on a selected flow:

- Click **Manage** in the **Operation** column. On the **Details** page displayed, view details about the flow. You can modify the source stream and output information. You can click **Refresh** in the upper right corner of the page to refresh the source stream and output status.
- Click **Stop** in the **Operation** column to stop the flow. If the flow is in use by a channel, stopping it will cause the channel to malfunction.
- Click **Delete** in the **Operation** column to delete the flow.

----End

4.2 Pushing Streams to a Third Party Through SRT

For a flow created on the **Flows** page, you can configure the function of pushing streams from Media Live to a third party through SRT.

Prerequisites

You have created a flow. For details, see [Creating a Flow](#).

Notes

- A maximum of 10 outputs can be configured for a flow.
- If the output protocol of a flow is set to **SRT listener**, only one third party can pull streams at a time.

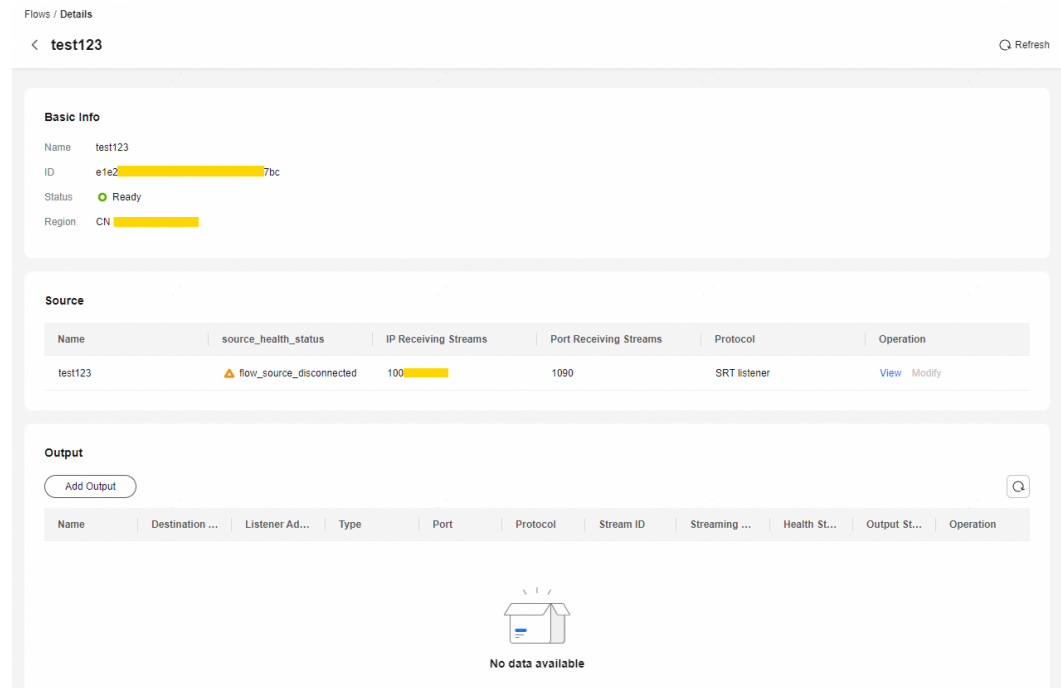
Procedure

Step 1 Log in to the [Live console](#).

Step 2 In the navigation pane on the left, choose **Flows**.

Step 3 Click **Manage** on the right of the created flow. The **Details** page is displayed, as shown in [Figure 4-2](#).

Figure 4-2 Flow details



Step 4 Click **Add Output** in the **Output** area. The **Add Output** dialog box is displayed, as shown in [Figure 4-1](#).

Figure 4-3 Adding an output

Add Output

✕

Name

Start with a letter and use up to 64 characters of letters, digits, hyphens (-), and underscores (_).

Protocol

SRT listener
▼

Description (Optional)

CIDR IP Whitelist

Delete

+ Add

Whitelists you can still add: 19

Example: 10.0.0.0/16

Minimum Latency (Optional)

ms

Decryption

Output Status

Cancel

OK

See [Table 4-2](#).

Table 4-2 Parameters

Parameter	Description
Name	Name of the third party to which Media Live pushes streams through SRT. Start with a letter and use up to 64 characters of letters, digits, hyphens (-), and underscores (_).

Parameter	Description
Protocol	<p>Protocol used by the flow.</p> <p>Options:</p> <ul style="list-style-type: none"> • SRT listener: Media Live does not need to push streams. You can wait for the third party to pull streams. • SRT caller: Media Live needs to push streams. After an output is added to the flow, go to the Details page to view the Destination Address and Port, and assemble them into an ingest URL, for example, <code>srt://{Destination address}:{Port}</code>. <p>NOTICE Streams can be pushed only after the flow is started.</p>
SRT listener protocol parameters	<ul style="list-style-type: none"> • Description (Optional): Description of the flow. • CIDR IP Whitelist: Enter the IP address of the stream pull client. You can click Add to add up to 19 more IP addresses. • Minimum Latency (Optional): Latency of third-party stream pull. The value ranges from 10 to 15,000, in milliseconds.
SRT caller protocol parameters	<ul style="list-style-type: none"> • Description (Optional): Description of the flow. • Destination Address: Third-party destination address to which media streams are pushed through SRT. The value can be an IP address or domain name. • Port: Third-party port to which media streams are pushed through SRT. The value ranges from 1024 to 65535, excluding 2077 and 2088. • Minimum Latency (Optional): Latency of pushing streams to a third party through SRT. The value ranges from 10 to 15,000, in milliseconds. • Stream ID (Optional): Stream ID used for pushing streams to a third party through SRT.
Decryption	<p>If the output of the customer encoder is encrypted, the encryption algorithm and passphrase need to be provided.</p> <ul style="list-style-type: none"> • Algorithm: Decryption algorithm. • Passphrase: Decryption key. <p>Note: You are advised to use encrypted input streams. Unencrypted streams have security risks.</p>
Output Status	You can enable the output status as required.

Step 5 Click **OK**. An output of pushing streams to a third party through SRT is added to the **Output** area.

You can also perform the following operations on a selected output:

- Click **View** in the **Operation** column to view details about the selected output in the displayed **Output** dialog box.

- Click **Modify** in the **Operation** column to modify the selected output in the displayed **Modify Output** dialog box.
- Click **Delete** in the **Operation** column. In the displayed **Delete Output** dialog box, enter **DELETE**. Click **OK** to delete the selected output.

----End

5 Channels

5.1 Creating a Channel

You can play channel video on Media Live only after creating a channel.

Prerequisites

- [You have added an ingest domain name.](#)
- [You have created a live transcoding template.](#)
- If you need to enable DRM encryption for a channel and set **Interconnection Mode** to **FunctionGraph proxy access** to provide the key for integrating DRM, you need to:
 - enable **FunctionGraph agency** in advance by referring to [Cloud Resource Authorization](#);
 - [create a function](#) on FunctionGraph.

Notes

- A tenant can create a maximum of 500 channels. If more channels are required, [submit a service ticket](#).
- All channels support only single-bitrate inputs, and multi-bitrate outputs are available only after transcoding.
- **RTMP_PUSH** channels require RTMP ingest domain names. **SRT_PUSH** channels require SRT ingest domain names.
SRT_PUSH channels and **RTMP_PUSH** channels cannot be created simultaneously for the same domain name.
- To ensure reliability, **SRT_PUSH** channels must:
 - support primary/standby regions. The encoder needs to push streams to both the primary and standby URLs.
 - If the encoder supports *streamid*, only the primary input URL is returned by default, as shown in [Figure 5-1](#).

Figure 5-1 Channel details

< | Update Channel

Channel Name (Optional)

Channel ID

App Name

Input Type

Ingest Domain Name

Stream ID Mode

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

CIDR IP Whitelist (Optional)

Separate multiple CIDR IP addresses using commas (,).

^ Primary Input Parameters

URL `srt://push[redacted]com:5000?streamid=#:h=push[redacted]com.r=live/zftest_srt_0428001,request_source=ott,channel_id=zftest_srt_0428001,m=publish`

- If the encoder does not support *streamid*, both the primary and standby input URLs are returned, as shown in [Figure 5-2](#).

Figure 5-2 Channel details

< | Update Channel

Channel Name (Optional)

Channel ID

App Name

Input Type

Ingest Domain Name

Stream ID Mode

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

CIDR IP Whitelist

Separate multiple CIDR IP addresses using commas (,).

^ Primary Input Parameters

URL

^ Primary Input Decryption Parameters

Decryption

^ Standby Input Parameters

Standby Input URL

^ Standby Input Decryption Parameters

Decryption

- Resume stream push when the stream push by the encoder is interrupted. The recommended interval for resuming stream push is shorter than the duration of one segment.

- It is recommended that DRM encryption be enabled and the FunctionGraph proxy access mode be used. If the HTTPS direct access mode is used, you are advised to add an authentication header.
- When FunctionGraph is used for DRM-based channel encryption, the FunctionGraph version information is not contained. By default, the latest version is used.
- If the DRM is faulty, 404 will be returned on channel playback.
- To ensure reliability, if you have configured a standby streaming URL for an **HLS_PULL** or **SRT_PULL** channel, and the standby input of an **SRT_PUSH** channel is pushed, transcoding will be performed in the standby region and generate fees.
- If you select multiple transcoding templates when creating or modifying a channel, all transcoding templates must meet the following conditions:
 - Each template must use a different video bitrate.
 - The settings of **Use Source I-Frame**, **GOP Unit**, **GOP Size**, and **Video Frame Rate** must be identical across all selected templates.
 - If a template is modified during live transcoding and this results in mismatched GOP size, GOP unit, or video frame rate settings across templates, no output stream will be generated.
 - If **Use Source I-Frame** is disabled, the channel supports only one input and up to six outputs.
- Changes to the transcoding settings of a channel take effect only after the channel is restarted or the stream is pushed again. You will then be billed according to the new settings.

Creating a Channel

Step 1 Log in to the [Live console](#).

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

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

Configure **Basic Info** as follows:

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

Step 4 Click **Next**.

Configure input parameters based on [Table 5-1](#).

Table 5-1 Parameters

Parameter	Description
Input Type	<p>Input type of a channel media asset.</p> <p>Options:</p> <ul style="list-style-type: none">● FLV_PULL: Stream push is not required. Streams pulled by Media Live from the streaming URL provided you will go to the origin server. A streaming URL supports only HTTP.● RTMP_PUSH: RTMP streams are pushed to the origin server through Huawei CDN.● HLS_PULL: Stream push is not required. Streams pulled by Media Live from the streaming URL provided by you will go to the origin server. <p>Constraints on streaming URLs:</p> <ul style="list-style-type: none">– A streaming URL supports only HTTP and HTTPS.– Encrypted streams are not supported.– Audio-only streams are not supported.– Subtitling is not supported. <ul style="list-style-type: none">● SRT_PULL: Stream push is not required. Streams pulled by Media Live from the SRT streaming URL provided by you will go to the origin server.● SRT_PUSH: An SRT ingest domain name needs to be configured for stream push. To ensure reliability, SRT_PUSH channels must:<ul style="list-style-type: none">– support primary/standby regions. The encoder needs to push streams to both the primary and standby URLs.– Resume stream push when the stream push by the encoder is interrupted. The recommended interval for resuming stream push is shorter than the duration of one segment.● STREAM_CONNECT: Stream push and pull are implemented through custom stream connections. By default, STREAM_CONNECT is not displayed. If you need to use it, submit a service ticket.

