

**Live**

# Cloud Live

**Issue** 01  
**Date** 2026-03-05



**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

---

<b>1 Service Subscription.....</b>	<b>1</b>
<b>2 Using IAM to Grant Access to Live.....</b>	<b>2</b>
2.1 Using IAM Roles or Policies to Grant Access to Live.....	2
2.2 Using IAM Identity Policies to Grant Access to Live.....	5
<b>3 Domain Name Management.....</b>	<b>9</b>
3.1 Adding Domain Names.....	9
3.1.1 Domain Name Admission Standards and Process.....	9
3.1.2 Verifying Domain Name Ownership.....	11
3.1.3 Adding Domain Names.....	14
3.1.4 Associating Domain Names.....	20
3.1.5 Configuring CNAME Records.....	21
3.1.6 Managing Domain Names.....	25
3.2 Configuring Ingest Domain Names.....	28
3.2.1 Assembling an Ingest URL.....	28
3.2.2 Transcoding.....	29
3.2.3 Adaptive Bitrate.....	36
3.2.4 Recording Live Video to OBS.....	37
3.2.4.1 Creating a Recording Template.....	38
3.2.4.2 Configuring a Recording Callback.....	45
3.2.4.3 Managing Recordings.....	50
3.2.5 Recording Live Video to VOD.....	50
3.2.5.1 Creating a Recording Template.....	50
3.2.5.2 Configuring a Recording Callback.....	56
3.2.5.3 Managing Recordings.....	62
3.2.6 Snapshot Capturing.....	62
3.2.7 Stream Status Notifications.....	68
3.2.8 HLS Configuration.....	72
3.2.9 Stream Push Authentication.....	74
3.3 Configuring Streaming Domain Names.....	74
3.3.1 Assembling a Streaming URL.....	74
3.3.2 Configuring Stream Delay.....	77
3.3.3 Configuring Origin Pull.....	79

3.3.4 HTTPS Certificates.....	82
3.3.4.1 Configuration Method.....	82
3.3.4.2 HTTPS Certificate Requirements.....	86
3.3.5 Playback Authentication.....	90
3.3.5.1 Overview.....	90
3.3.5.2 Referer Validation.....	91
3.3.5.3 URL Validation.....	93
3.3.5.4 ACL.....	107
3.3.6 Configuring a Geo-blocking Whitelist.....	108
<b>4 Streaming.....</b>	<b>111</b>
4.1 Streams.....	111
4.2 Relay.....	113
4.3 Watermarks.....	116
<b>5 Usage Statistics.....</b>	<b>121</b>
<b>6 Service Monitoring.....</b>	<b>126</b>
<b>7 LLL Statistics.....</b>	<b>139</b>
<b>8 Log Management.....</b>	<b>143</b>
8.1 Offline Log Download.....	143
<b>9 OBS Authorization.....</b>	<b>147</b>
<b>10 Tools.....</b>	<b>148</b>
10.1 Signed URL Generation Tool.....	148
<b>11 Cloud Eye Monitoring.....</b>	<b>150</b>
11.1 Monitoring Metrics.....	150
11.2 Creating an Alarm Rule.....	151
11.3 Viewing Monitoring Metrics.....	152

# 1 Service Subscription

---

Before using Live, you need to perform the operations in this section.

## Huawei Cloud Account Registration

- You have [registered](#) a HUAWEI ID, enabled Huawei Cloud services, and completed [real-name authentication](#).

### NOTE

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

- Purchase and use cloud services in Huawei Cloud regions 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 Huawei Cloud regions in the Chinese mainland.
- Log in to the [Live console](#) to subscribe to Live as instructed.

## Account Balance

By default, Live uses pay-per-use billing. The generated service fees will be directly deducted from your account balance. Ensure that your account is available and has sufficient balance.

## Quick Start

Learn how to get started with Live. For details, see [Getting Started](#).

# 2 Using IAM to Grant Access to Live

---

## 2.1 Using IAM Roles or Policies to Grant Access to Live

System-defined permissions in [role/policy-based authorization](#) provided by [Identity and Access Management \(IAM\)](#) let you control access to Live. With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing Live resources
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Entrust a Huawei Cloud account or a cloud service to perform efficient O&M on your Live resources.

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

[Figure 2-1](#) shows the process of role/policy-based authorization.

### Notes

- You need to [submit a service ticket](#) to apply for role/policy-based authorization 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 [role/policy-based authorization](#) is enabled, unauthorized [IAM users](#) cannot call Live APIs. To gain access, they must have the corresponding Live permissions.
- After assigning an IAM user the **Live FullAccess** permissions, you need to assign the user the following Cloud Eye permissions to monitor metrics of Live:
  - To authorize Live console access through a custom policy instead of the system-defined policies **Live FullAccess** and **Live ReadOnlyAccess**, the

permission **live:tenant:getTenantInformation** must be included in the custom policy.

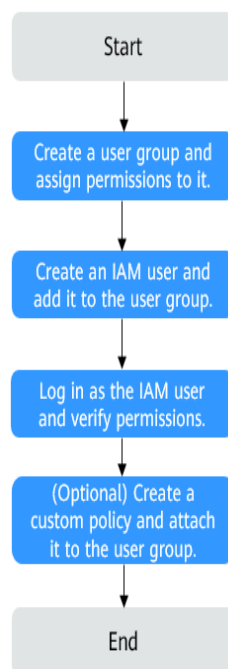
- After assigning an IAM user the **Live FullAccess** permission, you need to assign the user the following Cloud Eye permissions to monitor metrics of Live:
  - **CES ReadOnlyAccess:** On the Cloud Eye console, choose **Cloud Service Monitoring > Live** to view resource monitoring metrics of Live.
  - **CES FullAccess:** On the Cloud Eye console, choose **Cloud Service Monitoring > Live** to view resource monitoring metrics of Live and perform operations.

## Prerequisites

Before granting permissions to user groups, learn about system-defined permissions in [role/policy-based authorization](#) for Live. To grant permissions for other services, learn about all [system-defined permissions](#) supported by IAM.

## Process Flow

**Figure 2-1** Process of granting Live permissions



1. On the IAM console, [create a user group and grant it permissions](#)  
Create a user group on the IAM console and assign it the **Live ReadOnlyAccess** policy.

## 2. Create an IAM user and add it to the created user group.

On the IAM console, create a user and add it to the user group created in 1.

## 3. Log in as the IAM user and verify permissions.

In the authorized region, perform the following operations:

- Choose **Service List > Live**. On the Live console, choose **Domains** in the navigation pane and click **Add Domain**. If a message is displayed indicating that you have insufficient permissions to perform the operation, the **Live ReadOnlyAccess** policy is in effect.
- Choose another service from **Service List**. If a message is displayed indicating that you have insufficient permissions to access the service, the **Live ReadOnlyAccess** policy is in effect.

## Example Custom Policies

You can create custom policies to supplement the system-defined policies of Live. For details about the actions supported by custom policies, see [Actions Supported by Policy-based Authorization](#).

To create a custom policy, choose either visual editor or JSON:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy grammar.
- JSON: Create a JSON policy or edit an existing one.

For details, see [Creating a Custom Policy](#). Examples of common Live custom policies:

- Example 1: Assigning a user all permissions for Live

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "live:*:*"
      ]
    }
  ]
}
```

- Example 2: Assigning a user the read-only permission for Live

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "live*:get*",
        "live*:list*"
      ]
    }
  ]
}
```

- Example 3: Denying Live domain name deletion

A policy with only "Deny" permissions must be used with other policies. If the permissions granted to an IAM user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

Assume that you want to assign a user the permissions of the **Live FullAccess** policy but do not want them to delete Live domain names. You can create a

custom policy for denying Live domain name deletion, and attach this policy together with the **Live FullAccess** policy to the user. As an explicit deny in any policy overrides any allows, the user can perform all operations on Live resources except for deleting Live domain names.

Example of "Deny" permissions:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "live:domain:deleteDomain"
      ]
    }
  ]
}
```

- Example 4: Creating a custom policy containing multiple actions

A custom policy can contain the actions of one or multiple services that are of the same type (global or project-level).

Example policy containing multiple actions:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "live:domain:createDomain"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "smn:topic:create"
      ]
    }
  ]
}
```

## 2.2 Using IAM Identity Policies to Grant Access to Live

System-defined permissions in **identity policy-based authorization** provided by **Identity and Access Management (IAM)** let you control access to Live. With IAM, you can:

- Create IAM users or user groups for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing Live resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Entrust a Huawei Cloud account or a cloud service to perform efficient O&M on your Live resources.

If your Huawei Cloud account meets your permissions requirements, you can skip this section.

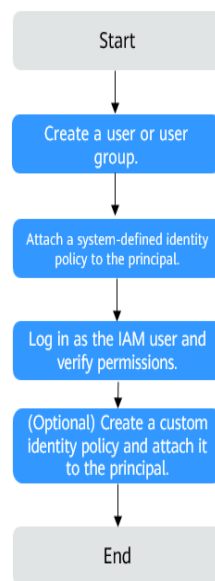
**Figure 2-2** shows the process of identity policy-based authorization.

## Prerequisites

Before assigning permissions, learn about the system-defined permissions in [Identity Policy-based Authorization](#) for Live. To grant permissions for other services, learn about all [system-defined permissions](#) supported by IAM.

## Process Flow

Figure 2-2 Process of granting Live permissions



1. On the IAM console, [create an IAM user](#) or [create a user group](#).  
Create a user or user group on the IAM console.
2. [Attach a system-defined identity policy](#) to the user or user group.  
Attach the **LiveReadOnlyPolicy** system-defined identity policy to the user or user group.
3. [Logging in as the IAM user](#) and verifying permissions  
In the authorized region, perform the following operations:
  - Choose **Live** in **Media Services** under **All Services**. On the Live console, choose **Domains** in the navigation pane to add a domain name. If a message is displayed indicating insufficient permissions for performing the operation, the **LiveReadOnlyPolicy** policy has taken effect.
  - Choose another service. If a message is displayed indicating insufficient permissions for performing the operation, the **LiveReadOnlyPolicy** policy has taken effect.

## Example Custom Identity Policies

You can create custom identity policies to supplement the system-defined identity policies of Live. See [actions supported by identity policy-based authorization](#).

To create a custom identity policy, choose either visual editor or JSON.

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy grammar.
- JSON: Create a JSON policy or edit an existing one.

For details, see [Creating a Custom Identity Policy and Attaching It to a Principal](#).

Examples of common Live custom identity policies:

- Example 1: Assigning a user all permissions for Live

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "live:*:*",
        "eps:enterpriseProjects:list",
        "smn:topic:listTopic",
        "billing:contract:viewDiscount",
        "billing:coupon:update"
      ]
    }
  ]
}
```

- Example 2: Assigning a user the read-only permission for Live

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "live:*:get*",
        "live:*:list*",
        "eps:enterpriseProjects:list",
        "smn:topic:listTopic",
        "billing:contract:viewDiscount"
      ]
    }
  ]
}
```

- Example 3: Creating a custom identity policy containing multiple actions  
A custom identity policy can contain the actions of one or more services.

Example identity policy containing multiple actions:

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "live:domain:createDomain"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
    "smn:topic:create"  
  }  
]  
}
```

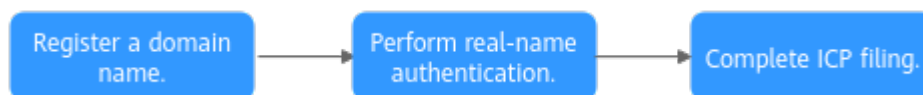
# 3 Domain Name Management

## 3.1 Adding Domain Names

### 3.1.1 Domain Name Admission Standards and Process

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

#### Domain Name 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** as the ingest domain and **test-play.example.com** as the streaming domain.

2. Complete 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 user of Huawei Cloud (International) or Huawei Cloud (Europe), you need to complete real-name authentication when you:

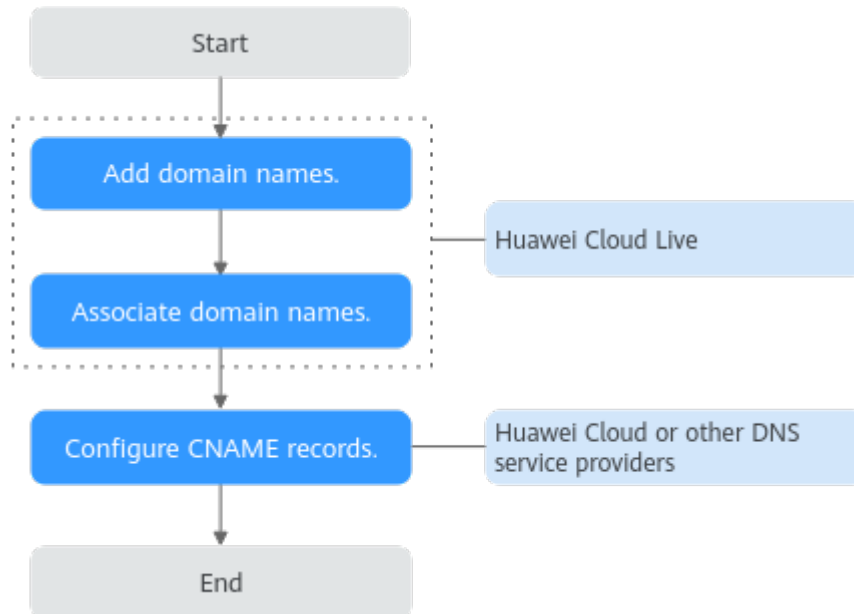
- Purchase and use cloud services in Huawei Cloud regions in the Chinese mainland. In this case, real-name authentication is required by the laws and regulations of the Chinese mainland.
  - Plan to use Live in Huawei Cloud regions in the Chinese mainland.
3. Complete ICP filing. If you want to perform livestreaming acceleration in Huawei Cloud regions in or outside the Chinese mainland, the domain names

must complete ICP filing in advance as required by the Ministry of Industry and Information Technology (MIIT).

## Domain Name Addition Process

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

**Figure 3-1** Domain name addition process



1. **Add an ingest domain name and a streaming domain name (both licensed) to Live.**
2. **Associate the ingest domain name with the streaming domain name.**
3. **Configure CNAME records** at your domain names' DNS provider so that the CNAME addresses allocated by Live point to your domain names.

## 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

Live does not allow accessing 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 the use of your 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 Live and can no longer access Live. Acceleration domain name quota of the account will be reduced to 0.

## Domain Name Rules

[Table 3-1](#) lists the detailed 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, enable it again.
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.

### 3.1.2 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, a.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** Log in to the [Live console](#).

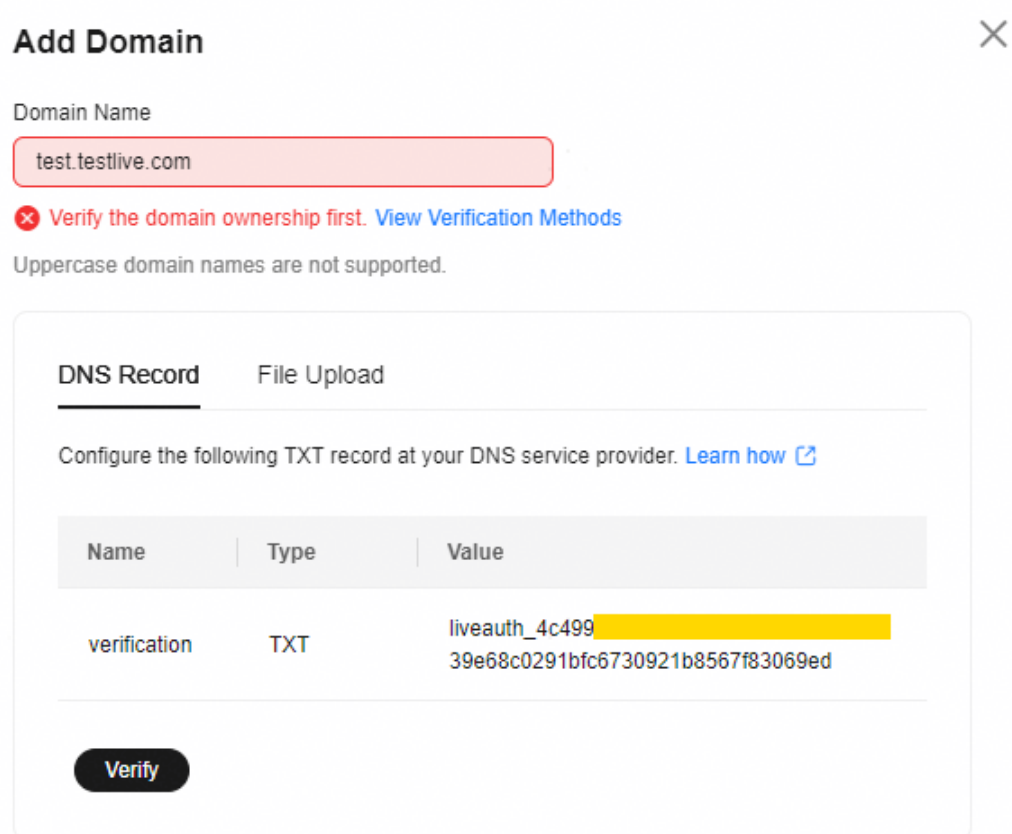
**Step 2** In the navigation pane, choose **Domains**.

**Step 3** Click **Add Domain**. On the displayed page, enter your domain name.

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 3-2** Verifying the domain name ownership



**Step 4** 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, Xinnet, 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 3-2**. 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 5** 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** Log in to the **Live console**.

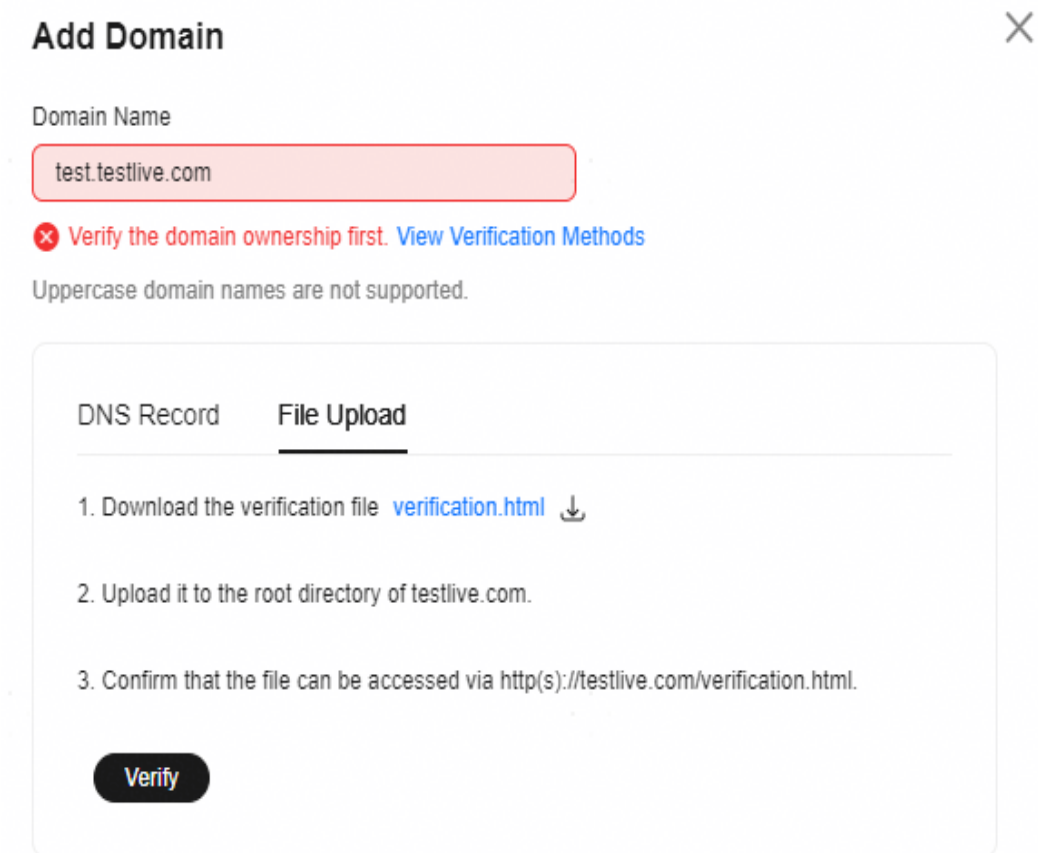
**Step 2** In the navigation pane, choose **Domains**.

**Step 3** Click **Add Domain**. On the displayed page, enter your domain name.

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 3-3 Verifying the domain name ownership



**Step 4** Download the **verification.html** file.

**Step 5** 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 6** 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

### 3.1.3 Adding Domain Names

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

#### Prerequisites

- You have [registered](#) a HUAWEI ID, enabled Huawei Cloud services, and completed [real-name authentication](#).

 **NOTE**

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

- Purchase and use cloud services in Huawei Cloud regions 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 Huawei Cloud regions in the Chinese mainland.
- Domain names for Live are available. Live requires an ingest domain name and a streaming domain name, and the two domain names must be different.

 **NOTE**

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

## Notes

- An area needs to be specified for stream push, and the streaming domain name needs to be associated with the ingest domain name. This allows viewers to watch the livestream only in the region where the ingest domain name is hosted. In other words, a streaming domain name cannot be used to watch livestreams 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 acceleration area, the playback quality may be compromised.
- If the **Service Area** of the streaming domain name is **Chinese mainland** or **Global**, and the origin server of the ingest domain name is in the Chinese mainland, the domain names must be licensed in the Chinese mainland.
- If you add, modify, or delete a domain name, the change will be reflected on the [My Resources](#) page within 24 hours. Please check the data later.

## 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 your streaming or ingest domain name.

Figure 3-4 Adding a domain name

### Add Domain ✕

Domain Name

Uppercase domain names are not supported.

Enterprise Project

 Q Create

Subservice Type ?

Cloud Live  Media Live

Type

Streaming domain name  Ingest domain name

Associate the streaming domain name with an ingest domain name before livestreaming.  
[Learn more](#)

Live Origin Server

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.

Supported Protocol

FLV+RTMP+RTC  HLS

Select the protocol to be supported. Currently, the protocol cannot be changed.

**Table 3-2** Domain name 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 <b>View Verification Methods</b> on the right and perform operations by referring to <a href="#">Verifying Domain Name Ownership</a>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• A domain name can contain a maximum of 64 characters and cannot contain uppercase letters.</li> <li>• An ingest domain name must be different from a streaming domain name. Wildcard domains are not allowed.</li> <li>• By default, you can add up to 64 domain names in your account. If you need to add more domain names, <a href="#">submit a service ticket</a>.</li> <li>• Domain names must be unique across all regions.</li> </ul>
Enterprise Project	<p>Add the domain name to an enterprise project for unified management.</p> <p>You can <a href="#">create an enterprise project</a> or use the default one whose name is <b>default</b>. 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 <a href="#">Authorizing a User Group to Manage an Enterprise Project</a>. By doing so, users in this user group obtain the permissions on the domain names in the enterprise project.</p> <p><b>NOTE</b> Only enterprise accounts can configure enterprise projects.</p>
Subservice Type	<p>Select a subservice type of Live.</p> <p>Options:</p> <ul style="list-style-type: none"> <li>• <b>Cloud Live:</b> This easy-to-use livestreaming service provides diverse live acceleration capabilities for entertainment, e-commerce, and education scenarios.</li> <li>• <b>Media Live:</b> This broadcast-grade livestreaming service provides features such as channel management and content encryption for media organizations and broadcasters.</li> </ul> <p>Select <b>Cloud Live</b>.</p>
Type	<p>If you enter an ingest domain name for <b>Domain Name</b>, then select <b>Ingest domain name</b> for <b>Type</b>. The domain name type cannot be changed after the domain name is added.</p>

Parameter	Description
Live Origin Server	<p>Select the region where the Live origin server for this domain is located. For details, see <a href="#">How Do I Select a Live Origin Server and Acceleration Area?</a> The Live origin server cannot be changed after the domain is added. You are advised to select the origin server nearest to your services.</p> <p>Currently, Live origin servers are deployed in the following regions:</p> <ul style="list-style-type: none"> <li>• CN North-Beijing4 of Huawei Cloud (Chinese Mainland): CN North-Beijing4 and AP-Singapore.</li> <li>• AP-Singapore of Huawei Cloud (International): AP-Singapore, LA-Sao Paulo1, and CN North-Beijing4.</li> <li>• EU-Dublin of Huawei Cloud (Europe): EU-Dublin.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• The origin server for the ingest domain name must be in the region where the streamer is. Streamers cannot push streams across regions. For example, if a streamer needs to livestream in both the Chinese mainland and Malaysia, two sets of streaming and ingest domain names need to be configured. The origin servers of each set of domain names are located in the Chinese mainland and Singapore, respectively.</li> <li>• The origin servers of the ingest and streaming domain names to be associated must be in the same region.</li> <li>• The OBS buckets that you use for storing live video recordings and snapshots must be in the same region as the Live origin servers.</li> </ul>

Parameter	Description
Service Area	<p>Select the area where the streaming domain name is to be accelerated. For details, see <a href="#">How Do I Select a Live Origin Server and Acceleration Area?</a> This parameter is available only for streaming domain names. This setting cannot be modified after the domain is added.</p> <p>If the livestream 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"> <li> <b>Chinese mainland</b>            Select this option if you are targeting viewers in the Chinese mainland.             The domain name must be licensed by the Ministry of Industry and Information Technology (MIIT).         </li> <li> <b>Outside Chinese mainland</b>            Select this option if you are targeting viewers outside the Chinese mainland, such as those in Hong Kong (China), Macao (China), and Taiwan (China), or other countries or regions.         </li> <li> <b>Global</b>            Select this option if you are targeting viewers in and outside the Chinese mainland, such as those in the Chinese mainland, Hong Kong (China), Macao (China), Taiwan (China), or other countries or regions.             The domain name must be licensed by the Ministry of Industry and Information Technology (MIIT).         </li> </ul> <p><b>NOTICE</b>            If the <b>Service Area</b> 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 <a href="#">Live Service Agreement</a>.</p>
Supported Protocol	<p>Select the streaming protocols supported by your streaming domain name.</p> <ul style="list-style-type: none"> <li>This parameter is available only for streaming domain names.</li> <li>This setting cannot be modified after the domain name is added. The default value is <b>FLV+RTMP+RTC</b>.</li> </ul> <p>Options:</p> <ul style="list-style-type: none"> <li><b>FLV+RTMP+RTC</b>: The streaming domain name can use HTTP-FLV, RTMP, and WebRTC to play cloud-based livestreams.</li> <li><b>HLS</b>: The streaming domain name can use HLS to play cloud-based livestreams.</li> </ul>

**Step 4** Click **OK**.

The domain name is displayed in the domain name list, and its **Status** is **Configuring**. If **Status** changes to **Normal** in 3 to 5 minutes, the domain name has been added.

**Step 5** After adding the streaming domain name, associate the streaming domain name with the ingest domain name before using Live. The ingest and streaming domain names must use the same Live origin server. For details, see [Associating Domain Names](#).

**Step 6** [Configure CNAME records](#) at your DNS provider to point your domain names to the CNAME addresses assigned by CDN. Once the configuration takes effect, livestreaming acceleration is automatically enabled for the domain names.

----End

### 3.1.4 Associating Domain Names

After an ingest domain name and streaming domain name are added, you must associate them so that they can take effect.

#### Notes

- A streaming domain name can be associated with only one ingest domain name.
- Modifying the stream association may cause livestream playback exceptions. Exercise caution when performing this operation.

#### Prerequisites

You have added an ingest domain name and streaming domain name by referring to [Procedure](#).

#### Procedure

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

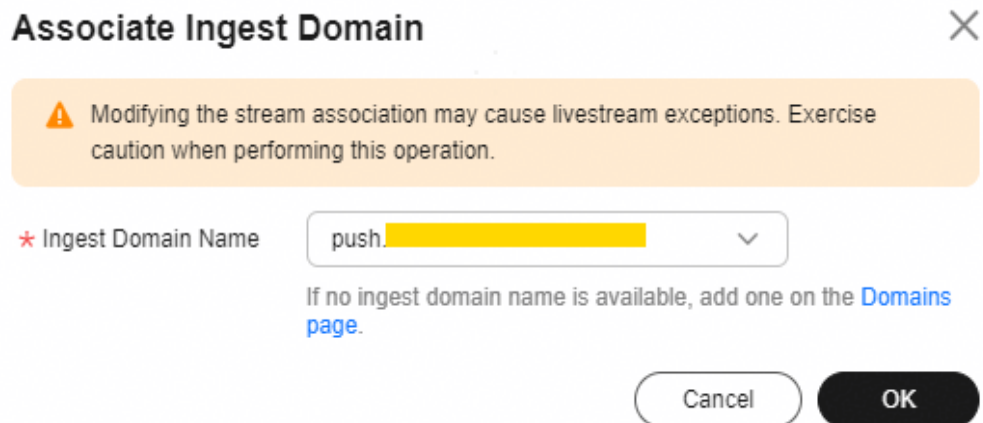
**Step 2** In the navigation pane, choose **Domains**.

**Step 3** Locate the target streaming domain name, and click **Manage** in the **Operation** column.

The **Basic Info** page is displayed.

**Step 4** In the **Ingest Info** area, click **Associate Ingest Domain** and select the added ingest domain name.

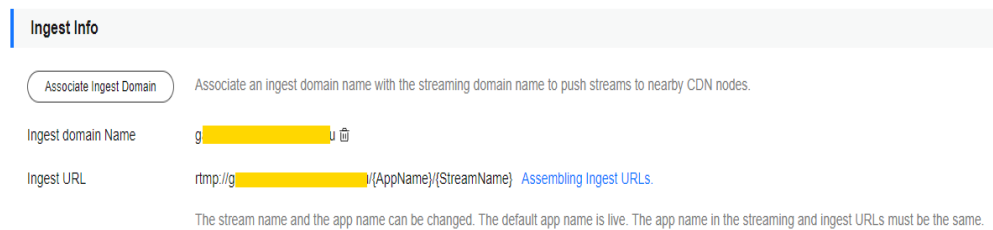
Figure 3-5 Associating domain names



Step 5 Click **OK**.

After the association is complete, you can view the stream ingest information.

Figure 3-6 Ingest Info



----End

### 3.1.5 Configuring CNAME Records

After a domain name is added, a CNAME address is automatically assigned to the domain name. You need to configure a CNAME record at your DNS provider. Acceleration is enabled once the configuration takes effect.

#### Notes

- If the domain name you added is on Huawei Cloud, configure a CNAME record following the [procedure](#) below. If the domain name you added is not on Huawei Cloud, configure a CNAME record following the guidance provided by your DNS provider.
- You need to configure CNAME records for your ingest domain name and streaming domain name separately.

#### Prerequisites

The ingest domain name and streaming domain name have been **added** and **associated**.

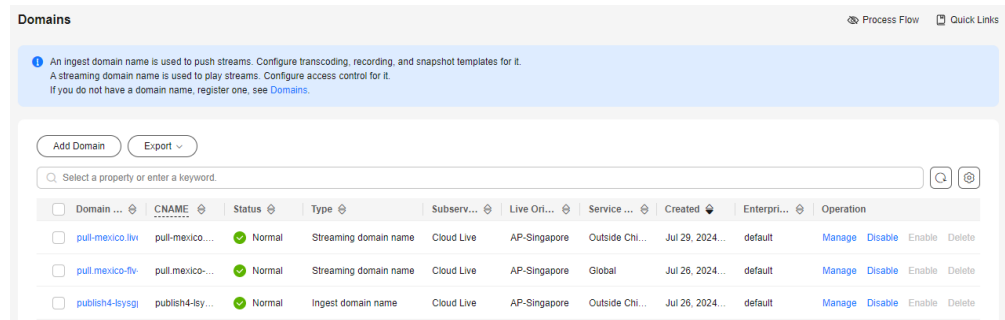
## Procedure

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

### Step 1 Obtain the CNAME address.

1. Log in to the [Live console](#).
2. In the navigation pane on the left, choose **Domains**.
3. Obtain the corresponding CNAME in the **CNAME** column.

**Figure 3-7** Obtaining the CNAME address

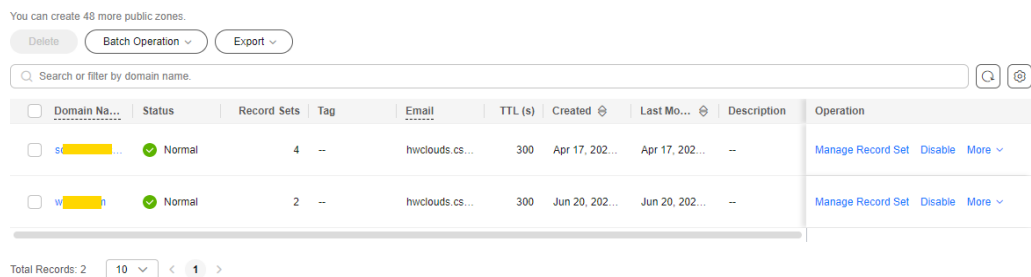


### Step 2 Log in to the [DNS console](#).

### 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 3-8](#).

**Figure 3-8** Domain name list



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

**Figure 3-9** 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 <b>CNAME – Map one domain to another</b> here.

Parameter	Description
Name	<p>Enter the second-level domain name. You do not need to enter the suffix.</p> <p>For example, if the streaming domain name is <b>play-test.example.com</b>, enter <b>play-test</b>.</p>
Line	<p>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 <a href="#">Resolution Lines</a>.</p> <p>This parameter is available only for public domain names.</p> <p>Select <b>Default</b>.</p>
TTL (s)	<p>How long a local DNS server caches the DNS record. It is measured in seconds.</p> <p>The smaller the value is, the quicker the record takes effect.</p> <p>The default value is 300 seconds. You can retain the default value.</p>
Value	<p>Domain name to be pointed to, that is, the CNAME address obtained in step 1 of this section.</p> <p>For example, if the streaming domain name is <b>play-test.example.com</b>, enter <b>play-test.example.com.cdnhwc3.com</b>.</p>
Alias	<p>Whether to associate the record set with a cloud resource.</p> <ul style="list-style-type: none"> <li>Enabled: The record set will be associated with a cloud resource.</li> <li>Disabled: The record set will not be associated with a cloud resource.</li> </ul> <p>Toggle off the switch, that is, disable this function.</p>
Weight	<p>(Optional) Weight of a record set. The value ranges from <b>0</b> to <b>1000</b> and defaults to <b>1</b>.</p> <p>This parameter is available only for public domain names.</p> <p>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 <a href="#">Configuring Weighted Routing</a>.</p> <p>Set this parameter to <b>1</b>.</p>
Tag	<p>(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 <a href="#">Adding a CNAME Record Set</a>.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>example_key1</li> <li>example_value1</li> </ul>
Description	<p>(Optional) Supplementary information about the domain name.</p> <p>You can enter up to 255 characters.</p>

**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 a CNAME record for the ingest domain name.

----End

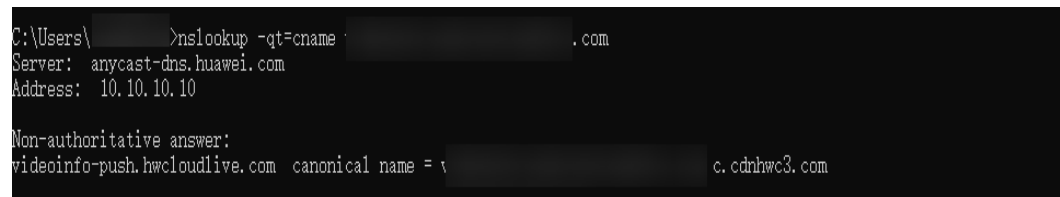
## Checking Whether the CNAME Records Have Taken Effect

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 record has taken effect. A typical command output is shown in **Figure 3-10**.

**Figure 3-10** Checking whether a CNAME record has taken effect



```
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.odnhwc3.com
```

## 3.1.6 Managing Domain Names

After an ingest domain name or streaming domain name is added, you can view the basic information about the added domain names on the **Domains** page. You can disable, enable, or delete domain names, and change their associations.

### Notes

- If you add, modify, or delete a domain name, the change will be reflected on the **My Resources** page within 24 hours. Please check the data later.
- Before disabling a domain name, have your domain requests resolved to the origin server or to a CNAME record not assigned by Huawei Cloud to prevent service interruptions.
- You can delete a domain name only if it is in the **Disabled**, **Configuration failed**, or **Rejected** state.
- The system automatically disables domain names that have no access traffic for more than 90 days, including those that are running properly.  
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, enable it again.
- The system automatically deletes domain names that have been disabled for more than 90 days, including those that are rejected.  
The records related to the domain name will be automatically deleted. If you want to continue using the domain name, add it again.
- 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 Live and can no longer access Live. Acceleration domain name quota of the account will be reduced to 0.

- Deleting a domain name removes its configuration from Live PoPs, and the domain will no longer incur Live charges.

## 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, type, status, and creation time of each domain name.

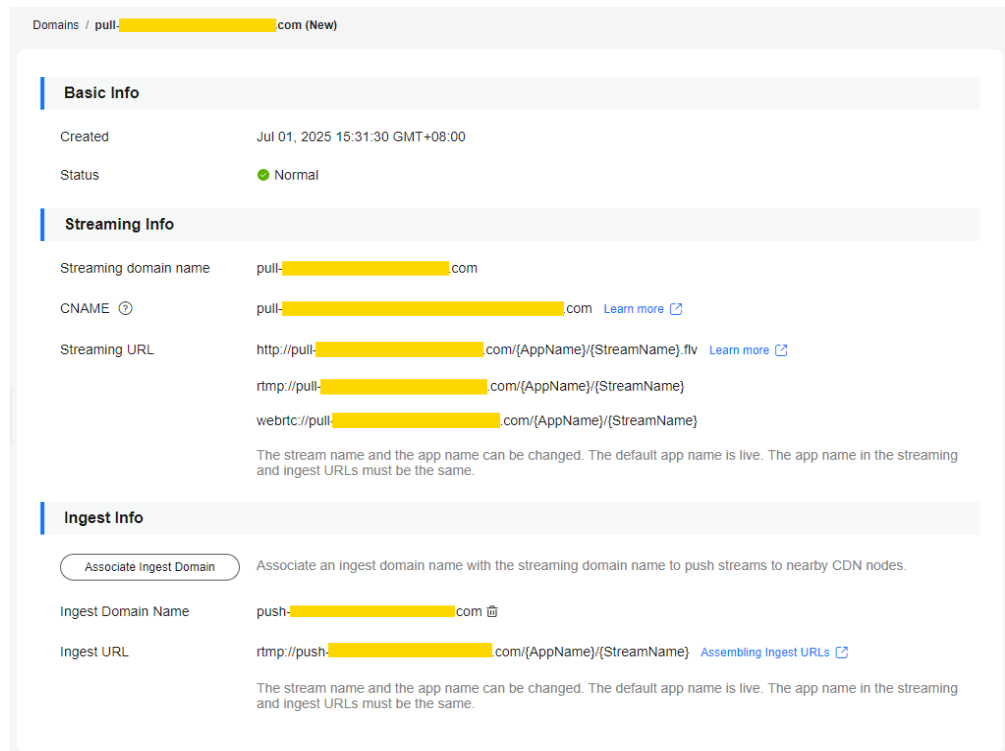
**Figure 3-11** Domain name management


The screenshot shows the 'Domains' management interface. At the top, there are buttons for 'Add Domain' and 'Export'. Below is a search bar with the placeholder text 'Select a property or enter a keyword'. The main content is a table with the following columns: Domain, CNAME, Status, Type, Subserv., Live Ori., Service, Created, Enterpri., and Operation. Three domain entries are visible:

Domain	CNAME	Status	Type	Subserv.	Live Ori.	Service	Created	Enterpri.	Operation
pull-mexico-liv	pull-mexico...	Normal	Streaming domain name	Cloud Live	AP-Singapore	Outside Chi...	Jul 29, 2024...	default	Manage Disable Enable Delete
pull-mexico-iv	pull-mexico...	Normal	Streaming domain name	Cloud Live	AP-Singapore	Global	Jul 26, 2024...	default	Manage Disable Enable Delete
publish4-4ysgj	publish4-4sy...	Normal	Ingest domain name	Cloud Live	AP-Singapore	Outside Chi...	Jul 26, 2024...	default	Manage Disable Enable Delete

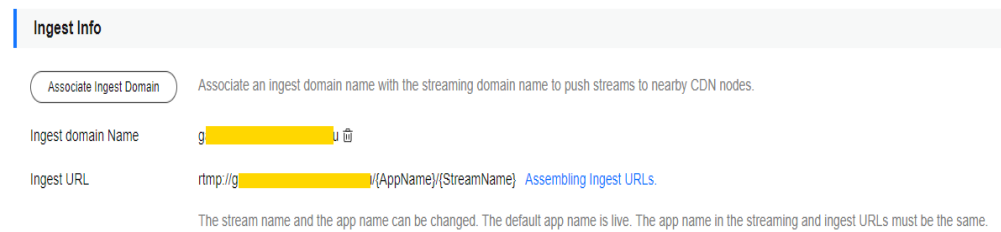
Click **Manage** in the **Operation** column of the desired domain name to view its basic information. Streaming URLs are provided based on the protocols supported by the streaming domain name.

**Figure 3-12** Domain information



- **Disable a domain name.**  
To disable a domain name, click **Disable** in the row that contains that domain. When its status changes to **Disabled**, the domain name has been disabled.
- **Enable a domain name.**  
To enable a disabled domain name, click **Enable** in the row that contains that domain. When its 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.
- **Disassociate domain names.**  
To disassociate an ingest domain name from a streaming domain name, click **Manage** in the **Operation** column of the streaming domain name. In the **Ingest Info** area, click .

**Figure 3-13** Ingest Info



----End

## 3.2 Configuring Ingest Domain Names

### 3.2.1 Assembling an Ingest URL

After domain names are configured, you can assemble an ingest URL and then push streams through the URL. You can also use the [tool](#) to quickly generate a signed URL of the ingest domain name.

#### Prerequisites

- You have [added an ingest domain name](#).
- You have [configured CNAME records](#) at your domain names' DNS provider.
- To secure live resources, Live provides URL validation to encrypt and sign the ingest URL. If necessary, configure [stream authentication](#) and push streams through the signed URL.

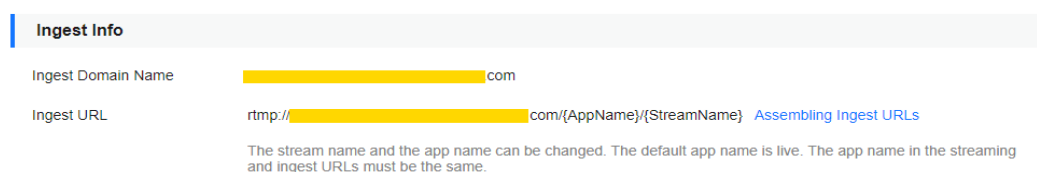
#### Procedure

**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 ingest domain name. On the displayed page, you can view the stream push information.

**Figure 3-14** Ingest info



- You need to customize **StreamName** to generate an ingest URL. For details, see [Original Ingest URL](#).
- If URL validation is configured, you can add a signed string to the original ingest URL to generate a new ingest URL. For details, see [Signed Ingest URL](#).

----End

## Original Ingest URL

### Assembling rules

The following formats are supported:

- Format 1: `rtmp://Ingest domain name/AppName/StreamName?args=xxx`
- Format 2: `rtmp://ip/Ingest domain name/AppName/StreamName?args=xxx`
- Format 3: `rtmp://ip/AppName/StreamName?vhost=Ingest domain name&args=xxx`

The ingest URL format cannot be `rtmp://ip/AppName/StreamName?domain=Ingest domain name&args=xxx`.

The parameters are described as follows:

- *Ingest domain name* is the one you added on the Live console.
- *AppName*: application name. The default value is **live**. You can customize the application name. Only letters, digits, underscores (\_), and hyphens (-) are allowed.
- *StreamName*: livestream name. Multiple livestreams can be created for each application. You can customize the stream name, for example, huawei1.

A stream name can contain 1 to 512 characters. The recommended length is 12 to 256 characters. Only digits, letters, hyphens (-), underscores (\_), asterisks (\*), and slashes (/) are allowed. Digits and letters are recommended. If you set the stream name to an asterisk (\*), all livestreams of the application will share one streaming URL.

### Examples

If the added ingest domain name is **test-push.example.com**, *AppName* is **livetest**, and *StreamName* is **huawei1**, the ingest URL is:

```
rtmp://test-push.example.com/livetest/huawei1
```

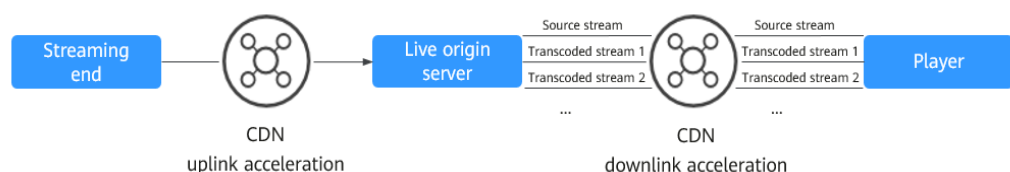
## Signed Ingest URL

If **URL validation** is configured, you must assemble a signed URL based on obtained authentication information and then push streams through the signed URL. For details, see **URL Validation**.

## 3.2.2 Transcoding

You can transcode livestreams into video streams with different resolutions and bitrates to meet a broad range of requirements.

**Figure 3-15** Transcoding architecture



## 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. H.265 codec and low-bitrate HD can reduce the bitrate by about 20% at the same resolution.
- Customize a transcoding template with settings such as ID, resolution, bitrate, and frame rate.

## Notes

- You can configure multiple transcoding templates for one domain name. After a transcoding request is received, the transcoding template whose **App Name** matches that in the request URL will be applied. If you do not need transcoding, [delete the transcoding template](#) before stream push.
- The transcoding template takes effect when livestreams are started. If the transcoding configuration is modified, the modification does not take effect for ongoing livestreams. The modification takes effect only for livestreams pushed after the modification.
- Low-bitrate HD is disabled by default. If you enable it, you will be charged based on the low-bitrate HD transcoding pricing. For details, see [Live Pricing Details](#).
- Upsampling transcoding is not supported. Even if you specify a resolution higher than the source in the template, the streaming URL generated for transcoded streams will be functional, but the streams will still be played at the original resolution.
- After a transcoding template is configured, you need to add *\_transcoding template name* to the end of the corresponding stream name to generate a streaming URL for the transcoded stream. Therefore, the original stream name cannot contain the transcoding template name. For example, if the transcoding template name is **hd**, the original stream name cannot contain **\_hd**. Otherwise, the program cannot correctly determine whether to trigger transcoding during playback, causing a stream pull exception.
- For high-volume transcoding or 4K livestreaming requirements, please [submit a service ticket](#) in advance. This allows us to evaluate resource availability and ensure your service requirements are met.

## Prerequisites

- You have [added an ingest domain name](#).
- You have [configured CNAME records](#) at your domain names' DNS provider.

## Pricing Notes

The transcoding function is a billing item. You are charged based on a combination of the codec, output resolution, and length of an output video. Standard transcoding and low-bitrate transcoding are billed differently. For details about the transcoded output resolution, see the **Output Resolution** column in

[Live Pricing Details](#). If you use transcoding frequently, you are advised to [buy a Live package](#).

## Creating a Transcoding Template

You can customize a template on the Live console or by calling the [Live API](#). If you want to play transcoded livestreams, obtain a transcoded streaming URL. For details, see [Transcoded Streaming URL](#).

**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 ingest domain name.

The subservice type of the domain name must be Cloud Live.

**Step 4** In the navigation pane, choose **Templates > Transcoding** to view the transcoding template information.

**Step 5** Click **Create Transcoding Template**. The **Create Transcoding Template** page is displayed, as shown in [Figure 3-16](#).

Configure transcoding parameters based on [Table 3-4](#).

**Figure 3-16** Creating a transcoding template

### Transcoding ✕

**Template Name**

**App Name**  
  
The value can contain uppercase letters, lowercase letters, digits, underscores ( \_ ), and hyphens (-).

**Triggered By**

By stream pull: Transcoding only starts upon playback requests. Only the specific templates matching the requests will generate transcoded streams and incur fees.

**Transcoding Type**

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)**

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** (?)

**Resolution (W x H)**  
 \*

**Table 3-4** Transcoding template parameters

Parameter	Description
Template Name	Name of the transcoding template. Chinese characters are not supported.

Parameter	Description
App Name	<p>Application name. The default value is <b>live</b>.</p> <p>You can customize the application name. Only letters, digits, underscores (_), and hyphens (-) are allowed.</p>
Triggered By	<p>Cloud Live transcoding can be triggered by stream push or stream pull. An application can have up to 20 transcoding templates.</p> <ul style="list-style-type: none"> <li>• Transcoding triggered by stream push: When a stream is pushed, a transcoding task is initiated, and the corresponding transcoding fee is generated. If multiple transcoding templates are configured for an application, each template generates its own transcoded stream and incurs the corresponding transcoding fee, regardless of whether the streams are pulled.</li> <li>• Transcoding triggered by stream pull: When a viewer plays a livestream, only the transcoding template corresponding to the pulled stream generates a transcoded stream and incurs the corresponding fee.</li> </ul> <p>Note: Transcoding templates are distinguished by name. Templates with different names are treated as different templates, even if they use identical parameter settings. The default value is <b>Stream pull</b>. If no value is specified, transcoding is triggered by stream push.</p> <p><b>CAUTION</b></p> <ul style="list-style-type: none"> <li>• The triggering mode must be consistent across all transcoding templates in an application. Changing the <b>Triggered By</b> value for any template will update all templates under the application to that mode.</li> <li>• If multiple transcoding templates are configured, the transcoding price is aggregated based on the output specifications of each transcoding template.</li> </ul>
Transcoding Type	<p>Live transcoding type.</p> <p>Options:</p> <ul style="list-style-type: none"> <li>• <b>Standard transcoding</b></li> <li>• <b>Low-bitrate HD</b></li> </ul> <p>For the same resolution, low-bitrate HD transcoding consumes 20% less bitrate than standard transcoding but costs more.</p> <p>Low-bitrate HD 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. For details, see <a href="#">Live Pricing Details</a>.</p>
Video Encoding	<p>H.264 and H.265 are supported.</p>

Parameter	Description
Presets (Optional)	Screen resolution. After the resolution level is selected, the <b>Video Bitrate</b> and <b>Resolution (W x H)</b> parameters are automatically set and the recommended values are provided. You can also change the values as needed.
Video Bitrate	Average bitrate of the transcoded video, in kbit/s. Value range: 40 to 30,000
Bitrate Control	Bitrate control policy. Options: <ul style="list-style-type: none"> <li>● <b>Disabled:</b> The output uses the specified bitrate. No adaptation is performed.</li> <li>● <b>Not higher than source stream:</b> The output bitrate is the lower of the specified bitrate and the source stream bitrate. It never exceeds the source stream bitrate.</li> <li>● <b>Adaptive to source stream:</b> The output bitrate is automatically adjusted based on the source stream bitrate.</li> </ul>
Resolution (W x H)	Width and height of the video, in pixels. If both the width and height are set to <b>0</b> , the output resolution matches the source resolution. If either the width or height is set to <b>0</b> , the output resolution will be scaled based on the non-zero dimension. Value range: <ul style="list-style-type: none"> <li>● <b>Width:</b> The value must be 0 or an even number from 32 to 3,840.</li> <li>● <b>Height:</b> The value must be 0 or an even number from 32 to 2,160.</li> </ul>
Video Frame Rate	Frame rate of the transcoded video. Options: <ul style="list-style-type: none"> <li>● <b>Retain the original</b></li> <li>● <b>Set a new one:</b> If you select this option, you need to enter the frame rate. The value ranges from 0 to 60. If the value is set to <b>0</b>, the frame rate is adaptive.</li> </ul>

Parameter	Description
Use Source I-Frame	<p>Policy for outputting I-frames during encoding.</p> <ul style="list-style-type: none"> <li>• If this function is disabled, I-frames are output based on the configured GOP duration.</li> <li>• If this function is enabled, the output preserves the source I-frame positions. If the source contains I-frames, the output inserts I-frames at the same positions. If the source contains no I-frames, the output contains no I-frames.</li> </ul> <p>If this function is enabled, the GOP duration setting does not apply. For multi-bitrate transcoding, enable <b>Use Source I-Frame</b> so outputs at different bitrates share the same I-frame positions.</p>
GOP Duration	<p>I-frame interval by time, in seconds.</p> <p>The value ranges from 0 to 10 and defaults to 2.</p> <p>If the value is not 0, the I-frame interval is set based on the GOP duration. If the value is 0, the default value is used.</p> <p>A larger GOP duration increases live-streaming latency. A smaller GOP duration increases the likelihood of frame freezing.</p>
B-Frame Removal	<p>After this function is enabled, the transcoded video does not contain B-frames.</p> <p>To configure a transcoding template for low-latency livestreaming, enable <b>B-Frame Removal</b>.</p>

**Step 6** Click **OK**.

A transcoding template is added on the live transcoding page.

**Step 7** Obtain a transcoded streaming URL if you need to stream your video via a transcoded streaming URL. For details, see [Transcoded Streaming URL](#).

----End

## Transcoding Template Management

You can perform the following operations on your transcoding templates:

- Edit a transcoding template.

Click **Edit** in the **Operation** column to modify parameters in the template. The value of **AppName** cannot be changed.

 **CAUTION**

The transcoding template takes effect when livestreams are started. If the transcoding configuration is modified, the modification does not take effect for ongoing livestreams. The modification takes effect only for livestreams pushed after the modification.

- Delete a transcoding template.  
Click **Delete** in the **Operation** column.

### 3.2.3 Adaptive Bitrate

Cloud Live supports adaptive bitrate (ABR) through multiple transcoding templates to accommodate different types of client devices. In this mode, multiple output streams with the same content but different bitrates or resolutions are generated for the player. The player is then delivered the most suitable stream, improving the overall livestreaming experience.

#### Prerequisites

You have created [transcoding templates](#) with **Triggered By** set to **Stream push** and **Use Source I-Frame** enabled.

#### 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 ingest domain name.  
The subservice type of the domain name must be Cloud Live.
- Step 4** In the navigation pane, choose **Templates > Adaptive Bitrate (ABR)**.
- Step 5** Click **Create ABR Template**. The page shown in [Figure 3-16](#) is displayed on the right.  
Configure ABR template parameters by referring to [Table 3-4](#).

**Figure 3-17** Create ABR Template

### Adaptive Bitrate (ABR) ✕

**Name**

**App Name**

The value can contain uppercase letters, lowercase letters, digits, underscores (\_), and hyphens (-).

**Transcoding Template List**

You can only select a transcoding template with Use Source I-Frame enabled and Triggered By set to Stream push.

**Table 3-5** Parameters

Parameter	Description
Name	Name of the ABR template.
App Name	Application name. The default value is <b>live</b> . The value is automatically obtained by the system and cannot be configured.
Transcoding Template List	Select all matched transcoding templates from the drop-down list. For details about how to create a transcoding template, see <a href="#">Transcoding</a> . You can only select transcoding templates with <b>Triggered By</b> set to <b>Stream push</b> and <b>Use Source I-Frame</b> enabled.

**Step 6** Click **OK**. An ABR template is added.

You can perform the following operations on the added template:

- Click **Modify** in the **Operation** column of the ABR template to modify the ABR template settings. You can only modify the transcoding template list.
- Click **Delete** in the **Operation** column of the ABR template to delete the template.

----End

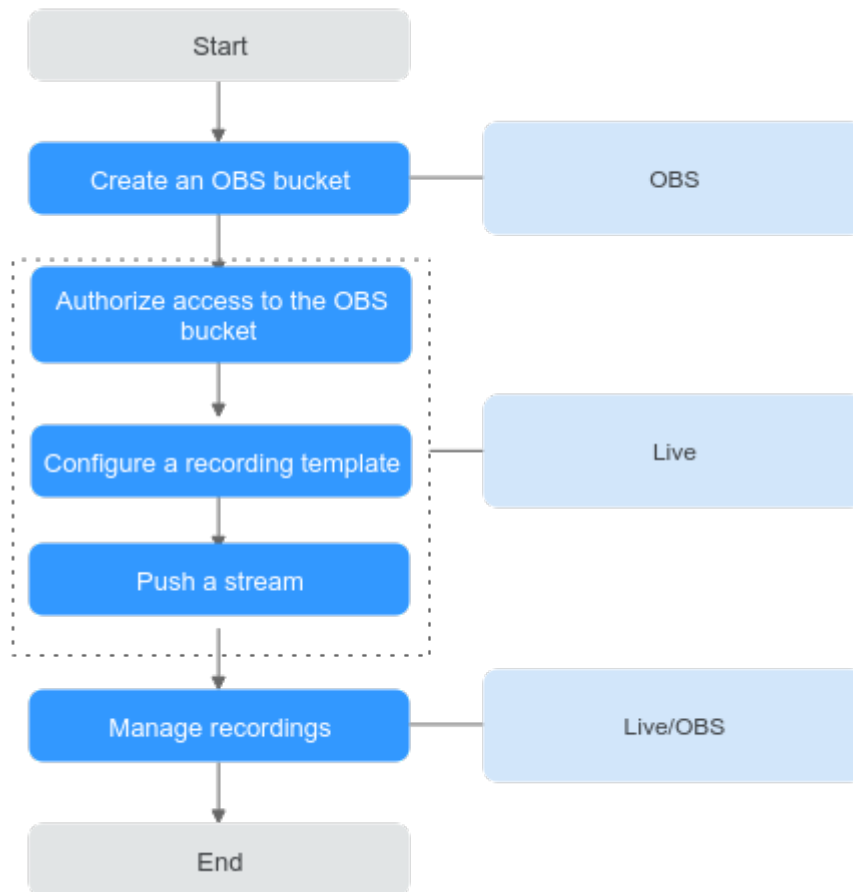
### 3.2.4 Recording Live Video to OBS

### 3.2.4.1 Creating a Recording Template

Live allows you to record a livestream and store the recording in OBS, where you can download and share the recording.

**Figure 3-18** shows the process of recording and storing a live video in OBS.

**Figure 3-18** Process of recording and storing a live video in OBS



1. **(Optional) Create an OBS bucket** for storing recordings. If you already have one, go to 2.

**NOTE**

The created OBS bucket must be in the same region as Live.

2. **Authorize access to the OBS bucket** so that the system can save the recordings in the OBS bucket.

**NOTE**

- Authorizing access to an OBS bucket can only be completed using a Huawei Cloud account. It cannot be done by **IAM users**.
- The OBS bucket that Live is authorized to access must be in the same region as Live.
- If you want to cancel the authorization of access to a bucket, check whether there are recordings or screenshots in the bucket. If there are, the recordings or screenshots will be removed from the bucket after the authorization is canceled.

3. **Configure a recording template.** You can configure multiple templates. The recording template whose **App Name** and **Stream Name** match those in your ingest URL will be applied, and recordings will be stored in OBS based on template settings. You can set a callback address to get notifications about the recording status.
4. Push a stream through an ingest URL and record the livestream based on the configured recording template. For details about how to create an ingest URL, see [Assembling an Ingest URL](#).
5. **Manage recordings.** You can view basic information about recordings on the Live console, and manage recordings, such as preview, sharing, and deletion, on the OBS console.

 **NOTE**

The recordings have the same resolution as the pushed stream.

## Notes

- This function is unavailable in AP-Bangkok.
- Recording templates can be configured at domain name, application, and stream levels. Templates at the stream level take effect first. Templates at the same level must have the same recording type.
- Recordings cannot be deleted from Live because Live does not store recordings. Live logs recording events and stores them for 30 days. You can manually delete recordings from OBS or configure [OBS lifecycle management rules](#) to set a retention period and policy for recordings.
- If stream push is interrupted due to network jitter during live recording, recording stops. When stream push resumes, recording restarts accordingly.
- Recording starts when stream push starts and stops until stream push ends. Recording cannot be stopped or started during stream push. If the recording template is deleted during stream push, recording continues until stream push ends.
- Your account is not in arrears. If this happens, OBS will be suspended, and recording will fail. You are advised to [buy an OBS storage package](#).
- Only input livestreams can be recorded. Transcoded livestreams cannot be recorded.
- If the value of **Max Stream Pause Duration** is greater than 0, you are still billed based on the number of concurrent recording streams during the stream pause duration. For example, if a livestream is pushed from 9:00 to 10:00 in the morning and **Max Stream Pause Duration** is set to 300s, the recording task from 9:00 to 10:05 will also be included in the billing statistics.

## Prerequisites

- You have [added an ingest domain name](#).
- You have [configured CNAME records](#) at your domain names' DNS provider.
- Recordings are stored in OBS. You must [enable OBS](#) before storing recordings in OBS.

## Pricing Notes

- Live recording is billed by Live. For details, see [Recording Billing](#).
- Live recordings are stored in OBS. Therefore, OBS charges you for the storage. For details, see [OBS Pricing Details](#).

## Step 1: (Optional) Create an OBS Bucket

If you have not created an OBS bucket, [create one](#). If you already have one, go to [Step 2: Authorize Access to the OBS Bucket](#).

## Step 2: Authorize Access to the OBS Bucket

For details, see [OBS Authorization](#).

## Step 3: Configure a Recording Template

If you want to record livestreams for replay, configure recording templates. The recording template whose **App Name** and **Stream Name** match those in your ingest URL will be applied.

**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 ingest domain name.

**Step 4** In the navigation pane, choose **Templates > Recording (New)**.

**Step 5** Click **Create Recording Template**. The **Recording** dialog box is displayed on the right, as shown in [Figure 3-19](#).

Configure recording parameters based on [Table 3-6](#).

Figure 3-19 Creating a recording template

### Recording ✕

Recording Type

Automatic  Manual

App Name

Default: live. To match all names, use an asterisk (\*).

Stream Name

To match all names, use an asterisk (\*).

Storage Location

Object Storage Service (OBS)

Video files recorded during livestreaming and video files hosted by VOD for transcoding or packaging are stored in OBS. The storage fee is charged by OBS. See [OBS Pricing Details](#)

Storage Bucket

No OBS buckets available? [Authorize](#)

After access to the OBS bucket is authorized, Live can access the OBS bucket. Ensure that the bucket processes only workloads related to Live. Do not store confidential files in the bucket.

Storage Path (Optional)

Record As

HLS  FLV  MP4

For details about the audio/video formats supported by live recording, see [Constraints](#).

**Table 3-6** Parameters

Parameter	Description
Recording Type	<ul style="list-style-type: none"> <li>• <b>Automatic:</b> Recording automatically starts when livestreams that match the recording template are pushed.</li> <li>• <b>Manual:</b> When livestreams that match the recording template are pushed, you can call the API for <a href="#">submitting a recording command</a> to start or stop recording. Manual recording can only begin after the livestreams have been successfully pushed. To avoid manual recording failures caused by unsuccessful stream pushes, you can configure stream status notifications. After a start notification is received, the system sends the manual recording request.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• The recording type cannot be changed after the template is created.</li> <li>• You can call the API to start recording only when the livestreams have been pushed.</li> <li>• Manual recording supports only recording start and stop for a specific stream. Even if the recording template is at the domain name level, the stream name must be specified when you deliver the recording start and stop commands.</li> <li>• To manually stop recording, you can set <b>Maximum Stream Pause Length</b> when configuring the recording template, so that recording will stop when the stream has been paused beyond the time indicated by <b>Maximum Stream Pause Length</b>. You can also call an API to stop recording.</li> <li>• After the command for stopping recording is manually delivered, it takes a period of time to clear resources for the recording task. If the command for starting recording is delivered again shortly after the stop command is delivered, a message indicating that the recording task is not complete may be returned.</li> </ul>
App Name	Application name. The default value is <b>live</b> . You can customize the application name. Only letters, digits, underscores (_), and hyphens (-) are allowed. If this parameter is set to *, the recording template applies to all applications under the domain name.
Stream Name	Livestream name. If this parameter is set to *, the recording template applies to all livestreams under the specified application.
Storage Location	Where recordings are stored
Storage Bucket	OBS bucket where recordings are stored
Storage Path (Optional)	OBS path where recordings are stored To change the path later, click <b>Edit</b> in the <b>Operation</b> column of the row containing the template in the recording template list.

Parameter	Description
Record As	Format of recordings. Live videos can be recorded in HLS, FLV, or MP4 format.
HLS	<p><b>M3U8 File Naming:</b> The storage path and file name prefix need to be specified. Record/{publish_domain}/{app}/{record_type}/{record_format}/ {stream}_{file_start_time}/{stream}_{file_start_time}</p> <p>Parameter description:</p> <ul style="list-style-type: none"> <li>● <b>Record:</b> Retain the default value.</li> <li>● <b>publish_domain:</b> the ingest domain name added on the Live console</li> <li>● <b>app:</b> application name, which defaults to <b>live</b></li> <li>● <b>record_type:</b> value of <b>Recording Type</b> on the current page</li> <li>● <b>record_format:</b> value of <b>Record As</b> on the current page</li> <li>● <b>stream:</b> livestream name</li> </ul> <p><b>TS File Naming:</b> The file name prefix needs to be specified. {file_start_time_unix}_{file_end_time_unix}_{ts_sequence_number}</p> <p><b>Recording Length:</b> Its value ranges from 1 to 720 minutes. If a live video has been recorded for more than 12 hours, a new M3U8 file will be created based on the naming rule.</p> <p>Options of <b>Max Stream Pause Length:</b></p> <ul style="list-style-type: none"> <li>● <b>Generate a new file when a stream is paused</b></li> <li>● <b>Do not generate a new file when a stream is paused</b></li> <li>● <b>Other:</b> If the interruption duration of a livestream exceeds the specified range, a new recording file is generated. The maximum interruption duration of a livestream is 300s.</li> </ul>
FLV	<p><b>File Naming:</b> The storage path and file name prefix need to be specified. Record/{publish_domain}/{app}/{record_type}/{record_format}/ {stream}_{file_start_time}/{file_start_time}</p> <p>Parameter description:</p> <ul style="list-style-type: none"> <li>● <b>Record:</b> Retain the default value.</li> <li>● <b>publish_domain:</b> the ingest domain name added on the Live console</li> <li>● <b>app:</b> application name, which defaults to <b>live</b></li> <li>● <b>record_type:</b> value of <b>Recording Type</b> on the current page</li> <li>● <b>record_format:</b> value of <b>Record As</b> on the current page</li> <li>● <b>stream:</b> livestream name</li> </ul> <p><b>Recording Length:</b> Its value ranges from 1 to 360 minutes. If a live video has been recorded for more than six hours, a new file will be created based on the naming rule.</p>

Parameter	Description
	<p>Options of <b>Max Stream Pause Length</b>:</p> <ul style="list-style-type: none"> <li>• <b>Generate a new file when a stream is paused</b></li> <li>• <b>Other</b>: If the interruption duration of a livestream exceeds the specified range, a new recording file is generated.</li> </ul>
MP4	<p><b>File Naming</b>: The storage path and file name prefix need to be specified. Record/{publish_domain}/{app}/{record_type}/{record_format}/{stream}_{file_start_time}/{file_start_time}</p> <p>Parameter description:</p> <ul style="list-style-type: none"> <li>• <b>Record</b>: Retain the default value.</li> <li>• <b>publish_domain</b>: the ingest domain name added on the Live console</li> <li>• <b>app</b>: application name, which defaults to <b>live</b></li> <li>• <b>record_type</b>: value of <b>Recording Type</b> on the current page</li> <li>• <b>record_format</b>: value of <b>Record As</b> on the current page</li> <li>• <b>stream</b>: livestream name</li> </ul> <p><b>Recording Length</b>: Its value ranges from 1 to 360 minutes. If a live video has been recorded for more than six hours, a new file will be created based on the naming rule.</p> <p>Options of <b>Max Stream Pause Length</b>:</p> <ul style="list-style-type: none"> <li>• <b>Generate a new file when a stream is paused</b></li> <li>• <b>Other</b>: If the interruption duration of a livestream exceeds the specified range, a new recording file is generated.</li> </ul>

 **NOTE**

- If livestream push is normal, the time when HLS recordings are generated in the OBS bucket is related to the keyframe interval configured on the player. By default, the first recording is generated after three keyframe intervals (6 seconds). An FLV or MP4 recording is generated only after the recording ends.
- For MP4 and FLV recordings, if **Max Stream Pause Length** is enabled, the video encoding format cannot be changed.
- The value of **Max Stream Pause Length** affects the triggering of the recording callback event **RECORD\_FILE\_COMPLETE**.
  - **Do not generate a new file when a stream is paused**: When the recording duration reaches the configured recording length, a recording file is generated and the recording callback event is triggered.
  - **Generate a new file when a stream is paused**: Every time a stream is interrupted, a new recording file is generated and the recording callback event is triggered.
  - **Other**: Every time the stream pause duration reaches the specified value, a new recording file is generated and the recording callback event is triggered. If the stream pause duration does not reach the specified value but the recording duration does, a recording file is generated and the recording callback event is triggered.

**Step 6** Click **OK**.

You can create multiple recording templates. The recording template whose **App Name** and **Stream Name** match those in your ingest URL will be applied.

**Step 7** **Obtain an ingest URL** to **push streams**.

The resolution and bitrate of the generated recordings match those of the livestreams.

----End

You can **manage recordings** on the OBS console, such as preview, download, and share.

## Modifying or Deleting a Recording Template

You can perform the following operations on your recording templates:

- Editing a recording template  
Click **Edit** in the **Operation** column of the row containing the target recording template in the template list to edit the template.  
The recording type cannot be changed.
- Deleting a recording template  
Click **Delete** in the **Operation** column of the row containing the target recording template in the template list to delete the template.

### 3.2.4.2 Configuring a Recording Callback

You can configure an HTTP/HTTPS URL to receive recording status feedback. The system will send POST requests in JSON format to your server, so that you can know the recording status.

#### Prerequisites

- You have **added an ingest domain name**.
- You have **configured CNAME records** at your domain names' DNS provider.

#### 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 ingest domain name.

**Step 4** In the navigation pane, choose **Templates > Recording (New)**.

**Step 5** Click **Create Callback Template**.

In the displayed dialog box, enter a callback URL, as shown in **Figure 3-20**. **Table 3-7** describes the callback parameters.

**Figure 3-20** Adding a callback URL

✕

### Add Callback Template

Protocol

HTTPS
HTTP

HTTP may have security problems. HTTPS is recommended

Callback URL

https://

Callback Type

Record File Complete

Record Start

Record New File Start

Record Over

Record Failed

Callback Authentication

Cancel
OK

**Table 3-7** Recording callback parameters

Parameter	Description
Protocol	A callback URL supports HTTP and HTTPS. HTTPS is more secure than HTTP and is recommended.
Callback URL	The callback URL cannot contain message headers or parameters. Only the HTTP/HTTPS protocol is supported. HTTPS is recommended.
Callback Type	When callback messages are sent. The options are as follows: <ul style="list-style-type: none"> <li>● Record File Complete</li> <li>● Record Start</li> <li>● Record New File Start</li> <li>● Record Over</li> <li>● Record Failed</li> </ul> For details about callback types, see <a href="#">Table 3-8</a> .
Callback Authentication	If this function is enabled, you need to configure <b>Authentication Algorithm</b> and <b>Authentication Key</b> .

Parameter	Description
Authentication Algorithm	The encrypted content in callback messages varies depending on the authentication methods. MD5 is not secure and HMACSHA256 is recommended. <ul style="list-style-type: none"> <li>• <b>MD5:</b> MD5(<i>key</i> + <i>auth_timestamp</i>)</li> <li>• <b>HMACSHA256:</b> HMACSHA256(<i>auth_timestamp</i> + <i>event_type</i> + <i>publish_domain</i> + <i>app</i> + <i>stream</i> + <i>download_url</i> + <i>play_url</i>, <i>key</i>)</li> </ul>
Authentication Key	Authentication key. The value can be customized and contains at least 32 characters, including digits and letters.

**Step 6** Click **OK** to add a callback rule to the list.

----End

## Editing or Deleting a Recording Callback

You can perform the following operations on your recording callback:

- Editing a recording callback  
Click **Edit** in the **Operation** column of the row containing the target recording callback in the callback list to edit the callback.
- Deleting a recording callback  
Click **Delete** in the **Operation** column of the row containing the target recording callback in the callback list to delete the callback.

## Callback Example

**Table 3-8** describes the fields in a callback message body.