Parameter	Description
<p>Input Type set to FLV_PULL</p>	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> ● Primary Input Parameters: URL, indicating the media stream URL obtained from the channel provider. Media Live directly uses the URL to push streams to the origin server. ● Standby Input Parameters: <ul style="list-style-type: none"> - Primary/standby Input: You can enable this function to set the standby media stream URL. - Standby Input URL: Obtain the standby media stream URL from the channel provider. - Switchover Duration Threshold: When the duration of abnormal channel playback reaches the threshold, the system automatically switches to another URL for stream pull and playback. - Priority Settings: Select PRIMARY (mainly the primary input URL) or EQUAL (switchover between primary and standby input URLs) as needed.
<p>Input Type set to RTMP_PUSH</p>	<p>Configure the following parameters:</p> <p>Ingest Domain Name: Select an RTMP ingest domain name from the drop-down list. If no ingest domain name is available, click Create on the right and add an RTMP ingest domain name on the Add Domain page.</p>

Parameter	Description
Input Type set to HLS_PULL	<p>Configure the following parameters:</p> <ul style="list-style-type: none">● Max Bandwidth (Optional): A streaming URL provided by a user contains the parameter BANDWIDTH for media files of different bitrates.<ul style="list-style-type: none">– If Max Bandwidth is specified and Media Live pulls streams using the URL, the media stream with the highest bitrate and bandwidth lower than the value of Max Bandwidth will be pushed to the origin server.– If Max Bandwidth is not specified and Media Live pulls streams using the URL, the media stream with the largest BANDWIDTH value will be pushed to the origin server.● Primary Input Parameters: URL, indicating the media stream URL obtained from the channel provider. Media Live directly uses the URL to push streams to the origin server.● Standby Input Parameters:<ul style="list-style-type: none">– Primary/standby Input: You can enable this function to set the standby media stream URL.– Standby Input URL: Obtain the standby media stream URL from the channel provider.– Switchover Duration Threshold: When the duration of abnormal channel playback reaches the threshold, the system automatically switches to another URL for stream pull and playback.– Priority Settings: Select PRIMARY (mainly the primary input URL) or EQUAL (switchover between primary and standby input URLs) as needed.● Audio Selectors: Up to eight audio selectors can be added. Click Add Audio Selector to add Audio Selector 1. Configure the following parameters:<ul style="list-style-type: none">– Selector Name: Enter an audio selector name using only letters, digits, hyphens (-), and underscores (_). The name of each selector in the same channel must be unique.– Selector Settings:<ul style="list-style-type: none">PID selection: This mode requires specifying PID.PID: ID of the audio stream in the input source.Language selection: This mode requires specifying Language Code and Language Selection Policy.Language Code: Confirm the language of each audio stream in the source input, select an audio stream, and enter the language code (2–3 lowercase letters) of that audio stream. For example, eng indicates English.Language Selection Policy: The value LOOSE indicates that the audio stream language is loosely matched with the

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

Parameter	Description
Input Type set to SRT_PUSH	<p>Configure the following parameters:</p> <ul style="list-style-type: none">● Ingest Domain Name: Select an SRT ingest domain name from the drop-down list. If no ingest domain name is available, click Create on the right and add an SRT ingest domain name on the Add Domain page.● Stream ID Mode: indicates whether the encoder allows inputting a stream ID. If not, you must specify CIDR IP Whitelist.● CIDR IP Whitelist (Optional): Enter whitelisted CIDR IP addresses in a maximum of 256 characters. Separate IP addresses using commas (,).● Primary Input Decryption Parameters: Decryption: Enable this function if the source stream is encrypted. Disable it if the source stream is not encrypted. If this function is enabled, provide the decryption algorithm and key.<ul style="list-style-type: none">- For stream push by stream ID, configure only Primary Input Decryption Parameters. For stream push of primary/standby regions, use the same passphrase.- For stream push by IP address + port, if primary/standby regions are involved, you can configure Standby Input Decryption Parameters. That is, the standby region has its own encryption parameters. Standby Input Decryption Parameters will appear only when you modify a created channel.Algorithm: Decryption algorithm. Passphrase: Decryption key. Note: You are advised to use encrypted input streams. Unencrypted streams have security risks.● Audio Selectors: Up to eight audio selectors can be added. Click Add Audio Selector to add Audio Selector 1. Configure the following parameters:<ul style="list-style-type: none">- Selector Name: Enter an audio selector name using only letters, digits, hyphens (-), and underscores (_). The name of each selector in the same channel must be unique.- Selector Settings: PID selection: This mode requires specifying PID. PID: ID of the audio stream in the input source. Language selection: This mode requires specifying Language Code and Language Selection Policy. Language Code: Confirm the language of each audio stream in the source input, select an audio stream, and enter the language code (2-3 lowercase letters) of that audio stream. For example, eng indicates English.

Parameter	Description
	<p>Language Selection Policy: The value LOOSE indicates that the audio stream language is loosely matched with the selected language code. In the example of eng, the audio stream whose language is English in the source input will be preferentially selected. If audio streams in the language represented by the selected language code cannot be found, the audio stream with the lowest PID will be selected. The value STRICT indicates that the audio stream language is strictly matched with the selected language code. In the example of eng, only audio streams in English in the source input will be selected. If audio streams in the language represented by the selected language code cannot be found, a muted segment will be automatically added. When a device uses this audio selector to play a video, the playback is muted.</p>

Parameter	Description
Input Type set to SRT_PULL	<p>Configure the following parameters:</p> <ul style="list-style-type: none">● Primary Input Parameters: URL, indicating the media stream URL obtained from the channel provider. Media Live directly uses the URL to push streams to the origin server.● SRT Minimum Latency (Optional): stream pull latency when the channel type is SRT_PULL● Stream ID (Optional): stream ID of the streaming URL when the channel type is SRT_PULL● Primary Input Decryption Parameters: Decryption: Enable this function if the source stream is encrypted. Disable it if the source stream is not encrypted. If this function is enabled, provide the decryption algorithm and key.<ul style="list-style-type: none">- For stream push by stream ID, configure only Primary Input Decryption Parameters. For stream push of primary/standby regions, use the same passphrase.- For stream push by IP address + port, if primary/standby regions are involved, you can configure Standby Input Decryption Parameters. That is, the standby region has its own encryption parameters. Standby Input Decryption Parameters will appear only when you modify a created channel.Algorithm: Decryption algorithm. Passphrase: Decryption key. Note: You are advised to use encrypted input streams. Unencrypted streams have security risks.● Standby Input Parameters:<ul style="list-style-type: none">- Primary/standby Input: You can enable this function to set the standby media stream URL.- Standby Input URL: Obtain the standby media stream URL from the channel provider.- Switchover Duration Threshold: When the duration of abnormal channel playback reaches the threshold, the system automatically switches to another URL for stream pull and playback.- Priority Settings: Select PRIMARY (mainly the primary input URL) or EQUAL (switchover between primary and standby input URLs) as needed.● Audio Selectors: Up to eight audio selectors can be added. Click Add Audio Selector to add Audio Selector 1. Configure the following parameters:<ul style="list-style-type: none">- Selector Name: Enter an audio selector name using only letters, digits, hyphens (-), and underscores (_). The name of each selector in the same channel must be unique.

Parameter	Description
	<p>– Selector Settings:</p> <p>PID selection: This mode requires specifying PID. PID: ID of the audio stream in the input source.</p> <p>Language selection: This mode requires specifying Language Code and Language Selection Policy.</p> <p>Language Code: Confirm the language of each audio stream in the source input, select an audio stream, and enter the language code (2–3 lowercase letters) of that audio stream. For example, eng indicates English.</p> <p>Language Selection Policy: The value LOOSE indicates that the audio stream language is loosely matched with the selected language code. In the example of eng, the audio stream whose language is English in the source input will be preferentially selected. If audio streams in the language represented by the selected language code cannot be found, the audio stream with the lowest PID will be selected. The value STRICT indicates that the audio stream language is strictly matched with the selected language code. In the example of eng, only audio streams in English in the source input will be selected. If audio streams in the language represented by the selected language code cannot be found, a muted segment will be automatically added. When a device uses this audio selector to play a video, the playback is muted.</p>

Parameter	Description
Input Type set to STREAM_CONNECT	<p>Configure the following parameters:</p> <ul style="list-style-type: none">● Primary Input Parameters: Flow indicates the media streams created on the Flows page of the primary region. You can also click Create Flow on the right. In the dialog box displayed, add a media stream.● Standby Input Parameters of the primary region:<ul style="list-style-type: none">– Primary/standby Input: You can enable this function to configure a standby media stream.– Flow: From the drop-down list box, select the media stream created on the Flows page of the primary region. The primary and standby streams must be in the same region and use the same protocol.– Switchover Duration Threshold: When the duration of abnormal channel playback reaches the threshold, the system automatically pulls another stream for playback.– Priority Settings: Select PRIMARY (mainly the primary input) or EQUAL (switchover between primary and standby inputs) as needed.● Primary Input Parameters of Standby Region: Flow indicates the media streams created on the Flows page of the standby region.● Standby Input Parameters of Standby Region:<ul style="list-style-type: none">– Primary/standby Input: You can enable this function to configure a standby media stream.– Flow: From the drop-down list box, select the media stream created on the Flows page of the standby region. The primary and standby streams must be in the same region and use the same protocol.– Switchover Duration Threshold: When the duration of abnormal channel playback reaches the threshold, the system automatically pulls another stream for playback.– Priority Settings: Select PRIMARY (mainly the primary input) or EQUAL (switchover between primary and standby inputs) as needed.● Audio Selectors: Up to eight audio selectors can be added. Click Add Audio Selector to add Audio Selector 1. Configure the following parameters:<ul style="list-style-type: none">– Selector Name: Enter an audio selector name using only letters, digits, hyphens (-), and underscores (_). The name of each selector in the same channel must be unique.– Selector Settings:<ul style="list-style-type: none">PID selection: This mode requires specifying PID.PID: ID of the audio stream in the input source.