```
{
  "project_id": "70b76xxxxxx34253880af501cdxxxxxx",
  "job_id": "dc0a1773-0cef-xxxx-xxxx-9a38fdb095d2",
  "task_id": "51126d0ebe94b1da00d2e21a10xxxxxx",
  "event_type": "RECORD_FILE_COMPLETE",
  "publish_domain": "push.example.com",
  "app": "live",
  "stream": "mystream",
  "record_format": "HLS",
  "download_url": "https://obs.cn-north-4.myhuaweicloud.com/live/record-xxxx-mystream-1589967495/record-push.example.com-live-mystream-1589967495.m3u8",
  "asset_id": "1a0d8e9bfaxxxxxxbe5021e62aa1e96",
  "file_size": 3957964,
  "record_duration": 120,
  "start_time": "2020-03-08T14:10:25Z",
  "end_time": "2020-03-08T14:12:25Z",
  "width": 1280,
  "height": 720,
  "obs_location": "https://obs.cn-north-4.myhuaweicloud.com",
  "obs_bucket": "mybucket",
  "obs_object": "live/record-xxxx-mystream-1589967495/record-hwpublish.myun.tv-live-mystream-1589967495.m3u8",
  "auth_sign": "4f97f46759axxxxxx7ad21e9935dc175",
  "auth_timestamp": 1583676745
}
```

**Table 3-8** Message body

Field	Description
project_id	Project ID.
job_id	Name of a file. This parameter is carried when the value of <b>event_type</b> is <b>RECORD_NEW_FILE_START</b> or <b>RECORD_FILE_COMPLETE</b> .
task_id	Recording task ID, which uniquely identifies a recording task.
event_type	<p>Message type.</p> <p>Options:</p> <ul style="list-style-type: none"> <li>• <b>RECORD_START</b>. This event is triggered when you start recording.</li> <li>• <b>RECORD_NEW_FILE_START</b>. This event is triggered in either of the following scenarios: <ul style="list-style-type: none"> <li>– The system starts creating the first recording file.</li> <li>– After a livestream is resumed, if <b>Maximum Stream Pause Length</b> is set to <b>Generate a new file after a stream is paused.</b>, the system starts to create a recording file.</li> <li>– If the current recording duration exceeds the configured one, the system starts to create another recording file.</li> </ul> </li> <li>• <b>RECORD_FILE_COMPLETE</b>. This event is triggered in either of the following scenarios: <ul style="list-style-type: none"> <li>– When the recording duration reaches the configured recording length, a recording file has been generated. The system starts creating a new recording file.</li> <li>– After a livestream is interrupted, if <b>Maximum Stream Pause Length</b> is set to <b>Generate a new file after a stream is paused.</b>, a recording file has been created. Once the stream is resumed, the system will start creating a new recording file.</li> </ul> </li> <li>• <b>RECORD_OVER</b>. This event is triggered when a livestream has been paused beyond the time indicated by <b>Maximum Stream Pause Length</b> and a recording has been created.</li> <li>• <b>RECORD_FAILED</b>. This event is triggered when stream pulling fails or uploading recordings to OBS fails.</li> </ul>
publish_domain	Ingest domain name.
app	Application name.

Field	Description
stream	Stream name.
record_format	Recording format. The HLS, FLV, and MP4 formats are supported.
download_url	Address to download the recording. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> . <b>NOTE</b> The quality of video playback using the download address cannot be guaranteed.
asset_id	Name of a recording file This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .
file_size	File size. Unit: byte
record_duration	Duration of a recording. Unit: second
start_time	Start time of a recording, which is, time when the first frame is received. The format is yyyy-mm-ddThh:mm:ssZ. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .
end_time	End time of a recording. The format is yyyy-mm-ddThh:mm:ssZ. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .
width	Width of a video recording. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .
height	Height of a video recording. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .
obs_location	Region where the OBS bucket for storing the recording is located. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .
obs_bucket	OBS bucket where recordings are stored. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .

Field	Description
obs_object	OBS path where recordings are stored. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .
auth_sign	Event notification signature. This parameter is carried when an authentication key is configured. <ul style="list-style-type: none"> <li>• MD5: <b>auth_sign</b> = MD5(<i>key</i> + <i>auth_timestamp</i>)</li> <li>• <b>HMACSHA256</b>: HMACSHA256(<i>auth_timestamp</i> + <i>event_type</i> + <i>publish_domain</i> + <i>app</i> + <i>stream</i> + <i>download_url</i> + <i>play_url</i>, <i>key</i>)</li> </ul> <i>key</i> indicates the key used for authentication.
auth_timestamp	UNIX timestamp when the event notification signature expires. This parameter is carried when an authentication key is configured. The value is a decimal Unix timestamp, that is, the number of seconds that have elapsed since January 1, 1970 00:00:00 UTC/GMT. If the time specified by <b>auth_timestamp</b> has expired, the notification will become invalid to avoid network replay attacks.
error_message	Description about a failed recording. This parameter is used only when <b>event_type</b> is <b>RECORD_FAILED</b> .

### 3.2.4.3 Managing Recordings

When the live recording is complete, view recordings on the OBS console.

#### Managing Recordings Using the OBS Console

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

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

**Step 3** In the bucket list, click the bucket that stores recordings.

On the page displayed, you can download and share the recordings.

----End

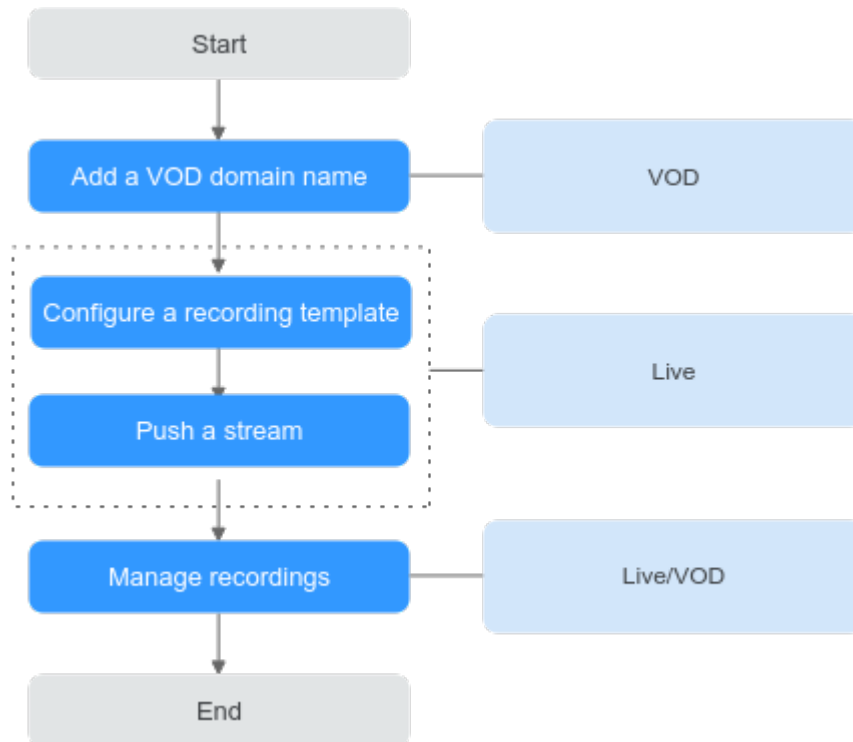
### 3.2.5 Recording Live Video to VOD

#### 3.2.5.1 Creating a Recording Template

Live allows you to record a livestream and store the recording in VOD, where you can download and share the recording.

**Figure 3-21** shows the process of recording live video to VOD.

**Figure 3-21** Process of recording live video to VOD



1. **Add a VOD domain name.** Before managing recording files in VOD, you need to enable the VOD service and add a domain name for VOD acceleration. For details, see [Getting Started with VOD](#).
2. **Configure a recording template.** You can configure multiple templates. The recording template whose **App Name** and **Stream Name** match those in your ingest URL will be applied, and recordings will be stored in VOD based on template settings. You can set a callback address to get notifications about the recording status.
3. Push a stream through an ingest URL and record the livestream based on the configured recording template. For details about how to create an ingest URL, see [Assembling an Ingest URL](#).
4. **Manage recordings.** You can view basic information about recordings on the Live console, and manage recordings, such as preview, sharing, and deletion, on the VOD console.

**NOTE**

The recordings have the same resolution as the pushed stream.

**Notes**

- This function is available only in AP-Singapore.
- Recording templates can be configured at domain name, application, and stream levels. Templates at the stream level take effect first. Templates at the same level must have the same recording type.

- Recordings cannot be deleted from Live because Live does not store recordings. Live logs recording events and stores them for 30 days.
- If stream push is interrupted due to network jitter during live recording, recording stops. When stream push resumes, recording restarts accordingly.
- Recording starts when stream push starts and stops until stream push ends. Recording cannot be stopped or started during stream push. If the recording template is deleted during stream push, recording continues until stream push ends.
- Only input livestreams can be recorded. Transcoded livestreams cannot be recorded.
- If the value of **Max Stream Pause Duration** is greater than 0, you are still billed based on the number of concurrent recording streams during the stream pause duration. For example, if a livestream is pushed from 9:00 to 10:00 in the morning and **Max Stream Pause Duration** is set to 300s, the recording task from 9:00 to 10:05 will also be included in the billing statistics.

## Prerequisites

- You have [added an ingest domain name](#).
- You have [configured CNAME records](#) at your domain names' DNS provider.
- You have enabled the function of recording to VOD. To enable it, [submit a service ticket](#).
- You have enabled the VOD service and added a domain name for VOD acceleration. This is a required step before you can manage recording files in VOD. For details, see [Getting Started with VOD](#).

## Pricing Notes

- Live recording is billed by Live. For details, see [Recording Billing](#).
- Live recordings are stored in VOD. Therefore, VOD charges you for the storage. For details, see [VOD Pricing Details](#).

## Step 1: Add a VOD Domain Name

Before managing recording files in VOD, you need to enable the VOD service and add a domain name for VOD acceleration. For details, see [Getting Started with VOD](#).

## Step 2: Configure a Recording Template

If you want to record livestreams for replay, configure recording templates. The recording template whose **App Name** and **Stream Name** match those in your ingest URL will be applied.

**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 ingest domain name.

**Step 4** In the navigation pane, choose **Templates > Recording (New)**.

**Step 5** Click **Create Recording Template**. The **Recording** dialog box is displayed on the right, as shown in [Figure 3-22](#).

Configure recording parameters based on [Table 3-9](#).

**Figure 3-22** Creating a recording template

**Recording** ✕

Recording Type  
 Automatic  Manual

App Name  
  
Default: live. To match all names, use an asterisk (\*).

Stream Name  
  
To match all names, use an asterisk (\*).

Storage Location  
 Object Storage Service (OBS)  Video on Demand (VOD)  
Media files recorded during livestreaming are stored in OBS or VOD. The storage fee is charged by the storage service you use. See [OBS Pricing Details](#) [VOD Pricing Details](#)

Transcoding Template Group Name (Optional)

Record As  
 HLS  FLV  MP4  
For details about the audio/video formats supported by live recording, see [Constraints](#)

^ **HLS**

Recording Length  
 min  
If the livestream duration exceeds the preset recording length, a new recording file will be generated.

Max Stream Pause Length

**Table 3-9** Parameters

Parameter	Description
Recording Type	<ul style="list-style-type: none"> <li>● <b>Automatic:</b> Recording automatically starts when livestreams that match the recording template are pushed.</li> <li>● <b>Manual:</b> When livestreams that match the recording template are pushed, you can call the API for <a href="#">submitting a recording command</a> to start or stop the recording. Manual recording can only begin after the livestreams have been successfully pushed. To avoid manual recording failures caused by unsuccessful stream pushes, you can configure stream status notifications. After a start notification is received, the system sends the manual recording request.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>● The recording type cannot be changed after the template is created.</li> <li>● You can call the API to start recording only when the livestreams have been pushed.</li> <li>● Manual recording supports only recording start and stop for a specific stream. Even if the recording template is at the domain name level, the stream name must be specified when you deliver the recording start and stop commands.</li> <li>● To manually stop recording, you can set <b>Maximum Stream Pause Length</b> when configuring the recording template, so that recording will stop when the stream has been paused beyond the time indicated by <b>Maximum Stream Pause Length</b>. You can also call an API to stop recording.</li> <li>● After the command for stopping recording is manually delivered, it takes a period of time to clear resources for the recording task. If the command for starting recording is delivered again shortly after the stop command is delivered, a message indicating that the recording task is not complete may be returned.</li> </ul>
App Name	Application name. The default value is <b>live</b> . You can customize the application name. Only letters, digits, underscores (_), and hyphens (-) are allowed. If this parameter is set to *, the recording template applies to all applications under the domain name.
Stream Name	Livestream name. If this parameter is set to *, the recording template applies to all livestreams under the specified application.
Storage Location	Where recordings are stored Select <b>Video on Demand (VOD)</b> .
Transcoding Template Group Name	Enter the name of the transcoding template group configured in VOD. You can create a transcoding template group in VOD or use an existing one. For details, see <a href="#">Transcoding Settings</a> .

Parameter	Description
Record As	Format of recordings. Live videos can be recorded in HLS, FLV, or MP4 format.
HLS	<p><b>Recording Length:</b> Its value ranges from 1 to 720 minutes. If a live video has been recorded for more than 12 hours, a new M3U8 file will be created based on the naming rule.</p>
	<p>Options of <b>Max Stream Pause Length:</b></p> <ul style="list-style-type: none"> <li>• <b>Generate a new file when a stream is paused.</b> This option is not supported for HLS.</li> <li>• <b>Do not generate a new file when a stream is paused</b></li> <li>• <b>Other:</b> If the interruption duration of a livestream is within the specified range, no new recording file is generated. Otherwise, a new recording file is generated. The maximum interruption duration of a livestream is 300s.</li> </ul>
FLV	<p><b>Recording Length:</b> Its value ranges from 1 to 360 minutes. If a live video has been recorded for more than six hours, a new file will be created based on the naming rule.</p>
	<p>Options of <b>Max Stream Pause Length:</b></p> <ul style="list-style-type: none"> <li>• <b>Generate a new file when a stream is paused.</b></li> <li>• <b>Other:</b> If the interruption duration of a livestream is within the specified range, no new recording file is generated. Otherwise, a new recording file is generated.</li> </ul>
MP4	<p><b>Recording Length:</b> Its value ranges from 1 to 360 minutes. If a live video has been recorded for more than six hours, a new file will be created based on the naming rule.</p>
	<p>Options of <b>Max Stream Pause Length:</b></p> <ul style="list-style-type: none"> <li>• <b>Generate a new file when a stream is paused.</b></li> <li>• <b>Other:</b> If the interruption duration of a livestream is within the specified range, no new recording file is generated. Otherwise, a new recording file is generated.</li> </ul>

 NOTE

- If livestream push is normal, the time when HLS recordings are generated is related to the keyframe interval configured on the player. By default, the first recording is generated after three keyframe intervals (6 seconds). An FLV or MP4 recording is generated only after the recording ends.
- For MP4 and FLV recordings, if **Max Stream Pause Length** is enabled, the video encoding format cannot be changed.
- The value of **Max Stream Pause Length** affects the triggering of the recording callback event **RECORD\_FILE\_COMPLETE**.
  - **Do not generate a new file when a stream is paused:** This option is not supported for recording to VOD.
  - **Generate a new file when a stream is paused:** Every time a stream is interrupted, a new recording file is generated and the recording callback event is triggered.
  - **Other:** Every time the stream pause duration reaches the specified value, a new recording file is generated and the recording callback event is triggered. If the stream pause duration does not reach the specified value but the recording duration does, a recording file is generated and the recording callback event is triggered.

**Step 6** Click **OK**.

You can create multiple recording templates. The recording template whose **App Name** and **Stream Name** match those in your ingest URL will be applied.

**Step 7** [Obtain an ingest URL](#) to [push streams](#).

The resolution and bitrate of the generated recordings match those of the livestreams.

----End

You can [manage recordings](#) on the Live or VOD console, such as preview, download, and sharing.

## Modifying or Deleting a Recording Template

You can perform the following operations on your recording template:

- Editing a recording template  
Click **Edit** in the **Operation** column of the row containing the target recording template in the template list to edit the template.  
The recording type cannot be changed.
- Deleting a recording template  
Click **Delete** in the **Operation** column of the row containing the target recording template in the template list to delete the template.

### 3.2.5.2 Configuring a Recording Callback

You can configure an HTTP/HTTPS URL to receive recording status feedback. The system will send POST requests in JSON format to your server, so that you can know the recording status.

## Prerequisites

- You have [added an ingest domain name](#).
- You have [configured CNAME records](#) at your domain names' DNS provider.

## 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 ingest domain name.

**Step 4** In the navigation pane, choose **Templates > Recording (New)**.

**Step 5** Click **Create Callback Template**.

In the displayed dialog box, enter a callback URL, as shown in [Figure 3-23](#). [Table 3-10](#) describes the callback parameters.

**Figure 3-23** Adding a callback URL

**Add Callback Template** ×

Protocol

**HTTPS** HTTP

HTTP may have security problems. HTTPS is recommended

Callback URL

https://

Callback Type

Record File Complete  Record Start  Record New File Start

Record Over  Record Failed

Callback Authentication

**Table 3-10** Parameters

Parameter	Description
Protocol	A callback URL supports HTTP and HTTPS. HTTPS is more secure than HTTP and is recommended.
Callback URL	The callback URL cannot contain message headers or parameters. Only the HTTP/HTTPS protocol is supported. HTTPS is recommended.
Callback Type	When callback messages are sent. The options are as follows: <ul style="list-style-type: none"> <li>Record File Complete</li> <li>Record Start</li> <li>Record New File Start</li> <li>Record Over</li> <li>Record Failed</li> </ul> For details about callback types, see <a href="#">Table 3-11</a> .
Callback Authentication	If this function is enabled, you need to configure <b>Authentication Algorithm</b> and <b>Authentication Key</b> .
Authentication Algorithm	The encrypted content in callback messages varies depending on the authentication methods. MD5 is not secure and HMACSHA256 is recommended. <ul style="list-style-type: none"> <li><b>MD5:</b> MD5(<i>key</i> + <i>auth_timestamp</i>)</li> <li><b>HMACSHA256:</b> HMACSHA256(<i>auth_timestamp</i> + <i>event_type</i> + <i>publish_domain</i> + <i>app</i> + <i>stream</i> + <i>download_url</i> + <i>play_url</i>, <i>key</i>)</li> </ul>
Authentication Key	Authentication key. The value can be customized and contains at least 32 characters, including digits and letters.

**Step 6** Click **OK** to add a callback rule to the list.

----End

## Editing or Deleting a Recording Callback

You can perform the following operations on your recording callback:

- Editing a recording callback  
Click **Edit** in the **Operation** column of the row containing the target recording callback in the callback list to edit the callback.
- Deleting a recording callback  
Click **Delete** in the **Operation** column of the row containing the target recording callback in the callback list to delete the callback.

## Callback Example

[Table 3-11](#) describes the fields in a callback message body.

```
{
  "project_id": "70b76xxxxx34253880af501cdxxxxx",
  "job_id": "dc0a1773-0cef-xxxx-xxxx-9a38fdb095d2",
  "task_id": "51126d0ebe94b1da00d2e21a10xxxxx",
  "event_type": "RECORD_FILE_COMPLETE",
  "publish_domain": "push.example.com",
  "app": "live",
  "stream": "mystream",
  "record_format": "HLS",
  "download_url": "https://obs.cn-north-4.myhuaweicloud.com/live/record-xxxx-mystream-1589967495/record-push.example.com-live-mystream-1589967495.m3u8",
  "asset_id": "1a0d8e9bfaxxxxx5021e62aa1e96",
  "file_size": 3957964,
  "record_duration": 120,
  "start_time": "2020-03-08T14:10:25Z",
  "end_time": "2020-03-08T14:12:25Z",
  "width": 1280,
  "height": 720,
  "auth_sign": "4f97f46759axxxxx7ad21e9935dc175",
  "auth_timestamp": 1583676745
}
```

**Table 3-11** Message body

Field	Description
project_id	Project ID
job_id	Name of a file. This parameter is carried when the value of <b>event_type</b> is <b>RECORD_NEW_FILE_START</b> or <b>RECORD_FILE_COMPLETE</b> .
task_id	Recording task ID, which uniquely identifies a recording task.

Field	Description
event_type	<p>Message type.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>RECORD_START</b>. This event is triggered when you start recording.</li> <li>• <b>RECORD_NEW_FILE_START</b>. This event is triggered in either of the following scenarios: <ul style="list-style-type: none"> <li>– The system starts creating the first recording file.</li> <li>– After a livestream is resumed, if <b>Maximum Stream Pause Length</b> is set to <b>Generate a new file after a stream is paused.</b>, the system starts to create a recording file.</li> <li>– If the current recording duration exceeds the configured one, the system starts to create another recording file.</li> </ul> </li> <li>• <b>RECORD_FILE_COMPLETE</b>. This event is triggered in either of the following scenarios: <ul style="list-style-type: none"> <li>– When the recording duration reaches the configured recording length, a recording file has been generated. The system starts creating a new recording file.</li> <li>– After a livestream is interrupted, if <b>Maximum Stream Pause Length</b> is set to <b>Generate a new file after a stream is paused.</b>, a recording file has been created. Once the stream is resumed, the system will start creating a new recording file.</li> </ul> </li> <li>• <b>RECORD_OVER</b>. This event is triggered when a livestream has been paused beyond the time indicated by <b>Maximum Stream Pause Length</b> and a recording has been created.</li> <li>• <b>RECORD_FAILED</b>. This event is triggered when stream pulling fails or uploading recordings to OBS fails.</li> </ul>
publish_domain	Ingest domain name
app	Application name
stream	Stream name
record_format	Recording format. The HLS, FLV, and MP4 formats are supported.

Field	Description
download_url	Address to download the recording. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> . <b>NOTE</b> The quality of video playback using the download address cannot be guaranteed.
asset_id	If you set <b>Storage Location</b> to <b>Video on Demand</b> when <b>configuring a recording template</b> , this parameter is the media asset ID in VOD and is used to identify a recording file. Otherwise, it is only used to identify a recording file. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .
file_size	File size Unit: byte
record_duration	Duration of a recording Unit: second
start_time	Start time of a recording, which is, time when the first frame is received. The format is yyyy-mm-ddThh:mm:ssZ. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .
end_time	End time of a recording. The format is yyyy-mm-ddThh:mm:ssZ. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .
width	Width of a video recording. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .
height	Height of a recording. This parameter is used only when <b>event_type</b> is <b>RECORD_FILE_COMPLETE</b> .
auth_sign	Event notification signature. This parameter is carried when an authentication key is configured. <ul style="list-style-type: none"> <li>• MD5: <b>auth_sign</b> = MD5(<i>key</i> + <i>auth_timestamp</i>)</li> <li>• HMACSHA256: HMACSHA256(<i>auth_timestamp</i> + <i>event_type</i> + <i>publish_domain</i> + <i>app</i> + <i>stream</i> + <i>download_url</i> + <i>play_url</i>, <i>key</i>)</li> </ul> <i>key</i> indicates the key used for authentication.

Field	Description
auth_timestamp	UNIX timestamp when the event notification signature expires. This parameter is carried when an authentication key is configured.  The value is a decimal Unix timestamp, that is, the number of seconds that have elapsed since January 1, 1970 00:00:00 UTC/GMT.  If the time specified by <b>auth_timestamp</b> has expired, the notification will become invalid to avoid network replay attacks.
error_message	Description about a failed recording.  This parameter is used only when <b>event_type</b> is <b>RECORD_FAILED</b> .

### 3.2.5.3 Managing Recordings

You can view recordings on the Live or VOD console or by calling the VOD API.

#### Managing Recordings Using VOD

- View recordings on the VOD console.
  - a. On the **Audio and Video Management** page of the [VOD console](#), query recordings by date or name keyword.
  - b. Click **Details** in the row containing the target recording. On the displayed page, you can transcode, categorize, add a thumbnail, and upload subtitles for the recording. For details, see [VOD User Guide](#).
- Obtain recordings by calling a VOD API.

Call an API for [querying media files](#) and set **query\_string** to **Record\_** to obtain details about recordings.

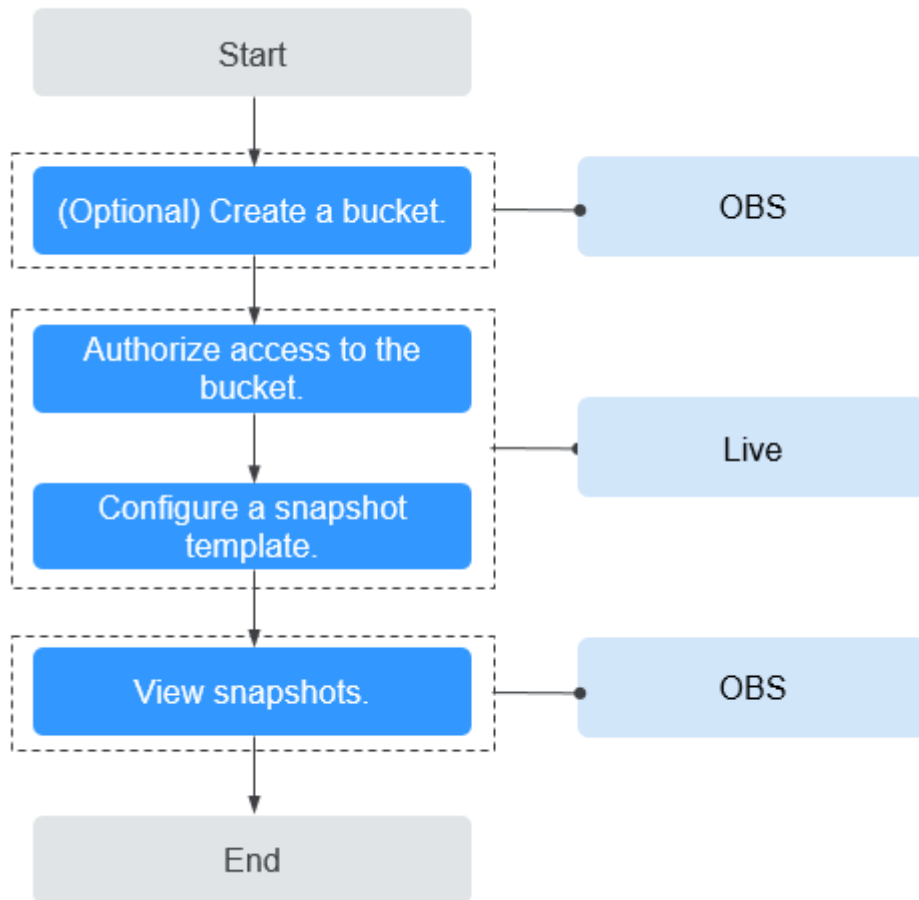
### 3.2.6 Snapshot Capturing

Live captures snapshots from a livestream based on a configured template and stores the captured snapshots in an OBS bucket. Multiple snapshot templates can be configured for an ingest domain name. The template whose *App Name* matches that in your ingest URL will be applied.

#### Process Flow

[Figure 3-24](#) shows the process for configuring a snapshot template.

Figure 3-24 Process for configuring a snapshot template



1. **(Optional) Create an OBS bucket** for storing live video snapshots. If you already have one, go to 2.

**NOTE**

The OBS bucket for storing live video snapshots must be in the same region as the Live service. For example, if you use Live in the **CN North-Beijing4** region, then snapshots must be stored in an OBS bucket in the **CN North-Beijing4** region.

2. **Authorize access to the OBS bucket** so that the system can save the snapshots in the OBS bucket.
3. **Configure a snapshot template** to capture snapshots from a video stream at a specified interval and save them as JPG files in an authorized OBS bucket.
4. **View snapshots** in the output path.

## Notes

- Live and the OBS bucket for storing snapshots must be in the same region.
- You are advised to set the OBS bucket as a private bucket. The differences between a private bucket and a public bucket are as follows:

- Private bucket: You must add authentication information before accessing the bucket and downloading snapshots. For details about the authentication information, see [Creating a Signed URL \(SDK for Go\)](#).
- Public bucket: You can directly access the bucket and download snapshots.
- Multiple snapshot templates can be configured for a domain name. The snapshot template whose **App Name** matches that in your ingest URL will be applied.
- Only JPG files can be generated.
- In the **AP-Bangkok** region, [submit a service ticket](#) for review after configuring a template. The configuration takes effect only after it is approved.
- Huawei Cloud Live plans to bring offline the function of carrying authentication information in a snapshot callback URL on August 15, 2024.

## Prerequisites

- You have [added an ingest domain name](#).
- You have [configured CNAME records](#) at your domain names' DNS provider.
- Snapshots are stored in OBS. You must [enable OBS](#) before storing recordings in OBS.

## Pricing Notes

- Snapshot capturing is a billing item. For details, see [Live Pricing Details](#).
- Snapshots are stored in OBS. Therefore, OBS charges you for the storage. For details, see [OBS Pricing Details](#).

## Step 1: (Optional) Create an OBS Bucket

If you have not created an OBS bucket, [create one](#) in the region of Live. If you already have one, go to [Step 2: Authorize Access to the OBS Bucket](#).

## Step 2: Authorize Access to the OBS Bucket

For details, see [OBS Authorization](#).

## Step 3: Configure a Snapshot Template

After OBS authorization is successful, you can configure a snapshot template.

**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 ingest domain name.

**Step 4** In the navigation pane, choose **Templates > Snapshot Capturing**.

**Step 5** Click **Create Snapshot Template**. The **Snapshot Capturing** dialog box is displayed on the right.

Figure 3-25 Creating a snapshot template

### Snapshot Capturing ✕

**i** You are advised to set the OBS bucket as a private bucket. The differences between a private bucket and a public bucket are as follows:

- Private bucket: You must add authentication information before accessing the bucket and downloading snapshots. For details about the authentication information, see [Creating a Signed URL \(SDK for Go\)](#)[Learn more](#) [↗](#)
- Public bucket: You can directly access the bucket and download snapshots.

App Name

Defaults to live and can contain letters, digits, underscores ( \_ ), and hyphens (-). The template takes effect only when the App Name is the same as that in the ingest URL.

Storage Location

Object Storage Service (OBS)

Live screenshots are stored in OBS buckets. The storage fee is charged by OBS.  
[OBS Pricing Details](#) [↗](#)

Storage Bucket

No OBS buckets available?[Authorize](#) [↗](#)

After access to the OBS bucket is authorized, Live can access the OBS bucket. Ensure that the bucket processes only workloads related to Live. Do not store confidential files in the bucket.

Storage Path (Optional)

Capturing Frequency

seconds

Value range: 5–3,600

Storage Mode

All: All snapshots are saved. Latest: Only the latest snapshot is saved.

Callback [?](#)

Table 3-12 describes the parameters.

**Table 3-12** Template parameters

Parameter	Description
App Name	Application name. The default value is <b>live</b> . You can customize the application name. Only letters, digits, underscores (_), and hyphens (-) are allowed. The snapshot template whose application name matches that in your ingest URL takes effect.
Storage Location	Live snapshots are stored in OBS.
Storage Bucket	OBS bucket for storing snapshots
Storage Path (Optional)	OBS bucket path for storing snapshots
Capturing Frequency	Snapshot capturing frequency, in seconds. Value range: 5 to 3,600
Storage Mode	Snapshot file storage mode. <ul style="list-style-type: none"><li>• <b>All</b>: A snapshot file name contains the timestamp. All snapshot files of each stream are stored in OBS. Example: <code>snapshot/{domain}/{app_name}/{stream_name}/{UnixTimestamp}.jpg</code></li><li>• <b>Latest</b>: A snapshot file name does not contain the timestamp. Only the latest snapshot file of each stream will be saved. A new snapshot file overwrites the previous one. Example: <code>snapshot/{domain}/{app_name}/{stream_name}.jpg</code></li></ul>
Callback	Whether to enable callback. If this function is enabled, you need to deploy an HTTP/HTTPS service to receive callback messages and configure a callback URL on the console or using APIs. When a snapshot is successfully captured, the Live server sends a POST request to the callback URL. The request body is in JSON format.
Protocol	A callback URL supports HTTP and HTTPS. HTTPS is more secure than HTTP and is recommended.
Callback URL	Enter a callback URL when <b>Callback</b> is enabled. A callback URL cannot contain message headers or parameters. HTTP and HTTPS (recommended) are supported. Callback messages in JSON format are sent in POST requests to your server through HTTP APIs. For details about a callback message body, see <a href="#">Callback Message</a> .
Authentication Key (Optional)	Authentication key. Configure this parameter only when callback authentication is required. <ul style="list-style-type: none"><li>• A key contains 32 to 128 characters.</li><li>• A key can also be automatically generated.</li></ul>

**Step 6** Click **OK**.

After the snapshot template is configured, you can start streaming live videos. The Live service will take snapshots for livestreams based on the snapshot template.

**Step 7** Click **Edit** in the **Operation** column to modify template parameters. **App Name** cannot be modified.

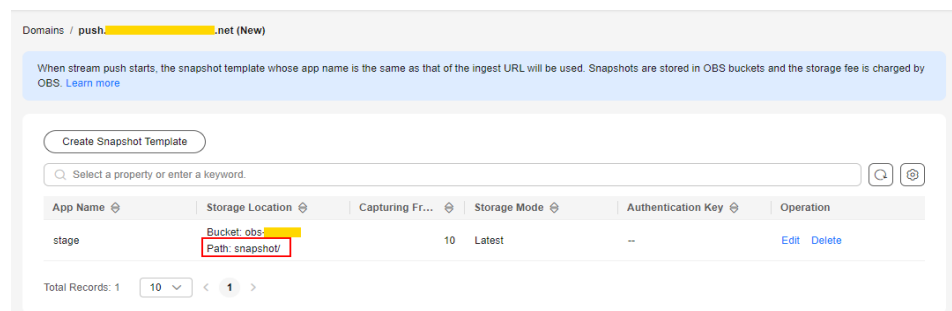
----End

## Step 4: View Snapshots

View snapshots in the predefined output path or from a download link in your received callback message.

- Viewing snapshots on the console
  - a. Log in to the [Live console](#).
  - b. In the navigation pane, choose **Domains**.
  - c. Click **Manage** in the **Operation** column of the desired ingest domain name.
  - d. In the navigation pane, choose **Templates > Snapshot Capturing**.
  - e. Click the output path in the **Storage Location** column to go to the OBS bucket and view snapshot details.

**Figure 3-26** Viewing snapshot details



You can download and share the snapshots. For details, see [OBS Help Center](#).

- Viewing snapshots through a callback message
 

If you set a callback URL when [configuring a snapshot template](#), then you will receive a message each time a snapshot is generated. [Table 3-13](#) describes the fields in a callback message.