Parameter	Description
	<p>Language selection: This mode requires specifying Language Code and Language Selection Policy.</p> <p>Language Code: Confirm the language of each audio stream in the source input, select an audio stream, and enter the language code (2–3 lowercase letters) of that audio stream. For example, eng indicates English.</p> <p>Language Selection Policy: The value LOOSE indicates that the audio stream language is loosely matched with the selected language code. In the example of eng, the audio stream whose language is English in the source input will be preferentially selected. If audio streams in the language represented by the selected language code cannot be found, the audio stream with the lowest PID will be selected. The value STRICT indicates that the audio stream language is strictly matched with the selected language code. In the example of eng, only audio streams in English in the source input will be selected. If audio streams in the language represented by the selected language code cannot be found, a muted segment will be automatically added. When a device uses this audio selector to play a video, the playback is muted.</p>


Step 5 Click **Next**.

Table 5-2 shows **Output Settings**.

Table 5-2 Parameters

Item	Parameter	Description
Audio Output	Add Audio Output	<p>This parameter (optional) is displayed when the input type is HLS_PULL, SRT_PULL, or SRT_PUSH.</p> <p>You can bind an audio selector in Audio Output and set the language and stream name to be displayed in either of the following cases:</p> <ul style="list-style-type: none">• The actual audio language and stream name are not displayed during channel output playback.• You need to change the language and stream name of the audio. <p>Note: Each Audio Output allows binding only one audio selector, and the audio selector of each Audio Output must be unique. Therefore, Audio Output configurations cannot outnumber audio selectors.</p> <p>Specifically, click Add Audio Output and add Audio Output 1 by configuring the following parameters:</p> <ul style="list-style-type: none">• Audio Output Name: Enter a name consisting of letters, digits, hyphens (-), and underscores (_). Each audio output name of the same channel must be unique.• Selector Name: Select a configured audio selector from the drop-down list. The audio selector of each audio output must be unique.• Language Code Control: This setting changes only the displayed audio language, not the actual one. Options:<ul style="list-style-type: none">– Follow input: If the output audio of the selected audio selector has a language, the language code and stream name of the output audio will be used. Otherwise, the language code and stream name configured here will be used. The default value is recommended.– User-defined: You can customize the language code and stream name of the output audio.• Language Code: Enter a language code consisting of two or three lowercase letters. For example, eng indicates English.• Stream Name (Optional): stream name displayed on the GUI

Item	Parameter	Description
Transcoding Settings	Transcoding Template	<p>Select one or more created Media Live transcoding templates. For details, see Creating a Transcoding Template.</p> <p>If you select multiple transcoding templates, they must meet the following requirements:</p> <ul style="list-style-type: none">• Each template must use a different video bitrate.• The settings of Use Source I-Frame, GOP Unit, GOP Size, and Video Frame Rate must be identical across all selected templates.• If a template is modified during live transcoding and this results in mismatched GOP size, GOP unit, or video frame rate settings across templates, no output stream will be generated.• If Use Source I-Frame is disabled, the channel supports only one input and up to six outputs.
Other	Catch-Up TV and Time-Shifted Viewing	<p>Enabling this function requires setting Startover Window, that is, the duration of the catch-up TV content that can be viewed of a channel.</p> <p>Unit: second.</p> <p>For details, see Obtaining a Catch-Up TV/Time-Shifted Viewing URL.</p> <p>NOTE</p> <ul style="list-style-type: none">• The OBS path for storing live recordings is <i>OBS address/push_domain/AppName/Channelid</i>.• After deleting channel A, use the ingest domain name, App Name, and channel ID of channel A to create channel B. If the recordings of channel A are not completely aged, the catch-up TV URL created by channel B can be used to view the recordings of channel A. The recordings of channel A cannot be viewed when they are completely aged.
Output Segment Parameters	Segment Duration	<p>Duration of a single segment. The value defaults to 4s and must be an integer multiple of the GOP duration.</p> <p>The value ranges from 1 to 10, in second.</p> <p>CAUTION</p> <p>Exercise caution when changing the segment duration, as this operation will affect the time-shifted viewing of catch-up TV content.</p>

Item	Parameter	Description
<p>Output Group Settings</p> <p>NOTE You can click  on the right to add multiple output types.</p>	<p>Output Protocol</p>	<p>Protocol used for video output.</p> <p>Options:</p> <ul style="list-style-type: none">• HLS• DASH• MSS

Item	Parameter	Description
	HLS	<p>Configure the following parameters:</p> <ul style="list-style-type: none">• Live Playlist Window Duration: total duration of all playable media segments in the index file, in seconds• Distribution URL: Select a streaming domain name from the first drop-down list box and enter a playback address in the second drop-down list. After both are assembled, a streaming URL is generated. Example for HLS: <code>https://live-play.example.com/{channelld}/hls/{unique_string}/index.m3u8</code> Streaming URLs support HTTPS. You need to configure an HTTPS certificate by referring to HTTPS Certificates. <p>NOTICE</p> <ul style="list-style-type: none">- If Input Type is set to RTMP_PUSH or SRT_PUSH in Step 4, the streaming domain name configured here and the ingest domain name configured in Input Type must be in the same region.- If Input Type is set to FLV_PULL, HLS_PULL, or SRT_PULL in Step 4 and multiple output types have been set, the streaming domain names of all output types must be in the same region.- Neither encrypted nor unencrypted MSS streams (H.265) can be output. <ul style="list-style-type: none">• Stream Selection: Sort HLS, DASH, and MSS output streams by video bitrate. The configuration is as follows:<ul style="list-style-type: none">- Stream Order: Sort output streams by video bitrate. The default value is Original. Options:<ul style="list-style-type: none">Original: sorts the output streams in the same order as the input streams.Ascending: sorts the output streams by bitrate, from lowest to highest.Descending: sorts the output streams by bitrate, from highest to lowest.- Min Video Bitrate (bit/s): lowest video bitrate allowed for output streams. Only video streams at or above this bitrate are included in the output.- Max Video Bitrate (bit/s): highest video bitrate allowed for output streams. Only video streams at or below this bitrate are included in the output.• DRM Encryption: To enable DRM encryption, configure the parameters in Table 5-3.

Item	Parameter	Description
		<p>NOTICE</p> <ul style="list-style-type: none">- It is recommended that DRM encryption be enabled and the FunctionGraph proxy access mode be used. If the HTTPS direct access mode is used, you are advised to add an authentication header.- If you need to enable DRM encryption for a channel and set Interconnection Mode to FunctionGraph proxy access to provide the key for integrating DRM, you need to: enable FunctionGraph agency in advance by referring to Cloud Resource Authorization; create a function on FunctionGraph.- If the DRM system is faulty, 404 is returned.

Item	Parameter	Description
	DASH	<p>Configure the following parameters:</p> <ul style="list-style-type: none">● Manifest Window Duration: total duration of all playable media segments in the index file, in seconds● Streaming Delay: corresponds to the attribute suggestedPresentationDelay, which indicates the suggested streaming delay for the player. The value (in seconds) ranges from 1 to 120 and defaults to 20.● Minimum Update Period: corresponds to the attribute minimumUpdatePeriod, which indicates the suggested minimum interval for the player to update the MPD. The value (in seconds) ranges from 1 to 120 and defaults to 2.● Minimum Buffer Time: corresponds to the attribute minBufferTime, which indicates the suggested buffering duration for the player. The value (in seconds) ranges from 1 to 120 and defaults to 10.● Distribution URL: Select a streaming domain name from the first drop-down list box and enter a playback address in the second drop-down list. After both are assembled, a streaming URL is generated. Example for DASH: <code>https://live-play.example.com/{channelId}/dash/{unique_string}/index.mpd</code> Streaming URLs support HTTPS. You need to configure an HTTPS certificate by referring to HTTPS Certificates. <p>NOTICE</p> <ul style="list-style-type: none">- If Input Type is set to RTMP_PUSH or SRT_PUSH in Step 4, the streaming domain name configured here and the ingest domain name configured in Input Type must be in the same region.- If Input Type is set to FLV_PULL, HLS_PULL, or SRT_PULL in Step 4 and multiple output types have been set, the streaming domain names of all output types must be in the same region.- Neither encrypted nor unencrypted MSS streams (H.265) can be output. <ul style="list-style-type: none">● Stream Selection: Sort HLS, DASH, and MSS output streams by video bitrate. The configuration is as follows:<ul style="list-style-type: none">- Stream Order: Sort output streams by video bitrate. The default value is Original.

Item	Parameter	Description
		<p>Options:</p> <p>Original: sorts the output streams in the same order as the input streams.</p> <p>Ascending: sorts the output streams by bitrate, from lowest to highest.</p> <p>Descending: sorts the output streams by bitrate, from highest to lowest.</p> <ul style="list-style-type: none"> - Min Video Bitrate (bit/s): lowest video bitrate allowed for output streams. Only video streams at or above this bitrate are included in the output. - Max Video Bitrate (bit/s): highest video bitrate allowed for output streams. Only video streams at or below this bitrate are included in the output. <ul style="list-style-type: none"> ● DRM Encryption: To enable DRM encryption, configure the parameters in Table 5-3. <p>NOTICE</p> <ul style="list-style-type: none"> - It is recommended that DRM encryption be enabled and the FunctionGraph proxy access mode be used. If the HTTPS direct access mode is used, you are advised to add an authentication header. - If you need to enable DRM encryption for a channel and set Interconnection Mode to FunctionGraph proxy access to provide the key for integrating DRM, you need to: enable FunctionGraph agency in advance by referring to Cloud Resource Authorization; create a function on FunctionGraph. - If the DRM system is faulty, 404 is returned.

Item	Parameter	Description
	MSS	<p>Configure the following parameters:</p> <ul style="list-style-type: none">● Manifest Window Duration: total duration of all playable media segments in the index file, in seconds● Distribution URL: Select a streaming domain name from the first drop-down list box and enter a playback address in the second drop-down list. After both are assembled, a streaming URL is generated. Example for MSS: <code>https://live-play.example.com/{channelId}/mss/{unique_string}.ism/Manifest</code> Streaming URLs support HTTPS. You need to configure an HTTPS certificate by referring to HTTPS Certificates. <p>NOTICE</p> <ul style="list-style-type: none">- If Input Type is set to RTMP_PUSH or SRT_PUSH in Step 4, the streaming domain name configured here and the ingest domain name configured in Input Type must be in the same region.- If Input Type is set to FLV_PULL, HLS_PULL, or SRT_PULL in Step 4 and multiple output types have been set, the streaming domain names of all output types must be in the same region.- Neither encrypted nor unencrypted MSS streams (H.265) can be output. <ul style="list-style-type: none">● Stream Selection: Sort HLS, DASH, and MSS output streams by video bitrate. The configuration is as follows:<ul style="list-style-type: none">- Stream Order: Sort output streams by video bitrate. The default value is Original. Options:<ul style="list-style-type: none">Original: sorts the output streams in the same order as the input streams.Ascending: sorts the output streams by bitrate, from lowest to highest.Descending: sorts the output streams by bitrate, from highest to lowest.- Min Video Bitrate (bit/s): lowest video bitrate allowed for output streams. Only video streams at or above this bitrate are included in the output.- Max Video Bitrate (bit/s): highest video bitrate allowed for output streams. Only video streams at or below this bitrate are included in the output.● DRM Encryption: To enable DRM encryption, configure the parameters in Table 5-3.