```
{
  "domain": "play.example.com",
  "app": "live",
  "stream_name": "test001",
  "snapshot_url": "https://xxx.obs.cn-north-4.myhuaweicloud.com:443...",
  "width": "720",
  "height": "1280",
  "obs_addr": {
    "bucket": "xxx",
    "location": "cn-north-4",
    "object": "xxx.jpg"
  },
  "auth_timestamp": 1587954140,
}
```

```
"auth_sign":"4918b1axxxxxb583cffa119d72513bbc35a989f8569fxxxxx057646154a04a"
}
```

**Table 3-13** Message body

Field	Description
domain	Ingest domain name
app	Application name
stream_name	Stream name
snapshot_url	URL to download snapshots
width	Image width Unit: pixel
height	Image height Unit: pixel
obs_addr	Address of the OBS bucket where snapshots are stored. <ul style="list-style-type: none"> <li>• <b>bucket:</b> OBS bucket name</li> <li>• <b>location:</b> Region where the OBS bucket is located</li> <li>• <b>object:</b> OBS object path</li> </ul>
auth_timestamp	UNIX timestamp when the event notification signature expires. This parameter is carried when an authentication key is configured.  The value is a decimal Unix timestamp, that is, the number of seconds that have elapsed since January 1, 1970 00:00:00 UTC/GMT.  Example: <b>1592639100</b> (June 20, 2020 15:45)
auth_sign	Event notification signature. This parameter is carried when an authentication key is configured. auth_sign = HmacSHA256(domain + app + stream_name + snapshot_url + width + height + obs_addr.bucket + obs_addr.location + obs_addr.object + auth_timestamp,key)  <i>key</i> indicates the key used for authentication.

### 3.2.7 Stream Status Notifications

You can add a URL on the Live console for receiving messages when stream push starts or ends. The messages are sent as POST requests to your server through an HTTP API. Then your server returns the status code 200 to confirm that the messages have been received.

#### Notes

In the AP-Bangkok region, [submit a service ticket](#) for review after configuring stream status notifications. The configuration takes effect only after it is approved.

After stream status notifications are enabled, you will receive a message each time when a livestream is pushed or disconnected. However, when a stream is disconnected soon after it was pushed, the server may receive the message on stream disconnection before receiving the message on stream push due to network transmission latency. In this case, you need to check the Unix timestamp parameter **publish\_timestamp** in the message to check whether the stream push and stream disconnection are in the same stream push event. The timestamps generated for the stream push and stream disconnection of the same stream push event are the same.

## Prerequisites

- You have [added an ingest domain name](#).
- You have [configured CNAME records](#) at your domain names' DNS provider.

## Adding a Notification URL

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

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

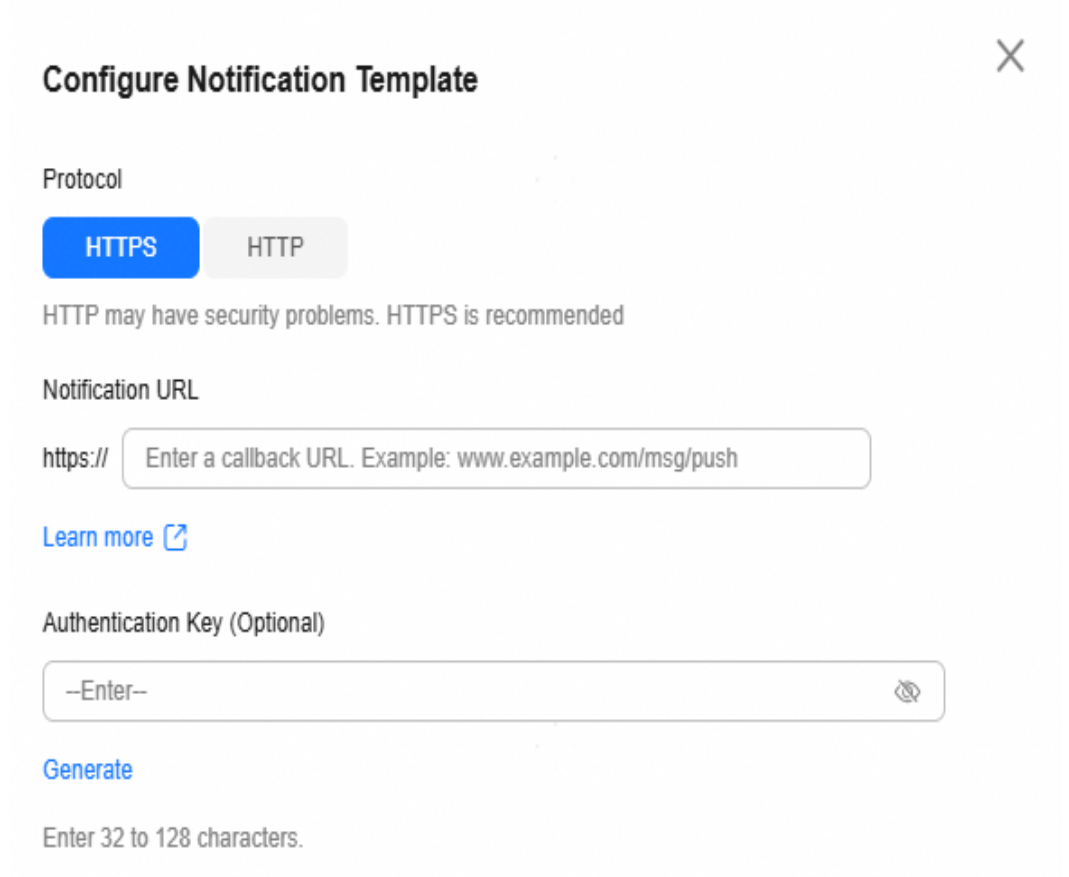
**Step 3** Click **Manage** in the **Operation** column of the desired ingest domain name.

**Step 4** In the navigation pane, choose **Template > Stream Status Notifications**.

**Step 5** Click **Add**. In the **Configure Notification Template** dialog box displayed on the right, add the URL for receiving stream start and stop notifications, as shown in [Figure 3-27](#).

[Table 3-14](#) describes the parameters.

**Figure 3-27** Adding a notification URL



**Table 3-14** Parameters

Parameter	Description
Protocol	A notification URL supports HTTP and HTTPS. HTTPS is more secure than HTTP and is recommended.
Notification URL	Only HTTP and HTTPS URLs are supported.
Authentication Key (Optional)	Authentication key. You need to configure this parameter only when notification authentication is required. <ul style="list-style-type: none"> <li>• A key contains 32 to 128 characters.</li> <li>• A key can also be automatically generated.</li> </ul>

**Step 6** Click **OK**.

When stream push starts or ends, you will receive a notification message. For details about the notification message body, see [Callback Example](#).

----End

## Managing Notification URLs

You can also perform the following operations:

- Editing a notification URL  
Click **Edit** in the **Operation** column to edit the URL or authentication key for receiving stream push messages.
- Deleting a notification URL  
Click **Delete** in the **Operation** column to delete the URL or authentication key for receiving stream push messages.

## Callback Example

The following is an example of stream push and stream disconnection messages. [Table 3-15](#) describes the fields in a message body.

```
{
  "domain": "push.example.com",
  "app": "live",
  "stream": "example_stream",
  "user_args": "auth_info=yz1TG0PVN/5isfyrGrRj10gKPCWqSS2X02t6QsRrocH+mEq0gQ0g8k6KhalS84sQ+kDprFyqI0yajbYiFmUO8e45B7ryaS+MpJBlykhwnuFLnRiKK/IXG7.33436b625354564f6e4d4d434f55&cdn=hw",
  "client_ip": "100.111.*.*",
  "node_ip": "112.11.*.*",
  "publish_timestamp": "1587954134",
  "event": "PUBLISH",
  "auth_timestamp": "1587954140",
  "auth_sign": "ff3b2bxxx5cfd56e76d72bed4c4aa2dxxxca8c2e46467d205a6417d4fc"
}
```

**Table 3-15** Message body

Field	Description
domain	Ingest domain name
app	Application name
stream	Stream name
user_args	Stream push parameter
client_ip	IP address of the stream push device
node_ip	IP address of the receiver
publish_timestamp	Unix timestamp. One single timestamp is generated for each stream push event.
event	Stream push or stream disconnection Options: <ul style="list-style-type: none"> <li>• <b>PUBLISH</b>: Stream push starts.</li> <li>• <b>PUBLISH_DONE</b>: Stream push ends.</li> </ul>

Field	Description
auth_timestamp	<p>UNIX timestamp when the event notification signature expires. This parameter is carried when an authentication key is configured.</p> <p>The value is a decimal Unix timestamp, that is, the number of seconds that have elapsed since January 1, 1970 00:00:00 UTC/GMT.</p> <p>Example: <b>1592639100</b> (June 20, 2020 15:45)</p>
auth_sign	<p>Event notification signature. This parameter is carried when an authentication key is configured.</p> <p><math>auth\_sign = \text{HmacSHA256}(\text{event} + \text{domain} + \text{app} + \text{stream} + \text{auth\_timestamp}, \text{key})</math></p> <p><i>key</i> indicates the key used for authentication.</p>

### 3.2.8 HLS Configuration

For an ingest domain name, parameters of an HLS livestream, such as **TS Segment Length**, **Segments in Each M3U8 File**, and **Segments in First M3U8 File**, can be modified.

#### Prerequisites

- You have [added an ingest domain name](#).
- You have [configured CNAME records](#) at your domain names' DNS provider.

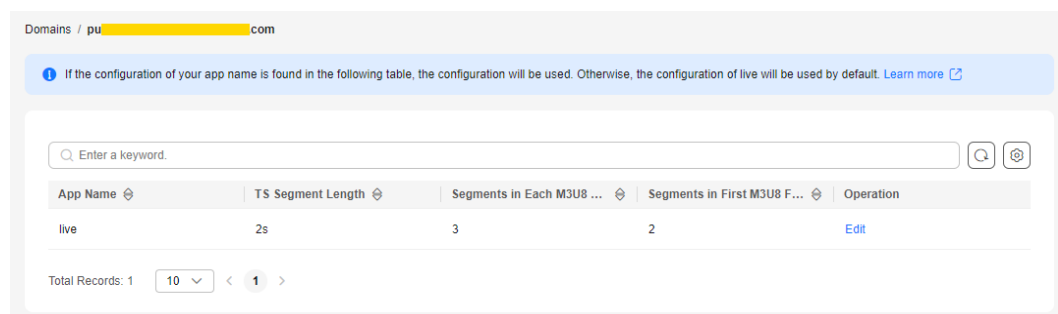
#### Procedure

- 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 ingest domain name.
- Step 4** In the navigation pane, choose **Templates > HLS**.

On the page displayed, you can see the configuration of **live**, as shown in [Figure 3-28](#).

If you have other applications, they are not displayed by default. You need to [submit a service ticket](#) to display them on the current page.

**Figure 3-28** HLS configuration



**Step 5** Click **Edit** in the **Operation** column. On the page displayed on the right, modify the HLS configuration, as shown in **Figure 3-29**.

**Figure 3-29** HLS configuration

**Table 3-16** describes the parameters.

**Table 3-16** HLS configuration

Parameter	Description
App Name	App name of the ingest domain name, which cannot be changed. If the ingest domain name contains applications other than <b>live</b> but no service ticket is submitted to display them, the configuration of <b>live</b> will apply to these applications.
TS Segment Length	TS segment length for the HLS. The value must be a multiple of the GOP duration. The value ranges from <b>1</b> to <b>10</b> , in seconds. A value that is too small may cause frame freezing. The recommended value is <b>4</b> . Default value: <b>2</b>
Segments in Each M3U8 File	Number of segments in an M3U8 file. The value ranges from <b>3</b> (recommended) to <b>10</b> . Default value: <b>3</b>

Parameter	Description
Segments in First M3U8 File	Number of segments in the first M3U8 file. The value cannot exceed the number of segments in each M3U8 file. The value ranges from <b>2</b> to <b>10</b> . Default value: <b>2</b>

**Step 6** Click **OK**.

----End

## 3.2.9 Stream Push Authentication

Live provides multiple authentication methods for stream push, including referer validation, URL validation, and IP address access control lists (ACLs), to prevent livestream resources from being stolen. 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 [ACL](#).

## 3.3 Configuring Streaming Domain Names

### 3.3.1 Assembling a Streaming URL

After domain names are configured, you can assemble a streaming URL and play the video through the URL. You can also use the [tool](#) to quickly generate a signed URL of the streaming domain name.

#### Prerequisites

- The ingest domain name and streaming domain name have been [added](#) and [associated](#).
- You have [configured CNAME records](#) at your domain names' DNS provider.
- To prevent unauthorized access to livestreams, Huawei Cloud Live provides URL validation to encrypt and authenticate the streaming URL. If necessary, configure URL validation and play the video through the signed URL. For details about how to configure URL validation, see [URL Validation](#).
- You can transcode livestreams into multiple video renditions at different resolutions and bitrates to meet a broad range of requirements. If necessary, [configure a transcoding template](#), and then use the transcoded streaming URL to play live video.

#### Procedure

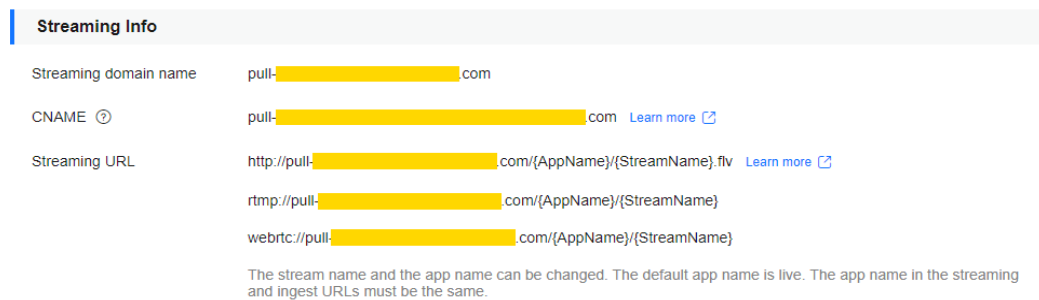
**Step 1** Log in to the [Live console](#).

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

- Step 3** Click **Manage** in the **Operation** column of the desired streaming domain name. On the displayed page, you can view streaming information.

Streaming URLs are provided based on the protocols supported by the streaming domain name, as shown in **Figure 3-30**. If a streaming domain name supports FLV, RTMP, and RTC, the corresponding streaming URLs are generated.

**Figure 3-30** Viewing the streaming URLs



- You need to customize *StreamName* to generate a streaming URL. For details, see **Original Streaming URL**.
- If URL validation is configured, you need to generate a signed streaming URL by referring to **URL Validation**.
- To generate a signed streaming URL for the transcoded stream, you need to add *\_transcoding template ID* to the end of *StreamName* in the original streaming URL to generate a new *StreamName*, generate new authentication parameters by referring to **URL Validation**, and assemble the streaming URL of the transcoded stream.

----End

## Original Streaming URL

### Assembling rules

- **Cloud Stream Live**

You can play FLV, M3U8, and RTMP streams.

RTMP format: **rtmp://Streaming domain name/AppName/StreamName**

FLV format: **http://Streaming domain name/AppName/StreamName.flv**

M3U8 format: **http://Streaming domain name/AppName/StreamName.m3u8**

- **LLL**

You can only play WebRTC streams.

**webrtc://Streaming domain name/AppName/StreamName**

Parameters in the example:

- *Streaming domain name* is the one you added on the Live console.
- *AppName*: application name. The default value is **live**. You can customize the application name. Only letters, digits, underscores (`_`), and hyphens (`-`) are allowed.
- *StreamName*: livestream name. Multiple livestreams can be created for each application. You can customize the stream name.

A stream name can contain 1 to 512 characters. The recommended length is 12 to 256 characters. Only digits, letters, hyphens (-), underscores (\_), asterisks (\*), and slashes (/) are allowed. Digits and letters are recommended. If you set the stream name to an asterisk (\*), all livestreams of the application will share one streaming URL.

### Examples

- **Cloud Stream Live**

If the added streaming domain name is **test-play.example.com**, **AppName** is **livetest**, and **StreamName** is **huawei1**, the assembled streaming URL is:

```
RTMP format: rtmp://test-play.example.com/livetest/huawei1
FLV format: http://test-play.example.com/livetest/huawei1.flv
M3U8 format: http://test-play.example.com/livetest/huawei1.m3u8
```

- **LLL**

If the added *streaming domain name* is **test-play.example.com**, *AppName* is **livetest**, and *StreamName* is **huawei1**, the assembled streaming URL is:

```
webrtc://test-play.example.com/livetest/huawei1
```

## Signed Streaming URL

If URL validation is enabled, you must generate a signed streaming URL based on obtained authentication information and stream your content through the signed URL. For details, see [URL Validation](#).

## Transcoded Streaming URL

If you have configured [transcoding](#), you must assemble a transcoded streaming URL. The URL needs to be set differently when URL validation is enabled or disabled.

### Assembling rules

Add *\_Transcoding template ID* to the end of the **StreamName** field in the [original streaming URL](#) and [signed streaming URL](#).

- **Cloud Stream Live**

```
RTMP format: rtmp://Streaming domain name/AppName/StreamName_Transcoding template ID
FLV format: http://Streaming domain name/AppName/StreamName_Transcoding template ID.flv
M3U8 format: http://Streaming domain name/AppName/StreamName_Transcoding template ID.m3u8
```

- **LLL**

```
webrtc://Streaming domain name/AppName/StreamName_Transcoding template ID
```

*Transcoding template ID*: ID of the template used for livestream transcoding. The ID of a custom transcoding template can be customized. To obtain a transcoding template ID, access the [Live console](#) and switch to the **Domains** page, locate the desired ingest domain name, and click **Manage** in the **Operation** column. On the displayed page, choose **Templates > Transcoding**.

### Examples

If the original streaming URL is **http://test-play.example.com/livetest/huawei1.flv** and transcoding template ID is 110:

- The transcoded streaming URL is as follows when URL validation is disabled:
  - **Cloud Stream Live**

```
http://test-play.example.com/livetest/huawei1_110.flv
```

– **LLL**

```
webrtc://test-play.example.com/livetest/huawei1_110
```

- The transcoded streaming URL is as follows when URL validation is enabled:

– **Cloud Stream Live**

```
http://test-play.example.com/livetest/huawei1_110.flv?  
auth_info=z6uwSWUceM2%2FZeDpc2LqjHEFhXpjQ5IQJhrLoIARQ2%2Bn  
%2BJV4DrzGRqXxWxMLQBU.44393135353831414132454633374139
```

– **LLL**

```
webrtc://test-play.example.com/livetest/huawei1_110?  
auth_info=z6uwSWUceM2%2FZeDpc2LqjHEFhXpjQ5IQJhrLoIARQ2%2Bn  
%2BJV4DrzGRqXxWxMLQBU.44393135353831414132454633374139
```

For details about how to generate authentication information, see [Signed Streaming URL](#).

## 3.3.2 Configuring Stream Delay

You can configure a proper stream delay on the console. Low delay may cause frame freezing.

### Notes

- You can configure a delay for RTMP and HTTP-FLV streams of the **live** app on the console. To configure a stream delay for other apps, [submit a service ticket](#).
- The GOP of the streaming end cannot be greater than the configured delay. The actual delay is influenced by factors including the player's network conditions.
- After the stream delay is modified, you need to push the stream again for the modification to take effect.
- If the stream delay is set to 2s, the playback experience of HLS videos will be affected. For example, the playback will start in seconds. To avoid poor user experience, set a longer stream delay (4s or 6s).
- This function is not recommended for LLL.

### Prerequisites

- The ingest domain name and streaming domain name have been [added](#) and [associated](#).
- You have [configured CNAME records](#) at your domain names' DNS provider.

### Procedure

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

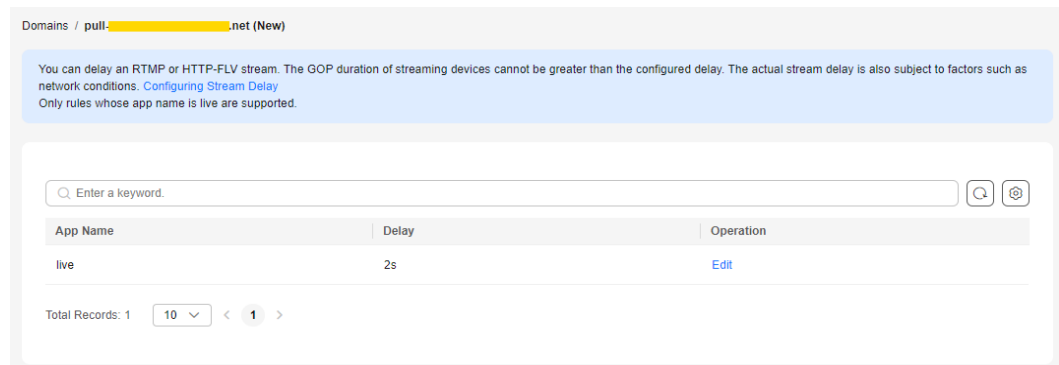
**Step 2** In the navigation pane, choose **Domains**.

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

**Step 4** In the navigation pane, choose **Templates > Stream Delay**.

**Step 5** Click **Edit** in the **Operation** column.

**Figure 3-31** Modifying the stream delay



**Step 6** On the page displayed, set **Delay**, as shown in [Figure 3-32](#).

The default delay is 2s. You can change it to 4s or 6s. The GOP duration affects the livestream delay, as shown in [Table 3-17](#).

Note: The actual livestream delay is also influenced by factors including the player's network conditions.

**Figure 3-32** Modifying the delay



**Table 3-17** Livestream delay

Delay	GOP Duration (1s)	GOP Duration (2s)	GOP Duration (4s)
Estimated delay when <b>Delay</b> is set to <b>2s</b>	2-3s	2-4s	2-6s
Estimated delay when <b>Delay</b> is set to <b>4s</b>	4-5s	4-6s	4-8s
Estimated delay when <b>Delay</b> is set to <b>6s</b>	6-7s	6-8s	6-10s

**Step 7** Click **OK**.

----End

### 3.3.3 Configuring Origin Pull

By default, a streaming domain name created on Huawei Cloud Live pulls live content from Huawei origin servers. If you want to play live content of non-Huawei origin servers through Huawei Cloud, you can configure an origin address on the Live console so that you can pull live content from your own origin server to a Huawei origin server for accelerated delivery.

#### Notes

- If you set **Origin Server** to **My origin server (domain name)** or **My origin server (IP address)** for a streaming domain name, livestreams of the ingest domain name associated with this streaming domain name cannot be played, and functions such as transcoding cannot be used.
- The default origin port number is 80 for HTTP and 1935 for RTMP.
- For LLL, ensure that there is no B-frame for origin pull.
- Origin pull settings only support RTMP and FLV domain names.

#### Prerequisites

- If **Origin Server** is set to **Huawei origin server**, ensure that you have **added an ingest domain name and a streaming domain name, associated the domain names**, and **configured CNAME records** at your domain names' DNS provider.
- If **Origin Server** is set to **My origin server (domain name)** or **My origin server (IP address)**, ensure that you have **added a streaming domain name** and **configured a CNAME record** at your domain names' DNS provider.

#### Procedure

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

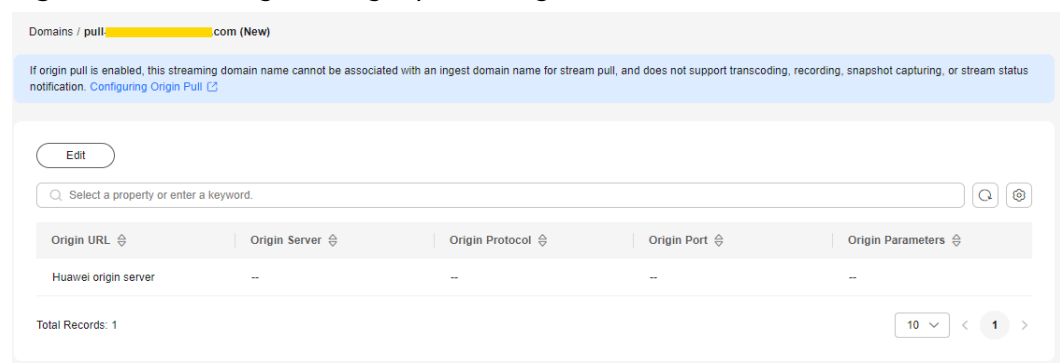
**Step 2** In the navigation pane, choose **Domains**.

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

**Step 4** In the navigation pane, choose **Templates > Origin Pull**.

**Step 5** View the origin pull configuration.

**Figure 3-33** Viewing the origin pull configuration



**Step 6** Click **Edit** to modify the origin pull configuration.

**Figure 3-34** Configuring origin pull

**Modify** ✕

**⚠** Modifying the origin pull configuration may cause livestream exceptions. Exercise caution when performing this operation.

**ℹ** If the existing origin pull methods are not suitable, [submit a service ticket](#).

Origin Server ?  
My origin server (domain... ▼

Origin Protocol ?  
 RTMP  HTTP-FLV

Origin Domain ?  
Enter a value. Delete

+ Add

Origin Port (Optional) ?  
1935

Origin Parameters (Optional)  
Key = Value Delete

+ Add

Cancel OK

**Table 3-18** describes the parameters.

**Table 3-18** Origin pull parameters

Parameter	Description
Origin Server	<p>There are three options:</p> <ul style="list-style-type: none"> <li>• <b>Huawei origin server</b>: pulls livestreams from the Huawei origin server by default</li> <li>• <b>My origin server (domain name)</b>: pulls livestreams from your own origin server. You can configure multiple origin domains.</li> <li>• <b>My origin server (IP address)</b>: pulls livestreams from your own origin server. You can configure multiple origin IP addresses and one origin domain.</li> </ul>
Origin Protocol	<p>Protocol used by Live to pull streams from the origin server. This parameter is used only when <b>Origin Server</b> is not <b>Huawei origin server</b>. Only RTMP and HTTP-FLV are supported.</p>
Origin IP Address	<p>You can configure a maximum of 10 IP addresses. If an origin pull fails, the system polls origin IP addresses in the configured sequence.</p> <p>This parameter is mandatory when <b>Origin Server</b> is set to <b>My origin server (IP address)</b>.</p>
Origin Domain (Optional)	<p>Currently, the value can only be a pure domain name, for example, www.example.com.</p> <ul style="list-style-type: none"> <li>• This parameter is mandatory when <b>Origin Server</b> is set to <b>My origin server (domain name)</b>. A maximum of 10 origin domains can be configured. If multiple origin domains are configured, the system polls the domains in the configured sequence when an origin pull fails.</li> <li>• This parameter is optional when <b>Origin Server</b> is set to <b>My origin server (IP address)</b>. A maximum of one origin domain can be configured. If an origin domain is configured, both the <b>HTTP-FLV HOST</b> header and the <b>RTMP tcurl</b> field are set to the origin domain. If there is no origin domain, <b>HOST</b> is set to the current IP address.</li> </ul>
Origin Port (Optional)	<p>Customizable.</p> <p>Default values:</p> <ul style="list-style-type: none"> <li>• If <b>Origin Protocol</b> is set to <b>HTTP-FLV</b>, the default value is <b>80</b>.</li> <li>• If <b>Origin Protocol</b> is set to <b>RTMP</b>, the default value is <b>1935</b>.</li> </ul>

Parameter	Description
Origin Parameters (Optional)	<p>(Optional) When <b>Origin Server</b> is set to <b>My origin server (IP address)</b> or <b>My origin server (domain name)</b>, you can specify the additional parameters carried in the origin URL.</p> <p>Each <b>key</b> corresponds to one <b>value</b>. You can add multiple pairs. During origin pull, origin parameters are separated using <b>&amp;</b>.</p> <p>Example: key1=value1&amp;key2=value2</p>

**Step 7** Click **OK**.

**Step 8** **Assemble a streaming URL** for playback.

----End

## 3.3.4 HTTPS Certificates

### 3.3.4.1 Configuration Method

You can enable HTTPS secure acceleration to protect your live resources.

#### Context

**Force HTTPS:** If a user initiates an HTTP request, the server returns a 302 status code and the request is forcibly 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 to ensure data integrity.
- Key user information is encrypted to prevent session IDs or cookies from being captured by attackers.

#### Prerequisites

- The ingest domain name and streaming domain name have been **added** and **associated**.
- You have **configured CNAME records** at your domain names' DNS provider.
- An HTTPS certificate is available. If not, 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.

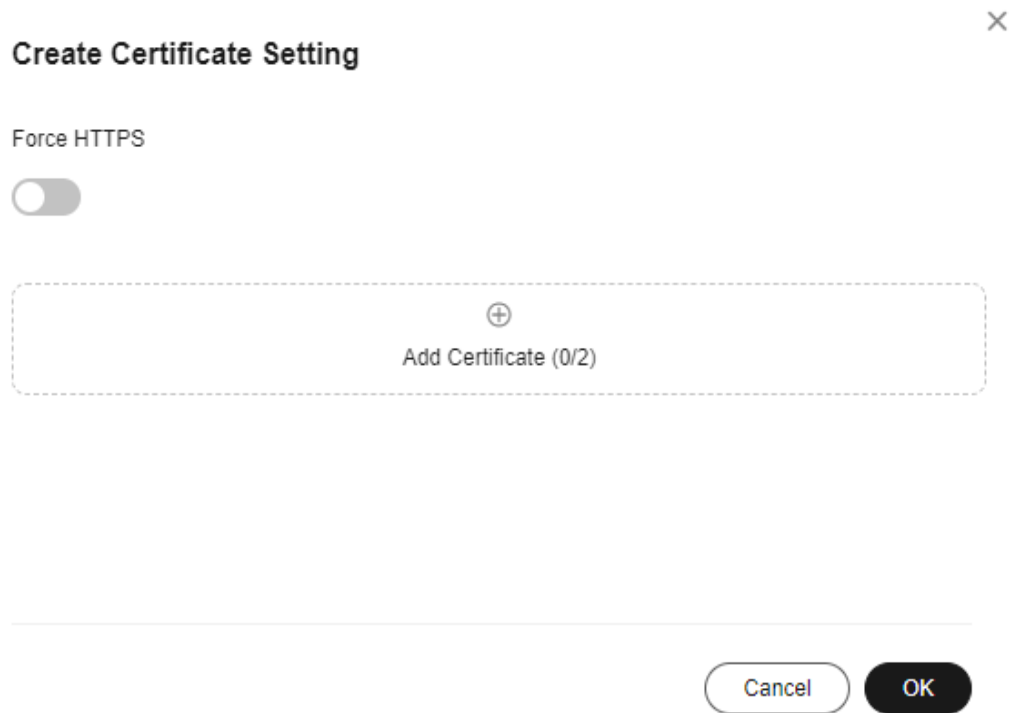
#### Enabling HTTPS

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

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

- Step 3** Click **Manage** in the **Operation** column of the desired streaming domain name.
- Step 4** In the navigation pane, choose **Templates > HTTPS Certificates**.
- Step 5** Click **Create**. The page for creating certificate settings is displayed, as shown in [Figure 3-35](#).

**Figure 3-35** Creating certificate settings



- Step 6** Click **Add Certificate**. The settings of certificate 1 are displayed, as shown in [Figure 3-36](#).

[Table 3-19](#) describes the parameters. 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 3-36 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 3-19** Parameters

Parameter	Description
Certificate Standard	Standard of the HTTPS certificate. Options: - <b>International</b> - <b>Chinese (SM)</b>
Certificate Source	Source of the HTTPS certificate. Options: - <b>My certificate</b> : a certificate obtained from a compliant channel - <b>SCM certificate</b> : a certificate purchased from Huawei Cloud SCM
<b>International &gt; My certificate</b>	<p>Open the obtained certificate file and private key file using a text tool, and copy the certificate body and private key content to the text boxes.</p> <p>Certificates issued by different organizations have the following differences:</p> <ul style="list-style-type: none"> <li>- If your certificate is issued by a root CA, the certificate is a complete one. Copy the certificate body.</li> </ul> <p><b>Figure 3-37</b> HTTPS certificate</p>  <p>- If your <b>certificate is issued by an intermediate CA</b>, the certificate file contains multiple certificates. You need to combine all the certificates into a single certificate.</p>
<b>Chinese (SM) &gt; My certificate</b>	
<b>International &gt; SCM certificate</b>	Click <b>Create SCM Certificate</b> on the right of <b>Certificate Name</b> to go to the SCM console and purchase a certificate as prompted.
<b>Chinese (SM) &gt; SCM certificate</b>	After the certificate is issued, it will be automatically displayed in the <b>Certificate Name</b> drop-down list box.

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

If this option is enabled, all requests for your website are converted 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 live video. If the playback is successful, HTTPS secure acceleration has taken effect.

----End

## Updating a Certificate

If your certificate has been changed, you need to synchronize the new certificate body to the HTTPS settings. The procedure for updating a certificate is the same as that for [enabling HTTPS](#).

If the certificate is your own one, the content in the **Private Key** text box is empty by default to ensure the security and confidentiality of the private key. You need to enter and submit the content again.

### 3.3.4.2 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 3-38](#).

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 3-39 A combined certificate

```
-----BEGIN CERTIFICATE-----
MIIE/DCCA+SgAwIBAgIUOWwvEj41j5OamNabjVbGY42BBcQwDQYJKoZIhvcNAQEL
BQAwYIxCzAJBgNVBAYTAmNuMRIwEAYDVQQIDAlHdWZ3ZWRkbmVzZmVzZmVzZmVz
CFNoZW56aGVuMjEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEw
DCVIdWF3ZWkgV2ViIFN1Y3VyZSBjb2R1cm5ldCBHYXR1d2F5IENBMB4XDTE3MTAx
ODAwNDA0N1oXDTE4MTAxODAwNDA0N1owZzoxcm5ldCBHYXR1d2F5IENBMB4XDTE3
DAdqaWZ3ZWkgV2ViIFN1Y3VyZSBjb2R1cm5ldCBHYXR1d2F5IENBMB4XDTE3
dHdhcmUgVGVjaG5vbG9naWVzIENvLiVzZSBjb2R1cm5ldCBHYXR1d2F5IENB
RSBEZXB0MRwwGgYDVQDDBN3d3cuaHVhd2VpY2xvdWQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA3f5hC6J20XSF/Y7Wb8o6l30yzgaUYWGLEX8t
ldQ1JAus93xMC2Jr6UOXmXR6WaRu5lZxpPFLT/IV6UnvMLnxJQBavqauykCskadW
stYA9ttTI/FYq+MR1XKbNrqK/ADhrfmR4owS/3w1wxdpwy5TRZ+V/D6TjxHZCjc
+8lSmUuLxsgoUe79B/ruccY1ufuqr3v0TToaNN4c37kwjJeKf+b2F/IqO/KF+9zF
AgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMEIGA1UdEQQ7MDmCE3d3dy5odWF3ZW1j
bG91ZC5jb22CESouaHVhd2VpY2xvdWQuY29tgg9odWF3ZW1jbG91ZC5jb20wDQYJ
KoZIhvcNAQELBQADggEBACsLP7Hj+4KY1ES38OnOWuwQ3st8axvhDD9jZGoninzW
JSGpdm04NEshlvSfDEHpy/xKSLCIgg5Ue8tTI8zOF13U0ROnMeHKSXsJG6zc8X
h/3N217oBygPgvpmc6YX66kvwXmbA7KRniYS0nmCi2KUyng5Bv4dsx21djlqQ3b
HI+i026Q9odLsmhsKOsfUC0vDKoMIJz0Socy7Cq1+tFWF9S79MI4QjxaXVEvpIEg
QLEze3BXSsoiWRkdfsDB9s+UtdWeJy0HMh/otwUQQtB6areV2+CPthfmDENA+A8
IK6GzHyp/mgrwKdDh97aQ42ARreAv4KVFAiJGZ02LOY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID2CCAsGgAwIBAgIJALQPO9XxFFZmMA0GCSqGSIb3DQEBCwUAMIGCMQswCQYD
VQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25nMREwDwYDVQQHDAhTaGVuemh1bjEP
MA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDLDAJVVDEuMwYDVQsGA1UEAww1SHVhd2Vp
YiBTZWN1cmUgSW50ZXJ1ZXQgR2F0ZXdhcSBDb2R1cm5ldCBHYXR1d2F5IENBMB4X
DTE3MTAxODAwNDA0N1oXDTE4MTAxODAwNDA0N1owZzoxcm5ldCBHYXR1d2F5IENB
NjA1MDgwOTAyMjdaMIGCMQswCQYDVQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25n
MREwDwYDVQQHDAhTaGVuemh1bjEPMA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDLDAJ
VDEuMwYDVQsGA1UEAww1SHVhd2VpYiBTZWN1cmUgSW50ZXJ1ZXQgR2F0ZXdhcSBDb
rG0CAwEAAaNQME4wHQYDVRO0BBYEFDB6DZX4Am+isCoa48e4ZdrAXpsMB8GA1Ud
IwQYMBaAFDB6DZX4Am+isCoa48e4ZdrAXpsMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAKN9ksjRX56yw2Ku5Mm3gzU/kQQw+mLkIuJEeDwS6LWjW0Hv
3l3xlv/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 3-40](#).

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 3-40** An RSA private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909eY1vLCqow
wEPqs6vyqQM3gKo8qCkNkmS5QgMPOFI4fx2G22mHvT0x8PHjm6GTQDPDniWaIuky
luFqVpD/zqK0oBl2AeAvbzKxWwRqf4JTLA3136B415y2VoDjRfU5EKY6LW1sD/00
5uF0qE3td5KQwQc6ZzbnkAof0Oyp5PbMfajM9My2mcvQJzWPLRxET3eWHYdBUtEg
1rxdrWxLheKjENzW3P7Mz/7KycIRxAlur1/Z9s8ytj3124AQY7NE1t1iL9wwA47k
0EumxTaLz8H/vHB1fLMouvYfsSDEr3Snf6eSSwIDAQABAoIBAQCDCNmxC3qHXPgvI
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
```

## 3.3.5 Playback Authentication

### 3.3.5.1 Overview

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

URL validation protects live resources from unauthorized download and theft. Referer validation uses referer blacklists/whitelists to prevent hotlinking. However, because the referer content can be forged, referer validation cannot well protect live resources. Therefore, you are advised to use URL validation. [Table 3-20](#) shows the authentication mechanism of the Live service.

**Table 3-20** Authentication mechanism

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

### 3.3.5.2 Referrer 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.
- Whitelists and blacklists 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 add `^http://test.*com$` to a blacklist or whitelist, `http://test.example.com` and `http://test.example01.com` are matched.

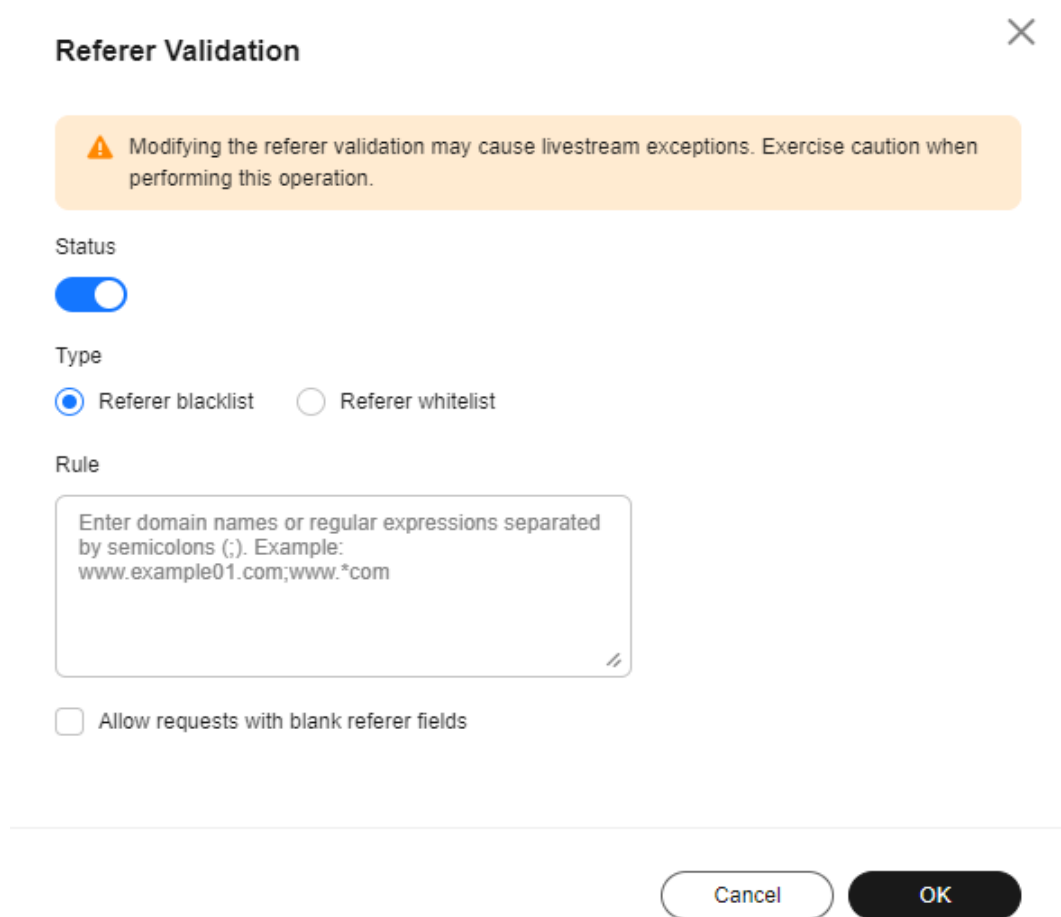
#### Prerequisites

- The ingest domain name and streaming domain name have been **added** and **associated**.
- You have **configured CNAME records** at your domain names' DNS provider.

#### 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 the edit icon on the right of **Referer Validation**. The **Referer Validation** dialog box is displayed on the right.
- Step 6** Toggle on the switch and configure related parameters.

**Figure 3-41** Configuring referer validation



**Table 3-21** describes the parameters.

**Table 3-21** Referer validation parameters

Parameter	Description
Type	<p>Blacklists and whitelists are supported.</p> <ul style="list-style-type: none"> <li>• <b>Referer blacklist</b> allows requests from all domains except those in the blacklist.</li> <li>• <b>Referer whitelist</b> denies requests from all domains except those in the whitelist.</li> </ul> <p>You can control whether to allow requests with an empty referer field, that is, whether to allow access through the browser address bar.</p>
Rule	<p>Domain name in the blacklist or whitelist.</p> <ul style="list-style-type: none"> <li>• You can input 1 to 100 domain names. Use semicolons (;) to separate domain names.</li> <li>• 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 matched.</li> </ul>

**Step 7** Click **OK**.

----**End**

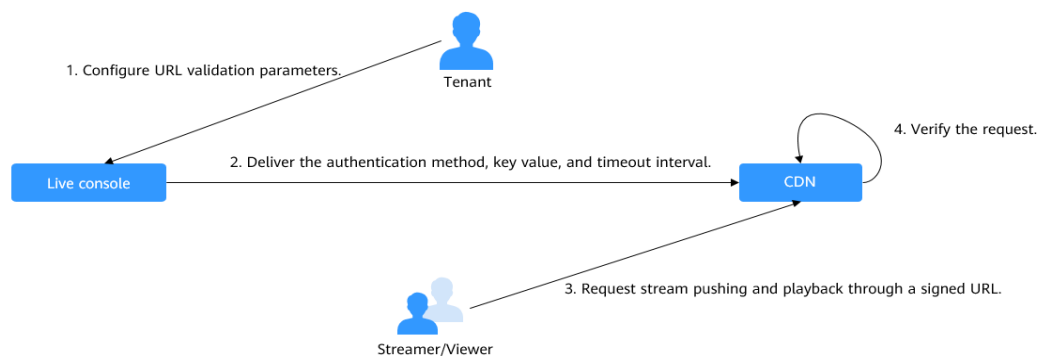
### 3.3.5.3 URL Validation

To prevent live resources from being stolen, you can configure URL validation to add authentication information to the end of the original ingest or streaming URL. When a 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 3-42** URL validation working principles



The process is as follows:

1. A tenant enables URL validation on the Live console and configures the authentication method, key, and timeout interval.
2. The Live service delivers the configured authentication method, key value, and timeout interval to CDN PoPs.
3. A streamer or viewer requests CDN to push or play streams through a signed ingest or streaming URL.
4. CDN verifies the request based on authentication information carried in the URL. Only verified requests can be handled.

## Notes

- This function is optional and is disabled by default. After this function is enabled, the original URLs cannot be used. New signed URLs must be generated based on rules.
- Use different keys for stream push authentication and playback authentication to enhance security. If a signed URL expires or the signature fails to be authenticated, the livestream fails to be played and the message "403 Forbidden" is returned.

- For persistent connection services such as RTMP and FLV, the server verifies the validation parameters only when receiving a user request. Once verified, the content can be played continuously.
- For HLS services, users keep sending requests that contain the same validation parameters after content is played. Once the validation parameters expire, the server rejects the access request because the verification fails, which will interrupt the playback.

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

## Prerequisites

- The ingest domain name and streaming domain name have been **added** and **associated**.
- You have **configured CNAME records** at your domain names' DNS provider.

## Enabling URL Validation

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

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

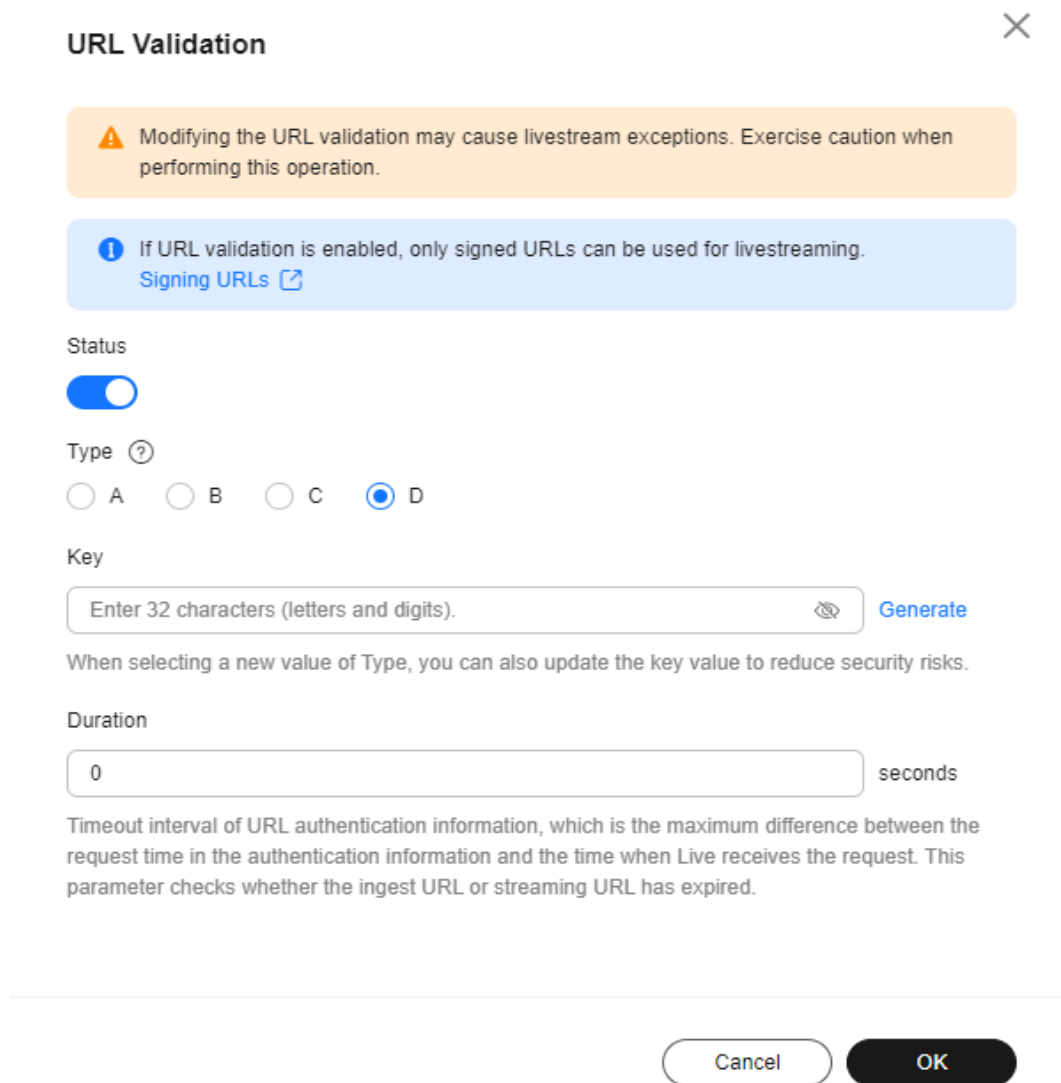
**Step 3** Click **Manage** in the **Operation** column of the desired domain name.

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

**Step 5** Click the edit icon on the right of **URL Validation**. The **URL Validation** dialog box is displayed on the right.

**Step 6** Toggle on the switch and configure related parameters.

**Figure 3-43** Configuring URL validation



**Table 3-22** URL validation parameters

Parameter	Description
Method	<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 <a href="#">Signing Method A</a> and <a href="#">Signing Method B</a>.</p> <p>Signing method C: A symmetric encryption algorithm is used. For details, see <a href="#">Signing Method C</a>.</p> <p>Signing method D: The HMAC-SHA256 algorithm is used. For details, see <a href="#">Signing Method D</a>.</p> <p><b>NOTE</b> Signing methods A, B, and C have security risks. Signing method D is more secure and recommended.</p>

Parameter	Description
Key	<p>Authentication key.</p> <ul style="list-style-type: none"> <li>You can customize a key. A key consists of 32 characters. Only letters and digits are allowed.</li> <li>A key can also be automatically generated.</li> </ul>
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><b>NOTE</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>For HLS services, users keep sending requests that contain the same validation parameters after content is played. Once the validation parameters expire, the server rejects the access request because the verification fails, which will interrupt the playback. For such services, you need to set a proper authentication expiration time to prevent playback failures. For example, if the estimated HLS playback lasts less than 1 hour each time, you can set the expiration time to 3600 seconds.</li> </ul>

**Step 7** Click **OK**.

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

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

**Step 9** Verify whether URL validation has taken effect.

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

----End

## Signing Method A

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

Signed URL format:

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

Formula for calculating **md5hash** is:

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

**Table 3-23** 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: <b>1592639100</b> (June 20, 2020 15:45)
Duration	How long a signed URL remains effective. If the validity period is set to 1800s, users can access the streaming URL within 1800s since the time indicated by <b>timestamp</b> . Authentication fails and the URL is inaccessible if users access the streaming URL 1800s later. For example, if the access time is 00:00:00 (GMT +08:00) on June 30, 2020, the URL expires at 00:30:00 (GMT+08:00) on June 30, 2020.
rand	Random number. The recommended value is a UUID, which cannot contain hyphens (-). Example: 477b3bbc253f467b8def6711128c7bec
uid	User ID. This parameter is not used now. Set it to <b>0</b> .
md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of digits (0 to 9) and lowercase letters. sstring = "{URI}-{Timestamp}-{rand}-{uid}-{Key}" HashValue = md5sum(sstring)
URI	Path from the domain name to the end in the original URL <ul style="list-style-type: none"> <li>• <b>Cloud Stream Live</b> Example: /livetest/huawei1.flv</li> <li>• <b>LLL</b> Example: /livetest/huawei1.sdp</li> </ul>
Key	Key value set on the console. For details, see <a href="#">URL Validation</a>

Signed URL example:

- **Cloud Stream Live**

Generating a signed streaming URL is used as an example.

```
Original URL: http://test-play.example.com/livetest/huawei1.flv
timestamp: 1592639100
Validity period: 1800s
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
rand: 477b3bbc253f467b8def6711128c7bec
uid: 0
URI: /livetest/huawei1.flv
```

Obtain **md5hash** using the calculation formula.

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

The signed streaming URL is:

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

- **LLL**

Generating a signed streaming URL is used as an example.

```
Original URL: webrtc://test-play.example.com/livetest/huawei1
timestamp: 1592639100
Validity period: 1800s
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
rand: 477b3bbc253f467b8def6711128c7bec
uid: 0
URI: /livetest/huawei1.sdp
```

Obtain **md5hash** using the calculation formula.

```
HashValue = md5sum("/livetest/huawei1.sdp-1592639100-477b3bbc253f467b8def6711128c7bec-0-GCTbw44s6MPLh4GqgDpnfuFHgy25Enly") = 4116c2c7939307e86c6654178addc987
```

The signed streaming URL is:

```
webrtc://test-play.example.com/livetest/huawei1?
auth_key=1592639100-477b3bbc253f467b8def6711128c7bec-0-4116c2c7939307e86c6654178addc987
```

## Signing Method B

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

Signed URL format:

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

**Table 3-24** Authentication fields

Field	Description
txTime	Set <b>txTime</b> to the current time, expressed as the hexadecimal representation of the Unix timestamp. Example: 5eed5888 (that is, 2020.06.20 08:30:00)
Key	Key value set on the console. For details, see <a href="#">URL Validation</a>
txSecret	Encryption parameter in the URL. The value is obtained by using the MD5 encryption algorithm to encrypt the string consisting of <b>key</b> , <b>Stream Name</b> , and <b>txTime</b> . $txSecret = md5 (Key + Stream Name + txTime)$
Duration	How long a signed URL remains effective. If <b>txTime</b> 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:

- **Cloud Stream Live**

Generating a signed streaming URL is used as an example.

```
Original URL: http://test-play.example.com/livetest/huawei1.flv
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
Stream Name: huawei1
txTime: 5eed5888
Duration: 1249s
```

Obtain **txSecret** based on the calculation formula.  
 $txSecret = md5(GCTbw44s6MPLh4GqgDpnfuFHgy25Enlyhuawei15eed5888) = 5cdc845362c332a4ec3e09ac5d5571d6$

The signed streaming URL is:

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

- **LLL**

Generating a signed streaming URL is used as an example.

```
Original URL: webrtc://test-play.example.com/livetest/huawei1
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
Stream Name: huawei1
txTime: 5eed5888
Duration: 1249s
```

Obtain **txSecret** based on the calculation formula.  
 $txSecret = md5(GCTbw44s6MPLh4GqgDpnfuFHgy25Enlyhuawei15eed5888) = 5cdc845362c332a4ec3e09ac5d5571d6$

The signed streaming URL is:

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

## Signing Method C

A signed string is calculated based on the **Key, Timestamp, App Name, Stream Name, 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 [Code Example](#).

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

**Table 3-25** describes encryption parameters in the algorithm.

**Table 3-25** Encryption parameters

Field	Description
App Name	Application name, which is the same as the value of <b>App Name</b> in an ingest or streaming URL
Stream Name	Stream name, which is the same as the value of <b>Stream Name</b> in an ingest or streaming URL
Key	Key value set on the console. For details, see <a href="#">URL Validation</a>

Field	Description
LiveID	Livestream ID, which uniquely identifies a livestream. The value consists of <b>App Name</b> and <b>Stream Name</b> . LiveID = <App Name>+"/"+<Stream Name>
Timestamp	UTC time when an authentication parameter is generated, in <b>yyyyMMddHHmmss</b> format. This parameter is used to check whether the authentication parameter has expired, that is, whether the absolute value of the difference between <b>Timestamp</b> and the current time is greater than the configured timeout interval.
CheckLevel	Check level. The value is <b>3</b> or <b>5</b> . <ul style="list-style-type: none"> <li>• If <b>CheckLevel</b> is <b>3</b>, the system only checks whether the value of <b>LiveID</b> is matched.</li> <li>• If <b>CheckLevel</b> is <b>5</b>, the system checks whether the value of <b>LiveID</b> is matched and whether <b>Timestamp</b> times out.</li> </ul>
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:

- **Cloud Stream Live**

Generating a signed streaming URL is used as an example.

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

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

```
Encrypted string = I90KW7GhxOMwoy5yaeKMStZsOC %2B6WlyqU2kLBYAvco %3D
EncodIV = 79436d453636364e335941713330534e
```

The signed streaming URL is:

```
http://test-play.example.com/livetest/huawei1.flv?auth_info=I90KW7GhxOMwoy5yaeKMStZsOC
%2B6WlyqU2kLBYAvco%3D.79436d453636364e335941713330534e
```

- **LLL**

Generating a signed streaming URL is used as an example.

```
Original URL: webrtc://test-play.example.com/livetest/huawei1
App Name: livetest
Stream Name: huawei1
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
LiveID: livetest/huawei1
Timestamp: 20190428110000
CheckLevel: 3
IV: yCmE666N3YAq30SN
```

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

Encrypted string = I90KW7GhxOMwoy5yaeKMStZsOC %2B6WlyqU2kLBYAvco %3D  
 EncodIV = 79436d453636364e335941713330534e

The signed streaming URL is:

webrtc://test-play.example.com/livetest/huawei1?auth\_info=I90KW7GhxOMwoy5yaeKMStZsOC  
 %2B6WlyqU2kLBYAvco%3D.79436d453636364e335941713330534e

## Signing Method D

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

Signed URL format:

*Original URL?hwSecret=hmac\_sha256(Key, Stream Name + hwTime)&hwTime=hex(timestamp)*

**Table 3-26** Authentication fields

Field	Description
hwTime	Effective time of a streaming URL. The value is a hexadecimal Unix timestamp.  If the value of <b>hwTime</b> + <i>duration</i> 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 <a href="#">URL Validation</a>
hwSecret	Encryption parameter in the URL.  The value is obtained using the HMAC-SHA256 algorithm, with <i>Key</i> and <i>Stream Name</i> + <i>hwTime</i> as parameters.  <i>hwSecret</i> = <i>hmac_sha256 (Key, Stream Name + hwTime)</i>
Duration	How long a signed URL remains effective.  If <b>hwTime</b> is set to the current time and the validity period is set to 1249s, the streaming URL expiration time is the current time plus 1249s.

Signed URL example:

- **Cloud Stream Live**

Generating a signed streaming URL is used as an example.

Original URL: <http://test-play.example.com/livetest/huawei1.flv>  
 Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly  
 Stream Name: huawei1  
 hwTime: 5eed5888  
 Duration: 1249s

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

*hwSecret* = *hmac\_sha256(GCTbw44s6MPLh4GqgDpnfuFHgy25Enly, huawei15eed5888)* =  
 ce201856a0957413319e883c8ccae13602f01d3d91e21daf5161964cf708a6a8

The signed streaming URL is:

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

- **LLL**

Generating a signed streaming URL is used as an example.