Item	Parameter	Description
		<p>NOTICE</p> <ul style="list-style-type: none"> - It is recommended that DRM encryption be enabled and the FunctionGraph proxy access mode be used. If the HTTPS direct access mode is used, you are advised to add an authentication header. - If you need to enable DRM encryption for a channel and set Interconnection Mode to FunctionGraph proxy access to provide the key for integrating DRM, you need to: enable FunctionGraph agency in advance by referring to Cloud Resource Authorization; create a function on FunctionGraph. - If the DRM system is faulty, 404 is returned.

Table 5-3 DRM configuration

Parameter	Description
Resource ID	Content resource ID provided by the DRM system
SPEKE Version	AWS SPEKE version. Currently, only version 1.0 is supported. For details, see SPEKE . This protocol must comply with license requirements .
DRM System	DRM encryption type. Constraints: <ul style="list-style-type: none"> • The HLS output protocol supports FairPlay. • The DASH output protocol supports Widevine, PlayReady, and PlayReady + Widevine. • The MSS protocol supports only PlayReady.
Encryption Level	DRM encryption level. The encryption key needs to be obtained from the DRM vendor. Options: <ul style="list-style-type: none"> • content: Each channel has one specific DRM encryption key. • profile: Each stream of a channel has one specific DRM encryption key. <p>Constraints: HLS and DASH streams support both preceding encryption modes, while MSS streams support only content encryption.</p>

Parameter	Description
Interconnection Mode	<p>Mode of interconnecting with a DRM system. Options:</p> <ul style="list-style-type: none">• HTTPS direct access: Enter an HTTPS URL to obtain the DRM system. HTTP URLs cannot be used. Key and Value in the header are used to verify the accuracy and validity of the URL used for obtaining the DRM system. These two fields are optional. To add them, click Add a Header and specify Header Key and Header Value. A maximum of five groups of Key and Value can be added, but each Key must be unique.• FunctionGraph proxy access: You can build a function using FunctionGraph to package the obtained Key and Value. Key and Value can be dynamically obtained using functions. Other token authentication methods are also supported. This mode requires enabling FunctionGraph agency (see Cloud Resource Authorization) to authorize Media Live to call FunctionGraph functions. This mode also requires specifying the Function parameter in FunctionGraph Region and selecting a region and a function from the drop-down list. <p>NOTICE When FunctionGraph is used for DRM-based channel encryption, the FunctionGraph version information is not contained. By default, the latest version is used.</p>
URL	<p>URL of the key for DRM encryption.</p> <ul style="list-style-type: none">• HTTPS direct access requires entering an HTTPS URL.• If FunctionGraph proxy access is selected, the URL is automatically filled in and cannot be changed.
Standby FunctionGraph	<p>You can enable this function and configure the following parameters:</p> <ul style="list-style-type: none">• FunctionGraph Region: Select the region of the standby FunctionGraph.• Function: Select a function from the drop-down list.• URL: The URL is automatically filled in and cannot be changed.

Step 6 Click **Finish**. A new channel is added to the **Channels** page.

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

----End

5.2 Managing Channels

After a channel is created, you can view the channel information and running status on the channel management page. You can also disable, enable, modify, or delete the channel as required.

Procedure

Step 1 Log in to the [Live console](#).

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

Step 3 Perform the following operations as required.

- Starting a channel

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

- Stopping a channel

Click **Stop** in the **Operation** column to stop the channel.

- Modifying a channel

Click **Manage** in the **Operation** column to modify the channel information.

If you select multiple transcoding templates when modifying the channel, all transcoding templates must meet the following conditions:

- Each template must use a different video bitrate.
- The settings of **Use Source I-Frame**, **GOP Unit**, **GOP Size**, and **Video Frame Rate** must be identical across all selected templates.
- If a template is modified during live transcoding and this results in mismatched GOP size, GOP unit, or video frame rate settings across templates, no output stream will be generated.
- If **Use Source I-Frame** is disabled, the channel supports only one input and up to six outputs.

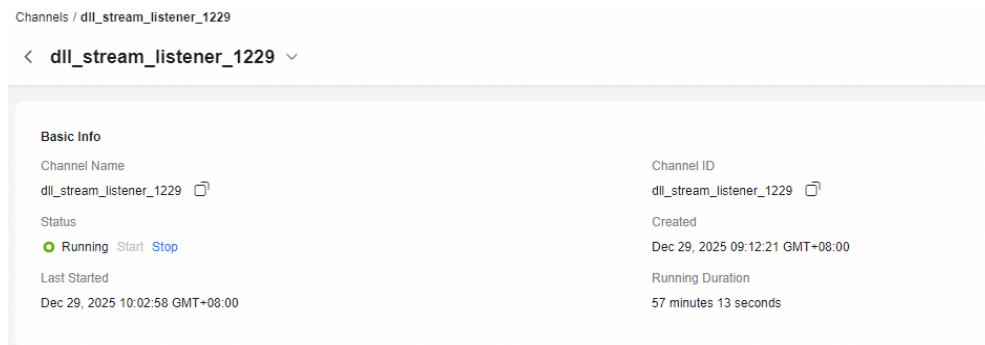
You need to restart the channel for the modification to take effect. If the channel has been started, it will automatically restart after the modification. This restart takes about 30 seconds.

Note: The restart operation will interrupt the connection to the headend encoder, and consequently interrupt the media stream. You will need to manually push the stream again after the restart is complete.

- Viewing the configuration and running status of a channel

Click the channel ID or **View Details** in the **Operation** column. The channel details page is displayed, where you can view the basic information and running status of the channel, as shown in [Figure 5-3](#).

Figure 5-3 Channel details



- Deleting a channel

Stop the channel and then choose **More > Delete** in the **Operation** column to delete the channel. If there is an ongoing live-to-VOD task in the channel, the channel cannot be deleted until the task is completed.

----End

6 Media Processing

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 low-bitrate HD is selected in the transcoding template, live transcoding is billed according to the low-bitrate HD billing standard. For details, see [Live Pricing Details](#).

- Upsampling transcoding is not supported, that is, the resolution and frame rate of transcoded outputs cannot be higher than those of the source stream. Even if you specify a resolution higher than the source stream in the template, the streaming URL generated for transcoded streams will be functional, but the streams will still be played at the original resolution. Upsampling is not supported for the frame rate either.
- 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 configured](#) at your domains' DNS provider.

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, choose **Media Processing > Live Transcoding** under **Media Live**.

Step 3 Click **Create Transcoding Template**. The **Transcoding** page is displayed on the right, as shown in [Figure 6-1](#).

Configure transcoding parameters as instructed by [Table 6-1](#).

Figure 6-1 Creating a transcoding template

×

Transcoding

Template Name

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

Triggered By

Stream push ▼

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

Transcoding Type

Standard transcoding ▼

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

Video Encoding

H.264 H.265

Presets (Optional)

360p

540p

720p

1080p

1440p

Custom

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

Video Bitrate

 Kbit/s

Bitrate Control ?

Disabled ▼

Resolution (W x H)

+

Cancel

OK

Table 6-1 Transcoding settings

Parameter	Description
Template Name	Name of a Media Live transcoding template. You can customize the name in letters, digits, and hyphens (-).
Triggered By	Transcoding is triggered by stream push.
Transcoding Type	Transcoding type of Media Live. Options: <ul style="list-style-type: none">● 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 transcoding means achieving the same image quality at a lower output bitrate. If you enable this function, you will be billed based on the rates of low-bitrate HD transcoding. For details, see Live Pricing Details .
Video Encoding	Supported video encoding formats: <ul style="list-style-type: none">● H.264● H.265 NOTICE <ul style="list-style-type: none">- Only one encoding format can be selected for a channel.- H.265 is displayed only when Input Type of a created channel is set to SRT_PUSH, HLS_PULL, SRT_PULL, or STREAM_CONNECT.
Presets (Optional)	Resolution levels: <ul style="list-style-type: none">● 360p● 540p● 720p● 1080p● 1440p● Custom Select a level to see preset values for Video Bitrate and Resolution (W x H) below. Change them as needed.
Video Bitrate	Average bitrate of the transcoded video, in Kbit/s. Value range: 40 to 30,000

Parameter	Description
Bitrate Control	<p>Bitrate control policy.</p> <p>Options:</p> <ul style="list-style-type: none">● Disabled: Bitrate adaptation is disabled. The target bitrate is output as specified.● Not higher than source stream: The target bitrate is the smaller value between the specified bitrate and the bitrate of the source file.● Adaptive to source stream: The target bitrate is adaptive to the bitrate of the source file. <p>Default value: Disabled</p>
Resolution (W x H)	<p>Width and height of the video, in pixel.</p> <p>If the input value of both sides is set to 0, the video is output using the resolution of the source stream. If the value of one side is set to 0, the value of that side will be converted proportionally according to the input value of the other side.</p> <p>Value range:</p> <ul style="list-style-type: none">● Width: The value must be 0 or a multiple of 2 between 32 and 3,840.● Height: The value must be 0 or a multiple of 2 between 32 and 2,160. <p>NOTICE</p> <ul style="list-style-type: none">- The transcoded output resolution cannot be higher than the input resolution.
Video Frame Rate	<p>Frame rate of the transcoded video.</p> <p>Options:</p> <ul style="list-style-type: none">● Retain the original● Set a new one: If you select this option, you need to enter the frame rate. The value ranges from 0 to 60. 0 means adaptive frame rate. <p>The output frame rate cannot exceed the input frame rate. If a higher output frame rate is specified, the system defaults to using the source stream's frame rate.</p>
B-Frame Removal	<p>After this function is enabled, the transcoded video does not contain B-frames.</p>

Step 4 Click **OK**.

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

----End

Managing Transcoding Templates

You can perform the following operations on your transcoding template:

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

6.2 Creating a Watermark Template

You can create an image watermark template.

Procedure

- Step 1** Log in to the [Live console](#).
- Step 2** In the navigation pane, choose **Media Processing > Watermark Templates** under **Media Live**.
- Step 3** Click **Create**. The **Create Watermark Template** page is displayed, as shown in [Figure 6-2](#).

Configure watermark template parameters by referring to [Table 6-2](#). You can preview the watermark in the area on the right.

Figure 6-2 Watermark template configuration

< | Create Watermark Template

Template Name
Enter a value.

Template Description
Enter a value.

Watermark Type
Image

Watermark Image URL
Enter a value.
PNG and JPG only. Enter an authentication-free download URL and ensure content compliance.

Watermark Position
Upper left

Offset Unit
%

Horizontal Offset
0% 49% 99% -- 0.00 + %
Horizontal distance between the watermark and the reference position, as a proportion of output video width.