```
Original URL: webrtc://test-play.example.com/livetest/huawei1
Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
Stream Name: huawei1
hwTime: 5eed5888
Duration: 1249s
```

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

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

The signed streaming URL is:

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

## Signing Method A - Code Example

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

```
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.time.Instant;
import java.util.UUID;

public class Main {
    public static void main(String[] args) {
        // Obtain the current timestamp, for example, 1592639100.
        long timestampSeconds = Instant.now().getEpochSecond();

        // The default value of UID is 0.
        int uid = 0;

        // Generate a random UUID, for example, 477b3bbc253f467b8def6711128c7bec.
        String rand = UUID.randomUUID().toString().replace("-", "");

        // The example streaming URI is used here. Replace it with the actual URI.
        String uri = "/livetest/huawei1.flv";

        // The example key is used here. Replace it with the actual key set on the console.
        String key = "GCTbw44s6MPLh4GqgDpnfuFHgy25Enly";

        String sstring = uri + '-' + timestampSeconds + '-' + rand + '-' + uid + '-' + key;

        String md5hash = md5(sstring);

        String authKey = timestampSeconds + "-" + rand + "-" + uid + "-" + md5hash;

        System.out.println("auth_key: " + authKey);
    }

    /**
     * Encrypt a string using MD5.
     * @param input The string to be encrypted.
     * @return Encrypted hexadecimal character string (32 lowercase letters)
     */
    public static String md5(String input) {
        try {
            // Obtain a MessageDigest instance for the MD5 algorithm.
            MessageDigest digest = MessageDigest.getInstance("MD5");

            // Convert the string to a byte array (using the default encoding of the platform).
            byte[] inputBytes = input.getBytes();

            // Calculate the hash value.
            byte[] hashBytes = digest.digest(inputBytes);
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

```
        // Convert the byte array into a hexadecimal string.
        StringBuilder hexString = new StringBuilder();
        for (byte b : hashBytes) {
            // Use & 0xff to ensure unsigned processing and String.format("%02x") to ensure two-digit
            hexadecimal representation.
            hexString.append(String.format("%02x", b & 0xff));
        }

        return hexString.toString();
    } catch (NoSuchAlgorithmException e) {
        e.printStackTrace();
        return null;
    }
}
```

## Signing Method B - Code Example

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

```
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.time.Instant;

//Signing method B
public class Main {
    public static void main(String[] args) {
        // Obtain the current timestamp, for example, 1592613000
        long timestampSeconds = Instant.now().getEpochSecond();

        String txTime = hexTimestamp(timestampSeconds);

        // The example stream name is used here. Replace it with the actual stream name.
        String streamName = "huawei1";

        // The example key is used here. Replace it with the actual key set on the console.
        String key = "GCTbw44s6MPLh4GqgDpnfuFHgy25Enly";

        String txSecret = md5(key + streamName + txTime);

        System.out.println("txSecret: " + txSecret);
    }

    private static String hexTimestamp(long timestampSeconds) {
        // Convert the string into a hexadecimal string (lowercase).
        String hexSeconds = Long.toHexString(timestampSeconds);

        // Output the result.
        System.out.println("Current timestamp (second): " + timestampSeconds);
        System.out.println("Hexadecimal (lowercase): " + hexSeconds);
        return hexSeconds;
    }

    /**
     * Encrypt a string using MD5.
     *
     * @param input The string to be encrypted.
     * @return Encrypted hexadecimal character string (32 lowercase letters)
     */
    public static String md5(String input) {
        try {
            //Obtain a MessageDigest instance for the MD5 algorithm.
            MessageDigest digest = MessageDigest.getInstance("MD5");

            // Convert the string to a byte array (using the default encoding of the platform).
            byte[] inputBytes = input.getBytes();
```

```
// Calculate the hash value.
byte[] hashBytes = digest.digest(inputBytes);

// Convert the byte array into a hexadecimal string.
StringBuilder hexString = new StringBuilder();
for (byte b : hashBytes) {
    // Use & 0xff to ensure unsigned processing and String.format("%02x") to ensure two-digit
hexadecimal representation.
    hexString.append(String.format("%02x", b & 0xff));
}

return hexString.toString();
} catch (NoSuchAlgorithmException e) {
    e.printStackTrace();
    return null;
}
}
```

## Signing Method C - Code Example

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();
}
}
```

## Signing Method D - Code Example

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

```
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import java.nio.charset.StandardCharsets;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.time.Instant;

//Signing method D
public class Main {
    public static void main(String[] args) {
        //Obtain the current timestamp, for example, 1592613000 (08:30:00 on June 20, 2020).
        long timestampSeconds = Instant.now().getEpochSecond();
        String hwTime = hexTimestamp(timestampSeconds);

        // The example key is used here. Replace it with the actual key set on the console.
        String key = "GCTbw44s6MPLh4GqgDpnfuFHgy25Enly";

        // The example stream name is used here. Replace it with the actual stream name.
        String streamName = "huawei1";

        String hwSecret = hmacSha256(key, streamName + hwTime);
        System.out.println("hwSecret: " + hwSecret);
    }

    private static String hexTimestamp(long timestampSeconds) {
        // Convert the string into a hexadecimal string (lowercase).
        String hexSeconds = Long.toHexString(timestampSeconds);

        // Output the result.
        System.out.println("Current timestamp (second): " + timestampSeconds);
        System.out.println("Hexadecimal (lowercase): " + hexSeconds);
        return hexSeconds;
    }

    private static String hmacSha256(String secretKey, String data) {
        System.out.println("StreamName + hwTime ." + data);
        try {
            //Obtain a Mac instance for HMAC-SHA256.
            Mac mac = Mac.getInstance("HmacSHA256");

            //Convert the key to a SecretKeySpec object.
            SecretKeySpec secretKeySpec = new SecretKeySpec(secretKey.getBytes(StandardCharsets.UTF_8),
"HmacSHA256");

            //Initialize the Mac object.
            mac.init(secretKeySpec);
            //Calculate the HMAC.

            byte[] hmacBytes = mac.doFinal(data.getBytes(StandardCharsets.UTF_8));

            return bytesToHex(hmacBytes);
        } catch (InvalidKeyException | NoSuchAlgorithmException e) {
            e.printStackTrace();
        }
    }
}
```

```
    } catch (NoSuchAlgorithmException | InvalidKeyException e) {
        e.printStackTrace();
        return null;
    }
}

private static String bytesToHex(byte[] bytes) {
    StringBuilder hexString = new StringBuilder(2 * bytes.length);
    for (byte b : bytes) {
        String hex = Integer.toHexString(0xff & b);
        hexString.append(hex.length() == 1 ? "0" + hex : hex); // Zero padding
    }
    return hexString.toString();
}
}
```

### 3.3.5.4 ACL

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

#### Notes

- This function is optional and is disabled by default.
- Whitelists and blacklists cannot be used simultaneously.
- A maximum of 1,000 IP addresses can be added to a whitelist or blacklist.

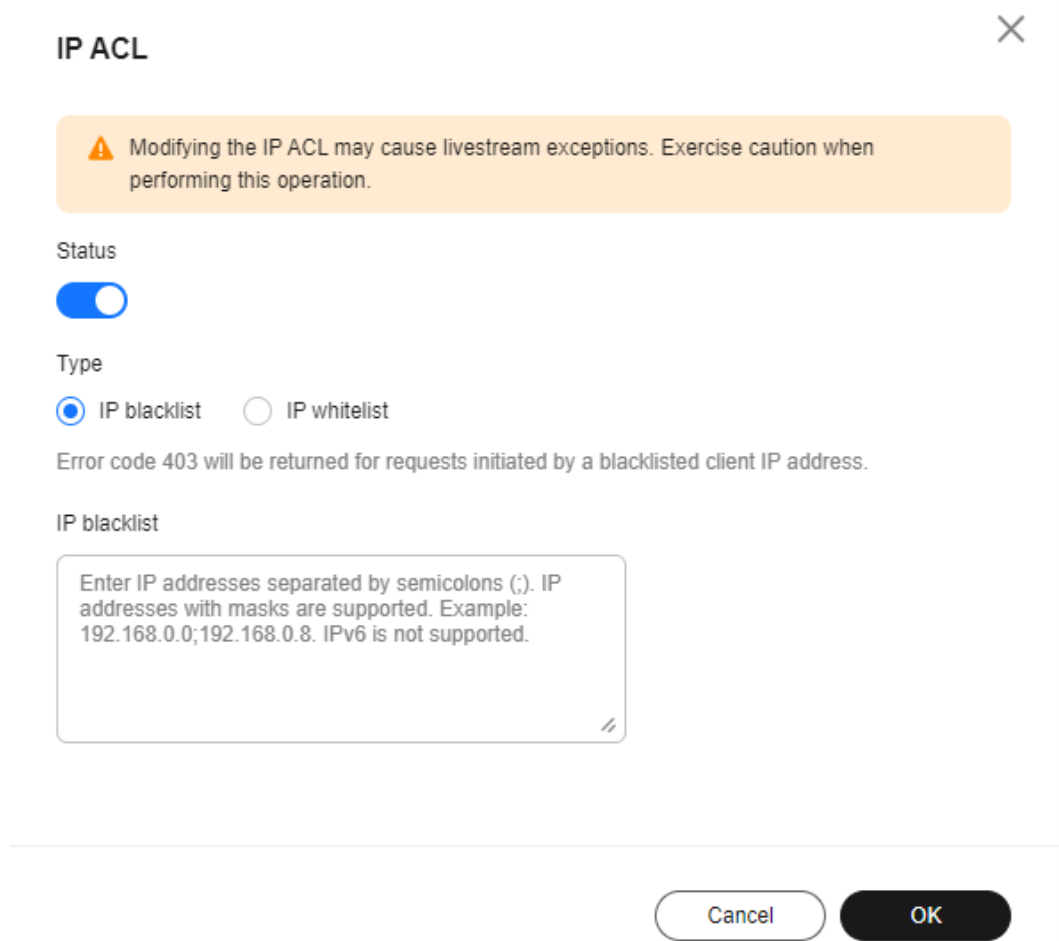
#### Prerequisites

- The ingest domain name and streaming domain name have been **added** and **associated**.
- You have **configured CNAME records** at your domain names' DNS provider.

#### 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.  
The subservice type of the domain name must be Cloud Live.
- Step 4** In the navigation pane, choose **Basic Settings > Access Control**.
- Step 5** Click the edit icon the right of **IP ACL**. The **IP ACL** dialog box is displayed on the right.
- Step 6** Toggle on the switch and configure an IP address blacklist or whitelist, as shown in **Figure 3-44**.

**Figure 3-44** Configuring an IP address ACL



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

**Step 8** Click **OK**.

----End

### 3.3.6 Configuring a Geo-blocking Whitelist

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

#### Notes

- Huawei Cloud periodically updates IPv4 databases in all areas around the world. The geo-blocking whitelist configured here may not be able to identify all IP addresses. Terminals cannot identify a small number of IP addresses that are not in the databases. If high accuracy is required, exercise caution when using this function.

- If IP addresses in the databases cannot be accurately identified, the request may be scheduled to an unexpected billing area and billed in that area. For details, see [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

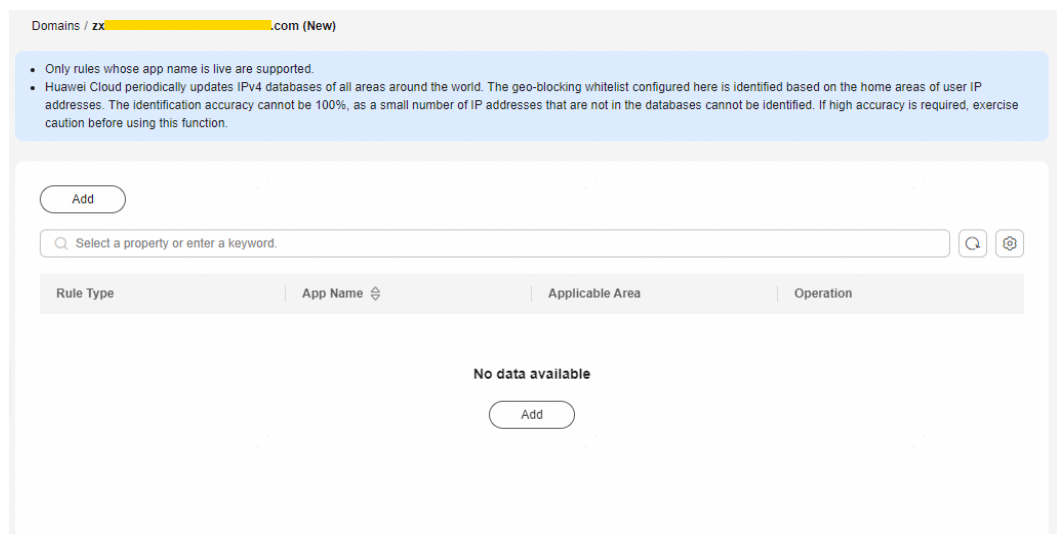
**Step 1** Log in to the [Live console](#).

**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.

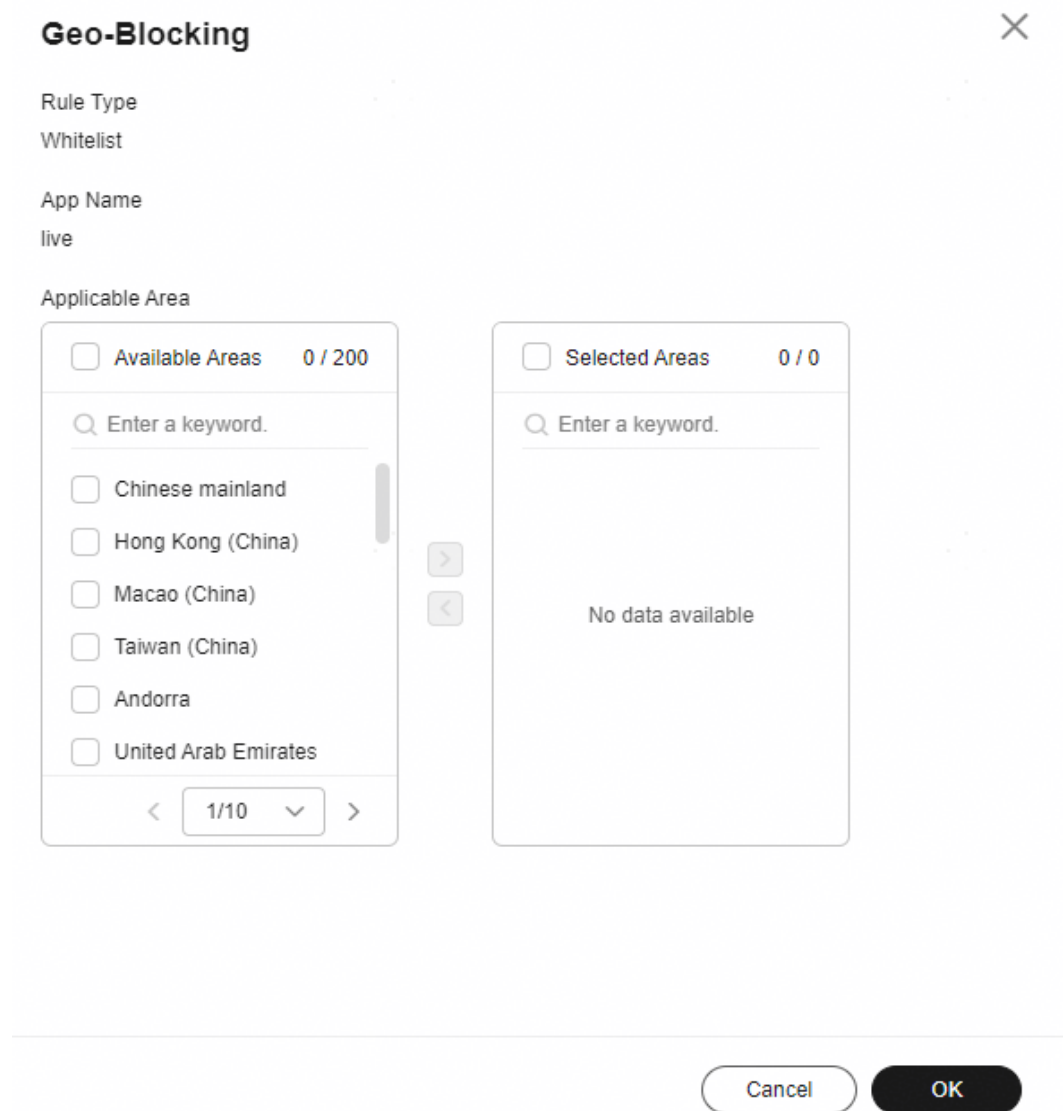
**Step 4** In the navigation pane, choose **Templates > Geo-blocking**, as shown in [Figure 3-45](#).

**Figure 3-45** 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 3-46](#).

**Figure 3-46** 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

# 4 Streaming

## 4.1 Streams

You can view the online streaming status in real time. You can disable a livestream, so its ingest URL cannot be used to push the stream. You can also resume the livestream to allow stream push using the ingest URL.

### Notes

This function is available only in **AP-Singapore** and **CN North-Beijing4**.

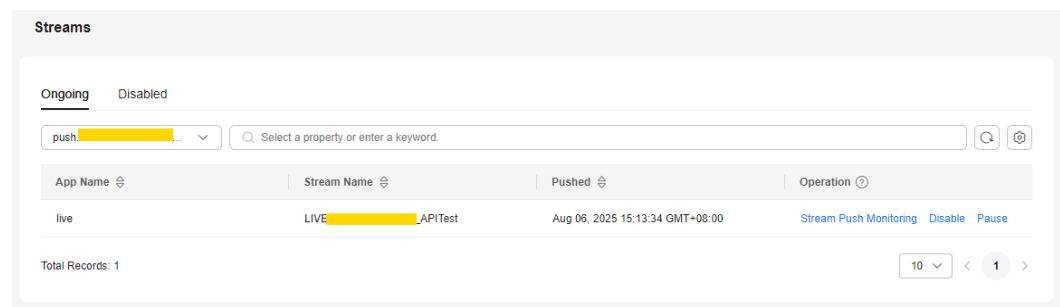
### Viewing Stream Push Information

#### CAUTION

After a livestream is pushed successfully, it takes about 2 to 4 minutes for its information to appear.

- Step 1** Log in to the [Live console](#).
- Step 2** In the navigation pane, choose **Streaming > Streams**.
- Step 3** Select a domain name to view information about a livestream being pushed.

**Figure 4-1** Viewing stream push information



- Step 4** Perform the following operations on the ongoing stream:
- Viewing stream push monitoring information: Click **Stream Push Monitoring** in the **Operation** column of the ongoing stream. On the displayed **Stream Push Monitoring** tab under **Cloud Live > Service Monitoring**, view the charts for frame rate and bitrate of the current stream.
  - Disabling the stream push: When disabling the current stream push, you can preset a time point to resume the stream. For details, see [Disabling Stream Push](#) and [Resuming Stream Push](#).
  - Pausing the stream push: Click **Pause** in the **Operation** column. In the displayed **Warning** dialog box, click **OK**.
- After the ongoing stream is paused, it takes 1 to 3 minutes for the stream to disappear from the **Ongoing** tab.

----End

## Disabling Stream Push

Only a livestream that is being pushed can be disabled. After a livestream is disabled, the ingest URL cannot be used to push livestreams.

To disable a livestream, perform the following operations:

- Step 1** Log in to the [Live console](#).
- Step 2** In the navigation pane, choose **Streaming > Streams**.
- Step 3** Locate the domain name for which stream push is to be disabled.
- Step 4** Click **Disable** in the **Operation** column.

Select the time when stream push is resumed. You can view information about disabled livestreams on the **Disabled** tab.

**Figure 4-2** Configuration of disabling stream push

**Disable** ×

\* App Name

\* Stream Name

Limited duration

Resumed

**Limited duration:** The livestream cannot be pushed until the time indicated by **Resumed** arrives. Livestreams can be disabled for up to 90 days.

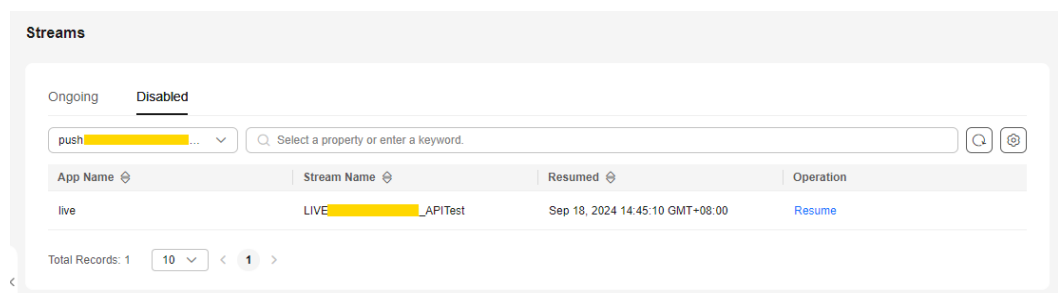
----End

## Resuming Stream Push

To resume stream push for a domain name, perform the following operations:

- Step 1** Log in to the [Live console](#).
- Step 2** In the navigation pane, choose **Streaming > Streams**.
- Step 3** Select the domain name for which stream push needs to be resumed from the drop-down list.
- Step 4** Click the **Disabled** tab.
- Step 5** Click **Resume** in the **Operation** column.

**Figure 4-3** Resuming stream push



----End

## 4.2 Relay

In contrast to traditional cloud livestreaming, which requires dedicated tools to push content, the relay feature lets you pull source streams, whether live feeds or VOD assets for pseudo-live or loop broadcasting, and push them to target URLs. This enables efficient content transmission and distribution.

### Notes

- By default, the **Streaming > Relay** menu is hidden. To access it, you need to [submit a service ticket](#).  
Relay is in the open beta test (OBT) phase and is available for free. Once the OBT ends, billing will apply. The timeline will be announced at a later date.
- When **Source Stream Type** is set to **Video path**, the supported video file container formats are FLV and HLS. If you are using an MP4 file as the source stream, it must have the MOOV metadata located in the file header.

### Creating a Relay Task

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

**Step 2** In the navigation pane, choose **Streaming > Relay**.

**Step 3** Click **Create Relay Task** to open the **Configure Relay Task** dialog box on the right, as shown in **Figure 4-4**.

Configure parameters by referring to **Figure 4-4**.

**Figure 4-4** Creating a relay task

**Configure Relay Task** ✕

Task Region

Execution Time

Event Callback URL (Optional)

HTTP may have security problems. HTTPS is recommended

Source Stream Type  
 Livestream  Video path

Source Stream Addresses

HTTP may have security problems. HTTPS is recommended

Destination Ingest URL

Only RTMP is supported. Format: `rtmp://{domain name}/{application name}/{stream name}` or `rtmp://{domain name}/{application name}/{stream name}?{stream push parameter}`

**Table 4-1** Parameters

Parameter	Description
Task Region	Region where the current task is deployed.

Parameter	Description
Execution Time	Start time and end time of the task. This parameter is mandatory. The start time must be later than the current time, and the end time must be later than the start time.
Event Callback URL (Optional)	Add an event callback address. If this parameter is set, an HTTP/HTTPS message is sent to the event callback address each time the relay task is triggered. HTTPS is more secure than HTTP and is recommended.
Source Stream Type	Source stream type. Available options are: <ul style="list-style-type: none"> <li>• <b>Livestreams:</b> You can pull livestreams and push them to Live origin servers or third-party origin servers.</li> <li>• <b>Video path:</b> You can pull one or more recorded videos and push them to Live origin servers or third-party origin servers. When <b>Source Stream Type</b> is set to <b>Video path</b>, the supported video file container formats are FLV and HLS. If you are using an MP4 file as the source stream, it must have the MOOV metadata located in the file header.</li> </ul>
Source Stream Addresses	If <b>Source Stream Type</b> is set to <b>Livestream</b> , you can configure only one source stream address. If it is set to <b>Video path</b> , you can configure multiple source stream addresses and must also set the number of playbacks. You can add the same source stream address multiple times. Add addresses one by one, or click <b>Batch Add</b> to add them in batches. Separate multiple addresses with line breaks or commas (,). HTTPS is more secure than HTTP and is recommended.
Playbacks	This parameter is available only when <b>Source Stream Type</b> is set to <b>Video path</b> . You can loop the source video indefinitely or specify a fixed number of playbacks.
Destination Ingest URL	Destination ingest URL. Only the RTMP protocol is supported. The format is as follows: <ul style="list-style-type: none"> <li>• <code>rtmp://{Domain name}/{Application name}/{Stream name}</code></li> <li>• <code>rtmp://{Domain name}/{Application name}/{Stream name}?{Streaming parameters}</code></li> </ul>

**Step 4** Click **OK**. The relay task is created.

----End

## Managing a Relay Task

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

**Step 2** In the navigation pane, choose **Streaming > Relay**. The **Relay** page is displayed, as shown in [Figure 4-5](#).

Figure 4-5 Relay page

Task ID	Status	Source Stream Type	Destination Ingest URL	Started	Ended	Operation
e9a239fe-fbf...	Completed	Video path	rtmp://sy09-push...	Feb 26, 2025 19:35:05 GMT+08:00	Feb 27, 2025 22:00:05 GMT+08:00	View Details Start Pause More
dea92a3a-08...	Not started	Livestream	rtmp://192.168.4...	Feb 28, 2025 02:32:02 GMT+08:00	Feb 28, 2025 02:35:02 GMT+08:00	View Details Start Pause More
0f8080df-580...	Not started	Livestream	rtmp://192.168.4...	Feb 28, 2025 02:48:58 GMT+08:00	Feb 28, 2025 02:51:58 GMT+08:00	View Details Start Pause More
7174b129-db...	Not started	Livestream	rtmp://192.168.4...	Feb 28, 2025 04:14:20 GMT+08:00	Feb 28, 2025 04:17:20 GMT+08:00	View Details Start Pause More
bd1b4654-df...	Not started	Livestream	rtmp://192.168.4...	Feb 28, 2025 04:23:59 GMT+08:00	Feb 28, 2025 04:26:59 GMT+08:00	View Details Start Pause More
c8f0b598-74...	Not started	Livestream	rtmp://192.168.4...	Feb 28, 2025 08:25:06 GMT+08:00	Feb 28, 2025 08:28:07 GMT+08:00	View Details Start Pause More
b0689f56-31...	Not started	Livestream	rtmp://192.168.4...	Feb 28, 2025 08:26:47 GMT+08:00	Feb 28, 2025 08:29:47 GMT+08:00	View Details Start Pause More
767fd06e-0a...	Not started	Livestream	rtmp://192.168.4...	Feb 28, 2025 08:39:26 GMT+08:00	Feb 28, 2025 08:42:26 GMT+08:00	View Details Start Pause More
04bce416-85...	Not started	Livestream	rtmp://192.168.4...	Feb 28, 2025 08:40:23 GMT+08:00	Feb 28, 2025 08:43:23 GMT+08:00	View Details Start Pause More
695a716a-01...	Not started	Livestream	rtmp://192.168.4...	Mar 04, 2025 15:01:16 GMT+08:00	Mar 04, 2025 15:04:16 GMT+08:00	View Details Start Pause More

**Step 3** Perform the following operations on a relay task:

- Viewing relay task details: Click **View Details** in the **Operation** column of the relay task. On the **Relay Task Details** page displayed on the right, view all configuration information about the current relay task.
- Starting a task: Click **Start** in the **Operation** column of the relay task. You can start a task only after the task is paused.
- Pausing a task: Click **Pause** in the **Operation** column of the relay task. You can pause a task only when its **Source Stream Type** is set to **Video path** and the task is running.
- Modifying a task: Choose **More > Modify** in the **Operation** column of the relay task to modify the task. You can modify a task only when its **Source Stream Type** is set to **Video path**.
- Viewing task monitoring information: Choose **More > Monitor** in the **Operation** column of the relay task. You can then view line charts for audio frame rate, video frame rate, audio bitrate, and video bitrate.
- Deleting a task: Choose **More > Delete** in the **Operation** column of the relay task to delete the task.

----End

## 4.3 Watermarks

Live's watermarks support the following functions:

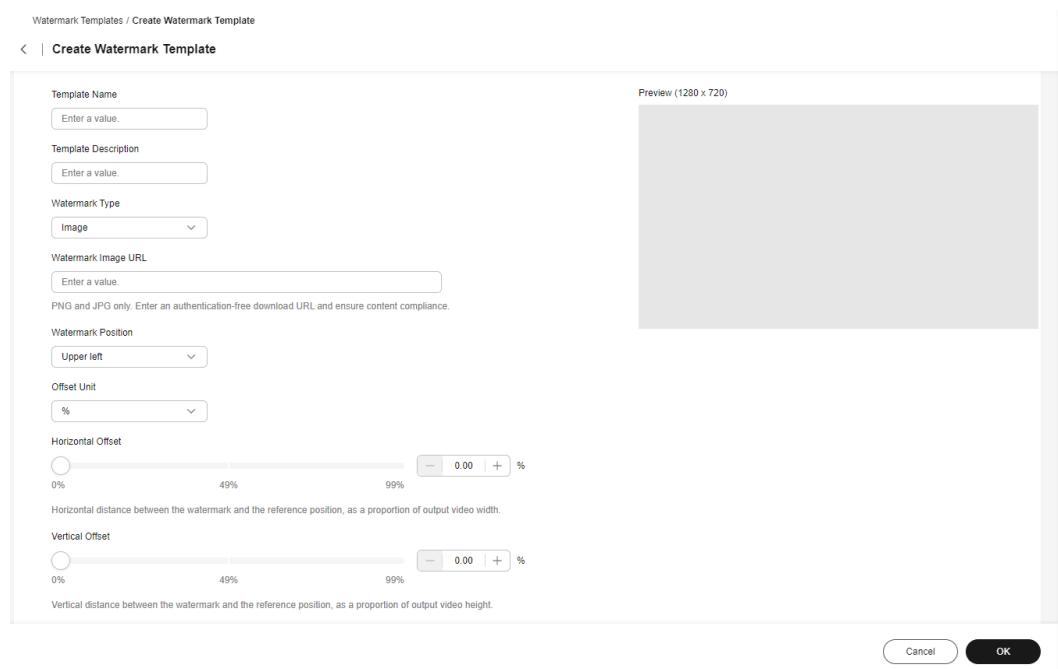
- **Creating a Watermark Template:** You can create an image watermark template.
- **Creating a Watermark Rule:** Cloud Live allows you to bind a watermark template to a specific stream to secure its playback.

## Creating a Watermark Template

- Step 1** Log in to the [Live console](#).
- Step 2** In the navigation pane, choose **Streaming > Watermarks** under **Cloud Live**.
- Step 3** On the **Watermark Templates** tab page, click **Create** to go to the **Create Watermark Template** page, as shown in [Figure 4-6](#).

Configure watermark template parameters by referring to [Table 4-2](#). You can preview the watermark in the area on the right.

**Figure 4-6** Watermark template configuration



**Table 4-2** Watermark template configuration

Parameter	Description
Template Name	(Mandatory) Enter a custom template name.
Template Description	(Optional) Enter the template description.
Watermark Type	Currently, only image watermarks are supported.
Watermark Image URL	(Mandatory) URL of the watermark image. Currently, only PNG and JPG images are supported. Enter an authentication-free download path and ensure the image compliance. Example: <code>https://{IP address}/watermark.png</code>

Parameter	Description
Watermark Position	The options are <b>Upper left</b> , <b>Upper right</b> , <b>Lower left</b> , <b>Lower right</b> , and <b>Random</b> . If you select <b>Random</b> , 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 <b>%</b> and <b>px</b> .
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 (<b>%</b>) or pixel (<b>px</b>).</p> <ul style="list-style-type: none"> <li>If the unit is <b>%</b>, the parameter's value sets the watermark's width and height as a percentage of the output video's width and height.</li> <li>If the unit is <b>px</b>, the watermark's width and height are the specified values (range: 8 to 4,096).</li> </ul> <p>Note:</p> <ul style="list-style-type: none"> <li>If the watermark's width or height is left empty or set to <b>0</b>, the watermark size will be scaled accordingly.</li> <li>If both the watermark's width and height are left empty or set to <b>0</b>, the input and output resolutions are the same.</li> <li>You are advised to set either the width or the height to avoid watermark distortion.</li> </ul>
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

## Creating a Watermark Rule

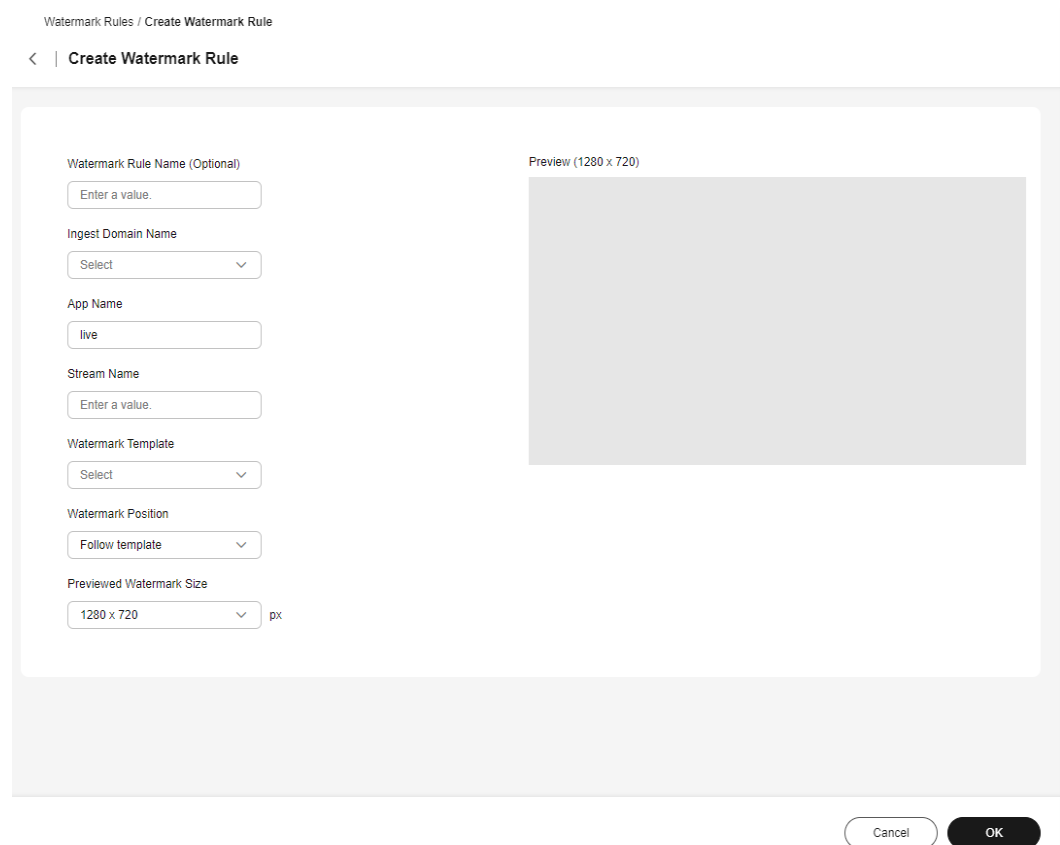
**Step 1** Log in to the [Live console](#).

**Step 2** In the navigation pane, choose **Streaming > Watermarks** under **Cloud Live**.

**Step 3** On the **Watermark Rules** tab page, click **Create** to go to the **Create Watermark Rule** page, as shown in **Figure 4-7**.

Create a watermark rule, as shown in **Table 4-3**. You can preview the watermark in the area on the right.

**Figure 4-7** Watermark rule configuration



**Table 4-3** Watermark rule configuration

Parameter	Description
Watermark Rule Name (Optional)	Enter a watermark rule name. The default value is <i>Ingest domain name:App name:Stream name</i> . The value length ranges from 1 to 255 characters.
Ingest Domain Name	Select the ingest domain name for which you want to set a watermark from the drop-down list.
App Name	(Optional) App name in the ingest URL. The default value is <b>live</b> . If this parameter is left blank, the current watermark rule applies to all applications in the selected ingest domain by default.

Parameter	Description
Stream Name	(Mandatory) Stream name in the ingest URL.
Watermark Template	Select the watermark template created in <a href="#">Creating a Watermark Template</a> from the drop-down list.
Watermark Position	Position of the watermark in the video. Options: <ul style="list-style-type: none"> <li>• <b>Follow template:</b> The watermark's position is determined by the selected watermark template.</li> <li>• <b>Upper left, Upper right, Lower left, Lower right, and Random:</b> Select one of these options to reset the watermark position. If you select <b>Random</b>, the image watermark may appear in the upper left, upper right, lower left, or lower right of the video.</li> </ul>
Offset Unit	Unit of horizontal or vertical offset. The options are <b>%</b> and <b>px</b> .
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

# 5 Usage Statistics

You can check the downstream bandwidth/traffic of all streaming domain names, and the total transcoding duration, maximum number of concurrent recording streams, and number of snapshots of all ingest domain names.

## 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).
- You can query bandwidth/traffic data of the past 24 hours.
- You can query transcoding/recording/snapshot data of the past 90 days. The maximum query time span is 31 days.
- You can click  on each tab to export specific usage statistics to the local PC.

## Procedure

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

**Step 2** In the navigation pane, choose **Usage Statistics**.

**Step 3** View statistics on the **Bandwidth/Traffic**, **Transcoding**, **Recording**, or **Snapshot Capturing** tab.

----End

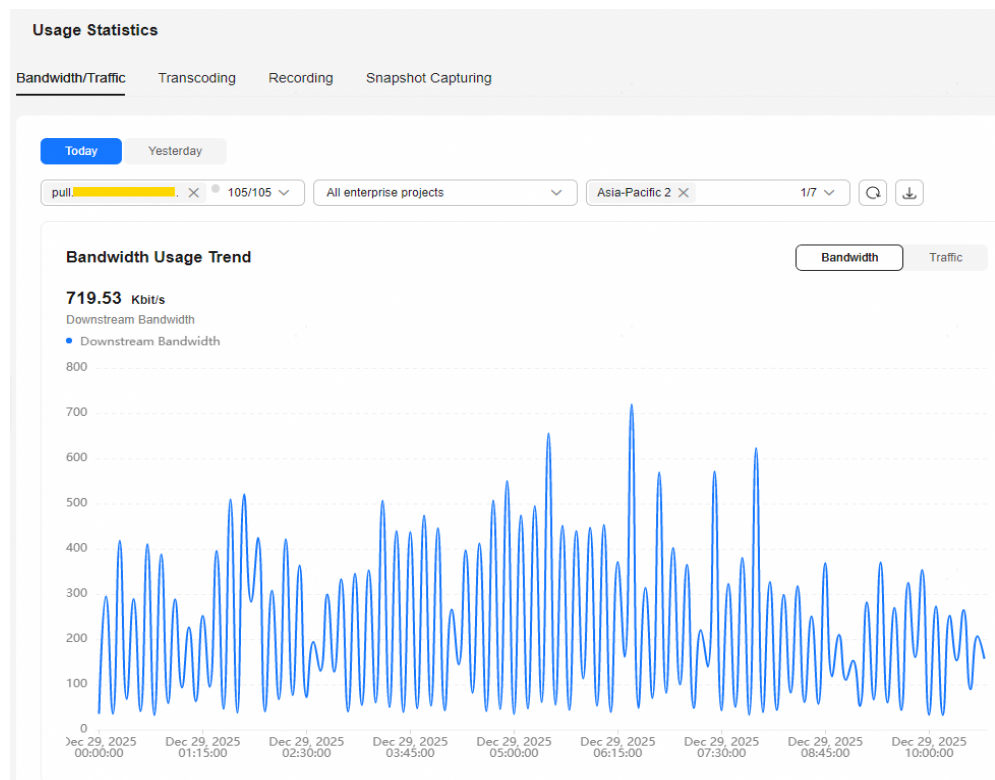
## Bandwidth/Traffic

Specify the time, streaming domain name, and billing region to view data in the **Bandwidth Usage Trend** or **Traffic Usage Trend** area. You can also filter data by enterprise project if you have enabled the Enterprise Project Management (EPS) service.

- **Bandwidth Usage Trend** displays the bandwidth usage trend of the selected domain name.

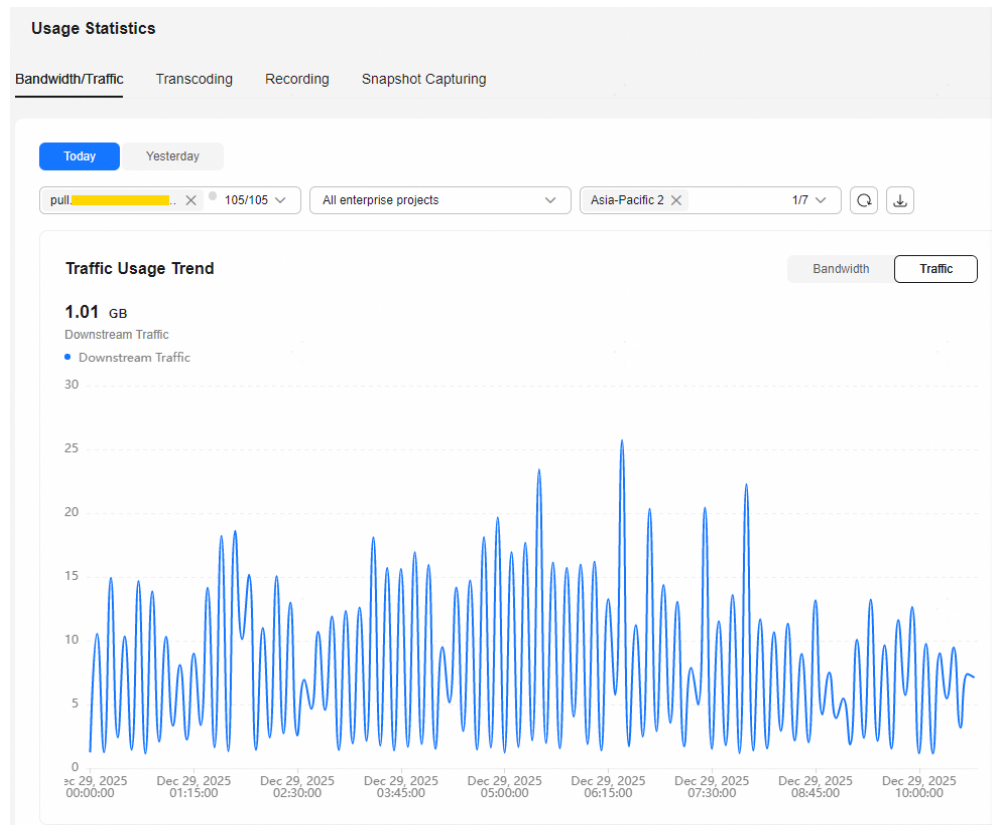
You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

Figure 5-1 Downstream bandwidth trend



- **Traffic Usage Trend** displays the traffic usage trend of the selected domain name.  
You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

Figure 5-2 Downstream traffic details



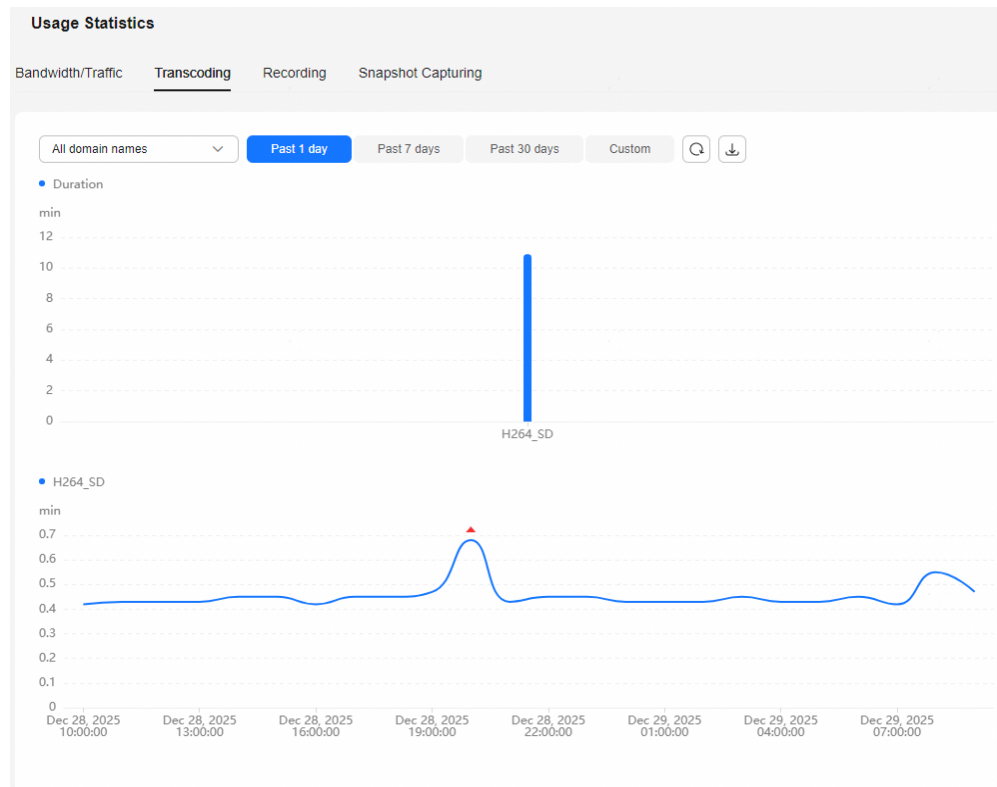
## Transcoding

Specify the time and ingest domain name to view the total transcoding duration and transcoding duration trend.

- **Total Transcoding Duration** displays the total duration of different transcoded outputs of a selected domain name in the query period.
- **Transcoding Duration Trend** displays the total duration of different transcoded outputs of a selected domain name in the query period.

You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

Figure 5-3 Transcoding



## Recording

The system collects statistics on the total number of concurrent recording streams every 5 minutes and obtains 12 values every hour. It then uses the maximum value as the number of concurrent recording streams in the hour.

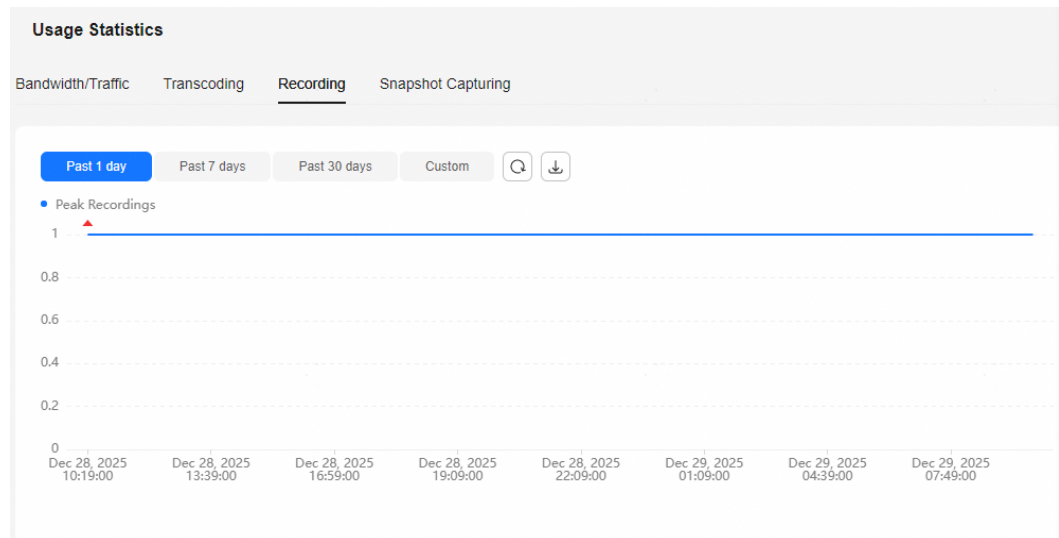
Specify the time to view the peak recording trend.

The peak recording trend area displays the maximum number of recorded concurrent livestreams of an account per hour, as shown in [Figure 5-4](#).

You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

**Figure 5-4** Peak concurrent recording stream trends



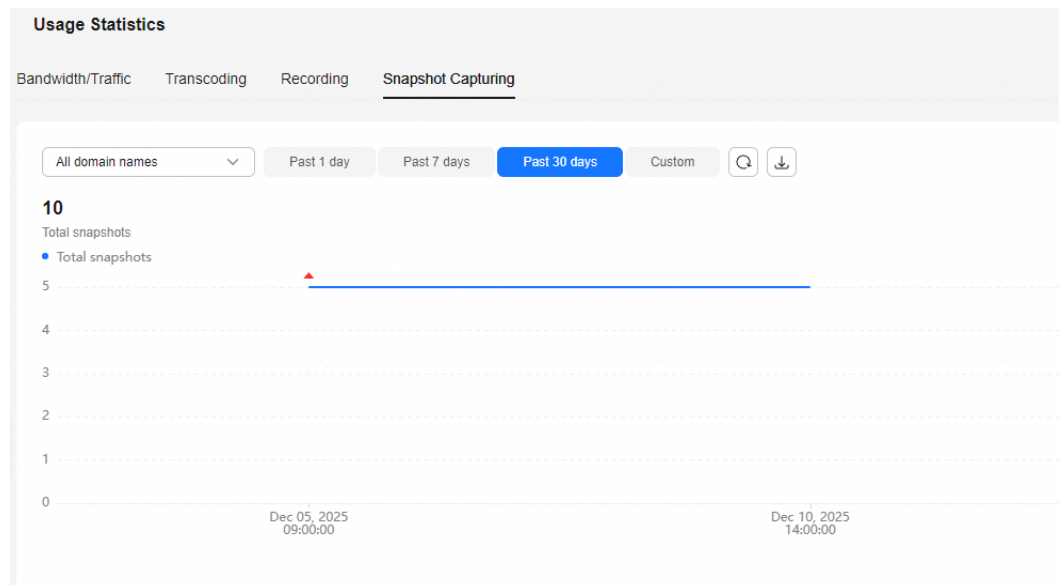
## Snapshot

Specify the time and ingest domain name to view the number of snapshots.

The **Screenshot Trends** area displays the number of snapshots captured for a selected domain name during livestream push, as shown in [Figure 5-5](#).

You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

**Figure 5-5** Snapshot trends



# 6 Service Monitoring

---

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

- **Downstream Bandwidth/Traffic:** downstream bandwidth or traffic usage of a streaming domain name, that is, the downstream bandwidth or traffic used by the client to pull streams from Live
- **Upstream Bandwidth/Traffic:** upstream bandwidth or traffic usage of an ingest domain name, that is, the bandwidth or traffic used by the device to push streams to Live
- **Status Codes:** all status codes returned in response to the stream pull requests, and the change trends of these status codes
- **Viewers:** number of online viewers of a livestream and its change trend
- **Streams:** total number of streams pushed by the selected domain name to the origin server and its change trend
- **Pushed Streams:** details about the historical streams of an ingest domain name, including the stream name, domain name, application name, stream push start time, stream push end time, stream push type, streamer IP address, and audio/video encoding
- **Streaming Records:** stream push disconnection records of the selected domain name
- **Stream Playback Profiles:** information including the total traffic consumed for video playback, accumulated duration of video playback, number of video playback requests, total number of viewers, peak number of viewers, peak bandwidth for video playback, and accumulated duration of stream push
- **Stream Push Monitoring:** frame rates and bitrates of the livestreams (of the selected domain name) pushed to the origin server and their change trends

## 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, choose **Service Monitoring**.


**Step 3** Select **Downstream Bandwidth/Traffic**, **Upstream Bandwidth/Traffic**, **Status Codes**, **Viewers**, **Streams**, **Pushed Streams**, **Streaming Records**, **Stream Playback Profiles**, or **Stream Push Monitoring** to view the corresponding statistics.

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

----End

## Downstream Bandwidth/Traffic

Specify the time, streaming domain name, area, application name, stream name, statistical granularity, and packaging protocol. Click **Bandwidth** or **Traffic** on the right of the page to view the bandwidth or traffic usage trend. You can also filter data by enterprise project if you have enabled the Enterprise Project Management (EPS) service.

You can click  on the right to export specific data.

### NOTE

- You can query statistics of the past 365 days.
- You can query statistics in a time span of up to 31 days.
- The minimum statistical granularity is five 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 bandwidth uses the average value of the selected statistical granularity, and the traffic uses the accumulated value of the selected statistical granularity.
- The stream name is the name of the stream pulled by the player. For example, if the player pulls a transcoded stream, set the stream name to the name of the transcoded stream.
- The exported data cannot be classified by carrier.
- **Bandwidth Usage Trend** displays the bandwidth usage trend of the selected domain name. You can also view the downstream peak bandwidth of the selected domain name within the query period below the **Bandwidth Trends** area, as shown in [Figure 6-1](#).

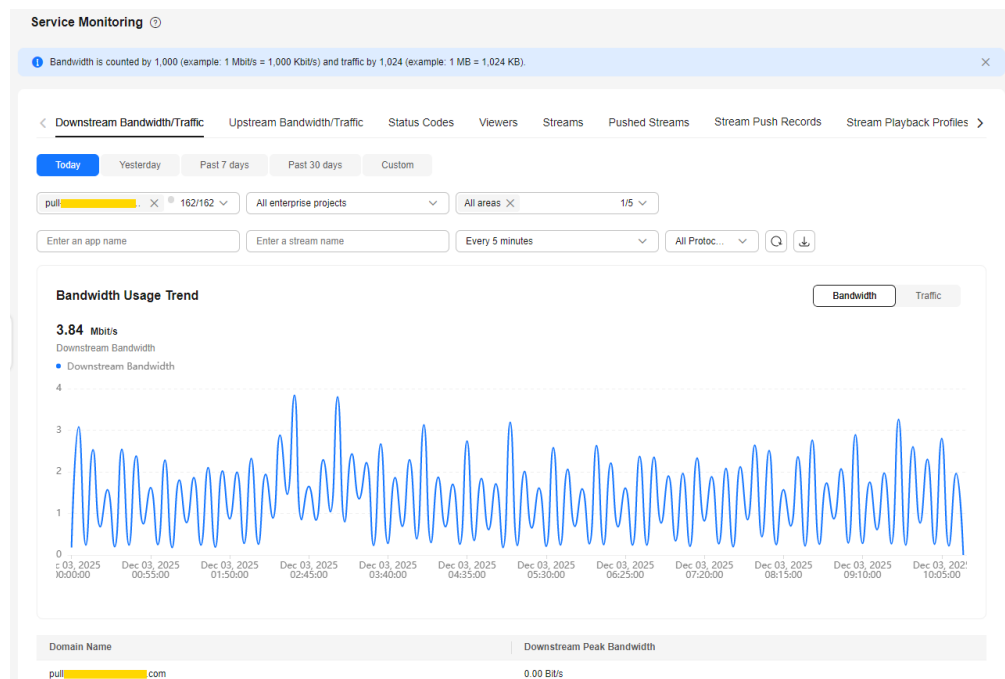
---

### NOTICE

HLS domain names do not support query by application or stream.

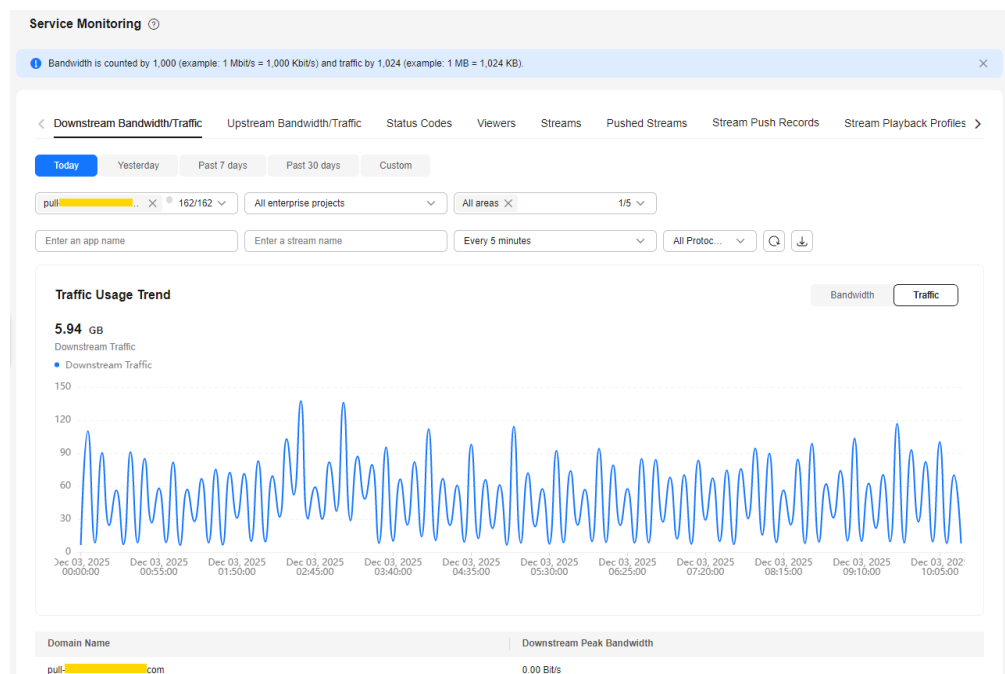
---

Figure 6-1 Downstream bandwidth statistics



- **Traffic Usage Trend** displays the traffic usage trend of the selected domain name. You can also view the traffic data of the selected domain name within the query period below the **Traffic Trends** area, as shown in [Figure 6-2](#).

Figure 6-2 Downstream traffic statistics




**NOTICE**

The total traffic displayed in the traffic table and traffic trend chart is the sum of traffic measured every five minutes and converted from byte into MB, accurate to two decimal places. Therefore, there may be a slight difference from the sum of the values in the **Downlink Traffic Summary** column in the exported traffic statistics table. This is because the values are rounded off during calculation.

## Upstream Bandwidth/Traffic

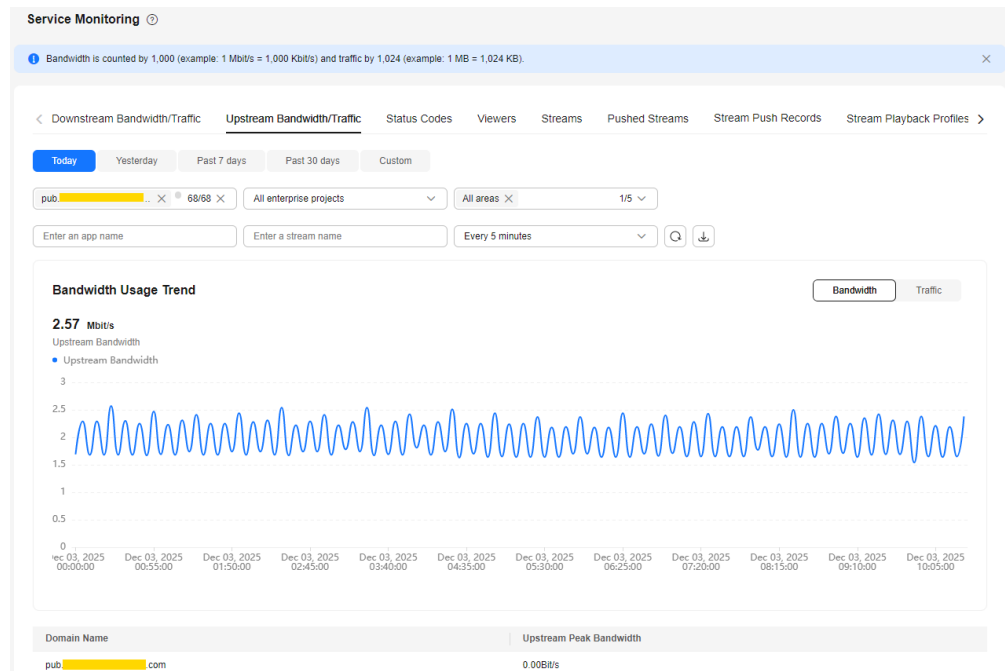
Specify the time, ingest domain name, area, province/state, carrier, app name, stream name, statistical granularity, and packaging protocol. Click **Bandwidth** or **Traffic** on the right of the page to view the bandwidth or traffic usage trend. You can also filter data by enterprise project if you have enabled the Enterprise Project Management (EPS) service.

You can click  on the right to export specific data.

** NOTE**

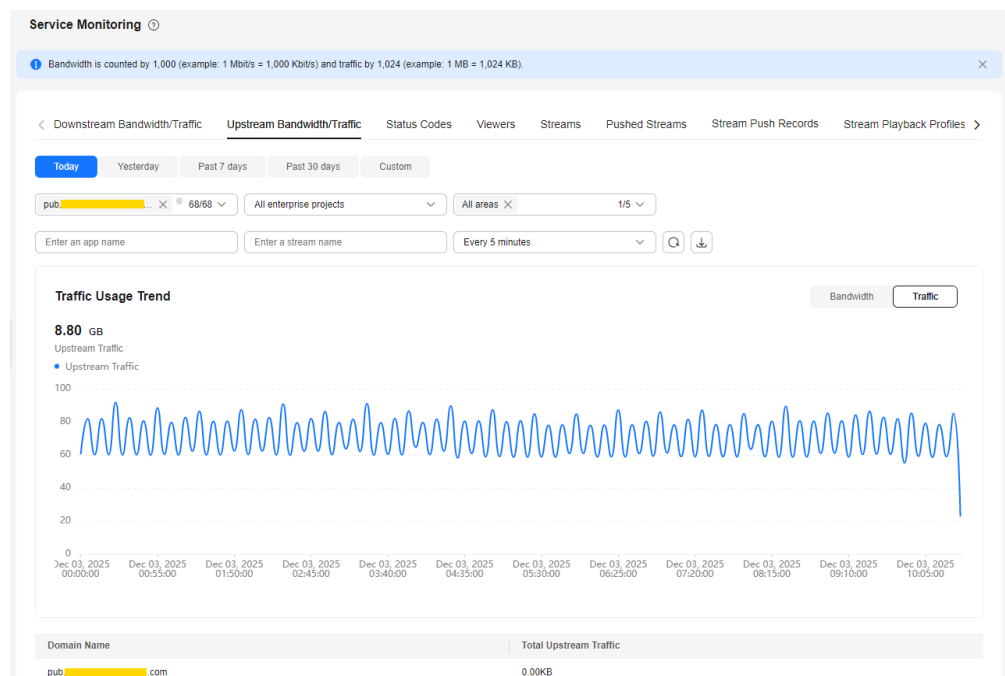