Vertical Offset
0% 49% 99% -- 0.00 + %
Vertical distance between the watermark and the reference position, as a proportion of output video height.

Preview (1280 x 720)

Cancel OK

Table 6-2 Watermark template configuration

Parameter	Description
Template Name	Enter a template name.
Template Description	Enter the template description.
Watermark Type	Currently, only image watermarks are supported.
Watermark Image URL	<p>URL of the watermark image.</p> <ul style="list-style-type: none"> Currently, only PNG and JPG images are supported. Enter an authentication-free download path and ensure the image compliance. If the width or height of the watermark image exceeds 2560 pixels, real-time transcoding may be affected. You need to adjust the width and height of the image to be within 2560 pixels. <p>Example: <code>https://{IP address}/watermark.png</code></p>
Watermark Position	The options are Upper left , Upper right , Lower left , Lower right , and Random . If you select Random , the image watermark may appear in the upper left, upper right, lower left, or lower right of the video.
Offset Unit	Unit of horizontal or vertical offset. The options are % and px .
Horizontal Offset	The image watermark can move horizontally in the preview area on the right.
Vertical Offset	The image watermark can move vertically in the preview area on the right.
Watermark Size (W x H)	<p>Set the watermark's width or height in percentage (%) or pixel (px).</p> <ul style="list-style-type: none"> If the unit is %, the parameter's value sets the watermark's width and height as a percentage of the output video's width and height. If the unit is px, the watermark's width and height are the specified values (range: 8 to 4,096). <p>Note:</p> <ul style="list-style-type: none"> If the watermark's width or height is left empty or set to 0, the watermark size will be scaled accordingly. If both the watermark's width and height are left empty or set to 0, the input and output resolutions are the same. You are advised to set either the width or the height to avoid watermark distortion.

Parameter	Description
Previewed Watermark Size	Size of the preview area on the right. Set it based on the video resolution.

Step 4 Click **OK**.

A new watermark template is added to the **Watermark Templates** page. You can also perform the following operations on the watermark template:

- Click **Modify** in the **Operation** column of the watermark template. On the **Create Watermark Template** page, modify the watermark configuration.
- Click **Delete** in the **Operation** column of the watermark template to delete the template.

----End

6.3 Creating a Watermark Rule

You can create a watermark template for a channel to safeguard its video streams. If a channel has multiple transcoding templates, you can create a watermark template for each transcoding template.

Prerequisites

You have created a channel by referring to [Creating a Channel](#), and the channel ID exists.

Procedure

Step 1 Log in to the [Live console](#).

Step 2 In the navigation pane, choose **Media Processing** > **Watermark Rules** under **Media Live**.

Step 3 Click **Create**. The **Create Watermark Rule** page is displayed, as shown in [Figure 6-3](#).

Create a watermark rule based on [Table 6-3](#). You can preview the watermark in the area on the right.

Figure 6-3 Watermark rule configuration

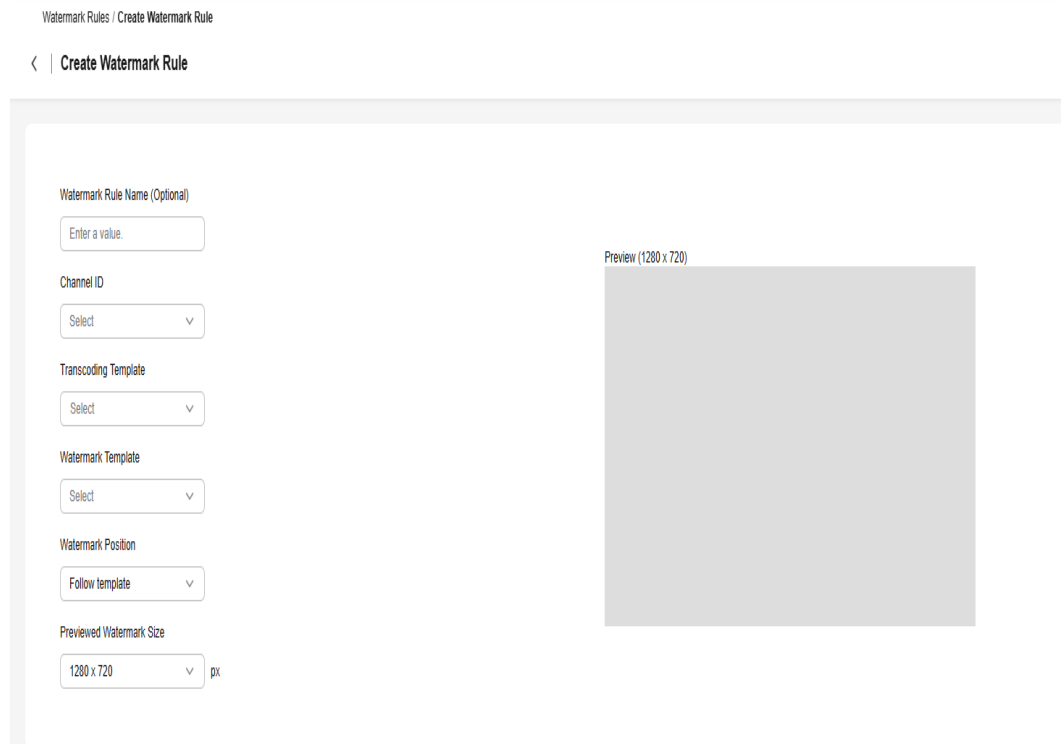


Table 6-3 Watermark rule configuration

Parameter	Description
Watermark Rule Name (Optional)	Enter a watermark rule name.
Channel ID	Select the ID of the channel on which you want to overlay a watermark from the drop-down list.
Transcoding Template	If a channel has multiple transcoding templates, you can create a watermark template for each transcoding template. You can select one or more transcoding templates.
Watermark Template	Select the watermark template created in Creating a Watermark Template from the drop-down list.

Parameter	Description
Watermark Position	Position of the watermark in the video. Options: <ul style="list-style-type: none">● Follow template: The watermark's position is determined by the selected watermark template.● Upper left, Upper right, Lower left, Lower right, and Random: Select one of these options to reset the watermark position. If you select Random, the image watermark may appear in the upper left, upper right, lower left, or lower right of the video.
Offset Unit	Unit of horizontal or vertical offset. The options are % and px .
Horizontal Offset	The image watermark can move horizontally in the preview area on the right.
Vertical Offset	The image watermark can move vertically in the preview area on the right.
Previewed Watermark Size	Size of the preview area on the right. Set it based on the video resolution.

Step 4 Click **OK**.

A new watermark rule is added to the **Watermark Rules** page. You can also perform the following operations on the watermark rule:

- Click **Modify** in the **Operation** column of the watermark rule. On the **Create Watermark Rule** page, modify the watermark rule.
- Click **Delete** in the **Operation** column of the watermark rule to delete the rule.

----**End**

7 Service Monitoring

You can view the following information on the **Service Monitoring** page:

- **CDN Downstream Bandwidth/Traffic:** downstream bandwidth or traffic usage of streaming domain names, that is, the downstream bandwidth or traffic used by clients to pull streams from CDN
- **CDN Status Codes:** all status codes returned by CDN in response to the stream pull requests by Media Live, and the trend chart of these status codes
- **CDN Concurrent Downstream Requests:** downstream concurrent requests of the streaming domain name, that is, the downstream concurrent requests by the client to pull streams from CDN
- **Transcoding Metrics:** including **Input bandwidth, Input video frame rate, Input disconnections, Dropped packets, Input switches for failover, Continuity errors, PID errors, Dropped frames, Duration of input without received packets,** and **Output bandwidth,** and the trend charts of these metrics
- **Packaging Metrics:** including **2xx status codes, 4xx status codes, 5xx status codes, HLS requests, DASH requests, MSS requests, Input traffic,** and **Output traffic,** and the trend charts for these metrics

Notes

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

Procedure

- Step 1** Log in to the [Live console](#).
- Step 2** In the navigation pane on the left, choose **Service Monitoring** under **Media Live**.
- Step 3** Select [CDN Downstream Bandwidth/Traffic](#), [CDN Status Codes](#), [CDN Concurrent Downstream Requests](#), [Transcoding Metrics](#), or [Packaging Metrics](#) to view the statistics.

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

----End

CDN Downstream Bandwidth/Traffic

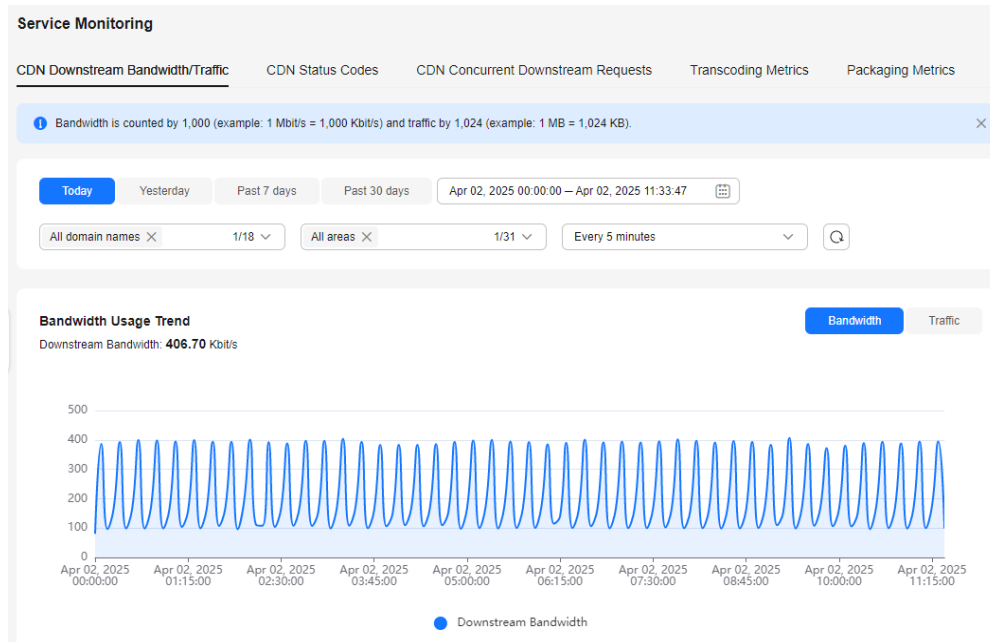
NOTE

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

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

- **Bandwidth Usage Trend** displays the bandwidth usage trend of the selected domain name, as shown in [Figure 7-1](#). **Downstream Bandwidth: 2.00 Mbit/s** indicates the downstream peak bandwidth of the selected domain name in the query period.

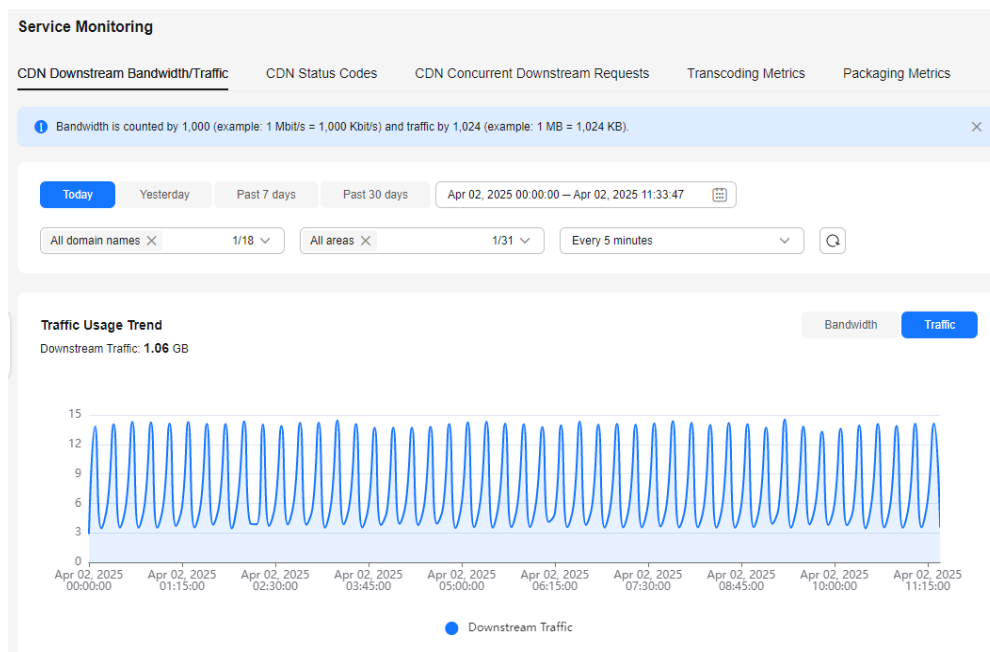
Figure 7-1 CDN downstream bandwidth statistics



- **Traffic Usage Trend** displays the traffic usage trend of the selected domain name, as shown in [Figure 7-2](#). **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 bytes into MB, accurate to two decimal places.

Figure 7-2 CDN downstream traffic statistics



CDN Status Codes

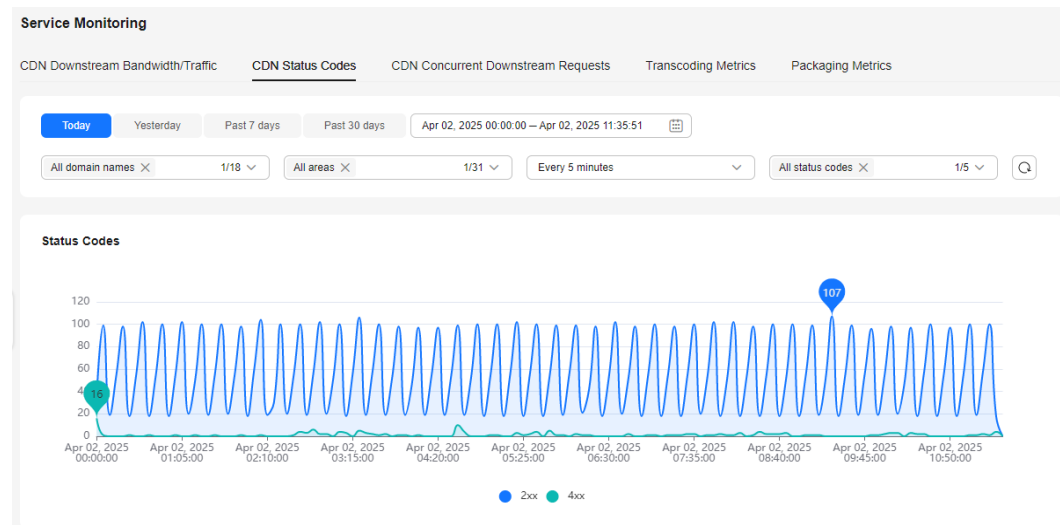
NOTE

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

You can specify the time, streaming domain name, area, statistical granularity, and status code to view the trend chart of the corresponding status code, as shown in [Figure 7-3](#).

The trend chart shows the number of status codes returned by CDN in response to the stream pull requests by Media Live.

Figure 7-3 CDN status code statistics



CDN Concurrent Downstream Requests

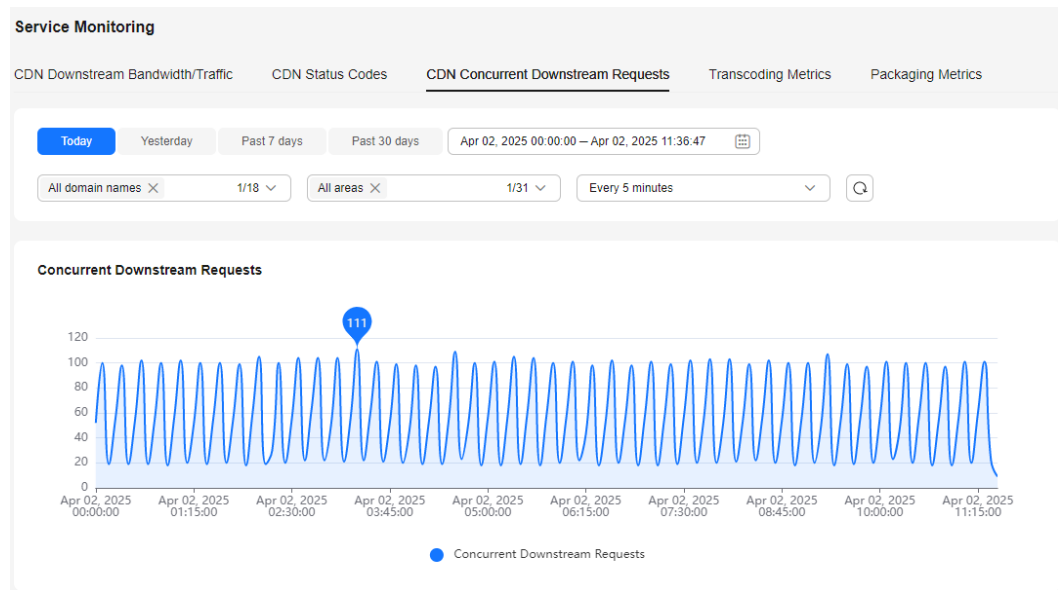
NOTE

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

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

The trend chart shows the number of downstream concurrent requests by the client to pull streams from CDN.