- You can query statistics of the past 365 days.
- You can query statistics in a time span of up to 31 days.
- The minimum statistical granularity is five minutes. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 08:04:59 (GMT+08:00) is displayed at the statistical point November 6, 2020 08:00:00 (GMT+08:00). The bandwidth uses the average value of the selected statistical granularity, and the traffic uses the accumulated value of the selected statistical granularity.
- The exported data cannot be classified by carrier.
- **Bandwidth Usage Trend** displays the upstream bandwidth usage trend of the selected domain name, as shown in [Figure 6-3](#).

Figure 6-3 Upstream bandwidth trend



- **Traffic Usage Trend** displays the traffic usage trend of the selected domain name. You can also view the traffic data of the selected domain name within the query period below the **Traffic Trends** area, as shown in [Figure 6-4](#).

Figure 6-4 Upstream traffic statistics



**NOTICE**

The total traffic displayed in the traffic table and traffic trend chart is the sum of traffic measured every five minutes and converted from byte into MB, accurate to two decimal places. Therefore, there may be a slight difference from the sum of the values in the **Downlink Traffic Summary** column in the exported traffic statistics table. This is because the values are rounded off during calculation.


## Status Codes

Specify the time, domain name, province/state, carrier, and status code, as shown in [Figure 6-5](#). You can also filter data by enterprise project if you have enabled the Enterprise Project Management (EPS) service.

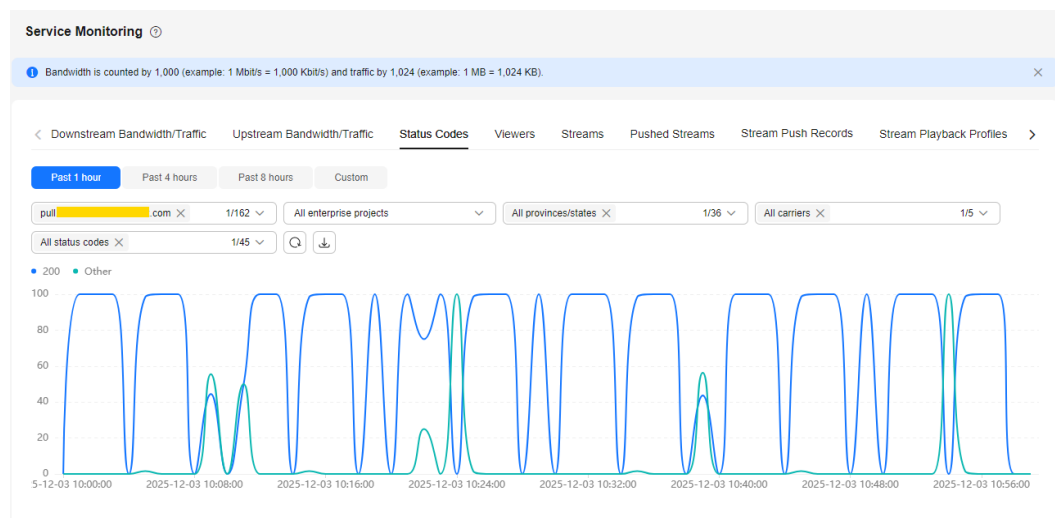
**NOTE**

- You can query statistics of the past seven days.
- You can query statistics in a time span of up to one day.
- You can query statistics about up to 10 domain names at a time.
- The minimum statistical granularity is one 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 trend chart displays the status codes returned for the selected domain name in the query period. For details, see [Status Codes](#).

You can click  on the right to export specific data.

**Figure 6-5** Status code statistics




## Viewers

Specify the time, streaming domain name, app name, stream name, packaging protocol, province/state, carrier, and statistical granularity.

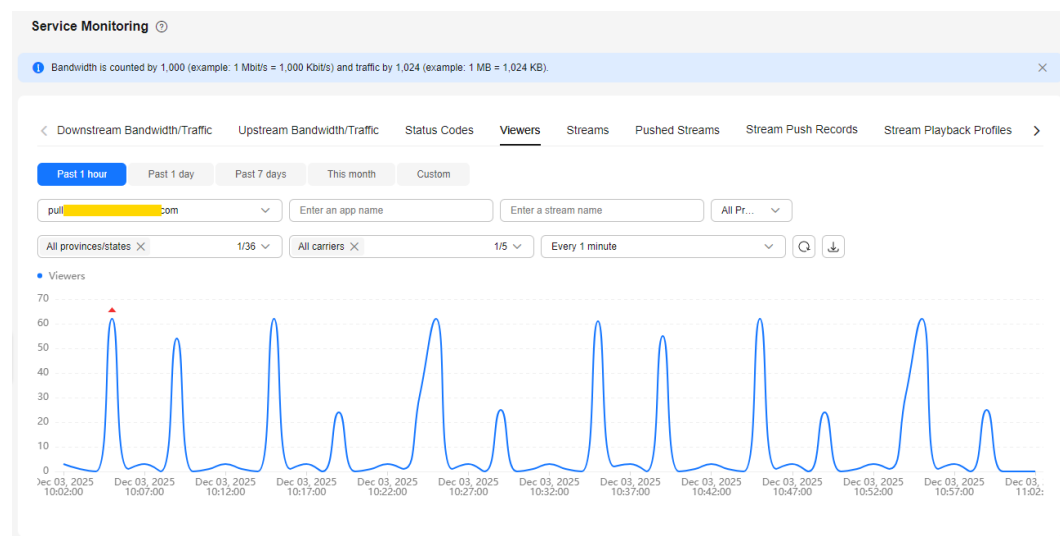
**NOTE**

- Only the number of viewers for FLV and RTMP streams can be queried.
- You can query statistics of the past 365 days.
- You can query statistics in a time span of up to 31 days.
- You can query the number of viewers of only one domain name each time.
- The number of viewers is the number of unique IP addresses. The minimum statistical granularity is one 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 chart displays the changes of the number of online unique viewers for the selected domain name over time, as shown in **Figure 6-6**.

You can click  on the right to export specific data.

**Figure 6-6** Online unique viewer trend




## Streams

Specify the ingest domain name and time. You can also filter data by enterprise project if you have enabled the Enterprise Project Management (EPS) service.

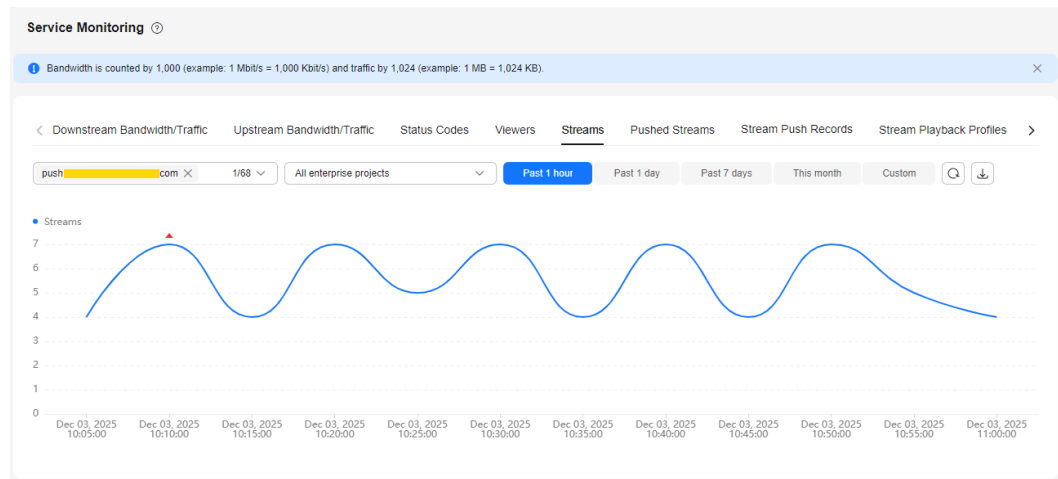
**NOTE**

- You can query statistics of the past 365 days.
- You can query statistics in a time span of up to 31 days.
- You can query statistics about up to 10 domain names at a time.
- The minimum statistical granularity is five 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 of the selected statistical granularity.


The trend chart displays the trend of the total number of streams (of the selected domain name) pushed to the Live origin server, as shown in **Figure 6-7**.

You can click  on the right to export specific data.

**Figure 6-7 Streams**



## Pushed Streams

Specify the time, ingest domain name, app name, and stream name. Click  to view the details about the pushed streams of the ingest domain name, as shown in [Figure 6-8](#).

[Table 6-1](#) describes the parameters. You can click **Export** to export specific data.

### NOTE

- The pushed streams of a domain name that is pushing streams cannot be queried.
- You can query statistics of the past seven days.
- You can query statistics in a time span of up to one day.

Figure 6-8 Pushed stream details

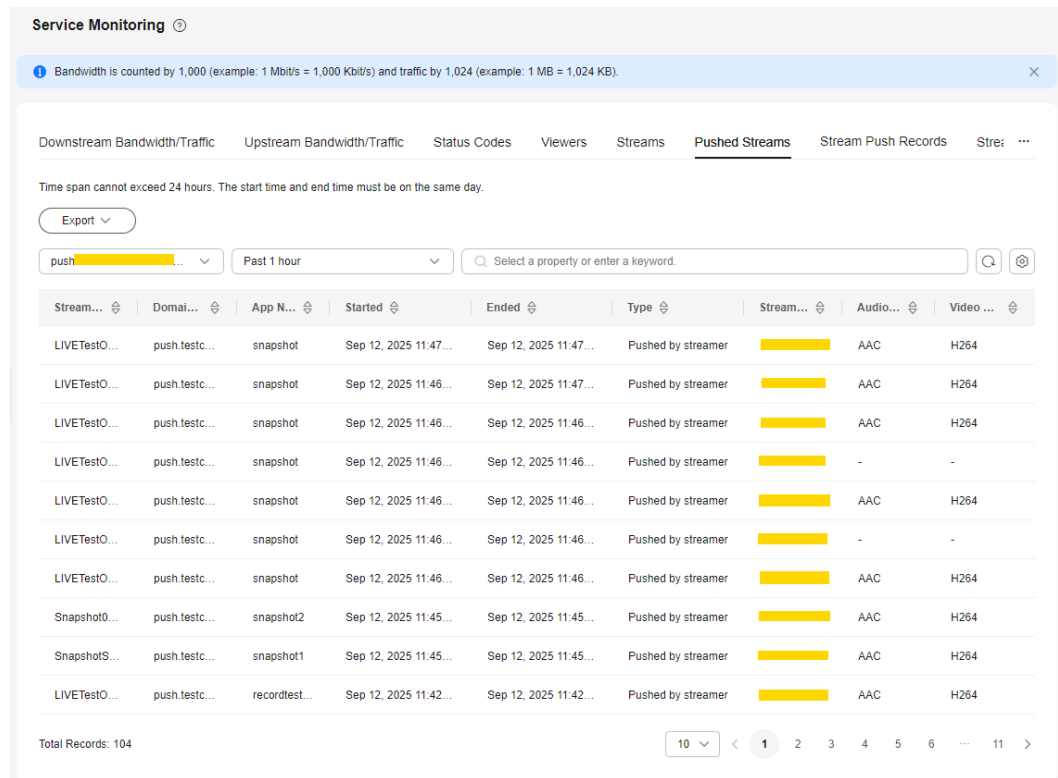




Table 6-1 Parameters

Parameter	Description
Stream Name	Livestream name, that is, the custom value of <b>Stream Name</b> in the ingest URL.
Domain Name	Ingest domain name.
App Name	Application name, that is, the default or custom value of <b>App Name</b> in the ingest URL.
Started	Time when livestream push starts. The format is YYYY-MM-DD hh:mm:ss, for example, 2020-11-06 14:39:42.
Ended	Time when livestream push ends. The format is YYYY-MM-DD hh:mm:ss, for example, 2020-11-06 14:39:44.
Type	Stream push type, which can be <b>Pushed by streamer</b> or <b>Pulled from third-party CDN</b> .
Streamer IP	IP address of the stream push device.
Audio Coding	Audio codec.
Video Coding	Video codec.

## Streaming Records

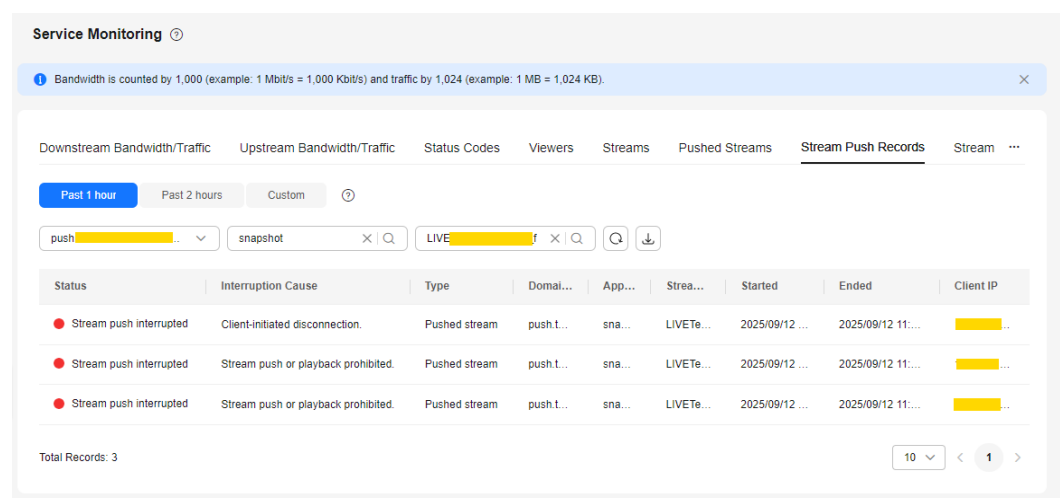
Specify the time, domain name, app name, and stream name. Click  to view the streaming records of the selected domain name, as shown in [Figure 6-9](#).

[Table 6-2](#) describes the parameters. You can click  to export specific data.

### NOTE

Due to a large amount of data, the maximum query period is 3 days, with a maximum time granularity of 3 hours.

**Figure 6-9** Streaming records




**Table 6-2** Parameters

Parameter	Description
Status	Stream status. <ul style="list-style-type: none"> <li>Pushing streams</li> <li>Stream push interrupted</li> </ul>
Interruption Cause	Cause for streaming interruption.
Type	The stream type is <b>Pushed stream</b> .
Domain Name	Ingest domain name.
App Name	Application name, that is, the default or custom value of <b>App Name</b> in the ingest URL.
Stream Name	Stream name, that is, the custom value of <b>Stream Name</b> in the ingest URL.
Started	Time when the stream push starts. The format is YYYY/MM/DD HH:mm:ss.SSS [GMT]Z, for example, 2023-05-16 14:39:42.629 GMT+08:00.

Parameter	Description
Ended	Time when the stream push stops. The format is YYYY/MM/DD HH:mm:ss.SSS [GMT]Z, for example, 2023-05-16 14:39:42.629 GMT+08:00.
Client IP	IP address of the stream push device.

## Stream Playback Profiles

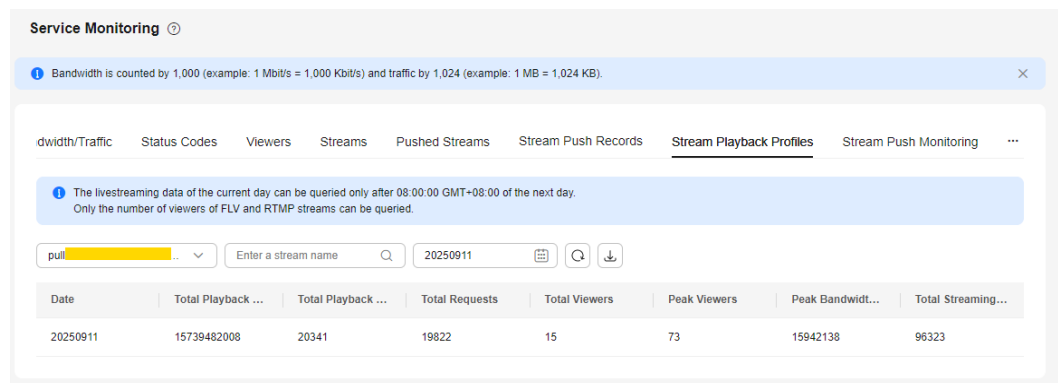
Specify the domain name, stream name, and time, as shown in [Figure 6-10](#).

[Table 6-3](#) describes the parameters. You can click  on the right to export specific data.

### NOTE

- You can query statistics of the past 31 days.
- You can query statistics in a time span of up to one day.
- Query the livestreaming data of the current day after 08:00:00 (GMT+08:00) of the next day.
- Only the number of viewers for FLV and RTMP streams can be queried.

**Figure 6-10** Stream playback profiles



**Table 6-3** Parameters

Parameter	Description
Date	Playback profile information from 00:00 to 23:59 on the selected date is collected. The format is YYYYMMDD, for example, 20201104.
Total Traffic (Byte)	Total traffic consumed during playback.
Total Playback Duration (s)	Total playback duration of a video.

Parameter	Description
Total Requests	Total number of video playback requests.
Total Viewers	Total number of viewers.
Peak Viewers	Peak number of viewers.
Peak Bandwidth (bit/s)	Peak bandwidth consumed during playback.
Total Streaming Duration (s)	Total stream push duration.

## Stream Push Monitoring

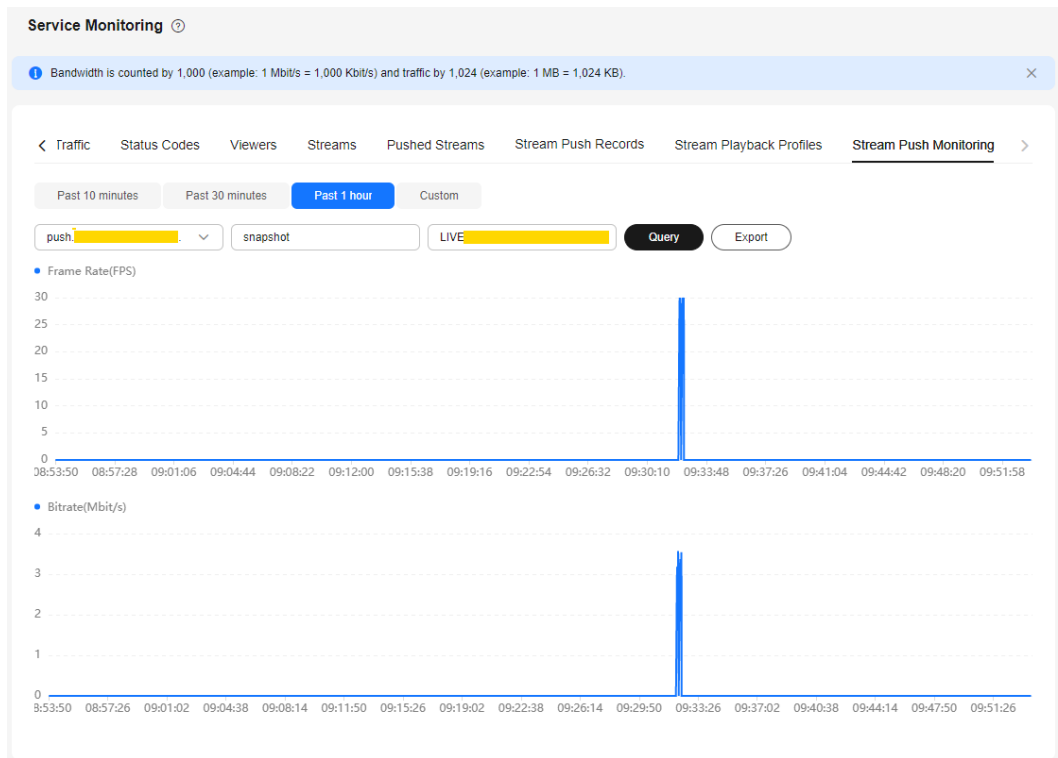
Specify the time, ingest domain name, app name, and stream name. Click **Query**. You can view related data in the **Frame Rate** and **Bitrate** areas.

### NOTE

- You can query statistics of the past seven days.
- There is a 5-minute delay for the latest data to be displayed.
- You can query statistics in a time span of up to 24 hours.

The **Frame Rate** and **Bitrate** areas display the trends of the frame rate and bitrate of livestreams (of the selected domain name) pushed to the origin server. You can click **Export** to export specific data.

Figure 6-11 Stream push monitoring



# 7 LLL Statistics

---

You can view the statistics of the LLL service for streaming domain names. The metrics include the downstream bandwidth/traffic usage, the number of viewers, global stream playbacks, and single-stream playbacks.

## 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, choose **LLL Statistics**.
- Step 3** Select **Downstream Bandwidth/Traffic**, **Viewers**, **Global Streams**, or **Single Stream** to view the statistics of the LLL service.

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

----End

## Downstream Bandwidth/Traffic

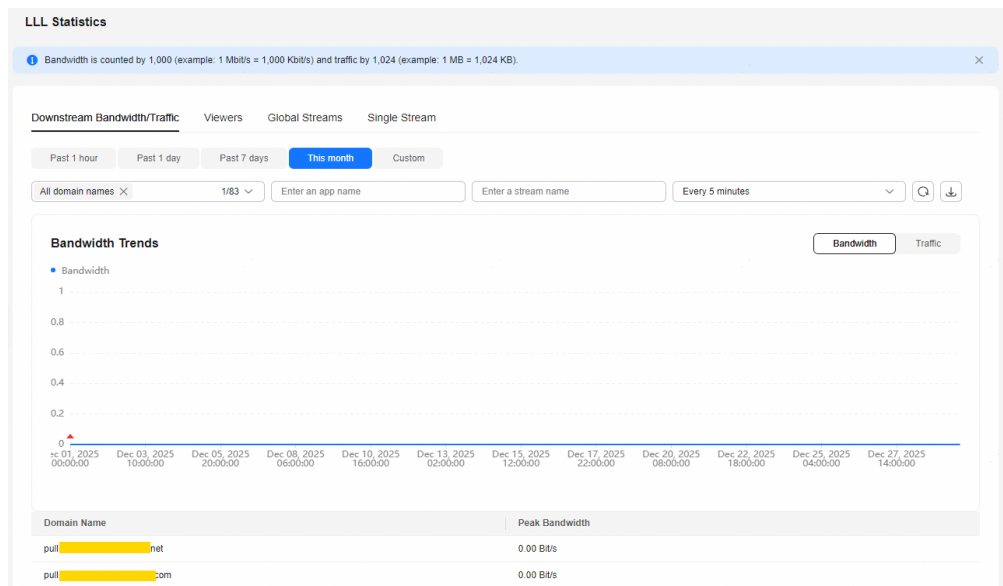
Specify the time, streaming domain name, area, application name, stream name, and statistical granularity. Click **Bandwidth** or **Traffic** on the right of the page to view the specific data.

You can click  on the right to export specific data.

 NOTE

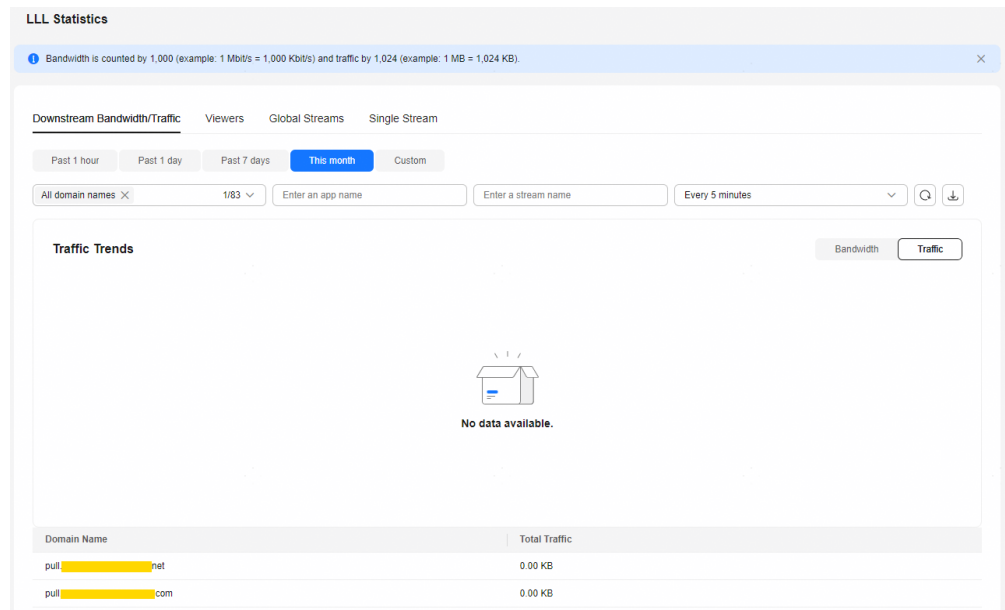
- You can query statistics of the past 365 days.
- You can query statistics in a time span of up to 31 days.
- The minimum statistical granularity is five minutes. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 08:04:59 (GMT+08:00) is displayed at the statistical point November 6, 2020 08:00:00 (GMT+08:00). The bandwidth uses the average value of the selected statistical granularity, and the traffic uses the accumulated value of the selected statistical granularity.
- The stream name is the name of the stream pulled by the player. For example, if the player pulls a transcoded stream, set the stream name to the name of the transcoded stream.
- The exported data cannot be classified by carrier.
- **Bandwidth Trends:** the total bandwidth trend of the selected domain name. You can also view the downstream peak bandwidth of the selected domain name within the query period below the **Bandwidth Trends** area, as shown in [Figure 7-1](#).

**Figure 7-1** Downstream bandwidth statistics



- **Traffic Trends:** the total traffic trend of the selected domain name. You can also view the traffic data of the selected domain name within the query period below the **Traffic Trends** area, as shown in [Figure 7-2](#).

**Figure 7-2** Downstream traffic statistics



**NOTICE**

The total traffic displayed in the traffic table and traffic trend chart is the sum of the LLL service traffic measured every five minutes and converted from byte into MB, accurate to two decimal places. Therefore, there may be a slight difference from the sum of the values in the **Downlink Traffic Summary** column in the exported traffic statistics table. This is because the values are rounded off during calculation.

**Viewers**

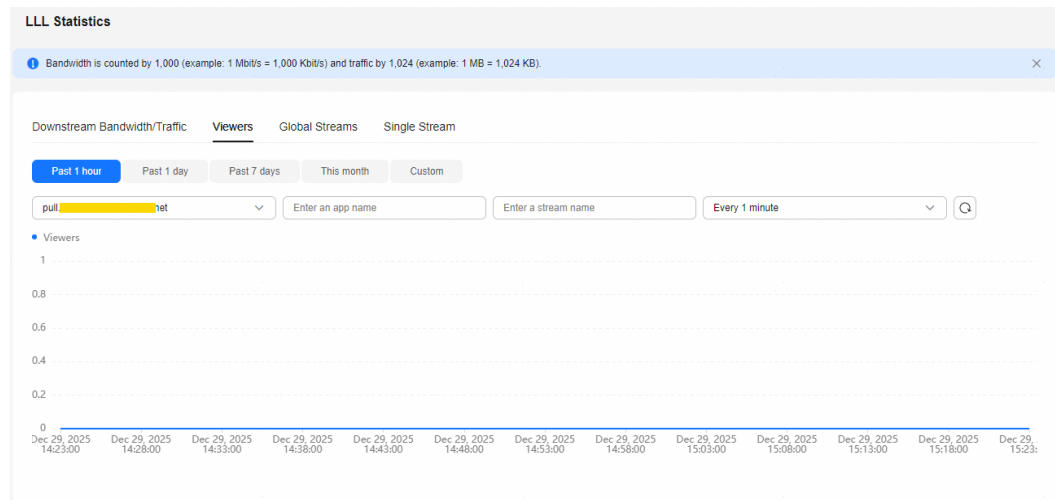
Specify the time, streaming domain name, application name, stream name, and statistical granularity.

**NOTE**

- You can query statistics of the past 365 days.
- You can query statistics in a time span of up to 31 days.
- You can query the number of viewers of only one domain name each time.
- The number of viewers is the number of unique IP addresses. The minimum statistical granularity is one 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 chart displays the changes of the number of online unique viewers for the selected domain name over time, as shown in **Figure 7-3**.

Figure 7-3 Online unique viewer trend



## Global Streams


You can view global playback statistics of LLL streams, including the stream pull success rate, average playback frame rate, average first-screen latency, average frame freezing rate, and CPU usage.

### NOTE

- You can query statistics of the past three days.
- You can query playback statistics on Web, iOS, and Android devices.

## Single Stream

You can view playback statistics of a single LLL stream, including the stream pull success rate, number of online viewers, average first-screen latency, average playback frame rate, average downstream bitrate, average frame freezing rate, and CPU usage.

Specify the time, streaming domain name, area, application name, stream name, and statistical granularity. Then click  to view the playback statistics of a single LLL stream corresponding to the selected streaming domain name.

### NOTE

- You can query statistics of the past 365 days.
- You can query statistics in a time span of up to 31 days.
- The minimum statistical granularity is one 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).
- You can query playback statistics of a single stream on Web, iOS, and Android devices.

# 8 Log Management

## 8.1 Offline Log Download

The offline log page displays detailed logs about the network users' access to all streaming domain names. You can download logs of a specific period to analyze the access to your service resources.

### NOTICE

Log records are for data analysis and reference only. Service fees are charged based on bills.

### Download Rules

- You can download logs of the past 90 days.
- You can query and download logs in a time span of up to seven days. To query and download logs in a longer time span, perform the operations multiple times.

### Log Description

**Log package name format:** *Streaming domain name\_Log generation time.log.gz*

**Log generation rule:** By default, logs are collected at an interval of 5 minutes. If no request is sent to a domain name, no log data package is generated. Generally, the complete log file can be obtained four hours after the livestream pull is completed.

#### Log format

- Cloud Stream Live  
[time\_local]|play\_domain|client\_ip|cdn\_ip|url|http\_code|cache\_hit|scheme|method|period\_bytes\_sent|period\_duration|ua|refer|app|stream
- LLL

[time\_local]|play\_domain|client\_ip|cdn\_ip|url|http\_code|cache\_hit|scheme|method|period\_bytes\_sent|period\_duration|ua|refer|app|stream

 **NOTE**

If a field is not involved or is empty, the value of this field will be a hyphen (-). If the field information contains spaces, each space must be enclosed in double quotation marks ("").

**Log example**

- **Cloud Stream Live**  
[06/Mar/2023:06:51:26 +0800]|pullexample.huaweicloud.com|49.1.1.\*|42.11.1.2|http://pullexample.huaweicloud.com/live/stream-123.flv|200|HIT|HTTP|GET|1024|4|Lavf/58.12.100|-|live|stream-123
- **LLL**  
[06/Mar/2023:06:51:26 +0800]|pullexample.huaweicloud.com|49.1.1.\*|42.11.1.2|webrtc://pullexample.huaweicloud.com/live/stream-123.sdp|200|HIT|WebRTC|GET|1024|4|Lavf/58.12.100|-|live|stream-123

**Table 8-1** describes the fields.

**Table 8-1** Log fields

Field Name	Field Description	Example
time_local	Local time in the common format, which is used to record the time when statistics are collected.	[06/Mar/2023:06:51:26 +0800]
play_domain	Accelerated domain name added to CDN.	pullexample.huaweicloud.com
client_ip	IP address of the client.	49.1.1.*
cdn_ip	IP address of the CDN node accessed by the viewer.	42.11.1.2
url	Complete access URL.	<ul style="list-style-type: none"> <li>• Cloud Stream Live http://pullexample.huaweicloud.com/live/stream-123.flv</li> <li>• LLL webrtc://pullexample.huaweicloud.com/live/stream-123.sdp</li> </ul>
http_code	HTTP status code.	200
cache_hit	Cache hit status. <ul style="list-style-type: none"> <li>• HIT</li> <li>• MISS</li> </ul>	HIT

Field Name	Field Description	Example
scheme	Access protocol. <ul style="list-style-type: none"> <li>• HTTP</li> <li>• HTTPS</li> <li>• RTMP</li> <li>• WebRTC</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud Stream Live: HTTP, HTTPS, or RTMP</li> <li>• LLL: WebRTC</li> </ul>
method	HTTP method.	GET
period_byte_s_sent	Number of bytes sent in a statistical period. The statistical period is the value of <b>period_duration</b> .	1024
period_duration	Statistical period, in seconds.	4
ua	User agent information.	Lavf/58.12.100
refer	Referer information.	-
app	Application name. The default value is <b>live</b> .	live
stream	Stream name	stream-123

## Log Download

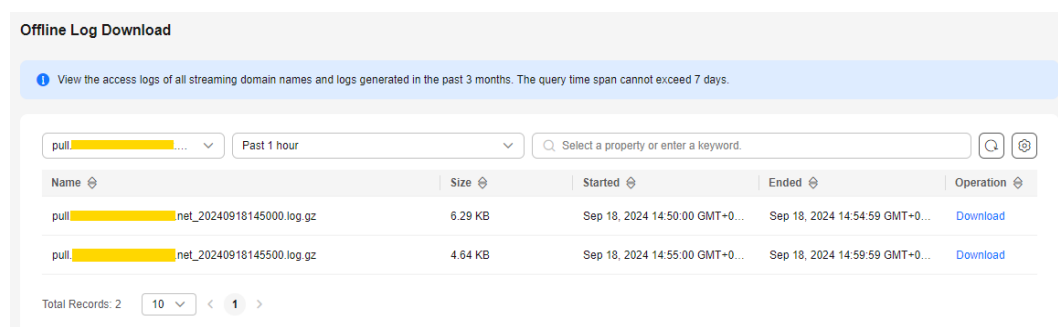
**Step 1** Log in to the [Live console](#).

**Step 2** In the navigation pane, choose **Logs > Offline log download**.

**Step 3** On the displayed page, specify the domain name and time.

The system displays all logs generated in the specified time. A log file is generated every 5 minutes.

**Figure 8-1** Downloading logs



**Step 4** Click **Download** in the **Operation** column of the desired log and download the log to your local PC.

----End

# 9 OBS Authorization

To store recordings and snapshots in OBS buckets, you need to authorize Live to access those buckets.

**CAUTION**

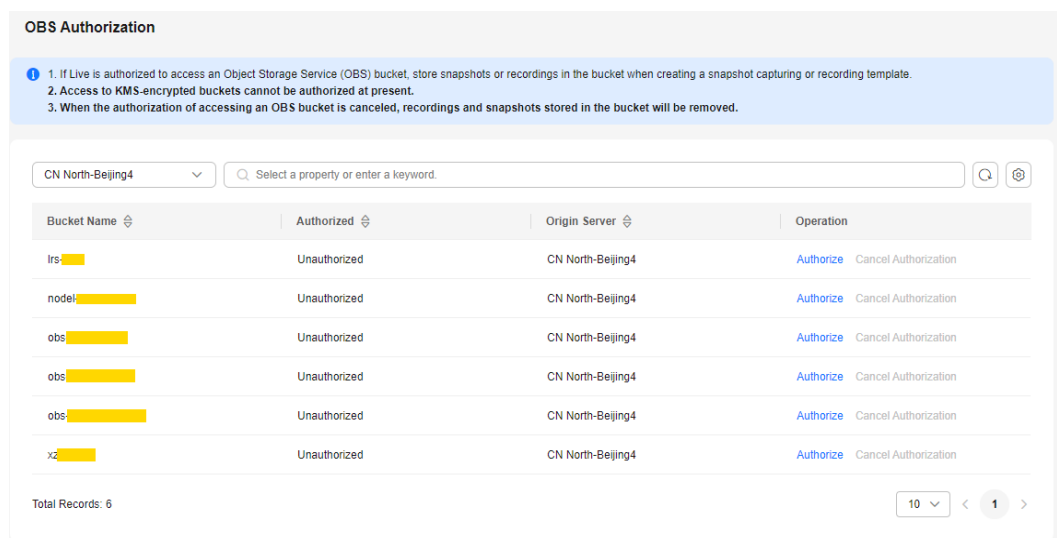
After access to an OBS bucket is authorized, Live can access the OBS bucket. Ensure that the bucket processes only workloads related to Live. Do not store confidential files in the bucket.

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

**Step 2** In the navigation pane, choose **OBS Authorization**.

Find the OBS bucket where recordings and snapshots are to be stored, and click **Authorize** on the right.

**Figure 9-1** OBS authorization



----End

# 10 Tools

---

## 10.1 Signed URL Generation Tool

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

### Notes

- Currently, Live does not support the generation of HLS authentication addresses using the URL validation address generation tool. You can manually assemble an HLS authentication address by referring to [URL Validation](#).

### Prerequisites

You have configured URL validation for your ingest and streaming domain names by referring to [Stream Push Authentication](#) and [URL Validation](#).

### Procedure

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

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

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

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

#### NOTE

To generate a signed streaming URL after transcoding, set **Stream Name** to the value of *Stream Name\_Transcoding template ID*, for example, **huawei01\_1ld**. You can obtain the transcoding template ID on the **Transcoding** page of the Live console.

**Figure 10-1** Generating a signed URL

The screenshot shows the 'URL Signing' configuration page. At the top, there is a light blue notification banner with an information icon and the text: 'Signed URLs can be generated only for domain names deployed on the new version of Live.' Below this, the form is organized into sections:

- Streaming Domain Name:** A dropdown menu currently showing '--Select--'.
- Validation:** A text label that says 'Select a domain name to obtain the URL validation configuration.'
- Ingest Domain Name:** A dropdown menu currently showing '--Select--'.
- Validation:** A text label that says 'Select a domain name to obtain the URL validation configuration.'
- App Name:** A text input field containing the value 'live'. Below the field is a note: 'Default: live. Only letters, digits, underscores (\_), and hyphens (-) are allowed.'
- Stream Name:** A text input field currently showing '--Enter--'.

At the bottom of the form, there is a 'Generate' button and a 'Learn more' link with an external icon.

**Step 4** Click **Generate** to generate signed ingest and streaming URLs.

Signed streaming URLs are provided according to the protocols supported by the streaming domain name.

- If the streaming domain name supports FLV, RTMP, and RTC, signed URLs for these protocols will be generated accordingly.
- If the streaming domain name supports HLS, signed URLs for HLS will not be generated automatically, and the console will display a notification indicating this limitation. To generate a signed URL for the HLS protocol, see [URL Validation](#).

----End

# 11 Cloud Eye Monitoring

## 11.1 Monitoring Metrics

This section describes Live metrics reported to Cloud Eye as well as their namespaces and dimensions. You can use the Cloud Eye console or [APIs](#) to query the Live metrics and alarms.

You can [view metrics](#) on the management console, [configure alarm rules](#) for metrics, and enable SMN to receive notifications. If a metric meets the alarm condition, Cloud Eye notifies you by SMS message, email, HTTP, or HTTPS.

### Namespaces

SYS.LIVE

### Monitoring Metrics

**Table 11-1** Monitoring metrics of online viewers and playback bandwidth

ID	Name	Description	Value Range	Unit	Conversion Rule	Dimension	Monitoring Interval (Raw)
online	Playback concurrency	Number of online viewers of a streaming domain name	$\geq 0$	count	-	Domain	1 minute
bandwidth	Playback bandwidth	Bandwidth data of a streaming domain name	$\geq 0$	bit/s	1000	Domain	1 minute
play_traffic	Playback traffic	Playback traffic of a streaming domain name	$\geq 0$	Byte	1024	Domain	1 minute

ID	Name	Description	Value Range	Unit	Conversion Rule	Dimension	Monitoring Interval (Raw)
qps	QPS	QPS of a streaming domain name	≥ 0	count	-	Domain	1 minute
http_4xx_proportion	4xx status code proportion	Percentage of 4xx status codes of a streaming domain name	0–100%	%	-	Domain	1 minute
http_5xx_proportion	5xx status code proportion	Percentage of 5xx status codes of a streaming domain name	0–100%	%	-	Domain	1 minute
inject_concurrency_number	Injection concurrency	Number of concurrent streams of an ingest domain name	≥ 0	count	-	Domain	1 minute
inject_bandwidth	Injection bandwidth	Streaming bandwidth of an ingest domain name	≥ 0	bit/s	1000	Domain	1 minute


## Dimensions

Key	Value
Domain	Streaming and ingest domain names of Live You can obtain the value by referring to <a href="#">Querying the Original Dimension Values in Server Monitoring</a> .

## 11.2 Creating an Alarm Rule

You can create an alarm rule to customize monitored objects and notification policies, so that you can be well-informed of the status of streaming and ingest domain names.

## Procedure

- Step 1** Log in to [Huawei Cloud console](#). Choose **Service List > Management & Governance > Cloud Eye**.
- Step 2** Click  in the upper left corner of the console and select **AP-Singapore** or **CN North-Beijing4**.
- Step 3** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 4** In the upper right corner of the page, click **Create Alarm Rule**.
- Step 5** Set parameters as prompted.

For more information, see [Creating an Alarm Rule](#). The key parameters are as follows:

- **Name:** The system generates a random name, and you can change it if needed.
- **Alarm Type:** Select **Metric**.
- **Cloud Product:** Select **Live - Domain**.
- **Resource Level:** Select **Specific dimension**.
- **Monitoring Scope:** Select **All resources**, **Resource groups**, or **Specific resources**.

- Step 6** Click **Create**.

After the alarm rule is created, the system automatically notifies you when an alarm is triggered.

----End

## 11.3 Viewing Monitoring Metrics


Cloud Eye monitors the statuses of streaming and ingest domain names. You can view Live metrics on the management console.

### Notes

- To authorize Live console access through a custom policy instead of the system-defined policies **Live FullAccess** and **Live ReadOnlyAccess**, the permission **live:tenant:getTenantInformation** must be included in the custom policy.
- After assigning an IAM user the **Live FullAccess** permission, you need to assign the user the following Cloud Eye permissions to monitor metrics of Live:
  - **CES ReadOnlyAccess:** On the Cloud Eye console, choose **Cloud Service Monitoring > Live** to view resource monitoring metrics of Live.
  - **CES FullAccess:** On the Cloud Eye console, choose **Cloud Service Monitoring > Live** to view resource monitoring metrics of Live and perform operations.

## Procedure

Cloud service dashboards allow you to view cloud service monitoring data. Data of a cloud service is displayed on one monitoring dashboard. A cloud service dashboard is automatically generated and does not need to be configured. You can create a [dashboard](#).

- Step 1** Log in to [Huawei Cloud console](#). Choose **Service List > Management & Governance > Cloud Eye**.
- Step 2** Click  in the upper left corner of the console and select **AP-Singapore** or **CN North-Beijing4**.
- Step 3** In the navigation pane, choose **Cloud Service Monitoring**.
- Step 4** Choose **Live**. The page of cloud service monitoring details is displayed.
- Step 5** On the **Resources** tab, click **View Metric** in the **Operation** column of the desired domain name to view its monitoring metrics.

----End