Figure 7-4 Trend chart of CDN concurrent downstream requests



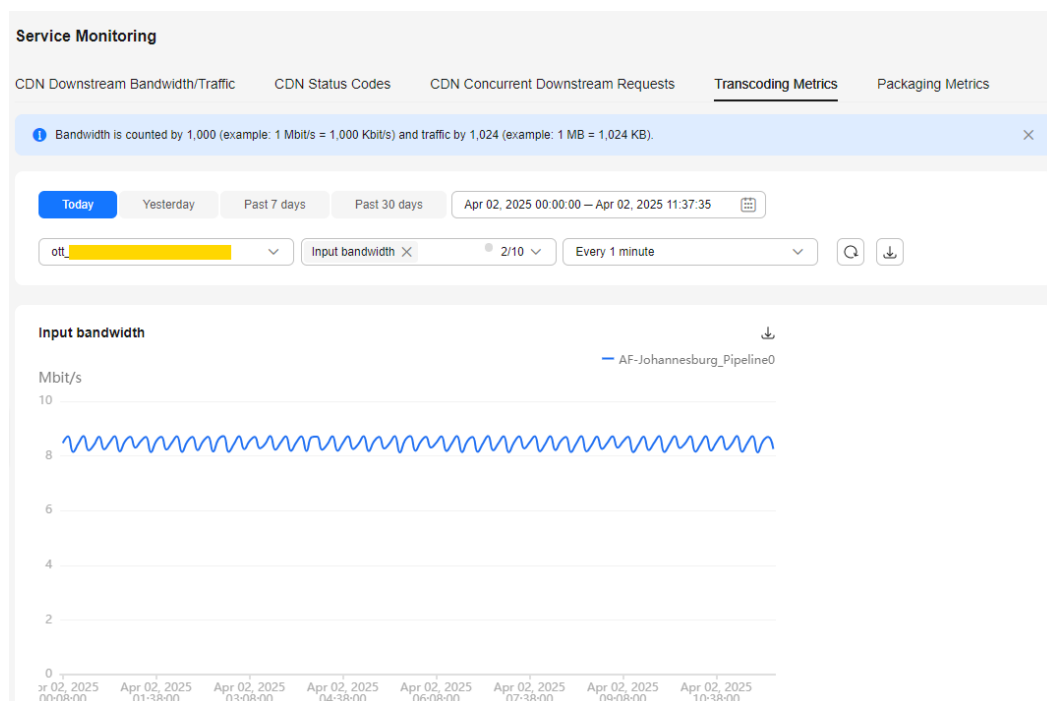
Transcoding Metrics

NOTE

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

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

Figure 7-5 Trend chart



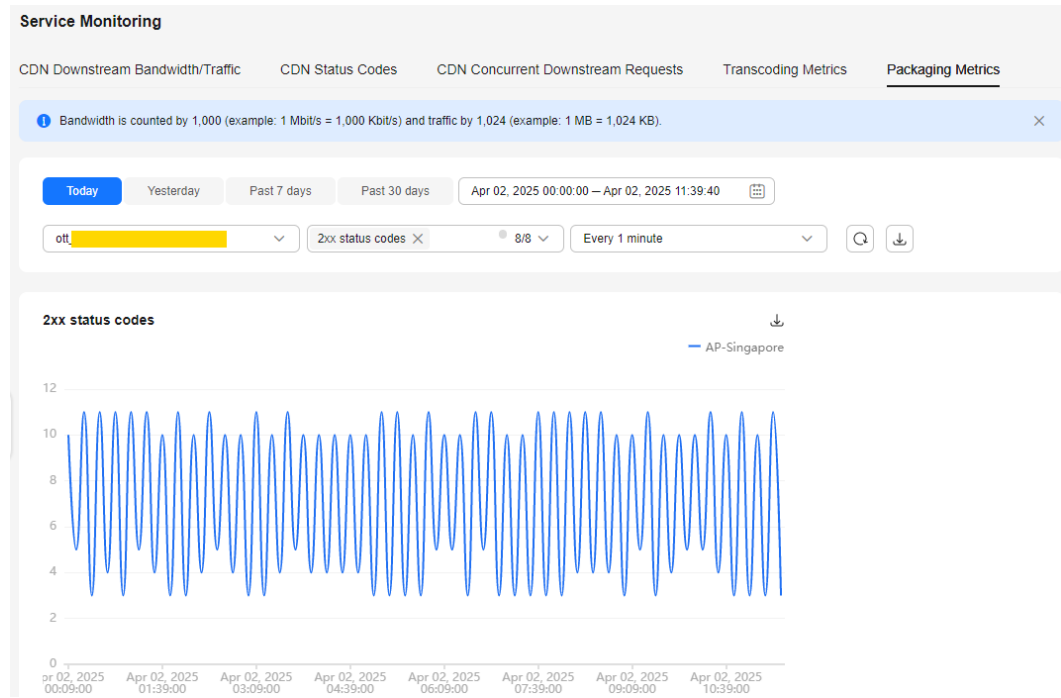
Packaging Metrics

NOTE

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

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

Figure 7-6 Trend chart of packaging metrics



8 Cloud Resource Authorization

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

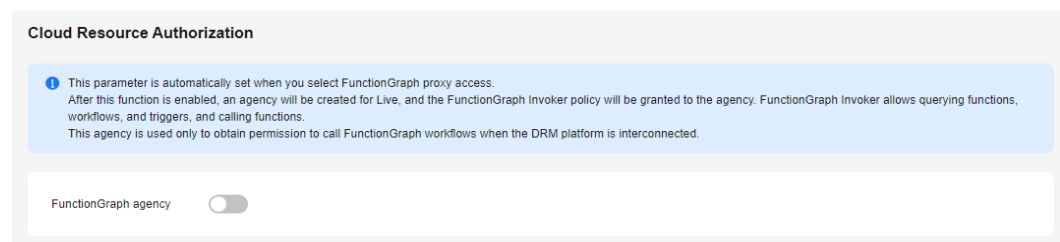
Procedure

Step 1 Log in to the [Live console](#).

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

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

Figure 8-1 Cloud resource authorization



Step 3 Go to the [IAM console](#).

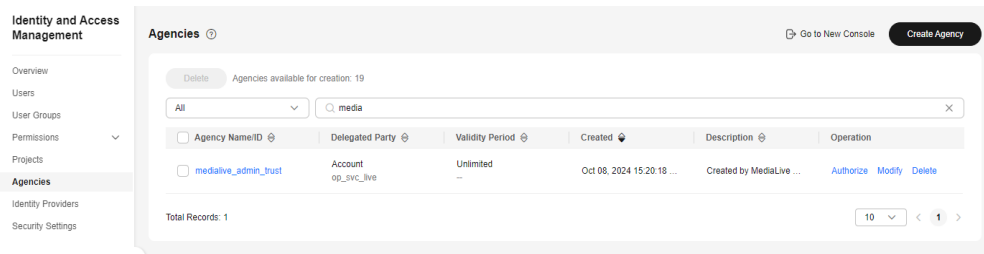
Step 4 In the navigation pane, choose **Agencies**, as shown in [Figure 8-2](#).

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

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

medialive_admin_trust will be automatically re-created and its permissions will be reset to the default permissions.

Figure 8-2 IAM agencies



-----End

9 Tools

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

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

Constraints

- You have created a channel, as shown in [Creating a Channel](#). The channel is running and **Catch-Up TV and Time-Shifted Viewing** has been enabled.
- HLS stream pull will not generate a URL for hotlink protection.

Procedure

Step 1 Log in to the [Live console](#).

Step 2 In the navigation pane, choose **Tools > Catch-Up TV/Time-Shifted Viewing URL Generation** under **Media Live** to go to the **Catch-Up TV/Time-Shifted Viewing URL Generation** page, as shown in [Figure 9-1](#).

See [Table 9-1](#).

Figure 9-1 Catch-up TV/Time-shifted viewing URL generation

Catch-Up TV/Time-Shifted Viewing URL Generation

Channel ID

Streaming URL

Catch-up TV Time-shifted viewing


Started


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

Ended

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


Table 9-1 Parameters

Parameter	Description
Channel ID	Select the ID of the desired channel from the drop-down list box. Before selecting a channel, click  on the right to hide deleted channels or channels with catch-up TV/time-shifted viewing disabled.
Streaming URL	Select the streaming URL of the channel from the drop-down list box.

Parameter	Description
Catch-up TV	<p>Configure the following parameters:</p> <ul style="list-style-type: none">• Started: When catch-up TV/time-shifted viewing is enabled for a channel, you need to set Startover Window. Users can view only the recorded content within the startover window. <p>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.</p> <p>NOTICE The start time must be earlier than the current time. For example, if the current time is 14:51 on August 16, the start time must be earlier than 14:51 on August 16.</p> <ul style="list-style-type: none">• Ended: A catch-up TV URL can be used to watch catch-up TV content of up to 24 hours, so the end time can be at most one day later than the start time.
Time-shifted viewing	<p>Configure the following parameters:</p> <p>Time-Shifted Duration: Enter a value for hour, minute, and second, respectively. The maximum value is 24 hours. When catch-up TV/time-shifted viewing is enabled for a channel, you need to set Startover Window. Users can view only the recorded content within the startover window.</p>

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

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

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

----End

9.2 Querying SCTE Signals

You can query SCTE-35 signal events of channel inputs.

Prerequisites

You have created a channel by referring to [Creating a Channel](#), and the channel ID exists.

Procedure

Step 1 Log in to the [Live console](#).

Step 2 In the navigation pane, choose **Tools > SCTE Signals** under **Media Live**. The **SCTE Signals** page is displayed, as shown in [Figure 9-2](#).

You can configure the following filter parameters:

- Channel ID: Select the desired channel ID from the drop-down list.
- Region: If a channel supports primary/standby regions, you can query SCTE signals in the primary region, standby region, or both.
- Ad type: Select **Splice Insert**, **Time Signal**, or **ALL Type** from the drop-down list.
- Query time span: You can query data within the past half hour or one hour. You can also select **Custom** to query data of a maximum of past seven days.

Figure 9-2 Querying SCTE signals

The screenshot shows the 'SCTE Signals' interface with the following data in the table:

Channel ID	Region	Event ID	Started	Duration (s)	Type	Segmentation Type	Operation
wfestsrtpush121...	CN North...	1	Dec 16, 2025 19:55:26 GMT+08:00	20 s	Time Signal	ProviderPlacementOpportunityStart	View Raw Data
wfestsrtpush...	CN North...	1	Dec 16, 2025 19:53:17 GMT+08:00	20 s	Time Signal	ProviderPlacementOpportunityStart	View Raw Data
wfestsrtpush...	CN North...	1	Dec 16, 2025 19:38:30 GMT+08:00	20 s	Time Signal	ProviderPlacementOpportunityStart	View Raw Data
wfestsrtpush...	CN North...	1	Dec 16, 2025 19:31:58 GMT+08:00	20 s	Time Signal	ProviderPlacementOpportunityStart	View Raw Data
wfestsrtpush...	--	1	Dec 16, 2025 15:16:45 GMT+08:00	20 s	Time Signal	ProviderPlacementOpportunityStart	View Raw Data

Total Records: 5

See [Table 9-2](#).

Table 9-2 Query result list

Parameter	Description
Channel ID	ID of the channel to be queried.
Region	Primary or standby region of the channel to be queried.
Event ID	ID of the SCTE-35 signal event of the channel input to be queried.
Started	Time when the ad signal execution starts, that is, the program date time (PDT) of the first TS segment when the ad starts playing.
Duration (s)	Duration of ad signal execution.
Type	The value can be Splice Insert or Time Signal .

Parameter	Description
Segmentation	<ul style="list-style-type: none">● When Type is Splice Insert, the value is empty.● When Type is Time Signal, the value can be:<ul style="list-style-type: none">- ProviderAdvertisementStart- ProviderAdvertisementEnd- DistributorAdvertisementStart- DistributorAdvertisementEnd- ProviderPlacementOpportunityStart- ProviderPlacementOpportunityEnd- DistributorPlacementOpportunityStart- DistributorPlacementOpportunityEnd
Operation	Click View Raw Data to open the corresponding dialog box on the right. You can view the raw data of the current SCTE ad signal.

----End

10 Third-Party CDN Interconnection (OBT)

10.1 Adding Domain Names

Media Live now supports interconnection with third-party CDNs. You need to add an origin domain name before performing subsequent operations.

Prerequisites

- The third-party CDN interconnection feature is currently in an open beta test (OBT). By default, the **Origin domain name** option is not available. You need to [submit a service ticket](#) to request access.
- If you need to configure a standby origin server, you need to add another origin domain name and set its origin region to the CN-Hong Kong region. Before doing so, you also need to [submit a service ticket](#) to apply for the permission.

Procedure

The procedure is the same as that described in [Adding Domain Names](#). You only need to set **Type** to **Origin domain name**, as shown in [Figure 10-1](#).

An HTTPS certificate must be configured for the origin domain name. For details, see [HTTPS Certificates](#). In addition, **Force HTTPS** is disabled by default and cannot be modified.

Figure 10-1 Adding a domain name

Add Domain ✕

Domain Name

Enter a value.

Uppercase domain names are not supported.

Enterprise Project

default ▼ 🔄 [Create](#)

Subservice Type ?

Cloud Live Media Live

Type

Streaming domain name Ingest domain name Origin domain name

Live Origin Server

CN North ▼

Cancel OK

If a standby origin server is required, you need to add an origin domain name for the standby origin server. If the primary origin server is in AP-Singapore, the standby origin server can be in CN-Hong Kong.

10.2 Creating a Channel

Media Live supports third-party CDNs. Before using third-party CDNs to distribute content, you need to create a channel with independent origins.

Notes

- The function of connecting to third-party CDNs is available only in the AP-Singapore, ME-Riyadh, and CN-Hong Kong regions.
- In independent origin mode, extra data transmission fees are incurred when third-party CDNs access the Media Live origin server through the Internet. For more details, submit a [service ticket](#).

Prerequisites

During the creation of a channel, the **Channel Mode** parameter is not available by default. You need to [submit a service ticket](#) to request access.

Procedure

The procedure is the same as that described in [Creating a Channel](#). You only need to note that:

- On the **Basic Info** page for creating a channel, the **Channel Mode** and **Channel Region** parameters are available, as shown in [Figure 10-2](#).

For details about the parameter settings, see [Table 10-1](#).

Figure 10-2 Creating a channel

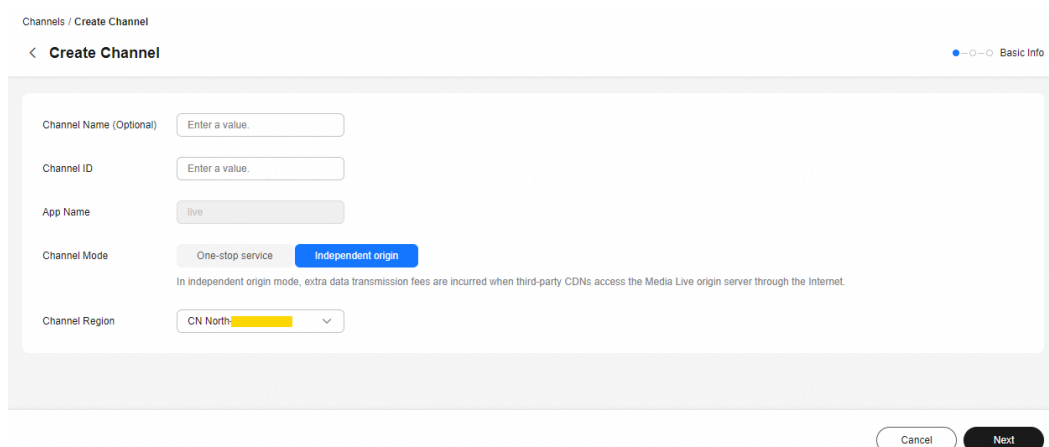


Table 10-1 Parameters

Parameter	Description
Channel Mode	<p>This parameter is available only when you have enabled the function of connecting to third-party CDNs.</p> <p>Options:</p> <ul style="list-style-type: none"> One-stop service: This is the default option for using Media Live when no third-party CDNs need to be connected, as described in Creating a Channel. Independent origin: This option is available only when you have enabled the function of connecting to third-party CDNs. In independent origin mode, extra data transmission fees are incurred when third-party CDNs access the Media Live origin server through the Internet.
Channel Region	Region where the channel connected to third-party CDNs is located.

- In the **Output Group Settings** area on the **Output Settings** page for creating a channel, some new parameters are available, as shown in [Figure 10-3](#).

For details about the parameter settings, see [Table 10-2](#).

Figure 10-3 Output group settings

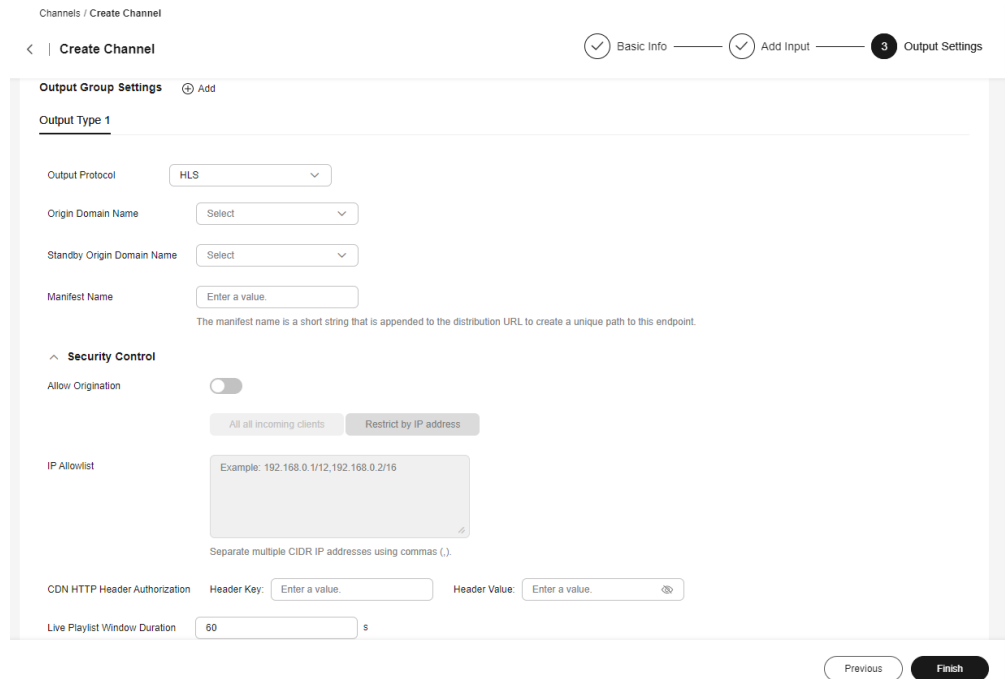


Table 10-2 Parameters

Parameter	Description
Origin Domain Name	Select the origin domain name created in Adding Domain Names .
Standby Origin Domain Name	If the primary origin domain name has been added in AP-Singapore and the standby origin domain name has been added in CN-Hong Kong, you can select the standby origin domain name from the drop-down list.
Manifest Name	The manifest name is a short string that is appended to the distribution URL to create a unique path to this endpoint. You can customize a manifest name. If you do not enter a manifest name, the default value index is used.

Parameter	Description
Security Control	<p>The security control parameters are as follows:</p> <ul style="list-style-type: none">● Allow origination: indicates whether to allow access from the Internet. By default, this option is disabled. If it is enabled, you can choose from the following options based on your actual needs:<ul style="list-style-type: none">– All incoming clients: allows access from all public IP addresses.– Restrict by IP address: does not allow access from all public IP addresses. You must specify the IP addresses allowed to access using the IP allowlist.● IP Allowlist: specifies the IP addresses allowed to access from the Internet. Use commas (,) to separate multiple CIDR IP addresses. For example, 192.168.0.1/12,192.168.0.1/16.● CDN HTTP Header Authentication: authenticates HTTP URLs that access CDN. Header Key and Header Value are used to verify the accuracy and validity of the URLs that access CDN. These two fields are optional.

11 Video Bitrate Filtering

Media Live allows you to filter output streams by video bitrate.

To achieve it, you need to:

- On the console, set **Minimum Video Bitrate (bit/s)** and **Max Video Bitrate (bit/s)**. For details, see [Creating a Channel](#).
- Add URL request parameter **pkg_manifestfilter**. For details about the parameter, see [Table 11-1](#).

[Table 11-2](#) describes the status codes returned for URL requests.

Table 11-1 URL request parameter for filtering bitrates

URL Parameter	Configuration	Description
pkg_manifestfilter	video_bitrate	Filters video bitrates, in bit/s. Value range: 0-2147483647. By default, the values at both ends are inclusive. Example value: stream.mpd?pkg_manifestfilter=video_bitrate:0-2147483647 If a range is specified, the start value must be less than the end value. Up to five ranges are supported, separated by commas (,).

Table 11-2 Status codes

S t a t u s C o d e	Bitrate Filtering Parameter Example	Error Message	Error Descript ion	Solution
200	? pkg_manifestfilter=video_bitrate:0-1	-	This is normal. Videos are filtered.	-
400	? pkg_manifestfilter=video_bitrate:0-48000&pkg_manifestfilter=video_bitrate:0-48000	parse bandwidth filter error	Duplicate bitrate filtering parameters.	Delete duplicate bitrate filtering parameters.
400	? pkg_manifestfilter=video_bitrate:rhododendron	parse bandwidth filter error	Invalid parameter.	Correct the configuration.
400	? pkg_manifestfilter=video_bitrate:300-0 ? pkg_manifestfilter=video_bitrate:300-300	parse bandwidth filter error	Invalid value range.	If a range is specified, the start value must be less than the end value.
400	? pkg_manifestfilter=video_bitrate:0-2147483648	parse bandwidth filter error	Invalid range value (exceeds the maximum allowed value).	The parameter value must be within the allowed range.

S t a t u s C o d e	Bitrate Filtering Parameter Example	Error Message	Error Descript ion	Solution
4 0 0	? pkg_manifestfilter=video_bitrate:is:0-44100	parse bandwidth filter error	The query string format is incorrect .	Correct the configuration.
4 0 0	? pkg_manifestfilter=video_bitrate:abcdef...	parse bandwidth filter error	The paramet er string contains more than 1,024 characte rs.	Correct the configuration.

S t a t u s C o d e	Bitrate Filtering Parameter Example	Error Message	Error Descript ion	Solution
4 0 0	rate.m3u8? pkg_manifestfilter=video_bitrate:0-48000	parse bandwidth filter error	Paramet ers in the bitrate index request must be consiste nt with those in the top- level index response . The bitrate index request should not contain the pkg_ma nifestfil ter paramet er.	<p>The bitrate index request should not contain the pkg_manifestfilter parameter.</p> <p>Example: https://example.com/out/v1/ad06307d7d8b42faba42db50d100aaee/index.m3u8?pkg_manifestfilter=video_bitrate:0-1499999&aaa=bbb</p> <p>The returned top-level manifest URLs do not contain the pkg_manifestfilter parameter, as shown below:</p> <pre>#EXTM3U #EXT-X-VERSION:3 #EXT-X-INDEPENDENT-SEGMENTS #EXT-X-STREAM- INF:BANDWIDTH=2753858,AVERAG E- BANDWIDTH=1792323,RESOLUTIO N=640x480,FRAME- RATE=30.000,CODECS="avc1.4D401 E,mp4a.40.2" index_3.m3u8?aaa=bbb #EXT-X-STREAM- INF:BANDWIDTH=1433841,AVERAG E- BANDWIDTH=967305,RESOLUTION =320x240,FRAME- RATE=30.000,CODECS="avc1.4D400 D,mp4a.40.2" index_4.m3u8?aaa=bbb</pre>

S t a t u s C o d e	Bitrate Filtering Parameter Example	Error Message	Error Descript ion	Solution
4 0 0	1.[ts m4v m4a...]? pkg_manifestfilter=video_bitrate:0-48000	parse bandwidth filter error	Paramet ers in the segment request must be consiste nt with those in the index response . The segment request should not contain the pkg_ma nifestfil ter paramet er.	The segment request should not contain the pkg_manifestfilter parameter.
4 0 0	? pkg_manifestfilter=video_bitrate:0-1	parse bandwidth filter error	The video bitrate filtering result is empty.	If the video bitrate filtering result is empty, the parameter configuration is incorrect. Correct the settings.
4 0 0	? pkg_manifestfilter=video_bitrate:0-10,110-200,300-400,500-600,700-900,1000-2000	parse bandwidth filter error	A maximu m of five video bitrate ranges can be configur ed.	The value of video_bitrate cannot contain more than five ranges.

12 Appendix

12.1 Signed URL Generation Tool

After URL validation is configured for an RTMP ingest domain name on Media Live, you can use this tool to quickly generate a signed URL.

Prerequisites

URL validation has been configured for RTMP ingest domain names. For details, see [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 RTMP ingest domain name for which you want to generate a signed URL, and set the **App Name** and **Stream Name**.

NOTE

If you want to generate a signed streaming URL after transcoding, enter *Stream name_Transcoding template ID* in **Stream Name**. The *Transcoding template ID* can be obtained from **Media Live > Media Processing > Live Transcoding** page on the Live console. Example: huawei01_lld

Figure 12-1 Generating a signed URL

URL Signing

i Signed URLs can be generated only for domain names deployed on the new version of Live.

Streaming Domain Name

Validation Select a domain name to obtain the URL validation configuration.

Ingest Domain Name

Validation Select a domain name to obtain the URL validation configuration.

App Name
Default: live. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Stream Name

[Learn more](#)

Step 4 Click **Generate** to generate the signed ingest URL.

----End